UNIVERSIDAD MICHOACANA DE
SAN NICOLÁS DE HIDALGO

FACULTAD DE CONTADURIA y CIENCIAS
ADMINISTRATIVAS

DIAGNÓSTICO DE LA SEGURIDAD LÓGICA A TRAVÉS DE NMAP EN LA FACULTAD DE CONTADURIA Y CIENCIAS ADMINISTRATIVAS

PRESENTA

JOSE ROBERTO FLORES MENDOZA

ASESOR
DOCTOR EN CIENCIAS SALVADOR ALTEMO CASANOVA VALENCIA

CO-ASESOR
DOCTOR EN CIENCIAS PEDRO CHAVEZ LUGO

TESINA
PARA OBTENER EL TÍTULO DE
LICENCIADO EN INFORMÁTICA ADMINISTRATIVA

MORELIA, MICHOACÁN, SEPTIEMBRE2013.

INDICE

CAPITULO I REDES DE CÓMPUTO

CAPITULO II SEGURIDAD EN REDES

CAPITULO III. HERRAMIENTAS DE SEGURIDAD LÓGICA

CAPITULO IV REVISIÓN /ANÁLISIS/ DIAGNÓSTICO DE LA SEGURIDAD LÓGICA A TRAVES DE NMAP EN LA FCCA.

CAPITULO V. CONCLUCIONES

INTRODUCCIÓN

Hoy en día, el Internet se ha transformado en una de las herramientas más indispensable para todos. Dándole diferentes usos como lo es el trabajo, estudio o diversión e interacción social. Sin embargo aunado a este crecimiento también sehan desarrollado una serie de amenazas que dependen de dicho medio.

Tomando en cuenta este factor se han desarrollado programas para minimizar el hecho de ser víctimas de robos, perdida de información, etc. Es de suma importancia el hecho de saber cómo proteger las redes y los sistemas de información, para disminuir los problemas de seguridad.

La seguridad de las redes y sistemas de información pueden tomar una gran importancia, debido al impacto que pueden representar las fallas y perdida de información. Para tratar de obtener un nivel de seguridad y una funcionalidad aceptable sería necesario mantener actualizados y correctamente configurados los programas, así como también administrar correctamente los servicios de red.

OBJETIVOS

Objetivo general del caso

- Identificar y comparar los servicios de red que se encuentren operando en un servidor o equipo local. Con esta información se podría conocer que puertos están disponibles para conexión (abiertos), el tipo servicio que se está ofertando y la versión de desarrollo.

Objetivos particulares del caso

- Identificar los servicios de red ofertados en el servidor principal de La Facultad De Contaduría Y Ciencias Administrativas de la Universidad Michoacana De San Nicolás De Hidalgo.

- Comparar los servicios de red identificados con los servicios instalados por el administrador.

JUSTIFICACIÓN

Como administrador de sistemas se tiene la responsabilidad de identificar fallas de seguridad en las redes y sistemas de información. Para resolver algunos problemas de seguridad, se pueden utilizar herramientas de escaneo. Las cuales permiten Identificar los servicios de red que se encuentren operando en un equipo, así como las versiones asociadas a tales servicios.

Un ejemplo de un problema de seguridad lo puede generar un virus, un gusano, o un software malicioso que para difundirse en una red requiere utilizar un servicio de red.

Nmap es una opción para este fin, la cual es una herramienta gratuita, de código abiertola cual permite obtener información para la auditoria de sistemas y redes.

CAPITULO I. REDES DE CÓMPUTO

1.1 Redes de cómputo

Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones. Un ejemplo es Internet, la cual es una gran red de millones de computadoras ubicadas en distintos puntos del planeta interconectadas básicamente para compartir información y recursos.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red en siete capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

Para poder formar una red se requieren elementos: hardware, software y protocolos. Los elementos físicos se clasifican en dos grandes grupos: dispositivos de usuario final (hosts) y dispositivos de red. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás elementos que brindan servicios directamente al usuario y los segundos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

El fin de una red es la de interconectar los componentes hardware de una red , y por tanto, principalmente, las computadoras individuales, también denominados hosts, a los equipos que ponen los servicios en la red, los servidores, utilizando el cableado o tecnología inalámbrica

soportada por la electrónica de red y unidos por cableado o radiofrecuencia. En todos los casos la tarjeta de red se puede considerar el elemento primordial, sea ésta parte de un ordenador, de un conmutador, de una impresora, etc. y sea de la tecnología que sea (Ethernet, Wi-Fi, Bluetooth, etc.).

1.2 Clasificación de las redes

Una red puede recibir distintos calificativos de clasificación en base a distintas taxonomías: alcance, tipo de conexión, tecnología, etc.

Por alcance

- **Red de área personal**, o PAN (Personal Area Network) en inglés, es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora cerca de una persona.

- **Red inalámbrica de área personal**, o WPAN (Wireless Personal Area Network), es una red de computadoras inalámbrica para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella. El medio de transporte puede ser cualquiera de los habituales en las redes inalámbricas pero las que reciben esta denominación son habituales en Bluetooth.

- **Red de área local**, o LAN (Local Área Network), es una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de localización. No utilizan medios o redes de interconexión públicos.

- **Red de área local inalámbrica**, o WLAN (Wireless Local Área Network), es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas.

- **Red de área de campus**, o CAN (Campus Área Network), es una red de computadoras de alta velocidad que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, una base militar, hospital, etc. Tampoco utiliza medios públicos para la interconexión.

- **Red de área metropolitana** (MetropolitanáreaNetwork o MAN, en inglés) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica más extensa que un campus, pero aun así limitado. Por ejemplo, una red que interconecte los edificios públicos de un municipio dentro de la localidad por medio de fibra óptica.

- **Redes de área amplia**, o WAN (Wide Área Network), son redes informáticas que se extienden sobre un área geográfica extensa utilizando medios como: satélites, cables interoceánicos, Internet, fibras ópticas públicas, etc.

- **Red de área de almacenamiento**, en inglés SAN (Storage Área Network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte, permitiendo el tránsito de datos sin afectar a las redes por las que acceden los usuarios.

- **Red de área local virtual**, o VLAN (Virtual LAN), es un grupo de computadoras con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden alcanzar a los otros por medio de broadcast (dominio de broadcast) en la capa de enlace de datos, a pesar de su diversa localización física. Este tipo surgió como respuesta a la necesidad de poder estructurar las conexiones de equipos de un edificio por medio de software, permitiendo dividir un conmutador en varios virtuales.

Por tipo de conexión

Medios guiados

- El **cable coaxial** se utiliza para transportar señales electromagnéticas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo y uno exterior denominado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes; los cuales están separados por un material dieléctrico que, en realidad, transporta la señal de información.

- El **cable de par trenzado** es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes. Dependiendo de la red se pueden utilizar, uno, dos, cuatro o más pares.

- La **fibra óptica** es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

Medios no guiados

- **Red por radio** es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red.

- **Red por infrarrojos**, permiten la comunicación entre dos nodos, usando una serie de ledsinfrarrojos para ello. Se trata de emisores/receptores de ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita al otro para realizar la comunicación por ello es escasa su utilización a gran escala. No disponen de gran alcance y necesitan de visibilidad entre los dispositivos.

- **Red por microondas**, es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. Los protocolos más frecuentes son: el IEEE 802.11b y transmite a 2,4 GHz, alcanzando velocidades de 11 Mbps (Megabits por segundo); el rango de 5,4 a 5,7 GHz para el protocolo IEEE 802.11a; el IEEE 802.11n que permite velocidades de hasta 600 Mbps; etc.

Por relación funcional

- **Cliente-servidor** es la arquitectura que consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta.
- **Peer-to-peer**, o red entre iguales, es aquella red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

Por tecnología

- Red **Point-To-Point** es aquella en la que existe multitud de conexiones entre parejas individuales de máquinas. Este tipo de red requiere, en algunos casos, máquinas intermedias que establezcan rutas para que puedan transmitirse paquetes de datos. El medio electrónico habitual para la interconexión es el conmutador, o switch.

- Red **broadcast** se caracteriza por transmitir datos por un sólo canal de comunicación que comparten todas las máquinas de la red. En este caso, el paquete enviado es recibido por todas las máquinas de la red pero únicamente la destinataria puede procesarlo. Los equipos unidos por un concentrador, o hub, forman redes de este tipo.

1.3Topología de redes

La topología de red se define como una familia de comunicación usada por los computadores que forman una red para intercambiar datos. El concepto de red puede definirse como "conjunto de nodos interconectados". Un nodo es el punto en el que la curva se intercepta a sí misma. Lo que un nodo es concretamente, depende del tipo de redes a que nos referimos.

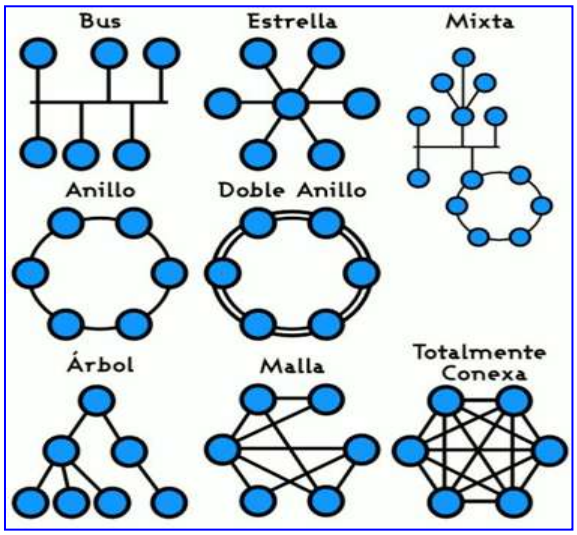

Figura 1. Topologías físicas de red. Fuentes: Groth, David; Skandier, Toby, (2005).

Topologías físicas de red.

- La **red en bus** se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos.
- En una **red en anillo** cada estación está conectada a la siguiente y la última está conectada a la primera.
- En una **red en estrella** las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.
- En una **red en malla** cada nodo está conectado a todos los otros.
- En una **red en árbol** los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central.
- En una **red mixta** se da cualquier combinación de las anteriores.

Por la direccionalidad de los datos

- Simplex o unidireccional: un equipo terminal de datos transmite y otro recibe.
- Half-duplex, en castellano semidúplex: el método o protocolo de envío de información es bidireccional pero no simultánea obidireccional, sólo un equipo transmite a la vez.
- Full-duplex, o dúplex,: los dos equipos involucrados en la comunicación lo pueden hacer de forma simultánea, transmitir y recibir.

Por grado de autentificación

- Red privada: una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.
- **Red de acceso público**: una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

Por grado de difusión

- 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.
- **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.

Por servicio o función

- Una **red comercial** proporciona soporte e información para una empresa u organización con ánimo de lucro.
- Una **red educativa** proporciona soporte e información para una organización educativa dentro del ámbito del aprendizaje.

Una **red para el proceso de datos** proporciona una interfaz para intercomunicar equipos que vayan a realizar una función de cómputo conjunta.

1.4Modelo TCP/IP

Este modelo es el implantado actualmente a nivel mundial: fue utilizado primeramente en ARPANET y es utilizado actualmente a nivel global en Internet y redes locales. Su nombre deriva de la unión del los nombres de los dos principales protocolos que lo conforman: TCP en la capa de transporte e IP en la capa de red.

Se compone de cuatro capas:

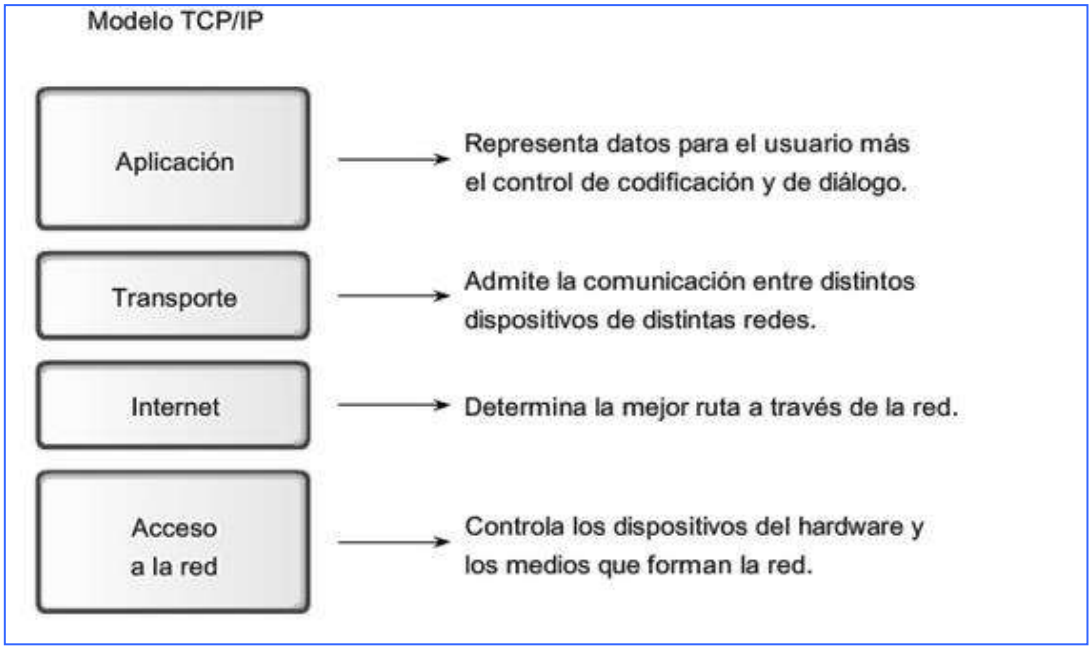

Figura 1.1 Modelo TCP/IP. Fuente: Robert E. Kahn.(1970)

1.5 Modelo OSI

El modelo OSI (*Open SystemsInterconnection*) fue creado por la ISO y se encarga de la conexión entre sistemas abiertos, esto es, sistemas abiertos a la comunicación con otros sistemas. Los principios en los que basó su creación eran: una mayor definición de las funciones de cada capa, evitar agrupar funciones diferentes en la misma capa y una mayor simplificación en el funcionamiento del modelo en general.

Este modelo divide las funciones de red en siete capas diferenciadas:

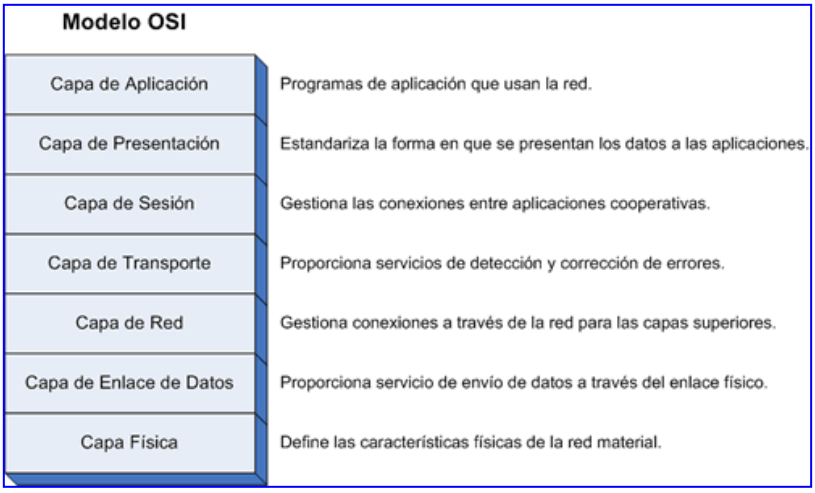

Figura 1.2 Modelo OSI. Fuente: Estándar ISO 7498-1(1994)

1.6Protocolos de red

En informática, un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. En su forma más simple, un protocolo puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos. A su más bajo nivel, un protocolo define el comportamiento de una conexión de hardware.

Los protocolos son reglas de comunicación que permiten el flujo de información entre equipos que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma, por tal sentido el protocolo TCP/IP, que fue creado para las comunicaciones en Internet, para que cualquier computador se conecte a Internet, es necesario que tenga instalado este protocolo de comunicación.

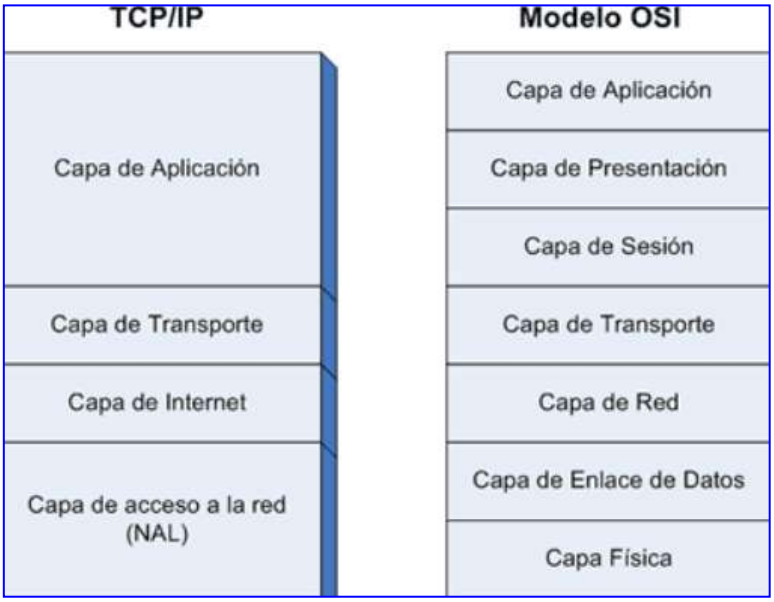

Figura 1.3 Protocolos de red. Fuente: Estándar ISO 7498-1(1994)

Ejemplos de protocolos de red

- **Capa 1: Nivel físico**
    - Cable coaxial o UTP categoría 5, categoría 5e, categoría 6, categoría 6a Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232.

- **Capa 2: Nivel de enlace de datos**
    - ARP, RARP, Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, HDLC,cdp

- **Capa 3: Nivel de red**
    - IP (IPv4, IPv6), X.25, ICMP, IGMP, NetBEUI, IPX, Appletalk.

- **Capa 4: Nivel de transporte**
    - TCP, UDP, SPX.

- **Capa 5: Nivel de sesión**
    - NetBIOS, RPC, SSL.

- **Capa 6: Nivel de presentación**
    - ASN.1.

- **Capa 7: Nivel de aplicación**
    - SNMP, SMTP, NNTP, FTP, SSH, HTTP, CIFS (también llamado SMB), NFS, Telnet, IRC, POP3, IMAP, LDAP, Internet Mail 2000, y en cierto sentido, WAIS y el desaparecido GOPHER.

1.7 Puertos de Red

Un puerto de red es una interfaz para comunicarse con un programa a través de una red. Un puerto suele estar numerado. La implementación del protocolo en el destino utilizará ese número para decidir a qué programa entregará los datos recibidos. Esta asignación de puertos permite a una máquina establecer simultáneamente diversas conexiones con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes.

Los números de puerto se indican mediante una palabra, 2 bytes (16 bits), por lo que existen 65535. Podemos usar cualquiera de ellos para cualquier protocolo, no obstante existe un órgano, la IANA, encargado de la asignación de los mismos, el cual creó tres categorías:

- Los puertos inferiores al 1024; son puertos reservados para el sistema operativo y usados por "protocolos bien conocidos", si queremos usar uno de estos puertos tendremos que arrancar el servicio que los use teniendo permisos de administrador.
- Los comprendidos entre 1024 (0400 en hexadecimal) y 49151 (BFFF en hexadecimal); son denominados "registrados" y pueden ser usados por cualquier aplicación, existe una lista publica en la web del IANA donde ver que protocolo usa cada uno de ellos.
- Los comprendidos entre los números 49152 (C000 en hexadecimal) y 65535 (FFFF en hexadecimal); son denominados dinámico o privados porque son los usados por el sistema operativo cuando una aplicación tiene que conectarse a un servidor y por tanto necesita un puerto por donde salir.

1.7.1 Clasificación de puertos de comunicación

Cuando hablamos de puertos en informática nos referimos en general a dos tipos de puertos, los físicos y los lógicos

Así que, los puertos de computadoras se dividen en dos tipos:

- Puertos físicos
- Puertos lógicos

Puertos físicos:

Así de esta manera cuando concretamente en el ámbito de redes de computadoras por Puerto Físico se entiende como un conector o toma en un dispositivo de red en el cual el medio se conecta con un host o con otro dispositivo de red"

Son todos conectores integrados en tarjetas de expansión ó en la Motherboard de la computadora; utilizados para interconectar una gran gama de dispositivos externos (eSATA, USB, FireWire, PS/2, HDMI, VGA, RJ45, Jack 3.5, etc.) e internos (PATA/IDE, SATA, PCI, PCIe, RAM, AGP, Socket o Slot para CPU, etc.), con la computadora

Puertos Físicos de Red: permiten la interconexión de computadoras por medio de cables.

- Puerto RJ45.- para red local (LAN) vía cable par trenzado con velocidad de <= 1Gbps
- Puerto RJ11.- para red telefónica via cable telefónico con velocidad <= 2Mbps
- Puerto de red BNC.-LAN via cable coaxial con velocidad de <= 10Mbps.
- Puerto de red DB15.- (en desuso) via cable de 15 pines, con velocidad <=10 Mbps.

Puertos físicos o Interfaces físicas

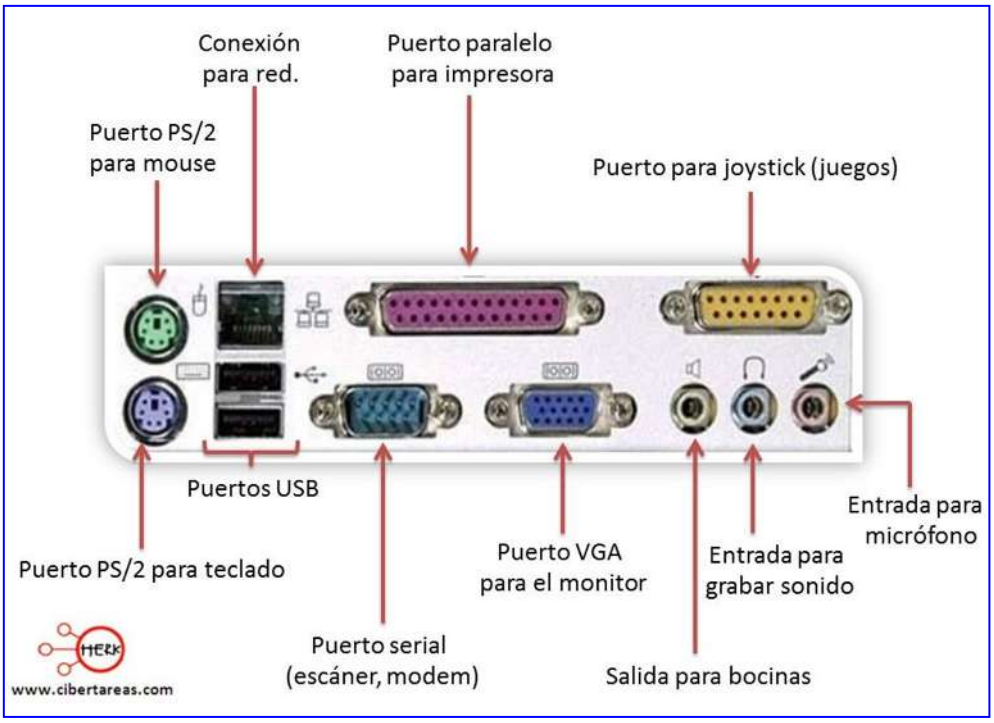

Figura 1.4 Puerto físicos. Fuente www.cibertareas.com (2012)

Puertos lógicos

Son "Lugares de conexión lógica y concretamente, utilizando el protocolo de Internet, la forma en que un programa cliente especifica un programa servidor determinado en una computadora en una red, o dicho de otra manera, son puntos de acceso entre equipos para el uso de servicios y flujo de datos entre ellos.

Puertos Lógicos de Red: suelen estar numerados "para de esta forma poder identificar la aplicación que lo usa. La implementación del protocolo en el destino utilizará ese número para decidir a qué programa entregará los datos recibidos. Esta asignación de puertos permite a una máquina establecer simultáneamente diversas conexiones con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes." . Originalmente estos números de puertos fueron usados solo por TCP y UDP, pero ahora también los utilizan SCTP

y DCCP. Estos protocolos pertenecen al cuarto nivel del modelo OSI, encargados de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red.

Existen 65535 puertos lógicos de red. Aunque podemos usar cualquiera de ellos para cualquier protocolo, existe una entidad, la **IANA**, encargada de su asignación, la cual **creó tres categorías**:

- **Puertos bien conocidos**: Puertos del 0 al 1023 son puertos reservados para el sistema operativo y usado por "Protocolos Bien Conocidos" como por ejemplo HTTP (servidor Web), POP3/SMTP (servidor de e-mail), Telnet y FTP.
- **Puertos registrados**: Comprendidos entre 1024 y 49151 son denominados "registrados" y pueden ser usados por cualquier aplicación. Existe una lista publica en la web del IANA, donde se puede ver qué protocolo usa cada uno de ellos.
- **Puertos dinámicos o privados**: Comprendidos entre los números 49152 y 65535 son denominados dinámicos o privados, normalmente se asignan en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Su uso es poco común, son usados en conexiones peer to peer (P2P).

Listado de los puertos más usados o comunes.

Puerto	Nombre	Información
20	FTP Data	Puerto utilizado en modo activo para el proceso de transferencia de datos FTP.
21	FTP	Servicio para compartir archivos FTP.
22	SSH	SecureSHell, utilizado principalmente para conexión por línea de comandos entre otras muchas funciones. Uso casi exclusivo para Linux, en Windows algunas aplicaciones pueden abrirlo.
23	Telnet	TELecommunicationNETwork permite controlar un equipo remotamente. Puerto potencialmente peligroso.
25	SMTP	TELecommunicationNETwork, usado para envío de correo electrónico. Un puerto muy escaneado para aprovechar vulnerabilidades para el envío de SPAM. Asegúrate de validar usuarios para el envío de correo.
53	DNS	Sistema de nombre de dominio, utilizado para resolver la dirección IP de un dominio.
80	HTTP	Servidor Web. Utilizado para navegación web. Este servicio por si solo ya supone un riesgo, suele ser escaneado y se las ingenian para encontrar nuevas entradas por el.
110	POP3	Una de las formas de acceder a los correos de tu cuenta de correo electrónico personal.
67	DHCP	Protocolo de configuración dinámica, permite a los clientes de una red IP obtener sus parámetros de configuración automática.
443	HTTPS	Usado para navegación Web en modo seguro. Se usa junto con un certificado de seguridad. Los comercios electrónicos

		por ejemplo aseguran sus ventas gracias a este servicio.
1080	Proxy	Servicio de proxy. Garantiza a los clientes del servicio mas seguridad en las conexiones en Internet, ya que tu IP no aparece en las conexiones, apareciendo la IP del servidor proxy.
1723	PPTP	Virtual privatenetwork (VPN). Puerto usado para conectar equipos por medio de Red Privada Virtual.
3306	MySQL	Base de datos MySQL. La base de datos usada de forma más frecuente como complemento a las páginas web dinámicas.

Tabla 1. Lista de números de puertos más comunes. Fuente www. wireshark.org (2013)

CAPITULO II SEGURIDAD EN REDES

2.1 Definición de Seguridad Lógica

La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

La seguridad lógica se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. La "seguridad lógica" involucra todas aquellas medidas establecidas por la administración -usuarios y administradores de recursos de tecnología de información- para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información.

2.2 Objetivos de la Seguridad Lógica

Los objetivos de la seguridad lógica son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.3 Definición de Seguridad Física

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc.; la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma, no.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Tipos de desastres

No será la primera vez que se mencione en este trabajo, que cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara. A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.
A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

Incendios

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.
El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Seguridad del equipamiento

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.
Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18o C y el límite de humedad no debe superar el 65% para evitar el deterioro.

- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.

- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

Inundaciones

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Condiciones climatológicas

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para emergencia.

Terremotos

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

Instalación eléctrica

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Picos y ruidos electromagnéticos

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

Cableado

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:
1. Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.

2. Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.

3. Daños en el cable: los cables normales con el uso pueden dañar al apantallamiento que preservan la integridad de los datos trasmitidos o dañar el propio cable, lo que hacen que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

Sistema de airea condicionado

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

Ambiente luminoso

Se parte de la base que las oficinas mal iluminadas son la principal causa de la pérdida de la productividad en las empresas y de un gasto energético excesivo. Una iluminación deficiente provoca dolores de cabeza y perjudica a los ojos.

Ambiente climático

En cuanto al ambiente climático, la temperatura de una oficina con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar comprendida entre el 45% y el 65%. En todos los lugares hay que contar con sistemas que renueven el aire periódicamente. No menos importante es el ambiente sonoro por lo que se recomienda no adquirir equipos que superen los 55 decibeles, sobre todo cuando trabajan muchas personas en un mismo espacio.

Robo

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

Fraude

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.
Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

Sabotaje

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

CAPITULO III. HERRAMIENTAS DE SEGURIDAD LOGICA

3.1 Principales Herramientas De Seguridad Lógica

Dentro de las principales herramientas de seguridad lógica encontramos las siguientes:

Firewall

Antivirus

Snifers

3.1.2 Firewall

Un cortafuegos (o firewall en inglés) es una parte de un sistema o una red que está diseñado 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. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Tipos de firewall

- Nivel de aplicación de pasarela

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

- Circuito a nivel de pasarela

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

- Cortafuegos de capa de red o de filtrado de paquetes

Funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino, etc. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (nivel 4) como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección MAC. Este es uno de los principales tipos de cortafuegos. Se considera bastante eficaz y transparente pero difícil de configurar.

- Cortafuegos de capa de aplicación

Trabaja en el nivel de aplicación (nivel 7), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder.

Un cortafuegos a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los computadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

- Cortafuegos personal

Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red. Se usa por tanto, a nivel personal.

Ventajas de un firewall

- Establece perímetros confiables.
- Protege de intrusiones.- El acceso a ciertos segmentos de la red de una organización sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.

- Protección de información privada.- Permite definir distintos niveles de acceso a la información, de manera que en una organización cada grupo de usuarios definido tenga acceso sólo a los servicios e información que le son estrictamente necesarios.

- Optimización de acceso.- Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

Limitaciones de un firewall

Las limitaciones se desprenden de la misma definición del cortafuegos: filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuegos (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red, seguirá constituyendo una amenaza. La siguiente lista muestra algunos de estos riesgos:

- Un cortafuego no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.

- El cortafuego no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuego no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y sustraerlas del edificio.

- El cortafuego no puede proteger contra los ataques de ingeniería social.

- El cortafuegos no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.

- El cortafuego no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en Internet.

3.1.3 Antivirus

Los antivirus son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos (a veces denominado malware).

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como heurística) o la verificación contra virus en redes de computadoras. Actualmente existe una nueva tecnología basada en Inteligencia artificial llamada TruPrevent que cuenta con la capacidad de detección de virus desconocidos e intrusos.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados, en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador web (ActiveX, Java, JavaScript).

Los antivirus son esenciales en sistemas operativos cuya seguridad es baja, como Microsoft Windows, pero existen situaciones en las que es necesario instalarlos en sistemas más seguros, como Unix y similares.

3.1.4Sniffers

En informática, un packetsniffer es un programa de captura de las tramas de red. Es algo común que, por topología de red y necesidad material, el medio de transmisión sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el sniffer pone la tarjeta de red o NIC en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos (ver niveles OSI) no son descartadas las tramas no destinadas a la MAC address de la tarjeta; de esta manera se puede capturar (sniff, esnifar) todo el tráfico que viaja por la red.

Un sniffer se podría resumir como un programa que lo que hace es capturar todos los datos que pasan a través de una tarjeta de red. Para ello se basa en un defecto del protocolo Ethernet (el que se usa normalmente en las redes locales). Este protocolo lo que hace es mandarla información a todos los ordenadores de la red, aunque no vaya dirigida a ellos, luego son los propios ordenadores los que basándose en la cabecera del paquete Ethernet aceptan el paquete o no, según vaya dirigidos a ellos o no. Normalmente todas las redes tienen este defecto, aunque se puede evitar, porejemplohay algunos hubs con inteligencia que en redes en estrella lo que hacen es examinar el encabezado de los paquetes Ethernet para ver a qué dirección van dirigidos y a mandar información solo a ese ordenador .Pues como decía, el Ethernet normalmente hace sniffer es poner la tarjeta en modo promiscuo. El modo promiscuo significa que la tarjeta captura todos los paquetes Ethernet, aunque no vayan dirigidos a ella.

Los packetsniffers tienen diversos usos como monitorizar de redes para detectar y analizar fallos o ingeniería inversa de protocolos de red. También es habitual su uso para fines maliciosos, como robar contraseñas, interceptar mensajes de correo electrónico, espiar conversaciones de chat, etc.

Existen diferentes herramientas para monitorizar el tráfico de datos estas son algunas:

Tcpdump, Darkstat, Traffic-vis, Ngrep, Snort, Nwatch, Ethereal (wireshark), Ettercap, Kismet

CAPITULO IV REVISIÓN /ANÁLISIS/ DIAGNÓSTICO DE LA SEGURIDAD LÓGICA A TRAVÉS DE NMAP EN LA FCCA.

4.1 NMAP

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias FyodorVaskovich). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

4.1.1 Historia

Nmap apareció en septiembre de 1997, en un artículo de la revista Phrack Magazine. El código fuente venía incluido.

Otros desarrollos incluyeron mejores algoritmos para determinar qué servicios estaban funcionando, reescritura de código de C a C++, se agregaron tipos de scan adicionales y nuevos protocolos como IPv6.

Nmap 3.5 apareció en febrero de 2004, y la versión 4.0 en enero de 2006, con cientos de mejoras.

4.1.2 Características

- Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo listando aquellas que responden
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como fingerprinting).
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

4.1.3 Aplicaciones Típicas

Ha llegado a ser uno de las herramientas imprescindibles para todo administrador de sistema, y es usado para pruebas de penetración y tareas de seguridad informática en general.

Como muchas herramientas usadas en el campo de la seguridad informática, es también una herramienta muy utilizada para hacking.

Los administradores de sistema pueden utilizarlo para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, así como los crackers pueden usarlo para descubrir objetivos potenciales.

Nmap permite hacer el inventario y el mantenimiento del inventario de computadores de una red. Se puede usar entonces para auditar la seguridad de una red, mediante la identificación de todo nuevo servidor que se conecte.

Nmap es a menudo confundido con herramientas para verificación de vulnerabilidades como Nessus. Nmap es difícilmente detectable, ha sido creado para evadir los Sistema de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas.

4.1.4 Entornos de trabajo

Nmap puede funcionar en sistemas operativos basados en Unix (GNU/Linux, Solaris, BSD y Mac OS X), y también en otros Sistemas Operativos como Microsoft Windows y MacOS.

4.2. Escaneo de puertos al servidor de la Facultad De Contaduría Y Ciencias Administrativascon Nmap

Instalacion de la aplicacion

La aplicación fue descargada de este sitio web http://nmap.org/

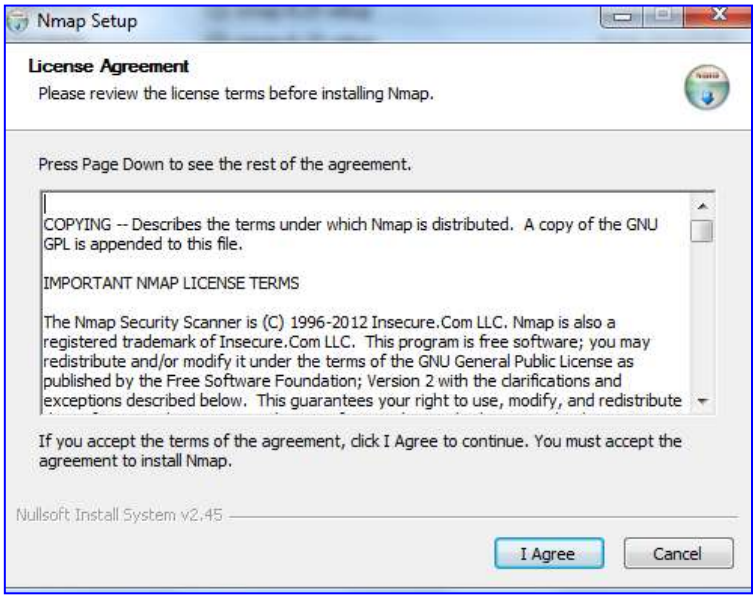

Figura 2. Descarga de Nmap. Fuente: http://nmap.org/(2013)

La instalación esta completada

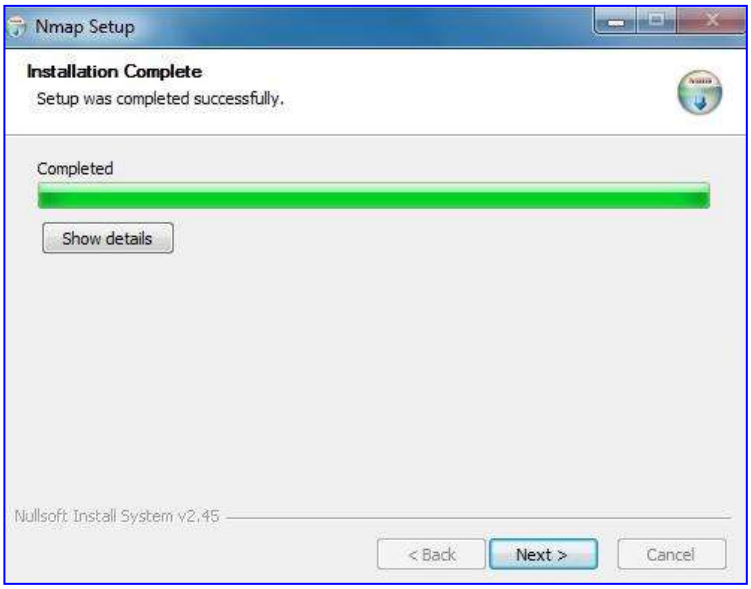

Figura 2.1 Instalación de Nmap. Fuente: http://nmap.org/(2013)

Finalmente terminamos la instalación de la aplicación

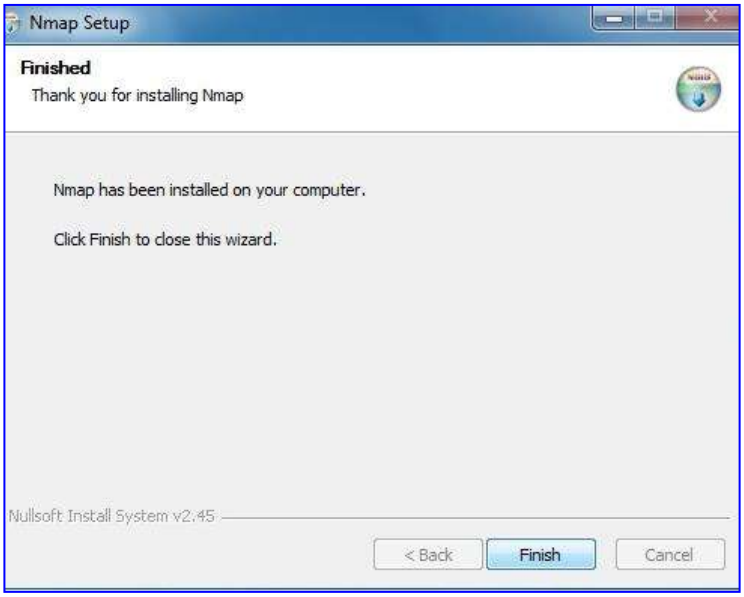

Figura 2.2 Termino de Instalación. Fuente: http://nmap.org/(2013)

Primero iniciamos Nmap, donde definiremos los equipos que seránanalizados, aquí aparecerán los objetos, ya sean los nombres de máquinas, Direcciones IP, o cualquier formato aceptado por Nmap, aparecerán cada uno en líneas distintas.Usando por defecto un listado de los puertos más comunes.

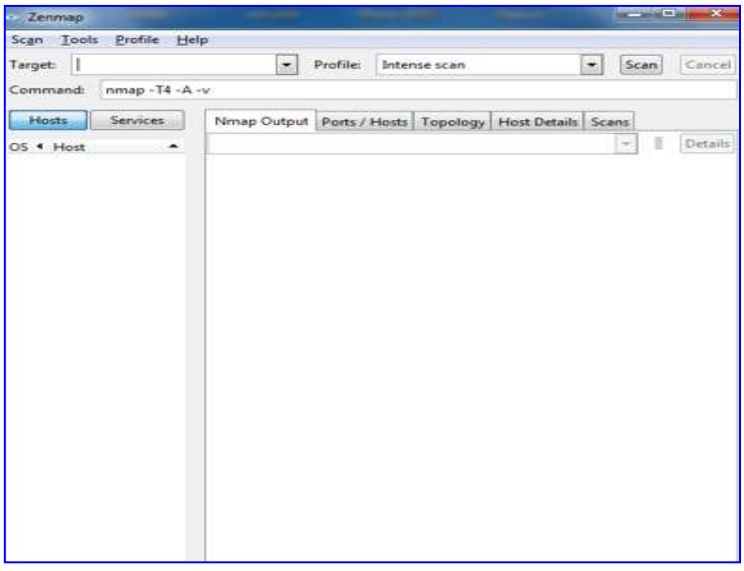

Figura 2.3 Pantalla principal de Nmap. Fuente: http://nmap.org/(2013)

El escaneo que se realizo fue al servidor de la Facultad de Contaduría y Ciencias Administrativas www.fcca.umich.mx (148.216.29.45).

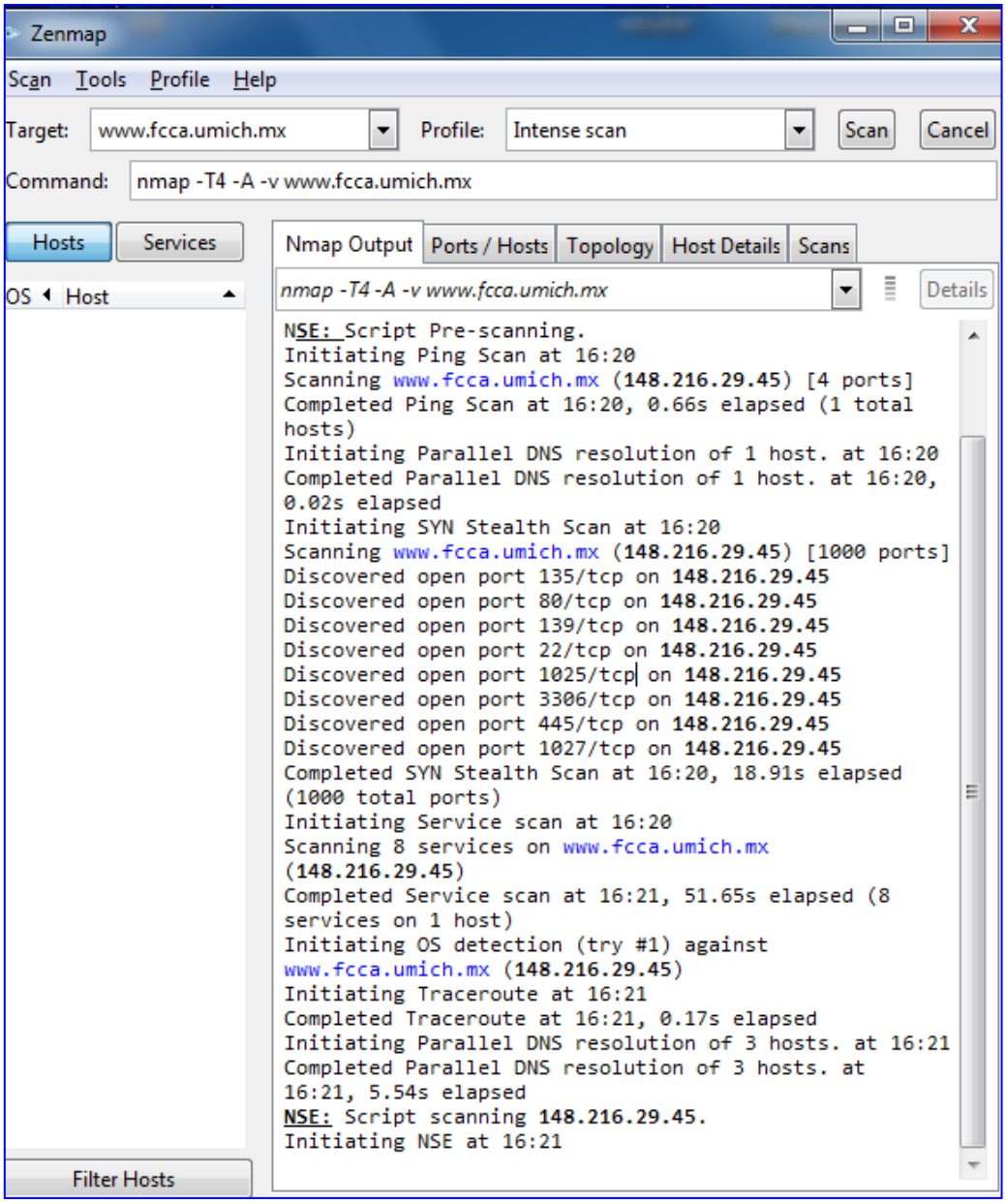

Figura 2.4 Escaneo al servidor .Fuente: Escaneo realizados al servidor de la Facultad de Contaduría y Ciencias Administrativas (2013)

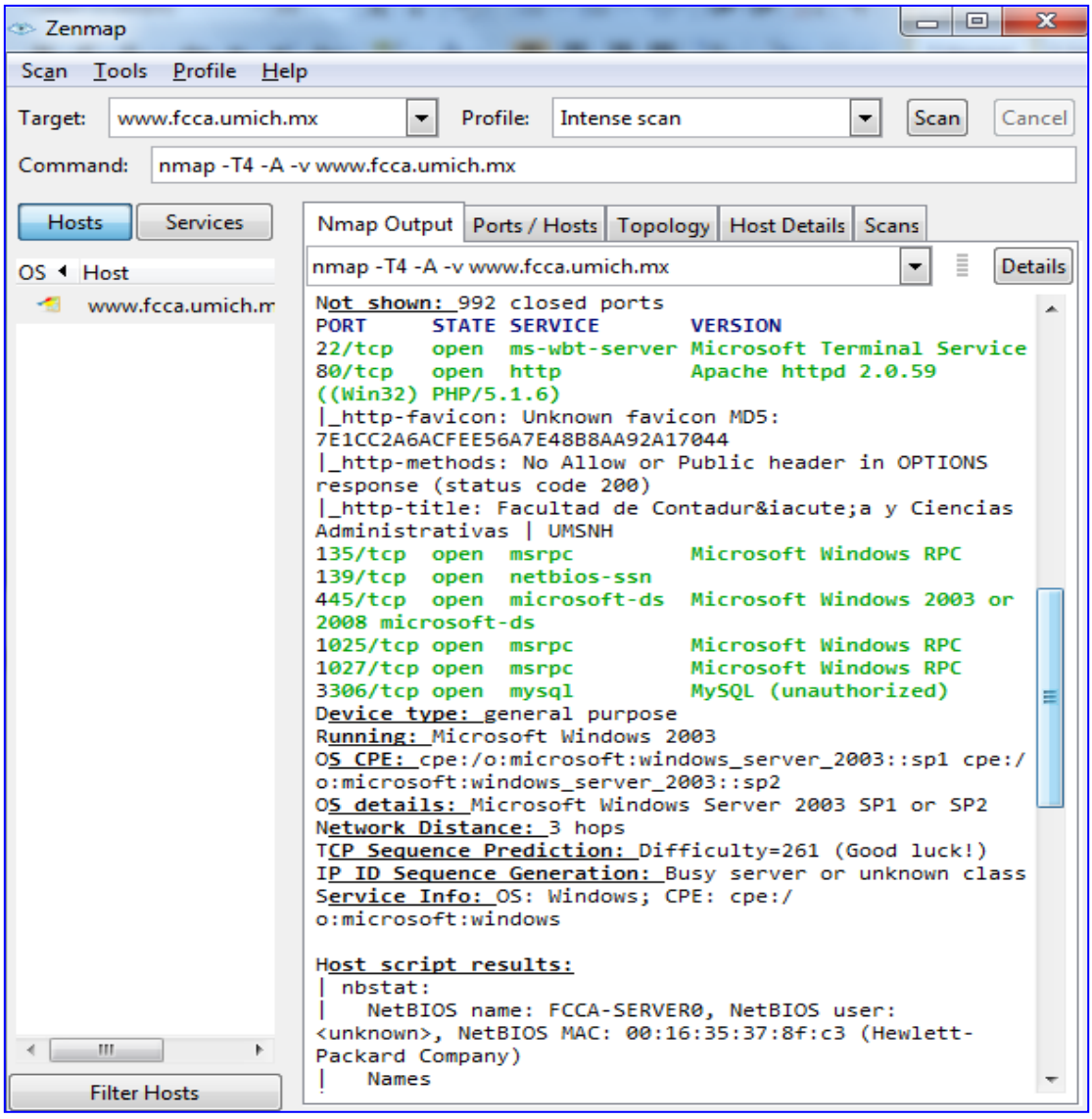

Figura 2.4.2 Continuación de figura 2.4

4.3. Conclusión del escaneo

Una vez finalizado el escaneo de puertoscon Nmap al servidor de la Facultad De Contaduría y Ciencias Administrativas se obtiene conjunto de puertos abiertos detectados así como los servicios y versiones en puertos abiertos, se investigo con el administrador del servidor de la Facultad De Contaduría Y Ciencias Administrativas y nos dio un informe de cuales aplicaciones fueron instaladas por él.

A continuación se muestra una tablacon los puertos que se encontraron abiertos, así como de los puertos que fueron utilizados por las aplicaciones instaladas por el administrador y cuales puerto utilizados por el sistema operativo.

Puerto	Servicio	Instaladas por el administrador
• **135/tcp**	msrpc	Aplicación instalada por el sistema operativo.
• **80/tcp**	http	Aplicación instalada por el administrador.
• **139/tcp**	netbios-ssn	Aplicación instalada por el sistema operativo.
• **22/tcp**	ms-wbt-server	Aplicación instalada por el sistema operativo.
• **1025/tcp**	msrpc	Aplicación instalada por el sistema operativo.
• **3306/tcp**	mysql	Aplicación instalada por el administrador.
• **445/tcp**	microsoft-ds	Aplicación instalada por el sistema operativo.
• **1027/tcp**	msrpc	Aplicación instalada por el sistema operativo.

Tabla 2. Tabla de Puertos abiertos.Fuente: Resultado obtenido del escaneo realizado al servidor de la Facultad De Contaduría y Ciencias Administrativas

CAPITULO V. CONCLUCIONES

5.1 Conclusiones

A través de la implementación correcta de algunas herramientas de seguridad incrementamos nuestro nivel de seguridad, haciendo los sistemas más confiables.Nmap es una herramienta de gran importancia en la actualidad utilizada para escaneo de puertos abiertos, ya que algún puerto abierto representa una amenaza a un sistema, primero que nada debemos identificar cuales tenemos abiertos y qué función tiene cada uno de ellos, así como identificar cuales puertos son utilizados por el sistema operativo para su funcionamiento, esto es de vital importancia para poder prever futuras amenazas a nuestro a un sistema.

Durante el desarrollo de esta tesina hemos tenido la posibilidad de valorar los diferentes criterios de seguridad, así como de conocer las principales amenazas físicas y lógicas que algún sistema puede ser expuesto, como también el manejo de esta herramienta de seguridad.

5.2 Resumen

UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO
FACULTAD DE CONTADURIA Y CIENCIAS
ADMINISTRATIVAS

RESUMEN

Esta tesina fue realizada con el fin de identificar y comparar los servicios de red que se encuentren operando en un servidor o equipo local. Con esta información se podría conocer que puertos están disponibles para conexión, el tipo de servicio que se está ofertando y la versión de desarrollo.

Se podrá apreciar que servicios fueron instalados por el administrador y los aquellos servicios que han sido instalados por el sistema operativo.

Esta información fue obtenida al realizar un escaneo al servidor de la Facultad de Contaduría y Ciencias Administrativas con nmap la cual es una herramienta gratuita, de código abierto la cual permite obtener información para la auditoria de sistemas y redes.

En el escaneo se pudo conocer los puertos se encuentren abiertos, que servicios se encuentran asociados a estos puertos, y con ello valorar diferentes criterios de seguridad para conocer las principales amenazas físicas y lógicas y en base a estas poder prevenir amenazas futuras al sistema.

BIBLIOGRAFÍA

- Aldedani, Gustavo. Miguel. (1997).*Seguridad Informática*. MP Ediciones. 1° Edición. Argentina.

- Borghello, C. (n.d.). segu-info. *Seguridad Lógica*. Revisado, 2 Abril del 2013, en: http://www.segu-info.com.ar/logica/seguridadlogica.htm

- Computer logical ports. (n.d.). *Computer training in chicago and the chicagolandárea*. Revisado,15 de Mayo 2013, en:http://www.escotal.com/ports.html

- Puerto de red - Wikipedia, la enciclopedia libre. (Enero 3 del 2013) .*Wikipedia, la enciclopedia libre*. Revisada 17 Mayo, 2013, en: http://es.wikipedia.org/wiki/Puerto_de_red

- Protocolo de comunicaciones - Wikipedia, la enciclopedia libre. (n.d.). Wikipedia, la enciclopedia libre. Revisado 27 de marzo, del 2013, en: http://es.wikipedia.org/wiki/Protocolo_(inform%C3%A1tica)

- Protocolo de comunicaciones - Wikipedia, la enciclopedia libre. (n.d.). *Wikipedia, la enciclopedia libre*. Revisado 12 de Mayo , 2013, en: http://es.wikipedia.org/wiki/Capa_de_transporte