Security Policies of Corporate Multiservice Network; Employing Ethical Hacking

Hidalgo Y. Jessica, Ing.[1], Tupiza L. Diana, Ing.[1] and Sánchez A. Tarquino, MSc.[1]
[1] Escuela Politécnica Nacional, Ecuador, pao7_2010@hotmail.com, diana_tupiza@hotmail.com, tarquino.sanchez@epn.edu.ec

***Abstract*— Organizations have long had major security concerns when transmitting data outside of a closed system. Establishing information security policies for a large organizational network that transmits sensitive data in voice, video, and other forms is of key importance in information security. This article discusses existing vulnerabilities in an organizational network, previous theory and research, and then recommends ways to prevent attacks using ethical hacking techniques.**

The system under consideration is a multiservice network infrastructure. By performing a series of attacks on a honeynet replica of the system in question, the project tests the effectiveness of employing ethical hacking to detect network vulnerabilities and risks while testing the effectiveness of proposed procedures to ensure network security.

We found that the two most important factors in maintaining a secure multiservice network are (1) creating a network in which external ports are closed and carefully protected and (2) establishing rules and regulations for the users, particularly regarding password security, that are strictly enforced. Thus, ethical hacking allows regulations and procedures to be created to address the security issues of a particular network system. The implementation of these policies could be implemented following the ISO 27001*.

Keywords — Ethical hacking, Seguridad en redes, LAN, Honeynet

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2016.1.1.251
ISBN: 978-0-9822896-9-3
ISSN: 2414-6390

*

Políticas de Seguridad de una Red Multiservicios Corporativa; Utilizando Hacking Ético

Hidalgo Y. Jessica, Ing.[1], Tupiza L. Diana, Ing.[1] and Sánchez A. Tarquino, MSc.[1]
[1] Escuela Politécnica Nacional, Ecuador, pao7_2010@hotmail.com, diana_tupiza@hotmail.com, tarquino.sanchez@epn.edu.ec

Resumen– Las organizaciones han tenido desde hace mucho tiempo problemas de seguridad durante la transmisión de datos desde fuera de un sistema cerrado. El establecimiento de políticas de seguridad de la información es clave para la seguridad de la información para una red multiservicios de una organización que transmite datos sensibles; de voz, video y otras formas de información. Previo al marco teórico y la investigación realizada, este artículo analiza las vulnerabilidades existentes en una red de datos de una organización corporativa, y, a continuación se recomienda las formas de prevenir ataques utilizando técnicas de hacking ético.

El sistema en cuestión es una infraestructura de red multiservicio. Mediante la realización de una serie de ataques contra una réplica virtual de la red del sistema de la organización, el proyecto pone a prueba la eficacia del empleo de hacking ético para detectar vulnerabilidades y los riesgos de la red mientras se prueba la eficacia de los procedimientos propuestos para garantizar la seguridad de la red.

Se encontró que los dos factores más importantes en el mantenimiento de una red multiservicio segura son (1) la creación de una red en la que los puertos externos están cerrados y cuidadosamente protegidos y (2) el establecimiento de normas y reglamentos para los usuarios, en particular en relación con la seguridad de contraseñas, que son estrictamente personales. Por lo tanto, hacking ético permite que los reglamentos y procedimientos que se han creado hagan frente a los problemas de seguridad de un sistema de red en particular. La aplicación de estas políticas podrá implementarse siguiendo la norma ISO 27001[2].

Palabras Clave -- Hacking ético, Seguridad en redes, LAN, Honeynet.

I. INTRODUCCIÓN

El activo más importante en las organizaciones públicas y privadas, es la información que se administra. Entre más grande es la organización más grande es la información y el interés de mantener la seguridad en la red de datos. [1]

La seguridad no es solamente el crear usuarios y contraseñas, es implementar políticas que garanticen la seguridad tanto física como lógica de la información. Se debe asegurar la privacidad de la información y protegerla tanto de daños no intencionados como deliberados.

Se analizó una empresa corporativa de la ciudad de Quito, los servicios de la intranet que ofrece, la seguridad informática, además se verifico el estado de los equipos de conectividad como routers y switches, así como también los servidores de monitoreo y de telefonía IP.

Como resultado de este análisis se evidenció que en general las empresas pueden ser blanco de ataques externos que buscan violentar la información que administran, debido a que los principales equipos de comunicación presentan configuraciones básicas de seguridad no acordes a la sensibilidad de la información que gestionan.

Por ello, mediante la utilización de hacking ético se determinarán las vulnerabilidades existentes y se establecerán políticas de seguridad que servirán para que el personal del área de informática pueda hacerle frente a los ataques que pudiera sufrir la institución

II. MARCO TEÓRICO

Una red es la disposición física o virtual de equipos y dispositivos, que permiten compartir información y recursos a través de un medio de comunicación.

Actualmente, las redes permiten garantizar calidad de servicio (QoS)[3] y asegurar varios parámetros de red, tales como: tasa de error, ancho de banda, throughput, retraso en la transmisión, disponibilidad, etc. [2]

Los servicios corporativos de red por lo general son:

A. Servicios de red

- FTP (File Transfer Protocol)**:** El servicio FTP permite la transferencia de archivos entre un servidor y un

[2] ISO 27001: Es un estándar para la seguridad de la información

[3] QoS: Conjunto de tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo determinado.

computador (local y/o remoto) conectados a la red. Al utilizar esta aplicación se facilita el intercambio de archivos.[3]

- DNS (Domain Name System): Este protocolo permite traducir un nombre de dominio (ej. www.google.com) a una dirección IP (ej.173.194.75.103), lo que facilita al usuario realizar la búsqueda de un determinado servidor en la red.
- DHCP (Dynamic Host Configuration Protocol): Permite asignar direcciones IP y otras configuraciones de manera dinámica a los host de una red por un intervalo de tiempo determinado.
- Proxy: El servidor proxy actúa como un intermediario entre la intranet y la extranet, permitiendo registrar y restringir cierto tipo de tráfico que llevan a cabo los usuarios de la red corporativa
- Servidor Web: Los servidores web son aquellos cuya tarea es alojar sitios y/o aplicaciones, las cuales son accedidas por los clientes utilizando un navegador que se comunica con el servidor utilizando el protocolo HTTP (hypertext markup language).[4]
- VOIP: Es un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP (Protocolo de Internet).[5]
- Correo Electrónico: Los protocolos SNMP y POP de la capa aplicación basado en el modelo cliente/servidor, que se utiliza para el intercambio de mensajes.

B. Seguridad en la Red

En sus inicios las redes de computadoras eran utilizadas por universidades para el intercambio de información y a nivel corporativo para la compartición de impresoras, por tal motivo la seguridad quedaba en segundo plano. En la actualidad los múltiples servicios que prestan las redes informáticas y de comunicación como; servicios bancarios, compras online, homeworkers, etc., promueven la existencia de ataques a la integridad de los datos en las transacciones en linea.

Al viajar la información a través de diferentes medios de comunicación (cableado e inalámbrico) torna vulnerable la confidencialidad de la misma, por tal razón en los últimos años se han encontrado formas de prevenir los ataques a las redes corporativas.

Existen dos tipos de atacantes, los activos que son aquellos que provocan daños y modificaciones al funcionamiento normal de la red y los pasivos que no producen ninguna alteración, pero que sin embargo, utilizan la información capturada de manera fraudulenta [6]. Por tal razón la protección de los elementos activos y pasivos de la red se debe priorizar en tres ejes fundamentales:

- Prevención: Se deben tomar medidas que eviten que la información sea modificada, dañada o hurtada.
- Detección: Se deben tomar acciones que permitan identificar cuándo, cómo, dónde y quién dañó un determinado elemento.
- Reacción: La capacidad de tomar medidas correctivas una vez ocurrido un ataque a la seguridad de la red.

Para proporcionar la seguridad adecuada a una red de datos es necesario enfocarse en los siguientes parámetros:

- Confidencialidad: Asegurar que únicamente la persona autorizada tendrá acceso a la información (cifrado/descifrado, privacidad).
- Integridad: Asegurar que los datos son correctos, que no han sido modificados en el trayecto del origen al destino (firma digital, intercambio de autenticación).
- Disponibilidad: Asegurar que una entidad pueda acceder cuando desea a un recurso o servicio para el que está autorizado (servidores espejo, replicación de datos, enlaces redundantes).
- Autenticación: Asegurarse de que la entidad es quien dice ser mediante la identificación, para de esta manera aseverar que las transacciones se efectúan entre entidades legítimas (contraseñas, certificados, biométricos).

C. Hacking Ético

Inicialmente los procesos informáticos no eran objeto a ningún tipo de estudio de seguridad; los administradores y técnicos estaban encargados de realizar pruebas para encontrar posibles agujeros en la seguridad de la red. Posteriormente con el desarrollo tecnológico y la presencia de equipos y dispositivos que permiten gestionar grandes volúmenes de información sensible, se dio como resultado la aparición de hackers, personas que tomaban como retos intelectuales corromper la seguridad de los sistemas, descifrar contraseñas y causar daños a la integridad de la información.

En la actualidad, la palabra hacker no se encuentra relacionada únicamente con un delito, sino a la capacidad de encontrar fallos en la seguridad de los sistemas para proporcionar una solución; de esta manera aparece el hacking ético, que no es más que un método basado en el ataque deliberado a los sistemas para encontrar vulnerabilidades en la seguridad y posteriormente corregirlos e impedir que un atacante malicioso cause daños graves a los sistemas informáticos de la organización. [7]

III. DIAGNOSTICO DE LA RED CORPORATIVA MULTISERVICIOS Y PROPUESTA DE SEGURIDAD DE SU INTRANET

A. Descripción del problema

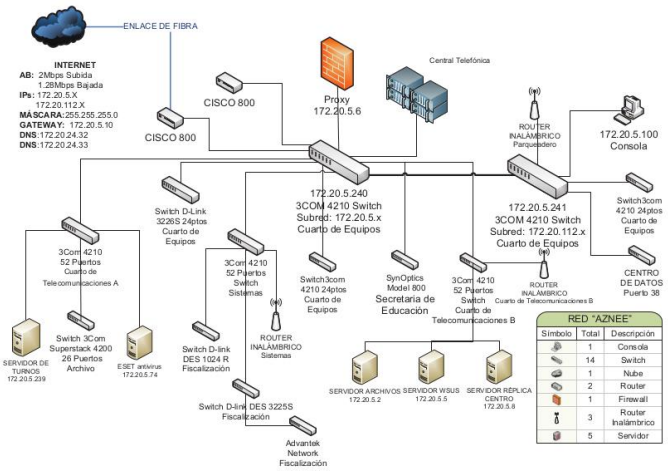


Fig.1 . Diagrama de la red inicial.
Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D., Sánchez T.)

La red analizada Fig. 1, corresponde a la sucursal de una empresa pública, que depende de una oficina matriz, cuenta con una red de voz y datos que no cumple con estándares de calidad de servicio, cableado estructurado deteriorado y sin organización física, insuficientes políticas de seguridad de servidores, personal técnico no capacitado en seguridad informática, escasos mecanismos de seguridad de servidores y servicios, medios de transmisión inadecuados entre cuartos de telecomunicaciones. Así:

El cableado estructurado está constituido por cable UTP categoría 5, el cual no posibilita el diseño de una red multiservicios. Cuenta con 3 racks en donde se ubican los principales equipos que proveen de conectividad a la red, además de existir otros equipos secundarios como switches distribuidos según la necesidad de extender nuevos puntos para la red.

Tiene alrededor de 150 usuarios y debido al constante crecimiento de los mismos, se ha extendido al uso de dos subredes: 172.20.5.0/24 y 172.20.112.0/24, las cuales están distribuidas indistintamente sin orden ni gestión.

Sus principales servicios son: correo electrónico, página Web, recursos de impresión, carpetas compartidas, proxy, antivirus, servidor de réplica. Además se identificó que la empresa ha sufrido varios ataques informáticos, entre ellos se destaca el realizado por "Anonymous", donde se verifico que se afectó al servidor web de la empresa pública paralizando sus actividades por 24 horas, así como también una administración deficiente de las contraseñas de equipos de conectividad y servidores.

B. Rediseño de la Intranet

Se planea implementar una nueva solución de cableado estructurado que permita mejorar la relación señal a ruido y una mayor fiabilidad en los servicios actuales, además mejorar la velocidad de acceso a las aplicaciones futuras.

Los lineamientos base para el rediseño del cableado estructurado se basan en las siguientes normas:

- ANSI/TIA 568.C, agrupa los requerimientos actuales de los sistemas, tanto en características y rendimiento de los componentes como en su estructura.
- ANSI/TIA 569.B, determina los requerimientos de rutas y espacios de telecomunicaciones.
- ANSI/TIA 606.A, define la documentación y administración para el etiquetado y registro de las distintas secciones de la red, sean éstos cables, patch panel, patch cords, espacios de telecomunicaciones y ductos.

Para el rediseño de la intranet se establece el siguiente procedimiento:

1) El sistema de cableado estructurado utilizará cable categoría 6 UTP, con una velocidad de 1 Gbps y un ancho de banda de 250 MHz, lo que permitirá tener una infraestructura que se adapte a aplicaciones que demanden mayores recursos de la red.
2) Reubicación de la acometida de servicios de telecomunicaciones hacia el cuarto de equipos, de esta forma se asegura la no manipulación de los enlaces de datos, que son el eje principal del funcionamiento de la empresa pública.
3) Reubicación de los equipos activos instalados en los gabinetes de pared, ubicados actualmente en las oficinas hacia el cuarto de telecomunicaciones para la gestión adecuada de los enlaces.
4) Proveer la seguridad física necesaria a los cuartos de telecomunicaciones para que no sean sensibles a ataques malintencionados.
5) Proveer de enlaces de fibra óptica multimodo para comunicar los cuartos de telecomunicaciones con el cuarto de equipos de la empresa.

En base al análisis de problemas se rediseño la red la cual se indica en la Fig. 2.

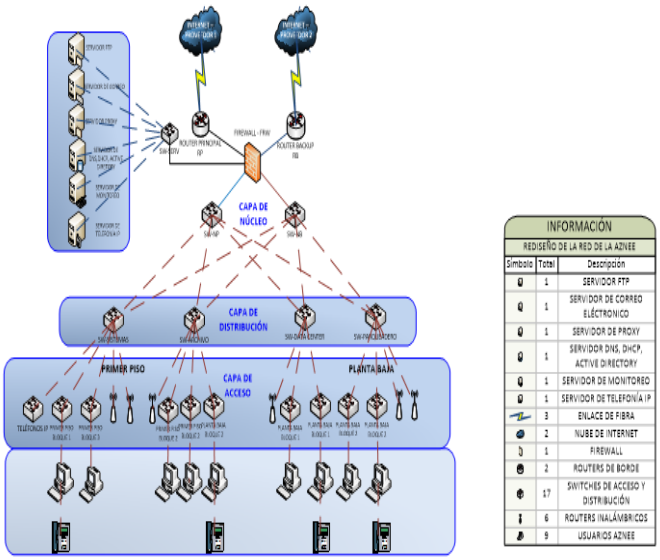


Fig.2 . Diagrama del rediseño
Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D.,Sánchez T.)

C. *Sistema de seguridad*

Para determinar los parámetros de seguridad que dispone la empresa, se realizó un estudio dirigido a 10 informantes calificados con base a preguntas concernientes a la seguridad informática del sistema. En la Tabla I se describe la información obtenida.

TABLA I
RESULTADOS DEL ESTUDIO A INFORMANTES CALIFICADOS

Parámetro de Seguridad consultado	Descripción de parámetro de seguridad	Fortaleza de la empresa	Debilidad de la empresa
Backups	Existen copias almacenadas en una empresa externa de los servidores.	Existen copias almacenadas fuera de la institución.	No existe política que establezca un cronograma para la realización de backups.
Lista de control de acceso	Access Control List ACLs implementadas y controladas por la Dirección informática de la empresa.	Existe un filtrado de paquetes basando en criterios determinados por la Dirección informática	Desconocimiento por parte del área de sistemas de la empresa del criterio con el que se realiza la configuración de ACLs.
Firewall	Controlado e implementado en el edificio principal de la empresa pública.	Existe una barrera primaria para bloquear el acceso no autorizado.	No se encuentra ubicado dentro de la empresa.
Antivirus	El software implementado en la institución es ESET Smart Security Corporativo.	Detección de amenazas informáticas.	
Antispam	El software implementado en la institución es ESET Smart Security Corporativo.	Filtrado de correo basura o no deseado.	
Proxy	Implementado en la empresa donde el acceso a internet es limitado por cargo y por usuario.	Optimización del ancho de banda restringiendo el acceso a páginas definidas por el administrador.	Falta de procedimientos para establecer privilegios de acceso a páginas web.
Autenticación	El departamento financiero utiliza un token valido para firma electrónica	Disminución en el tiempo de trámites legales y bancarios.	No definida.
	Contraseñas de mediano grado compuesto por números y letras (5 a 8 caracteres).	No definida.	Cambio de contraseña únicamente cuando el Usuario pierde sus credenciales.

Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D.,Sánchez T.)

Una vez identificado subjetivamente las vulnerabilidades de la red de datos se procedió a utilizar las técnicas de hacking ético con el propósito de evaluar técnicamente la red, con este fin se implementó una red de prueba virtual utilizando el software honeynet, en la cual se realizarán los ataques informáticos en busca de brechas en la seguridad. Los pasos a seguir son los siguientes:

1. Realización de la red de prueba- Honeynet
2. Utilización de técnicas de hacking ético
3. Análisis de resultados

1) *Realización de la red de prueba- Honeynet*

La honeynet se implementó con las configuraciones de los servicios de la red real, para emular de manera virtual los diversos ataques que puede sufrir la red y recolectar información de intrusiones para el análisis, monitoreo e investigación de vulnerabilidades y a la postre realizar los correctivos sobre dicha red.
Los componentes del sistema se detallan a continuación:

- **Honeypots**: Conjunto de computadores destinados para ser atacados, simulando ser sistemas débiles.
- **Honeywall:** Software basado en Linux que contiene herramientas necesarias para crear una honeynet, con el objetivo de filtrar el trafico producido por los honeypots sin interferir en su normal funcionamiento.
  Las herramientas que utiliza son:

  ✓ **Iptables:** Es un programa que permite el filtrado de paquetes que ingresan y salen de la honeynet.
  ✓ **P0f:** Es un programa utilizado para el monitoreo del tráfico que ingresa a la honeynet.
  ✓ ***Snort:*** Es un IDS (Intrusion Detection System) de red, que actúa como gateway para toda la información recopilada en honeynet.

La implementación virtual de la honeynet se realizó utilizando la herramienta de virtualización VirtualBox, donde constarán los sistemas operativos y aplicaciones que se maneja en la red.

Los honeypots serán configurados en máquinas virtuales con las copias de las imágenes de los discos de dos servidores

proporcionados por la empresa. *Cabe recalcar que los servicios principales están instalados en la empresa matriz y no en la administración analizada, por lo que no se puede realizar un análisis más completo sobre la red.*
Las imágenes de los discos duros que se obtuvieron son:

- Antivirus
- Archivos (Windows Server)

Los servicios restantes fueron simulados con la utilización del software ZENTYAL, el cual fue instalado en una máquina virtual y configurado con los siguientes servicios:

- **DNS:** Servicio de nombres de dominio
- **Email:** Servicio de correo electrónico
- **Proxy:** Bloqueo de URLs y puertos no autorizados.
- **Lighweight Directory Access Protocol (LDAP):** Servicio de directorio activo para entornos Linux similar a Active Directory en entornos Windows.

En la Fig. 3 se muestra el diseño de la honeynet que se implementó, la misma que será ubicada fuera de la red real.

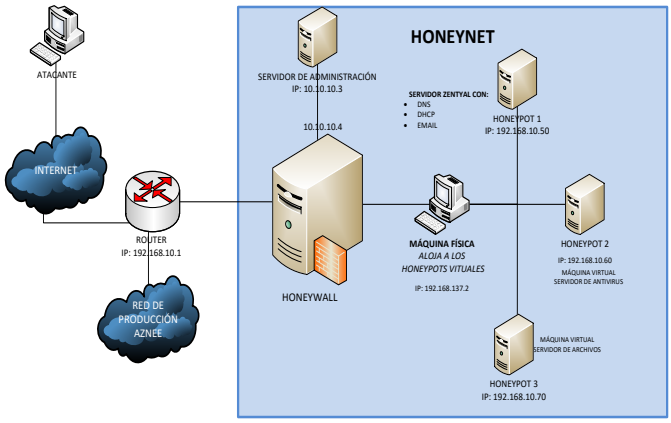


Fig. 3 Diagrama de la honeynet
Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D.,Sánchez T.)

2) *Utilización Del Hacking Ético Para Determinar Vulnerabilidades*

Partiendo de la premisa de que la información en la actualidad es uno de los activos más importantes en cualquier empresa tanto pública como privada, este recurso tiene un valor inconmensurable y para el caso particular de la empresa en análisis, que gestiona documentos sensibles de diversa naturaleza departamental, como son: catastros, predios, permisos de funcionamiento, patentes, etc. se debe tener mayor precaución con la gestión de los mismos, por lo que para mitigar los riesgos dentro y fuera de la red, se realizó un rediseño total de la infraestructura tecnológica de la empresa.

Para realizar un correcto rediseño de la red multiservicios se identifica las vulnerabilidades existentes; se utiliza técnicas de hacking ético que no son más que la búsqueda de debilidades mediante el manejo de herramientas informáticas llevadas a cabo por una persona especializada en ataques a sistemas y servicios informáticos.

Los resultados obtenidos a partir de estas técnicas permitirán tomar acciones de prevención necesarias, mitigando posibles ataques maliciosos. Las técnicas a utilizar son:

- Footprinting
- Scanning
- Enumeration
- Troyanos y puertas traseras
- Ingeniería Social

A continuación el detalle de los ataques realizados y los resultados obtenidos:

*Footprinting***;** mediante esta técnica es posible determinar los accesos ocultos o puertas traseras (BackDoors) para vulnerar una red. Permite recolectar datos relevantes de una empresa, persona, dominio o cuentas de correo antes de realizar ataques; la herramienta utilizada es el software Maltego [8], mismo que obtiene información concerniente al dominio de la empresa analizada. Este es el primer paso para determinar qué tan expuesta se encuentra una organización en el internet, y tratar de proporcionar seguridad a cada entrada del sistema de la empresa.

*Scanning***;** es una técnica pre-ataque, permite escanear puertos y vulnerabilidades de los diferentes equipos dentro de una red para identificar posibles agujeros de seguridad, el comando utilizado para ejecutar esta técnica es Nmap[4]. Se realizó el escaneo de puertos de los servidores, obteniendo la información necesaria para determinar políticas de seguridad que mejoren la administración de acceso a los puertos.

Este análisis se realizó en cada uno de los servidores de la red. El resumen consolidado de los puertos abiertos por servidor se muestra en la Tabla II.

TABLA II
PUERTOS ABIERTOS DENTRO DE LOS SERVIDORES

Servidor	Puertos abiertos
DHCP	80, 135, 139, 445, 3389, 49152, 49153, 49154.

[4] Nmap: Network Mapper (Mapeador de puertos de red)

DNS1	53, 88, 135, 139, 389, 445, 593, 636, 3268, 3269, 3389, 49152, 49153, 49154.
DNS2	22, 23, 53, 88, 135, 139, 389, 445, 464, 593, 636, 1026, 1433, 1434, 1443, 1500, 1501, 1503, 1521, 1503, 1521, 1524, 1533, 3268, 3269, 3389, 5555, 5900, 49152, 49153, 49154, 49155, 49157, 49158.
Turnos	21, 80, 90, 135, 139, 445, 500, 990, 1947, 5000, 5001, 5002, 5432, 5500, 5800, 5900, 5901, 7001, 49152, 49153, 49154, 49155, 49157, 49158.
Aplicaciones	No se tuvo acceso al servidor dado que es una réplica del servidor de la matriz.

Fuente: Diagrama de autoría propia (Hidalgo J. y Tupiza D.)

En la Tabla III, se muestra el listado de los puertos abiertos encontrados en los servidores ligados a las vulnerabilidades que representan cada uno de ellos y el grado de incidencia en el sistema.

Esta información permitirá determinar los puertos que deben permanecer abiertos para que los procesos se desarrollen con normalidad y los que necesitan ser cerrados para minimizar posibles violaciones de seguridad.

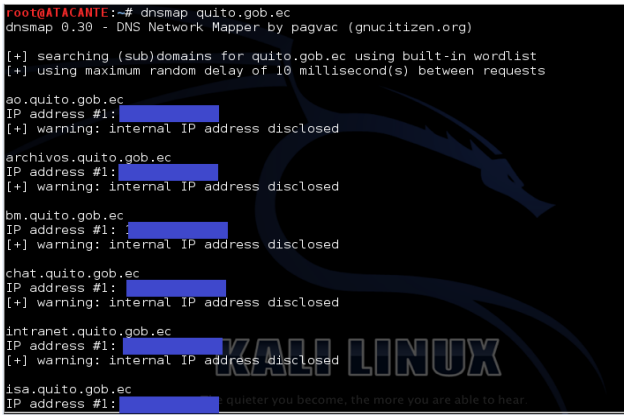
TABLA III
PUERTOS ABIERTOS SENSIBLES A ATAQUES

Puerto abierto	Servicio	Vulnerabilidad	Grado
23/tcp	telnet	Las contraseñas de Telnet no se encuentran encriptadas por lo que son vulnerables a ataques de sniffing[5].	Alto
135/tcp	msrpc	Funcionaría como puerta trasera dando acceso al servidor de manera remota, este puerto viene habilitado por defecto.	Alto
139/tcp	netbios-ssn	Establece un servicio de sesión que emula TCP con un equipo remoto y permite sondear el tráfico compartido como archivos e impresoras	Medio
445/tcp	microsoft-ds	Permite la transferencia de archivos de forma remota, y un atacante puede utilizarlo para provocar desbordamiento de memoria.	Medio
3389/tcp	ms-wbt-server	Permite acceso remoto al equipo y la manipulación de los archivos del sistema.	Alto
5555/tcp	freeciv	Permite acceso por puerta trasera mediante una secuencia de comandos para causar fallos.	Medio
5900/tcp	VNC	Permite conexión remota a los servidores.	Alto
1521/tcp	Oracle database	Puerta de escucha del servidor de base de datos Oracle.	Alto
5432/tcp	PostgreSQL	Puerto de escucha del servidor de base de datos PostgreSQL	Alto
80/tcp	HTTP	Puerto de acceso web.	Alto
21/tcp	FTP	Puerto de transferencia de archivos.	Medio
49152,49153, 53, 49154,49155,88, 593, 636, 3268, 3269,22,23 ,389, 464,1026, 1434 433,1443, 1500, 90,1501,1503, 1524, 1533, 5900, 49158,500, 9157, 990,1947, 5000, 5002,5500, 5800.		Puertos de uso general manejados por Windows Server, Active Directory y LDAP.	Bajo o nulo

Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D., Sanchez T.)

Como se puede apreciar en la Tabla III, existen puertos de escucha que permiten conectarse a base de datos de la matriz, sin embargo, son réplicas que deberían ser accedidas a través de los servicios requeridos y no visibles para todos, y más bien presentan un grado de vulnerabilidad alto, por lo que se procederá a realizar las acciones correctivas necesarias para mitigar o eliminar los puertos que mantengan un riesgo de seguridad alto.

Enumeration; **e**ste pre-ataque permite enumerar los recursos dentro del objetivo como por ejemplo: identificar grupos, cuentas de usuario, contraseñas y recopilar información de recursos compartidos (impresoras, dispositivos de almacenamiento externo, etc.), con esta información un atacante podría conseguir escalar privilegios hasta llegar al nivel del administrador e instalar software malicioso que le permitirá tener control sobre la máquina, recolectar o robar datos y dejar puertas traseras para próximas intrusiones como se indica en la Fig. 4.



[5] Sniffing: Técnica de escucha del tráfico de la red.

Fig. 4 Ejemplo de información encontrada con Dnsmap
Fuente: Diagrama obtenido de software Kali Linux

En la Fig. 4, se muestran los subdominios pertenecientes a www.quito.gob.ec (empresa analizada), que son invisibles para el público pero que existen en los registros de DNS y que pueden ser explotados mediante ataques basados en dominios, por confidencialidad no se muestran las direcciones IP respectivas.

Este es el siguiente paso que ejecuta un atacante cuando no ha podido acceder a la información de la empresa pública mediante "footprinting" o "scanning", regularmente son archivos o dominios que no están siendo usados por los administradores de la red y que cuentan con información útil para el atacante.

Troyanos y puertas traseras; los troyanos son programas que se hacen pasar por genuinos, cuyo verdadero objetivo es ejecutar software malicioso en el equipo donde sean instalados. Al ejecutarse se auto incluye en la rutina de inicio del equipo y desde ese instante, puede vigilar el equipo hasta que el usuario se conecta a Internet. Las puertas traseras o backdoors por su parte son bugs[6] que permiten acceso a un equipo de forma remota, aprovechan la arquitectura de internet que se basa en el modelo cliente-servidor. Para determinar qué tan expuesta se encuentra la red a un ataque de esta naturaleza se utilizó la herramienta Ettercap [9]. Con este software se envenenó la red con paquetes ARP[7] para producir un desbordamiento de la memoria caché de los equipos de red y capturar paquetes de información bajo la técnica de hombre en el medio. Esta técnica fue bloqueada por el antivirus instalado en las máquinas de la empresa, como se indica en la Fig. 5.

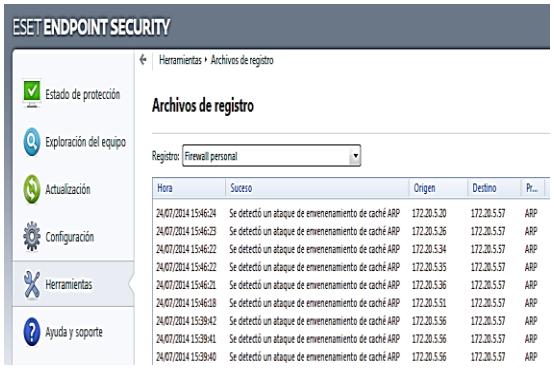


Fig. 5 Archivo de registro del antivirus
Fuente: Diagrama obtenido del Servidor de antivirus ESET

Ingeniería Social; la ingeniería social es una técnica que se basa en el engaño o abuso de confianza de personas inescrupulosas que obtienen información sensible de los usuarios y personal de la entidad, y la utilizan para realizar ataques maliciosos a la integridad de la institución. En la empresa analizada existe personal ajeno a la institución que de una u otra forma tiene acceso a información sensible o confidencial, por citar un ejemplo; se encuentran estudiantes secundarios realizando pasantías, estos sujetos son fáciles de atacar. Un ejemplo de la aplicación de esta técnica fue obtener información relevante de la institución como contraseñas de equipos, direcciones IPs y claves de acceso a ciertos servicios que administra la empresa, que por motivos de confidencialidad no pueden ser expuestos en este proyecto.

3) *Resultados de Hacking Ético*

Con las técnicas de Hacking Ético mencionadas anteriormente se encontraron las siguientes vulnerabilidades, las cuales se indican en la Tabla IV.

TABLA IV
RESULTADOS

Técnica de hacking ético	Herramienta utilizada	Datos obtenidos	Vulnerabilidad encontrada	Observaciones
Footprinting	Maltego	Dominios ligados a quito.gob.ec que se encuentran expuestos en el internet.	26 dominios que podrían ser blancos de ataques.	Los dominios listados con esta herramienta muestran únicamente los expuestos en internet, mas no los que se obtuvieron con Dnsmap.
Scanning	Nmap	Puertos abiertos en los servidores de la institución.	Puertos innecesarios abiertos en los servidores de DNS, DHCP y Turnos.	Se debe habilitar únicamente los puertos necesarios para realizar las transacciones específicas de cada servidor.
Enumeration	Dnsmap	Subdominios pertenecientes a quito.gob.ec invisibles para el público pero que existen en los registros del DNS.	Subdomininios que podrían ser explotados mediante la técnica de ataques basados en dominios para escalar privilegios dentro de la red.	Es recomendable eliminar los subdominios que van a dejar de ser utilizados para disminuir la probabilidad de ataques.

[6] Bugs: Debilidad, error o defecto en un sistema informático.

[7] ARP: Address Resolution Protocol , permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP.

Troyanos y puertas traseras	Ettercap	No se pudieron obtener datos debido a que el antivirus bloqueó el ataque de paquetes ARP.	No se pudo capturar mensajes enviados entre equipos de la red.	La institución cuenta con el antivirus ESET ENDPOINT SECURITY que bloquea ataques de troyanos en el sistema.
Ingeniería social	Indagación	Contraseñas de switches y routers	Información sensible sin la debida codificación y protección física.	Esta información no puede ser expuesta por motivos de confidencialidad.

Fuente: Diagrama de autoría propia (Hidalgo J.,Tupiza D., Sánchez T.)

En base a las vulnerabilidades encontradas mediante la implementación de la honeynet y utilizando las técnicas respectivas se requiere lo siguiente:

- Implementar políticas de seguridad para la administración y gestión de los servidores.
- Implementación de políticas de seguridad para la administración y gestión de usuarios en el Active Directory y Lightweight Directory Access Protocol (LDAP).
- Creación de un instructivo para la gestión y administración de los espacios de telecomunicaciones, redes alámbricas e inalámbricas y las posibles medidas de seguridad a tener en cuenta para mitigar riesgos de seguridad en las mismas.
- Establecer lineamientos para el manejo de copias y respaldos de seguridad de los servidores que manejen información sensible.
- Políticas de actualizaciones de antivirus y equipos de escritorio.

IV. ESTABLECIMIENTO DE POLÍTICAS Y MECANISMOS DE SEGURIDAD

Se plantea una solución viable para diseñar la red multiservicios y satisfacer los requerimientos y necesidades de los usuarios de la empresa.

Se observa que las redes de las administraciones de la empresa matriz no cuentan con un diseño basado en estándares, por el contrario, han evolucionado según el movimiento del personal (despidos, traslados, ingresos, etc.), debido al crecimiento de usuarios se convirtió en un ambiente desorganizado.

A. Seguridad a nivel de servidores

Considerando los servicios que se gestiona en la empresa, se procede a desarrollar un conjunto de políticas que ayudan a mitigar los riesgos de la red.

a. Políticas de seguridad para el Active Directory

Al utilizar en la red de datos y de comunicaciones servicios proporcionados por la empresa matriz, se observó inconvenientes, como la falta de fechas de caducidad de contraseñas y desorganización en la formación de grupos de usuarios, afectando al rendimiento y seguridad de la red. Pensando en esto se ha generado las siguientes políticas:

1) Definir períodos de caducidad de contraseñas entre 3 a 6 meses máximo.
2) Crear contraseñas que mantengan una longitud no menor a ocho caracteres entre números, letras y símbolos especiales.
3) Generar grupos de trabajo que se encuentren acordes a las actividades que desempeñan los usuarios, un buen punto de partida sería catalogar a los usuarios por coordinación y por departamento.

b. Políticas de seguridad para servicios de uso general

1) FTP**;** Restringir el acceso a las carpetas y directorios compartidos en la red interna a los usuarios que estén dentro del mismo dominio.
2) Telefonía IP; Instalar únicamente teléfonos IP para los usuarios que lo ameriten considerando el cargo, coordinaciones y administraciones generales.
   Se deberá evitar mantener abiertas líneas que permitan realizar llamadas de índole personal sin previo consentimiento de un superior. Se configurará un código de salida que sea de una complejidad media y se lo asignará a un grupo de personas bajo un formulario de requerimiento.
3) Proxy; Instalar un servidor de proxy que ayude a bloquear “URLs” (Uniform Resource Locator) y sitios web no deseables, para mantener a los usuarios de la red libre de distracciones que afecten su rendimiento.

B. Mecanismos de seguridad

Se eligió Linux como el sistema operativo base de los servidores, por ser una plataforma de libre distribución con altas prestaciones por su gran soporte para drivers, herramientas de desarrollo, programas para usuario y flexibilidad para realizar instalaciones complejas.

En esta sección, se configuran los servicios para proteger los equipos informáticos que son utilizados como estaciones

de trabajo y servidores en general. Para ello se utiliza: Iptables [10], active directory y LDAP [11].

Actualmente, en la empresa están abiertos un gran número de puertos, que se deberían controlar en base a reglas que ayuden a mitigar los riesgos de seguridad para la red.

Considerando estos antecedentes, se procede a generar un conjunto de políticas para garantizar la seguridad del equipo y la integridad de la información gestionada por los mismos.

En base a las buenas prácticas en servidores se recomienda:

1) Cerrar todos los puertos, para posteriormente abrir aquellos que sean requeridos por los servicios y aplicativos utilizados por los usuarios de la red.
2) Mantener a los equipos informáticos con las últimas actualizaciones de seguridad, para garantizamos un grado elevado de seguridad.
3) No se debe actualizar los servidores de aplicaciones a menos que sea íntegramente necesario para el buen funcionamiento de los servicios que mantiene. Se debe considerar que una actualización innecesaria podría afectar el buen funcionamiento de los servicios y aplicaciones.
4) Se recomienda cambiar las credenciales de acceso en periodos de tiempo no extendidos máximo 30 días. Adicionalmente, se sugiere que las claves se las almacene en un gestor de contraseñas, un buen punto de partida es el software KeePassX [12], que ayuda a mantener las claves encriptados en un repositorio local libre de la vista de intrusos.
5) Se considera necesario mantener un cronograma activo para la gestión de backups y respaldos de información, que pueden generarse en cintas magnéticas, cds o algún dispositivo electrónico de almacenamiento de información.
6) Todos los servidores deberán ser monitoreados constantemente para evitar cualquier pérdida de información o problemas de disponibilidad que pueda afectar el trabajo de los usuarios en la red.

A continuación se procederá a detallar criterios para desarrollar las buenas prácticas antes mencionadas:

a. Mecanismos de bloqueo de puertos

Se procederá a instalar dependiendo de la distribución de Linux que se utilice, el sistema de firewall denominado Iptables. Para ambientes en base a una distribución Debian - Ubuntu, el procedimiento será el siguiente:

sudo apt-get install ufw

Para ambientes basados en plataformas Red Hat, se instalará de la siguiente manera:

yum install Iptables

Después de haber instalado el sistema, se muestra la manera de cómo interactuar con las políticas de seguridad necesarias para cada servidor. Las instrucciones para bloquear los puertos que no son necesarios en el servidor DHCP se enumeran a continuación:

- Inicialmente se cierran todos los puertos

  $ sudo ufw default deny

- Se añaden reglas para abrir los puertos, en este caso se deben abrir los puertos 67 (envío de respuesta) y 68 (recepción de petición).

  $ sudo ufw allow 67
  $ sudo ufw allow 68

b. Mecanismos de respaldos de información

La información sensible dentro de la empresa se la podría respaldar de la siguiente manera:

Cintas magnéticas: La información almacenada en este tipo de medio, se la debe realizar en periodos de tiempo cortos o largos que dependerán exclusivamente de la sensibilidad de la información que se gestione en la dependencia. En la empresa, se deberían realizar respaldos en periodos de tiempo que fluctúan entre 15 días a un mes como máximo, dado que las documentación que se maneja no es muy sensible y no está sujeta a cambios constantes como es el caso de documentos de catastros, planos y trámites de permisos de funcionamiento, pues la empresa en análisis corresponde a la Administración Zonal Norte "Eugenio Espejo" del Distrito Metropolitano de Quito.

V. CONCLUSIONES

1) Para el caso que nos compete, se trata de una Administración Zonal del Distrito Metropolitano de Quito, en el cual el manejo de la información sensible es crítico por lo que es necesario protegerla de los ataques de intrusos, con este fin se utiliza el hacking ético. En la empresa se consideró necesario realizar algunas de las técnicas de hacking ético, como son: footprinting, scanning, enumeration, puertas traseras e ingeniería social,

y con base a los resultados obtenidos se generaron políticas que permiten asegurar la confidencialidad, integridad y disponibilidad de la información de los usuarios incrementando el beneficio económico y social de los activos de la empresa.

2) Entre las principales vulnerabilidades encontradas se destacan los puertos que se encuentran innecesariamente abiertos, mismos que funcionan como un agujero en la seguridad, por ejemplo, el puerto 23/TCP, que está ligado al servicio Telnet y que permite conectarse de forma remota a los servidores; no encripta las contraseñas, por lo cual se convierte en un blanco fácil para ataques por sniffing. En total se encontraron siete puertos de alto riesgo (23,80,135,3389,59000,1521,5432) y cuatro puertos de riesgo moderado (21,139,445,5555), como indica la Fig. 6, los puertos de color rojo son los que más riesgos presentan y se encuentran abiertos, tal como se mencionó en la Tabla III.

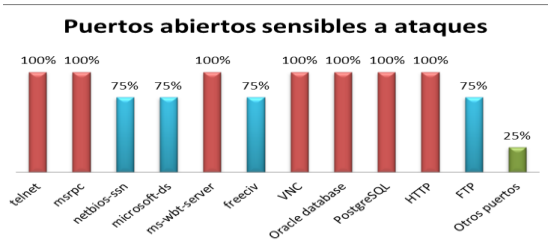


Fig. 6 Puertos Abiertos Sensibles a ataques
Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D., Sánchez T.)

3) Se encontraron subdominios pertenecientes a www.quito.gob.ec, que no son visibles para el público en general pero que se encuentran en los registros de DNS y que pueden ser explotados mediante ataques de dominio, y esto debido a que son creados para un objetivo específico y posteriormente no son borrados quedando con información que puede ser útil para los intrusos.

4) Una de las técnicas más utilizadas y que pasan por desapercibidas es la de ingeniería social, la cual se aprovecha de un cargo o de afinidad de los individuos para obtener información sensible y de esta forma tener acceso a los sistemas sin la necesidad de forzar o utilizar técnicas de intrusión. Por lo que se vuelve indispensable definir una política que establezca los lineamientos con los que un funcionario proporciona información de la red a terceros, ya que será responsabilidad de cada uno precautelar la información de cada departamento de la empresa.

5) Según la Fiscalía General del Estado del Ecuador, se tienen 626 denuncias entre enero y mayo del 2015 según fuente oficial (http: //www.fiscalia.gob.ec/), para delitos por fraude informático a pesar de contar con un Código Orgánico Integral Penal, estas denuncias podrían disminuir si se cuenta con políticas de seguridad claras y bien estructuradas para las empresas como las entidades bancarias cuya información es de alta sensibilidad.

REFERENCIAS

[1] C. Tori "Hacking Ético" Primera edición, Rosario Argentina 2008
[2] Scrib, « FUNDAMENTOS DE REDES » 2013. [En línea]. Disponible: http://es.scribd.com/doc/5881631/FUNDAMENTOS-DE-REDES [Último acceso: 11 Marzo 2013].
[3] Monografías.com «Como funciona el internet y las aplicaciones Peer to Peer» , 2016.[En línea]. Disponible: http://www.monografias.com/trabajos87/internet-aplicaciones-peer-to-peer/internet-aplicaciones-peer-to-peer.shtml[Último acceso: 25 Enero 2016].
[4] Instituto Tecnológico de Tijuana «Tipos de Servidores», 2016.[En línea]. Disponible: http://velazquezriosbrandon.jimdo.com/investigaciones/servidores/ [Último acceso: 25 Enero 2016].
[5] Wikipedia, «Voz sobre protocolo de internet» 2014. [En línea]. Disponible: https://es.wikipedia.org/wiki/Voz_sobre_protocolo_de_internet [Último acceso: 07 Diciembre 2014].
[6] TANENBAUM, A. S. (2003). REDES DE COMPUTADORAS (Cuarta Edición ed.). México: PEARSON EDUCACIÓN,ISB 970-26-0162-2.
[7] TORI CARLOS. (2008). HACKING ÉTICO (Primera Edición ed.). ROSARIO: ISBN 978-987-05-4364-0.
[8] Maltego, «Paterva Main Page» 2014. [En línea]. Disponible: https://www.paterva.com/web6/ . [Último acceso: 07 Febrero 2014].
[9] Ettercap, «Ettercap Homepage,» 2014. [En línea]. Disponible: https://ettercap.github.io/ettercap/ [Último acceso: 10 Febrero 2014].
[10] Iptables, «Cortafuegos iptables» 2014. [En línea]. Disponible: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/cortafuegos_iptables.html [Último acceso: 30 Marzo 2014].
[11] LDAP, «OpenLDAP» 2014. [En línea]. Disponible: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/openldap.html. [Último acceso: 18 Junio 2014].
[12] KeePassX, « KeePassX Homepage,» 2015. [En línea]. Disponible: http://www.alfresco.com/es. [Último acceso: 06 Mayo 2015].

Políticas de Seguridad de una Red Multiservicios Corporativa, Utilizando Hacking Ético

Hidalgo Y. Jessica [1], y Tupiza L. Diana [2] y Sánchez A. Tarquino [3]
[1] Escuela Politécnica Nacional, Facultad de Ingeniería en Electrónica y Redes de Información, Quito, Ecuador, pao7_2010@hotmail.com
[2] Escuela Politécnica Nacional, Facultad de Ingeniería en Electrónica y Redes de Información, Quito, Ecuador, diana_tupiza@hotmail.com
[3] Escuela Politécnica Nacional, Facultad de Ingeniería en Electrónica y Redes de Información, Quito, Ecuador, tarquino.sanchez@epn.edu.ec

Resumen– *Este proyecto tiene como objetivo establecer políticas de seguridad de información para una red corporativa que transmite voz, datos y video, para el efecto se analizan las vulnerabilidades existentes en la red frente a los ataques, utilizando técnicas de Hacking Ético. Se diseñará métodos y mecanismos para que el sistema de información sea seguro mediante la aplicación de las reglas definidas en la política de seguridad.*

Se inicia la investigación con el fundamento teórico que sirve de base para el desarrollo del proyecto, se realiza el diagnostico de la infraestructura de red multiservicios a ser analizada y se levanta la información a nivel de hardware, software y usuarios, posteriormente se realizan ataques utilizando técnicas de hacking ético para detectar la vulnerabilidad y riesgos del sistema en base a la importancia y sensibilidad de la información, para ello se construyó una honeynet virtual para evaluar la seguridad de la red, sin necesidad de atacar a los equipos físicamente. Con base a estos resultados experimentales se estableció las políticas de seguridad informática que permitirán mitigar vulnerabilidades de la red multiservicios corporativa. La aplicación de estas políticas podrá implementarse siguiendo la norma ISO 27001[1].

Abstract. - *This project aims to establish information security policies to a corporate network that transmits voice, data and video, to the effect of existing vulnerabilities are discussed in the network against attacks, using ethical hacking techniques. Methods and mechanisms for the information system is secure by applying the rules defined in the security policy will be designed.*

The research begins with the theoretical foundation that is the basis for project development, the diagnosis of network infrastructure multiservice to be analyzed and the information concerning hardware, software and users up is done, then attacks are performed using ethical hacking techniques to detect system vulnerabilities and risks based on the importance and sensitivity of the information., to do a virtual honeynet to evaluate the safety of the network, without having to physically attack the equipment was built. Based on these experimental results, the security policies that will mitigate vulnerabilities of the corporate multiservice network was established. The implementation of these policies will be implemented following the ISO 27001[1] standard.

Palabras Clave -- Hacking ético, Seguridad en redes, Redes LAN, Honeynet.

I. INTRODUCCIÓN

El activo más importante en las organizaciones públicas y privadas, es la información que se administra. Entre más grande es la organización más grande es la información y el interés de mantener la seguridad en la red de datos. [1]

La seguridad no es solamente el crear usuarios y contraseñas, es implementar políticas que garanticen la seguridad tanto física como lógica de la información. Se debe asegurar la privacidad de la información y protegerla tanto de daños no intencionados como deliberados.

Se analizó una empresa corporativa de la ciudad de Quito, los servicios de la intranet que ofrece, la seguridad informática, además se verifico el estado de los equipos de conectividad como routers y switches, así como también los servidores de monitoreo y de telefonía IP.

Como resultado de este análisis se evidenció que en general las empresas pueden ser blanco de ataques externos que buscan violentar la información que administran, debido a que los principales equipos de comunicación presentan configuraciones básicas de seguridad no acordes a la sensibilidad de la información que gestionan.

Por ello, mediante la utilización de hacking ético se determinarán las vulnerabilidades existentes y se establecerán políticas de seguridad que servirán para que el personal del área de informática pueda hacerle frente a los ataques que pudiera sufrir la institución

II. MARCO TEÓRICO

Una red es la disposición física o virtual de equipos y dispositivos, que permiten compartir información y recursos a través de un medio de comunicación.

[1] ISO 27001: Es un estándar para la seguridad de la información

Digital Object Identifier (DOI): http://dx.doi.org/10.18687/LACCEI2016.1.1.251
ISBN: 978-0-9822896-9-3
ISSN: 2414-6390

Actualmente, las redes permiten garantizar calidad de servicio (QoS)[2] y asegurar varios parámetros de red, tales como: tasa de error, ancho de banda, throughput, retraso en la transmisión, disponibilidad, etc. [2]
Los servicios corporativos de red por lo general son:

A. *Servicios de red*

- FTP (File Transfer Protocol)**:** El servicio FTP permite la transferencia de archivos entre un servidor y un computador (local y/o remoto) conectados a la red. Al utilizar esta aplicación se facilita el intercambio de archivos.[3]
- DNS (Domain Name System): Este protocolo permite traducir un nombre de dominio (ej. www.google.com) a una dirección IP (ej.173.194.75.103), lo que facilita al usuario realizar la búsqueda de un determinado servidor en la red.
- DHCP (Dynamic Host Configuration Protocol): Permite asignar direcciones IP y otras configuraciones de manera dinámica a los host de una red por un intervalo de tiempo determinado.
- Proxy: El servidor proxy actúa como un intermediario entre la intranet y la extranet, permitiendo registrar y restringir cierto tipo de tráfico que llevan a cabo los usuarios de la red corporativa
- Servidor Web: Los servidores web son aquellos cuya tarea es alojar sitios y/o aplicaciones, las cuales son accedidas por los clientes utilizando un navegador que se comunica con el servidor utilizando el protocolo HTTP (hypertext markup language).[4]
- VOIP: Es un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP (Protocolo de Internet).[5]
- Correo Electrónico: Los protocolos SNMP y POP de la capa aplicación basado en el modelo cliente/servidor, que se utiliza para el intercambio de mensajes.

B. *Seguridad en la Red*

En sus inicios las redes de computadoras eran utilizadas por universidades para el intercambio de información y a nivel corporativo para la compartición de impresoras, por tal motivo la seguridad quedaba en segundo plano. En la actualidad los múltiples servicios que prestan las redes informáticas y de comunicación como; servicios bancarios, compras online, homeworkers, etc., promueven la existencia de ataques a la integridad de los datos en las transacciones en linea.

Al viajar la información a través de diferentes medios de comunicación (cableado e inalámbrico) torna vulnerable la confidencialidad de la misma, por tal razón en los últimos años se han encontrado formas de prevenir los ataques a las redes corporativas.

Existen dos tipos de atacantes, los activos que son aquellos que provocan daños y modificaciones al funcionamiento normal de la red y los pasivos que no producen ninguna alteración, pero que sin embargo, utilizan la información capturada de manera fraudulenta [6]. Por tal razón la protección de los elementos activos y pasivos de la red se debe priorizar en tres ejes fundamentales:

- Prevención: Se deben tomar medidas que eviten que la información sea modificada, dañada o hurtada.
- Detección: Se deben tomar acciones que permitan identificar cuándo, cómo, dónde y quién dañó un determinado elemento.
- Reacción: La capacidad de tomar medidas correctivas una vez ocurrido un ataque a la seguridad de la red.

Para proporcionar la seguridad adecuada a una red de datos es necesario enfocarse en los siguientes parámetros:

- Confidencialidad: Asegurar que únicamente la persona autorizada tendrá acceso a la información (cifrado/descifrado, privacidad).
- Integridad: Asegurar que los datos son correctos, que no han sido modificados en el trayecto del origen al destino (firma digital, intercambio de autenticación).
- Disponibilidad: Asegurar que una entidad pueda acceder cuando desea a un recurso o servicio para el que está autorizado (servidores espejo, replicación de datos, enlaces redundantes).
- Autenticación: Asegurarse de que la entidad es quien dice ser mediante la identificación, para de esta manera aseverar que las transacciones se efectúan entre entidades legítimas (contraseñas, certificados, biométricos).

C. *Hacking Ético*

Inicialmente los procesos informáticos no eran objeto a ningún tipo de estudio de seguridad; los administradores y técnicos estaban encargados de realizar pruebas para encontrar posibles agujeros en la seguridad de la red. Posteriormente con el desarrollo tecnológico y la presencia de equipos y dispositivos que permiten gestionar grandes volúmenes de información sensible, se dio como resultado la aparición de hackers, personas que tomaban como retos intelectuales corromper la seguridad de los sistemas, descifrar contraseñas y causar daños a la integridad de la información.

En la actualidad, la palabra hacker no se encuentra relacionada únicamente con un delito, sino a la capacidad de encontrar fallos en la seguridad de los sistemas para

[2] QoS: Conjunto de tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo determinado.

proporcionar una solución; de esta manera aparece el hacking ético, que no es más que un método basado en el ataque deliberado a los sistemas para encontrar vulnerabilidades en la seguridad y posteriormente corregirlos e impedir que un atacante malicioso cause daños graves a los sistemas informáticos de la organización. [7]

III. DIAGNOSTICO DE LA RED CORPORATIVA MULTISERVICIOS Y PROPUESTA DE SEGURIDAD DE SU INTRANET

A. Descripción del problema

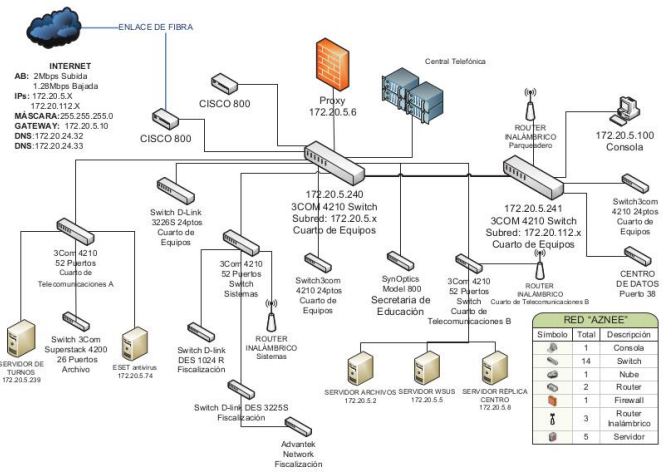


Fig.1 . Diagrama de la red inicial.
Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D., Sánchez T.)

La red analizada Fig. 1, corresponde a la sucursal de una empresa pública, que depende de una oficina matriz, cuenta con una red de voz y datos que no cumple con estándares de calidad de servicio, cableado estructurado deteriorado y sin organización física, insuficientes políticas de seguridad de servidores, personal técnico no capacitado en seguridad informática, escasos mecanismos de seguridad de servidores y servicios, medios de transmisión inadecuados entre cuartos de telecomunicaciones. Así:

El cableado estructurado está constituido por cable UTP categoría 5, el cual no posibilita el diseño de una red multiservicios. Cuenta con 3 racks en donde se ubican los principales equipos que proveen de conectividad a la red, además de existir otros equipos secundarios como switches distribuidos según la necesidad de extender nuevos puntos para la red.

Tiene alrededor de 150 usuarios y debido al constante crecimiento de los mismos, se ha extendido al uso de dos subredes: 172.20.5.0/24 y 172.20.112.0/24, las cuales están distribuidas indistintamente sin orden ni gestión.

Sus principales servicios son: correo electrónico, página Web, recursos de impresión, carpetas compartidas, proxy, antivirus, servidor de réplica. Además se identificó que la empresa ha sufrido varios ataques informáticos, entre ellos se destaca el realizado por "Anonymous", donde se verifico que se afectó al servidor web de la empresa pública paralizando sus actividades por 24 horas, así como también una administración deficiente de las contraseñas de equipos de conectividad y servidores.

B. Rediseño de la Intranet

Se planea implementar una nueva solución de cableado estructurado que permita mejorar la relación señal a ruido y una mayor fiabilidad en los servicios actuales, además mejorar la velocidad de acceso a las aplicaciones futuras.

Los lineamientos base para el rediseño del cableado estructurado se basan en las siguientes normas:

- ANSI/TIA 568.C, agrupa los requerimientos actuales de los sistemas, tanto en características y rendimiento de los componentes como en su estructura.
- ANSI/TIA 569.B, determina los requerimientos de rutas y espacios de telecomunicaciones.
- ANSI/TIA 606.A, define la documentación y administración para el etiquetado y registro de las distintas secciones de la red, sean éstos cables, patch panel, patch cords, espacios de telecomunicaciones y ductos.

Para el rediseño de la intranet se establece el siguiente procedimiento:

1) El sistema de cableado estructurado utilizará cable categoría 6 UTP, con una velocidad de 1 Gbps y un ancho de banda de 250 MHz, lo que permitirá tener una infraestructura que se adapte a aplicaciones que demanden mayores recursos de la red.
2) Reubicación de la acometida de servicios de telecomunicaciones hacia el cuarto de equipos, de esta forma se asegura la no manipulación de los enlaces de datos, que son el eje principal del funcionamiento de la empresa pública.
3) Reubicación de los equipos activos instalados en los gabinetes de pared, ubicados actualmente en las oficinas hacia el cuarto de telecomunicaciones para la gestión adecuada de los enlaces.
4) Proveer la seguridad física necesaria a los cuartos de telecomunicaciones para que no sean sensibles a ataques malintencionados.
5) Proveer de enlaces de fibra óptica multimodo para comunicar los cuartos de telecomunicaciones con el cuarto de equipos de la empresa.

En base al análisis de problemas se rediseño la red la cual se indica en la Fig. 2.

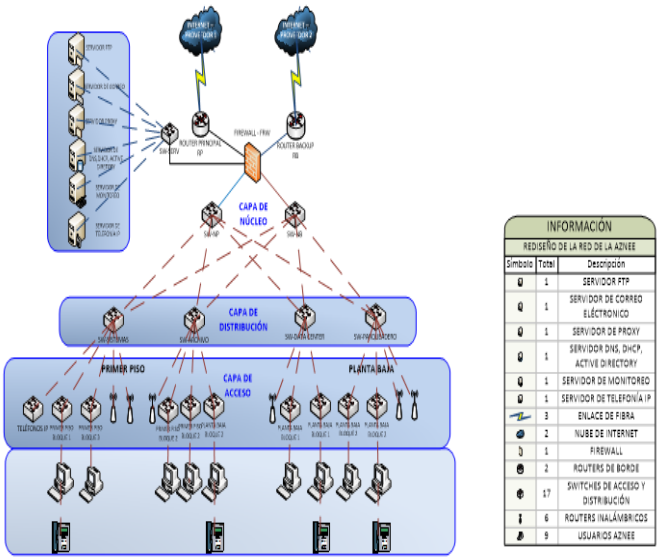


Fig.2 . Diagrama del rediseño
Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D.,Sánchez T.)

C. *Sistema de seguridad*

Para determinar los parámetros de seguridad que dispone la empresa, se realizó un estudio dirigido a 10 informantes calificados con base a preguntas concernientes a la seguridad informática del sistema. En la Tabla I se describe la información obtenida.

TABLA I
RESULTADOS DEL ESTUDIO A INFORMANTES CALIFICADOS

Parámetro de Seguridad consultado	Descripción de parámetro de seguridad	Fortaleza de la empresa	Debilidad de la empresa
Backups	Existen copias almacenadas en una empresa externa de los servidores.	Existen copias almacenadas fuera de la institución.	No existe política que establezca un cronograma para la realización de backups.
Lista de control de acceso	Access Control List ACLs implementadas y controladas por la Dirección informática de la empresa.	Existe un filtrado de paquetes basando en criterios determinados por la Dirección informática	Desconocimiento por parte del área de sistemas de la empresa del criterio con el que se realiza la configuración de ACLs.
Firewall	Controlado e implementado en el edificio principal de la empresa pública.	Existe una barrera primaria para bloquear el acceso no autorizado.	No se encuentra ubicado dentro de la empresa.
Antivirus	El software implementado en la institución es ESET Smart Security Corporativo.	Detección de amenazas informáticas.	
Antispam	El software implementado en la institución es ESET Smart Security Corporativo.	Filtrado de correo basura o no deseado.	
Proxy	Implementado en la empresa donde el acceso a internet es limitado por cargo y por usuario.	Optimización del ancho de banda restringiendo el acceso a páginas definidas por el administrador.	Falta de procedimientos para establecer privilegios de acceso a páginas web.
Autenticación	El departamento financiero utiliza un token valido para firma electrónica	Disminución en el tiempo de trámites legales y bancarios.	No definida.
	Contraseñas de mediano grado compuesto por números y letras (5 a 8 caracteres).	No definida.	Cambio de contraseña únicamente cuando el Usuario pierde sus credenciales.

Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D.,Sánchez T.)

Una vez identificado subjetivamente las vulnerabilidades de la red de datos se procedió a utilizar las técnicas de hacking ético con el propósito de evaluar técnicamente la red, con este fin se implementó una red de prueba virtual utilizando el software honeynet, en la cual se realizarán los ataques informáticos en busca de brechas en la seguridad. Los pasos a seguir son los siguientes:

1. Realización de la red de prueba- Honeynet
2. Utilización de técnicas de hacking ético
3. Análisis de resultados

1) *Realización de la red de prueba- Honeynet*

La honeynet se implementó con las configuraciones de los servicios de la red real, para emular de manera virtual los diversos ataques que puede sufrir la red y recolectar información de intrusiones para el análisis, monitoreo e investigación de vulnerabilidades y a la postre realizar los correctivos sobre dicha red.
Los componentes del sistema se detallan a continuación:

- **Honeypots**: Conjunto de computadores destinados para ser atacados, simulando ser sistemas débiles.
- **Honeywall:** Software basado en Linux que contiene herramientas necesarias para crear una honeynet, con el objetivo de filtrar el trafico producido por los honeypots sin interferir en su normal funcionamiento.
  Las herramientas que utiliza son:

  ✓ **Iptables:** Es un programa que permite el filtrado de paquetes que ingresan y salen de la honeynet.
  ✓ **P0f:** Es un programa utilizado para el monitoreo del tráfico que ingresa a la honeynet.
  ✓ ***Snort:*** Es un IDS (Intrusion Detection System) de red, que actúa como gateway para toda la información recopilada en honeynet.

La implementación virtual de la honeynet se realizó utilizando la herramienta de virtualización VirtualBox, donde constarán los sistemas operativos y aplicaciones que se maneja en la red.

Los honeypots serán configurados en máquinas virtuales con las copias de las imágenes de los discos de dos servidores

proporcionados por la empresa. *Cabe recalcar que los servicios principales están instalados en la empresa matriz y no en la administración analizada, por lo que no se puede realizar un análisis más completo sobre la red.*
Las imágenes de los discos duros que se obtuvieron son:

- Antivirus
- Archivos (Windows Server)

Los servicios restantes fueron simulados con la utilización del software ZENTYAL, el cual fue instalado en una máquina virtual y configurado con los siguientes servicios:

- **DNS:** Servicio de nombres de dominio
- **Email:** Servicio de correo electrónico
- **Proxy:** Bloqueo de URLs y puertos no autorizados.
- **Lighweight Directory Access Protocol (LDAP):** Servicio de directorio activo para entornos Linux similar a Active Directory en entornos Windows.

En la Fig. 3 se muestra el diseño de la honeynet que se implementó, la misma que será ubicada fuera de la red real.

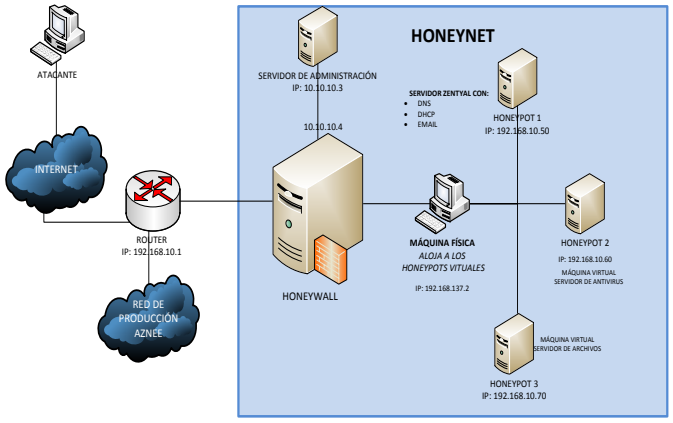


Fig. 3 Diagrama de la honeynet
Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D.,Sánchez T.)

2) *Utilización Del Hacking Ético Para Determinar Vulnerabilidades*

Partiendo de la premisa de que la información en la actualidad es uno de los activos más importantes en cualquier empresa tanto pública como privada, este recurso tiene un valor inconmensurable y para el caso particular de la empresa en análisis, que gestiona documentos sensibles de diversa naturaleza departamental, como son: catastros, predios, permisos de funcionamiento, patentes, etc. se debe tener mayor precaución con la gestión de los mismos, por lo que para mitigar los riesgos dentro y fuera de la red, se realizó un rediseño total de la infraestructura tecnológica de la empresa.

Para realizar un correcto rediseño de la red multiservicios se identifica las vulnerabilidades existentes; se utiliza técnicas de hacking ético que no son más que la búsqueda de debilidades mediante el manejo de herramientas informáticas llevadas a cabo por una persona especializada en ataques a sistemas y servicios informáticos.

Los resultados obtenidos a partir de estas técnicas permitirán tomar acciones de prevención necesarias, mitigando posibles ataques maliciosos. Las técnicas a utilizar son:

- Footprinting
- Scanning
- Enumeration
- Troyanos y puertas traseras
- Ingeniería Social

A continuación el detalle de los ataques realizados y los resultados obtenidos:

*Footprinting***;** mediante esta técnica es posible determinar los accesos ocultos o puertas traseras (BackDoors) para vulnerar una red. Permite recolectar datos relevantes de una empresa, persona, dominio o cuentas de correo antes de realizar ataques; la herramienta utilizada es el software Maltego [8], mismo que obtiene información concerniente al dominio de la empresa analizada. Este es el primer paso para determinar qué tan expuesta se encuentra una organización en el internet, y tratar de proporcionar seguridad a cada entrada del sistema de la empresa.

*Scanning***;** es una técnica pre-ataque, permite escanear puertos y vulnerabilidades de los diferentes equipos dentro de una red para identificar posibles agujeros de seguridad, el comando utilizado para ejecutar esta técnica es Nmap[3]. Se realizó el escaneo de puertos de los servidores, obteniendo la información necesaria para determinar políticas de seguridad que mejoren la administración de acceso a los puertos.

Este análisis se realizó en cada uno de los servidores de la red. El resumen consolidado de los puertos abiertos por servidor se muestra en la Tabla II.

TABLA II
PUERTOS ABIERTOS DENTRO DE LOS SERVIDORES

Servidor	Puertos abiertos
DHCP	80, 135, 139, 445, 3389, 49152, 49153, 49154.

[3] Nmap: Network Mapper (Mapeador de puertos de red)

DNS1	53, 88, 135, 139, 389, 445, 593, 636, 3268, 3269, 3389, 49152, 49153, 49154.
DNS2	22, 23, 53, 88, 135, 139, 389, 445, 464, 593, 636, 1026, 1433, 1434, 1443, 1500, 1501, 1503, 1521, 1503, 1521, 1524, 1533, 3268, 3269, 3389, 5555, 5900, 49152, 49153, 49154, 49155, 49157, 49158.
Turnos	21, 80, 90, 135, 139, 445, 500, 990, 1947, 5000, 5001, 5002, 5432, 5500, 5800, 5900, 5901, 7001, 49152, 49153, 49154, 49155, 49157, 49158.
Aplicaciones	No se tuvo acceso al servidor dado que es una réplica del servidor de la matriz.

Fuente: Diagrama de autoría propia (Hidalgo J. y Tupiza D.)

En la Tabla III, se muestra el listado de los puertos abiertos encontrados en los servidores ligados a las vulnerabilidades que representan cada uno de ellos y el grado de incidencia en el sistema.

Esta información permitirá determinar los puertos que deben permanecer abiertos para que los procesos se desarrollen con normalidad y los que necesitan ser cerrados para minimizar posibles violaciones de seguridad.

TABLA III
PUERTOS ABIERTOS SENSIBLES A ATAQUES

Puerto abierto	Servicio	Vulnerabilidad	Grado
23/tcp	telnet	Las contraseñas de Telnet no se encuentran encriptadas por lo que son vulnerables a ataques de sniffing[4].	Alto
135/tcp	msrpc	Funcionaría como puerta trasera dando acceso al servidor de manera remota, este puerto viene habilitado por defecto.	Alto
139/tcp	netbios-ssn	Establece un servicio de sesión que emula TCP con un equipo remoto y permite sondear el tráfico compartido como archivos e impresoras	Medio
445/tcp	microsoft-ds	Permite la transferencia de archivos de forma remota, y un atacante puede utilizarlo para provocar desbordamiento de memoria.	Medio
3389/tcp	ms-wbt-server	Permite acceso remoto al equipo y la manipulación de los archivos del sistema.	Alto
5555/tcp	freeciv	Permite acceso por puerta trasera mediante una secuencia de comandos para causar fallos.	Medio
5900/tcp	VNC	Permite conexión remota a los servidores.	Alto
1521/tcp	Oracle database	Puerta de escucha del servidor de base de datos Oracle.	Alto
5432/tcp	PostgreSQL	Puerto de escucha del servidor de base de datos PostgreSQL	Alto
80/tcp	HTTP	Puerto de acceso web.	Alto
21/tcp	FTP	Puerto de transferencia de archivos.	Medio
49152,49153, 53, 49154,49155,88, 593, 636, 3268, 3269,22,23, 389, 464,1026, 1434 433,1443, 1500, 90,1501,1503, 1524, 1533, 5900, 49158,500, 9157, 990,1947, 5000, 5002,5500, 5800.		Puertos de uso general manejados por Windows Server, Active Directory y LDAP.	Bajo o nulo

Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D., Sanchez T.)

Como se puede apreciar en la Tabla III, existen puertos de escucha que permiten conectarse a base de datos de la matriz, sin embargo, son réplicas que deberían ser accedidas a través de los servicios requeridos y no visibles para todos, y más bien presentan un grado de vulnerabilidad alto, por lo que se procederá a realizar las acciones correctivas necesarias para mitigar o eliminar los puertos que mantengan un riesgo de seguridad alto.

Enumeration; **e**ste pre-ataque permite enumerar los recursos dentro del objetivo como por ejemplo: identificar grupos, cuentas de usuario, contraseñas y recopilar información de recursos compartidos (impresoras, dispositivos de almacenamiento externo, etc.), con esta información un atacante podría conseguir escalar privilegios hasta llegar al nivel del administrador e instalar software malicioso que le permitirá tener control sobre la máquina, recolectar o robar datos y dejar puertas traseras para próximas intrusiones como se indica en la Fig. 4.

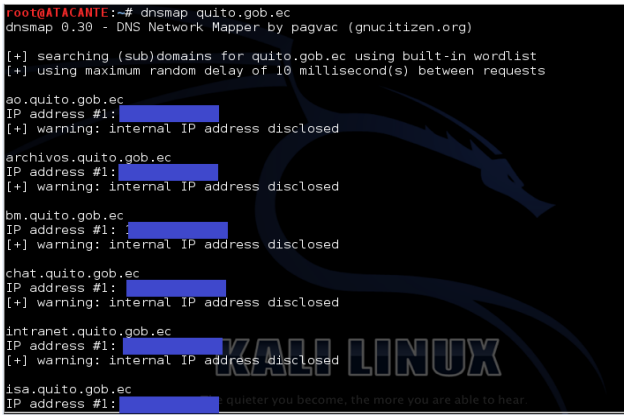


Fig. 4 Ejemplo de información encontrada con Dnsmap
Fuente: Diagrama obtenido de software Kali Linux

[4] Sniffing: Técnica de escucha del tráfico de la red.

En la Fig. 4, se muestran los subdominios pertenecientes a www.quito.gob.ec (empresa analizada), que son invisibles para el público pero que existen en los registros de DNS y que pueden ser explotados mediante ataques basados en dominios, por confidencialidad no se muestran las direcciones IP respectivas.

Este es el siguiente paso que ejecuta un atacante cuando no ha podido acceder a la información de la empresa pública mediante "footprinting" o "scanning", regularmente son archivos o dominios que no están siendo usados por los administradores de la red y que cuentan con información útil para el atacante.

Troyanos y puertas traseras; los troyanos son programas que se hacen pasar por genuinos, cuyo verdadero objetivo es ejecutar software malicioso en el equipo donde sean instalados. Al ejecutarse se auto incluye en la rutina de inicio del equipo y desde ese instante, puede vigilar el equipo hasta que el usuario se conecta a Internet. Las puertas traseras o backdoors por su parte son bugs[5] que permiten acceso a un equipo de forma remota, aprovechan la arquitectura de internet que se basa en el modelo cliente-servidor. Para determinar qué tan expuesta se encuentra la red a un ataque de esta naturaleza se utilizó la herramienta Ettercap [9]. Con este software se envenenó la red con paquetes ARP[6] para producir un desbordamiento de la memoria caché de los equipos de red y capturar paquetes de información bajo la técnica de hombre en el medio. Esta técnica fue bloqueada por el antivirus instalado en las máquinas de la empresa, como se indica en la Fig. 5.

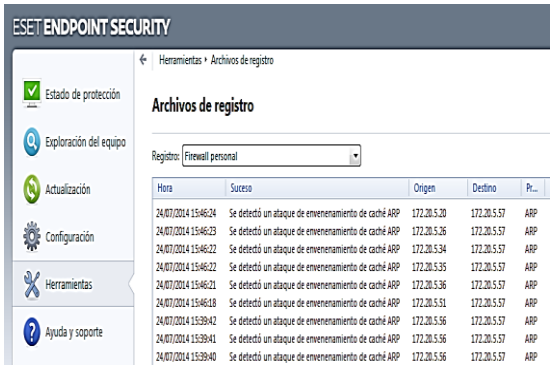


Fig. 5 Archivo de registro del antivirus
Fuente: Diagrama obtenido del Servidor de antivirus ESET

Ingeniería Social; la ingeniería social es una técnica que se basa en el engaño o abuso de confianza de personas inescrupulosas que obtienen información sensible de los usuarios y personal de la entidad, y la utilizan para realizar ataques maliciosos a la integridad de la institución. En la empresa analizada existe personal ajeno a la institución que de una u otra forma tiene acceso a información sensible o confidencial, por citar un ejemplo; se encuentran estudiantes secundarios realizando pasantías, estos sujetos son fáciles de atacar. Un ejemplo de la aplicación de esta técnica fue obtener información relevante de la institución como contraseñas de equipos, direcciones IPs y claves de acceso a ciertos servicios que administra la empresa, que por motivos de confidencialidad no pueden ser expuestos en este proyecto.

3) *Resultados de Hacking Ético*

Con las técnicas de Hacking Ético mencionadas anteriormente se encontraron las siguientes vulnerabilidades, las cuales se indican en la Tabla IV.

TABLA IV
RESULTADOS

Técnica de hacking ético	Herramienta utilizada	Datos obtenidos	Vulnerabilidad encontrada	Observaciones
Footprinting	Maltego	Dominios ligados a quito.gob.ec que se encuentran expuestos en el internet.	26 dominios que podrían ser blancos de ataques.	Los dominios listados con esta herramienta muestran únicamente los expuestos en internet, mas no los que se obtuvieron con Dnsmap.
Scanning	Nmap	Puertos abiertos en los servidores de la institución.	Puertos innecesarios abiertos en los servidores de DNS, DHCP y Turnos.	Se debe habilitar únicamente los puertos necesarios para realizar las transacciones específicas de cada servidor.
Enumeration	Dnsmap	Subdominios pertenecientes a quito.gob.ec invisibles para el público pero que existen en los registros del DNS.	Subdomininios que podrían ser explotados mediante la técnica de ataques basados en dominios para escalar privilegios dentro de la red.	Es recomendable eliminar los subdominios que van a dejar de ser utilizados para disminuir la probabilidad de ataques.
Troyanos y puertas traseras	Ettercap	No se pudieron obtener datos debido a que el antivirus bloqueó el ataque de paquetes ARP.	No se pudo capturar mensajes enviados entre equipos de la red.	La institución cuenta con el antivirus ESET ENDPOINT SECURITY que bloquea ataques de troyanos en el sistema.

[5] Bugs: Debilidad, error o defecto en un sistema informático.
[6] ARP: Address Resolution Protocol , permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP.

Ingeniería social	Indagación	Contraseñas de switches y routers	Información sensible sin la debida codificación y protección física.	Esta información no puede ser expuesta por motivos de confidencialidad.

Fuente: Diagrama de autoría propia (Hidalgo J.,Tupiza D., Sánchez T.)

En base a las vulnerabilidades encontradas mediante la implementación de la honeynet y utilizando las técnicas respectivas se requiere lo siguiente:

- Implementar políticas de seguridad para la administración y gestión de los servidores.
- Implementación de políticas de seguridad para la administración y gestión de usuarios en el Active Directory y Lightweight Directory Access Protocol (LDAP).
- Creación de un instructivo para la gestión y administración de los espacios de telecomunicaciones, redes alámbricas e inalámbricas y las posibles medidas de seguridad a tener en cuenta para mitigar riesgos de seguridad en las mismas.
- Establecer lineamientos para el manejo de copias y respaldos de seguridad de los servidores que manejen información sensible.
- Políticas de actualizaciones de antivirus y equipos de escritorio.

IV. ESTABLECIMIENTO DE POLÍTICAS Y MECANISMOS DE SEGURIDAD

Se plantea una solución viable para diseñar la red multiservicios y satisfacer los requerimientos y necesidades de los usuarios de la empresa.

Se observa que las redes de las administraciones de la empresa matriz no cuentan con un diseño basado en estándares, por el contrario, han evolucionado según el movimiento del personal (despidos, traslados, ingresos, etc.), debido al crecimiento de usuarios se convirtió en un ambiente desorganizado.

A. Seguridad a nivel de servidores

Considerando los servicios que se gestiona en la empresa, se procede a desarrollar un conjunto de políticas que ayudan a mitigar los riesgos de la red.

a. Políticas de seguridad para el Active Directory

Al utilizar en la red de datos y de comunicaciones servicios proporcionados por la empresa matriz, se observó inconvenientes, como la falta de fechas de caducidad de contraseñas y desorganización en la formación de grupos de usuarios, afectando al rendimiento y seguridad de la red. Pensando en esto se ha generado las siguientes políticas:

1) Definir períodos de caducidad de contraseñas entre 3 a 6 meses máximo.
2) Crear contraseñas que mantengan una longitud no menor a ocho caracteres entre números, letras y símbolos especiales.
3) Generar grupos de trabajo que se encuentren acordes a las actividades que desempeñan los usuarios, un buen punto de partida sería catalogar a los usuarios por coordinación y por departamento.

b. Políticas de seguridad para servicios de uso general

1) FTP**;** Restringir el acceso a las carpetas y directorios compartidos en la red interna a los usuarios que estén dentro del mismo dominio.
2) Telefonía IP; Instalar únicamente teléfonos IP para los usuarios que lo ameriten considerando el cargo, coordinaciones y administraciones generales.
   Se deberá evitar mantener abiertas líneas que permitan realizar llamadas de índole personal sin previo consentimiento de un superior. Se configurará un código de salida que sea de una complejidad media y se lo asignará a un grupo de personas bajo un formulario de requerimiento.
3) Proxy; Instalar un servidor de proxy que ayude a bloquear "URLs" (Uniform Resource Locator) y sitios web no deseables, para mantener a los usuarios de la red libre de distracciones que afecten su rendimiento.

B. Mecanismos de seguridad

Se eligió Linux como el sistema operativo base de los servidores, por ser una plataforma de libre distribución con altas prestaciones por su gran soporte para drivers, herramientas de desarrollo, programas para usuario y flexibilidad para realizar instalaciones complejas.

En esta sección, se configuran los servicios para proteger los equipos informáticos que son utilizados como estaciones de trabajo y servidores en general. Para ello se utiliza: Iptables [10], active directory y LDAP [11].

Actualmente, en la empresa están abiertos un gran número de puertos, que se deberían controlar en base a reglas que ayuden a mitigar los riesgos de seguridad para la red.

Considerando estos antecedentes, se procede a generar un conjunto de políticas para garantizar la seguridad del equipo y la integridad de la información gestionada por los mismos.

En base a las buenas prácticas en servidores se recomienda:

1) Cerrar todos los puertos, para posteriormente abrir aquellos que sean requeridos por los servicios y aplicativos utilizados por los usuarios de la red.
2) Mantener a los equipos informáticos con las últimas actualizaciones de seguridad, para garantizamos un grado elevado de seguridad.
3) No se debe actualizar los servidores de aplicaciones a menos que sea íntegramente necesario para el buen funcionamiento de los servicios que mantiene. Se debe considerar que una actualización innecesaria podría afectar el buen funcionamiento de los servicios y aplicaciones.
4) Se recomienda cambiar las credenciales de acceso en periodos de tiempo no extendidos máximo 30 días. Adicionalmente, se sugiere que las claves se las almacene en un gestor de contraseñas, un buen punto de partida es el software KeePassX [12], que ayuda a mantener las claves encriptados en un repositorio local libre de la vista de intrusos.
5) Se considera necesario mantener un cronograma activo para la gestión de backups y respaldos de información, que pueden generarse en cintas magnéticas, cds o algún dispositivo electrónico de almacenamiento de información.
6) Todos los servidores deberán ser monitoreados constantemente para evitar cualquier pérdida de información o problemas de disponibilidad que pueda afectar el trabajo de los usuarios en la red.

A continuación se procederá a detallar criterios para desarrollar las buenas prácticas antes mencionadas:

a. Mecanismos de bloqueo de puertos

Se procederá a instalar dependiendo de la distribución de Linux que se utilice, el sistema de firewall denominado Iptables. Para ambientes en base a una distribución Debian - Ubuntu, el procedimiento será el siguiente:

sudo apt-get install ufw

Para ambientes basados en plataformas Red Hat, se instalará de la siguiente manera:

yum install Iptables

Después de haber instalado el sistema, se muestra la manera de cómo interactuar con las políticas de seguridad necesarias para cada servidor. Las instrucciones para bloquear los puertos que no son necesarios en el servidor DHCP se enumeran a continuación:

- Inicialmente se cierran todos los puertos

  $ sudo ufw default deny

- Se añaden reglas para abrir los puertos, en este caso se deben abrir los puertos 67 (envío de respuesta) y 68 (recepción de petición).

  $ sudo ufw allow 67

  $ sudo ufw allow 68

b. Mecanismos de respaldos de información

La información sensible dentro de la empresa se la podría respaldar de la siguiente manera:

Cintas magnéticas: La información almacenada en este tipo de medio, se la debe realizar en periodos de tiempo cortos o largos que dependerán exclusivamente de la sensibilidad de la información que se gestione en la dependencia. En la empresa, se deberían realizar respaldos en periodos de tiempo que fluctúan entre 15 días a un mes como máximo, dado que las documentación que se maneja no es muy sensible y no está sujeta a cambios constantes como es el caso de documentos de catastros, planos y trámites de permisos de funcionamiento, pues la empresa en análisis corresponde a la Administración Zonal Norte "Eugenio Espejo" del Distrito Metropolitano de Quito.

V. CONCLUSIONES

1) Para el caso que nos compete, se trata de una Administración Zonal del Distrito Metropolitano de Quito, en el cual el manejo de la información sensible es crítico por lo que es necesario protegerla de los ataques de intrusos, con este fin se utiliza el hacking ético. En la empresa se consideró necesario realizar algunas de las técnicas de hacking ético, como son: footprinting, scanning, enumeration, puertas traseras e ingeniería social, y con base a los resultados obtenidos se generaron políticas que permiten asegurar la confidencialidad,

integridad y disponibilidad de la información de los usuarios incrementando el beneficio económico y social de los activos de la empresa.

2) Entre las principales vulnerabilidades encontradas se destacan los puertos que se encuentran innecesariamente abiertos, mismos que funcionan como un agujero en la seguridad, por ejemplo, el puerto 23/TCP, que está ligado al servicio Telnet y que permite conectarse de forma remota a los servidores; no encripta las contraseñas, por lo cual se convierte en un blanco fácil para ataques por sniffing. En total se encontraron siete puertos de alto riesgo (23,80,135,3389,59000,1521,5432) y cuatro puertos de riesgo moderado (21,139,445,5555), como indica la Fig. 6, los puertos de color rojo son los que más riesgos presentan y se encuentran abiertos, tal como se mencionó en la Tabla III.

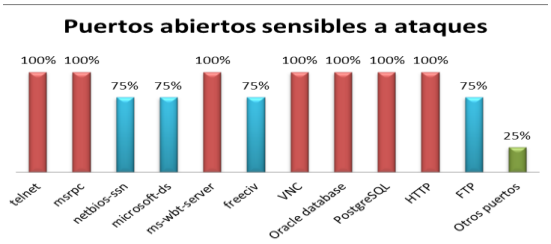


Fig. 6 Puertos Abiertos Sensibles a ataques
Fuente: Diagrama de autoría propia (Hidalgo J., Tupiza D., Sánchez T.)

3) Se encontraron subdominios pertenecientes a www.quito.gob.ec, que no son visibles para el público en general pero que se encuentran en los registros de DNS y que pueden ser explotados mediante ataques de dominio, y esto debido a que son creados para un objetivo específico y posteriormente no son borrados quedando con información que puede ser útil para los intrusos.

4) Una de las técnicas más utilizadas y que pasan por desapercibidas es la de ingeniería social, la cual se aprovecha de un cargo o de afinidad de los individuos para obtener información sensible y de esta forma tener acceso a los sistemas sin la necesidad de forzar o utilizar técnicas de intrusión. Por lo que se vuelve indispensable definir una política que establezca los lineamientos con los que un funcionario proporciona información de la red a terceros, ya que será responsabilidad de cada uno precautelar la información de cada departamento de la empresa.

5) Según la Fiscalía General del Estado del Ecuador, se tienen 626 denuncias entre enero y mayo del 2015 según fuente oficial (http: //www.fiscalia.gob.ec/), para delitos por fraude informático a pesar de contar con un Código Orgánico Integral Penal, estas denuncias podrían disminuir si se cuenta con políticas de seguridad claras y bien estructuradas para las empresas como las entidades bancarias cuya información es de alta sensibilidad.

REFERENCIAS

[1] C. Tori "Hacking Ético" Primera edición, Rosario Argentina 2008
[2] Scrib, « FUNDAMENTOS DE REDES » 2013. [En línea]. Disponible: http://es.scribd.com/doc/5881631/FUNDAMENTOS-DE-REDES [Último acceso: 11 Marzo 2013].
[3] Monografías.com «Como funciona el internet y las aplicaciones Peer to Peer» , 2016.[En línea]. Disponible: http://www.monografias.com/trabajos87/internet-aplicaciones-peer-to-peer/internet-aplicaciones-peer-to-peer.shtml[Último acceso: 25 Enero 2016].
[4] Instituto Tecnológico de Tijuana «Tipos de Servidores», 2016.[En línea]. Disponible: http://velazquezriosbrandon.jimdo.com/investigaciones/servidores/ [Último acceso: 25 Enero 2016].
[5] Wikipedia, «Voz sobre protocolo de internet» 2014. [En línea]. Disponible: https://es.wikipedia.org/wiki/Voz_sobre_protocolo_de_internet [Último acceso: 07 Diciembre 2014].
[6] TANENBAUM, A. S. (2003). REDES DE COMPUTADORAS (Cuarta Edición ed.). México: PEARSON EDUCACIÓN,ISB 970-26-0162-2.
[7] TORI CARLOS. (2008). HACKING ÉTICO (Primera Edición ed.). ROSARIO: ISBN 978-987-05-4364-0.
[8] Maltego, «Paterva Main Page» 2014. [En línea]. Disponible: https://www.paterva.com/web6/ . [Último acceso: 07 Febrero 2014].
[9] Ettercap, «Ettercap Homepage,» 2014. [En línea]. Disponible: https://ettercap.github.io/ettercap/ [Último acceso: 10 Febrero 2014].
[10] Iptables, «Cortafuegos iptables» 2014. [En línea]. Disponible: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/cortafuegos_iptables.html [Último acceso: 30 Marzo 2014].
[11] LDAP, «OpenLDAP» 2014. [En línea]. Disponible: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/openldap.html. [Último acceso: 18 Junio 2014].
[12] KeePassX, « KeePassX Homepage,» 2015. [En línea]. Disponible: http://www.alfresco.com/es. [Último acceso: 06 Mayo 2015].