Hacker Highschool
SECURITY AWARENESS FOR TEENS

ÍNDICE
Y
GLOSARIO

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

Información sobre la "Licencia de Uso"

Las lecciones y cuadernos de trabajo siguientes son de acceso público y están disponibles bajo las siguientes condiciones de ISECOM:

Todos los trabajos del proyecto "Hacker Highschool" son proporcionados para su uso no comercial con estudiantes de escuelas primarias, secundarias, bachilleratos y ciclos formativos dentro de las actividades académicas propias de la institución. Dichos materiales no pueden ser reproducidos con fines comerciales de ningún tipo. La impartición con estos materiales de cualquier clase, curso o actividad de formación para el que sea necesario pagar un importe, queda totalmente prohibida sin la licencia correspondiente, incluyendo cursos en escuelas y universidades, cursos comerciales o cualquier otro similar. Para la compra de una licencia visite la sección "LICENSE" de la página web del proyecto "Hacker Highschool" en www.hackerhighschool.org/license.

El proyecto HHS es una herramienta de aprendizaje y, como tal, la formación final debe proceder realmente de la influencia del instructor y no basarse únicamente en el uso de la herramienta.

ISECOM no puede aceptar bajo ningún concepto responsabilidad alguna sobre la forma de aplicar, ni sus consecuencias, de cualquier información disponible dentro del proyecto.

El proyecto HHS es un esfuerzo de una comunidad abierta, por lo que si encuentra útil este proyecto le invitamos a esponsorizarlo a través de de la compra de una licencia, una donación o una esponsorización.

Índice

Lección 1: Ser un Hacker

1.1. Introducción
1.2. Recursos
    1.2.1 Libros
    1.2.2 Magazines y Periódicos
        1.2.2.1. Ejerci
    1.2.3 Zines y Blogs
        1.2.3.1. Ejerci
    1.2.4 Forums y Listas de Correo
        1.2.4.1. Ejerci
    1.2.5 Grupos de Notícias
        1.2.5.1. Ejerci
    1.2.6 Páginas W
        1.2.6.1. Ejerci
    1.2.7 Chat
        1.2.7.1. Ejerci
    1.2.8 P2P
1.3. Más lecciones

Lección 2: Nociones de Comandos de Windows y Linux

2.1. Objetivos
2.2. Requerimientos y escenario
    2.2.1 Requerimientos
    2.2.2 Escenario
2.3. Sistema Operativo: WINDOWS
    2.3.1 ¿Cómo abrir una ventana de MS-Dos?
2.4. Sistema operativo: LINUX
    2.4.1 ¿Cómo abrir una ventana de consola?
    2.4.2 Comandos básicos
    2.4.3 Herramientas de red
2.5. Ejercicios Prácticos
    2.5.1 Ejercicio 1
    2.5.2 Ejercicio 2
    2.5.3 Ejercicio 3

Lección 3: Puertos y Protocolos

3.1. Objetivos
3.2. Conceptos básicos de redes
    3.2.1 Dispositivos
    3.2.2 Topologías
3.3. Modelo TCP/IP
    3.3.1 Introducción

3.3.2 Capas TCP/IP
3.3.2.1 Aplicacionón
3.3.2.2 Transporte
3.3.2.3 IP
3.3.2.4 Acceso a Red
3.3.3 Protocolos
3.3.3.1 Protocolos de la capa de Aplicación
3.3.3.2 Protocolos de la capa de Transporte
3.3.3.3 Protocolos de la capa de Internet
3.3.4 Direcciones IP
3.3.5 Puertos
3.3.6 Encapsulación
3.4. Ejercicios
3.4.1 Ejercicio 1: Netstat
3.4.2 Ejercicio 2: Puertos y protocolos
3.4.3 Ejercicio 3: Mi primer servidor
3.5. Lecturas recomendadas

Lección 4: Servicios y Conexiones

4.1. Introducción
4.2. Servicios
4.2.1 HTTP y la Web
4.2.2 E-mail – POP y SMTP
4.2.3 IRC
4.2.4 FTP
4.2.5 Telnet y SSH
4.2.6 DNS
4.2.7 DHCP
4.3. Conexiones
4.3.1 ISPs
4.3.2 Servicio de telefonía tradicional
4.3.3 DSL
4.3.4 Cable Modems
4.4. Lecturas recomendadas

Lección 5: Identificación de Sistemas

5.1. Introducción
5.2. Identificación de un servidor
5.2.1 Identificación del propietario de un dominio
5.2.2 Identificación de la dirección IP de un dominio
5.3. Identificación de servicios
5.3.1 Ping y Traceroute
5.3.2 Obtención del banner
5.3.3 Identificación de servicios a partir de puertos y protocolos
5.4. Identificación de un sistema
5.4.1 Escaneo de ordenadores remotos
5.5. Lecturas recomendadas

Lección 6: Malware

6.0 Introducción
6.1 Virus
    6.1.1 Introducción
    6.1.2 Descripción
        6.1.2.1 Virus de Sector de Arranque (Boot Sector Viruses)
        6.1.2.2 Virus de Archivos Ejecutables
        6.1.2.3 Virus Residentes en Memoria (Terminate and Stay Resident - TSR)
        6.1.2.4 Virus Polimórfico
        6.1.2.5 Virus de Macro
6.2 Gusanos
    6.2.1 Introducción
    6.2.2 Descripción
6.3 Troyanos y Spyware
    6.3.1 Introducción
    6.3.2 Descripción
6.4 Rootkits y Backdoors
    6.4.1 Introducción
    6.4.2 Descripción
6.5 Bombas Lógicas y Bombas de Tiempo
    6.5.1 Introducción
    6.5.2 Descripción
6.6 Contramedidas
    6.6.1 Introducción
    6.6.2 Anti-Virus
    6.6.3 NIDS (Sistemas de detección de intrusiones de red)
    6.6.4 HIDS (Sistemas de detección de intrusiones de host)
    6.6.5 Firewalls (Cortafuegos)
    6.6.6 Sandboxes (Cajas de arena)
6.7 Sanos Consejos de Seguridad

Lección 7: Attack Analysis

7.0 Introducción
7.1 Netstat y Cortafuegos –firewall - de aplicaciones de hospedaje
    7.1.1 Netstat
    7.1.2 Cortafuegos (Firewalls)
    7.1.3 Ejercicios
7.2 Analizadores de paquetes
    7.2.1 Analizando
    7.2.2 Decodificando el tráfico de red
    7.2.3 Analizando otras computadoras
    7.2.4 Sistemas de Detección de Intrusos –IDS por sus siglas en inglés
    7.2.5 Ejercicios
7.3 Redes y Sistemas Tipo Señuelo (Honeypots y Honeynets)
    7.3.1 Tipos de Sistemas Tipo Señuelo
    7.3.2 Construyendo un Sistema Tipo Señuelo
    7.3.3 Ejercicios

Lección 8: Digital Forensics

8.1. Introducción
8.2. Principios del Forensics
    8.2.1. Introducción
    8.2.2. Evita la contaminación
    8.2.3. Actúa metódicamente
    8.2.4. Cadena de Evidencias
    8.2.5. Conclusiones
8.3. Análisis forense individualizado
    8.3.1. Introducción
    8.3.2. Fundamentos sobre discos duros y medios de almacenaje
    8.3.3. Encriptación, Desencriptación y Formatos de Ficheros
    8.3.4 Buscando una aguja en un pajar
        8.3.4.1 Find
        8.3.4.2 Grep
        8.3.4.3 Strings
        8.3.4.4 Awk
        8.3.4.5 El pipe " | "
    8.3.5 Haciendo uso de otras fuentes
8.4 Network Forensics
    8.4.0 Introducción
    8.4.1 Firewall Logs
    8.4.2 La cabecera de los mails
8.5 Lecturas de interés

Lección 9: Seguridad del Correo Electrónico (E-Mail)

9.0 Introducción
9.1 ¿Cómo funciona el correo electrónico?
    9.1.1 Cuentas de correo electrónico
    9.1.2 POP y SMTP
    9.1.3 Correo Web
9.2 Utilización segura del Correo Parte 1: Recibiendo
    9.2.1 Spam, Phishing y Fraude
    9.2.2 Correo HTML
    9.2.3 Seguridad en Archivos Anexados
    9.2.4 Encabezados Falsos / Forged headers
9.3 Utilización Segura del Correo Parte 2: Enviando
    9.3.1 Certificados Digitales
    9.3.2 Firmas Digitales
    9.3.3 Obteniendo un certificado
    9.3.4 Encriptación / Cifrado
    9.3.5 ¿Cómo funciona?
    9.3.6 Desencriptación
    9.3.7 ¿Es el cifrado irrompible?
9.4 Seguridad en las Conexiones

Lesson 10: Web Security

in progress

Lección 11: Passwords

11.1. Introducción
11.2. Tipos de Passwords
    11.2.1. Cadenas de caracteres
    11.2.2. Cadenas de caracteres más un token
    11.2.3. Passwords biométricos
11.3. Historia de las Contraseñas
    11.3.1. Ejercicio 1
11.4. Construcción de passwords robustos
    11.4.1. Ejercicio 1
    11.4.2. Ejercicio 2
11.5. Cifrado de los passwords
    11.5.1. Ejercicio 1
    11.5.2. Ejercicio 2
    11.5.3. Ejercicio 3
11.6. Password Cracking (password Recovery)
    11.6.1. Ejercicio
11.7. Protección contra el descifrado de passwords
    11.7.1. Ejercicio

Lección 12: Legalidad y Ética en Internet

12.1. Introducción
12.2. Delitos transfronterizos versus Derechos locales
12.3. Delitos relativos a las TIC's
    12.3.1. Delitos relacionados con la pornografía
    12.3.2. Descubrimiento y revelación de secretos: Correo Electrónico
    12.3.3. Descubrimiento y revelación de secretos: Secretos de Empresa
    12.3.4. Delitos relacionados con instrumentos tecnológicos para la manipulación de accesos y/o contenidos
    12.3.5. Daños en programas o documentos electrónicos, soportes o sistemas informáticos
    12.3.6. Delitos por agresión a la propiedad intelectual
12.4. Prevención de Delitos y Tecnologías de doble uso
    12.4.1. Los sistemas globales de vigilancia: el concepto "COMINT"
    12.4.2. El sistema "ECHELON"
    12.4.3. El sistema "CARNIVORE"
    12.4.4. Ejercicio 1
    12.4.5. Ejercicio 1
12.5. Hacking Ético
    12.5.1. Ejercicio
12.6. Los 10 delitos y fraudes más usuales en Internet
    12.6.1. Ejercicio
12.7. Lecturas recomendadas

Glosario

Para mas definiciones de términos computacionales, se puede consultar www.webopedia.com, la cual proporcionó algunas de las definiciones reproducidas aquí.

awk – Lenguaje de programación diseñado para el trabajo con cadenas de caracteres.

Baudio – bits por segundo, se utilizan para describir la tasa de intercambio de información de una computadora.

BIOS – basic input/output system (sistema básico de entrada/salida). Es el software incluído en una computadora que determina lo que puede hacer esta sin acceder a un programa en disco. En las computadoras personales, el BIOS contiene todo el código necesario para controlar la pantalla, teclado, unidades de disco, puertos seriales y diversas funciones adicionales. Típicamente el BIOS se encuentra en una memoria ROM (Memoria de solo acceso) que viene en la placa base.

blog (weblogs) – Página web que funciona como diario electrónico para un individuo, y es accesible publicamente.

Bombas de tiempo – Código diseñado para ejecutarse en un momento específico en una computadora. Un ejemplo es cuando se llega a la fecha de expiración de un software de prueba.

Bombas lógicas – Código diseñado para ejecutarse cuando se cumple una condición o sucede una actividad específica en una red o computadora.

Cache – Es un tipo de memoria especial de alta velocidad. Puede ser una sección reservada de la memoria principal o un dispositivo independiente. Existen dos tipos principales de cache: de disco y de memoria.

Cliente – Un programa en la computadora local que es utilizado para intercambiar datos con una computadora remota. Ver Servidor.

Cluster /unidad de asignación – Grupo de sectores de disco. El sistema operativo asigna un identificador único a cada cluster y mantiene el rastro de los archivos de acuerdo a los clusters que utilizan.

Concentrador – Punto común de conexión para dispositivos de red. Generalmente utilizado para conectar equipos en redes locales.

Cookie – Es un mensaje proporcionado a un navegador por el servidor web. El navegador guarda el mensaje en un archivo de texto que puede estar cifrado. Este mensaje es enviado de vuelta al servidor cada vez que el cliente solicita una página nueva. Las cookies pueden ser encriptadas en disco.

Correo electrónico – Servicio que permite la transmisión de mensajes a través de diversas redes.

CRC – Cyclical redundancy check. Prueba de redunancia cíclica.

DHCP – Dynamic Host Configuration Protocol. Protocolo de configuración dinámica de host.

Digital Subscriber Line (DSL) – Línea de suscripción digital. Es una tecnología que permite la transmisión simultanea de voz y datos a alta velocidad utilizando como medio las líneas telefónicas tradicionales.

Dirección IP – Identificador para una computadora en Internet o una red TCP/IP. El formato de una dirección IP es un número de 32 bits, escrito como cuatro números separados por puntos. Cada número puede ir desde cero hasta 255.

Dirección MAC (Media Access Control) – Dirección de hardware única que identifica a cada nodo de una red.

DNS – Domain Name Server. Servidor de nombres de dominio.

Domain Name Server (DNS) – Es un servicio que traduce los nombres de dominio a direcciones IP.

DSL – Digital Subscriber Line.

Dynamic Host Configuration Protocol (DHCP) – Ver DHCP.

Ethereal – Analizador de protocolos que registra el tráfico que circula por la red a la que se encuentra conectado.

Ethernet – Arquitectura de LAN desarrollada por Xerox Corporation en conjunto con DEC e Intel en 1976. Es uno de los estándares de LAN ampliamente implementados.

Filtrado (puertos) – puertos abiertos en un host, para los cuáles un firewall examina la cabecera de un paquete y determina si dejará o no pasar el paquete. (ver puertos abiertos).

Firewall – Sistema designado para prevenir el acceso no autorizado de una red a otra. Los firewalls pueden ser implementados a través de hardware, software o una combinación de ambos.

Firma de archivo – Es una pequeña cabecera de 6 bytes al inicio de un archivo, que identifica que tipo de archivo es.

Foro – Grupo de discusión en línea. Los servicios en línea y servicios de boletines (BBS´s) proveen una variedad de foros que los participantes pueden intercambiar mensajes de acuerdo a intereses comúnes.

FTP – File transfer protocol. Protocolo de transferencia de archivos.

FTP Anónimo – Método por el cual, los archivos en una computadora son puestos a disposición del público general para su descarga.

GCHQ – Government Communications Headquarters, oficinas de comunicaciones de gobierno. Es una organización relacionada con la seguridad e inteligencia en el Reino Unido.

Grupo de noticias – Newsgroups. Es lo mismo que un foro, un grupo de discusión en línea.

grep – Acrónimo de global-regular-expression-print. Es una utilería de UNIX que permite al usuario realizar búsquedas de cadenas de caracteres en uno o mas archivos. La salida de la herramienta consta de las líneas donde aparece la cadena buscada.

Gusano – Worm. Programa que se reproduce a si mismo en una red de computadoras, y generalmente realiza acciones maliciosas como el uso de recursos, pueden incluso llegar a dar de baja el sistema.

HIDS – Acrónimo de host intrusion detection system. Sistema de detección de intrusos basado en host.

Honeypot – Equipo conectado al Internet, que actúa como un señuelo para atraer intrusos y así poder estudiar sus actividades, además de monitorear el proceso de intrusión a un sistema.

Http – Hypertext transfer protocol.

Hypertexto – Método de organizar y presentar datos, de manera que sea fácil al usuario el movimiento entre elementos relacionados.

Hypertext transfer protocol (http) – El protocolo utilizado por el World Wide Web. HTTP define el formato y transmisión de mensajes. También define las acciones que pueden tomar los navegadores en respuesta a diversos comandos.

IANA – Internet Assigned Numbers Authority.

ICMP – Internet Control Message Protocol.

IM – Instant messaging.

Instant messaging (IM) – Mensajería instantanea. Es un servicio de comunicación que permite crear una plática privada con otro individuo, en tiempo real, a través del Internet.

Interfaces – Límites entre el cual dos sistemas independientes se comunican entre ellos.

Internet Assigned Numbers Authority (IANA) – Organización de trabajo auspiciada por la Internet Architecture Board (IAB). Es responsible de asignar direcciones IP en Internet.

Internet Control Message Protocol (ICMP) – Extensión del IP (Internet Protocol) definido en el RFC 792. ICMP se encarga del envío de mensajes de error, control e información. El comando PING es un ejemplo del uso de ICMP para probar una conexión.

Internet protocol (IP) – IP especifica el formato y direccionamiento de los paquetes. La mayoría de las redescombinan IP con un protocolo de capa superior como TCP (Transmision Control Protocol). TCP establece un circuito virtual entre la fuente y el destino.

Internet Relay Chat (IRC) – Servicio que permite la comunicación entre usuarios de internet en tiempo real, basada en texto.

IP – Internet protocol.

Ingeniería Social – El acto de obtener, o intentar obtener información o datos confidenciales a través del uso de técnicas de engaño, entre otras, con las personas.

Ipconfig – Herramienta de Windows para desplegar información de las interfaces activas en la computadora.

IRC – Internet Relay Chat.

ISP – Internet Service Provider. Ver Proveedor de servicio de Intenet.

Lógica Booleana – La lógica booleana es una forma de algebra, en la cual todos los valores se reducen a VERDADERO o FALSO. Esta lógica es importante para las ciencias computacionales, ya que se acomoda perfectamente al sistema numérico binario en el que los posibles valores son 1 y 0.

Loopback – Es cuando una computadora se refiere a si misma. La dirección IP de la interface de loopback es un número especial (127.0.0.1). Esta interface es virtual, ya que no existe hardware asociado, ni se encuentra conectada a la red.

MAC – Media access control.

MD5 hash – Algoritmo utilizado para crear firmas digitales. MD5 es una función de una vía, toma un mensaje de longitud variable y lo convierte en una salida de longitud fija conocido como digestión. Su intención es para utilizarse con máquinas de 32 bits. Es mas seguro que el algoritmo MD4, el cual ya ha sido comprometido.

Modem – Modulador/Demodulador. Dispositivo que convierte las señales analógicas en señales digitales y viceversa, permitiendo así la comunicación entre computadoras a través de las líneas telefónicas.

MS-DOS (Microsoft Disk Operating System) – MS-DOS es un sistema operativo. Permite la comunicación entre los usuarios y el hardware de la computadora. También controla el acceso a los recursos, tales como memoria, dispositivos y uso de procesador.

Navegador – Programa que permite a los usuarios conectarse a servidores web para visualizar las páginas almacenadas.

netstat – comando que despliega el estado de la red.

NIDS – Network intrusion detection system.

nmap – programa que realiza un barrido de puertos a una computadora, en busca del estado de estos (abierto, cerrado, filtrado).

Nombre de dominio – Nombre que identifica una o mas direcciones IP. Cada nombre de dominio cuenta con un sufijo que indica a que dominio raíz (TLD) pertenece.

Existe solo un número limitado de dichos dominios, por ejemplo:

.gov – Agencias gubernamentales

.edu – Instituciones educacionales

.org – Organizaciones (sin ánimo de lucro)

.com – Organización comercial

.net – Organización de red

Dado que Internet se basa en direcciones IP en lugar de nombres de dominio, todos los servidores web requieren un servicio de nombres de dominio (DNS) que traduzca los nombres en direcciones IP.

NSA – National Security Agency. Agencia nacional de seguridad de Estados Unidos. Es la organización que coordina, dirige y realiza actividades altamente especializadas para proteger los sistemas de información de Estados Unidos y producir información para la inteligencia.

P2P – Punto a punto (peer to peer).

Paquete – Es una parte de un mensaje que es transmitido a través de una red de conmutación de paquetes.

Punto a punto (P2P) – es un tipo de red en la cual cada estación cuenta con responsabilidades y capacidades equivalentes.

Ping – Utilería para determinar si una dirección IP específica es accesible. Su funcionamiento se basa en enviar un paquete ICMP a una dirección IP y esperar una respuesta.

POP – Post Office Protocol. Es el protocolo utilizado para extraer el correo electrónico de un servidor de correo. La mayoría de las aplicaciones cliente de correo utilizan el protocolo POP o IMAP.

Proveedor de servicio de Internet (ISP) – Compañía que proporciona acceso a internet a los usuarios.

POTS – Plain old telephone service.

ppp – Protocolo punto a punto. Es un método de conectar una computadora al Internet. PPP es mas estable que sus predecesores como SLIP, y además provee de características de control de errores.

Privilegios de acceso – El privilegio de utilizar la información de una computadora en alguna forma. Por ejemplo, un usuario puede tener permisos de lectura y acceso a un archivo, significando que puede leer el archivo pero no modificarlo ni eliminarlo. La mayoría de los sistemas operativos cuentan con diferentes dipos de privilegios de acceso que pueden ser establecidos para los usuarios o grupo de estos.

Protocolo – Formato establecido entre partes para la transmisión de datos.

Protocolo de transferencia de archivos (FTP) – Protocolo utilizado para permitir la descarga de archivos remotamente.

Prueba de redundancia cíclica (CRC) – Es una técnica común para detectar errores de transmisión de datos. Los mensajes transmitidos son divididos en longitudes determinadas, que son divisibles entre un número establecido. De acuerdo al cálculo, el número que sobra de esta división se anexa al mensaje al momento de ser enviado. Cuando el mensaje es recibido, la computadora vuelve a calcular el sobrante y compara el recibido con su propio resultado, si los números no son iguales, se detecta un error.

Puertas traseras – Forma indocumentada de ganar acceso a un programa, servicio en linea, o todo un sistema computacional.

Puerto – Es la interface de una computadora a través de la cual se conecta un dispositivo. Las computadoras personales cuentan con diversos puertos; internamente se utilizan para conectar unidades de disco, pantallas y teclados. Externamente se conectan modems, impresoras, ratones y otros dis´positivos periféricos.

Puerto Abierto – puertos que permiten que los paquetes tengan acceso al servicio proporcionado.

RAM (Random Access Memory) – Memoria de acceso aleatorio. Es untipo de memoria que puede ser accesada de manera aleatoria, significando que se puede acceder cualquier byte sin la necesidad de tocar los bytes precedentes.

Red telefónica conmutada – También conocida como POTS (Plain Old Telephone System). Término utilizado para describir la red telefónica conmutada tradicional.

Rompimiento de contraseñas – Es el proceso de intentar determinar una contraseña desconocida.

Rootkit – programa malicioso que permite mantener el acceso a un equipo.

Ruteador – Dispositivo que reenvia paquetes entre redes. Un router debe conectarse en la frontera de dos redes, comunmente entre dos redes de área local, o una red local y un proveedor de servicios. Los ruteadores utilizan la información del encabezdo de los paquetes y tablas de ruteo para determinar el mejor camino para reenviar un paquete. Entre routers se utilizan diversos protocolos para la comunicación de rutas, y así determinar el mejor camino.

Sandbox – Medida de seguridad utilizada en JAVA. Consta de reglas que son utilizadas cuando se crea un applet, y que previene que ciertas funciones sean ejecutadas cuando el applet es enviado como parte de una página web.

Script kiddie – Persona que utiliza herramientas de hackeo sin conocer su funcionamiento o propósito.

Sector – es la mínima unidad de acceso en un disco.

Secure Shell – Protocolo diseñado como un reemplazo para Telnet. Utiliza cifrado de datos en la comunicación y permite la ejecución remota de comandos, así como también la transferencia de archivos.

Servidor – Programa en una computadora remota que provee datos o un servicio a una computadora cliente.

Servidor Web – Computadora donde se almacenan páginas para que puedan ser accesadas por otras computradoras.

Servicios – Los servicios de red permiten a computadoras remotas el intercambio de información.

Sector de arranque – Es el primer sector de un disco duro, donde se encuentra un pequeño programa que se ejecuta cuando se enciende una computadora. Este programa es registro maestro de arranque (MBR – Master Boot Record).

Sistema de detección de intrusos en red (NIDS) – Network intrusion detection system. Es un sistema de detección de intrusos en el cual cada paquete que atraviesa la red es analizado.

Sistema operativo – El programa de bajo nivel que se ejecuta en una computadora. Cada computadora de propósito general debe tener un sistema operativo para ejecutar otros programas. El sistema operativo proporciona las tareas básicas de bajo nivel como: reconocel el teclado, enviar las salidas al monitor, mantener un control sobre los archivos y directorios del sistema, y controlar los dispositivos de entrada y salida. Algunos sistemas operativos son Windows, Unix y Linux.

SMTP – Simple Mail Transfer Protocol. Protocolo para el envío de correo electrónico entre servidores. La mayor parte de los sistemas de correo electrónico envían utilizan SMTP en Internet.

Sniffer – También conocido como analizador de protocolos. Es un programa o dispositivo que monitorea los datos que viajan a través de una red.

Spyware – Software que obtiene información del usuario, sin el conocimiento de este, y lo envía a través de la conexión a Internet.

SSH – Secure Shell.

Switch – En el ámbito de las redes, dispositivo que filtra y reenvia paquetes entre segmentos de una red local.

Tabla de ruteo – Es la tabla donde se almacenan los caminos disponibles para realizar el proceso de ruteo.

TCP – Transmission Control Protocol. Protocolo de control de transmisión. Permite establecer una conexión entre dos equipos, y realizar un intercambio de flujos de datos. TCP garantiza la recepción de los datos en el orden en que son enviados.

TCP/IP – Transmission Control Protocol/Internet Protocol. El conjunto de protocolos utilizados para la comunicación en algunas redes locales e Internet.

Tcpdump – analizador de protocolos que registra el tráfico que circula por la red.

Telnet – Protocolo que permite a un usuario establecer una sesión remota que permite el uso de recursos y ejecución de comandos.

Topología – La estructura de una red de área local (LAN) o un sistema de comunicaciones.

Tracert – Utilería que realiza el trazado de un paquete desde un equipo hacia otro, desplegando el número de saltos del paquete, el tiempo que tarda en cada salto, y el nombre o dirección de cada nodo.

Track – Parte de un disco donde se pueden almacenar datos. Un disco flexible cuenta con 80 (doble densidad)) o 160 (alta densidad) tracks. Para los discos duros, cada plato se divide en tracks; una posición de track en todos los platos (por ambos lados) se llama cilindro. Un disco duro cuenta con miles de cilindros.

Troyano – Programa destructivo que se oculta como una aplicación legítima. A diferencia de los virus y gusanos, los troyanos no se replican pero pueden llegar a ser igual de destructivos.

Weblogs (blogs) – Ver blog.

Whois – Utilería de internet que permite consultar la información referente a un dominio de Internet o una dirección IP.

World Wide Web (www)– Servicio para la presentación y transmisión de hypertexto.

Zine – Pequeña publicación gratuita, producida generalmente por periodistas novatos o aficionados.