Universidad Nacional Autónoma de México

Facultad de Ingeniería

Tecnologías para la Seguridad de Redes

T E S I S

Que para obtener el título de:

Ingeniero en Computación

P R E S E N T A:

Jesús Enrique Enriquez Castañeda

Director de Tesis: M. en C. Leobardo Hernández

Ciudad Universitaria, Distrito Federal, Noviembre 2008

Dedicatoria

"No hay palabras que puedan describir mi profundo agradecimiento hacia mis Padres, quienes durante todos estos años confiaron en mí; comprendiendo y apoyando mis ideales en las diferentes etapas de mi vida”

"Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología"

Bruce Schneier

Índice

Índice de Figuras

Prólogo

Cada época se ha caracterizado por algún tipo de tecnología, por ejemplo, en el siglo XVIII se hicieron presentes los sistemas mecánicos, que impulsaron la Revolución Industrial; en el siglo XIX, la máquina de vapor revolucionó los sistemas de transporte principalmente los barcos, automóviles y trenes, permitiendo con esto llegar a lugares jamás imaginados, ahorrando esfuerzo y tiempo. Pero lo que sin duda revolucionó a la humanidad fueron los adelantos del siglo XX, clave en la obtención, procesamiento y distribución de la información.

La aparición de los medios de comunicación revolucionaron la forma de intercambio de la información, la invención de las primeras redes como las telefónicas, la aparición de la radio y la televisión, el nacimiento y desarrollo sin precedentes de la industria de la computación. Jamás en la historia de la humanidad algo se había apoderado tan rápido de ella, además de hacer a todos dependientes de ella.

Este crecimiento exponencial se debe a la unión de las computadoras y las comunicaciones, que causó gran impacto en la humanidad. La aparición de redes como Internet creó nuevas formas de intercambiar información. En principio parecían inofensivas, pero hoy, al ser tan dependientes de ellas, es cuando la seguridad ha tomado un papel importantísimo, para cualquier persona, organización o gobierno.

Existe mucha información, tanto en libros, revistas, Internet, como en publicaciones de investigación y empresas que venden herramientas de seguridad, relacionada con la protección de redes de comunicaciones. Muchas veces resulta complicado para las organizaciones, estudiantes y especialista en seguridad, consultar todas estas fuentes de manera rápida y confiable.

Es por eso que surge la necesidad de recopilar en un solo documento las características, clasificación, beneficios y debilidades de las diferentes tecnologías de seguridad en redes existentes. Tecnologías como firewalls[1], IDS[2]*(Intrusion Detection System)*, IPS[3]*(Intrusion Prevention System)*, honeypots[4], detectores de vulnerabilidades y buscadores de redes, que son necesarias para salvaguardar una red.

---

[1] *Firewalls*, conocidos en español como cortafuegos, son elementos de hardware o software utilizados en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

[2] *IDS* (Intrusion Detection System), conocidos en español como Sistemas de Detección de Intrusos, es un hardware o software usado para detectar accesos no autorizados a una computadora o a una red.

[3] *IPS* (Intrusion Prevention System), conocidos en español como Sistemas de Prevención de Intrusos, es un hardware o software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Este trabajo está integrado por 6 capítulos, cuyo contenido se describe a continuación. El Capítulo 1 “Introducción a la Seguridad de la Información y Seguridad de Redes” trata todo el marco teórico necesario para poder entender los conceptos que se utilizaran para fundamentar los capítulos posteriores. El Capítulo 2 “Principales métodos de ataques” contiene una clasificación de las metodologías más comunes de ataques existentes, definiendo puntualmente las características de cada una. El capítulo 3 “Firewalls y Honeypots” , se tratan dos herramientas especificas para el manejo de la información, que operan en conjunto con la red para proteger tanto para proteger los sistemas de quien lo implementa como para los sistemas de otras organizaciones en la Internet. El capítulo 4 “Escaneo de Vulnerabilidades” se describen las técnicas usadas para obtener información de un sistema u organización, realizar el mapeo de una red y escaneos de vulnerabilidades. El capítulo 5 “IDS” examina como los IDS basados en host y los IDS basados en red trabajan y como estas herramientas pueden beneficiar a la organización identificando amenazas y ataques en contra de sus sistemas y redes. En el capítulo 6 “IPS”, por ser una tecnología en expansión, se identificarán los diferentes tipos de HIPS que existen y cuáles son sus ventajas y desventajas.

Espero además, que este trabajo pueda servir como referencia para futuras investigaciones, sobre seguridad, así como para los estudiantes y personas interesadas legítimamente en ampliar sus conocimientos sobre seguridad de redes.

[4] *Honeypots*, es un software o conjunto de computadoras cuya intención es atraer atacantes, simulando ser sistemas vulnerables o débiles a los ataques.

Capítulo 1. Introducción a la Seguridad de la Información y Seguridad de Redes

El término seguridad en los últimos años ha sido ampliamente utilizado en cuestiones de Información. En la actualidad el activo más grande de corporaciones y de gobiernos es la información, esta abarca una amplia gama de posibilidades incluyendo: datos de computadoras, estrategias de marketing, expedientes personales, estrategias militares, datos financieros, comunicaciones, planes empresariales, etc. Las organizaciones que valoran la información saben que es algo crucial en su crecimiento, además de ser una herramienta que les permitirá ser competitivos.

No basta únicamente con poseer la información, también debe ser compartida, por ello es necesario medios que permitan su fácil envió y recepción. Es entonces, cuando herramientas como las redes de computadoras, por ejemplo Internet, toman un papel importante en este intercambio.

Al intercambiar información, a través de redes de computadoras, surge un gran problema, garantizar la seguridad de la información, una tarea muy difícil de lograr, por ello, se deben implementar mecanismos de seguridad que protejan el medio y a su vez lo que viaja en él.

En este capítulo se definen los conceptos básicos de seguridad de la información y seguridad de redes que permiten entender claramente cómo es que cada herramienta de seguridad puede ayudar a proteger a una organización o simplemente equipos de cómputo.

1.1 Seguridad de la Información

Podemos considerar que la Información es un:

"Conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. De esta manera, si por ejemplo organizamos datos sobre los inicios de un país y escribimos por ejemplo, el capítulo de un libro, podemos decir que ése constituye información sobre ese país. Cuando tenemos que resolver un determinado problema o tenemos que tomar una decisión, empleamos diferentes fuentes de información y construimos lo que en general se denomina conocimiento o información organizada que permite la resolución de problemas o la toma de decisiones" [53]

Actualmente, en los sistemas de información recae el funcionamiento de las empresas, el cumplimiento de sus objetivos y su misión como organización, debido a que ayuda a mejorar procesos, reducir tiempo y descentralizar tareas.

El ser humano siempre ha tratado de resguardar la información de diferentes maneras tan variadas como su imaginación se lo permite. El motivo de este resguardo es el valor que puede tener para él u otra persona. La invención de técnicas de resguardo se desarrolla principalmente en conflictos bélicos, que es cuando la información juega un papel crucial en la obtención de la victoria.

El término Seguridad de la Información se refiere a los procesos y metodologías que están diseñados y se implementan para proteger principalmente la integridad, disponibilidad y confidencialidad de la información contenida en una hoja de papel, medio electrónico o cualquier otra forma en donde se pueda guardar y proteger de usuarios no autorizados.

La seguridad de la información tiene la premisa de proteger a ésta, de diferentes tipos de amenazas[1], con la finalidad de garantizar por ejemplo, en una organización, la continuidad de los negocios, minimizar el daño como consecuencia de una vulnerabilidad[2], así como, la puesta en marcha de las operaciones si algo llegara a pasar.

1.1.2 Servicios de seguridad

La misión de la seguridad de la información es proveer de características como confidencialidad, integridad y autenticidad a la información en cada uno de los estados que se encuentre, es decir, prevenir durante estos procesos que esta se comprometa y además que sea accesible cuando se requiera por los usuarios legítimos. Estas características son mejor conocidas como servicios de seguridad y se describirán a continuación [6]:

[1] *Amenaza.* Es la forma en que un atacante podría intentar afectar a un activo mediante una vulnerabilidad.
[2] *Vulnerabilidad*. hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

- **Confidencialidad.** Característica de la seguridad de la información, se entiende como permitir o denegar el acceso a determinada información, es decir, sobre cuáles activos del sistema se otorgan o conceden accesos y sobre quién o qué recaerá la facultad de autorizar o no el acceso.

- **Disponibilidad.** Se aplica a los datos y recursos como: la presencia de datos y recursos en forma usable, la capacidad de responder a necesidades y la respuesta en tiempo.

- **Integridad.** Protege a los activos del sistema contra modificaciones, alteraciones, borrado e inserción.

- **Autenticidad.** Se refiere a la certeza, de una manera no controversial y responsable, del origen de los datos, es decir, desechar la posibilidad de haber suplantado el origen.

- **Control de acceso**. Protege a los archivos del sistema contra accesos y usos no autorizados.

- **No repudio**. Proporciona protección contra la posibilidad de que alguna de las partes involucradas en una comunicación niegue haber enviado o recibido un mensaje.

1.1.3 Mecanismos de seguridad

Los mecanismos de seguridad permiten implementar los servicios de seguridad. Un servicio de seguridad puede utilizar uno o varios mecanismos de seguridad. Se debe tener en claro que ningún mecanismo de seguridad por si sólo podrá implementar todos los servicios de seguridad, normalmente éstos, trabajan en conjunto para cumplir con los requerimientos de seguridad de la información.

Los mecanismos de seguridad más comunes son:

- **Cifrado.** Garantiza que la información no sea legible para usuarios no autorizados, esto lo logra mediante un proceso de cifrado, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave para cifrar y descifrar, se dice que se utiliza un sistema simétrico. Por el contario, cuando se emplea una llave para cifrar y otra diferente para descifrar se le considera un sistema asimétrico. El cifrado proporciona la confidencialidad de la información de datos o del tráfico.

- **Control de Acceso.** Implementación de puntos de división físicos o lógicos para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red. Se pueden basar en conocimiento, posesión o alguna característica particular del usuario.

- **Firma digital.** La firma digital representa un rasgo distintivo del firmante, ya que es infalsificable, no reusable, inalterable y no repudiable. Se basa en las características de la firma autógrafa, pero aplicada en una forma digital.

- **Integridad de datos.** Este mecanismo implica el cifrado de una cadena de datos a transmitir. Este cifrado se adjunta a la información que se quiere enviar. El receptor repite el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

- **Intercambio de autenticación**. se trata de corroborar la identidad ya sea del receptor o emisor, para que de alguna manera se corrobore que es quien dice ser.

- **Tráfico de Relleno**. Se utilizan métodos para proteger a la información en contra de un análisis de tráfico.

1.2 Seguridad de Redes

Definiremos a una red de computadoras, como un conjunto de equipos autónomos, conectados entre sí a través de cables, señales, ondas o cualquier tipo de transporte de datos que compartan entre sí información, recursos y servicios.

Las redes de computadoras se han convertido en una herramienta primordial para el intercambio de información. Es imposible imaginar el mundo en que vivimos sin estar interconectado de manera directa o indirecta a algún medio de información, es por eso que salvaguardar este medio ha tomado una gran relevancia.

La seguridad de redes es el componente más importante en la seguridad de la información porque es la responsable de resguardar la información que pasa a través de los diferentes equipos de cómputo. Seguridad de redes se refiere a todo el hardware y software, funciones, características, procedimientos y políticas que son requeridas para proveer un nivel aceptable de su seguridad a la información de una red. Para que la seguridad de redes cumpla su cometido deberá considerar las siguientes tres características: primero, una red segura deberá garantizar la integridad de toda la información que es almacenada y que pasa por ella, evitando cualquier tipo de modificación; segundo, para hacer segura una red ésta debe brindar confidencialidad, o bien, la opción de compartir información sólo con personas que puedan ser identificadas claramente; tercero, una red segura requiere disponibilidad de la información en todo momento. Estos tres principios son los que se deben cumplir para que una red sea considerada segura.

1.2.1 Modelo OSI

En 1977, la Organización Internacional de Estándares (ISO), integrada por industrias representativas del medio, creó un subcomité para desarrollar estándares de comunicación de datos que promovieran la accesibilidad universal y una interoperabilidad entre productos de diferentes fabricantes.[3]

El resultado de estos esfuerzos es el Modelo de Referencia Interconexión de Sistemas Abiertos (OSI).

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI.

El Modelo OSI nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.

Estos equipos presentan diferencias en:

- Procesador Central.
- Velocidad.
- Memoria.
- Dispositivos de Almacenamiento.
- Interfaces para Comunicaciones.

- Códigos de caracteres.
- Sistemas Operativos.

Estas diferencias propician que el problema de comunicación entre computadoras no tenga una solución simple. Dividiendo el problema general de la comunicación, en problemas específicos, facilitamos la obtención de una solución a dicho problema.

Estructura del Modelo OSI

El objetivo perseguido por OSI establece una estructura que presenta las siguientes particularidades:

Estructura multinivel: Se diseñó una estructura multinivel con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación. Esto es, cada nivel ejecuta funciones especificas.

El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora. La comunicación internivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1.

Puntos de acceso: Entre los diferentes niveles existen interfaces llamadas "puntos de acceso" a los servicios.

Dependencias de Niveles: Cada nivel es dependiente del nivel inferior y también del superior.

Encabezados: En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información. Cualquier nivel dado, puede incorporar un encabezado al mensaje. Por esta razón, se considera que un mensaje esta constituido de dos partes: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso. Sin embargo, como la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

El modelo consta de siete capas que son (ver figura 1):

7	APLICACIÓN	Se entiende directamente con el usuario final, al proporcionarle el servicio de información distribuida para soportar las aplicaciones y administrar las comunicaciones por parte de la capa de presentación.
6	PRESENTACIÓN	Permite a la capa de aplicación interpretar el significado de la información que se intercambia. Ésta realiza las conversiones de formato mediante las que se logra la comunicación de dispositivos.
5	SESIÓN	Administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación, flujo de datos y conclusión de la conexión.
4	TRANSPORTE	Esta capa proporciona el control de extremo a extremo y el intercambio de información con el nivel que requiere el usuario. Representa el corazón de la jerarquía de los protocolos que permite realizar el transporte de los datos en forma segura y económica.
3	RED	Proporciona los medios para establecer, mantener y concluir las conexiones conmutadas entre los sistemas del usuario final. Por lo tanto, la capa de red es la más baja, que se ocupa de la transmisión de extremo a extremo.
2	ENLACE	Asegura con confiabilidad del medio de transmisión, ya que realiza la verificación de errores, retransmisión, control fuera del flujo y la secuenciación de las capacidades que se utilizan en la capa de red.
1	FISICO	Se encarga de las características eléctricas, mecánicas, funcionales y de procedimiento que se requieren para mover los bits de datos entre cada extremo del enlace de la comunicación.

Figura 1. Modelo OSI

1.2.2 Modelo TCP/IP[3] (Transmission Control Protocol/Internet Protocol)

TCP/IP (Transmission Control Protocol/Internet Protocol) es un conjunto protocolos que proviene de los nombres de dos protocolos importantes: el protocolo TCP y del protocolo IP.

En algunos aspectos, TCP/IP representa todas las reglas de comunicación para Internet y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos. Debido a que el conjunto de protocolos TCP/IP originalmente se creó con fines militares, está diseñado para cumplir con una cierta cantidad de criterios, entre ellos:

- dividir mensajes en paquetes;
- usar un sistema de direcciones;
- enrutar datos por la red;
- detectar errores en las transmisiones de datos.

[3] *TCP/IP* (Transmission Control Protocol/Internet Protocol), conocido en español como Protocolo de Control de Transmisión (TCP) y Protocolo de Internet

El conocimiento del conjunto de protocolos TCP/IP no es esencial para un simple usuario, de la misma manera que un espectador no necesita saber cómo funciona su red audiovisual o de televisión. Sin embargo, para las personas que desean administrar o brindar soporte técnico a una red TCP/IP, su conocimiento es fundamental[1].

En general, TCP/IP relaciona dos nociones:

- la noción de estándar: TCP/IP representa la manera en la que se realizan las comunicaciones en una red;

- la noción de implementación: la designación TCP/IP generalmente se extiende a software basado en el protocolo TCP/IP. En realidad, TCP/IP es un modelo cuya aplicación de red utilizan los desarrolladores. Las aplicaciones son, por lo tanto, implementaciones del protocolo TCP/IP.

Para poder aplicar el modelo TCP/IP en cualquier equipo, es decir, independientemente del sistema operativo, el sistema de protocolos TCP/IP se ha dividido en diversos módulos. Cada uno de éstos realiza una tarea específica. Además, estos módulos realizan sus tareas uno después del otro en un orden específico, es decir que existe un sistema estratificado. Ésta es la razón por la cual se habla de modelo de capas[54].

El término capa se utiliza para reflejar el hecho de que los datos que viajan por la red atraviesan distintos niveles de protocolos. Por lo tanto, cada capa procesa sucesivamente los datos (paquetes de información) que circulan por la red, les agrega un elemento de información (llamado encabezado) y los envía a la capa siguiente (ver figura 2).

Las capas del modelo TCP/IP son:

4	Aplicación	Define los protocolos de aplicación TCP/IP y cómo se conectan los programas de host a los servicios del nivel de transporte para utilizar la red.
3	Transporte	Permite administrar las sesiones de comunicación entre equipos host. Define el nivel de servicio y el estado de la conexión utilizada al transportar datos.
2	Internet	Empaqueta los datos en datagramas IP, que contienen información de las direcciones de origen y destino utilizada para reenviar los datagramas entre hosts y a través de redes. Realiza el enrutamiento de los datagramas IP.
1	Interfaz de red	Específica información detallada de cómo se envían físicamente los datos a través de la red, que incluye cómo se realiza la señalización eléctrica de los bits mediante los dispositivos de hardware que conectan directamente con un medio de red, como un cable coaxial, un cable de fibra óptica o un cable de cobre de par trenzado.

Figura 2. Modelo TCP/IP

1.2.3 Protocolos de Red

Un protocolo no es más que un acuerdo entre dos entidades diferentes de cómo actuarán y reaccionarán en ciertas circunstancias. Por ende un protocolo de red será un acuerdo entre dos equipos de cómputo de cómo trabajarán.

Los protocolos de red tienen tres propósitos principales:

- Para estandarizar el formato de la comunicación.
- Para especificar el orden y el tiempo de cada comunicación.
- Para que cualquiera de las partes involucradas determine el sentido de la comunicación.

1.2.3.1 IP (Internet Protocol)

El protocolo IP es parte de la capa de Internet del conjunto de protocolos TCP/IP. Es uno de los protocolos de Internet más importantes ya que permite el desarrollo y transporte de datagramas de IP (paquetes de datos), aunque sin garantizar su "entrega". En realidad, el protocolo IP procesa datagramas de IP de manera independiente al definir su representación, ruta y envío.

El protocolo IP determina el destinatario del mensaje mediante 3 campos:

- el campo de dirección IP: Dirección del equipo;
- el campo de máscara de subred: una máscara de subred le permite al protocolo IP establecer la parte de la dirección IP que se relaciona con la red;
- el campo de pasarela predeterminada: le permite al protocolo de Internet saber a qué equipo enviar un datagrama, si el equipo de destino no se encuentra en la red de área local.

Los datos circulan en Internet en forma de datagramas (también conocidos como paquetes). Los datagramas son datos encapsulados, es decir, datos a los que se les agrega un encabezado que contiene información sobre su transporte (como la dirección IP de destino).

Los routers analizan (y eventualmente modifican) los datos contenidos en un datagrama para que puedan transitar.

El formato de los paquetes IP se muestra en la figura 3:

<table>
<tr><td>0-3</td><td>4-7</td><td>8-15</td><td>16-18</td><td>19-31</td></tr>
<tr><td>Versión</td><td>Tamaño Cabecera</td><td>Tipo de Servicio</td><td colspan="2">Longitud Total</td></tr>
<tr><td colspan="3">Identificador</td><td>Flags</td><td>Posición de Fragmento</td></tr>
<tr><td colspan="2">Time To Live</td><td>Protocolo</td><td colspan="2">Checksum Cabecera</td></tr>
<tr><td colspan="5">Dirección IP de Origen</td></tr>
<tr><td colspan="5">Dirección IP de Destino</td></tr>
<tr><td colspan="4">Opciones</td><td>Relleno</td></tr>
</table>

Figura 3. Paquete IP

1.2.3.2 TCP[4] (Transmision Control Protocol)

Es un protocolo de conexión de la capa de transporte que proporciona transmisión fiable de datos. Es un entorno orientado a conexión, dicha conexión se establece entre ambos extremos antes de iniciar la transferencia de datos. TCP es el responsable de dividir los mensajes en segmentos, reensamblarlos en la estación destino, reenviar cualquiera que no se haya recibido y componer los mensajes a partir de los segmentos. TCP ofrece un circuito virtual entre las aplicaciones finales del usuario.

En la capa de transporte, los paquetes de bits que constituyen las unidades de datos de protocolo se llaman "segmentos". El formato de los segmentos TCP se muestra en la figura 4:

+	Bits 0 - 3	4 - 7	8 - 15	16 - 31
0	Puerto Origen			Puerto Destino
32	Número de Secuencia			
64	Número de Acuse de Recibo (ACK)			
96	longitud cabecera TCP	Reservado	Flags	Ventana
128	Suma de Verificación (Checksum)			Puntero Urgente
160	Opciones + Relleno (opcional)			
224	Datos			

Figura 4. Segmento TCP

[4] *TCP* (Transmision Control Protocol), se conoce en español como Protocolo de Control de Transmisión.

1.2.3.3 UDP[5] (User Datagram Protocol)

En la familia de protocolos de Internet UDP proporciona una sencilla interfaz entre la capa de red y la capa de aplicación. UDP es un sencillo protocolo que intercambia datagramas sin confirmación ni entrega garantizada, se le considera un protocolo no orientado a conexión. Esta simplicidad se evidencia cuando se comparan el formato de un segmento UDP con otro TCP. El procesamiento de errores y la retransmisión deben ser manipulados por protocolos de capas superiores[1].

En la figura 5 se muestra el formato del segemento UDP:

+	Bits 0 - 15	16 - 31
0	Puerto origen	Puerto destino
32	Longitud del Mensaje	Suma de verificación
64	Datos	

Figura 5. Segmento UDP

1.2.3.4 ICMP [6] (*Internet Control Message Protocol)*

[5] *UDP* (User Datagram Protocol), conocido en español como Protocolo de Datagrama de Usuario

Es un protocolo que permite obtener información relacionada con errores de los equipos en red. ICMP no permite corregir los errores sino que los notifica a los protocolos de capas cercanas.

Los mensajes de error ICMP se envían a través de la red en forma de datagramas, como cualquier otro dato. Por lo tanto, los mismos mensajes de error pueden contener errores.

En la figura 6 se muestra el formato del segmento UDP:

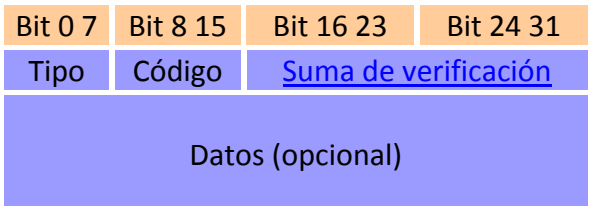


Figura 6. Segmento ICMP

[6] ICMP (*Internet Control Message Protocol*), *conocido en español como* Protocolo de Mensajes de Control de Internet

Conclusiones Capítulo 1

La información siempre ha sido fundamental en el desarrollo de cualquier individuo, organización o nación. Es por ello, que protegerla, puede llegar a ser una cuestión de vida o muerte.

Con el auge de los equipos y redes de computadoras, se ha vuelto más fácil que nunca su intercambio, favoreciendo el crecimiento y desarrollo exponencial de la humanidad. Pero este tipo de ventajas traen consigo responsabilidades muy grandes, que no se deben tomar a la ligera.

Cada ente da un valor a su información, dependiendo de la relevancia que tenga para él. Por ejemplo, una organización no quisiera por ningún motivo que información confidencial cayera en manos de su competencia, porque esto podría causar fuertes daños económicos, o quizá, su desaparición.

El resguardo de la información podría llegar a ser más importante aún en tiempos de guerra, en donde el robo o intercepción de la información podrían causar la muerte de personas inocentes.

Dada la magnitud del problema es necesario y obligatorio aplicar técnicas de seguridad para proteger la información, tanto por el bien de la organización, como el de las que la rodean.

Más importante aún, es entender claramente los principios con los que operan redes y dispositivos necesarios para el intercambio de información, ya que de lo contrario será muy difícil aplicar un mecanismo de seguridad que resuelva un problema.

Capíulo2. Principales Métodos de Ataques

2.1 Métodos de Ataque

Tiempo atrás podíamos examinar un ataque fácilmente, ya que éstos utilizaban pocas técnicas para tener éxito. Aunque actualmente existen probablemente miles de diferentes exploits[1] que los atacantes pueden usar en contra de los sistemas, casi todos pueden ser clasificados en una o más categorías. Se ha realizado mucha investigación a lo largo del tiempo tratando de definir una taxonomía estándar de las vulnerabilidades, pero ninguna de éstas ha sido ampliamente aceptada.

En el sentido clásico de un ataque planeado y ejecutado por un atacante con intenciones maliciosas, una secuencia de eventos típicos tiene lugar del modo siguiente: primero, en la fase de reconocimiento, el atacante suavemente prueba el sistema(s) o red(es) para tener una idea de con qué está tratando; segundo, después de descubrir el potencial del objetivo, el atacante puede hacer un escaneo[2] del sistema más profundo y con esto obtener datos más precisos tales como: usuarios del sistema o de la red, nombres específicos de los sistemas operativos, carpetas u archivos compartidos y muchas cosas más. Usando cualquier cantidad de métodos, el atacante puede tratar de penetrar el sistema o la red y poder tener acceso y control del recurso en cuestión.

Finalmente, sabemos que existen innumerables métodos de ataques y formas de comprometer un sistema o red. En este capítulo se presentarán algunos tipos de vulnerabilidades que se han visto a lo largo del tiempo. No se hablará sobre algún tipo de exploit en específico o de algún tipo de software, sino de clases de ataques que pueden ser aplicados a casi cualquier sistema. Sería casi imposible describir todas las posibles técnicas de ataques, pero sí podemos analizar las más comunes[12].

[1] *Exploit.* Programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa (llamadas bugs).
[2] El término *escaneo* alude a la palabra en inglés scanning, que hace referencia a buscar, analizar, inspeccionar, explorar o investigar, según sea el caso.

2.1.1 Código Malicioso

Un código malicioso es todo aquel hardware, software o firmware[3] que es intencionalmente introducido en un sistema con un fin malicioso. Actualmente existen diferentes tipos de código malicioso como: bombas lógicas, caballos de troya y puertas traseras, son sólo algunos ejemplos, de éstos, que particularmente se han hecho muy comunes.

Las bombas lógicas son programas o secciones de programa que están relacionadas con algún evento, tal como una fecha u hora específica, algún porcentaje de disco duro lleno o quizá al borrado de un archivo en particular. Por ejemplo un programador puede poner una bomba lógica para borrar secciones críticas de código si es despedido.

Los caballos de troya o troyanos, son programas que necesitan ser instalados o ejecutados por el usuario para que tengan efecto. A menudo son encubiertos en programas de entretenimiento o programas fidedignos tales como parches de sistemas operativos, aplicaciones gratuitas o juegos.

Las puertas traseras son pedazos de código puestos en programas por el programador para tener acceso rápidamente al sistema en otra ocasión. Las puertas traseras son casi imposibles de remover y comúnmente la única manera de asegurar que se eliminarán es formateando el equipo.

[3] *Firmware.* Es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria de tipo no volátil (ROM, EEPROM, flash,...), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

2.1.2 Denegación de Servicio

Los ataques de DoS[4] *(Denial of Service)*, se han vuelto muy populares en los últimos años, pero éstos llevan presentes casi lo mismo que tienen las computadoras. Como el nombre lo dice, un DoS ocurre cuando un usuario es privado de algún dato, componente(s) de un sistema o algún servicio debido a las acciones realizadas por el atacante. Las condiciones para un DoS no siempre son malintencionadas, puede ser resultado de un simple error en alguna parte del sistema, pero usualmente no son considerados ataques, al menos que se realicen intencionalmente.

Existen diferentes tipos de ataques de DoS. La siguiente es una lista de algunos de los más interesantes y comunes:

- **Smurf.** En un ataque de DoS tipo smurf, el atacante falsifica la dirección IP de la víctima y manda un ICMP ECHO request [5]a las direcciones de broadcast de la red. Cuando cada uno de los sistemas le responde a la víctima, este equipo no podrá responder a todas las peticiones al mismo tiempo, ya que el buffer preestablecido para este tipo de conexiones se llenará fácilmente provocando así un DoS.

- **SYN floods.** Una dirección IP falsificada es utilizada para enviar paquetes SYN[6] al objetivo. Este le responderá con paquetes del tipo SYN/ACK[7], pero nunca recibirá un ACK[8] final para completar el Three-way Handshake[9]. Esta conexión queda pendiente ocupando un espacio en el buffer preestablecido para las conexiones TCP. Llenando este buffer con falsos paquetes SYN lograremos realizar el ataque deseado.

- **Ataques DDoS[10]** *(Distributed Denial of Service).* En un DDoS, el atacante recluta equipos, también llamados "zombies", para que al mismo tiempo inunden de tráfico a la víctima imposibilitando con esto todo tipo de comunicación.

---

[4] *DoS* (Denial of Service) en español Denegación de Servicio.

[5] *ICMP ECHO request.* El Echo Request, en el protocolo ICMP, es un mensaje que se envía a un host para que éste le responda con un Echo Reply.

[6] Paquetes *SYN*. Realizan una apertura activa de un puerto

[7] Paquetes *SYN/ACK.* Este paquete se utiliza para responder a una petición SYN, en caso de que el puerto este abierto.

[8] Paquetes *ACK*. Contestación afirmativa a un paquete SYN/ACK

[9] *Three-way Handshake.* Proceso para el establecimiento de una conexión TCP, consta de tres tipos de paquetes SYN, SYN/ACK, ACK.

[10] *DDoS* (Distributed Denial of Service), conocido en español como Denegación de Servicio Distribuido.

2.1.3 Ataques Físicos

Probablemente este tipo de ataques son los más fáciles de entender. Alguien con acceso físico al sistema en cuestión puede hacer cualquier cosa que quiera y probablemente no hay nada que se pueda hacer en ese momento. El atacante puede reiniciar la máquina, desconectar el cable de red, robar medios de almacenamiento que probablemente tienen información crítica o, en un caso extremo, destruir la máquina entera.

Este tipo de ataques hacen ver lo importante que es tener implementados controles de acceso físico y que estos deben tener la misma importancia que los controles de acceso lógico, tales como firewalls, políticas de contraseñas, etc. Proteger la infraestructura crítica detrás de puertas con cerraduras fuertes, o métodos de autenticación robustos, es un buen comienzo para mitigar este tipo de ataques.

2.1.4 Buffer Overflow[11]

Se produce cuando se copia una cantidad de datos sobre la memoria en un área que no es lo suficientemente grande para contenerlos, sobrescribiendo de esta manera otras zonas de memoria. Esto se debe en general, a un fallo de programación. La consecuencia de escribir en una zona de memoria imprevista puede resultar impredecible. Existen zonas de memoria protegidas por el sistema operativo. Si se produce la escritura fuera de una zona de memoria protegida se producirá una excepción del sistema de acceso a memoria seguido de la terminación del programa. Bajo ciertas condiciones, un usuario obrando con malas intenciones puede aprovecharse de este mal funcionamiento o una vulnerabilidad para acceder y tener control sobre el sistema. Si el programa que tiene el error en cuestión tiene privilegios especiales se convierte además en un fallo de seguridad.

[11] *Buffer Overflow*, en español desbordamiento de buffer.

2.1.5 Flooding y Spam

La palabra flooding significa inundación y es precisamente lo que lleva a cabo este tipo de ataque. Consiste en bombardear los servidores de correo con e-mails y con esto lograr saturarlos rápidamente para que queden inhabilitados. Este tipo de ataques de e-mails también son utilizados para forjar la identidad de un atacante, degradar los sistemas de comunicaciones, poner en duda la integridad de las organizaciones o quizá distribuir material ilícito. El término Spam hace referencia al correo basura o no deseado que es enviado a millones de personas normalmente con fines publicitarios o portando archivos con código malicioso que afectan directamente al usuario u organización.

2.1.6 Fuerza Bruta

Los ataques por fuerza bruta son tal vez de los menos sofisticados que existen en la actualidad, pero podemos asegurar que siempre son certeros. Su meta es tratar de adivinar un secreto, tal como una contraseña o una llave cifrada. El problema es que regularmente, no se cuenta con ningún tipo de información y esto lleva a realizar búsquedas indirectas y probar con cada una de las combinaciones posibles hasta encontrar la correcta. Como podemos ver, esto puede tomar muchísimo tiempo, incluso años, haciendo de este tipo de ataque uno de los menos eficientes.

2.1.7 Mantenimiento Remoto o Conexiones Remotas

Cuando escuchamos el término mantenimiento remoto, normalmente creemos que sólo usuarios autorizados como administradores, tendrán ese privilegio para llevar a cabo acciones de soporte o mantenimiento a sus sistemas. Pero, qué pasa si este derecho se extiende a vendedores y técnicos que necesitan hacer uso de este recurso para configurar o resolver problemas de dichos sistemas, esto implica un gran agujero de seguridad para los sistemas.

Se debe estar consciente que cualquier acceso remoto a los sistemas implica un gran riesgo para toda la organización, es por eso que se deben tomar medidas de seguridad como: implementaciones de VPN[12] *(Virtual Private Network)*, políticas de contraseñas, asignación de privilegios, etc.

2.1.8 Contraseñas Predefinidas

Por alguna razón, algunos equipos de sistemas cuentan con nombres de usuarios y contraseñas pre-configuradas y listas para usarse. Los vendedores asumen que los administradores cambiarán esta configuración antes de hacer cualquier cosa, pero esto no siempre es así. Las contraseñas predefinidas son muy comunes y muy utilizadas por los intrusos para crear nuevas cuentas o tomar control inmediato del sistema.

Este tipo de contraseñas se pueden encontrar fácilmente en Internet, innumerables listas aparecerán incluyendo marca, modelo, usuario y contraseña del equipo, facilitándonos mucho el trabajo de investigación.

Una de las listas más comunes y mejor documentadas en Internet es la de Johnny Long, autor del libro Google Hacking en la dirección http://johnny.ihackstuff.com.

2.1.9 Condiciones de Carrera

Este término hace referencia al lapso de tiempo que transcurre cuando se aplica un control de seguridad y éste está disponible. Normalmente son muy difíciles de eliminar. Un ejemplo es, cuando se actualizan las listas de control de acceso en un ruteador[13], toma un cierto período de tiempo, que, aunque en ocasiones sea de menos de un segundo, el sistema queda desprotegido, pudiendo ser vulnerable a un ataque.

---

[12] *VPN* (Virtual Private Network), en español Red Privada Virtual.

[13] *Ruteador*, es un dispositivo de hardware para interconexión de red de computadoras que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

2.1.10 Interrupciones

Debido a que el procesador no puede procesar múltiples datos al mismo tiempo (procesa un dato a la vez), el sistema de multitareas es en realidad una alternancia de fragmentos de instrucciones de muchas tareas diferentes. Es posible suspender momentáneamente un programa que se estaba ejecutando mediante una interrupción. El atacante puede usar una interrupción ejecutando una llamada al sistema y con esto realizar una acción maliciosa.

Se espera que con el tiempo se fortalezcan las políticas del software para que puedan reconocer este tipo acciones de código malicioso.

2.1.11 Browsing[14]

Browsing consiste en examinar qué es lo que hay en una red. Por ejemplo, si el atacante logra tener acceso ya sea de manera física o remota a un equipo, éste puede saber muchísima información referente a la persona u organización, desde datos personales de los usuarios, contraseñas, archivos confidenciales, nombres de impresoras, servidores de archivos, servidores de correo, etc.

La mayoría de las máquinas con Windows, permiten navegar en la red y con esto poder descubrir qué es lo que está al alcance e incluso descubrir la topología de la red y ver entre qué equipos existen relaciones de confianza.

2.1.12 Análisis de Tráfico

El análisis de tráfico es un tipo especial de técnica de interferencia que consiste en interceptar las comunicaciones entre las diferentes entidades de un sistema. Sabiendo quién está hablando con quién, cuándo y por cuánto tiempo le puede dar varias pistas al atacante de qué es lo que está pasando e inclusive obtener la información deseada.

[14] *Browsing*, hace referencia al término navegar en español.

El análisis de tráfico también puede ser utilizado como una técnica de defensa para identificar posibles anomalías en el sistema. Usando el análisis de tráfico, los administradores pueden crear un línea base de cómo se comporta el tráfico en su red, inclusive puede crear algún tipo de gráfica. Diariamente, el administrador puede revisar éstas gráficas y compararlas, para con ello detectar anomalías de tráfico, conexiones entre host, conexiones entrantes/salientes no permitidas, ataques de denegación de servicio, problemas de ancho de banda, etc.

2.1.13 Alteración de Código

Los ataques de alteración de código consisten en modificar de manera no autorizada códigos o datos, alterar con esto su integridad. Este tipo de ataque tiene diferentes formas y puede tener variadas consecuencias. El ejemplo más común de este tipo de ataque son los virus y los gusanos, ya que ellos modifican algo dentro del sistema para que puedan trabajar.

2.1.14 Rootkits

Uno de los ataques de alteración de código más comunes es la utilización de un rootkit. Un rootkit es una herramienta que se inserta en el S.O. que permite prácticamente tener acceso a cualquier cosa que se realice en la PC, inclusive puede engañar y esconder procesos u archivos, con esto nunca se podra saber si se ha sido comprometido.

Los rootkits son normalmente implementados para ser cargados sobre el kernel[15] de Unix, Linux, y Windows. Una vez que el código corre sobre el Kernel, el rootkit tiene acceso sobre la memoria que utiliza el kernel, comprometiendo así inicios de sesiones, procesos u archivos y hasta inclusive análisis forenses[16].

[15] *Kernel.* Software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.

[16] *Análisis forense*. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados.

Conclusiones Capítulo 2

Para la mejor comprensión de los riesgos que se presentan comúnmente en los sistemas, se expone una lista que trata de brindar un panorama general de los ataques. Aunque en esta área se investiga constantemente, muy periódicamente surgen nuevos tipos de ataques. El propósito de esta clasificación es mostrar todas las posibilidades que existentes, ya que cada sistema tiene diferentes puntos de ataque.

Existen muchos métodos de ataque, de hecho no podemos confiar únicamente en uno o dos métodos de defensa. Se debe tratar de cierta manera de abarcar todo el abanico de posibilidades, prevención, detección y soluciones. Sólo de esta manera se puede tener cierta esperanza de reducir los riesgos asociados a los diferentes ataques.

Capítulo 3.
Firewalls y Honeypots

En este capítulo se tratarán dos métodos específicos para el manejo de riesgos en la información: firewalls y honeypots. Los dos operan en conjunto con la red para salvaguardar sistemas y redes además de ayudar a proteger los sistemas de otras personas en la Internet. Se habla de qué son y qué no son los firewalls, qué pueden hacer por la organización, los tipos disponibles y cómo conformarlos con las políticas.

3.1 Firewalls

El principal objetivo de una red es el compartir recursos e información de manera eficiente y confiable sin importar distancias, partiendo de esta base, es muy importante para cualquier tipo de red contar con un mecanismo de seguridad capaz de mantener fuera del alcance de los intrusos, recursos e información a compartir. La tecnología fundamentalmente utilizada para lograr este cometido es, la instalación de un firewall o como se le conoce en español cortafuegos. Podemos entender a un firewall como un sistema de contención para todo aquel usuario o aplicación que no esté autorizada a entrar o salir del perímetro de seguridad[17].

3.1.1 Concepto de Firewall

Antes de hablar de bits y bytes, se debe saber cómo es que los firewalls encajan en el mundo de la seguridad de la información, cuáles son sus beneficios y deficiencias. Empecemos por definir ¿Qué es un Firewall?.

El término firewall hace referencia a un medio para prevenir que el fuego se propague entre una porción de una estructura hacia otra dentro de una construcción. Un firewall, en el sentido tecnológico, es un medio de control que se encuentra en algún punto de la red como un mecanismo para fortalecer las políticas de seguridad. Los firewalls son utilizados en diversas posiciones dentro de una red, dos de las más populares son:

- Entre el Internet y la red privada.
- Entre la NIC[1] (Network Interface Card) de una computadora y el resto de ella.

[1] *NIC* (Network Interface Card), en español Tarjeta de Red.

Los firewalls pueden ser implementados de diferentes maneras, como:

- Hardware dedicado (appliances[2]).
- Hardware o Software insertado dentro de algún dispositivo de red como un ruteador o switch[3].
- Software instalado en una computadora de propósito general.

Antes de contar con los appliances, los firewall eran implementados instalando software en una computadora de propósito general, fortaleciendo el sistema operativo. En años recientes los firewalls personales se han vuelto populares e importantes en las computadoras personales.

3.1.2 Beneficios de un Firewall

Los firewalls resultan ser herramientas muy importantes para la seguridad, ya que pueden jugar diferentes roles, cada uno con beneficios particulares, que sirven para reforzar las políticas de seguridad de una organización. Los firewalls pueden:

- Reduce riesgos protegiendo los sistemas de tráfico de entrada y salida que desea explotar las vulnerabilidades.
- Incrementa la privacidad haciendo difícil que el atacante tenga acceso a información confidencial.
- Filtra las comunicaciones basándose en su contenido, esto sirve para detectar algún tipo de amenaza que está contenida dentro de algo que no lo es.
- Provee un registro en el que podemos observar el tráfico que fue permitido y el que fue rechazado. Esta información es de mucha ayuda para el manejo de incidentes y análisis forense.
- Sirve como un filtro de ruido, además de conservar el ancho de banda.

[2] *Appliance,* hardware dedicado a funciones especificas
[3] *Switch*, Un conmutador interconecta dos o más segmentos de red, pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Incluso un firewall en modo permisivo (firewall que permite pasar tráfico que no haya sido bloqueado mediante reglas), reduce el peligro de ser atacado. Firewalls de diferentes tipos pueden ser puestos según las necesidades de la red. Algunas de las redes más seguras usan diferentes marcas y tipos de firewalls como parte de una estrategia de defensa en profundidad.

3.1.3 Deficiencias de un Firewall

Son tantos los beneficios que proporciona un firewall que quizá se pudiera creer que esta solución es más que suficiente, pero no es así. Los firewalls no son herramientas todo en uno, no pueden parar todos los tipos de ataque. Incluso un firewall puede ser atacado por el mismo.

Mucha gente cree ciegamente en la protección que brindan los firewalls. Muchas veces se pueden escuchar cosas como: “Estamos detrás de un firewall. ¿Por qué necesitamos instalar parches a los sistemas o usar controles de accesos para los servidores?”. Una de las desventajas de tener un firewall es que la organización que lo posee tiende a descuidar otros aspectos de seguridad, creen que por el simple hecho de tenerlo sus problemas de seguridad se verán solucionados y esto es un gran error. El mejor modo de ver a un firewall conceptualmente hablando es como una sombrilla. Cuando se usa una sombrilla esta protege en gran parte de la lluvia, especialmente la cabeza, pero mucha de esta lluvia sí alcanza a mojar, ya que logra penetrar de alguna forma el perímetro de defensa.

3.1.4 Reglas por Default

Los firewalls están diseñados con algo llamado regla de default, si el paquete no es igual con alguna regla, la regla por default elimina el paquete. Este tipo de regla también se le conoce como política restrictiva, como se muestra en la figura 7, en la que se deniega todo el tráfico excepto el que está explícitamente permitido. El firewall obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.

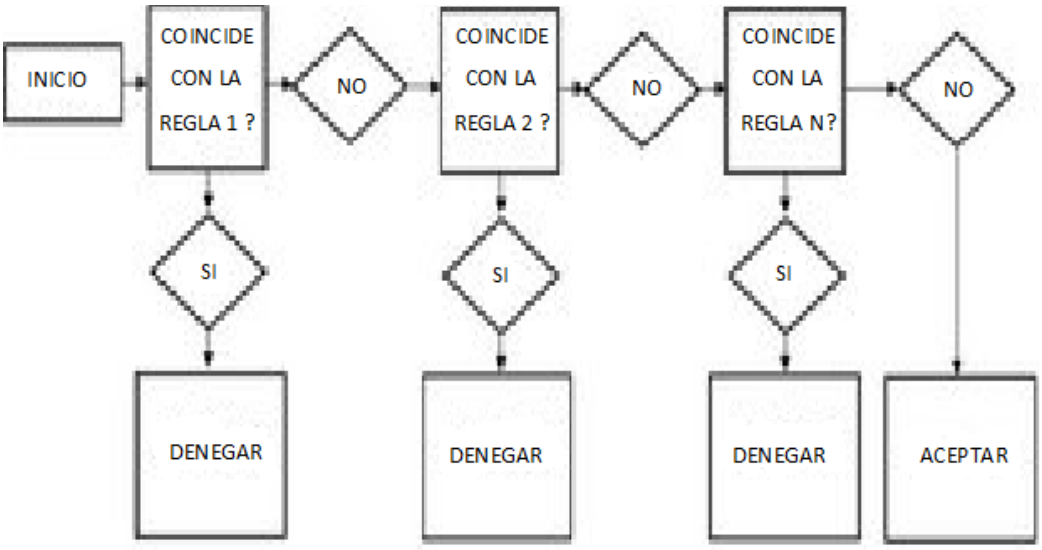


Figura 7.Política restrictiva

También podemos hacer uso de una política permisiva, como la de la figura 8, ésta consiste en permitir todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado caso por caso, mientras que el resto del tráfico no será filtrado.

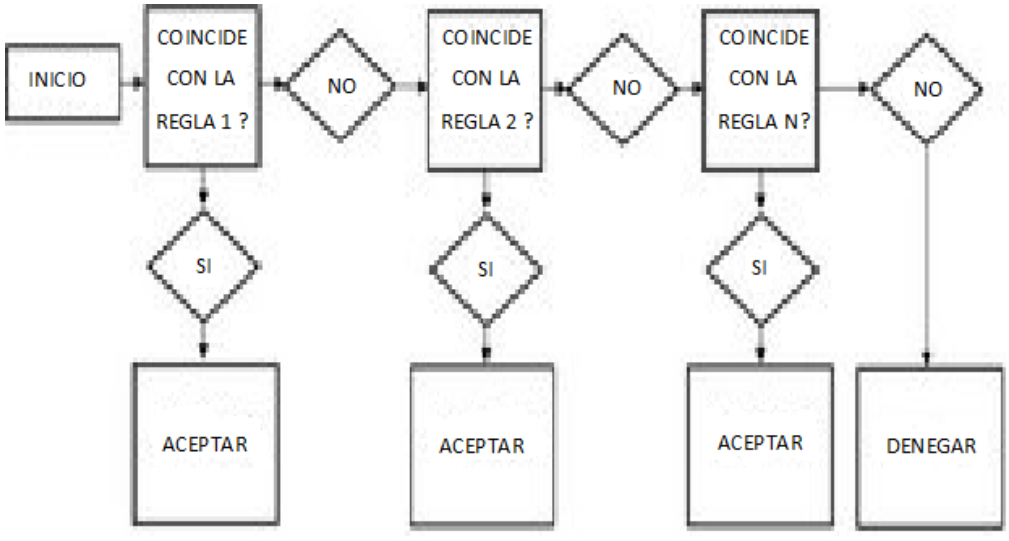


Figura 8.Política permisiva

Al tener estas dos posibilidades la pregunta que surge es, ¿Cuál de estas dos posturas es la mejor? la permisiva o la restrictiva. Para poder responder esta pregunta podemos tomar en cuenta las siguientes consideraciones. Los empleados de alguna organización, con estándares de seguridad muy altos como los de algún sitio militar o de gobierno, normalmente no tienen muchos grados de libertad, por ello es conveniente en su caso optar por una política restrictiva, aunque esto a veces es un poco complicado ya que pueden buscar formas para poder romper las políticas del firewall tales como: instalar un módem, configurar una red inalámbrica o implementar una red P2P[4] (Peer to Peer).

Las redes de las universidades normalmente son permisivas, especialmente la porción que corresponde a sus estudiantes. Las organizaciones que tienen políticas permisivas y no bloquean al menos las vulnerabilidades más comunes operan con un riesgo significante a no ser que cuenten con otro tipo de medidas de seguridad. Cada paquete que el firewall bloquea incrementa la seguridad de la organización ya que evita que una amenaza penetre el perímetro de seguridad.

3.1.5 Filtrado

Filtrado de Ingreso

El término filtrado de ingreso se refiere a filtrado aplicado al tráfico de entrada, desde la perspectiva de la propia red. Generalmente, la mayoría de la reglas son aplicadas al tráfico de entrada y muchos de los recursos son utilizados para determinar qué hacer con este tráfico.

Todos los paquetes de entrada deben ser desechados sí estos contienen una dirección destino diferente de las direcciones protegidas de red de la organización. Si estos paquetes son el resultado de un ataque de IP spoofing [5]por parte de un atacante o un problema de ruteo, no deberá permitírseles entrar.

[4] *P2P* (Peer to Peer), se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red.
[5] *IP Spoofing*, ataque que consiste en falsificar una dirección IP.

Filtrado de Egreso

Filtrado de Egreso aplica a todo el tráfico de salida, normalmente se relaciona con el filtrado de direcciones. Este tipo de filtrado aplica tanto a computadoras personales como redes, sólo las direcciones que pertenecen a la red protegida serán permitidas para salir por Internet.

Si una empresa aplica filtrado de egreso al punto de acceso entre su red y el Internet, obviamente será considerado un buen vecino, ya que no permitirá la salida de ningún tipo de código malicioso, previniendo con esto la proliferación del mismo.

El filtrado de egreso puede servir como una técnica de detección de intrusos, utilizando los archivos de log del firewall. Supongamos que una de las máquinas internas ha sido infectada por un macro virus, indirectamente se puede detectar por sus numerosos intentos por salir de la red para poder infectar a equipos del exterior.

3.1.6 NAT[6] *(Network Address Translation)*

NAT es una herramienta que debe ser usada cada vez que sea posible. Permite que varias computadoras participen en Internet sin necesidad de que cada una cuente con una dirección pública de Internet, además de proveer privacidad acerca del esquema de direcciones privadas de la organizacion.

En el pasado jamás se hubiese podido imaginar quedar fuera del espacio de direcciones de Internet, después de todo existen 68,719,476,736 direcciones para utilizar. Sin embargo, en la práctica muchas de las direcciones son desperdiciadas especialmente en Estados Unidos. NAT ofrece una solución para disminuir el número de direcciones requeridas para conectarse a Internet ya que con sólo una dirección pública podemos conectar una red entera[14].

[6] *NAT* (Network Address Translation), en español Traducción de Dirección de Red

El uso de NAT permite garantizar que los hosts estarán blindados. Desde el punto de vista que no los podrán reconocer a través de la Internet, ya que lo único que se podrá ver desde afuera de la red, será una sola dirección pública y no toda la topología de red.

RFC´s [7] *(Request for Comments)* **relacionados con NAT**

Los estándares de Internet son llamados RFC´s. Estos estándares son enumerados secuencialmente y nunca modificados al menos que hayan sido reemplazados por otro RFC. Si uno es actualizado, tendrá por consiguiente otro número para su identificación. Existen diferentes variaciones de NAT que están documentadas en varios RFC´s. Por lo regular, se utiliza NAT en dirección de salida, desde la red interna hacia Internet. Generalmente, para llevar a cabo este cometido utilizamos NAT y PAT[8] *(Port Address Translation)*, para poder asignar tanto direcciones como los puertos de salida.

Los RFC´s relacionados a NAT son:

- RFC 1918. Direcciones asignadas para redes privadas.
- RFC 2663. NAT, terminología y consideraciones.
- RFC 2993. NAT, Implicaciones.
- RFC 3235. NAT, Guía de aplicación de diseño.

Sin duda el estándar RFC 1918 es muy importante ya que determina los segmentos de direcciones que una red privada puede utilizar, que son:

- Red 10.0.0.0 – 10.255.255.255
- Red 172.16.0.0 – 172.31.255.255
- Red 192.168.0.0 – 192.168.255.255

[7] *RFC´s* (Request for Comments), en español petición de comentarios

[8] *PAT* (Port Address Transaltion), en español traducción de dirección de puerto, es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna.

Los paquetes que utilizan estas redes no tendrán permitido salir a Internet y si llegasen a intentarlo el ISP[9] no lo permitirá. Este tipo de direcciones no son ruteables a través del Internet, ya que solamente son utilizadas para el uso en redes privadas.

3.1.7 PAT

El proceso de trasladar tráfico de múltiples hosts internos a una sola dirección externa se le conoce como PAT. Usando PAT se puede disfrazar la presencia de múltiples usuarios internos con el uso de una dirección de red pública.

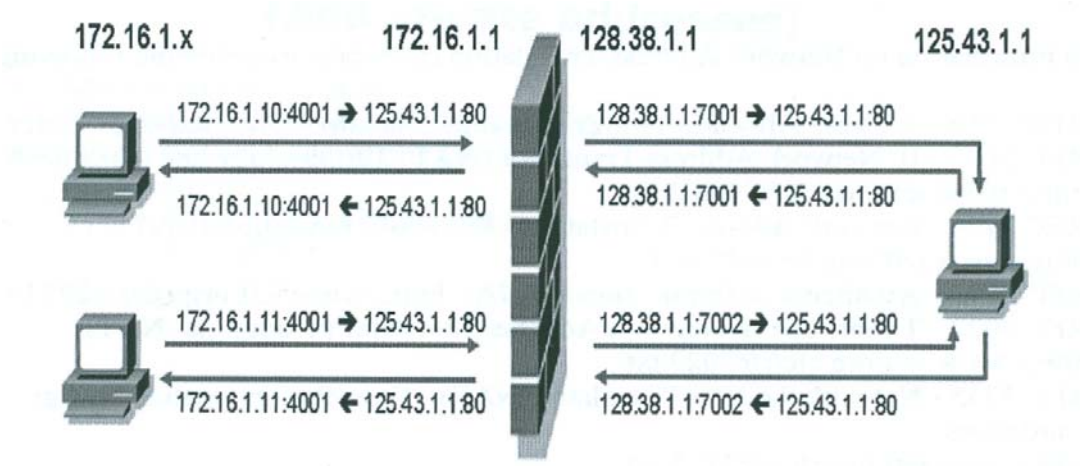


Figura 9. Ejemplo de PAT

En la figura 9 se tiene un diagrama de una red con direcciones IP privadas. El tráfico de salida pasa a través de un Firewall que utiliza NAT antes de alcanzar el Internet. Podemos asignar una sola dirección de Internet pública o un bloque de éstas a la interfaz externa del firewall. Estas direcciones públicas son las únicas direcciones de Internet del sitio que se pueden ver desde afuera, ya que, la red interna está hecha únicamente con direcciones privadas, como se define en el RFC 1918. Cuando una computadora interna (como la 172.16.1.10) inicia una conexión con Internet, el dispositivo que implementa NAT modifica el paquete que va a salir de la siguiente manera:

[9] *ISP* (Internet Service Provider), en español Proveedor de Servicios de Internet, es una empresa dedicada a conectar a Internet a los usuarios o las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente

- El host 172.16.1.10 desea conectarse a un servidor web que se encuentra en Internet. Por ello, manda un paquete SYN a la dirección del destinatario que debe pasar sobre el firewall.

- La interfaz que implementa NAT se da cuenta de que una sesión hacia el exterior se quiere iniciar a través de un paquete SYN, el cual proviene de una dirección privada.

- Por ello el dispositivo cambia la dirección origen y el puerto origen de estos paquetes, remplazando la dirección privada con la dirección pública de la interfaz que implementa NAT y el próximo puerto origen disponible por el dispositivo. Después de esto los paquetes pasan hacia Internet. Desde este momento todo el tráfico que pase por la interfaz parecerá que proviene de una sola dirección pública.

- Después que el paquete es recibido por el servidor web y éste manda una réplica (SYN/ACK), el dispositivo NAT toma este paquete y modifica la dirección de destino a la dirección privada (172.16.1.10) y su respectivo puerto origen (4001) del host que inició sesión.

Volviendo a la figura 9, veamos más a fondo la transmisión de datos que se quiere iniciar. Un host de la red interna, quiere ir a la dirección 125.43.1.1. El firewall ve un paquete con el puerto destino 80 (HTTP), un puerto origen que es el 4001 y la bandera de SYN, que significa que el usuario quiere iniciar una sesión. Cuando el paquete pasa por el firewall cambia esta dirección origen por su propia dirección pública antes de alcanzar el Internet. Cuando la dirección 125.43.1.1 responde, lo hará a la dirección pública de la interfaz configurada con NAT. Este dispositivo NAT es capaz de asociar el paquete previo de SYN con la respuesta desde 125.43.1.1 basado en el puerto utilizado al establecer la sesión (7001).

El firewall ha reservado las conexiones al puerto 7001 desde la dirección 125.43.1.1 para el host interno que ha iniciado la sesión. El host interno replica con un ACK para completar el three-way handshake. Este paquete es pasado a través de NAT hacia Internet para continuar la sesión[12].

Analicemos la segunda conexión desde el host 172.16.1.11 hacia 125.43.1.1. En este caso el host interno coincidentemente está usando el mismo puerto aleatorio (4001) como el host 172.16.1.10. Si el dispositivo NAT no remplazara el puerto origen, después de reemplazar la dirección interna sería imposible determinar si la respuesta desde 125.43.1.1 debe ser mandada hacia 172.16.1.10 o 172.16.1.11. Gracias a que PAT cambia el puerto origen, el host 172.16.1.11 puede contestar a esta petición y el firewall correctamente sabrá a qué host origen entregará el paquete.

Finalmente, muchos firewalls pueden utilizar múltiples direcciones públicas en lo que se conoce como NAT pool. Esto incrementa el número de conexiones NAT que se pueden tener simultáneamente, ya que cada dirección pública podrá tener 65,535 sesiones a la vez.

El punto importante es que el host de Internet, en este caso 125.43.1.1, jamás se conecta directamente con un host interno. El host 125.43.1.1 únicamente ve la dirección pública asignada a la interfaz NAT del firewall. Esto incrementa notablemente la privacidad de los hosts de la red interna. NAT está disponible en la mayoría de los productos de defensa perimetral y es altamente recomendable su implementación.

3.1.8 Clasificación de los Firewalls

3.1.8.1 Filtrado de paquetes

Los firewalls de filtrados de paquetes, fueron los primeros en ser desarrollados, estos pueden ser implementados en el hardware ya existente dentro de la red, como los ruteadores. Los ruteadores tienen la capacidad de inspeccionar paquetes rápidamente, solamente se requiere ser cuidadoso del nivel de procesamiento de paquetes conforme a las características del equipo. Los firewalls que utilizan esta tecnología suelen ser los más rápidos y baratos del mercado. El mejor ejemplo de este tipo de firewalls es un ruteador CISCO usando listas de control de acceso ya sean sencillas o extendidas[16].

Estos firewall se basan en un conjunto de reglas que especifican la acción a tomar dependiendo de las características del paquete analizado más:

- IP origen.
- IP destino.
- Puerto de origen (en paquetes TCP o UDP).
- Puerto de destino (en paquetes TCP o UDP).
- Cabeceras de estado (en paquetes TCP).

Este tipo de firewall no almacena un registro de qué conexiones han sido establecidas con éxito, debido a esto y al hecho de que las cabeceras TCP/IP de un paquete pueden ser falsificadas estos filtros son susceptibles a Spoofing de paquetes.

Aunque existen nuevas y más sofisticadas tecnologías de firewalls en el mercado, no se debe pensar que no hay espacio para este tipo de firewalls. Los firewalls de filtrados de paquetes tienen un rol exitoso en la detección de simples ataques a gran velocidad antes de que éstos sean revisados más a detalle, por ejemplo, con un firewall de filtrado de circuito.

3.1.8.2 Filtrado de Circuito

Un firewall de filtrado de circuito, es muy similar al de filtrado de paquetes la diferencia es que éste se enfoca especialmente en las cabeceras IP y TCP, estos tipos de firewalls no inspeccionan ningún dato de la aplicación.

La diferencia principal entre el filtrado de circuito y el filtrado de paquetes es que el primero, mantiene un registro de todas las conexiones que pasan a través del firewall. Para ello utiliza una tabla de dónde se encuentra la dirección y puerto origen, además de la dirección destino, información del puerto y la bandera de estado. La bandera de estado identifica la relación entre la dirección origen y destino además de sus respectivos puertos y cuál es el estado de la conexión. Los posibles valores del estado de la conexión son:

- SYN_SENT. Un paquete con la bandera de SYN ha sido enviado desde el host A al host B, el primer estado del three way handshake.

- SYN_RECV. Un paquete con la bandera SYN/ACK ha sido recibido del host B, el segundo paso del three-way handshake.

- ESTABLISHED. Éste es el tercer paso del three-way handshake, indica que la conexión ha sido establecida.

- FIN_WAIT1. Uno de los hosts manda un paquete FIN indicando que la conexión debe ser cerrada de forma correcta.

- LAST_ACK. El otro host contesta a la petición de cerrar la conexión de manera correcta.

- FIN_WAIT2. EL otro host manda un paquete con la bandera de FIN en respuesta a la petición. Los dos hosts han finalizado comunicación.

- CLOSED. Conexión nula entre hosts.

Al guardar el estado de las conexiones TCP, el firewall puede responder inteligentemente a los paquetes que llegan fuera de orden o a aquellos que tienen alguna malformación en las banderas TCP.

Esto significa una mejora en el desempeño al permitir que los paquetes que pertenecen a conexiones ya establecidas y válidas pasen a través del firewall sin tener que ser analizados nuevamente y una mayor confiabilidad al verificar la validez de las conexiones evitando que paquetes con cabeceras falsificadas vulneren la seguridad del entorno que se pretende proteger[9].

Como los protocolos ICMP[10] (*Internet Control Message Protocol)* y UDP no cuentan con banderas que indiquen que la conexión ha sido finalizada, los firewalls de filtrado de circuito se basan en un cierto período de tiempo para poder determinar cuándo pueden ser removidos de la tabla de estado. Una vez que el tiempo ha sido excedido, el tráfico del host externo será ignorado, hasta que un paquete ICMP o UDP de la dirección y puerto origen/destino se vuelva a originar desde adentro de la red.

Una de las ventajas más importantes de este tipo de firewalls es que no sólo guardan el estado de las conexiones, sino que también algunos de ellos añaden inspección de protocolos para poder tomar decisiones inteligentes.

---

[10] *ICMP* (Internet Control Message Protocol), en español Protocolo de Mensajes de Control de Internet, es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un ruteador o host no puede ser localizado.

Un ejemplo de esto, son los mensajes de error de paquetes ICMP. Si un host interno trata de conectarse mediante paquetes UDP a un servidor externo que no está escuchando en el puerto destino, generará un mensaje ICMP Port Unreachable en respuesta. El firewall de filtrado de circuito es capaz de diferenciar entre este tipo de mensajes de error legítimos a los de un atacante mandando este mismo tipo de mensajes a un host interno.

Esto lo logra haciendo una inspección del payload[11] del tráfico y analiza las características más importantes del mismo para poder realizar un filtrado inteligente.

3.1.8.3 Proxy o Aplicación

Los firewalls mencionados anteriormente, son rápidos, pero pueden ser engañados con facilidad, ya que sacrifican seguridad por ganar velocidad. Entre todos los firewalls estos son los que tienen un performance más lento y resultan ser los más inconvenientes de manejar, como por ejemplo, cuando un protocolo no es soportado, a pesar de esto este tipo de firewalls ofrecen la mayor seguridad. En un ambiente que requiere de alta seguridad el firewall proxy, tendrá como regla de default "denegar si no está explícitamente definido". Esto puede resultar ser un gran problema, cuando algún nuevo protocolo no está aún disponible. Los más importantes firewalls de proxy son Sidewinder, Raptor (de Symantec) y Gauntlet.

Los firewalls proxy esencialmente analizan cada paquete capa por capa, capturándolos en la interfaz de entrada y construyendo un respaldo que fluye a la interfaz de salida. De hecho, el tráfico es liberado a una terminal virtual dentro del firewall proxy, antes de salir por la interfaz de salida, en donde es desencapsulado y examinado. Después de ser comparado contra las políticas del firewall, si cumple, es regenerado y enviado a la interfaz de salida, de lo contrario será desechado. Todo este esfuerzo resulta en un pobre rendimiento y alto costo, pero a la vez muy seguro[15].

[11] Payload. Material transmitido sobre la red que incluye dos cosas: datos e información que identifican el origen y destino del material.

El firewall de proxy mantiene el estado y la secuencia de una conexión TCP, entre dos hosts:

- La sesión del usuario (origen) con el proxy.
- El proxy con el servidor destino.
- Los firewalls proxy utilizan una tabla de procesos para mantener las conexiones en orden.

Desde la perspectiva del destinatario, el tráfico proviene del firewall proxy y no de la fuente. Debido a esto, este tipo de firewalls debe implementar translación de direcciones. Esto puede ser una espada de doble filo; por ejemplo, un servidor destino que aplica una política sobre las direcciones origen, no lo podrá hacer correctamente ya que sólo podrá ver la dirección del proxy. Supongamos que un servidor solamente acepta la conexión de un cliente con la dirección 1.2.3.4, pero como entre ellos existe un firewall proxy con la dirección 2.3.4.5, el servidor no permitirá este tipo de conexión del cliente ya que la petición que llega al servidor proviene de una dirección que no es permitida.

Aunque el servidor puede cambiar la dirección origen a la dirección del proxy, todas las conexiones serán permitidas, no sólo las del host 1.2.3.4. Esto es un gran problema ya que no podrá hacer ningún tipo de filtrado con direcciones IP. Por ellos las políticas de seguridad del servidor tendrán que ser cambiadas.

Si el tráfico de salida pasa por un proxy, tanto los navegadores como otras aplicaciones deberán ser reconfiguradas, esto puede llegar a ser un gran problema en ambientes con cientos de hosts.

Los firewalls que realizan filtrado de aplicación (Capa 7 del modelo OSI) son grandes suites que realizan filtrado de paquetes con control de estado de conexión, además de que incluyen o utilizan software de Proxy para protocolos específicos.

Este software de Proxy analiza los paquetes a nivel de contenido y puede, por ejemplo:

- Filtrar contenidos en transferencias HTTP[12] (*HyperText Transfer Protocol)* o FTP[13] (*File Transfer Protocol*)
- Examinar el tráfico de correo electrónico en busca de SPAM o virus

Este tipo de firewall es ideal para organizaciones que dispongan del capital necesario para mantener este tipo de soluciones, ya que se requiere una gran capacidad de procesamiento para que el análisis del tráfico sea realizado de manera óptima y no se convierta en un cuello de botella, adicionalmente los servicios de soporte y actualización de definiciones de virus y filtros suelen venderse por suscripción anual y a un precio bastante alto.

3.1.8.4 Firewalls Personales

Cambiando un poco de contexto, pasaremos de los firewalls que controlan tráfico de grandes redes y protegen cientos de hosts a los firewalls que se encargan de dar protección individual a computadoras personales y comúnmente residen dentro de las mismas computadoras como software.

Fuertes discusiones sobre cuáles son las mejores soluciones en el campo de la seguridad, se dan diariamente y el tema de los firewalls personales no es la excepción. Existen diferentes y muy diversos productos, cada uno con características particulares, que dificulta la elección de uno. Podemos considerar que una de sus debilidades más comunes, es la falta de filtrado de tráfico de salida, que casi ninguno de los firewalls personales toma en cuenta. Normalmente ellos se centran únicamente en el tráfico de entrada.

El filtrado de paquetes utilizado por los firewalls personales únicamente toma en cuenta el tráfico que va de la red al host y no del host a la red haciendo creer que todos los hosts pueden ser confiables, que no es del todo verdadero.

[12] *HTTP* (HyperText Transfer Protocol), es el protocolo usado en cada transacción de la Web (WWW).
[13] FTP (File Transfer Protocol), es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.

Una de las ventajas más interesantes de este tipo de firewalls personales es el control de filtrado de aplicación. Zone Labs´ Zone alarm, Symantec´s Internet Security and Tinysoft´s Tiny Personal Firewall son algunos ejemplos que contienen este tipo de filtrado. Tienen la capacidad de seleccionar los paquetes entrantes, además de poder configurar una serie de reglas para las aplicaciones. Esto permite poder tener un control más granular del host. Por ejemplo, se puede configurar un regla que permita a una aplicación específica conectarse a una dirección y puerto determinados, o bien, cuando una aplicación trata de concertase hacia el Internet, le da al usuario el poder de decisión ya sea de permitirlo o denegarlo.

Una de las características más sobresalientes es el control que pueden ejercer sobre el sistema operativo. Este tipo de herramientas no permitirán que se ejecute ninguna a aplicación, mucho menos que ésta se conecte a Internet hasta que sea aprobada por el usuario. Alguno firewalls personales como el CalliSoft´s Personal Firewall son capaces de controlar la ejecución de archivos *.exe, incluyendo entre éstos a los famosos caballos de troya.

Existen diferentes opciones bajo la plataforma UNIX, por ejemplo ipchains es un programa que puede proveernos filtrado de paquetes o bien netfilter (iptables) que provee filtrado de circuitos.

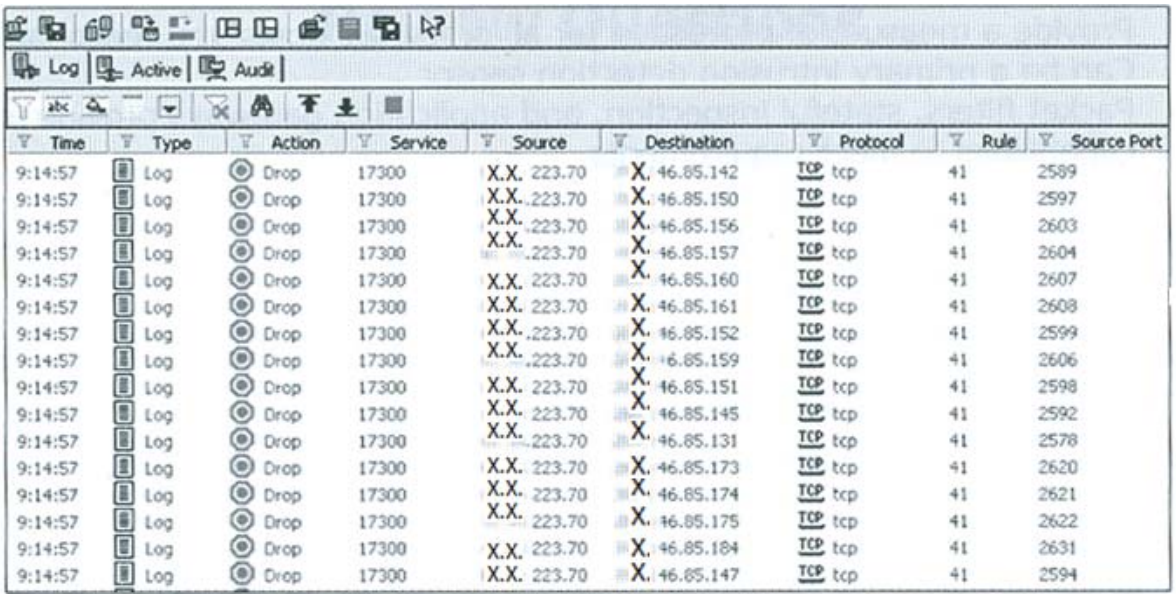
Los firewalls personales pueden ser obtenidos de manera gratuita o tener un costo aproximado de $80 dlls para su uso comercial. Estos deberían ser considerados como un requerimiento indispensable para cada computadora que no está protegida por un firewall de red bajo el control de una organización, como, por ejemplo, cuando una computadora personal de casa o una laptop son conectadas a Internet a través de una red desconocida.

3.1.9 Firewall como un IDS

Una de las capacidades normalmente pasadas por alto de los firewalls es utilizar su función de logging[14] para generar evidencia que pueda ser de gran utilidad en un análisis forense.

La información del log del firewall puede ser de gran ayuda, principalmente, cuando se evalúan los síntomas que conducen a un sistema que quiere ser comprometido y más importante, estos datos pueden ser usados para identificar las intenciones del atacante hacia la red antes de que logre comprometer el sistema.

Por ejemplo, la figura 10 es una pantalla capturada de un firewall en funcionamiento, podemos observar que la dirección origen X.X.223.70 (cuarta columna) está escaneando a diferentes hosts destino de manera secuencial incrementando el cuarto octeto de la dirección IP. También podemos ver que la hora 9:14:57 (primera columna) se mantiene constante y que el número de puerto origen se incrementa secuencialmente para cada host destino escaneado.


Log | Active | Audit

Time	Type	Action	Service	Source	Destination	Protocol	Rule	Source Port
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.142	tcp	41	2589
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.150	tcp	41	2597
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.156	tcp	41	2603
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.157	tcp	41	2604
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.160	tcp	41	2607
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.161	tcp	41	2608
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.152	tcp	41	2599
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.159	tcp	41	2606
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.151	tcp	41	2598
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.145	tcp	41	2592
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.131	tcp	41	2578
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.173	tcp	41	2620
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.174	tcp	41	2621
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.175	tcp	41	2622
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.184	tcp	41	2631
9:14:57	Log	Drop	17300	X.X. 223.70	X. 46.85.147	tcp	41	2594

Figura 10. Firewall en funcionamiento

3.1.10 Topologías de Firewalls

[14] *Logging.* Es la práctica de grabar datos secuencialmente o en orden cronológico

Cuando implementamos una estrategia de protección perimetral para una red, una de las preguntas que surgen en el camino es ¿Dónde se debe poner el firewall para que sea 100% efectivo?. Existen tres topologías básicas recomendables, ya que cada red y sus necesidades son diferentes, pero éstas resultan ser muy convenientes para tener una referencia inicial.

3.1.10.1 Bastión Host

La primera y más básica opción es el uso de una topología bastión host. En este escenario, el firewall es puesto entre Internet y la red protegida. Su misión es filtrar todo el tráfico de entrada o el tráfico que deja la red[17].

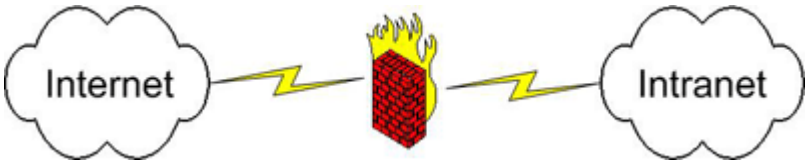


Figura 11. Topología Bastión Host

La topología bastión host es utilizada en redes sencillas, que no ofrecen servicios públicos de Internet. El factor clave a tener en cuenta es que esta topología sólo ofrece un solo frente de protección. Una vez que alguien logra pasar este único perímetro de seguridad logrará tener acceso total a la red privada (en el sentido de protección perimetral). Este tipo de topología es aceptable si sólo se está usando el firewall para proteger una red que solamente es usada para navegar en Internet, pero seguramente no será buena opción si esta red está alojando servicios de Internet como: páginas Web o un servidor de correo (vea figura 11).

3.1.10.2 Subred Monitoreada

La segunda opción, es la topología de Subred Monitoreada. Esta ofrece ventajas adicionales en comparación con una tipo bastión host. Su característica más importante es el uso de un firewall con tres tarjetas de red, tal como se muestra en la figura 12.

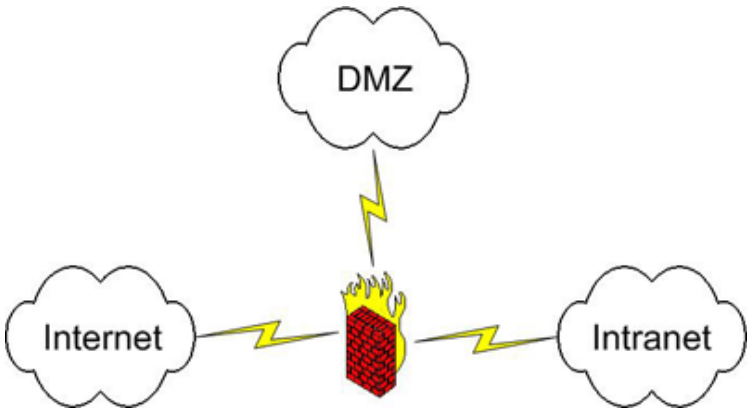


Figura 12. Topología de Subred Monitoreada

La topología Subred Monitoreada provee una solución que permite a las organizaciones ofrecer servicios seguros a los usuarios de Internet. Cualquier servicio público está puesto en la DMZ[15], la que separa a Internet de la red protegida. Por lo tanto, si un usuario malicioso logra comprometer al firewall por medio de los servicios públicos que la red ofrece, éste no tendrá acceso a la red privada, siempre y cuando todo se encuentre correctamente configurado.

3.1.10.3 Doble Firewall

La opción más segura y costosa es implementar una topología de doble firewall. En este caso, la DMZ está puesta entre dos firewalls, tal como se muestra en la figura 13.

[15] *DMZ* (Demilitarized Zone), en español zona desmilitarizada, es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

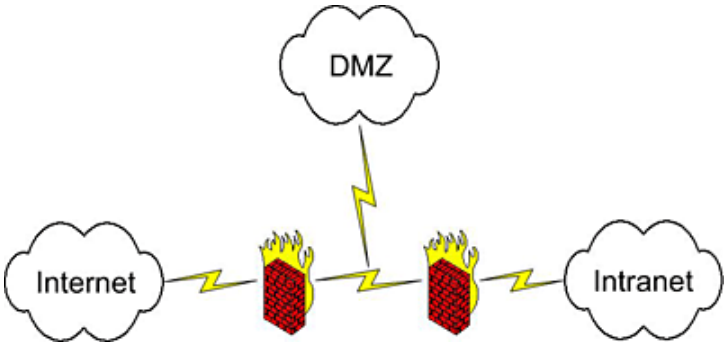


Figura 13. Topología de doble firewall

El uso de dos firewalls permite ofrecer servicios a los usuarios de Internet utilizando una DMZ, proveyendo una capa más de seguridad. Es muy común en las arquitecturas de seguridad implementar este esquema utilizando diferentes marcas de firewalls. Con esto se tiene una capa adicional de seguridad en el caso de que un intruso encuentre cierta vulnerabilidad sobre uno de los firewalls.

Existen firewalls considerados de alto rendimiento que pueden soportar variaciones de este tipo de topologías. Mientras los firewalls básicos algunas veces ofrecen 3 interfaces como máximo, los firewalls de alto rendimiento pueden tener un gran número de interfaces tanto físicas como virtuales. Por ejemplo, existen firewalls en el mercado con hasta 20 interfaces físicas, adicionalmente se puede hacer el uso de interfaces lógicas para la implementación de VLAN´s [16] vinculadas a interfaces físicas. La ventaja más importante que brinda este tipo de firewalls es el poder implementar diferentes zonas de seguridad en la red. Por ejemplo, se podría tener la siguiente configuración en las interfaces, si una organización requiriera barreras de seguridad más fuertes:

- Zona 1: Internet.
- Zona 2: Estaciones de trabajo restringidas.
- Zona 3: Estaciones de trabajo de uso general.
- Zona 4: DMZ pública.
- Zona 5: DMZ interna.
- Zona 6: Servidores con información crítica.

[16] *VLAN (*Virtual LAN), en español Red de Área Local Virtual, es un método de crear redes lógicamente independientes dentro de una misma red física.

3.2 Honeypot

Una de las más recientes metas de la seguridad es tratar de reducir o eliminar amenazas críticas para las redes de las organizaciones. Idealmente, esto se intenta lograr previniendo ataques, pero uno de los lemas claves en la seguridad es “Prevenir es ideal, pero la detección es un deber”.

Es necesario darse cuenta cuando la red podría ser atacada y se requiere estar listos para detectar el ataque lo más pronto posible y tomar ventaja. Una de las formas de hacer esto es usando las tecnologías honey-x, como por ejemplo los honeypots.

3.2.1 Concepto de Honeypot

La función de los honeypots es tan diversa que representa un gran reto su definición. Un honeypot tiene diferentes propósitos para cada tipo de organización. Generalmente, un honeypot es una fuente de información del sistema cuyo valor reside en identificar el uso sin autorización o ilícitamente de la fuente. De hecho su valor radica en su mal uso. La fuente de información del sistema puede ser:

- Un servidor dedicado.
- Un sistema simulado.
- Un servicio en un host específico, como Tiny Honeypot que escucha todos los puertos en busca de un uso ilegítimo.
- Un servidor virtual, como el proyecto honeynet.
- Un archivo con atributos especiales, algunas veces llamado honeytoken.

Cuando las personas escuchan el término honeypot, se imaginan un equipo sin ninguna medida de seguridad que no ha sido parchado y es puesto en Internet, con la finalidad de que éste sea comprometido. Aunque esto funciona bien en un lugar donde no se cuenten con sistemas críticos, simplemente para el propósito de investigación, esto no puede ser aplicado a una DMZ. Nadie quisiera que su DMZ fuera atacada o que quedara comprometida. Si se cuentan con sistemas críticos, lo deseable es mantener a los atacantes lo más lejos posible y no invitarlos a penetrar la DMZ poniendo un equipo que no ha sido parchado[24].

3.2.1.1 Uso de un honeypot

Un honeypot permite entender mucho mejor lo que está pasando en los sistemas claves. Teniendo en cuenta que un servidor típico de web puede tener millones de visitas al día, intentar identificar la diferencia entre conexiones legítimas y los atacantes es imposible. Un segundo uso, es poner en el mismo segmento de red un honeypot tan seguro como el servidor web, cuando algún código malicioso o atacante compromete el sistema, él intentará atacar a los dos, tanto el honeypot como el servidor legítimo. Como el honeypot no tiene ningún uso legítimo, entonces podrá identificarse fácilmente el tráfico del atacante y usar esta información para construir mejores defensas.

Hacer uso de un honeypot implica una gran responsabilidad ya que éste, puede dañar a otros. Por ejemplo, si éste es usado para atacar otros sistemas o algún recurso, los dueños de éste pueden llegar a demandar legalmente.

3.2.2 Ejemplo de un Honeypot

Las organizaciones que hacen uso de honeypots deben tener cuidado de que éstos no incrementen las debilidades y/o decrementen la seguridad. Un honeypot es un sistema desarrollado con la meta de ser atacado. No existen usuarios legítimos para un honeypot. Cualquiera que se conecte a éste deberá ser considerado un atacante. La cuestión de la responsabilidad debe ser altamente considerada, antes de implementarlo se debe consultar la legislación en curso para cuidar de no violar ninguna ley. Por ejemplo una organización de alguna manera motiva al atacante para penetrar los recursos, la organización puede resultar responsable si el atacante utiliza su sitio para realizar un ataque a través de él. Esto quiere decir que, el atacante puede utilizar la plataforma de la organización para lanzar un ataque hacia otros sistemas. Además, si se invita al atacante a romper el sistema, resultara más complicado encontrarlo culpable (vea figura 14).

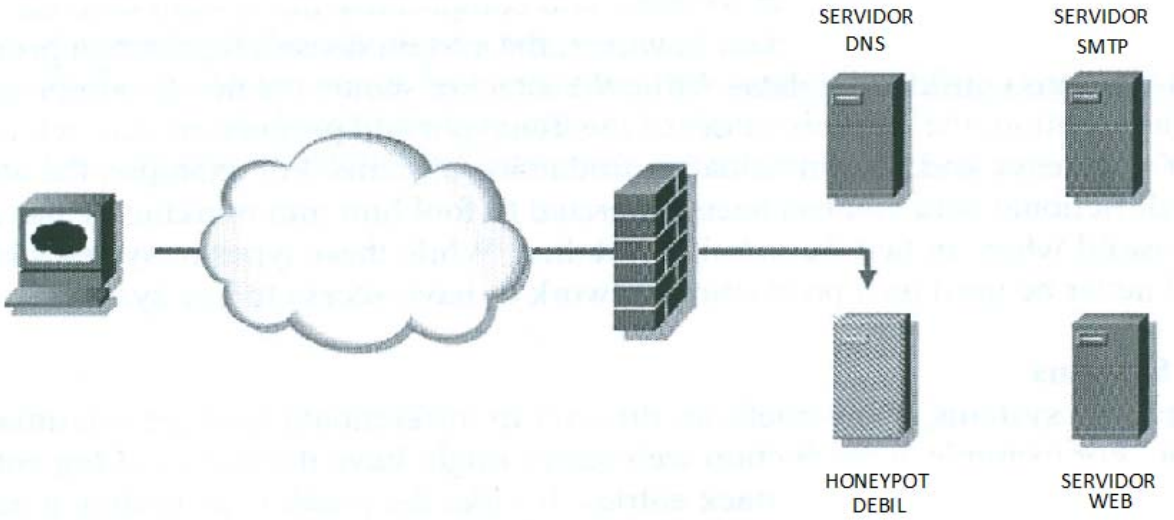


Figura 14. Ejemplo de un Honeypot

Otra gran preocupación referente a los honeypots se ve implicada directamente con la seguridad. Se debe estar seguro de que los honeypots no decrementen la seguridad. Muchos sitios despliegan honeypots como trampas para host, que son configuradas como hosts débiles sin ninguna medida de seguridad. Esto es una situación peligrosa porque un atacante generalmente primero detectará a los host débiles. El atacante tratará de establecer su presencia en la red en un lugar donde pueda comprometer más sistemas. Por tanto, si se pone un host débil en la DMZ, puede ser utilizado por el atacante para comprometer otros sistemas en la DMZ, es por eso que no es recomendable implementar honeypots en una DMZ. De hecho es muy recomendable implementar honeypots únicamente con fines de investigación.

3.2.2.1 Honeypots de investigación

Un honeypot de investigación es un sistema débil, que no ha sido parchado y es vulnerable. Su meta es entender cómo los atacantes penetran los sistemas. Este host débil o honeypot de investigación, le provee al atacante que busca un equipo para comprometer una opción fácil de atacar, con la ventaja de que éste no contiene información confidencial. Mientras el atacante busca en este equipo algún tipo de información que le sea valiosa, el administrador del honeypot y/o de la red puede reaccionar ante la presencia del atacante protegiendo sus sistemas de producción más importantes[34].

3.2.3 Ventajas de un Honeypot

Si se implementan correctamente, los honeypots pueden jugar un rol muy importante dentro de todas las herramientas de seguridad. No existe una herramienta que solucione todos los problemas o una perfecta solución cuando hablamos de seguridad en redes, por eso, es importante entender las ventajas de cada tecnología para poder implementarla correctamente. Algunas de las ventajas de los honeypots son:

- Nos permiten conocer las tácticas, motivo y herramientas que los atacantes utilizan.
- Reduce falsos-positivos[17], falsos-negativos [18]y da patrones para identificar tráfico del atacante.
- Provee defensa en profundidad adicional para las organizaciones.

3.2.3.1 Visión

Uno de los principales propósitos de las organizaciones y desarrolladores que implementan honeypots es aprender acerca de las tácticas y motivaciones de los atacantes. Utilizando los honeypots y viendo cómo los atacantes comprometen los sistemas y lo que hacen después, podremos identificar qué tipo de herramientas utilizan, su nivel de conocimientos y cuáles son los motivos que tiene para atacar el sistema. Además, en redes de gran volumen, los honeypots pueden ayudar enfocándose en el tráfico que genera el atacante, permitiéndoles aislar el tráfico legítimo.

---

[17] Un *falso-positivo*, es un error por el que un software o hardware reporta que un archivo o área de sistema está en peligro, cuando en realidad el objeto está seguro.

[18] Un *falso negativo*, es un error mediante el cual el software o hardware falla en detectar un archivo o área del sistema está realmente en peligro.

3.2.3.2 Reducción de falsas alarmas

Un honeypot se desarrolla para que éste no tenga accesos autorizados, por default todo el tráfico y procesos realizados sobre éste no son autorizados, por decirlo así son ilegítimos. A diferencia de los IDS, que pueden tener falsos-positivos y falsos-negativo, de hecho es una de sus grandes metas a corregir, cualquier tipo de tráfico es almacenado en un log, esto quiere decir que, puede capturar e identificar actividad hostil de exploits que aun no han sido descubiertos.

3.2.3.3 Defensa en profundidad

Algunos honeypots son utilizados para aumentar las técnicas de defensa en profundidad que ayudan a proteger a la organización de los ataques. Como se ha mencionado, el atacante trata inicialmente de comprometer los sistemas más débiles. Si el sistema más débil es específicamente un honeypot, el administrador puede tomar acciones para proteger otros sistemas o bloquear la dirección origen del atacante. Algunos honeypot comerciales extienden esta función en sus productos para hacer monitorear de manera pasiva la red. Cuando el sistema de honeypot es probado y escaneado por atacantes de manera remota, éste puede en forma silenciosa actualizar las reglas del firewall para bloquear el acceso de fuentes específicas, antes de que éstos puedan intentar comprometer recursos que se encuentren en producción.

3.2.4 Desventajas de un Honeypot

Una de las principales razones por la que una organización no implementa honeypots es el riesgo de una mala configuración, la que podría incrementar la amenaza a las redes de producción. Lo último que se quisiera es proveer de una plataforma al atacante con la que pueda extender su ataque por toda la red. Si un atacante logra comprometer un honeypot y el resto de los equipos de producción no están lo suficientemente protegidos, estos correrían un gran peligro.

Otra desventaja es el riesgo de que el atacante se de cuenta de que lo que está comprometiendo no es un recurso de producción, sino un honeypot. Esto puede causar que el atacante se mueva a otra red por el temor de ser detectado por otro honeypot que no pueda detectar. También puede ser que el atacante intente comprometerlo de manera diferente, utilizando tácticas y motivos falsos, confundiendo al administrador.

Un honeypot sólo es exitoso si es escaneado y explotado antes que el atacante descubra otros sistemas vulnerables. Un honeypot solamente puede ver el tráfico que va dirigido hacia él, no identifica si algún otro recurso ha sido comprometido antes que él. Un Honeypot no es lo mismo que un IDS que puede ver todo el tráfico, éste sólo ve lo que pasa específicamente por él. El hecho de que el honeypot no vea el tráfico del atacante no significa que la red esté correctamente protegida.

Los honeypots pueden ser una fuerte carga para las organizaciones, no son una tecnología que se pueda configurar y olvidarse de ella; su implementación requiere constante monitoreo, respuesta rápida y un análisis detallado cuando han sido comprometidos. Si la organización en donde se pretende implementar un honeypot tiene problemas con otras medidas de seguridad, no es recomendable ya que ésta en lugar de ser una ayuda, sería un problema más, que puede traer complicaciones muy graves.

Una de las más complejas cuestiones alrededor de la tecnología de los honeypots es la variedad de implicaciones legales que pueden llegar a tener. Las organizaciones están obligadas a consultar la legislación actual de su país antes de desarrollar cualquier tecnología de honeypot.

En el caso de que un atacante utilice el honeypot de la organización para realizar un ataque, la organización podría ser cómplice, por facilitar las herramientas con las que se dio el ataque.

3.2.5 Clasificación de los Honeypots

Un honeypot es una tecnología que una organización puede implementar. Sin embargo, dependiendo de su clasificación, el rol y función que desempeña es muy diferente. Existen cuatro diferentes categorías[31]:

- Propósito.
- Ubicación.
- Objetivo.
- Interacción.

3.2.5.1 Propósito

Cuando se refiere al propósito de un honeypot, éstos se pueden clasificar en dos grandes categorías.

Honeypots de Producción

Este tipo de honeypots son utilizados como una medida para incrementar la defensa en profundidad de una red. Como ejemplo podemos imaginar un honeypot que sirve de monitor para el escaneo de actividad por parte del atacante hacia otras direcciones, esto permite identificar las intenciones del atacante, así como poder bloquear su dirección origen, antes de que éste logre comprometer recursos de producción. Los honeypots de producción pueden dar información variada de cuál es la metodología del atacante y cómo piensa atacar los sistemas. Adicionalmente este honeypot es capaz de captar ataques que tal vez podrían haber sido para un sistema crítico o de producción.

Honeypots de investigación

Los honeypots de investigación son usados para estudiar las diferentes técnicas y motivos de los atacantes. Aunque estos pueden ser usados como fuente de ayuda en prevención, detección y respuesta. Están diseñados específicamente para grabar las actividades del atacante y sus herramientas. A través de los honeypots podemos identificar los motivos del atacante, cuáles son sus motivaciones sociales, como el formar parte de algo o si sus motivaciones son financieras (por ejemplo, buscando número de tarjetas de crédito) o cualquier otro motivo.

3.2.5.2 Ubicación

La configuración del honeypot y el tipo de información que se espera recibir está basada en la ubicación del honeypot. La Internet está llena de atacantes, por ello no es una sorpresa que un honeypot externo tenga un gran número de conexiones. Generalmente, el propósito de los honeypots externos es tratar de entender el comportamiento del tráfico de un ataque y poder usar esta información para la creación de defensas.

Sin embargo, las amenazas internas y el daño que éstas pueden causar siguen en aumento. Podíamos suponer que en una red interna no deberían existir atacantes. Por lo tanto, un honeypot interno está destinado a encontrar atacantes en la red interna. Dado que es muy común tener un gran número de atacantes internos, es recomendable que el administrador cree una lista de usuarios que necesitan ser vigilados.

3.2.5.3 Objetivo

Los honeypots pueden ser implementados en diferentes niveles de una organización. El método más común es a nivel de sistema, comúnmente llamado honeypot. Este es fácil de configurar y con el uso de vmware[19], puede ser configurado y dado de baja sin ningún esfuerzo. Para un análisis más detallado, se pueden implementar honeytokens, que son archivos individuales o directorios en un sistema que no tienen ningún uso práctico. Finalmente, para tener una mejor visibilidad, se puede implementar una honeynet, que es una red entera de honeypots, ésta puede ser configurada utilizando tecnologías de vitalización.

3.2.5.4 Interacción

Otra clasificación de los honeypots está basada en el nivel de interacción del atacante con el honeypot. Un honeypot de baja interacción es el que ofrece pocos

[19] *Vmware*, es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un ordenador, un hardware) con unas características de hardware determinadas.

servicios, que el atacante pueda utilizar, por ello es fácil de mantener para el administrador. Un honeypot de alta interacción es el que le ofrece todos los servicios disponibles al atacante para ser utilizados, lo que resulta más complicado de mantener para el administrador.

Como los honeypots de alta interacción resultan ser muy flexibles para los atacantes, éstos representan una fuente de investigación muy grande para el administrador.

3.2.6 Proyecto honeynet

Los honeypots son excelentes para detectar ataques antes de que éstos alcancen los sistemas de producción. Sin embargo, las metas del proyecto honeynet son un poco diferentes. Fundado por Lance Spitzner en abril de 1999, el proyecto honeynet está constituido por 30 profesionales de la seguridad, que voluntariamente donan su tiempo y recursos con el propósito de hallar nuevas herramientas de ataque y técnicas que están en uso en Internet.

El proyecto honeynet está compuesto por redes enteras compuestas por honeypots. De manera ideal una honeynet incluye diferentes tipos de sistemas operativos, servicios, y hardware de red con una configuración que imita a un ambiente de producción. La mayor diferencia es que toda la actividad, no importa sí esta es muy insignificante es almacenada y analizada. Después de todo, si suponemos que ningún usuario real debería de interactuar con las máquinas, toda actividad debe ser resultado de usuarios no autorizados. El proyecto honeynet cree fuertemente en la importancia de las honeynets y muestran de manera pública todas sus herramientas y resultados a la comunidad de la seguridad informática[32].

El proyecto ha dividido su trabajo en cuatro generaciones, cada una representa parte importante de la evolución del mismo. La primera generación se enfatizaba en la captura de datos y el control de los mismos. En otras palabras, usaban una combinación de las técnicas estándar de logs, rutas de los paquetes capturados como un sniffer de red y los logs del firewall para examinar el tráfico de la red que pasa entre la honeynet y la Internet. También implementaba soluciones para controlar el número de conexiones hacia el exterior que el atacante generaba cada hora. Esto ayudaba a proteger los sistemas en contra de gusanos, herramientas de denegación de servicio y otros tipos de código malicioso que podrían atacar otros sistemas fuera de la red. Esta fase del proyecto fue

completada en el año 2001 y sus resultados fueron publicados en una serie de artículos titulados "Know your enemy[20]" (ver figura 15).

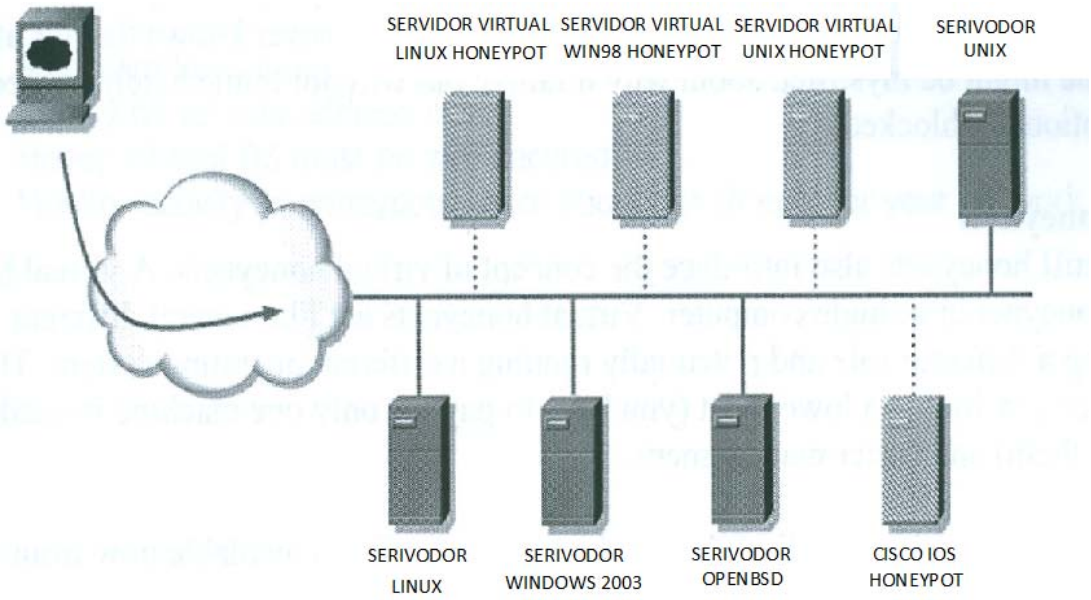


Figura 15. Ejemplo de Honeynet

La segunda generación fue empezada a construir en el año 2001, con base en las lecciones aprendidas de la primera generación. Esta generación de honeynets son más fáciles de implementar y hacen más difícil para el atacante detectar que ha sido engañado. La razón principal por lo que son más fáciles de configurar, es porque, unen todos los datos capturados en un solo lugar, como por ejemplo los logs de los servidores, sniffers y firewalls. Un gateway customizado de capa 2 actúa como capturador de todo el tráfico que entra y sale de la red, además del tráfico que se genera en el interior de la honeynet. Esto pone a la organización en la posición perfecta para ver todo lo que está pasando en el sistema. Como opera en Capa 2 del modelo OSI, este Gateway no cuenta con un stack de direcciones IP, por ello es invisible a escaneos de red.

La primera generación de honeynets captura casi todos sus datos examinando los logs de los paquetes, pero las sesiones cifradas generadas por ejemplo con SSH eran inmunes a esta técnica de recolección.

[20] *Know you enemy*, en español significa conoce a tu enemigo.

La segunda generación resolvió este problema adicionando algunos módulos al kernel de cada honeypot, que les permiten almacenar los datos en un log una vez que han sido descifradas.

Las tecnologías de la segunda generación en cuanto a control de datos fueron mejoradas. Algo que simplemente contaba el número de conexiones salientes que cada sistema generaba por hora, fue mejorado para que estas conexiones fueran dirigidas a un IDS. A los paquetes que no parecieran ser maliciosos se le permitía el libre paso. Aquellas conexiones que parecían tener comportamientos extraños, de igual manera eran permitidas después de un proceso especial. Este proceso consistía en modificar el exploit para que fuese inofensivo. El atacante nunca se daba cuenta de que su ataque había sido modificado y no tenía forma de percatarse de lo que sucedía, hasta después de un tiempo notaba que había sido intencionalmente bloqueado.

Finalmente, en la segunda generación de honeynets se introdujo el concepto de honeynets virtuales. Una honeynet virtual es una honeynet entera en una sola computadora. Las honeynets virtuales actúan como diferentes tipos de sistemas, cada uno jugando un rol diferente y corriendo un tipo diferente de sistema operativo. Esto tiene numerosas ventajas, incluyendo el bajo costo, ya que se necesita pagar por una sola máquina en lugar de una red completa y su fácil mantenimiento. Su desarrollo tuvo fin en el año 2004, dando paso a dos siguientes generación.

La tercera generación nace en el año de 2005, esta expande todas las soluciones de la segunda, enfocándose principalmente en hacer que la tecnología sea más fácil tanto de implementar como de manejar. Esta generación de honeynets está basadas inicialmente en un live-cd[21] que contiene un Gateway honeynet. Lo único que se tiene que hacer para crear una honeynet es poner el Gateway al frente de sistemas estándar y arrancar el Gateway desde el cd. Esto es muy útil para simplificar la implementación de una honeynet, pero limita el performance y capacidades por la naturaleza de sólo lectura de los drives de CD-ROM.

Actualmente se continúan haciendo modificaciones a la tercera generación para poder dar paso a una cuarta, la cual mejore las capacidades de implementación en live-cd y sea más difícil de identificar por parte del atacante.

[21] *Live-cd*. Es un sistema autónomo en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de ficheros.

3.2.6 Implementación de Honeypots

Cuando se implementan honeypots, es buena idea empezar con algo pequeño y entender cómo es que trabaja. Se necesita monitorear con detenimiento el honeypot, además de aprender las técnicas y tácticas que utiliza el atacante. Conforme el nivel de conocimiento acerca de cómo funciona el honeypot se incrementa, se podra incrementar el nivel de interacción con el atacante para poder aprender más de él. Los siguientes son los pasos que se deben seguir al momento de implementar honeypots:

1.- Empezar con un honeypot de baja interacción con fines de investigación. Los honeypots más simples y fáciles de implementar son los de baja interacción. Con esto, se puede conseguir valiosa información, sin interactuar con el atacante. Entre más se interactúe con el atacante, más complejo será el sistema y su complejidad. Después de implementar un honeypot de baja interacción y poder entender toda la información que éste recibe, entonces se podrán implementar más honeypots con un mayor nivel de interacción con el atacante.

2.- Implementarlo en un espacio de direcciones que no esté en uso. Se debe tener mucho cuidado al implementar honeypots en un espacio de direcciones que estén en uso. Es muy fácil que un ruteador se desconfigure o peor aún, que un honeypot asuma la identidad de un sistema de producción ocasionando con eso una denegación de servicio para los usuarios legítimos.

3.- La herramienta a utilizar para implementar el honeypot debe ser segura. Aquellos honeypots que emulan el sistema operativo de diferentes hosts tienen una gran ventaja, ya que el atacante direcciona los ataques en contra de hosts virtuales mientras el sistema del honeypot no sufre daño alguno. De igual forma, es importante asegurar el sistema operativo del host que controla el honeypot para prevenir que éste sea comprometido y manipulado por el atacante.

4.- Monitorear la actividad del honeypot y aprender acerca de las amenazas a la red. Finalmente, es importante mantener un monitoreo constante sobre los honeypots, asegurando que no son manipulados con fines maliciosos en contra de otros sistemas. Si no se dispone del tiempo necesario y el conocimiento suficiente para su monitoreo sería una mejor idea no considerar su implementación.

3.2.7 Honeypot Checklist

Para asegurar que una organización implemente correctamente honeypots, necesitamos abordar los siguientes puntos clave:

- Estar seguros que tendremos los recursos necesarios para el análisis de los resultados.
- Determinar si un honeypot es la mejor solución .
- Determinar si un honeypot disminuirá los posibles riesgos.
- Identificar qué información obtendremos del honeypot.

Recursos

Un honeypot no es una herramienta que pueda instalarse y olvidarse. El valor de un honeypot reside en analizar toda la información capturada y ser usada para incrementar la seguridad. Tener mucha información normalmente no tiene un gran valor, si ésta no es revisada y analizada a conciencia, de lo contrario sólo estaría utilizando espacio y recursos que pudiéramos utilizar en otras cosas o bien estos pueden ser comprometidos, lo que no sería conveniente.

Si se cuenta con los recursos para analizar la información almacenada por el honeypot, se debe preguntar si es buena idea gastar una gran cantidad de tiempo haciéndolo. Por ejemplo, si las reglas del firewall no han sido correctamente configuradas o los no han sido blindados, no tiene mucho sentido tener un administrador que gaste tiempo revisando el honeypot, cuando existen otras prioridades que deben ser atendidas, ya que pueden presentar un riesgo mayor.

¿Es la solución adecuada?

Los honeypots son una herramienta novedosa que tiene un factor de moda muy alto, es por eso que mucha gente quiere implementarlos. Sin embargo, la organización necesita estar segura, si un honeypot es la mejor solución a sus problemas. Para cualquier solución de alto riesgo, lo primero que se debe hacer es identificar las posibles soluciones, realizar un breve análisis del costo-beneficio y después, escoger la solución más apropiada. Por ejemplo, si un nuevo gusano es propagado por la Internet, es mejor bloquearlo con el firewall que dejarlo pasar para analizarlo con un honeypot.

Reducción de riesgo

La meta de la seguridad es disminuir o eliminar por completo los riesgos, lo menos que queremos es que se incrementen. Los honeypots están hechos para ser escaneados, conectados y comprometidos por los atacantes, aunque esto a veces puede incrementar potencialmente los problemas en lugar de darles solución. Por lo tanto, para asegurar su valor, es necesario que el honeypot sea cuidadosamente diseñado e implementado. Un honeypot sin monitoreo o análisis puede ser rápidamente comprometido, especialmente si el atacante comienza hacer daño sin consentimiento.

Metas claras

Antes de que una solución sea implementada, sus objetivos deben ser documentados claramente. Entonces, las metas serán compradas contra los riesgos. Si no se puede encontrar una solución para un riesgo, es mejor no implementarla. Después de que los objetivos hayan sido validados, la implementación del sistema será comparada con los objetivos, para asegurar que éstos se cumplan. Si alguno no se logra, la solución será modificada o en su defecto descartada.

Conclusiones Capítulo 3

En este capítulo se presentaron dos métodos para el riesgo del manejo de la información. Los dos operan junto con la red para proteger los sistemas de atacantes en Internet. Se señalaron algunos de sus beneficios y desventajas de cada uno.

Los firewalls proporcionan una buena relación entre costo y efectividad para la protección y detección de intrusos. Aunque existen diferentes tipos de firewalls, se pueden dividir en tres categorías: proxy o aplicación, filtrado de paquete o filtrado de circuito. Dependerá de las necesidades y capacidades de adquisición de cada organización el decidir qué herramienta es la mejor para ellas. En la actualidad es casi una obligación tener un firewall, desde equipos personales hasta las grandes organizaciones deberán tener la capacidad de instalarlo, configurarlo y darle el mantenimiento necesario, ya que si todos cumplimos con esto, el número de ataques y amenazas en la red disminuirían considerablemente.

También se analizó otra técnica novedosa: los Honeypots. Permiten ver de manera clara el tipo de ataque que se quiere llevar a cabo en la red y/o sistemas, además de poder identificar de dónde proviene. Toda la información que recolecta un honeypot será de gran ayuda para poder eliminar las vulnerabilidades de los sistemas, además de, aprender de cada evento que quede registrado en ellos. Se debe considerar que en un honeypot siempre existe la posibilidad de que éste sea comprometido por el atacante, implicando con esto, un riesgo legal para la organización, ya que este puede ser utilizado para atacar a otros equipos y podríamos ser acusados por ello.

Capítulo 4. Escaneo de Vulnerabilidades

En este capítulo se abordarán tecnologías, herramientas, técnicas usadas para la obtención de información, mapeo de redes y escaneo de vulnerabilidades además de aprender cómo es el manejo de las tecnologías utilizadas para mapear y escanear.

4.1 Introducción al Escaneo de Vulnerabilidades

Ya sea que se esté en busca de un sistema específico o sólo a la expectativa de un objetivo débil, un atacante utiliza un arsenal de herramientas para automáticamente localizar nuevos sistemas, mapear redes externas y probar vulnerabilidades específicas que puedan ser explotables. Este primer paso del ataque es llamado de reconocimiento y puede ser lanzado por el atacante mucho tiempo antes de que saque ventaja de las vulnerabilidades y tenga acceso al sistema y/o redes. De hecho, la evidencia recogida de la actividad de reconocimiento puede ser una pista de que un nuevo ataque puede ser dirigido a ese sistema o red.

Aquellos a cargo de la seguridad de los sistemas como de la red, no pueden permitirse el lujo de ser menos competentes en descubrir y eliminar sus vulnerabilidades antes de que los atacantes las encuentren y logren explotarlas. Una estrategia es hacer uso de cada herramienta que se tenga disponible, en contra de la propia organización para poder identificarlas, además, este proceso deberá ser repetido constantemente.

4.2 ROI [1] (Return on Investment)

ROI se puede interpretar como el cálculo del beneficio económico o recompensa recibida que se obtendrá al proporcionar una cantidad de dinero o un capital de inversión para un producto, servicio o negocio.

Este término es usado comúnmente en el campo de tecnologías de la información y seguridad de la información y es calculado con la siguiente fórmula:

[1] *ROI* (Return on Investment), se conoce en español como Retorno de la Inversión.

ROI= (ganancia – gastos)/(gastos) X 100%

Los usos más comunes de ROI se aplican en el desarrollo de algún negocio, para evaluar si es viable la compra de un producto, servicio o la predicción de ingresos. Recordemos que cualquier gasto en seguridad no deberá ser mayor que el costo del que se pretende proteger. La seguridad normalmente es considerada un gasto inútil por algunas empresas ya que sus beneficios no son tangibles hasta que algún tipo de amenaza se consolida.

4.2.1 Reconocimiento + Protección de los Recursos + ROI = R^3

Normalmente los programas de escaneo de vulnerabilidades no son utilizados inteligentemente. El mejor uso que se le puede dar a cada peso invertido en seguridad, será que cada herramienta de escaneo que se adquiera tenga un sólido proceso de remedio a los posibles problemas. Escanear sin ofrecer soluciones puede llegar a ser considerado como negligencia en algunos casos. Conocer las vulnerabilidades es un estado crítico en la protección de los recursos. Es por eso que debe estar seguro de que todos los encargados de la seguridad entiendan perfectamente lo que ROI significa y puedan empezar a aplicarlo en el manejo de vulnerabilidades.

4.3 Vectores de Ataque

La primera meta es entender cómo se manifiesta y cómo se puede controlar una amenaza, esto será indispensable en el escaneo de vulnerabilidades y sus remedios. Si no existen vulnerabilidades, la amenaza no podrá ser manifestada. Sin embargo, muchas clases de vulnerabilidades son imposibles de detectar con un escaneo de vulnerabilidades estándar.

En términos de los controles que podemos utilizar, necesitamos que tanto los controles defectivos, correctivos y preventivos trabajen en conjunto para aumentar el nivel de protección. La detección es la acción de poder identificar la amenaza, lo controles correctivos actuarán en contra de la amenaza una vez que haya sido detectada. La prevención es otra medida de contención, que permite evitar que lleguen a estar en contacto las vulnerabilidades con las amenazas.

Las formas o lugares en las que se pueden presentar las amenazas son también llamadas vectores. Los podemos clasificar en 5 diferentes grupos:

- Ataques que provienen de afuera desde una red.
- Ataques que provienen de afuera desde un teléfono.
- Ataques que provienen del interior de la red.
- Ataques que provienen del interior desde un sistema local.
- Ataques por algún tipo de código malicioso.

Algunas de las amenazas que más preocupan a las organizaciones y en consecuencia las más comunes son:

- Códigos maliciosos que pueden ser ejecutados con el fin de borrar la información de los medios de almacenamiento.
- Correos maliciosos que pueden exponer información sensible en la Internet.
- Servidores de WEB comprometidos que pueden hacer quedar en vergüenza a la empresa.
- Servidores WEB que pueden exponer datos privados de clientes.
- Trabajadores enojados con la organización ejecutando bombas lógicas.
- Trabajadores traidores que venden información secreta de la compañía.
- Secretarias engañadas mediante ingeniería social proporcionando información clasificada a adversarios.
- Hacker que penetra el sistema y tiene acceso a la información.

Una buena manera de saber cuáles son las vulnerabilidades que se deben atender primero, son las que pueden causar mayor impacto a la organización.

4.4 Sobrepasando Firewalls

El firewall es el dispositivo en el que ponemos las primeras esperanzas. Por tanto, se debe considerar que existen diversas formas de sobrepasarlo y penetrar el sistema. Esto incluye: gusanos, troyanos, redes inalámbricas, conexiones por módem, HTTP Tunnel, VPN´s, laptops, etc.

El punto clave es, si se basa el manejo de riesgos en la toma de decisiones del firewall y éste es sobrepasado, probablemente se necesite replantear el manejo de riesgos, ya que no será de lo más confiable que se pueda tener.

4.4.1 Kazza

Las redes P2P se han vuelto muy comunes en los últimos años y simultáneamente han introducido una nueva amenaza de Internet. Kazaa, Morpheus, Napster y Gnutella son sólo algunos ejemplos de este tipo de redes que han surgido recientemente. En esta sección se analizara únicamente Kazaa, pero otro tipo de redes y protocolos ofrecen funciones y amenazas similares.

La aplicación Kazaa llamada KDM (Kazaa Desktop Manager), actúa como un servidor de archivos que a su vez actúa como cliente, al buscar y descargar archivos de otros usuarios de Kazaa.

Cuando uno busca un archivo en particular, la red Kazaa hace uso de servidores con gran ancho de banda llamados supernodos, para localizar hosts a los que se está conectado y a su vez a cuáles están conectados ellos y así consecutivamente. Cuando el archivo es encontrado, la aplicación Kazaa podrá descargar el archivo estableciendo una conexión TCP del cliente remoto.

Kazaa fue diseñado con el propósito de ser gratuito, fácil de utilizar y lo más importante llevar a cabo el intercambio anónimo de la información. Es ahí donde radica su lado oscuro ya que esto implica severas debilidades de seguridad para los usuarios que lo utilizan. La primera preocupación es que los usuarios de Kazaa situados detrás de un firewall rompen de manera efectiva la protección que éstos le brindan, así, este usuario podrá conectarse a una red externa. Sin embargo, Kazaa también revela información importante acerca de la red interna, que debería ser privada. Esta información puede ser utilizada para lanzar algún ataque de denegación de servicio. El programa Kazaa también puede ser un medio de entrada (vector) que puede utilizar los caballos de Troya para penetrar el sistema. Es por eso que la popularidad de kazaa ha aumentado considerablemente en la comunidad hacker.

Normalmente los usuarios no están muy bien enterados de las políticas de seguridad de su organización y, si lo están, no las cumplen si éstas van en contra de sus intereses. Normalmente ellos saben o intuyen que lo que están haciendo está mal, pero aún así lo hacen sin darse cuenta de todos los riesgos que pueden correr. Supongamos que el firewall de una organización permite cualquier tipo de conexión que se origina desde adentro hacia el exterior, en este caso el vector de amenaza serían los mismos usuarios.

En la figura 16 se muestra cómo Kazaa puede sobrepasar un firewall. En la izquierda, el host A esta detrás de un firewall y se conecta con el host B, haciendo una red Kazaa. El firewall permite al host A iniciar comunicación, ya que en este escenario se permiten todas las conexiones hacia el exterior. El firewall denegará el acceso a una conexión TCP por parte del host C, entonces C no podrá iniciar una comunicación con el host A. Sin embargo, Kazaa provee de un mecanismo que permitirá que el host C rompa la protección proporcionada por el firewall y establezca conexión con el host A.

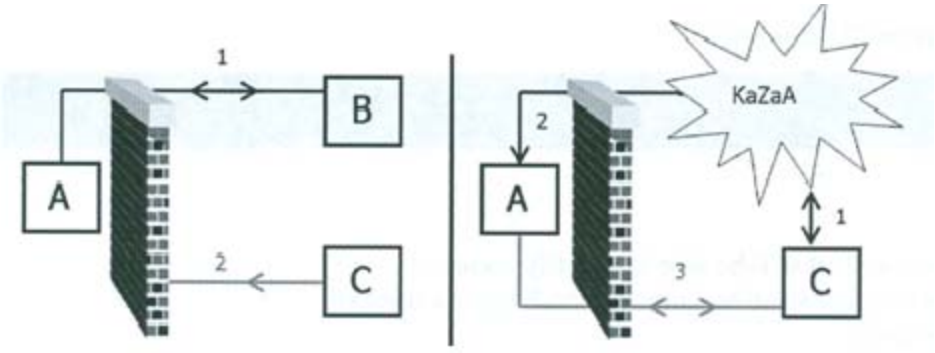


Figura 16. Sobrepasando un firewall con Kazaa

En la figura 16, el host C establece una conexión a la red Kazaa, que previamente estaban conectados A y B. Como el host B está usando el protocolo Kazaa, el host C ahora puede ver los archivos del host A. Para poder descargar archivos el host C necesita establecer una conexión TCP con el host A, por ello envía esa petición a la red Kazaa que la hace llegar al host A, obligando al host A a iniciar conexión con C. Ya que el firewall no provee las conexiones que se inician en el host A, se podrá conectar con el host C sin ningún problema. De manera indirecta se logró que el host C estableciera una conexión con un puerto a través de un firewall que no permitía conexiones TCP del exterior ha aplicaciones no conocidas.

4.4.1.1 Información de Red

Cuando se busca un archivo o se descarga en la red Kazaa se suele dejar un cierto rastro, que contiene información valiosa para el atacante, como: una dirección IP activa de la red, el estado de una conexión y/o la secuencia de la conexión TCP, el número de ACK y la dirección MAC. Aunque se sabe que la seguridad no debe ser implementada mediante la obscuridad, éstos son datos que no deberían ser compartidos con nadie a través de Internet.

4.4.1.2 Ataques de Denegación de Servicio

Además de compartir información confidencial, Kazaa puede actuar como medio para realizar un ataque de denegación de servicio. Por ser compatible con NAT, Kazaa incorpora la posibilidad de suplantar tanto puertos como direcciones IP. Dicho esto, el atacante puede suplantar la identidad del host víctima anunciando que tiene en su poder ciertos archivos que sean de interés para una gran cantidad de personas, éstas tratarán de conectarse y enviarán simultáneamente paquetes SYN para tratar de iniciar la conexión. Todos estos host contribuirán al ataque al tratar de descargar estos archivos que aparentemente ofrece el host víctima, provocando así una denegación de servicio.

4.4.1.3 Troyanos

La mejor forma de distribuir un troyano, es alterar un producto que es usado por multitudes. En marzo de 2002 se ofreció una versión de Kazaa por Internet que contenía software adicional, llamado *"Brilliant Digital Entertainment".* El propósito de este software era permitir que este programa estableciera su propia red P2P dentro de la red Kazaa. Esta red distribuía anuncios, propagandas, contenido multimedia sobre archivos ejecutables.

Kazaa es un ejemplo específico del daño que puede causar instalar software no autorizado dentro de una organización. Cada cambio que se realiza en la configuración debe ser analizado cuidadosamente, para que no introduzca nuevas vulnerabilidades. Como Kazaa existen otro tipo de productos con sus propias vulnerabilidades que deben ser tomadas en consideración.

4.4.2 Firewalls, Conexiones Inalámbricas y Módems

Sabemos que aplicaciones como Kazaa no son la única manera de pasar un perímetro de seguridad. Algunas veces, la propia topología de red actúa en contra de las organizaciones. Supongamos que en una organizacion está conectada hacia Internet a través de un ruteador cisco configurado como firewall. Detrás de este ruteador existe un firewall dedicado. ¿Podrán estos sistemas ser alcanzados con facilidad?, la respuesta es sí. Si alguno de los dispositivos de la red contara con una tarjeta de red inalámbrica podría realizarse una conexión con el exterior pasando así el doble perímetro de seguridad.

O peor aún, sí alguno de los sistemas cuenta con un módem, igualmente podrá establecer una conexión. De hecho los módems son uno de las principales y más comunes herramientas para pasar un firewall.

4.4.2.1 Módems

Entre más restrictiva sea las políticas del firewall, los empleados tratarán más de romperla. Existen dos maneras, por lo menos, de utilizar un módem en contra de un firewall. La primera es iniciando una conexión a Internet a través de él, la segunda es que aunque no se inicie desde adentro el atacante pueda hacer contacto con él y éste le responda de manera automática.

El modo de auto-contestación no es muy bien entendido por los administradores. Si se deja un módem configurado en este modo, el atacante eventualmente podrá localizarlo a través de aplicar la técnica de "war-dialer[2]" y tener acceso remoto a él. La mejor defensa en contra de este ataque es revisar todos los módems periódicamente para asegurarnos que no se encuentren en modo de auto-contestación.

Actualmente otra forma más común es establecer una conexión con un ISP a través de un módem, con esto se tendría una conexión de tipo bidireccional. Muchas organizaciones entienden alguno o todos los riesgos que se corren al conectarse a Internet por medio de un ISP, por ello bloquean ciertas conexiones por medio de un firewall haciendo uso de ACL´s. Aunque tomen todas estas precauciones, cualquier sistema

[2] *War dialer*. Técnica que consiste en hacer llamadas a una serie de números de teléfono automáticamente con el fin de encontrar módems conectados y permitiendo la conexión con algún equipo e inclusive toda la red.

conectado a la red por medio de un módem, no estará protegido bajo ninguna circunstancia.

La figura 17 da una idea de cómo este tipo de ataque es totalmente exitoso. Por un lado, contamos con un firewall perfectamente configurado, con las mejores políticas que una organización pudiera tener. El firewall está realizando su trabajo perfectamente, pero el perímetro de seguridad no es suficiente para protegerlo completamente. En este caso el vector de amenaza es el módem que se conecta con un ISP externo.

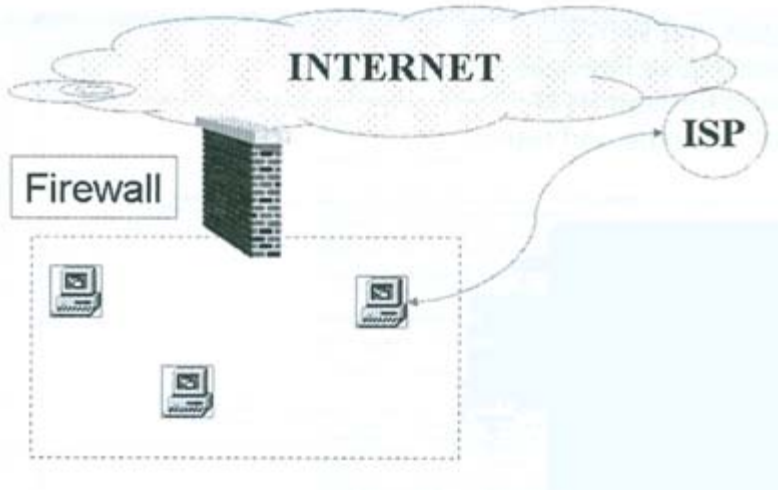


Figura 17. Sobrepasando un Firewall con un Módem

4.4.2.2 Túnel HTTP

El lenguaje HTTP es un lenguaje de marcado, no un lenguaje de programación propiamente, esto quiere decir que permite codificar un documento que, junto con el texto, incorpora etiquetas o marcas que contienen información adicional acerca de la estructura del texto o su presentación, dentro de estas estructuras se puede insertar código binario que podrá pasar el firewall rompiendo el perímetro de seguridad. Este ocurre porque el puerto 80 y el 443 siempre están abiertos. Este ataque es posible de detectar manualmente, pero no es viable ya que pueden estar pasando cientos de páginas a través de el firewall dificultando esta tarea. Afortunadamente existen herramientas que pueden ayudar.

4.4.2.3 Ingeniería Social

Las personas son normalmente el punto más débil en los esquemas de seguridad. Ni juntando toda la tecnología se podría proteger una red de un usuario que proporcione su contraseña a otra persona o inconscientemente instale un software malicioso.

Ingeniería social es el término utilizado para describir el intento de manipular o engañar a una persona para que proporcione información valiosa o permita el acceso a la misma. Es el proceso de atacar una red o sistema explotando a las personas que interactúan con ellos.

La ingeniería social se aprovecha de la naturaleza del humano, en su deseo de ayudar, el miedo a tener problemas o la tendencia que tiene en confiar en la gente y sistemas con los que interactúa.

4.4.2.4.1 Ingeniería Social basada en los humanos

La mayor parte de la ingeniería social se basa en los humanos, engañando a una persona con el fin de obtener información. La mejor forma de lograrlo es utilizando técnicas tales como, imprimir urgencia, que sea impersonal, además de hablar por otra persona. Un clásico ejemplo sería la siguiente llamada telefónica: “Bueno, mi nombre es Juan Pérez y soy el vicepresidente de la empresa, me encuentro de viaje y no recuerdo mi contraseña, ¿la podrían restablecer?, estoy en espera de un mail urgente para asistir a una junta”. Mucha gente al presentársele este escenario accede casi de manera inmediata a cumplir sus peticiones, porque tratan de ser serviciales, ya que la persona que llama es el vicepresidente y si no lo hicieran podría tener graves consecuencias para ellos.

5.4.2.4.2 Ingeniería Social basada en computadoras

La ingeniería social también puede estar basada en computadoras. Por ejemplo: un usuario esta navegando en la red, cuando de repente en su navegador aparece un

ventana de pop-up[3], en la que le indica que su tiempo de conexión ha terminado y necesita volver a poner su usuario y contraseña, para volver a conectarse. Esta es una forma muy común en la que el atacante puede robar la contraseña de la víctima. También, algunos de los gusanos más recientes que vienen junto con un mail, contienen leyendas que tratan de obligar al usuario para que abra un attachment[4] y muchos de ellos lo hacen a pesar de que conocen el peligro que corren. Explotar la curiosidad del humano, su incredibilidad o su codicia, automáticamente por medio de mails masivos, es puro trabajo de ingeniería social.

Estos ejemplos muestran cómo la misma naturaleza del ser humano le permite al atacante acceder a las redes y/o sistemas. ¿Para qué tratar de pasar un sistema por la fuerza, si es posible que alguien del interior abra la puerta?

5.4.2.4.3 Defensas ante la Ingeniería Social

Defenderse de la ingeniería social es una de las cosas más difíciles en el ámbito de la seguridad. La debilidad más grande es la facilidad con la que un humano puede brindar su ayuda. Tecnológicamente hablando, productos de defensa perimetral (como por ejemplo: algún antivirus que permita proteger a una organización de algún usuario que ejecute en su equipo algún virus o troyano), pueden brindar cierto tipo de protección. Sin embargo, la mejor herramienta es establecer políticas de seguridad y asegurar que éstas se cumplan.

Las políticas de seguridad deben establecer claramente diferentes tipos de cosas, como quién está autorizado para entrar, qué personas pueden autorizar un acceso y bajo qué circunstancias éste se puede permitir. Adicionalmente, se establecerán procedimientos para la activación y desactivación de cuentas, cambio y restablecimiento de contraseñas, además de establecer cuáles son sus derechos y privilegios de cada una. Finalmente, educar a los usuarios acerca de las amenazas a las que pueden ser expuestos al navegar en la red. En muchos casos, los usuarios crean sin darse cuenta problemas de seguridad, debido en gran parte a su ignorancia. Si los usuarios tienen un plano general de todos los peligros que pueden correr, podrán guardar su distancia y estar prevenidos ante cualquier tipo de contingencia.

En cierto sentido, se puede considerar que todos los ataques son producto de la ingeniería social. Cualquier tecnología o técnica que utilice el atacante, siempre producirá un efecto en la víctima. Por esta razón, es que mucha gente empieza a sentirse indefensa

[3] *Pop-up.* El término denomina a las ventanas que emergen automáticamente (generalmente sin que el usuario lo solicite) mientras se accede a ciertas páginas Web.
[4] *Attachment.* Es un archivo que se envía junto a un mensaje de correo electrónico

ante el gran número de amenazas y la manera tan rápida en la que estas crecen y se manifiestan. Se debe procurar estar siempre al tanto de las noticias, boletines, etc., para mantenerse lo más actualizado posible y así poder responder ante las amenazas con gran rapidez.

Mucha gente confía excesivamente en sus firewalls, creen que por tener uno de ellos estarán a salvo de todo peligro. Los firewalls son importantes, pero ellos como cualquier herramienta de defensa tienen limitaciones, algunas de las más importantes se han mencionado anteriormente, pero no son las únicas que existen, diariamente se crean nuevas y más novedosas amenazas que ponen en peligro los bienes más preciados de las organizaciones.

4.5 Escaneo de Redes

El lema de la compañía SUN es: "The Network is the Computer[5]" y en el momento en que se esta viviendo esto es más cierto que nunca. Tanto negocios pequeños como empresas multinacionales; desde pequeñas redes caseras hasta redes de cafés Internet, el número de computadoras y dispositivos se ha ido incrementando de igual forma que las redes lo han hecho y no sólo por el trabajo que desarrollan en lo individual sino por lo que hacen en conjunto.

Scott McNealy co-fundador de Sun Microsystems, comenta:

"There's a pendulum thing where stuff is on the client side and then goes back into the network where it belongs," the magazine quoted him as saying. "The answering machine put voicemail by the desk, and then it went back into the network." He continued, "Your iPod is like your home answering machine. I guarantee you it will be hard to sell an iPod five or seven years from now when every cell phone can access your entire music library wherever you are."[12]

En la cita anterior Mcnealy hace una semejanza entre cómo en el pasado las máquinas contestadoras eran muy importantes y en la actualidad lo han dejado de ser porque podemos enviar mensajes instantáneos a la persona con la que se quiere

[5] *"The Network is the Computer"* significa "La red es la computadora"

comunicar. Además, considera que en un lapso de 5 a 7 años el ipod será obsoleto, ya que cualquier dispositivo portátil podrá conectarse a una biblioteca de música infinita donde quiera que éste se encuentre.

Cualquiera que sea el uso de una red, tendrá hosts conectados a ella. Después de todo este es el punto que define a las redes: Comunicar a dispositivos que necesitan servicios el uno del otro. Desde el punto de vista del usuario la pregunta clave es: ¿Qué puede hacer esta red por mí?, si la persona que está enfrente es un administrador de red o de un sistema, su respuesta sería: proveer un servidor de DNS, servidores de correo, conexiones remotas y muchos otros servicios. Pero la visión de un administrador de seguridad es muy diferente, su cuestionamiento sería: ¿Qué puede hacer esta red por mí, que aún no sepa? o peor todavía ¿Qué puede hacer esta red por los atacantes?

En general, las redes son criaturas un tanto amorfas, difíciles de entender. Cualquiere persona puede ver los cables, ruteadores y switches, pero no todos pueden interactuar directamente con los bits. Hasta los administradores más experimentados, no pueden ver de manera clara en todo momento qué es lo que está pasando. Cualesquiera que sean los propósitos, diseñar o auditar políticas de seguridad, hacer una prueba de penetración o adicionar más hardware a la red, tener una lista actualizada de la topología y dispositivos conectados a la red debe ser obligatorio.

4.5.1 Escaneo de Puertos

El mapeo de una red es el proceso por el que se enumeran todos los hosts que responden satisfactoriamente en una red. El escaneo de puertos es el segundo paso y proporcionará la información de qué puertos están escuchando y listos para iniciar comunicación. Por supuesto, si un puerto está abierto es porque algún servicio está siendo proveído por él hacia otras máquinas en la red.

Hacer un escaneo de puertos simple es una tarea trivial. Imaginemos un programa similar a un pseudocódigo, por ejemplo:

```
HOST= “pc.ejemplo.com”
For PORT_NUMBER in 1 to 65535 {
If (connect_to(HOST,PORT_NUMBER)==SUCCESS){
```

Print “puerto PORT_NUMBER is listening”

Close: connection (HOST, PORT_NUMBER)

Este código tratará de conectarse con cada puerto del host pc.ejemplo.com. Como en un principio no sabemos qué puertos estén o no contestando, éste simplemente tratará de conectarse con cada uno de los 65,535 puertos posibles, uno tras otro. Siempre que una conexión sea exitosa, imprimirá en pantalla el mensaje que indique que ese puerto está escuchando e inmediatamente cerrará la conexión sin haber enviado ningún dato. Si el puerto no está escuchando no hace nada, sólo pasará a analizar el siguiente.

Por supuesto, éste es un ejemplo del escaneo de puertos más sencillo que se puede hacer. Si un escaneador de puertos comienza desde el número uno y sigue así sucesivamente tratando de conectarse hasta el 65,535 muy probablemente será detectado con facilidad. Varios de los mejores escaneadores[6] de puertos cuentan con diferentes tipos de tácticas que les permiten a los atacantes evitar ser detectados. Lo primero que pueden hacer para no ser detectados es dejar pasar un periodo de tiempo entre cada intento. Haciéndolo lentamente y probando pocos puertos por cierto tiempo, pueden llegar a engañar inclusive a un detector de intrusos. Algunos detectores de intrusos pueden interpretar que más de 5 intentos a diferentes puertos en un periodo de 2 segundos, es una intrusión y automáticamente bloquear los paquetes que realizan el escaneo. Es común que un atacante experimentado envíe muy pocos paquetes por hora, volviendo el escaneo muy lento, pero reduciendo en gran medida la posibilidad de ser detectado.

Otra técnica que se puede utilizar para identificar un escaneo de puertos, es monitorear todos los intentos de conexiones y tratar de determinar cuál de ellos trata de conectarse siguiendo un orden secuencial. Por ejemplo, un escaneo que sigue la siguiente secuencia: empieza en 192.168.1.1 y sigue con 192.168.1.2, 192.168.1.3, (…) sería muy obvio. Para hacer un escaneo más discreto, algunas herramientas van brincando entre todo el rango de direcciones, por ejemplo: 192.168.1.203, 192.168.1.52 y quizá después 192.168.25, haciendo con esto más difícil su detección.

4.5.1.1 Escaneo de Puertos con Nmap

[6] *Escaneadores,* Término que hace referencia a las herramientas que realizan un escaneo

Por muchos años, los escaneadores de puertos fueron simples herramientas que arrojaban como resultado qué puertos estaban escuchando y cuáles no. Por ejemplo, si el escáner encontraba que el puerto 80 de pc.ejemplo.com estaba escuchando, se podría suponer que este equipo era un servidor web ya que el puerto 80 es el puerto estándar para HTTP. Esta es una buena aproximación, pero se seguiria sin estar 100% seguro. El hecho es que, no se puede asegurar qué servicio está respondiéndonos con un simple escaneo. Lo único de lo que se puede estar seguro es que algo está escuchando. La mayoría de los escaneadores imprimen un reporte muy agradable a la vista al finalizar el escaneo, con los nombres de los servicios que están escuchando en cada puerto, pero esta información puede ser engañosa, puesto que se basa en el servicio que comúnmente escucha por ese puerto y normalmente estos nombres provienen de, en el caso de unix /etc/services o su equivalente en otras plataformas. Básicamente, es un archivo de texto que mapea los números de cada puerto con sus nombres bien conocidos. Así, que los escaneadores imprimen este reporte, lo que no los hace sumamente fiables.

Esto se puede volver más confuso si se considera que algunos usuarios tratan de engañar. Incluso usuarios legítimos caen presos en la tentación. Algunos administradores dejan por default abierto el puerto 80 a sus usuarios, en lugar de configurar a cada uno su propio puerto. Esto se debe a que HTTP es un protocolo vital en diferentes tipos de ambientes, además de que, muchos ruteadores y firewalls están configurados para dejar pasar prácticamente todo por ese puerto, haciendo de esto un hoyo de seguridad muy importante. Si el administrador es descuidado, dejará la configuración de fábrica que es equivalente a poner la regla “permit any tarffic going to port 80”. Por ello, si los usuarios desean ejecutar un software de P2P en la red lo podrán hacer redireccionando el puerto de salida al 80, esperando que con esto puedan atravesar el perímetro de seguridad. De forma parecida, es muy común que los usuarios hagan que servicios bien conocidos se comuniquen a través de puertos inusuales, para esconderse a la vista de los administradores. Muchos atacantes modifican los servidores de SSH dejándolos escuchar por puertos muy altos, para poder regresar a conectarse después[6].

Mientras aún no se pueda determinar la aplicación que está corriendo en un sistema remoto con el 100% de efectividad, herramientas como amap y nmap incluyen esta funcionalidad descifrando la respuesta que reciben al conectarse al puerto, con ello pueden identificar el software que está escuchando, algunas veces hasta incluyendo la versión y si ésta ha sido actualizada o no.

Amap es una herramienta conocida como “banner grabber[7]”, que trata de conectarse a los puertos que previamente identificó nmap que están escuchando, para decir con claridad qué tipo de aplicación es la que está escuchando. Esto lo logra

[7] *Banner grabber*, en español significa capturador de banderas.

examinando la bandera que es mandada después de conectarse al servicio. Aunque es una manera fiable de identificar la aplicación, amap podría ser engañado por el administrador del equipo, este podría mandar una bandera diferente a la de la aplicación que realmente se está escuchando en ese puerto, anulando con esto su credibilidad.

Nmap utiliza las técnicas manejadas por amap para la identificación de aplicaciones después de realizar su escaneo. El poder de nmap radica en el gran número de usuarios que escanean sistemas, siendo éste un software con licencia libre, tanto su código como sus bases de datos están a la vista de cualquier persona, además de que toda la comunidad puede aportar algo para hacerlo más potente y efectivo.

La única manera de estar 100% seguro de qué aplicaciones están escuchando en cada puerto es hacerlo como administrador de manera local en cada equipo. Existen diferentes aplicaciones como Fport para Windows que permiten obtener resultados claros y fiables (ver figura 18).

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ )
Interesting ports on server.example.com (10.10.10.172):
(The 1184 ports scanned but not shown below are in state: closed)
PORT      STATE    SERVICE     VERSION
21/tcp    open     ftp         ProFTPD 1.2.8
22/tcp    open     ssh         OpenSSH 3.7.1p2 (protocol 1.99)
25/tcp    open     smtp        Sendmail 8.12.10/8.12.9
79/tcp    open     finger?
80/tcp    open     http        Apache httpd 1.3.26 ((Unix) PHP/4.2.2)
110/tcp   open     pop3        vm-pop3d 1.1.6 (derived from gnu-pop3d)
113/tcp   open     ident       FreeBSD identd
143/tcp   open     imap
587/tcp   open     smtp        Sendmail 8.12.10/8.12.9
1027/tcp  open     http        Mini_httpd 1.19
2121/tcp  open     ftp         ProFTPD 1.2.8
3306/tcp  open     mysql       MySQL 3.23.54
6000/tcp  open     irc         Unreal ircd
```

Figura 18. Resultados de un escaneo de puertos con NMAP

Ahora que ya se tiene una lista de todos los puertos que podrían responder en una cierta máquina, el siguiente paso es poder expandir esto al resto de la red. Las herramientas de escaneo de puertos son muy buenas para saber qué es lo que está pasando en un host, pero muchas veces es necesario saber aún más. Es por eso que existen herramientas que facilitan el trabajo ayudándo hacer escaneos para cada host en la red. Hacerlo manualmente tomaría mucho tiempo, es por eso que estas herramientas

pueden tomar todo el rango de una red para analizarla. Este tipo de herramientas hacen lo que se conoce como mapeo de redes.

El mapeo de redes es una técnica complementaria al escaneo de puertos. Aunque la red sea pequeña y se encuentre en el mismo cuarto, nunca se puede estar seguro de qué es lo que un usuario está haciendo en su porción de red. Podrían estar utilizando conexiones no autorizadas con un ISP, redes inalámbricas, programas P2P, etc.

Con este tipo de mapeos se podrá identificar no sólo a los usuarios sino también hardware que quizá no se sabía que existía. Es por eso que es recomendable hacer periódicamente un mapeo de la red de la organización escaneando cada dirección posible.

¿Qué tan seguido es recomendable hacer un escaneo de la red?, ésta es un pregunta muy común entre los administradores de seguridad y redes, la respuesta más simple es tan seguido como se pueda. Una respuesta más compleja sería, lo más seguido que la misma red lo permita, esto en el caso de que sea un red muy grande. Se debe tomar en cuenta que se tiene que disponer de tiempo para elaborar un informe, para así poder compararlo con los siguientes, para poder darse cuenta qué cambios ha sufrido la red.

4.6 Escaneadores de Vulnerabilidades

Para cualquier administrador es un paso crítico el entender cuáles son todas las vulnerabilidades con las que cuenta un sistema. Un escaneo de puertos arroja información acerca de cuáles puertos están escuchando, quizá qué sistema operativo está usando y las aplicaciones del host, pero no evalúa las vulnerabilidades que pueden ser aprovechadas por el atacante. Se pueden usar los datos generados por el escaneo de puertos y para introducirlos en un analizador de vulnerabilidades, que pueda examinar cada sistema, puerto y aplicación de manera más detallada para identificar vulnerabilidades.

La mejor forma de defenderse en contra de los vectores de amenazas es auditar los perímetros de seguridad regularmente. Ésta es una manera amable de decir que se tienen que penetrar los sistemas de la misma organización. La principal regla para realizar un escaneo de vulnerabilidades es asegurar que sólo se esta escaneando sistemas para los

que se tiene autorización, de otro modo se estará penetrando sistemas de manera ilegal pudiendo ser detectados, generando con esto un problema.

Existen una gran variedad de escaneadores tanto comerciales como gratuitos. Si se va a comprar un escaneador es mejor adquirir uno que abarque el mayor número de vulnerabilidades, como por ejemplo: ISS´s Internet Scanner, Symantec´s NetRecon, Nessus, etc. Todo ellos tienen falsos-positivos que necesitan ser analizados manualmente. Antes de invertir dinero y tiempo, existen 4 cosas que se deben considerar:

- ¿Cómo maneja sus licencias el producto?, ¿es fácil actualizarlo?
- ¿Qué tan interoperable es el producto? ¿Tiene soporte para todo tipo de vulnerabilidades?
- ¿Se puede hacer de manera sencilla una comparación entre el escaneo de hoy y el de semanas después?
- ¿El reporte de salida es fácil de interpretar?

4.6.1 Formas de realizar un Escaneo de Vulnerabilidades

Realizar un escaneo de vulnerabilidades puede ser una tarea peligrosa tanto para la organización como para la persona que la realiza. La diferencia entre hacer una prueba de penetración y un ataque, son los permisos. Se debe estar seguro de contar con la autorización y permisos necesarios para realizarlo. Si aún no se cuenta con políticas referentes a escaneos es preferible realizarlas antes, definiendo los permisos de hacerlo a los mandos más altos, como el administrador de TI, red o Jefe de seguridad. Esto no debe tomarse a la ligera, existen diferentes casos en los que empleados han sido consignados a las autoridades por hacer este tipo de escaneos.

Se debe tener gente al pendiente de todo lo que pueda ocurrir antes de iniciar un escaneo. Las cosas pueden resultar muy malas al implementar el escaneo, algunas veces éstos pueden hacer que los sistemas dejen de funcionar y esto puede causar muchas molestias a los usuarios, ya que estarían perdiendo mucho tiempo. Se debe poder tener contacto directo en todo momento con la persona que realiza el escaneo, de lo contrario puede resultar un gran problema para la organización si algo llega a fallar.

No se debe configurar el escáner para que de una sola vez haga el escaneo por toda la red, aunque ésta sea pequeña. Se debe escanear una subnet, un grupo de trabajo o cualquier otra forma de división que se pueda hacer en la red a la vez. De esta manera la red no podrá venirse abajo por completo si algo malo llegara a suceder y no se tendrá un gran número de vulnerabilidades para resolver al mismo tiempo.

Si uno se decide por escanear todo de una vez, sólo se logrará tener una gran lista de problemas y serán muy difícil de reparar todas por la cantidad de tiempo que tomaría cada una, además de que puede ser peligroso. Imagine que se ejecuta un escaneo en una red grande, por ello se obtendrá una lista de vulnerabilidades aún más grande, cada una con su propio riesgo. Se presenta un reporte con los altos mandos de la empresa, los cuales acceden a darles respuesta. Como no será lo único que se tenga que hacer, ya que esto sólo es una parte de la implementación de seguridad, nunca se tendrá el tiempo de poder resolver todas en el tiempo que la organización haya pactado.

La clave es empezar por secciones pequeñas y al resolver estos problemas poder seguir con otra sección y así sucesivamente.

Otra manera de aprovechar mejor el tiempo y los recursos es utilizar la lista del top 20 de amenazas para la seguridad de Internet creadas por el SANS y el FBI. La mayoría de los escaneadores cuentan con esta opción, de esta manera se podra lidiar en un principio solamente con los problemas más serios.

4.7 Técnicas Alternativas para el Mapeo de Redes

Tiempo atrás, los perímetros de seguridad eran mucho más simples. Casi toda la gente podía describir el área donde se conectaba Internet con la red de la organización como el perímetro de red, usualmente llamado DMZ. Desafortunadamente, en la actualidad éste no parece ser casi nunca el caso. Recientemente todas las organizaciones han implementado algún tipo de mecanismo para acceder de manera remota a su red interna, aunque algunas veces ellos no lo sepan[6].

4.7.1 Escaneo de Redes Inalámbricas

Las tecnologías inalámbricas se han convertido en fáciles y baratas de implementar y brindan una nueva dimensión de seguridad para cualquier red. Antes de las redes inalámbricas, se podía salvaguardar una red, protegiendo únicamente el cableado y cuartos de servidores, todo se resumía a protección física. Las redes LAN inalámbricas y sus Access points [8]pueden extender su cobertura muy a lo lejos de lo que las claves lo podrían hacer, inclusive a las afueras de las instalaciones de donde se encuentren, provocando con esto un gran problema de seguridad.

Los atacantes ya no necesitan romper los perímetros de seguridad o comprometer equipos de manera remota. Un atacante puede manejar su automóvil dentro del estacionamiento de una organización, con una laptop, tarjeta de red inalámbrica y una pequeña antena, logrando tener acceso al tráfico interno de la red. Hoy en día no se puede dar el lujo de pensar que se estara a salvo con tan solo estar detrás de un firewall, actualmente el perímetro de red está limitado a cualquier punto por el que un atacante pueda tener acceso. Una vez que el atacante haya comprometido la seguridad de la LAN inalámbrica, tendrá los mismos privilegios que un usuario autorizado, además poder estar en cualquier locación física que esté en el rango de la red inalámbrica.

La información que proporciona una herramienta para escanear redes inalámbricas es:

- Modo de operación.
- Canal.
- Dirección MAC del Access point.
- Nombre de la red (SSID).
- Nivel de la señal y ruido (esto puede ser usado para ubicar la locación física del Access point).
- Marca del equipo.
- Número de frames por segundo.
- Detectan el algoritmo de cifrado que se está usando.

[8] *Access points*. Dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica

Existen diferentes escaneadores de redes inalámbricas en el mercado entre los más destacados se tienen: NetStumbler por la parte de Windows y Kismet para los usuarios de Linux. Los dos cuentan con características muy parecidas, además de permitir hacer escaneos de forma pasiva, esto quiere decir que lo harán sin dejar rastro alguno.

4.7.2 WarDriving

En pocas palabras, Wardriving es manejar (o en su caso caminar, sentarse, etc.) con el equipo necesario para detectar redes inalámbricas. En muchos de los casos, gente que hace este tipo de detecciones, publica los resultados de sus mapeos en Internet para que todos los puedan ver[47].

En la figura 19 se muestra un mapa de wardriving generado con netstumbler a mediados del año 2007, de todos los acces points en el metro de Boston a finales de 2007.

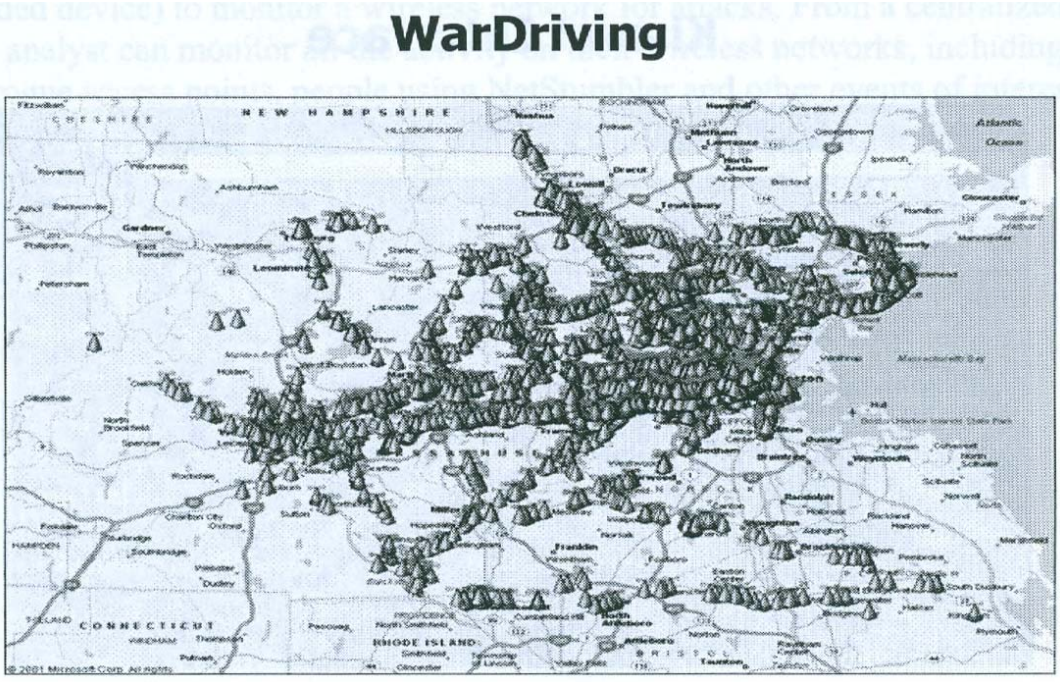


Figura 19. Acces Points en Boston

Muchos de estos access points están ubicados en lugares de renta de computadoras y cafeterías como Starbucks, ofreciendo este servicio al público. Sin

embargo, muchos de estos puntos son redes inalámbricas de organización que no han sido bien configuradas. De acuerdo con recientes estudios, se cree que aproximadamente el 68% de todos los acces points en el mundo no cuentan por lo menos con cifrado web habilitado y aproximadamente cerca de un 28% siguen utilizando el identificador de la red (SSID), probablemente muchos de ellos sólo fueron sacados de la caja y conectados a la corriente eléctrica y no se hizo ningún esfuerzo por configurarlos o aplicar medidas de seguridad.

4.7.3 Mitigación del Escaneo de Redes Inalámbricas

Debido a la naturaleza de las redes inalámbricas, existe una oportunidad muy baja de evitar mapeos de red. Si una red inalámbrica se encuentra en un área muy poblada, se puede esperar que esa red sea mapeada con frecuencia, algunas veces por wardrivers o por curiosos en busca de conectarse a Internet y algunas otras por personas que quieren explotar las debilidades de la red. Se puede reducir el rango de cobertura de la red, reduciendo la señal de alcance de equipo, usar diferentes técnicas para evitar el esparcimiento de señales de radiofrecuencia como utilizar barreras metálicas en las paredes o ventanas especiales, aunque esto no siempre es viable ya que resulta muy costoso.

Otra opción menos costosa es utilizar sistemas de cifrado y autenticación fuertes. Usualmente se cree que el monitoreo de redes inalámbricas se reduce únicamente al monitoreo de radiofrecuencias y no es así, también se puede monitorear la información de los logs, de los access points y los servidores de autenticación (RADIUS, LDAP) y así poder ubicar algún uso erróneo. Si se ve que un mismo usuario se conecta a la red en repetidas ocasiones con diferentes direcciones IP origen, esto puede ser indicio de que algo anda mal.

Finalmente, se debe tomar el tiempo para escanear la red de la organización y así darse cuenta de qué es lo que el atacante puede aprender de ella. Con esto se podra conocer cuáles son las vulnerabilidades y remediarlas antes de que una amenaza por parte de un atacante se haga presente.

4.7.4 War Dialers

Las redes inalámbricas son el más reciente peligro en el mundo de las redes, pero por ningún motivo se pueden olvidar los módems que representan un peligro latente

para la organización. Un módem mal configurado o que no ha sido autorizado, puede hacer que un atacante cruce el perímetro de red con facilidad, además de proveer una puerta trasera para cuando éste quiera regresar.

La mayoría de las computadoras se venden con módems pre-instalados de fábrica. Resulta muy sencillo que un empleado se conecte a través de él a Internet sobrepasando todas las medidas de seguridad.

Estas herramientas pueden marcar listas de números telefónicos y guardar en memoria cuáles de ellos son contestados por un módem. Éstos escanean todo un rango de números telefónicos en busca de un módem que tenga habilitada la opción de contestación automática, una vez encontrados estos equipos pueden ser atacados.

4.7.4.1 Protección ante War Dialing

La manera más fácil y efectiva de protegerse en contra este tipo de ataque es quitando por completo los módems de los equipos de cómputo. Nadie podrá atacar un módem que no existe.

Existen también, módems seguros que son mucho más difíciles de comprometer, éstos tienen diferentes medidas de seguridad, como por ejemplo: el módem que intente conectarse al módem seguro debe estar previamente registrado, tener un número específico de ID y una llave de cifrado.

Una estricta política de seguridad para el uso de módems, sumada a revisiones físicas periódicas sin avisar a los usuarios, es una buena manera de estar tranquilo de que ningún módem fue conectado ilegalmente a la red.

4.7.5 Técnicas de Pruebas de Penetración

Algunas de las técnicas de penetración más comunes son:

- War dialing.
- Wardriving.
- Eavesdropping.
- Monitoreo de radiación.
- Ingeniería Social.
- Dumpster diving (Recolección Urbana).

Algunas de estas técnicas fueron tratadas con anterioridad, por lo tanto, se revisaran las que aún no se han mencionado.

Eavesdropping es el término utilizado en inglés para la acción de “escuchar detrás de las puertas”. Es una de las tácticas más viejas utilizadas por los profesionales en seguridad. Se trata del simple hecho de escuchar conversaciones privadas en las que se puede revelar qué puede facilitar el acceso a la red. Esto se puede llevar a cabo a través de un micrófono o mediante la utilización de equipo para grabar las conversaciones telefónicas o cualquier tipo de comunicación electrónica[7].

Aprovechando la radiación emitida por dispositivos electrónicos no protegidos, como teclados o monitores, se pueden recibir datos, imágenes y hasta audio/video. El equipo de monitoreo de radiación puede ser instalado dentro de una camioneta, que podría estar estacionada afuera de la ventana de una organización y conseguiría reconstruir cada cosa que pasa en los monitores, tal cual se aprecia en ellos.

Dumpster diving o Trashing son los términos utilizados en inglés para la acción de “recolección”. Se trata de recolectar información de la basura de la organización hasta encontrar algo que permita tener acceso. Esto no resulta ser muy placentero que digamos, pero quizá podamos encontrar una nota con una contraseña válida.

Conclusiones Capítulo 4

Cualquier tipo de firewall, no importa cómo esté configurado, nunca es perfecto. Normalmente éste puede ser sobrepasado por las acciones de usuarios internos. Los atacantes toman ventaja de las debilidades de los firewalls, como por ejemplo el uso de software P2P, redes inalámbricas y conexiones de módem.

Los atacantes también han desarrollado métodos para tomar ventaja de las vulnerabilidades de la red. Han desarrollado toyanos que los mismos usuarios involuntariamente ejecutarán, dejando escapar información importante que el atacante aprovechará para ganar acceso a la red. También han desarrollado gusanos que automáticamente escanean hosts y se esparcen exponencialmente. La única forma de combatir todos estos vectores de amenaza es asegurándose de que el sistema operativo y aplicaciones del sistema estén siempre parchadas y actualizadas.

Es claro que los atacantes seguirán haciendo escaneos de sistemas a través de Internet, es por eso que es recomendable que se realizar escaneos en los sistemas antes que ellos, para encontrar vulnerabilidades y poder corregirlas antes de que sea tarde. Se debe recordar siempre que para hacer este tipo de escaneos deben existir políticas que dicten cómo hacerlo, además de contar con los permisos necesarios, de lo contrario se podrían tener problemas legales.

También es buena idea hacer escaneos periódicos en busca de redes inalámbricas, con esto se podrá hacer un reconocimiento de qué redes son las que comúnmente están en el rango de alcance e irnos familiarizando con el ambiente de la organización. Así, sí un empleado o atacante intenta montar otra red ayudándose de un acces point, se podrá identificar fácilmente.

Las pruebas de penetración, sirven para probar las vulnerabilidades. Pueden ser usadas en lugar de hacer un escaneo de vulnerabilidades, pero es más eficiente cuando estos resultados se comparan con un escaneo anterior. La mayoría de los escaneadores de vulnerabilidades pueden generar falsos-positivos y una prueba de penetración puede ayudar a corroborar que fueron marcados erróneamente.

Capítulo 5.
IDS

Los IDS son una excelente manera de monitorear anomalías en una red que pueden indicar un ataque o dar señales de que alguien quiere penetrar la red.

En este capítulo se examinaran cómo trabajan tanto los IDS basados en host como los que se basan en red y cómo estas herramientas pueden brindar a una organización el beneficio de identificar amenazas y ataques en contra de sus sistemas y redes.

5.1 Concepto de un IDS

La detección de intrusos es el proceso de monitorear la actividad en un host o red, identificando pistas que puedan dar indicio de atentados o brechas de seguridad. Un IDS monitoreará la actividad que se sospecha o se sabe maliciosa, mandando alertas a las personas para que estas sean atendidas.

La persona que es responsable de dar atención a las alertas (manejador de incidentes) podrá usar la información generada por el IDS para tratar de identificar la actividad sospechosa y tomar alguna acción basada en su análisis.

En este sentido, un IDS es un sistema de alarma para identificar actividad no deseada en la red o en los hosts. Igual que un sistema de alarma, éste no podrá detener las amenazas por sí solo, un IDS no provee ningún tipo de protección en contra de los atacantes. De hecho un IDS sólo podrá alertar sobre la existencia de actividad que lograría ser una amenaza para la red, permitiendo al manejador de incidentes responder a este tipo de actividad dependiendo de la severidad de las alertas[42].

Cualquier tipo de organización no deberá implementar un IDS como primer método o medida de seguridad para proteger sus recursos. Los IDS se usan en conjunto con los firewalls, anti-virus, analizadores de vulnerabilidades y herramientas de parcheo de sistemas para implementar una postura de defensa en profundidad.

La tecnología de los IDS no es algo nuevo, de hecho, tiene muchos años participando activamente en el mercado. Muchas organizaciones hacen buen uso de esta tecnología para identificar ataques y algunas otras cosas positivas aunque muchas otras siguen sin tener la capacidad de implementación por diversas razones.

5.2 Lo que un IDS no es

Cualquier tipo de IDS no es un reemplazo para otro mecanismo de seguridad para proteger la red. Las organizaciones deben considerar la implementación de un IDS, solamente después de tener un firewall, políticas de seguridad, hardening[1] de sistemas y alguna otra técnica de defensa. Siempre se debe tener en cuenta que un IDS sólo es un sistema de alarma, que enviará alertas únicamente si se está siendo atacado o existe alguna actividad sospechosa. No previene o puede mitigar los ataques.

Un error común en la implementación de tecnologías de IDS es gastar una buena cantidad de dinero en la compra o desarrollo sin tener un plan de mantenimiento y utilización. Debe considerarse que es mucho más costoso mantener en funcionamiento un IDS que su adquisición.

Dependerá de la configuración y topología de la red el lugar donde se coloque un IDS además del cómo se monitoreará y reaccionará a todos los posibles eventos, que fácilmente puede ser un trabajo de todo un equipo. Toma tiempo a un analista bien entrenado poder entender e interpretar correctamente las alertas generadas por un IDS, esto debe considerarse en el monto de la inversión que hará la organización que lo implemente.

Finalmente, un IDS no es una navaja todo en uno para una organización que busca implementar seguridad en su red y hosts. Inclusive el mejor analista sólo puede procesar alertas de un punto en específico. Sí el analista, en primera instancia, no entiende con claridad las políticas de seguridad de la organización, será muy difícil que pueda atender una alerta, además de que no podrá ejecutar las acciones que se requieran para proteger los bienes de la organización.

5.3 Tecnologías de IDS

[1] *Hardening*. Proceso por el que se asegura un sistema

Como ya se dijo, un IDS identifica ataques en contra del sistema que monitorea. Por ello un IDS puede ser muy simple o tan complejo como se requiera.

De manera básica, la información contenida en el log de un dispositivo constituye a un IDS. Por ejemplo, el siguiente mensaje fue obtenido de un ruteador CISCO:

```
Dec 31 18:09:52.388 UTC: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to
RSHELL from 192.168.116.105
```

CISCO no vende sus ruteadores diciendo que tienen la capacidad de detectar intrusos, pero este mansaje del log indica que alguien intenta conectarse al ruteador a través del puerto de SHELL.

En la práctica, este es el típico mensaje del resultado de un ruteador al que se le está haciendo un escaneo de puertos, por ejemplo, con nmap. Éste podría ser el resultado de actividad no deseada en contra del dispositivo que fue detectada y guardada en el log para ser analizada.

Cuando se reportan mensajes de log con un comportamiento inesperado, podría considerarse esto como una implementación simple de un IDS, de igual forma una herramienta de IDS puede ser mucho más compleja. Los IDS de uso distribuido pueden analizar el tráfico entero de una organización, actividades de clientes o de los propios hosts y hacer reportes globales bien detallados de toda esta información.

Los IDS son clasificados de acuerdo con su implementación como IDS basados en Host o basados en red, que se analizarán a continuación.

5.4 Tipos de alertas

Cuando un IDS detecta actividad, cualquiera que ésta sea, debe poder identificarla y clasificarla. Esta clasificación comúnmente entra en dos grupos, positivo cuando es un evento de interés para la organización, o bien, negativo cuando no lo es. Un evento de interés puede ser cualquier cosa que el analista quiera identificar con el IDS, incluyendo herramientas específicas de atacantes, ciertas letras o contenidos dentro de un mail, mensajes instantáneos o inclusive el nombre específico de un archivo que pueda ser transmitido entre dos hosts. Si el IDS ve eventos que cree que no son de interés para la organización los clasificará como negativos y continuará haciendo su trabajo sin mandar ninguna alerta. De lo contrario, si el IDS identifica actividad que considera es un evento de interés, lo clasificará como positivo y mandará una alerta[5].

Desafortunadamente, los IDS no arrojan resultados siempre correctos, ya que pueden tomar malas decisiones. Los analistas de IDS deberán trabajar con 4 diferentes clasificaciones de eventos:

- Verdadero Positivo. En este caso el IDS trabaja como se esperaba, marcando correctamente la actividad que parece tener un comportamiento malicioso.
- Falso Positivo. Es cuando el IDS genera una alerta advirtiendo actividad que parece tener un comportamiento malicioso. El analista deberá decidir cómo manejar el incidente ya que puede ser que en realidad no sea algo malo.
- Verdadero Negativo. Este tipo de evento es el que quisiéramos ver siempre en un IDS, es cuando la información no indica ningún tipo de contenido malicioso y esto es verdadero, por ende el IDS no generará ningún tipo de alerta.
- Falso Negativo. El IDS identifica que todos los datos son benignos, cuando de hecho son maliciosos, además de que no se genera ningún tipo de alerta.

En un mundo perfecto, los IDS sólo generarían verdaderos positivos y verdaderos negativos. Desafortunadamente, la naturaleza del análisis de datos y las tácticas que utilizan los atacantes dificultan esta tarea, por ello los analistas estarán obligados a aceptar la realidad y trabajar también con falsos positivos y falsos negativos en sus sistemas.

5.5 NIDS

Los NIDS[2] *(Network Intrusion Detection Systems)* son aquellos IDS interesados en los eventos que ocurren en una red. Esta variedad de IDS recolecta paquetes desde la red de manera pasiva. Cada paquete que es recolectado es procesado para encontrar eventos de interés y ser reportados al analista.

Para recolectar la información del tráfico necesaria, el NIDS es implementado en puntos donde pase mucho tráfico por la red, además de que muchas veces es apoyado por otros equipos que mandan una copia del tráfico que capturan hacia el IDS. Gracias a esto, un IDS puede captar todo el tráfico que pasa por todos los dispositivos, esto dependerá de la capacidad y características de procesamiento con las que cuente.

Un dispositivo NIDS puede estar dentro de un servidor o ser un appliance con un sistema operativo lo suficientemente blindado para que pueda resistir cualquier tipo de ataque. Tener la posibilidad de monitorear todo el tráfico de la red, hace que un NIDS sea muy atractivo para los atacantes que busquen capturar información de la red. Los vendedores que producen IDS han tratado de reducir la posibilidad de que reciban ataques, reduciendo el número de servicios disponibles en el dispositivo, usando sistemas de cifrado robustos para cualquier comunicación entre el IDS y las estaciones que está monitoreando.

Los NIDS utilizan diferentes métodos para identificar eventos de interés en una red, incluyendo análisis de firmas, análisis de anomalías, protocolos y aplicaciones.

5.5.1 Análisis de firmas

El análisis de firmas es el método más común para identificar eventos de interés en una red. Una característica única es identificada para un evento de interés en particular y cada firma es creada para identificar esa característica, haciendo que IDS genere una alarma.

En la práctica, el análisis de firmas puede resultar un mecanismo complicado, requiere de un análisis cuidadoso y cautela cuando se trata de identificar alguna

[2] *NIDS* (Network Intrusion Detection Systems), *en español Sistemas de detección de intrusos basados en red.*

característica única de cierta herramienta que pueda utilizar un atacante o algún evento de interés.

La correcta identificación de características peculiares de un evento de interés es esencial para el buen funcionamiento de un IDS, la mala identificación de firmas de eventos que pudiera realizar un atacante darán como resultado falsos positivos y falsos negativos.

La mayoría de las implementaciones de firmas están basadas en una serie de reglas, donde cada regla identifica a un evento de interés en particular. Cada regla identifica las características de un evento de interés utilizando los criterios disponibles por el IDS. Esto quiere decir que, el IDS tiene la posibilidad de buscar por cadenas específicas dentro de un paquete o el checksum, [3]de un archivo, más reglas complejas que contengan múltiples características para identificar eventos.

Cuando un IDS se inicia, checa cada una de las reglas que tiene configuradas para mandar alertas, además de construir tablas de almacenamiento para optimizar el análisis de datos. Cuando el IDS recibe datos para ser procesados, los compara con las características específicas de los eventos de interés previamente almacenados en las tablas, el IDS generará alertas cuando existan coincidencias entre ambos. Este proceso es transparente para el analista que usa el IDS, solamente tiene que entender cómo es la clasificación de los criterios para cada evento y las alertas generadas por el IDS. Si algún analista crea sus propias reglas deberá comprender perfectamente el lenguaje de las reglas para identificar los eventos de interés deseados.

5.5.1.1 Criterios de reglas y firmas

Un IDS debe poseer un lenguaje flexible para escribir las reglas, para que la organización pueda agregar las propias conforme a sus necesidades. Con reglas hechas a la medida, el analista tiene la posibilidad de incrementar o decrementar la complejidad del monitoreo de una red o host y las podrá agregar rápidamente para detectar vulnerabilidades, exploits, virus y actividad de gusanos o cualquier otra actividad no deseada en la red.

[3] Checksum. Es una medida muy simple para proteger la integridad de datos, verificando que no hayan sido corrompidos.

El lenguaje utilizado para crear reglas puede ser un poco complejo si se requiere que éstas tengan muchas características o patrones para la identificación de un evento de interés. La mayoría de los IDS permiten al analista examinar y clasificar los datos de acuerdo con las siguientes características de los paquetes:

- Información del Protocolo: Generar eventos de interés para protocolos específicos, normalmente protocolos de capa 3, como IP o de capa 4 como TCP, UDP, ICMP.
- Información de direcciones: Generar eventos basados en una dirección origen y/o destino específico. Esta característica puede ser buena para monitorear tráfico entre dos puntos específicos o bien limitar las opciones sólo a la red interna así, cuando una dirección no pertenezca a la red interna, una alerta lo podrá indicar.
- Información del Puerto. Permite al analista generar eventos de interés basados en puertos origen y destino.
- Contenido del Payload[4]: Es uno de los mecanismos más comunes para identificar eventos de interés específicos, un analista podrá identificar partes específicas del payload o inclusive todo su contenido.
- Comparación de cadenas. Generar eventos de interés basados en una cadena de caracteres específica que se encuentra en un paquete.
- Análisis de flujo de tráfico: Permite identificar cuándo fluye tráfico desde una fuente interna a una externa o viceversa.
- Banderas en la cabeceras de protocolos: Generar alertas basadas en la banderas de las cabeceras de los protocolos, como TCP, UDP, IP y ICMP

Esta lista es una muestra de todas las características disponibles en un IDS moderno, para el desarrollo de reglas.

5.5.2 Análisis de anomalías

El análisis de anomalías es otra técnica que un IDS puede usar para identificar eventos de interés en una red. A diferencia del análisis de firmas, el análisis de anomalías está basado en eventos de protocolos y aplicaciones específicas que salen del funcionamiento típico de operaciones. El IDS puede obtener información de estos eventos inusuales para generar eventos que podrán ser analizados.

[4] Payload. Son los datos, información que son anexados a las cabeceras.

El análisis de anomalías es desarrollado por el vendedor del IDS para ciertos protocolos y aplicaciones. El vendedor identifica condiciones especiales que no son parte del comportamiento normal de una aplicación y genera las condiciones bajo las que el IDS generará una alerta. Este tipo de análisis se basa típicamente en el tráfico que generan las aplicaciones, lo que puede generar falsos positivos. El vendedor debe establecer y entender cuál es el comportamiento normal de una aplicación, basándose típicamente en una línea base de información generada por paquetes capturados cuando se tienen las condiciones óptimas del protocolo o aplicación. Sólo las condiciones que han sido identificadas por el vendedor serán reportadas por el IDS.

5.5.3 Análisis de Protocolos y Aplicaciones

Mientras que el análisis de anomalías usa una serie de condiciones para encontrar un evento de interés, el análisis de protocolos y aplicaciones trabaja examinando cuidadosamente y completamente la operación de los protocolos y aplicaciones.

El IDS debe ser capaz de reconocer cómo es el comportamiento del protocolo tanto en su etapa de entrada, procesamiento y salida. Una vez que el IDS lo ha entendido, usará un método específico para detectar condiciones anormales en la red. Cualquier uso del protocolo o aplicación que no encaje con las definiciones que el IDS entiende como normales, serán reportadas como comportamiento anormal, generando con esto una alerta.

El uso de este tipo análisis es muy poderoso ya que permitirá identificar tanto amenazas conocidas como las que aún no se conocen.

Dado que existen pocos protocolos que tengan un comportamiento constante, este tipo de análisis es muy difícil de implementar por parte de los vendedores ya que los obliga a entender perfectamente cada protocolo y a veces, muchos de ellos son propietarios o bien sufren cambios constantemente lo que implica una gran inversión por parte del vendedor. Dependerá del vendedor escoger cuáles son los protocolos que deberá incluir, ya que sería imposible abarcar todos con este nivel de detalle.

5.5.4 Tipos de Inspección de Paquetes

Los vendedores de NIDS han implementado dos mecanismos diferentes para inspeccionar el tráfico, basados típicamente en análisis de reglas.

Inspección de Paquetes Ligera

Con la inspección de paquetes ligera, el IDS sólo toma una porción del paquete para analizar. Este método de análisis extrae y evalúa únicamente el contenido de de los campos más importantes de los paquetes. La ventaja más interesante que brinda este método de análisis, es que es muy rápido y por ende se optimiza el uso del hardware. Los eventos de interés que pueden ser identificados son:

- Dirección y puerto de origen/destino.
- Mensajes de error específicos de ICMP.
- Combinaciones extrañas de las banderas de TCP.
- Tamaño de los paquetes.

Inspección de Paquetes Profunda

Es lo contrario a la inspección de paquetes ligera, ésta hace un análisis completo del paquete, incluyendo la composición y tamaño de todos los campos. Este tipo de inspección utiliza muchos recursos del hardware además de ser muy lenta.

Los IDS modernos generalmente utilizan una combinación de ambas inspecciones. La mayoría de los análisis basados en firma, se realizan con una inspección ligera. Por el contrario los análisis de anomalías y los análisis de protocolo se realizan utilizando inspección profunda.

5.5.5 Ventajas de un NIDS

La primera intención de un NIDS es detectar actividad hostil en la red y generar alertas para que el administrador tome acciones al respecto, pero un NIDS puede tener algunas otras ventajas como:

- **Conocimiento del tráfico de red**

Pocos administradores conocen la naturaleza del tráfico de sus redes. Muchos de ellos especulan acerca de su comportamiento, pero muy pocos implementan mecanismos para monitorear y analizar el tráfico.

Utilizando un NIDS, un analista puede implementar eventos de interés para identificar y clasificar aplicaciones ya sea por información de capa 3 o capa 4, como también puede usar reglas para identificar tráfico de otras capas.

Esta información puede ser usada para identificar el uso erróneo de la red, además de tener una base comportamiento para identificar cuando algo ande mal.

- **Ayuda a detectar problemas de operación en la red**

Con los datos generados por un NIDS, se pueden rápidamente identificar patrones de actividad en la red que la hagan ineficiente. De hecho un IDS puede actuar como un mecanismo de auditoría para asegurarnos que las aplicaciones trabajen conforme a su diseño.

- **Ayuda a las organizaciones a responder de manera rápida a incidentes**

Identificando los puntos clave y las técnicas que usan los atacantes, el administrador podrá comprender más fácilmente sus vulnerabilidades y las posibles amenazas que pueden sacar ventaja de ellas y así poder defenderse de manera rápida.

6.5.6 Retos de los NIDS

Limitaciones por topología

Para que un NIDS pueda capturar tráfico para analizarlo, debe operar con tarjetas de red en modo promiscuo, ésta configuración permite capturar toda la información que pasa por la red y no solamente la que va dirigida a esa tarjeta. El problema es que ésta forma de tráfico sólo funciona en segmentos de red interconectados con hubs. En una red conformada por switches, el escenario es diferente, ya que éstos mantienen tablas internas con sus destinos y sólo envía el tráfico a los puertos donde se mandó la información. Este problema se puede solucionar de dos maneras[4]:

1) **Spanning Ports**

Los spanning Ports, son puertos que reciben todo el tráfico que pasa por el switch. El NIDS puede ser conectado directamente a este puerto, pero en la práctica esto no resulta tan fácil, ya que éste solamente pude manejar información de una VLAN a la vez, además de que su configuración se puede perder fácilmente, lo que implicaría que el NIDS no detectará nada.

2) **Network Taps**

Los Network Taps son dispositivos de hardware que se conectan directamente al cable coaxial, par trenzado o fibra óptica. El Tap manda una copia del tráfico que pasa a través de él al NIDS. Como éste no tiene ningún impacto en el switch no necesita ser configurado. La solución del problema es un poco costosa ya que se necesita un Tap para cada nodo.

Análisis de tráfico cifrado

Otra barrera para los NIDS es el propio tráfico. Si los sensores de un NIDS no pueden interpretar el tráfico que reciben, no podrán analizarlo. Este problema se vuelve aún más grande con los protocolos que aplican criptografía, que se han vuelto cada vez más populares.

El problema de poder contar con la posibilidad de descifrar los paquetes, es el tiempo en procesamiento que tomaría y esto puede causar que el NIDS pierda de vista otro evento que está pasando por la red.

Si la mayor parte del tráfico de la red va cifrado es necesario quizá pensar en medidas alternativas como los Host IDS (HIDS).

Calidad de las reglas

Lo más importante en un NIDS no es la cantidad de reglas que se tengan o que ofrezca el vendedor, es la calidad de éstas lo que realmente importa

Una mala regla puede causar miles de alertas, las que tendremos que analizar, es por eso que se debe ser muy cuidadoso al momento de agregar una regla más a la base de datos.

Lo importante es fijarse en qué técnicas utilizan los vendedores para reducir los falsos positivos y falsos negativos, además detectar e incrementar los verdaderos positivos.

Limitaciones de rendimiento

Con el incremento en los últimos años del ancho de banda los vendedores de IDS, ha necesitado cada vez tener mejor rendimiento, aunque algunas veces esto sea imposible de lograr. Por ejemplo el tamaño de los paquetes en una red Ethernet son de entre 60 a 1518 bytes, en una red Gigabit Ethernet los paquetes pueden ser de hasta 9216 bytes de tamaño, imaginen el procesamiento requerido para realiza una inspección completa de un paquete de 96K, además de que este proceso de inspección posiblemente necesite ser descifrado, esto haría casi imposible su análisis.

Costo

Muchas organizaciones adquieren un NIDS sin saber todo lo que les espera, creen que por tener el dinero para adquirirlo bastará y no toman en cuenta todo el capital que se tendrá que invertir en él. No sólo se trata de desembolsar dinero para su adquisición el costo real de un NIDS es el costo por implementarlo y mantenerlo. Se requiere tener administradores entrenados específicamente en esa tecnología para que se sepa interpretar los datos con claridad y pueda hacer un buen análisis.

5.6 HIDS

Las siglas HIDS[5] *(Host Intrusion Detection System)* hacen referencia a los sistemas de detección de intrusos basados en un host. Este tipo de IDS trabaja únicamente en un host, identificando eventos de interés que son configurados por el administrador. A diferencia de los NIDS, los HIDS deberán ser instalados en el host y sólo podrán monitorear a ese host.

Tienen la habilidad de proveer granularidad adicional al analista ya que pueden monitorear actividad con más detalle que la que un NIDS puede ver. Además de estar habilitados para monitorear la red, los HIDS pueden monitorear el estado del sistema operativo y puertas traseras como conexiones inalámbricas y módems.

Como un NIDS, las herramientas de HIDS utilizan firmas y análisis de comportamiento para identificar ataques en la red. También pueden corroborar la integridad de archivos.

Desafortunadamente la implementación de esta tecnología no es tan simple como comprar un producto e instalarlo. Para poder manejar este tipo de herramienta, se debe crear un plan para identificar cuáles de los hosts deben ser seleccionados para tener un HIDS y en qué orden. Se necesitan también constantes actualizaciones y monitoreos, que tomarán buena cantidad de tiempo, si se considera que el número de usuarios puede ser muy grande. Las primeras opciones a considerar son: servidores web, servidores de correo, servidores de DNS y firewalls. Además se debe calcular el costo total de la

[5] *HIDS (Host Intrusion Detection System), en español Sistema de detección de intrusos basado en host)*

implementación de esta tecnología por host. El costo aproximado en el mercado de un HIDS va desde los $50.00 dlls hasta los $500.00 dlls, si se calcula que una red pequeña tiene 20 hosts el costo total es una suma considerable.

Otra cosa a tomar en cuenta es que los hosts regularmente son reconfigurables y esto provocará que existan más falsos positivos, por eso es recomendable instalarlos en equipos que no tienen que cambiar sus opciones o sistemas operativos constantemente.

5.6.1 Verificación de integridad

La verificación de integridad es usada para identificar cuando un archivo ha sido cambiado en el sistema del host. Cualquier archivo que se desee monitorear puede ser definido por el administrador. Éstos pueden ser documentos de negocios, como políticas o contratos, o archivos de sistemas operativos como el etc/passwd de los sistemas UNIX o inclusive el contenido de servidores.

Para identificar cambios que no han sido autorizados, se hace uso de funciones matemáticas llamadas "HASH" las que producen un valor, que se usará para monitorear el archivo. El algoritmo hash siempre generará el mismo valor, a menos que el archivo haya sido cambiado. El programa de chequeo de integridad crea un índice de todos los archivos que deben ser monitoreados junto con sus valores hash. Regularmente el HIDS deberá obtener los valores hash de los archivos a monitorear y verificarlos con su índice, para verificar si existe algún cambio, si esto resulta positivo se enviará una alerta[6].

Existen diferentes algoritmos de funciones hash como por ejemplo: MD4[6], MD5[7], SHA-1[8]. Normalmente los HIDS utilizan MD5 o SHA-1 para calcular los hashes.

5.6.2 Monitoreo de LOG

[6] *MD4* (Message-Digest Algorithm 4) es un algoritmo de resumen del mensaje (el cuarto en la serie) diseñado por el profesor Ronald Rivest del MIT. Implementa una función criptográfica de hash para el uso en comprobaciones de integridad de mensajes.

[7] *MD5* (Message-Digest Algorithm 5) es el sucesor de MD4 y al igual que el implemeta una función criptográfica de hash para el uso en comprobaciones de integridad de mensajes.

[8] *SHA-1* (Secure Hash Algorithm) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology.

El monitoreo de logs es otro mecanismo que utilizan lo HIDS, este analiza los mensajes del LOG de los sistemas operativos y las aplicaciones. Este mecanismo de monitoreo utiliza dos formas de análisis, el inclusivo y el exclusivo para definir eventos de interés dentro de los LOGS.

- **Análisis Inclusivo**

  Este tipo de monitoreo de log utiliza una lista de palabras o frases que definen eventos de interés para el analista. La lista debe contener palabras que sean parte de los log del sistema operativo, como por ejemplo “acceso no autorizado”.

  El HIDS toma la lista de palabras para generar alertas cuando estas sean iguales a las del log del sistema.

- **Análisis Exclusivo**

  Tal como lo hace el análisis inclusivo, se genera un archivo con palabras o frases, pero en este caso se usan para excluirlas de los log. Si las entradas del log del sistema no concuerdan con las palabras o frases de la lista, se generará una alerta.

  Este tipo de configuración funciona para configuraciones limitadas, en donde la información contenida en el log del sistema es predecible o se repite frecuentemente.

5.6.3 Monitoreo de redes

El sistema de monitoreo de red para HIDS es muy similar que el de los NIDS. En un NIDS utiliza análisis de firma para encontrar eventos de interés en el tráfico que atraviesa por la interfaz. Con el monitoreo de redes que hace un HIDS se puede monitorear todo el tráfico de la red, que va desde el host hacia el resto de las interfaces. La ventaja de este

tipo de monitoreo es que podemos monitorear puertas traseras, redes inalámbricas, VPN y módems.

El análisis de red de un HIDS es como el análisis de un NIDS pero de manera distribuida. Se propagan diversos sensores de HIDS por toda la red, reduciendo con esto el tiempo de procesamiento aminorando así, la carga de trabajo.

5.6.4 Ventajas de un HIDS

El uso de HIDS ofrece diferentes ventajas para una organización, incluye un análisis más detallado de lo que se puede hacer con un NIDS. Un HIDS no tiene tantos problemas para analizar paquetes cifrados, ya que sólo tendrá que descifrar la parte que le corresponde al host y no todo lo que pasa por la red. De hecho, como la capacidad de monitoreo del HIDS es distribuida en cada uno de los host se pueden realizar análisis más profundos, sin agregarle sobrecarga.

La gran ventaja de este tipo de IDS es que pueden detectar ataques que se presenten dentro del perímetro de seguridad de la organización, ya sea que provengan de otros hosts o de usuario internos.

5.6.5 Retos de un HIDS

Al igual que los NIDS, la implementación de HIDS requiere de planeación y consideraciones especiales. Aunque un HIDS genera menos alertas que un NIDS en una red con mucho tráfico, el manejo y administración de estas alertas requiere de muchos recursos de la organización, especialmente por el número de HIDS que puede llegar a tener en sus equipos.

Algunos HIDS ofrecen muchísimas características pero requieren continua actualización y análisis de sus firmas. Manejar las actualizaciones del software y sus firmas puede llegar hacer una tarea difícil, ya que cada actualización debe ser probada antes de ser instalada en un equipo de producción. Siempre existe el riesgo de que una actualización cause algún tipo de inestabilidad en el software, por eso hay que hacer diferentes pruebas antes de instalarlas.

Los HIDS requieren de una herramienta que permita llevar a cabo un monitoreo centralizado para identificar intentos de ataque a gran escala en diferentes host.

La opción más viable es instalar HIDS únicamente en hosts con servicios o recursos críticos, si son implementados en todos los equipos podría resultar más costoso que un NIDS, ya que no solamente es el costo del software y la instalación sino también la configuración y el continuo monitoreo, que en el caso de algunas redes con más de 1000 equipos sería casi imposible de logar.

Siempre que se instala un HIDS en un host se deberá calcular el impacto que tendrá en cuanto a rendimiento y capacidades del equipo. Tal vez podría ser necesario cambiar el equipo, lo que implicaría un gasto adicional.

Finalmente el reto más grande es, ¿qué hacer con toda la información recopilada por el HIDS?. Muchas organizaciones que implementan HIDS encuentran que no tienen los recursos necesarios para responder a todos los eventos de interés que se le presentan. Guardar eventos pasados para su futuro análisis es una buena idea, pero se debe considerar el espacio que ocupará en disco duro, ya que podría llegar hacer inclusive terabytes.

Conclusiones Capítulo 5

En este capítulo se analizaron los dos tipos de detectores de intrusos que existen en el mercado: NIDS y HIDS. Cada uno cumple con una función específica en el diagrama de seguridad.

NIDS trabajan analizando el contenido de los datos que se envían a través de la red, utilizando una combinación de análisis de firma, análisis de anomalías y análisis de protocolos y/o aplicaciones. El análisis de firma utiliza reglas para identificar eventos de interés basados en criterios específicos en cada paquete. El análisis de anomalías utiliza una lista de eventos anómalos para detectar eventos de interés. El análisis de protocolos o aplicaciones utiliza las definiciones del protocolo y la violación de banderas que cumplan con la definición de eventos de interés.

Los HIDS trabajan analizando el tráfico que recolecta el servidor o equipo en donde se encuentra instalado, utilizando una combinación de monitoreo de integridad de archivos, monitoreo de logs y monitoreo de red.

El monitoreo de la integridad de archivos trabaja calculando los valores de hash de los archivos que el administrador considere importantes y monitoreándolos continuamente en busca de cambios. Si se encuentra un cambio en el valor del hash, esto indicara que hubo una modificación en el archivo y por ende el HIDS generará una alarma.

El monitoreo de red utilizado por un HIDS, es comúnmente usado por firewalls personales y otras herramientas para detectar ataques que pasan por las interfaces de red. La gran ventaja de los HIDS a diferencia de los NIDS, es que éstos pueden monitorear tráfico de red proveniente de otros medios como de redes inalámbricas, VPN y módems.

Se debe recordar también que un IDS proporciona datos para responder a un ataque pero no protege como tal a la organización contra alguno. Un IDS no reemplazará las estrategias de defensa en profundidad, sino será sólo una herramienta que forme parte del plan de seguridad.

Finalmente, cualquier organización que intente implementar un IDS deberá considerar mejorar la seguridad de los sistemas y redes con los que cuenta antes de hacer una inversión que tal vez no sea la solución óptima para sus necesidades. Muchas de las organizaciones podrían empezar haciendo uso de los logs de Windows o Linux, de sus firewalls y ruteadores, para poder así identificar ataques sin la necesidad de un IDS.

Capítulo 6.
IPS

Es difícil definir con claridad qué es exactamente un IPS, porque la funcionalidad de éste puede variar dependiendo el vendedor. En este capítulo se verán en detalle cómo es que cada uno de estos productos identifica un ataque tanto a nivel de host como de red.

6.1 Concepto de IPS

Un IPS es una tecnología que agrega otra capa de defensa para la protección de los recursos. A diferencia de los IDS que sólo reportan ataques en contra de los sistemas que monitorean, los IPS tratarán de detectar el ataque antes de que éste haya sido exitoso. Dependerá de cada vendedor el cómo se lleve a cabo la defensa de los recursos, aunque todos tendrán el mismo nombre, IPS.

Los IPS se clasifican generalmente en dos categorías, los basados en red llamados NIPS[1] *(Network Intrusion Prevention System)*, o bien, los basados en host llamados HIPS[2] *(Host Intrusion Prevention System)*. Como su nombre lo indica, a nivel de red analizan el tráfico de forma similar a los NIDS. HIPS son instalados en host y detienen los ataques al sistema operativo o a nivel de aplicación.

Como la tecnología de IPS es reciente, se están haciendo esfuerzos significativos para reducir falsos positivos, reducir el impacto que tienen sobre el host/red y detener los ataques no conocidos hacia el objetivo. Muchas organizaciones que han implementado este tipo de herramienta son capaces de mitigar los efectos de diferentes tipos de ataque en contra de sistemas vulnerables, como ataques de hackers, gusanos y virus. El campo de los IPS crece de manera muy rápida y ha ganado importancia en empresas grandes.

[1] *NIPS (Network Intrusion Prevention System), en español Sistemas de prevención de intrusos basados en red.*

[2] HIPS (*Host Intrusion Prevention System), en español Sistemas de prevención de intrusos basados en host.*

6.2 Lo que un IPS no es

Desafortunadamente, los IPS no resuelven todos los tipos de amenazas que se pueden enfrentar. Implementar un IPS, no es un reemplazo del hardening de sistemas operativos o la instalación de actualizaciones, pero sí permite ganar mucho tiempo. Las organizaciones que utilizan sistemas de IPS, normalmente tienen más tiempo para actualizar sus equipos, resolver problemas de sus aplicaciones, realizar e implementar calendarios y planes de actualización.

Como los sistemas de IDS, un sistema IPS no debe considerarse una tecnología todo en uno, capaz de brindarnos seguridad por sí sola. Requieren mantenimiento y monitoreo para ser herramientas efectivas. Los IPS no son herramientas que estén al alcance de cualquier organización, ya que éstas suelen ser muy costosas. Un IPS incluye un software de manejo centralizado y una licencia por servidor, que tiene un costo desde los $150,000 dlls por 250 servidores. También se necesita, un ambiente de prueba en donde se puedan verificar las actualizaciones antes de ser instaladas en el ambiente de producción, además de contar con una gran cantidad de espacio de almacenamiento para que el IPS puede realizar la correlación de eventos, se necesitan también herramientas de análisis; todos estos requerimientos pueden llegar a exceder fácilmente los $500,000 dlls.

6.3 Tipos de IPS

Al ser una tecnología en desarrollo y ofrecer diferentes posibilidades en una sola, es difícil poder clasificar este tipo de herramientas. Cada una de las diferentes marcas que desarrollan herramienta de seguridad, tienen una forma muy peculiar de describir sus productos de IPS, dificultando con esto su clasificación.

Veamos las siguientes definiciones de IPS:

"La única arquitectura de seguridad de Internet que conecta y protege empleados, oficinas y recursos de red a través del globo "

CheckPoint

"Construidos por el líder en la industria seguridad de la información y tecnologías, los sistemas de seguridad de Internet Preventia Dynamic Therast Protection appliances*, identifican y detienen ataques sin la intervención del usuario"*

ISS

"La solución de NetScren, realiza análisis de información a gran velocidad, inclusive si está se encuentra cifrada"

NetScreen

"Si usted necesita puertas y pistolas en su red NFR es lo que usted busca"

NFR Security

Podemos clasificar los IPS que se encuentran en el mercado, en cuatro diferentes categorías:

- IPS e IDS.
- IPS y Firewall.
- IPS y Anti-Virus.
- Hardware dedicado.

6.3.1 IPS e IDS

Esta categoría se refiere a aquellos vendedores que tradicionalmente han tenido IDS confiables a los que les han añadido la funcionalidad de detener la actividad que generó la alerta, antes de que ésta haya sido deliberada en la red o ejecutada por un host. Esta funcionalidad de evaluar y desechar actividad maliciosa puede ejecutarse a nivel de red o a nivel de host.

Se sabe que los falsos positivos pueden ser un gran problema para la tecnología de IDS, pero lo son aún más en los IPS. Un falso positivo de un IDS genera una alerta que pudiese ser falsa, pero la actividad del IDS es benigna. Un falso positivo en un IPS detendrá servicios o tráfico legítimo, los que podrían ser una función de una aplicación de producción, un servidor de bases de datos o bien, un visitante entrando a una página web. Falsos positivos en un IPS realmente tienen un costo significativo para la organización, ya que pueden causar ataques de denegación de servicio en recursos de producción.

6.3.2 IPS y Firewall

Los firewalls de filtrado de circuito se han convertido en una fuerte tecnología para muchas organizaciones. El paso siguiente para cada vendedor de firewalls es agregar las capacidades de un IPS a sus firewalls. Por la posición en la topología de red que tiene el firewall, es excelente para identificar eventos maliciosos en la red, implementando análisis desde la capa de transporte hasta la capa de aplicación para la identificación de ataques. Como un firewall recolecta y analiza cada paquete que pasa a través de él, una evolución lógica sería que identificara el tráfico malicioso y generar una alerta o bien, que generara una alerta y lo eliminara, esto prevendría que el ataque fuera exitoso[12].

Vendedores como CISCO, NetScreen y ChekPoint han integrado tecnologías de IPS a su línea de productos, además de desarrollar sus propias herramientas. El resultado son firewalls elegantes en lugar del clásico IPS, aunque este término puede confundirse a veces, ya que podrían no quedar claros los beneficios y sobre todo las limitaciones que la tecnología de IPS ofrece.

6.3.3 IPS y Anti-Virus

Un anti-virus es por mucho la herramienta de seguridad con más penetración en el mercado. La mayoría de las organizaciones han implementado manejos de control de distribución, implementación y actualización de sus antivirus. Pocas organizaciones son las que se atreven a poner un equipo en su red sin algún tipo de antivirus instalado.

Los vendedores de antivirus, se encuentran un paso atrás en el mercado de adicionar a sus productos. Tradicionalmente, los antivirus detectan actividad de virus y gusanos, pero están limitados a ese tipo de código malicioso. Recientemente, estos vendedores han empezado a expandir sus productos para identificar otros tipos de código malicioso incluyendo, spyware, puertas traseras, troyanos, etc. Este es un gran paso para la comunidad de antivirus, ya que muchos vendedores se han visto forzados a implementar en sus productos tecnologías similares a las de los antivirus para poder competir contra éstos. Compañías como Symantec han extendido su gama de productos para poder identificar todo tipo de código malicioso, en comparación de lo que tienen otros vendedores.

Las herramientas de antivirus generalmente utilizan dos métodos para proteger tanto las computadoras como los servidores de los virus. El primer método, analiza secuencialmente todos los archivos del sistema, pudiendo iniciarse dado un calendario o porque alguien lo solicite. Cuando un archivo que está infectado es ubicado, el antivirus los limpiará. Este proceso puede llevar demasiado tiempo y consumir muchos recursos, que un equipo de producción no puede darse el lujo de desperdiciar.

Al segundo método, se le conoce como analizador de memoria ya que únicamente analizará los archivos cuando éstos son abiertos y cerrados. Este método de análisis no detectará virus que estén en un estado inactivo en el sistema, pero requiere de mucho menos recursos de procesamiento. Este tipo de método no abre para su análisis archivos que no vayan hacer usados inmediatamente.

Un IPS basado en antivirus trabajará de forma muy similar a un antivirus configurado en realizar análisis de memoria, pero este incluirá también llamadas al sistema en el servidor donde esté siendo utilizado. El escáner de IPS podrá redireccionar las llamadas al sistema (incluyendo exploits y códigos maliciosos) para ser examinadas antes de que el sistema las ejecute. Una vez que el IPS las identifica como benignas, podrán ser pasadas al sistema operativo para que completen su acción. Si estás resultan ser un daño potencial para el sistema, como la alteración de un archivo, correr un proceso o escuchar un puerto, en específico para establecer una puerta trasera, el IPS rechazará la llamada y matará la aplicación.

6.3.4 Hardware dedicado

Este tipo de IPS toma lo mejor de los firewalls, herramientas de IDS y ruteadores/switches poniendo todo esto en un dispositivo de alto rendimiento.

Este dispositivo puede describirse como un NIDS, ya que es instalado en línea en la red. Utiliza una combinación de aplicaciones de análisis, anomalías y reglas basadas en firma para identificar eventos que son malignos para la red. El tráfico de y para la red pasará a través de este dispositivo y todos los paquetes serán analizados antes de ser enviados a su siguiente destino. El tráfico que no genere ningún tipo de alerta será deliberado y el que sea marcado como tráfico malicioso será eliminado y almacenado en un log para su futura revisión.

Esta tecnología parece muy buena, pero su implementación es muy compleja. Como este dispositivo será puesto en línea en la red, deberá ser capaz de soportar la tasa de tráfico, pudiendo tener velocidades de gigabits, además de que el manejo de paquetes debe hacerse de manera rápida y efectiva, implicando un gran consumo de recursos.

6.4 HIPS

Uno de los beneficios más grandes de la tecnología de un HIPS es la habilidad de identificar y detener tanto ataques conocidos como los que no lo son. Esta opción les permite a las organizaciones tener mucho más tiempo para desplegar parches y actualizaciones a sus equipos, ya que un HIPS los tendrá prevenidos ante las técnicas más comunes de ataques.

Para ser efectivo deteniendo los ataques, el HIPS usa una técnica llamada intercepción de llamadas al sistema, que es muy similar a lo que muchos antivirus han utilizado por años. El HIPS inserta sus propios procesos entre las aplicaciones que acceden a los recursos del host y los recursos del sistema operativo. De esta manera el HIPS tiene

la habilidad de permitir o denegar aquellas peticiones basándose en sí este las considera malignas o benignas.

Los HIPS utilizan una combinación de análisis de firma y análisis de anomalías para identificar los ataques, esto es realizado con base en el tráfico de monitoreo de las interfaces de red, monitoreando la integridad de archivos y el monitoreo del comportamiento de las aplicaciones.

6.4.1 Monitoreo de integridad de archivos

Las herramientas tradicionales utilizadas para el chequeo de integridad hacen uso de funciones criptográficas de tipo hash para determinar si algún tipo de cambio se ha realizado. Un software de HIPS utiliza su propio sistema operativo para monitorear si un archivo fue abierto con permisos de lectura/escritura o únicamente escritura en el sistema operativo. Cuando un programa o proceso intenta llamar a una función que cambiara el contenido del archivo como write(), fwritw() o cualquier llamada de modificación, el sistema operativo revisará si este archivo corresponde a alguno de los que se encuentra en la lista de archivos que deben ser monitoreados. Si el archivo debe ser monitoreado, el software de HIPS revisará en la lista si el usuario o aplicación tiene el permiso para hacerlo. Si éste no lo tenía, eliminará la petición de escritura al archivo y enviará una alerta. Si por el contrario, el usuario o aplicación tienen permiso dejará que la llamada al sistema se realice.

Una ventaja significante de un HIPS es la habilidad de definir usuarios autorizados en tiempo real para el monitoreo de integridad de archivos. Esto se puede utilizar en un servidor WEB para prevenir que personas no autorizadas hagan cambios en las páginas de Internet, pero permitiendo a los desarrolladores web de la página hacer cambios cuando sea necesario.

6.4.2 Monitoreo de Redes

Tal como lo hace un NIDS un HIPS monitoreará la red en busca de actividad maliciosa. Un HIPS utiliza análisis de firma y anomalías para identificar los ataques en contra de sistemas individuales. La diferencia es que en lugar de monitorear en forma pasiva, el software de HIPS interceptará los paquetes que se envían y reciben en la red. Al establecerse como intermediario, tendrá la posibilidad de primero analizar y después

enviar el paquete a su destino o bien eliminarlo y generar una alerta. Este proceso es abstracto al tipo de red, interfaz o driver con el que se cuente. Un HIPS es capaz de monitorear tráfico del host con cualquier medio a través de una red inalámbrica, cableada, VPN o un módem.

6.4.3 Comportamiento de las aplicaciones

El monitoreo del comportamiento de las aplicaciones es otra opción que brinda un HIPS cuando un vendedor selecciona una aplicación y graba el funcionamiento de la aplicación en uso normal.

Por ejemplo, si un vendedor provee monitoreo del comportamiento de Microsoft Word, él grabará cómo Microsoft Word interactúa con el sistema operativo y las otras aplicaciones, identificando todas las funciones del producto. Después de juntar todos los datos de cómo la aplicación trabaja, el vendedor crea una base de datos que detalla el funcionamiento de la aplicación. Una vez instalado el software de HIPS identificará y monitoreará el uso de esta aplicación. Si Microsoft Word intenta abrir un archivo del sistema e imprime su contenido, el HIPS reconocerá que es una función normal. Por el contrario si Microsoft Word trata de enviar mails a cada contacto de la lista de Microsoft Outlook, el HIPS reconocerá esta actividad como inapropiada, cerrando por ello la aplicación y enviando una alerta al administrador.

En la práctica, el monitoreo del comportamiento de aplicaciones es difícil de llevar a cabo correctamente, ya que las aplicaciones cambian constantemente incrementando sus funciones mediante actualizaciones o versiones nuevas. La mayoría de los vendedores implementan soluciones híbridas que utilizan una combinación de comportamiento de aplicaciones con análisis de anomalías, usando una lista de eventos anómalos que no deben ser permitidos en el sistema.

Es importante recordar que el análisis de comportamiento de aplicaciones no funciona con cualquier aplicación, sólo con las que son soportadas por el vendedor.

6.4.4 Ventajas de un HIPS

El uso de un HIPS incluye todas las ventajas de un HIDS, ya que identifica el cambio no autorizado de archivos, monitorea la actividad de la red y puede analizar tráfico cifrado. El beneficio que agrega un HIPS es, por supuesto, la habilidad de detener un ataque antes de que éste sea exitoso. Esto representa una gran ventaja para muchas organizaciones que luchan por tener tiempo para realizar actualizaciones y parches de sus equipos.

Representa una gran ventaja para aquellas organizaciones que en los últimos años han tenido que emplear su perímetro de red. No hace muchos años las organizaciones sólo se preocupaban por los ataques provenientes de Internet, pero actualmente los ataques pueden provenir desde redes inalámbricas, módems, VPN, código malicioso introducido por usuarios que viajan hacia la red. Un HIPS provee un mejor método de defender el perímetro de la organización, cuando éste no está claramente definido.

6.4.5 Retos de un HIPS

Se debe recordar siempre, que un HIPS no es una herramienta todo en uno, toda tecnología puede seguir teniendo mejoras. La implementación de un HIPS implica retos tanto de desarrollo como de mantenimiento, pruebas y despliegue de actualizaciones, solución de problemas de configuración, etc. Falsos positivos es el mayor reto en el mercado de los IPS, aunque en un HIPS pueden ser un poco menos significativos ya que afectan sólo al host. De igual forma este reto sigue siendo importante ya que un HIPS puede ser instalado en un servidor web y si un falso positivo se presentara podría dejar en el mejor de los casos, inhabilitada la página de Internet de la organización o en el peor, iniciar un ataque hacia otros equipos.

La capacidad de detectar ataques no conocidos y monitorear el comportamiento anómalo de aplicaciones es una de las grandes ventajas de la tecnología de los IPS, aunque esta característica sólo funciona para las aplicaciones soportadas, las que son decididas por el vendedor. El fortalecimiento de sistemas operativos y las prácticas de código seguro siguen siendo una buena idea para proteger aplicaciones de futuros ataques.

Aunque un HIPS tiene la habilidad de identificar y parar ataques, no puede reemplazar las actualizaciones de los sistemas y las defensas que proporciona un antivirus.

Los IPS aún están en proceso de crecimiento y no es todavía muy claro qué tipo de vulnerabilidades podrían encontrar los atacantes en contra de ellos.

Un software de HIPS reducirá entre un 20% y 30% el rendimiento del equipo en donde sea utilizado, tanto de memoria como de procesamiento, dependiendo de su configuración y opciones de análisis.

Finalmente, se necesita una consola de manejo para llevar un control de los HIPS instalados en una organización, tal y como se haría actualmente con la configuración y mantenimiento de los antivirus. Esto implica un gasto considerable para las organizaciones tanto económico como de tiempo.

6.5 NIPS

Desde la perspectiva de una red, un dispositivo NIPS opera como un switch conectando los segmentos internos y externos de la red. A diferencia de un switch, un NIPS usa una variedad de técnicas para detener ataques desde que entran hasta que salen de la red. Utilizando muchas de las técnicas empleadas por los NIDS, los dispositivos de NIPS pueden identificar eventos en la red que se consideren hostiles. Debido a su posición, en línea con el tráfico de red, un NIPS puede eliminar la actividad hostil antes de ser deliberada al objetivo.

Antes de que un NIPS se considerado como dispositivos efectivo, deberá superar varios retos:

Capacidades de detección

Los dispositivos NIPS utilizan las mismas técnicas de los tradicionales NIDS para reducir el riesgo de falsos negativos, pero no pueden tolerar falsos positivos en la red. Este es un reto muy importante para los NIPS y la mayoría de los vendedores están utilizando evaluación pasiva tanto de sistemas operativos como de vulnerabilidades.

Estabilidad

Debido a que un NIPS es un dispositivo que se pone en línea con el tráfico, representa un único punto de fallo para una red. Los dispositivos NIPS deben ser igual de estables que un firewall o switch para ganar la aceptación en el mercado. Deben ser también resistentes al tráfico malformado y no dejar de funcionar ante los protocolos de red existentes. Este es un riesgo muy similar que el de los falsos positivos, ya que si un NIPS no puede interpretar el tráfico correctamente o falla en el intento, puede causar una falla en la red y denegar así peticiones legítimas. Este tipo de fallas podrían ser accidentales o intencionales por parte del atacante buscando hacer una denegación de servicio.

Rendimiento de procesamiento

Los NIPS deben ser capaces de poder dar salida a todo el tráfico de red. Para ser prácticos y para monitorear redes, el IPS debe manejar velocidades de Gigabit Ethernet.

Latencia

Además de los requerimientos para usar técnicas extensivas de análisis de tráfico de red para identificar ataques, un NIPS debe ser capaz de tener una latencia muy baja, en el rango de los milisegundos.

Seguridad

Un NIPS debe ser seguro en para evitar ser comprometido, ya que un NIPS comprometido puede darle al atacante la habilidad de establecer un ataque de hombre en el medio[3] en contra del tráfico que entra y sale en una red. Esto es logrado comúnmente configurando el NIPS sin ninguna dirección IP o MAC en las interfaces de dato o bien no contar con políticas claras de qué persona puede administrar el NIPS. Todos los atacantes

[3] *Hombre en el medio*, es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

no perderán oportunidad para atacar un NIPS, hacer un ataque de denegación de servicio a la red o eludir la protección que provee, por lo tanto, los NIPS deben ser capaces de resistir cualquier ataque directo.

Con el fin de resistir las demandas de procesamiento y poder identificar tráfico malicioso a alta velocidad y sin latencia, los NIPS deben utilizar hardware de tipo ASICS[4](Application-Specific Integrated Circuit) para realizar procesamientos paralelos. Usando ASICS especializados, los NIPS pueden satisfacer las demandas de rendimiento y escalabilidad, pero sacrificando flexibilidad. Mientras que los NIDS tradicionales operan bajo sistemas como Unix, Linux y Windows, los NIPS requieren más capacidad de procesamiento para cumplir las demandas de procesamiento y baja latencia.

Muchos vendedores están buscando la manera de clasificar e identificar actividad maliciosas con menor demanda de procesamiento del sistema y capacidad de memoria. Una técnica es usar un esquema de clasificación para rápidamente explorar el tráfico para identificar eventos maliciosos. Muchos vendedores utilizan el término de filtrado de multiresolución, en esta técnica, análisis simples son aplicados en primera instancia. El análisis simple contiene sólo una parte de todas las capacidades del NIPS y aquel paquete que falle en una prueba, deberá ser sometido a un análisis profundo.

Por ejemplo, un NIPS requiere que el tráfico que pase a la red tenga algún tipo de dato en el payload. Si ésta primera prueba falla (Tamaño del paquete – Tamaño de la cabecera del paquete = 0), el NIPS no clasificará este paquete para un análisis profundo, simplemente lo desechará. De este modo, el NIPS puede reservar recursos del sistema para análisis más complejos.

Después de aplicar reglas simples, el NIPS procede a aplicar un set de reglas más complejas que puedan examinar la información de la cabecera, estado de la capa de transporte, estado de la sesión en la capa de aplicación, comparativa de cadenas y expresiones en contra del payload, etc.

[4] *ASICS (*Application-Specific Integrated Circuit), en español Circuito Integrado para Aplicaciones Específicas, es un circuito integrado hecho a la medida para un uso en particular, en vez de ser concebido para propósitos de uso general.

6.5.1 Análisis Pasivo

Para ayudar a los NIPS a identificar tráfico falso positivo, los vendedores usan técnicas de análisis pasivo para identificar sistemas operativos de los hosts, arquitectura de la red y qué vulnerabilidades están presentes en una red.

Aprender la arquitectura de red, le permite al NIPS identificar ataques internos basándose en si la dirección IP es interna y el número de saltos que cuenta el ruteador. Si el NIPS ve tráfico en su red interna con una dirección IP que no concuerda con la lista de direcciones internas, o bien, el valor de tiempo de vida es anormal basándose en la historia de la dirección IP, el NIPS podrá identificar estos paquetes falsos en la red interna, eliminándolos antes de que puedan dañar servidores fuera de la organización.

6.5.2 Retos de un NIPS

Un falso positivo en un NIPS significa que tráfico legítimo será eliminado, causando con esto una denegación de servicio. Cualquier organización no puede darse el gusto de provocar falsos positivos con un NIPS, por ello los vendedores utilizan una combinación de análisis pasivo, detección de vulnerabilidades, identificación de la arquitectura de red, jerarquización de reglas y menos reglas que los NIDS tradicionales.

Calcular los requerimientos de procesamiento de un NIPS es un gran reto, debido a que los NIPS realizan un procesamiento y análisis complejo para poder eliminar falsos negativos y falsos positivos mientras examinan el tráfico. La latencia es otro detalle significante, debido al tiempo que es requerido para procesar cada paquete antes de decidir si se transmite o elimina. Tal como un falso positivo, si el NIPS no es capaz de seguir con la demanda de tráfico, causará una denegación de servicio cuando el paquete a transmitir sea eliminado.

Finalmente un NIPS no puede tener una lista muy grande de reglas para identificar ataques en la red. Mientras que un IDS puede pasar al analista una alerta para que éste decida qué hacer, un NIPS tendrá que hacerlo por su cuenta.

6.5.3 Recomendaciones

Las siguientes recomendaciones se deberán tomar en cuenta cuando se considere la implementación de un NIPS:

Revisar los productos en el modo de sólo reporte. Antes de empezar a usar un NIPS y que éste empiece a bloquear ataques en la red, se debe ejecutar en modo de solo reporte. Se puede usar esta información para identificar al evento que el NIPS hubiera eliminado y el impacto que hubieran tenido en la red.

Cautela con los mecanismos de auto-actualización. Se debe probar las nuevas reglas en el modo de sólo reporte, antes de aplicarlas de forma automática.

Documentar un cambio en el mecanismo. Identificar quién será el responsable del manejo de actualizaciones en el NIPS, qué tan seguido y de qué manera éstas se deben llevar a cabo.

Usar una combinación de NIPS y NIDS cuando sea apropiado. No es necesario eliminar un NIDS cuando un NIPS llega a la organización, Se puede seguir utilizando los IDS para identificar amenazas, estadísticas de ataques y un IPS para darle solución a los problemas de la red. O bien, usar ese NIDS para el monitoreo de la red interna.

Identificar los procedimientos de prueba por parte de los vendedores. Esto dará una idea de sí un NIPS se adapta a las necesidades de la organización. Se debe preguntar al vendedor qué técnica utiliza para eliminar falsos positivos y cómo hace para no dejar de lado la verificación de algún tipo de ataque.

Conclusiones Capítulo 6

Existe demasiada especulación en el mercado de los IPS, de hecho cada vendedor lo clasifica y agrega características que cree convenientes. En este capítulo se presentaron las dos grandes clasificaciones de los IPS, los HIPS y los NIPS, que están divididos en 4 diferentes tecnologías.

Los vendedores de firewalls, han adaptado a sus productos la habilidad de poder detener ataques, analizando cada paquete que pasa a través de ellos. Estos tipos de NIPS tienen dos grandes desafíos, el primero y más importante es la capacidad de procesamiento que debe tener el firewall para poder lidiar con tráfico de alta velocidad, además de tener que mantener una latencia muy baja, de lo contrario este dispositivo podría causa una denegación de servicio en la red.

Los vendedores de antivirus han añadido a sus productos la opción de interceptar las llamadas al sistema para ser analizadas, antes de que causen algún daño al sistema. Otra opción que presenta este tipo de IPS es la verificación de integridad de los archivos más importantes para el administrador así como también de checar el comportamiento de las aplicaciones.

Finalmente, es importante recordar que la tecnología de los IPS solamente puede ser utilizada por personal capacitado que comprende claramente la tecnología, tanto sus ventajas como limitaciones. Un IPS no es un reemplazo para las estrategias de defensa en profundidad, pero es una gran tecnología para la seguridad de una organización.

Conclusiones Generales

Dentro de este trabajo, se logro abordar las principales tecnologías de seguridad disponibles en el mercado para la seguridad de redes. Se enumeraron sus principales características, ventajas, desventajas, retos, opciones de configuración, etc. Además se brindó información actual y precisa, utilizando un lenguaje claro y sencillo, para que desde una persona común como hasta un experto en seguridad pudiera entenderla.

Es muy importante entender que toda la información contenida en este trabajo, debe de considerarse como un todo, ya que, teniendo una visión clara de todos los temas, será más fácil visualizar y atacar los problemas de seguridad con los que se puedan enfrentar.

Recordemos que ninguna tecnología de seguridad de redes, es una herramienta todo en uno, a pesar de que los IPS son una de las tecnologías más avanzadas y se pudiese pensar que resuelve cualquier tipo de problemas, no es así. Cualquier tecnología que se implemente, no es sustituto de tener buenas políticas de seguridad, fortalecimiento de sistemas operativos, actualizaciones de antivirus, buenas prácticas, etc.

Cada herramienta que se mencionó tiene un fin particular y cumple con requerimientos muy específicos, de hecho en organizaciones de gran tamaño y con necesidades de seguridad muy grandes, podemos ver interactuar a todas al mismo tiempo y aunque para implementar esto se necesitarían grandes cantidades de dinero, la inversión más grande es en tiempo, pero debido a la importancia y relevancia de su información, la falta de seguridad es algo que no están dispuestos a tolerar.

No se debe olvidar que la herramienta más efectiva y menos costosa en contra de los atacantes es la capacitación y concientización de las personas, ya sean trabajadores de una organización o simples usuarios de internet. Concientizar a las personas de todas las amenazas existentes en cualquier tipo de red, desde una pequeña red casera hasta el mismo Internet, es crucial para poder garantizar niveles aceptables de seguridad. Además de ser una medida que perdurara mucho más tiempo vigente que cualquier hardware o software, la capacitación de las personas ayudara a reducir el número de ataques a otras redes, evitando así la propagación de códigos maliciosos que afecten a terceros.

Se logro, no solo definir y dar las características de cada tecnología, si no también, dar una serie de recomendaciones para su implementación, que muchas veces es lo más difícil de hacer. Muchas personas y organizaciones creen que por tener la capacidad económica podrán implementar seguridad, lo cual no es del todo cierto. El gasto más significativo será la implementación, configuración y mantenimiento de las herramientas. Por ello cualquier organización que decida implementar alguna, deberá de hacer un análisis exhausto tanto de dinero, como el tiempo que esta le consuma.

El siguiente paso a seguir para este trabajo, deberá ser su actualización constante, ya que toda la información referente al mundo de las tecnologías de la información se vuelve obsoleta en un periodo de tiempo muy corto. Podría ser que en menos de tres meses las herramientas vistas en este documento tengan cambios significativos, o bien, que aparezcan nuevas herramientas que dejen a las estudiadas en este trabajo obsoletas.

Glosario

Access points, dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.

Amenaza, es la forma en que un atacante podría intentar afectar a un activo mediante una vulnerabilidad.

Análisis forense, es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados.

Appliance, hardware dedicado a funciones especificas.

ASICS (Application-Specific Integrated Circuit), en español Circuito Integrado para Aplicaciones Específicas, es un circuito integrado hecho a la medida para un uso en particular, en vez de ser concebido para propósitos de uso general.

Attachment, archivo que se envía junto a un mensaje de correo electrónico.

Banner grabber, en español significa capturador de banderas.

Browsing, hace referencia al término navegar en español.

Buffer Overflow, en español desbordamiento de buffer.

Checksum, medida muy simple para proteger la integridad de datos, verificando que no hayan sido corrompidos.

DDoS (Distributed Denial of Service), conocido en español como Denegación de Servicio Distribuido.

DMZ (Demilitarized Zone), en español zona desmilitarizada, es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

DoS (Denial of Service), en español Denegación de Servicio.

Escaneadores, término que hace referencia a las herramientas que realizan un escaneo.

Escaneo, alude a la palabra en inglés scanning, que hace referencia a buscar, analizar, inspeccionar, explorar o investigar, según sea el caso.

Exploit, programa malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa (llamadas bugs).

Falso negativo, es un error mediante el cual el software o hardware falla en detectar un archivo o área del sistema está realmente en peligro.

Falso-positivo, es un error por el que un software o hardware reporta que un archivo o área de sistema está en peligro, cuando en realidad el objeto está seguro.

Firewall, conocido en español como cortafuego, es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

Firmware, es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria de tipo no volátil (ROM, EEPROM, flash,...), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

FTP (File Transfer Protocol), es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.

Hardening, proceso por el que se asegura un sistema.

HIDS (Host Intrusion Detection System), en español Sistema de detección de intrusos basado en host).

HIPS (Host Intrusion Prevention System), en español Sistemas de prevención de intrusos basados en host.

Hombre en el medio, es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

Honeypots, es un software o conjunto de computadoras cuya intención es atraer atacantes, simulando ser sistemas vulnerables o débiles a los ataques.

HTTP (HyperText Transfer Protocol), es el protocolo usado en cada transacción de la Web (WWW).

ICMP (Internet Control Message Protocol), conocido en español como Protocolo de Mensajes de Control de Internet.

ICMP ECHO request, es un mensaje que se envía a un host para que éste le responda con un Echo Reply.

IDS (Intrusion Detection System), conocidos en español como Sistemas de Detección de Intrusos, es un hardware o software usado para detectar accesos no autorizados a una computadora o a una red.

IP Spoofing, ataque que consiste en falsificar una dirección IP.

IPS (Intrusion Prevention System), conocidos en español como Sistemas de Prevención de Intrusos, es un hardware o software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

ISP (Internet Service Provider), en español Proveedor de Servicios de Internet, es una empresa dedicada a conectar a Internet a los usuarios o las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente.

Kernel, software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.

Live-cd, sistema autónomo en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de ficheros.

Logging, es la práctica de grabar datos secuencialmente o en orden cronológico.

MD4 (Message-Digest Algorithm 4), es un algoritmo de resumen del mensaje (el cuarto en la serie) diseñado por el profesor Ronald Rivest del MIT. Implementa una función criptográfica de hash para el uso en comprobaciones de integridad de mensajes.

MD5 (Message-Digest Algorithm 5), es el sucesor de MD4 y al igual que él, implementa una función criptográfica de hash para el uso en comprobaciones de integridad de mensajes.

NAT (Network Address Translation), en español Traducción de Dirección de Red.

NIC (Network Interface Card), en español Tarjeta de Red.
NIDS (Network Intrusion Detection Systems), en español Sistemas de detección de intrusos basados en red.

NIPS (Network Intrusion Prevention System), en español Sistemas de prevención de intrusos basados en red.

P2P (Peer to Peer), se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red.

Paquetes ACK, Contestación afirmativa a un paquete SYN/ACK.

Paquetes SYN, Realizan una apertura activa de un puerto.

Paquetes SYN/ACK, este paquete se utiliza para responder a una petición SYN, en caso de que el puerto este abierto.

PAT (Port Address Transaltion), en español traducción de dirección de puerto, es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna.

Payload, material transmitido sobre la red que incluye dos cosas: datos e información que identifican el origen y destino del material.

Pop-up, término que denomina a las ventanas que emergen automáticamente (generalmente sin que el usuario lo solicite) mientras se accede a ciertas páginas Web.

RFC´s (Request for Comments), en español petición de comentarios.

ROI (Return on Investment), se conoce en español como Retorno de la Inversión.

Ruteador, dispositivo de hardware para interconexión de red de computadoras que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

SHA-1 (Secure Hash Algorithm), es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology.

Switch, conmutador que interconecta dos o más segmentos de red, pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

TCP (Transmision Control Protocol), se conoce en español como Protocolo de Control de Transmisión.
TCP/IP (Transmission Control Protocol/Internet Protocol), conocido en español como Protocolo de Control de Transmisión (TCP) y Protocolo de Internet.

Three-way Handshake, proceso para el establecimiento de una conexión TCP, consta de tres tipos de paquetes SYN, SYN/ACK, ACK.

UDP (User Datagram Protocol), conocido en español como Protocolo de Datagrama de Usuario.

VLAN (Virtual LAN), en español Red de Área Local Virtual, es un método de crear redes lógicamente independientes dentro de una misma red física.

Vmware, es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un ordenador, un hardware) con unas características de hardware determinadas.

VPN (Virtual Private Network), en español Red Privada Virtual.

Vulnerabilidad, hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

War dialer, técnica que consiste en hacer llamadas a una serie de números de teléfono automáticamente con el fin de encontrar módems conectados y permitiendo la conexión con algún equipo e inclusive toda la red.

Referencias

Libros:

[1] Ariganello, Ernesto.
"***Redes CISCO"***
Ed. Alfaomega, México, 2007.

[2]Bragg, Roberta., Rhodes Ousley, Mark., Strassberg, Keith.
" The complete reference: Network Security"
Ed. McGraw-Hill, USA, 2004.

[3]CISCO Systems.
"Guía del primer año CCNA 1 y 2"
Tercera Edición
Ed. Cisco Press, España, 2004.

[4]CISCO Systems.
"Guía del segundo año CCNA 3 y 4"
Tercera Edición
Ed. Cisco Press, España, 2004.

[5]De Laet, Gert., Schauwers, Gert.
"Network security fundamentals"
Ed. Cisco Press, USA, 2004.

[6] Hernández, Leobardo., Daltabuit, Enrique.
"Material del Diplomado de Seguridad de la Información"
Décimo Tercera Edición
México, 2007.

[7]Hernández, Leobardo., Daltabuit, Enrique., Mallén, Guillermo., Vázquez, Jesús.
"La Seguridad de la Información"
Ed. LIMUSA, México, 2007.

[8]Lock, Hart.
"Network security hacks"
Second Edition
Ed. O´Reilly, USA, 2006.

[9] Maiwald, Eric.
"Network Security: A Beginner's Guide"
Second Edition
Ed. McGraw-Hill, USA, 2003.

[10]SANS Institute.
"Defense in depth"
Ed. SANS Institute, USA, 2007.

[11]SANS Institute.
"Networking Concepts"
Ed. SANS Institute, USA, 2007.

[12]SANS Institute.
"Secure Comunications"
Ed. SANS Institute, USA, 2007.

[13]Stallings, William.
"Network Security Essentials"
Third Edition
Ed. Prentice Hall, USA, 2006.

[14]Tanenbaum, Andrew S.
"Redes de Computadoras"
Cuarta Edición
Ed. Prentice Hall, México, 2003.

Internet (Consultadas antes del 7 de Noviembre de 2008):

Firewalls

[15]http://www.tech-faq.com/firewall.shtml
[16]http://linuxiandounrato.blogspot.com/2006/09/conceptos-sobre-firewalls-de-filtrado.html
[17]http://www.ramonmillan.com/tutorialeshtml/cortafuegos_parte1.htm
[18]http://www.sidewinder.com/
[19]http://www.dsd.gov.au/infosec/evaluation_services/epl/network_security/Secure_GauntletFirewall.html
[20]http://www.zonealarm.com/
[21]http://www.symantec.com/norton/internet-security
[22]http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci906407,00.html
[23]http://es.wikipedia.org/wiki/DMZ

Honeypot

[24]http://www.securityfocus.com/infocus/1803
[25]http://www.securityfocus.com/infocus/1828
[26]http://www.first.org/resources/papers/conf2006.html
[27]http://es.wikipedia.org/wiki/VMware
[28]http://www.governmentsecurity.org/articles/HoneypotsDefinitionsandValueofHoneypots.php

[29]http://awprofessional.com/articles/article.asp?p=30489&seqNum=5&rl=1
[30]http://www.securityfocus.com/infocus/1492
[31]http://books.google.com/books?id=3tOVQwCaKikC&dq=external+honeypots
[32]http://www.honeynet.org
[33]http://www.philippinehoneynet.org/index.php?option=com_docman&task=cat_view&gid=16&Itemid=29
[34]http://www.securityfocus.com/infocus/1498
[35]http://www.honeynet.org/papers/individual/HPframework.pdf
[36]http://www.10t3k.org/security/tools/honeypot

IDS/IPS

[37]http://www.securityfocus.com/infocus/1520
[38]http://www.snort.org/docs/iss-placement.pdf
[39]http://isc.sans.org/
[40]http://es.wikipedia.org/wiki/Suma_de_verificaci%C3%B3n
[41]http://www.techterms.com/definition/payload
[42]http://www.sans.org/reading_room/whitepapers/detection/1665.php
[43]http://es.wikipedia.org/wiki/Ataque_Man-in-the-middle

Vulnerabilidades

[44]http://es.wikipedia.org/wiki/Ventana_emergente
[45]http://www.sans.org/top20.htm
[46]http://es.wikipedia.org/wiki/Punto_de_acceso
[47]http://wardriving.com/
[48]http://en.wikipedia.org/wiki/McNealy

Varios

[49]http://www.cert.org/tech_tips/home_networks.html
[50]http://www.nsa.gov/snac/support/sixty_minutes.pdf
[51]http://nsit.uchicago.edu/services/safecomputing/
[52]http://www.first.org/resources/papers/
[53] http://es.wikipedia.org/wiki/Informacion
[54]http://nautopia.coolfreepages.com/snort/snort1/tcp_ip_osi.jpg
[55]http://technet2.microsoft.com/windowsserver/es/library/d1e53415-9a93-4407-87d2-3967d62182dc3082.mspx?mfr=true
[56]http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
[57]http://openlearn.open.ac.uk/mod/resource/view.php?id=183166