ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Gestión de Seguridades en Redes de Comunicaciones: Análisis e Implementación de Herramientas de Gestión de Seguridad en la Red de Datos de la FIEC"

TOPICO ESPECIAL DE GRADUACION

Previo a la obtención del Título de

INGENIERO EN ELECTRICIDAD

ESPECIALIZACION ELECTRONICA

Presentada por:

Daniel Efrén Pineda Mejillones

GUAYAQUIL – ECUADOR

AÑO 2004

Agradecimiento

Al Ing. Edgar Leyton

Director de Tópico, por su valiosa ayuda y colaboración para la realización de este trabajo.

Dedicatoria

A Dios por guiarme y darme la fortaleza y sabiduría para culminar mi carrera profesional.

A mis padres y hermanas por todo el apoyo y amor que siempre me han brindado

A la memoria de mi abuelita, profesora Olga Villao de Mejillones, quien siempre me dio ánimos y fuerzas para cumplir con mis objetivos.

Daniel Pineda M.

Tribunal

Ing. Hernán Gutiérrez Presidente del Tribunal	Ing. Edgar Leyton Director de Tópico
Ing. Guido Caicedo Vocal Principal	Ing. Juan Carlos Avilés Vocal Principal

Declaración Expresa

La responsabilidad por los hechos, ideas y doctrinas expuesto en este proyecto, nos corresponden exclusivamente; y, el Patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

(Reglamento de Exámenes y Títulos Profesionales de la ESPOL)

Daniel Efrén Pineda Mejillones

RESUMEN

En la actualidad, la seguridad en redes de datos se ha convertido en tema de vital importancia en todas las empresas. El área de Sistemas y Comunicaciones en las corporaciones son las responsables que la confidencialidad de la información y los procesos que se ejecutan en las empresas estén seguros de cualquier infiltración de atacantes informáticos que pudieran hacer un mal uso de la información de la compañía.

Los ataques a redes de computadoras de diferentes empresas son cada vez más frecuentes, algunos de esos ataques han sido críticos a nivel de dejar pérdidas económicas muy grandes por la baja de los servidores que han sido objeto de los ataques. La industria de la informática está atenta a la diversidad de ataques que los denominados “hackers” realizan, cada vez con técnicas más avanzadas; es por esto que se han desarrollado herramientas de gestión que ayudan al administrador de la red a verificar las vulnerabilidades que existen (confirmadas o potenciales) en la red y a monitorear la actividad del tráfico que circula por la misma.

Este proyecto está enfocado en el análisis y aplicación de estas herramientas y en los criterios de diseño para una red de datos segura, gracias a la ayuda de las herramientas de rastreo de vulnerabilidades (conocidas como *scanners* de red), las herramientas de detección de intrusiones y los sistemas de firewall. La aplicación de estas herramientas se la ejecuta en la red de datos de la FIEC con el objetivo de verificar si existe algún tipo de vulnerabilidad de la red de datos y sugerir topologías que permitan incrementar el nivel de seguridad en la red.

En el capítulo 1 se describen conceptos básicos de seguridades en redes corporativas; se analiza los diferentes puntos en una red que son propensos a ataques. Se describe también los diferentes tipos de falencias en las tecnologías de transmisión de datos y de los protocolos utilizados en una red de computadoras. También se describe las diferentes herramientas que existen en el medio para prevenir ataques en redes de datos y que ayudan en la gestión de la red.

El capítulo 2 se profundiza en los tipos de vulnerabilidades en redes de datos, los métodos y herramientas que los piratas informáticos utilizan para aprovechar estas vulnerabilidades y así obtener acceso a los sistemas e información en una red privada. También conoceremos los pasos básicos que el administrador de red debe seguir para protegerse de los diferentes ataques que pudieran ocurrir en la red.

En el capítulo 3 se realiza un análisis de la infraestructura de red de la FIEC, a nivel físico y lógico, describiendo el tipo de equipos, protocolos y dispositivos de

seguridad con que cuenta la red. En este punto también hablaremos de las herramientas de gestión de seguridad que se implementaron: CISCO SECURE SCANNER que es una herramienta de verificación de vulnerabilidades en dispositivos de red y la herramienta de detección de intrusiones ETRUST INTRUSION DETECTION con la que verificaremos actividad en la red que pudiera ser sospechosa y ser considerada como algún tipo de ataque.

En el capítulo 4 analizaremos los resultados que se obtuvieron con las pruebas de verificación de vulnerabilidades, enfocadas principalmente en los servidores CEIBO, PALMA y CEDRO que son los que brindan servicios de internet (email, web, dns, etc.) a los usuarios de la FIEC. Los resultados son dados en base a la implementación de las herramientas ETRUST INTRUSION DETECTION y CISCO SECURE SCANNER.

En el capítulo 5 se expone las sugerencias que se brinda a la FIEC para incrementar el nivel de seguridad para la red de computadoras de la FIEC, con alternativas de diseño para la red LAN, basado en la implementación de un firewall y la aplicación de políticas de acceso para proteger los servidores de accesos no autorizados.

ÍNDICE GENERAL

CAPÍTULO II

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La seguridad en las redes de datos es un factor fundamental en las comunicaciones. Millones de dispositivos de red compartiendo información por medio de la Internet obliga a que las redes privadas de las diferentes corporaciones mantengan altos esquemas de protección y de gestión para controlar el acceso a los diferentes recursos de una red.

Gracias al avance tecnológico que se ha desarrollado en el campo de la seguridad en redes de datos, podemos contar con herramientas muy efectivas para el control de ataques: las herramientas "cortafuegos" o *firewalls*, las herramientas de detección de intrusiones, los programas de gestión de redes, etc.

En cuestión de seguridad informática, no está dicha la última palabra; cada vez los piratas informáticos, conocidos como "*hackers*" desarrollan técnicas avanzadas para tratar de evadir los sistemas de protección de redes. Sin embargo, siempre hay que estar un paso mas allá y eso depende de la iniciativa de las personas encargadas de la administración de la red. No es suficiente con esperar a que seamos víctimas de un ataque para tomar las medidas correctivas sino siempre estar alertas y verificar siempre que nuestros sistemas estén protegidos contra cualquier tipo de vulnerabilidad.

Se eligió a la red de la FIEC para poder implementar herramientas que ayuden al administrador a detectar o controlar si los recursos de la red (servidores principalmente) son propensos a sufrir un tipo de ataque por alguna vulnerabilidad en el sistema operativo de los mismos y también para controlar si existe algún tipo de tráfico en la red que tenga un patrón de ataque.

El objetivo de este proyecto es brindar a la FIEC un análisis de la seguridad de la red y recomendar diseños en la topología que incluyen equipos y herramientas que la protejan no solo de posibles ataques desde Internet sino también de ataques que puedan provenir de algún usuario en la misma red interna.

CAPÍTULO I

INTRODUCCIÓN A LOS CONCEPTOS DE SEGURIDAD PARA REDES COORPORATIVAS ANTE LOS RIESGOS DE INTERNET Y EL PORQUÉ DE UN PLAN DE GESTIÓN DE SEGURIDAD

1.1. Introducción

En este capítulo revisaremos el por qué la necesidad de la seguridad en redes de computadoras a nivel corporativo. Actualmente las diferentes empresas en el mundo tienen presencia en Internet, la economía en Internet está cambiando de manera rápida la manera en que trabajamos, vivimos, aprendemos, etc. Las grandes compañías e instituciones reconocen el rol estratégico que juega la Internet en la capacidad que tengan las mismas para sobrevivir en la dura competencia – a todo nivel – que se juega en este siglo 21.

El comercio electrónico se ha popularizado en los últimos años, por lo tanto, compradores y vendedores necesitan que la información de las diferentes transacciones que se realizan sea transmitida de manera segura. De igual

manera, mucha de la información de una compañía como datos de clientes, proveedores, proyectos actuales o futuros, bases de datos con información crítica, etc. se encuentra en la red privada de cada empresa, esta información en manos de personas inescrupulosas que de alguna manera se infiltran en la red puede causar grandes perjuicios a las empresas; el robo de información o el daño a sistemas o recursos son algunos de los problemas que se pueden presentar, por lo que es necesario restringir el acceso a la red solo a personas autorizadas.

Ante la necesidad de seguridad de la información, han surgido varios métodos de protección para las redes de computadoras, métodos como los cortafuegos (*firewalls*), sistemas de detección de intrusos (*Intrusion Detection Systems o IDS*) y sistemas de detección de contenido (*Content Inspection*), por nombrar a los mecanismos más conocidos.

Sin embargo, los métodos para burlar estos mecanismos de seguridad son cada vez mas complejos, mas avanzados, por lo que ninguna medida de seguridad que se tome para salvaguardar la red es ciento por ciento efectiva, de ahí la necesidad de implementar un sistema más formal de seguridad; no en el hecho de instalar un dispositivo para asegurar la red, sino en un plan de gestión de seguridad que implique revisión permanente de los componentes que protegen la red, actualización de políticas de seguridad en *firewalls*, y pruebas de vulnerabilidad para evaluar si los equipos o mecanismos de protección están trabajando de manera eficiente.

Ese es el propósito de este proyecto, realizar una gestión de seguridades para Internet, en otras palabras ¿qué es lo que se debe hacer para mantener mi red segura ante ataques de piratas informáticos (*hackers*)?.

Esta gestión se la implementará en la red de computadoras de la Facultad de Ingeniería en Electricidad y Computación de la ESPOL, para esto contaremos con herramientas que nos ayudarán a detectar la confiabilidad del sistema de protección actualmente implementado, así como con los criterios necesarios para establecer las recomendaciones para mejorar el esquema de protección en la red de la FIEC.

En este capítulo se revisará los principales problemas de seguridad en una red, los diferentes tipos de ataques, los diferentes dispositivos de seguridad disponibles y los criterios para el diseño de redes seguras.

1.2. Conceptos básicos de seguridades

Las entidades (organizaciones, empresas o instituciones educativas) con presencia en Internet tienen varios servicios disponibles al público:

- Uno o más servidores Web
- Servidores de correo electrónico u otro sistema de comunicación global
- Servidores para almacenaje y transferencia de archivos (servidores FTP)

Adicionalmente a estos servidores “públicos”, en la red pueden existir recursos como por ejemplo servidores de base de datos con información crítica referente a la compañía, este tipo de información obviamente está disponible de manera restringida. Para un hacker este puede ser un blanco interesante de ataque, puede valerse de otros servidores para llegar al blanco, por lo que es imprescindible aplicar reglas de acceso a los recursos de la red.

Lo primero que se debe tener en cuenta es conocer cuales son los recursos disponibles en la red y a los que se desea proteger. Como se mencionó anteriormente, se debe establecer lo que se conoce como **Reglas o Políticas de Seguridad en la Red**.

1.2.1. Políticas de Seguridad de la Red

Una política de seguridad es un conjunto de normas que rigen el comportamiento de una red de computadoras en relación a la seguridad. Es por eso que lo primordial es establecer los recursos disponibles en la red para establecer reglas de qué es lo que se puede y debe hacer por parte de los usuarios (internos y externos) con estos recursos.

La seguridad en las redes debe empezar desde el acceso físico a los equipos o componentes de la red. Por lo general existe un centro de cómputo en el que se encuentran los equipos de conectividad como lo son los ruteadores (*routers*), conmutadores (*switches*) y concentradores (*hubs*), los servidores (Web, FTP, Proxy, Mail, base de datos, etc.) y los equipos de protección (firewalls, IDS, etc.).

Esta área siempre es considerada crítica para cualquier empresa, por lo tanto una de las primeras medidas es restringir el acceso físico al área solo a personal debidamente autorizado.

Una red segura es aquella capaz de ofrecer típicamente las siguientes características:

- **Confidencialidad:** Este concepto está orientado a los datos, es decir, la información debe mantenerse reservada dentro de los límites de la empresa. Para mantener el nivel de confidencialidad se recomienda como solución la encriptación de la data.
- **Integridad:** El nivel de integridad de los datos se rige en los parámetros de información completa y exacta. Ambos factores son críticos después de haber manipulado los datos. Una medida de seguridad típica es el uso de firmas digitales, permisos de acceso a los archivos o carpetas a nivel de sistemas operativos.
- **Autenticación:** Es decir, buscar asegurar que sólo los usuarios autorizados tengan acceso a los datos y/o servicios. Como soluciones típicas se suele implementar las claves de acceso, sistemas de acceso biométrico, por citar algunos ejemplos.

En la actualidad se puede probar la confiabilidad de un sistema realizando pruebas de detección de vulnerabilidades en una red y pruebas de detección de intrusos. Existen diferentes tipos de herramientas (las mismas que utiliza un hacker) para realizar esta evaluación, es lo que se conoce como ***ethical***

hacking. Este es un concepto que se puede definir como “Probar los diferentes métodos que un pirata informático puede seguir para dañar a la red, antes de que realmente lo haga”.

La infraestructura de seguridad es el complemento de las medidas, políticas, procedimientos y prácticas a las tecnologías y productos que representan una iniciativa de seguridad de la organización. El éxito de estas medidas es principalmente detectar los problemas para retardar el daño y para mitigar los efectos de los errores y ataques.

Desde esta perspectiva el realizar pruebas de vulnerabilidades y de detección de intrusos son partes necesarias de la infraestructura de seguridades, pero no representan por ellas mismas una infraestructura completa de seguridad.

1.3. Tipos de vulnerabilidades en redes de computadoras

La causa típica de las redes con seguridad inadecuada es la falla en la implementación de políticas de seguridad y en el mal o nulo uso de herramientas que estén disponibles. Es vital que las empresas desarrollen planes operativos de seguridad y respuesta a eventos relativos.

Existen tres principales problemas que tienen que ver con la seguridad en una red de computadoras:

- **Debilidad en la tecnología**—Cada tecnología de redes y de computadoras tiene inherentes problemas de seguridad.
- **Debilidad en la configuración**—Hasta la tecnología más segura, cualquier deficiencia en la configuración o en el uso puede representar problemas de seguridad.
- **Debilidad en las políticas**—Una pobre definición o inapropiada implementación en la administración de políticas de seguridad puede convertirse en una fuente para el ingreso de usuarios no autorizados a los recursos de la red.

Existe gente técnicamente calificada que ansiosa espera tomar ventaja de las debilidades en la seguridad de redes y continuamente descubrir nuevas brechas de seguridad. A continuación se explica con mayor detalle cada una de los problemas descritos anteriormente.

1.3.1. Debilidad en la tecnología

Las tecnologías en computadoras y redes de datos tienen debilidades o vulnerabilidades en la parte de seguridad de manera intrínseca. Las debilidades en la tecnología que analizaremos en esta sección incluyen TCP/IP, los sistemas operativos y las debilidades en los equipos activos de red, como se ilustra en la figura 1-1.

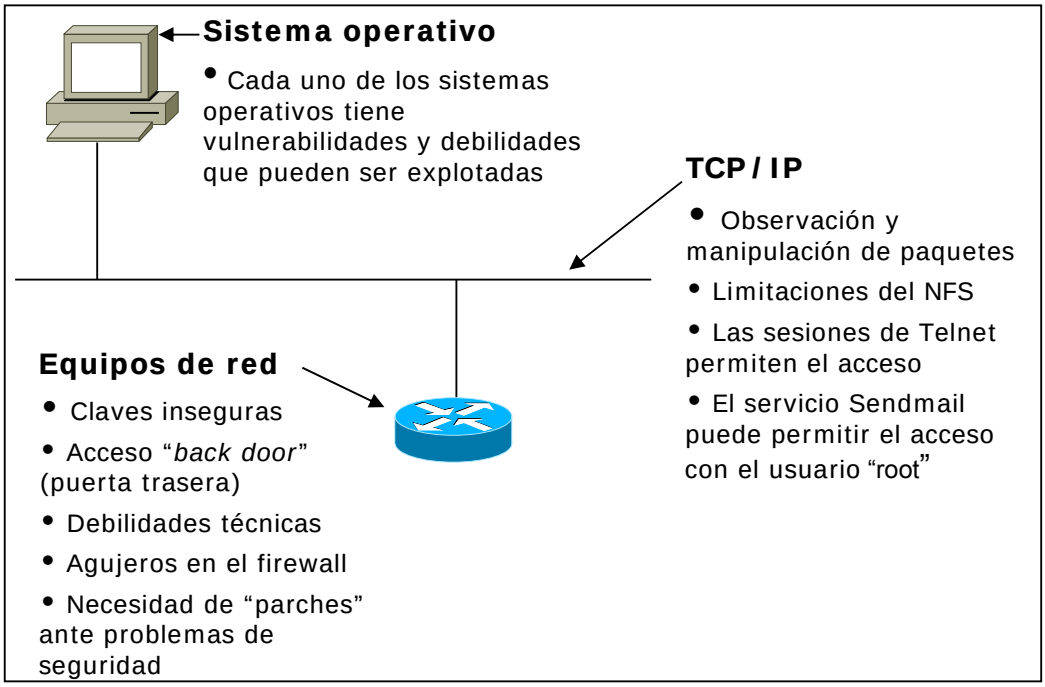


Figura No. 1-1. Equipos de computación y de redes de datos que contienen debilidad en la tecnología

1.3.1.1. Debilidad de TCP / IP

TCP/IP es un protocolo que fue diseñado como un estándar abierto para facilitar las comunicaciones. Cada uno de los servicios, herramientas y utilitarios derivados de este protocolo fueron diseñados para ayudar a las comunicaciones abiertas. Ponemos a consideración del lector algunos ejemplos de las vulnerabilidades intrínsecas de TCP/IP y sus servicios:

- Los paquetes de cabecera (*headers*) IP, TCP y UDP y su contenido pueden ser observados, modificados y re-enviados sin ser detectados.

- El sistema de archivos de red NFS (*Network File System*) puede habilitar acceso confiable pero inseguro a un host. NFS no provee autenticación de usuario y utiliza puertos UDP asignados de manera aleatoria para las sesiones, lo que hace virtualmente imposible limitar el protocolo y el acceso de usuario.

- Telnet es un servicio poderoso que brinda a los usuarios acceso a algunas utilidades y servicios de Internet. Los hackers pueden utilizar sesiones de Telnet especificando un parámetro como lo es el número de puerto adicionalmente al nombre de host o dirección IP para iniciar un diálogo interactivo con un servicio disponible en Internet.

- En sistemas UNIX está disponible el *demonio* **sendmail**, este demonio puede permitir el acceso como usuario root de UNIX. Sendmail es un programa usado para enviar correos electrónicos en sistemas UNIX. Es un programa muy complejo que tiene un largo historial de problemas de seguridad que incluye lo siguiente:

    - Sendmail puede ser utilizado para obtener acceso a nivel de usuario root en el sistema, explotando los comandos propios de sendmail en transmisiones de e-mail fabricadas.
    - Los intrusos pueden determinar sobré que versión de UNIX se está ejecutando sendmail, revisando el número de versión dentro de los e-mails de retorno durante el proceso de transmisión de e-mails fabricados. Esta información puede entonces ser utilizada para

realizar ataques sobre vulnerabilidades específicas para esa versión de sistema operativo.

- Con sendmail se puede aprender cuáles hosts pertenecen a un mismo nombre de dominio.
- Sendmail puede ser explotado para re-dirigir correos a destinatarios no autorizados.

1.3.1.2. Debilidad en los sistemas operativos

Distribuciones de Linux, UNIX, Microsoft Windows 2000, Windows NT, Windows 9X e IBM OS/2; cada uno de estos sistemas operativos tienen problemas que han sido detectados y publicados.

El organismo CERT (Computer Emergency Response Team, www.cert.org) tiene una gran base de información sobre debilidades reportadas para sistemas operativos así como la solución a aplicarse para cada caso reportado.

1.3.1.3. Debilidad en los equipos de red

Los equipos de red de cada fabricante tienen debilidades en la seguridad que deben ser detectados; es responsabilidad de las casas fabricantes de estos equipos informar sobre la medida de protección contra la vulnerabilidad detectada. Algunos ejemplos incluyen protección inapropiada de las claves de acceso, fallas en la autenticación, fallas en los protocolos de enrutamiento y fallas en los sistemas de firewall.

Estas fallas son rápidamente corregidas por los fabricantes cuando son descubiertas. El método más común para reparar estas debilidades es realizando una actualización en la versión de sus sistemas operativos (*firmware*) con la aplicación de parches o actualizaciones de seguridad en los equipos.

1.3.2. Debilidad en la configuración

La debilidad en la configuración de los sistemas de seguridad o en general en la configuración de cualquier equipo de comunicaciones en la red, está cercanamente relacionado con la debilidad en la tecnología.

Los problemas de debilidad en la configuración de equipos de comunicaciones son provocados al no fijar de manera correcta ciertos parámetros contra problemas de seguridad conocidos. Una buena noticia sobre estos problemas de mala configuración es que una vez que se los detecta, son fácilmente corregibles a un mínimo costo.

En la figura 1-2 vemos el ejemplo de un error en la configuración de un ruteador que fácilmente puede ser corregido.

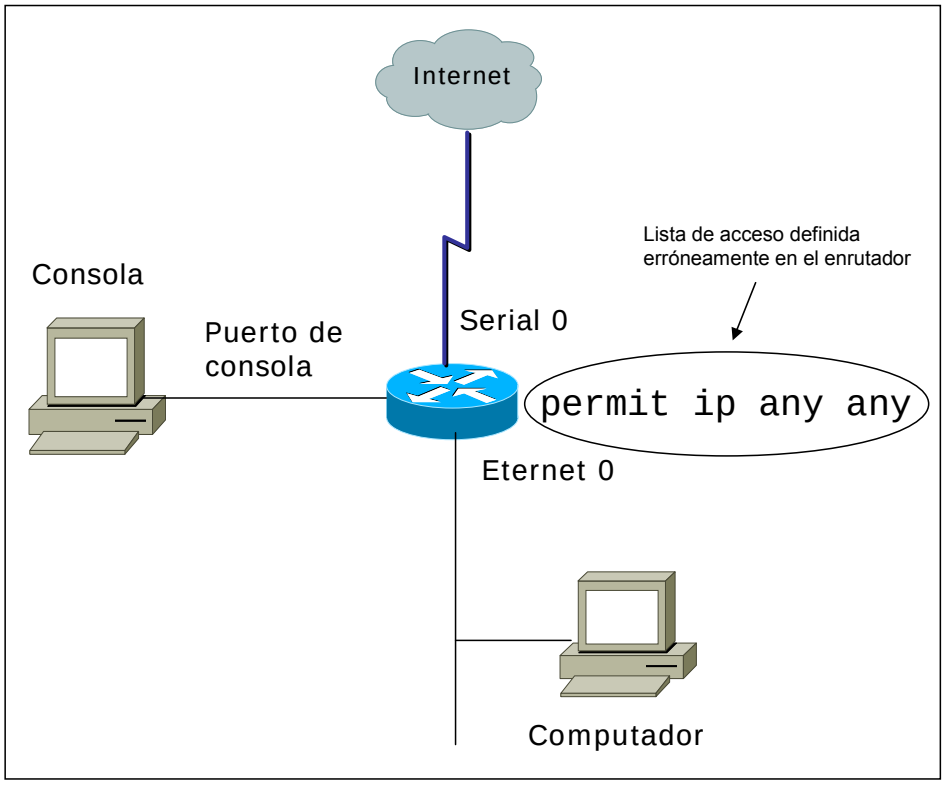


Figura No. 1-2. Problemas de seguridad causados por debilidad en la configuración de equipos

A continuación mostramos algunos ejemplos de debilidad en la configuración:

- **Parámetros por defecto (*default*) en la configuración de productos**—Algunos productos tienen configurados parámetros default que habilitan brechas de seguridad. Los usuarios deben consultar con el fabricante para identificar o corregir estos parámetros default inseguros.

- **Equipos de red mal configurados**—Errores en la configuración de los equipos de red representan problemas de seguridad. Por ejemplo, listas

de accesos mal configurados, fallas en la configuración de protocolos de enrutamiento, o nombres de comunidades SNMP pueden abrir grandes hoyos de seguridad.

- **Cuentas inseguras de usuario**—La información sobre cuentas de usuario puede ser transmitida de manera insegura a través de la red, exponiendo nombres de usuario y claves de acceso que pueden ser descubiertas con un analizador de tráfico (*sniffer*).

- **Cuentas de sistemas con claves fácilmente descubiertas**—Este es uno de los problemas más comunes, no se tiene la buena costumbre de utilizar claves difíciles de descubrir. No se deben utilizar palabras del diccionario ni sobrenombres como claves de acceso ya que esto es lo primero que utilizarán los intrusos para acceder a un sistema, se recomienda utilizar caracteres especiales y combinación de números y letras (mayúsculas y minúsculas).

- **Servicios de Internet mal configurados**—Equipos de red o los sistemas operativos pueden habilitar servicios TCP/IP inseguros que podrían permitir acceso remoto.

Como se mencionó anteriormente, las debilidades en la configuración de computadoras y dispositivos de red que han sido descubiertas se encuentran publicadas así como también los métodos para corregirlas. Se debe consultar los anuncios realizados por la CERT; también se sugiere revisar la información

proporcionada por los RFC (*Request for Comments*) en la que se describe las prácticas más comunes para configuración de redes, en el documento RFC 2827 “Network Ingress Filtering”.

1.3.3. Debilidad en las políticas de seguridad de la red

Algunos de los problemas que se producen por la debilidad en las políticas de acceso, incluyen lo siguiente:

- **Falta de una política de seguridad escrita**—Una política que no está escrita no puede ser aplicada o reforzada.

- **Políticas internas**—Cuando no existe un acuerdo común dentro de la corporación (por problemas internos de la compañía) se obstruye el hecho de tener o reforzar políticas de seguridad consistentes.

- **Falta de control de acceso lógico para equipos de red**—Una pobre administración de claves de usuario puede permitir acceso no autorizado a la red.

- **La administración de seguridad, incluyendo monitoreo y auditoria es deficiente—**Un inadecuado monitoreo y auditoria, así como la inadecuada corrección de problemas permite que los ataques y el uso no autorizado de los recursos de la red continúen. Esto gasta los recursos de la compañía y los expone a acciones legales.

- **Instalación de software y hardware y cambios que no siguen las normas o políticas—**Los cambios no autorizados en la topología de la red o la instalación de aplicaciones no productivas (juegos, programas de descarga, etc.) crean brechas de seguridad.

- **Falta de planes de contingencia ante problemas críticos—**La falta de planes ante incidentes de seguridad también llamado "recuperación ante desastres" crea pánico, caos y confusión cuando alguien ataca a la empresa.

1.4. Qué es un Firewall?

Un firewall es un medio que sirve para regular el acceso a la red de computadoras de una organización. El papel de un firewall en una red de computadoras es similar al de un guardián de seguridad que protege la puerta de entrada en una empresa. El firewall es responsable de proteger la entrada a la red de una compañía.

Por ejemplo, un edificio de oficinas posee numerosas dependencias con funciones diversas, como los despachos de los empleados, las salas de conferencia, y los almacenes de equipos y suministros. Lo más probable es que dichas dependencias estén conectadas entre sí por una serie de pasillos y, para desplazarse de unas a otras, los empleados deben abandonar sus despachos y recorrerlos. Estas habitaciones contienen recursos importantes de una

compañía: información privada de la organización, costosos suministros, equipos de oficina y empleados.

Conceptualmente, la red de computadoras de una organización es similar a un edificio de oficinas. Puede considerarse cada habitación de un edificio como un sistema anfitrión integrado en la red. Hay despachos individuales para empleados (como un PC) y grandes salas divididas por mamparas para alojar múltiples empleados (como un segmento de red de área local). Existen también dependencias, como la habitación de fotocopiadoras, en la que, por lo general, no trabajan permanentemente personas sino que proporcionan un servicio a estas (como los servidores de archivo, los servidores de correo, etc.). Los pasillos de un edificio representan la red de datos. Para comunicarse con otro despacho o para utilizar un servicio que se encuentra en una habitación distinta, es necesario recorrer los pasillos. La figura 1-3 ilustra esta analogía.

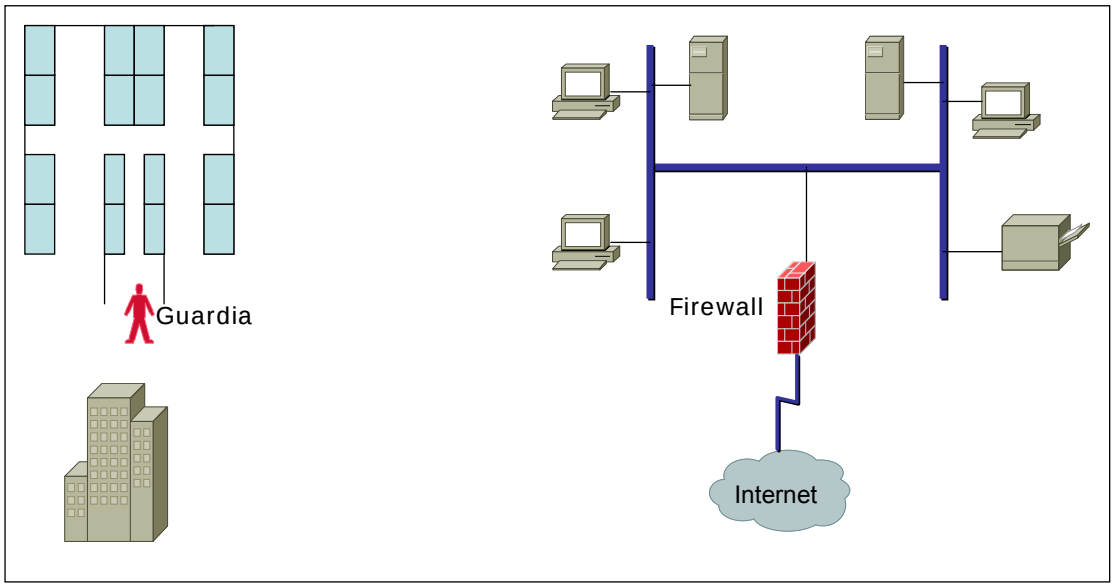


Figura No. 1-3. Comparación entre un edificio de oficinas y una red de computadoras

Ampliando la analogía, la entrada principal del edificio es la puerta que da acceso al mundo exterior, de forma muy parecida el firewall es la puerta por la cual la red de la organización accede a Internet. Así mismo, en el exterior del edificio hay un gran número de calles que llevan a otros edificios de oficinas de otras organizaciones, de forma muy similar a como Internet permite conectarse a otras redes privadas. A fin de proteger los recursos que contiene un edificio, la mayoría de las organizaciones emplean un guardia de seguridad en la entrada del edificio. Siguiendo con esta analogía, un firewall es el guardián de la red.

La función principal del guardia es controlar la entrada de personas en el edificio. Este trabajo lo lleva a cabo deteniendo a estas personas según entran al edificio, solicitándoles información de identificación como el nombre, la persona o el

despacho que desean visitar y el objetivo de su visita; el guardia debe decidir entonces si las deja entrar de acuerdo con un conjunto de instrucciones (una política de seguridad) definido por la organización. Además, puede anotar la visita de una persona en un registro donde indica la fecha y la hora de la misma.

Para la red de computadoras de una organización un firewall realiza las mismas funciones: controlar el acceso y registrar los intentos de acceso. Para ello consulta la información de identificación asociada a la comunicación procedente del exterior (direcciones fuente, direcciones destino, etc. Estos parámetros se tratarán en capítulos siguientes). El firewall decide entonces permitir o no la comunicación de acuerdo con la política de seguridad configurada por el administrador del firewall. Además, la mayoría de firewalls registra la actividad del tráfico que se ha generado desde la red privada hacia Internet y viceversa.

1.4.1. Servicios que ofrece un firewall estándar

Entre los principales servicios que un firewall ofrece para la protección de una red, se encuentran los siguientes:

- Control de acceso
- Registro de actividades
- Servicios especiales

1.4.1.1. Control de acceso

El objetivo principal de un firewall es proporcionar control de acceso hacia y desde la Intranet de una organización. Esto lo consigue obteniendo tanta información como le sea posible sobre un paquete o sesión que pase por él. Mediante esta información y una política de seguridad definida, el firewall decide autorizar o denegar el paso del paquete; si se niega, la sesión asociada al mismo no se completa satisfactoriamente.

Una de las diferencias importantes entre diversos firewalls es la cantidad de y la calidad de la información utilizada para tomar decisiones. Cuanta más información se consigue acerca de una sesión, menos probabilidad de éxito tendrá un intruso para atravesar el firewall.

Como mínimo, todos los firewalls utilizan los cinco elementos de información que contiene un paquete IP para tomar las decisiones. Estos cinco parámetros los mostramos en la tabla I.

Componentes del paquete IP	Descripción
Dirección IP destino	Cada host que pertenece a una IP de Internet o Intranet debe poseer una dirección IP única
Protocolo	Los protocolos estándar situados por encima de IP son TCP y UDP
Número de puerto destino	Identifica la aplicación de red de la que recibe el paquete
Dirección IP origen	Así la aplicación sabe adónde enviar las contestaciones
Número de puerto origen	Para identificar la aplicación del host origen adonde se envían los paquetes de retorno

Tabla I. Componentes de un paquete IP

Otro elemento de información importante, utilizado por varios firewalls es la interfaz de red (tarjeta de red) desde la cual el paquete entra en el sistema. Esto es importante para impedir o limitar la falsificación de la dirección de un host. Es decir, un paquete enviado por una fuente mal intencionada o errante puede deambular alrededor del host del cual procede, pero no puede hacerlo alrededor de la interfaz que emplea para entrar al firewall.

Otro de los elementos de información que es tomado en consideración por algunos sistemas de firewalls es el reconocimiento de que un paquete de entrada está asociado a una sesión autorizada existente, esta característica es conocida como **inspección de estado completo** (*satate-full inspection*). Sin esta característica no sería posible distinguir entre los paquetes de retorno correspondientes a una conexión de salida autorizada hacia Internet y los paquetes asociados a una sesión que procede de esta última. En otras palabras, esta característica permite una política de seguridad parecida en líneas generales a la siguiente: “No me hables hasta que yo no te haya hablado antes”.

Algunos firewalls utilizan también un nombre de usuario autentificado a los efectos de control de acceso. Las formas de autentificación estándar son contraseñas o tarjetas inteligentes. Sin embargo, algunos proveedores de firewalls están considerando el uso de la criptografía a fin de proporcionar la autentificación continua de usuarios, hosts u otros firewalls. Algunos firewalls utilizan también la hora y el día de la semana para tomar decisiones de acceso (en otras palabras, solamente permiten accesos FTP durante horas laborables normales, por ejemplo).

La decisión de acceso se basa en un grupo de reglas que emplean esta información para identificar grupos o clases de sesiones y asociarlas a una acción de autorización o de negación. Por ejemplo, una regla puede permitir todas las sesiones procedentes de cualquier host externo que acceden a la aplicación de correo que se encuentra en un *gateway* (puerta de acceso) de correo interno. Tradicionalmente, la mayoría de firewalls deniegan cualquier acceso que no esté

permitido explícitamente; es decir, si no existe una regla que autorice el acceso, la acción predeterminada es de negarlo.

1.4.1.2. Registro de Actividades

Un firewall eficaz puede registrar importantes elementos de información referente a todos los intentos de sesiones exitosas e infructuosas que se efectúan a través del firewall. Esta herramienta puede ser muy valiosa para supervisar la actividad de un intruso de la red para averiguar las áreas susceptibles de haber sido dañadas, e incluso para atraparla. La información almacenada como resultado de esta actividad de registro se conoce como registro de auditoria. Generalmente, los registros de auditoria contienen la información obtenida para tomar la decisión de acceso además de las horas de inicio y fin de una sesión y el número de paquetes que se ha dejado pasar.

La mayoría de los mejores firewalls poseen una función de alarma que permite al administrador especificar una acción definida que se ejecuta cuando se detecta un evento predefinido. Por ejemplo, un administrador puede definir una alarma que envíe un mensaje de correo cuando alguien ajeno a la organización pretende acceder a una computadora interna que contiene información delicada. Esto permite a los administradores definir actividades sospechosas acerca de las cuales deben ser informados inmediatamente.

1.4.1.3. Servicios Especiales

Varias características diferencian unos firewalls de otros. Entre ellas se incluyen aplicaciones proxy que ofrecen protección ante algunos ataques a protocolos de aplicaciones, detección de virus, correlación de direcciones para ocultar direcciones internas delicadas o ilegales, y redes virtuales privadas (VPN) mediante encriptación.

1.4.2. La seguridad que proporciona un Firewall

Muchos creen que un firewall es la única protección necesaria y que basta para proteger una Intranet de todas las amenazas posibles. Esta creencia no es más cierta que la suposición de que un guardia de seguridad puede impedir todos los robos que se producen en un edificio. Tal vez un enfoque más realista es pensar que un firewall puede reducir la vulnerabilidad de una Intranet, pero no erradicarlo.

Tenga en cuenta que los firewalls actúan como filtros; si cierra un filtro completamente, ningún ataque conseguirá atravesarlo, si bien, tampoco podrá realizarse ninguna otra actividad autorizada. En consecuencia, cuando se abre el filtro se asume el riesgo de que alguien pueda penetrar por esa abertura. En otras palabras, en el ámbito de una red existe siempre un riesgo inherente a la misma, y los firewalls han sido pensados para reducir los riesgos, pero no pueden eliminarlos completamente.

Cada servicio de red conlleva su propio riesgo exclusivo. Por ejemplo, permitir la recepción de correo en la red a través de una única puerta de acceso de correo que no presenta ninguna imperfección de seguridad (como el defecto del sendmail de UNIX) presentará un riesgo directo mínimo para la red. Naturalmente, el mensaje de correo puede contener virus incrustados o un caballo de Troya, aunque éste es un problema habitual en los PCs. No obstante, permitir atravesar el firewall a otros tipos de servicios como el Network File System (NFS) de UNIX implica riesgos considerables, por lo cual debe evitarse.

El administrador del firewall, en colaboración con el personal de la red y el personal de gestión, debe determinar la lista de servicios que pueden entrar y salir de la red. Los riesgos asociados deben evaluarse y documentarse. Los riesgos inaceptables deben eliminarse o, en su defecto, incorporar una seguridad adicional a la red a fin de poder gestionar la amenaza asociada a los mismos.

1.5. Herramientas que ayudan a la gestión de seguridad

Una vez que se ha implementado un firewall en una red de computadoras y en base a las políticas de seguridad que se ha definido para permitir el paso de cierto tipo de tráfico, no es suficiente el hecho de dejar a este dispositivo funcionando y pensar que con esto es suficiente para mantener protegida a la red de la organización; nada más alejado de la verdad. Como se ha descrito en el desarrollo de este capítulo, las técnicas que utilizan los hackers son cada vez mas complejas, por lo tanto es necesario realizar un monitoreo constante en busca de algún tipo de actividad sospechosa que ocurra en nuestra red.

Según datos estadísticos, la mayoría de ataques son provocados desde la red interna de la organización, por los mismos usuarios de la organización. Esto se da cuando nuestro sistema de firewall está configurado para proteger la red interna de ataques desde Internet; por lo tanto, es muy importante contar con herramientas que ayuden al proceso de gestión de seguridad para el administrador de la red.

Para cumplir con este objetivo, se han desarrollado herramientas cuyo objetivo principal es detectar potenciales vulnerabilidades en los sistemas de la red, así como herramientas que monitorean el tráfico en la red y pueden reconocer, en base a un patrón de tráfico, actividad sospechosa que pueda ser considerada como un posible ataque.

Estas herramientas son los sistemas de detección de intrusos (IDS) y los scanners (detectores) de puertos, a continuación presentamos con mayor detalle el funcionamiento de estos componentes que complementan el funcionamiento de un firewall y que son muy importantes en el modelo de seguridad en la red de computadoras de una organización.

1.5.1. Herramientas de verificación de vulnerabilidades

Las herramientas que prueban o detectan vulnerabilidades (también conocidos como *scanners*) realizan un examen riguroso a los diferentes sistemas (plataformas de sistemas operativos montados en servidores) para determinar

debilidades que puedan permitir violaciones de seguridad. Estas herramientas utilizan la siguiente estrategia para realizar este análisis.

De manera pasiva y utilizando mecanismos basados en host, estas herramientas realizan una inspección de los archivos de configuración del sistema en busca de parámetros default que no son seguros (debilidad en la configuración), también realizan una inspección de archivos que contengan claves de acceso al sistema en busca de claves “débiles” (debilidad de claves de acceso), y en general de otros objetos del sistemas en busca de violaciones a políticas de seguridad.

A este análisis le sigue, en la mayoría de los casos, una evaluación basada en red en la que la herramienta revisa o reactiva programas (*scripts*) comunes de intrusión, registrando respuestas del sistema a estos scripts.

Los resultados de estas herramientas de evaluación de vulnerabilidad representan una vista instantánea de los problemas de vulnerabilidad del sistema. Sin embargo, estas herramientas no pueden detectar de manera ciento por ciento confiable un ataque en progreso, lo que sí están en capacidad de detectar es que un ataque es posible y además, estas herramientas pueden algunas veces que un ataque ha ocurrido.

1.5.2. Sistemas de detección de intrusos (IDS)

Los sistemas de detección de intrusos (IDS por sus siglas en inglés) es una tecnología emergente para detectar usuarios no autorizados y comportamiento sospechoso o abusivo en redes y sistemas computacionales.

Los sistemas de detección de intrusos ayudan a los sistemas de computadoras a preparase y actuar ante eventuales ataques informáticos. Estos sistemas cumplen este objetivo recolectando información de diferentes fuentes de sistemas y de redes, analizan la información tratando de encontrar síntomas de problemas de seguridad. En algunos casos, los sistemas de detección de intrusos permiten al administrador de la red responder (en tiempo real) a estos intentos de ataques.

Los sistemas de detección de intrusos realizan una variedad de funciones, resaltamos las más importantes:

- Monitorean y analizan la actividad de los usuarios y del sistema.
- Realizan auditoria de la configuración del sistema y de posibles vulnerabilidades.
- Evalúa la integridad de sistemas considerados como críticos así como la integridad de base de datos.
- Realizan un reconocimiento por patrones de actividad que reflejan ataques conocidos.
- Análisis estadístico por patrones de actividad anormal.

- Auditoria a sistemas operativos, con reconocimiento de la actividad que realizan los usuarios que pueda reflejarse como violación de políticas.

Algunos sistemas proveen características adicionales, que incluyen:

- Instalación automática de actualizaciones (que las provee el fabricante) del producto.
- Instalación y operación de servidores “señuelo” para registrar información acerca de intrusos.

La combinación de estas características permite a los administradores de sistemas manejar de una manera mucho más fácil monitorear, auditar y evaluar sus sistemas y redes.

Todas las funciones que cumplen los sistemas de detección de intrusos es parte necesaria de la administración de seguridades.

1.6. Integración de los componentes para la gestión de seguridad

Es importante para el administrador de la red conocer las ventajas del uso de cada uno de los componentes que forman parte de la seguridad de la red. El correcto uso de cada uno de estos componentes es fundamental para mantener protegido los recursos de una red, es aquí donde es fundamental la gestión de seguridad.

La Administración de Seguridades de Red es un proceso mediante el cual se establece y mantiene políticas, procedimientos y prácticas requeridas para proteger recursos de una red de computadoras. Los sistemas de firewall y las herramientas de detección de intrusos y de evaluación de vulnerabilidades proveen las capacidades necesarias como parte de la solución global en la administración de seguridades en una red.

1.6.1. La Jerarquía de Seguridad

El siguiente diagrama en la figura 1-4 muestra la jerarquía en la seguridad de la información. Para cualquier tipo de tecnología de seguridad, la jerarquía que se describe en el siguiente gráfico se debe cumplir.

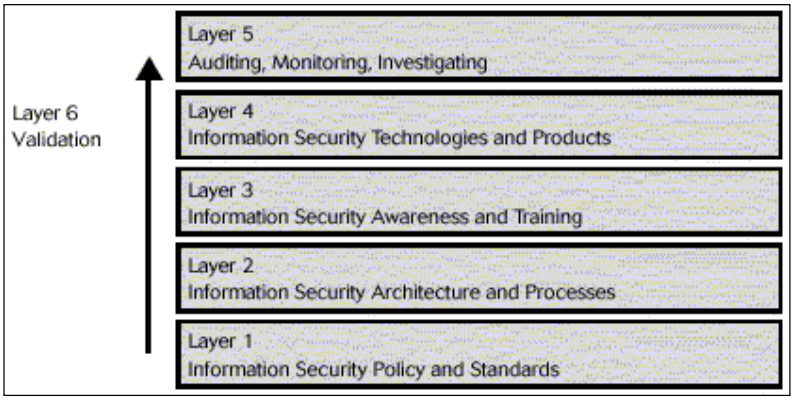


Figura No. 1-4. Jerarquía de la Seguridad de la Información

1.7. Criterio para el diseño de redes seguras

En esta sección se discuten todos los aspectos generales para diseñar un modelo de seguridad y prevenir problemas futuros. Entre estos se encuentran:

- Identificación de posibles problemas
- Diseño de controles de políticas
- Detección y monitoreo de actividad no autorizada
- Reportes de procedimientos

1.7.1. Identificación de posibles problemas

En este campo se incluye todos los tipos de vulnerabilidades descritos en la sección 1.3. de este documento bajo el título “tipo de vulnerabilidades en las redes de computadoras”. Sin embargo podemos también añadir lo siguiente:

- Puntos de acceso
- Amenazas de usuarios internos
- Seguridad física

1.7.1.1. Puntos de acceso

Hay que identificar todos los posibles accesos externos a la red, ya que estos se pueden convertir en puntos de entrada para usuarios no autorizados. Tener muchos puntos de acceso incrementará los riesgos en la red.

En las redes de la figura 1-5 se observan diversos puntos de ingreso a las redes. En el segmento A los puntos de acceso son el servidor de terminales y el ruteador 2. Además el computador 1 tiene un módem privado el cual es usado

para conexiones dial-out. En el segmento B, el host 2 también tiene un punto de acceso a la red.

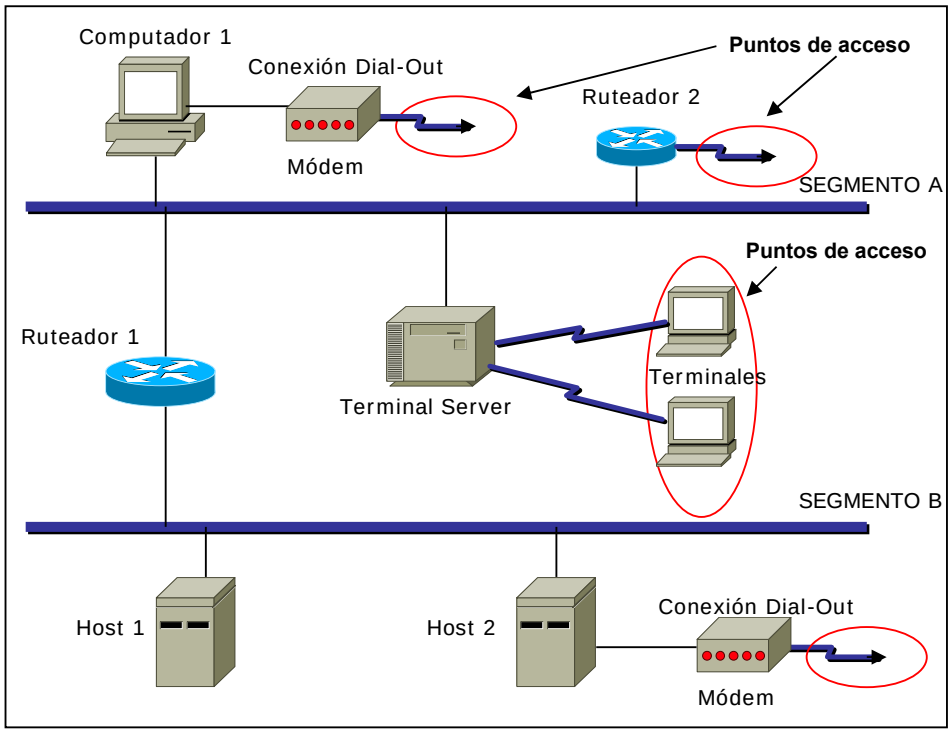


Figura No. 1-5. Identificando los puntos de acceso a la red

Considere el siguiente caso: el usuario del computador 1 en el segmento A puede tener una cuenta con un proveedor de Internet. Supongamos que este usuario utiliza una conexión SLIP o PPP. Si el software TCP/IP que el usuario corre en el computador 1 está configurado con características de ruteador, es decir, que pueda enviar paquetes tanto adentro como afuera de su red, es muy posible que un intruso pueda invadir la red. Hay que notar que el usuario pudo no

deliberadamente habilitar el computador como ruteador. El sistema operativo pudo haberlo hecho por defecto.

Si las políticas de seguridad establecen prohibición de conexiones privadas las situaciones de riesgo de este tipo pueden ser prevenidas. Esto también subraya la importancia de tener políticas de seguridad que claramente delinean el uso aceptable de políticas para la red.

Los servidores terminales pueden representar un riesgo de seguridad si no son adecuadamente protegidos, ya que muchos de estos servidores terminales no requieren algún tipo de autenticación. Por lo tanto, los intrusos pueden usar los servidores de terminales para disfrazar sus acciones.

1.7.1.2. Amenazas de usuarios internos

Si un usuario interno decide atacar la red, puede representar una considerable amenaza a la seguridad de la red. Si se tiene acceso físico a los componentes de un sistema, éste es aún más fácil de comprometer. Por ejemplo, muchas estaciones de trabajo, fácilmente pueden ser manipuladas para otorgar acceso. Muchos servicios de aplicaciones TCP/IP tales como Telnet, rlogin y FTP tienen mecanismos muy débiles de autenticación donde las contraseñas son enviadas por teclado.

1.7.1.3. Seguridad Física

Todos los recursos críticos tales como el segmento principal de la red (*backbone*), enlaces de comunicación, hosts, servidores importantes y equipos de red clave deben ser localizados en áreas físicamente seguras. Físicamente segura significa que la máquina es colocada en una habitación o colocada en una manera que restrinja el acceso físico a los dispositivos de almacenamiento de datos.

Muchas veces no siempre es fácil mantener una seguridad física en las máquinas. También hay que limitar el acceso de máquinas no muy seguras a las demás que sí son seguras. En particular no permitir ingresos a hosts usando mecanismos de acceso remoto (SSH, rlogin, rcp, etc.).

1.7.2. Diseño de control de las políticas

Para diseñar los controles en las políticas, es necesario tener en mente los tipos de protección y estrategias de seguridad como la implementación de firewalls, herramientas de detección de intrusos y las herramientas de detección de vulnerabilidades descritas en los puntos 1.4 y 1.5 de este capítulo. El objetivo principal de estos controles es solucionar los problemas de seguridad que posee la red interna.

Los mecanismos de control y protección deben ser adecuadamente seleccionados, ya que ellos brindarán seguridad y podrán registrar apropiadamente los daños encontrados durante un posible ataque. Estos

controles deben ser implementados de acuerdo a sus costos reales, es decir, no gastar esfuerzos en sobreproteger y restringir el uso de un recurso si el riesgo de exposición de éste es muy bajo.

El sentido común es frecuentemente una herramienta efectiva para diseñar un modelo de seguridad. Si se elaboran esquemas muy sofisticados e impresionantes, éstos pueden ser muy caros. También si la solución de seguridad es muy elaborada, puede resultar difícil de implementarla y administrarla.

Los controles que se seleccionen constituyen la primera línea de defensa en protección de la red. Si la mayor amenaza al sistema son usuarios externos (de Internet), no debería gastarse por ejemplo en tarjetas de identificación magnética para cada usuario interno sino más bien en la implementación de un firewall. Si la mayor amenaza son los accesos no autorizados, habría que establecer procedimientos para cambiar las contraseñas de los usuarios periódicamente.

1.7.3. Detectando y monitoreando actividades no autorizadas

Monitorear un sistema involucra observar diversas partes de un sistema y buscar cualquier situación inusual o sospechosa (actividades no autorizadas). La meta del monitoreo es detectar las posibles brechas de seguridad lo más tempranamente posible a fin de poder responder inmediatamente.

El monitoreo debe realizarse periódicamente: por días o semanas. Lo recomendable es no dejar más de una semana entre los monitoreos, de esta manera si se perpetra un ataque, éste puede ser rápidamente detectado.

Si se utiliza herramientas de monitoreo, se deben examinar salidas de las mismas. Si se tienen archivos de registros de actividad de tráfico en el segmento de red monitoreado que son voluminosos, los cuales resultan complicados de leer y manipular, se pueden utilizar programas alternativos que lean estos archivos y obtengan la información deseada.

En las siguientes secciones se dan ideas de cómo se puede monitorear un sistema.

1.7.3.1. Mecanismos de monitoreo

Muchos sistemas operativos almacenan información del registro de ingreso de usuarios en la red (*login*) en archivos especiales. Los siguientes consejos pueden resultar muy apropiados para realizar un monitoreo basado en estos archivos:

- Se pueden comparar listas de los actuales usuarios conectados con historias de login pasado. La mayoría de los usuarios tienen horas regulares de trabajo y si una cuenta presenta actividad en una hora fuera de lo normal, debe ser monitoreada muy cercanamente ya que puede tratarse de un intruso.

- El sistema operativo puede tener facilidades de sistemas de login, tales como el Syslog usado en UNIX. Los logs o registros producidos por tales herramientas pueden ser examinados buscando mensajes de error del software del sistema. Por ejemplo, un gran número de fallas en el login intentado en un periodo de tiempo indica que alguien posiblemente está tratando de adivinar la contraseña.
- Muchos sistemas operativos tienen comandos, como el ***ps*** en UNIX, para listar los procesos que se están ejecutando. Estos pueden ser utilizados para detectar a usuarios corriendo programas a los que ellos no están autorizados a usar.
- Los firewalls pueden ser usados para producir un archivo de log para todos los accesos a la red.
- Si se tienen recursos especiales que se quieren monitorear se puede construir una herramienta propia usando utilitarios estándares del sistema operativo. Por ejemplo se puede combinar los comandos ***ls*** y ***find*** en un programa para examinar los accesos a archivos privilegiados y cambio de permisos a los mismos. Las diferencias en los permisos a archivos claves indicarían modificaciones no autorizadas.

1.7.3.2. Esquemas de Monitoreo

El administrador puede realizar monitorios frecuentes a lo largo del día. Si el monitoreo es hecho permanentemente, puede llegar a ser muy tedioso, pero algunos comandos de monitoreo pueden ejecutarse en algún tiempo durante los momentos ociosos.

Si el administrador ejecuta varios comandos para monitorear a diferentes tiempos a lo largo del día, es muy difícil para un intruso predecir las acciones del administrador. Si el intruso no puede adivinar cuando el administrador hizo un monitoreo, corre un gran riesgo de ser detectado.

Por otro lado, si un intruso conoce que a las 06:00 PM diariamente el sistema es chequeado para saber quien está conectado los intrusos esperarán para conectarse después del monitoreo.

1.7.4. Reportando Procedimientos

Si un evento de acceso no autorizado es detectado, se deben tener procedimientos de cómo actuar ante este evento y a quién debe ser reportado. Las políticas de seguridad también deben cubrir los siguientes aspectos:

- Procedimientos de manejo de cuentas
- Procedimientos para manejo de configuración
- Procedimientos de recuperación
- Procedimientos de reportes de problemas para administradores del sistema

Estos aspectos nombrados son establecidos de acuerdo al criterio del administrador de la red. Se trata de procedimientos internos que deben ser definidos por el administrador ya que él es quién va a manejar la red.

1.7.4.1. Procedimiento de Manejo de Cuentas

Cuando se crean cuentas a los usuarios, se debe tener cuidado de no dejar cualquier agujero en la seguridad. Las cuentas sin contraseñas son peligrosas aún cuando éstas no ejecuten un interpretador de comandos, tales como cuentas que existen sólo para ver quién está conectado en el sistema. Si éstas no están configuradas correctamente, la seguridad del sistema puede ser comprometida. Por ejemplo, si el usuario anónimo usado por FTP no es configurado correctamente, podría permitir que cualquier usuario ingrese al sistema y descargue archivos. Si existen errores en la configuración de esta cuenta y los permisos de escritura son otorgados, un intruso puede cambiar el archivo de contraseñas o destruir el sistema.

Las políticas deben incluir procedimientos para mantener rastros de quien tiene una cuenta con privilegios, tales como la cuenta del administrador en UNIX (root). Si se conoce la contraseña de la cuenta root, se podría usar el comando ***su*** y asumir privilegios de usuario root. Se deben implementar políticas que pongan énfasis al cambio de contraseñas para usuarios privilegiados en tiempos regulares.

1.7.4.2. Procedimientos para el manejo de la configuración

Se debe mantener actualizadas las versiones del sistema operativo y utilitarios críticos. Las debilidades de seguridad en sistemas viejos son usualmente bien conocidas, y es muy probable que cualquier intruso conozca de estos problemas. Desafortunadamente algunas nuevas versiones de programas, mientras por un

lado arreglan viejos problemas de seguridad, por otro introducen nuevos problemas.

1.7.4.3. Procedimientos de Recuperación

Cuando se instale una nueva versión de un sistema operativo, no sólo hay que sacar respaldo del kernel, sino también de los archivos que son usados para compilar y configurar el sistema operativo. Lo mismo se aplica para otras aplicaciones y programas de la red.

Los respaldos de archivo de un sistema representan una seguridad dentro de las políticas. No sólo protegen en el eventual caso en que un dispositivo de hardware falle, sino también contra eliminaciones accidentales o como medida de seguridad si el sistema ha sido violado. Si el administrador sospecha que el sistema ha sido comprometido, se puede restaurar todo desde un respaldo de protección. Si no se puede detectar cuando un cambio no autorizado toma lugar, se tiene que examinar los diversos respaldos a fin de encontrar la configuración original.

1.7.4.4. Procedimientos de reportes de problemas para administradores del sistema

Los administradores del sistema deben tener un procedimiento definido para reportar problemas de seguridad al jefe de la organización. En instalaciones de

una red grande, puede ser hecho creando “listas de correo” que contengan las direcciones de correo electrónico de todos los administradores en la organización.

CAPÍTULO II

AMENAZAS REALES PARA LA INTRANET

2.1. Introducción

Sin duda alguna, la identificación de los riesgos de seguridad para una Intranet, tal como se lo ha expuesto anteriormente, proporciona un sólido punto de partida para decidir si, en verdad, es necesario un firewall. Y como hemos sugerido, si piensa conectar una Intranet al ámbito público de Internet, probablemente decidirá que necesita un firewall.

Sin embargo, una vez que se llegue a esta conclusión, el administrador deberá responder a nuevas preguntas sobre las amenazas reales para su Intranet y la mejor manera de contrarrestarlas. Es decir, tendrá que determinar los tipos de ataques a la seguridad que deben evitarse, la forma como se integrará el firewall a la red y la disposición y organización de los diversos componentes del mismo.

Este capítulo trata cuestiones más específicas referentes a las amenazas para la seguridad. Para ello describe las amenazas reales a las que se enfrentará en el momento de configurar y hacer operativo un firewall. Específicamente, se describe la evolución de las diversas tecnologías que han influido considerablemente en la seguridad. Se proporciona también un resumen de los diversos ataques habituales que se producen en Internet y en las Intranets, centrándonos no sólo en los detalles técnicos de estos, sino también en las estrategias generales implicadas en ellos, con el fin de perfeccionar su intuición sobre los problemas de seguridad que pueden llegar a producirse.

2.2. La Amenaza de la Interconexión de Sistemas Abiertos

El concepto de sistemas abiertos está enraizado en la noción de un enfoque estándar de la informática y de las redes que proporciona una mayor interoperabilidad, flexibilidad y portabilidad del software y de los componentes del sistema. Antes de que surgieran los sistemas abiertos, un gran número de fabricantes de computadores y de software promovían la idea de que los sistemas propietarios eran la mejor opción. El sistema operativo UNIX, que fue inventado por AT&T, fue uno de los primeros intentos comerciales principales para la consecución del concepto de sistema abierto para sistemas operativos.

Dentro de la comunidad de redes, en estos últimos años las principales contribuciones hacia el objetivo de los sistemas abiertos se han concentrado en el ámbito público de Internet, en el conjunto de protocolos y servicios de TCP/IP y

en la World Wide Web (WWW). Estas tendencias han favorecido la promoción de las ventajas de la computación en sistemas abiertos, si bien esto ha revelado la principal desventaja inherente a los mismos, es decir, la seguridad se ha convertido en un desafío todavía mayor. En especial, al permitir a los usuarios la mejor comprensión de los detalles de un sistema determinado, éste queda expuesto también a atacantes potenciales.

2.2.1. Una Analogía con la Red Telefónica

Para comprender las amenazas para la seguridad asociadas con la conexión en red de sistemas abiertos, consideremos la situación que existía en los inicios del servicio telefónico. Los primeros abonados a éste se encontraban normalmente en ciudades grandes; era una decisión fácil para la compañía telefónica, puesto que la mayor concentración de clientes potenciales se encontraban en las zonas urbanas, así pues la compañía podía obtener mayores beneficios al proporcionar el servicio a dichas zonas.

Sin embargo, a medida que el servicio fue extendiéndose, aparecían en ocasiones en ciudades que precisaban un servicio telefónico local pequeñas islas que contaban con su propia red telefónica pero aún desconectada con el resto del mundo. En entornos como ése era imposible para alguien del exterior de estas islas infiltrar sus servicios en ellas. Sin embargo, una vez conectadas estas islas al resto del mundo, dejó de existir este nivel de seguridad basado en la separación y el aislamiento.

Esta analogía con el sistema de conexión telefónica ilustra un gran número de las características de la evolución de la conexión de redes digitales. Por ejemplo, a partir de las décadas de los 60 y 70 comenzaron a crearse islas locales de redes digitales dentro de las típicas organizaciones empresariales, académicas y gubernamentales. Inicialmente, uno de los aspectos más importantes de estas redes fue que no estaban conectadas con otras redes, lo que dio como resultado redes a cuyos activos no podían acceder fácilmente los atacantes del exterior.

Sin embargo, debido a la reciente expansión de las conexiones a Internet en las décadas de los 80 y 90, es difícil encontrar actualmente redes aisladas. Así, la seguridad de las redes modernas ha disminuido debido a su mayor capacidad de conexión, pues ha facilitado la disponibilidad de los activos de las mismas a los atacantes potenciales.

Tal vez sea instructivo observar que las únicas redes aisladas que se pueden encontrar habitualmente hoy día son aquellas que han sido diseñadas según necesidades especiales de seguridad.

2.2.2. La amenaza de los sistemas abiertos

La analogía con el sistema telefónico demuestra el extraordinario efecto que puede conllevar el aumento de la conectividad. Además, el uso de un enfoque de sistemas abiertos conectados en la red, tal como ilustra una Intranet basada en el sistema Web y provisto de un gateway hacia el ámbito público de Internet, promueve este tipo de aumento de posibilidades de interconexión. De hecho,

este aumento es precisamente la amenaza que pretenden atenuar los firewalls en un entorno abierto con redes conectadas entre si. A medida que se incorporan islas de conexión locales surge una vía potencial que pueden utilizar los intrusos del exterior como medio para acceder a los servicios locales.

No pretendemos dar a entender que los enfoques basados en sistemas abiertos no son deseables. De hecho, han supuesto una revolución en el campo de la computación que ya han cambiado nuestras vidas para bien. Pero estos avances en la conexión en red de los sistemas abiertos, así como su efecto en la seguridad, son en realidad simplemente otro caso de interacción entre la facilidad de acceso y la seguridad. Esta relación se ilustra gráficamente en la figura 2-1

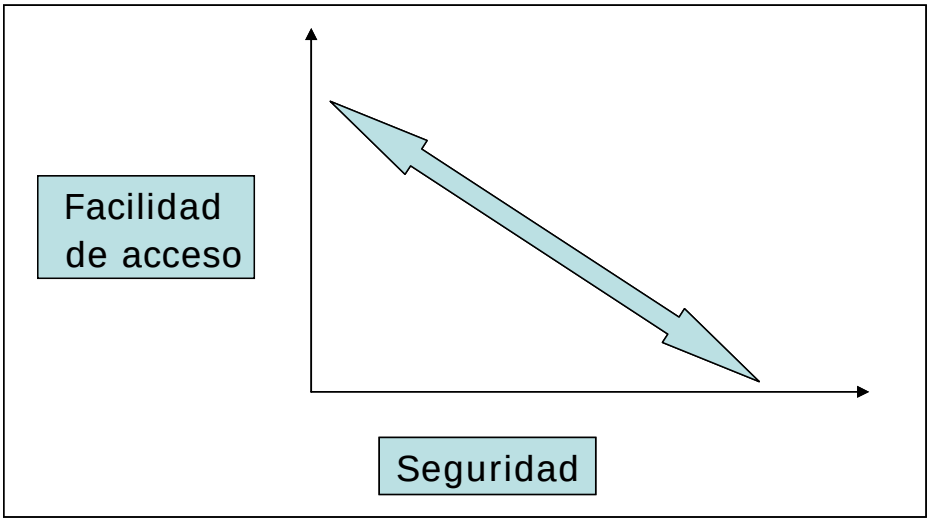


Figura No. 2-1. La facilidad de acceso frente a la amenaza malintencionada

A fin de representar esta relación en una situación conocida, considere esta sencilla analogía: si deja abiertas siempre las puertas y ventanas de su casa, es

más fácil entrar y salir de ella. Nunca se podrá quedar cerrado fuera y ahorrará tiempo al no tener que buscar las llaves. Si hace eso, no obstante, los intrusos también encontrarán más fácil entrar y salir de su casa. La conclusión que puede extraerse de este ejemplo es que el concepto “abierto” es, en realidad, una espada de doble filo.

En suma, debido a que los enfoques de los protocolos y sistemas de redes abiertos aumentan la posibilidad de compartir información, mejorar la conexión y facilitar un mayor acceso a la red subyacente, también incrementan los riesgos de sufrir ataques malintencionados.

2.3. El crecimiento de Internet

Otra tendencia de computación y las redes directamente relacionada con la expansión de los sistemas de redes abiertos, es el crecimiento espectacular que está experimentando la Internet pública. Dicho crecimiento ha sido impulsado por avances fundamentales en la tecnología de redes que se han producido a una velocidad vertiginosa. Observe que las intranets de las empresas son simplemente una ampliación natural del crecimiento de Internet. En lugar de conectar entre sí clientes de usuario único según un sistema uniforme, el nuevo modelo de Internet incluye la conexión de intranets de organizaciones según un sistema uniforme.

2.3.1. Evolución de las redes

Hace mucho tiempo que el Gobierno de los Estados Unidos, tomó la decisión de asegurar la generalización y uniformidad del servicio telefónico local y de larga distancia al permitir a AT&T la creación de un monopolio. A lo largo y ancho de la red se implementaron estándares y convenciones basados en las decisiones técnicas de los ingenieros de Bell Telephone Laboratorios y de Western Electric. Así pues, los usuarios de los servicios telefónicos no hubieron de preocuparse por la incompatibilidad de los equipos telefónicos o de los protocolos. Todo era relativamente sencillo.

Por otra parte, la conexión digital ha evolucionado algo diferente. Paralelamente, a la conexión entre redes que comenzó a implantarse en todo el mundo durante los 60, 70 y 80, aparecieron diversos equipos para redes y protocolos propios e incompatibles. De hecho, muchos administradores de red se identifican todavía a sí mismos con el primer enfoque de redes propias que aprendieron (o que aprendieron mejor). El protocolo de red SNA de IBM y la enorme comunidad de entusiastas que lo respaldan es el ejemplo más destacado.

2.3.2. Desarrollo del TCP / IP

Al reconocer que esta diversidad de enfoques de redes podía suponer algún problema, el Gobierno de los Estados Unidos comenzó a patrocinar proyecto de investigación y desarrollo de un conjunto de protocolos con fondos de la Advanced Research Projects Agency (ARPA). El conjunto de protocolos llamado TCP/IP (Transmission Control Protocol/Internet Protocol), nunca fue pensado

como un estándar global, pero el uso generalizado y su adopción por parte del público corriente lo convirtieron en un estándar aceptado. En ello tuvieron su importancia algunos desarrolladores de la Universidad de California de Berkeley que incluyeron el TCP/IP en su conocido dialecto de UNIX (llamado BSD UNIX). La difusión del TCP/IP quedó garantizada cuando se distribuyó el BSD UNIX por todo el país, y comenzó a utilizarse en universidades, institutos de enseñanzas y colegios mayores, así como en un gran número de organizaciones comerciales.

En resumen, conviene saber que el conjunto de protocolos TCP/IP se convirtió en el "idioma" básico para la joven Internet. El gobierno utilizaba una red llamada ARPANET como parte de su compromiso de mejorar la conexión entre diversos organismos del mismo. TCP/IP fue el conjunto de protocolos que se empleó en ARPANET. A medida que se generalizó el uso de ARPANET, el gobierno aumentó su capacidad, encargó a la National Science Foundation (NSF) la gestión de un nodo principal que se encontraba en proceso de evolución (NSFnet) y, poco después, toda esta infraestructura pasó a ser conocida como Internet, siendo TCP/IP el conjunto de protocolos utilizado en ella.

Una de las diferencias entre el TCP/IP y los protocolos privados anteriores, como SNA, consistía en que un único proveedor no podía controlar las especificaciones asociadas a aquel. En consecuencia, las especificaciones de interfaz asociadas al TCP/IP estaban a la disposición de cualquiera. De hecho, una completa infraestructura comenzó a evolucionar gradualmente en Internet para proporcionar comentarios técnicos sobre éste protocolo, proponer nuevas características para el conjunto y documentar cualquier otro aspecto relacionado.

Dicha infraestructura, conocida como Request For Comment (RFC) ha tenido un éxito extraordinario aunque el término “RFC” es en realidad una denominación errónea, puesto que gran número de RFC se consideran actualmente como descripciones técnicas estables.

Debido a que el TCP/IP era un protocolo abierto, cualquier proveedor que desease fabricar productos basados en él podía hacerlo libremente.

2.3.3. Aparición de la Web

Durante muchos años, la ARPANET, y entonces la primitiva Internet, era empleada por científicos, ingenieros y por quien tuviera conocimientos computacionales para intercambiar resultados de investigaciones, artículos y cualquier tipo de datos técnicos. Este intercambio sigue siendo actualmente parte importante de Internet.

Sin embargo, en los últimos años ha aparecido una aplicación conocida como World Wide Web, o también “aplicación asesina”, que ha puesto la Internet a disposición de las “masas”, sin conocimientos técnicos pero con ansias de intercambiar información y opiniones. La Web se basa en los primeros trabajos sobre la computación de hipertexto realizados en el European Particle Physics Laboratory (CERN) de Ginebra, Suiza. Emplea un protocolo conocido como Hypertext Transfer Protocol (http) para enviar documentos entre sitios que tienen direcciones llamadas Uniform Resource Locators (URL).

Además del trabajo del CERN, el National Center for Supercomputing Applications (NCSA) llevó a cabo inicialmente diversos proyectos en el área del acceso de clientes a la Web consistentes en el desarrollo de navegadores. Un navegador es un paquete de software que permite consultar fácilmente la información de Internet almacenada en servidores Web. El conocido navegador Mosaic es producto de ese trabajo. Desde entonces han aparecido compañías como Netscape ante el extraordinario éxito de la Web y el uso de navegadores en computadores de escritorio.

Como resultado, las intranets corporativas y de organizaciones han surgido como flores silvestres. Una reciente estimación publicada en *Business Week* sugiere que el número de Intranets crecerá vertiginosamente en los próximos años, sustituyendo a rígidas aplicaciones como Lotus Notes. Todavía queda por ver si dichos paquetes serán realmente reemplazados o no, aunque nadie puede poner en duda la potencia y crecimiento de la Web.

La profusión de las Intranets conlleva implicaciones de seguridad fundamentales: la diversidad de las redes será sustituida por un enfoque de sistemas abiertos basados en TCP/IP y en la tecnología Web. Si los piratas informáticos pueden entrar en su Intranet, poco podrá hacer (excepto con las a menudo denostadas técnicas de seguridad para sistemas anfitriones) para impedirles que causen estragos en su red. Este punto es importante, ya que resalta una de las razones primordial para la protección por firewall.

2.4. Descripción de algunos ataques procedentes de Internet

En esta sección veremos las categorías en las que se ha clasificado a los tipos de amenazas de seguridad:

- Reconocimiento
- Acceso no autorizado
- Negación de Servicio
- Manipulación de Información

Las categorías de amenazas de seguridad son generalmente conocidas como *vulnerabilidades*. Las **vulnerabilidades** son atributos de una computadora o red de computadoras que permite a alguien iniciar un *exploits* contra la red. Un ***exploit*** es un método para tomar ventaja de una vulnerabilidad por un procedimiento manual, una secuencia de comandos (*script*) o un programa ejecutable.

El propósito de un exploit es recolectar información del sistema (reconocimiento), denegar servicios para validar usuarios, obtener acceso no autorizado a sistemas o datos o manipular información.

Cada uno de los exploits y vulnerabilidades tienen un identificador o firma (*signature*), como una especie de identificador. Los sistemas de detección de intrusos (IDS) pueden reconocer las firmas de estos exploits. Tan pronto como

este identificador del exploit es reconocido y registrado, se puede identificar las medidas para reparar la vulnerabilidad o para bloquear el exploit.

2.4.1. Reconocimiento

El ataque de tipo *Reconocimiento* es el descubrimiento, diagramación (*mapping*) y monitoreo de sistemas, servicios o vulnerabilidades en una red **de manera no autorizada**. El reconocimiento también incluye el monitoreo de tráfico de red.

Este tipo de ataque puede ser llevado a cabo de manera activa y de manera pasiva: La información obtenida por reconocimiento puede ser utilizada para planear otros ataques a la red o para robar información sumamente importante. La figura 2-2 ilustra los lugares en la red donde los ataques de reconocimiento pueden ocurrir.

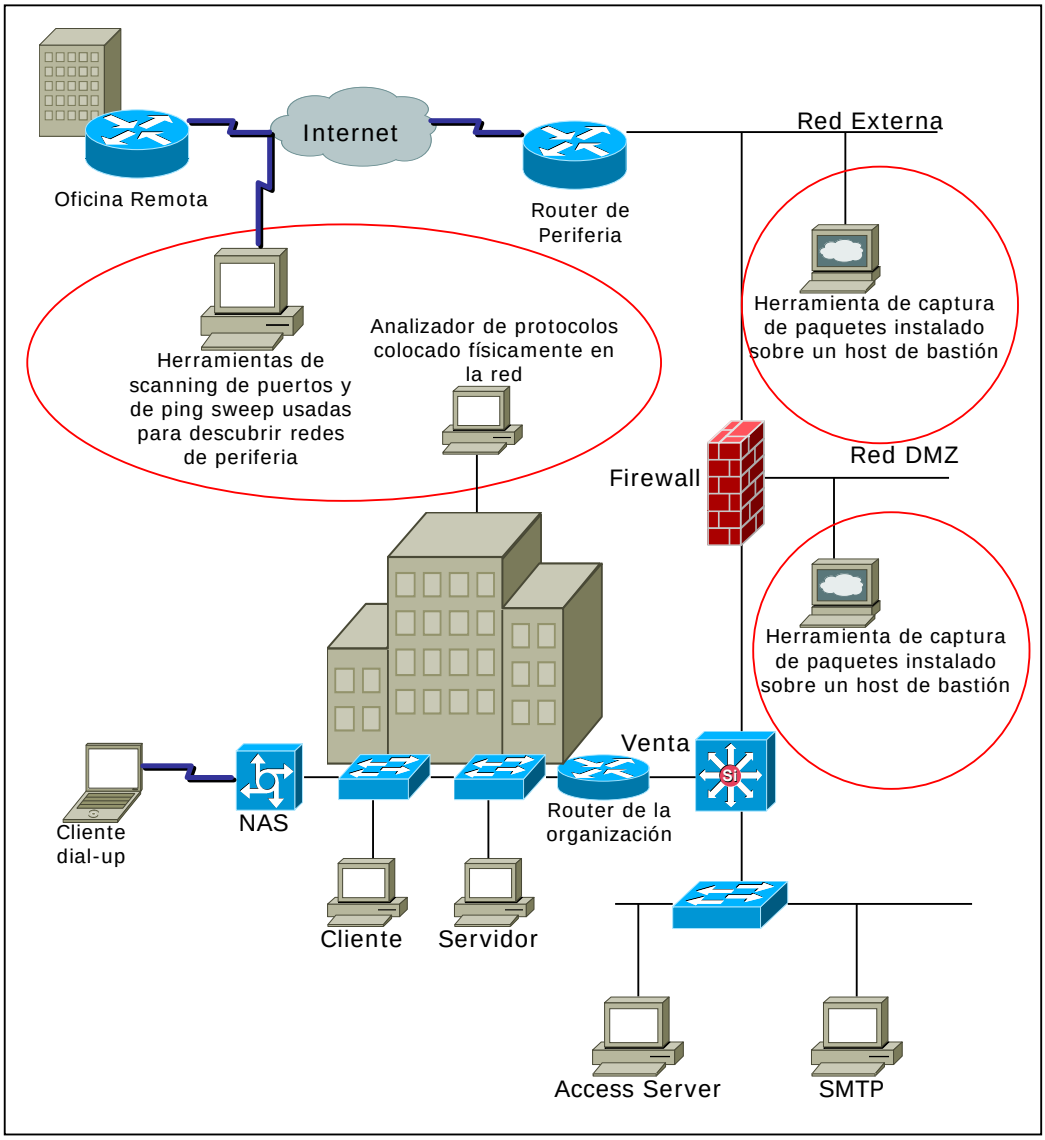


Figura No. 2-2. Ejemplos de Localidades para ataques del tipo Reconocimiento

En las siguientes secciones se considera los tipos de ataques de reconocimiento, se examina los exploits usados para llevar a cabo el ataque y describe las medidas que se pueden tomar para prevenir los ataques de reconocimiento.

2.4.1.1. Descubrimiento del Objetivo (*Target Discovery*)

El descubrir los objetivos incluye encontrar nombres de dominio y asociar las respectivas direcciones IP, aprender el rango de direcciones IP de una organización o descubrir las direcciones IP de hosts específicos a los cuales atacar.

Cuando ya se ha identificado el objetivo a ser atacado se requerirá saber los servicios o la información que ese host tiene disponible. Por ejemplo, el hacker puede tratar de aprender la IP de la interfaz del router de periferia que se conecta al proveedor de servicios de Internet (ISP) para que él pueda atacar al router. Los ataques del tipo Target Discovery se pueden realizar con comandos de red, barrido de ping y con barrido (*scanning*) de puertos.

2.4.1.1.1. Comandos de Red

El reconocimiento se lo puede realizar con simples comandos de red disponibles en sistemas UNIX, Windows y Linux: *ping, whois, finger, rusers, nslookup, rpcinfo, telnet, dig, nmap* y otros comandos y utilitarios que proveen información sobre un host o red. Estos comandos pueden ser ejecutados de manera individual o utilizando herramientas de dominio público que combinan comandos "query-type" (comandos que realizan requerimientos o consultas) para cumplir un propósito específico.

Algunas de estas herramientas sirven para recoger información sobre dispositivos de red alterando las opciones de la cabecera IP utilizando paquetes sintetizados y luego recogiendo la información enviada como respuesta a estos paquetes.

2.4.1.1.2. Barrido de Ping (*Ping Sweeps*)

A pesar que el comando ping es usado para obtener información sobre una red o host, existen herramientas conocidas como *Ping Sweeps* que han sido diseñadas para descubrir automáticamente hosts dentro de una red o subred.

La herramienta Ping Sweep ejecuta un ping a un rango de direcciones IP; esta herramienta también identifica objetivos potenciales a ser atacados. El comando Ping genera un paquete ICMP (Internet Message Control Protocol) del tipo "echo-request" contra un host específico. El host debe responder con una variedad de mensajes ICMP de contestación. Algunas veces, la herramienta Ping Swep combina las series de ICMP echo-request con otros mensajes ICMP Request como ICMP Timestamp, ICMP Address Mask o ICMP Information Request para obtener mayor información.

2.4.1.1.3. Barrido de Puertos (*Port Scan*)

Cuando un hacker descubre un host interesante, el (o ella) puede realizar un scanning (verificación) de puertos contra ese host.

Una herramienta de scanning de puertos revisa rangos de puertos TCP o UDP sobre un host para determinar los servicios de red que están disponibles, como Telnet, FTP, http, o RCP. Un scanning de puertos puede ser general, en los que un rango de puertos son probados como los puertos 1 al 1023. Un scanning de puertos puede también ser específico, concentrándonos en ciertos puertos con tal de descubrir información como por ejemplo el sistema operativo, el nombre de host o nombre de usuario. Algunas herramientas de scanning de puertos pueden usar fragmentación de paquetes y combinar los bits SYN y FIN en la cabecera TCP para tratar de ocultar el scanning de puertos.

Después de descubrir los puertos que están abiertos en un host, se puede realizar un ataque sobre un puerto específico. Por ejemplo, después de descubrir que SMTP está disponible en un host, el hacker puede enviar comandos SMTP para obtener más información o para obtener acceso no autorizado. También el hacker puede tratar de obtener acceso por Telnet o por FTP hacia el host.

2.4.1.2. Recolección de Información (*Eavesdropping*)

La recolección de información, es un método de observación pasiva del tráfico de la red mediante un dispositivo o herramienta. El propósito de la recolección de información es observar patrones de tráfico y capturarlo para su posterior análisis. “Olfateo de red” u “olfateo de paquetes” son sinónimos comunes para el esta técnica de ataque. La información recogida es usada para planificar otro tipo de ataques o para robar otro tipo de información.

El intruso puede usar esta técnica de ataque para identificar nombres de usuario y claves para ganar acceso no autorizado a hosts de la red o para identificar información que es llevada en los paquetes como números de tarjetas de crédito o información personal muy sensible. Un ejemplo de data susceptible a esta técnica de ataque son los caracteres que forman el nombre de una comunidad SNMP en la versión 1 de este protocolo ya que esta información es enviada en texto plano. Un intruso puede realizar solicitudes utilizado SNMP par obtener el nombre de la comunidad y de este modo aprender información sobre la configuración de los equipos de red. La tabla II describe algunos de los dispositivos usados para recolección de información.

CATEGORÍA	TIPO	DESCRIPCIÓN
Herramientas de captura de paquetes	**tcpdump**, **esniff.c** para UNIX **linsniffer.c** para Linux **Microsoft Network Monitor** sobre sistemas Windows NT	Herramientas de software instalados en host. Requieren tarjetas de red instalados en modo promiscuo.
Analizadores de Protocolo	Net XRay HP Internet Advisor LAN Protocol Analyzers	Software instalado en host o equipo dedicado para pruebas.

Tabla II. Dispositivos usados para recolección de información

2.4.1.3. Robo de Información

La recolección de información en una red puede tener como consecuencia el robo de información. El robo puede ocurrir cuando la data es transmitida sobre la red interna o externa; el intruso puede hurtar data de computadoras en la red obteniendo acceso no autorizado. Un tipo de intrusión en la red que es muy común es aquel en la que el intruso toma archivos o utiliza recursos que no le pertenecen.

Entre los ejemplos se incluye cuando el intruso "fuerza la entrada" de instituciones financieras y obtiene números de tarjetas de crédito; otro ejemplo es cuando el intruso accede y copia el archivo de claves de una computadora y utiliza otra computadora para violar (crakear) el archivo.

La tabla III describe los métodos a seguir para contrarrestar los ataques de reconocimiento contra la red.

ATAQUE	PREVENSIÓN
Descubrimiento del Objetivo (*Target Discovery*)	• Deshabilitar las respuestas a comandos "query-type" como finger y nslookup en routers y hosts en la red. • Usar un IDS para detectar tales intentos.
Barrido de Ping (*Ping Sweep*)	• Deshabilitar las respuestas a los pings y utilizar un IDS para detectarlo.
Barrido de puertos (*Port Scan*)	• Utilizar un scanner de puertos para identificar puertos abiertos. Desactivar servicios no esenciales en routers y hosts en la red y usar un IDS para detectar el scanning de puertos.
Recolección de Información (*Eavesdropping*)	• Limitar el acceso físico a los equipos de red de la organización para prevenir la instalación de analizadores de protocolos en segmentos de red. • Utilizar switches ethernet en la red interna para segmentar la LAN y prevenir la captura de tráfico de toda la red desde una Workstation. • Prevenir el acceso no autorizado a la red para hosts con el fin de prevenir la instalación de herramientas de captura de paquetes. Utilizar verificadores de integridad de archivos en hosts para detectar cualquier instalación no autorizada. • Utilizar tarjetas de red que no puedan ser configuradas en modo promiscuo en hosts sensibles. Físicamente

	chequear las interfaces de los hosts por modo promiscuo. • Ejecutar software que verifique modo promiscuo como **ifstatus** y **cpm** en cada host. • Utilizar tecnología de encriptación para limitar la capacidad de observar el contenido del tráfico de una red a través de redes no seguras.

Tabla III. Métodos para contrarrestar ataques del tipo Reconocimiento

2.4.2. Acceso no autorizado

Un intruso de red puede obtener acceso remoto no autorizado a computadoras o dispositivos de networking de varias maneras. Un punto a favor para el intruso es tener acceso a computadoras en la red como usuario root (en sistemas UNIX) o como usuario Administrador (en Windows); con esto, el intruso tiene gran poder para controlar la computadora objetivo o para acceder a otras redes. La figura 2-3 ilustra algunos de los puntos en los que un intruso puede intentar obtener acceso no autorizado.

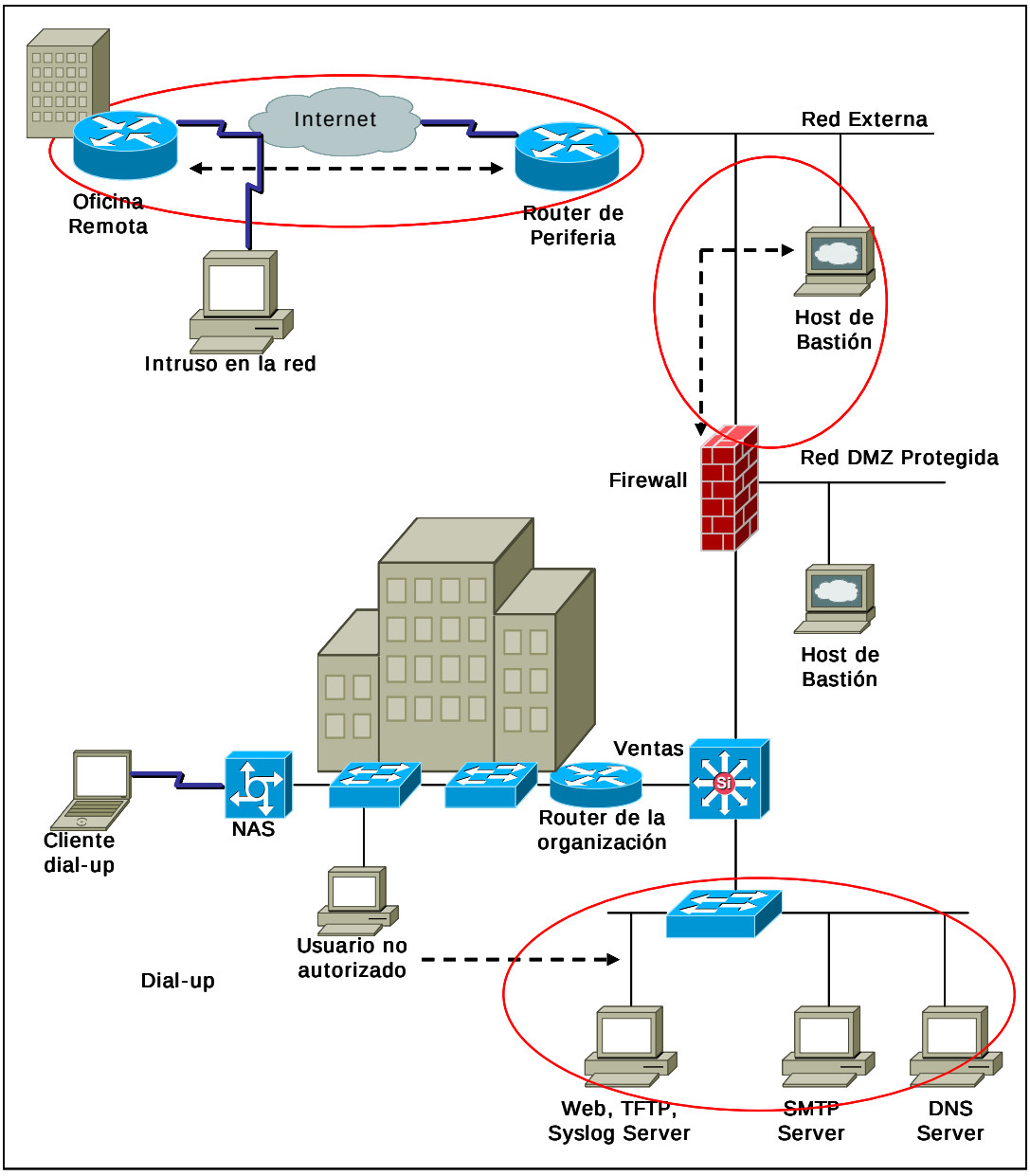


Figura No. 2-3. Puntos de ataque para acceso no autorizado

2.4.2.1. Obteniendo acceso Inicial

Un atacante usualmente intentará obtener acceso inicial hacia un host en la red, una vez que haya alcanzado este primer objetivo tratará de seguir accesando a través de este host a todas las demás redes que se conecten con este. El intruso establece una conexión con algún host sin utilizar una cuenta (una cuenta válida dentro de la base del host) y tratará de encontrar alguna vulnerabilidad en la seguridad que le permita tener mayor privilegio en el acceso (como acceso como usuario root en sistemas basados en UNIX).

El intruso tratará de obtener la mayor cantidad de información como le sea posible sobre el host al cual va a atacar por medio de técnicas de reconocimiento, para luego utilizar esa información y obtener acceso inicial. El intruso podría descubrir las direcciones IP del host que quiere penetrar y luego utilizar un sniffer de paquetes para capturar nombres de usuario y claves de ese host. El usuario podría también encontrar vulnerabilidad en los servicios de Internet utilizando un barredor o verificador de puertos (*port scanner*); la vulnerabilidad que se encuentre en estos servicios podría ser explotada y ganar acceso remoto a ese host.

Otra táctica que el intruso podría utilizar para obtener acceso inicial es utilizando lo que se conoce como “Ingeniería Social”. La Ingeniería Social en una manera de obtener información sobre algún dispositivo convenciendo a alguien de revelar la información necesaria, como nombres de usuario y claves o alguna otra información sobre algún tipo de acceso remoto.

EL intruso podría tratar de obtener acceso por medio de una conexión dialup (por marcaje telefónico) utilizando una herramienta conocida como “war dialer”, que es un programa que simplifica el marcado de un rango de números telefónicos con la esperanza de encontrara puertos de datos conectados a algún módem.

Un intruso también podría tratarse de un empleado dentro de la organización, es decir, un usuario local. Este empleado podría explotar la relación de confianza que goza al ser un empleado; al contra con una cuenta puede libremente ingresar a la red.

2.4.2.2. Ataques Basados en Contraseñas

Una variedad de ataques basados en contraseñas puede permitir al intruso obtener acceso remoto. Tan pronto como el intruso ha conseguido el nombre de usuario, espera que este usuario haya creado una clave fácil de adivinar. Tratará de adivinar esta clave manualmente utilizando tácticas de fuerza bruta. La manera más fácil de acceder a algún host en la red es a través de la puerta frontal ingresando el comando login. El intruso entonces, tratará de ingresar una clave que le permita ganar acceso inicial.

Como lo indicamos anteriormente, el intruso es capaz de descubrir nombres de usuarios y claves utilizando un analizador sniffer de paquetes; o una alternativa es obteniendo de algún host el archivo con las claves de los usuarios, como por ejemplo en sistemas UNIX, el archivo /etc/password o en sistemas basados en

Windows, el NT SAM. Luego utilizar alguna herramienta para decodificar el contenido de estos archivos y visualizar las claves e ingresar al host de la red.

Es posible proteger a los hosts de la red contra ataques de este tipo creando y reforzando políticas de seguridad que requieran claves difíciles de decodificar o de adivinar que incluyan caracteres no alfanuméricos, no enviar claves en texto claro en una red no segura y siendo muy cuidadoso con el acceso remoto al archivo de claves de un host.

2.4.2.3. Obteniendo acceso privilegiado

En términos de seguridad informática, una host confiable es una computadora que usted tiene bajo control administrativo o también es una computadora en la que usted de manera consciente toma la decisión de “confiar” para permitir el acceso a su red.

Tan pronto como el intruso ha ingresado a la red, aprovechará este acceso para poder escalar privilegios y explotar también las relaciones de confianza con otras redes y tratar de ingresar a otros hosts en esas otras redes. El éxito de ganar acceso privilegiado es ingresar con niveles de root o Administrador en un host sin apropiarse de una cuenta privilegiada sobre éste.

Las aplicaciones más comunes utilizadas sobre sistemas UNIX para obtener acceso privilegiado son los comandos *rlogin, rsh y rpc*.

2.4.2.4. Obteniendo Acceso Secundario

Una vez que el intruso obtiene acceso inicial, tratará de borrar cualquier pista o huella que evidencie su intrusión. El intruso puede intentar alguno de los siguientes medios para ocultar su acceso no autorizado:

- Limpiar archivos de registro y remover pistas o huellas de acceso remoto.
- Mover archivos de cuenta del directorio temporal.
- Instalar un analizador (*sniffer*) de paquetes para observar el tráfico.
- Instalar una herramienta de "puerta trasera" (*backdoor*) y establecer nombres de usuario y claves o instalando programas "Troyanos" como ***rootkit*** o ***BackOrifice***.

2.4.2.5. Atacando Servicios que Permiten Acceso Remoto

Algunas aplicaciones y servicios que utilizan TCP/IP pueden hacer que los host o dispositivos de red sean muy vulnerables a ataques de acceso remoto. Algunas aplicaciones fueron desarrolladas para facilitar, no para prevenir, las comunicaciones. Algunos servicios tienen métodos de autenticación muy básicos y en algunos casos simplemente no poseen ningún método de autenticación; esto fue hecho para asegurar que el usuario remoto tenga acceso permitido. Se debe deshabilitar servicios no utilizados que puedan habilitar el acceso remoto sobre hosts o equipos de red.

La tabla IV muestra alguno de los servicios IP que son vulnerables a ataques. También muestra el tipo de servicio y brevemente describe la vulnerabilidad del servicio.

TIPO	DESCRIPCIÓN DE LA VULNERABILIDAD
BSD r commands	La autenticación de acceso remoto utilizando los comandos **r** es por dirección fuente y es fácil de realizar un spoofing, con esto se provee total acceso a los host remotos que corren los servicios remotos.
FTP	El acceso por FTP utilizando el usuario "anonymous" permite al intruso leer y posiblemente escribir archivos de un host. No lo utilice a menos que sea absolutamente necesario.
Finger	El servicio **finger** puede ser usado para descubrir información sobre los usuarios, como preludio para obtener los *usernames*.
NFS	Permite el acceso a archivos sobre sistemas remotos. Tiene un esquema de autenticación débil (basado en direcciones IP fuentes) que fácilmente puede ser blanco de *spoofing*.
Telnet	Permite a los usuarios ingresar remotamente a un shell de comandos en texto claro. Controlado por un simple mecanismo de autenticación de usuario y clave que puede

	ser fácilmente rastreado por *spoofing*.
TFTP	Los intrusos pueden fácilmente solicitar una transferencia de archivos usando TFTP ya que no hay mecanismo de autenticación.
Aplicaciones de mensajería SMTP, POP, MIME	Los intrusos pueden manipular los ambientes de mensajería para obtener privilegios de root.
Servicios Web, HTTP	La vulnerabilidad en estos servicios incluye bugs (fallas) en software del servidor, mala configuración y sistemas operativos inseguros. Java, JavaScripts y ActiveX applets pueden actuar como virus o caballos de Troya.

Tabla IV. Servicios o aplicaciones IP que son vulnerables a ataques de acceso remoto

2.4.2.6. Vulnerabilidad en Programas que Permiten Acceso Remoto

Algunos programas y aplicaciones que se utilizan para la comunicación por Internet fueron desarrollados en lenguaje de programación C. Los programas utilizan *buffers* que son áreas o sectores (en la memoria) de longitud fija para el almacenamiento de la data variable. Una sobrecarga o desbordamiento de estos sectores de memoria (conocido como ***Buffer Overflow***) ocurre cuando un atacante con conocimientos de programación en lenguaje C deliberadamente

trata de exceder el tamaño o longitud fija de los buffers del programa para ganar acceso no autorizado al host que es blanco del ataque.

Probablemente el ejemplo más famoso de un ataque de este tipo explotando errores de buffer overflow en programas es el “gusano Morris” (Morris Worm) que se expandió a través de la Internet en 1988. Buffer overflow es un error muy común en la programación. Es posible protegerse de este tipo de ataques instalando las últimas actualizaciones (parches) de los programas; las actualizaciones están disponibles en el sitio Web del fabricante del software.

La debilidad en los sistemas operativos es también aprovechada por los intrusos para intentar obtener acceso a las computadoras en la red. Una medida de protección es visitar constantemente en Internet el sitio en búsqueda de las últimas actualizaciones de los sistemas operativos.

2.4.2.7. Mal Uso de los Sistemas después de Obtener acceso no Autorizado

Después que el intruso obtiene acceso a una red de computadoras, puede hacer uso de los hosts con propósitos no autorizados como por ejemplo, colocar archivos o recursos sobre otro sistema para que sean disponibles por otro intruso. Ejemplos de archivos no autorizados incluyen lo siguiente:

- **GIFs** – el uso no autorizado de una computadora para crear una librería de GIF u otro tipo de archivo gráfico. Alterando GIFs y el contenido del sitio Web.
- **Herramientas de Hacking** – el uso no autorizado de una computadora para almacenar, probar y distribuir herramientas de software que son útiles para los intrusos de red. Estas herramientas son entonces ampliamente disponibles por asociaciones de intrusos de red.
- **Versiones no licenciadas de software para libre distribución** – el término en inglés *WareZ* aplica ala distribución no autorizada de software.

2.4.2.8. Métodos Utilizados Para Contrarrestar Ataques por Acceso Remoto

La siguiente tabla explica los diferentes métodos que se pueden utilizar como medida de prevención para posibles ataques por acceso remoto:

Ataque	Prevención
Acceso Inicial	▪ Limitar los puntos de acceso a la red, así como también controlar la configuración para acceso dialup de los usuarios internos. ▪ Utilizar un servidor AAA (Authentication, Authorization and Accounting) para administrar los privilegios de acceso remoto, usernames y passwords. ▪ Utilizar protocolos de acceso más seguros como PPP, CHAP o MS-CHAP.

Ataques de password	▪ Reforzar una política de passwords difíciles de adivinar o de crackear. ▪ Ejecutar herramientas de crack como administrador para detectar passwords débiles. ▪ Utilizar la característica que tienen los sistemas operativos para obligar a que el usuario cambie su clave cada cierto tiempo.
Confianza en el Acceso	▪ Asegurar el nivel de acceso par alos niveles de root o Administrator. ▪ Vigilar y mantener las relaciones de confianza entre las diferentes redes.
Acceso Secundario	▪ Realizar un scanning de virus (Troyanos principalmente) que podrían estar instalados como backdoors. ▪ Realizar un scanning para verificar la existencia de puertos habilitados por Troyanos. ▪ Instalar y ejecutar programas que verifiquen la integridad de de los archivos y prevenir la existencia de archivos no autorizados dentro del sistema. ▪ Utilizar encriptación para asegurar la data en los discos duros de los hosts.

Servicios de Acceso Remoto	▪ Deshabilitar todos los servicios y comandos que no se utilizan normalmente. ▪ Verificar que las relaciones de confianza entre los hosts son seguras. ▪ Instalar versiones seguras de programas que ejecutan servicios de Internet como las últimas versiones de servidores Web, Correo y FTP. ▪ Cambiar los valores de configuración por defecto como por ejemplo el permitir acceso de lectura y escritura a todos los usuarios por otros valores más restrictivos.

Tabla V. Métodos Para contrarrestar Ataques de Acceso Remoto

2.4.3. Negación de Servicio (*Denial of Service*)

La negación de servicio (*Denial of Service* o DoS por sus siglas en inglés) es un intento por deshabilitar o corromper redes, sistemas o servicios de tal manera que se niega servicios de red a usuarios legítimos. Los intrusos de red a veces obtienen placer al negar el uso de un servicio público a otros usuarios, similar al vandalismo. Los intrusos pueden usar ataques DoS para comprobar la vulnerabilidad de un sistema para atacarlo, como un preludio a futuros ataques, para cubrir sus huellas después de obtener acceso no autorizado o simplemente como retaliación. El protocolo IP es vulnerable a ataques DoS; algunos tipos de ataques están disponibles y son relativamente fáciles de realizar. Los ataques

del tipo DoS se pueden realizar contra un router de periferia, un host de bastión o un firewall, como se muestra en la figura 2-4.

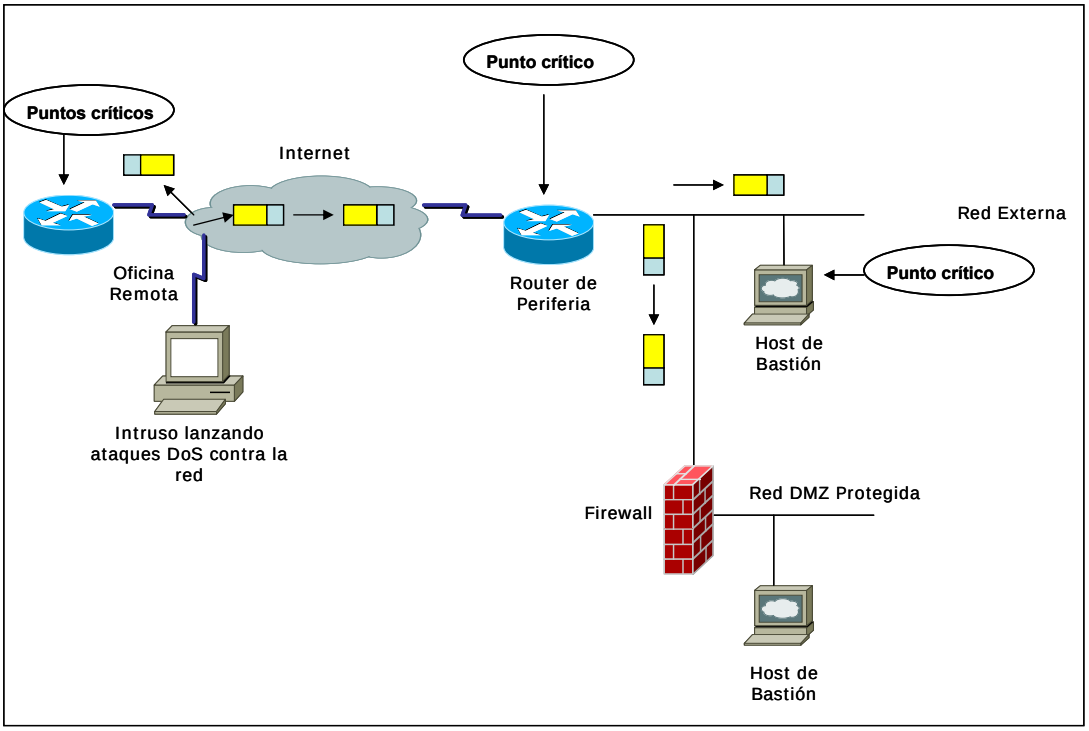


Figura No. 2-4. Puntos Críticos Para Ataques de Negación de Servicio

2.4.3.1. Sobrecarga del Recurso

Los exploits de negación de servicio que son del tipo “sobrecarga del recurso” son un intento de sobrecargar los recursos de un host o equipo de red con el objetivo de que los hosts objeto de ataque dejen de funcionar o no estén disponibles a usuarios legítimos. Los exploits intentan sobrecargar recursos como por ejemplo, el ancho de banda de la interfase de red, espacio en la memoria interna

(buffers), capacidad de procesamiento del CPU o espacio en los dispositivos de almacenamiento.

La siguiente tabla muestra los diferentes tipos de ataques DoS y las herramientas utilizadas para realizar este ataque; describe el exploit así como las medidas que se deben tomar para mitigar el ataque.

Tipo	Nombre del Exploit	Descripción	Contramedidas
Ping flood	**Pingflood.c** **Smurf.c** **Fraggle.c** **Papasmurf.c**	**pingflood.c** envía un gran número de paquetes ICMP del tipo Echo Request (ping) a un host. **smurf** envía gran cantidad de trafico ICMP Echo Request a una dirección de broadcast; cada uno de estos paquetes contiene la dirección fuente (dirección cambiada) del host que va a ser atacado. Cuando estos paquetes llegan a la red destino, todos los host de esa red responden con tráfico ICMP Echo Reply a la dirección del host víctima. El paquete original (ICMP Echo Request) es contestado por todos los hosts	Configurar a los routers de periferia para rechazar las respuestas de paquetes ICMP Echo Request. Desactivar el broadcast directo sobre todos los routers internos y externos. Configurar los routers de periferia para rechazar paquetes ICMP Echo Reply que le lleguen a sus interfaces.

		de la red; esto genera una tormenta de respuestas para el host víctima saturando el ancho de banda de la red, incrementando los recursos del CPU, etc. **fraggle** es la versión UDP de smurf.	
Half-open syn attak	**neptune.c** **synk4.c**	Inicia parcialmente numerosas sesiones TCP contra un puerto para que ninguna nueva conexión pueda ser inicia da por usuarios legítimos	Para routers Cisco, utilice la característica del IOS de Cisco para interceptar TCP. Utilice protección syn flooding en los firewalls Cisco PIX. Utilice un IDS para detectar este tipo de tráfico.
Packet Storms	**chargen** **Pepsi5.c** **UDP Bomb**	**chargen** corre sobre el puerto 19. Genera una cadena sin fin de caracteres ASCII para pruebas. Este tipo de ataque consiste en enviar un flujo de paquetes UDP con una dirección IP fuente cambiada (que corresponde a la del host víctima	Deshabilitar los servicios chargen y echo en todas las máquinas. Para firewalls Cisco PIX, utilizar la protección syn flooding.

	del ataque) y como dirección destino la del broadcast de la subred con puerto destino fijado en 19. El host víctima responde a cada broadcast, creando un flujo de paquetes UDP en un lazo infinito, lo que resulta en una negación de servicio del host. Existen algunas variaciones de este ataque. **Pepsi5.c** inunda un host víctima con paquetes UDP que contienen direcciones IP fuentes aleatorias. **UDP Bomb** forma paquetes UDP que tienen una longitud incorrecta en la cabecera del paquete, causando que algunos hosts sufran pánico en el kernel.	Instalar las últimas actualizaciones de los sistemas operativos.

Tabla VI. Ataques del Tipo Sobrecarga de Recursos

2.4.3.2. Ataques DoS del tipo "Data Fuera de Banda" (Out-of-Band Data)

Los ataques DoS del tipo Out-of-Band manipulan la cabecera IP (TCP o UDP) para tratar de exceder la operación normal de protocolo IP. El resultado es que el host o equipo de red que es víctima del ataque deje de operar.

La siguiente tabla muestra los diferentes tipos de ataques Out-of-Band y las herramientas utilizadas para realizar este ataque; describe el exploit así como las medidas que se deben tomar para mitigar el ataque.

Tipo	**Nombre del Exploit**	**Descripción**	**Contramedidas**
Paquetes Sobrecargados (*Oversized packets*)	**Ping of death (simping.c)**	Modifica la porción de la cabecera IP, indicando que hay más data en el paquete de lo normal, o envía data con exceso en el tamaño máximo permitido para un paquete (65535) causando que el host receptor se caiga.	Filtrar el tráfico ICMP que sea grande o fragmentado en la red. Utilizar sistemas IDS para detectar este tipo de tráfico.
Paquetes Sobrepuestos (*Overlapped packets*)	**winnuke.c**	Envía data fuera de banda (out-of-band) sobre una conexión establecida en un host Windows 95 o Windows NT (NetBIOS, puerto 137) ocacionando que el host reinicie o deje de operar.	Desactivar NetBIOS si es necesario. Instalar las actualizaciones de los sistemas operativos (parches)
Fragmentación	**teardrop.c**	Toma ventajas de algunas implementaciones del proceso de reensamblaje de fragmentación IP que no maneja apropiadamente el overlapping de fragmentos IP, causando un	Descartar paquetes IP fragmentados en los routers de periferia

		sobrante en el buffer de memoria.	
Spoofing de direcciones IP origen (*IP source address spoofing*)	**land.c**	Hace que un computador realice una conexión TCP hacia él mismo obteniendo un lazo y por lo tanto tenga que ser reiniciado.	Filtrar los paquetes IP-spoofed en los routers o hosts de periferia. Instalar las actualizaciones de los sistemas operativos.
Paquetes con cabecera deformada (*Packet headers malformed*)	**UDP Bomb**	Forma paquetes UDP que tienen una longitud incorrecta en la cabecera, causando que algunos hosts sufran pánico en el kernel.	Instalar las actualizaciones de los sistemas operativos.

Tabla VII. Ataques DoS del tipo Data Fuera de Banda

2.4.3.3. Otros Ataques DoS

Desafortunadamente, otros ataques de negación de servicio (DoS) son utilizados para atacar redes IP. Los ataques DoS pueden inclusive explotar vulnerabilidades en servicios o hardware específicos no necesariamente relacionado con el protocolo TCP/IP. A continuación mostramos ejemplos de otros tipos de ataques de negación de servicio:

- **Negación de Servicio Distribuido (DDoS).-** Utiliza múltiples sistemas coordinados para atacar un sitio Web o host.

- **Bombas de correo electrónico.-** Existen algunos programas gratuitos que envían correo basura a individuos, listas o dominios, monopolizando el servicio de correo electrónico.

- **CPU hogging.-** Programas como caballos de Troya o virus que afectan los recursos de memoria, CPU, etc. niegan de estos recursos a usuarios legítimos.

- **Misrouting traffic.-** Deshabilitando el tráfico por routers mal configurados para reenrutar el tráfico lejos de la red o destino.

- **Negación de servicio accidental.**- Usuarios legítimos o administradores del sistema pueden causar ataques de negación de servicio por mala configuración o mal uso.

- **Desbordamiento del Buffer.**- La versión 4.0 de Microsoft Internet Information Server es susceptible al desbordamiento del buffer que puede desplomar al servidor. Se han detectado vulnerabilidades de este tipo en varios sistemas que pueden ser corregidos con las actualizaciones correspondientes o service packs.

- **CGI Exploits.**- Los Web browsers podrían divulgar información crítica cuando un usuario malicioso añade ciertos caracteres al final de la dirección URL que refiere a un archivo en el servidor. Un usuario remoto puede recuperar el código fuente para el archivo, divulgando información propietaria, derechos

reservados del código fuente y usuarios y claves utilizados para ingresar a base de datos.

- **Server DoS.**- Los servidores Microsoft Windows NT 4.0 (con service pack 3 o 4) podrían reiniciarse o quedarse inhibidos dependiendo de la cantidad de memoria que el servidor tenga, cuando una cadena de caracteres de suficiente longitud aparece en un cierto puerto durante una sesión de Telnet, seguido por un comando de ejecución.

2.4.3.4. Métodos Utilizados para Contrarrestar Ataques de Negación de Servicio

Se puede utilizar los siguientes métodos para disminuir el impacto de los ataques de negación de servicio:

- Utilice auditoria de rastreo para detallar transacciones, registro de fecha y hora, host origen y destino, puertos, duración y número total de bytes transmitidos.
- Utilice registros (logs) de alerta en tiempo real para generar alarmas en el caso de ataques DoS o en el caso de condiciones pre-configuradas.

2.4.4. Manipulación de Datos

Un intruso puede capturar manipular y reenviar data que es enviada sobre un canal de comunicaciones usando manipulación de datos. La manipulación de datos también es conocida como “personificación”.

Los ataques de este tipo pueden tomar las siguientes variaciones conocidas en inglés por los siguientes nombres:

- Caracterización (*IP Address Spoofing*)
- Contestación a la sesión (*Session Reply and Hijacking*)
- Re-enrutamiento (*Rerouting*)
- Repudiación (*Repudiation*)

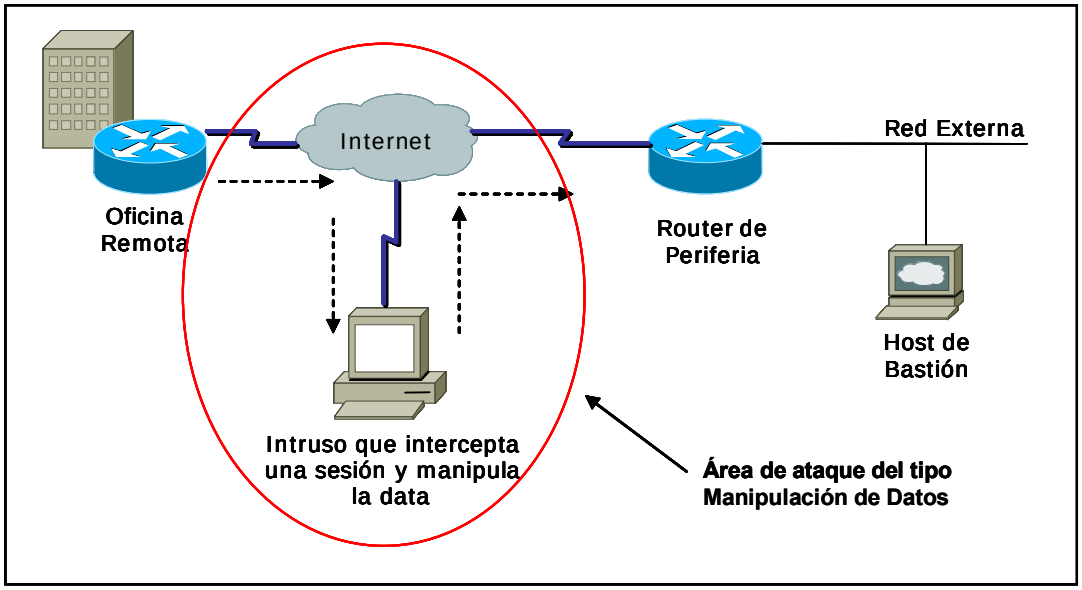


Figura No. 2-5. Punto de Ataque del tipo Manipulación de Datos

Estas variaciones en los ataques de manipulación son posibles por las vulnerabilidades en el protocolo IP asociado a servicios y aplicaciones. La figura 2-5 muestra los sitios en una red donde pueden ocurrir ataques de este tipo.

2.4.4.1. Caracterización (*IP Spoofing*)

Un intruso puede utilizar la técnica conocida como *IP spoofing* para personificar la identidad de un host para aplicaciones o servicios que utilizan direcciones IP fuente o destino para autenticación. Un ataque *IP spoofing* ocurre cuando un intruso fuera de la red de la organización pretende ser un host confiable (este host confiable puede estar dentro o fuera de la red de la organización). El spoof utiliza una dirección IP que está dentro del rango de direcciones de la red o puede utilizar una dirección IP externa pero que está autorizada y es confiable para proveer acceso a recursos de la red.

El *spoofing* usualmente incluye manipulación de paquetes TCP/IP para falsificación de direcciones IP, es por eso que parece ser otro host. Por ejemplo: el intruso puede usar *IP address spoofing* para asumir la identidad de un host válido o confiable y de esta manera obtener los privilegios de acceso a ese hosts falsificando la dirección fuente de un host confiable. *El spoofing* es conocido como ataque de “enmascaramiento”.

Un atacante puede especificar una dirección fuente arbitraria de un paquete de entrada e intentar hacer “bypass” de mecanismos de autenticación basados en

dirección. Esto es especialmente efectivo si la dirección fuente arbitraria es de un host que está detrás de un firewall o de un router de periferia.

Normalmente, un ataque *IP spoofing* está limitado a la inserción de datos o comandos dentro de una cadena de datos existente entre que circula entre un cliente y un servidor de aplicación en una conexión de red peer-to-peer.

Los atacantes que utilizan *IP spoofing* están en capacidad de hacer bypass a mecanismos de autenticación (sin son implementados de manera incorrecta) pueden derribar filtros en routers configurados con filtros de paquetes.

Las contramedidas para el *IP spoofing* incluye configurar los routers de periferia para que realicen filtrado (listas de acceso por direcciones IP y por puertos TCP/UDP) de tráfico entrante a la red. El uso de sistemas detectores de intrusión también ayuda a prevenir este tipo de ataque.

2.4.4.2. Contestación a la Sesión (*Session Reply*)

El ataque de contestación a la sesión consiste en interceptar y capturar una secuencia de paquetes o comandos de aplicación, manipular la data capturada (como por ejemplo, alterar la cantidad de dinero de una transacción) para luego devolver la data para causar una acción no autorizada.

El ataque “session hijacking” consiste en que el intruso asume el control de una sesión IP e inserta paquetes de datos falsificados después de que la sesión se ha

establecido. Los métodos de hijacking incluyen IP spoofing, manipulación de direcciónes IP o puertos TCP/UDP fuente y destino y alteración y predicción de secuencia de números. El intruso utiliza un analizador de protocolos para observar, predecir y luego alterar y retransmitir una secuencia de paquetes TCP/IP.

Los ataques de Session reply y hijacking solo pueden ser realizados por programadores expertos, así que ha habido pocos ataques documentados. Una herramienta para realizar sesiones de hijacking es el programa "hunt-1.0" que corre sobre plataforma Linux.

Las medidas a tomar contra los ataques de session reply y hijacking incluyen los siguientes métodos y tecnologías:

- Ajustar los parámetros de configuración de seguridad del visualizador Web (*Web browser*) para prevenir la descarga de códigos maliciosos (*applets*) o hacer que el browser anuncie una notificación para permitir ejecutar códigos móviles cuando estos son encontrados.
- Bloquear el acceso corporativo a sitios de correo electrónico público para limitar el riesgo de infección o acceso a información confidencial.
- Utilice listas de control de acceso en los equipos de periferia.
- Utilice autenticación con servidores de autenticación como por ejemplo RADIUS (*Remote Authentication Dial-In User Service*), TACACS (*Terminal Access Controller Access Control System*) o por medio de SSL (*Secure Socket Layer*).

- Utilice tecnologías de encriptación para proteger la integridad y confidencialidad de la información.
- Utilice firmas digitales ofrecidas por autoridades de certificación para la no-repudiación.

2.4.4.3. Re-enrutamiento (*Rerouting*)

Los intrusos de red pueden utilizar re-enrutamiento para obtener acceso no autorizado a routers y alterar la configuración de enrutamiento o para cambiar la identidad de routers o hosts a través de un camino de red. La consecuencia del re-enrutamiento es que puede permitir a un host remoto al presentarse como un host local en la red interna. Como resultado, los servicios que hacen relay sobre dirección IP como por ejemplo la autenticación pueden ser comprometidos.

La contramedida a los ataques de re-enrutamiento es limitar el acceso a los routers para prevenir re-configuración de rutas, deshabilitar el enrutamiento en todos los hosts de la red, implementar un sistema de detección de intrusiones (IDS) para detectar este tipo de ataques.

2.4.4.4. Repudiación (*Repudiation*)

Uno o más usuarios envueltos en una comunicación como por ejemplo una segura transacción bancaria puede denegar participación, comprometer transacciones electrónicas y acuerdos contractuales.

2.5. Cómo mantenerse informado sobre los ataques procedentes de Internet?

Naturalmente, existen muchos otros sistemas de ataque, aunque su estudio completo rebasa el objetivo de este documento. Sin embargo, los ingenieros de redes y los administradores de red en general se deben preguntar de qué forma pueden eliminar los diversos riesgos asociados a estos ataques en sus entornos de red. Hay dos estrategias distintas.

Se ha propuesto utilizar extensas listas de los ataques catalogados producidos en Internet. Así es posible disponer de la información más completa sobre los incidentes ocurridos.

Otro enfoque, que ha tenido cierto éxito, consiste en contactar con una biblioteca centralizada de información en línea que contiene riesgos de ataque a la seguridad.

La más conocida de estas bibliotecas está bajo la gestión del COMPUTER EMERGENCY RESPONCE TEAM (CERT), un organismo respaldado por el gobierno estadounidense situado en la Carnegie-Mellon University. EL CERT le proporcionará de buen grado cualquier información relacionada con ataques aplicables a su entorno. Con regularidad envía información de asesoramiento, y le corresponde a los usuarios administradores de red o consultores de seguridad decidir si quiere actuar o no según estos consejos.

Otras organizaciones que ofrecen información sobre seguridad y asesoramiento en línea o en tiempo real incluyen la COMPUTER INCIDENT ADVISORY CAPABILITY (CIAC) y el FORUM FOR INCIDENT RESPONSE IN SECURITY TECHNOLOGY (FIRST). Ambas organizaciones ponen información útil a disposición del público en Internet.

Tal vez la opción más adecuada para los administradores de seguridad de una Intranet sea emplear todos los recursos disponibles. No dude en utilizar las listas de ataques que consideren útiles, así como la información que proporcionan las organizaciones del CERT.

CAPÍTULO III

ANALISIS DE LA INFRAESTRUCTURA DE RED DE LA FIEC, PLANIFICACIÓN Y EJECUCIÓN DE PRUEBAS DE VERIFICACIÓN DE VULNERABILIDADES LOCAL Y REMOTO

3.1. Introducción

Una vez que se ha revisado los conceptos generales de seguridad en las redes de datos, así como los riesgos existentes en las mismas, realizaremos un análisis de la red de computadoras de la FIEC. Este análisis implica una revisión desde la parte física, es decir, tipo de equipos, conexión entre ellos, pasando por la parte lógica, lo cual implica los protocolos que utilizan para la comunicación, servicios disponibles, tipo de direccionamiento lógico, y esquemas de seguridad. Además explicaremos el funcionamiento de las herramientas que se utilizaron para las pruebas de verificación de vulnerabilidad (*scanning*) y para las pruebas de detección de intrusiones en la red de la FIEC.

Basados en el análisis de la red, realizaremos la planificación y ejecución de las pruebas de scanning local y remoto con herramientas diseñadas para este tipo de trabajo.

Los resultados de estas pruebas reflejarán los puntos débiles en la red; basado en las debilidades encontradas se analizará el origen de las mismas y las soluciones recomendadas para mejorar el nivel de seguridad en la red.

3.2. Análisis de la infraestructura física de la red

En esta sección se describirá mediante diagramas la estructura actual de la red, describiendo cada uno de los componentes que forman parte de la misma.

3.2.1. Descripción actual de la red

Esta "radiografía" a la red se la realizará en dos puntos fundamentales:

- Análisis de la red LAN
- Análisis del esquema de integración con la red de la ESPOL

El objetivo es identificar todos los puntos y objetos en la red que sean propensos a algún tipo de ataque por parte de hackers internos o externos. Estos puntos vulnerables serán relacionados con algún tipo de ataque de los analizados en el capítulo anterior.

También se tocará en un ítem aparte la estructura y análisis del esquema de seguridad y los recursos principales con los que cuenta la FIEC.

3.2.1.1. Infraestructura LAN

La estructura de red de la FIEC es muy sencilla, en lo que se refiere a equipos de conectividad cuentan con 4 hubs Bay Networks de 24 puertos RJ-45 que trabajan a 10 Mbps. La conexión entre los hubs es en cascada, es decir, desde un hub principal se distribuye la señal de datos hacia los tres hubs restantes por medio de cable UTP; con esto tenemos lo que se conoce como un dominio de colisión y un dominio de broadcast (dominio de difusión).

Existe un computador que realiza la función de ruteador utilizando dos tarjetas de red separando la red de la FIEC del resto de la red del campus de la ESPOL.

En esta red constan los puntos de red para los laboratorios, para las oficinas de los profesores y para la oficina de los administradores de la red con los servidores principales.

En la parte LAN se pudo identificar los siguientes equipos críticos que se describen en la tabla VIII.

EQUIPO	PLATAFORMA	FUNCIÓN	DIRECCIÓN IP
Ceibo.fiec.espol.edu.ec	Linux Red Hat 7.3	Servidor DNS, SMTP	200.9.176.5
Cedro.fiec.espol.edu.ec	Linux Red Hat 7.3	Servidor WWW	200.9.176.7
Palma.fiec.espol.edu.ec	Linux red Hat 8	Servidor Web Mail	200.9.176.3

Tabla VIII. Servidores Principales de la FIEC

Estos servidores tienen presencia en Internet, lo que los convierte en servidores públicos y por lo tanto posibles blancos a ataques.

La figura 3-1 nos muestra la infraestructura de red LAN de la FIEC de manera detallada.

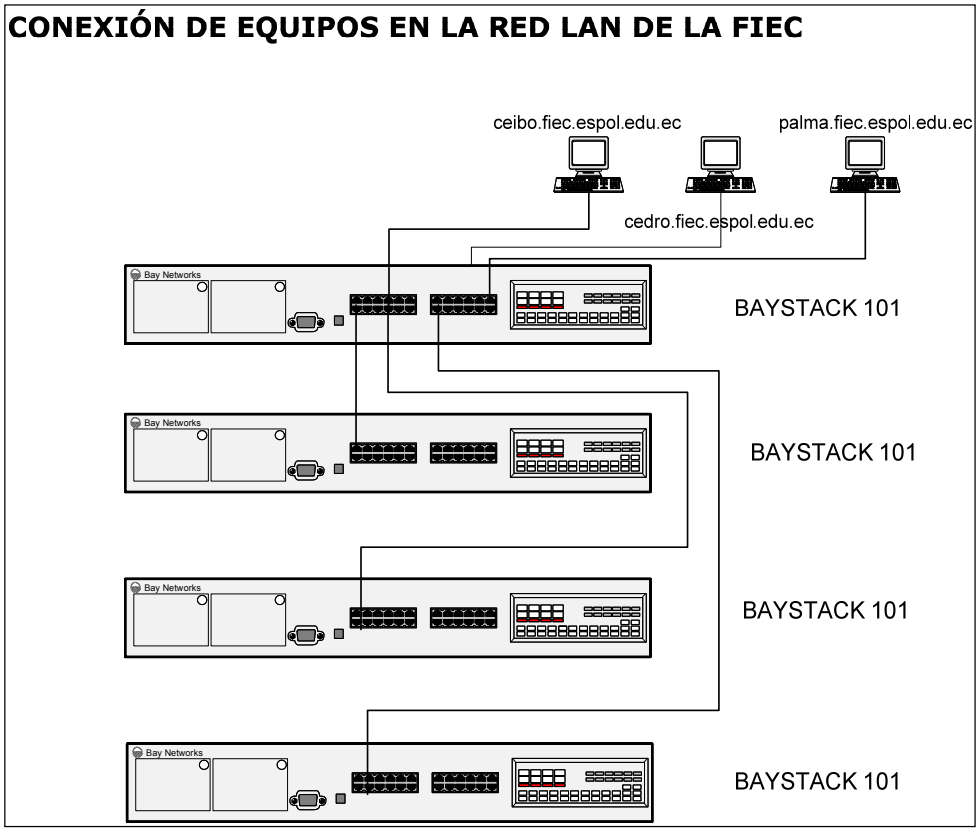


Figura No. 3-1. Diagrama de la red de área local (LAN) de la FIEC

3.2.1.2. Infraestructura de acceso a las demás redes de la ESPOL

Realmente, no aplica en un ciento por ciento el término WAN en la red de la FIEC. Las redes WAN (Wide Area Nework) son redes que geográficamente están separadas; para el caso de la FIEC, esta red se encuentra en el mismo campus de la universidad, y es una red más correspondiente al total de subredes de la ESPOL.

Como mencionamos anteriormente, el equipo de frontera es un PC con dos tarjetas de red para separar la red de la FIEC del resto de la red del campus, esta PC actúa como ruteador y como gateway (puerta de acceso) para la facultad.

El medio de transmisión para el acceso a la ESPOL es fibra óptica monomodo a una tasa de transmisión de solo 10 Mbps, por lo que está desperdiciando la mayor parte de los beneficios de tener un enlace de fibra óptica entre dos localidades.

Esta fibra llega hasta las oficinas de CECERCOMP que es la entidad que administra la red de datos de la ESPOL, es en CECERCOMP donde se concentra todos los requerimientos por consultas y servicios de Internet. Para el caso de la FIEC, CESERCOMP actúa como un proveedor de última milla puesto que los servicios que brinda la facultad son totalmente independientes de CECERCOMP.

En la figura 3-2 se muestra el esquema de conexión para la WAN de la FIEC

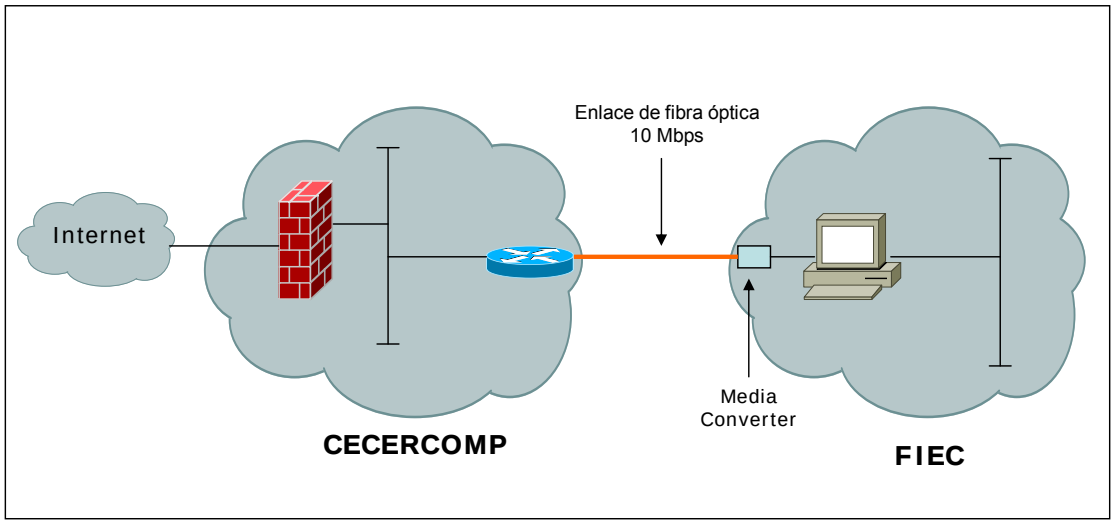


Figura No. 3-2. Esquema de conexión desde la red de la FIEC hacia el resto de la red de la ESPOL

3.3. Análisis de la estructura lógica y de los recursos de red de la FIEC

A nivel lógico, se analizarán varios aspectos fundamentales, entre ellos podemos mencionar los protocolos de comunicaciones que se utilizan en la red, el esquema de direccionamiento IP existente, la creación de redes virtuales (VLANs) y el esquema de seguridad a nivel lógico.

3.3.1. Protocolos utilizados en la red

Gracias a la ayuda del administrador de la red de la FIEC, nos pusimos al tanto de los protocolos de comunicaciones que se utilizan para las comunicaciones. Básicamente, TCP/IP es el protocolo utilizado para todas las aplicaciones disponibles en la red de datos de la Facultad.

El esquema de direccionamiento IP corresponde a la red 200.9.176.0 con máscara de subred 255.255.255.0; esto quiere decir que todos los hosts cuya dirección IP comience con los tres primeros octetos 200.9.176 pertenecerán a la red de la FIEC.

La característica de este esquema de direccionamiento es que existe un número de 256 direcciones de las cuales, la dirección 200.9.176.0 es el identificador de red (network ID) y la 200.9.167.255 representa a la dirección de broadcast y por lo tanto no pueden ser configuradas en ningún host. En conclusión se tiene un total de 254 direcciones disponibles para que puedan ser configuradas en los hosts de la red.

La siguiente tabla explica el rango de direcciones de la FIEC:

Dirección IP	Máscara de Subred	
200.9.176.0	255.255.255.0	Identificador de red
200.9.176.1	255.255.255.0	Primera dirección disponible
200.9.176.2	255.255.255.0	Segunda Dirección disponible
200.9.176.3	255.255.255.0	Tercera dirección disponible
.		
.		
.		
.		
200.9.176.254	255.255.255.0	Última dirección disponible
200.9.176.255	255.255.255.0	Dirección de broadcast

Tabla IX. Rango de Direcciones IP de la FIEC

Este rango de direcciones IP pertenecen al rango público de direcciones IP definidas por el INTERNIC que es el organismo encargado del control de la INTERNET a nivel mundial. La FIEC (como toda la red de la ESPOL) cuenta con direcciones públicas directamente configuradas en todos sus hosts lo que implica que llegará un momento en que las direcciones disponibles serán cada vez menos a medida que vaya creciendo la red en número de hosts.

3.3.2. Infraestructura de Seguridad

En lo referente a la seguridad en la red, el dispositivo que se encarga de realizar procesos de filtrado de paquetes es precisamente el gateway de la red (IP 200.9.176.2). Esta PC tiene instalado una aplicación que corre bajo sistema operativo D.O.S. con el que el administrador permite o deniega cierto tipo de tráfico desde o hacia la red interna.

Este equipo es el único equipo con que cuentan en la red para aplicar un esquema de seguridad a nivel lógico.

En cuanto a la seguridad de acceso físico al rack donde se encuentran los equipos de conectividad, el nivel es muy bajo, el sitio se encuentra casi a la intemperie y cualquier estudiante o persona particular ingresa al cuarto donde están los equipos y puede realizar (voluntaria o involuntariamente) algún tipo de acción que perjudique a la red de la FIEC, como por ejemplo, desconectar algún cable de red (vandalismo) y dejar sin conexión a alguna PC o servidor o a algún segmento de red.

No cuentan con ninguna herramienta de detección de intrusiones que permita verificar si hay algún patrón de tráfico que pueda ser considerado como un ataque, o alguna herramienta que detecte dentro del contenido de los correos que salen o entran a la red, archivos adjuntos que puedan ser virus.

En un esquema como el actual no está garantizado ciento por cierto la invulnerabilidad en los componentes de la red, más bien se debe seguir algunos

pasos para poder mejorar el esquema de red y obviamente para mejorar el nivel de seguridad.

En la figura 3-3 se muestra el diagrama completo de la FIEC, identificando los puntos críticos que pueden ser objetivos potenciales para posibles ataques.

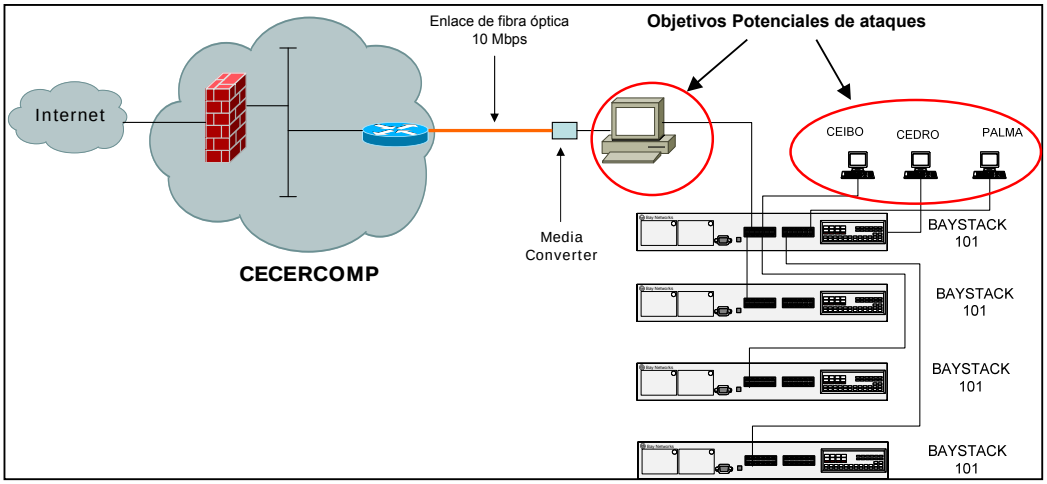


Figura No. 3-3. Diagrama de red completo de la FIEC

Como se puede apreciar en el gráfico, los equipos críticos son básicamente los tres servidores que se mencionan en la tabla VIII. Es importante recalcar que no es suficiente con definir políticas de acceso hacia Internet, y especificarlas por la dirección IP fuente y destino y por el tipo de puerto (TCP o UDP); para el caso de tráfico de salida es primordial que se definan las reglas necesarias para los protocolos más utilizados.

Se debe considerar también el hecho de saber administrar un recurso tan limitado como lo es el ancho de banda de acceso hacia Internet; a pesar que la red de CESERCOMP actúa como proveedor de Internet para la FIEC y en general para todas las redes de la ESPOL, en la salida hacia Internet a través del proveedor (en este caso ESPOLTEL) se forma un cuello de botella.

No es factible dejar que un estudiante que utiliza una de las computadoras del laboratorio de la FIEC descargue información no productiva como por ejemplo videos o archivos de audio (*.MPEG, *.mp3, *.avi). La descarga de este tipo de archivos desde Internet puede inclusive llegar a saturar el ancho de banda del enlace, y es mucho más crítico cuando en los equipos de conexión no existe la capacidad de configurar calidad de servicio, es decir, reservar un determinado ancho de banda para los protocolos más importantes y utilizados.
Bajo este esquema, la red de la FIEC no tiene aplicado una solución de este tipo, se tiene planeado implementar alguna solución que brinde este tipo de características.

Existen equipos en el mercado que son capaces de brindar calidad de servicio en enlaces de este tipo. La compañía CISCO SYSTEMS que diseña y fabrica equipos de comunicación de datos, tiene en sus ruteadores esta cualidad; para enlaces hacia Internet, donde la navegación y el envío y recepción de correos son las aplicaciones más comunes, se podría definir una distribución de ancho de banda de la siguiente manera:

PROTOCOLO	% DE RESERVA
http	50%
Smtp	25%
ftp	15%
Otros	10%

Tabla X. Ejemplo de distribución porcentual del ancho de banda de acceso a Internet por protocolos más utilizados

También existen otros criterios de reservación de ancho de banda, unos criterios se basan en la dirección IP origen, de tal manera que cualquier paquete que tenga una dirección IP origen definida por el administrador tendrá mayor porcentaje de capacidad del ancho de banda, por lo tanto la calidad del servicio para el dispositivo (host, PC, teléfono IP, etc) será mayor con relación a cualquier otro en la red.

Esto es muy utilizado actualmente en los establecimientos que brindan el servicio de Cyber Cafés, ya que en su mayoría estos locales son muy concurridos especialmente para utilizar el servicio de llamadas internacionales a través de Internet (voz sobre IP). Los teléfonos que se utilizan tienen una dirección IP definida, por lo tanto a las direcciones de estos teléfonos se les dará mayor capacidad del ancho de banda del enlace para que la calidad de la voz sea aceptable.

En el caso de la FIEC, no hay ningún dispositivo configurado para realizar esta tarea, por lo tanto, hay que tomar otras medidas para que el acceso hacia Internet sea controlado y de buena calidad.

Con relación a las reglas con el tráfico de entrada hacia la FIEC, se debe hacer un comentario necesario: Siempre se considera un riesgo el dejar una puerta de entrada hacia la red privada, pero es necesario hacerlo. Como se revisó en el capítulo 1, lo mejor es que siempre se mantenga "cerrada la puerta de ingreso" a nuestra red.

Indudablemente es muy necesario dar paso a "ciertas personas" (haciendo una analogía con un edificio) para comunicarse con nosotros. Este es el caso de aplicaciones como correo el electrónico mediante el cual otras personas en el mundo nos envían información vital. La FIEC tiene un servidor de correo basado en LINUX, este servidor se encuentra en físicamente en la red privada, sin embargo, el peligro que existe es que por lo general, un intruso tratará de atacar a un servidor de correo como objetivo número uno puesto que siempre los servidores de correo interactúan con las PCs que tengan un cliente de correo (como por ejemplo Microsoft Outlook Express).

Continuando con el análisis a nivel de seguridad, comentábamos la necesidad de verificar la reglas por tráfico entrante a la red, recordemos que existe un servidor Web dentro de la red y a que ingresan desde Internet para revisar la página Web de la FIEC, es importante entonces restringir el acceso a este servidor solo por protocolo http (puerto tcp 80). De igual manera, solo se debe brindar acceso por

el protocolo SMTP (*Simple Mail Transfer Protocol*, puerto TCP: 25) al servidor **ceibo** (IP: 200.9.176.5), para que pueda recibir requerimientos desde Internet por este protocolo y de esta manera los usuarios puedan recibir correos electrónicos desde Internet.

Una gran desventaja (hasta cierto punto) es que la red de la FIEC consta de direcciones IP públicas (200.9.176.0 / 255.255.255.0) con una capacidad de 254 direcciones disponibles para hosts. A pesar de que en la actualidad les sobren direcciones IP para configurar a los hosts, se va a llegar a un punto en que las direcciones sean limitadas, por lo tanto, es importante pensar en una solución para esto. Aquí entra en juego lo que se conoce como NAT (Network Address Translation, por sus siglas en inglés). Lo que se consigue con esto es que varios dispositivos en la red compartan una misma dirección pública para acceder a Internet y de esta manera tener mayor disponibilidad en número de direcciones IP públicas.

La administración de la red de la FIEC cuenta con un sistema de validación de usuarios para control del uso de las computadoras (especialmente las del laboratorio); cada estudiante debe obtener su nombre de usuario y su correspondiente clave de acceso para poder utilizar las computadoras del laboratorio de la FIEC. Adicionalmente, cada computador cuenta con una herramienta de protección contra virus debidamente actualizada para prevenir que virus se infiltren en la red.

El control del tiempo de uso de cada computador está definido a dos horas por cada estudiante; desde el momento que el estudiante ingresa su nombre de usuario y su clave empieza a ejecutarse un software de control que gestiona el tiempo de utilización del computador para cada estudiante. Esta herramienta provee un registro para el administrador de la red puesto que se tiene el registro de cuál fue la persona (o al menos el nombre de usuario) que utilizó determinada computadora durante el transcurso del día.

Finalmente debemos aclarar que no se nos proporcionó ningún tipo de información adicional sobre las políticas definidas en el equipo que funciona como firewall por razones de seguridad y confidencialidad, por lo tanto no fue posible realizar un análisis exhaustivo sobre las reglas de acceso para la FIEC, sin embargo, las conclusiones realizadas como resultado de las pruebas que se hicieron en la red podrían indicar cualquier tipo de deficiencia en las reglas de acceso en el firewall.

3.4. Herramientas de Gestión de seguridades

Como habíamos mencionado en el capítulo 1, es muy importante para el administrador de cualquier red de datos realizar el monitoreo de la actividad de su red, no solo para verificar el correcto funcionamiento de toda la infraestructura que la conforma, sino para controlar el correcto uso de todos los recursos que esta ofrece a los usuarios.

Existen diferentes herramientas que sirven para gestionar redes, la gran mayoría basadas en el protocolo SNMP (Simple Network Management Protocol), que están catalogadas como herramientas de administración de equipos y dispositivos de red. También están disponibles otro tipo de herramientas cuyo objetivo principal es brindar seguridad (como el caso de un Firewall) y otras que sirven para descubrir las deficiencias en una red (como los detectores de intrusiones).
También están disponibles las herramientas diseñadas para "escudriñar" y sacar provecho de las deficiencias en una red, logrando con esto el acceso a algún recurso de la red y hacer mal uso de este. Precisamente es que en la actualidad, estas herramientas que han sido diseñadas con un fin poco ético son utilizadas con un objetivo más útil, esto se conoce como "*Ethical Hacking*".

Recordemos que Ethical Hacking se lo puede definir como el servicio brindado por profesionales en la rama de seguridades en redes de datos cuyo objetivo de descubrir las vulnerabilidades y deficiencias en una red con tal de sugerir al cliente cuáles son las mejoras que debe realizar para eliminar esas deficiencias y de esta manera mantener una red más segura.

Precisamente, el utilizar las mismas herramientas que un intruso utilizaría para descubrir deficiencias y ganar acceso a algún host de la red es lo que hacen quienes se dedican al ethical hacking; se debe tener un nivel de confidencialidad y confianza muy alto ya que la información obtenida como resultado de esta auditoria de seguridades es crítica para los intereses de la corporación.

En el desarrollo de este proyecto, hemos enfocado nuestras pruebas utilizando dos herramientas de gestión de seguridades: CISCO SECURE SCANNER y ETRUST INTRUSION DETECTION. Ambas herramientas están dentro del grupo de herramientas de reconocimiento ya que con ellas se puede averiguar los hosts que están disponibles en una red (hosts activos) y saber detalles de los mismos, es decir, si son servidores, ruteadores, switches, plataforma de sistema operativo, servicios TCP-IP disponibles, etc.

A continuación mencionaremos brevemente detalles de estas herramientas:

3.4.1. Cisco Secure Scanner

La casa fabricante CISCO SYSTEMS (líder en soluciones de networking) ofrece una amplia gama de soluciones de seguridad para las empresas. La línea de seguridad de Cisco incluye el CISCO SECURE SCANNER, una herramienta de detección de vulnerabilidades. Esta herramienta permite diagnosticar y reparar problemas de seguridad en ambientes de red.

3.4.1.1. Características del Cisco Secure Scanner

Podemos mencionar las siguientes:

- **Descubrimiento de Vulnerabilidades.-** El scanner descubre puntos débiles de seguridad en la red antes que algún intruso pueda explotarlas. La herramienta permite automáticamente compilar un inventario de los dispositivos y servidores en la red; luego utilizando una base de datos, el

scanner identifica las vulnerabilidades asociadas con servicios de red para mostrar al usuario en una tabla todas las deficiencias en los servicios de red de los dispositivos escaneados.

- **Detalle de las vulnerabilidades.-** Esta herramienta provee detalles sobre cada vulnerabilidad así como del host en el que ha sido detectado dicha falencia (el host vulnerable), la debilidad en el sistema operativo, una descripción de la vulnerabilidad y las acciones que se deben tomar para corregir la debilidad.
- **A qué redes escanear.-** Se puede utilizar esta herramienta para toda red basada en el protocolo TCP/IP. La herramienta puede escanear redes conectadas a Internet así como también redes *standalone* (redes aisladas de Internet).

3.4.2. eTrust Intrusion Detection

eTrust Intrusion Detection es una herramienta que brinda protección contra el desarrollo y ejecución de ataques del tipo Distributed Denial of Service (DDoS) y permite al administrador realizar de manera efectiva un control y monitoreo del uso de la conexión a Internet.

Esta solución cuenta con una máquina integrada de antivirus que se actualiza automáticamente. También provee monitoreo en tiempo real del tráfico del segmento de red, detección de tráfico considerado como un patrón de ataque y las respectivas alertas configuradas por el usuario.

Esta herramienta refuerza las políticas de acceso a Internet por medio del bloqueo de direcciones URL clasificándolas por categorías (sitios para adultos, de entretenimiento, etc.). Con esto se restringe el acceso a sitios no productivos optimizando el uso del ancho de banda así como la productividad de los usuarios de la empresa.

3.4.2.1. Características del eTrust Intrusion Detection

Esta herramienta ofrece las siguientes características:

- **Control de Acceso a la Red –** eTrust Intrusion Detection utiliza una base de reglas para definir a los usuarios que pueden acceder a determinado recurso en la red, asegurando solo acceso autorizado a recursos de la red.
- **Motor de Antivirus Avanzado –** una máquina scanner de virus detecta el tráfico en la red que contenga virus de computadoras. De esta manera se protege al usuario de la descarga inconsciente de archivos infectados con virus. Las actualizaciones de virus se encuentran disponibles en el sitio Web del fabricante.
- **Base de Datos con Patrones de Ataques –** eTrust Intrusion Detection de manera automática detecta patrones de ataques en el tráfico de la red incluso mientras el ataque está en marcha. Existe una base de ataques que se actualiza regularmente y que se encuentra disponible en el sitio Web del fabricante.

- **Tecnología de Olfateo de Paquetes –** eTrust trabaja u opera en modo "disimulado", manteniéndose indetectable para los atacantes.
- **Bloqueo por URL –** Los administradores pueden designar las direcciones URL a las que los usuarios no pueden acceder previniendo la navegación no productiva.
- **Registro de la Utilización de la Red –** Esta herramienta permite al administrador de la red tener un registro de la actividad (logs) que los usuarios le han dado a la red; este registro puede ser por aplicaciones, por usuarios, etc. Esto ayuda a mejorar la planeación de las políticas de la red.

3.5. Plan de Pruebas Realizado

Como mencionamos en el desarrollo de este capítulo, hemos enfocado nuestro estudio utilizando la herramienta CISCO SECURE SCANNER; esta herramienta la podemos categorizar dentro del gripo de herramientas de descubrimiento. Básicamente es un scanner de puertos TCP/UDP activos en hosts de bastión.

También utilizamos la herramienta eTrust Intrusion Detection que es un sniffer de paquetes y cuya función principal es monitorear segmentos de red (básicamente el segmento de la red interna del firewall) para detectar el tipo de tráfico que circula por el mismo y patrones de tráfico que representen posibles ataques.

Estas pruebas fueron realizadas en tres fases:

- La primera fase se realizó desde el la red de la FIEC, instalando la herramienta en un computador y conectándola a un punto de la red.
- La segunda fase se realizó desde la red pública, es decir, desde Internet, contamos con la colaboración de la compañía MAINT para esta prueba ya que desde sus instalaciones realizamos el scanning hacia la FIEC.
- La tercera fase corresponde a monitoreo del segmento de red interno del firewall de la FIEC con el software de detección de intrusos y verificar que detecte el momento en el que se realizan las pruebas de scanning remoto.

3.5.1. Objetivos de las pruebas de verificación de vulnerabilidades local y remoto

El objetivo principal de las pruebas de scanning es detectar de manera general algún tipo de vulnerabilidad en los hosts de la red; esta "posibilidad" se puede ver reflejada al encontrar algún puerto TCP o UDP abierto en los hosts escaneados como resultado de algún tipo de vulnerabilidad en el protocolo o en la plataforma de sistema operativo.

Recordemos que el primer paso para un ataque es el reconocimiento de una vulnerabilidad que pueda ser aprovechada por el algún sistema para poder ser víctima de un ataque.

Al realizar la primera fase de scanning de manera local (desde la FIEC misma) estamos simulando la posibilidad de que el atacante sea un usuario de la red o "alguien" que se encuentra físicamente en las instalaciones de la FIEC.
La segunda fase, la de scanning remoto, simula la posibilidad de que el ataque de reconocimiento sea realizado por alguien en la red pública (desde Internet). Con esto podemos averiguar la deficiencia en la configuración de las reglas del firewall y la necesidad de implementar mecanismos adicionales de seguridad.

En el gráfico 3-4 y 3-5 se aprecia la ubicación del equipo con la herramienta Cisco Secure Scanner para las pruebas de scanning local y remoto.

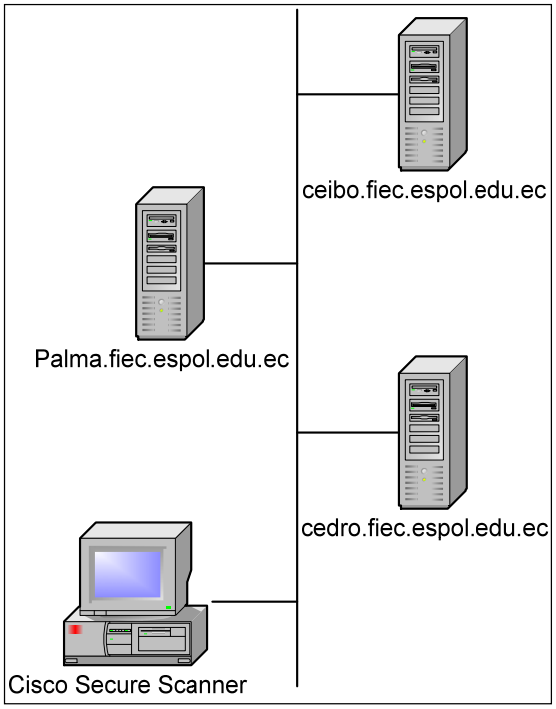


Figura No. 3 – 4. Esquema de Pruebas de Scanning Local

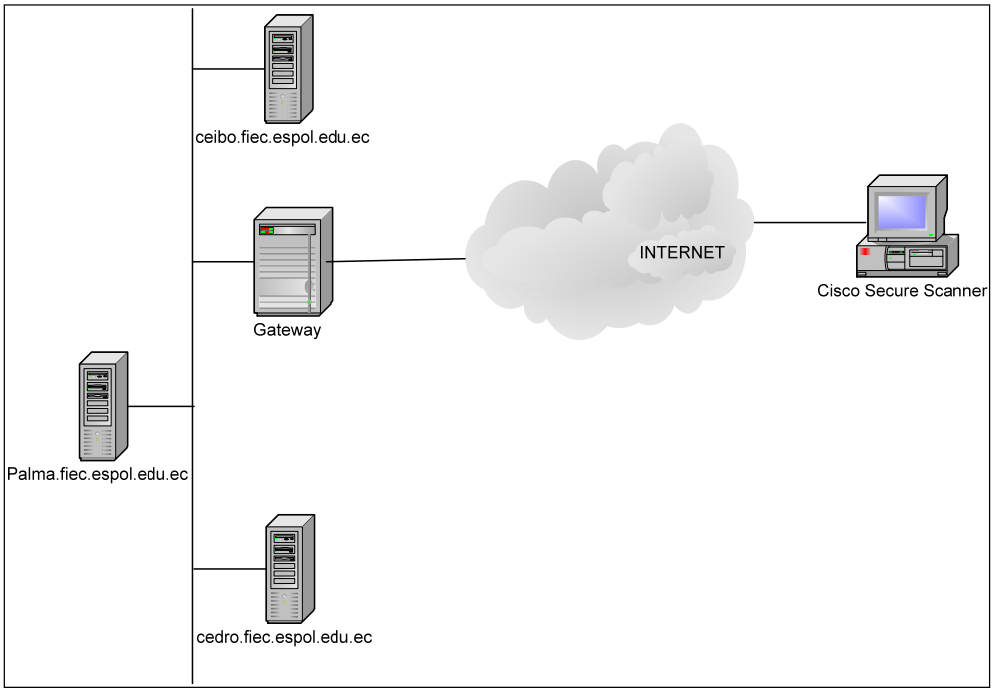


Figura No. 3 – 5. Esquema de Pruebas de Scanning Remoto

3.5.2. Objetivos de las pruebas de detección de intrusiones

Con la ayuda de la herramienta eTrust Intrusion Detection monitorearemos el tráfico que indique un posible ataque.

Durante las pruebas de scanning remoto, la herramienta de detección de intrusiones debe identificar el scanning como un patrón de tráfico de ataque; con esto simularemos un ataque real que puede ser ejecutado por cualquier pirata informático.

Para la prueba de detección de intrusiones, el esquema a seguir es como indica el gráfico 3-6:

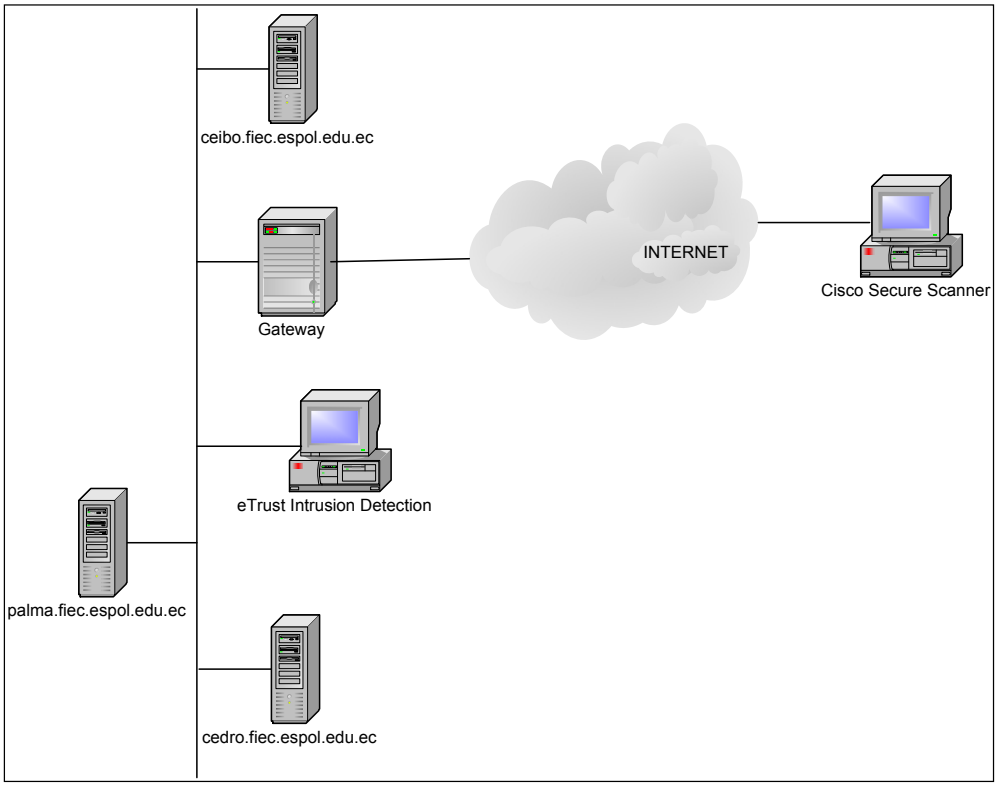


Figura No. 3 – 6. Esquema de Pruebas de Scanning Remoto y de Detección de Intrusiones

Bajo este esquema, las pruebas son realizadas desde el exterior de la red de la FIEC, en este caso, directamente desde Internet y con el IDS monitoreando el tráfico que genera el scanner de puertos. Como mencionamos anteriormente, el objetivo es solo monitorear un patrón de tráfico que sea identificado como un ataque, basado en esto se definirán las acciones a tomar cuando se detecte cualquier tipo de ataque.

3.5.3. Estrategia del plan de pruebas

- En la fase de prueba de scanning local, se elegirá un día normal de actividades en la red para tener un ambiente real en el caso de que un verdadero ataque se esté realizando.
- En la fase de pruebas de scanning remoto, se ha elegido un día no laborable para no afectar el rendimiento del ancho de banda del enlace a Internet.
- Para no afectar el rendimiento general de la red LAN de la FIEC y del enlace de acceso a Internet, todas las pruebas se realizarán específicamente a los tres servidores principales de la FIEC: CEIBO, PALMA y CEDRO. Estos servidores están publicados en Internet por lo que las pruebas remotas son válidas.
- No es conveniente realizar un scanning a todo el rango de direcciones IP de la FIEC ya que este proceso toma mucho tiempo e implica una posible degradación en el rendimiento de la red. A un atacante real no le importará si el host o la red que es objeto de su ataque se degrada en su rendimiento, mas bien lo contrario, puede ocasionar una negación de servicio al host y quedar fuera de servicio para los usuarios válidos por un tiempo indefinido.

3.5.4. Observaciones al plan de pruebas

- Un factor a favor en las pruebas que se realizaron, es la infraestructura de los equipos de conectividad de la red; como se analizó previamente, los equipos son concentradores (hubs) conectados en configuración cascada.
- Un hub en una red es un dominio de colisión, es decir, el ancho de banda con que trabaja ese hub (10 o 100 Mbps, dependiendo si la tecnología es ethernet o fast ethernet) es compartido por todos los dispositivos conectados a los puertos RJ-54 del mismo. El tráfico que genera un dispositivo conectado en uno de los puertos es escuchado por todos los demás (difusión o broadcast), por lo tanto va a existir más de un host que quiera transmitir al mismo tiempo, cuando esto sucede se produce una colisión de paquetes en el segmento.
- Una colisión obliga al host, esperar un tiempo adicional hasta volver a transmitir, esperando que el medio esté disponible, mientras más hosts estén conectados al hub, mayor es la probabilidad de colisiones, por lo que la comunicación puede degradarse.
- Esta breve explicación sobre los dominios de colisión y el broadcast en la red sirve como premisa para explicar el funcionamiento del IDS. El detector de intrusiones es básicamente un sniffer, monitorea el tráfico del segmento de red en el que se encuentre conectado.
- Para el caso de la red de la FIEC, no importa en cual de los hubs esté el IDS, al ser toda la infraestructura un solo dominio de colisión y un solo dominio de broadcast, escuchará todo el tráfico de la red y procesará la información que origina o que reciba cualquier host de la FIEC.

- Cabe destacar que el IDS no influye de ninguna manera al rendimiento de la red, es un equipo pasivo que es totalmente transparente para los usuarios y servidores de la red.

3.6. Proceso de Ejecución de las pruebas en la FIEC

Para ejecutar las pruebas, se instaló las herramientas Cisco Secure Scanner y eTrust Intrusion Detection en computadoras de última generación.

Para las pruebas se eligió horas donde el tráfico en la red sea bajo (horas no laborables) de tal manera de no perjudicar o entorpecer el trabajo diario en la red de la FIEC.

Fueron dos días de sesiones en que las herramientas realizaron la labor de descubrir la existencia de fallas en la plataforma de servidores y de ser así, cuáles son las recomendaciones para corregir estos problemas.

En los anexos de este documento está gráficamente el proceso de scanning local y remoto.

CAPITULO IV

RESULTADOS DE LAS PRUEBAS REALIZADAS EN LA FIEC

4.1. Introducción

En este capítulo revisaremos los resultados obtenidos en las pruebas de detección de vulnerabilidades local y remoto así como los registros del IDS contra los servidores ceibo, palma y cedro de la FIEC.

Con la exposición de tablas y gráficos se apreciará las vulnerabilidades potenciales y confirmadas que se han encontrado en estos hosts así como la explicación del origen o razón de las deficiencias encontradas y las sugerencias para reforzar la seguridad. También se revisará las posibles deficiencias en la configuración de los equipos de frontera de la red.

La información obtenida como resultado de estas pruebas es considerada altamente confidencial, por lo que solamente emitiremos resultados generales y las sugerencias o medidas necesarias para resolver los problemas detectados.

El realizar este tipo de pruebas es una de las tareas que todo administrador debería realizar durante una eficiente labor de gestión de seguridad en la red de la corporación por lo que, en el desarrollo de este proyecto son puestas como un ejemplo del resultado que se obtendría si se realizan estas pruebas en cualquier red de cualquier corporación.

Recalcamos que en ningún momento los resultados encontrados han sido revelados a personas ajenas a este proyecto, o peor aun, utilizados en contra de los intereses de la Facultad de Ingeniería en Electricidad Computación de la Escuela Superior Politécnica del Litoral.

4.2. Configuración de la herramienta Cisco Secure Scanner para ejecutar las pruebas de verificación de vulnerabilidades local y remota

Durante el mes de febrero, se realizó desde la red de la FIEC un scanning a los servidores ceibo, palma y cedro. La herramienta Cisco Secure Scanner fue instalada en un computador con características de última generación y conectada a un punto de la red. La herramienta ejecuta una prueba por ICMP realizando un barrido de direcciones IP con el comando PING.

Claro está que el PING ejecutado no es el paquete normal de 32 bits, sino más bien, un paquete modificado en sus diferentes parámetros como el tipo de trama, tiempos de respuesta, etc.

A continuación presentamos gráficos más explícitos que indican las diferentes opciones de configuración y los parámetros fijados especialmente para estas pruebas:

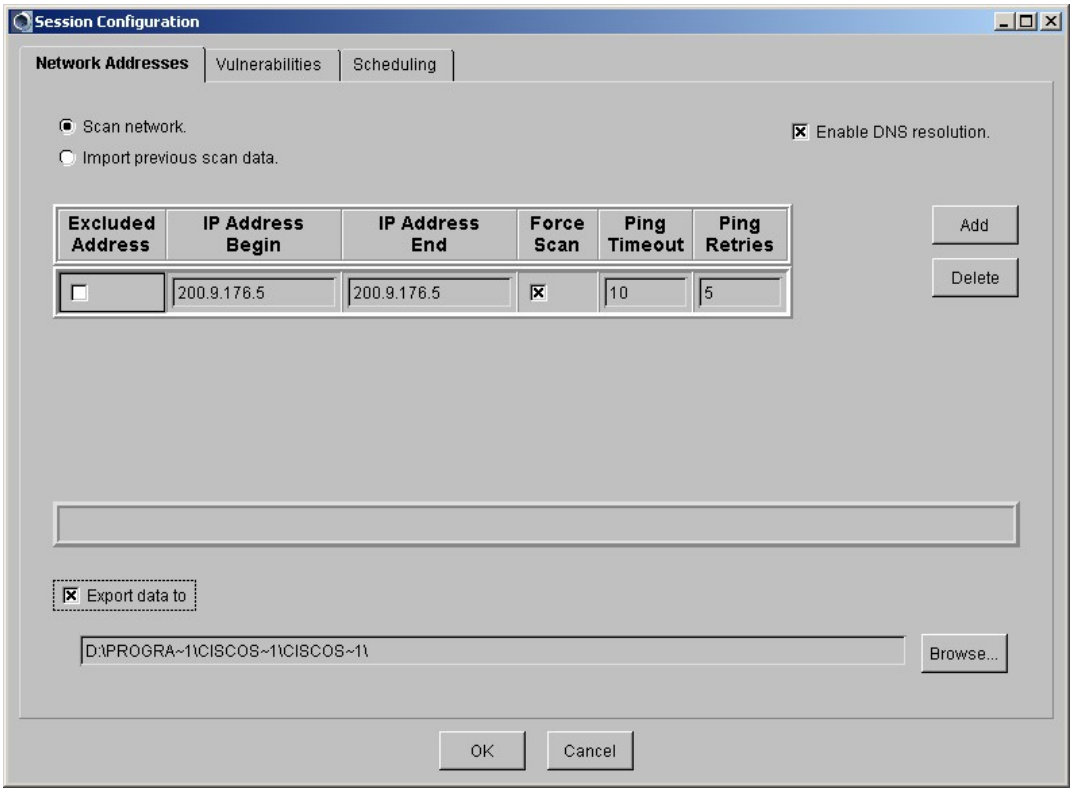


Figura No. 4-1. Configuración del Cisco Secure Scanner para pruebas con servidor CEIBO

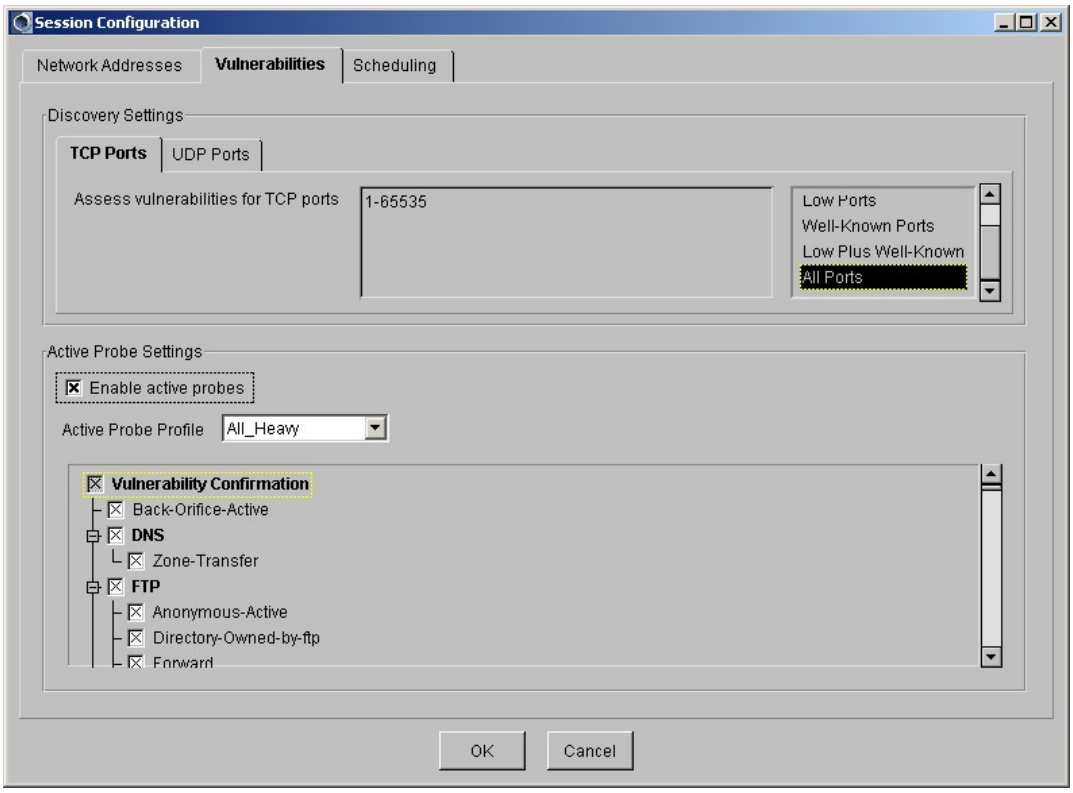


Figura No. 4-2. Configuración del Cisco secure scanner para pruebas con servidor CEIBO (2)

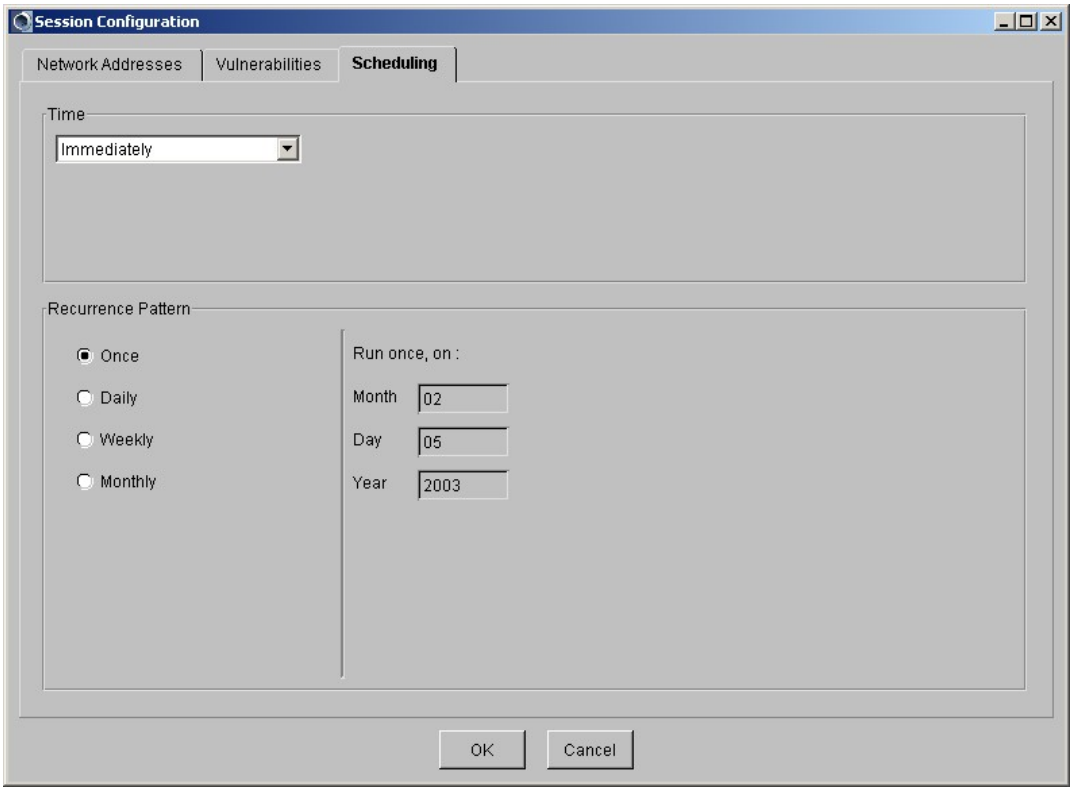


Figura No. 4-3. Configuración del Cisco secure scanner para pruebas con servidor CEIBO (3)

En nuestras pruebas se ejecutó el scanning de un host a la vez con el objetivo de no interferir en el rendimiento de la red. En la figura 4.1 se indica a la herramienta la dirección IP del host que va a ser objeto del análisis así como el directorio en el que se guardará la información obtenida.

La figura 4.2 muestra la configuración de puertos TCP/UDP en el que será detectado algún tipo de servicio activo en el host.

Finalmente en la figura 4.3 se detalla el instante en que el scanning debe ser realizado; esta herramienta brinda la oportunidad de programar el horario y la fecha en la que el administrador de la red desee realizar el scan de algún host en particular o de un grupo de hosts.

Para los servidores CEDRO y PALMA, la configuración fue exactamente la misma, tanto para las pruebas locales y remotas.

4.3. Configuración de la herramienta eTrust Intrusion Detection

La herramienta de detección de intrusiones eTrust Intrusion Detection fue instalado en un segundo computador de última generación, conectado a un punto de red de la FIEC.

El principio de funcionamiento de esta herramienta es la de "olfatear" el tráfico del segmento de red, analizar los paquetes desde la capa física hasta la capa de aplicación del modelo OSI con el objetivo de identificar las direcciones origen y destino, los puertos TCP o UDP que han sido utilizados en los paquetes y el tipo de sesión que se ha establecido. Todo esto queda registrado en una base local en el que se establece la fecha y hora para cada evento registrado.

La herramienta trae previamente configurado reglas para el monitoreo del segmento de red donde está instalado el IDS, dentro de las reglas existen dos conjuntos que son de importancia para las pruebas que se realizarán: Las

Reglas de Detección de Intentos de Intrusión y las **Reglas de Detección de Actividad Sospechosa en la Red.**

Este tipo de reglas me permitirán detectar si existen intentos de ataques en el segmento, y de haberlo, hacia qué dirección IP se realiza y cuál es la dirección IP del host que está realizando la sesión de ataque. La base de ataques que tiene el IDS es muy extensa y es actualizable cada determinado tiempo, por lo que resulta muy complicado explicar cada uno de ellos.

En los siguientes gráficos se muestra las pantallas con la configuración de las reglas que se han definido para estas pruebas.

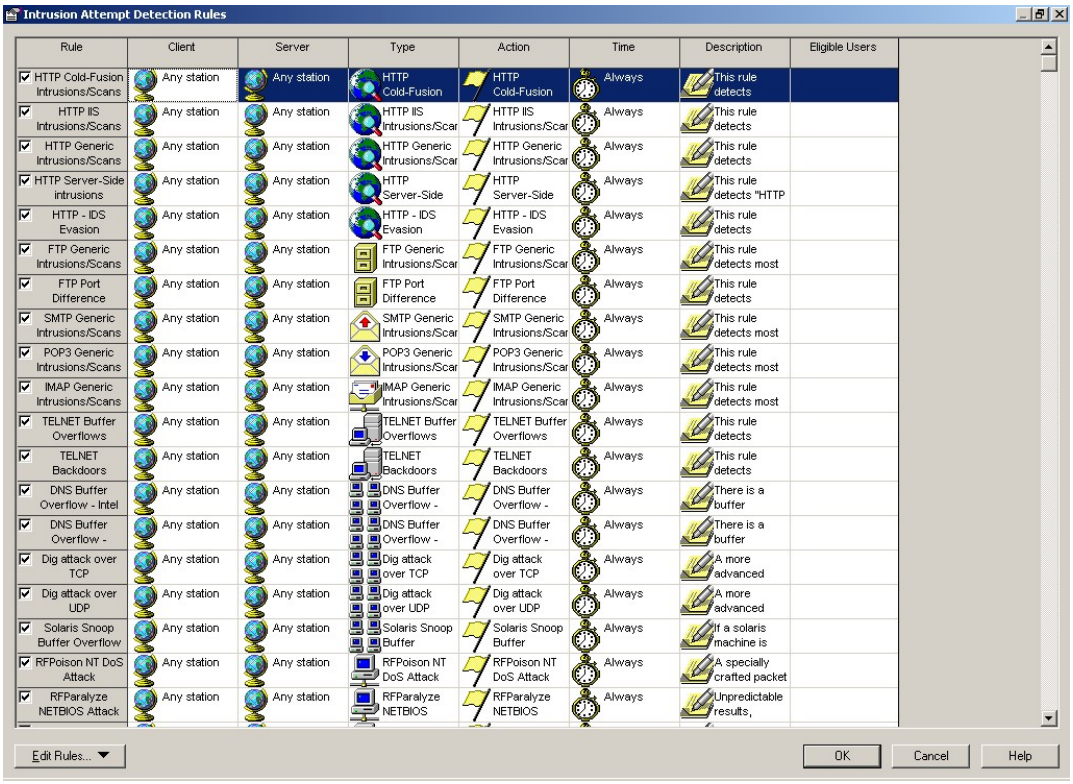


Gráfico No. 4-4. Reglas de Detección de Intentos de Intrusión

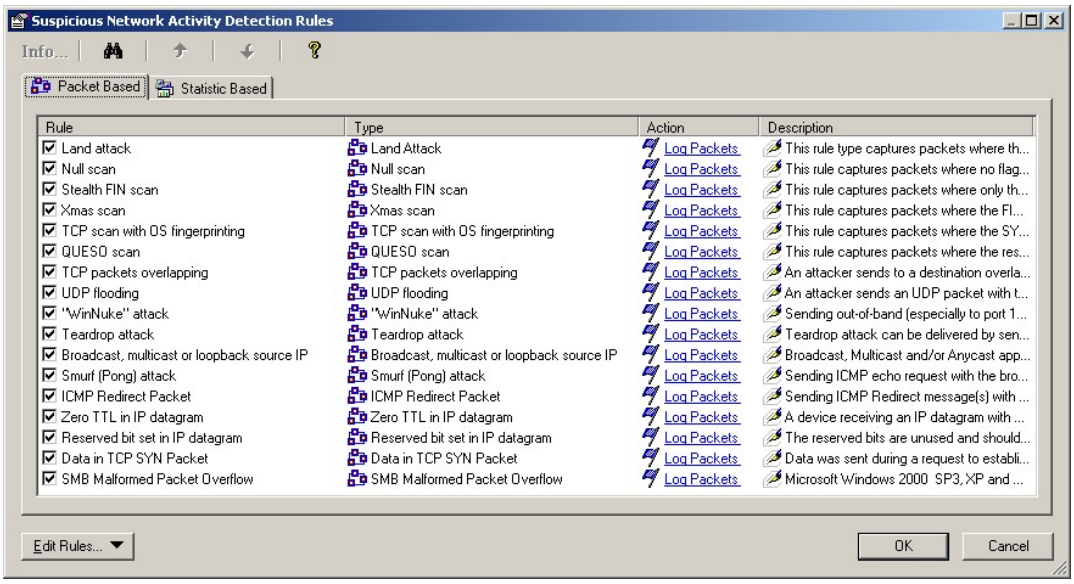


Gráfico No. 4-5. Reglas de Detección de Actividad Sospechosa en la Red

4.4. Resultados de las pruebas locales con la herramienta Cisco Secure Scanner

En esta prueba, los siguientes puertos (TCP/UDP) fueron encontrados activos en los tres hosts de la red:

Dirección IP	Plataforma de Sistema Operativo	Puertos que Respondieron	Tipo de Protocolo
200.9.176.3	OS:workstation:unix:samba-server:2:2:5	22	TCP
		23	TCP
		25	TCP
		80	TCP
		109	TCP
		110	TCP
		111	TCP
		139	TCP
		143	TCP
		443	TCP
		111	UDP
200.9.176.5	OS:workstation:unix:samba-server:2:2:3a	22	TCP
		23	TCP
		25	TCP
		53	TCP
		79	TCP
		80	TCP
		109	TCP
		110	TCP
		111	TCP
		113	TCP
		139	TCP

		143	TCP
		443	TCP
		53	UDP
		111	UDP
		2049	UDP
200.9.176.7	OS:workstation:unix:samba-server:2:2:3a	21	TCP
		22	TCP
		23	TCP
		25	TCP
		79	TCP
		80	TCP
		110	TCP
		111	TCP
		139	TCP
		443	TCP
		10000	TCP
		111	UDP
		2049	UDP

Tabla XI. Puertos TCP/UDP encontrados activos en los hosts de prueba

A continuación se muestran los servicios que cada host tiene levantado en el sistema y que fueron identificados por la herramienta Cisco secure scanner:

Servicio	Dirección IP
Authentication:auth	200.9.176.5
Authentication:nt-domain-controller	200.9.176.5
	200.9.176.7
Data-Transfer:ftp	200.9.176.7
File-Sharing:rpc-mountd	200.9.176.5
	200.9.176.7
File-Sharing:rpc-nfs	200.9.176.5
	200.9.176.7
File-Sharing:rpc-nlockmgr	200.9.176.5
	200.9.176.7
File-Sharing:samba:2:2:3ª	200.9.176.5
	200.9.176.7
File-Sharing:samba:2:2:5	200.9.176.3
File-Sharing:windows-server-service	200.9.176.3
	200.9.176.5
	200.9.176.7
File-Sharing:windows-workstation-service	200.9.176.3
	200.9.176.5
	200.9.176.7
Info-Status:finger	200.9.176.5
	200.9.176.7
Info-Status:ms-browser-service-election	200.9.176.3
	200.9.176.5

	200.9.176.7
Info-Status:ms-domain-master-browser	200.9.176.5
	200.9.176.7
Info-Status:ms-domain-name	200.9.176.3
	200.9.176.5
	200.9.176.7
Info-Status:ms-master-browser	200.9.176.5
	200.9.176.7
Info-Status:rpc-portmapper	200.9.176.3
	200.9.176.5
	200.9.176.7
Info-Status:rpc-rquotad	200.9.176.5
	200.9.176.7
Info-Status:rpc-rstatd	200.9.176.3
	200.9.176.5
	200.9.176.7
Mail:imap	200.9.176.3
	200.9.176.5
Mail:ms-messenger-service	200.9.176.3
	200.9.176.5
	200.9.176.7
Mail:pop	200.9.176.3
	200.9.176.5
	200.9.176.7

Mail:smtp	200.9.176.3
	200.9.176.5
	200.9.176.7
Net-Management:dns	200.9.176.5
NetBIOS:netbios-ss	200.9.176.3
	200.9.176.5
	200.9.176.7
Remote-Access:ssh	200.9.176.3
	200.9.176.5
	200.9.176.7
Remote-Access:telnet	200.9.176.3
	200.9.176.5
	200.9.176.7
Web:http	200.9.176.3
	200.9.176.5
	200.9.176.7
Web:http-ssl	200.9.176.3
	200.9.176.5
	200.9.176.7

Tabla XII. Servicios detectados en cada host

La tabla XIII muestra un resumen del estatus de la prueba, indicando de manera general toda la información al respecto:

CATEGORÍA	DESCRIPCIÓN
Fecha y Hora	Feb 05 12:10:04 GMT-05:00 2003
Duración del Scanning	16 min 32 sec
Direcciones IP	200.9.176.5 200.9.176.7 200.9.176.3
Número de Hosts Vivos	3
Número de Vulnerabilidades	19
Número de Vulnerabilidades de Alta Severidad	3
Número de Vulnerabilidades de Mediana Severidad	0
Número de Vulnerabilidades de Baja Severidad	16
Número de Vulnerabilidades Potenciales	13
Número de Vulnerabilidades Confirmadas	6

Tabla XIII. Resumen general de las pruebas de scanning local

Los siguientes valores numéricos representan el valor dado para cada nivel de vulnerabilidad:

VALOR	NIVEL DE VULNERABILIDAD
3	Alto
2	Medio
1	Bajo

Basado en los valores asignados, la siguiente tabla muestra las diferentes vulnerabilidades encontradas en los hosts clasificadas por vulnerabilidades potenciales y confirmadas:

Dirección IP	Vulnerabilidad	Estatus
200.9.176.3	Access:SSH.RSAREF-Overflow:Vp:10060	Potencial
	Recon:RPC.portmapper-Active:Vp:1121	Potencial
	Recon:RPC.rstatd-Active:Vp:1124	Potencial
200.9.176.5	Access:SSH.RSAREF-Overflow:Vp:10060	Potencial
	Recon:Finger.Active:Vp:101	Potencial
	Recon:RPC.portmapper-Active:Vp:1121	Potencial
	Recon:RPC.rquotad-Active:Vp:1109	Potencial
	Recon:RPC.rstatd-Active:Vp:1124	Potencial
	Recon:Finger.Global:Vc:103	Confirmado
	Recon:Finger.walk-digit:Vc:104	Confirmado
	Recon:Finger.walk-multiple-digits:Vc:104	Confirmado
	Recon:NFS.Dump:Vc:811	Confirmado
200.9.176.7	Access:SSH.RSAREF-Overflow:Vp:10060	Potencial
	Recon:Finger.Active:Vp:101	Potencial

	Recon:RPC.portmapper-Active:Vp:1121	Potencial
	Recon:RPC.rquotad-Active:Vp:1109	Potencial
	Recon:RPC.rstatd-Active:Vp:1124	Potencial
	Recon:Finger.Global:Vc:103	Confirmado
	Recon:NFS.Dump:Vc:811	Confirmado

Tabla XIV. Vulnerabilidades encontradas en cada host

Finalmente, mostramos la clasificación por nivel de severidad de cada una de las vulnerabilidades encontradas en los hosts de prueba. Cabe aclarar que según la tabla anterior, un mismo tipo de vulnerabilidad es encontrado en más de un host:

Valor Numérico	Nivel de Severidad	Vulnerabilidad
1	Bajo	Recon:RPC.rstatd-Active:Vp:1124
1	Bajo	Recon:RPC.rquotad-Active:Vp:1109
1	Bajo	Recon:RPC.portmapper-Active:Vp:1121
1	Bajo	Recon:NFS.Dump:Vc:811
1	Bajo	Recon:Finger.walk-multiple-digits:Vc:104
1	Bajo	Recon:Finger.walk-digit:Vc:104
1	Bajo	Recon:Finger.Global:Vc:103
1	Bajo	Recon:Finger.Active:Vp:101
3	Alto	Access:SSH.RSAREF-Overflow:Vp:10060

Tabla XV. Vulnerabilidades por nivel de severidad

Aclaramos que estos resultados son clasificados como información confidencial por lo que solo haremos referencia a la descripción de cada una de las debilidades encontradas en los anexos 2 y 3 que acompaña a este documento.

4.5. Resultados de las Pruebas Realizadas Remotamente.

La ejecución de las pruebas de scanning remoto se realizó desde una locación externa con el objetivo de simular un ataque real hacia la FIEC desde una locación en Internet.

La presentación de los resultados se la hará de la siguiente manera:

- Resultados con la herramienta eTrust Intrusion Detection
- Resultados con la herramienta Cisco Secure Scanner.

4.5.1. Resultados con la herramienta eTrust IDS

El tráfico generado por el Cisco secure scanner, fue registrado por el IDS como un intento de ataque hacia los hosts que son objeto del análisis, en los siguientes gráficos mostramos los registros del IDS que efectivamente comprueban lo explicado:

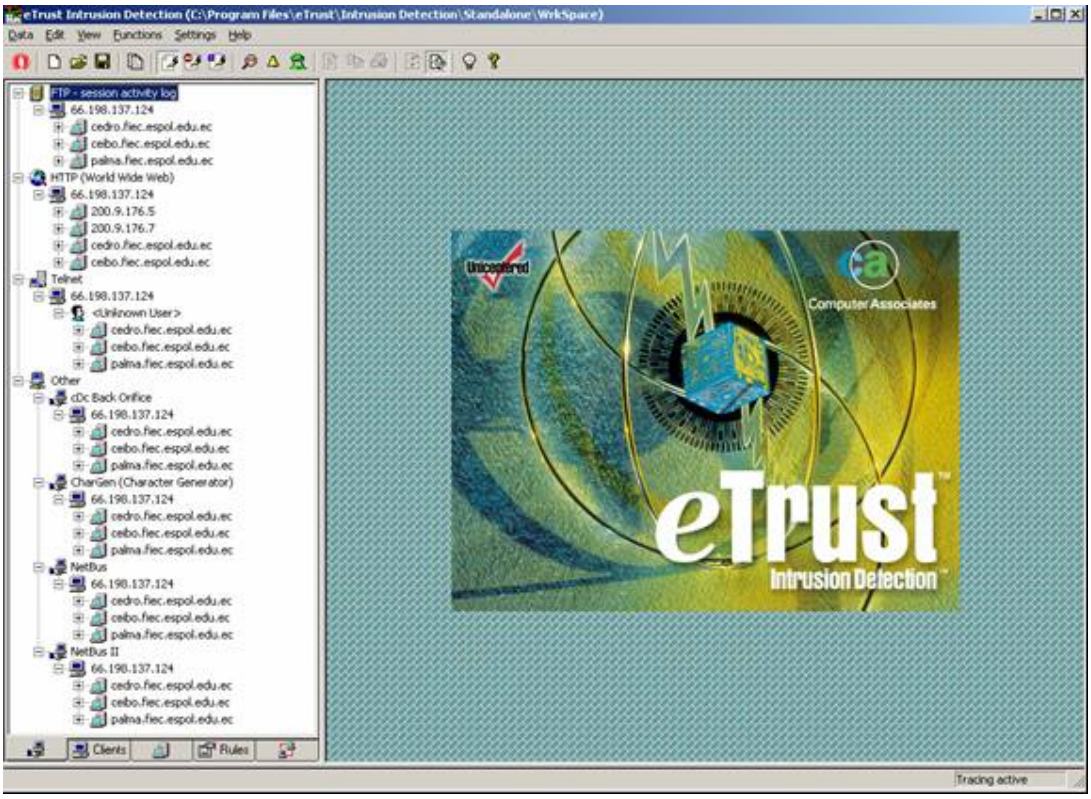


Gráfico No. 4-6. Vista general de la consola del eTrust IDS

Tal como se aprecia en la gráfica, el tráfico que genera el scanner al tratar de detectar algún tipo de vulnerabilidad en los host, es detectado por la herramienta eTrust IDS como posibles.

Claramente se aprecia que el scanner trata de iniciar sesiones por los puertos TCP que utilizan los protocolos FTP (puerto tcp:20), http (tcp:80), Telnet (tcp:23).

Dentro del parámetro others, se encuentra intentos del Cisco Secure Scanner por iniciar sesiones que la herramienta IDS claramente los identifica como ataques del tipo “Back Orifice”, y “NetBus”.

En las siguientes gráficas mostramos las diferentes sesiones que el scanner de puertos intentó realizar contra los servidores de la FIEC, así como loas alertas que se visualizó en la consola del IDS indicando tráfico sospechoso, esto para comprobar la eficacia de la herramienta IDS:

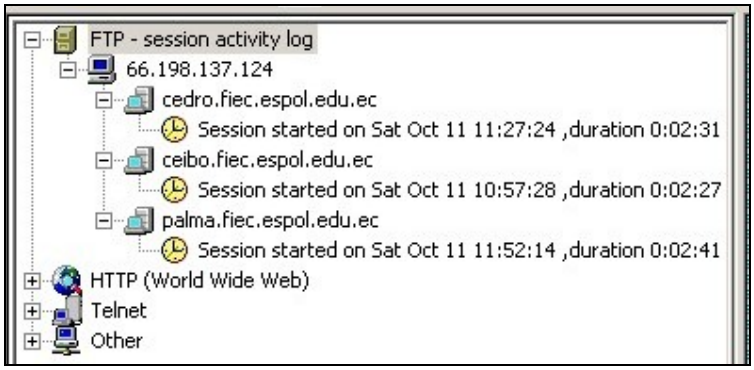


Gráfico No. 4-7. Sesiones de intrusión por FTP

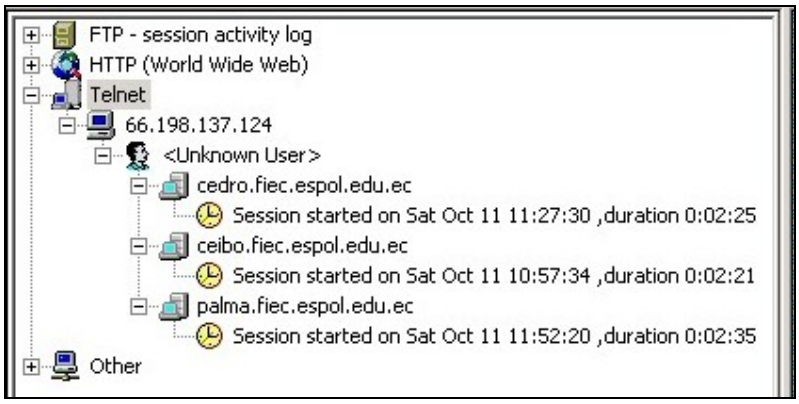


Gráfico No. 4-8. Sesiones de intrusión por TELNET

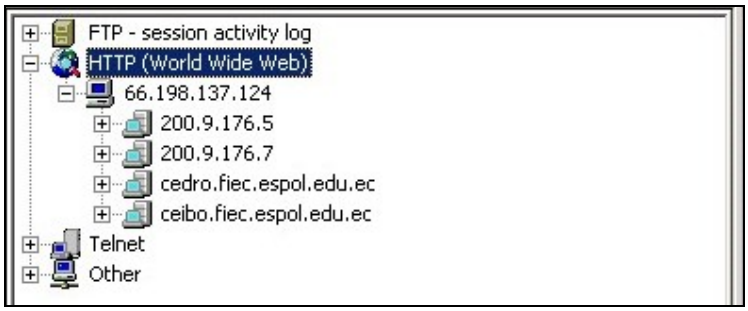


Gráfico No. 4-9. Sesiones de intrusión por http

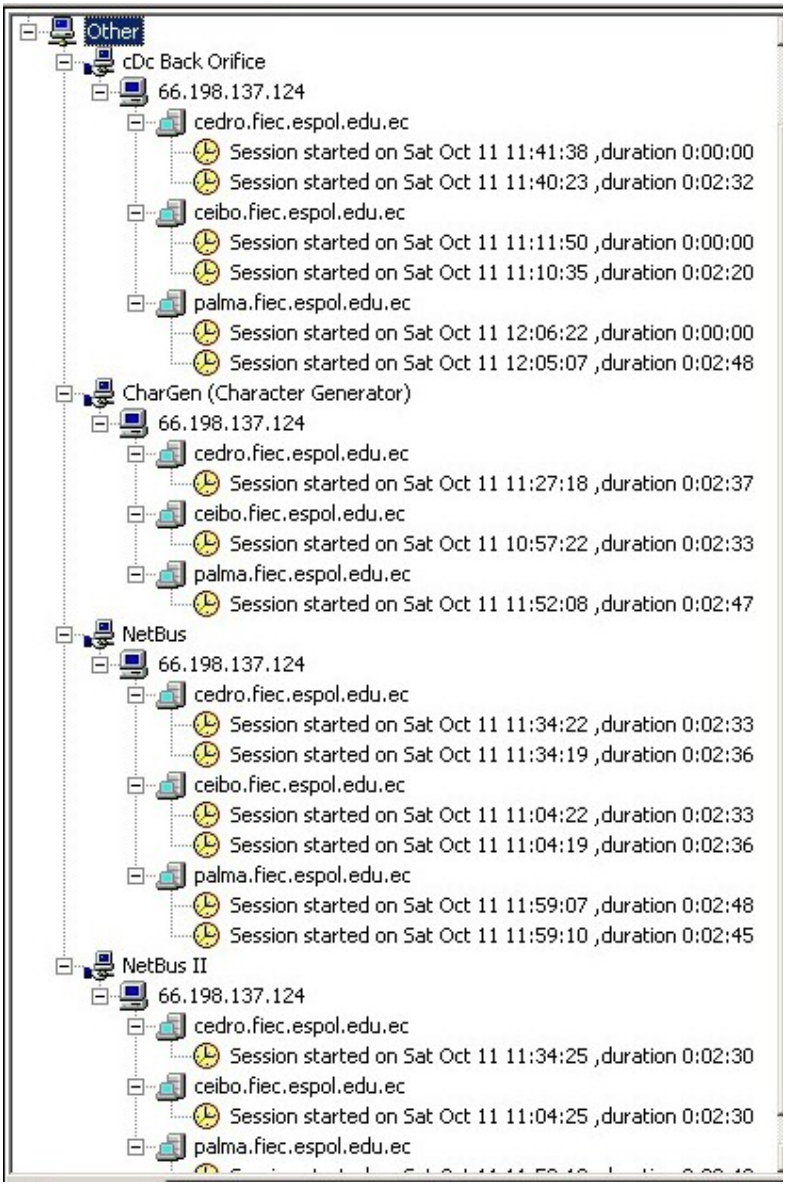


Gráfico No. 4-10. Sesiones de intrusión por diferentes tipos de ataques

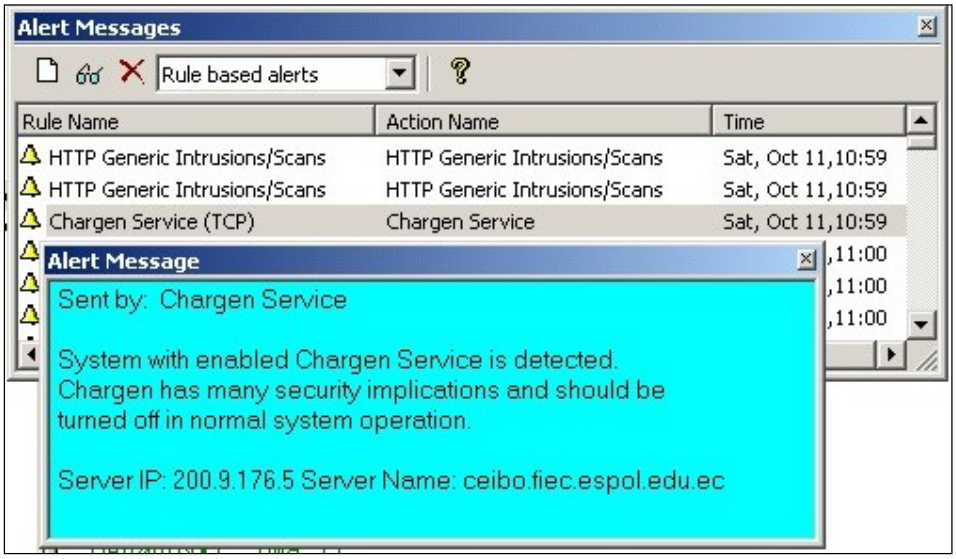


Gráfico No. 4-11. Alertas en la consola del IDS por actividad sospechosa en el segmento de red

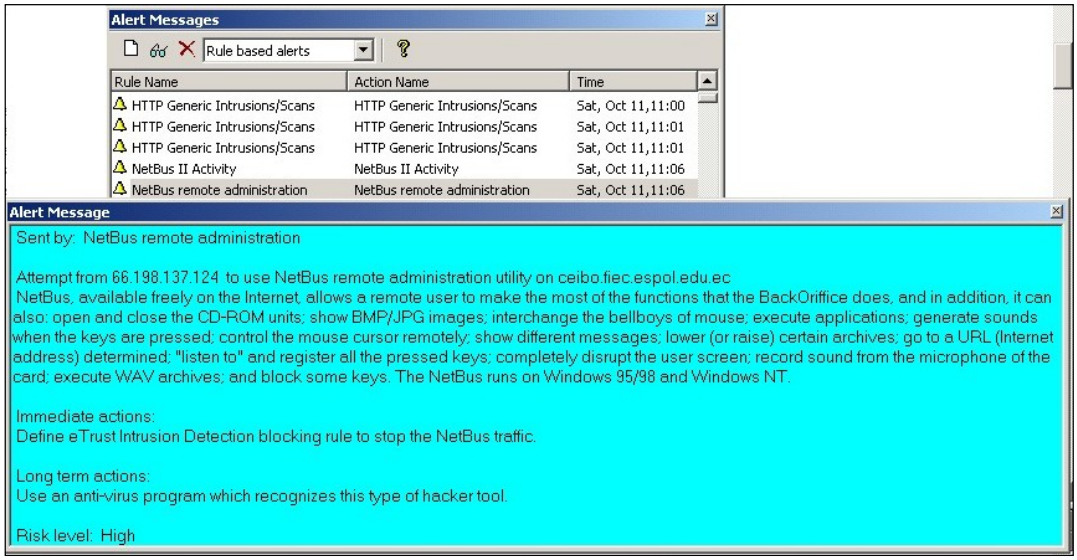


Gráfico No. 4-12. Alertas en la consola del IDS por actividad sospechosa en el segmento de red

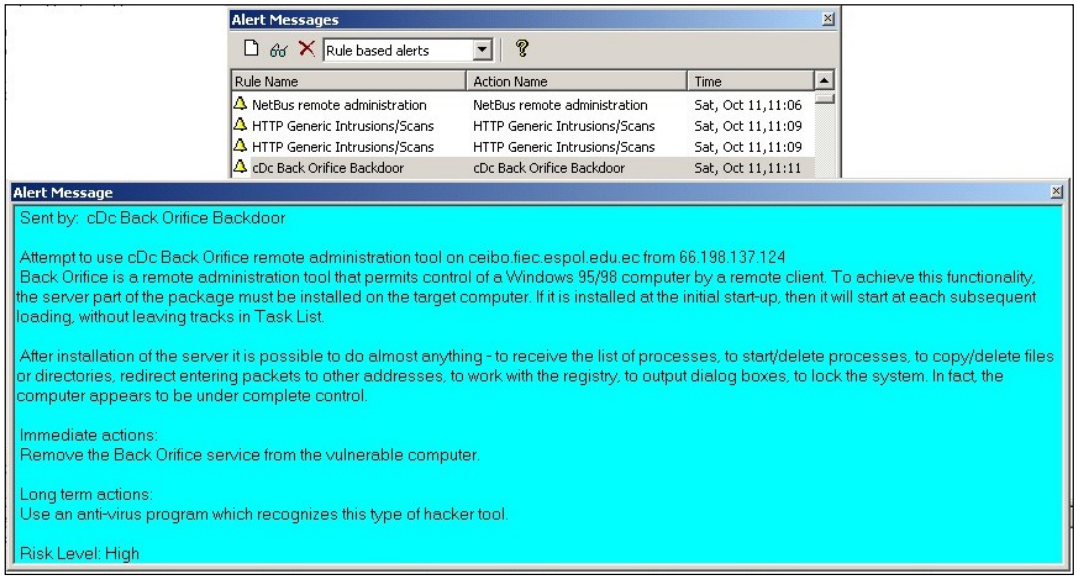


Gráfico No. 4-13. Alertas en la consola del IDS por actividad sospechosa en el segmento de red

Todos los registros y alarmas obtenidas con la herramienta denotan la efectividad de la herramienta eTrusts Intrusion Detection; sin embargo, el punto al que queremos llegar es que este tipo de herramientas son altamente útiles para los administradores de la red.

Por motivo de pruebas, solo se configuró la herramienta para que notifique con alarmas los intentos de intrusiones, sin embargo existe la posibilidad de bloquear este tipo de tráfico en el segmento.

4.5.2. Resultados con la herramienta Cisco Secure Scanner

En esta prueba, los siguientes puertos (TCP/UDP) fueron encontrados activos en los tres hosts de la red:

Dirección IP	Plataforma de Sistema Operativo	Puertos que Respondieron	Tipo de Protocolo
200.9.176.3	OS:unknown	443	TCP
		53	UDP
200.9.176.5	OS:unknown	25	TCP
		80	TCP
		110	TCP
		53	UDP
200.9.176.7	OS:unknown	80	TCP
		53	UDP

Tabla XVI. Puertos TCP/UDP encontrados activos en los hosts de prueba

A continuación se muestran los servicios que cada host tiene levantado en el sistema y que fueron identificados por la herramienta Cisco secure scanner:

Servicio	Dirección IP
Data-Transfer:cu-seeme	200.9.176.3
	200.9.176.5
	200.9.176.7
Data-Transfer:talk	200.9.176.3
	200.9.176.5
	200.9.176.7
Data-Transfer:tftp	200.9.176.3
	200.9.176.5
	200.9.176.7
File-Sharing:rpc-nfs	200.9.176.3
	200.9.176.5
	200.9.176.7
Info-Status:biff	200.9.176.3
	200.9.176.5
	200.9.176.7
Info-Status:name	200.9.176.3
	200.9.176.5
	200.9.176.7
Info-Status:rpc-portmapper	200.9.176.3
	200.9.176.5
	200.9.176.7
Info-Status:rwho	200.9.176.3
	200.9.176.5

	200.9.176.7
Info-Status:snmp-agent	200.9.176.3
	200.9.176.5
	200.9.176.7
Info-Status:syslog	200.9.176.3
	200.9.176.5
	200.9.176.7
Mail:pop	200.9.176.5
Mail:smtp	200.9.176.5
Net-Management:dhcp	200.9.176.3
	200.9.176.5
	200.9.176.7
Net-Management:dns	200.9.176.3
	200.9.176.5
	200.9.176.7
Other:appletalk	200.9.176.3
	200.9.176.5
	200.9.176.7
Remote-Access:pc-anywhere	200.9.176.3
	200.9.176.5
	200.9.176.7
Web:http	200.9.176.5
	200.9.176.7
Web:http-ssl	200.9.176.3

Tabla XVII. Servicios detectados en cada host

La tabla XVIII muestra un resumen del estatus de la prueba, indicando de manera general toda la información al respecto:

CATEGORÍA	DESCRIPCIÓN
Fecha y Hora	Oct 05 12:10:04 GMT-05:00 2003
Duración del Scanning	59 min 41 sec
Direcciones IP	200.9.176.5 200.9.176.7 200.9.176.3
Número de Hosts Vivos	3
Número de Vulnerabilidades	6
Número de Vulnerabilidades de Alta Severidad	0
Número de Vulnerabilidades de Mediana Severidad	0
Número de Vulnerabilidades de Baja Severidad	6
Número de Vulnerabilidades Potenciales	6
Número de Vulnerabilidades Confirmadas	0

Tabla XVIII. Resumen general de las pruebas de scanning remoto

Los siguientes valores numéricos representan el valor dado para cada nivel de vulnerabilidad:

VALOR	NIVEL DE VULNERABILIDAD
3	Alto
2	Medio
1	Bajo

Basado en los valores asignados, la siguiente tabla muestra las diferentes vulnerabilidades encontradas en los hosts clasificadas por vulnerabilidades potenciales y confirmadas:

Dirección IP	Vulnerabilidad	Estatus
200.9.176.3	Recon:RPC.portmapper-Active:Vp:1121	Potential
	Recon:Rwho.Active:Vp:1004	Potential
200.9.176.5	1:Recon:RPC.portmapper-Active:Vp:1121	Potential
	1:Recon:Rwho.Active:Vp:1004	Potential
200.9.176.7	1:Recon:RPC.portmapper-Active:Vp:1121	Potential
	1:Recon:Rwho.Active:Vp:1004	Potential

Tabla XIX. Vulnerabilidades encontradas en cada host

Finalmente, mostramos la clasificación por nivel de severidad de cada una de las vulnerabilidades encontradas en los hosts de prueba. Cabe aclarar que según la tabla anterior, un mismo tipo de vulnerabilidad es encontrado en más de un host:

Valor Numérico	Nivel de Severidad	Vulnerabilidad
1	Bajo	Recon:RPC.portmapper-Active:Vp:1121
1	Bajo	Recon:Rwho.Active:Vp:1004

Tabla XX. Vulnerabilidades por nivel de severidad

4.6. Análisis de los resultados

Básicamente, los resultados de estas pruebas se pueden resumir en lo siguiente:

Las pruebas de scanning local indican la existencia de vulnerabilidades POTENCIALES, es decir, vulnerabilidades que han sido probadas por el CISCO SECURE SCANNER y que de las que se obtuvieron respuestas de parte de los host que han sido objeto de pruebas.

De las vulnerabilidades potenciales, solo una está considerada como crítica, esta es *Access:SSH.RSAREF-Overflow:Vp:10060* y está presente en los tres servidores monitoreados. Dentro de la base de conocimiento de CISCO en Internet, se explica que es un ataque de "sobrecarga del buffer" (ver capítulo 2 de este informe) y que es una deficiencia del protocolo SSH versión 1 y versión 2.

Como contramedida, se recomienda aplicar el parche para SSH disponible en la página Web de Red Hat Linux.

También existen vulnerabilidades CONFIRMADAS que son vulnerabilidades que han sido probadas por el CISCO SECURE SCANNER y que han dado respuesta de parte del host. Sin embargo las vulnerabilidades detectadas son de nivel bajo, es decir, el atacante no estaría en capacidad de obtener mayor control del host que es objetivo del ataque.

Dentro de las vulnerabilidades confirmadas tenemos NFS.Dump:Vc:811 que hace referencia al sistema de archivos NFS (Network File System) y compartir archivos y carpetas en un sistema de este tipo. El atacante podría obtener información respecto a los hosts que tienen permisos para acceder a un archivo o recurso en el servidor y así realizar otras técnicas de ataque más complejas contra éste.

Para este caso se recomienda, en servidores críticos como es el caso de ceibo, palma y cedro, deshabilitar el servicio NFS si no es necesario dentro de las labores diarias.

En las pruebas de scanning remoto tenemos solo dos vulnerabilidades POTENCIALES y clasificadas con un nivel bajo de severidad.

Lo interesante de estas pruebas es visualizar las alertas de la herramienta de detección de intrusiones (eTrust IDS), ya que detectó y envió alertas en la consola para que el administrador se pueda percatar de actividad sospechosa en la red.

En los anexos 2 y 3 que acompañan a este documento se puede apreciar con mayor detalle la explicación de cada una de las vulnerabilidades encontradas, lo que podría causar cada una de ellas y la manera de cómo corregir las deficiencias encontradas.

CAPITULO V

DISEÑOS DE SEGURIDAD RECOMENDADOS A LA FIEC

5.1. Introducción.

En este capítulo daremos las indicaciones necesarias para mejorar la seguridad en la red de datos de la FIEC.

Estas sugerencias son basadas en el resultado de las pruebas de reconocimiento realizadas en le red así como en los criterios técnicos de diseño de redes seguras que se analizó en el capítulo uno de este documento.

5.2. Diseño de la topología de red recomendado para la FIEC.

Con el análisis de la topología de red de la FIEC podemos emitir los siguientes puntos para la mejora en la estructura de la red.

- Implementación de un equipo con funcionalidad exclusiva de firewall.
- Implementación de una zona desmilitarizada para servidores públicos.
- Implementación de NAT para optimizar el uso de direcciones públicas.
- Implementación de equipos o programas para el monitoreo de posibles ataques a la red interna desde Internet y desde la misma red de la FIEC.
- Distribución de carga para los servidores, es decir, no acumular todos los servicios en un solo equipo.
- Cambio en los equipos de conectividad final por otros de mejor rendimiento y con capacidad de administración remota por SNMP.
- Implementación de una herramienta de gestión de redes para el control y monitoreo de los equipos de conectividad y de los servidores críticos.
- Movilización del rack donde se encuentran los equipos de conectividad a un sitio más seguro y de acceso restringido junto con los servidores críticos.

Estos puntos resumen las mejoras sugeridas para incrementar el nivel de seguridad en la red de la FIEC.

A continuación hablaremos más a detalle de cada uno de los puntos expuestos.

5.2.1. Implementación de un equipo con funcionalidad exclusiva de firewall.

Es altamente recomendable reemplazar el actual dispositivo de seguridad que hay en la red (un PC con dos tarjetas de red y con una herramienta basada en DOS para aplicar reglas de acceso) por una herramienta basada en hardware o software para la implementación de políticas de acceso a la red y tener acceso solamente por los protocolos necesarios.

Como consecuencia de la implementación de un equipo especializado para la función de firewall se tiene los siguientes beneficios:

- Incremento de la seguridad al restringir el acceso desde y hacia Internet solo por protocolos específicos y desde direcciones IP origen específicas y consideradas confiables.

- Optimización del uso del ancho de banda de conexión a Internet al restringir el flujo de datos por protocolos específicos.

- Los firewalls ya sean basados en hardware o software cuentan con herramientas propias que monitorean el tráfico que ha pasado por sus interfaces de tal manera que se tiene un registro del tipo de protocolo que ha circulado así como el tipo de tráfico que ha sido bloqueado por no concordar con las reglas de acceso. Esto es muy importante ya que se puede registrar intentos de acceso no permitidos que podría tratarse de

ataques desde Internet o tal vez algún usuario que quiera conectarse a Internet por alguna aplicación no permitida por el administrador de la red.

Las características mínimas que debe tener el dispositivo que cumpla la función de firewall en la red son los siguientes:

- ✓ Debe tener como mínimo dos interfaces de red.
- ✓ Capacidad de hacer filtrado "statefull inspection"
- ✓ Capacidad de monitorear y alertar ataques típicos desde Internet como Denegación de Servicio o IP Spoofing.
- ✓ Capacidad de realizar NAT.

Dependiendo del producto seleccionado para esta función, las características de funcionalidad varían, pero siempre se mantendrán las características básicas mencionadas arriba.

5.2.2. Implementación de una zona desmilitarizada (DMZ) para servidores públicos.

La Facultad de Ingeniería en Electricidad y Computación de la ESPOL brinda varios servicios al personal administrativo, docente y alumnado como el acceso a navegación a Internet, el uso de mensajería electrónica y otros varios servicios que tienen que ver con Internet.

Como lo analizamos en el capítulo tres de este documento, La FIEC para proporcionar estos recursos cuenta con servidores especializados para este fin;

estos servidores necesariamente deben tener acceso desde Internet. Como ejemplo citamos el caso del servidor de correo electrónico (ceibo.fiec.espol.edu.ec), si este servidor no fuera accesado desde Internet (red pública) no fuera posible que los usuarios recibieran correos electrónicos de ninguna parte del mundo. Es el mismo caso para el servidor Web, para que los diferentes usuarios en el mundo puedan acceder a la información que está en la página Web de la FIEC, debe existir el acceso desde Internet al servidor Web.

Basados en estos criterios, es imprescindible la necesidad de mantener acceso desde Internet a estos servidores, pero no es menos cierto que es altamente riesgoso (si no se cuenta con las herramientas necesarias) que al permitir acceso, estos equipos sean blanco de ataques desde Internet.

Es por esto que sugerimos a la FIEC implementar una topología de seguridad de red implementando una zona desmilitarizada (DMZ) en la que se encuentren los servidores que brindan servicios hacia Internet, como lo son, el servidor Web y el servidor de correo electrónico. Con este esquema se separa físicamente la red privada de la red pública utilizando el firewall como equipo de control de acceso entre todas las redes.

El gráfico 5-1 muestra un ejemplo de un tipo de topología que podría implementarse en la FIEC

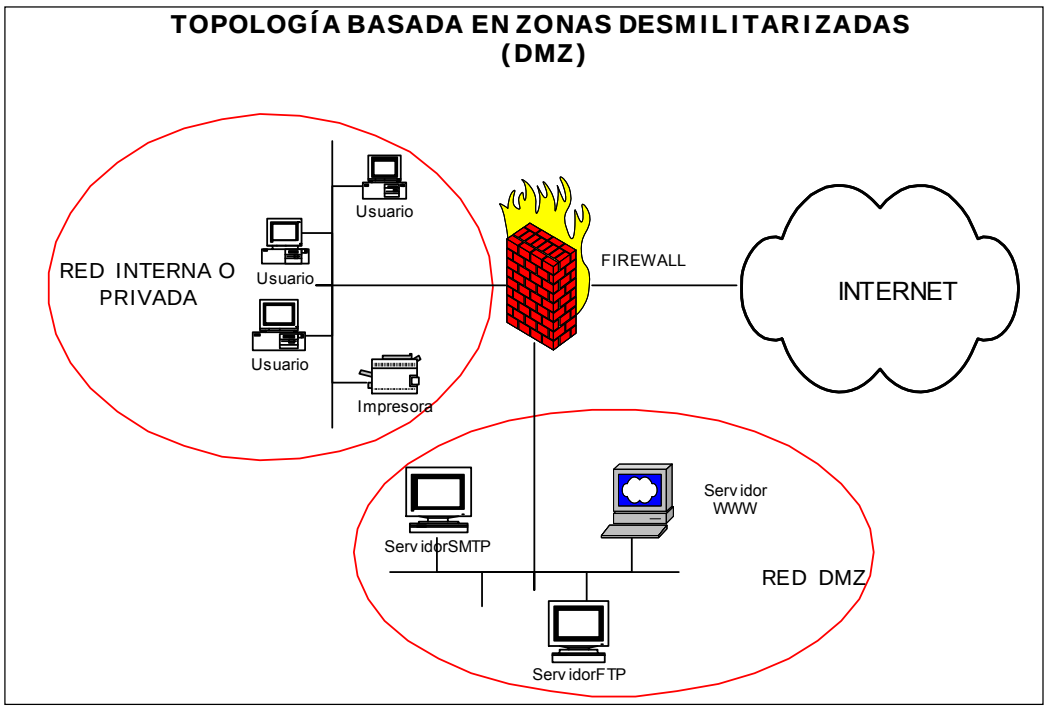


Figura No. 5-1 Diseño de red Sugerido para la FIEC

En el gráfico se aprecia una arquitectura “three homed” con el firewall como equipo central de control de tráfico con tres interfaces de red: red externa, red desmilitarizada y red interna.

Los servidores con servicios públicos hacia Internet instalados en la red DMZ, los usuarios en la red interna y en la red pública la conexión directa hacia el dispositivo de conexión a Internet.

Este tipo de configuración es la ideal para el ambiente de trabajo en la FIEC considerando la gran cantidad de usuarios que tiene la facultad; en este diseño

se ha puesto mucho énfasis en protección a los servidores de la red DMZ ya que no solo los ataques pueden provenir de Internet, sino también desde la misma red privada por lo que es necesario mantener un alto nivel de seguridad para eso equipos críticos.

5.2.3. Implementación de NAT (Network Address Translation) para optimizar el uso de direcciones IP públicas.

Como lo explicamos en el Capítulo 3 de este documento, el direccionamiento IP de la FIEC corresponde al network ID (identificador de red): 200.9.176.0 con máscara de subred 255.255.255.0 es decir, cada computador en la FIEC tiene asignado una dirección de esta red.

Si nos damos cuenta, las direcciones que utilizan estos equipos corresponden a un rango público de direccionamiento, con un límite máximo de 254 direcciones disponibles. Si bien es cierto, actualmente la FIEC no cuenta con 254 hosts, pero al incrementar el número de computadoras en la red (como consecuencia de un incremento en el número de usuarios) implica que el número de direcciones que aún queda disponible irá reduciendo.

Como para prevenir este inconveniente a futuro, sugerimos un cambio en el esquema de direccionamiento IP en la red de la FIEC, utilizando un rango de direcciones privadas como la red 172.16.0.0 con el que puedo abarcar un número mucho mayor de direcciones IP disponibles para los hosts ((2^16)-2 direcciones para hosts).

El acceso a Internet lo maneja el firewall con la característica de NAT de las direcciones privadas a IPs públicas sin necesidad de desperdiciar una IP pública para cada uno de los hosts que necesiten acceder a Internet.

Con la característica de NAT, todos los hosts internos pueden acceder a Internet a través de una sola dirección pública; los únicos hosts que tendrían una traducción de direcciones uno a uno (para una dirección privada le corresponde una dirección pública en las reglas de traducción) son los servidores que brindan servicios de Internet (mail, DNS, WWW) ya que actualmente en se encuentra registrado en el NIC-EC los servidores DNS para el dominio fiec.espol.edu.ec en el que se especifican los siguientes registros de host:

Tipo de Registro	Nombre	Dirección IP
NS (name server)	jupiter.espoltel.net	200.10.147.2
NS (name server)	ns.accessinter.net	64.46.64.254
NS (name server)	onl01.ramt.com	64.46.64.254
NS (name server)	goliat.espol.edu.ec	192.188.59.2
MX (mail exchanger)	ceibo.fiec.espol.edu.ec	200.9.176.5
WWW (word wide Web)	cedro.fiec.espol.edu.ec	200.9.176.7

Tabla XXI. Registros DNS para el dominio fiec.espol.edu.ec

Esta información está disponible de manera pública en el sitio Web del NIC-EC que es la entidad en el Ecuador responsable de administrar nombres de dominio ".ec"

5.2.4. Implementación de equipos o programas para el monitoreo de posibles ataques a la red interna.

Para tener un control total en el monitoreo de la seguridad en red, se sugiere instalar sistemas de detección de intrusiones en segmentos de red internos y en el segmento de la red DMZ, tal como lo mostramos en la figura 5.2.

Durante el desarrollo del proyecto utilizamos la herramienta eTrust Intrusion Detection de la casa *Computer Associates* con el que monitoreamos tráfico considerado como un patrón de ataque.

Es recomendable que el administrador de la red de la FIEC considere instalar durante un tiempo de evaluación esta herramienta que es una de las más completas que existe en el mercado, no solo por el hecho de detectar intentos de ataques hacia la red privada, sino por una característica muy importante que no la habíamos mencionado anteriormente que es la capacidad de bloquear el acceso a páginas Web que se encuentren clasificadas en varios tipos de categorías como por ejemplo, sitios para adultos, de apuestas, de entretenimiento, etc. en general, sitios no productivos para los intereses de la Facultad.

Esta característica es de mucha importancia si consideramos que podemos bloquear el acceso a sitios no productivos en Internet y por consiguiente, optimizar el ancho de banda de conexión a Internet.

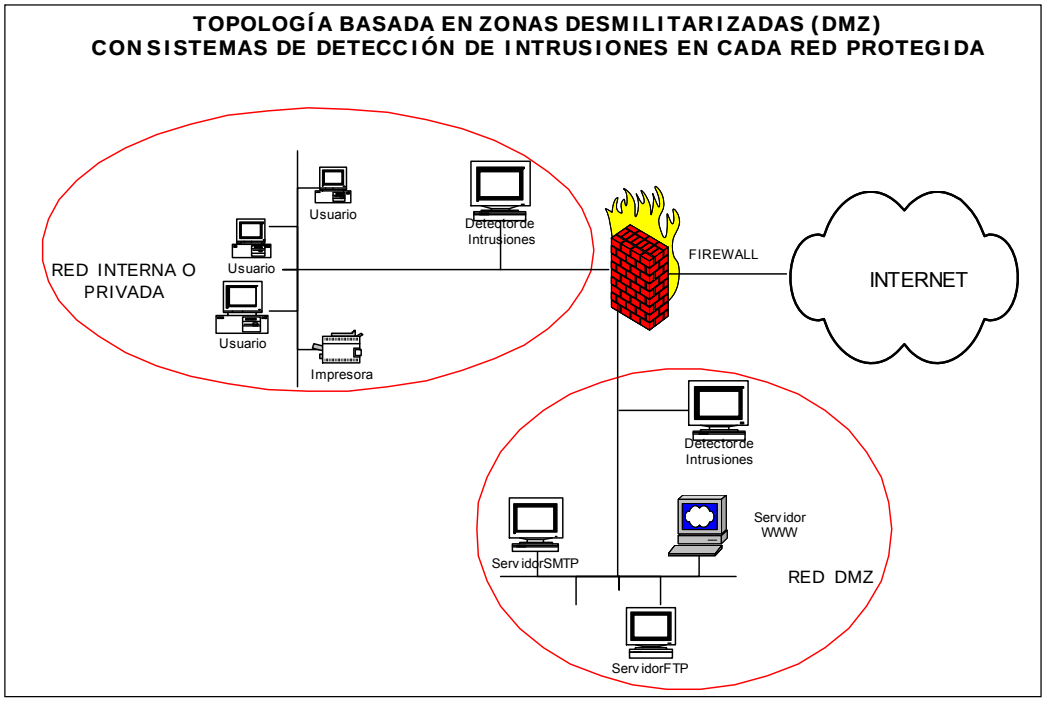


Figura No. 5-2. Topología basada en DMZ con sistemas de detección de intrusiones

5.2.5. Distribución de servicios de Internet en los equipos de la FIEC.

Es poco recomendable que varios servicios de Internet funcionen en un solo equipo ya que en el posible caso de una falla en un servidor que cumpla varias funciones, todos los servicios asociados al equipo con problemas no estarán disponibles para los usuarios de la red. Es mucho más crítico si no se cuenta con un esquema de redundancia o con equipos de contingencia en la red.

Como una medida preventiva para aminorar el impacto de un posible fallo en alguno de los servidores críticos es distribuir los servicios en varios equipos de la

red. En el caso de la FIEC, de acuerdo a la información proporcionada, solo hay un equipo con dos servicios de Internet: ceibo.fiec.espol.edu.ec que brinda servicio de DNS para resolución de nombres de dominio y SMTP para el tráfico de correo electrónico.

El servicio de Web y Web mail están en dos servidores diferentes por lo que no hay otros servicios que se vean afectados si a alguno de estos equipos fallara.

Para el caso de los servidores de la red interna (servidor de antivirus, servidor de archivos, servidor de impresión, servidor de autenticación, etc.) la sugerencia es la misma, no se debe concentrar todos los servicios en un mismo equipo, primero por rendimiento y segundo por posibles fallos que pueda sufrir el equipo.

5.2.6. Cambio en los equipos de conectividad final por otros de mejor rendimiento y con capacidad de administración remota por SNMP.

Los actuales equipos de conectividad de la FIEC son concentradores (hubs) de 10 Mbps conectados entre sí en cascada formando un solo dominio de colisión en la red. A estos concentradores se encuentran conectados tanto servidores como equipos clientes de la red

Para incrementar el rendimiento en la red de datos, es conveniente reemplazar los concentradores por switches de 100 Mbps; con esto se obtiene mayor tiempo de respuesta en el tráfico entre los usuarios y los servidores internos debido a

ancho de banda dedicado entre cada PC o servidor y el respectivo puerto del switch, a diferencia del concentrador en que los 10 Mbps son compartidos por todas las computadoras conectadas a sus puertos.

Una de las características que deben tener los switches es soportar el protocolo SNMP (Simple Network Management Protocol); dado la capacidad de este protocolo para poder administrar equipos que trabajen con TCP/IP, se podría administrar el estatus de cada uno de los switches a través de cualquier herramienta de gestión de redes basada en SNMP.

5.2.7. Implementación de herramienta de administración de redes basado en SNMP.

En la actualidad es sumamente importante gestionar la actividad en la red de cualquier organización, la FIEC como tal no puede ser la excepción. Actualmente no existe alguna herramienta que controle el estatus de todos los componentes de la red (equipos activos, servidores, PCs clientes, etc) por lo que no se sabe cuándo alguno de estos equipos pueda estar con problemas.

En un ambiente de administración de redes existen básicamente los siguientes componentes principales:

- Estación de gestión.- Un computador que utiliza un software de administración de redes.

- Elementos de red a ser administrados.- Deben proveer la capacidad de poder ser administrados, ejemplo: switches, routers, servidores.

- Protocolo de comunicación.- El protocolo que utilizan los componentes de la red para comunicarse con la estación de gestión, ejemplo: SNMP.

Existe el protocolo SNMP (Simple Network Management Protocol) que es un protocolo estándar basado en TCP/IP, y que es soportado por la mayoría de equipos de comunicaciones que trabajan con TCP/IP.

Dentro de las facilidades que las herramientas de este tipo ofrecen al administrador de la red se encuentran las siguientes:

- ✓ Control del estatus general del equipo.
- ✓ Verificación del estatus de utilización de memoria RAM y Procesador.
- ✓ Estatus de las interfaces de red que tenga el equipo.
- ✓ Cantidad de paquetes y bytes de tráfico a través de las interfaces del equipo.
- ✓ Dependiendo del fabricante de los equipos administrados, se puede visualizar la configuración y realizar modificaciones en los equipos de la red.

Sugerimos al administrador de la red utilizar alguna herramienta de administración de redes basado en SNMP que es un protocolo estándar para

monitorear el estatus general de la red ya que en la actualidad no cuentan con ninguna herramienta que pueda hacer gestión de la red. Inclusive, según las mejoras realizadas a este protocolo, existe disponible SNMP versión 3 que incluye mejoras a vulnerabilidades detectadas en el protocolo original y que atacaban a equipos que tenían levantado este protocolo con serias consecuencias como borrado de la configuración, modificación de permisos de acceso, etc.

Existen varias herramientas de gestión de redes en el mercado; podemos citar como ejemplos los siguientes programas:

Programa	**Casa Fabricante**
Cisco Works	Cisco Systems
HP Open View Network Node Manager	Hewlett Packard
Unicenter TNG	Computer Associates
Site Manager	Nortel Networks
NetSight Atlas	Enterasys Network
Net View	IBM

Tabla XXII. Principales Herramientas de Gestión de redes de Datos

Estas son algunas de las herramientas más utilizadas por los administradores de red dado su gran versatilidad para el manejo de eventos y alarmas en la consola; son herramientas altamente proactivas que se complementan con el uso de las herramientas de detección de intrusiones y con las herramientas de detección de contenido.

También existen herramientas más simples en su utilización pero que también cumplen con el objetivo de emitir algún tipo de alarma o simplemente para verificar el estatus de los equipos de la red. Sea cual fuere la herramienta que el administrador utilice para la FIEC, al implementar la administración remota se obtiene mayor facilidad de gestión y un menor tiempo de respuesta a posibles fallos ya que se identifica directamente al equipo que pueda estar con problemas e inmediatamente tomar las medidas necesarias.

5.2.8. Movilización del rack de comunicaciones a un sitio de acceso restringido.

En los actuales momentos el rack donde se encuentran los equipos de conectividad se encuentran en un cuarto cercano a los laboratorios de computación de la FIEC que no presta la mayor seguridad ya que se encuentra expuesto a las personas que circulan por los exteriores de los laboratorios.

Una de las primeras reglas de seguridad informática es el mantener los equipos de comunicaciones en una localidad con acceso restringido solo a personal autorizado por la organización, precisamente para prevenir ataques de vandalismo, o acceso a equipos para modificar algún parámetro de configuración.

Por este motivo se recomienda al administrador de la red de la FIEC realizar las gestiones pertinentes para solicitar la reubicación del rack en un centro de cómputo plenamente adecuado, donde inclusive estén los servidores de la red y mantener centralizado la ubicación y administración de todos los componentes.

5.3. Otras topologías alternativas para la red de la FIEC

En esta sección presentaremos otras alternativas para incrementar aún más el nivel de seguridad en la red de datos de la FIEC con topologías de red alternativas que implican la adquisición de nuevo equipamiento con características avanzadas que en un futuro podría ser implementada en la FIEC. Los esquemas propuestos incluyen la instalación de herramientas de detección de intrusos y herramientas de detección de contenido para contar con diseños altamente seguros.

5.3.1. ALTERNATIVA #1: Conexión a Internet por medio de un firewall basado en Linux.

Bajo este esquema, se cambia el actual equipo de conexión a Internet por un firewall basado en Linux con el servicio IPTABLES instalado para habilitar filtrado de paquetes y que permita hacia y desde Internet el tráfico necesario.

Para aumentar la seguridad en la LAN hemos considerado implementar segmentación en la red para separar al grupo de “estudiantes” (los diferentes laboratorios de computación de la FIEC) del grupo “administración y personal docente” (personal administrativo y profesores) y del grupo “servidores” (donde se incluye a todos los servidores críticos de la red).

El objetivo de separar en grupos de hosts es para prevenir que desde cualquier punto de red del grupo de estudiantes podamos acceder a las computadoras del

personal administrativo o peor aún, a alguno de los servidores para intentar realizar algún tipo de ataque.

Esta segmentación se la puede realizar utilizando un solo switch siempre que tenga la capacidad de realizar VLANs (Virtual LANs), es decir, crear grupos de puertos de tal manera que cada grupo sea como si fuera físicamente un switch diferente.

Con este diseño cada unidad o laboratorio dentro de la Facultad debe tener su propio equipo activo (switch o hub) con el cableado especialmente para cada área, el uplink (conexión) desde estos switches debe ir al switch principal en el centro de cómputo, conectado en uno de los puertos de la VLAN respectiva.

La figura 5.3 describe el diseño de esta alternativa con los equipos sugeridos incluyendo el número de parte de los mismos, cabe mencionar que se han sugerido equipos de la casa CISCO SYSTEMS que es en la actualidad uno de los fabricantes de equipos de comunicaciones con mayor prestigio.

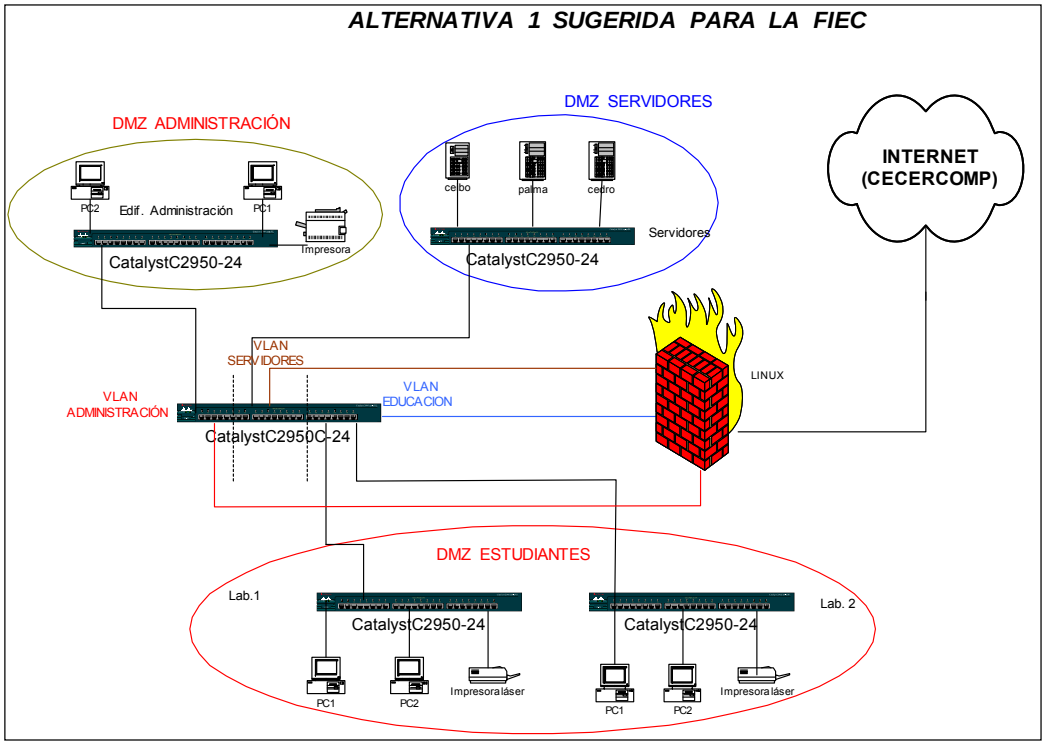


Figura No. 5-3 Alternativa No.1 de seguridad para la FIEC

5.3.1.1. Ventajas de la alternativa #1.

Podemos mencionar las siguientes ventajas respecto a este diseño:

- Cero costos en lo referente a licenciamiento del sistema operativo para el firewall por ser plataforma Linux.
- Cero costos en el licenciamiento el software de firewall ya que el servicio IPTABLES está incluido dentro de la distribución de Linux (Red Hat, Suse, Mandrake, etc).

- De manera centralizada se mantiene un control en las políticas de acceso entre las VLANS a través del firewall, recordemos que cada VLAN definida es una red desmilitarizada (DMZ) y por lo tanto, las reglas pueden aplicarse en el sentido que el administrador de red lo considere necesario, por ejemplo, si se desea que la VLAN de estudiantes tenga acceso a un servidor específico, por ejemplo, un servidor Web, se debe habilitar una política que permita el acceso desde la DMZ "estudiantes" a la DMZ "servidores" por el protocolo http.
- Una gran ventaja es la renovación de los equipos activos para la red LAN, se cambian los antiguos hubs de 10 Mbps por switches de 10/100 Mbps, esto es un cambio muy importante especialmente para los servidores que necesitan tener alta disponibilidad del ancho de banda del segmento de red.
- Cada VLAN, está asociada a una red DMZ en el firewall, y por lo tanto deben ser redes IP diferentes. Con este esquema se debe implementar un direccionamiento IP diferente al actual, definiendo subredes privadas para cada DMZ que pueden ser del tipo 172.16.0.0/16 o 192.168.0.0/24 y con esto ahorramos direcciones IP públicas que la FIEC actualmente utiliza para cada uno de sus hosts. La traducción de direcciones (NAT) lo maneja directamente el firewall para cada DMZ.

5.3.1.2. Desventajas de la alternativa #1.

- Una de las desventajas más palpables es el hecho de cambiar el direccionamiento IP actual de cada uno de los hosts de la FIEC por el nuevo esquema de direcciones privadas, incluyendo el cambio del default gateway (puerta de enlace predestinado), considerando el número de hosts existentes en la red, sería tedioso cambiar máquina por máquina los parámetros TCP/IP en la configuración de las tarjetas de red.
- Dependiendo del tipo de herramienta de detección de intrusiones que se utilice, se debería colocar una réplica de la herramienta en cada DMZ para que monitoree cada uno de las interfaces del firewall, sin embargo, existen herramientas que están montadas sobre un mismo equipo y tienen la capacidad de monitorear varios segmentos de red simultáneamente, en este caso, depende del criterio del administrador de la red para definir las interfaces del firewall más importantes a ser monitoreadas; sugerimos el monitoreo de la interfase donde están los servidores y de la interfase donde están los laboratorios de estudiantes.
- Cualquier cosa que implique cambio está sujeto a una inversión económica, decimos esto porque necesariamente se tiene que cambiar la infraestructura de equipos de conectividad, por lo menos para el switch que servirá de nuevo *core* (núcleo de conexión principal) en la red, debe tener capacidad de soportar VLANs y que sus interfaces sean 10/100 Mbps. Como mencionamos anteriormente, en este diseño se ha incluido switches de la marca CISCO SYSTEMS, pero solamente como referencia; existen otras casas fabricantes que tienen equipos de muy buen

rendimiento y con características similares y sobre todo a un costo inferior a CISCO, como por ejemplo, ENTERASYS NETWORKS o 3COM.

5.3.2. ALTERNATIVA #2: Conexión a Internet por medio de un firewall basado en Linux y configuración de redes DMZ sobre concentradores diferentes.

Esta alternativa es similar ala alternativa #1, se tiene como firewall un servidor basado en Linux con IPTABLES configuradas para otorgar los permisos de acceso entre las diferentes redes DMZ; la diferencia radica en que se utilizará los actuales hubs (concentradores) con que cuenta la FIEC para conectar los equipos y servidores.

Como primer punto de seguridad sugerimos que especialmente para los servidores, se utilice un hub exclusivamente para ellos, es decir, no dar oportunidad a que en algunos de los puertos disponibles se conecte a un usuario, solo para uso de servidores.

La figura 5.4 describe esta alternativa.

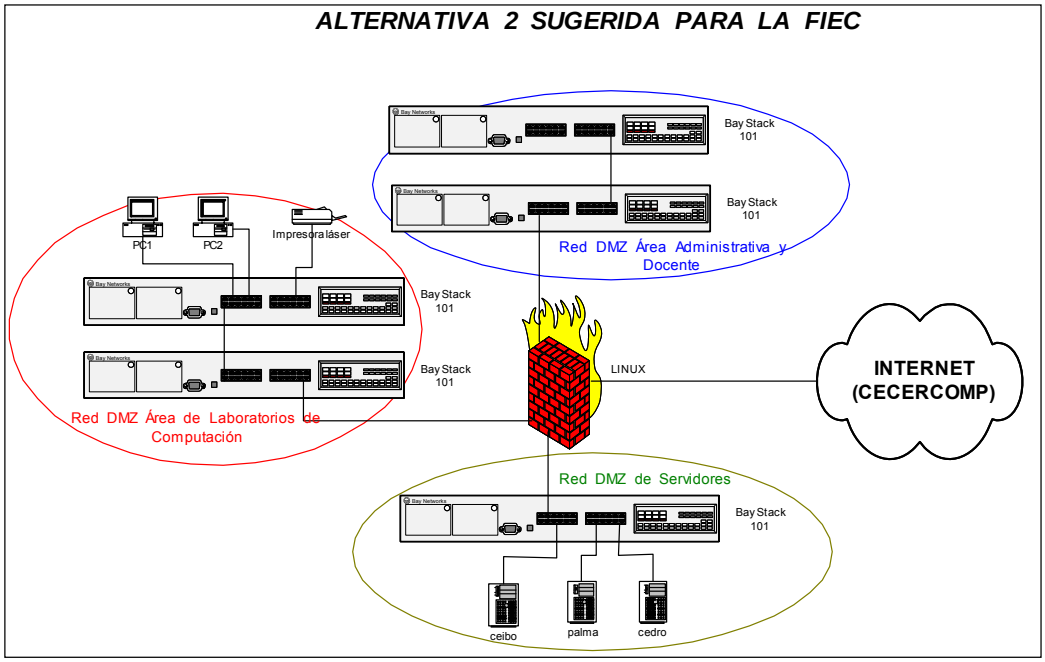


Figura No. 5-4 Alternativa No.2 de seguridad para la FIEC

5.3.2.1. Ventajas de la alternativa #2.

Podemos mencionar los siguientes puntos respecto a esta alternativa:

- Esta alternativa, al ser similar a la alternativa #1, brinda todas las ventajas de seguridad descritas en la sección anterior, es decir, costos por licencias de sistema operativo y aplicación de firewall, administración centralizada de políticas de acceso, y principalmente segmentación física y lógica de la red LAN.
- Se reducen costos al utilizar la misma infraestructura de equipos de conectividad, manteniendo el mismo nivel de seguridad.

5.3.2.3. Desventajas de la alternativa #2.

A las desventajas descritas en la alternativa #1, se suman las siguientes:

- Incapacidad de incrementar el rendimiento en velocidad en el tráfico de la red LAN, al estar limitados a un ancho de banda compartido de 10 Mbps.
- Los hubs disponibles en la FIEC no son administrables de manera local ni de manera remota por lo que se pierde el control de gestión de estos equipos.

Hacemos hincapié en que las alternativas aquí descritas deben ir complementadas con cada una de las sugerencias que se han realizado en este capítulo, ya que no se obtendrá mayor beneficio si se implementa una topología de red como las sugeridas en las alternativas 1 y 2 si por ejemplo, no se cambia la ubicación física del rack de equipos de comunicación.

Cada una de las alternativas propuestas puede sufrir variaciones con respecto al equipo que funcione como firewall. Por cuestiones de costos para la facultad, se incluye soluciones de firewall basadas en LINUX, pero no necesariamente tiene que ir un servidor LINUX como firewall.

En la actualidad existen varias soluciones en el mercado para seguridades en redes de datos, basadas en hardware y software, mencionamos algunas:

FABRICANTE	MODELO	TIPO
Cisco Systems	PIX 500 Series	Hardware
Checkpoint	Firewall-1	Software
Enterasys Networks	Aurorean	Hardware
Computer Associates	eTrusts Firewall	Software
Motorola	Watch Guard	Hardware
Microsoft	Internet Security and Acceleration Server	Software
eSoft	InstaGate	Hardware

Tabla XXIII. Principales Productos de Administración de Seguridades y sus Fabricantes

Los productos mencionados en esta tabla son solo referenciales, cada uno de ellos tienen características de funcionalidad que los distinguen, pero básicamente todo producto que funcione como firewall tiene el mismo principio de funcionamiento: filtro de paquetes y manejo de NAT. Corresponde a un análisis más exhaustivo el comprobar cuál producto es el que más le convendría a la FIEC para que funcione como firewall, sin embargo ese no es el tema a tratar en esta tesis.

5.4. Componentes de Seguridad Complementarios.

En un plan de gestión de seguridades no debemos olvidar que cualquier red, por más segura que pueda ser la topología que se ha elegido para implementar, siempre existe el riesgo de ser blanco de ataques de cualquier tipo.

Existen elementos adicionales que permiten al administrador de la red incrementar el nivel de protección en la red y a mejorar la productividad de los usuarios de la red, nos referimos a los sistemas de antivirus y a los filtros de URL

5.4.1. Sistemas de Antivirus.

Últimamente, la mayoría de redes de computadoras en el mundo han sido víctimas de los virus informáticos que a diario se desarrollan por programadores mal intencionados y que se distribuyen rápidamente por la Internet. Es por eso que toda red de computadoras debe contar programas de protección contra virus.

Estos programas actúan monitoreando la actividad de las computadoras en busca de algún tipo de archivo que pueda ser considerado como un posible virus. También casi todos los productos de antivirus tienen la capacidad de monitorear la actividad de la computadora a través de la red de datos de tal manera que si hay algún virus que quiera propagarse a través de la red LAN, el programa lo detecta y cura o elimina el archivo infectado.

En los esquemas de implementación de sistemas de antivirus, existe siempre un servidor central en la red que se descarga desde Internet las actualizaciones de bases de virus conocidos y sus respectivas defensas. Una vez que el servidor central se ha actualizado, éste comienza a distribuir las actualizaciones al resto de computadoras en la LAN, de esta forma se optimiza el ancho de banda de acceso a Internet ya que las computadoras en la red no se actualizan desde Internet sino desde el servidor central en la LAN.

5.4.2. Filtros por URL.

Esta es una característica de algunos de los productos que se utilizan como firewalls, y en algunos productos que funcionan como servidores PROXY.

El filtrado por URL es básicamente aplicar reglas para permitir o evitar que los usuarios que tienen acceso a Internet por http puedan ingresar a páginas que según el criterio del administrador de la red son consideradas como no productivas.

Es muy común hoy en día que los usuarios que pueden navegar a Internet, durante horas de trabajo ingresan a páginas de entretenimiento (novedades, horóscopo on-line, compras, etc.) e inclusive a sitios con contenido para adultos, utilizando de una mala forma un recurso tan limitado como lo es el ancho de banda de acceso a Internet de la empresa.

Al aplicar el filtro por URL se clasifica a los sitios Web por su contenido, por ejemplo, se puede crear la categoría “sitios par adultos” donde se incluyen sitios Web con ese tipo de contenido. Al aplicar la regla que se deniegue el acceso a este sitio se generan también registros que le pueden indicar al administrador de la red las direcciones IP de las computadoras que han tratado de ingresar a ese tipo de sitios e inclusive la hora del intento.

Esta característica actualmente es de mucha utilidad, especialmente en instituciones educativas y la ESPOL no es la excepción, por lo que se hace muy indispensable instalar o configurar esta característica en el equipo que funcione como firewall.

CONCLUSIONES Y RECOMENDACIONES

De lo expuesto en el desarrollo de este proyecto, y basado en las observaciones realizadas y los resultados que se obtuvieron de las pruebas con la herramienta de detección de intrusiones y con la herramienta de detección de vulnerabilidades en la red de la FIEC, mencionamos las siguientes conclusiones y recomendaciones.

Conclusiones

1. Dado que la seguridad en redes de datos es un tema de vital importancia en las empresas actuales, la protección de la información y en general, de los sistemas con los que cuenta la red debe ser siempre monitoreado y registrado por el personal técnico responsable y con las herramientas adecuadas.

2. Los puntos clave en la seguridad informática empiezan con algo tan básico como permitir el ingreso a los centros de cómputo solo al personal debidamente autorizado y siempre registrando el ingreso del personal en una bitácora para poder determinar quién o quienes estuvieron a determinada hora en el sitio. Si no se sigue este parámetro de seguridad básico, por muy buenos que sean los equipos o herramientas que se dispongan para la protección de la red, las posibilidades de que nuestra red sufra un ataque se incrementarán considerablemente.

3. La topología actual de la red de la FIEC es "dual hommed" es decir, una red pública y una red privada, con un hosts de frontera que brinda acceso a los usuarios internos hacia el resto de la red de la ESPOL (incluyendo el acceso hacia Internet a través de CECERCOMP), sin embargo, a pesar de tener restringido el acceso desde Internet a los servidores principales de la FIEC, la conectividad (a nivel del protocolo TCP/IP) es permitida. Si cualquier persona con conocimientos avanzados de TCP/IP y que conozca las debilidades que tiene el protocolo y de los servicios activos en los servidores, podría aprovechar estas debilidades para obtener acceso a los sistemas de la red y ocasionar un perjuicio importante a la Facultad.

4. De los resultados de las pruebas de detección de vulnerabilidades realizado desde Internet (capítulo IV de este documento), las

vulnerabilidades que fueron encontradas no están catalogadas como críticas y por lo tanto es poco probable que se produzca un ataque de un pirata informático. Los servicios que se encontraron activos son los que deben estar necesariamente habilitados o disponibles (correo, Web, DNS) ya que por estos protocolos se establece el acceso de los usuarios externos con la FIEC como por ejemplo, a través de correo electrónico, o a través de la página Web de la Facultad. Este tipo de acceso se lo obtiene en las políticas de acceso definidas en el firewall, por direcciones IP origen – destino y solo por los protocolos determinados por el administrador de la red.

5. Las pruebas de detección de vulnerabilidades mostraron que los servidores también tienen deficiencias de nivel bajo o no críticas. En ambos casos, los resultados son favorables para la FIEC ya que la plataforma de servidores es UNIX (distribución LINUX Red Hat) lo que brinda a la red un nivel de estabilidad alto para los servidores. Conocido es el hecho que son pocas las vulnerabilidades descubiertas en plataforma UNIX, aunque esto no garantiza que sea una plataforma invulnerable, cada vez más, los *hackers* están desarrollando técnicas avanzadas de ataque para obtener acceso a servidores UNIX, por lo que se debe estar siempre informado, en Internet principalmente, por las últimas vulnerabilidades descubiertas en plataformas de sistemas operativos y las técnicas de ataque utilizadas por los *hakers*.

6. Se pudo comprobar la eficiencia de la herramienta de detección de intrusiones ETRUST y con ello la importancia de contar con este tipo de programas que ayudan a la gestión de seguridad como complemento a la acción de los firewalls. La actividad monitoreada en la red por patrones de ataque (debido a la acción de la herramienta Cisco Secure Scanner) y las alertas por pantallas que envía al administrador es una de las grandes cualidades de esta herramienta. Es importante también mantener actualizada la base de información de las herramientas de detección de intrusiones debido al constante incremento de técnicas de ataque cada vez más avanzadas y a las nuevas vulnerabilidades descubiertas, no solo en plataforma de servidores sino en equipos de comunicaciones como routers, access servers, switches y cualquier tipo de equipamiento que funcione con el protocolo TCP/IP.

7. Concluimos además que la topología de red que brinda un mayor nivel de seguridad a la FIEC es basado en redes DMZ, aislando física y lógicamente los servidores que brindan servicios de Internet del resto de computadoras de la red. Con esto se consigue seguridad a servidores que brindan servicios internos (base de datos, servidores de aplicación, etc.) y también restringir el acceso a los servidores públicos solo por los protocolos necesarios. Esto se lo define en las reglas de acceso en el firewall y con el criterio del administrador de la red.

RECOMENDACIONES

1. Si bien es cierto, el objetivo de este proyecto no es el de evaluar productos o herramientas de firewall, recomendamos implementar un equipo dedicado a las funciones de firewall en la red de la FIEC, el actual dispositivo no brinda las características competas de un buen firewall. En el capítulo V de este proyecto se indican firewalls basados en hardware y software podrían ser considerados como alternativas por la Facultad.

2. El diseño de red basado en "zonas desmilitarizadas" (DMZ) es el recomendado para la FIEC. La alternativa # 2 expuesta en este trabajo podría ser una alternativa adecuada por factores de costo al utilizar un servidor LINUX como firewall y utilizar los mismos equipos de conectividad con que cuenta actualmente la red. Sin embargo, recomendamos que la alternativa #1 sea implementada en la FIEC ya que los switches brindan un mejor rendimiento en la comunicación al eliminarse las colisiones de paquetes que se tienen en el esquema actual, incremento en el ancho de banda de la red (100 Mbps) además de tener la capacidad de ser gestionados para tener un control del tráfico que circula en la red de la Facultad.

3. La definición de las reglas o políticas de acceso desde la red interna hacia Internet y hacia la red DMZ debe ser planificada

cuidadosamente por el departamento de sistemas. En esta definición recomendamos establecer las direcciones IP origen y destino y los protocolos utilizados que sea estrictamente necesarios; esto para evitar que tráfico innecesario para la red sature el ancho de banda de acceso a Internet.

4. El administrador de la red debe contar con herramientas como los sistemas IDS (detección de intrusiones) para el monitoreo de tráfico sospechoso en la red. Recomendamos la herramienta ETRUST INTRUSION DETECTION de la casa fabricante COMPUTER ASSOCIATES que se ha utilizado en las pruebas realizadas en este proyecto. Esta herramienta demostró tener un nivel de eficiencia muy bueno y además se puede implementar filtrado del tráfico Web evitando el acceso a páginas en Internet con contenido nocivo para los usuarios (sitios de pornografía, de juegos, de descarga de archivos mp3s, etc.) que no contribuyen al objetivo de investigación y educación que debe tener Internet en las entidades educativas y que además consumen ancho de banda.

5. Es de vital importancia mantener actualizado la herramienta de antivirus que tengan los servidores y estaciones de trabajo Muchos de los ataques se deben a la ejecución de virus “troyanos” en computadoras y servidores y que brindan al *hacker* la posibilidad de tomar control de determinado host para tratar de ingresar a servidores más importantes. Además, al mantener

actualizado las herramientas de antivirus, brindamos mayor seguridad a la información almacenada en los servidores.

6. Finalmente, recomendamos que se tenga actualizado el sistema operativo de servidores y estaciones de trabajo con los últimos parches y actualizaciones (*fixes*) de seguridad para disminuir la probabilidad de ser víctimas de ataques de usuarios externos e internos.

GLOSARIO

CI	Content Inspection, inspección de contenido
DMZ	Demilitarized Zone, zona desmilitarizada
FTP	File Transfer Protocol, protocolo de transferencia de archivos
Hacker	Pirata Informático
Hosting	Alojamiento
HTTP	Hypertext Transfer Protocol, protocolo de transferencia de hypertexto
IDS	Intrusion Detection System, sistema de detección de Intrusiones
LAN	Local Area Network, red de área local
NAT	Network Address Translation, traducción de direcciones de red
NFS	Network File System, sistema de archivo de red
RPC	Remote Procedure Call, llamada de procedimiento remoto
SMTP	Simple Mail Transfer Protocol, protocolo simple de transferencia de mensajería

SNMP	Simple Network Management Protocol, protocolo simple de administración de red
TCP/IP	Transmision Control Protocol/Internet Protocol, protocolo de control de transmisión/protocolo de Internet
UDP	User Datagram Protocol, protocolo de datagrama de usuario
URL	Universal Resource Localizer, localizador de recursos universal
VLAN	Virtual Local Area network, red de área local virtual
WAN	Wide Area Network, red de área extensa

BIBLIOGRAFÍA

AMOROSO, Edward
SHARP, Ronald
Seguridad en Internet e Intranet.
Editorial Prentice Hall

WENSTROM, Michael J.
Managing Cisco Network Security.
Editorial Cisco Press

SCAMBRAY, Joel
MC. CLURE, Stuart
Hacking Exposed II Edition: Network Security Secrets and Solutions.
Editorial Mc. Graw Hill

http://www.cisco.com

http://support.ca.com

http://netsecurity.about.com

ANEXOS

ANEXO 1

RESUMEN DEL PROCESO DE FUNCIONAMIENTO DEL CISCO SECURE SCANNER

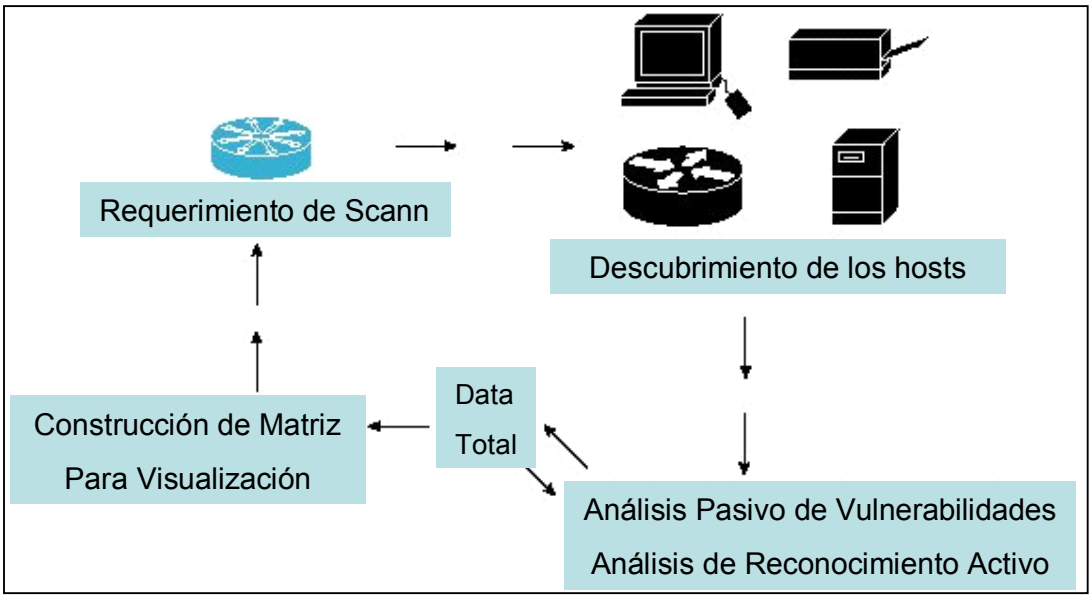
El proceso de evaluación de las vulnerabilidades de un host que ejecuta la herramienta Cisco Secure Scanner comienza con el **requerimiento del usuario para efectuar un scann**. La siguiente fase del proceso implica **descubrir el host**, el Scanner recopila todo tipo de información relacionado a este host como por ejemplo, los servicios que se ejecutan en el mismo.

Esta información es colocada en un **motor de análisis**, donde cada host es objeto de pruebas para detección de servicios, detección de sistema operativo y vulnerabilidades potenciales.

Si el requerimiento de scann incluye una confirmación de vulnerabilidades, entonces toda la información obtenida en la fase de descubrimiento es colocada en el **módulo de confirmación** que se encarga de confirmar vulnerabilidades del host. La **nueva información** que se obtiene del motor de análisis y del módulo de confirmación es añadida a la información original. En este punto se

crea una matriz que es enviada a la interfaz gráfica de usuario para visualizar los resultados al administrador de la herramienta.

El proceso de ejecución del Scanner es ilustrado en la siguiente figura:



ANEXO 2

VULNERABILIDADES POTENCIALES ENCONTRADAS EN LOS SERVIDORES DE LA FIEC

NOMBRE DE LA VULNERABILIDAD	NIVEL DE SEVERIDAD	SISTEMA OPERATIVO AFECTADO
RPC rstatd Active	1	UNIX

- **Descripción**

  El servicio *rpc.rstatd* regresa estadísticas de rendimiento obtenidas del kernel de UNIX del host sobre el que este servicio está ejecutándose. Se puede realizar una solicitud de estas estadísticas de manera remota.

- **Consecuencias**

  Un atacante puede de manera remota acceder al servicio *rstatd* por medio de programas como el "*perfmeter*" (una herramienta que permite monitorear rendimiento de servidores) para identificar sistemas inactivos, los cuales pueden ser fáciles destacar sin detección.

- **Hosts en los que fue encontrada esta vulnerabilidad**
  - 200.9.176.3
  - 200.9.176.5
  - 200.9.176.7

- **Medidas para mitigar la vulnerabilidad**

  Si usted no necesita este servicio, deshabilite rstatd en el archivo que se encuentra en la ruta: */etc/inetd.conf*

  Luego de eso pare el proceso *rpc.rstatd* que se ejecuta en el host.

NOMBRE DE LA VULNERABILIDAD	NIVEL DE SEVERIDAD	SISTEMA OPERATIVO AFECTADO
RPC rquotad Active	1	UNIX

- **Descripción**

  El demonio *rquotad* es utilizado para proveer información sobre espacio utilizado en discos duros en particiones NFS (plataforma UNIX).

- **Consecuencias**

  Esta información puede ser utilizada por atacantes para planificar ataques de denegación de servicios (denial of service) al identificar qué partición en un servidor UNIX está casi al límite de su capacidad y qué cantidad de data sería necesaria para llenar esa partición.

- **Hosts en los que fue encontrada esta vulnerabilidad**
  - 200.9.176.5
  - 200.9.176.7

- **Medidas para mitigar la vulnerabilidad**

  Deshabilite el servicio *rquotad* modificando el archivo *inetd.conf*.

NOMBRE DE LA VULNERABILIDAD	NIVEL DE SEVERIDAD	SISTEMA OPERATIVO AFECTADO
RPC portmapper Active	1	UNIX

- **Descripción**

  Portmapper es un servidor de registro para servicios RPC (Remote Procedure Call). Estos servicios no se ejecutan sobre puertos TCP o UDP fijos; en el momento en que estos servicios se inician, eligen un puerto aleatorio y luego registran ese puerto utilizado en el servidor *portmapper*.

  Los programas que desean utilizar los servicios RPC realizan un requerimiento al servidor *portmapper* preguntando el puerto del servicio que desean utilizar.

El comando "*dump*" da una lista completa de todos los puertos que utilizan estos servicios. Es por este motivo que los servidores *portmapper* son un objetivo clave para los ataques de tipo reconocimiento.

- **Consecuencias**

  Un atacante puede determinar el tipo y versión de servicios RPC y en qué hosts se están ejecutando. Hay algunos ataques de red que involucran denegación de servicio al servidor *portmapper* o utilizan vulnerabilidades en el servidor *portmapper* para violar la seguridad del sistema.

- **Hosts en los que fue encontrada esta vulnerabilidad**
  - 200.9.176.3
  - 200.9.176.5
  - 200.9.176.7

- **Medidas para mitigar la vulnerabilidad**

  Aplicar filtros para evitar que se ejecuten requerimientos hacia el servidor *portmapper* que se originen desde fuera de la red. Utilice un *portmaper* seguro que restrinja el acceso a clientes que tengan direcciones específicas. Consulte la siguiente dirección en Internet para obtener las últimas versiones de *portmap*: ftp://ftp.win.tue.nl/pub/security

NOMBRE DE LA VULNERABILIDAD	NIVEL DE SEVERIDAD	SISTEMA OPERATIVO AFECTADO
Finger Active	1	UNIX

- **Descripción**

  El demonio *finger* (*fingerd*) provee información sobre las identidades de los usuarios de un sistema. Al estar activo este servicio, el atacante remotamente podría descubrir login names (por ejemplo: usuario@sistema.dominio) y de esta manera obtener información sobre los usuarios.

- **Consecuencias**

  El atacante puede descubrir nombres de cuenta válidos y tratar de adivinar las claves de acceso. También el atacante puede ser capaz de determinar desde qué máquinas los usuarios están ingresando su cuenta y de esa manera descubrir otras rutas de ataque en la máquina.

- **Hosts en los que fue encontrada esta vulnerabilidad**

  - 200.9.176.5
  - 200.9.176.7

- **Medidas para mitigar la vulnerabilidad**

  Finger no es un servicio necesario para la operación diaria del servidor por lo que debe ser deshabilitado.

NOMBRE DE LA VULNERABILIDAD	NIVEL DE SEVERIDAD	SISTEMA OPERATIVO AFECTADO
SSH RSAREF2 Buffer Overflow	3	UNIX

- **Descripción**

  Versiones de SSH (secure shell, acceso seguro a la consola de UNIX) son vulnerables a ataques de tipo sobrecarga del recurso (buffer overflow). Esta falencia está presente en todas las versiones de SSH1 hasta (e inclusive) la versión 1.2.27.

- **Consecuencias**

  Debido a esta falencia es posible ejecutar comandos arbitrarios como usuario *root*.

- **Hosts en los que fue encontrada esta vulnerabilidad**

  - 200.9.176.3
  - 200.9.176.5

- 200.9.176.7

- **Medidas para mitigar la vulnerabilidad**

  Se debe aplicar un parche de seguridad que lo provee el sitio web de CERT y que certifica que se corrige de manera efectiva esta falencia: http://www.cert.org/advisories/CA-99-15/ssh-patch.txt

ANEXO 3

VULNERABILIDADES CONFIRMADAS ENCONTRADAS EN LOS SERVIDORES DE LA FIEC

NOMBRE DE LA VULNERABILIDAD	NIVEL DE SEVERIDAD	SISTEMA OPERATIVO AFECTADO
NFS Dump	1	UNIX

- **Descripción**

  El sistema de archivos NSF es una aplicación cliente/servidor que permite a un usuario visualizar, almacenar y actualizar archivos sobre un sistema remoto (es básicamente, un servidor de archivos). Existen mecanismos para controlar cuales son los usuarios que pueden tener acceso a estos sistemas de archivos.

  Como parte de este servicio, un usuario puede ingresar el comando de UNIX “showmount –a” para remotamente realizar un requerimiento NSF por una lista de las máquinas que tienen montado los sistemas de archivo “objetivo”.

Por ejemplo, si el host A está acesando al sistema de archivo del host B, entonces el host X (el atacante) puede realizar un requerimiento al host B para determinar cuáles hosts tienen un acceso confiable a su sistema de archivo.

De esta maneara el atacante se entera que el host A tiene acceso permitido al host B. Utilizando alguna técnica de personificación (*spoofing*) el atacante puede hacerse pasar por el host A y de esta manera tener acceso al host B.

- **Consecuencias**

  El atacante puede obtener información sobre relaciones de confianza entre hosts, es decir qué hosts son confiables para el servidor que va a ser atacado. El atacante puede utilizar técnicas de personificación par acceder al servidor como un host confiable.

- **Hosts en los que fue encontrada esta vulnerabilidad**
  - 200.9.176.5
  - 200.9.176.7

- **Medidas para mitigar la vulnerabilidad**

  Es necesario que el administrador del sistema evalúe la necesidad de compartir archivos y sistemas de archivos. Si no es necesario deshabilite NSF y el demonio *mountd*.

NOMBRE DE LA VULNERABILIDAD	NIVEL DE SEVERIDAD	SISTEMA OPERATIVO AFECTADO
Finger Walk with Digits	1	UNIX

- **Descripción**

  El demonio finger (fingerd) provee información sobre las identidades de los usuarios de un sistema. Al estar activo el demonio *fingerd* el atacante remoto puede descubrir nombres de cuentas y ayudar a obtener información de los usuarios. Al ejecutar el comando "*1@hostname*" o "*@hostname*" puede (muy posiblemente) retornar información sobre los usuarios que hayan ingresado (*loggin*) en un dominio. En algunos casos, el requerimiento podría regresar información que se encuentra en el archivo "*password*" de UNIX.

- **Consecuencias**

  El atacante puede descubrir nombres de cuenta válidos y tratar de adivinar las claves de acceso. También el atacante puede ser capaz de determinar desde qué máquinas los usuarios están ingresando su cuenta y de esa manera descubrir otras rutas de ataque en la máquina.

- **Hosts en los que fue encontrada esta vulnerabilidad**

  - 200.9.176.5

- **Medidas para mitigar la vulnerabilidad**

  Finger no es un servicio necesario para la operación diaria del servidor por lo que debe ser deshabilitado.

NOMBRE DE LA VULNERABILIDAD	NIVEL DE SEVERIDAD	SISTEMA OPERATIVO AFECTADO
Global Finger Vulnerability	1	UNIX

- **Descripción**

  El demonio *finger* (*fingerd*) provee información sobre la identidad de los usuarios de un sistema. Algunos demonios *finger* aceptan el comando "*finger@hostname*" y dar como resultado todos los usuarios que han ingresado al sistema (*loggin*).

- **Consecuencias**

  El atacante puede descubrir nombres de cuenta válidos y tratar de adivinar las claves de acceso. También el atacante puede ser capaz de determinar desde qué máquinas los usuarios están ingresando su cuenta y de esa manera descubrir otras rutas de ataque en la máquina.

- **Hosts en los que fue encontrada esta vulnerabilidad**
  - 200.9.176.5
  - 200.9.176.7

- **Medidas para mitigar la vulnerabilidad**

  Finger no es un servicio necesario para la operación diaria del servidor por lo que debe ser deshabilitado.