DECLARACION DE AUTENTICIDAD

Yo, José Antonio González Lozano, declaro que los contenidos y los resultados obtenidos en el presente proyecto, como requerimiento previo para la obtención del Título de Tecnólogo Analista de Sistemas, son absolutamente originales, auténticos y personales y de exclusiva responsabilidad legal y académica del autor.

José González Lozano

1714407150

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo sobre el tema: "DESARROLLO Y DOCUMENTACION DE UN HACKING ÉTICO AL ITSCO", presentado por el ciudadano: José Antonio González Lozano, estudiante de la Escuela de Sistemas, considero que dicho informe reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte del Tribunal de Grado, que el Honorable Consejo de Escuela designe, para su correspondiente estudio y calificación.

Quito, Septiembre del 2011

Ing. William Cueva

TUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

Los miembros del Tribunal de Grado designado por el Honorable Consejo de la Escuela de Sistemas, aprueban el trabajo de investigación de acuerdo con las disposiciones reglamentarias emitidas por el Centro de Investigaciones Tecnológicas y Proyectos del "Instituto Tecnológico Superior Cordillera" para proyectos de grado de Tecnólogos Analistas de Sistemas: del Sr: José Antonio González Lozano.

Quito, Septiembre del 2011

Para constancia firman:

PRESIDENTE

VOCAL1 **VOCAL2**

AGRADECIMIENTO

Agradezco a Dios, por darme la fuerza necesaria para cumplir mis metas cada día de mi vida, a mi madre por haberme guiado por el camino del

bien y la honestidad, a mis profesores por haber compartido sus conocimientos y haberme guiado para la feliz culminación de mi carrera y a ti mi incondicional compañera, gracias por darme tu

Gracias

DEDICATORIA

Dedico este proyecto a Dios, mi Madre y mi novia por el incondicional apoyo en cada una de mis metas, a ustedes.

José González Lozano

CAPITULO I

EL PROBLEMA

1.1 Planteamiento Del Problema

Las computadoras alrededor del mundo están siendo víctimas de ataques de hackers (piratas informáticos), capaces de manipular un sistema, robar información y borrarlo completamente en pocos minutos. Por esta razón resulta de vital importancia conocer si los sistemas informáticos y redes están protegidos de este tipo de intrusos.

El ITSCO al encontrarse en esta realidad, es candidato perfecto para llevar a cabo un hacking ético, es decir, se dará a conocer todas las medidas preventivas en contra de agresiones maliciosas, se valdrá para ello de los test de intrusión, que evaluaran la seguridad técnica de los sistemas de información, redes de computadoras, aplicaciones web, servidores, etc., y se implementará una estructura de seguridad adecuada para cada área dentro de la red del ITSCO.

Actualmente los servidores del ITSCO al contener información sensible, podrán ser objeto de ataques por parte de hackers, ya sea desde dentro de la Institución o desde afuera, dicha red podrá ser atacada, tanto por los estudiantes, al contener información valiosa como el sistema de calificaciones, o por personas externas para poder tener acceso a la red inalámbrica el ITSCO.

Las pruebas de intrusión, también conocidas como "Análisis de Penetración" o "*Hacking* Ético", son actualmente una práctica habitual para conocer el nivel de seguridad que tiene una organización.

Se encargan de evaluar el tipo y extensión de las vulnerabilidades de sistemas y redes en términos de confidencialidad e integridad. Comprueban la seguridad de la red y

verifican empíricamente la resistencia de las aplicaciones y servicios de usos indebidos.

Las pruebas de *Hacking* Ético son una evaluación de la seguridad, en la cual el analista trata realmente de comprometer las máquinas o redes objetivo. En el ataque al *hardware* o al *software*, el analista puede utilizar material de laboratorio para probar suposiciones y revisar planes de ataque cuando así lo necesite. El proceso es empírico, y está sometido a una metodología definida.

La zona fronteriza de la red, deberá tener las respectivas normas de seguridad, como son la implementación de firewalls, IDS's, honeypots, seguridad en puertos, contraseñas más seguras, software para auditar la seguridad en redes, de esa forma se podrá fortalecer la estabilidad en los sistemas informáticos, y de esta manera se evitará que pueda haber una infiltración por vulnerabilidades dentro de los servidores.

1.2 Formulación Del Problema

¿Cómo afectará la falta de seguridad o vulnerabilidades a los servidores del ITSCO y a su red informática?

1.3 Delimitación del Problema

La Implementación y documentación de un hacking ético para el ITSCO, se lo realizará en la ciudad de Quito, dentro de sus instalaciones, en el laboratorio 2 del edificio en la calle Zamora y en el servidor principal del edificio en la calle Bracomoros, a través

de herramientas pertinentes que nos permitirán un análisis detallado del comportamiento de estos equipos; además se realizará un test de penetración y se

llevará a cabo el análisis de vulnerabilidades para determinar si la Institución puede ser objeto de un ataque a la intranet, ya sea de manera interna o externa, o si pueden ser alterados los sistemas de información, para así poder ofrecer una solución y determinar la seguridad adecuada.

FIGURA 1-1: UBICACIÓN ITSCO

Fuente: Google maps

Elabora: José González

1.4 Objetivo General

- Desarrollar y documentar un hacking ético, a un segmento de la red informática del ITSCO, a fin de mejorar la seguridad, dentro de la zona fronteriza.

1.5 Objetivos Específicos

- Analizar la seguridad actual del servidor principal del ITSCO.
- Utilizar herramientas para auditoria de redes, y así analizar los equipos del laboratorio, en cuanto a seguridad informática.
- Incrementar el sistema de seguridad, dentro de la red informática, por medio de la utilización de firewalls, IDS's, o honeypots.
- Desarrollar un documento, con recomendaciones de seguridad, basado en los resultados obtenidos después de un análisis de vulnerabilidades, al laboratorio 2 y al servidor principal del ITSCO, para así poder fortalecer la zona de frontera en la Institución.

1.6 Justificación e Importancia

La utilización de herramientas adecuadas, para poder auditar la situación actual del ITSCO, dará conclusiones y recomendaciones basadas en pruebas reales, para así poder realizar los pasos correctos, en la resolución de los problemas actuales de seguridad.

Los principales beneficiados serán los usuarios, como los profesores de la Institución que podrán utilizar los sistemas informáticos, sin riesgo a que sean modificados, por ejemplo al momento de pasar notas, los estudiantes podrán contar con una red más segura, en los laboratorios de informática.

Este proyecto se enfoca en realizar procedimientos, para analizar la zona de frontera del ITSCO, para lo cual se utilizarán herramientas adecuadas, que nos ayudaran a verificar los procesos, en cuanto a seguridad, este proyecto será un beneficio para el

ITSCO, ya que se descubrirá vulnerabilidades que pueden ser usadas por personas del exterior, para la manipulación de la información, o robo, en los sistemas internos, y así poder tomar medidas para evitarlos.

Esta investigación será de utilidad para el ITSCO, ya que este documento guiará, hacia una mejor toma de decisiones, en cuanto a vulnerabilidades actuales dentro de la red LAN y el servidor, se podrán detallar medidas de seguridad, en base a problemas actuales, a fin de poder incrementar la estabilidad y reducir de esa forma la posibilidad de ataques informáticos, sean estos internos o externos.

1.7 Alcance

Se realizará un test de penetración en un segmento de la red del ITSCO, el cual será el servidor principal en el edificio de la Bracomoros y el laboratorio 2 del edificio de la Zamora, de esta forma se realizará un hacking ético de manera interna y externa, se empezará con la fase de footprinting, en el cual se recopilarán datos de manera externa para analizar el nivel de acceso a la información en cuanto a dns, proveedores de internet, si se encuentra protegido por un firewall, etc., o datos sobre la Institución que puedan ser visibles para un hacker, la siguiente fase será el scanning a en el cual se detallarán los puertos que se encuentran abiertos en el servidor y que puedan ser usados para el uso de troyanos o backdoors para comprometer la seguridad del mismo, así también se verificará la versión del sistema operativo y como llegan los paquetes hasta el servidor a través de herramientas para traza de paquetes.

Se llevará a cabo un test de vulnerabilidades con el software Languard, en el laboratorio 2 del edificio de la Zamora será de mucha ayuda en esta auditoría de seguridad, ya que se pueden documentar los principales análisis de riesgos como son, falta de actualizaciones, para mayor estabilidad en los sistemas operativos, gestión de

vulnerabilidades para analizar el estado actual de la red en el laboratorio y otro tipo de riesgos como son los puertos abiertos que se encuentran actualmente en un equipo o las aplicaciones que podrían causar inestabilidad en el sistema operativo.

Por medio de la utilización de estas herramientas, se podrá determinar la vulnerabilidad en el servidor principal ya que este comparte aplicaciones para uso

interno del ITSCO, se analizará la seguridad actual del Laboratorio 2 para determinar la situación de los sistemas operativos en los equipos por medio del scanning para analizar los puertos que se encuentran abiertos, se utilizará el Sniffing para captura de paquetes y detallar que trafico atraviesa por la red, además del system hacking, para evaluar la seguridad de las cuentas de usuario, y así poder documentar las recomendaciones, incrementar la seguridad actual, para dar estabilidad en la situación actual de las aplicaciones.

Se entregará un informe final sobre la situación actual, en el cual se detallarán los equipos del laboratorio con sus respectivas vulnerabilidades, además de los resultados en las fases de hacking ético orientadas al servidor principal, en el cual también se darán las recomendaciones para poder incrementar la seguridad del servidor y así asegurar las aplicaciones que este comparte.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes

Actualmente el ITSCO no consta con un documento real que acredite la seguridad informática (anti hacking), este proyecto se enfoca en realizar una auditoría general a los filtros de seguridad que existen actualmente en el ITSCO, los cuales se basa en el análisis y la respuesta al problema de la situación actual en la red informática, y así

poder detectar vulnerabilidades tales como la falta de antivirus, poca seguridad en el firewall, el ingreso de usuarios no deseados, no autorizados a nuestra red y así poder tomar las debidas precauciones, para de esta manera evitar ataques informáticos que puedan alterar los sistemas internos del ITSCO.

La seguridad informática consiste en asegurar, que los recursos del sistema de información (material informático o programas), del ITSCO sean utilizados de manera segura y que el acceso o su modificación a través de programas de acceso remoto tales como: SSH, TeamViewer, VNC, sólo sea posible realizarse por las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Para garantizar la seguridad informática se requiere de un conjunto de sistemas, métodos y herramientas destinados a proteger la información, en este punto es donde entran a desempeñar un rol protagónico, los servicios de ethical hacking, disciplina de la seguridad de redes que se sustenta en el hecho de que para estar protegido se debe conocer cómo operan y qué herramientas usan los hackers estas son: Snnifer, Exploits, Backdoors, Footprinting y Tunneling.

Ethical Hacking (hackeo ético) es explorar las vulnerabilidades existentes dentro de una red informática, para verificar y evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos,

servidores, entre otros, con la intención de ganar acceso y "demostrar" que una red puede ser vulnerable.

Estas pruebas dejan al descubierto vulnerabilidades, como falta de implementación de firewalls en la zona fronteriza, ausencia del servidor de antivirus, etc., que pudieran ser vistas y explotadas por individuos no autorizados y ajenos a la información como: crackers, hackers, ladrones, ex-empleados, ex – estudiantes, etc. Las pruebas de penetración, están totalmente relacionadas con el tipo de información que el ITSCO maneja, por tanto según la información que se desee proteger, como el

sistema para el ingreso de notas, servidores de correo, servidores de aplicaciones, etc.

Estas pruebas de penetración permiten:

- Evaluar vulnerabilidades como la ejecución de exploits, snnifers, escaneo de puertos o backdoors, dentro de la zona militarizada, y así poder identificar debilidades provocadas por una mala configuración en las aplicaciones.

Los hackers éticos también conocidos como Pen-Tester, realizan "Pruebas de Penetración", su función es atacar los sistemas de seguridad, con la intención de buscar y encontrar vulnerabilidades que un hacker malicioso podría explotar. Para probar los sistemas de seguridad, los hackers éticos, utilizan los mismos métodos que sus homólogos (hacker malicioso), pero se limitan únicamente a reportarlos en lugar de sacar ventaja de ellos.

2.2 Reseña Histórica

El Instituto Tecnológico Superior Cordillera fue fundado hace 17 años por el Ing. Cristóbal Flores y se encuentra ubicado en la Av. De La Prensa y Logroño, el primer campus fue el edificio de la Av. De La Prensa y Zamora en donde funcionaba el departamento financiero, secretaria, el rectorado y las especialidades de Sistemas,

Diseño y Administración de empresas, luego de un tiempo la infraestructura fue creciendo y se crearon más carreras, como optometría y educación, para lo cual se fundó un nuevo edificio, que se encuentra ubicado en la Av. De La Prensa y Bracomoros, donde actualmente se encuentran los laboratorios de informática para cada una de las diferentes especialidades.

Actualmente el Rector del ITSCO, es el Ing. Ernesto Flores y el director de La Escuela de Sistemas es el Ing. Robert Enríquez.

2.2.1 Misión

A la distancia el ITSCO ve a cada alumno como un caballero y cada alumna una dama, ciudadanos decentes y cabales, con la mirada en el mundo del mañana donde todo está por hacerse y en el que será los profesionales del país que debe ser Ecuador.

2.2.2 Visión

El ITSCO forma profesionales con un perfil de personas cultas, educadas y decentes preparadas moral, científico y técnicamente para afrontar los desafíos de un mundo en constante cambio y asumir la responsabilidad de guiar y salvar a la familia y a la sociedad del caos que amenaza a la humanidad para optar por una vida de dignidad y libertad.

2.3 Marco Referencial

2.3.1 Languard

GFI Languard es una solución de análisis de seguridad de red y gestión de actualizaciones, proporciona una visión completa de la seguridad de la red, con el mínimo esfuerzo administrativo.

Actúa como un consultor virtual para proporcionar una imagen completa de la configuración de red, proporciona análisis de riesgos y ayuda a mantener un estado seguro de la red más rápida y eficazmente. GFI Languard se enfoca en estas importantes áreas:

- Gestión de vulnerabilidad
- Auditoría de red y de software
- Análisis de riesgos y cumplimiento

Gestión de vulnerabilidad

GFI LANguard realiza más de 45.000 comprobaciones en el sistema operativo, entornos virtuales y aplicaciones instaladas utilizando bases de datos de comprobación de vulnerabilidad como OVAL y SANS Top 20. GFI LANguard permite analizar el estado de la seguridad de la red, cuales son los riesgos, cuán expuesta se encuentra y cómo actuar antes de que sea comprometida.

Auditoria de red y Software

La funcionalidad de auditoría de red de GFI LANguard proporciona un análisis detallado de lo que está ocurriendo en la red, qué aplicaciones o configuraciones por defecto suponen un riesgo de seguridad. Con GFI

LANguard, se obtiene una imagen completa de qué aplicaciones están instaladas, el hardware de la red, el estado de las aplicaciones de seguridad (AV, anti-spam, cortafuegos, etc.), qué puertos están abiertos, cualquier recurso compartido existente y servicios en ejecución de los equipos.

Análisis de riesgos y cumplimiento

Los problemas de seguridad se valoran por su nivel de severidad, y se da a cada equipo una valoración de riesgo y vulnerabilidad, de forma que se conocerán dónde están los principales problemas de la red. GFI LANguard proporciona numerosos informes ejecutivos, técnicos y estadísticos que ayudan a comprender lo que está ocurriendo en la red, para priorizar eficazmente las tareas de corrección y para probar, si es necesario, que la red es segura.

2.3.2 Whois

Whois nos permite obtener información acerca de los dominios existentes en la red, es un protocolo TCP basado en preguntas/repuestas que es usado para consultar de una base de datos para determinar el propietario de un nombre de dominio o una dirección IP en Internet.

2.3.3 Nslookup

NSLOOKUP es un comando que puede ser usado tanto en el ambiente Unix como en Windows para buscar la dirección IP del servidor de nombres de dominio de un computador en particular. El nombre nslookup significa "Name Server Lookup".

2.3.4 Traceroute

Es una herramienta de diagnóstico de redes que permite seguir la pista de los paquetes que van desde un *host* (equipo de red) a otro. Se obtiene además una estadística de las velocidades de transmisión de esos paquetes. Esta herramienta se llama *traceroute* en *Unix* y *Linux*, mientras que en *Windows* es conocido como *tracert*.

2.3.5 Visual Route

Esta aplicación comercial ayuda a determinar problemas de conectividad, muestra gráficamente los saltos hacia otras direcciones e indica los tiempos de respuesta en una escala gráfica.

Todas las ediciones de este software comercial contienen: *traceroute* gráfico, pruebas de ping, pruebas de DNS reverso, búsquedas de WHOIS y muestra la ruta y ubicación actual de las conexiones IP en un mapa.

2.3.6 SmartWhois

Esta es una herramienta muy útil que permite buscar toda la información posible de una dirección de Internet, IP o dominio. Esta información puede incluir país, estado o provincia, ciudad, nombre del proveedor de red, administrador y soporte técnico, lo cual permite encontrar respuestas acerca del dueño del dominio, la fecha de registro del dominio, y quién es el dueño del bloque de direcciones IP utilizadas en éste.

2.3.7 eMailTrackerPro

Esta herramienta permite identificar la verdadera fuente de un correo electrónico, para seguir las huellas de un remitente sospechoso y verificar desde donde fue enviado, además *eMailTrackerPro* analiza el encabezado de los *e-mails* que se reciben e informa la dirección IP de la máquina de donde fue enviado el correo y su localización geográfica.

2.3.8 Ping

Es una utilidad que comprueba el estado de la conexión con uno o varios equipos, por medio de los paquetes de solicitud de eco y de respuesta de eco, definidos en el protocolo de red ICMP3 para determinar si un sistema IP específico es accesible en una red.

Es útil para diagnosticar los errores en redes o enrutadores IP, es también utilizado para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos. Ping es uno de los comandos usados para solucionar problemas de accesibilidad, conectividad y resolución básica de nombres de equipos.

2.3.9 Pinger

Esta herramienta es útil para escanear puertos de computadores o cualquier equipo de red que maneje el protocolo TCP/IP. Es utilizado por administradores de red para verificar que los servidores o equipos estén conectados y respondiendo correctamente al comando *ping* en tiempos adecuados. Además permite almacenar un registro (*log*) de cada uno de los equipos a los que se encuentra monitoreando.

2.3.10 WS_Ping ProPack

Este software comercial fue diseñado para ejecutarse en procesadores de tipo Intel y con el sistema operativo *Windows*. *WS_Ping ProPack* es un conjunto de herramientas de información de red que proporciona los elementos necesarios para realizar un seguimiento de los problemas de red, obteniendo información acerca de usuarios, *hosts* y redes en Internet (o en una intranet).

2.3.11 IPSecScan

IPSecScan es una herramienta capaz de realizar un *scanning* de una dirección IP o un rango de direcciones en búsqueda de equipos que tengan habilitado IPSec

2.3.12 NetScanTools Pro

NetScanTools Pro es un conjunto de utilitarios reunidos en una sola aplicación, este software es usado para: determinar la pertenencia de direcciones IP y dominios, traducir una dirección IP a un nombre de equipo, realizar pruebas de puertos en búsqueda de servicios, validar direcciones de correo, listar los equipos de un dominio, entre otras.

2.3.13 SuperScan

SuperScan es un potente escáner de puertos; permite realizar algunos tipos de operaciones de escaneo, usando una IP o tomando las direcciones IP de un archivo dado. Es capaz de realizar conexiones a cualquier tipo de puerto que se descubra, usando aplicaciones apropiadas (*Telnet*, FTP, Web), además

realiza *pings* y resuelve nombres de dominio. Algunos antivirus lo catalogan como un software mal intencionado y lo eliminan.

2.3.14 NMap (Network Mapper)

Nmap es una utilidad para explorar redes extensas, aunque también funciona en un único equipo; además, permite explorar diferentes protocolos, como

UDP, TCP, ICMP, sin necesidad de tener algunos exploradores de puertos con diferentes interfaces y características.

2.3.15 Nessus, NeWT (Nessus Windows Technology)

Nessus es uno de los más populares buscadores de vulnerabilidades, escanea puertos con *NMap* o con su propio escaneador de puertos, para buscar puertos abiertos y después intentar varios *exploits* para atacarlos. Los resultados del escaneo pueden ser exportados en reportes en varios formatos, como: texto plano, XML y HTML. Los resultados también pueden ser guardados en una base de datos SQL (local o remota) para tener una referencia en futuros escaneos de vulnerabilidades.

2.3.16 SAINT (Security Administrator's Integrated Network Tool)

Esta herramienta es utilizada para detectar vulnerabilidades en cualquier equipo remoto, incluyendo servidores, estaciones de trabajo, equipos de red y cualquier otro tipo de nodo, obteniendo información del sistema que está corriendo en el nodo y de los puertos abiertos. El modo gráfico de este software provee acceso a la administración de la información obtenida, a través de configuraciones y programación de búsquedas por medio de un explorador Web.

2.3.17 ISS Scanner (Internet Security Systems Scanner)

Este escáner puede identificar más de 1300 tipos de equipos conectados a la red, incluyendo equipos de usuarios, servidores, *switches, firewalls*, dispositivos de seguridad y enrutadores.

Una vez que los dispositivos conectados a la red son identificados, se analiza: sus configuraciones, parches instalados, sistemas operativos y aplicaciones

instaladas para encontrar vulnerabilidades que pudieran ser explotadas por los *hackers* criminales, al intentar obtener acceso no autorizado.

2.3.18 NetRecon

Es una herramienta de valoración de la vulnerabilidad de las redes que encuentra, analiza e informa los huecos en la seguridad, mediante la exploración y sondeo de los sistemas y servicios de la red. Reproduce las situaciones de agresión o intrusión habituales para identificar e informar sobre los puntos vulnerables de la red, al mismo tiempo que propone medidas para corregirlos. Los administradores pueden programar exploraciones desde una interfaz fácil de utilizar y visualizar su avance y los resultados inmediatamente en una presentación gráfica en tiempo real.

2.3.19 Retina

Este programa permite identificar vulnerabilidades de seguridad, administración de parches, y administración de políticas; descubre toda clase de dispositivos de red, sistemas operativos, aplicaciones, parches instalados y configuración de políticas. Se trata de una herramienta relativamente rápida, ya que escanea una red de equipos de una organización identificando sistemas operativos y aplicaciones en alrededor de 15 minutos.

2.3.20 NMapWin

Esta es otra de las herramientas catalogadas como Virus informáticos por algunos fabricantes de antivirus. Se trata de una aplicación en modo gráfico para utilizar la herramienta *NMap*.

2.3.21 Userinfo

Userinfo es una pequeña utilidad de consola de *Linux* que muestra información adicional sobre los usuarios del sistema, está formada por un conjunto de pequeños sub-programas.

2.3.22 GetAcct

Es una aplicación sencilla que permite obtener información privilegiada acerca de todas las cuentas de usuario en los equipos que utilizan el sistema operativo *Windows*.

2.3.23 IP Network Browser

Este software es una herramienta para descubrimiento de subredes IP por medio de ICMP, DNS, y SNMP; de esta forma construye un árbol de todos los dispositivos que responden a las consultas. La información de los sistemas descubierta incluye: información de MIBs, información de interfaces y memoria disponible, estado operativo, tablas ARP y de rutas, direcciones MAC, información TCP/IP, servicios UDP, conexiones TCP, entre otras.

2.3.24 Vulnerabilidad

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

Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales (conocidas como exploits).

2.3.25 Bugs

Un bug es un error o un defecto en el software o hardware que hace que un programa funcione incorrectamente, dicho fallo puede presentarse en cualquiera de las etapas del ciclo de vida del software aunque los más evidentes se dan en la etapa de desarrollo y programación.

2.3.26 Spoofing

Hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación, se pueden clasificar los ataques de *spoofing*, en función de la tecnología utilizada. Entre ellos tenemos el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o email spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

2.3.27 Threats

Es una acción o evento que puede perjudicar a la seguridad, se trata de un indicador de intento de causar daños e interrupciones en un sistema informático.

2.3.28 Red Lan

Una red de área local, es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc.

2.3.29 Red Wan

Una red de área amplia, con frecuencia denominada WAN, acrónimo de la expresión en idioma inglés wide area network, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros.

Hoy en día, Internet proporciona WAN de alta velocidad, y la necesidad de redes privadas WAN se ha reducido drásticamente, mientras que las redes privadas virtuales que utilizan cifrado y otras técnicas para hacer esa red dedicada, aumentan continuamente.

Normalmente la WAN es una red punto a punto, es decir, red de paquete conmutado. Las redes WAN pueden usar sistemas de comunicación vía satélite o de radio. Fue la aparición de los portátiles y los PDA la que trajo el concepto de redes inalámbricas.

2.3.30 Intranet

Una intranet es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales. El término intranet se utiliza en oposición a Internet, una red entre organizaciones, haciendo referencia por el contrario a una red comprendida en el ámbito de una organización.

2.3.31 Dirección Ip

Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del protocolo TCP/IP. Dicho número no se ha de confundir con la dirección MAC que es un identificador de 48bits para identificar de forma única a la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP, decida asignar otra IP (por ejemplo, con el protocolo DHCP), a esta forma de asignación de dirección IP se denomina *dirección IP dinámica* (normalmente abreviado como *IP dinámica*).

2.3.32 TCP

Transmission Control Protocol (en español *Protocolo de Control de Transmisión*) o TCP, es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn.

Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear *conexiones* entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

TCP da soporte a muchas de las aplicaciones más populares de Internet (navegadores, intercambio de ficheros, clientes ftp,...) y protocolos de aplicación HTTP, SMTP, SSH y FTP.

2.3.33 UDP

User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Paquete de datos). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la

información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

2.3.34 ICMP

El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de *Internet Control Message Protocol*) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un Router o host no puede ser localizado.

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta ping y traceroute, que envían mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa.

2.3.35 Dirección MAC

En las redes de computadoras, la **dirección MAC** (siglas en inglés de *media access control*; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como **dirección física**, y es

única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el *organizationallyuniqueidentifier*. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64, las cuales han sido diseñadas para ser

identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

2.3.36 Dns

DomainNameSystem o DNS (en castellano: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

2.3.37 Servidor Web

Un servidor web o servidor HTTP es un programa que procesa cualquier aplicación del lado del servidor realizando conexiones bidireccionales y/o unidireccionales y síncronas o asíncronas con el cliente generando o cediendo una respuesta en cualquier lenguaje o Aplicación del lado del cliente. El código

recibido por el cliente suele ser compilado y ejecutado por un navegador web. Para la transmisión de todos estos datos suele utilizarse algún protocolo. Generalmente se utiliza el protocolo HTTP para estas comunicaciones, perteneciente a la capa de aplicación del modelo OSI. El término también se emplea para referirse al ordenador que ejecuta el programa.

2.3.38 Servidor de Correo

Un servidor de correo es una aplicación informática ubicada en una página web en internet cuya función es parecida al Correo postal solo que en este caso los correos (otras veces llamados mensajes) que circulan, lo hacen a través de nuestras Redes de transmisión de datos y a diferencia del correo postal, por este medio solo se pueden enviar adjuntos de ficheros de cualquier extensión y no bultos o paquetes al viajar la información en formato electrónico.

2.3.39 DMZ

En seguridad informática, una zona desmilitarizada (DMZ, demilitarizedzone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén

permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona

desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.

2.3.40 Sistema Operativo

Un sistema operativo (SO) es el programa o conjunto de programas que efectúan la gestión de los procesos básicos de un sistema informático, y permite la normal ejecución del resto de las operaciones.

Es un error común muy extendido denominar al conjunto completo de herramientas sistema operativo, es decir, la inclusión en el mismo término de programas como el explorador de ficheros, el navegador y todo tipo de herramientas que permiten la interacción con el sistema operativo, también llamado núcleo o kernel. Uno de los más prominentes ejemplos de esta diferencia, es el núcleo Linux, que es el núcleo del sistema operativo GNU, del cual existen las llamadas distribuciones GNU. Este error de precisión, se debe a la modernización de la informática llevada a cabo a finales de los 80, cuando la filosofía de estructura básica de funcionamiento de los grandes

computadores se rediseñó a fin de llevarla a los hogares y facilitar su uso, cambiando el concepto de computador multiusuario, (muchos usuarios al mismo tiempo) por un sistema monousuario (únicamente un usuario al mismo tiempo) más sencillo de gestionar.

Uno de los propósitos del sistema operativo que gestiona el núcleo intermediario consiste en gestionar los recursos de localización y protección de acceso del hardware, hecho que alivia a los programadores de aplicaciones de tener que tratar con estos detalles. La mayoría de aparatos electrónicos que utilizan microprocesadores para funcionar, llevan incorporado un sistema operativo. (Teléfonos móviles, reproductores de DVD, computadoras, radios, enrutadores, etc.).

2.3.41 Microsoft Windows

Microsoft Windows es el nombre de una familia de sistemas operativos desarrollados por Microsoft desde 1981, año en que el proyecto se denominaba *Interface Manager*

Anunciado en 1983, Microsoft comercializó por primera vez el entorno operativo denominado *Windows* en noviembre de 1985 como complemento para MS-DOS, en respuesta al creciente interés del mercado en una interfaz gráfica de usuario (GUI). Microsoft Windows llegó a dominar el mercado de ordenadores personales del mundo, superando a Mac OS, el cual había sido introducido previamente a Windows. En octubre de 2009, Windows tenía aproximadamente el 91% de la cuota de mercado de sistemas operativos en equipos cliente que acceden a Internet. Las versiones más recientes de

Windows son; Windows 7 para equipos de escritorio, Windows Server 2008 R2 para servidores y Windows Phone 7 para dispositivos móviles.

2.3.42 Linux

GNU/Linux es uno de los términos empleados para referirse a la combinación del núcleo o *kernel* libre similar a Unix denominado Linux, que es usado con herramientas de sistema GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU, *en inglés: General Public License*) y otra serie de licencias libres.

A pesar de que Linux es, en sentido estricto, el sistema operativo, parte fundamental de la interacción entre el núcleo y el usuario (o los programas de aplicación) se maneja usualmente con las herramientas del proyecto GNU o de otros proyectos como GNOME. Sin embargo, una parte significativa de la comunidad, así como muchos medios generales y especializados, prefieren utilizar el término *Linux* para referirse a la unión de ambos proyectos.

A las variantes de esta unión de programas y tecnologías, a las que se les adicionan diversos programas de aplicación de propósitos específicos o generales se las denomina distribuciones. Su objetivo consiste en ofrecer ediciones que cumplan con las necesidades de un determinado grupo de usuarios. Algunas de ellas son especialmente conocidas por su uso en servidores y supercomputadoras, donde tiene la cuota más importante del mercado. Según un informe de IDC, GNU/Linux es utilizado por el 78% de los principales 500 servidores del mundo, otro informe le da una cuota de mercado del 89 % en los 500 mayores supercomputadores. Con menor cuota de mercado el sistema GNU/Linux también es usado en el segmento de las

computadoras de escritorio, portátiles, computadoras de bolsillo, teléfonos móviles, sistemas embebidos, videoconsolas y otros dispositivos.

2.3.43 Internet

Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión.

2.3.44 ISP

Un proveedor de servicios de Internet (o ISP, por la sigla en inglés de *Internet ServiceProvider*) es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cable módem, GSM, Dial-up, Wifi, entre otros. Muchos ISP también

ofrecen servicios relacionados con Internet, como el correo electrónico, alojamiento web, registro de dominios, servidores de noticias, etc.

2.3.45 Tarjeta de Red

Una tarjeta de red o adaptador de red permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras (discos duros, CD-ROM, impresoras, etc.). A las tarjetas de red también se les llama NIC (por *network interface card*; en español "tarjeta de interfaz de red"). Hay diversos tipos de adaptadores en función del tipo de cableado o arquitectura que se utilice en la red (coaxial fino, coaxial grueso, Token Ring, etc.), pero actualmente el más común es del tipo Ethernet utilizando una interfaz o conector RJ-45.

2.3.46 Access Point

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta medios de comunicación wireless para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

2.3.47 Router

El enrutador (calco del inglés router), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red) del modelo OSI. Un enrutador es un

dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.

2.3.48 Firewall

Un cortafuegos (firewall en inglés), es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red, llamada Zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente.

2.3.49 Servidor

Un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Un servidor también puede ser un proceso que entrega información o sirve a otro proceso. El modelo Cliente-servidor no necesariamente implica tener dos ordenadores, ya que un proceso cliente puede solicitar algo como una impresión a un proceso servidor en un mismo ordenador.

2.3.50 Cliente

El **cliente** es una aplicación informática o un computador que accede a un servicio remoto en otro computador, conocido como servidor, normalmente a través de una red de telecomunicaciones.

El término se usó inicialmente para los llamados terminales tontos, dispositivos que no eran capaces de ejecutar programas por sí mismos, pero podían conectarse e interactuar con computadores remotos por medio de una red y dejar que éste realizase todas las operaciones requeridas, mostrando luego los resultados al usuario. Se utilizaban sobre todo porque su coste en esos momentos era mucho menor que el de un computador. Estos terminales tontos eran clientes de un computador mainframe por medio del tiempo compartido.

2.3.51 Hacker

Los términos *hacker* y *hack* tienen connotaciones positivas e, irónicamente, también negativas. Los programadores informáticos suelen usar las *hacking* y

hacker para expresar admiración por el trabajo de un desarrollador de software cualificado, pero también se puede utilizar en un sentido negativo para describir una solución rápida pero poco elegante a un problema. Algunos desaprueban el uso del *hacking* como un sinónimo de cracker, en marcado contraste con el resto del mundo, en el que la palabra hacker se utiliza normalmente para describir a alguien que "hackea" un sistema con el fin de eludir o desactivar las medidas de seguridad.

2.3.52 Cracker

El término cracker (del inglés crack, romper) se utiliza para referirse a las personas que rompen algún sistema de seguridad, normalmente estos individuos se encargan de destruir sistemas informáticos, a través de software malintencionado.

2.3.53 Phreaker

De phone freak ("monstruo telefónico"). Son personas con conocimientos amplios tanto en teléfonos modulares (TM) como en teléfonos móviles.

2.3.54 Lammer

Es un término coloquial inglés aplicado a una persona falta de madurez, sociabilidad y habilidades técnicas o inteligencia, un incompetente, que por lo

general pretenden hacer hacking sin tener conocimientos de informática. Solo se dedican a buscar y descargar programas de hacking para luego ejecutarlos, como resultado de la ejecución de los programas descargados estos pueden

terminar colapsando sus sistemas por lo que en general acaban destrozando la plataforma en la que trabajan.

2.3.55 WEP

Acrónimo de ***Wired Equivalent Privacy*** o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

2.3.56 WPA

WPA (*Wi-Fi Protected Access*, Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado). Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue

creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).

2.3.57 WPA2

WPA2 (*Wi-Fi Protected Access 2* - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA.

WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

El estándar 802.11i fue ratificado en junio de 2004, la alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise, los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard).

2.3.58 RC4

Dentro de la criptografía RC4 o ARC4 es el sistema de cifrado de flujo *Stream cipher* más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes

inalámbricas). RC4 fue excluido enseguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

2.3.59 IEEE 802.11

El estándar '*IEEE 802.11*' define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

Wifi N o 802.11n: En la actualidad la mayoría de productos son de la especificación b o g, sin embargo ya se ha ratificado el estándar 802.11n que sube el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen el estándar N con un máximo de 300 Mbps (80-100 estables).

El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 GHz y 5,4 GHz. Las redes que trabajan bajo los estándares 802.11b y 802.11g, tras la reciente ratificación del estándar, se empiezan a fabricar de forma masiva y es objeto de promociones por parte de los distintos ISP, de forma que la masificación de la citada tecnología parece estar en camino. Todas las versiones de 802.11xx, aportan la ventaja de ser compatibles entre sí, de forma que el usuario no necesitará nada más que su adaptador Wifi integrado, para poder conectarse a la red.

2.3.60 Snnifer

Un sniffer es un programa de para monitorear y analizar el tráfico en una red de computadoras, detectando los cuellos de botellas y problemas que existan en ella.

Un sniffer puede ser utilizado para "captar", lícitamente o no, los datos que son transmitidos en la red. Un ruteador lee cada paquete de datos que pasa por él, determina de manera intencional el destino del paquete dentro de la red. Un ruteador y un sniffer, pueden leer los datos dentro del paquete así como la dirección de destino.

2.3.61 Exploit

Exploit (del inglés to exploit, explotar o aprovechar) es una pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado). Con frecuencia, esto incluye cosas tales como la violenta toma de control de un sistema de cómputo o permitir la escalada de privilegios o un ataque de denegación de servicio

El fin del Exploit puede ser violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.

2.3.62 Backdoor

En la informática, una puerta trasera (o en inglés backdoor); en un sistema informático es una secuencia especial dentro del código de programación mediante la cual se puede evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema. Aunque estas puertas pueden ser utilizadas para fines maliciosos y espionaje no siempre son un error, pueden haber sido diseñadas con la intención de tener una entrada secreta.

2.3.63 Footprinting

Se le llama footprinting a la técnica utilizada para recopilar datos relevantes del objetivo a analizar con el fin de realizar un ataque.
Por ejemplo nombres, teléfonos, ips, contactos, usuarios, etc.
Se ocupan herramientas como ping, whois, tracert además de datos que se encuentran en Páginas Web, chat, diarios, etc.

2.3.64 Scanning

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

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

utilizado por usuarios malintencionados que intentan comprometer la seguridad de la máquina o la red.

2.3.65 Google Hacking

El *Google Hacking* consiste en explotar la gran capacidad de almacenamiento de información de Google, buscando información específica que ha sido añadida a las bases de datos del buscador. Si las búsquedas las orientamos a ciertas palabras clave que nos ayuden a encontrar información sensible o puntos de entrada a posibles ataques, este o cualquier otro tipo de información que tuviera carácter de sensibilidad, estaremos ejecutando un *Google hack*.

2.3.66 SQL Injection

Es un método de infiltración de código intruso, que se vale de una vulnerabilidad informática presente en una aplicación, en el nivel de validación de las entradas para realizar consultas a una base de datos.

El origen de la vulnerabilidad radica en el incorrecto chequeo y/o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que esté embebido dentro de otro.

Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado.

2.3.67 Denegación de Servicio

En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le denomina "denegación", pues hace que el servidor no dé abasto a la cantidad de solicitudes. Esta técnica es usada por los llamados Crackers para dejar fuera de servicio a servidores objetivo.

Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS (de las siglas en inglés Distributed Denial of Service) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

La forma más común de realizar un DDoS es a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz por su sencillez tecnológica.

En ocasiones, esta herramienta ha sido utilizada como un buen método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y afectar a los servicios que presta. Un administrador de redes puede así conocer la capacidad real de cada máquina.

2.3.68 Botnet

Es un término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet (llamado pastor) puede controlar todos los ordenadores/servidores infectados de forma remota y normalmente lo hace a través del IRC. Las nuevas versiones de estas botnets se están enfocando hacia entornos de control mediante HTTP, con lo que el control de estas máquinas será mucho más simple. Sus fines normalmente son poco éticos.

2.3.69 Telnet

(TELecommunication NETwork) es el nombre de un protocolo que sirve para acceder mediante una red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

2.3.70 SSH

SSH (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

2.3.71 Malware

Malware (del inglés *malicious software*), también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático es utilizado en muchas ocasiones de forma incorrecta para referirse a todos los tipos de malware, incluyendo los verdaderos virus.

2.3.72 Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador), creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU, con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

2.3.73 IDS

Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

2.3.74 Honeypot

Se denomina *honeypot* al software o conjunto de computadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para

recoger información sobre los atacantes y sus técnicas. Los *honeypots* pueden distraer a los atacantes de las máquinas más importantes del sistema y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al *honeypot*.

2.3.75 Hash

Se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una *función hash* o *algoritmo hash*.

2.3.76 Troyano

Los troyanos son programas que aparentan cumplir con una función, pero cuando son ejecutados, se ejecuta también alguna actividad maliciosa, un usuario puede pensar que el archivo es inofensivo para ejecutarlo, pero después que el archivo es ejecutado, libera su carga maliciosa para comprometer al sistema.

2.4 Marco Legal

En la realización de este proyecto interfieren las siguientes leyes:

- La ley de Educación Superior.
- La ley del derecho de autor.

Art. 2. Los derechos conferidos por esta Ley se aplican por igual a nacionales y extranjeros, domiciliados o no en el Ecuador

Art. 5. El derecho de autor nace y se protege por el solo hecho de la creación de la obra, independientemente de su mérito, destino o modo de expresión.

Art. 8. La protección del derecho de autor recae sobre todas las obras del ingenio, en el ámbito literario o artístico, cualquiera que sea su género, forma de expresión, mérito o finalidad. Los derechos reconocidos por el presente título son independientes de la propiedad del objeto material en el cual está incorporada la obra y su goce o ejercicio no están supeditados al requisito del registro o al cumplimiento de cualquier otra formalidad.

CAPITULO III

INVESTIGACION CIENTIFICA

3.1 Tipos de Investigación

3.1.1 Investigación de Campo

3.1.1.1 Descriptiva

Esta investigación es de utilidad en este proyecto para la búsqueda de soluciones, iniciando con la estructuración de explicaciones lógicas y definidas al árbol de problemas, a fin de poder encontrar las causas que originaron los distintos eventos y estos a su vez desencadenaron la problemática general; cabe recalcar que el enfoque general de un hacking ético, presenta condiciones y características reales, las mismas que pueden medirse y cuantificarse en cualquier momento, la utilización del análisis y síntesis en este proyecto, permitirá que los procedimientos enmarcados tengan una correcta descripción y sincronización con el resto de elementos que se tendrán que realizar en el desarrollo del documento de hacking ético.

3.1.1.2 Explicativa

Con esta investigación, podemos analizar la situación actual, para saber las causas que originan el problema, como la falta de firewall, antivirus, etc., y como esto podría afectar en el futuro a las aplicaciones informáticas del ITSCO, como el sistema para ingreso de notas, servidores de antivirus, servidores de internet, etc.

3.1.1.3 Exploratoria

Se utiliza para este proyecto ya que toda investigación de campo empieza siendo exploratoria debido al necesario e ineludible primer contacto con la

realidad, para esto realizamos un análisis de la vulnerabilidad actual, dentro del segmento de la red informática y de esta forma podemos llevar a cabo las medidas necesarias, para incrementar la seguridad de la zona fronteriza.

3.1.2 Investigación Bibliográfica Documental

Con este tipo de investigación podremos analizar la información existente para el desarrollo del proyecto. Se indagara en los procedimientos a seguir para la realización de un hacking ético, partiendo de pruebas ya realizadas, para auditar la seguridad actual de la red el ITSCO.

Podremos recopilar la mayor información mediante tutoriales, foros, páginas web, para capacitarnos en las diferentes herramientas a utilizar en el desarrollo del proyecto tales como pruebas de seguridad, test de penetración, etc.

3.2 Métodos De Investigación

3.2.1 Método Inductivo.

El método inductivo es un método científico que obtiene conclusiones generales a partir de premisas particulares. Se caracteriza por cuatro etapas básicas: la observación y el registro de todos los hechos: el análisis y la clasificación de los hechos; la derivación inductiva de una generación a partir de los hechos; y la contrastación.

Este proyecto utilizará este método para la realización de los siguientes temas:

- Realizar un análisis de la situación actual en el servidor del ITSCO, con la ejecución de herramientas como un Snnifer para saber la estructura y los

posibles fallos para ingresar, a través de un escaneo de puertos para saber cuáles se encuentran abiertos.

- Investigar los firewalls, dentro de la zona militarizada para saber si se encuentran aptos para boquear una intrusión desde la zona desmilitarizada, testear al software antivirus, para medir su capacidad de respuesta frente a una amenaza, como un software con código malicioso, como pueden ser un virus, un troyano o un malware.

3.2.2 Método Deductivo.

El método deductivo es un método científico que considera que la conclusión está implícita en las premisas. Por lo tanto, supone que las conclusiones sigue necesariamente a las premisas: si el razonamiento deductivo es válido y las premisas son verdaderas, la conclusión sólo puede ser verdadera.

En este proyecto utilizaremos este método para la realización de los siguientes temas:

- Análisis de la estructura actual de la red informática, como tecnología utilizada, que tipo de red se está usando, fibra óptica, wireless, etc., que tipo de servidores se encuentran protegiendo la frontera, tipo RISC, CISC o híbridos.
- Estructura actual de la seguridad, para el acceso a las aplicaciones internas del ITSCO, como son correo, internet, Wifi, ingreso al sistema de notas, que tipo de encriptación o contraseñas seguras son las que se está utilizando para el acceso seguro de cada usuario.

3.2.3 Método Analítico Sintético

El análisis y la síntesis son procesos mentales, el primero permite descomponer un todo en sus partes, de esta manera podemos partir del tema general que se refiere a la falta de seguridad dentro de la red informática, y analizar cada uno de los problemas, como la falta de herramientas de seguridad, antivirus o firewalls y el segundo integrar las partes para formar un todo.

3.2.4 Método Hipotético – Deductivo

Este método se utiliza en el proyecto, ya que posibilita el surgimiento de nuevos conocimientos a través de otros establecidos, estos son mediante los test de intrusión, como footprinting, scanning, etc., para poder deducir las posibles vulnerabilidades dentro de la zona militarizada de la red del ITSCO.

3.3 Técnicas de recolección de la información

3.3.1 Observación

Se utilizará esta técnica, para poder observar las condiciones actuales de seguridad y las herramientas que se están empleando, para evitar ataques informáticos, ya sea desde dentro o fuera de la red informática del ITSCO.

3.3.2 Entrevista

Se desarrollaran entrevistas a los encargados de la seguridad de la red, con el objetivo de conocer necesidades en cuanto a la seguridad dentro de la zona

militarizada, se podrá también conocer que tipos de ataques han recibido anteriormente, debido a vulnerabilidades y que medidas han tomado en contra de estos ataques.

Las preguntas que se usaron en la entrevista, fueron las siguientes:

1. ¿Qué tipo de servidores para las aplicaciones y seguridad se está usando actualmente en el ITSCO?
2. ¿Qué tipo de software antivirus se encuentra actualmente en los servidores?
3. ¿Qué herramientas se están usando actualmente para ataques externos a la red?
4. ¿De qué forma se está protegiendo la integridad de los datos frente a usuarios internos?
5. ¿Qué tipo de herramientas anti hacking se están ejecutando o con qué frecuencia se utilizan?
6. ¿La complejidad de las contraseñas son las recomendadas para las aplicaciones internas?
7. ¿Han tenido anteriormente ataques por parte de hackers en alguna de las aplicaciones?
8. ¿Se realizan respaldos de la información sensible en caso de ser víctimas de ataques por parte de hackers?
9. ¿Qué tipo de seguridad se utiliza para el acceso inalámbrico a la red wi-fi?
10. ¿Se ha realizado anteriormente un documento sobre hacking ético dentro de la red informática?

Las respuestas a la encuesta fueron las siguientes:

1. Los servidores que se están utilizando son de marca HP DL-360 G6, con sistema operativo Linux Cent.
2. Actualmente no se tiene un software antivirus.

3. Las herramientas que se están usando actualmente para ataques externos a la red, son un Firewall.
4. La integridad de los datos, está siendo protegida por contraseñas que son asignadas solo a los administradores de la red.
5. Actualmente no se utilizan herramientas anti-hacking, más que la seguridad propia de un firewall.
6. Si es la adecuada, consta de números, letras y caracteres alfanuméricos.
7. Si se ha tenido ataques por parte de hackers anteriormente.
8. Si, toda la información se respalda cierto intervalo de tiempo, en este respaldo se incluyen bases de datos, documentos y configuraciones de las estaciones de trabajo y servidores.
9. El tipo de seguridad que se utiliza para el acceso inalámbrico a la red wi-fi son: Contraseñas (WEP) y Filtrado de direcciones MAC.
10. No se ha realizado un documento sobre Hacking Etico en el ITSCO.

Análisis:

1. Actualmente la infraestructura de hardware y software en los equipos es casi la adecuada, se utilizan servidores y Sistemas Operativos exclusivamente para servidores, mas no se cuenta de manera total con servidores de seguridad o antivirus.
2. La utilización de un software antivirus nos brinda seguridad en contra de virus o programas con código malicioso, protegería la información de usuarios internos que posean medios extraíbles con virus.
3. Estas soluciones nos darán una estabilidad en la seguridad fronteriza, ya que el software antivirus asegura la zona militarizada y el firewall ayudaría para proteger la zona desmilitarizada y evitar ataques externos hacia la red interna.

4. Al asignar contraseñas solo a los administradores, se tiene más seguridad y menos posibilidades de ingresos no autorizados, que puedan poner en riesgo la información sensible en los servidores de aplicaciones.
5. Al no utilizar herramientas anti hacking no se puede establecer vulnerabilidades como puertos abiertos o backdoors, los cuales podrían ser utilizados para ingresos no autorizados a los sistemas informáticos.
6. Al cumplir estándares de seguridad en cuanto a longitud y formato de las contraseñas, se reduce el riesgo de ingresos no autorizados.
7. Se deben tomar las medidas de seguridad necesarias, para no tener inconvenientes dentro de la zona fronteriza y poner en riesgo la información de los servidores, si se realiza un ataque de los hackers
8. Al realizar respaldos de la información sensible, como configuraciones de los servidores, se pueden restablecer de manera rápida, en caso de un ataque externo, sin tener que detener sus aplicaciones y retrasar el trabajo de la Institución.
9. Esta seguridad se encuentra dentro de las recomendaciones para proteger el acceso no autorizado a la red wi-fi.
10. Las pruebas de vulnerabilidades sobre la situación actual de la red, servirán para poder recomendar herramientas y métodos en los cuales, la información y la estabilidad de la zona militarizada, se encontraran más protegidas.

CAPITULO IV

DESARROLLO DE LA PROPUESTA

4.1 Estructura Organizacional

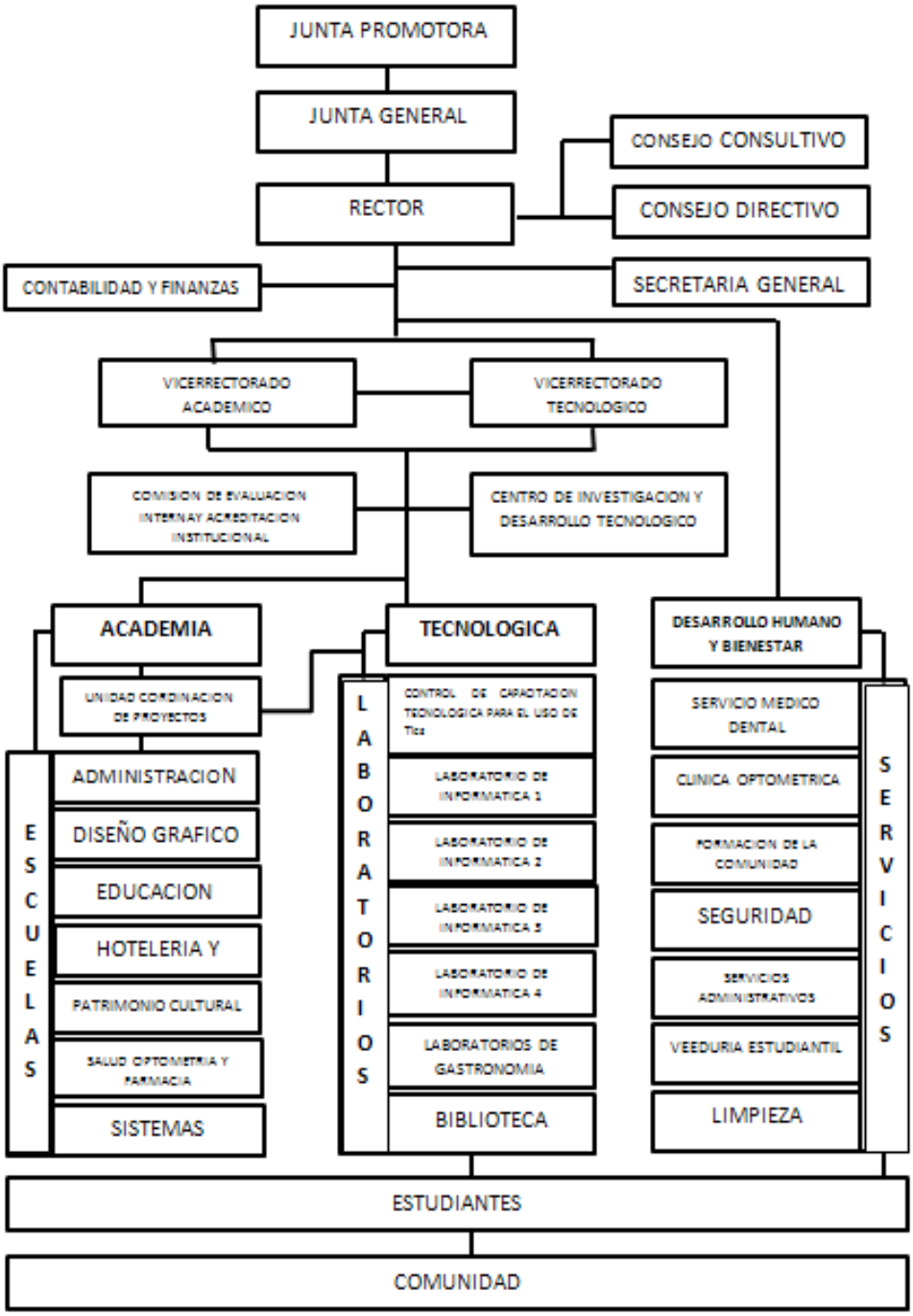


FIGURA 4-1: ESTRUCTURA ORGANIZACIONAL

4.2 Infraestructura Informática

La estructura informática de la red del ITSCO se encuentra de la siguiente manera:

Hardware	Arquitectura
2 Servidores DL360 G6	Servidores de tipo CISC
2 Servidores HP Proliant	Servidores de tipo CISC

TABLA 4-1: INFRAESTRUCTURA DE HARDWARE

Software	Tipo de Sistema Operativo
Sistema Operativo CENT	Sistema Operativo servidor
Windows Server 2008	Sistema Operativo servidor

TABLA 4-2: INFRAESTRUCTURA DE SOFTWARE

Comunicaciones	Descripción
Red Lan	Cable Utp y conectores Rj45
Red Wireless	Tarjetas Wireless y Access Point
Fibra Óptica	Bandeja de Fibra Óptica

TABLA 4-3: INFRAESTRUCTURA DE COMUNICACIONES

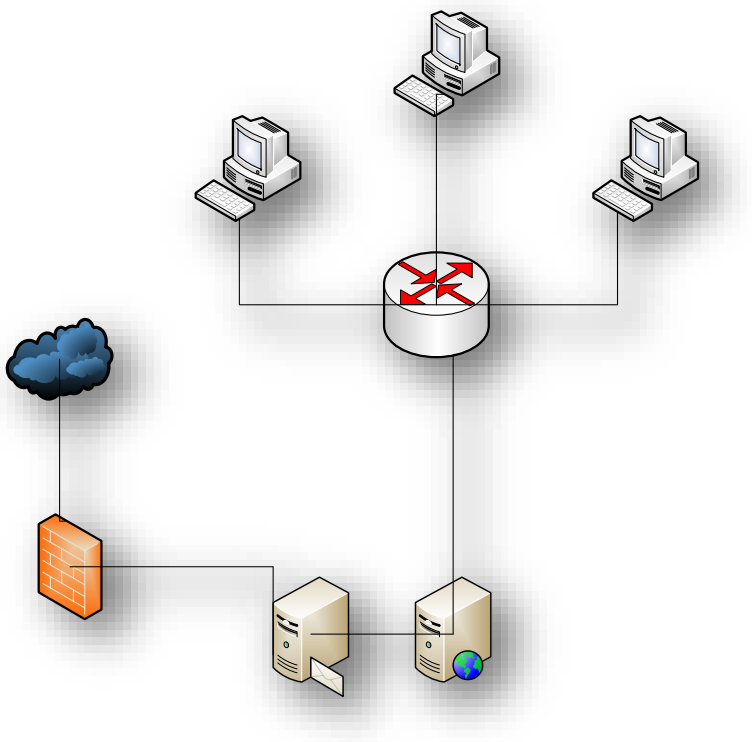


FIGURA 4-2: DIAGRAMA DE LA RED

Recurso Humano Técnico	
Ing. Octavio Cóndor	
Ing. Robert Enríquez	

Ing. Jorge Tatayo	

TABLA 4-4: RECURSO HUMANO TECNICO

4.3 Descripción de las Alternativas

Con la finalidad de poder evaluar las diferentes alternativas que se han presentado por parte de las empresas que ofrecen servicios de hacking ético y por el proyecto de desarrollo a fin de estandarizar cada uno de los ítems; se ha desarrollado especificaciones técnicas que cumpla con los requerimientos y objetivos planteados en el tema de proyecto, a su vez estos puedan ofrecer alternativas de solución técnicas y económicamente aplicables a las necesidades.

Alternativa 1: Empresa SAYO

Actividades	Cumple	No Cumple
Test de penetración	X	
Test de Software Antivirus	X	
Test de Firewall	X	

TIEMPO	COSTO	GARANTIA	SOPORTE	ENTREGA
2 semanas	600	Limitada	8X5	1 semana

TABLA 4-5: ALTERNATIVA 1

Alternativa 2: Empresa Applicalia

Actividades	Cumple	No Cumple
Test de penetración	X	
Test de Software Antivirus	X	
Test de Firewall	X	

TIEMPO	COSTO	GARANTIA	SOPORTE	ENTREGA
8 días	400	Limitada	8X6	8 días

TABLA 4-6: ALTERNATIVA 2

Alternativa 3: Propuesta de Grado

Actividades	Cumple	No Cumple

Test de penetración	X	
Test de Software Antivirus	X	
Test de Firewall	X	

TIEMPO	COSTO	GARANTIA	SOPORTE	ENTREGA
2 Meses	$ 200 (gastos personales)	Limitada	8X5	Septiembre 2011

TABLA 4-7: PROPUESTA DE GRADO

4.4 Evaluación y Selección de Alternativas

De acuerdo a las alternativas planteadas, realizaremos comparaciones porcentuales con la finalidad de calificar a cada una y tener una guía de cómo trabaja, para ello se ha determinado parámetros y porcentajes de acuerdo a la importancia en la realización del documento de Hacking Ético, la clasificación se encuentra de la siguiente manera:

Evaluación Técnica 70%

Evaluación Económica 20%

Garantía Técnica 5 %

Soporte Técnico 5%

Evaluación Técnica

Empresa	Puntos Técnicos	%
SAYO	9	40
APLICALIA	8	55
Proyecto de Grado	10	70

TABLA 4-8: EVALUACION TECNICA

Evaluación Económica

Costo económico	Costo	%
SAYO	600	10
APLICALIA	400	15
Proyecto de Grado	0	20

TABLA 4-9: EVALUACION ECONÓMICA

Evaluación Garantía Técnica

Garantía Técnica	Garantía/ Técnica	%
SAYO	Limitada	3
APLICALIA	Limitada	3
Proyecto de Grado	3 Meses	5

TABLA 4-10: EVALUACION GARANTIA TECNICA

Soporte Técnico

Empresas	Horario	%
SAYO	8 X 5	3
APLICALIA	8 X 6	5
Proyecto de Grado	8 X 6	5

TABLA 4-11: SOPORTE TECNICO

4.5 Factibilidad Técnica

De acuerdo a la comparativa y a la evaluación porcentual, podemos deducir que el Proyecto de Grado es la opción más conveniente, es la mejor en cuanto a la parte Técnica, Económica, Garantía y Soporte.

La misma establece que el aspecto técnico es la principal para poder realizar una calificación coherente y aceptada, por otra parte el aspecto económico favorece la ejecución del proyecto, igual tratamiento nos indica lo referente al soporte técnico y garantía técnica, por consiguiente es factible la realización del proyecto con la alternativa de desarrollo propio, lo que implica que su soporte y ejecución será estrictamente con apoyo de la Institución en todos los géneros que se puedan realizar (técnico, económico).

4.6 Objetivos de la Metodología

El método propuesto tiene como uno de sus principales objetivos la disminución del riesgo asumido por la Institución en lo que a Seguridad de la Información se refiere. Mediante el desarrollo de una documentación de hacking ético, se desarrollarán fases de implantación que permitan la elaboración del presente proyecto, cuyo objetivo será la incorporación de la seguridad en la información.

Obteniendo a su vez resultados parciales a corto plazo que identifiquen el estado actual de la seguridad en el ITSCO, para el desarrollo de estas fases se incorporará como requisito, el cumplimiento de estándares o normas que en cada acción puedan ser aplicables.

La seguridad es un estado del bienestar de la información y de las infraestructuras en el cual la posibilidad de hurto, tratar de forzar, interrupción de la información y de los servicios se ha mantenido en un punto bajo o tolerable.
Existen varios aspectos que tienen que ver con la seguridad en la actualidad; el dueño de un sistema deberá tener la confianza que se comportará según su especificación. A esto se le llama generalmente aseguramiento. Los sistemas, usuarios, y aplicaciones necesitan interactuar recíprocamente uno con otro en un ambiente de trabajo en red.

La identificación o la autentificación es el medio para garantizar la seguridad en tal panorama. Los administradores de sistema o cualquier otra autoridad necesitan saber quién ha tenido acceso a los recursos del sistema cuándo, dónde, y para qué propósito. Una auditoria a los *logs* (registros diarios) puede tratar el aspecto de la seguridad llamado *accounting* (manejo de cuentas). No todos los recursos estarán generalmente disponibles para todos los usuarios. Esto puede tener implicaciones

estratégicas; ya que teniendo controles de acceso en parámetros predefinidos, puede ayudar a alcanzar un mejoramiento en la seguridad.

Planeación de la Seguridad en la Red

El activo más importante que se posee es la información, y por lo tanto deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas brindan la Seguridad Lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo. En la seguridad lógica debe tomarse en cuenta lo que es bien conocido dentro de la seguridad informática: "lo que no está permitido debe estar prohibido".

Para esto hay que considerar las siguientes actividades:

- Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no llegue a otro.
- Asegurar que existan sistemas y rutas de emergencia alternativos para transmitir información entre diferentes localidades
- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o software empleados.

Los modelos de seguridad en redes nos permiten definir la forma en la que se protegerá principalmente la información que se encuentra dentro de una red.
Cabe mencionar que ningún modelo garantizará la seguridad total de un sistema; es decir, los modelos pueden fallar.

Seguridad por Oscuridad

Este modelo consiste en que los sistemas no son protegidos porque sus propietarios creen que nadie los va a atacar porque no les interesa, piensan que la probabilidad de que les ataquen es ínfima, por lo tanto, no hacen nada por mejorar su estado actual; es decir, no conocen sus vulnerabilidades y pueden ser atacados.

Perímetro de Defensa

Este modelo establece un cerco o perímetro de defensa externo, para que posibles atacantes externos no tengan acceso a los sistemas. Este modelo es vulnerable a usuarios o atacantes internos, debido a que internamente se puede tener acceso a la información sin restricciones de ningún tipo.
El modelo de Perímetro de Defensa también tiene sus falencias, dado que los sistemas de seguridad externos utilizados son susceptibles a fallas, dejando de esta manera la red desprotegida.

Defensa en Profundidad

Este modelo es el efecto de ir acortando los perímetros de defensa, puede diferenciar servidores de usuarios para establecer seguridades, y también permite diferenciar entre usuarios. Establece varios perímetros de seguridad, donde cada perímetro se

reduce hasta un nivel en el cual cada uno de los sistemas sea una isla o perímetro seguro.

Como contraparte, la administración de este modelo de seguridad resulta bastante compleja y costosa, pues se debe asegurar cada uno de los elementos de un sistema teniendo en cuenta sus características y funcionamiento.

Servicios implícitos en la Seguridad de Redes

La seguridad en redes por definición brinda servicios que permiten a la información y a los recursos estar disponibles a los usuarios de la organización y protegidos contra intentos de acceso no consentidos. A continuación se detallarán los principales servicios y sus funciones.

Confidencialidad

Este servicio permite mantener la privacidad de la información; es decir, solo usuarios autorizados pueden tener acceso a la información y entenderla. Para conseguir esto, la información que se desea proteger es cifrada; por consiguiente, si un intruso tiene acceso a la información no podrá entender su contenido.

Integridad

Este servicio garantiza que la información llegará a su destino durante el tiempo previsto y sin alteraciones. Para este propósito, el emisor obtiene un resumen de la información enviada y adjunta este resumen a la información.

En el destino la información es separada del resumen y el procedimiento se repite para obtener un nuevo resumen y poder comparar los dos resúmenes, si coinciden, se puede confiar en el contenido de la información.

Disponibilidad

La disponibilidad está dada por el tiempo que un sistema permanece en línea con respecto al tiempo que estará fuera de servicio, se mide en porcentajes.

Para que exista disponibilidad de hardware y software deben ser confiables; la disponibilidad siempre se ajustará a los requerimientos de una empresa específica, dado que para cumplir con este servicio se deberá disponer de redundancia ya sea en sistemas o canales de comunicación.

Identificación

Es el proceso mediante el cual se establece la identidad de un individuo en particular se puede identificar a personas o entidades, para esto se llevan a cabo procedimientos que garanticen que la identidad presentada corresponde a la entidad. Por ejemplo, se puede requerir la presentación de una cédula de identidad personal, pasaporte, fotografías, dirección, teléfono e incluso referencias personales.

Autenticación

Es un proceso que consiste en presentar una prueba de ser quien se dice ser, es muy importante cuando se ingresa o se comunica a través de una red. Para la autenticación se utilizan tres esquemas básicos:

- Algo que usted conoce: *password* o contraseña.
- Algo que usted tiene: tarjeta o llave.
- Algo que usted es: iris del ojo humano, huella dactilar, voz.

Estos esquemas generalmente son utilizados independientemente, aunque se recomienda que se usen al menos dos en conjunto.

Este servicio consiste en autorizar a usuarios lícitos el acceso a recursos e información de acuerdo a su función. Cada función de un usuario está definida en un perfil que determina que está permitido y que no lo está.

Aceptación (Para impedir la negación de eventos)

Este servicio permite garantizar que usuarios lícitos no puedan realizar acciones ilícitas, como realizar una transacción y después negarla. Para que este servicio sea garantizado se necesita integrar en los mensajes un registro del tiempo en que fueron enviados y recibidos.

4.7 Metodología de Trabajo

De forma general, la metodología comienza evaluando la seguridad de la Institución mediante la recolección de información, a través de entrevistas con el personal de esta, realizando pruebas de campo y análisis técnicos, para así, presentar un informe del estado de implantación de las distintas medidas de seguridad técnicas y organizativas, pasar a la elaboración y propuesta de un plan de acción que, tras ser aprobado por la dirección, se procederá a su elaboración e implementación.

En la elaboración de la presente metodología de trabajo se ha pretendido seguir un enfoque holístico y extremadamente práctico que permita al usuario del mismo una aplicación sencilla, mediante el seguimiento de fases secuenciales y diferenciadas que son mostradas en el siguiente diagrama y se describen en detalle a continuación.

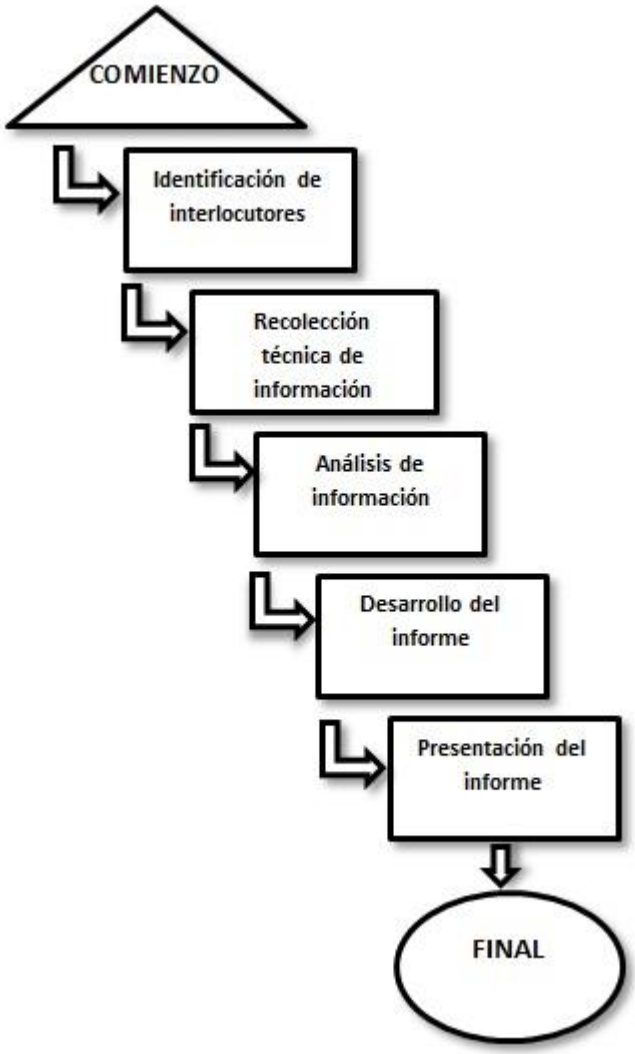


FIGURA 4-3: METODOLOGIA DE TRABAJO

4.7.1 Identificación de Interlocutores

La fase de recolección de información tiene una gran importancia en el desarrollo del método, puesto que la información obtenida en la misma será la fuente del análisis para saber el estado de la seguridad en la información y del posterior plan de acción. Por ello, para el desarrollo de esa fase deberá contarse con la colaboración total de la Institución para la obtención de la información correspondiente.

Adicionalmente, para determinadas tareas que serán claramente identificadas previamente por el desarrollador del proyecto, podrá ser necesario el acceso directo a determinados dispositivos y sistemas de la Institución para realizar comprobaciones de configuración, seguridad, etc. Este acceso deberá ser proporcionado por la Institución con los requisitos que ésta estime oportunos: bajo supervisión del personal propio, con diario de operaciones efectuadas, o cualquier mecanismo que ofrezca funcionalidades similares y salvaguarde la integridad de la información. El desarrollador del proyecto firmará un acuerdo de confidencialidad constituyendo una garantía para la Institución de no difusión, ni utilización de la información tratada. Así mismo la Institución deberá firmar por escrito una autorización para realizar las pruebas que el desarrollador del proyecto indique y estime oportunas para obtener la información necesaria para la realización de las tareas respectivas.

4.7.2 Recolección Técnica de Información

En esta fase inicial se recolectará la información necesaria de la Institución que supondrá el origen de las posteriores baterías de pruebas y análisis técnicos necesarios. Durante esta fase se tendrá una mayor interacción entre la Institución y el desarrollador del proyecto que se verá materializada por la presencia en la Institución, redundando todo esto en un diálogo fluido y efectivo que facilitará la obtención de la información deseada. Deberá por tanto proporcionarse el espacio y tiempo disponible del interlocutor para su realización. De forma previa a la presencia del desarrollador del proyecto en la Institución, podrá facilitarse al interlocutor seleccionado un cuestionario que, en su caso, deberá ser remitido adecuadamente cubierto al desarrollador, para llevar a cabo la recolección de información de la forma más eficiente posteriormente.

4.7.3 Análisis de Información

Existen muchas herramientas de trabajo, por así llamarlas que usa un *hacker* ético, las cuales son más bien técnicas bien definidas para obtener información de un objetivo, y que en malas manos pueden ser perjudiciales.

4.7.3.1 Footprinting

Footprinting se define como el análisis del perfil de seguridad de una empresa u organización, emprendido de una manera metodológica; se la considera metodológica debido a que se busca información crítica basada en un descubrimiento anterior.

No existe una sola metodología para realizar *footprinting*, un individuo puede escoger muchos caminos para llegar a la información, así mismo esta actividad es esencial debido a que toda la información crítica necesita ser recopilada antes de que el *hacker* pueda decidir sobre la mejor acción a realizar.

El *footprinting* necesita ser desarrollado correctamente y en una manera organizada, la información descubierta puede pertenecer a varias capas de red, por ejemplo se puede descubrir detalles del nombre del dominio, direcciones de red, servicios de red y aplicaciones, arquitectura del sistema, IDS's, direcciones IP específicas, mecanismos de control de acceso, números telefónicos, direcciones de contacto, mecanismos de autenticación, entre otros.

Este listado puede incluir mucha más información, dependiendo de cómo los aspectos de la seguridad son tratados dentro de la organización. La información recolectada durante la fase de *footprinting* se puede utilizar como un puente para poder escoger la metodología del ataque. Un aspecto de la información es que casi todo se puede conseguir por medio del Internet, la mayoría disponible al público en general.

4.7.3.2 Metodología para obtener información

El atacante primero recuperaría la información inicial (como nombre del dominio) del sistema objetivo, para lo cual se usan las herramientas *Nslookup*, WHOIS, y se comprueban las máquinas activas (haciendo ping a las direcciones de cada una), se descubren además puertos o puntos de acceso abiertos (con herramientas como *port scanners*), sistemas operativos usados (por medio de consultas con *telnet*), se descubren además servicios en puertos, y en última instancia, se hace un mapa de toda la red.

4.7.3.3 Herramientas para Footprinting

Whois

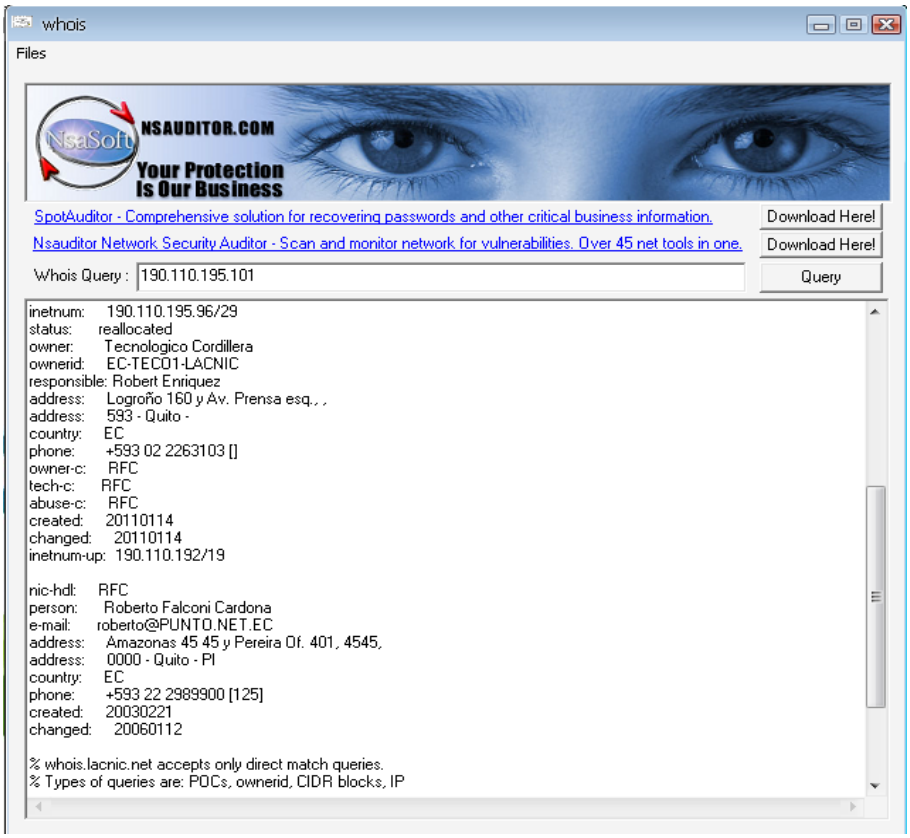


FIGURA 4-7-3-1: HERRAMIENTA WHOIS

Nslookup

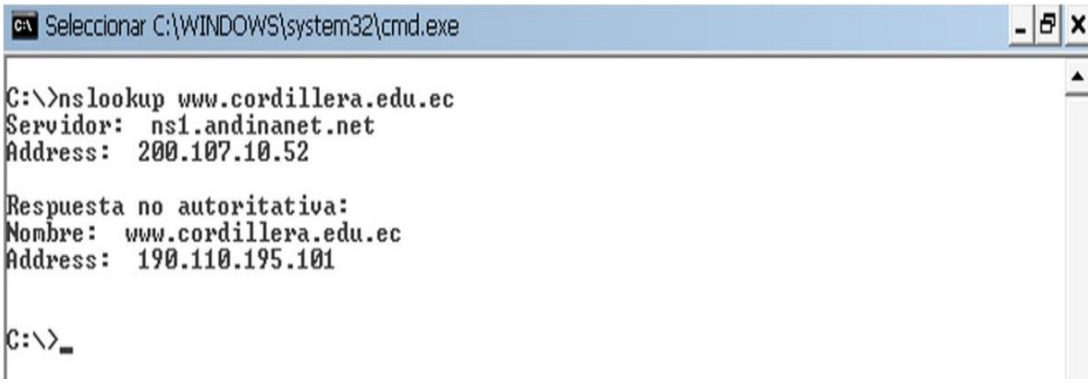


FIGURA 4-7-3-2: HERRAMIENTA NSLOOKUP

Visualroute

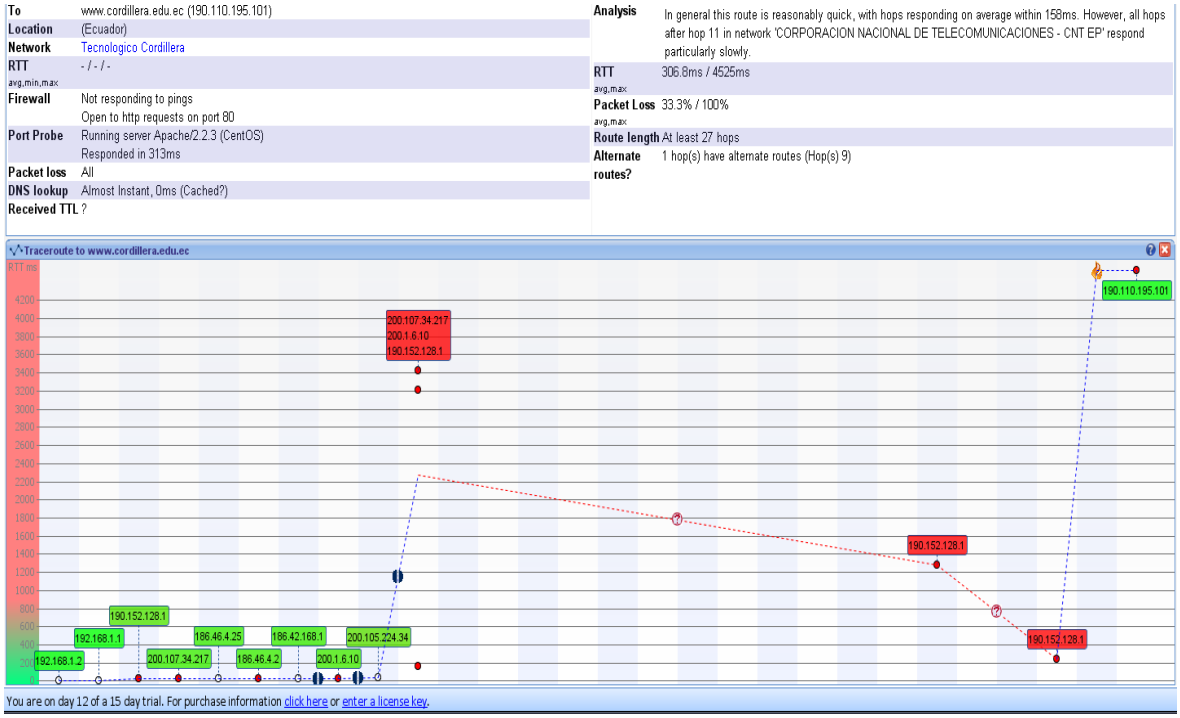


FIGURA 4-7-3-3: HERRAMIENTA VISUALROUTE

4.7.3.4 Scanning

Una de las principales actividades que un atacante realiza cuando intenta penetrar a un sistema es reunir toda la información posible y realizar un inventario de puertos abiertos usando alguna técnica de escaneo de puertos. El escaneo de puertos es una de las técnicas más populares de reconocimiento usada por *hackers* a nivel mundial.

Una vez completado este proceso, esta lista ayuda al atacante a identificar algunos servicios que están ejecutándose en el sistema objetivo, usando una lista de puertos conocidos; esto permite posteriormente crear una estrategia que conduzca a comprometer el sistema.

Los números de puerto son enteros sin signo de 16 bits, y pueden ser clasificados en tres categorías:

- Puertos del 0 al 1023 son 'puertos bien conocidos'.
- Puertos del 1024 al 49151 son 'puertos registrados'.
- Puertos del 49152 al 65535 son 'puertos dinámicos o privados'

Aunque es ciertamente posible escanear los 65535 puertos TCP y los 65536 puertos UDP, muchos de los atacantes no lo hacen, sólo se concentran en los primeros 1024 puertos. Estos 'puertos bien conocidos' son donde encontraremos la mayoría de las aplicaciones comúnmente usadas. Una lista completa de puertos puede ser encontrada en: http://www.iana.org/assignments/port-numbers

Herramientas para realizar un *Scanning:*

Ping

NMap (Network Mapper)

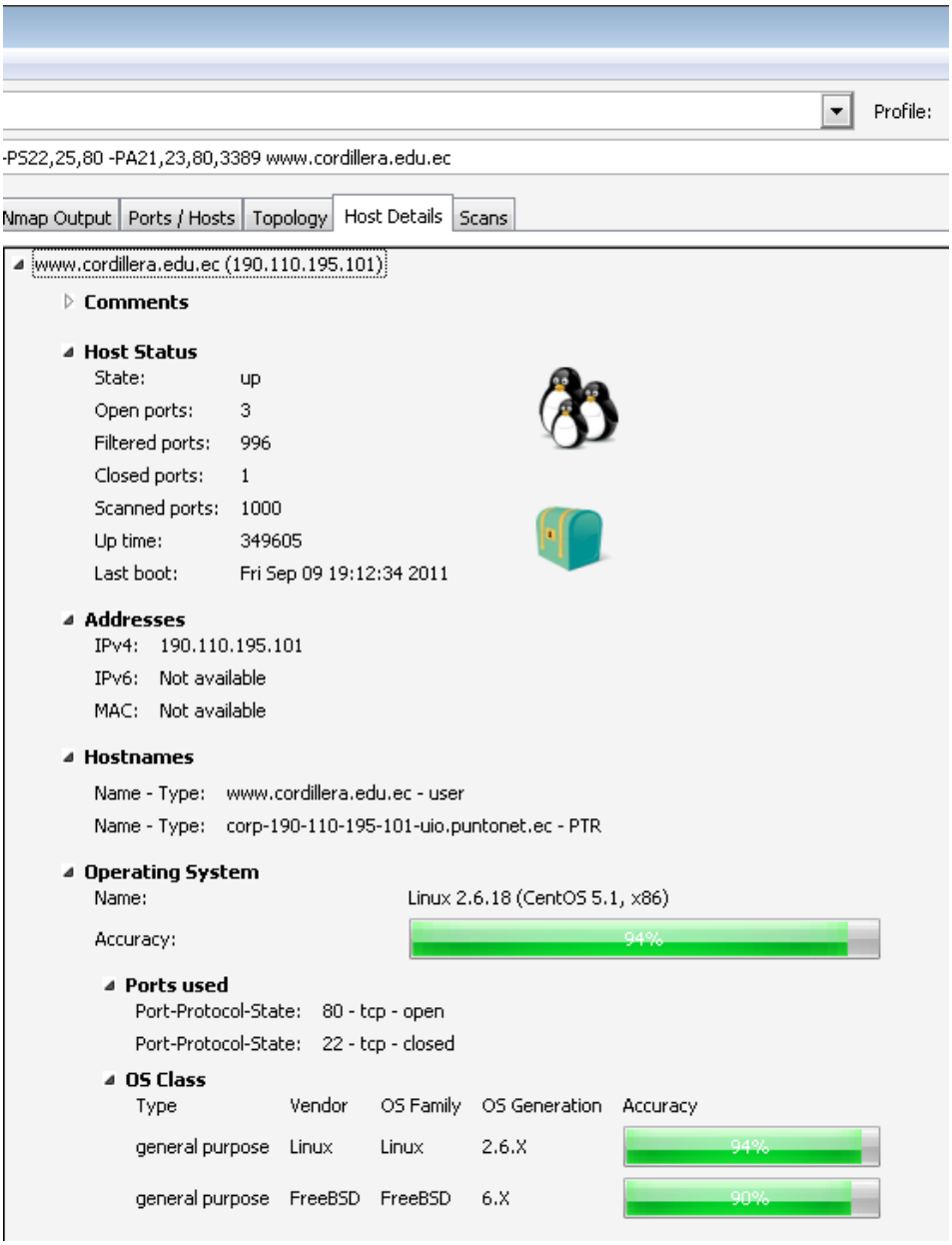


FIGURA 4-7-3-4: HERRAMIENTA NMAP

Nessus, NeWT (Nessus Windows Technology)

LANguard

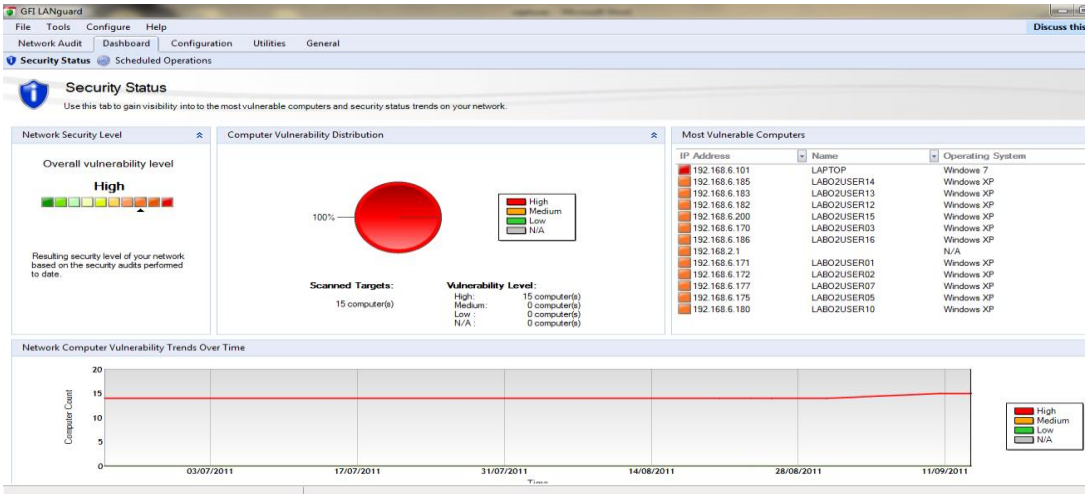


FIGURA 4-7-3-5: HERRAMIENTA LANGUARD

4.7.3.5 Enumeration

Si la adquisición de información y las pruebas no intrusivas no han retornado resultados satisfactorios, el siguiente paso del atacante es identificar cuentas de usuario válidas, y recursos compartidos de red poco protegidos.

La enumeración envuelve a conexiones activas a los sistemas y a consultas dirigidas a un equipo en particular. El tipo de información enumerada por los intrusos es:

- Recursos de red y compartidos.
- Usuarios y Grupos.
- Aplicaciones.

El objetivo del atacante será de identificar cuentas de usuario o grupos válidos, donde pueda seguir comprometiendo el sistema. Normalmente dichos intentos

de enumerar recursos del sistema se almacenarán en los *logs*, a menudo la información descubierta es aquella que el usuario la hizo pública, como las direcciones DNS. Así mismo es posible que el atacante se encuentre con un recurso compartido como el IPC$ en *Windows*, en donde puede probarse una sesión *null* para ver recursos compartidos y cuentas enumeradas.

En la fase de enumeración, el atacante obtiene información como nombres de usuarios y grupos, tablas de enrutamiento, información SNMP (*Simple Network Management Protocol*).

Herramientas para realizar *Enumeration*:

GetAcct
Userinfo
IP Network Browser

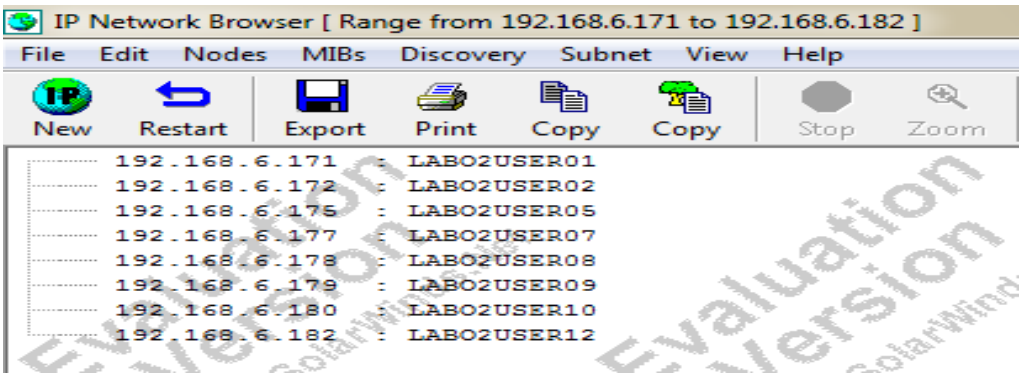


FIGURA 4-7-3-6: HERRAMIENTA IP NETWORK BROWSER

4.7.3.6 System Hacking

Windows hacking

En esta etapa del proceso de *hacking*, las cosas empiezan a ser diferentes, este paso trata acerca de irrumpir e ingresar al sistema. Los pasos previos como *footprinting, scanning* y *enumeration* son considerados pre ataques.

Antes de iniciar, el *hacker* ético debe asegurarse que tiene los permisos necesarios para realizar estas actividades en sistemas de otras personas.

La primera meta del *system hacking* es autenticarse en el *host* remoto con el más alto nivel posible. Existen algunas formas de las cuales esto se puede realizar:

- Adivinar nombres de usuario y contraseñas.
- Obtener los archivos *hash* de las contraseñas.
- Hacer *exploit* de una vulnerabilidad.

Adivinar nombres de usuario y contraseñas requiere que se revise lo que ya se ha encontrado hasta el momento en actividades previas. Las herramientas usadas durante la fase de *Enumeration*, como IP *Network Browser,* deben haber arrojado varias pistas acerca de cuentas específicas.

Ya se debería contar con información de cuentas de usuarios, nombre real del administrador de la red, conocimiento de nombres de recursos compartidos, nombres de máquinas; la forma más simple de usar esta información es a través de adivinar las contraseñas.

Las herramientas que se utilizan para *Windows Hacking* son las siguientes:

L0phtcrack (LC5)
Cain
John the Ripper

4.7.3.7 Puertas traseras (backdoors)

Las puertas traseras a menudo ofrecen a los atacantes una forma fácil de ingresar a los sistemas remotos, sin tener que usar *exploits* o aprovecharse de cualquier otra vulnerabilidad. Las puertas traseras más simples permiten a una ventana de comandos escuchar en determinado puerto (generalmente un número de puerto desconocido), el atacante necesita solamente ejecutar un *telnet* al puerto y estará adentro del sistema con una ventana de comandos remota.

Las puertas traseras pueden también ser implementadas en sistemas "vírgenes" que no han sido comprometidos de ninguna otra manera, los programas de *backdoor* pueden venir embebidos en archivos adjuntos (*attachments*) de correo electrónico, controles *ActiveX* o en cualquier archivo que proviene de Internet.

4.7.3.8 Troyanos

Los troyanos son programas que aparentan cumplir con una función, pero cuando son ejecutados, se ejecuta también alguna actividad maliciosa, un usuario puede pensar que el archivo es inofensivo para ejecutarlo, pero después que el archivo es ejecutado, libera su carga maliciosa para comprometer al sistema; esta carga puede permitir al atacante acceso remoto a su sistema, empezar a grabar actividades con un *keylogger*, establecer una

puerta trasera en el sistema, causar Negación de Servicios (DoS), e incluso deshabilitar la protección antivirus o software de *firewall* instalado.

4.7.3.9 Sniffers

Los *sniffers* son una herramienta de software muy poderosa, ya que tienen la capacidad de establecer en modo promiscuo la tarjeta de red de un PC cualquiera para poder recibir información que circula por esa red, no solo paquetes. Si se encuentra en un *Hub*, mucho tráfico puede potencialmente ser afectado, debido a que los *Hubs* ven todo el tráfico que pasa por un dominio de colisión.

Los *Sniffers* operan en la capa enlace del modelo OSI, eso significa que no tienen que apegarse a las mismas reglas que las aplicaciones y los servicios del sistema operativo. Los *sniffers* pueden almacenar cualquier cosa que pasa en la red y grabarlo para posterior revisión, permiten al usuario ver todo el tráfico contenido en el paquete, incluso información que debería permanecer oculta.

Herramientas para *Sniffing*

Ethereal
Windump
TCPdump

4.7.3.10 Revisión y Configuración

Para la revisión de las configuraciones será necesaria la participación de expertos en los distintos dispositivos analizados que puedan identificar fallos en las mismas, formas más eficientes de implementar una determinada funcionalidad o mecanismos alternativos que mejoren la seguridad y eficiencia del dispositivo.

Típicamente deberán revisarse al menos dispositivos de electrónica de red (routers, switches, bridges, etc.), dispositivos de seguridad (cortafuegos / firewalls, IDS/IPS/dispositivos de prevención de intrusiones, servidores de autenticación, etc.), aplicaciones (servidores Web, ftp, de correo, etc.) y en general cualquier dispositivo con una funcionalidad necesaria dentro de la Institución que pueda suponer una posible fuente de vulnerabilidades y por tanto de elevación del nivel de riesgo asumido por la Institución.

4.7.3.11 Visualización Externa

Existe una gran cantidad de información relativa a las organizaciones accesible de forma pública desde Internet. Esta información puede ser una pieza clave para el diseño de un eventual plan de ataque contra la Institución, porque

puede revelar interesantes detalles, tanto técnicos como organizativos, que utilizados de forma adecuada facilitan la tarea de potenciales atacantes.
Es importante, por tanto, que la Institución sea consciente de la existencia de esta información, por lo que deberá prestarse especial atención a los siguientes puntos.

4.7.3.12 Análisis de Tráfico

Mediante este punto se intentará caracterizar el tipo de tráfico que discurre habitualmente por las redes de la Institución, así como detectar posibles puntos de fallo o cuellos de botella en dichas redes.

Para un óptimo resultado del análisis, deberán identificarse cuales son los puntos sensibles en los que deberán realizarse las medidas, entendiendo por sensibles aquellos puntos con representatividad en su tráfico.

Dichos puntos, típicamente podrán ser:

- Interconexiones entre segmentos
- Segmentos de servidores/aplicaciones críticas
- Segmentos de usuarios

Cada medida deberá realizarse durante un periodo de tiempo significativo de forma que se capture una cantidad de tráfico suficiente para su posterior análisis. El tiempo de medida dependerá de la cantidad de tráfico que habitualmente soporte la red. En algunos entornos será suficiente mantener la medida durante unos pocos minutos, mientras que en otros será necesario realizar la medida a lo largo de un día completo o incluso, periodos más prolongados de tiempo.

4.7.3.13 Análisis de vulnerabilidades y Aplicaciones

El análisis de vulnerabilidades de sistemas y aplicaciones tiene como objeto detectar puntos débiles en la seguridad de los sistemas y aplicaciones que éstos soportan. Se entiende por puntos débiles, errores de programación o de

configuración en las aplicaciones y sistemas operativos que puedan ser causa de vulnerabilidades susceptibles de ser explotadas por potenciales atacantes.

Por tanto, será importante conocer cuáles son estos puntos débiles con el fin de implantar los controles adecuados para eliminarlos o evitar su explotación. No todos los sistemas tienen la misma importancia dentro de la Institución. Por esto el análisis de vulnerabilidades es una tarea que puede consumir mucho tiempo, deberá realizarse una selección de cuáles son los sistemas sobre los que se realizará el análisis. Objetivos típicos de este tipo de análisis serán los sistemas cuyo mal funcionamiento pueda causar un impacto importante en los procesos de la Institución (e.g. Servidores principales) o aquellos que por su visibilidad están más expuestos a posibles ataques (e.g. Servidores con acceso público desde Internet). Deberá ser la Institución objeto del análisis quien, con el asesoramiento del equipo de trabajo que efectúe el análisis, decida cuales son los sistemas que deben ser analizados.

4.7.3.14 Análisis Remoto

Se prestará especial atención a las vulnerabilidades que pueden ser explotadas remotamente, ya que éstas pueden suponer un mayor riesgo al no requerir de presencia física para su explotación. Dichas vulnerabilidades, habitualmente estarán asociadas a puertos de aplicación que esperan recibir conexiones remotas. El primer paso del análisis de vulnerabilidades, por tanto, será identificar cuáles son los puertos de los sistemas que son accesibles de forma remota. Un método para conseguir esta información será la realización de un escaneo de puertos.

El objetivo del escaneo de puertos será averiguar que puertos (típicamente TCP o UDP) están a la escucha en un sistema determinado, y por tanto, pueden recibir conexiones remotas. Es esta una información de suma importancia, ya

que una gran parte de las vulnerabilidades asociadas a aplicaciones, tienen que ver con las posibilidades de conexión remota de las mismas. La técnica básica para saber el estado de un puerto es tratar de realizar una conexión contra el mismo y analizar el resultado, pudiendo obtenerse tres valores para el estado de un puerto:

• Abierto: El puerto está a la escucha y listo para recibir conexiones.
• Cerrado: El puerto no está a la escucha
• Filtrado: Existe algún dispositivo (típicamente un cortafuegos/firewall) que no permite realizar conexiones contra el puerto. Tras realizar el escaneo de puertos, se dispone de la información referente a que puertos tiene disponibles cada sistema para aceptar conexiones remotas, cada uno de estos puertos estará asociado a un servicio y por tanto a una aplicación. El siguiente paso será averiguar cuáles son dichas aplicaciones y, si es posible, la versión de las mismas.

Conocer el software específico que está instalado en un sistema es una de las primeras labores que intentará abordar un potencial atacante, ya que con esta información, se pueden conocer cuáles son las vulnerabilidades que presentan las aplicaciones remotamente accesibles, y de esta forma acceder a los métodos de explotación de la vulnerabilidad (o *exploits*). El resultado de la ejecución de un *exploit* se materializa habitualmente en un compromiso del sistema, que puede ir desde, la eventual destrucción de sus datos al acceso no lícito de sus recursos.

4.8 Niveles De Seguridad De La Institución

De acuerdo con los estándares de seguridad en computadoras desarrollado en el libro naranja del Departamento de Defensa de Estados Unidos, se usan varios niveles de seguridad para proteger de un ataque al hardware, al software y a la información guardada.

4.8.1 Nivel D1

Es la forma más elemental de seguridad disponible, o sea, que el sistema no es confiable. Este nivel de seguridad se refiere por lo general a los sistemas operativos como MS-DOS, MS-Windows y System 7.x o más de Apple Macintosh. Estos sistemas operativos no distinguen entre usuarios y tampoco tienen control sobre la información que puede introducirse en los discos duros.

4.8.2 Nivel C1

El nivel C tiene dos sub-niveles de seguridad: C1 y C2. El nivel C1, o sistema de protección de seguridad discrecional, describe la seguridad disponible en un sistema típico Unix. Los usuarios deberán identificarse a sí mismos con el sistema por medio de un nombre de registro del usuario y una contraseña para determinar qué derechos de acceso a los programas e información tiene cada usuario.

4.8.3 Nivel C2

Junto con las características de C1, el nivel C2 tiene la capacidad de reforzar las restricciones a los usuarios en su ejecución de algunos comandos o el acceso de algunos archivos basados no sólo en permisos, sino en niveles de autorización.

Además requiere auditorias del sistema, la auditoría se utiliza para mantener los registros de todos los eventos relacionados con la seguridad, como aquellas actividades practicadas por el administrador del sistema, la auditoría requiere autenticación y procesador adicional como también recursos de disco del subsistema.

4.8.4 Nivel B1

El nivel B de seguridad tiene tres niveles. El nivel B1, o protección de seguridad etiquetada, es el primer nivel que soporta seguridad de multinivel, como la secreta y la ultra secreta. Parte del principio de que un objeto bajo control de acceso obligatorio no puede aceptar cambios en los permisos hechos por el dueño del archivo.

4.8.5 Nivel B2

Conocido como protección estructurada, requiere que se etiquete cada objeto como discos duros, terminales. Este es el primer nivel que empieza a referirse al problema de comunicación de objetos de diferentes niveles de seguridad.

4.8.6 Nivel B3

O nivel de dominios de seguridad, refuerza a los dominios con la instalación de hardware. Requiere que la terminal del usuario se conecte al sistema por medio de una ruta de acceso segura.

4.8.7 Nivel A

Nivel de diseño verificado, es el nivel más elevado de seguridad. Todos los componentes de los niveles inferiores se incluyen. Es de distribución confiable, o sea que el hardware y el software han sido protegidos durante su expedición para evitar violaciones a los sistemas de seguridad.

4.9 Desarrollo del Informe

A partir de los hallazgos obtenidos en la Recolección Técnica de datos, y tras haber procedido al análisis de toda la información recolectada, se desarrollará el informe del Estado de la Seguridad Informática. Este informe persigue dos objetivos.

- El primero, proporcionar una visión global y detallada del estado de la organización en cuanto a la seguridad de la información.

- El segundo objetivo, no menos importante, es señalar cuales son los aspectos mejorables que atañen a la seguridad de la información así como proponer acciones correctivas priorizándolas de acuerdo con la relevancia que tengan para la institución.

4.10 Presentación de informe a alta dirección

El desarrollo del Informe se refiere a la recolección técnica y general de información ya indicada anteriormente. En el cual se deberá especificar el estado técnico de la institución, el cual podrá ser utilizado posteriormente, como documentación de referencia, en el cual estará especificado el análisis de los equipos con cada una de sus vulnerabilidades.

La presentación deberá estructurarse adecuadamente, para lo cual se recomienda un esquema similar al siguiente:

- Descripción del estudio realizado y motivación del mismo
- Estado actual de la organización
- Ejemplos reales de hallazgos, problemas y/o vulnerabilidades existentes
- Conclusiones
- Recomendaciones

CAPITULO V

IMPACTOS ESPERADOS DEL PROYECTO

5.1 Científico

Este proyecto beneficiara a profesionales, ya que con la ayuda de este documento se podrá realizar pruebas futuras, para así realizar un hacking ético a medida que se incrementen los equipos en la red, o se realicen pruebas de un nuevo sistema que requiera el crecimiento de la misma o a su vez la creación de usuarios, este documento será una guía para poder seguir las medidas necesarias, y evitar intrusiones no autorizadas ya sean de manera interna o externa.

5.2 Educativo

Esta investigación tiene como finalidad ayudar a las futuras generaciones, como documento de consulta, para conocer las partes que conforman la seguridad en las redes, y poder así entender los modos como operan los hackers, de qué forma toman el control de un sistema, como ingresan a una intranet, etc., y de esta forma crear en los estudiantes un sentimiento de responsabilidad, compromiso y de ética.

5.3 Técnico

Las herramientas utilizadas en el proyecto son las adecuadas para realizar los test de intrusión, como es un footprinting, scanning, etc., ya que por medio de estas podemos conocer el estado de la red y de cada uno de sus equipos, así como su sistema operativo, plataforma, etc., profesionalmente me ayudó mucho para reforzar mis conocimientos en la parte de seguridades.

5.4 Tecnológico

En la actualidad a través de las herramientas para auditoria de redes se puede realizar un análisis en cuanto a la seguridad de una Institución, por medio de un hacking ético se puede incrementar la misma, para poder implementar sistemas de seguridad más estables.

5.5 Empresarial

Luego de analizar la estructura interna de la red se procedió a la utilización de las herramientas para realizar un hacking ético, este proceso favoreció al ITSCO para saber la situación actual de la red, que tipo de vulnerabilidades existen y que formas de intrusión podrían ser usadas por hackers para el ingreso no autorizado a los procesos de la institución.

El impacto de estas vulnerabilidades se vería reflejado en la alteración e intrusión al servidor actual de la Institución, ya que por medio de las conclusiones presentadas en el informe final un hacker podría realizar un ataque informático de forma maligna y explotar vulnerabilidades para poder acceder a los sistemas de información.

5.6 Social

Este proyecto ayuda a las personas que se encuentran trabajando actualmente en la institución ya que podrán realizar su trabajo de manera eficiente y rápida porque cuentan con una red que tiene los requerimientos de seguridad adecuados y los procesos se podrán ejecutar de manera más eficiente.

5.7 Económico

En el ámbito económico la institución se beneficia ya que el presente tema de investigación no tiene costo, los gastos realizados corren por cuenta del investigador como tema de tesis, dentro de los cuales se incluyen gastos de oficina, papelería, impresiones, movilización, servicios básicos, etc.

5.8 Conclusiones

- El servidor principal del ITSCO con la dirección 172.16.2.1 se encuentra en buenas condiciones pero no las óptimas de seguridad, por carecer de un sistema operativo actualizado.

- El medio de seguridad para intrusos está compuesto de un firewall, el cual no es totalmente efectivo si el ataque se realizara a través de múltiples direcciones y al mismo tiempo.

- Los equipos que se encuentran compartiendo las aplicaciones del servidor principal, pertenecientes a empleados del ITSCO, no se encuentran dentro de un directorio activo, por lo que un empleado interno tiene el acceso y credenciales necesarias para instalar cualquier tipo de software para intrusión.

- Los laboratorios se encuentran dentro de un grupo de trabajo, por lo cual no se tiene un nivel de jerarquía ni limitaciones para instalación de software, el total acceso al internet desde estos se podría reflejar en un ataque de gran magnitud por parte de los estudiantes que podría llevar al colapso de los sistemas de aplicación.

- Los equipos en los laboratorios se encuentran con vulnerabilidades altas, con puertos suficientes para poder tomar control de los mismos y llevar a cabo un

hacking malicioso, colapsando así sus sistemas operativos y comprometiendo el rendimiento de los equipos.

5.9 Recomendaciones

- En el servidor principal se debe realizar una actualización del sistema operativo Cent, para así proveer de mayor estabilidad a las aplicaciones ya que cada versión de sistema operativo tiene también su vulnerabilidad por lo que su versión más reciente corrige los errores de la anterior.

- Se debería implementar un IDS (Sistema de detección de intrusos) para poder realizar un monitoreo de la red y generar reportes sobre la actividad en la misma, o a su vez un honeypot para proteger la integridad de los datos, el honeypot se lo debería colocar ya sea en el mismo segmento de la DMZ o fuera de él, de esta forma se podría controlar si un intruso quiere tener acceso a la red y poder seguir sus pasos, mientras la información real estaría protegida.

- Para tener un control sobre las actividades de los usuarios internos del ITSCO se debería implementar un directorio activo para poder restringir la utilización e instalación de software no autorizado en sus equipos, como herramientas para hacking, backdoors o troyanos, y a la vez se tendría un control sobre que usuario ingresó, así como la fecha y la hora.

- En el laboratorio de cómputo se deberían implementar directorios activos para evitar el mal uso del internet, o evitar por medio de restricciones del mismo sistema operativo la instalación de software ajeno a lo laboral y restringir descargas de aplicativos, se deberían crear cuentas de usuario limitadas o de invitado para este fin.

- Para el correcto funcionamiento y estabilidad de los sistemas operativos en los equipos del laboratorio de computo se recomienda la instalación de un software antivirus corporativo, de esta forma se podrán evitar intrusiones externas, y solucionar problemas con los procesos actuales, se debe tomar muy en cuenta las actualizaciones de parches de seguridad, ya que al ser sistemas operativos de Microsoft son los más vulnerables a recibir ataques por sus fallas de seguridad, se debería realizar la instalación de sistemas operativos open source, para poder ganar mayor estabilidad y evitar inconsistencias en los equipos.

CAPITULO VI

6.1 Bibliografía

Shon Harris, Allen Harper, Chris Eagle, Jonattan Ness y Michael Lester, (2006), Hacking Etico, Anaya multimedia, 2da Edición, Estados Unidos.

Carlos Cervera Tortosa, (2010), Seguridad en Redes Inalámbricas, Libros de Luz, 1ra Edición, Colombia.

McClure, S., Scambray, J. and Kurtz, G., (2002), Hackers 3*, Secretos y soluciones para la seguridad de redes.* McGraw-Hill, 2da Edición, Estados Unidos.

Carlos Tori, (2008), Hacking Ético, Editorial Rosario, 1ra. Edición, Argentina

Bauer, Michael D., (2005), Seguridad en servidores Linux, Anaya Multimedia-Anaya Interactiva, 1ra edición, España

LONG, Johnny. *Google Hacking for Penetration Testers*, Syngress Publishing, USA, 2005, ISBN: 1-931836-36-1

WHITAKER, Andrew, NEWMAN Daniel. *Penetration Testing and Network Defense*, Cisco Press, USA, Noviembre 2005, ISBN: 1-58705-208-3

6.2 Net grafía

Conceptos sobre herramientas de sistemas operativos, hacking y redes.

www.wikipedia.com

Herramientas para test de intrusión

www.elhacker.net

Consulta de temas de hacking ético, como test de intrusión, denegación de servicios, etc.

www.eccouncil.org

Temas y herramientas sobre hacking ético, como google hacking, scanning, etc.

ANEXO 7. INFORME FINAL

INFORME GENERAL DEL SERVIDOR 172.16.2.1

Detalle general sobre los resultados de un escaneo al servidor que contiene el acceso principal a www.cordillera.edu.ec con su dirección ip 172.16.2.1

Profile:

-PS22,25,80 -PA21,23,80,3389 www.cordillera.edu.ec

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

www.cordillera.edu.ec (190.110.195.101)

Comments

Host Status

State:	up
Open ports:	3
Filtered ports:	996
Closed ports:	1
Scanned ports:	1000
Up time:	349605
Last boot:	Fri Sep 09 19:12:34 2011

Addresses

IPv4:	190.110.195.101
IPv6:	Not available
MAC:	Not available

Hostnames

Name - Type:	www.cordillera.edu.ec - user
Name - Type:	corp-190-110-195-101-uio.puntonet.ec - PTR

Operating System

Name: Linux 2.6.18 (CentOS 5.1, x86)

Accuracy: 94%

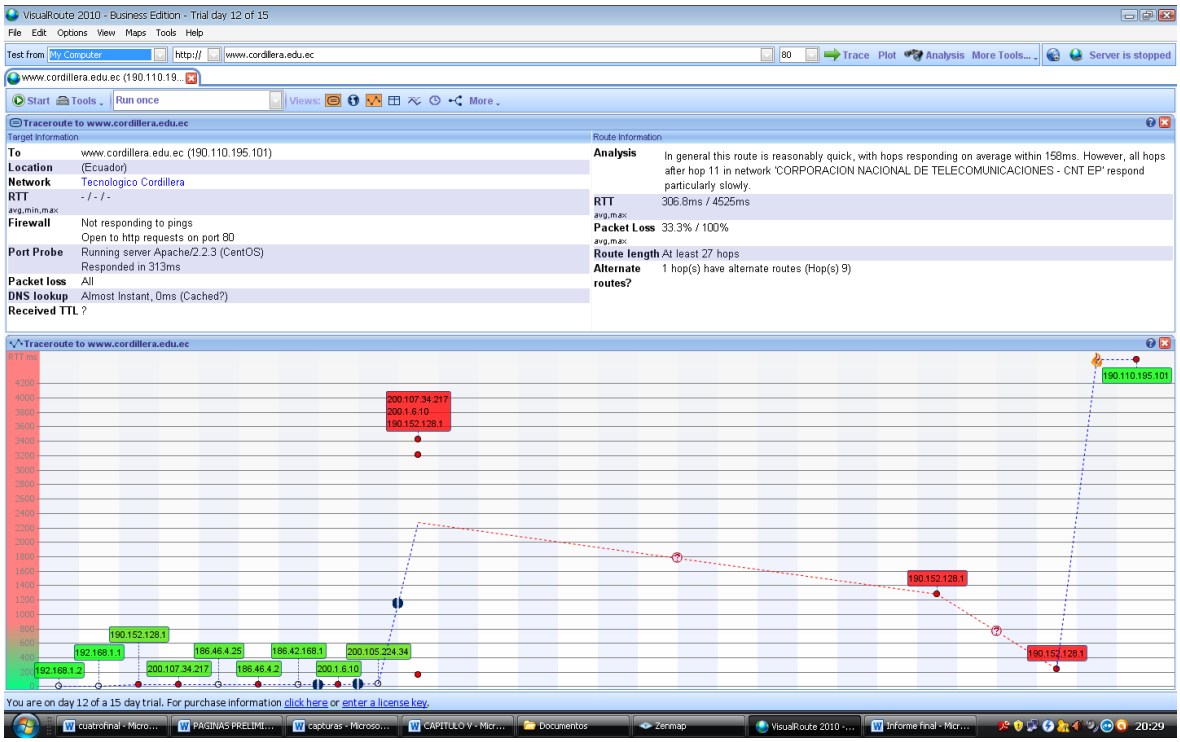
Ports used

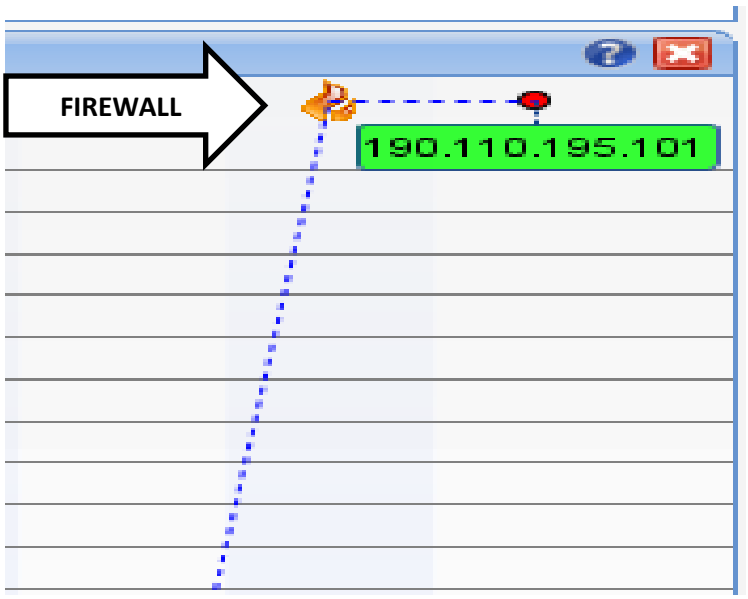
Port-Protocol-State:	80 - tcp - open
Port-Protocol-State:	22 - tcp - closed

OS Class

Type	Vendor	OS Family	OS Generation	Accuracy
general purpose	Linux	Linux	2.6.X	94%
general purpose	FreeBSD	FreeBSD	6.X	90%

Al realizar una traza hacia la dirección 190.110.195.101 se visualiza la presencia de un firewall el cual sirve para restringir el acceso a la DMZ.





INFORME GENERAL DE VULNERABILIDADES

A continuación se encuentra detallado el informe de vulnerabilidades dentro de la red del ITSCO, los cuales se encuentran detallados de acuerdo a la ip de cada equipo dentro de la red, catalogados de la siguiente manera:

High. Riesgo alto el cual debe ser solucionado a la brevedad posible

Medium. Riesgo para ser considerado a solucionar por poder agravarse con el pasar del tiempo

Low. Riesgo que no representa peligro para la estabilidad del equipo pero que debe ser solucionado y así no llegue al nivel medio.

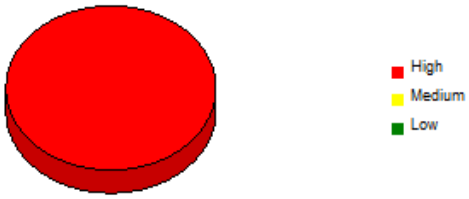
Hosts Severity Level Distribution

Vuln. Severity	Vuln. Count	%
High	49	49
Medium	1	1
Low	51	50

Top 10 Vulnerable Hosts (by Severity)

IP Address	Host Name	Severity		
		High	Med.	Low
192.168.6.101	LAPTOP	26	1	9
192.168.6.170	LABO2USER03	2	0	4
192.168.6.186	LABO2USER16	2	0	3
192.168.6.185	LABO2USER14	2	0	3
192.168.6.183	LABO2USER13	2	0	3
192.168.6.182	LABO2USER12	2	0	3
192.168.6.180	LABO2USER10	2	0	3
192.168.6.179	LABO2USER09	2	0	3
192.168.6.177	LABO2USER07	2	0	3
192.168.6.171	LABO2USER01	2	0	3

Hosts Vulnerability Level Distribution



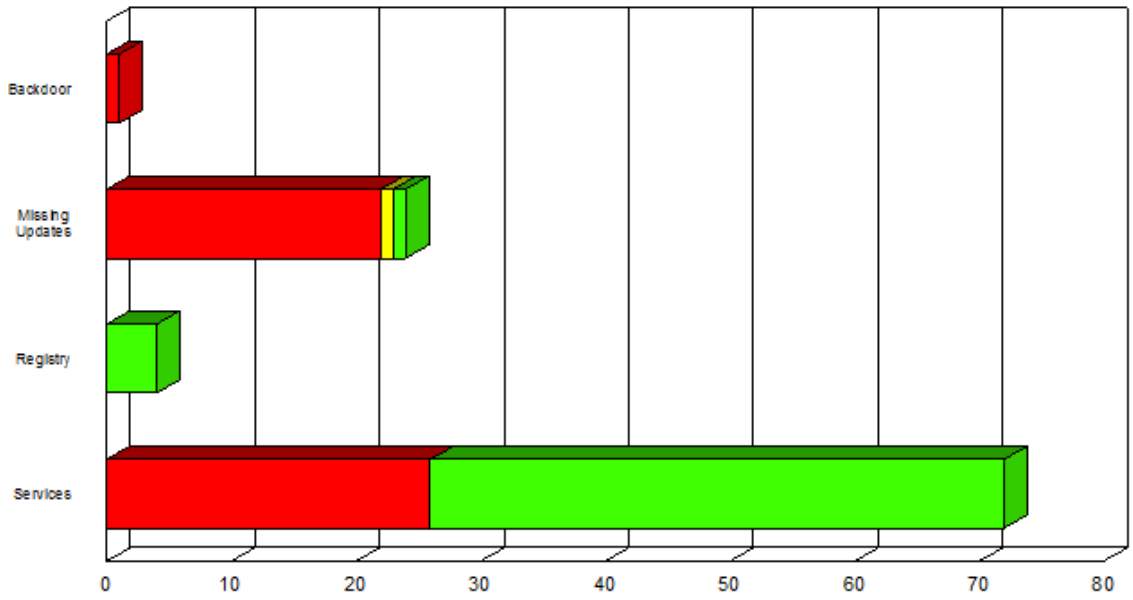
Vulnerability Level	Host Count
High	14
Medium	0
Low	0
Not Assigned	0
Total	14

FIGURA 7-1: INFORME GENERAL DE VULNERABILIDADES

INFORME DE VULNERABILIDADES EN EL SISTEMA OPERATIVO

Informe de vulnerabilidades en el sistema operativo, las cuales se encuentran clasificadas por categorías, backdoors, registro, parches de actualización y lo servicios que se encuentran activos.

Vulnerability Distribution (by Category)



Vulnerability Category	Severity Distribution			
	Total	High	Med.	Low
Backdoor	1	1	0	0
Missing Updates	24	22	1	1
Registry	4	0	0	4
Services	72	26	0	46

FIGURA 7-2: INFORME DE VULNERABILIDADES EN EL SISTEMA OPERATIVO

INFORME DE LAS PRINCIPALES APLICACIONES VULNERABLES

A continuación se encuentran detallados los productos más vulnerables dentro de esta auditoría, se encuentran clasificados por el total del número de vulnerabilidades y su nivel de riesgo.

Top 10 Most Vulnerable Products

Product	Severity Distribution			
	Total	High	Med.	Low
Office	14	14	0	0
Windows	11	8	1	2
MySQL 5	1	1	0	0
Windows NT	1	0	0	1
Developer Tools, Runtimes, and Redistributables	1	0	0	1

TABLA 7-1: INFORME DE LAS PRINCIPALES APLICACIONES VULNERABLES

INFORME DE EQUIPOS

DIRECCION IP	PUERTOS ABIERTOS	VULNERABILIDADES
192.168.6.170	20	6
192.168.6.171	10	5
192.168.6.172	10	5
192.168.6.175	10	4
192.168.6.177	10	5
192.168.6.178	20	6
192.168.6.179	10	5
192.168.6.180	10	5
192.168.6.182	10	5
192.168.6.183	10	5
192.168.6.185	23	5
192.168.6.186	10	5
192.168.6.200	10	4

TABLA 7-1: INFORME DE EQUIPOS

INFORME DE EQUIPOS

Los equipos con vulnerabilidades altas se detallan a continuación ya que deben ser tomadas soluciones de inmediato.

Equipo 192.168.6.170

Herramienta utilizada. Languard

Hallazgos.

- Se puede abrir una conexión mediante la cuenta de administrador ya que no posee contraseña.
- El servidor pop3 puede ser vulnerable a un ser controlado remotamente por un exploit.

Nivel de Vulnerabilidad. Alta

Acciones a Realizar.

- Se debe establecer una contraseña de administrador.

- Se debe detener el servicio de pop3 si el equipo no es un servidor pop3.

Equipo 192.168.6.171

Herramienta utilizada. Languard

Hallazgos.

- Se puede abrir una conexión mediante la cuenta de administrador ya que no posee contraseña.
- El servidor pop3 puede ser vulnerable a un ser controlado remotamente por un exploit.

Nivel de Vulnerabilidad. Alta

Acciones a Realizar.

- Se debe establecer una contraseña de administrador.
- Se debe detener el servicio de pop3 si el equipo no es un servidor pop3.

Equipo 192.168.6.178

Herramienta utilizada. Languard

Hallazgos.

- Se puede abrir una conexión mediante la cuenta de administrador ya que no posee contraseña.
- El servidor pop3 puede ser vulnerable a un ser controlado remotamente por un exploit.

Nivel de Vulnerabilidad. Alta

Acciones a Realizar.

- Se debe establecer una contraseña de administrador.
- Se debe detener el servicio de pop3 si el equipo no es un servidor pop3.

Equipo 192.168.6.182

Herramienta utilizada. Languard

Hallazgos.

- Se puede abrir una conexión mediante la cuenta de administrador ya que no posee contraseña.
- El servidor pop3 puede ser vulnerable a un ser controlado remotamente por un exploit.

Nivel de Vulnerabilidad. Alta

Acciones a Realizar.

- Se debe establecer una contraseña de administrador.
- Se debe detener el servicio de pop3 si el equipo no es un servidor pop3.

Equipo 192.168.6.200

Herramienta utilizada. Languard

Hallazgos.

- Se puede abrir una conexión mediante la cuenta de administrador ya que no posee contraseña.
- El servidor pop3 puede ser vulnerable a un ser controlado remotamente por un exploit.

Nivel de Vulnerabilidad. Alta

Acciones a Realizar.

- Se debe establecer una contraseña de administrador.
- Se debe detener el servicio de pop3 si el equipo no es un servidor pop3.

DESCRIPCION DE LOS PUERTOS ABIERTOS POR EQUIPO

DIRECCION IP	PUERTOS ABIERTOS
192.168.6.170	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3 **119** Network News Transfer Protocol (NNTP) **135** DCE endpoint resolution **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S) **3306** MySQL database system **123** Network Time Protocol (NTP) **137** NetBIOS NetBIOS Name Service **138** NetBIOS NetBIOS Datagram Service **445** Microsoft-DS SMB file sharing **500** Internet Security Association and Key Management Protocol (ISAKMP) **1026** Messenger, If this service is not installed beware could be Trojan: Remote Explorer 2000 **1900** Microsoft SSDP Enables discovery of UPnP devices **4500** IPsec NAT traversal (RFC 3947)
192.168.6.171	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares

	563 NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S)
192.168.6.172	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S)
192.168.6.175	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S)
192.168.6.177	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S)
192.168.6.178	**25** Simple Mail Transfer Protocol (SMTP)

	110 Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **135** DCE endpoint resolution **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S) **3306** MySQL database system **5432** PostgreSQL database system **123** Network Time Protocol (NTP) **137** NetBIOS NetBIOS Name Service **138** NetBIOS NetBIOS Datagram Service **445** Microsoft-DS SMB file sharing **500** Internet Security Association and Key Management Protocol (ISAKMP) **1900** Microsoft SSDP Enables discovery of UPnP devices **4500** IPsec NAT traversal (RFC 3947)
192.168.6.179	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S)
192.168.6.180	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS)

	995 Post Office Protocol 3 over TLS/SSL (POP3S)
192.168.6.182	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S)
192.168.6.183	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S)
192.168.6.185	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **135** DCE endpoint resolution **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S) **123** Network Time Protocol (NTP) **137** NetBIOS NetBIOS Name Service **138** NetBIOS NetBIOS Datagram Service **445** Microsoft-DS SMB file sharing

	500 Internet Security Association and Key Management Protocol (ISAKMP) **1900** Microsoft SSDP Enables discovery of UPnP devices **1977** Cisco TCO **1985** Cisco HSRP, If this service is not installed beware could be Trojan: Black Driver **1994** Cisco STUN-SDLC (Serial Tunneling - Synchronous Data Link Control) protocol **1998** Cisco X.25 over TCP (XOT) service **2612** QPasa from MQSoftware **4500** IPsec NAT traversal (RFC 3947)
192.168.6.186	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S)
192.168.6.200	**25** Simple Mail Transfer Protocol (SMTP) **110** Post Office Protocol 3 (POP3) **119** Network News Transfer Protocol (NNTP) **139** NetBIOS NetBIOS Session Service **143** Internet Message Access Protocol (IMAP) **445** Microsoft-DS Active Directory, Windows shares **563** NNTP protocol over TLS/SSL (NNTPS) **587** e-mail message submission (SMTP) **993** Internet Message Access Protocol over SSL (IMAPS) **995** Post Office Protocol 3 over TLS/SSL (POP3S)

TABLA 7-2: DESCRIPCION DE LOS PUERTOS ABIERTOS POR EQUIPO

Conclusiones

- El servidor principal del ITSCO con la dirección 172.16.2.1 se encuentra en buenas condiciones pero no las óptimas de seguridad, por carecer de un sistema operativo actualizado.

- El medio de seguridad para intrusos está compuesto de un firewall, el cual no es totalmente efectivo si el ataque se realizara a través de múltiples direcciones y al mismo tiempo.

- Los equipos que se encuentran compartiendo las aplicaciones del servidor principal, pertenecientes a empleados del ITSCO, no se encuentran dentro de un directorio activo, por lo que un empleado interno tiene el acceso y credenciales necesarias para instalar cualquier tipo de software para intrusión.

- Los laboratorios se encuentran dentro de un grupo de trabajo, por lo cual no se tiene un nivel de jerarquía ni limitaciones para instalación de software, el total acceso al internet desde estos se podría reflejar en un ataque de gran magnitud

por parte de los estudiantes que podría llevar al colapso de los sistemas de aplicación.

- Los equipos en los laboratorios se encuentran con vulnerabilidades altas, con puertos suficientes para poder tomar control de los mismos y llevar a cabo un hacking malicioso, colapsando así sus sistemas operativos y comprometiendo el rendimiento de los equipos.

Recomendaciones

- En el servidor principal se debe realizar una instalación actual del sistema operativo Cent, para así proveer de mayor estabilidad a las aplicaciones ya que cada versión de sistema operativo tiene también su vulnerabilidad por lo que su versión más reciente corrige los errores de la anterior.

- Se debería implementar un IDS (Sistema de detección de intrusos) para poder realizar un monitoreo de la red y generar reportes sobre la actividad en la misma, o a su vez un honeypot para proteger la integridad de los datos, se lo debería colocar ya sea en el mismo segmento de la DMZ o fuera de él, de esta forma se podría controlar si un intruso quiere tener acceso a la red y poder seguir sus pasos, mientras la información real estaría protegida.

- Para tener un control sobre las actividades de los usuarios internos del ITSCO se debería implementar un directorio activo para poder restringir la utilización e instalación de software no autorizado en sus equipos, como herramientas para

hacking, backdoors o troyanos, y a la vez se tendría un control sobre que usuario ingresó, así como la fecha y la hora.

- En el laboratorio de cómputo se deberían implementar directorios activos para evitar el mal uso del internet, o evitar por medio de restricciones del mismo sistema operativo la instalación de software ajeno a lo laboral y restringir descargas de aplicativos, se deberían crear cuentas de usuario limitadas o de invitado para este fin.

- Para el correcto funcionamiento y estabilidad de los sistemas operativos en los equipos del laboratorio de computo se recomienda la instalación de un software antivirus corporativo, de esta forma se podrán evitar intrusiones externas, y solucionar problemas con los procesos actuales, se debe tomar muy en cuenta las actualizaciones de parches de seguridad, ya que al ser sistemas operativos de Microsoft son los más vulnerables a recibir ataques por sus fallas de seguridad, se debería realizar la instalación de sistemas operativos open source, para poder ganar mayor estabilidad y evitar inconsistencias en los equipos.

ANEXO8. CARTA DE CONFIDENCIALIDAD

CARTA DE CONFIDENCIALIDAD

Yo José González Lozano con CI. 1714407150, alumno del sexto nivel de la carrera de Ing. en Sistemas en calidad de desarrollador de un hacking ético a la red del ITSCO, me comprometo a no divulgar la información sobre la infraestructura de la red interna, la cual fue confiada a mi persona para el desarrollo de mi tesis y usar dicha información únicamente con fines educativos y de manera confidencial, teniendo completo conocimiento de las consecuencias legales como institucionales al faltar a este compromiso.

Atentamente

José González

1714407150

ANEXO9. CARTA DE ENTREGA DEL INFORME FINAL

CARTA DE ENTREGA DEL INFORME FINAL

Luego de las pruebas realizadas a la red interna del ITSCO y elaborado el informe final, se entrega la investigación a la institución sobre los resultados obtenidos en cada una de las áreas objeto de estudio, en dicho informe se detallan los equipos en los que se realizó las pruebas necesarias con cada uno de sus resultados, para lo cual firman las partes involucradas, en este caso, el desarrollador del hacking ético y la persona encargada del área informática del ITSCO.

Ing. Octavio Cóndor

Área Informática ITSCO

Sr. José González

Desarrollador del Hacking Ético