ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTAR POLITICAS DE SEGURIDAD A NIVEL DE SOFTWARE"

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

Ivo Leodan Cabrera Sánchez
Marco Andrés Segura Romero
Daniel Enrique Granizo Franco

GUAYAQUIL – ECUADOR
2008

AGRADECIMIENTO

En primer lugar a Dios, por darnos la fuerza y permitirnos llegar a ésta etapa de nuestra vida en la cual terminamos un largo trecho.

Un agradecimiento para los Ingenieros Ivonne Martín y Jack Sánchez quienes nos brindaron su apoyo de forma desinteresada con sus conocimientos. Y en especial al Ingeniero José Escalante para incrementar con sus consejos la confianza y fe de persistir en el cumplimiento de nuestras metas.

DEDICATORIA

A Dios, Marco Vinicio, Melania, Tatiana,
Marco Andrés Jr. y Carlos Daniel, quienes
siempre de una u otra forma colaboraron
en la consecución de éste logro, gracias
por la paciencia y el tiempo.

Marco Andrés

A Dios; a mis padres; a todos quienes sin tener la obligación me brindaron su apoyo en el transcurso de esta carrera; y para aquellos profesores que supieron ser maestros.

Daniel Enrique

Al todopoderoso, mis padres,

a mis hermanos por el incondicional

apoyo, finalmente al movimiento

integración estudiantil.

Ivo Leodan

TRIBUNAL DE GRADUACIÓN

Ing. Holger Cevallos

SUB-DECANO DE LA FIEC

PRESIDENTE

Ing. José Escalante

DIRECTOR DE TESIS

Ing. Rebeca Estrada

VOCAL

Ing. Edgar Leyton

VOCAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL)

RESUMEN

Las políticas que se implementan dentro de una empresa, son los parámetros los cuales se han determinado para su estricto seguimiento; seguimiento que se consigue dando a cada uno de los usuarios de la red la información pertinente y detallada que cada uno de éstos necesita, estableciendo restricciones, permisos y todo aquello que se deba conocer por parte de los usuarios para que en lo posterior no existan dudas sobre las políticas. Siempre que se busca la seguridad, se debe tener en cuenta de que no existe sistema perfecto ni inviolable, uno de los mayores retos que presenta el establecer políticas es el tener claro cómo reaccionará el sistema ante ataques, que en teoría se pueden prever, pero no hay forma de experimentar éstos hasta sufrir uno realmente; al estar conscientes de aquello debemos procurar que el sistema esté en constante evolución para abarcar toda la gama de innovaciones tecnológicas que se dan para producir ataques a nivel de software.

INDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCION

Dado el hecho de que la seguridad en cualquier estrato de la vida es un factor preponderante, y el manejo de redes no se escapa de esto, cae por su propio peso lo extremadamente necesario que resulta el implementar políticas para manejar de una forma correcta y eficiente la seguridad a nivel del software que esté siendo utilizado en una red, sea cual fuese su topología y el campo para el cual ésta estuviese abocada.

Las políticas que se implementan dentro de una empresa, son los parámetros los cuales se han determinado para su estricto seguimiento; seguimiento que se consigue dando a cada uno de los usuarios de la red la información pertinente y detallada que cada uno de éstos necesita, estableciendo restricciones, permisos y todo aquello que se deba conocer por parte de los usuarios para que en lo posterior no existan dudas sobre las políticas.

Siempre que se busca la seguridad, se debe tener en cuenta de que no existe sistema perfecto ni inviolable, uno de los mayores retos que presenta el establecer políticas es el tener claro cómo reaccionará el sistema ante ataques, que en teoría se pueden prever, pero no hay forma de experimentar ésto hasta

sufrir uno realmente; al estar conscientes de aquello debemos procurar que el sistema esté en constante evolución para abarcar toda la gama de innovaciones tecnológicas que se dan para producir ataques a nivel de software, teniendo en cuenta no sólo la estructuración de nuevos programas, sino también percatándonos de que variantes presenta la llamada Ingeniería Social.

El contenido de nuestro trabajo se desarrolló en cuatro capítulos: en el capítulo 1 se muestran tipos de redes, el concepto claro de lo que representa la seguridad, restricciones que reducen peligros, como identificar recursos que nos proporcionan mayor ajuste a las políticas, así como el analizar los posibles riesgos que podrían presentarse, estableciendo claramente que variaciones pueden existir en cada uno de éstos; en el capítulo 2 se presenta lo que es una posible vulnerabilidad, un riesgo y también lo que son ataques, dando definiciones de términos concernientes al tema seguridad, y luego se presenta en extenso lo que son los diferentes tipos de vulnerabilidades, de riesgo y de ataque; en el capítulo 3 hemos realizado un análisis de la red, y hubo una revisión de las políticas, para luego estudiar las herramientas de red, su funcionamiento y diferentes especificaciones que presentan varias de éstas herramientas, utilizando NESSUS, NMAPS, CISCO RAT, diferentes dispositivos para análisis de la red; finalmente en el capítulo 4 se realizó el caso estudio,

implementando una red virtual con un servidor web, un host y un firewall de la marca Checkpoint, se compartieron archivos y carpetas dando privilegios diferentes según el usuario desde la interfaz del servidor, y sobre la red se realizaron ataques con diferentes formas para hallar cuál es la más efectiva, también captura de tráfico para obtener lo que se está transmitiendo a través de la red, y se actuó como un hacker ético buscando sólo probables agujeros en la seguridad del sistema, más no para hacer daño alguno.

CAPÍTULO 1

1 PRINCIPIOS BASICOS A LA SEGURIDAD DE REDES

1.1 Tipos de Redes

1.1.1 Cerrada

En lo que se refiere a redes cerradas, cabe mencionar dos variantes, la primera sería llamada exclusiva y es aquella que por motivo de seguridad, velocidad o ausencia de otro tipo de red, conecta dos o más puntos de forma exclusiva. Este tipo de red puede estructurarse en redes punto a punto o redes multipunto; y la segunda denominada privada es la que se gestiona por personas particulares, empresas u organizaciones de índole privado, en este tipo de red solo tienen acceso los terminales de los propietarios.

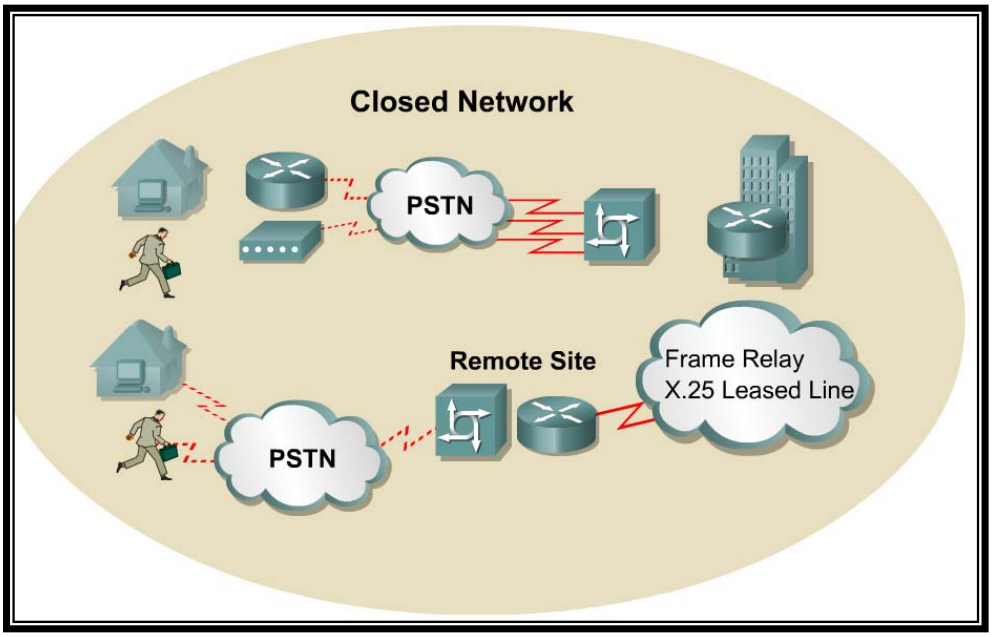


Figura 1.1 Red Cerrada

1.5 Abierta

En las llamadas redes abiertas se dan dos tipos diferentes, la primera de ellas llamada Compartida, denominada de ésta forma porque se une a ella un gran número de usuarios, compartiendo todas las necesidades de transmisión e incluso con transferencias de otra naturaleza; y la siguiente designada como Red Pública, y ésta debe su nombre al hecho de pertenecer a organismos estatales y se encuentra a disposición de cualquier usuario que lo solicite mediante el correspondiente contrato. La red abierta es una expresión de valores fundamentales como la libertad, la igualdad de oportunidades, la solidaridad y fraternidad a través del

derecho a comunicarse libremente y a extraer el máximo de prestaciones posibles. En caso de cualquier duda sobre algún aspecto concreto, siempre nos referimos a estos principios fundamentales. La red permite el acceso a todos los que lo deseen, y es el resultado de intercomunicar a todos sus miembros. Si hay mecanismos de control en su acceso se utilizarán para la correcta gestión de la red desde un punto de vista tecnológico y nunca para excluir el acceso a la red. Si bien los equipos e infraestructuras pueden responder a múltiples modelos de propiedad o titularidad, la red como tal nunca puede tener un dueño o propietario, con independencia de cual haya sido la aportación de cada parte a la red. Los participantes de la red abierta extienden la cobertura de la red en las mismas condiciones, aceptando la libre circulación de comunicaciones de otros miembros, sin manipularlas más allá de lo necesario para la gestión de la red. Los miembros de la red, con tal de facilitar el crecimiento y conectividad, se comprometen a considerar otorgar permiso para dejar instalar equipos que sean propiedad de otros miembros en sus instalaciones, aunque siempre se reserven la última decisión en este sentido y aunque lo autoricen, ésta autorización no genera ninguna servidumbre y es revocable.

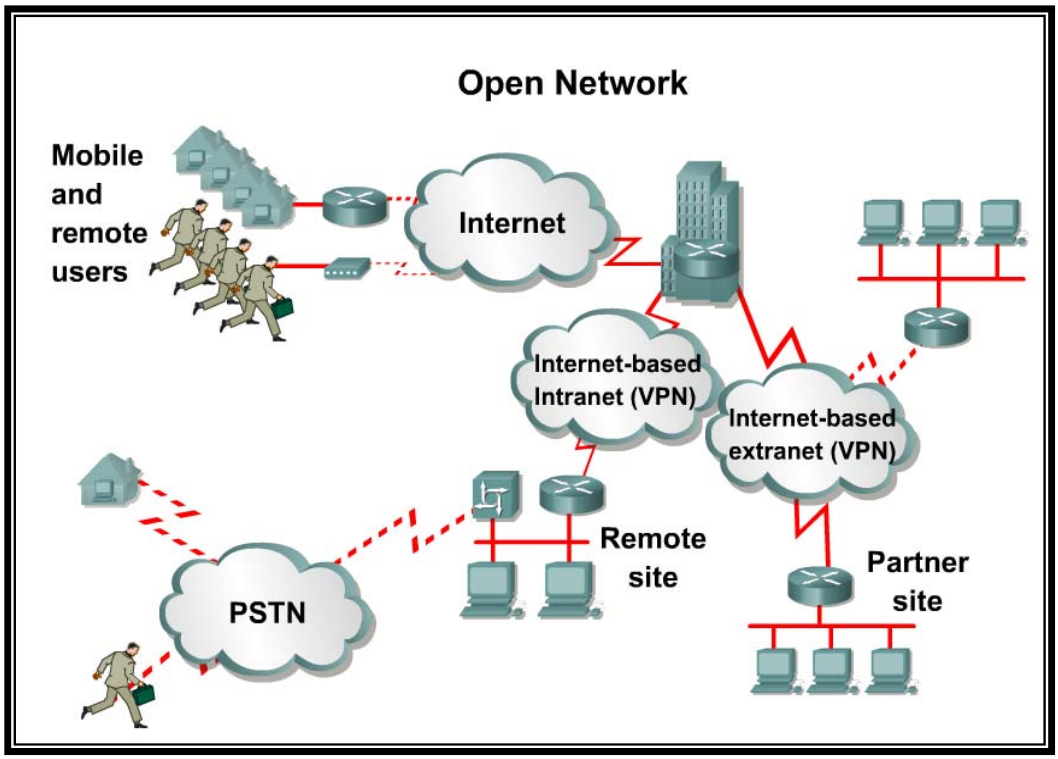


Figura 1.2 Red Abierta.

1.2 Seguridad

"Proceso que implica la protección de la operación de la Red y de la información que por ella transita". Esto es protección ante los ataques maliciosos externos que implican, también, los efectos producidos por fallos en los equipos usados para proteger. Cada día se confía más en las Tecnologías de la Información y en la comunicación digital entre la empresa y su entorno, e Internet se ha convertido en un importante canal de comunicación e interacción entre empresas. Esto provoca una falta de

contacto físico entre los interlocutores, lo que requiere un aumento de la seguridad para crear confianza. La única manera de que una máquina o red sea segura es el aislamiento de la misma (aun así existe riesgo de ataque), ya que una vez conectados a otros sistemas estamos asumiendo la posibilidad de ser atacados. Como eso no es posible, las políticas de seguridad tratan de aportar el mayor nivel de seguridad posible, manteniendo la operatividad de los sistemas y redes.

Cada miembro de la red es responsable de su seguridad, evitar la intrusión en sus propios sistemas de información y descifrar sus comunicaciones si así lo desea. La red abierta simplemente proporciona el medio de transporte para hacerlo posible; se pueden conectar redes privadas a la red abierta, y poner cortafuegos para controlar el acceso. La red abierta no se hace responsable de ningún daño causado a sus miembros durante el uso de la red.

1.3 Restricciones de seguridad a los usuarios.

En la arquitectura de seguridad de una red es fácilmente predecible que el factor humano es el factor más vulnerable a sufrir ataques, amenazas o daños: voluntarios o involuntarios; por acción u omisión de las políticas

internas de seguridad o a permitir, de igual manera, el acceso a potenciales aplicaciones o enemigos externos ayudándolos así a flanquear la delimitación periférica de la red.

Una empresa segura debe establecer, implementar y publicar políticas de seguridad claras y precisas pero además debe preocuparse de la absoluta comprensión y aplicación de dichas políticas por parte del recurso humano con que cada empresa cuenta, puesto que cada usuario de la red es un punto de acceso a los recursos informáticos y por medio de él, sus privilegios o las aplicaciones que desarrolle, podría presentarse una violación de la seguridad. Es indispensable que todos y cada uno de los miembros del personal que goce de privilegios de conexión conciba adecuada y sobre todo apliquen rigurosamente las políticas de seguridad si se desea obtener una implementación efectiva, ya que la mejor política de seguridad es absolutamente inútil si se la pasa por alto.

El error más frecuente en la mayoría del personal es descuidar el sigilo de sus propios medios de acceso a la intrared. De ello deriva la divulgación de claves o códigos de acceso que suele ser el error más duro de lidiar para el administrador ya que todos los sistemas y políticas de seguridad se basan

en el control del acceso, verificación de identidad y protección de los beneficios informáticos de la red ya que son la barrera de entrada a la potencial perdida de información restringida. Podría pensarse que el atesorar sus accesos es un criterio innato, natural, debido a todo lo que el acceso personal implica pero en la práctica no se cumple. El personal sigue y seguirá dejándolos en sitios tan visibles como un *Post-Note* en monitor de su ordenador o en notas sueltas en el escritorio, también reinciden en establecer *passwords* tan fácilmente predecibles como los nombres propios o de allegados y por último pero no menos peligrosos es dejar en los equipos la clave por *default* que es igual para todos los equipos similares del mismo fabricante.

Por ejemplo, un miembro de seguridad con acceso físico a todo el entorno de red que comprometa la verificación de su identidad por alguna de las causas anteriores podría exponer un UPS y dejar sin alimentación eléctrica a toda o parte de la estructura informática de la compañía.

Este es el punto directo en el que se debe remarcar la política de seguridad interna y es el ámbito en el que surte mejor efecto si se mantiene un estricto control y capacitación permanente sobre todo el personal. Además

se puede de clasificar la intrared para determinar las áreas de mayor susceptibilidad y por ende aplicar mayor énfasis en su manejo y control. Esta clasificación, hecha bajo las directrices y especificaciones administrativas de la empresa, es de vital importancia y básicamente se puede describir como la categorización vertical y horizontal de todos y cada uno de sus empleados. A saber; el orden jerárquico o vertical de los empleados habitualmente varia de acuerdo a su responsabilidad, la capacidad en la toma de decisiones e incidencia directa con algún sector productivo de la compañía; en contraparte la clasificación horizontal no es necesariamente igual ya que considerando el criterio de productividad y actividad de la empresa en la que se aplique la seguridad de redes tal vez no todos los empleados desarrollen actividades iguales para no redundar y desperdiciar recursos o quizá en otro caso, alguna categoría deba tener exactamente los mismos beneficios.

Dependiendo de esta clasificación se gerencian los privilegios de red que se deben otorgar a los usuarios. A mayores privilegios mayores seguridades y considerando la importancia y los recursos destinados por parte de la empresa podría combinarse con periféricos de control de acceso físico como un dispositivo biométrico.

PROTOCOLO	CARACTERISTICAS	PROTOCOLOS USADOS
Usuario/Password	Plaintext, Token memorizado	Telnet, http
CHAP(Challenge Handshake Authentication Protocol)	Uses hashes de passwords y datos variantes en el tiempo para evitar la transmisión directa de la clave.	MS-CHAP, PPP, APC http, Radius
RADIUS	CHAP metodos directos de claves, autorizaciones y cuentas.	Backend para Telnet, SSH, SSL, front end para Microsoft IAS Server. Metodos típicos para centrales de autenticación para dispositivos de red.
TACACS+	Soporte para autentificación, autorización, cuentas y encriptaciones de alto nivel.	Protocolos Cisco, central de autentificación y algunos RAS (Remote Access Service)

Keberos	Servicios de autentificación y autorización, encriptación de lato nivel.	Keberized aplicaciones como Telnet, autentificación de dominios de Microsoft con servicios integrados con Active Directory.

Tabla I: Protocolos de Autentificación.

Datos: La razón de la seguridad a nivel mundial, al existir varios niveles de importancia de datos para cada empresa, entonces se convierten en el tesoro mas preciado.

Los problemas de seguridad a nivel de datos son básicamente:

- ✓ Filtración de información confidencial tal como datos personales, secretos profesionales o información reservada de una empresa, al intercambiar datos en línea.
- ✓ Monitoreo de acceso o control de las actividades que una persona, realice en la Red.
- ✓ La seguridad de las transacciones electrónicas en sitios comerciales y de servicios bancarios.
- ✓ La protección contra la manipulación de datos personales y las posibilidades de rastreo de las actividades realizadas por medio de

redes, con la injerencia en la vida privada que ello supone son problemas que se suscitan a diario.

- ✓ La respuesta a formularios que contienen datos personales o empresariales para acceder a ciertos sitios de la red o realizar transacciones en línea son un medio común de irrigación de valiosa información; las posibilidades técnicas de recoger los datos incluidos en la información suministrada a cada computador por medio de programas que se instalan en él cuando se realiza una conexión con un sitio son muy altas, aunque para tranquilidad de los usuarios es necesario aclarar que no todos los *Cookies,* bloques de texto que son localizados en un archivo del disco duro de su computador por una página Web que es visitada y son utilizados para identificarlo la próxima vez que visite el sitio, tienen esas capacidades de recolección de información.

Aplicaciones: Son el interfaz final de los datos transmitidos y son el contacto con el usuario para que este los pueda comprender y sacar su optimo valor y dependiendo de la actividad de la empresa, el valor de la información que maneja y la seguridad que tengamos las perdidas pueden realmente significativas. Por Citar Algunos ejemplos:

Tele trabajo: Igualmente puede ser utilizada para la elaboración de documentos en línea, por varios profesionales conectados desde sus despachos u hogares o para la prestación de servicios a distancia, tales como conceptos, asesoría a distancia (De menor complejidad que el diagnóstico médico desde sitios remotos).

Telemedicina: Es la prestación de servicios de medicina a distancia. Para su implementación se emplean usualmente tecnologías de la información y las comunicaciones. La telemedicina puede ser tan simple como dos profesionales de la salud discutiendo un caso por teléfono hasta la utilización de avanzada tecnología en comunicaciones e informática para realizar consultas, diagnósticos y hasta cirugías a distancia y en tiempo real; cuando es utilizada la red por un médico y su paciente, éste debe estar dispuesto a la conexión, en caso contrario el paciente tiene la opción de esperar.

Comunicación: La red tiene aplicación en conexión de oficinas gubernamentales, despachos judiciales, centros de estudio e incluso Bufetes de abogados, dando ciertos parámetros bajo los cuales los

usuarios se encuentran regidos, comúnmente se dan jerarquías en función de los cargos de quienes ocupan la red.

1.4 Análisis de Riesgos

Los ataques e incidentes contra la seguridad de las redes mantienen un alarmante crecimiento en los últimos años y como la complejidad de las amenazas tienen una relación directa a dicho incremento en respuesta los administradores deben conocer a cabalidad sus redes y todos los dispositivos con que ellas cuentan además de los principios de seguridades mas eficientes que pueden aplicarse para poder proponer y mantener una protección efectiva a sus realidades.

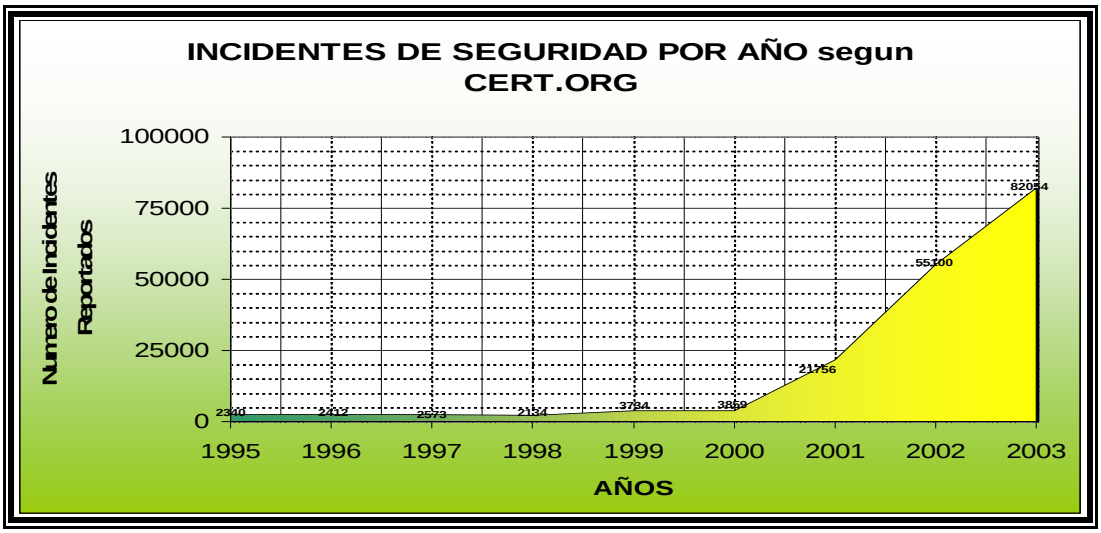


Figura 1.3 Incidentes de Seguridad Reportados por año.

Como su nombre lo indica, consiste en analizar el sistema de información y su entorno para detectar todos los riesgos que amenazan su estabilidad y su seguridad. Uno de estos análisis es la valoración de cada uno de los elementos de la red aplicando las características de seguridad necesarias**.** Existe un criterio que predica que “se puede asumir cualquier riesgo” que básicamente significa que las decisiones de aceptar, transferir o mitigar los riesgos se hacen de acuerdo con dos criterios:

- ✓ Que la persona encargada de tomar las decisiones tiene información suficiente para entender el riesgo.
- ✓ Que el alcance de autoridad y responsabilidad de la persona que toma las decisiones se circunscribe a los activos que están en riesgo.

Para un análisis exitoso de riesgos se establecen los siguientes principios:

- ✓ El establecimiento de mecanismos para mantener riesgos bajo revisión y asegurarse de que ellos están siendo bien diseccionados.
- ✓ El medio para identificar el riesgo potencial hacia el negocio.
- ✓ Una evaluación de la probabilidad de cada materialización de riesgo

- ✓ Una evaluación del impacto probable de cada riesgo
- ✓ La formulación de medidas para evitar cada ocasión de riesgo
- ✓ El desarrollo y el despliegue de medidas para mitigar los riesgos si existe una suspensión de acciones.
- ✓ La determinación de la urgencia del riesgo y el como tomar medidas apropiadas que contrarresten el riesgo.

1.4.1 Identificación de Recursos

Debido a que implementar una red no es una tarea sencilla muchos desafíos deben enfrentarse, a considerar: conectividad y confiabilidad, control, mantenimiento y manejo además de la flexibilidad de la red deben satisfacerse en un nivel aceptable para que pueda calificarse una red como funcional. Las redes de intercomunicación de equipos y periféricos informáticos para suelen iniciar como conexiones empíricas donde prima únicamente el interés de poder intercomunicar dispositivos y que dicha intercomunicación funcione adecuadamente pasándose por alto el otro pilar fundamental del networking, la seguridad. La experiencia dice que ocasionalmente será notable y claramente visible la necesidad de derivar en una red con al menos un

nivel básico de seguridad o protección para los usuarios y para los equipos. Es decir migrar a una red segura.

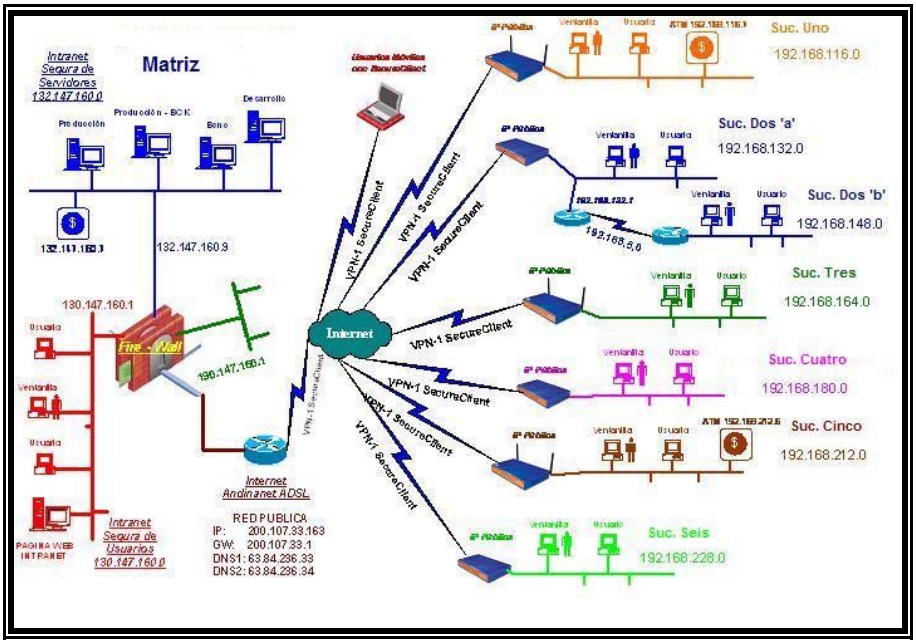


Figura 1.4 Bosquejo de una Estructura de red grande.

“No es posible proteger aquello que no se conoce”.

Siguiendo esta premisa entonces el primer paso a seguir para poder implementar una política efectiva de seguridad es identificar los elementos que componen nuestra red y el valor que ellos representan dentro del esquema de seguridad. Así, tenemos que priorizar algunos elementos que destacan por su nivel de importancia sobre el resto, como por ejemplo:

- ✓ Servidores.

- ✓ Bases de datos.
- ✓ Centrales de energía.
- ✓ Documentos y datos de vital importancia para la empresa.

Otro procedimiento primordial para el aspecto para establecer la seguridad de una red es el llevar presente en todas las consideraciones un inventario actualizado donde se especifiquen todos y cada uno de los dispositivos informativos o de soporte informático con que la red cuente, sus respectivas ubicaciones físicas y características principales, posibles debilidades en detalle por unidad informática y en conjunto, un calendario de mantenimientos y todo lo inherente a la red interna de transmisión de datos. También debe darse el respaldo físico o relaciones de dependencia necesarias para los elementos de la red como por ejemplo, si las computadores tienen un respaldo energético como es el caso de los UPS, dichos UPS se deben considerar parte de la red y aplicarse todos las políticas de seguridad sobre ellos también.

Componentes de Software

La seguridad de software busca optimizar los sistemas operativos y las aplicaciones que trabajan en el sistema de información, de manera que sean configurados de forma segura y solo permitan su utilización dentro de parámetros de funcionamiento predefinidos y aceptados (aseguramiento), que funcionen de manera continua y estable (disponibilidad), que ofrezcan un servicio con un nivel de calidad aceptable (calidad del servicio), que no permitan su utilización por personas no autorizadas (control de acceso), y que permitan establecer las responsabilidad de uso de cuentas (accountability).

Herramientas software

Las herramientas software son necesarias para monitorizar tendencias e identificar problemas en el rendimiento de la red. Algunas de las herramientas más útiles de este tipo son:

Monitores de red

Los monitores de red son herramientas software que analizan el tráfico de la red o de una parte. Examinan paquetes de datos y recopilan información sobre los tipos de paquetes, errores y tráfico

de paquetes desde y hacia cada equipo. Los monitores de red son muy útiles para establecer parte de la línea base de la red. Una vez que se ha establecido la línea base, podrá solucionar los problemas de la red y monitorear la utilización de la red para determinar cuándo es el momento de actualizar. Como ejemplo, supongamos que después de la instalación de una red nueva, determina que el tráfico de la red está utilizando un 40 por 100 de la capacidad estimada. Al volver a comprobar el tráfico de la red al año siguiente, observa que ahora se está utilizando un 80 por 100. Si ha estado realizando la monitorización a lo largo de ese tiempo, podría ser capaz de predecir la tasa de incremento de tráfico y predecir cuándo realiz2ar una actualización antes de que se produzca un fallo.

Algunos servidores ya incluyen software para la monitorización de la red. Por ejemplo, Windows NT Server incluye una herramienta de diagnóstico denominado Monitor de red. Esta herramienta da al administrador la posibilidad de capturar y analizar secuencias de datos de la red desde y hasta el servidor. Estos datos se utilizan para diagnosticar problemas potenciales de la red.

Los paquetes de datos de una secuencia de datos constan de la siguiente información:

- ✓ La dirección de origen del equipo que envió el mensaje.
- ✓ La dirección de destino del equipo que recibió la trama.
- ✓ Las cabeceras utilizadas por cada protocolo para enviar la trama.
- ✓ Los datos o parte de la información que se envió.
- ✓ Protocolo básico de gestión de red (SNMP).

El software de administración de la red sigue los estándares creados por los fabricantes del equipamiento de la red. Uno de estos estándares es el Protocolo básico de gestión de red (SNMP).

En un entorno SNMP, los programas denominados «agentes» se cargan en cada dispositivo administrado. Los agentes monitorean el tráfico de la red para recopilar datos estadísticos. Estos datos se guardan en una base de información de administración (MIB).

Los componentes SNMP incluyen:

- ✓ Hub.

- ✓ Servidores.
- ✓ NIC.
- ✓ Routers y bridges.
- ✓ Otro equipamiento de red especializado.

Para recopilar información en una forma utilizable, un programa de administración pregunta periódicamente a estos agentes y descarga la información de sus MIB. Una vez que se recopila esta información, el programa de administración puede realizar dos tareas más:

- ✓ Presentar la información en forma de gráficos y mapas.
- ✓ Enviar la información a los programas de base de datos para que sean analizados.

Si alguno de los datos cae dentro de los umbrales definidos por el administrador, el programa de administración puede avisar al administrador mediante alertas en el equipo o marcando automáticamente un número de un buscapersonas, mensajes sms, etc... A continuación, la organización, puede utilizar el programa de administración para implementar las modificaciones de la red.

Analizadores de protocolo

Los analizadores de protocolo, también llamados «analizadores de red», realizan análisis del tráfico de la red en tiempo real utilizando captura de paquetes, decodificación y transmisión de datos. Los administradores de la red que trabajan con redes de gran tamaño trabajan constantemente con el analizador de protocolos. Éstas son las herramientas que se suelen utilizar para monitorear la interactividad de la red. Los analizadores de protocolo miran dentro del paquete para identificar un problema. También pueden generar estadísticas basándose en el tráfico de la red para ayudarle a crear una imagen de la red, incluyendo:

- ✓ Cableado.
- ✓ Software.
- ✓ Servidores de archivos.
- ✓ Estaciones de trabajo.
- ✓ Tarjetas de red.

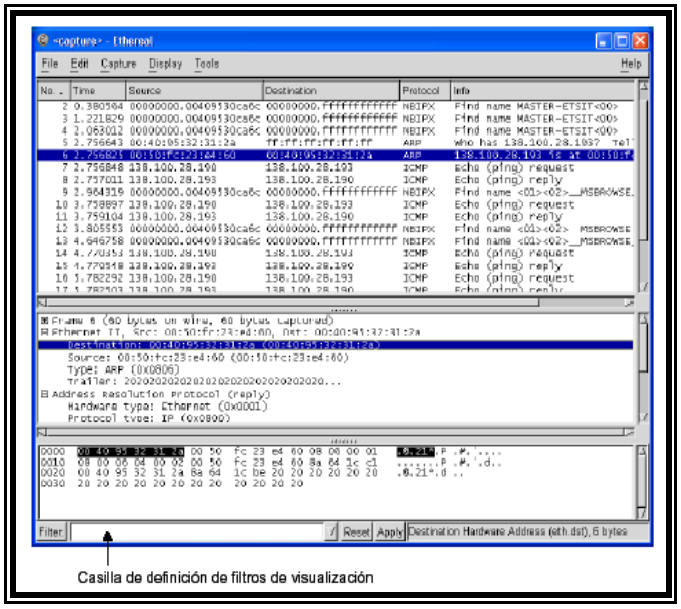


Figura 1.5 Aspecto de la ventana principal del analizador:

Los analizadores de protocolo tienen TDR incorporados.

El analizador de protocolos puede proporcionar pistas y detectar problemas de red como:

- ✓ Componentes defectuosos en la red.
- ✓ Errores de configuración o de conexión.
- ✓ Cuellos de botella en la LAN.
- ✓ Fluctuaciones en el tráfico.
- ✓ Problemas con los protocolos.
- ✓ Aplicaciones que pueden entrar en conflicto.
- ✓ Tráfico no habitual en el servidor.

- ✓ Los analizadores de protocolo pueden identificar muchos aspectos de la red:
- ✓ Identificar los equipos más activos.
- ✓ Identificar los equipos que están enviando paquetes con errores.
- ✓ Si un equipo genera mucho tráfico y está ralentizando la red, el equipo debería cambiarse a otro segmento de la red. Si un equipo está generando paquetes erróneos, debería retirarse y repararse.
- ✓ Ver y filtrar ciertos tipos de paquetes. Esto es útil para distribuir el tráfico.
- ✓ Los analizadores de protocolo pueden determinar qué tipo de tráfico está pasando por un segmento de red determinado.
- ✓ Conocer el rendimiento de la red para identificar tendencias.
- ✓ El análisis de tendencias puede ayudar al administrador a planificar y configurar mejor una red.

- ✓ Comprobar componentes, conexiones y el cableado generando paquetes de prueba y comprobando los resultados.
- ✓ Identificar condiciones problemáticas configurando parámetros para generar alertas.

Herramientas para monitorización y diagnóstico

Una vez que se haya instalado la red y se encuentre operativa, el administrador tiene que asegurarse de que funciona correctamente. Para hacer esto, el administrador tendrá que gestionar y controlar cada uno de los aspectos del rendimiento de la red.

Información general sobre la administración de la red

El ámbito de un programa de administración de la red depende de:

- ✓ El tamaño de la red.
- ✓ El tamaño y las capacidades de la organización.
- ✓ El presupuesto de la organización para la red.
- ✓ Las expectativas que tenga puesta la organización en la red.

- ✓ Las redes pequeñas peer-to-peer que consten de 10 equipos o menos pueden ser monitorizadas visualmente por una persona. En cambio, una red más grande o WAN puede necesitar un equipo dedicado y un equipamiento sofisticado para realizar la monitorización apropiada para la red.
- ✓ Una forma de asegurar que la red no falla es observar ciertos aspectos del comportamiento diario. Una monitorización consistente de la red permitirá observar que hay ciertas áreas en las que empieza a disminuir el rendimiento.

Monitores de rendimiento

La mayoría de los sistemas operativos de red actuales incluyen una utilidad de monitorización que ayudará al administrador a analizar el rendimiento del servidor de la red. Estos monitores pueden ver operaciones en tiempo real o en diferido para:

- ✓ Procesadores.
- ✓ Discos duros.
- ✓ Memoria.
- ✓ Utilización de la memoria.

- ✓ Toda la red.
- ✓ Estos monitores pueden:
- ✓ Guardar los datos de rendimiento.
- ✓ Enviar una alerta al administrador de la red.
- ✓ Iniciar otro programa que pueda devolver al sistema a unos rangos aceptables.

Al monitorear una red, es importante establecer una línea base. Esta documentación de los valores normales de operación de la red debería actualizarse periódicamente a medida que se realizan cambios en la red. La información de línea base le puede ayudar a identificar y monitorizar cambios dramáticos y sutiles en el rendimiento de su red.

Componentes de Hardware

La seguridad de software busca optimizar los componentes de hardware del sistema de información (equipos de cómputo, periféricos, medios de almacenamiento removibles, etc.), de manera que sean configurados de manera segura y solo permitan su utilización dentro de parámetros de funcionamiento predefinidos

y aceptados (aseguramiento), que funcionen de manera continua y estable (disponibilidad), que ofrezcan un servicio con un nivel de calidad aceptable (calidad del servicio), que no permitan su utilización por personas no autorizadas (control de acceso), y que permitan establecer las responsabilidad de uso (accountability).

Componente Humano

La seguridad humana busca optimizar el componente humano del sistema de información (usuarios, administradores, auditores, etc.) para que la interacción entre ellos y con terceros sea segura, no filtre información que pueda permitir la vulneración del sistema de información, y permita detectar ataques de ingeniería social en su contra.

Componentes de Interconectividad

La seguridad del componente de interconectividad busca optimizar el componente de comunicaciones del sistema de información (cableado, dispositivos de interconexión –hubs, switches, routers, etc.-, antenas, etc.), de manera que los canales funcionen de manera continua y estable (disponibilidad) se pueda establecer la

identidad de los participantes (autenticación), los datos transmitidos puedan ser accesados únicamente por personas autorizadas (confidencialidad), los datos no puedan ser modificados durante su transmisión (integridad) y se pueda establecer el origen de toda comunicación (no repudio).

Figura 1.6 Repetidores de Red (Switches).

Figura 1.7 Enrutadores de Red (Routers).

Infraestructura Física

La seguridad de la infraestructura física busca optimizar el entorno físico (las instalaciones) en las cuales opera el sistema de información, de manera que estas provean niveles de seguridad industrial adecuados para proteger los componentes del sistema de información que contiene.

1.4.2 Asesoramiento respecto a vulnerabilidades

Siempre que haya prudencia, existirán diferencias legítimas en el apetito de riesgo de las diferentes personas que toman las decisiones: no se puede considerar la combinación de una amenaza y una vulnerabilidad como un factor de riesgo de forma absoluta. El riesgo depende del contexto empresarial y de la disposición para aceptar los riesgos. Puesto que se trabaja con recursos empresariales, el hablar sobre este principio con las personas que toman las decisiones les permite saber que se comprende y respeta la autoridad que tienen para tomar decisiones básicas de riesgo, incluyendo aquellas decisiones relacionadas con la seguridad de la información.

Como lo ha señalado el Instituto de Gobernabilidad de TI (IT Governance Institute) en relación con el marco de referencia de COBIT(Control OBjectives for Information and related Technology | Objetivos de Control para tecnología de la información y relacionada), al final, la administración debe decidir el nivel de riesgo que está dispuesta a aceptar. Determinar el nivel que se puede aceptar, particularmente cuando se compara con el costo, puede ser una decisión administrativa difícil. Por consiguiente, la administración necesita claramente un marco de referencia para las prácticas de control y de seguridad de TI generalmente aceptadas con el fin de establecer el entorno de TI existente y planificado. Este marco de regencia es también conocido como POLITICA DE SEGURIDAD y es el cimiento más importante para la seguridad de la red.

1.4.3 Solución

La teoría nos indica que una red de comunicación aparte de garantizar la correcta emisión, transmisión y recepción de datos, también debe ser confidencial y absolutamente segura. Pero el cumplimiento absoluto de estas premisas en la practica es inviable

ya que la única manera en que un dispositivo de red este a salvo seria el aislamiento, de esta manera se puede garantizar que no se afecte a causa de la interoperabilidad con los otros elementos pero su integridad, debido a por ejemplo daño por uso inapropiado, aun seguiría en riesgo.

Como vemos la interconexión implica un riesgo tácito que corremos y que debemos estar dispuestos a aceptar para compensar con los beneficios de red. Ante esta posibilidad de riesgo tenemos alternativas de protección; Cuando decidimos implementar alguna de estas opciones de seguridad entonces hemos decidido implementar una red segura.

La seguridad de en una empresa es un pilar fundamental en la estructuración y la arquitectura de su intranet y se compone de varios puntos de iniciativa, entre los más importantes:

- ✓ Tomar y respaldar la decisión de invertir en seguridades de red y prevención de daños.
- ✓ Instalar y administrar seguridades a nivel de Software.

- ✓ Capacitar a todos los usuarios que tengan acceso a la red interna de la empresa.
- ✓ Establecer, explicar y actualizar constantemente políticas de seguridad. adecuadas a las necesidades de la compañía y sus actividades inherentes.

La administración de la seguridad informática consiste en una serie de procesos que tienen como propósito mantener un nivel adecuado de seguridad informática en el sistema de información a lo largo del tiempo. Los procesos no se limitan al mantenimiento y la optimización de la seguridad informática en el presente, sino que incluyen también procesos de planeación estratégica de seguridad informática, que garanticen que el nivel de seguridad se mantendrá en el futuro, y que le permitan al sistema de seguridad informática anticiparse a los requerimientos de seguridad impuestos por el entorno, o por la organización a la cual el sistema de información sirve.

El trabajo del administrador de los recursos informáticos de uso interno habrá alcanzado su nivel optimo una vez que hay sido

capaz de instruir a directivos y empleados de la compañía que la seguridad y prevención de ataques y siniestros a la red es una inversión altamente rentable y que el uso debido de las políticas es provechoso para todos.

Tool	Platforms	Type
COPS/Tiger	Linux, Solaris, Other Unix	Change/Intrusion Detection
Crack	Windows, Linux, Solaris, Other Unix	Password cracking
L0phtCrack	Windows NT	Password cracking
ISS	Windows NT, Linux, Solaris, HP-UX	Suite - Port scanner, network information
nmap	Linux, Solaris, Other Unix	Port Scanner
tcpdump	Linux, Solaris, Other Unix	Network Monitoring
sniffit	Linux, Solaris, Other Unix	Network Monitoring
CyberCop Security Scanner	Windows NT, Linux	Suite - Port Scanner, Password cracking, network information
Nessus	Linux, Windows NT, Other Unix	Exploit tester
TripWire	Unix	Change/Intrusion Detection

Figura 8 Herramientas, Plataformas y Tipos de Soluciones.

Esto nos lleva a la siguiente conclusión: las instituciones financieras deben realizar una evaluación total de riesgos de sus sistemas de información y redes actuales. De hecho, estas

evaluaciones deben programarse con frecuencia. O de acuerdo a los principios: “no se puede proteger lo que no se puede administrar, y no se puede administrar lo que no se puede medir”. En términos que son muy relevantes para el clima actual de reglamentaciones, se deben conocer los controles que se tienen y si funcionan adecuadamente. No se puede saber si lo que se administra cumple con las reglamentaciones a menos que se mida o controle. Esto nos conduce a otro principio relacionado: “ningún control es perfecto”. En otras palabras, el riesgo no se puede reducir a cero. El riesgo se puede aceptar, transferir o mitigar. Ningún control es una bala mágica. Cómo podemos ver, algunos de los principios básicos que he mencionado acercan el tema de la seguridad a la realidad, lo cual ha sido altamente favorable para los recursos empresariales con los que he trabajado durante años.

Si bien cada solución es individual según los requerimientos de cada empresa se puede mencionar varios tips:

- ✓ Capacite y demande del personal con privilegios de acceso de red que elijan claves de seguridad con combinaciones adecuadas (variación de mezclas entre

mayúsculas, minúsculas, símbolos, signos, números, etc.…) que le permitan alcanzar un grado de dificultad alto.

- ✓ Cerciórese que todos y cada uno de los usuarios cambien sus claves una frecuencia mínima de 1 vez cada 90 días.
- ✓ No permita que las subscripciones de software de seguridad tales como firewalls y antivirus caduquen.
- ✓ Capacite a todos los usuarios acerca de lo que implica de la seguridad informática y de los riesgos sobre e-mails y archivos adjuntados.
- ✓ Desarrolle e implemente políticas de seguridades fáciles y efectivas que sea aplicada por la totalidad del personal.
- ✓ Evalúe constante y permanentemente la política de seguridad de acuerdo a la evolución de las amenazas.
- ✓ Si un empleado sale de la compañía remueva inmediatamente su acceso y todos sus privilegios de red.
- ✓ Si permite que algún usuario trabaje desde casa utilice un seguro, servidor centralizado para el tráfico remoto.

- ✓ Actualice periódicamente el software de sus servidores.
- ✓ No ejecute aplicaciones ni servicios de red innecesarios.

1.4.4 Identificación de Riesgos

Las amenazas de seguridad para nuestra red provienen indistintamente de fuentes internas como externas y tanto las prevenciones como las defensas deben considerarse para ambas posibilidades indistintamente. Pero para poder aplicarse efectivamente dichas seguridades deben delimitar claramente el alcance de nuestra intranet para poder en lo posterior administrar los recursos y aplicaciones seguras.

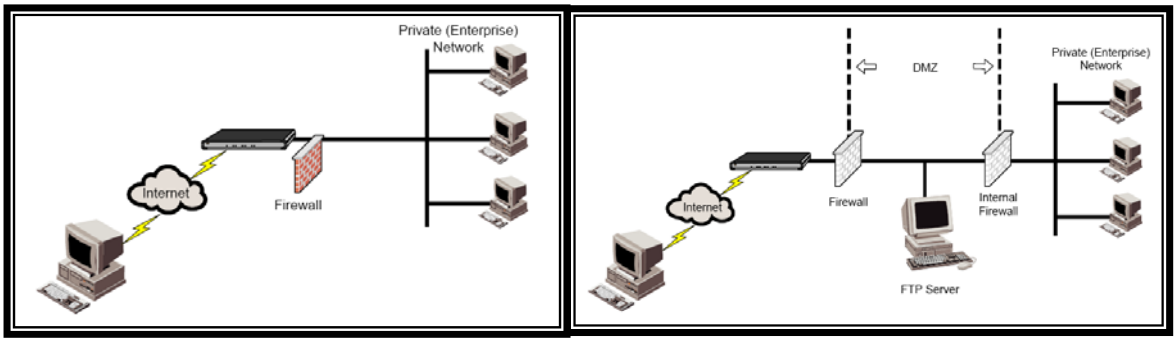


Figura 1.9 Topologías de Redes con Firewall.

Pero existe el peligroso y desgraciadamente reiterativo caso de una combinación altamente eficaz de ambas ya que una de ellas conlleva a la otra. A saber, una aplicación interna aunque

inintencionadamente puede dar paso a un ataque camuflado bajo un interfaz aparentemente inofensivo. El ejemplo más común son los virus que se infiltran en la red valiéndose de la correspondencia privada de uno de los integrantes de la empresa. Dada estas implicaciones inevitables tanto administradores como empleados con beneficios de recursos informáticos deben conocer y entender las aplicaciones que ellos habitualmente desarrollan y el riesgo que estas implican.

AMENAZA	INTERNA/EXTERNA	CONSECUENCIAS
E-mail con Virus	Origen externo/Aplicación Interna.	Al leer el mail puede infectar la red para luego esparcirse en toda la red.
Red con Virus	Externo	Puede infectar a través de puertos desprotegidos comprometiendo la red completa.
Infección vía Web	Interna navegando por un servidor	Se puede comprometer el sistema mediante la navegación y luego comprometer el resto de

		dispositivos.
Ataque a Servidor Web	Externo	Si el servidor Web es atacado el hacker puede obtener acceso a diferentes elementos de la red.
Ataque Denial Of Service Denegación de Servicios	Externo	Servicios externos como navegación, e-mail y ftp pueden quedar inútiles. Si se ataca un router la red puede descalabrase.
Ataque de Usuario a Red	Interno	Puede afectar indistintamente cualquier miembro de la red interna como externa. Inmunes a firewalls periféricos. Firewalls de segmentación pueden aislar el ataque.

Tabla II: Fuentes de amenazas para la red.

Entre las causas comunes de la inseguridad de los sistemas se encuentran: los defectos potenciales de seguridad en la instalación

del producto de software, en la configuración de los servicios de red, “huecos” típicos en las utilerías del sistema operativo y demás software base o de red, así como en la implantación de decisiones tácticas ignorantes de las condiciones mínimas de seguridad para los sistemas. Otros métodos que han resultado efectivos para un atacante son: la ingeniería social y el rompimiento de password.

Un claro ejemplo de Ingeniería Social más común es el de alguien que llama por teléfono a una empresa para decir que necesita ayuda o hablar con el administrador de la red porque hay que modificar algún aspecto de la configuración. Durante la conversación, y a través de escogidas y cuidadas preguntas, el atacante obtendrá los datos (como los códigos de acceso a los equipos) que necesita para vulnerar la seguridad de todo el corporativo, por ende hay que especificarle a cada usuario de la red, nunca emitir códigos o contraseñas bajo ninguna circunstancia, porque pueden ser usados por un atacante externo.

Errores comunes incluso han sido advertidos por los propios hackers y dan ciertas recomendaciones de qué no se debe hacer,

para evitar intrusos en nuestra red, y si éstos llegasen a entrar, no dejarles a la mano información valiosa:

- ✓ No tirar a la basura información importante que alguien pueda hallar, buscando en los contenedores.
- ✓ No publicar en Internet directorios telefónicos internos.
- ✓ Usar siempre un programa antivirus, otro que detecte los programas espía y un cortafuego que controle tanto el tráfico que entra como el que sale del computador.
- ✓ Es de vital importancia tener siempre los programas actualizados y aplicar con celeridad los parches de seguridad que vayan apareciendo.

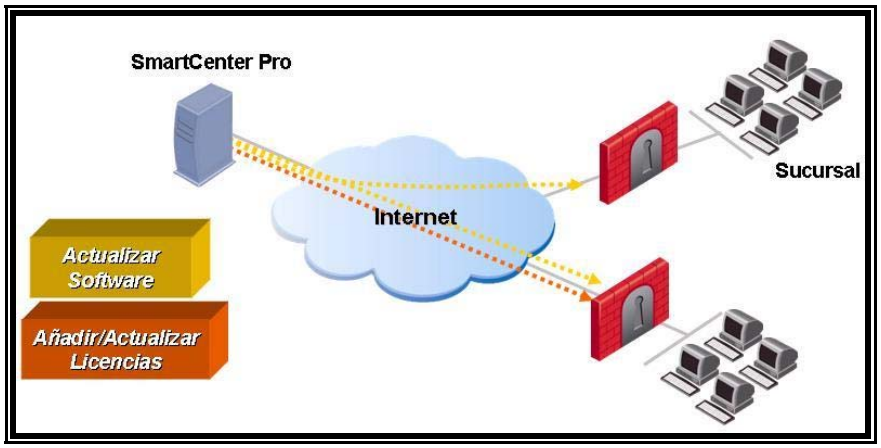


Figura 1.10 Una Red con Cierto Nivel de Seguridad.

Es recomendable no utilizar el navegador Internet Explorer, es mejor y más seguro el Firefox, y en caso de utilizar Internet Explorer, se debe desactivar los controles ActiveX, excepto cuando se visiten sitios confiables. Además, habiliten el servicio DEP (Data Execution Prevention), una prevención que Windows lleva de fábrica para evitar la ejecución de datos en su ordenador.

1.5 Modelos de Seguridad

Después de implementar la seguridad en los componentes físicos de la red, el administrador necesita garantizar la seguridad en los recursos de la red, evitando accesos no autorizados y daños accidentales o deliberados. Las políticas para la asignación de permisos y derechos a los recursos de la red constituyen el paso primordial de la seguridad de la red.

1.5.1 Objetivos

En un entorno de red debe asegurarse la privacidad de los datos sensibles. No sólo es importante asegurar la información sensible, sino también, proteger las operaciones de la red de daños no intencionados o deliberados. El mantenimiento de la seguridad de

la red requiere un equilibrio entre facilitar un acceso fácil a los datos por parte de los usuarios autorizados y restringir el acceso a los datos por parte de los no autorizados. Es responsabilidad del administrador crear este equilibrio.

Incluso en redes que controlan datos sensibles y financieros, la seguridad a veces se considera medida tardía. Las cuatro amenazas principales que afectan a la seguridad de los datos en una red son:

- ✓ Acceso no autorizado.
- ✓ Soborno electrónico
- ✓ Robo.
- ✓ Daño intencionado o no intencionado.

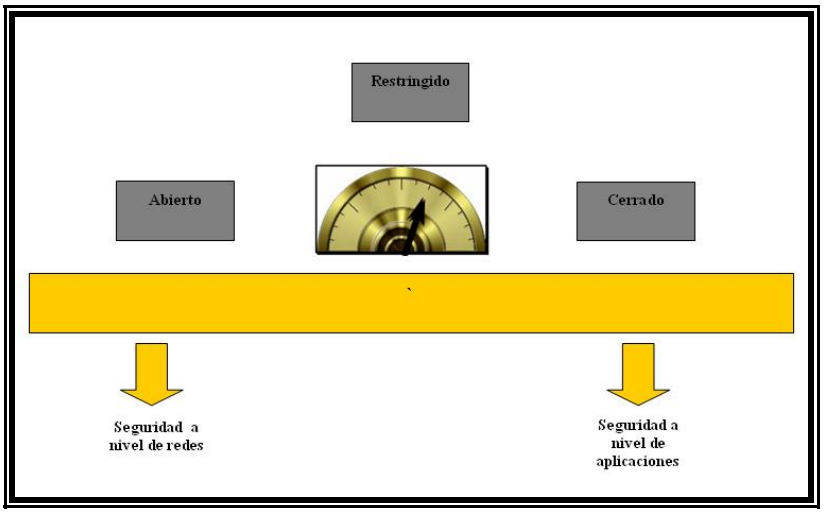


Figura 1.11 Clasificación de Políticas de Seguridad y niveles de aplicación.

La seguridad de los datos no siempre se implementa de forma apropiada, precisamente por la seriedad de estas amenazas. La tarea del administrador es asegurar que la red se mantenga fiable y segura. En definitiva, libre de estas amenazas.

1.5.2 Modelos

Se han desarrollado dos modelos de seguridad para garantizar la seguridad de los datos y recursos hardware:

- ✓ Compartición protegida por contraseña o seguridad a nivel de compartición.
- ✓ La implementación de un esquema para compartir recursos protegidos por contraseñas requiere la asignación de una contraseña a cada recurso compartido. Se garantiza el acceso a un recurso compartido cuando el usuario introduce la contraseña correcta.
- ✓ En muchos sistemas, se pueden compartir los recursos con diferentes tipos de permisos. Para ilustrar esto, utilizamos Windows 95 y 98 como ejemplos. Para estos sistemas

operativos se pueden compartir los directorios como sólo lectura, total o depende de la contraseña.

- ✓ Sólo lectura. Si un recurso compartido se configura de sólo lectura, los usuarios que conocen la contraseña tienen acceso de lectura a los archivos de este directorio. Pueden visualizar los documentos, copiar a sus máquinas e imprimirlos, pero no pueden modificar los documentos originales.
- ✓ Total. Con el acceso total, los usuarios que conocen la contraseña tienen acceso completo a los archivos de este directorio. En otras palabras, pueden visualizar, modificar, añadir y borrar los archivos del directorio compartido. Depende de la contraseña. Depende de la contraseña implica configurar una comparticion que utiliza dos niveles de contraseñas: Contraseña de sólo lectura y Contraseña de acceso total. Los usuarios que conocen la contraseña de sólo lectura tienen acceso de lectura y los usuarios que conocen la contraseña de acceso total tienen acceso completo.

- ✓ El esquema de compartir utilizando contraseña es un método de seguridad sencillo que permite a alguien que debidamente autorizado obtener el acceso a un recurso determinado.

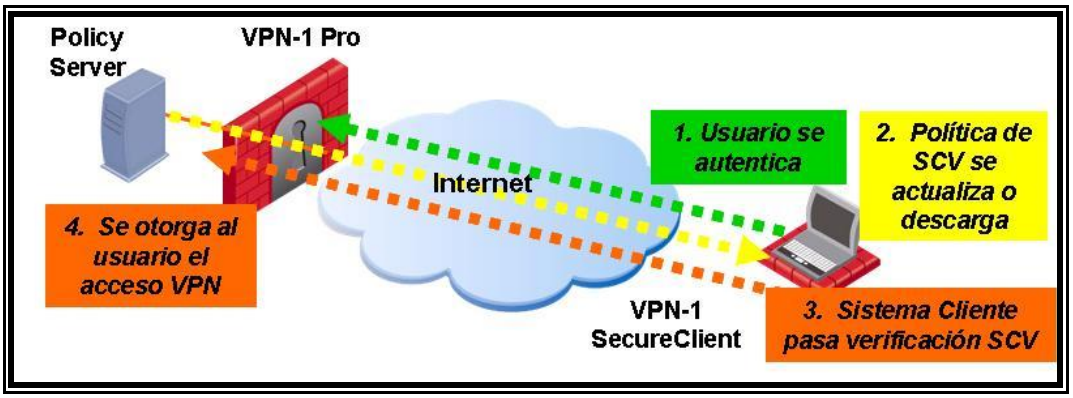


Figura 1.12 Control de accesos mediante autentificación de usuarios.

Permisos de acceso o seguridad a nivel de usuario.

La seguridad basada en los permisos de acceso implica la asignación de ciertos derechos usuario por usuario. Un usuario escribe una contraseña cuando entra en la red. El servidor valida esta combinación de contraseña y nombre de usuario y la utiliza para asignar o denegar el acceso a los recursos compartidos, comprobando el acceso al recurso en una base de datos de accesos de usuarios en el servidor.

La seguridad de los permisos de acceso proporciona un alto nivel de control sobre los derechos de acceso. Es mucho más sencillo para una persona asignar a otra persona una contraseña para utilizar una impresora, como ocurre en la seguridad a nivel de compartición. Para esta persona es menos adecuado asignar una contraseña personal.

La seguridad a nivel de usuario es el modelo preferido en las grandes organizaciones, puesto que se trata de la seguridad más completa y permite determinar varios niveles de seguridad.

Seguridad de los recursos

Después de autenticar a un usuario y permitir su acceso a la red, el sistema de seguridad proporciona al usuario el acceso a los recursos apropiados.

Los usuarios tienen contraseñas, pero los recursos tienen permisos. En este sentido, cada recurso tiene una barrera de seguridad. La barrera tiene diferentes puertas mediante las cuales los usuarios pueden acceder al recurso. Determinadas puertas

permiten a los usuarios realizar más operaciones sobre los recursos que otras puertas. En otras palabras, ciertas puertas permiten a los usuarios obtener más privilegios sobre el recurso.

El administrador determina qué usuarios tienen acceso a qué puertas. Una puerta asigna al usuario un acceso completo o control total sobre el recurso. Otra puerta asigna al usuario el acceso de sólo lectura.

Algunos de los permisos de acceso habituales asignados a los directorios o archivos compartidos son:

- ✓ Lectura: Leer y copiar los archivos de un directorio compartido.
- ✓ Ejecución: Ejecutar los archivos del directorio.
- ✓ Escritura: Crear nuevos archivos en el directorio.
- ✓ Borrado: Borrar archivos del directorio.
- ✓ Sin acceso: Evita al usuario obtener el acceso a los directorios, archivos o recursos.

Diferentes sistemas operativos asignan distintos nombres a estos permisos.

- ✓ Permisos de grupo
- ✓ El trabajo del administrador incluye la asignación a cada usuario de los permisos apropiados para cada recurso. La forma más eficiente de realizarlo es mediante la utilización de grupos, especialmente en una organización grande con muchos usuarios y recursos. Windows NT Server permite a los usuarios seleccionar el archivo o carpeta sobre la que se establecen los permisos de grupo.
- ✓ Los permisos para los grupos funcionan de la misma forma que los permisos individuales. El administrador revisa los permisos que se requieren para cada cuenta y asigna las cuentas a los grupos apropiados. Éste es el método preferido de asignación de permisos, antes que asignar los permisos de cada cuenta de forma individual.
- ✓ La asignación de usuarios a los grupos apropiados es más conveniente que asignar permisos, de forma separada, a cada usuario individualmente. Por ejemplo,

puede que no sea conveniente la asignación al grupo *Todos* del control total sobre el directorio público. El acceso total permitiría a cualquiera borrar y modificar los contenidos de los archivos del directorio público.

- ✓ El administrador podría crear un grupo denominado *Revisores,* asignar a este grupo permisos de control total sobre los archivos de los estudiantes e incorporar empleados al grupo *Revisores.* Otro grupo, denominado *Facultad,* tendría sólo permisos de lectura sobre los archivos de los estudiantes. Los miembros de la facultad asignados al grupo *Facultad,* podrían leer los archivos de los estudiantes, pero no modificarlos.

1.6 Potenciales Riesgos y Consecuencias

Muchas compañías no establecen seguridades o políticas que normen el uso adecuado de los recursos informáticos no solo por negligencia o falta de voluntad. Hay que reconocer los factores reales que inciden en la toma y ejecución de una decisión como esta. Habitualmente los inconvenientes que van en contra de las seguridades a nivel de software tienen relación directa con los

costos. Costos que difícilmente una compañía poco familiarizada con el uso de redes de comunicación [internas (INTRANET), la interconexión de la misma con redes de cobertura geográfica y de bondades de recursos mucho mayor (INTERNET) y la utilidad que ambas intercomunicaciones representan para los intereses de la compañía] están dispuestas a asumir pero el castigo a esta exposición genera resultados de corto o mediano plazo en desmedro de sus propias economías puesto que una red expuesta genera muchos mas costos que la prevención. Estos costos no son solo tangibles en el aspecto monetario otros costos deben ser considerados como el tiempo y eficiencia que pueden afectar el rendimiento de la compañía.

A parte de la inversión económica otro punto que se debe asumir es que una red segura puede ser muy compleja de administrar o de comprender por parte de administradores o de los usuarios finales, al menos hasta que la totalidad de los integrantes de la empresa asuma la seguridad como parte de las actividades productivas que generan un beneficio cuantificable para la

compañía y entonces apliquen conscientemente las normas, este lapso de adaptación también implica un “costo”.

CAPÍTULO 2

1.5 DESCRIPCION DE VULNERABILIDADES, RIESGOS Y ATAQUES

La evolución de las tecnologías de comunicación y su rápida penetración en nuestra vida diaria, ha provocado que los equipos conectados a redes públicas se encuentren expuestos ante la mirada de usuarios maliciosos.

Los problemas en el software se van exponiendo cada vez mas en el tema de seguridad, ya que los intrusos utilizan técnicas y sofisticados métodos para tomar ventaja de las fragilidades o problemas que puedan presentar y para este efecto utilizan la generación de códigos maliciosos que propagan en todo Internet.

Es necesario entonces que administradores y usuarios de red implementen las actualizaciones de seguridad más recientes a los sistemas operativos y todo el tipo de software a fin con el propósito de solucionar vulnerabilidades

que pueden ser explotadas por intrusos, internos o externos, y que pongan en riesgo la seguridad de la información de la organización.

Administraciones conservadoras o tradicionales, tanto en la mediana como la gran empresa, menospreciando la evaluación y control del flujo de datos informáticos por medio de su red, falta de previsión en materia de seguridad o enfoques tradicionales restringidos a la tecnología y/o a la seguridad estrictamente perimetral puede dar lugar a incidentes de seguridad o cotización total del sistema de trafico de datos.

Los problemas de seguridad pueden dar como resultado menores ingresos, mayores gastos y sanciones adicionales como también erosionar la confiabilidad de la información obtenida y el control informático con el tiempo. Las herramientas de supervisión de la red para identificar los puntos o vulnerabilidades técnicas ayudan a identificar los potenciales problemas o fuentes de ataque. Sin embargo, las personas y los procesos pueden comprometer los controles técnicos por medio de un uso indebido accidental o intencionado, poniendo en riesgo la información y hasta las redes mismas.

Cuando se intenta asegurar un vehiculo, una casa, una nación o una red informática siempre será indispensable saber quienes pueden ser los enemigos potenciales y cuales son las posibles debilidades.

Aunque la gran mayoría de usuarios de Internet tiene fines loables existe un pequeño grupo de ellos que tienen aspiraciones dirigidas a causar algún tipo de daño aunque sea de un bajo nivel destructivo.

Los daños pueden destruir el sistema operativo de las pc's, alterar datos, robar información, saturar servidores de Web o email, etc. Si la red no esta conectada al Internet u otra red aún puede estar expuesta debido al uso de dispositivos como CDs, USB drives o por el simple uso de personal con beneficios de accesos informáticos.

Para puntualizar algunos tipos de ataques podemos enumerar 4 aunque en el desarrollo de este capitulo se detallaran y profundizara en el resto de ellos, así:

1. Malware (software malicioso)._ Software desarrollado para causar daños o interrupciones.
2. Hackers._ Usuarios de Internet con intención de penetrar con fines nocivos a la intranet.
3. Saturación de Red._ Demasiado trafico sobre la red por exceso de accesos al Web Server o por medio de explotar con spam al mail Server.
4. Daños Físicos._ Ataques a infraestructura de la red que pudieran dejarla inoperativa comenzando por una simple interrupción de un cable de alimentación hasta llegar a catástrofes naturales.

2.1 Definiciones Básicas

Política de seguridad.

Son las normas establecidas para el correcto desempeño e interacción de elementos de red de modo que puedan funcionar adecuadamente. Las políticas de seguridad fueron concebidas para proteger los dispositivos de todas aquellas posibles amenazas y tratan de diferenciar entre las adecuadas e inadecuadas acciones que puedan realizarse.

Vulnerabilidad.

Punto o aspecto de la red que es susceptible de ser atacado o de dañar la seguridad de la misma. Representan las debilidades o aspectos falibles o atacables en el sistema informático.

Amenaza.

Posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, código malicioso, etc.), un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

Contramedida.

Técnicas de protección del sistema contra las amenazas en respuesta a las amenazas o los ataques mismos.

La seguridad informática se encarga de la identificación de las vulnerabilidades del sistema y del establecimiento de contramedidas que eviten que las distintas amenazas posibles exploten dichas vulnerabilidades. Una máxima de la seguridad informática es que: "No existe ningún sistema completamente seguro". Existen sistemas de mayor o de menor seguridad, y con mayor o menos vulnerabilidad, pero la seguridad nunca es absoluta.

Firewall.

Es un mecanismo por medio del cual se puede llevar en control del tráfico entrante y saliente de una red organizacional, conocidas también como intranet. Generalmente es router de aplicaciones específicas aunque puede ser solo un software ejecutable.

2.2 Tipos de Vulnerabilidades

Realmente la seguridad es la facultad de estar a cubierto de algún riesgo o amenaza. Desde este punto de vista la seguridad total es muy difícil de lograr, puesto que implicaría describir todos los riesgos y amenazas a que puede verse sometido el sistema. La característica que se manifiesta en los sistemas no es la seguridad, sino más bien la inseguridad o vulnerabilidad. No es posible hablar de una red totalmente segura, sino más bien de una en el que no se conocen tipos de ataques que puedan vulnerarlo debido a que se han establecido medidas para evitarlo. Existen varios tipos de

vulnerabilidades como son: Tecnológicas, De Configuración y de Políticas de Seguridad

2.5.2 Tecnológicas

La demanda de la tecnología a aumentado a niveles no previstos, llevando incluso a crear no solo una necesidad, sino una dependencia de la sociedad hacia diversos productos tecnológicos. Para satisfacer dicha demanda es debido mantener una producción acelerada y además renovar cada vez mas pronto las diversas alternativas del mercado. Pero como no se puede desconocer que la tecnología no es mas que el producto de la perspicacia y del talento humano y por ende factible a heredar de sus creadores imperfecciones de desarrollo, se presentan entonces cabos sueltos que al ser descubiertos desencadenan una serie de vulnerabilidades plausibles de explotar. Las vulnerabilidades tecnológicas se refieren a todas aquellas fallas de desarrollo en las diversas soluciones tecnológicas que componen una red de transmisión de datos informáticos y que son consecuencia de errores del fabricante pero que exponen todo el sistema informático del que forman parte. Dichas vulnerabilidades proporcionan backdoors o entradas subrepticias permitiendo causar daño sin que los administradores puedan reaccionar sino hasta que se sientan los estragos.

> Los fabricantes de software habitualmente invierten muchos recursos con el fin de que su producto revolucione el mercado a su lanzamiento e implementan innovadoras virtudes y aplicaciones que en su criterio lo convertirán en líder de su medio. Este fabricante lanza entonces, un producto funcional que presenta con nuevas soluciones, pero que en el apremio del lanzamiento, muchas veces no son probados adecuadamente en todas y cada una de sus prestaciones. Sin ser adecuadamente probadas estas nuevas soluciones pueden convertirse en falencias generalizadas bien aprovechadas por hackers.

Dichas falencias pueden ser tan solo un inconveniente que merme el desempeño de un programa o pueden ser todo un dolor de cabeza en el caso de un sistema operativo. Se puede visualizar este tipo de fallas como soluciones de software con porciones de su código incompleto o faltante que no permiten el correcto desempeño de su totalidad de funciones en su óptimo nivel de desenvolvimiento.

Una vez en el mercado los innumerables usuarios, particularmente, comienzan a utilizar y exigir de sus diferentes funcionabilidades el máximo rendimiento o por lo menos un rendimiento aceptable; es entonces cuando empiezan también a exponerse los problemas de su desarrollo. Pero dejando expuestos los usuarios el tiempo que tarden en darse las primeras soluciones. Estos desarrollos incompletos poco a poco

van afectando la reputación de los fabricantes y se ven reflejadas en la credibilidad y receptibilidad que esta compañía tiene en el lanzamiento de sus productos. Los problemas de desarrollo tienen la mayoría de sus correcciones durante sus primeros meses de funcionamiento pero también es posible que anos después se sigan corrigiendo sus fallas.

Afortunadamente un problemas es tan solo la necesidad de una solución y las soluciones a las falencias de desarrollo son complementar sus códigos incompletos que le permiten desarrollar a cabalidad sus función o cubrir los hoyos por los cuales se infiltraban las inseguridades. El medio informático a generalizado estos complementos con el termino “Parches” aunque Microsoft los denomina “Service Pack”. Los parches son una modificación llevada a cabo en un programa informático para sustituir una parte del código y con el fin de eliminar un error en su programación original, le aporta nuevas mejoras, actualiza al programa una versión mas moderna o evita que los hackers puedan realizar acciones malintencionadas dentro de un equipo.

La mayor o menor cantidad de estas fallas marca en gran medida la diferencia entre un producto y su competencia determinando las preferencias del mercado.

Como un ejemplo común se puede tomar la inagotable controversia entre Windows y Linux en el cual claramente se puede comprobar la competencia por estabilidad y seguridad. Mucha controversia se ha dado entre estas populares plataformas para determinar la mas estable, pero como los criterios suelen ser subjetivos, se evaluaran datos técnicos (entre los mas importantes las fallas de desarrollo que presentar) para ayudar al lector a obtener una conclusión. Para poder efectuar la comparación será necesario mencionar algunas creencias generalizadas con respectos a este tema.

“Los parches son menos necesarios y con mejor respuesta ante vulnerabilidades en Windows que en Linux.” Esta conclusión es definitivamente inaplicable no solo contra Linux sino contra cualquier otro sistema operativo competencia de Microsoft. Existe el reporte de eEye Digital Security publicado en el aviso AD20040210 que denuncia en el que Microsoft se tardo 7 meses para solucionar una de sus más críticas vulnerabilidades de seguridad (Microsoft Security Bulletin MS04-007 ASN.1 Vulnerability). Además un agravante es que existe una manifestación oficial y expresa de Microsoft que para algunas vulnerabilidades existentes de sus productos; El Microsoft Security Bulletin MS03-010 acerca de la vulnerabilidad de Denial Of Service en Windows NT expresamente manifiesta que dicha vulnerabilidad nunca será resarcida. Además recientemente Microsoft comunicó que las

vulnerabilidades del programa Internet Explorer no serán reparadas para versiones que funcionen en sistemas operativos anteriores a WinXP. Para Octubre del 2004 la comparación realizada entre Windows Server 2003 vs. Red Hat Enterprise Linux AS v.3 sobre los 40 últimos parches/vulnerabilidades evaluados en 2 criterios:

1. La severidad de las vulnerabilidades considerando:
    - ✓ Potencial de danos (cuanto daño puede recibir).
    - ✓ Potencial de explotación (que tan fácil es explotar esos danos).
    - ✓ Potencial de exposición (que tipo de acceso es necesario para explotar las vulnerabilidades)
2. El numero de vulnerabilidades críticas.

    Los resultados fueron los siguientes:
    - ✓ El 39 de 40 parches fueron catalogados como críticos para Microsoft.
    - ✓ Solo el 3 de los 40 de los parches Red Hat alcanzaron el nivel crítico.

    “Windows reporta mas ataques por ser el más popular y si Linux fuese más instalado fuese más o igual de vulnerable.”

La percepción de que Windows es la plataforma más utilizada, que por ser la más popular no puede ser tan insegura y que simplemente Linux es demasiado insignificante como para ser blanco de los ataques es cierta

pero solo parcialmente. En efecto Windows es la plataforma mas utilizada pero solo en elementos que tienen contacto directo con el usuario final de la totalidad de una red de transmisión de datos, por ejemplo los Hosts. Pero su popularidad no reside necesariamente en las bondades de su seguridad, su robustez o fiabilidad sino por factores ajenos como convenios de exclusividad con los fabricantes de hardware y otras estrategias de mercado.

Si las prioridades de ataque para los crackers están dadas en base a la importancia del papel que cumplen los elementos de red y al sistema operativo más común entre ellos entonces Apache o BSD son a claras luces un objetivo altamente atractivo. Si es que en efecto el problema fuese un problema de número y no de vulnerabilidad la mayoría de software malicioso apuntara hacia BSD o Apache y todos los programas que se ejecutan bajo ellos, también un mayor numero de ataques exitosos reportados; la realidad es que la el software malintencionado sigue siendo dirigido hacia Windows, la mayor cantidad de reportes y de parches de solución críticos son también diariamente lanzados para Windows.

Históricamente Microsoft IIS ha sido el blanco primario para gusanos, troyanos y similares con gran índice de éxito. El gusano Código Rojo se filtro y apodero de un servidor Web y logro esparcirse a otros 300.000 servidores, el número de infecciones solo se detuvo porque el gusano fue

concebido deliberadamente para detener su esparcimiento. Su variante Código Rojo. A obtuvo un mayor índice de efectividad aunque también se detuvo luego de 3 semanas. Otro ejemplo es el IISWorm que tuvo un impacto no tan alto debido a que fue mal desarrollado más no porque ISS tuvo una defensa exitosa.

Pero obviamente Linux también ha logrado ser vulnerado y un ejemplo es el SlapperWorm (pero en la actualidad solo logra explotar una conocida vulnerabilidad en sistemas OpenSSL, ya no en Apache). Pero los ataques a Linux rara vez son noticias debido al limitado rango de daño que pueden causar además de la facilidad de su erradicación. Limpiar y restaurar un sistema infectado es mas bien una labor sencilla de realizar utilizando pocos comandos e incluso sin siquiera necesitar un reinicio gracias a los módulos naturales de Linux o de Unix. Por esto surge la duda sobre si los crackers son tan eficientes atacando a Microsoft IIS por que no pueden causar danos similares en el resto de sistemas operativos.

Según las estadísticas de Netcraft la mayoría de los servidores del TOP 50 uptime (tiempo durante el cual no necesitan reinicio y con el record de 1768 días o casi 5 años) utilizan alguna variedad de BSD. Pero en defensa de las soluciones Linux vale destacar que sus contadores se reinician cada 497 días haciendo imposible una acumulación mayor a esta cifra aunque su estabilidad haya sido mucho más larga.

2.5.2 De Configuración

Las vulnerabilidades de configuración corresponden a todos aquellos errores u omisiones cometidos durante el proceso de instalación y configuración tanto de la red y las aplicaciones que van a desarrollarse en ella así también como de sus actualizaciones o migraciones a nuevos sistemas informáticos.

Desafortunadamente no es posible erradicar estas vulnerabilidades debido a que al depender del factor humano están sujetas a heredar sus imperfecciones. Considerando el gran número de razones que pueden influir sobre el nivel de concentración y las habilidades del hombre se incrementa entonces, el universo que inyecta incertidumbre en el proceso. Además cada instalación difiere de otra ya que la solución se personaliza dependiendo de cada compañía, de las actividades a las que se dedique y de los recursos con que cuente. Para puntualizar solo algunos ejemplos se puede mencionar:

Utilizar en el proceso de instalación personal que no se encuentra debidamente capacitado para dichas labores. Es cierto que esta mano de obra quizás puede abaratar los costos inicialmente pero también es muy probable que a corto o mediano plazo las consecuencias seas muy costosas, y no solo en el costo monetario sino en costos incuantificables

como puede ser el tiempo de reactivación y operación o por el valor de la información q pueda verse afectada.

Instalar sistemas operativos, programas, aplicaciones, etc. En su estado de default también suele ser error común ya que si no se toma la precaución de personalizar o reforzar la seguridad se queda expuesto a las mismas vulnerabilidades de configuraciones generales ya conocidas por los intrusos.

Inhabilitar aplicaciones de alto riesgo o de fácil penetración es parte crucial de la configuración de una red de transmisión de datos ya que son blancos mas buscados por los potenciales atacantes.

No establecer prioridades en cuanto al uso y acceso de los elementos de la red a sus respectivos privilegios genera mala comunicación y daños que perjudican la productividad de la empresa.

Estos son ejemplos que no son extraños en la mayoría de sistemas informáticos y que aunque aislados unos de otros parecieran tolerables una vez acumulados generan una gran brecha por la cual queda a la intemperie tanto equipos como información.

2.5.2 De Políticas de Seguridad

El hecho de existir políticas de seguridad implica el seguirlas de forma irrestricta; debido a que es posible implementarlas de una manera eficiente, pero sin aplicarlas para lo que fueron ideadas seria mejor que no existiesen.

Dentro de una empresa en la cual existan una gran cantidad de usuarios de la red, es indispensable el darle a todos y cada uno de estos las diferentes políticas que se aplican en cada caso, ya que estas se dan con ciertas jerarquizaciones y cada quien debe saber que parámetros debe respetar y seguir; la documentación de las políticas no puede estar inconclusa, mal redactada, o menos aun nunca haber sido escritas, ya que en esto se puede amparar cualquier usuario para justificar algún incidente que este ocasione a nivel de la red. Si se vulneran estas políticas la red esta expuesta a ataques tanto internos como externos, y aunque bien es cierto esto suele suceder muchas veces por desconocimiento de un usuario, el hecho de que ocurran da la pauta para estar siempre alerta, y preparado para cualquier tipo de contingencia que se puede suscitar; porque da a entender que tambien puede ser susceptible a maliciosos ataques de algún extraño a la red, por ende los controles deben ser aplicados de forma constante y completa en todos y cada uno de los usuarios de la red sin excepción, ya que esta es la unica forma de estar seguro de que las políticas son respetadas a cabalidad.

La seguridad es el bien intangible mas importante que cualquier empresa puede poseer, al referirnos a seguridad estamos hablando de todo aquello que ataña información, conexiones, transacciones, etc, y todos y cada uno de estos ítems deben estar imprescindiblemente seguros, esto se logra respetando de forma inexorable las políticas de seguridad establecidas por quien administra la red; asi mismo estas políticas deben ser constantemente revisadas para abarcar todos los ataques a los que la red se puede ver expuesta, ya que en el mundo informático los cambios se dan de forma diaria, dado este hecho las políticas deben ser flexibles para cualquier variación que se pueda dar a ultimo momento, el hecho de ser flexible no implica el que puedan ser irrespetadas, sino la posibilidad de tener la red en funcion de las necesidades de la empresa y de quienes accedan a ella, razon por la cual ahora las empresas están dejando de utilizar software sin licencia, ya que para actualizaciones posteriores se necesitan estas, esto en caso de usar software no abierto, porque obviamente si es open source no existe problema. Por ejemplo, puede llegar un instante en el cual se sature el ancho de banda de la conexión de la red, y se debe evitar el acceso a correos electrónicos individuales, Messenger, y todo programa que no sea indispensable en el desenvolvimiento de la empresa.

2.3 Tipos de Riesgo

Las amenazas al sistema informático pueden también clasificarse desde varios puntos de vista.

2.5.2 Desestructurados y Estructurados

Analizando con estricto cuidado podemos percatarnos del hecho de cuán peligroso puede ser un tipo de riesgo involuntario así como uno premeditado, a continuación se detallan ambos.

Desestructurados (Involuntarios)

Son riesgos relacionados con el uso descuidado del equipo por falta de entrenamiento o de concienciación sobre la seguridad. Entre las más comunes podemos citar:

- ✓ Borrar sin querer parte de la información
- ✓ Dejar sin protección determinados ficheros básicos del sistema
- ✓ Dejar papeles con información trascendental acerca de la red u olvidar salir del sistema.

Estructurados (Premeditados)

Los riesgos concebidos después de un analisis y desarrollo que resulta en una amenaza específica para infiltrarse en la red y cumplir

su tarea. Pueden borrar, modificar, robar la información, bloquear el sistema o solo por simple diversión del atacante.

Los causantes del daño pueden ser de dos tipos: internos y externos.

Los externos pueden acceder la intranet de múltiples formas:

- ✓ Entrando al edificio o accediendo físicamente al ordenador.
- ✓ Ingresando al sistema explotando las vulnerabilidades software del mismo.
- ✓ Consiguiendo acceso a través de personas que lo tienen de modo autorizado.

Una explicación más extensa de este ítem se da en el punto 2.5.5, en el cual haremos una revisión detallada de cada uno de los riesgos.

2.3.2 Externos e Internos

En busca de una eficiente política de seguridad debemos conocer y entender a fondo las posibles fuentes de ataque para poder establecer una solución adecuada para cada amenaza.

Se debe empezar por aceptar el hecho de que un ataque puede provenir tanto del exterior como del interior del perímetro de la red. En efecto muchas vulnerabilidades son explotadas desde adentro por los empleados que con diario acceso a la intrared poco a poco las descubren. Estos ataques basados o desencadenados por el factor

humano pueden ser un hecho premeditado o involuntario y es más, el término apropiado para referirse a ellos seria amenazas a la integridad o salud de la red en lugar de amenazas de seguridad. De cualquier modo un inconveniente conlleva al otro. Descargar un archivo aparentemente no contaminado tiene un origen externo pero se desencadena desde el interior infectando así la red. Otro ejemplo es el ataque dirigido que puede efectuar un empleado para acceder a información confidencial de la compañía. Según la penetración y el nivel de daño que los riesgos son capaces de causar se pueden clasificar por:

Intercepción

Si una persona, programa o proceso logra penetrar a una parte del sistema a la que no está autorizada. Por Ejemplo:

- ✓ Escucha de una línea de datos.
- ✓ Copias de programas o ficheros de datos no autorizados.

Son los más difíciles de detectar pues en la mayoría de los casos no alteran la información o el sistema.

Modificación

Se trata no sólo de acceder a una parte del sistema a la que no se tiene autorización, sino, además, de cambiar en parte o todo su contenido o modo de funcionamiento. Ejemplos:

- ✓ Cambiar el contenido de una base de datos.

- ✓ Cambiar líneas de código en un programa.
- ✓ Cambiar datos en una transferencia bancaria

Generación

Se refiere a la posibilidad de generar o añadir información o programas no autorizados en la red. Ejemplos:

- ✓ Añadir campos y registros en una base de datos.
- ✓ Añadir código en un programa (virus).
- ✓ Introducir mensajes no autorizados en una línea de datos.

Los internos pueden ser de tres tipos: empleados despedidos o descontentos, empleados coaccionados, y empleados con ambiciones personales.

Como puede observarse, la vulnerabilidad de los sistemas informáticos es muy grande, debido a la variedad de los medios de ataque o amenazas. Fundamentalmente hay tres aspectos que se ven amenazados: el hardware (el sistema), el software (programas de usuarios, aplicaciones, bases de datos, sistemas operativos, etc.), los datos.

Medidas de seguridad contra riesgos

Los sistemas informáticos pueden diseñarse de acuerdo con criterios de economía, de eficiencia y de eficacia, etc., porque son claramente conmensurables y se asocian a parámetros que, maximizando unos y minimizando otros, se puede tender hacia diseños óptimos.

El paso siguiente es identificar los “riesgos potenciales” a cada uno de estos elementos según las indicaciones de la Tabla 1. Riesgos pueden venir de fuentes internas y externas. Pueden ser basadas en humanos, automatizadas o aún sin intención por un fenómeno natural. La última razón se categorizaría más apropiadamente como salud del sistema a las amenazas en comparación con amenazas de la seguridad, pero algún suceso puede conducir a la otra. Un ejemplo es un paro del suministro eléctrico a una alarma antirrobo. La interrupción de la energía podría ser intencional o con un cierto acontecimiento natural tal como un relámpago. En cualquier caso se disminuye la seguridad.

Seguridad física se da con la protección en el interior. La mayoría de los expertos convendrían que toda la seguridad comienza con la seguridad física. Acceso físico que controla a las máquinas y los puntos de fijación de la red son quizás más críticos que cualquier otro aspecto de la

seguridad. Cualquier tipo de acceso físico a un sitio interno crea una exposición importante del sitio. Asegurar los archivos, contraseñas, certificados y todas las clases de otros datos pueden ser obtenidas generalmente si el acceso físico es posible. Hay afortunadamente toda clases de dispositivos del control de acceso y aseguran los gabinetes que pueden ayudar con este problema. Para más información de la seguridad física de los centros de datos se debe tener claro como funcionan los cuartos de la red.

Diseñar sistemas mediante criterios de seguridad es más complejo, pues las amenazas son en muchos casos poco cuantificables y muy variados. La aplicación de medidas para proteger el sistema supone un análisis y cuantificación previa de los riesgos o vulnerabilidades del sistema. La definición de una política de seguridad y su implementación o través de una serie de medidas.

AMENAZA	INTERNA/EXTERNA	CONSECUENCIAS
E-mail con Virus	Origen externo Aplicación Interna.	Al leer el mail puede infectar la red para luego esparcirse en toda la red.
Red con Virus	Externo	Puede infectar a través de puertos desprotegidos comprometiendo la red completa.
Infección vía Web	Interna navegando por un servidor	Se puede comprometer el sistema mediante la navegación y luego

		comprometer el resto de dispositivos.
Ataque a Servidor Web	Externo	Si el servidor Web es atacado el hacker puede obtener acceso a diferentes elementos de la red.
Ataque con Denegación de Servicios	Externo	Servicios externos como navegación, e-mail y ftp pueden quedar inútiles. Si se ataca un router la red puede descalabrase.
Ataque de Usuario a Red	Interno	Puede afectar indistintamente cualquier miembro de la red interna como externa. Inmunes a firewalls periféricos. Firewalls de segmentación pueden aislar el ataque.

Tabla I: Tipos y origen de las Amenazas.

En muchos casos las medidas de seguridad llevan un costo aparejado que obliga a subordinar algunas de las ventajas del sistema. Por ejemplo, la velocidad de las transacciones. En relación a esto, también se hace obvio que a mayores y más restrictivas medidas de seguridad, menos amigable es el sistema. Se hace menos cómodo para los usuarios ya que limita su actuación y establece unas reglas más estrictas que a veces dificultan el manejo del sistema. Por ejemplo, el

uso de una política adecuada de passwords, con cambios de las mismas.

Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales: lógicas, físicas, administrativas y legales. Vamos a verlas con más detalle.

Medidas Físicas

Aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. También protegen al sistema de desastres naturales o condiciones medioambientales adversas. Se trata fundamentalmente de establecer un perímetro de seguridad en nuestro sistema.

Existen tres factores fundamentales a considerar:

- ✓ El acceso físico al sistema por parte de personas no autorizadas
- ✓ Los daños físicos por parte de agentes nocivos o contingencias
- ✓ Las medidas de recuperación en caso de fallo

Concretando algo más los tipos de controles que se pueden establecer, estos incluyen:

- ✓ Control de las condiciones medioambientales (temperatura, humedad, polvo, etc.)
- ✓ Prevención de catástrofes (incendios, tormentas, cortes de fluido eléctrico, sobrecargas, etc.)
- ✓ Vigilancia (cámaras, guardias jurados, etc.)
- ✓ Sistemas de contingencia (extintores, fuentes de alimentación ininterrumpida, estabilizadores de corriente, fuentes de ventilación alternativa, etc.)
- ✓ Sistemas de recuperación (copias de seguridad, redundancia, sistemas alternativos geográficamente separados y protegidos, etc.)
- ✓ Control de la entrada y salida de material (elementos desechables, consumibles, material anticuado, etc.)

Medidas Lógicas

Incluye las medidas de acceso a los recursos y a la información y al uso correcto de los mismos, así como a la distribución de las responsabilidades entre los usuarios. Se refiere más a la protección de la información almacenada.

Entre los tipos de controles lógicos que es posible incluir en una política de seguridad podemos destacar los siguientes:

- ✓ Establecimiento de una política de control de accesos. Incluyendo un sistema de identificación y autentificación de usuarios autorizados y un sistema de control de acceso a la información.
- ✓ Definición de una política de instalación y copia de software.
- ✓ Uso de la criptografía para proteger los datos y las comunicaciones.
- ✓ Uso de cortafuegos para proteger una red local de Internet.
- ✓ Definición de una política de copias de seguridad.
- ✓ Definición de una política de monitorización (logging) y auditoria (auditing) del sistema.

Dentro de las medidas lógicas se incluyen también aquellas relativas a las personas y que podríamos denominar medidas humanas. Se trata de definir las funciones, relaciones y responsabilidades de distintos usuarios potenciales del sistema. Se trataría entonces de responder a preguntas tales como:

- ✓ ¿A quién se le permite el acceso y uso de los recursos?
- ✓ ¿Qué recursos puede acceder cada usuario y qué uso puede hacer de ellos?
- ✓ ¿Cuáles son las funciones del administrador del sistema y del administrador de la seguridad?
- ✓ ¿Cuáles son los derechos y responsabilidades de cada usuario?

A la hora de responder a las preguntas anteriores hemos de diferenciar cuatro tipos fundamentales de usuarios. A cada tipo se le aplicará una política de control de accesos distinta y se le imputaran distinto grado de responsabilidades sobre el sistema:

- ✓ El administrador del sistema y en su caso el administrador de la seguridad.
- ✓ Los usuarios del sistema.
- ✓ Las personas relacionadas con el sistema pero sin necesidad de usarlo
- ✓ Las personas ajenas al sistema

Medidas Administrativas

Las medidas administrativas son aquellas que deben ser tomada por las personas encargadas de definir la política de seguridad para ponerla en práctica, hacerla viable y vigilar su correcto funcionamiento. Algunas de las medidas administrativas fundamentales a tomar son las siguientes:

- ✓ Documentación y publicación de la política de seguridad y de las medidas tomadas para ponerla en práctica.
- ✓ Debe quedar claro quien fija la política de seguridad y quien la pone en práctica.
- ✓ Establecimiento de un plan de formación del personal.

Los usuarios deben tener los conocimientos técnicos necesarios para usar la parte del sistema que les corresponda. Este tipo de conocimiento es fundamental para evitar toda una serie de fallos involuntarios que pueden provocar graves problemas de seguridad. Los usuarios deben ser conscientes de los problemas de seguridad de la información a la que tienen acceso.

Los usuarios deben conocer la política de seguridad de la empresa y las medidas de seguridad tomadas para ponerla en práctica. Además deben colaborar, a ser posible voluntariamente, en la aplicación de las medidas de seguridad.

Los usuarios deben conocer sus responsabilidades respecto al uso del sistema informático, y deben ser conscientes de las consecuencias de un mal uso del mismo.

Medidas Legales

Es la aplicación de medidas legales para disuadir al posible atacante o un procedimiento de defensa ante la ley para demandar de la justicia local sanciones a los perpetrantes ante una violación, o en su defecto, ante las tentativas de violación de las seguridades informáticas de una red bajo ataque.

Este tipo medidas suelen trascender el ámbito de la empresa y pueden ser fijadas por instituciones gubernamentales e incluso instituciones internacionales. Un ejemplo de este tipo de medidas es la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal). Esta ley vincula a todas las entidades que trabajen con datos de carácter personal, define las medias de seguridad para su protección y las penas a imponer en caso de su incumplimiento.

2.4 Términos asociados a las amenazas

En esta sección se hará una breve reseña de la terminología asociada con la seguridad de redes y un resumen descriptivo de las mismas utilizada en el desarrollo de este trabajo con el fin de homogenizar los criterios que surgieren a partir de dicha lectura; así como también se intentará dejar sentados en el lector términos relacionados que puedan facilitar la comprensión de una eventual temática sobre seguridades de software.

Hackers._ Persona de gran habilidad y talento en el uso de computadores capaz de explotar el máximo provecho para obtener objetivos específicos de ellas o de las redes de comunicación a la que estos u otros ordenadores pertenecen accediendo inadvertidamente a ellas.

Habitualmente un hacker solo penetra un entorno seguro para demostrar que este entorno es vulnerable y para probarse a si mismo su efectividad en

ataques. Una vez dentro echan un vistazo según su interés y usualmente se retiran dejando su huella que no es más que una prueba visible de que estuvieron dentro. Si bien es cierto que esta huella puede considerarse como un ataque su nivel destructivo en mínimo es mas en la mayoría de casos no afecta el desempeño de los recursos informáticos. Por ejemplo mensajes en el desktop, cambios en el diseño Web u otro tipo de bromas.

Pero en efecto hay un tipo de hackers mucho más nocivos a los sistemas informáticos, aquellos hackers son conocidos como crackers.

Crackers._ Tipo de Hacker que penetra maliciosamente una estructura informática para causar danos severos, infiltra software de aplicaciones destructivas o crea virus. Práctica común de ellos es el hurtar o arruinar información valiosa o bases de datos enteras, saturar y colgar servidores de mail o aplicaciones Web, averiar un ordenador o red. Por medio de esta habilidad crackers han logrado penetrar para sus despropósitos en universidades, bancos y redes militares con resultados favorables para ellos previamente retirándose sin dejar rastro alguno de su trabajo de modo que los administradores quedan inadvertidos antes el daño.

Para encontrar las vulnerabilidades a explotar de una red los Hackers usan el ping para testear grandes rangos de direcciones, axial encuentran IP’s validas y en estas buscan los puertos abiertos que permitan su acceso. En

los procesadores en cambio se valen de los huecos de seguridad conocidos en los sistemas operativos que son fallas del fabricante para penetrar un sistema.

Phreaker._ Deriva su nombre de 2 palabras del idioma ingles PHONE (teléfono) y FREAK (monstruo, rareza) y se usa para describir dentro del ámbito relacionado con la informática a los individuos que enfocan sus conocimientos y estudios al estudio y discernimiento de sistemas telefónicos, informáticos, la totalidad de elementos de una red telefónica y la electrónica aplicada a sistemas telefónicos. Luego ponen sus conocimientos al servicio de fines personales o malintencionados.

La meta de los phreakers es generalmente superar retos intelectuales de complejidad creciente, relacionados con incidencias de seguridad o fallas en los sistemas telefónicos, que les permitan obtener privilegios no accesibles de forma legal. El phreak es una disciplina estrechamente vinculada con el hacking convencional. Auque a menudo es considerado y categorizado como un tipo específico de hacking informático: hacking orientado a la telefonía y estrechamente vinculado con la electrónica, en realidad el phreaking es el germen del hacking puesto que el sistema telefónico es anterior a la extensión de la informática a nivel popular, el hacking surgió del contacto de los phreakers con los primeros sistemas informáticos personales y redes de comunicaciones.

Spammer._ Propagan cualquier tipo de basura a través de las red para saturar correos electrónicos o para consumir ancho de banda.

Phiser (password harvesting fishing Pesca por una analogía con significado en ingles)._ En el medio informático es el individuo que propaga una clase de estafa que se vale de la ingeniería social mas sofisticada para adquirir fraudulentamente información especialmente financiera que luego utilizan para desfalcar las arcas personales de las victimas. Un breve resumen puede ser el decir que es el atacante engañando al posible estafado, suplanta la imagen de una empresa y/o entidad publica o privada, de esta manera persuaden a la posible víctima que realmente los datos solicitados proceden del sitio Oficial cuando en realidad no lo es.

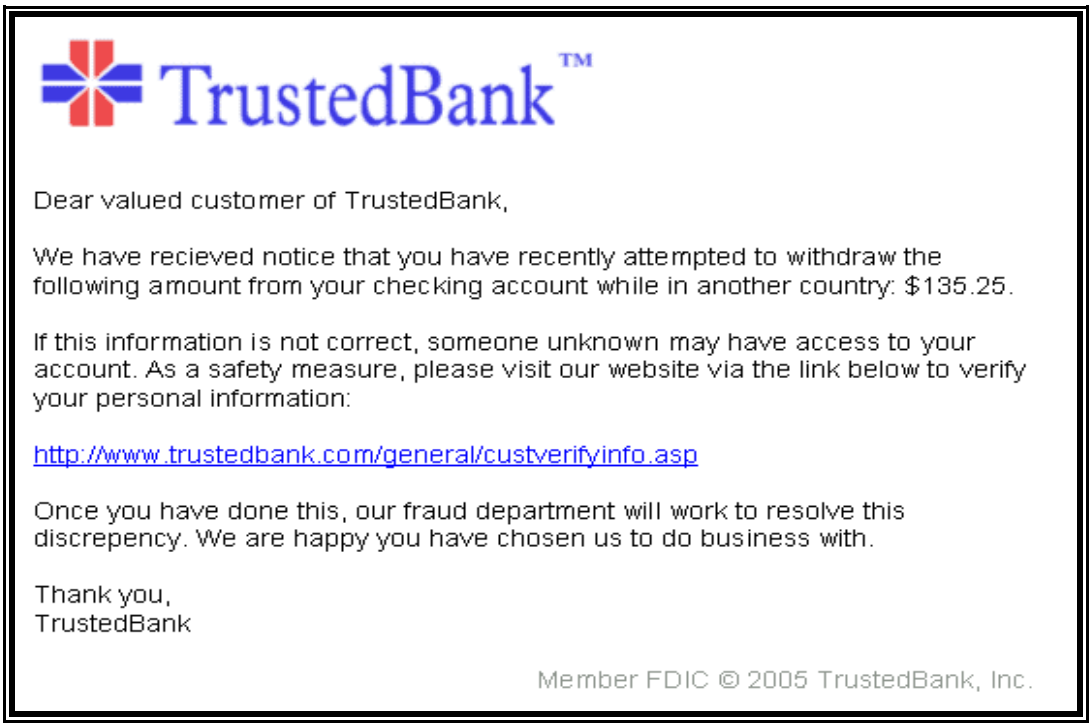


Figura 1.13 Ejemplo 1 de Phising.

El phishing puede producirse de varias formas de la ingeniería social, desde un simple mensaje a su teléfono móvil, una llamada telefónica, una Web que simula una entidad, una ventana emergente, y la más usada y conocida por los intel nautas, la recepción de un correo electrónico. Siendo estas ultimas las vías más sofisticadas y efectivas para los phisers.

Las páginas Web fungen como los sites oficiales de conocidas empresas en la cual las victimas depositan sus datos.

Figura 1.14 Ejemplo 2 de Phising.

Figura 1.15 Ejemplo 3 de Phising.

De estas páginas las más peligrosas debido a la credibilidad que despierta en las victimas son las que fungen como las home page de entidades bancarias.

El phising más popular es aquel que se esparce vía correo electrónico y que alega ser actualización personal de datos, herencias ficticias, recompensas monetarias de Microsoft u otras compañías mundiales y todo tipo de tretas que incentiven y despierten la avaricia de las victimas y luego compartan información confidencial.

Figura 1.16 Ejemplo 4 de Phising.

Para protegerse del phising se debe tener presentes las siguientes recomendaciones:

- ✓ Sospeche de cualquier mensaje que solicite datos financieros, de contraseñas, claves de acceso, nº de tarjeta de crédito, etc.
- ✓ Estos mensajes NO suelen ir personalizados, mientras que los enviados por su banco normalmente lo son.
- ✓ Si tiene alguna sospecha de un mensaje, no utilice los enlaces hacia otras páginas que vengan en él. En vez de eso, teclee usted mismo la dirección de la página.

- ✓ Siempre que introduzca datos 'sensibles' a través de una página Web, asegúrese de que lo hace bajo una conexión segura. Cuando en la dirección de la página vea '**https://**' en vez de '**http://**' sabrá que es una conexión segura.
- ✓ Asegúrese de tener instaladas las últimas actualizaciones de su sistema operativo y navegador.

Si decide arriesgarse a verificar una de estas direcciones tipeelas ud. mismo en lugar de acceder solo vía el link.

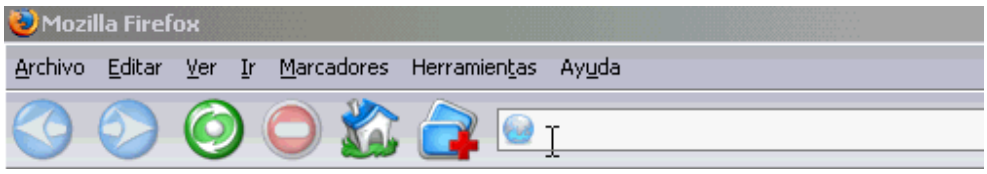


Figura 1.17 Tipear la dirección para evitar el Phising (no seguir link de procedencia dudosa).

Los daños causados por el phishing oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustanciales. Este tipo de robo de identidad se está haciendo cada vez más popular por la facilidad con que personas confiadas normalmente revelan información personal, incluyendo números de tarjetas de crédito y números de seguro social. Una vez esta información es adquirida, los phishers pueden usar datos personales para crear cuentas falsas utilizando el nombre de la víctima, gastar el crédito de la víctima, o incluso impedir a las víctimas acceder a sus propias cuentas.

Se estima que entre mayo del 2004 y mayo del 2005, aproximadamente 1.2 millones de usuarios de computadoras en USA tuvieron pérdidas a causa del phishing, lo que suma a aproximadamente US$929 millones. Los negocios en los Estados Unidos perdieron cerca de 2000 millones de dólares al año mientras sus clientes eran víctimas. Reino Unido también sufrió el alto incremento en la práctica del phishing. En marzo del 2005, la cantidad de dinero reportado que perdió el Reino Unido ha causa de esta práctica fue de aproximadamente £12 millones.

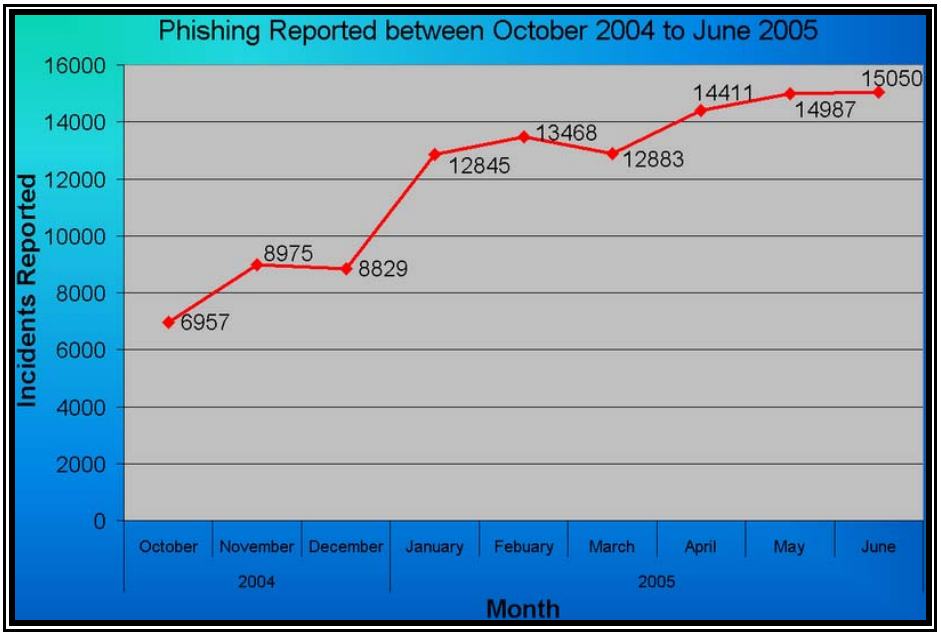


Figura 1.18 Ataques de Phising Reportados entre octubre 2004 a junio del 2005.

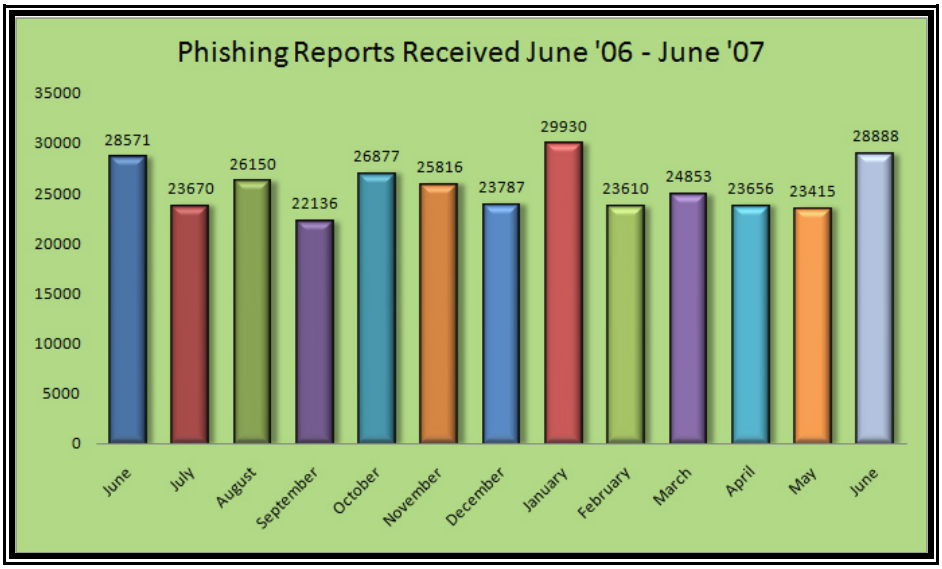


Figura 1.19 Ataques de Phising Reportados entre junio del 2006 al junio del 2007.

Virus._ Son los ataques a la seguridad mas conocidos. Son programas desarrollados por maliciosos programadores creados para auto reproducirse e infectar dañinamente cuando son accionados por un evento o aplicación especifica.

Una red puede infectarse solo si el virus logra infiltrarse desde una fuente externa infectada, casi siempre al compartir archivos vía floppy disk y pendrives o al bajarlos de Internet. Cuando una computadora de la red logra ser infectada el resto de dispositivos de red quedan inmediatamente expuestos a la reproducción del virus. Un virus tiene 3 características definidas: Es dañino, es auto reproductor, es subrepticio.

Asimismo, se pueden distinguir tres módulos principales de un virus informático aunque hay casos donde alguno de estos módulos pudiera faltar: módulo de reproducción, módulo de ataque, módulo de defensa.

Troyanos._ Como la alusión de su nombre lo indica los troyanos son el vehiculo perfecto para este tipo de software malicioso ya que a primera impresión parece software inofensivo y a veces hasta muy útil para el usuario pero sus aplicaciones ocultas pueden ser altamente destructivas.

Vándalos._ Los Web sites presentan aplicaciones de tipo ActiveX o Java que resaltan su presentación y por ende el interés del los cibernautas. Estas aplicaciones presentan animaciones y otros efectos visuales que se corren desde la PC del usuario generando así otra vía de esparcimiento para el malware o software malicioso. UN vándalo es software nocivo que puede causar varios niveles de daño que van desde destruir un simple archivo hasta corromper la mayor parte del sistema operativo de un ordenador.

DMZ (demilitarized zone).- Configuración de firewalls por medio del cual se intenta salvaguardar los más transcendentes elementos de la red. Esta arquitectura consiste en utilizar 2 firewalls: uno entre red externa y la zona desmilitarizada y el segundo entre la zona desmilitarizada y la red interna.

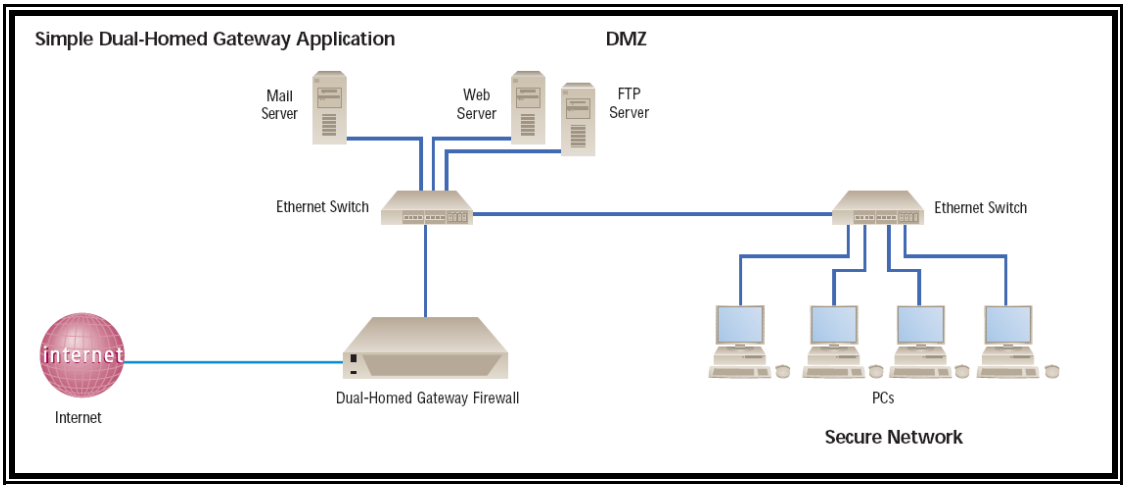


Figura 1.20 Ejemplo de una red con zona desmilitarizada.

2.5 Tipos de Ataque

Innumerables tipos de ataques han podido ser documentados y de entre la clasificación podemos resumir:

- ✓ Ataques de reconocimiento._ Se puede definir como todas las actividades relacionadas con la recolección de datos que puedan ayudar posteriormente a franquear las seguridades de la red.
- ✓ Ataques de acceso._ Son aquellos ataques orientados a explotar las vulnerabilidades de una red y se suelen enfocar en los servicios de autentificación y las funcionalidades FTP (file transfer protocol) para poder acceder a cuentas de e-mail, bases de datos u otras fuentes de información confidencial.
- ✓ Denial of Service (DoS)._ Estos ataques evitan el acceso a parte o a la totalidad de un sistema informático. Consisten en enviar gran cantidad de datos averiados pesados e imposibles de procesar

hacia una computadora conectada a una red de telecomunicaciones. Más peligroso aun es el DoS Distribuido que compromete a varios hosts.

A continuación detallaremos y ampliaremos todos y cada uno de los tipos de ataque.

2.5.2 Reconocimiento

Los ataques de reconocimiento están claramente orientados a la obtención de información confidencial útil para poder burlar las seguridades que pueda presentar una red de información. Los sniffers y scanners son utilizados para mapear los elementos de las redes deseadas y explotar sus potenciales falencias. Por ejemplo existe software dedicado a descifrar password, estos programas fueron desarrollados pensando en aquellos administradores que deben recuperar claves perdidas de los usuarios o para ingresar a computadores de empleados que salieron de la compañía dejándolos bloqueados al acceso. En las manos equivocadas la peligrosidad de uso puede ser inconmensurable.

Estas técnicas son conocidas también como ingeniería social. Precisamente la denominada ingeniería social se encarga de la obtención imperceptible de información confidencial por diversas vías no

específicas pero pueden detectarse y prevenirse tan solo con mantener las reservas necesarias. Varios ejemplos clásicos son el fungir ante los empleados de representante del soporte técnico para obtener respuestas de conocimiento restringido; enviar por correo formularios so pretexto de actualización de datos del departamento técnico informático o de recursos humanos; creación de paginas Web, blogs o afines donde la subscripción incluyen preguntas para obtener datos personales generalmente usados como claves de acceso; Llamadas para fungir como empresas ofreciendo v arios servicios gratuitos con tan solo entregar ciertos datos a cambio; se puede también hacer ingeniería social desde el interior de la empresa manipulando a compañeros para que cometan ilícitos en lugar del atacante o averiguando password de terceros para cometer los danos involucrando a otro usuario, etc.…

Puede también relacionarse la intercepción de datos ya que es posible intervenir una transmisión, decodificarla y hasta alterarla incluyendo la verificación de claves al accesar a un servicio. Para transmiciones que utilizan el protocolo IP (Internet Protocol) una herramienta muy utilizada es el IP sfoofing.

2.5.2 Acceso

Desde que se demostró que asumir las redes como absolutamente seguras antes la instrucción de personas ajenas a ellas era un craso

error fue necesaria la concepción de protocolos para el incremento de seguridades en sus diferentes niveles. La seguridad es trascendental en todos y cada uno de los ámbitos de la vida y en la medida de lo posible se debe implementarla para mantener la confidencialidad del pensar u obrar.

La seguridad de redes no dista mucho de la seguridad en cualquier otro campo ya que se trata básicamente de mantener el sigilo de la información que a través de ellas se intercambia. Aprovechando este factor y con el fin de explicar este ámbito de una manera mas comprensible se hará una analogía entre la seguridad de redes y la seguridad habitual de un edificio con la cual ud. señor lector puede hallarse mas familiarizado.

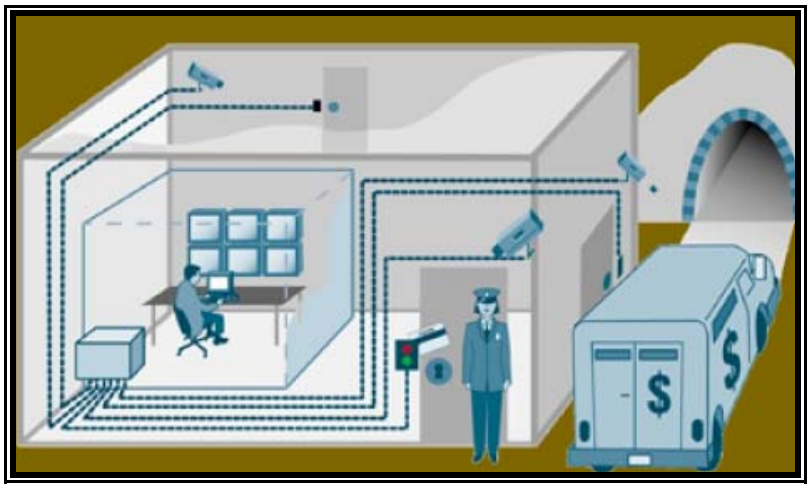


Figura 1.21 Como la seguridad de un edificio la seguridad de software es un proceso de varios niveles

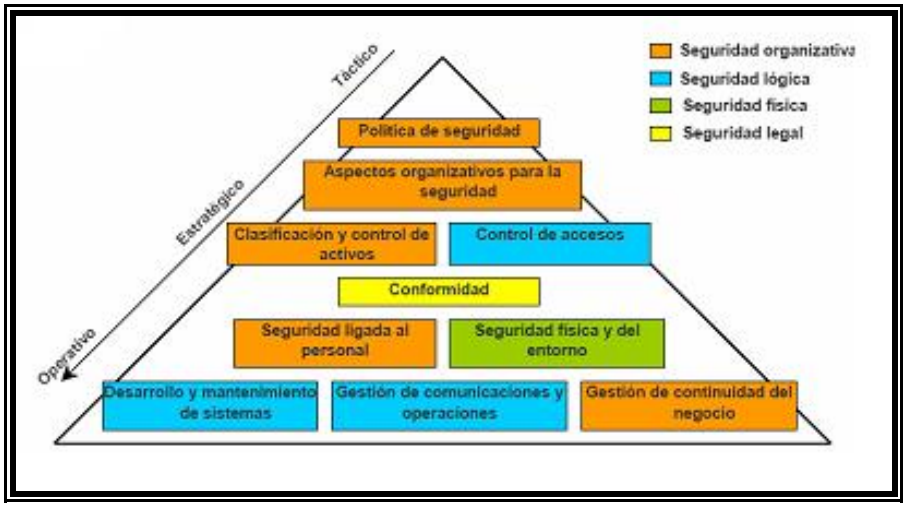


Figura 1.22 Niveles de seguridad y clasificación según usuarios.

El primer paso para implementar una política de seguridad en una red informática es establecer un nivel de acceso para cada empleado y los beneficios de red con que deben contar según el rol que desempeñen en la compañía y las aplicaciones que necesiten para cumplir satisfactoriamente sus obligaciones.

Esta clasificación es solo posible mediante la asignación de un usuario y su respectiva identidad a todos los miembros de la empresa y el nivel de accesos puede variar desde acceso nulo hasta acceso total.

Esencialmente el control de acceso se concentra en 2 puntos clave a resaltar: autentificación y encriptación.

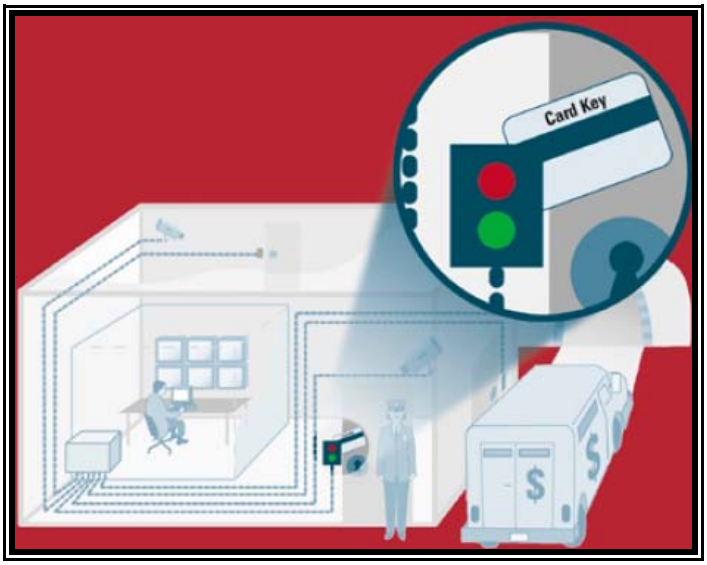


Figura 1.23 La verificación de identidad de usuario.

Autenticación de usuarios

La autentificación es la de verificación de identidad de aquellos usuarios que gozan de privilegios de red al intentar acceder a ellas. Este proceso se hace con una lista de control de acceso (Access List) con la cual se compara el usuario solicitante para permitir el paso y se divide en 2 procesos ordenados y sucesivos: autentificación de acceso general y la autorización funcional.

El acceso general es la simple verificación sobre si el usuario solicitante goza o no de acceso, cualquiera que este sea de entre todos los beneficios de red que el servidor esta en capacidad de proveer. Es decir no discierne a que privilegio especifico puede ingresar solo da el paso

para que siga el camino hacia el siguiente filtro. El acceso general se considera comúnmente como la “cuenta de usuario”.

La autorización funcional es la tangibilizacion de los derechos del usuario, lo que significa el discernimiento entre que aplicación puede y debe el solicitante obtener una vez que ya ha sido previamente autentificado. Es aquí donde por ejemplo se le brinda la potestad de editar la información a la que pudo ingresar o si tan solo le será factible leerla.

Figura 1.24 La autentificación de los usuarios en la analogía la puerta de seguridad que permite o no el paso a los usuarios.

Para la autentificación de identidad existen varios protocolos.

PROTOCOLO	CARACTERISTICAS	PROTOCOLOS USADOS
Usuario/Password	Plaintext, Token memorizado	Telnet, http
CHAP(Challenge Handshake Authentication Protocol)	Uses hashes de passwords y datos variantes en el tiempo para evitar la transmisión directa de la clave.	MS-CHAP, PPP, APC http, Radius
RADIUS	CHAP métodos directos de claves, autorizaciones y cuentas.	Backend para Telnet, SSH, SSL, front end para Microsoft IAS Server. Métodos típicos para centrales de autenticación para dispositivos de red.
TACACS+	Soporte para autentificación, autorización, cuentas y encriptaciones de alto nivel.	Protocolos Cisco, central de autentificación y algunos RAS (Remote Access Service)
Keberos	Servicios de autentificación y autorización, encriptación	Keberized aplicaciones como Telnet, autentificación de dominios

	de lato nivel.	de Microsoft con servicios integrados con Active Directory.

Tabla II: Aplicación de diferentes protocolos

Restringir el acceso es uno de los aspectos más importantes cuando se asegura una red. Desde que las estructuras de las redes se conforman tanto de elementos de computación como de dispositivos periféricos para comprometer la red entera basta con comprometer a tan solo uno de ellos, es por eso que no sirve de mucho asegurar el perímetro y servidores con firewall si el resto queda desprotegido.

La autentificación tiene un mejor desempeño cuando esta absolutamente centralizada tanto en los esquemas donde bien sea muchos usuarios comparten limitados elementos de red o en redes con gran numero de elementos de red. La muestra mas tangible es el control de acceso remoto. Asumiendo múltiples usuarios y múltiples servidores de autentificación de acceso entonces el sistema debería poder validar el acceso de cualquier usuario en todos los centros de verificación de usuario y por ende mantener dichos centros constantemente actualizados sobre los cambios de usuarios o de claves de acceso que se puedan presentar.

Pero la solución a estos problemas son los sistemas de autentificación centralizados. Estos esquemas centralizados permitirán almacenar la información en una sola base de datos en lugar de varias así, si alguna cuenta sufre alguna modificación bastara con una sola tarea para validar correctamente a este usuario en todo el sistema.

También si un empleado deja la compañía será más fácil de eliminar inmediatamente su cuenta desde la central. Un típico problema de los sistemas de autentificación no centralizados es recordar eliminar una sola cuenta en todos los puntos de verificación.

El siguiente grafico muestra un Windows Domain Controller operando como LDAP Directory (Microsoft Active Directory) y como un sistema de autentificación centralizado RADIUS.

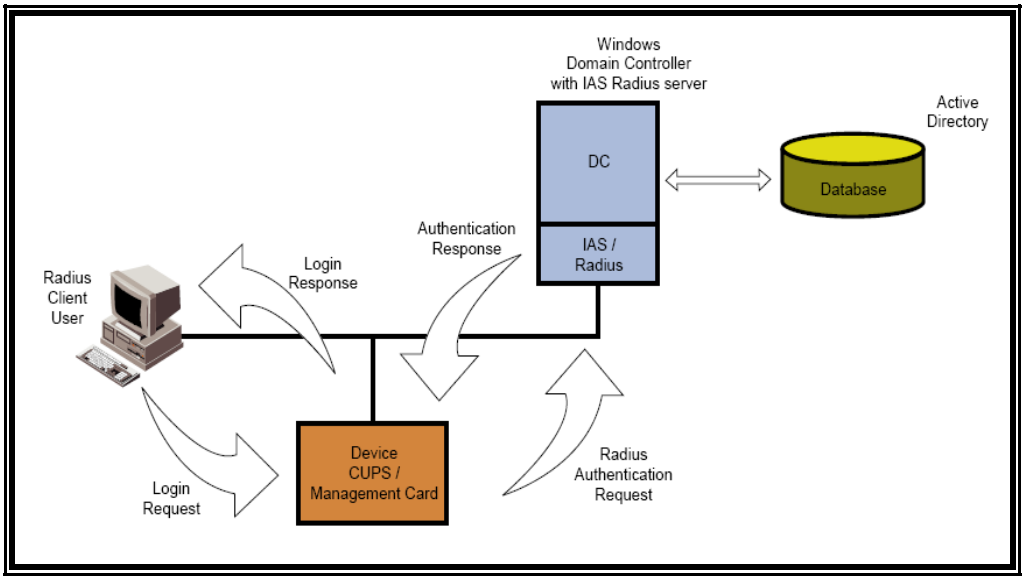


Figura 1.25 Funcionamiento de un Windows Domain Server.

Encriptacion

Es la tecnología utilizada para asegurar que los mensajes no puedan ser descifrados en caso de que la información llegue a ser interceptada por otro usuario diferente al destinatario para evitar su mal uso. Es necesario encriptar cierta trascendental información que es intercambiada entre elementos específicos de la red o incluso fuera de ella, ejemplo de ello son las VPNs (Virtual Private Network). En las VPNs la encriptación de la información es el factor gravitante en torno al cual debe girar el flujo de intercambio de datos ya que al atravesar redes públicas pueden ser blancos de ataques.

Si bien es cierto que es necesario proteger o no los datos dependiendo del nivel de importancia para la empresa existe un campo que tienen la mas alta clasificación en esta clasificación puesto que brindan accesos ilimitados si pueden ser descifrados, estos campos son las claves de acceso o passwords y el punto mas critico para su intercepción es precisamente la validación de acceso los usuarios.

Aunque es una práctica menos común muchas organizaciones están empezando a implementar políticas de seguridad donde ya se maneja la encriptación de toda la información que a través de su red pasa o se origina, no solo durante el proceso de autentificación. En ambos casos la encriptación es indispensable.

La encriptación puede ser descrita como la combinación de simple texto (plaintext o información comprensible para el ojo humano) con una clave determinada por medio de un algoritmo de encriptación (ejemplo: 3DES, AES, etc.), el resultado es el texto encriptado. Una vez que el texto ha sido encriptado no puede ser revertido a simple texto a menos que el atacante conozco el código clave.

Podemos comparar entonces en el ejemplo a los métodos de encriptación con camiones blindados que transportan seguramente los datos a través de la red.

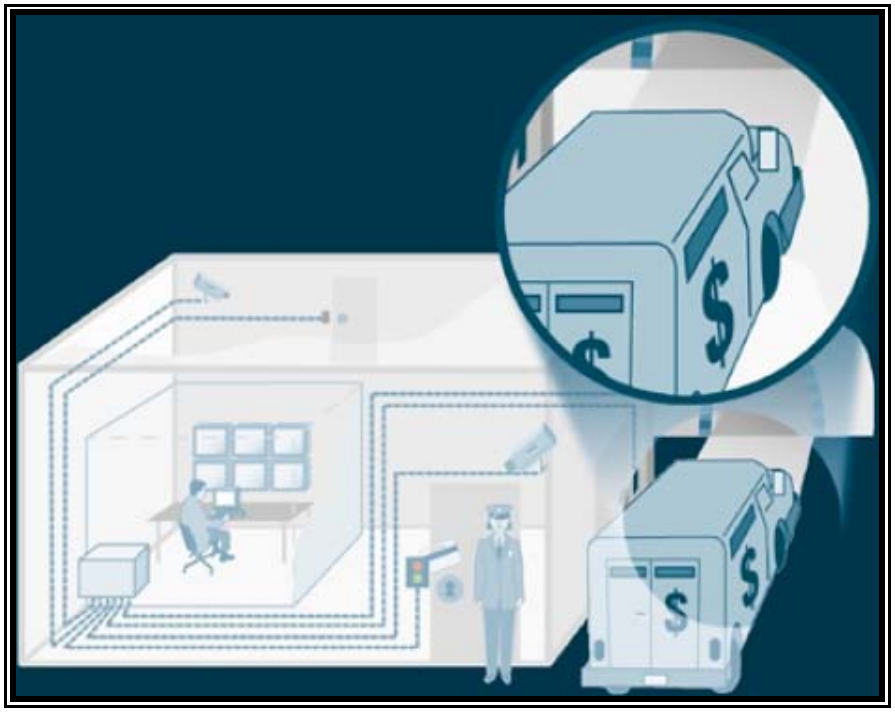


Figura 1.26 En la analogía la encriptación una segura transportación.

Existen varios protocolos de encriptación y como es fácil de prever unos son más eficientes que otros. Entre estas encriptaciones de nivel mas

alto están los “Hash”. Los métodos de encriptación Hash toman el texto simple y tal vez una clave y los computan con un número muy grande denominado Hash, de allí su nombre. Este número tiene un tamaño definido en un gran número de bits sin considerar si la entrada de datos simples es también grande o no.

A diferencia de los métodos de encriptación reversibles, el Hash es tan solo unidireccional, esto es, que no puede ser revertido. Su estructura lo hace matemáticamente imposible de regresar a simple texto y por ende desencriptado. Por esta razón los Hashes son utilizados únicamente como IDS (Intrusión Detección Sistema). Una red basada en IDS analiza las cadenas de datos con protocolo similares a los CRC (Cyclic Redundant Check usados para detección de errores en transmisión de datos) en busca de actividades inusuales como ataques de hackers y permitiendo a los usuarios responder ante la ruptura de la seguridad antes de que la red sea comprometida.

Cuando la vulnerabilidad es detectada los Hash (IDS) son alterados en su valor y pueden enviar alarmas hacia la administración con detalles de la actividad para que las políticas de respuesta ante ataques puedan ser desplegadas inmediatamente, así por ejemplo, la sesión de origen del ataque pueda ser desactivada para evitar que el ataque surta algún efecto.

En la analogía los Hashes vendrían a ser las cámaras de seguridad que constantemente monitorean en busca de algún intruso dentro de la red.

Figura 1.27 Analogía de los hashes con la vigilancia permanente

La tabla no indica varios métodos de encriptación y su aplicación.

Algoritmo	Uso Principal	Protocolos Usados
DES	Encriptación	SSH, SNMPv3, SSL/TLS
3DES	Encriptación	SSH, SNMPv3, SSL/TLS
RC4	Encriptación	SSL/TLS
Blowfish	Encriptación	SSH
AES	Encriptación	SSH,SSL/TLS
MD5	Encriptación	SSH, SNMPv3, SSL/TLS
SHA	Encriptación	SSH, SNMPv3, SSL/TLS

Tabla III: Protocolos de encriptación.

2.5.3 Denegación de Servicio(DoS)

La denegación de servicios es el mas conocido de los ataques por saturación de la red. La saturación de redes de transmisión de paquetes se considera un tipo de ataque malicioso pero puede también ser originada por instancias fortuitas o una proyección inusitada por ejemplo: una pagina Web puede volverse exponencialmente popular por su gran calidad e interés de su contenido; la empresa tiene un repunte nunca antes imaginado en la bolsa de valores; la primicia de una noticia mundial en un blog; o simplemente un site ser inesperadamente promovido por un medio como la radio o incluso televisión lo que orientaría un numero masivo de solicitudes para los cuales el servidor no se encuentre preparado.

Pero a pesar se ello, DoS sigue siendo un subconjunto de dicho universo, es por esto que a continuación se detallan este como otros ataques maliciosos debido al método de saturación de redes.

DoS

La Denegación de Servicios (DoS, Denial of Service) satura los servidores Web o de e-mail con un numero de solicitudes de atención mucho mayores a los que puede manejar causando progresivamente danos no habituales que inician en la disminución de la velocidad del servicio y terminan en la deshabilitacion total del

servicio. Pueden ser originados personalmente por un hacker o en su defecto por un virus insertado. Algunas clases de DoS son las siguientes:

- ✓ Buffer Attack: Es la practica mas común de DoS y no es mas que enviar mas trafico del estimado hacia una dirección especifica. Casi siempre es el envió deliberado de paquetes sobredimensionados en tamaño o e-mail con archivos adjuntos demasiado pesados imposibles de procesar.
- ✓ SYN: Son los ataques de sincronización y es el envió consecutivo de un gran numero de solicitudes de conexión a una frecuencia mayor de la frecuencia de procesamiento del servidor imposibilitando que las solicitudes de legitimación de sesiones puedan establecerse.
- ✓ Teardrop Attack: Es el envío de paquetes demasiado grandes con valores insertados en él que dificultan al protocolo IP su reagrupación una vez que han logrado interrumpir la transmisión absorbiendo toda la capacidad de procesamiento.
- ✓ Smurf Attack: Envía solicitudes de PING al site de un tercero pero altera la dirección de respuesta intercambiándola con la dirección del servidor a ser atacado saturándolo de respuestas de ping.
- ✓ Mail Bomb: Este ataque bombardea un servidor de e-mail con muchos más mails de los que puede manejar.

Spam

Spam es otro causal de la saturación de redes y es el nombre que se ha otorgado a esa gran cantidad de desperdicios que invaden los sistemas sin haber sido solicitados jamás. El spam significa perdida de tiempo, satura anchos de banda y cuelga los servidores de e-mail y peor aun es un problema cada vez más creciente a través de la red. Quizá pueda resultar más fácil para el lector reconocer el spam si se describe al spam como aquellos mails que inesperadamente llegan a los correos en tal numero que llenan el buzón de entrada con promociones y ofertas de dudosos productos, con links que redireccionan a paginas pornográficas, correos cadenas sobre una amplia variedad de contenidos, falsas advertencias sobre el cierres de dominios o servidores de correos e inclusive intentos de estafa masiva acerca de premios de loterías ficticias, herencias insólitas y cualquier otra similar.

En efecto el spam es perturbante pero a diferencia de la creencia general de que tan solo son una molestia inofensiva el spam puede también tornarse peligroso. Spammers (creadores del spam) consiguen sus listas de direcciones e-mail “minando” los sites conocidos como newsgroups y rondando la Web en busca de base de datos o direcciones sueltas. También suelen vender o intercambiar listas de direcciones para incrementar el número de sus

victimas. Ya que la mayoría de los ISPs bloquean los e-mails provinentes de los Spammers conocidos, ellos se valen de virus para infectar los PCs de terceros y routear sus spams desde usuarios no delatados ante los ISPs como fuentes de origen de spam. Estos PCs son conocidos como zombis y son ellos quienes hacen posible que los servidores de e-mails se saturen de spam no deseado y aun peor, los hace sospechosos del esparcimiento de spam a través de la red no siendo ellos responsables.

Otra técnica comúnmente usada por los spammers es abrir una cuenta depositable en un ISP y para cuando este nota el hecho ya se han enviado decenas de miles de e-mails basura y tan solo le queda el hecho de limpiar los vestigios del ataque.

Spam Publicitario

Es el tipo generalmente mas enviado de Spam y habitualmente promocionan productos y ofertas inconsistentes o fraudulentas. Entre las mas populares están negocios de fácil y rápido enriquecimiento, oportunidades de excelentes trabajos de pocas horas y desde el hogar, curas milagrosas, investigaciones extravagantes, formas y medios para robar televisión por cable, ofertas de cupos ilimitados de crédito en almacenes de fama

reconocida, vacaciones y cruceros gratuitos, posiciones mágicas para mejor desempeño sexual, etc.…

Los spammers envían Spam publicitario vía e-mail porque es la vía mas barata, es publicitar en un medio por el cual no se tiene que pagar. Por ser el Spam un medio de tan bajo costo no tiene sentido el orientar la difusión hacia un target (en marketing el segmento especifico del mercado al cual esta enfocado la promoción de un producto) si por el mismo precio se puede atacar un millón de direcciones e-mail.

Spam Dañino

Algunos Spam pueden atacar al transportar virus o tratar de persuadir a la victima a facilitar datos de tarjetas de crédito o cuentas bancarias. Muchos Spam no provienen precisamente de crackers sino de gusanos que se esparcen a si mismos generando e-mails infectados desde un host no sospechosos. De estos gusanos se han generado ataques tan graves al punto que muchos usuarios encontraron en su buzón de mensajes mas spam infectados que correos electrónicos.

Otras estafas que tratan de conseguir dinero del usuario a toda costa. Recientemente mucha gente recibió e-mails que aparentemente provenían de las tiendas eBay o de PayPal, aduciendo que necesitaban actualizar sus cuentas. Los correos eran fiel copia de aquellos correos originados en los mencionados sites, incluso contenían los logos originales y redireccionaban a paginas iguales a las legitimas donde los ingenuos usuarios facilitaron la información financiera que era requerida. Días después descubrieron que sus números de tarjetas de crédito y su identidad habían sido usurpadas.

Hoax Spam

Muchos Spams son propagados pero no precisamente por Spammers profesionales o gusanos sino por gente ingenua que recibe y cree en cadenas y tratan de ayudar a encontrar por ejemplo niños perdidos o de advertencias sobre virus inexistentes. Las cadenas son cartas que deben reenviarse por el usuario a muchos contactos generando una reproducción geométrica y que brindan una gran respuesta de esparcimiento con poco esfuerzo. Casi siempre apelan a no avergonzarse de la fe o las promesas de de mala suerte si se rompe la cadena. Si las cadenas incluyen intercambio de dinero pasan de ser una perturbante molestia a ser un delito. Los Hoax saben bien que

puntos son manipulables en la mayoría de seres humanos y es común atacar el altruismo. Mails que prometen salvar la vida de niños enfermos, caridad para fundaciones de ayuda humanitaria. También variedades usan cualquier otro sentimiento arraigado fuertemente en la sociedad como la avaricia y prometen remuneración, reducción de impuestos, recibir la recompensa de Microsoft o la herencia de Hill Gates tan solo con reenviar estos correos a toda la lista de contactos.

Otros en cambio advierten sobre la existencia de un falso virus y ofrecen ayuda mientras en realidad están infectando el ordenador y llegan incluso a ofrecer la venta del software para reparar la reciente infección.

2.5.4 Código Malicioso

Desde que la Internet tuvo un nivel de aceptación tan alto como del que hoy goza se han desarrollado muchos tipos de códigos de programación para hacerla un entorno amigable, entretenido, útil y beneficioso. Estos códigos mejoran día a día los servicios como las paginas Web, los servicios de e-mail, transferencia de archivos, aplicación streming o real time, etc. Si bien es cierto que los códigos de programación han sido extremadamente útiles para el desarrollo de todo ámbito en el que sea utilizado un sistema informático, no es menos cierto que las bondades

que el código no entrega son solo una transferencia de los conocimientos e intenciones del programador.

Como ya se expuso al inicio de este capitulo existen varios tipos de programadores y desafortunadamente también existen aquellas mentes extremadamente brillantes, genios llenos de talento informático que se dedican al desarrollo se códigos destructivos o de alto poder dañino como puede ser la transmisión de información confidencial, alteración de datos, simple daño parcial de un PC, etc. Este tipo de códigos son el alma de programas como los virus. A diferencia de la errática creencia generalizada no todo aquello que afecta el correcto desempeño de una computadora es un virus, pero si todo aquello que altera el buen desempeño de un elemento informático y que proviniere de una fuente externa es un código malicioso. La manera mas practica de distinguir cuando un código es un virus o no es constatando si este tiene las características que definen al virus (dañino, autor reproductor y subrepticio).

Un ejemplo de esto es un caso ocurrido algunos años atrás, cuando la red de IBM, encargada de conectar más de 130 países, fue virtualmente paralizada por haberse saturado con un correo electrónico que contenía un mensaje de salutación navideña que, una vez leído por el destinatario, se enviaba a sí mismo a cada integrante de las listas de

distribución de correo del usuario. Al cabo de un tiempo, fueron tantos los mensajes que esperaban ser leídos por sus destinatarios que el tráfico se volvió demasiado alto, lo que ocasionó la caída de la red. Queda demostrado que este caso de Spam sin llegar a ser virus es sí un ejemplo de código malicioso.

Para evitar perjuicios por código malicioso es preferible no ejecutar códigos de fuentes desconocidas o no confiables ya que en la mayoría de los casos los usuarios abren y ejecutan aplicaciones de software sin tener en cuenta de donde provienen los archivos. Tomar seguridades complementarias como configurar el MS Outlook para leer los e-mails en texto plano (Tools/Options/Preferentes, click en Opciones de E-mail y active “Enable Read all standard mail in plain text”) de este modo evitara que los códigos utilizados para enriquecer los formatos HTML puedan infiltrar algún código malicioso.

Las infinitas variantes que se pueden hallar de estos códigos hacen que con fines de autoprotección los usuarios se eximan de utilizar aquellas aplicaciones que puedan contener infiltradas porciones de código capaces de desestabilizar el sistema informático. A continuación se presenta un resumen de los códigos maliciosos más destacados del primer semestre del 2007 (según Eset fabricante del antivirus NOD32):

1. El Win32/TrojanDownloader.Ani.Gen se mantiene firme en la primera posición del ranking de hasta junio del 2007, es una amenaza que aprovecha una vulnerabilidad (ya corregida por Microsoft) en los archivos “.ANI”; es decir, aquellos que brindan la posibilidad de contar con cursores e íconos animados en Windows. Este *malware* aprovecha dicha inseguridad para descargar otros códigos maliciosos como troyanos, gusanos o ladrones de contraseñas.

2. Win32/BHO.G, con el 2,41% del total. Este código malicioso es un troyano que roba información del sistema infectado. Su nombre proviene de "*Browser Helper Object*" y, utiliza objetos de Internet Explorer para obtener, de forma fraudulenta, información que es introducida al navegador (como usuarios, claves, tarjetas de crédito, etc.). Además registra direcciones Web de las páginas visitados por el usuario.

3. Win32/RJump.A con el 2,26% del total. Esta amenaza es un gusano con características de troyano que abre un acceso por puerta trasera; puede propagarse copiándose a dispositivos de almacenamiento masivo, incluyendo discos duros externos, cámaras digitales, teléfonos móviles, memorias USB y otros.

4. Win32/Spy.VBStat.J este *malware* modifica la página de inicio, agrega barras de navegación y abre ventanas *pop-up* en distintos navegadores, como Internet Explorer y Firefox.

5. INF/Autorun para archivos Autorun.inf, que son aquellos utilizados para ejecutar programas automáticamente cuando un medio óptico como un CD o un DVD, o un dispositivo USB, son leídos por un ordenador. Muchos programas maliciosos actuales están utilizando dicha técnica para propagarse a través de medios no convencionales.

6. Win32/Pacex.Gen, un gusano de correo electrónico que fue descubierto a mediados de marzo y tuvo altos niveles de propagación durante dicho mes.

7. Win32/Adware.Virtumonde este *malware* es un *adware* que es utilizado para enviar publicidad de distintos productos a los usuarios infectados.

8. Win32/Netsky.Q es una versión del Netsky. Algunos antivirus la detectan como la variante "R". Se propaga por correo electrónico con numerosos asuntos y textos. El adjunto es un archivo .PIF o .ZIP. Se vale de una antigua vulnerabilidad del Internet Explorer

(5.x), que permite que se ejecute el adjunto por solo leer el mensaje o verlo en el panel de vista previa (MIME header vulnerability)

9. Win32/PSW.QQRob es un "keylogger" (capturador de la salida del teclado), del tipo PSW (abreviatura de password o contraseña), capaz de obtener información del usuario y del equipo infectado. Ello incluye contraseñas, nombres de usuario, y cualquier información confidencial que la víctima haya ingresado en cualquier página o documento a través del teclado

10. Win32/Rootkit.Vanti.E un Caballo de Troya liberado por otros troyanos. Cuando se ejecuta, puede ocultar diversa información, que incluye sus propios procesos y los de otros malwares que se estén ejecutando. Es utilizado por otros troyanos del tipo adware para ocultarse en un sistema infectado.

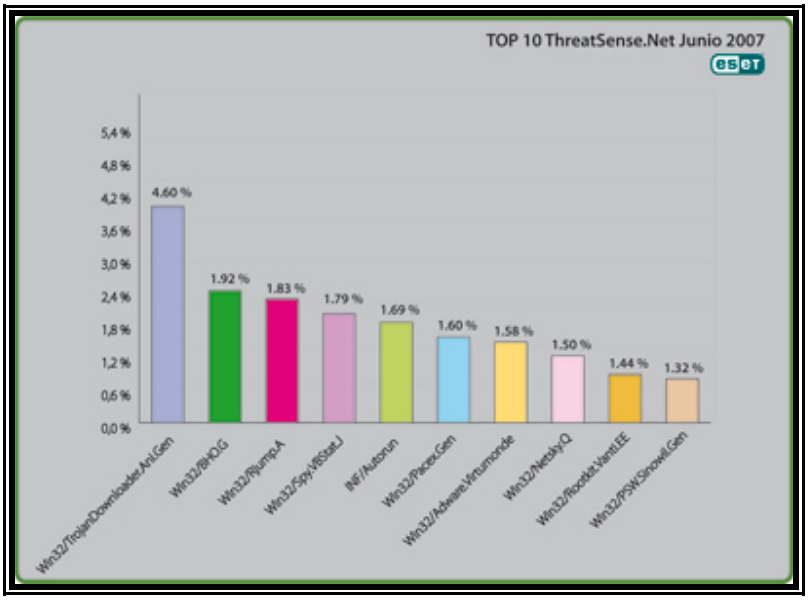


Figura 1.28 Ranking de *Eset* de los códigos maliciosos más esparcidos en la red en el 1er semestre del 2007.

Aunque el segundo semestre parece denotar una tendencia distinta ya que se ve un predominio de los botnets como el malware con mayor presencia dentro del ranking. Esta creciente de detecciones de troyanos del tipo bot es un término que hace referencia a una colección de software robots, o bots, que se ejecutan de manera autónoma (normalmente es un gusano que corre en un servidor infectado con la capacidad de infectar a otros servidores). El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota y normalmente lo hace a través del IRC. Sus fines normalmente son poco éticos, los cuales se encargan de generar redes de equipos zombies, es decir, cada equipo infectado es utilizado por malware de forma remota para enviar Spam o cualquier tipo de amenaza informática.

También aparecen Win32/PSW.Sinowal.Gen y sus alias. Se trata de un "keylogger" (capturador de la salida del teclado), del tipo PSW (abreviatura de password o contraseña), capaz de obtener información del usuario y del equipo infectado. Ello incluye contraseñas, nombres de usuario, y cualquier dato confidencial que la víctima haya ingresado en cualquier página o documento a través del teclado. Esta información suele estar relacionada con ciertos sitios bancarios.

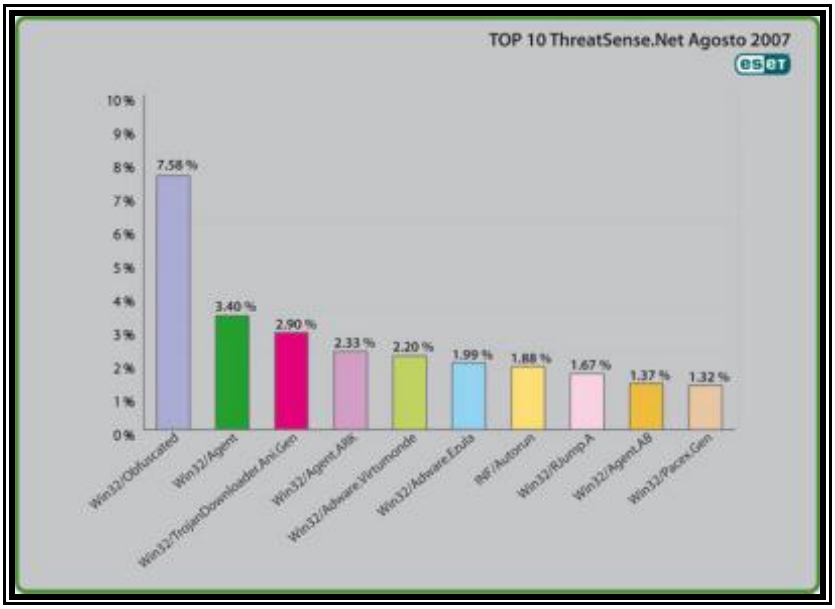


Figura 1.29 Agosto del 2007 marcando la tendencia de los codigos maliciosos para el 2do. Semestre de ese año.

Otras medidas para contrarrestar codigos maliciosos es escanear constantemente tanto el perímetro con el interior de nuestra red. A pesar de que la mayoría de codigos escanean en busca de codigos reconocidos como dañinos, variantes o derivaciones de los mismos, pero debido al permanente desarrollo diario de nuevos métodos de

ataque este método podría resultar ineficiente contra los nuevos codigos o contra aquellos que no han sido aun reportados. Para revertir esta brecha los fabricantes han desarrollado alternativas varias según cada producto se denomina por ejemplo: la heurística que son algoritmos con buenos tiempos de ejecución y buenas soluciones, usualmente las óptimas. Una heurística es un algoritmo que ofrece uno o ambos objetivos. Estos complejos algoritmos matemáticos que intentan anticiparse a las acciones que pudiera efectuar un código determinado si éste fuera ejecutado; la inoculación al método por el cual este antivirus toma las características principales de los sectores de booteo y archivos para luego chequear su integridad u otros algoritmos inteligentes de evaluación.

Algunas herramientas utilizan una lista negra donde definen que clase de archivos no están permitidos por la politica de seguridad y estos son rechazados. Pero esta alternativa puede resultar compleja de manejar debido a que la lista de archivos nocivos es extremadamente numerosa y hay que añadir las nuevas versiones que a diario se reportan, de modo que mantenerla actualizada puede resultar una labor difícil de cumplir. En contra parte existe la lista blanca que no es sino la lista de todos aquellos archivos y aplicaciones permitidas por ser útiles, necesarias y no dañinas al sistema. De cualquier modo la combinación adecuada de las mencionadas técnicas es la solución más efectiva. Por

ejemplo si una extensión altamente usada en la compañía es la “*.abc” se la debe incluir en la lista blanca pero si se esparce un virus bajo el nombre “destuctor.abc” podemos incluir el nombre especifico a ser filtrado en la lista negra. Las derivaciones de los códigos maliciosos mas comunes son encuentran los virus, troyanos, spams, vándalos, etc.

2.5.5 Software Malicioso

El software malicioso o también conocido como Malware son software de aplicación derivados de un código malicioso y cumplen las diversas funciones que este tipo código le ordena. El Malware incluye viruses, adware, y spyware. Lo que tienen en común todos estos desarrollos de software es que se instalan en los ordenadores sin autorización ni notificación alguna.

2.5.5.1 Virus

Son bits de un código malicioso, usualmente inofensivo a primera vista que se instala el mismo en un ordenador luego de ser activado por alguna aplicación del usuario.

El término virus esta mal concebido por la mayoría de usuarios de redes para definir un amplio rango de códigos maliciosos, aunque muchos de ellos técnicamente según su clasificación no sean virus.

Desarrollar virus según normas internacionales esta tipificado como un crimen. Leyes contra virus han sido expedidas por ejemplo la Electronic Privacy Act en 1986 para los Estados Unidos de América y The Computer Misuse Act en 1991 para Europa.

Algunos virus pueden necesitar de ayuda para esparcirse y otros lo pueden hacer por si mismos pero siempre sin autorización ni notificación.

Los virus tienen una fase de infección que es donde se instala y produce su reproducción y la fase de ataque que es donde comienzas a causar danos al sistema. También son el método numero uno en el mundo de vandalismo informático con nuevos cientos identificados cada día. Al momento se han reportado mas de 250000 virus con niveles de daño tan variados como puede ser ningún daño, mensajes de humor mostrados por pantalla, datos alterados, o colapso daño total del sistema.

Existe una clasificación definida de los diversos tipos de virus y son:

Virus contaminadores de archivos, gusanos, troyanos, macro virus, virus de booteo, Stealth virus, virus polimorfitos, multipartite virus, software invasivo.

2.5.5.1.1 Virus Contaminadores de Archivos

Son los más populares de la familia de los virus, ellos infectan archivos ejecutables al añadir su propio código sobre el código original del archivo. Al no poder ejecutarse por si mismos necesitan de una aplicación “detonante” que los active para comenzar la infección del dispositivo, este detonante puede ser un ejecutable cualquiera como un juego o algún archivo adjunto en un e-mail. Su contaminación se esparce y repite con cada transferencia entre dispositivos.

Hay una variedad de esta clase de virus que no infecta el ejecutable por necesitarlo para su expansión, en su lugar infecta archivos del tipo *.DLL que es el tipo de archivo que un ejecutable llama para su ejecución.

2.5.5.1.2 Gusanos

Son virus autoreproductivos, a diferencia del resto de virus estos no dependen de ningún tipo de transferencia de archivos para reproducirse. Un gusano es un ente autónomo que generalmente se valen de e-mails (utilizando la lista de contactos del usuario) y medios no tradicionales programas de

mensajeria instantánea o programar P2P de transferencia de datos como medio de transporte.

Muchos de los nuevos virus que causan noticia son gusanos. En agosto del 2003 el gusano blaster colgó muchas redes corporativas, afectó el control de trafico aéreo en Estados Unidos y saboteo la red de la marina de USA (NMCI); en septiembre del 2003 el gusano Swen infecto un millón y medio de computadoras y colgó servidores de e-mail fingiendo ser un parche de Microsoft® afectando incluso a usuarios no infectados, para citar 2 ejemplos.

2.5.5.1.3 Troyanos

Son software de aplicación, casi siempre un juego o una utilidad que aparenta realizar únicamente su actividad pero en realidad conlleva otra incorporada subrepticiamente que se encarga del daño, transfiere información sobre el sistema infectado o permite el acceso para el creador hacia el ordenador. Los troyanos no se auto reproducen y técnicamente no son un virus pero guardan una estrecha relación. A saber, comúnmente son parte de virus híbridos o multipartitud. Los troyanos pueden ser plantados por gusanos durante su fase de infección o pueden llevar incorporados un virus. Algunas veces

pueden causar danos visibles pero otras pueden parecer programas legítimos haciendo que imperceptibles sus acciones destructivas. Muchos troyanos son utilizados para espiar las actividades personales y robar información, pero, a menos que se trate de un servidor o base de datos de un alto valor informático, los hackers no se encuentran en absoluto interesados en aquellas actividades personales sino que buscan un computador con una permanente conexión de banda ancha para distribuir pornografía, spam, o lanzar DoS Distribuido. Esto no tiene otra explicación sino que una vez que el hacker ha desenvuelto un largo historial delictivo se vuelven blanco reconocido para las seguridades de los ISP y de los filtros de servidores. Una vez que detecta los PCs con las condiciones mencionadas obtiene un aliado ideal en sus ataques, anónimo y altamente eficiente. Esto vuelve al hacker casi imposible de rastrear.

El funcionamiento de un troyano puede ser tan bueno que si no se lo busca quizás nunca se percate de su existencia. Un ejemplo conocido de troyanos es el Backdoor Trojan que permitía al hacker acceder al ordenador a traves del IRC (Internet Relay Chat).

2.5.5.1.4 Macrovirus

Una aplicación macro es un conjunto de instrucciones de un programa que el administrador asigna a un pequeño código clave (key code) de modo que al tipear el código clave en el programa empiezan a ejecutarse todas las actividades dispuestas en la configuración. Los macro pueden simplificar de gran manera las operaciones del día a día al configurar, grabar y repetir a voluntad todas las labores en lugar de realizarlas una a una.

Muchos programas permiten extender el lenguaje macro con lenguajes de programación mucho más complejos para poder configurar rutinas complejas tan solo como un macro. Estos procedimientos no son solo posibles sino que es muy sencillo crear o modificar virus existentes. Los macros son extremadamente comunes en los formatos de Microsoft Excel® y Microsoft Word® con millares de variantes ya que son archivos que se intercambian entre usuarios frecuentemente (no como los ejecutables). Existen macros que, en el mismo modo que los gusanos, se esparcen a si mismos vía e-mail hacia todas las direcciones de la lista de contactos. Adicionalmente como los macros se divulgan con cada

documento pueden también divulgarse entre sistemas operativos que bien pueden ser de una PC hacia una Mac®.

Los macro se activan cuando el documento es abierto y, como todos los virus, su nivel de daño es variable. Un caso de macro virus fue el Melissa y consistía en auto propagarse en un e-mail con asunto “Importan Mézale ROM (mensaje importante de) <nombre del usuario>” con un documento de Word adjunto. El cuerpo del mail decía “Here is that document you asked for... don’t show anyone else ;-) (Aquí esta el documento que solicitaste… no se lo muestres a nadie)” y cuando la victima lo confundía con un correo amigable lo abría y comenzaba su infección para luego continuar la cadena hacia todos sus contactos.

2.5.5.1.5 Virus Booteables (De Arranque)

Estos virus se encuentran en el sector de arranque del disco duro (MBR, Master Boot Record) sobrescribiendo el código original de arranque. El MBR reside en los primeros sectores del disco duro y controlan la secuencia de arranque al encender el computador. Los virus de arranque son especialmente peligrosos ya que cada vez que se enciende el ordenador se cargan en la memoria de donde pueden migrar a otros sectores del mismo disco duro o de otro. Casi siempre causan falla del

sistema donde el ordenador no puede inicializarse o encontrar el disco duro. Cuando un sector de arranque (boot sector) o de arranque maestro (MBR) ha sido infectado, es preferible restaurar el sector desde algún respaldo, puesto que en ocasiones, los sectores de arranque genéricos utilizados por los antivirus no son perfectamente compatibles con el sistema operativo instalado. Además, los virus no siempre dejan un respaldo del sector original donde el antivirus espera encontrarlo. Antes de restaurar los respaldos es importante no olvidar apagar la computadora por más de cinco segundos y arrancar desde el disco libre de virus.

2.5.5.1.6 Stealth Virus

El virus es un pequeño software (cuanto más pequeño más fácil de esparcir y más difícil de detectar), que permanece inactivo hasta que un hecho externo hace que el programa sea ejecutado. De esa forma el programa del virus es activado y se carga en la memoria RAM de la computadora, desde donde puede esperar otro evento que dispare su sistema de destrucción o se replique a sí mismo o comenzar automáticamente luego de ser ejecutado. Los virus de acero poseen un módulo de defensa que tiene, obviamente, la misión de proteger al virus. Sus rutinas apuntan a evitar todo aquello

que provoque la remoción del virus y retarda, en la medida de sus posibilidades su detección.

Los virus pueden llegar a mutar "camuflarse" y esconderse para evitar la detección y reparación. Como lo hacen:

- ✓ El virus re-orienta la lectura del disco para evitar ser detectado;
- ✓ Los datos sobre el tamaño del directorio infectado son modificados en la FAT, para evitar que se descubran bytes extra que aporta el virus;
- ✓ Encriptación: el virus se encripta en símbolos sin sentido para no ser detectado, pero para destruir o replicarse DEBE desencriptarse siendo entonces detectable;
- ✓ Subrepticio: pueden ocultarse incluso a nivel de consumo de memoria.
- ✓ Polimorfismo: mutan cambiando segmentos del código para parecer distintos en cada "nueva generación", lo que los hace muy difíciles de detectar y destruir;
- ✓ Gatillables: se relaciona con un evento que puede ser el cambio de fecha, una determinada combinación de tecleo; un macro o la apertura de un programa asociado al virus (Troyanos).

2.5.5.1.7 Virus Polimorfitos

Esta clase de virus intenta defenderse de los software de escaneo de software al usar un algoritmo para encriptarse a si mismo cada vez que infecta un nuevo host. Así el virus encriptado elude el escaneo inicial pero luego se desencripta para infectar el computador, entonces dificulta su detección ya que varia constantemente su firma de desarrollo. Algunos polimorficos mas sofisticados varían incluso sus métodos de encriptación haciendo de este modo su detección mucho más complicada aún.

2.5.5.1.8 Multipartitude Virus

Esta clase de virus son híbridos, suelen ser una combinación de virus contaminadores de archivos y los virus booteables de modo que infectan tanto el sistema de arranque como los archivos. Son especialmente difíciles de encontrar ya que su desarrollo es muy complejo pero cuando son detectados su poder destructivo tiende ser muy alto.

2.5.5.2 Adware

El adware es adquirido cuando el usuario descarga desde Internet software denominado Freeware o Shareware y no es más que aquel software disponible en la red para descargas gratuitas o por

cantidades irrisorias. Este tipo de programas regularmente poseen adware oculto pero existen casos en que inclusive programas comercializados tradicionalmente lo llevan oculto. El escenario común es que al escoger un programa de descarga gratuita, puede ser un juego o una aplicación muy útil, antes de descargarlo el site presenta las condiciones de uso y entrelineas solicita el permiso para la instalación y uso del adware inadvertido, la lectura de estas condiciones de uso son siempre omitidas por el lector confiando en que los desarrolladores no tienen otra intención sino la de ayudar a los navegantes de la red y por ende aceptan todos los términos presentados facultando incluso legalmente al fabricante para ejecutar el mencionado adware en toda su magnitud. Pronto y sin razón aparente comienza a incrementarse la presencia de popups y de entonces no pasara mucho tiempo hasta que el host empiece a reportar el historial de navegación hacia el fabricante del adware.

Cada día miles y miles de usuarios descargan e instalan software con términos que no entienden o aun peor, que nunca leen. A consecuencia miles de hosts descargan involuntariamente software que afecta el normal desempeño de los ordenadores.

Pero existe también adware producido legítimamente y con fines probos, son honestos y exponen claramente al usuario que tipo de

actividades desempeñan, como lo hacen y con que fines. Podemos mencionar como ejemplo el Gator una aplicación que ayuda al usuario a llenar formas de topo tipo en la Web. Gator informa, sin tratar de burlar al usuario, que conlleva adware y cual es su funcionamiento, incluso el adware instala un icono de acceso directo en el escritorio del PC y explica como ser removido en caso que el usuario no este interesado en usarlo mas.

2.5.5.3 Spyware

Tal como el Adware se puede descargar oculto en otros software de aplicación pero la diferencia se da en que el Spyware se infiltra en los ordenadores sin siquiera molestarse en solicitar permiso, de ningún tipo, en ninguna forma. Ni tan siquiera entrelineas con letra menuda ni con artificios que puedan interpretarse como autorización en lo posterior. Su descarga e instalación es arbitraria. Tan arbitrario puede resultar este software que incluso se puede inhalar con solo visitar un portal Web de la misma manera que se instalan los coolíes y a veces como una aplicación más.

La mayoría de Spyware se clasifica como variantes de gusanos, troyanos y stealth virus ya que se ocultan y dificultan su detección y erradicación. Aquellos con un modulo de defensa más avanzado se posesionan como parte del sistema operativo del PC.

Aunque varias de sus funciones se asemejan al Adware como añadir add ons en el navegador de red el Spyware va más allá en su comportamiento antisocial. Los niveles de daño más bajos suelen alterar la configuración de la página de inicio del navegador, aumentan en la escala de danos y van desde enviar información personal a terceros, modificar archivos, activar “Key logging” que son aplicaciones que almacenan y transfieren todo aquello que es tapeado por el usuario incluyendo desde luego direcciones de correo y sus claves, mensajes de correo electrónico, números de tarjetas de crédito etc. Algunos incluso invaden la privacidad física espiando a traves de la cámara Web del mismo computador.

2.5.5.4 Otras clases de software invasivo

Existen miembros menos conocidos de la familia de Software malicioso pero no menos perturbador. Se puede mencionar por ejemplo:

- ✓ Scumware._ Software diseñado para hurtar trafico, datos e incluso dinero desde legítimos Web sites.
- ✓ Drug Dealer Ware._ Ofrece software de descarga sin costo alguno para luego demandar dinero declarándose perjudicados por el tiempo de uso de su software propietario (tipo software que se

comercializa bajo la venta de licencia de uso) sin haber percibido remuneración por derechos de autor.

- ✓ Theftware hijacks._ Alteran las paginas Web reemplazando los ads de la pagina original por los suyos.

Todas estas clases de software arriban a los computadores, incluso a veces con autorización involuntaria previa, y se dedican a desarrollar sus actividades como llenar la pantalla con ads, enviar información sobre el user a traves del Internet, reducir memoria y disminuyendo la velocidad de procesamiento o causando conflictos en el sistema operativo. También pueden compararse con Troyanos o Stealth virus que se infiltran y rehúsan su eliminación por todos los medios a su alcance. Es una muestra más de las miles de contaminaciones que se dan a diario a traves del Internet y que deben hacer mentir un poco más a los navegantes sobre si saben en realidad que es lo que están buscando y que necesitan o no descargar.

CAPITULO 3

3. ANALISIS DE VULNERABILIDADES

Este capitulo de forma general se encamina al análisis de toda la red, para poder así tener la certeza de en que puntos tenemos un alto grado de seguridad y conocer aquellos que se presenten como los más sensibles a ataques, como prevenir éstos y que hacer en caso de que ocurran.

3.1 REVISION DE POLITICAS

En el mercado existen diferentes herramientas para analizar vulnerabilidades de una red. Estas herramientas son muy útiles, para los administradores de red preocupados por al seguridad e integridad de su red y la información que en ella manejan.

Podemos citar varios analizadores, entre ellos se puede encontrar NESSUS y SATAN, los cuales ofrecen una amplia gama de reglas para evaluar las vulnerabilidades y además permiten la incorporación de nuevas reglas para hacer más riguroso y específico el análisis. Sin embargo, estas herramientas se convierten en armas de doble filo, pues pueden ser usadas con el objetivo de mejorar la seguridad de la red o pueden ser usadas por hackers con el objetivo de detectar vulnerabilidades y realizar ataques.

Internet ha facilitado y promovido el desarrollo de las comunicaciones a nivel global en los últimos años. Este aumento en la comunicación, ha estado fuertemente ligado al desarrollo de nuevas redes y nuevas aplicaciones que permiten compartir más información entre usuarios remotos. Ha surgido en las empresas, la importante función de los administradores de red, los cuales deben promover un uso correcto de la red y a su vez garantizar la seguridad y confidencialidad de la información que manejan. Sin embargo, cada día aumentan los ataques contra redes y contra computadores conectados a la red. “La omnipresencia de Internet los está volviendo [virus] pan de cada día y están aumentando su poder”. El nivel de sofisticación de estos ataques es cada vez mayor, lo cual exige el desarrollo y actualización de herramientas pertinentes.

Se puede por tanto evidenciar, la gran importancia de desarrollar mecanismos de autoprotección contra estos ataques, los cuales deben pasar por una fase de identificación de los potenciales riesgos a los que se está expuesto, luego a una fase de análisis de las debilidades para posteriormente definir acciones de mejora y defensa así como planes de mitigación ante sucesos indeseables.

En las etapas de identificación y análisis, los Analizadores de Vulnerabilidades juegan un papel fundamental para una clara y eficaz detección de falencias en seguridad. Se debe tener un horizonte claro de lo que deseamos establecer como parámetros a conseguir con el uso de los Analizadores, a continuación se detallan éstos:

- ✓ Conocer a que llamamos una vulnerabilidad y como se hacen los análisis.
- ✓ Saber cuales son las herramientas existentes para realizar análisis de vulnerabilidades.
- ✓ Para cada herramienta, entender como funciona, cuales son sus características y funcionalidades.
- ✓ Estar al tanto de como cada herramienta analizadora de vulnerabilidades genera reportes o información importante para el análisis de los riesgos de una red.

Las vulnerabilidades de un sistema surgen a partir de errores individuales en un componente, sin embargo nuevas y complejas vulnerabilidades surgen de la interacción entre varios componentes como el kernel del sistema, sistemas de archivos, servidores de procesos, entre otros. Estas vulnerabilidades generan problemas de seguridad para la red en cuestión. Entre las más conocidas se encuentran el “finger username” y la notificación de mensajes de correo a través de “comsat”. Para el primero de estos la vulnerabilidad es originada en la interacción entre el servidor fingerprint y la forma en que el sistema de archivos representa los links para acceder al directorio raíz de username. En el segundo caso el programa comsat supone que etc/utmp es correcto, el sistema de archivos configura este archivo para otorgar permisos y el programa de correo asume que todo esta correcto. Sin embargo, existen fuertes críticas sobre los analizadores de vulnerabilidades ya que funcionan bajo un esquema de reglas, que son sólo generadas por expertos en el tema y que se configuran para vulnerabilidades. La posibilidad de acceder a estas reglas y conocerlas, permite que personas malintencionadas realicen ataques contra redes no protegidas para estas vulnerabilidades. Adicionalmente, la identificación y definición de reglas se deja en manos de expertos que puedan comprender las interacciones de las cuales surgen las

vulnerabilidades.

Por otra parte, aunque existen diversas formas de realizar auditorias de seguridad apoyadas en las herramientas descritas anteriormente, en todos los casos se utilizan herramientas para la detección de las vulnerabilidades. Estas herramientas que detectan fallas de seguridad pueden ser utilizadas de dos formas diferentes: interna o externamente a la maquina que se analiza. Cuando se aplican internamente, se realiza la auditoria desde el interior de la máquina (generalmente utilizando el súper usuario), lo que otorga numerosas ventajas críticos del sistema. En el caso de las auditorias externas, la detección de vulnerabilidades se realiza desde una máquina diferente a la que está siendo analizada. En este tipo de auditorias se realizan ataques para verificar la existencia de vulnerabilidades. De la variedad y cantidad de ataques que alguna de estas herramientas sea capaz de realizar, dependerá, en gran parte, el éxito en la detección de vulnerabilidades. Aunque este factor es, probablemente, el más importante, conviene considerar otros aspectos como por ejemplo la forma de realizar los ataques.

3.2 HERRAMIENTAS PARA ANALISIS DE RED

3.2.1 CISCO AUTOSECURE

Cisco IOS AutoSecure: Esta innovadora característica basada en interfaz de comando-en-línea (CLI) del Software Cisco IOS, hace posible cerrar un router “con un solo botón”. Un solo comando transforma instantánea y fácilmente las configuraciones de seguridad del router al desarmar procesos no esenciales del sistema operativo, obligando el acceso seguro y habilitando las características de salida segura.

3.2.2 CISCO OUTPUT INTERPRETER

Esta es propiamente la herramienta que nos permitirá de modo sencillo y sin demasiadas complicaciones analizar de modo completo el resultado de la ejecución de un comando show o debug. Esta herramienta nos permite revisar tanto el resultado de la ejecución de comandos show como debug. En la misma página de acceso se ofrece una lista de los comandos soportados. Es ciertamente muy útil y fácil de utilizar. Todo lo que requiere es que se copie y pegue el resultado de la ejecución de un comando show en la ventana que se presenta con ese propósito específico. No es una herramienta nueva, pero si es renovada permanentemente ya que de

modo continuo se incorporan nuevos comandos que pueden ser "traducidos" por este intérprete.

Al momento de utilizar la herramienta tenga en cuenta los siguientes "tips":

- ✓ Asegúrese de que está copiando el resultado de la ejecución del comando completa y que el comando se encuentra en la lista de comandos soportados.
- ✓ En la ventana se pueden ingresar los resultados de varios comandos show que se han ingresado secuencialmente, o también se puede subir un archivo de texto que contenga la misma información utilizando la ventana de diálogo que se presenta con ese propósito.
- ✓ No se debe esperar a tener un problema serio para ensayar esta herramienta. Se debe ingresar, tomar al menos un archivo de configuración y un show interfaces serial y realizar el ejercicio. Esto ayudará a conocer la herramienta y la información que ésta proporciona.

Entre la información que se puede obtener con esta herramienta encontrará:

- ✓ Una lista de errores, advertencias, notas sobre estado y referencias útiles.
- ✓ Para cada comando IP que recomienda, proporciona el enlace a la explicación del mismo.
- ✓ Cuando corresponde (por ejemplo, al analizar una configuración), realiza un análisis sobre las prestaciones de seguridad y NAT; sugerencias de seguridad; recomendaciones para mejorar la performance.

Sin dudas que es una herramienta útil para el análisis de cualquier comando de monitoreo, mientras se encuentre en la lista de comandos soportados. Más allá de esto, se detalla una lista de los comandos en los que ésta herramienta puede ser usada más frecuentemente:

- ✓ show running-config
- ✓ show interfaces
- ✓ debugs
- ✓ show controllers
- ✓ show diag
- ✓ show version
- ✓ show process cpu

- ✓ show memory

Es muy buena, no sólo porque ayuda a interpretar el resultado de estos comandos, sino también porque aporta una cantidad de ideas y sugerencias muy importantes para mejorar el rendimiento y performance de los dispositivos de la red.

3.2.3 GUÍAS DE LA NSA Y CRSG (CISCO ROUTER SECURITY GUIDES).

Éste artículo es un suplemento de la Guía de Seguridad para la configuración del Router NSA/SNAC versión 1.1. Este describe rápidamente pero de formas efectivas como aseverar la seguridad de un router Cisco, con algunos principios generales importantes para mantener la buena seguridad del router. Para más información, se detallan las recomendaciones de cada sección en ésta guía.

Recomendaciones Generales

1. Crear y mantener una política escrita de seguridad para el router. La política debería identificar quien está autorizado para acceder al router, quién lo está para configurarlo y modificarlo, y delimitar el acceso y prácticas administrativas para ello.

2. Comentar y organizar sin estar conectado ediciones maestras de tus archivos de configuración del router. Este sondeo molestará a pesar de ser un gran triunfo de seguridad. También, mantener las copias fuera de linea de todas las configuraciones de router en sincronía con las configuraciones actuales que están corriendo en los routers. Esto es invaluable para diagnosticar ataques sospechosos y recuperarse de ellos.

3. Las listas de implementos de acceso que permiten sólo éstos protocolos, puertos y direcciones IP que son requeridos por los usuarios de la red y sus servicios, y que niegan todo.

4. Trabajar con la última versión disponible de Despliegue General (GD).

5. Probar la seguridad de sus routers regularmente, especialmente después de cualquier cambio de configuración considerable.

Recomendaciones Específicas: Acceso al Router

1. Reduce los servicios innecesarios en el router. Los servidores que no estén funcionando no pueden descansar. También, más memoria y procesadores particionados son accesibles. Empezar a correr el comando *show proc* en el router, entonces apagar cuidadosamente facilidades y servicios innecesarios. Algunos servidores que estarían apagados casi todo

el tiempo, y sus correspondientes comandos para desactivarlos están enlistados abajo.

- ✓ **no service tcp-small-servers (sin servicio a servidores tcp)**
- ✓ **no service udp-small-servers (sin servicio a servidores udp)**

BOOTP	**- no ip bootp server**
Finger	**- no service finger**
HTTP	**- no ip http Server**
SNMP	**- no snmp-server**

Tabla VI: Comandos de desactivación en servidores

2. Reducir servicios innecesarios en los routers. Estos servicios permiten que paquetes seguros atraviesen el router, ó el envío de paquetes especiales, o son usados para la configuración remota del router. Algunos servicios que estarían apagados casi todo el tiempo, y sus correspondientes comandos para desactivarlos están enlistados abajo.

- ✓ CDP **- no cdp run**
- ✓ Configuración remota. **- no service config**
- ✓ Ruteando recursos **- no ip source-route**

3. Las interfaces en el router pueden ser hechos más seguras al usar comandos seguros en el modo de Configuración de la interfaz. Estos

comandos serían aplicados para cada interfaz.

- ✓ Interfaces no usadas **- shutdown**
- ✓ No ataques maliciosos **- no ip directed-broadcast**
- ✓ Respuesta de mascara **- no ip mask-reply**
- ✓ Ruteando Ad-hoc **- no ip proxy-arp**

4. La línea de consola, la línea auxiliar y las líneas de terminales virtuales en el router pueden ser hechos de forma segura en el modo de Configuración de Línea. La línea de consola y las líneas de terminales virtuales estarían seguras como se muestra abajo. La línea auxiliar estaría desactivada, como abajo se muestra, si no está siendo usado.

Tarjeta del Sumario Ejecutivo

Linea de Consola **- line con 0 exec-timeout 5 0 login**

Linea Auxiliar **- line aux 0 no exec exec-timeout 0 10 transport input none**

Lineas VTY **- line vty 0 4 exec-timeout 5 0 login transport input telnet ssh**

5. Contraseñas pueden ser configuradas más seguramente. Configurar la activación de contraseñas secretas, la cual está protegida con un algoritmo basado en MD5. También, configurar contraseñas para la línea de consola,

la línea auxiliar y las líneas de terminales virtuales. Proveen protección básica para el usuario y las contraseñas usando el comando *service password-encryption***.** Se ven ejemplos en la parte inferior.

- ✓ Activar secretamente **- enable secret 0 2manyRt3s**
- ✓ Linea de Consola **- line con 0 password Soda-4-jimmY**
- ✓ Linea Auxiliar **- line aux 0 password Popcorn-4-sara**
- ✓ Lineas VTY **- line vty 0 4 password Dots-4-georg3**
- ✓ Protección básica **- service password-encryption**

6. Considerar la adopción de SSH, si tu router lo soporta, para toda la administración remota.

7. Protege tu archivo de configuración del router desde una ubicación no autorizada.

Recomendaciones Específicas: Listas de Acceso

1. Siempre empieza la definición de una lista de acceso con el comando privilegiado *no access-list nnn* para eliminar cualquier versión previa de los números nnn de las listas de acceso.

East (config) # **no access-list 51**

East (config) # **access-list 51 permit host 14.2.9.6**

East (config) # **access-list 51 deny any log**

2. Cargar la lista de acceso del puerto de mensajes apropiadamente. Para asegurar que los accesos contienen información correcta del número del puerto, usa los argumentos del puerto de rangos mostrados debajo del fin de la lista de accesos.

access-list 106 deny udp any range 1 65535 any range 1 65535 log
access-list 106 deny tcp any range 1 65535 any range 1 65535 log
access-list 106 deny ip any log

La última línea es necesaria para asegurar que los paquetes de otros protocolos rechazados como TCP y UDP sean apropiadamente registrados.

3. Reforzar las restricciones de tráfico de direcciones usando listas de acceso. En un router perimetral, permitir solo direcciones internas para acceder al router desde las interfaces internas, y permitir solo tráfico destinado para direcciones internas para acceder al router desde fuera de la red (interfaces externas). Bloquear direcciones ilegales de las interfaces externas. Para prevenir un ataque usando el router para atacar otros sitios, esto ayuda a identificar pobres configuraciones internas de usuarios o de la

red. Esto detalle podría no ser sencillo para redes complicadas.

East (config) # **no access-list 101**

East (config) # **access-list 101 permit ip 14.2.6.0 0.0.0.255 any**

East (config) # **access-list 101 deny ip any any log**

East (config) # **no access-list 102**

East (config) # **access-list 102 permit ip any 14.2.6.0 0.0.0.255**

East (config) # **access-list 102 deny ip any any log**

East (config) # **interface eth 1**

East (config-if) # **ip access-group 101 in**

East (config-if) # **exit** East (config) # **interface eth 0**

East (config-if) # **ip access-group 101 out**

East (config-if) # **ip access-group 102 in**

4. Bloquear paquetes que vengan desde fuera (redes no confiables) que son obviamente peligrosos o tienen recurso o dirección de destino que son

reservados, redes de ejemplo 0.0.0.0/8, 10.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.168.0.0/16. Esta protección debería ser parte de todo el tráfico filtrado hacia la interface atacada desde redes no confiables.

5. Bloquear paquetes entrantes que tengan una dirección de recurso de cualquier red interna (confiable). Esto impide el adivinar secuencias numéricas de TCP y otros ataques. Incorporar esta protección a las listas de acceso aplicadas a las interfaces encara cualquier red no confiable.

6. Rechazar paquetes entrantes con direcciones de lazo, red 127.0.0.0/8. Estos paquetes pueden ser falsos.

7. Si la red no necesita IP multicast, entonces se debe bloquear los paquetes multicast.

8. Bloquear paquetes broadcast. (Nótese que esto podría bloquear servicios DHCP y BOOTP, pero estos servicios no deberían ser usados en interfaces externas y ciertamente no cruzarían routers perimetrales).

9. Un numero de pruebas remotas y ataques usan ICMP, redirigen y enmascaran mensajes de búsqueda, bloquéenlos. (Un superior pero más difícil detalle es para permitir solo paquetes de tipo ICMP necesarios.) El ejemplo detallado a continuación muestra una forma para implementar estas

recomendaciones.

North (config) # **no access-list 107**

North (config) #! **block our internal addresses**

North (config) # **access-list 107 deny ip 14.2.0.0 0.0.255.255 any log** North (config) # **access-list 107 deny ip 14.1.0.0 0.0.255.255 any log**

North (config) #! **block special/reserved addresses**

North (config) # **access-list 107 deny ip 127.0.0.0 0.255.255.255 any log** North (config) # **access-list 107 deny ip 0.0.0.0 0.255.255.255 any log**

North (config) # **access-list 107 deny ip 10.0.0.0 0.255.255.255 any log** North (config) # **access-list 107 deny ip 169.254.0.0 0.0.255.255 any log** North (config) # **access-list 107 deny ip 172.16.0.0 0.15.255.255 any log** North (config) # **access-list 107 deny ip 192.168.0.0 0.0.255.255 any log**

North (config) #! **block multicast (if not used)**

North(config)# **access-list 107 deny ip 224.0.0.0 15.255.255.255 any** North(config)# **! block some ICMP message types**

North (config) # **access-list 107 deny icmp any any redirect log**

North (config) # **access-list 107 deny icmp any any echo log**

North (config) # **access-list 107 deny icmp any any mask-request log**

North (config) # **access-list 107 permit ip any 14.2.0.0 0.0.255.255**

North (config) # **access-list 107 permit ip any 14.1.0.0 0.0.255.255**

North (config) # **interface Eth 0/0**

North (config-if) # **description External interface**

North (config-if) # **ip access-group 107 in**

10. Bloquear paquetes entrantes que parezcan tener el mismo destino y fuente de dirección. Incorporar esta protección a la lista de acceso para restringir tráfico entrante a cada interface, usando una regla como la abajo mostrada.

access-list 102 deny ip host 14.1.1.250 host 14.1.1.250 log

interface Eth 0/1

ip address 14.1.1.250 255.255.0.0

ip access-group 102 in

11. Configurar una lista de acceso para las lineas de terminales virtuales para controlar los accesos Telnet. Ver ejemplos de comandos abajo.

South (config) # **no access-list 92**

South (config) # **access-list 92 permit 14.2.10.1**

South (config) # **access-list 92 permit 14.2.9.1**

South (config) # **line vty 0 4** South (config-line) # **access-class 92 in**

Carta de Sumario Ejecutivo

Recomendaciones Especificas: Accesando y Desconectando

1. Encender la capacidad de acceso del router, y usarlo para detectar errores y bloquear paquetes desde el servidor interno (confiable). Estar seguro que el router bloquee el tráfico desde redes no confiables. Ver ejemplo de comandos debajo.

Central (config) # **logging on**

Central (config) # **logging 14.2.9.1**

Central (config) # **logging buffered 16000**

Central (config) # **logging console critical**

Central (config) # **logging trap informational**

Central (config) # **logging facility local1**

2. Configurar el router para incluir información a tiempo en el acceso. Configurar al menos dos diferentes servidores NTP para asegurar confiabilidad de la buena información de tiempo. Esto permitirá al administrador trazar ataques a la red más acuciosamente. Ver ejemplos a continuación.

East (config) # **service timestamps log datetime localtime show-timezone msec**

East (config) # **clock timezone GMT 0**

East (config) # **ntp server 14.1.1.250**

East (config) # **ntp server 14.2.9.1**

3. Si tu red requiere SNMP, entonces configura el SNMP ACL y cadenas de comunidades SNMP difíciles de adivinar. Los ejemplos de comando debajo muestran como cambiar la cadena de comunidades iniciales y establecer

una mejor cadena de comunidades de solo lectura con un ACL.

East (config) # **no snmp community public ro**

East (config) # **no snmp community private rw**

East (config) # **no access-list 51**

East (config) # **access-list 51 permit 14.2.9.1**

East (config) # **snmp community BTRl8+never ro 51**

Lista de chequeo para la seguridad del router

Esta lista de seguridad esta diseñada para ayudar a revisar tu configuración de seguridad del router, y recordarte cualquier area de seguridad que posiblemente hayas olvidado.

Políticas de seguridad del router deben ser escritas, aprobadas y distribuidas. La versión del Router IOS revisada y actualizada a la fecha. La configuración del router debe estar fuera de linea, realimentarse y ser de acceso limitado. Se debe documentar y comentar de buena forma la configuración del router. Los usuarios y contraseñas de routers deben estar

configurados y mantenidos. La encriptación de la contraseña en uso, activar secreto en uso Activar secretos difíciles de adivinar, el conocimiento de esto es estrictamente limitado (si no se debe cambiar inmediatamente la activación del secreto).

Restricciones de acceso impuestas en Consola, Auxiliar y VTYs.

Servidores de red innecesarios y facilidades desconectadas.

Servicios de red necesarios configurados correctamente (e.g. DNS)

Interfaces y VTYs sin uso se apagan o desconectan.

Servicios de interface de riesgo desconectados.

Puerto y protocolo necesarios de la red identificados y revisados.

Las listas de acceso limitan el tráfico para identificar puertos y protocolos.

Las listas de acceso bloquean direcciones reservadas e inapropiadas.

Configurar rutas estáticas donde sea necesaria.

Protocolos de ruteo configurados para usar mecanismos integrados.

Habilitar el acceso para usuarios que estén identificados y configurados.

Tiempo del router establecido cuidadosamente, mantenido con NTP.

Acceso necesita incluir consistente información de tiempo.

Accesos revisados, chequeados y archivados en concordancia con políticas locales.

SNMP desconectado o habilitado con buenas cadenas de comunidades y ACLs.

3.2.4 CISCO RAT

En los enrutadores de Cisco la seguridad y auditoria ha sido una tarea que siempre consume mucho tiempo. Hay muchos pasos requeridos para modificar la configuración por default de un enrutador Cisco. En el entorno de una gran red esto podría tomar varias horas para confirmar que los enrutadores son seguramente configurados. Imagina una herramienta que podría reducir esto a solo pocos minutos. El Centro para Seguridad de Internet (CIS) ha provisto una herramienta para hacer exactamente esto, la Herramienta de Auditoria para Enrutadores RAT (por sus siglas en ingles), fue diseñado para ayudar a auditar las configuraciones de los enrutadores Cisco rápida y eficientemente.

RAT establece una linea base para examinar la configuración de un Router Cisco. El nivel 1 es modelado en el Router Security Configuration Guide publicado por la Agencia Nacional de Seguridad de los Estados Unidos NSA (por sus siglas en ingles). La herramienta provee una lista de vulnerabilidades potenciales de seguridad descubiertas en un formato Fácil de leer. Este establece una lista de comandos para ser aplicados al router en orden para corregir los potenciales problemas de seguridad descubiertos.

Este capitulo discutirá la necesidad de una herramienta como rat y su función. La instalación y las secciones de la guía para una rápida Instalación proveen toda la información necesaria para empezar usando RAT. Para hallar mas detalles, se incluye una narrativa paso a paso para usar y configurar el RAT. Esto incluye casos de cómo reducir las vulnerabilidades de un nuevo router y como configurar la Instalación del RAT.

RAT es un programa PERL. Este consolida otros cuatro (4) programas PERL, los cuales son: snarf, ncat, ncat_report y ncat_config. Snarf es usado para descargar la configuración de archivos desde el router. Ncat

lee la base de reglas y la configuración de archivos y provee la salida en un archivo de texto. Ncat_report crea la pagina html desde los archivos de texto. Ncat_config es usado para establecer localización de la base de reglas. Todos los componentes de RAT poseen licencia bajo la Licencia Publica General GNU (por sus siglas en ingles). La licencia GNU es uno de los beneficios prominentes de RAT llevando consigo la posible modificación del programa. Las lineas de guía para el RAT obtienen su licencia de la NSA bajo los términos incluidos en el paquete de Instalación. Las reglas y los documentos de linea de base reciben su licencia de parte del CIS.

RAT establece una auditoria comparando textos alfanuméricos en la configuración del archivo desde el router con expresiones regulares en las reglas. Cada regla tampoco tiene requerimiento u obligación de un elemento de expresión regular. Basado en este elemento RAT determina si una regla es aprobada o fallida. Debido al uso o expresiones regulares, la regla base de RAT es extremadamente flexible. Actualmente CIS diferencia entre el Nivel 1 y el Nivel 2 de auditoria. El Nivel 1 de auditoria esta basado en las guías de NSA. El Nivel 2 incluye pruebas adicionales de diferentes fuentes incluyendo Cisco. La mayoría de las reglas se dan

para la protección del router. Hay sin embargo varias reglas que proveen protección limitada a las redes que sirven. Reglas adicionales pueden ser añadidas a la regla base con relativa facilidad. Esto permite a Rat trabajar con cualquier configuración.

Instalación

RAT funciona en Unix, Linux y en la plataforma de Microsoft con ActiveState o Cygwin. La herramienta puede ser descargada desde el Centro para Seguridad de Internet. La Instalación de rat es comúnmente simple y la documentación provista en el archivo INSTALL.txt es Fácil de seguir.

Antes de instalar RAT es importante decidir si snarf va a ser usado para descargar la configuración de archivos o si será provisto un archivo de texto que ya contenga las configuraciones. Para descargar las configuraciones es necesario proveer a snarf el usuario y contraseñas para el router. Como sugerencia para utilizar el archivo INSTALL.txt deja la paranoia al seguir la guía, y se debe pensar si es realmente seguro escribir las contraseñas del router en una herramienta gratuita. Si no puedes confirmar que la fuente del código para snarf es segura, es preferible bajar

los archivos de configuración de otra manera.

3.3 HERRAMIENTAS PARA ANÁLISIS DE HOST

El término host puede referirse a:

- ✓ A una máquina conectada a una red de ordenadores y que tiene un nombre de equipo (en inglés, *hostname*). Es un nombre único que se le da a un dispositivo conectado a una red informática. Puede ser un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc. Este nombre ayuda al administrador de la red a identificar las máquinas sin tener que memorizar una dirección IP para cada una de ellas.
- ✓ Por extensión, a veces también se llama así al dominio del equipo (Un dominio es la parte de una URL por la que se identifica al servidor en el que se aloja)
- ✓ También es el nombre de un fichero (fichero Hosts) que se encuentra en los ordenadores y resuelve algunos DNS.

3.3.1 NMAPS

El término escáner de puertos o **escaneo de puertos** se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un cortafuegos.

Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos. Es usado por administradores de sistemas para analizar posibles problemas de seguridad, pero también es utilizado por usuarios malintencionados que intentan comprometer la seguridad de la máquina o la red.

Existen varios programas escaneadores de puertos por la red. Uno de los más conocidos es Nmap, disponible tanto para Linux como Windows.

Rastreo de puertos TCP SYN scan

Para establecer una conexión normal TCP, es necesario seguir una negociación de tres pasos. Esta negociación es iniciada con un paquete SYN en la máquina de origen, al que la máquina de destinto corresponde con un paquete SYN/ACK, que es finalmente respondido por la máquina que inicia la conexión por un paquete ACK. Una vez que se han cumplido estos pasos, está hecha la conexión TCP.

Un rastreador de puertos envía muchos paquetes SYN a la máquina que se está probando, y mira de qué forma regresan los paquetes para ver el estado de los puertos en el destino, interpretándolos de la siguiente forma:

- Si al enviar un paquete SYN a un puerto específico, el destino devuelve un SYN/ACK, el puerto está abierto y escuchando conexiones. - En otro caso, si regresa un paquete RST, el puerto está cerrado. - Por último, si no regresa el paquete, o si se recibe un paquete ICMP Port Unreachable, el puerto está filtrado por algún tipo de cortafuegos. Haciendo este procedimiento para una lista de puertos conocidos, se logra obtener un informe de estado de los puertos de la máquina probada.

3.3.2 NESSUS

NESSUS es definido por su autor como un escaneados remoto de seguridad. Este término aunque es muy adecuado, de ahora en adelante será referido como analizador de vulnerabilidades para evitar confusiones con otros analizadores de vulnerabilidades dentro de este paper. NESSUS es un proyecto fundado por Renaud Deraison que intenta crear un analizador de vulnerabilidades gratuito, poderoso, actualizado y fácil de utilizar. Este programa además es extensible, robusto, seguro, de propósito general (no está limitado a un solo tipo de vulnerabilidades) y más importante que cualquier otra característica, es su amplia aceptación por la comunidad. También puede llegar a ser una herramienta mortífera si se le da un mal uso, pero este no es su fin. A continuación se discutirá en detalle las características y el funcionamiento de NESSUS. Cabe aclarar que se trabajará en la última versión estable de NESSUS a la fecha de publicación de este paper (versión 2.0.10). Sin embargo muchas de las cosas aquí expuestas aplican para otras versiones tanto anteriores como posteriores.

A través de este paper se expondrán las características principales de Nessus, los resultados de sus escaneos y la veracidad de sus reportes.

Más que sus cualidades se intentará revelar sus defectos.

El paradigma de funcionamiento de NESSUS

Esta herramienta es bastante diferente a lo que se expone en este paper para el análisis de vulnerabilidades de una red en particular. Lo que se espera de un programa para efectuar ataques es simplemente un comando como *atacar-víctima* (Figura). NESSUS arroja esta concepción por la borda y toma una forma completamente distinta de hacer sus tareas. NESSUS fue diseñado para ser una herramienta distribuida (Figura) y de fácil administración. De esta forma un administrador de red puede efectuar su análisis de vulnerabilidades desde cualquier lugar del mundo pero desde el interior de su red. Esto se logra haciendo a NESSUS una herramienta cliente/servidor. El servidor espera solicitudes del cliente para llevar a cabo su análisis. Los ataques son efectuados desde el servidor y los resultados son enviados directamente al cliente. El cliente además es el responsable de la configuración y de la administración del servidor.

```
nessus-user@attacker.org>$ atacar-victima 192.121.211.10 > resultados.log
```

Figura 3.1 Este estilo de comando es el que se espera utilizar para una herramienta convencional de análisis de vulnerabilidades. NESSUS no trabaja de esta manera.

Esta característica de administración y ejecución remota permite que no solo pueda ejecutarse remotamente sin importar la plataforma en la que se ejecute el cliente, sino también hace a un lado la restricción del lugar desde donde se corra el cliente. Fácilmente el administrador de red puede correr NESSUS desde su casa, desde un avión, desde su celular, etc. Todo esto al costo de una instalación un poco compleja. Pero como todo lo bueno en la vida, esta característica tiene sus problemas y más adelante se expondrán los mismos. La instalación del servidor en plataformas Unix es muy sencilla, simplemente se necesita que libpcap esté instalado. La instalación de los clientes es aún más sencilla, ya que lo único que necesita la máquina en donde se instala es una conexión a Internet.

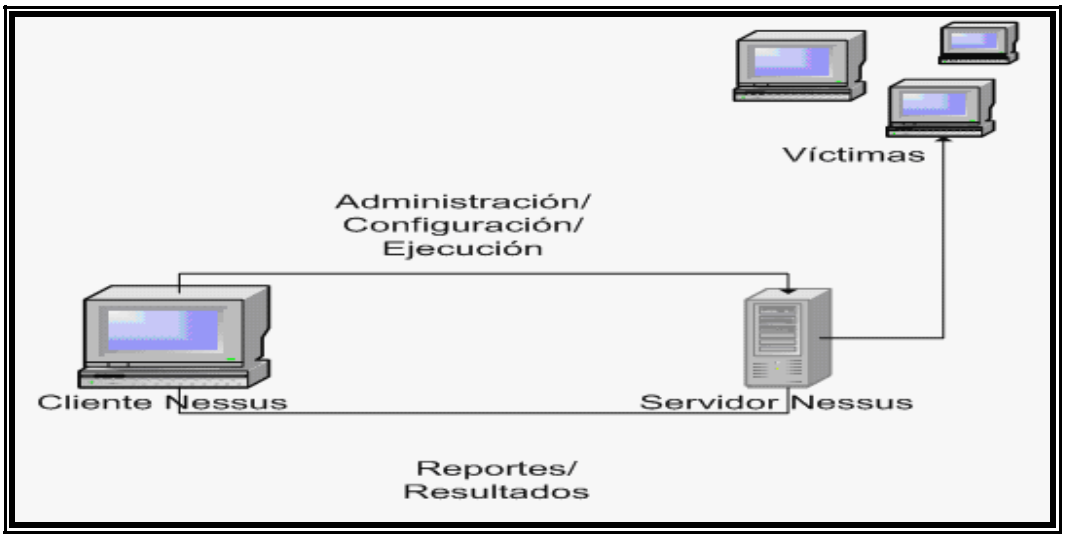


Figura 3.2 Funcionamiento de NESSUS.

En la figura superior se muestra como el cliente (Cliente NESSUS) puede configurar, administrar y ejecutar el servidor de NESSUS (Servidor NESSUS). El servidor de NESSUS puede ejecutar su análisis de vulnerabilidades sobre una o más víctimas especificadas por el cliente.

Cómo funciona

Ya se sabe cómo se distribuye Nessus y cómo se instala en una red. También se discutió sobre las ventajas de disponer a Nessus de esta manera. Ahora se discutirá cómo aprovecha esta disposición al máximo y qué es lo que puede hacer.

Manejo de usuarios

Nessus se vale del modelo cliente/servidor para su funcionamiento. El servidor se encarga de llevar a cabo los ataques, y el cliente se encarga de decirle al servidor qué debe hacer y cómo debe hacerlo. El servidor también se encarga de enviar los resultados al cliente, para que este provea el procesamiento necesario de los mismos. Está bien, un administrador puede ejecutar sus análisis desde cualquier parte del mundo, pero a su vez un atacante puede realizar estos ataques desde cualquier parte del mundo y sus análisis no serán atribuidos a él, sino a la

máquina que realizó los ataques, es decir, el servidor de Nessus. Por esta razón Nessus maneja sesiones de usuario independientes del sistema operativo en el que se ejecute (esto también lo hace más portable, ya que no se limita a un método de autenticación nativo). Un usuario puede ser autenticado a través de una contraseña, o bien, a través de un certificado digital. Además de la autenticación de la sesión, Nessus se vale de SSL para la encriptación del flujo de datos entre el cliente y el servidor. Para este fin se debe crear un certificado para el servidor. Este certificado es presentado al usuario para la posterior encriptación del flujo de datos. Nessus provee al usuario con herramientas tanto para la creación del certificado como para la creación de usuarios: nessus-mkcert y nessus-adduser, respectivamente.

La herramienta nessus-mkcert genera una entidad de certificación dentro del servidor y un certificado para el servidor. Un cliente también puede hacer uso de un certificado para la encriptación de datos, en cuyo caso la encriptación se dará en doble vía y no solo servidor-cliente. Nessus provee la herramienta nessus-mkcert-client para la creación del certificado del cliente.

Para que un usuario pueda llevar a cabo un análisis de vulnerabilidades,

es necesario que éste se autentique primero. Si el password o el certificado dado por el usuario no son válidos, el servidor de Nessus responderá con un error de autenticación, de lo contrario responderá con el certificado generado con nessus-mkcert para la posterior encriptación del flujo de datos entre servidor y cliente. A partir de este momento todo el tráfico entre servidor y cliente estará encriptado. Así todos los resultados enviados por el servidor son mucho más difíciles de descifrar sin el conocimiento de la llave utilizada en el algoritmo de encripción.

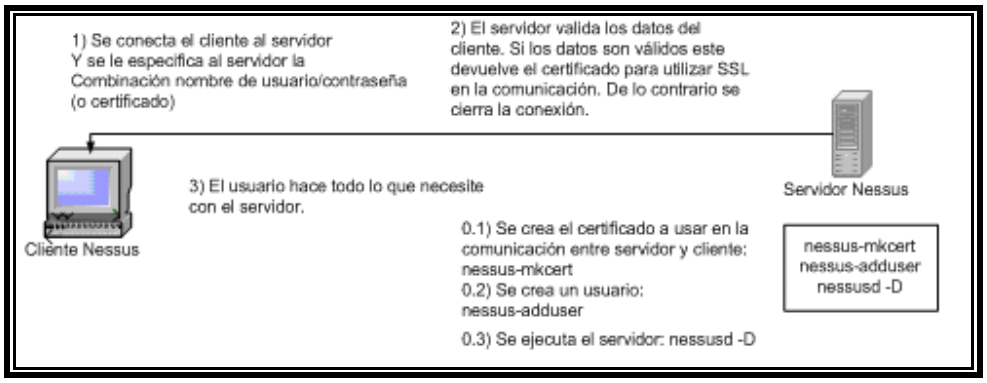


Figura 3.3 Proceso de configuración del servidor y de comunicación entre cliente y servidor.

La Figura 3.3 ilustra el proceso de autenticación y comunicación entre servidor y usuario. Antes de cualquier cosa el servidor debe conocer tanto el certificado que va a usar como algún usuario. No se puede utilizar Nessus si no existen usuarios. Por razones obvias es necesario

que el servidor de Nessus esté en ejecución antes que el cliente pueda hacer uso del mismo. Los pasos 0.1, 0.2 y 0.3 son los pasos preparatorios y son necesarios en caso que no se hayan realizado. Si ya se han realizado pueden obviarse.

Configuración del análisis

Una vez el usuario ha sido autenticado, el mismo tiene que indicarle al servidor qué ataques debe llevar a cabo y a cuáles máquinas analizar. También es necesario especificar cómo llevar a cabo este análisis.

Para llevar a cabo un análisis de vulnerabilidades es necesario conocer las direcciones IP de las víctimas. Nessus no es ningún tipo de adivino ni tampoco está programado para realizar magia negra para saber de antemano qué sistemas analizar. Puede escanearse tanto un conjunto de computadores, así como computadores en particular. Es decir, puede indicársele a Nessus si se desea escanear un conjunto de computadores que cumplan con una dirección de red y máscara de red determinadas, o bien se puede indicar la dirección IP exacta de la víctima. Puede también especificarse una lista de direcciones IP a las cuales analizar. A la hora del análisis Nessus se cerciorará que dichas víctimas en realidad se encuentran disponibles, ya que Nessus cuenta con varias herramientas

para lograr este fin. La primera y más eficiente es el Ping. Esta simplemente envía un paquete ICMP Echo Request hacia la víctima, y si esta responde en un intervalo de tiempo límite significa que la máquina está disponible. De lo contrario se deshabilitan los ataques para esa máquina en particular. El problema con este método es que por lo general ICMP es bloqueado por firewalls (si el análisis se está haciendo desde una red externa o desde Internet). Por lo tanto Ping es utilizado únicamente para una ejecución interna a la red. Nessus también provee la opción de TCP Pings que intentan establecer conexiones a puertos comunes como los son el puerto 80, el puerto 53, etc.

Una vez se ha establecido qué método utilizará Nessus para verificar los hosts activos, es hora de verificar qué puertos tiene abiertos la víctima. Para este fin Nessus provee tres medios especiales: el método connect (), el SYN scan y el escaneo de puertos por medio de la herramienta NMAP. El método connect () intenta establecer una conexión (three way handshake) con cada puerto escaneado. El SYN scan envía un paquete TCP SYN a la víctima al puerto que se desea escanear. Si se recibe un paquete SYN+ACK correspondiente al paquete SYN previamente enviado, el puerto está vivo. A diferencia del método connect (), el

método SYN scan no cierra las conexiones. Aunque el SYN scan es bastante silencioso para el escaneo de un puerto, puede llegar a ser bastante sospechoso para muchos puertos en muchos hosts. Por otro lado NMAP provee una gran cantidad de opciones para llevar a cabo el escaneo de puertos. NMAP es la herramienta más utilizada para este fin. Además de proveer gran cantidad de métodos de escaneo de puertos, NMAP permite establecer la precisión y velocidad a la que se quiere que se realice el escaneo de puertos. Cabe anotar que a mayor velocidad, menor precisión y viceversa. Entre más puertos se escaneen, más tiempo tomará.

Si se escanean únicamente los puertos necesarios, el análisis puede tardar menos y hacer menos ruido (con ruido se hace referencia a lo evidente desde el punto de vista de un IDS del análisis de puertos). Nessus únicamente llevará a cabo ataques para aquellos puertos que estén abiertos.

Una vez se han determinado qué hosts y qué puertos de los hosts están disponibles, Nessus ejecuta un plugin especial denominado el Services Plugin (expuesto en más detalle en una sección siguiente). Este plugin tiene la tarea de determinar qué servicios se están ejecutando en cuáles

puertos. Esta fase es necesaria debido a que muchos servicios se ejecutan sobre puertos no estándar, i.e. Apache sobre el puerto 8080. Este plugin es suficientemente preciso para determinar qué servicios se están ejecutando sobre qué puerto.

Una vez configurados los métodos de identificación de hosts y de análisis de puertos, se deben elegir los plugins (ataques) a ejecutar sobre las víctimas. Nessus provee una gran cantidad de plugins (en una sección siguiente se explicarán en más detalle los plugins). Por ahora basta con resaltar que los plugins son los ataques que se realizarán sobre las víctimas. Nessus categoriza los ataques por familias, las cuales simplemente caracterizan el tipo de vulnerabilidad que un plugin en particular explota, i.e. Ataque CGI, Ataque RPC, etc.

Además de las familias Nessus distingue tres tipos principales de plugins:

- ✓ Peligrosos: Los plugins peligrosos son en general ataques de denegación de servicio que pueden hacer que una máquina detenga su funcionamiento. Se consideran peligrosos porque perjudican a las máquinas víctimas
- ✓ Chequeos seguros (safe checks): Están simplemente basados en

información de la víctima y determinan si ésta es o no vulnerable a un ataque de denegación de servicio. Sin embargo, aunque este tipo de plugins es seguro, puede generar muchas falsas alarmas ya que únicamente se determina la versión de un software y esto no es suficiente para saber si un servicio es o no vulnerable.

- ✓ Otros.

Muchos plugins necesitan privilegios especiales para ser ejecutados, por lo que Nessus también provee facilidades para especificar nombres de usuario y contraseñas para diversos servicios que puedan necesitarlos (ataques SMB, FTP, POP3, etc.).

La siguiente Tabla muestra las características configurables de Nessus a través del cliente.

Característica	**Descripción**
Hosts Víctimas	Nessus necesita que el usuario especifique las víctimas a ser analizadas. Las víctimas se pueden especificar por su nombre de host, por su dirección IP o por la combinación dirección de red/máscara. Nessus permite que los hosts se especifiquen

	dentro de un archivo para que pueda ser reutilizado posteriormente. Ej.:127.0.0.1, 198.200.123.2, chie.uniandes.edu.co, 153.215.12.0/24
Método de identificación de hosts activos	Una vez especificados los hosts a analizar, Nessus verificará cuáles de estos efectivamente están activos. Para este puede usar uno o ambos métodos. Estos métodos son Ping y TCP Ping.
Método de escaneo de puertos	Una vez se identifican los hosts activos, Nessus necesita verificar qué puertos están abiertos para determinar qué ataques llevar a cabo. Nessus permite al usuario especificar qué método de escaneo de puertos utilizar: connect (), SYN scan, o cualquiera de los métodos que utiliza NMAP.
Selección de plugins	Una vez se sabe cómo hacer las cosas, Nessus necesita saber qué hacer. Para esto el usuario debe indicarle a Nessus que plugins ejecutar sobre las víctimas. Todo ataque que necesite de un puerto que no esté abierto será descartado.

Tabla VII: Las principales características configurables de Nessus.

Proceso de análisis de vulnerabilidades

Tal y como se expuso en la sección anterior, tres fases indispensables de preparación son realizadas para determinar qué plugins (ataques) ejecutar sobre la(s) víctima(s). Primero se determina qué hosts están disponibles (por medio de un Ping o por medio de un TCP Ping). Los hosts que no estén activos son descartados y se remueven del análisis. Una vez determinados los hosts activos, se realiza un escaneo de puertos sobre los mismos. Los ataques dirigidos a los puertos que no estén disponibles son descartados. Luego se verifica qué servicios está ejecutando cada puerto, y de acuerdo a este análisis se asignan los ataques correspondientes a cada puerto.

Con estas tres fases preparatorias Nessus proporciona la mayor precisión posible de su análisis. Sin estos pasos preparatorios el ruido generado por Nessus sería exagerado, también la precisión de sus resultados sería menor y además la rapidez del análisis sería bastante reducida. Una vez realizados estas tres fases de reconocimiento, Nessus procede a ejecutar los plugins convenientes. En la siguiente sección se explican los plugins en detalle.

La siguiente figura ilustra el proceso de análisis de vulnerabilidades realizado por Nessus.

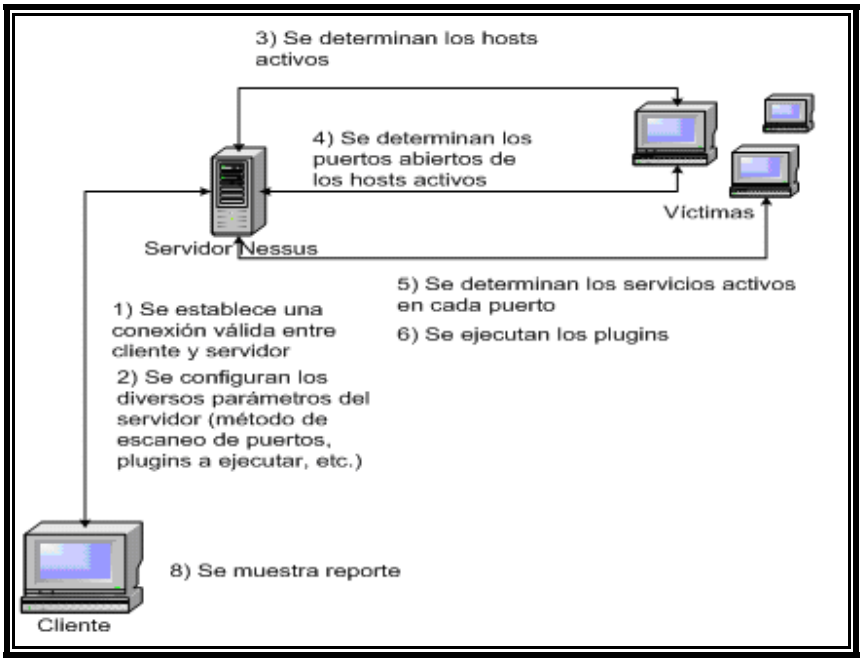


Figura 3.4 Proceso de ejecución del análisis de vulnerabilidades. Después del paso 2, todos los resultados del servidor son enviados al cliente. Los datos que viajan del servidor al cliente están encriptados. Para esto se utiliza SSL.

Knowledge Base

Aunque todo este proceso de reconocimiento suena sorprendente, aún hay más. Nessus cuenta con una característica bastante sofisticada para

la reutilización de análisis previos. Esto quiere decir que Nessus puede basarse en ataques ya realizados para realizar nuevos ataques. Esta característica se denomina Knowledge Base (KB). La KB no es más que una lista de toda la información recopilada sobre un host analizado. Esta característica tan sofisticada sirve a propósitos como evitar la redundancia de los análisis, así si por ejemplo se determina una vulnerabilidad en el servidor HTTP de una máquina, otro análisis puede basarse en esta información para llevara a cabo sus ataques. La versión actual de Nessus únicamente permite la utilización de la KB para el análisis actual. Una vez se termina la ejecución del análisis, la KB es liberada de memoria. En la KB se almacenan todos los resultados del escaneo de puertos, el análisis de servicios y los hosts activos. A través de esta base de datos es que los plugins saben cómo realizar sus tareas más eficientemente. Es una forma de que tanto Nessus como los plugins tengan inteligencia y aprendan de los demás ataques.

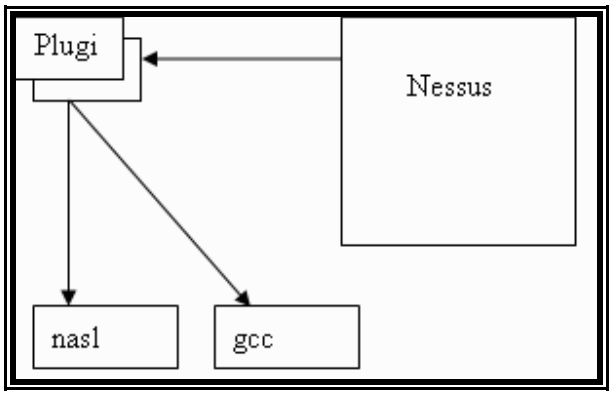


Figura 3.5 Los plugins de Nessus no hacen parte de su núcleo. Su naturaleza modular permite que se creen nuevos módulos. Nessus provee su propio lenguaje de script (nasl) para crear los plugins. C también puede ser utilizado.

Plugins

Los ataques realizados por Nessus no están embebidos en su núcleo (hard-coded). Para mayor extensibilidad y modularidad, éstos se encuentran como porciones de software externo llamados plugins.

Los plugins pueden ser creados en dos lenguajes de programación: NASL (Nessus Attack Scripting Language) y C. Nessus provee todas las herramientas necesarias para la creación de plugins en estos dos lenguajes. La documentación de Nessus recomienda utilizar NASL debido a que es más portable, sin embargo, C puede llegar a ser necesario por razones de flexibilidad y de capacidades. Todo lo que no se pueda hacer con NASL se podrá hacer con C. Sin embargo según los plugins pueden ser escritos en cualquier lenguaje de programación. Esto es cierto debido a que la gran mayoría de los lenguajes de programación tiene interfaces con C. Sin embargo no son muchos los plugins creados en otros lenguajes de programación. La gran mayoría está escrita en NASL.

Primero se expondrá la estructura básica de un plugin escrito en C (y eventualmente se mostrará un ejemplo real) y sus características, y luego se discutirá la estructura y características de un plugins escrito en NASL.

Plugins en C

Es cierto, si no lo puede hacer NASL, lo puede hacer C. Hay una gran cantidad de librerías creadas para C que no se encuentran en otros lenguajes de programación. Las propias librerías del sistema operacional están generalmente escritas en C. Si se escribe un plugin en C, se puede hacer todo lo que no se puede hacer en NASL. Sin embargo, C no es tan portable como se quiere. Pero no es leguaje en sí el que no es portable, sino sus librerías. No es lo mismo compilar bajo Solaris 8 que compilar bajo AIX. NASL no tiene este problema de incompatibilidades. Más adelante se revisará NASL.

Para que los plugins escritos en C puedan ser utilizados, estos deben ser compilados en librerías compartidas. Estas librerías generalmente no son portables entre diferentes plataformas. Nessus provee su propia herramienta para la compilación de plugins en C: nessus-build.

Para escribir un plugin en C primero se hace necesaria la inclusión de ciertas cabeceras proveídas por Nessus:

- ✓ ***includes.h:*** Este archivo contiene todos los incluyes necesarios para escribir un plugin para nessus. Es decir, todas las librerías y demás que necesitan ser importadas, son importadas por includes.h.
- ✓ ***nessusraw.h:*** Si se quiere trabajar con manipulación directa de paquetes, Nessus también provee todas las funciones necesarias para este fin a través de la inclusión de este archivo. Este archivo provee funciones para la manipulación directa de IP, UDP, TCP e ICMP. Ataques como el teardrop se valen de las funciones importadas por este archivo para sus fines macabros. La inclusión de este archivo es obligatoria si se va a utilizar manipulación de paquetes. De lo contrario no es necesaria.

Una vez incluidas una o ambas de estas cabeceras (y todas las demás que necesite) son indispensables dos funciones:

- ✓ ***int plugin_init (struct arglist *desc).-*** Esta indispensable función cumple el papel de identificación del plugin ante el

motor de Nessus. Dentro de esta función se especifica la función del plugin, el autor y todas las características que describen al plugin. Para los fines de dicha identificación se vale de las siguientes funciones:

plug_set_name () -> El nombre del plugin.

plug_set_category () -> La categoría del plugin Especifica qué forma de ataque realiza. Existen varias categorías: recopilación de información (ACT_GATHER_INFO), ataque remoto (ACT_ATTACK), denegación de servicio (ACT_DENIAL), ataque pasivo (ACT_PASSIVE) y escaneador de puertos (ACT_SCANNER).

Plug_set_family () -> La familia del plugin.

Simplemente provee una forma de agrupar los diversos plugins por características comunes. Una familia no es más que un identificador. Un ejemplo de familia puede ser Windows, y se refiere a un ataque que afecta a plataforma Windows.

plug_set_description () -> La descripción detallada del plugin

plug_set_summary () -> La descripción resumida del plugin

plug_set_copyright () -> Los derechos de autor y de copia.

- ✓ ***int plugin_run (struct arglist *desc).-*** Dentro de esta función se encuentra la ejecución real del plugin. Toda la lógica del ataque se encuentra dentro de esta función.

Este es el esqueleto principal de un plugin escrito en C. Son muchas más las funciones que provee Nessus, sin embargo no es el fin de este paper exponer a fondo la creación de un plugin en C. A medida que se encuentren funciones no expuestas, éstas serán debidamente explicadas y analizadas.

3.4 Herramientas para análisis de host.

Para reducir las vulnerabilidades generales de la red es imprescindible primero establecer y delimitar exactamente las funciones adecuadas de cada uno de los dispositivos que la componen. Uno de los elementos de red de contacto directo con el usuario final más importantes son los host. La secuencia mas adecuada será en primer lugar determinar para cada host un papel adecuado, esto quiere decir, asignar las funciones según las actividades que deban realizar tanto el host en mención como los posibles usuarios que a él accedan. De modo que bajo este host no pueda ejecutarse aplicación alguna que haya sido previamente denegada y en cambio

aquellas que si se consideran aplicaciones aprobadas gocen de la totalidad de recursos con las que el ordenador cuenta; así también deberán validarse las cuentas de los usuarios que cumplan un rol en el área destinada para dicho host de modo que una vez que el usuario haya accedido no obtenga ningún beneficio de red ajeno a la actividad que desempeña en la empresa. En segundo lugar el uso de herramientas de escaneo para analizar el desempeño del host en sí y conocer sus fragilidades tanto del hardware como de software para asignarle aplicaciones que no excedan su rendimiento optimo o demanden mas allá de los recursos con los que cuenta.

Determinando el papel de los host.

Una excelente estrategia para poder establecer el rol de un host se puede subdividir en 4 secciones:

- Aplicaciones y servicios.- La determinación de las aplicaciones y servicios que un host debe cumplir obedece a la estructuración general de las jerarquías establecidas por la administración de la empresa. Es la administración quien determina las diferentes actividades que debe cumplir cada área. Una vez que se determina en que nivel jerárquico que un host va a desempeñar debe también clasificarse horizontalmente. De esta sucesión

de procesos finalmente se obtiene el rol preciso determinado al host y por ende las aplicaciones y servicios relacionados a esta actividad. Al restringir la ejecución de aplicaciones según el area de desempeno se logran varios beneficios: mejor velocidad y rendiemiento del procesador al no tener activas aplicaciones que mermen su desempeno, optimizacion del ancho de banda compartido de la red al no demandar a traves de ella servicios innecesarios pero que si consumen recursos, espacio en memoria y disco duro ya que algunas aplicaciones disminuyen disponibilidad de espacio, robustez y estabilidad ya que al solo ejecutar actividades categorizadas como seguras entonces disminuyen al maximo nivel las posibilidades de infeccion y de dano por eventuales ataques, mayor tiempo de vida util al funcionar bajo mantenimiento y condiciones ideales, mejor tiempo de respuesta en cada actividad que ejecute por brindarle la totalidad de recursos, optimizacion del rendimiento productivo del host al no ejecutar sino solo aplicaciones autorizadas y entonces solo actividades productivas para los intereses de la compania y la capacidad poder brindar accesos y restricciones diferenciadas en caso de que el Terminal llegara a ser compartido entre varios usuarios.

Al igual que los host deben ser clasificados tambien deben clasificarse y

restringirse las cuentas de usuarios usando un criterio semejante. Cada usuario debe restringirse al uso del ordenador o cualquier otro dispositivo de red unica y exclusivamente para actividades pertinentes a su labor en la compania, de modo que no pueda desviar su atención en actividades que brindan una distracción momentanea pero que una vez que se considera una sumatoria general logran acumular un desperdicio de recursos considerable que podría invertirse a favor de la empresa.

El hecho de que una cuenta brinda acceso para que un usuario acceda a una red interconectada de transmisión de datos introduce en la misma un error por factor humano con gran inherencia y repercusión en ella. Por esta razon el analisis para proporcionar beneficios de red a un usuario debe ser más exhaustivo aun ya que un dano premeditado o un error (dano involuntario) podrian causar el mismo efecto, de modo que se debe proteger todos los componentes del sistema y conforme a su nivel de importancia brindarles una mayor o menor proteccion, el primer paso para conseguir este objetivo es restringir adecuadamente las sesiones con los alcances necesarios para los usuarios que es un equilibrio de sus requerimientos laborales y el acceso que pueden o no tener a niveles de información y

beneficios trascendentales. Este proceso de establecer beneficios diferenciados entre un usuario y otro debe considerar tambien la responsabilidad que la compania esta dispuesta a otorgar ya que existe una relacion directa que determina esta relacion; a mayores benecifios y privilegios mayor sera la responsabilidad ya que este usuario privilegiado debe no solo justificar en la posterioridad el porque de todos estos accesos sino tambien rentabilidad que puede obtener de ellas solventando asi su merecimiento a continuar gozando de estos privilegios o no.

Las restricciones de actividades tambien mejoran el rendimiento de los usuarios ya que el equipo no les permite destinar su atención a actividades no rentables o productivas. Aunque no es menos cierto que existen aplicaciones que no son directamente rentables para las compañías pero si pueden resultarlo indirectamente al no ser nocivas para los recursos informáticos pero que indirectamente pueden estimular las labores y rendimiento de los empleados, por esta razon no esta demás manejar una pequeña incertidumbre a la rigurosidad de de las políticas de seguridad.

Mantener estas políticas brinda un mejor rendimiento ya que permite un monitoreo detallado y puntualizado lo que permite un control exacto para mejorar, enmendar, corregir o rastrear orígenes y responsabilidades ante una eventual falla o ataque. Además proporciona las herramientas para llevar una bitácora actualizada para rastrear vulnerabilidades y corregirlas.

- ✓ Sistema operativo y parches.
- ✓ Antivirus actualizados.
- ✓ Monitorización de servidores que conectan al exterior con rutas únicas.
- ✓ Herramientas más famosas: NMAPS (escáner de puertos) y Nessus (Escáner más auditoria de host).

Herramientas de análisis genéricas.

Knoppix-STD, LIVE Cd.

Real Time Operating Systems (RTOS) utilizados para el control de sistemas eléctricos y mecánicos de parámetros de gran precisión.

Los RTOS son altamente demandados como soporte de proyectos que desempeñan aplicaciones en tiempo real por proporcionar aportes invaluables:

1. Al ser una solución general que puede personalizarse según las

necesidades reduce considerablemente el tiempo de desarrollo ya que evita crear un sistema operativo nuevo con cada proyecto además del hecho de que no es necesario validar fallas o errores ya consideradas por los creadores del RTOS.

2. Al existir una gran variedad de RTOS de probada estabilidad, fiabilidad y robustez basados en Open Source o GNU General Public License puede utilizarse, copiarse, modificarse o distribuirse con total y absoluta libertad pero si debe asumirse la responsabilidad por el producto creado.

   Aunque estos sistemas cuentan con una gran cantidad y variedad de herramientas y esa es su virtud mayor sin embargo aun necesitan de ser instalados, configurados y personalizados para las aplicaciones requeridas. Entonces surge la necesidad de un especialista descalificando a los novatos para estas funciones. El panorama se complica cuando se escoge una alternativa Open Source ya que no existe una compañía encargada del soporte técnico quedando a la expensas de foros y comunidades.

La solución a este inconveniente nace con los denominados Live CD, discos que al insertarlos en cualquier computador inmediatamente reinician y corren

su propio sistema operativo (RTOS) tan solo desde la memoria ofreciendo una completa y util plataforma con extensión de herramientas sin necesidad de instalación o preconfiguracion alguna ideal para inicializar novatos en sistema de tiempo real. Una vez cumplidos los objetivos tan solo se reinicia el sistema y retira el Cd (DVD o USB Flash Memory) e inmediatamente el computador volverá a su estado normal.

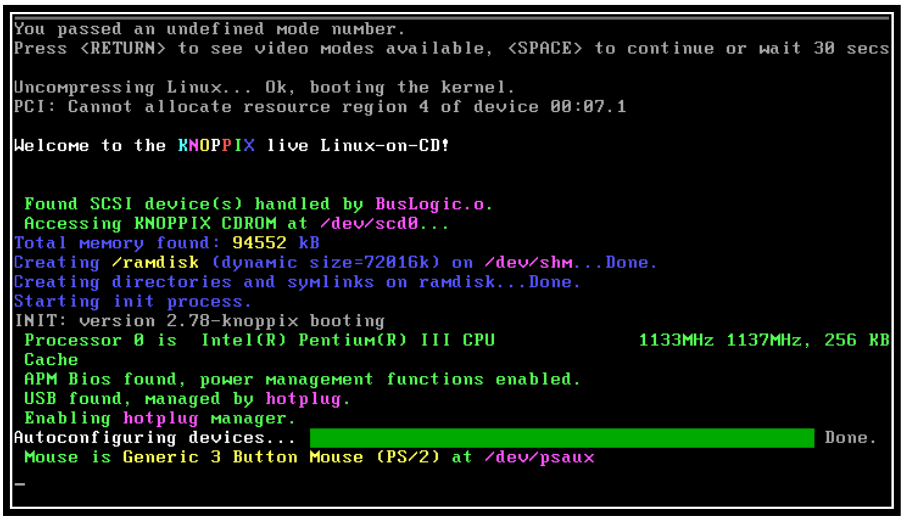


Figura 3.6 Consola de Knoppix

Muchos esfuerzos se hicieron para convertir el Kernel de Linux en un Kernel de tiempo real y producto de estos esfuerzos se originaron algunas variedades de Linux: Xenomai [Xenomai 2007], RTLinux1 [Yodaiken 1999], KURT [University of Kansas, Center for Research, Inc. 2007], RTAI [Dipartimento di Ingegneria Aerospaziale – Politecnico di Milano 2007], algunos son propietarios como Montavista [Montavista

2007], BlueCat Linux [LynuxWorks 2007] and WindLinux2 [Wind River 2007b]. También se cuenta entre estos desarrollos Knoppix-STD

Figura 3.7 Knoppix-STD

Figura 3.8 Encriptación en Knoppix

- ✓ **2c2** : planeacion de texto multiple -> un texto de cifras
- ✓ **4c** : tal cual 2c2 (piensa de forma plausible las denegaciones)
- ✓ **acfe** : analisis de encriptacion tradicional (como Vigenere)
- ✓ **cryptcat** : netcat + encriptación
- ✓ **gifshuffle** : herramienta para imágenes gif
- ✓ **gpg 1.2.3** : Guardia Privada GNU
- ✓ **ike-scan** : Impresión manual VPN
- ✓ **mp3stego** : herramienta stego para mp3
- ✓ **openssl 0.9.7c**
- ✓ **outguess** : herramienta stego
- ✓ **stegbreak** : fuerza bruta stego JPG
- ✓ **stegdetect** : descubrimiento stego JPG
- ✓ **sslwrap** : envoltura SSL
- ✓ **stunnel** : envoltura SSL
- ✓ **super-freeSWAN 1.99.8** : soporte de kernel IPSEC
- ✓ **texto** : hace que una armadura de gpg-ascii parezca ingles

misterioso

- ✓ **xor-analyze** : otra herramienta dentro del analisis de encriptación

Análisis Forense

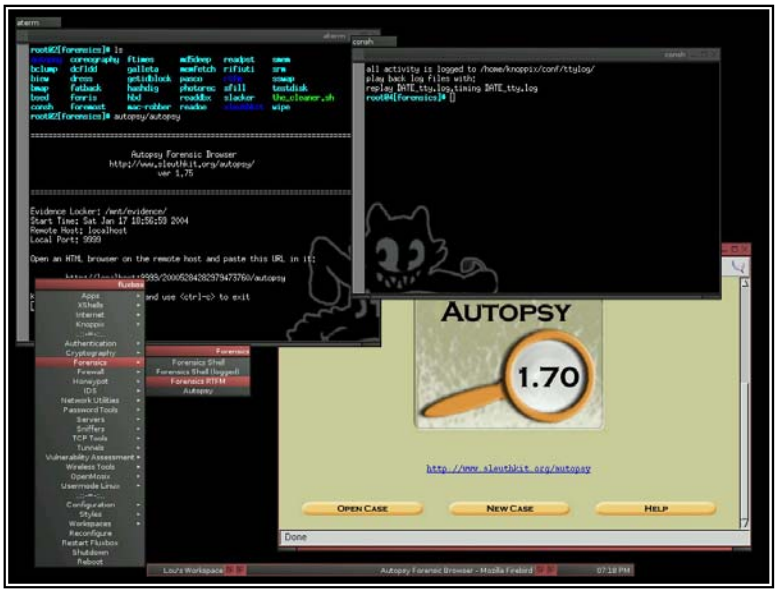


Figura 3.9 Consola de Análisis Forense

- ✓ **sleuthkit 1.66** : extensiones a la caja de herramientas forenses del kit de el Coronel
- ✓ **1.75**: Web front-end to TASK. Evidence Locker defaults to /mnt/evidence

- ✓ **biew** : vista binaria
- ✓ **bsed** : editor de cadenas binarias
- ✓ **consh**: logged shell (from F.I.R.E.)
- ✓ **coreography** : analiza archivos del núcleo
- ✓ **dcfldd** : US DoD Computer Forensics Lab version of dd
- ✓ **fenris :** herramienta para ejecutar, trazar, compilar y retroceder
- ✓ **fatback** : Archivos imborrables FAT
- ✓ **foremost** : recubre archivos de tipo especifico desde discos de imagines (como todos los archivos JPG)
- ✓ **ftimes** : herramienta del sistema de linea base (ser proactivo)
- ✓ **galleta** : recubre de cookies al Internet Explorer
- ✓ **hashdig** : busca a traves de trozos de la base de datos
- ✓ **hdb** : decompilador de java
- ✓ **mac-robber** : TCT's graverobber escrito en C
- ✓ **md5deep** : ejecuta md5 en múltiples archivos y directorios
- ✓ **memfetch** : forza a vaciar la memoria
- ✓ **pasco** : browse IE index.dat
- ✓ **photorec** : grab files from digital cameras
- ✓ **readdbx** : convierte los archivos del Outlook Express .dbx a mbox
- ✓ **readoe**: convierte el directorio completo del Outlook Express .directory

al formato mbox.

- ✓ **rifiuti**: busca archivos Windows Recycle Bin INFO2.
- ✓ **secure_delete**: elimina archivos, memoria, swap de manera segura.
- ✓ **testdisk**: prueba y recupera particiones perdidas.
- ✓ **wipe**: Prepara a una partición segura. Útil para inicializar una partición para DD y otras herramientas tipicas utilizadas para forense (dd, lsof, strings, grep, etc.)

Herramientas de actividades y autopsia que permiten chequear imágenes dentro y fuera de evidencia:

- ✓ Qparted – permite hacer copias de particiones sin traslapar datos.
- ✓ Glimpse – indexa grandes cantidades de datos para información.
- ✓ Strings – siempre clásico.

Cortafuegos

Figura 3.10 Interfaz del firewall

- ✓ **blockall**: script para bloquear todos los TCP entrantes (excepto del host local).
- ✓ **flushall**: alinear todas las reglas de los firewalls.
- ✓ **firestarter**: via rapida hacia un firewall.
- ✓ **firewalk**: mapea las reglas bases de firewall.
- ✓ **floppyfw**: convierte un floppy en firewall.
- ✓ **fwlogwatch**: monitorea los accesos al firewall.
- ✓ **iptables 1.2.8**
- ✓ **gtk-iptables** : GUI front-end
- ✓ **shorewall 1.4.8-RC1**: tablas ip basadas en paquetes.

Detección de intrusos

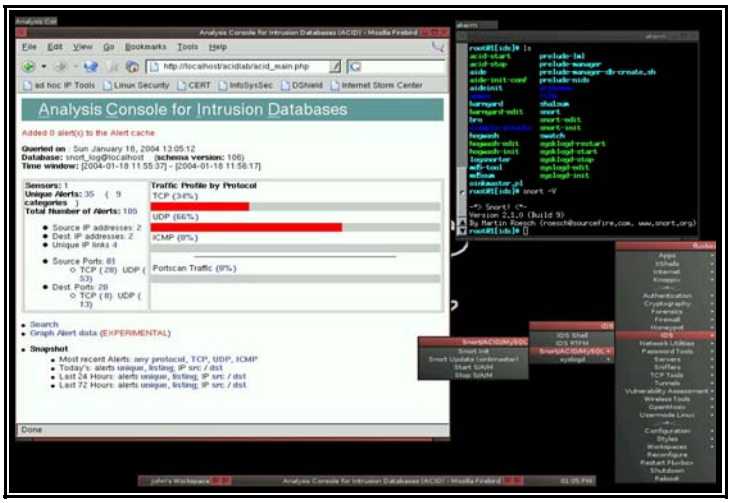


Figura 3.11 Interfaz del programa de Detección de Intrusos

- ✓ **labrea**: ataca el desempeño de gusanos y scanners de puertos.
- ✓ **thp**: pequeño honeypot.
- ✓ **snort 2.1.0**: IDS de red preferidos de todos.
- ✓ **ACID**: reporta el contenido Web visualizado.
- ✓ **barnyard**: procesador rapido de reportes de acceso.
- ✓ **oinkmaster**: mantiene las reglas de reporte actualizada.
- ✓ **hogwash**: Control de Acceso basadas en señales de reportes.
- ✓ **bro**: IDS de red.
- ✓ **prelude**: IDS de red y host.
- ✓ **WIDZ**: IDS inalambricos, ap y monitor de pruebas.

- ✓ **aide** : Herramienta host baseline, tripwire-esque
- ✓ **logsnorter**: monitor de accesos.
- ✓ **swatch** : monitorea cualquier archivo como syslog

Utilidades de red.

Cheops – Herramienta para probar y mapear una red.

Nessus – excelente herramienta de escaneo.

Nmap – Herramienta para escanear puertos.

Etherape –Muestra las actividades de la red.

Honeyd – Pequeña herramienta para crear Money Redes sencillas.

Labrea – Reduce el desempeño de escaneos de puertos y algunos otros tipos de ataques.

Snort – Herramienta de uso general incluida en muchas soluciones de software.

Iptraf –Visualización de trafico IP.

Ethereal – Captura y reproduce tráfico.

Ettercap – Sniffer++ para redes switcheadas.

Dsniff – Busca trafico de datos importantes como pueden ser usernames y Passwords.

Whisker – Analizador de vulnerabilidades web.

Spike Proxy – Proxy Man in the middle.

- ✓ **LinNeighboorhood**: busca redes SMB como un vecindario de red Windows.
- ✓ **argus**: auditor de red.
- ✓ **arpwatch**: Mantiene un rastreo sobre el medio de transmisión fisica de las MACs.
- ✓ **cdpr**: reporte de descubrimiento de protocolo de descubrimiento cisco.
- ✓ **cheops**: snmp, herramienta de decubrieminto y monitoreo.
- ✓ **etherape**: Herramienta de monitoreo y visualizacion de red.
- ✓ **iperf**: mide en desempeño IP.
- ✓ **ipsc**: Calculadora de subnet IP.
- ✓ **iptraf**: monitor de red.
- ✓ **mrtg**: Graficador de trafico multi router.
- ✓ **mtr**: traceroute.
- ✓ **ntop 2.1.0** : Analizador de protocolo
- ✓ **rrdtool**: Base de Datos round robin.
- ✓ **samba**: soporte opensource SMB.
- ✓ **tcptrack**: Rastrea conexiones existentes.

Utilidades de contraseña

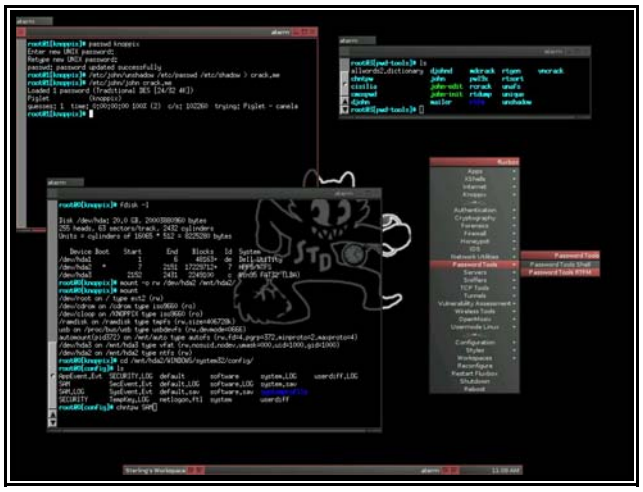


Figura 4.12 Configuración de Contraseñas

- ✓ **john 1.6.34**: Es un Ripper password cracker.
- ✓ **allwords2**: Diccionario en ingles CERIAS's 27MB.
- ✓ **chntpw** : resetea passwords bajo Windows box (including Administrator)
- ✓ **cisilia**: password cracker distribuido.
- ✓ **cmospwd**: averigua password de CMOS.
- ✓ **djohn**: John the Ripper el comúnmente distribuido.
- ✓ **pwl9x**: Archivos de documentos crack Win9x.
- ✓ **rcrack**: rainbow crack.

Servidores

- ✓ **apache**
- ✓ **ircd-hybrid**
- ✓ **samba**
- ✓ **smail**
- ✓ **sshd**
- ✓ **vnc**
- ✓ **net-snmp**
- ✓ **tftpd**
- ✓ **xinetd**

Sniffers

- ✓ **aimSniff**: rastrea AIM traffic.
- ✓ **driftnet**: Rastrea por imágenes.
- ✓ **dsniff** : rastrea passwords comunes, ósea muy sencillas (thanks Dug)
- ✓ **ethereal 0.10.0**: standard. Analiza la red. incluyes tethereal
- ✓ **ettercap 0.6.b**: Analiza una red switcheada en una red y mas.
- ✓ **filesnarf**: Graba archivos de trafico NFS.
- ✓ **mailsnarf**: rastrea tráfico de smtp/pop.
- ✓ **msgsnarf** : Rastrea aol-im, msn, yahoo-im, irc, icq traffic

- ✓ **ngrep**: Red grep, un sniffer habilidades de filtro Grep.
- ✓ **tcpdump**: El corazón de todo.
- ✓ **urlsnarf**: Controla y registra acceso a todas las urls visitados en el medio físico.
- ✓ **webspy**: refleja todos los URLs visitados por un host en el navegador local.

Tcptools

- ✓ **arpfetch**: Clona una MAC.
- ✓ **arping** : ping para MAC addresses
- ✓ **arpspoof** : spoof arp
- ✓ **arpwatch**: monitorea las direcciones MAC sobre el medio físico.
- ✓ **despoof**: detecta falsos paquetes via mediciones TTL.
- ✓ **excalibur**: Generador de paquetes.
- ✓ **file2cable**: reproduce paquetes capturados.
- ✓ **fragroute**: Herramienta de fragmentación de paquetes.
- ✓ **gspoof**: Generador de paquetes.
- ✓ **hopfake**: falsas respuestas de hopcount.
- ✓ **hunt** : tcp hijacker
- ✓ **ipmagic**: Generador de paquetes.

- ✓ **lcrzoex**: Herramientas tcp.
- ✓ **macof**: Inunda un switch con MAC address.
- ✓ **packetto** : Herramientas de Dan Kaminsky's (incluye 1.10 and 2.0pre3)
- ✓ **net sed**: Inserta y reemplaza cadenas en tráfico en tiempo real.
- ✓ **packETH**: Generador de paquetes.
- ✓ **tcpkill**: Elimina protocolo tcp.
- ✓ **tcpreplay**: Reproduce paquetes capturados.

Túneles

- ✓ **cryptcat**: encripta netcat.
- ✓ **httptunnel**: túnel de datos en http.
- ✓ **icmpshell**: túnel de datos en icmp.
- ✓ **netcat**: Herramienta tcp.
- ✓ **shadyshell**: Túnel de datos en udp.
- ✓ **stegtunnel**: oculta datos en cabeceras TCP/IP.
- ✓ **tcpstatflow**: detecta túnel de datos.
- ✓ **tiny shell**: Pequeña herramienta de encriptación.

Asesoramiento de vulnerabilidades.

Existen muchas maneras de enlistarlos. Hay muchos desde THC, ADM, RFP,

NMRC, TESO, Phenoelit. Se debe ser muy cuidadoso con estas herramientas. Recordar siempre que no se ofrecen garantías y que el usuario es enteramente responsable por sus acciones.

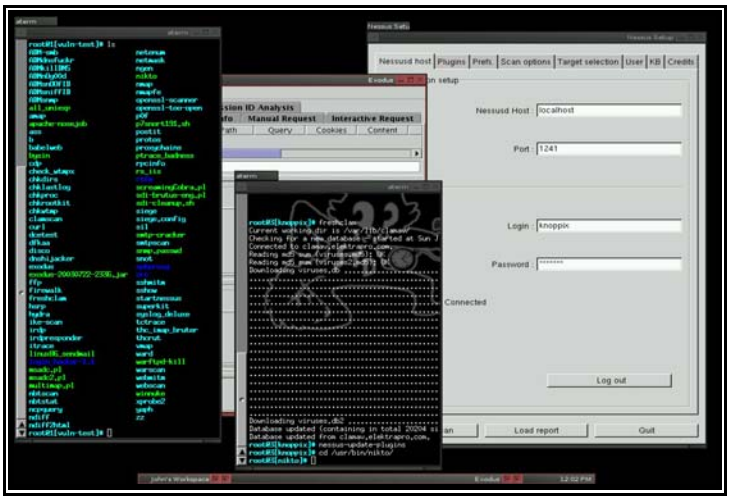


Figura 4.13 Configuración de Vulnerabilidades

- ✓ **ADM tools** : como ADM-smb y ADMkillDNS
- ✓ **amap 4.5** : aplicaciones de mapas funcionando en usuarios remotos
- ✓ **IRPAS** : Internet Routing Protocol Attack Suite
- ✓ **chkrootkit 0.43** : búsqueda del núcleo
- ✓ **clamAV**: escáner de virus. actualiza las asignaturas con freshclam
- ✓ **curl** : comando util para transferir algo con un URL
- ✓ **exodus** : aplicación del auditor de la red
- ✓ **ffp** : huellas digitales borrosas para conexiones encriptadas

- ✓ **firewalk** : mapea una linea de base del firewall
- ✓ **hydra** : herramienta de fuerza bruta
- ✓ **nbtscan** : escanea redes SMB
- ✓ **ncpquery** : escanea servidores NetWare
- ✓ **nessus 2.0.9**: escáner de vulnerabilidades. actualiza tus accesos con la herramienta nessus
- ✓ **nikto** : escáner CGI
- ✓ **nmap 3.48** : enumeración estándar de puerto/usuario
- ✓ **p0f** : huella digital pasiva
- ✓ **proxychains**: servidores de múltiples cadenas
- ✓ **rpcinfo** : información desde RPC
- ✓ **screamingCobra** : escáner CGI
- ✓ **siege** : testea http y pruebas de mercado
- ✓ **sil** : pequeño router de bloqueo
- ✓ **snot**: reproduce reglas sigilosamente dentro de la red. Prueba tu ids/incidencias en respuestas/etc.
- ✓ **syslog_deluxe** : mensajes engañosos syslog
- ✓ **thcrut** : red para diseñar mapas
- ✓ **vmap** : versiones de aplicaciones de mapas
- ✓ **warscan** : aprovecha herramientas automáticas

- ✓ **xprobe2** : usa ICMP para huella digital
- ✓ **yaph** : aun otro servidor cazador
- ✓ **zz** : zombie zapper kills DDoS zombies

Herramientas para WLAN.

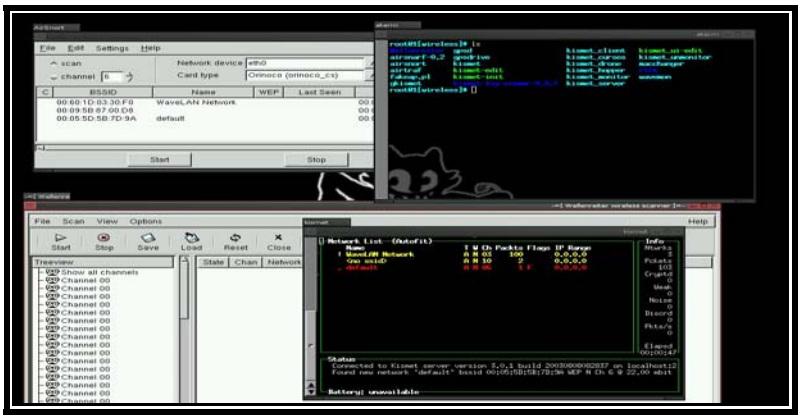


Figura 4.14 Configuración para Herramientas WLAN

- ✓ **airsnarf** : utilidad de Instalación rogue AP
- ✓ **airsnort**: busca, encuentra, crackea 802.11b
- ✓ **airtraf**: 802.11b analizador de desarrollo de redes
- ✓ **gpsdrive**: usa GPS y mapas
- ✓ **kismet 3.0.1**: for 802.11
- ✓ **kismet-log-viewer**: controla los accesos y destinos
- ✓ **macchanger:** cambia la MAC address

- ✓ **wellenreiter:** 802.11b descubierto y auditado
- ✓ **patched orinoco drivers**: automático (no se necesita ejecutable)

CAPITULO 4

4. CASO ESTUDIO

En el presente capítulo se muestra la implementación de una red la cual utilizamos para poder realizar todo lo requerido con respecto a nuestra tesis.

4.1 Evaluación de Vulnerabilidades de Sistemas Operativos

Los sistemas operativos deben ser constantemente revisados para tener claro que vulnerabilidades se presentan, a continuación se detalla todo lo pertinente para éste cometido.

4.1.1 Integridad de cuentas de usuarios

Debe existir un procedimiento formal de registro y salida de usuarios para otorgar acceso a todos los sistemas y servicios de información

multi-usuario. El acceso a servicios de información multi-usuario debe ser controlado a través de un proceso formal de registro de usuarios, el cual debe incluir los siguientes puntos:

- ✓ Utilizar IDs de usuario únicos de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones. El uso de IDs grupales solo debe ser permitido cuando son convenientes para el trabajo a desarrollar.
- ✓ Verificar que el usuario tiene autorización del propietario del sistema para el uso del sistema o servicio de información. También puede resultar apropiada una aprobación adicional de derechos de acceso por parte de la gerencia.
- ✓ Verificar que el nivel de acceso otorgado es adecuado para el propósito del sistema y que este sea coherente con la política de seguridad de la organización.
- ✓ Entregar a los usuarios un detalle escrito de sus derechos de acceso, y requerir que los usuarios firmen declaraciones señalando que comprenden las condiciones para el acceso.
- ✓ Garantizar que los proveedores de servicios no otorgan acceso hasta que se hayan completado los procedimientos de autorización.

- ✓ Mantener un registro formal de todas las personas registradas para utilizar el servicio; y cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas o se desvincularon de la organización.
- ✓ Verificar periódicamente, y cancelar IDs y cuentas de usuarios redundantes; y garantizar que los IDs de usuario redundantes no se asignen a otros usuarios.

Se debe considerar la inclusión de cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados. Los sistemas deben ser monitoreados para detectar desviaciones respecto a la política de control de accesos y registrar eventos para suministrar evidencia en caso de producirse incidentes relativos a la seguridad. El monitoreo de los sistemas permite comprobar la eficacia de los controles adoptados y verificar la conformidad con el modelo de política de acceso.

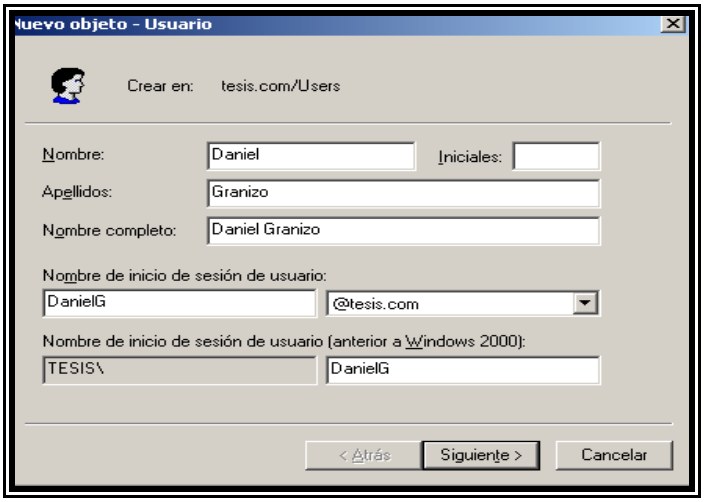


Figura 4.1 Interfaz para Creación de Usuario

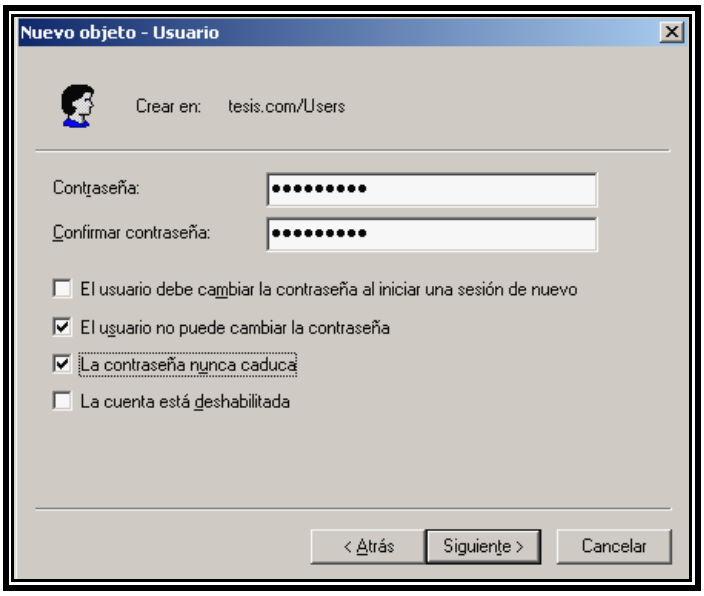


Figura 4.2 Asignación de contraseña

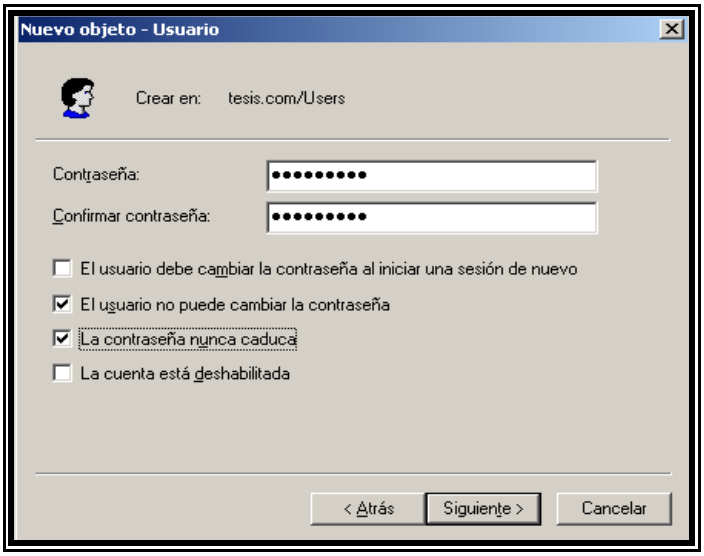


Figura 4.3 Estableciendo parámetros de la contraseña

Registro de eventos

Deben generarse registros de auditoria que contengan excepciones y otros eventos relativos a seguridad, y deben mantenerse durante un periodo definido para acceder en futuras investigaciones y en el monitoreo de control de accesos. Los registros de auditorias también deben incluir:

- ✓ ID de usuario.
- ✓ Fecha y hora de inicio y terminación.
- ✓ Identidad o ubicación de la Terminal, si es posible.
- ✓ Registros de intentos exitosos fallidos de acceso al sistema.

- ✓ Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

Podría requerirse que ciertos registros de auditoria sean archivados como parte de la política de retención de registros o debido a los requerimientos de recolección de evidencia.

Monitoreo del uso de los sistemas

Procedimientos y áreas de riesgo

Se debiera establecer procedimientos para monitorear el uso de las instalaciones de procesamiento de la información. Dichos procedimientos son necesarios para garantizar que los usuarios solo estén desempeñando actividades que hayan sido autorizadas explícitamente. El nivel de monitoreo requerido para cada una las instalaciones debe determinarse mediante una evaluación de riesgos.

Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

a) acceso no autorizado, incluyendo detalles como:
    1) ID de usuario.
    2) Fecha y hora de eventos clave.
    3) Tipos de eventos.
    4) Archivos a los que se accede.

5) Utilitarios y programas utilizados.

b) todas las operaciones con privilegio, como:

1) Utilización de cuenta de supervisor.

2) Inicio y cierre (start-up and stop) del sistema.

3) Conexión y desconexión de dispositivos I/O.

c) intentos de acceso no autorizado, como:

1) Intentos fallidos.

2) Violaciones de la política de accesos y notificaciones para “gateways” de red y “firewalls”.

3) Alertas de sistemas patentados para detención de intrusiones.

d) alertas o fallas de sistema como:

1) alertas o mensajes de consola.

2) excepciones del sistema de registro.

3) alarmas del sistema de administración de redes.

Factores de riesgo

Se debe revisar periódicamente el resultado de las actividades de monitoreo. La frecuencia de la revisión debe depender de los riesgos involucrados. Entre los factores de riesgo que se deben considerar se encuentran:

- ✓ La criticidad de los procesos de aplicaciones.
- ✓ El valor, la sensibilidad o criticidad de la información involucrada.
- ✓ La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
- ✓ El alcance de la interconexión del sistema (en particular las redes públicas).

Revisión de los registros de eventos

Una revisión de los registros implica la comprensión de las amenazas que afronta el sistema y las maneras que surgen.

Frecuentemente, los registros del sistema contienen un gran volumen de información, gran parte de la cual es ajena al monitoreo de seguridad. Para asistir en la identificación de eventos significativos, a fin de desempeñar el monitoreo de seguridad, se debe considerar la posibilidad de copiar automáticamente los tipos de mensajes adecuados a un segundo registro, y/o utilizar herramientas de auditoria o utilitarios adecuados para llevar a cabo el examen de archivo, al asignar la responsabilidad por la revisión de registros, se debe considerar una separación de funciones entre quien/es emprende/n la revisión y aquellos cuyas actividades están siendo

monitoreadas. Se debe prestar especial atención a la seguridad de la herramienta de registro, debido a que si se accede a la misma en forma no autorizada, esto puede propiciar una falsa percepción de la seguridad. Los controles deben apuntar a proteger contra cambios no autorizados y problemas operativos. Estos incluyen:

- ✓ La desactivación de la herramienta de registro.
- ✓ Alteraciones a los tipos de mensajes registrados.
- ✓ Archivos de registro editados o suprimidos.
- ✓ Medio de soporte archivos de registro saturado, y falla en el registro de eventos o sobre escritura de los mismos.

4.1.2 Acceso a archivos

Impedir el acceso no autorizado en los sistemas de información y para esto se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información.

Los procedimientos deben comprender todas las etapas del ciclo de vida de los accesos de usuario, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Se debe

conceder especial atención, cuando corresponda, a la necesidad de controlar la asignación de derechos de acceso de privilegio, que permiten a los usuarios pasar por alto los controles de sistema.

Es valedero anotar ciertos parámetros a seguir en función de que el acceder a archivos por parte de los usuarios sea tan seguro para la empresa como para cada uno de ellos, a fin de mantener un control eficaz del acceso a los datos y servicios de información, la gerencia debe llevar a cabo un proceso formal a intervalos regulares, a fin de revisar los derechos de acceso de los usuarios, de manera tal que:

- ✓ Los derechos de acceso de los usuarios se revisen a intervalos regulares (se recomienda un periodo de seis meses) y después de cualquier cambio.
- ✓ Las autorizaciones de privilegios especiales de derechos de acceso se revisen a intervalos mas frecuentes (se recomienda un periodo de tres meses).
- ✓ Las asignaciones de privilegios se verifiquen a intervalos regulares, a fin de garantizar que no se obtengan privilegios no autorizados.

Figura 4.4 Consola de Configuración del servidor

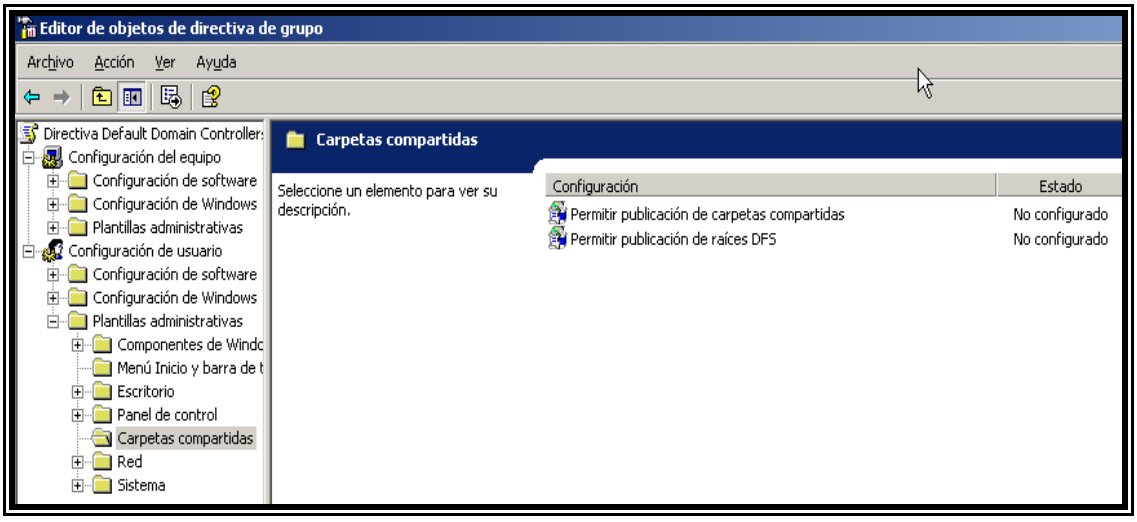


Figura 4.5 Estableciendo Compartición de Carpetas

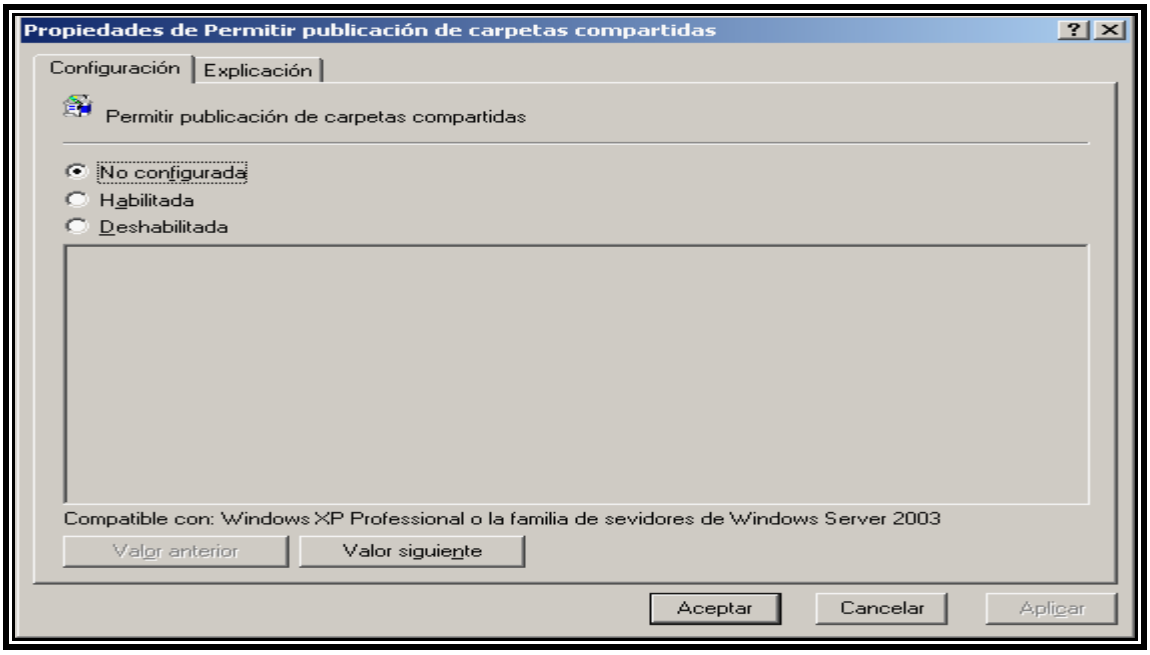


Figura 4.6 Parámetros para la Compartición de Carpetas

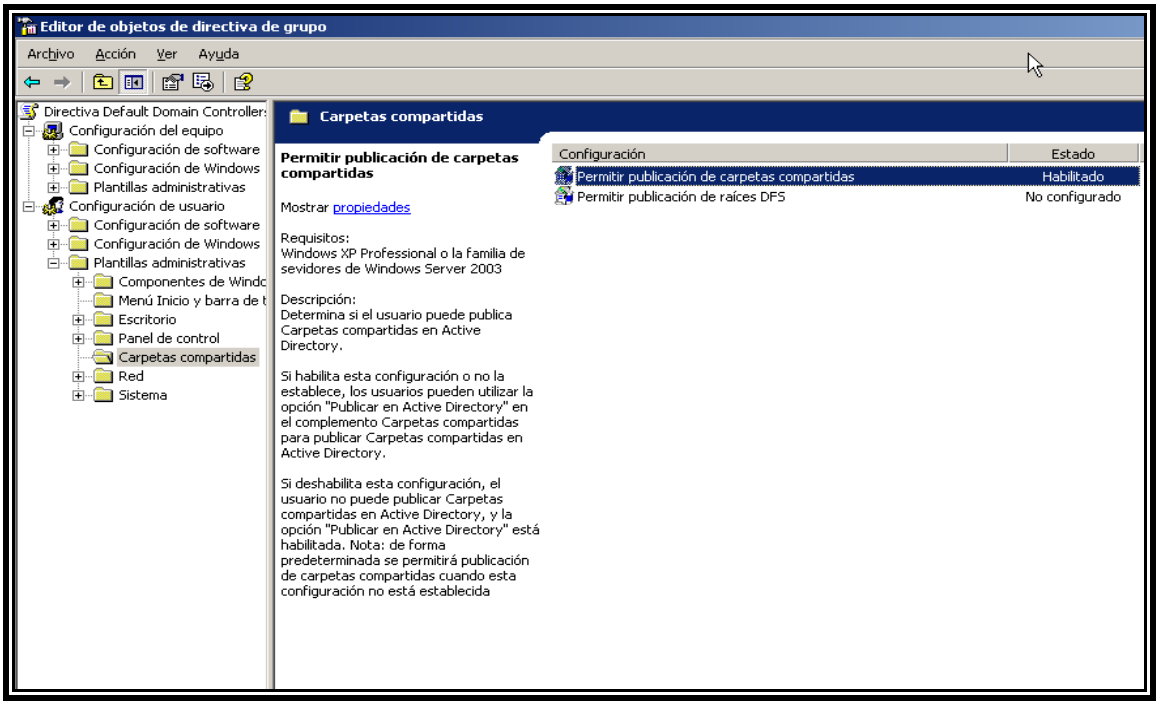


Figura 4.7 Compartición de Carpetas configurada

4.1.3 Atributos sobre archivos (Permisos)

Para la administración de los atributos los S.O. cuentan con una amplia variedad de permisos pero en el grupo los más trascendentes se pueden considerar:

- ✓ Permisos de sistemas de archivos._ Controla el acceso a los archivos en las unidades NTS para lo cual cada usuario necesita un permiso concedido según su relación con estos archivos.
- ✓ Permisos de archivos compartidos._ Permite la administración de los recursos y archivos compartidos entre usuarios ya sean estos datos o dispositivos periféricos como por ejemplo las impresoras.
- ✓ Permisos de Registro._ Administra el ingreso a campos medulares del servidor como son los registros.

Se debe limitar y controlar la asignación y uso de privilegios (cualquier característica o servicio de un sistema de información multi-usuario que permita que el usuario pase por alto los controles de sistemas o aplicaciones). El uso inadecuado de los privilegios del sistema resulta frecuentemente en el más importante factor que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multi-usuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un

proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- ✓ Deben identificarse los privilegios asociados a cada producto del sistema y las categorías de personal a las cuales deben asignarse los productos.
- ✓ Los privilegios deben asignarse a individuos sobre las bases de la necesidad de uso y evento por evento.
- ✓ Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización; y también se debe promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
- ✓ Los privilegios deben asignarse a una identidad de usuario diferente de aquellas utilizadas en las actividades normales.

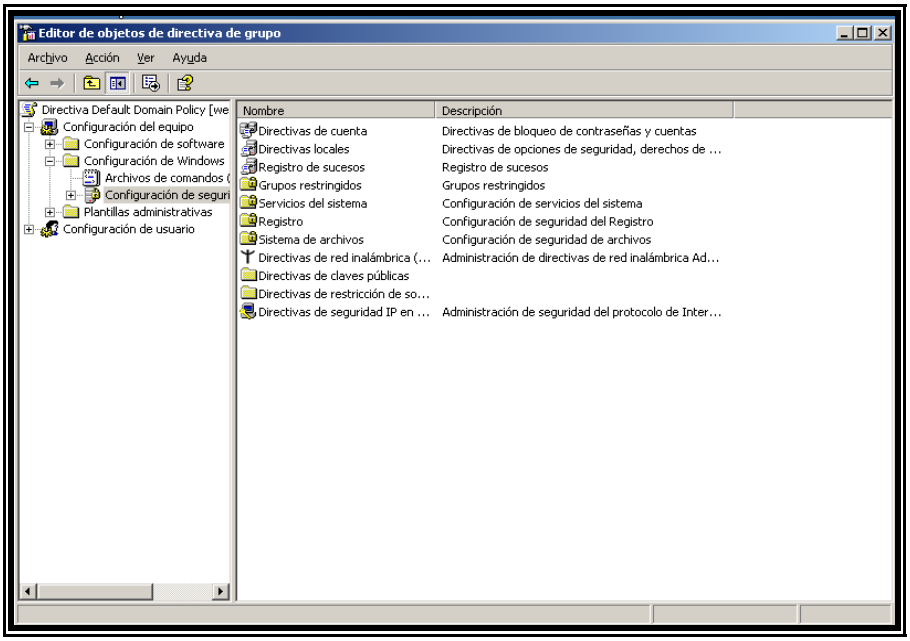


Figura 4.8 Interfaz de Configuración del Servidor

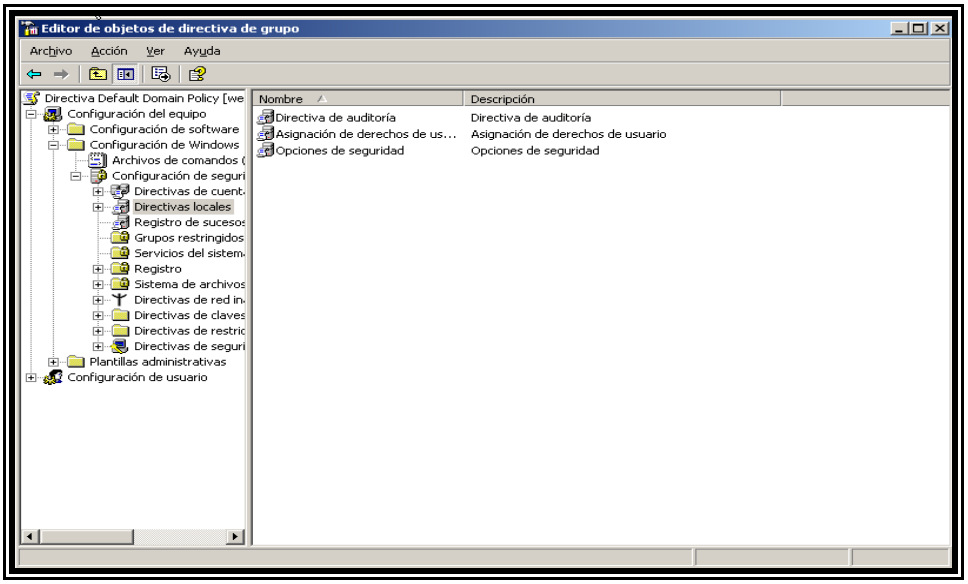


Figura 4.9 Establecimiento de Directivas Locales

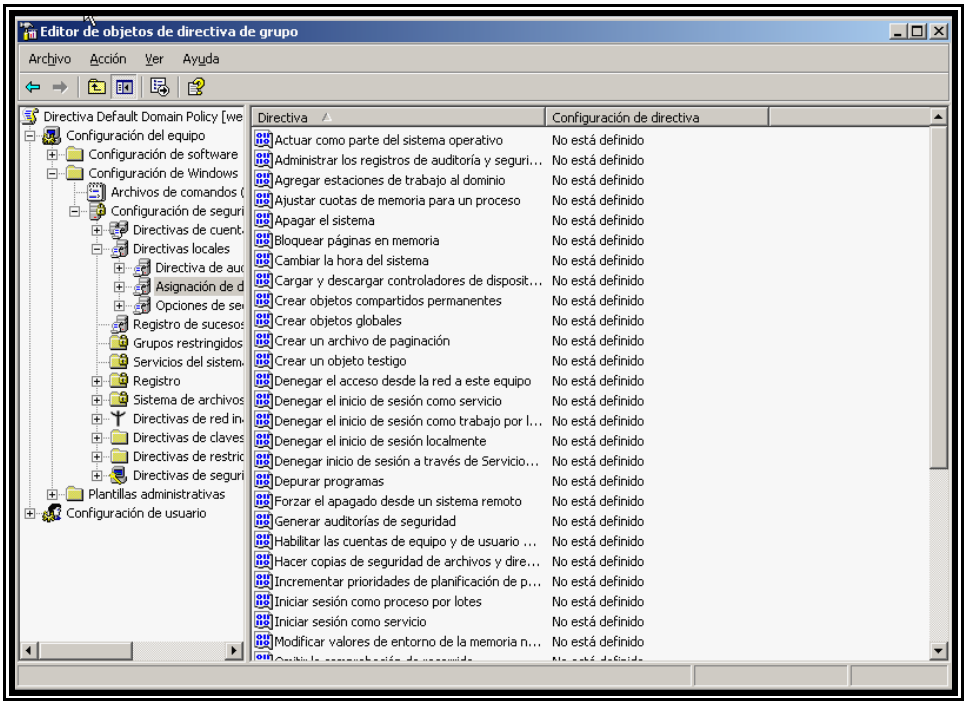


Figura 4.10 Opciones de configuración de dispositivos

Algo a resaltar se da en los cambios que pueden darse en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que inicia el administrador y sobre las reglas que requieren la aprobación del administrador o de otros antes de entrar en vigencia y aquellas que no.

4.1.4 Parámetros de login

Al especificar las reglas de control de acceso, se debe considerar cuidadosamente lo siguiente:

- ✓ Diferenciar entre reglas que siempre deben imponerse y reglas optativas o condicionales.
- ✓ Establecer reglas sobre la base de la premisa “Qué debe estar generalmente prohibido a menos que se permita expresamente”, antes que la regla más débil “Todo esta generalmente permitido a menos que se prohíba expresamente”.
- ✓ Las reglas que requieren la aprobación del administrador o de otros antes de entrar en vigencia y aquellas que no.

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) deben tener un identificador único (ID de usuario) para su uso personal, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los IDs de usuario no deben dar ningún inicio del nivel de privilegio del usuario, por ej.: gerente, supervisor, etc.

En circunstancias excepcionales, cuando existe un claro beneficio para la empresa, puede utilizarse un ID compartido para un grupo de usuarios o una tarea especifica. Para casos de esta índole, se debe documentar la aprobación de la gerencia. Podrían requerirse controles adicionales para mantener la responsabilidad.

Existen diversos procedimientos de autenticación, los cuales pueden ser utilizados para sustentar la identidad alegada del usuario. Las contraseñas constituyen un medio muy común para proveer la identificación y autenticación (I y A) sobre la base de un secreto que solo conoce el usuario. También se puede llevar a cabo lo mismo con medios criptográficos y protocolos de autenticación.

Los objetos como “tokens” con memoria o tarjetas inteligentes que poseen los usuarios también pueden utilizarse para I y A. Las tecnologías de autenticación biométrica que utilizan las características o atributos únicos de un individuo también pueden utilizarse para autenticar la identidad de una persona. Una combinación de tecnologías y mecanismos vinculados de manera segura tendrá como resultado una autenticación más fuerte.

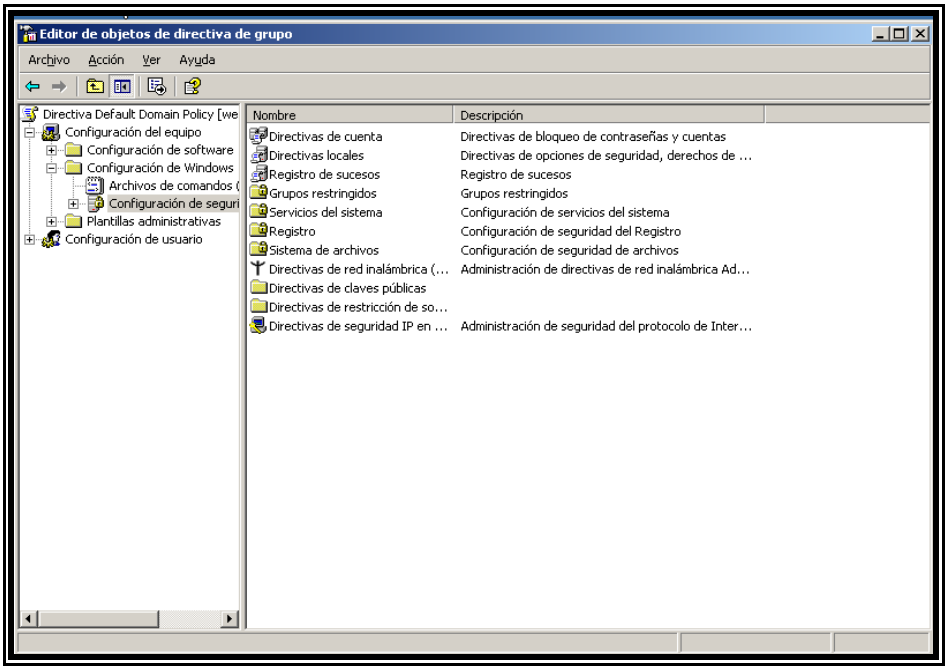


Figura 4.11 Interfaz de Configuración del Equipo

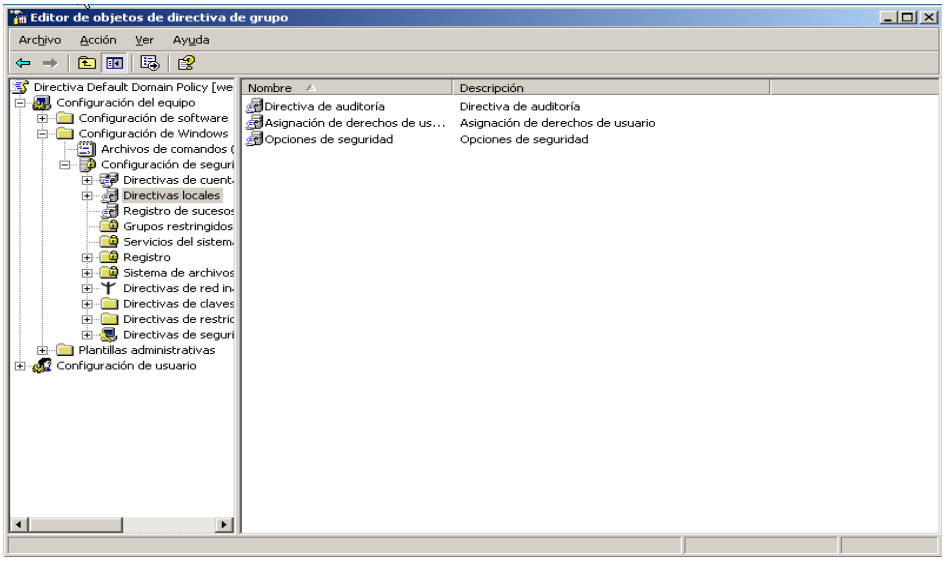


Figura 4.12 Establecimiento de Opciones de Seguridad

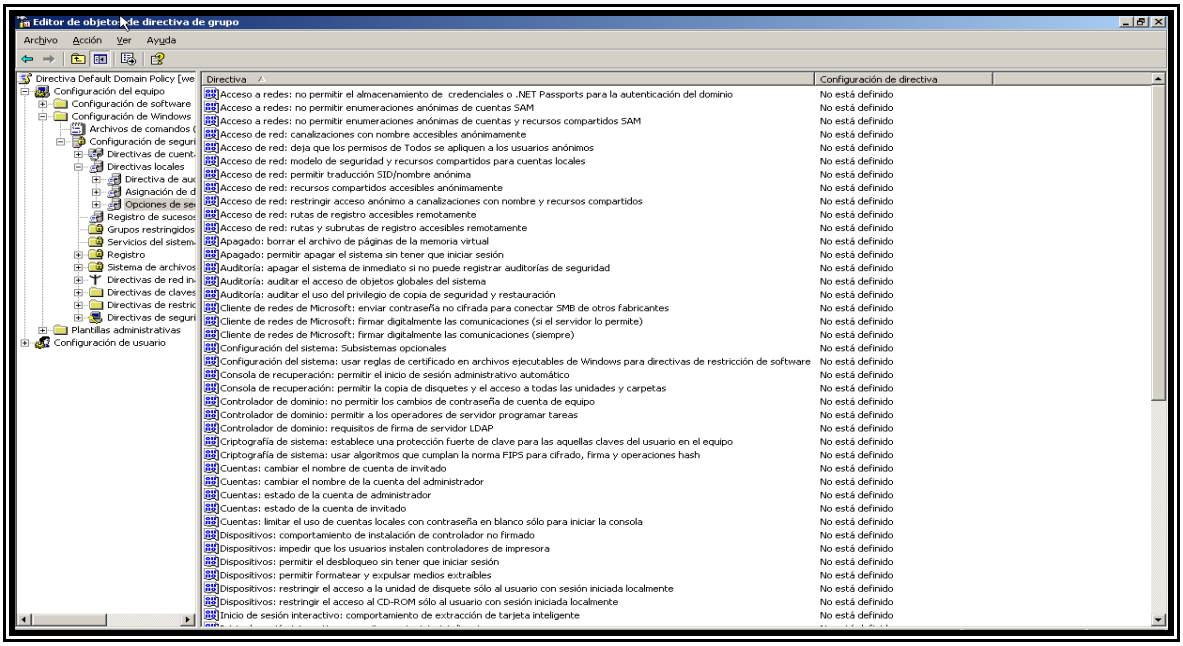


Figura 4.13 Opciones para Configurar Parámetros de Login

Trabajo remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar fijo fuera de la organización. Se debe implementar la protección adecuada del sitio de trabajo remoto contra, por ej. El robo de equipamiento e información, la divulgación no autorizada de información, el acceso remoto no autorizada a los sistemas internos de la organización o el uso inadecuado de los dispositivos e instalaciones. Es importante que el trabajo remoto sea autorizado y controlado por la gerencia, y que se implementen disposiciones y acuerdos para esta forma de trabajo.

Las organizaciones deben considerar el desarrollo de una política, de procedimientos y de estándares para controlar las actividades de trabajo remoto.

Las organizaciones sólo deben autorizar actividades de trabajo remoto si han comprobado satisfactoriamente que se han implementado disposiciones y controles adecuados en materia de seguridad y que estos cumplen con la política de seguridad de la organización. Se deben considerar los siguientes parámetros:

- ✓ La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.
- ✓ El ambiente de trabajo remoto propuesto.
- ✓ Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.

- ✓ La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ej. familia y amigos.

Los controles y disposiciones comprenden:

- ✓ La provisión de mobiliario para almacenamiento y equipamiento, adecuado para las actividades de trabajo remoto; y aparatos de comunicación, con inclusión de métodos para asegurar el acceso remoto.
- ✓ Una definición del trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar y los sistemas internos y servicio a los cuales el trabajador remoto esta autorizado a acceder.
- ✓ Reglas y orientación para cuando familiares y visitantes accedan al equipamiento e información.
- ✓ La provisión de hardware y el soporte y mantenimiento del software; los procedimientos de back-up y para la continuidad de las operaciones.
- ✓ Seguridad física; dando también auditoria y monitoreo de la seguridad.
- ✓ Anulación de la autoridad, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

4.1.5 Integridad de objetos

La integridad de los objetos se basa en que estos solo pueden ser modificados (escribir, cambiar, borrar, crear) por elementos autorizados y siempre de manera controlada.

Con respecto a la integridad de los datos debemos tener la seguridad de que estos sean recibidos exactamente como se los envió desde la entidad de origen (no presentan modificación, inserción, omisión o repetición), y la posible distorsión a nivel de un flujo completo de mensajes (integridad de conexión) o referida a un mensaje concreto o a porciones (campos) de un mensaje. Opcionalmente, puede incluir soporte para la recuperación de los datos originales (reenvío, uso de redundancia para auto-corrección) o simplemente soportar la detección de problemas de integridad.

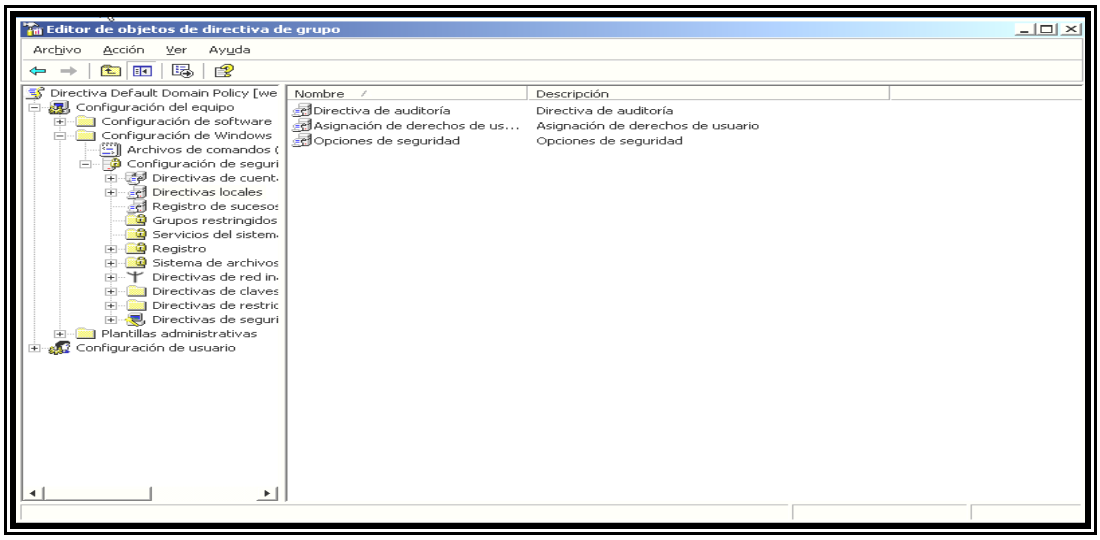


Figura 4.14 Interfaz de Configuración de Directivas de Auditoria

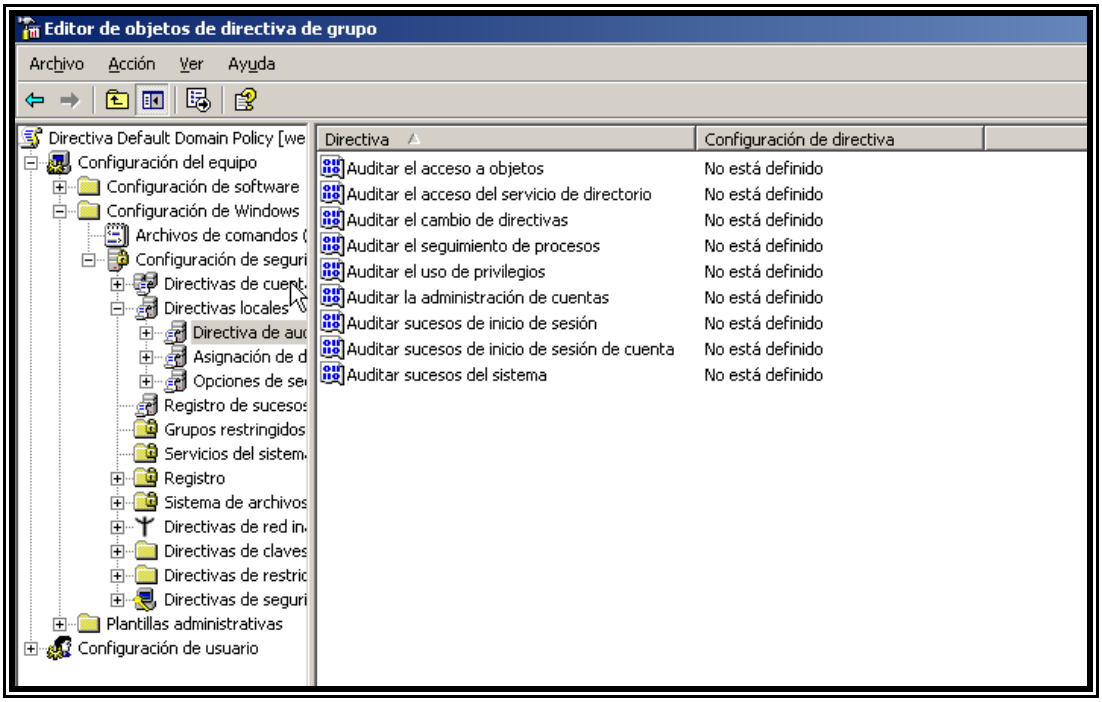


Figura 4.15 Opciones para la Configuración de Objetos

4.1.6 Políticas de contraseñas

Las contraseñas constituyen un medio común de validación de la identidad de un usuario para acceder a un sistema o servicio de información. La asignación de contraseñas debe controlarse a través de un proceso de administración formal, mediante el cual debe llevarse a cabo lo siguiente:

- ✓ Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los

miembros del grupo (esto podría incluirse en los términos y condiciones de empleo).

- ✓ Garantizar, cuando se requiera que los usuarios mantengan a sus propias contraseñas, que se provea inicialmente a los mismos de una contraseña provisoria segura, que deberán cambiar de inmediato. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, solo debe suministrarse una vez identificado el usuario.
- ✓ Requerir contraseñas provisorias para otorgar a los usuarios de manera segura. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro). Los usuarios deben acusar recibo de la recepción de la clave (password).

Las contraseñas nunca deben ser almacenadas en sistemas informativos sin protección.

Si resulta pertinente, se debe considerar el uso de otras tecnologías de identificación y autenticación de usuarios, como la biométrica, por ej.: verificación de huellas dactilares, verificación de firma y uso de “tokens” de hardware, como las tarjetas de circuito integrado (“chip-cards”).

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, estas constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Se debe notificar a los usuarios que deben cumplir con los siguientes puntos:

- ✓ Mantener las contraseñas en secreto.
- ✓ Evitar mantener un registro en papel de las contraseñas, a menos que este pueda ser almacenado en forma segura.
- ✓ Cambiar las contraseñas siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- ✓ Seleccionar contraseñas de calidad, con una longitud mínima de seis caracteres que:
  1) Sean fáciles de recordar.
  2) No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ej. nombres, números de teléfono, fecha de nacimiento, etc.
  3) No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o total-mente alfabéticos.

Cambiar las contraseñas a intervalos regulares o según el número de acceso (las contraseñas de cuentas con privilegios deben ser modificadas con mayor frecuencia que las contraseñas comunes), y evitar reutilizar o reciclar viejas contraseñas.

Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”), no incluir contraseñas en los procesos automatizados de inicio de sesión, por ej.: aquellas almacenadas en una tecla de función o macro.

No compartir las contraseñas individuales de usuario, si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se debe notificar a los mismos que pueden utilizar una contraseña de calidad única para todos los servicios que brinden un nivel razonable de protección de las contraseñas almacenadas.

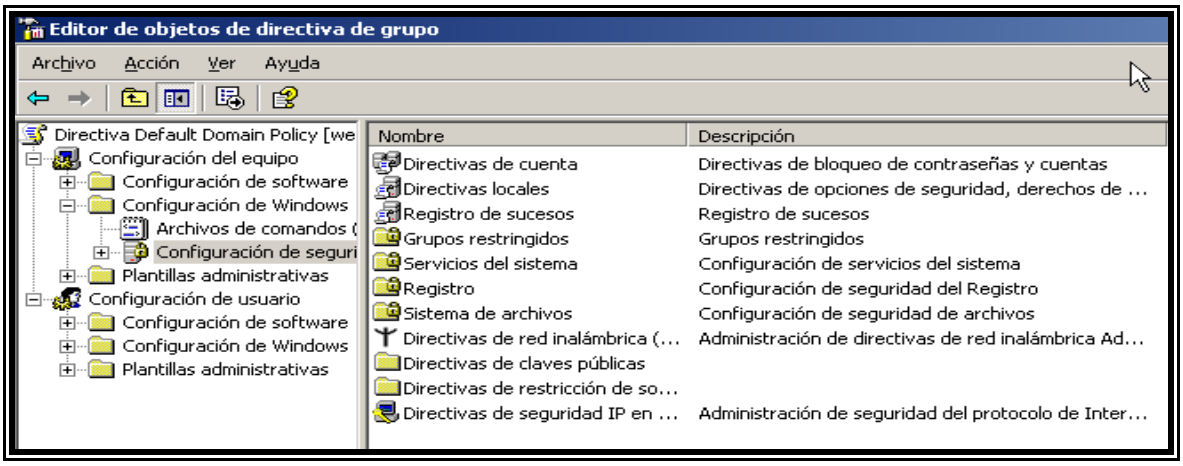


Figura 4.16 Interfaz para la Configuración de Seguridad

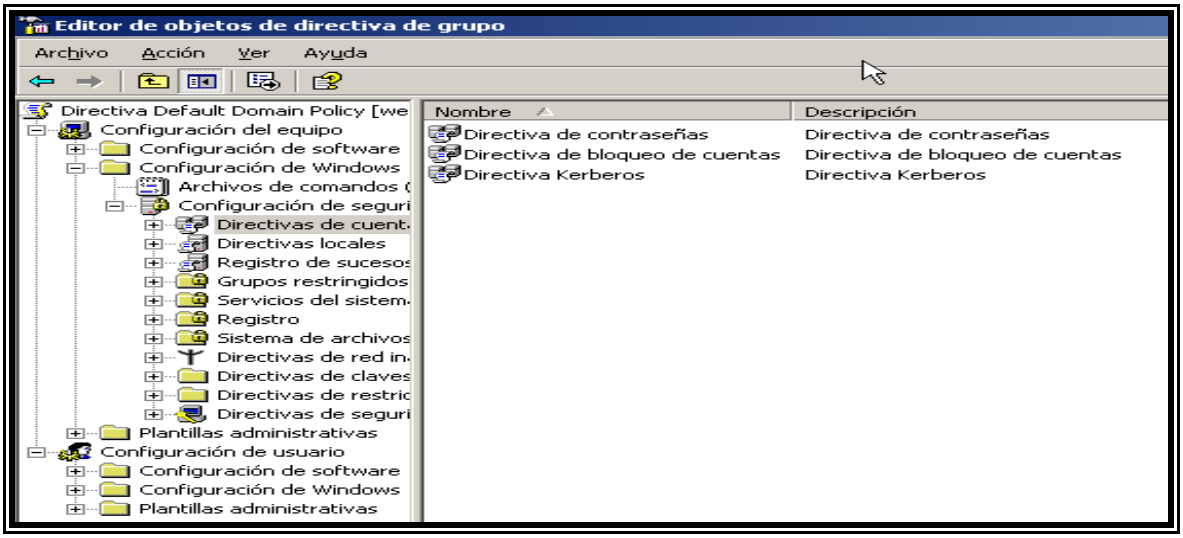


Figura 4.17 Elementos a configurar para establecer Seguridades

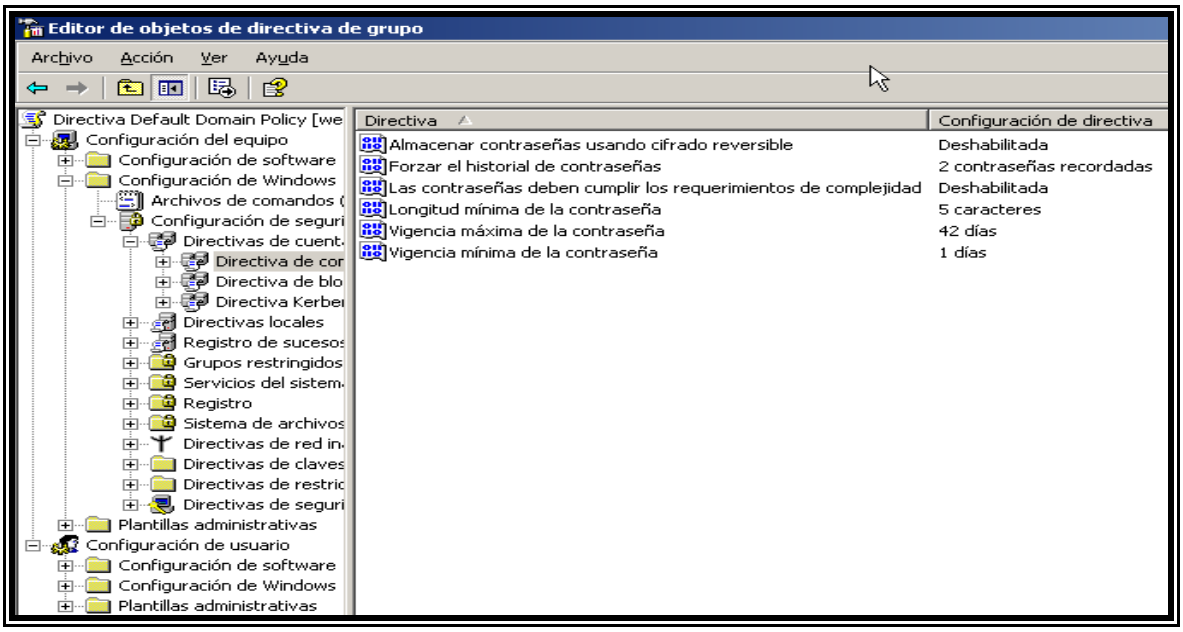


Figura 4.18 Parámetros variables en la Configuración de Contraseñas

4.2 Evaluación de Vulnerabilidades de la Red de Datos

La Red de Datos debe estar bajo revisión constante para que las vulnerabilidades que se presentan sean brevemente controladas.

4.2.1 Análisis de Fortaleza de Passwords

El crackeo por fuerza bruta es una técnica bastante deficiente debido a que hace una búsqueda de forma muy básica dentro de la IP dada, empezando con caracteres alfabéticos y posteriormente numéricos, realizando todas las permutaciones posibles, por lo que se convierte en un proceso lento; tiene ciertas variantes para realizar búsquedas limitadas y así poder hacer ataques desde varias fuentes a la vez, también se puede cambiar el orden de las permutaciones para darle una versatilidad mayor a la búsqueda. En nuestra red no hallo nada debido a que las contraseñas están basadas para soportar este tipo de ataques, dicho sea de paso bastante elemental.

Figura 4.19 Ejecución del crackeo por Fuerza Bruta

En la búsqueda con el Diccionario, el programa nos brinda treinta y cinco (35) diferentes archivos con varias temáticas para poder utilizar en el ataque, rinde de mejor manera si se conoce o se tiene cierta noción de a quien se le va a realizar el ataque, se pueden hacer ediciones a estos diccionarios y también permutarlos entre ellos según los términos que supongamos nos servirían.

En la red propuesta se ejecuto el programa con un diccionario que llego hasta doscientos catorce (214) palabras, sin encontrar lo buscado, cabe anotar que en el diccionario ajustado para el ataque no se encontraba nada que este programa pudiese encontrar.

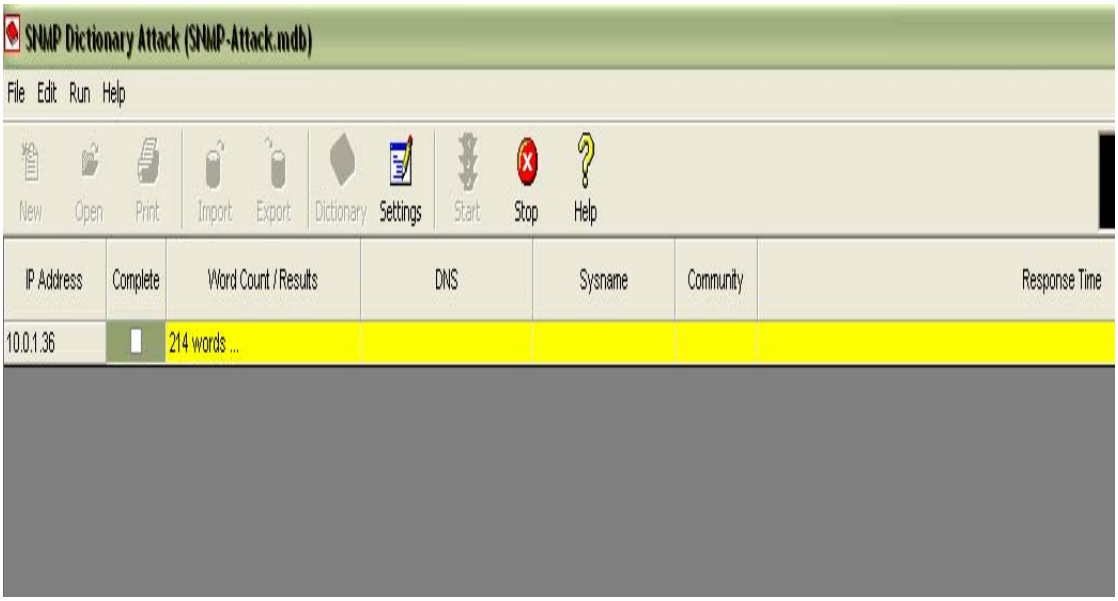


Figura 4.20 Búsqueda con el Diccionario

4.2.2 MS Windows Networking (Compartir carpetas e impresoras)

Es común dentro de una empresa compartir no solo archivos sino también equipos como por ejemplo impresoras, scanner, etc., para aquello debemos tener en cuenta los privilegios que tiene cada usuario.

En lo que se refiere al compartimiento de carpetas debemos considerar todas las opciones de seguridad al momento de configurar una carpeta como lo es el acceso solo a lectura de los archivos.

En la imagen a continuación se muestra la interfaz en la cual se configura la compartición o no de la carpeta en cuestión, dando ciertos parámetros que el usuario puede modular de acuerdo a sus necesidades, como puede ser el número de usuarios que accedan a ella y demás.

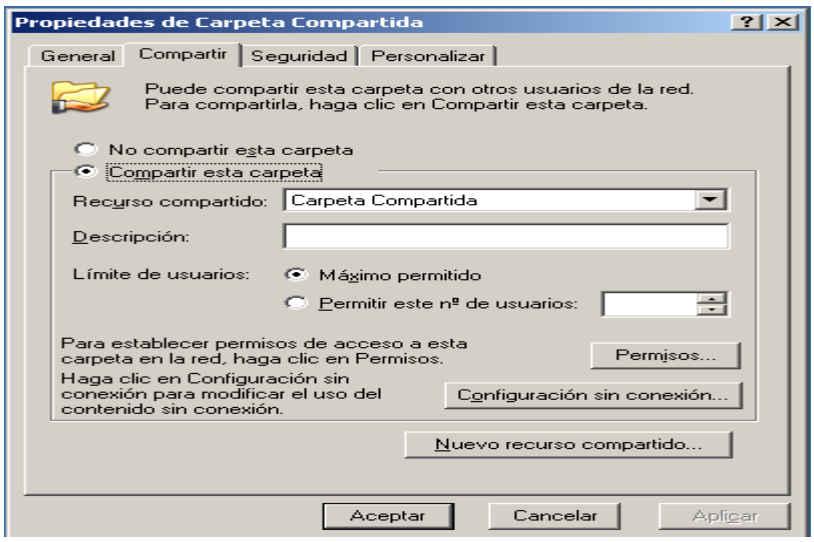


Figura 4.21 Ventana para configurar la Comparticion de Carpetas

Una muestra de una perdida total de seguridad es indicada en la imagen inferior en la cual al acceder a la carpeta compartida se puede hacer sobre ella todo lo que se desee; debido a que existen ciertos casos en los que al servidor le interesaría que cada usuario pueda leer determinados archivos, seria lo obvio activar esta opción, pero es bastante incongruente que el servidor entregue un control total sobre lo que se le pueda realizar a ciertos archivos, dando la posibilidad de leerlos, escribir sobre ellos, ejecutarlos, y en fin usándolos de una u otra forma.

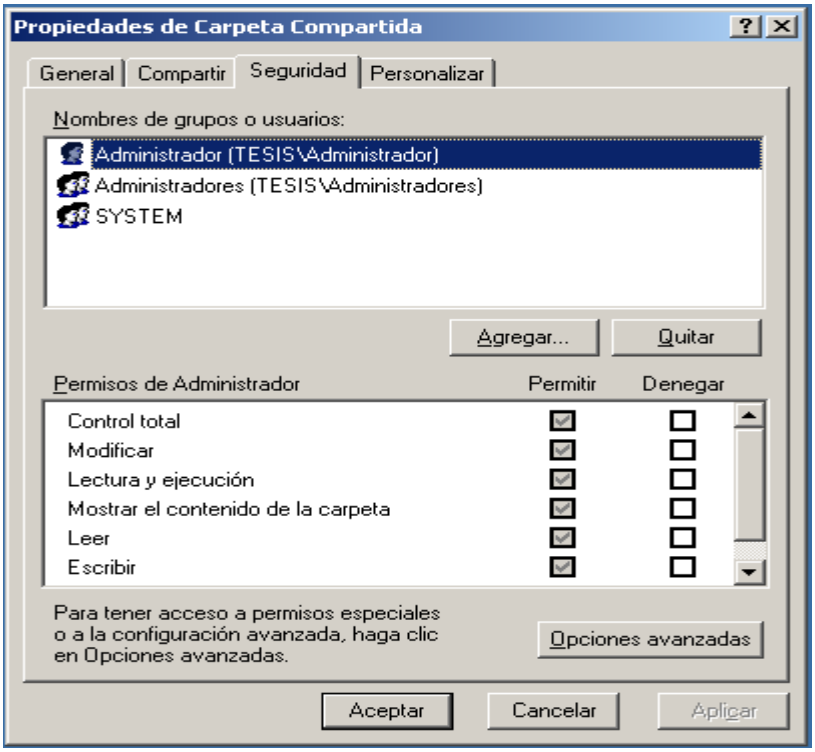


Figura 4.22 Propiedades de Seguridad de Compartición de Carpetas

4.2.3 Seguridad Perimetral.

Sin duda esta es la parte mas importante en este proyecto, es mas es aquí donde se ve si una red puede ser considerada como segura o fácilmente vulnerable en este caso gracias al software proporcionado por Checkpoint y las políticas en el configuradas; nuestra red es altamente segura pasando todas las pruebas tanto internas como externas a ella.

Figura 4.23 Pantalla de Entrada al Firewall

Figura 4.24 Información del estado del Dispositivo

Este grafico muestra la información sobre el dispositivo instalado y ciertas configuraciones que vienen dadas por default para un manejo adecuado posterior a la instalación.

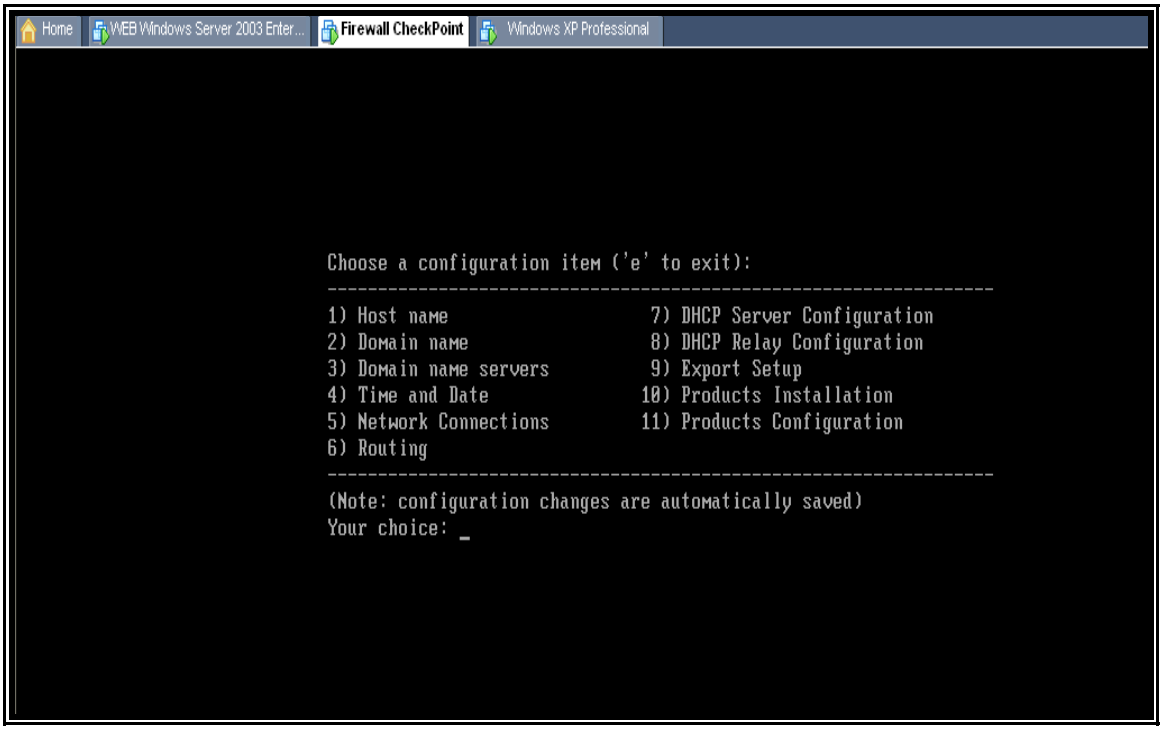


Figura 4.25 Consola de Configuración del Firewall

Utilizando la consola del firewall podemos dar la configuración que consideremos necesaria para nuestros requerimientos, con la posibilidad de cambios tan sencillos como la variación del nombre del usuario hasta el hecho de cambiar las conexiones de la red, el ruteo, etc.

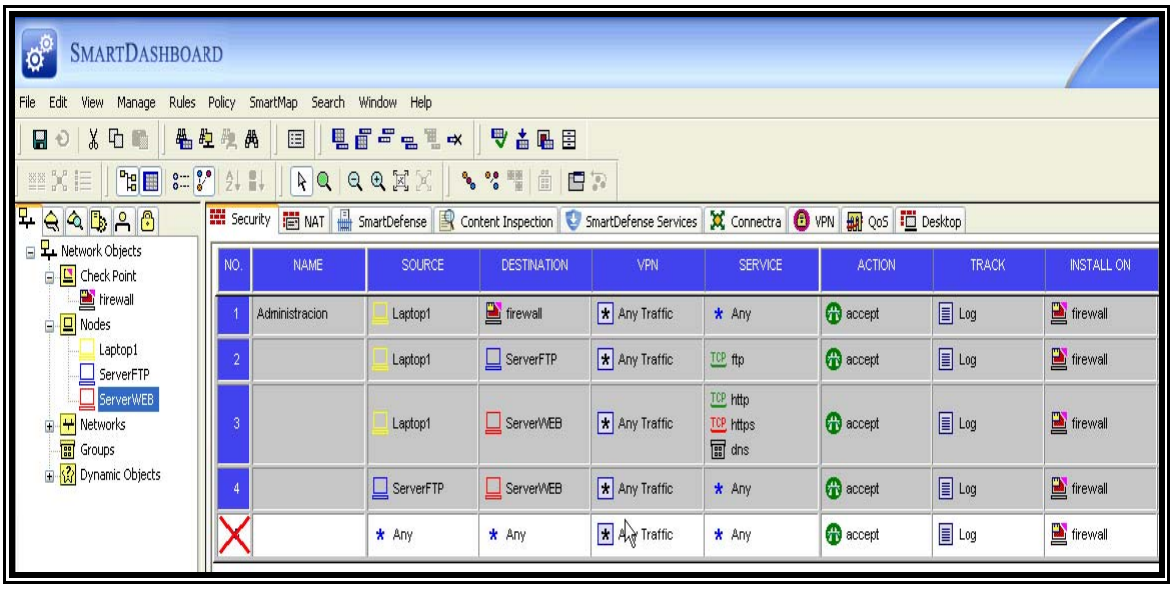


Figura 4.26 Interfaz para la configuración de Políticas

Las políticas dentro del firewall son muy fáciles de establecer en esta interfaz, la cual da la posibilidad de interactuar entre todos los usuarios de la red y los posibles servidores, manejando protocolos, trafico de la red, así como también el hecho de permitir o negar ciertos parámetros que consideráramos necesario hacerlo.

4.2.4 Captura de tráfico (Sniffing)

Para la captura de tráfico, se utilizo el programa Ethereal, del cual mostramos su pantalla antes de su ejecución en la cual obviamente tiene todos los protocolos posibles de los paquetes a capturar aun en cero.

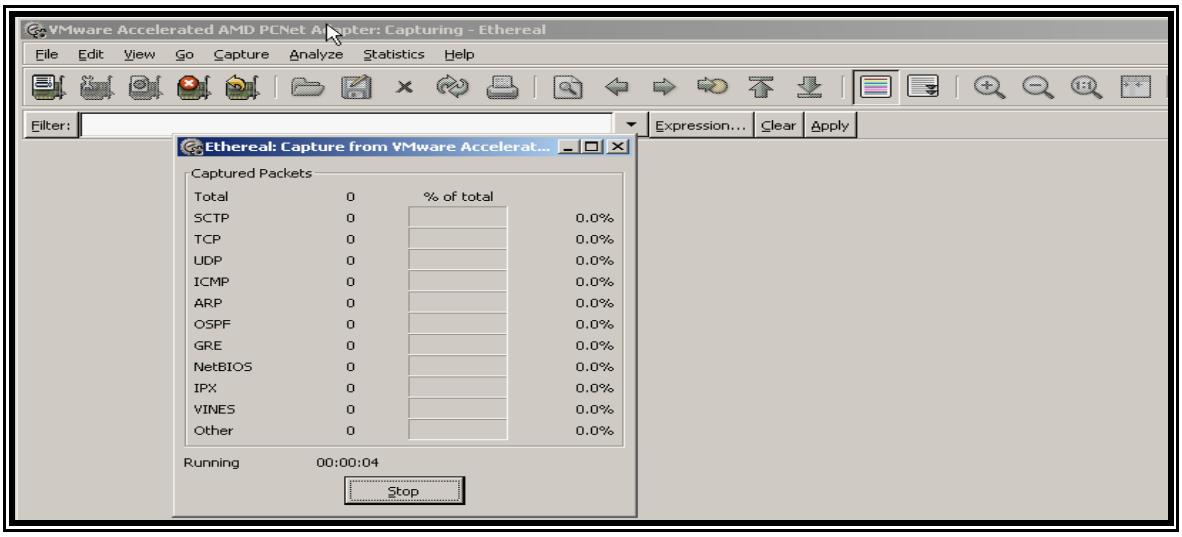


Figura 4.27 Ethereal iniciando captura de Tráfico

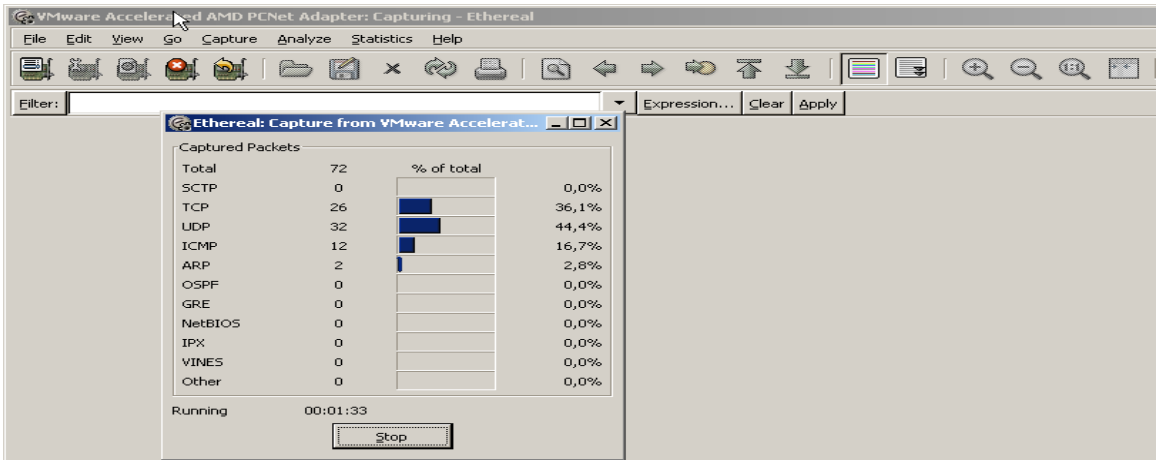


Figura 4.28 Captura de Tráfico finalizado

Esta imagen muestra el proceso de la captura de tráfico hasta donde se decidió detenerlo, mostrando que tipos de protocolos fueron los utilizados y se da su cantidad numeral y porcentual, para tener claro que se estuvo haciendo sobre la red.

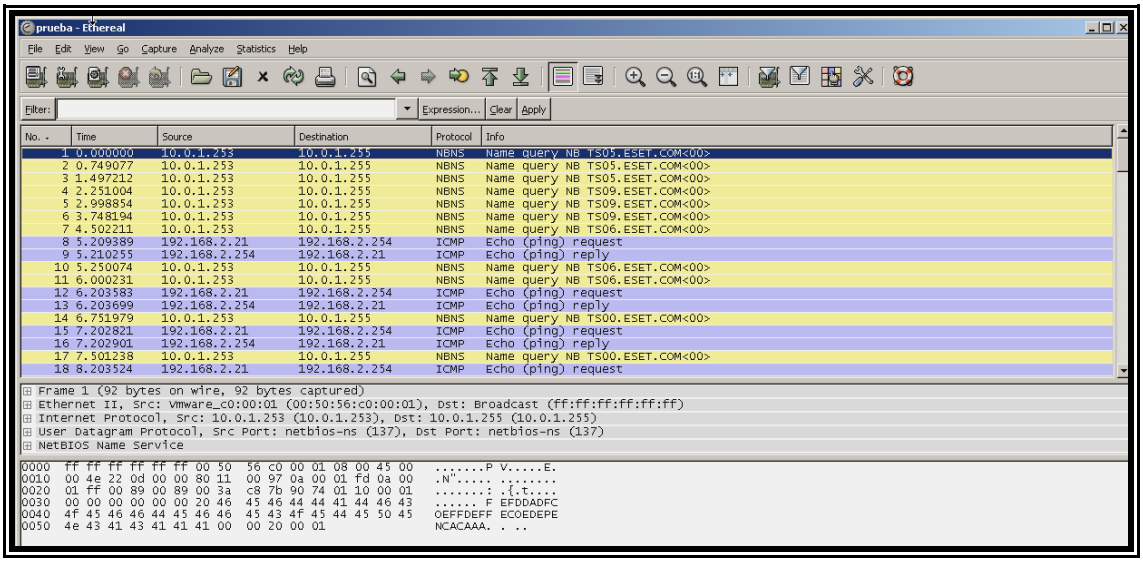


Figura 4.29 Informe detallado final de la captura

Este es el informe que se graba después de la captura, mostrando claramente fuentes, destinos, el protocolo utilizado y una vasta información sobre lo realizado en la red, así como también en lenguaje de maquina se ve en la parte inferior el resultado de la captura; cabe resaltar que no es suficiente el hecho de tener esta información para saber lo que exactamente tenia cada paquete debido a que estos pueden ir encriptados, lo cual complica el conocer su contenido exacto.

4.2.5 Evaluación de Daemons presentes en la red

La evaluación de Daemons se maneja a través del firewall para lo cual se debe tener activado el comando snmp, tal cual lo indica la siguiente imagen, en nuestra red no hubo Daemons por lo que el firewall no detecto nada.

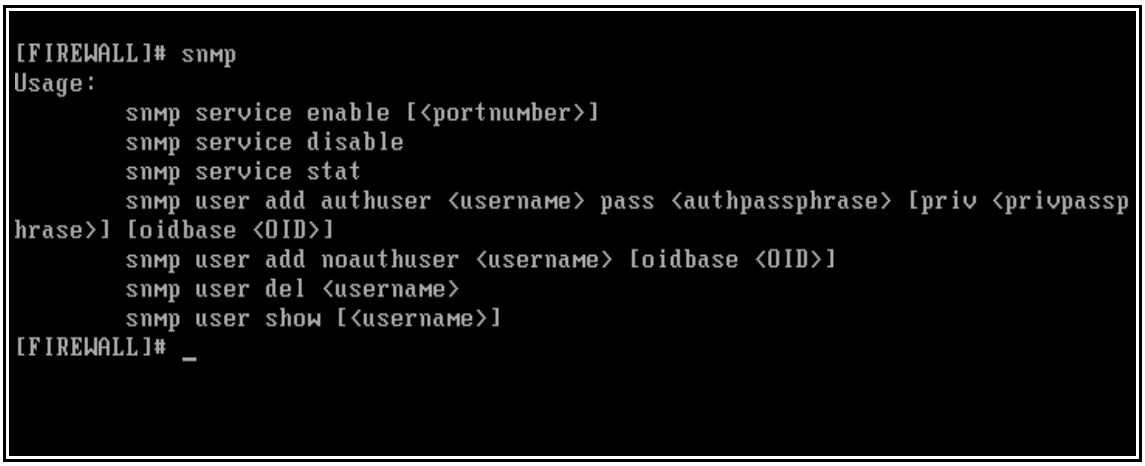


Figura 4.30 Configuración del Firewall para detectar Daemons

El comando snmp puede ser desactivado tal cual se muestra en el grafico siguiente, algo totalmente desaconsejable debido a que en el caso de existir Daemons no los detectaría el firewall.

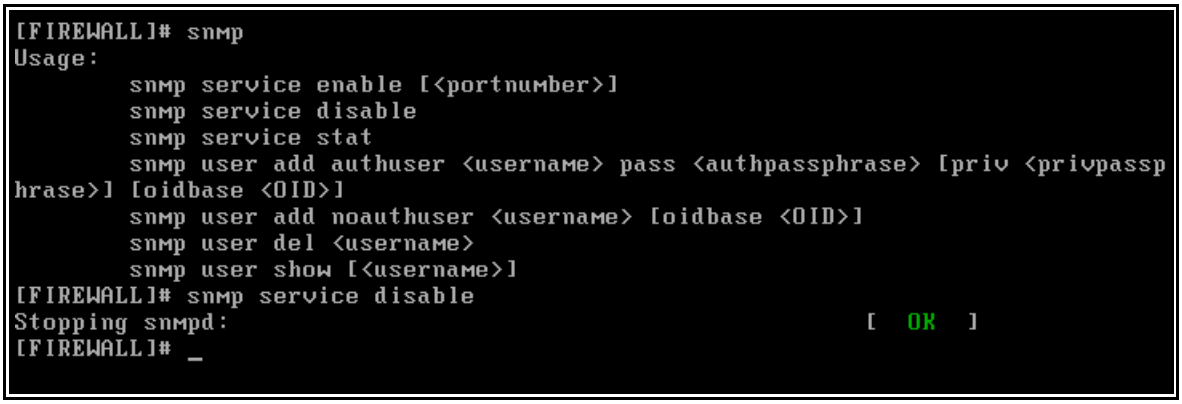
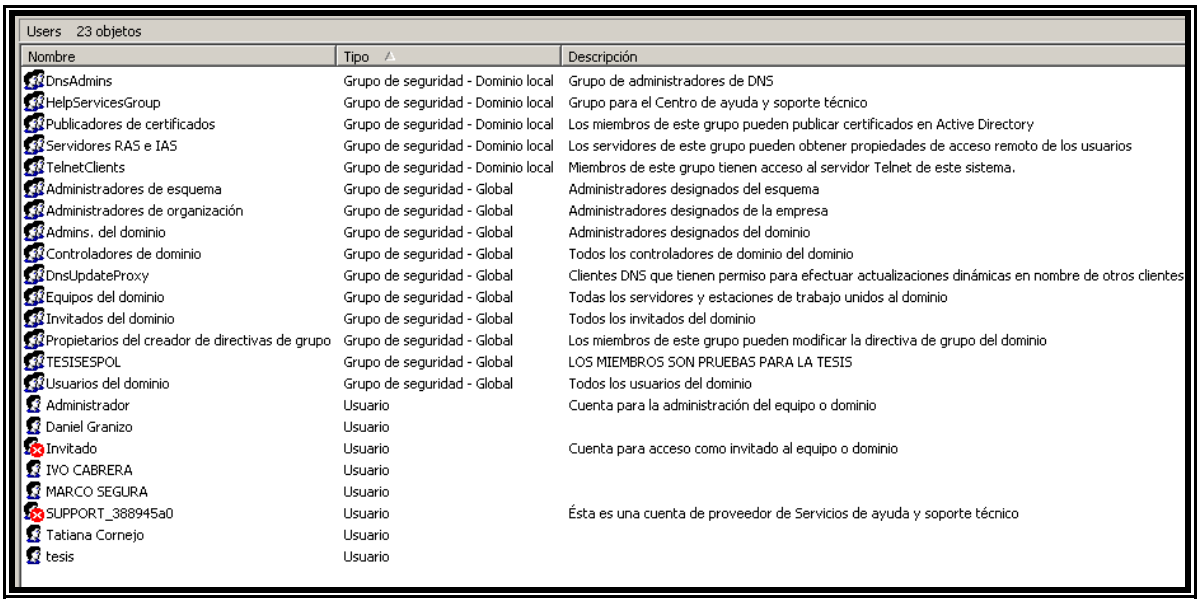


Figura 4.31 Desactivando la detección de Daemons

4.2.6 Usuarios, Grupos de Usuarios NT/2000/XP"

En el proceso de la creación de Usuarios y Grupos de Usuarios se deben configurar las políticas que se consideren pertinentes para cada uno de estos, respetando jerarquizaciones predeterminadas por la organización, así también sabiendo que permisos conceder y cuales no, esto puede hacerse usuario por usuario, o en su defecto creando un grupo de usuarios determinado para lo cual cada aspecto o variante de la red se aplique a todos los usuarios del grupo sin diferencia, y si por una u otra razón se desea aplicar exclusivamente a un usuario algún otro tipo de control, se lo puede realizar sin la necesidad de incluir a todo el grupo.



Users 23 objetos

Nombre	Tipo	Descripción
DnsAdmins	Grupo de seguridad - Dominio local	Grupo de administradores de DNS
HelpServicesGroup	Grupo de seguridad - Dominio local	Grupo para el Centro de ayuda y soporte técnico
Publicadores de certificados	Grupo de seguridad - Dominio local	Los miembros de este grupo pueden publicar certificados en Active Directory
Servidores RAS e IAS	Grupo de seguridad - Dominio local	Los servidores de este grupo pueden obtener propiedades de acceso remoto de los usuarios
TelnetClients	Grupo de seguridad - Dominio local	Miembros de este grupo tienen acceso al servidor Telnet de este sistema.
Administradores de esquema	Grupo de seguridad - Global	Administradores designados del esquema
Administradores de organización	Grupo de seguridad - Global	Administradores designados de la empresa
Admins. del dominio	Grupo de seguridad - Global	Administradores designados del dominio
Controladores de dominio	Grupo de seguridad - Global	Todos los controladores de dominio del dominio
DnsUpdateProxy	Grupo de seguridad - Global	Clientes DNS que tienen permiso para efectuar actualizaciones dinámicas en nombre de otros clientes
Equipos del dominio	Grupo de seguridad - Global	Todas los servidores y estaciones de trabajo unidos al dominio
Invitados del dominio	Grupo de seguridad - Global	Todos los invitados del dominio
Propietarios del creador de directivas de grupo	Grupo de seguridad - Global	Los miembros de este grupo pueden modificar la directiva de grupo del dominio
TESISESPOL	Grupo de seguridad - Global	LOS MIEMBROS SON PRUEBAS PARA LA TESIS
Usuarios del dominio	Grupo de seguridad - Global	Todos los usuarios del dominio
Administrador	Usuario	Cuenta para la administración del equipo o dominio
Daniel Granizo	Usuario	
Invitado	Usuario	Cuenta para acceso como invitado al equipo o dominio
IVO CABRERA	Usuario	
MARCO SEGURA	Usuario	
SUPPORT_388945a0	Usuario	Ésta es una cuenta de proveedor de Servicios de ayuda y soporte técnico
Tatiana Cornejo	Usuario	
tesis	Usuario	

Figura 4.32 Grupos y Usuarios determinados en el Servidor

Determinando claramente las diferencias entre grupos y usuarios, es mas sencillo el evitar que algún usuario no autorizado acceda a una u

otra zona de la red, o que pueda realizar algo inclusive en su sesión, si esto esta negado para el grupo al cual este pertenece.

4.3 Pruebas de Penetración Externa (Ethical Hacking)

Ethical Hacking se ha vuelto una práctica común y es básicamente el recibir una intrusión en la cual no se da un ataque, en este tipo de intrusiones el atacante solo nos indica que nuestro sistema tiene falencias a nivel de seguridad y obviamente donde están ubicadas estas falencias, más no se aprovecha de estas en detrimento de la red.

En la red que implementamos las pruebas fueron hechas de esta forma, ya que solo buscamos errores que presentara el servidor o el firewall, sin la intención de obtener algún recurso en particular; de una u otra forma el Ethical Hacking ayuda a que sepamos en que nos estamos equivocando y buscar medios para la corrección de estos errores, para así estar preparados para ataques que si tengan la intención de hacernos daño.

4.4 Herramientas

Las herramientas para seguridad son muy variadas y se diferencian claramente entre ellas, dando un uso particular a cada uno, el cual se detalla a continuación.

4.4.1 Backdoors

Es una secuencia especial dentro del código de programación mediante la cual el programador puede acceder o escapar de un programa en caso de emergencia o contingencia en algún problema.

A su vez, estas puertas también pueden ser perjudiciales debido a que los crackers al descubrirlas pueden acceder a un sistema en forma ilegal y aprovecharse la falencia. Los más conocidos mundialmente son el BackOrifice y el NetBus, dos de los primeros backdoors, que hasta nuestros días siguen vigentes aunque en menor cantidad dado que la mayoría de los programas antivirus los detectan. Otro muy conocido es el SubSeven, que también se encargó de infectar millones de ordenadores en el mundo.

Los Troyanos Backdoor, se han consolidado como la temible nueva generación de vandalismo cibernético, debido a su modalidad de incursión ilegal en servidores, estaciones de trabajo o PCs, pudiendo tomar el control de los sistemas comprometidos, con los consiguientes daños que ello implica, nada menos que a través de cualquiera de los 65535 puertos TCP/IP. Los Troyanos Backdoor no son esencialmente virus, sino "Herramientas de Control Remoto". Además de codificación

propia, usan cualquier servicio de Internet: correo, mensajería instantánea, Chat, FTP, HTTP, Telnet, etc.

En el año 2007 se han reportado una alarmante cantidad de Troyanos/Backdoor y se estima que existen más de 12,000 troyanos creados desde 1997, los cuales pueden ser monitoreados y controlados a través de un software Cliente asociado. En muchos portales de hackers se distribuyen estos ilegales sistemas, incluyendo las potentes herramientas de "barrido" de puertos TCP/IP que permiten detectar las "puertas traseras" abiertas, mediante las cuales pueden ingresar uno de sus componentes.

Troyanos/Backdoor de acceso remoto

Tienen dos componentes principales: el programa Servidor, que se instala en el sistema de la victima y el programa Cliente que actúa en la computadora del atacante. Ambos programas establecen una relación Cliente/Servidor entre la PC infectada y la del atacante. Por medio de estos troyanos el atacante puede ejecutar remotamente en los sistemas infectados las mismas acciones que el administrador de un Servidor o usuarios de las PC involucradas.

Troyano/Backdoor Cliente

El Cliente se encuentra en el equipo del atacante y generalmente tiene una interfaz con opciones y desde las cuales puede ejecutar las funciones que se hayan programado para que interactúen con los sistemas de las víctimas.

Troyano/Backdoor Servidor

El Servidor que se instala en el sistema de la victima, es un programa que ocupa muy poco espacio y está asociado al Cliente, para poder recibir las instrucciones o través del mismo, ejecutar las funciones que el intruso esté facultado. Los troyanos/backdoor se pueden transmitir por diversos medios:

- ✓ Mensajes de Correo
- ✓ Telnet
- ✓ Redes Compartidas
- ✓ Otros servicios de Internet (HTTP, FTP, ICQ, Chat, Mensajería Instantánea)
- ✓ Usuarios de una misma red local o por medio de dispositivos de almacenamiento.

Recomendaciones:

Algunos aspectos importantes para disminuir el riesgo de intrusiones:

- ✓ Filtrado y protección de las comunicaciones (Firewall).
- ✓ Actualización de software (parches de seguridad).
- ✓ Monitoreo intensivo.
- ✓ No usar Claves de Acceso con nombres obvios o asociados al de los usuarios, como fechas de nacimiento, apelativos, etc.
- ✓ Una estricta política de manejo y control de los usuarios en carpetas compartidas.
- ✓ Cualquier acción preventiva, jamás estará de más.

4.4.2 Firewall

Es un dispositivo de hardware y software que actúa como una barrera protectora entre una red privada y el mundo exterior; se usa para proteger el acceso a los recursos internos desde el exterior, así como para controlar los recursos externos que son accedidos desde la red privada.

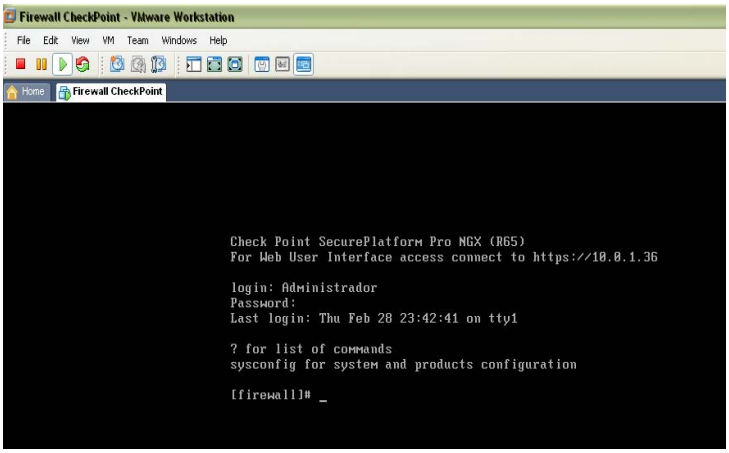


Figura 4.33 Interfaz del Firewall

4.4.3 Networks Sniffers

Son programas de captura de las tramas de red. Generalmente se usan para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.

Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, UTP, fibra óptica etc.) sea compartido por varias usuarios y dispositivos de la red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el sniffer pone la tarjeta de red o NIC en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos (ver niveles OSI) no son descartadas las tramas no destinadas a la MAC address de la tarjeta; de esta manera se puede obtener todo tipo de información de cualquier aparato conectado a la red como contraseñas, e-mail, conversaciones de chat o cualquier otro tipo de información personal (por lo que son muy usados por crackers, aunque también suelen ser usados para realizar comprobaciones y solucionar problemas en la red de modo legal).

Dentro de los principales usos que se les pueden dar a los Networks Sniffers podemos acotar los siguientes:

- ✓ Captura automática de contraseñas enviadas en claro y nombres de usuario de la red. Esta capacidad es utilizada en muchas ocasiones por crackers para atacar sistemas a posteriori.
- ✓ Conversión del tráfico de red en un formato entendible por los humanos.
- ✓ Análisis de fallos para descubrir problemas en la red, tales como: ¿por qué el ordenador A no puede establecer una comunicación con el ordenador B?
- ✓ Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.
- ✓ Detección de intrusos, con el fin de descubrir hackers. Aunque para ello existen programas específicos llamados IDS (Sistema de Detección de Intrusos), estos son prácticamente sniffers con funcionalidades específicas.
- ✓ Creación de registros de red, de modo que los hackers no puedan detectar que están siendo investigados.

4.4.4 Parches Windows

Es sumamente importante el estar actualizado en relación a éste ítem, ya que es común y muy conocido que Windows suele traer errores en sus programas y también en sus sistemas operativos, errores de los cuales un hacker puede valerse y entrar a una PC, y ya que los parches

son programas que se instalan en la PC para corregir estos errores, una vez que Microsoft detecta algún error en sus programas crea éstos para solucionar cualquier inconveniente de forma inmediata.

A continuación se enuncia una definición de lo que es un parche lógico: “Conjunto de instrucciones de corrección para un software en especial, que atañen a una parte o a la totalidad de este que permite resolver vulnerabilidades en el código original de este”.

En resumidas cuentas un parche es una aplicación con la finalidad de cubrir un error encontrado en otra aplicación, en ocasiones solo corrige detalles en el sistema operativo, para protegerlo de posibles ataques exteriores.

4.4.5 X-Windows

El sistema de ventanas **X** fue desarrollado a mediados de los años 1980 en el MIT para dotar de una interfaz gráfica a los sistemas Unix. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para éste. Generalmente se refiere a la versión 11 de este protocolo, **X11**, el que está en uso actualmente.

X es el encargado de mostrar la información gráfica y es totalmente independiente del sistema operativo. El sistema de ventanas X distribuye el procesamiento de aplicaciones especificando enlaces cliente-servidor. El servidor provee servicios para acceder a la pantalla, teclado y ratón, mientras que los clientes son las aplicaciones que utilizan estos recursos para interacción con el usuario. De este modo mientras el servidor se ejecuta de manera local, las aplicaciones pueden ejecutarse remotamente desde otras máquinas, proporcionando así el concepto de transparencia de red.

Debido a este esquema cliente-servidor, se puede decir que **X** se comporta como una terminal gráfica virtual. El hecho que exista un estándar definido para **X** permite que se desarrollen servidores X (XServers) para distintos Sistemas Operativos, plataformas, Hardware, etc... Lo que hace que el código sea muy portable. Por ejemplo: permite tener Xclients ejecutándose en potente servidor UNIX mientras los resultados son visualizados en una PC de escritorio con cualquier otro sistema operativo funcionando.

La comunicación entre el Xclient y el Xserver se realiza por medio de un protocolo conocido como Xprotocol, que constituye una serie bytes interpretados como comandos básicos para generar ventanas,

posicionarlas, o controlar eventos. Los Xclients acceden al Xprotocol mediante el uso de una librería llamada Xlib, que evita al programador de Xclients tener que lidiar con el código binario del Xprotocol. Sin embargo los aspectos de decoración de ventana y manejos de ventanas no están definidos en esta librería. **X** NO ES UN WINDOWS MANAGER, necesita de uno para controlar el manejo de ventanas. Esto trae la ventaja de que permite al usuario instalar el administrador de ventanas que más le agrade, e incluso tener varios instalados eligiendo el más apropiado a la hora de acceder a **X**. También trae la ventaja de que hace de **X** estrictamente un sistema gráfico, de tal modo que un Xclient podría estar enviando un gráfico a una pantalla, a una impresora o a cualquier otro hardware sin darse cuenta, flexibilizando la salida gráfica. Por otro lado, la desventaja que trae el hecho de no tener un único Windows manager es que los programadores de Xclients que desean hacer uso de los recursos de los Windows Manager (botones, barras de deslizamientos, etc) deben elegir un Windows manager específico para programar y contar que el usuario tenga por los menos las librerías de dicho Windows manager instalado. Las librerías de los Windows Manager se conocen como "Tool kits", el estándar **X** provee sólo de un conjunto de herramientas básicas llamadas Xintrisics que permiten a los programadores de Windows Manager armar sus Toolkits sobre estas.

4.4.6 Protocol Spoofing

En términos de seguridad de redes éstos hacen referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Existen diferentes tipos de spoofing dependiendo de la tecnología a la que nos refiramos (los cuales se describirán más adelante) como el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

A continuación se detallan los tipos de Spoofing arriba mencionados:

- ✓ **IP SPOOFING**.- Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UDP o TCP. Hay que tener en cuenta que las respuestas del host que reciba los paquetes irán dirigidas a la IP falsificada. Por ejemplo si enviamos un ping (paquete icmp "echo request") spoofeado, la respuesta

será recibida por el host al que pertenece la IP legalmente. Este tipo de spoofing unido al uso de peticiones broadcast a diferentes redes es usado en un tipo de ataque de flood conocido como smurf ataque. Para poder realizar IP SPOOFING en sesiones TCP, se debe tener en cuenta el comportamiento de dicho protocolo con el envío de paquetes SYN y ACK con su ISN específico y teniendo en cuenta que el propietario real de la IP podría (si no se le impide de alguna manera) cortar la conexión en cualquier momento al recibir paquetes sin haberlos solicitado. También hay que tener en cuenta que los routers actuales no admiten el envío de paquetes con IP origen no perteneciente a una de las redes que administra (los paquetes spoofeados no sobrepasarán el router).

- ✓ **ARP SPOOFING**.- Suplantación de identidad por falsificación de tabla ARP. Se trata de la construcción de tramas de solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo. Explicándolo de una manera más sencilla: El protocolo Ethernet trabaja mediante direcciones MAC, no mediante direcciones IP. ARP es el protocolo encargado de traducir direcciones IP a direcciones MAC para que la comunicación pueda

establecerse; para ello cuando un host quiere comunicarse con una IP emite una trama ARP-Request a la dirección de Broadcast pidiendo la MAC del host poseedor la IP con la que desea comunicarse. El ordenador con la IP solicitada responde con un ARP-Reply indicando su MAC. Los Switches y los hosts guardan una tabla local con la relación IP-MAC llamada "tabla ARP". Dicha tabla ARP puede ser falseada por un ordenador atacante que emita tramas ARP-REPLY indicando su MAC como destino válido para una IP específica, como por ejemplo la de un router, de esta manera la información dirigida al router pasaría por el ordenador atacante quien podrá sniffar dicha información y redirigirla si así lo desea. El protocolo ARP trabaja a nivel de enlace de datos de OSI, por lo que esta técnica sólo puede ser utilizada en redes LAN o en cualquier caso en la parte de la red que queda antes del primer Router. Una manera de protegerse de esta técnica es mediante tablas ARP estáticas (siempre que las ips de red sean fijas), lo cual puede ser difícil en redes grandes. Para convertir una tabla ARP estática se tendría que ejecutar el comando:

- **FORMULA** # *arp -s [IP] [MAC]*

- **EJEMPLO** # *arp -s 192.168.85.212 00-aa-00-62-c6-09*

Otras formas de protegerse incluyen el usar programas de detección de cambios de las tablas ARP (como Arpwatch) y el usar la seguridad de puerto de los switches para evitar cambios en las direcciones MAC.

- ✓ **DNS SPOOFING**.- Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Esto se consigue falseando las entradas de la relación Nombre de dominio-IP de un servidor DNS, mediante alguna vulnerabilidad del servidor en concreto o por su confianza hacia servidores poco fiables. Las entradas falseadas de un servidor DNS son susceptibles de infectar (envenenar) el caché DNS de otro servidor diferente (DNS Poisoning).

- ✓ **WEB SPOOFING**.- Suplantación de una página web real (no confundir con phising). Enruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información de dicha víctima (páginas WEB vistas, información de formularios, contraseñas etc.). La página WEB falsa actúa a modo de proxy solicitando la información requerida por la

víctima a cada servidor original y saltándose incluso la protección SSL. El atacante puede modificar cualquier información desde y hacia cualquier servidor que la víctima visite. La víctima puede abrir la página web falsa mediante cualquier tipo de engaño, incluso abriendo un simple LINK. El WEB SPOOFING es difícilmente detectable, quizá la mejor medida es algún plugin del navegador que muestre en todo momento la IP del servidor visitado, si la IP nunca cambia al visitar diferentes páginas WEB significará que probablemente estemos sufriendo este tipo de ataque.

- ✓ **MAIL SPOOFING**,- Suplantación en correo electrónico de la dirección e-mail de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de e-mails hoax como suplemento perfecto para el uso de phising y para SPAM, es tan sencilla como el uso de un servidor SMTP configurado para tal fin. Para protegerse se debería comprobar la IP del remitente (para averiguar si realmente esa ip pertenece a la entidad que indica en el mensaje) y la dirección del servidor SMTP utilizado. Otra técnica de protección es el uso de firmas digitales.

4.4.7 Daemon

Ésta denominación tan particular se deriva de las siglas en inglés de *Disk And Execution Monitor*, y es un tipo especial de proceso informático que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario (es un proceso no interactivo). Este tipo de programas se ejecutan de forma continua (infinita), vale decir, que aunque se intente cerrar o matar el proceso, este continuará en ejecución o se reiniciará automáticamente. Todo esto sin intervención de terceros y sin dependencia de consola alguna.

Los programas daemons reciben este nombre en los sistemas UNIX. En otros sistemas existen procesos similares como los TSRs de MS-DOS o los servicios de Windows. Los daemons suelen tener las siguientes características:

- ✓ No disponen de una interfaz directa con el usuario, ya sea gráfica o textual.
- ✓ No hacen uso de la entradas y salidas estándar para comunicar errores o registrar su funcionamiento, sino que usan archivos del sistema en zonas especiales (/var/log/ en los UNIX más modernos)

o utilizan otros *demonios* especializados en dicho registro como el syslogd.

Por ejemplo, una máquina que alberga un servidor web utilizará un demonio httpd (HTTP Daemon) para ofrecer el servicio y que los visitantes a dicha web puedan acceder. Otro ejemplo son los demonios *"cronológicos"* como *cron*, que realizan tareas programadas como mantenimiento del sistema en segundo plano.

4.4.8 SNMP

SNMP (por sus siglas en inglés) o Protocolo Simple de Administración de Red es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de SNMP más utilizadas son dos: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas versiones tienen un número de características en común, pero SNMPv2 ofrece mejoras, como por ejemplo, operaciones adicionales. SNMP en su última versión

(SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

Una red administrada a través de SNMP consiste de tres componentes claves:

- ✓ Dispositivos administrados.- son nodos de red que contienen un agente SNMP y residen en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

- ✓ Agente.- es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

- ✓ Sistemas administradores de red (NMS's).- un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.

Comandos básicos de SNMP

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos, los cuales se detallan a continuación:

- ✓ El comando de lectura es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.
- ✓ El comando de escritura es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.
- ✓ El comando de notificación es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.
- ✓ Las operaciones transversales son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y

para recoger secuencialmente información en tablas de variables, como por ejemplo, una tabla de rutas.

Base de información de administración SNMP (MIB)

Una Base de Información de Administración (MIB) es una colección de información que está organizada jerárquicamente. Las MIB's son accedidas usando un protocolo de administración de red, como por ejemplo, SNMP.

Un objeto administrado (algunas veces llamado objeto MIB, objeto, MIB) es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables; existen dos tipos de objetos administrados: Escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un ejemplo de un objeto administrado es *atInput*, que es un objeto escalar que contiene una simple instancia de objeto, el valor entero

que indica el número total de paquetes AppleTalk de entrada sobre una interfaz de un router. Un identificador de objeto (*object ID*) únicamente identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones.

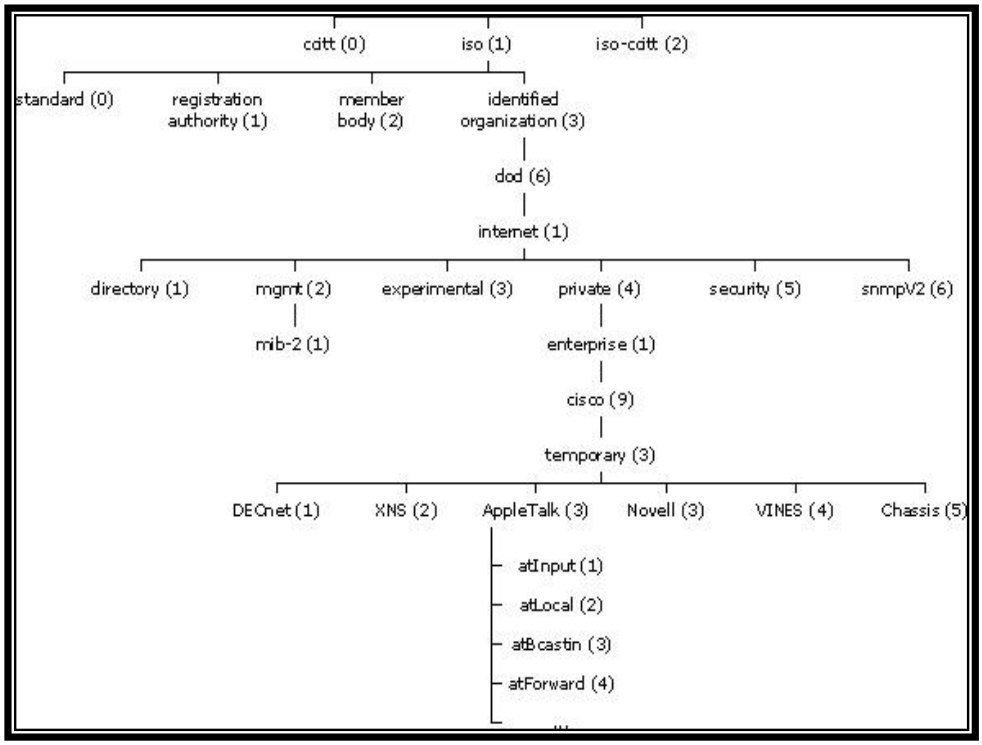


Figura 4.34 El árbol MIB ilustra las variadas jerarquías asignadas por las diferentes organizaciones

Los identificadores de los objetos ubicados en la parte superior del árbol pertenecen a diferentes organizaciones estándares, mientras los identificadores de los objetos ubicados en la parte inferior del árbol son colocados por las organizaciones asociadas.

Los vendedores pueden definir ramas privadas que incluyen los objetos administrados para sus propios productos. Las MIB's que no han sido estandarizadas típicamente están localizadas en la rama experimental. El objeto administrado atInput podría ser identificado por el nombre de objeto *iso.identifiedorganization.dod.internet.private.enterprise.cisco.temporary.AppleTalk.atInput* o por el descriptor de objeto equivalente *1.3.6.1.4.1.9.3.3.1*.

El corazón del árbol MIB se encuentra compuesto de varios grupos de objetos, los cuales en su conjunto son llamados mib-2. Los grupos son los siguientes:

- ✓ System (1);
- ✓ Interfaces (2);
- ✓ AT (3);
- ✓ IP (4);

- ✓ ICMP (5);
- ✓ TCP (6);
- ✓ UDP (7);
- ✓ EGP (8);
- ✓ Transmission (10);
- ✓ SNMP (11).

Es importante destacar que la estructura de una MIB se describe mediante el estándar Notación Sintáctica Abstracta 1 (Abstract Syntax Notation One).

Mensajes SNMP

Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP.

Los puertos comúnmente utilizados para SNMP son los siguientes:

Número	Descripción
161	SNMP
162	SNMP-trap

Tabla VIII: Puertos utilizados por SNMP

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el siguiente formato:

Versión	Comunidad	SNMP PDU

Tabla IX: Formato de Paquetes para SNMP

- ✓ Versión: Número de versión de protocolo que se está utilizando (por ejemplo 1 para SNMPv1);
- ✓ Comunidad: Nombre o palabra clave que se usa para la autenticación. Generalmente existe una comunidad de lectura llamada "public" y una comunidad de escritura llamada "private";
- ✓ SNMP PDU: Contenido de la unidad de datos del protocolo, el que depende de la operación que se ejecute.

Los mensajes GetRequest, GetNextRequest, SetRequest y GetResponse utilizan la siguiente estructura en el campo SNMP PDU:

Tipo	Identificador	Estado de error	Índice de error	Enlazado de variables

Tabla X: Estructura de mensajes

- ✓ Identificador: Es un número utilizado por el NMS y el agente para enviar solicitudes y respuesta diferentes en forma simultánea;
- ✓ Estado e índice de error: Sólo se usan en los mensajes GetResponse´ (en las consultas siempre se utiliza cero). El campo "índice de error" sólo se usa cuando "estado de error" es distinto de 0 y posee el objetivo de proporcionar información adicional sobre la causa del problema. El campo "estado de error" puede tener los siguientes valores:
  - o 0: No hay error;
  - o 1: Demasiado grande;
  - o 2: No existe esa variable;
  - o 3: Valor incorrecto;
  - o 4: El valor es de solo lectura;
  - o 5: Error genérico.
- ✓ Enlazado de variables: Es una serie de nombres de variables con sus valores correspondientes (codificados en ASN.1).

GetRequest.- A través de este mensaje el NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre. En respuesta el agente

envía una respuesta indicando el éxito o fracaso del requerimiento. Si el requerimiento fue adecuado, el mensaje resultante también contendrá el valor del objeto solicitado. Este mensaje puede ser usado para recoger un valor de un objeto, o varios valores de varios objetos, a través del uso de listas.

GetNextRequest.- Este mensaje es usado para recorrer una tabla de objetos. Una vez que se ha usado un mensaje GetRequest para recoger el valor de un objeto, puede ser utilizado el mensaje GetNextRequest para repetir la operación con el siguiente objeto de la tabla. Siempre el resultado de la operación anterior será utilizado para la nueva consulta. De esta forma un NMS puede recorrer una tabla de longitud variable hasta que haya extraído toda la información para cada fila existente.

SetRequest.- Este tipo de mensaje es utilizado por el NMS para solicitar a un agente modificar valores de objetos. Para realizar esta operación el NMS envía al agente una lista de nombres de objetos con sus correspondientes valores.

GetResponse.- Este mensaje es usado por el agente para responder un mensaje GetRequest, GetNextRequest, o SetRequest. En el campo "Identificador de Request" lleva el mismo identificador que el "request" al que está respondiendo.

Trap.- Una trap es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración. El formato de la PDU es diferente:

Tipo	Enterprise	Dirección del agente	Tipo genérico de trap	Tipo específico de trap	Timestamp	Enlazado de variables

Tabla XI: Formato de la PDU

- ✓ Enterprise: Identificación del subsistema de gestión que ha emitido el trap;
- ✓ Dirección del agente: Dirección IP del agente que ha emitido el trap;
- ✓ Tipo genérico de trap:
  - o Cold start (0): Indica que el agente ha sido inicializado o reinicializado;
  - o Warm start (1): Indica que la configuración del agente ha cambiado;
  - o Link down (2): Indica que una interfaz de comunicación se encuentra fuera de servicio (inactiva);

- Link up (3): Indica que una interfaz de comunicación se encuentra en servicio (activa);
- Authentication failure (4): Indica que el agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad);
- EGP neighbor loss (5): Indica que en sistemas en que los routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio;
- Enterprise (6): En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.

✓ Tipo específico de trap: Es usado para traps privados (de fabricantes), así como para precisar la información de un determinado trap genérico;

✓ Timestamp: Indica el tiempo que ha transcurrido entre la reinicialización del agente y la generación del trap;

✓ Enlazado de variables: Se utiliza para proporcionar información adicional sobre la causa del mensaje.

GetBulkRequest.- Este mensaje es usado por un NMS que utiliza la versión 2 del protocolo SNMP típicamente cuando es requerida una larga transmisión de datos, tal como la recuperación de largas tablas. En este sentido es similar al mensaje GetNextRequest usado en la versión 1 del protocolo, sin

embargo, GetBulkRequest es un mensaje que implica un método mucho más rápido y eficiente, ya que a través de un solo mensaje es posible solicitar la totalidad de la tabla.

InformRequest.- Un NMS que utiliza la versión 2 del protocolo SNMP transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados.

4.5 Alcances del Servicio

4.5.1 Objetivo

El objetivo clave de la Implementación de Políticas de Seguridad es el evitar intrusiones a la red de agentes externos, los cuales podrían poner en peligro a los usuarios de la red y a toda la información que cada uno de estos maneja.

4.5.2 Consideraciones

Se debe tratar de lograr un balance entre funcionalidad y disponibilidad, ya que en teoría mientras menos servicios disponibles tenga la red para acceder, menor será la probabilidad de que esta sea atacada, pero se presenta el dilema de hasta que punto esto sirve y es funcional, dado que la idealización de una red busca la conectividad entre usuarios y

estos a su vez con todos los servicios disponibles para realizar cada requerimiento.

4.5.3 Componentes

El poder contar con el Firewall de Checkpoint es estar preparado con un gran producto de seguridad, este dispone de innumerables componentes, los cuales se estima son explotados en un porcentaje no mayor al 60%, pero aun así constituyen un arma excelente en función de tener una red segura.

4.5.4 Técnicas

Diferentes maneras para abordar una red y su detalle son expuestos a continuación.

4.5.4.1 Pruebas de detección, validación y explotación de problemas de seguridad.

Se debe realizar pruebas sobre los siguientes elementos de la red de forma continua para que se demuestre si estamos en capacidad de soportar ataques y cuan vulnerables somos, y también la velocidad de respuesta del sistema a problemas:

- ✓ Servidores (Windows)
- ✓ Bases de datos (MS-SQL y Oracle)
- ✓ Servicios comunes (Web, correo, DNS, FTP)

- ✓ Elementos de comunicación activos (Switches, routers)
- ✓ Mecanismos de seguridad (Firewalls, IPS-IDS, VPN)

4.5.4.2 Desbordamiento de buffer en el segmento de datos, para los servicios de aplicación (capa OSI).

Un desbordamiento de buffer ocurre cuando los datos que se escriben en un buffer corrompen aquellos datos en direcciones de memoria adyacentes a los destinados para el buffer, debido a una falta de validación de los datos de entrada. Esto se da comúnmente al copiar cadenas de caracteres de un buffer a otro.

En el siguiente ejemplo, un programa tiene definidos dos elementos de datos continuos en memoria: un buffer de 8 bytes tipo string, A, y otro de dos bytes tipo entero, B. Al comienzo, A contiene bytes nulos y B contiene el número 3 (cada carácter se representa mediante un byte).

0	0	0	0	0	0	0	0	0	3
Buffer A								Buffer B	

Tabla XII: Buffer antes del desbordamiento

A continuación, el programa intenta almacenar la cadena de caracteres "demasiado" en el buffer A, seguido de bytes nulos para

marcar el fin de string. Al no validarse la longitud de la cadena, se sobrescribe el valor de B:

'd'	'e'	'm'	'a'	's'	'i'	'a'	'd'	'o'	0
Buffer A								Buffer B	

Tabla XIII: Buffer después del desbordamiento

A pesar de que el programador no quería cambiar el contenido del buffer B, el valor de éste ha sido reemplazado por un número equivalente a parte de la cadena de caracteres. Para este ejemplo, en un sistema big-endian que use ASCII, el carácter "e" seguido del byte nulo equivale al número 25856. Si B fuese la única variable aparte de A definida en el programa, la escritura de datos que sobrepasen los límites de B generarían un error como segmentation fault, concluyendo así el programa.

4.5.4.3 Ataque de denegación de servicios para usuarios legítimos por medio de IDS pro-activos.

Las arquitecturas de seguridad buscan aumentar la seguridad por medio de la inclusión dinámica de reglas en el firewalls a partir de los ataques detectados por los IPD-IDS. Este tipo de configuraciones añaden, en algunas ocasiones, mas problemas de los que

solucionan, ya que por medio de IP spoofing se puede lograr la denegación de servicio a usuarios legítimos, para tal efecto, el administrador deberá construir un conjunto de paquetes malformados que permitan verificar la existencia o no de esta vulnerabilidad.

4.5.4.4 Acceso o denegación de servicios sobre servicios perimetrales aledaños a los blancos.

El administrador realizará por medio del escenario externo una evaluación de las condiciones de seguridad de los componentes aledaños a los componentes que puedan convertirse en blanco del ataque. Estos componentes pueden ser: Enrutadores, protectores de intrusos, firewalls, servidores de nombres, entre otros.

4.5.4.5 Fuerza bruta sobre el servicio de acceso remoto.

Se deben poner en práctica controles de contraseñas complejas para todos los usuarios de acceso remoto, independientemente de si el acceso se concede mediante tecnologías de marcación telefónicas o VPN. Se considera que una contraseña es compleja si cumple alguna de las siguientes condiciones:

- ✓ Alfanumérica.
- ✓ Mayúsculas y minúsculas.
- ✓ Contiene al menos un caracter especial.

- ✓ Contiene como mínimo 8 caracteres.

Si se desea, también se pueden utilizar controles avanzados para la administración de cuentas y el registro de acceso a las cuentas (no se debe permitir que se compartan cuentas). Con respecto al acceso remoto, resulta especialmente importante proteger el ambiente mediante políticas estrictas de administración de cuentas, prácticas seguras de registro y funciones para detectar incidentes. Para limitar aún más los riesgos de ataques de fuerza bruta a las contraseñas, puede poner en práctica los controles siguientes:

- ✓ Vencimiento de contraseñas.
- ✓ Bloqueo de la cuenta después de entre 7 y 10 intentos de registro fallidos.
- ✓ Registro del sistema.

Para los servicios de acceso remoto también deben considerarse los sistemas que se utilizarán para acceder a la red o a los hosts. Por tanto, podría resultar conveniente controlar los hosts con acceso remoto a la red.

4.5.4.6 Google Hacking

Consiste en explotar la gran capacidad de almacenamiento de información de Google, buscando información específica que ha sido añadida a las bases de datos del buscador. Si las búsquedas las

orientamos a ciertas palabras clave que nos ayuden a encontrar información sensible, puntos de entrada sensibles a posibles ataques, o cualquier otro tipo de información que tuviera carácter de sensibilidad, estaremos ejecutando un Google hack.

Figura 4.35 Realizando Google Hacking

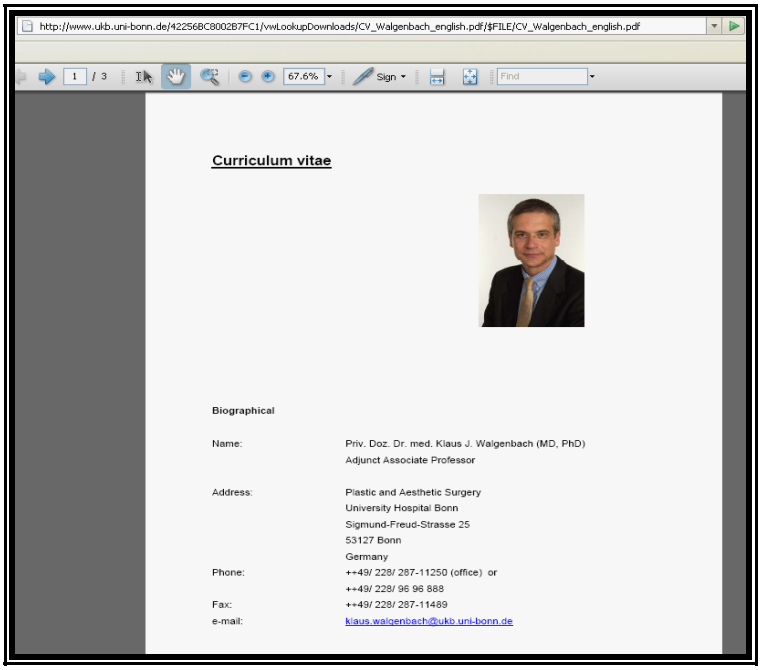


Figura 4.36 Archivo encontrado con Google Hacking

4.5.4.7 Inyección de SQL sobre URLs de sitio Web con parámetros

Algunos formularios o aplicativos Web que se encuentran instalados en los servidores Web, son susceptibles a ataques por medio de manipulación de la entrada, que permite la modificación de sentencias dirigidas a la base de datos. Para tal efecto, el contratista identificará todas aquellas URL en las cuales reciban parámetros de entrada, y realizará las respectivas manipulaciones sobre las entradas, para lograr la modificación de las sentencias SQL.

4.5.4.8 Inyección de comandos de sistema operativo sobre URLs del sitio Web con parámetros.

Algunos formularios o aplicativos Web que se encuentran instalados en los servidores Web, son susceptibles a ataques por medio de manipulación de la entrada, que permite la modificación de los filtros dirigidos al sistema operativo. Para tal efecto, el contratista identificará todas aquellas URL en las cuales reciban parámetros de entrada, y realizará las respectivas manipulaciones sobre las entradas, para lograr la modificación de los comandos de sistema operativo.

4.5.4.9 Pruebas de intrusión y Ethical Hacking

El administrador deberá realizar periódicamente pruebas de intrusión. Con estas pruebas de intrusión se busca analizar la posibilidad de explotación de las vulnerabilidades en la infraestructura tecnológica, la red, Internet y los aplicativos, tendiendo a mejorar los controles y a disminuir los riesgos. También se deben aplicar técnicas de ingeniería social para buscar vulnerabilidades de seguridad relacionadas con las personas de la organización.

4.5.4.10 Endurecimiento de seguridad de servidores, bases de datos y aplicaciones.

Se debe tener una constante revisión de la seguridad, debido a que siempre aparecen nuevas formas de ataques, y se debe estar preparado para recibirlos; una vez instalados los sistemas de seguridad, estos se encuentran dispuestos a salvaguardar la red sobre parámetros de ataque conocidos, pero estos siempre presentan variantes, y conociendo que nuestro servidor es quien permite la viabilidad de la red, es a este a quien debemos dar énfasis en el aspecto seguridad y tratar de endurecer esta periódicamente.

4.6 Perspectiva Externa

4.6.1 Análisis y Diagnóstico conjunto servidores

Los servidores que se encuentren dentro de la red deben estar tipificados claramente para conocer la función que desempeña cada uno (por ej. Web Server, FTPServer), para que en caso de que uno de estos sea atacado, el otro siga trabajando de forma normal, tomando en cuenta que el elemento de protección trabaje exclusivamente sobre el servidor en cuestión.

4.6.2 Análisis y Diagnóstico conexiones con terceros

Siempre que la red deba conectarse a otra la cual no estaba estipulada de forma inicial, se debe dejar en claro que los parámetros y políticas a seguir deben ser exactamente los mismos para que algún usuario de las redes en común no tenga privilegios ni restricciones excesivos o fuera de lugar.

4.6.3 Análisis y Diagnóstico arquitectura de seguridad informática

En esta fase se debe revisar el estado de la infraestructura de seguridad informática y diseñar una arquitectura óptima que disminuya el riesgo para la red a un nivel aceptable. Esta fase debe cubrir los siguientes componentes:

- ✓ Servidores (Sistemas operativos y Servicios).
- ✓ Bases de datos.
- ✓ Aplicaciones.
- ✓ Arquitectura de red.
- ✓ Elementos de comunicación activos (Switches, routers)
- ✓ Elementos de seguridad (Firewalls, IPS-IDS)
- ✓ Modelo de seguridad

Se debe tener claro en que lugar de la red va a ir ubicado cada elemento que compete a la seguridad de la red (por ej. El Firewall), y

estableciendo que función desempeñara cada uno con relación a la parte física (por ej. Un Switch).

4.7 Perspectiva Interna

4.7.1 Análisis y Diagnóstico red inalámbrica

Las redes inalámbricas son las mas susceptibles a ataques debido a que se encuentran dispersas de forma aérea y basta que un usuario se encuentre en el área de cobertura para poder acceder a ella, esto da a entender claramente la necesidad imperativa de una seguridad alta, incluyendo una autenticación con contraseñas complejas, y dando autorización para ciertos equipos de forma tal que la Mac Address también sea un medio de autenticar el ingreso a la red, ya que si alguien penetra y utiliza algún programa de captura de trafico logrando obtener alguna contraseña o en su defecto alguna dirección IP y desea conectarse en un momento posterior, debido a que su Mac Address no esta registrada el sistema lo delatara.

4.7.2 Análisis y Diagnóstico de seguridad LDAP

Algunos formularios o aplicativos Web que se encuentran instalados en los servidores Web, son susceptibles a ataques por medio de manipulación de la entrada, que permite la modificación de los filtros dirigidos a los directorios (LDAP). Para tal efecto, el administrador debe

identificar todas aquellas URL en las cuales reciban parámetros de entrada, y realizará las respectivas manipulaciones sobre las entradas, para lograr la modificación de los filtros de consulta al directorio (LDAP).

CONCLUSIONES Y RECOMENDACIONES

La premisa del trabajo desarrollado es el proveer políticas para conseguir la mayor seguridad posible dentro de un sistema, teniendo presente que no existirá nunca la certeza de estar exentos de un ataque o vulnerabilidad desde el exterior como del interior.

Se realizó una recopilación en base a los principios básicos de la seguridad de redes, incluyendo diferenciaciones claras entre topologías, y variables que se dan en las restricciones que posee cada usuario de la red. Se estableció también un análisis de riesgos, identificando recursos y vulnerabilidades, y la solución que se puede generar para tratarlos, dejando un modelo de seguridad efectivo en cada caso.

Las vulnerabilidades que se pueden suscitar no siempre tienen el mismo origen, claro está que se considera como la principal fuente de problemas a algún factor externo, se debe tener presente que también se puede generar desde el interior de la red, por uno o varios usuarios, quienes tal vez por desconocimiento y/o descuido o algún fallo en la configuración del sistema incurren en errores que comprometen el funcionamiento y desempeño normal de la red.

El proceso en el cual se implementan las políticas tiene que ir de la mano con el asesoramiento a todos y cada uno de los usuarios de la red, y obviamente instalando el sistema que sea el óptimo para los fines determinados de la empresa, esto es fundamental, ya que poniendo como imperativo el hecho de que la seguridad no es una opción, se debe adquirir el software correcto, y cuando digo correcto implica que cubra la gestión de seguridad de forma completa, y sin excesos que le sean demasiados onerosos a la empresa, debido a que si bien es cierto la inversión en seguridad es extremadamente necesaria, no se debe incurrir en gastos excesivos y en ciertas ocasiones hasta innecesarios.

Para éste proceso existen dos variantes, comprar productos licenciados de varias marcas existentes en el mercado (CHECKPOINT, CISCO) y también los denominados Open Source, que como es de conocimiento general abaratan los costos totalmente; el factor a resaltar es que el asesoramiento y capacitación que uno consigue si adquiere productos con licencia no los va a poder conseguir en productos sin una licencia específica.

Estas políticas están en búsqueda del cuidado de algo intangible, pero aún así tal vez lo más valioso de cualquier empresa, su información; si se permite al no tomar las medidas necesarias que alguien acceda a ésta,

estaremos expuestos a cualquier tipo de ataque, mediante el cual se pueda sustraer o averiar dicha información.

Otro acápite importante es el tener un complemento ideal entre funcionabilidad y disponibilidad, debido a que llega una instancia en la cual por tratar de tender una red tan segura, perdemos ciertas funciones que en un momento determinado uno o varios usuarios tendrán la necesidad de utilizarlas, así como también si se da una disponibilidad total de recursos, nos veremos propensos a recibir cualquier tipo de ataque; el balance entre ambos (funcionabilidad y disponibilidad) debe ser muy sensible en función de los requerimientos de la red.

El intercambio de datos debido al crecimiento y necesidad de servicios y productos de consumo mundial tornan la conectividad, entre redes y equipos, obligatoria pero esta condición presenta riesgos que deben ser asumidos en prevención y resolución de forma eficiente y eficaz.

Invertir en seguridad es básico y necesario si se pretende mantener operativa una red de transmisión de datos puesto que eventualmente se presentaran danos por acción u omisión, por simples errores o por ataques premeditados y la seguridad, si bien no los evita en su totalidad, si disminuye las incidencias hasta el punto de hacer estos ataques manejables. Al final todo el dinero invertido en seguridad se vera reflejado

en ganancias por menores perdidas económicas y de tiempo en el que pudiesen quedar fuera de servicio por efecto de reparación los medios de producción informáticos de la empresa.

La implementación de una política de seguridad comienza por demostrar a directivos y a usuarios que la aplicación estricta de las seguridades de redes debe ser tomada en serio y ser conscientes que todo beneficio otorgado conlleva la responsabilidad de velar por la integridad no solo del privilegio otorgado sino por la totalidad de la red.

Considerando que todos los planes de defensa son netamente reactivos, es decir se deducen a partir de la ocurrencia de un incidente y de los daños ocasionados por dicho evento, es necesario mantenerse alerta del desarrollo y tendencias mundiales de las amenazas y especialmente de aquellas que podrían desarrollarse dentro de la red que se intenta proteger.

El desarrollo de una política de seguridad es un proceso específico, puntual y único para cada estructura de red y va acorde a los recursos, deficiencias y vulnerabilidades característicos de los sistemas informáticos. Esta política debe ser un balance entre el grado de dificultad que se le quiera inyectar a la red, sin olvidar que a mayor grado de seguridad mayor dificultad de aplicación procesamiento retardos y manejo

de información, y la simplicidad necesaria para que puedan ser puestas en practica por todos los usuarios.

Mantener la rigidez pero tener presente que otorgar un bajo nivel de grados de libertad permite a los miembros de la empresa despejar su mente e indirectamente mejorar su productividad.

Capacitar constante y periódicamente a todos los miembros de la compañía sobre las actuales tendencias de los riesgos, sus formas más comunes de presentación y las consecuencias en que derivan. Mantener un contacto permanente y amigable con los usuarios hace que apliquen en mayor medida los puntos expuestos y que se sientan en confianza de concurrir en consultas derivando en optimización de la política de seguridad aplicada.

APÉNDICE

Políticas de Seguridad

Las Políticas de seguridad se pueden resumir en visión, prevención, capacitación y predisposición por parte de todos para contribuir a la protección de los recursos.
Pero una políticas mas concreta se puede detallar en una clasificación dentro de los siguientes grupos:

1. Sistemas Operativos:
    - Corregir y protegerse de la configuración de fábrica blindando las vulnerabilidades conocidas.
    - Centralizar control únicamente a terminales y usuarios específicos.
    - Gestionar adecuadamente dominios, usuarios, y claves. Evitando usuarios compartidos.
    - Gestión de cuentas.
    - Restringir comandos esenciales a usuarios estratégicos.
    - Únicamente Aplicaciones adecuadas permitidas.
    - Puertos riesgosos o en desuso bloqueados.
    - Bloqueo de paneles de controles, archivos de registros y eventos.
    - Compartir los dispositivos periféricos estrictamente necesarios.
    - Software Licenciado, adecuadamente parchado y actualizado.
    - Configurar VPN en caso de necesitar usuarios remotos.
2. Administrador
    - Análisis de vulnerabilidades y pruebas de intrusión periódicas.
    - Aislar independientemente los servidores por servicios.
    - Mantenimiento preventivo, esquemático, coordinado y programado tanto de hardware y software.
    - Imágenes de restauración y respaldos de los elementos de red.

- Monitoreo de eventos permanentes y reportes hacia celulares, correo u otro medio de acceso inmediato.
- Monitoreo remoto de procesos y aplicaciones.
- Usuarios compartidos bajo petición puntual y formal acuerdo estratégico.
- Historial de danos, vulnerabilidades y eventos más comunes en la red organizado por equipos y por usuarios.
- Diagrama preciso y exacto al día de la red y todos sus elementos.
- Conocimiento actualizado de riesgos potenciales en vigencia local y mundial.
- Plan inmediato de contingencia para enfrentar los eventos.
- Control de accesos lógicos y físicos.
- Usuarios remotos únicamente en caso de ser necesarios utilizando VPNs.
- Gestionar cuentas especialmente en remover empleados removidos.
- Bloquear interfaces y puertos riesgosos o en desuso en todos y cada uno de los elementos de red.
- Denegar peticiones de direcciones críticas como aquellas direcciones de loop.
- En caso de conexiones con redes ajenas exigir como condición minima políticas de seguridad semejantes en rigidez a las locales.
- Advertir y publicar todos los medios de ataque al usuario especialmente sobre todos los tipos de ingeniería social y sus consecuencias.
- Capacitación permanente a todos los usuarios con privilegios de acceso de red.
- Implementar políticas de seguridad precisa, efectiva y concreta pero sobre todo fácil de aplicar contra ataques inminentes.

- Brindar flexibilidad con aplicaciones no productivas que más bien pueden incentivar el rendimiento de los usuarios al despejarlos mentalmente.

3. Contra Fuegos.
    - Blindaje y corrección contra la configuración de fábrica.
    - Bloqueo de interfaces en desuso.
    - Restricción de aplicaciones.
    - Mails seguros en plain text (texto plano).
    - Encriptación.
    - Acceso seguro para validación de todas las cuentas.
    - Software parchado y actualizado.
    - Políticas de transferencias denegados por defecto y permitidos puntualmente.
4. Contraseñas
    - Son únicas e intransferibles.
    - Claves provisionales iniciales como de restitución deben ser variadas al primer acceso.
    - Base de datos de claves deben almacenarse y respaldarse en medios debidamente protegidos.
    - No usar recordatorios visibles postnotes en la pantalla, flys, agendas, etc.
    - Cambiar claves periódicamente (tiempo de validación).
    - Tiempo máximo de vida 3 meses.
    - Fácil de recordar.
    - Mínimo de 8 y máximo de 14 caracteres.
    - Combinación de la menos 2 mayúsculas, 2 minúsculas, 2 numéricos y 2 caracteres especiales.
    - No utilizar secuencias elementales numéricas ni alfabéticas ya sea ascendente o descendente.
    - Mayores atributos mayores responsabilidades por parte de los usuarios.

- Si se va a usar una clave única debe ser suficientemente compleja y rigurosamente vigilada.
- No almacenar contraseñas en macros, teclas de función ni en ningún medio de acceso automático.

5. Usuarios
    - Mantener el sigilo inherente a todo lo relativo a su situación laboral y contraseñas en uso.
    - Asistir y aplicar concientemente todas las capacitaciones para contribuir a la seguridad informática.
    - Administrar responsablemente los atributos con ciertos grados de libertad teniendo presente que la actividad principal del trabajador es producir.
    - No publicar en Internet archivos, ni información de interés aunque fueren datos personales.
    - Usar y actualizar software de protección como antivirus, contrafuegos personales, antimalware, antispy, etc.
    - Usar aplicaciones seguras menos vulnerables como navegar en firefox, desactivar ActiveX, leer mails en PlainText, etc.…
    - No abrir links directamente en fuentes no confiables. Tipearlos directamente en la barra de direcciones.
    - Tomar precaución contra todos los variados métodos de ingeniería social (recopilación de información primordial) especialmente no llenar formularios ni encuestas en Internet.
    - No recibir ni enviar cadenas de mails ni los archivos que en ellas se envían.

BIBLIOGRAFIA

Microsoft Corporation, "Managing and maintaining a Microsoft Windows Server 2003 Environment", Craig Zacker.

Guía rápida de seguridad de la NSA (National Security Agency, U.S.A.)
www.nsa.gov/snac/support/sixty_minutes.pdf

Synmatec, "Understandig Virus behaviour"
http://www.symantec.com/avcenter/reference/virus.behavior.under.win.32.pdf

Eset Ranking
http://www.eset.eu/global-threat-trends-2007-july
www.eset.com/threat-center/case_study/Global_Threat_Trends_July_2008.pdf

Eset Definiciones
http://www.eset.eu/threat-centre/threat-dictionary

Checkpoint Internal Network Security
http://www.checkpoint.com/form/whitepaper/WebWhitePaperCheck_Point_Bouchard_Internal_Networks_ty.html

Definiciones de Peligros potenciales
http://www.viruslist.com/en/viruses/encyclopedia
http://www.viruslist.com/en/glossary

E-Crimes Security Summary 2007
http://www.cert.org/insider_threat/ecrimesurvey07.pdf
http://www.cert.org/insider_threat/ecrimesurvey06.pdf

Peligros cibernéticos
http://www.cert.org/insider_threat/combatthreat0408.pdf

Denial of Services según Cert
http://www.cert.org/tech_tips/denial_of_service.html
http://www.cert.org/historical/Managing_DoS.pdf

Reporte anual 2007 según Cert
www.cert.org/research/2007research-report.pdf

Standard ISO17799
http://17799.standardsdirect.org/

Cyber Threats según kaspersky
http://www.kaspersky.com/cyberthreats