ANEXOS

ANEXO 1

PRÁCTICA - ALUMNOS

REFORZAMIENTO DE LA SEGURIDAD CON BASTILLE (HARDENING)

1.- OBJETIVOS DE APRENDIZAJE

Al terminar esta práctica, el alumno:

- Comprenderá la importancia de la herramienta de seguridad Bastille Linux, para el reforzamiento del sistema operativo.
- Será capaz de realizar la instalación de Bastille Linux.
- Podrá configurar Bastille Linux para reforzar el sistema operativo de acuerdo con las políticas de seguridad que requiera.

2.- Conceptos teóricos

Bastille Linux es una herramienta de seguridad para el reforzamiento del sistema operativo. Se trata de un conjunto de secuencias de comandos que permiten realizar la configuración del sistema de manera simplificada, de manera que podemos obtener que nuestro sistema operativo sea lo menos vulnerable posible. Mediante una buena configuración de Bastille Linux se pueden eliminar un gran número de vulnerabilidades comunes en plataformas Linux/Unix.

De manera interactiva Bastille Linux crea una configuración segura para el sistema basado en las respuestas del usuario.

Con Bastille se pueden realizar cuatro pasos para asegurar el sistema:

- Aplicar un firewall para prevenir el acceso a posibles servicios vulnerables.
- Aplicar actualizaciones para los agujeros de seguridad conocidos.
- Realizar un SUID, root audit (establecer permisos de acceso a archivos y directorios).
- Desactivar o restringir servicios innecesarios.

Los anteriores pasos se subdividen en módulos que cubren cada una de las áreas anteriormente descritas.

- Módulo ipchains: permite la configuración de un firewall para filtrar el tráfico y así proteger la red.

- Módulo patch download: ayuda a mantener actualizados los servicios que se usan en el servidor. Lo más importante es aplicar actualizaciones a los agujeros de seguridad conocidos.

- Módulo file permissions: este módulo permite realizar una auditoría sobre los permisos de archivos en el sistema. Restringe o habilita permisos para el uso de servicios y archivos binarios.

- Módulo account security: con este módulo se obliga al administrador a tener "buenas prácticas" en el manejo de cuentas, además de que provee algunos trucos para realizar de una manera más efectivo el manejo de cuentas.

- Módulo boot security: en este módulo podemos habilitar ciertas opciones de arranque para hacerlo más seguro y evitar que sean aprovechadas las vulnerabilidades inherentes a los sistemas operativos tipo Linux/Unix.

- Módulo secure inetd: con este módulo podemos deshabilitar servicios que podrían significar una vulnerabilidad grave al poder ser iniciados con privilegios de root. En caso de que no se pueda deshabilitar dichos servicios por ser necesarios para los usuarios o para el sistema, entonces se restringen los privilegios. En este caso se recomienda deshabilitar telnet, ftp, rsh, rlogin y talk. Pop e imap son protocolos de correo que deben ser deshabilitados únicamente si no se requieren en el sistema.

- Módulo disable user tools: en este módulo podemos restringir el uso del compilador para que únicamente sea accesible para el usuario root.

- Módulo configure misc pam: partiendo de la idea de que un servidor debe tener únicamente los servicios y herramientas necesarias, en este módulo se pueden hacer ciertas modificaciones que harán difícil a los usuarios, incluidos los usuarios "nobody", "web" y "ftp", que abusen de los recursos para producir un ataque de *denegación de servicios*.

- Módulo logging: aquí manejamos y configuramos las bitácoras adicionales que contienen información del sistema, mensajes del kernel, mensajes de errores graves, etc.

- Módulo miscellaneous daemons: en este módulo se desactivan todos los demonios del sistema que no sean necesarios, los cuáles se pueden volver a activar con el comando chkconfig.

- Módulo sendmail: permite deshabilitar comandos sendmail que son usados para obtener información acerca del sistema para realizar cracking o spamming.
- Módulo remote access: el acceso remoto se puede configurar de manera que se realice mediante *secure shell* client, un programa seguro de cifrado de información.
- Los módulos dns, *apache*, printing y ftp permiten configurar cada uno de los servicios que previamente se han asegurado en caso de que no se haya deshabilitado y establecer cierta seguridad en la forma de levantar dichos servicios.

Todos los módulos mencionados anteriormente se establecen al momento de responder a las preguntas que el script de Bastille realiza al ejecutarse, por lo que se simplifica la tarea de configuración de esta herramienta, sin embargo, es muy importante contestar dicho cuestionario de acuerdo con las políticas de seguridad establecidas por cada institución. En este caso se consideran los aspectos que generalmente se aseguran en un sistema tipo Linux, multiusuario y con características de servidor web.

3.- MATERIAL NECESARIO

Computadora con sistema operativo Linux con alguno de los siguientes sistemas operativos soportados por bastille:

LINUX:
'DB2.2' 'DB3.0' 'RH6.0' 'RH6.1' 'RH6.2'
'RH7.0' 'RH7.1' 'RH7.2' 'RH7.3' 'RH8.0'
'RH9' 'RHEL5' 'RHEL4AS' 'RHEL4ES' 'RHEL4WS'
'RHEL3AS' 'RHEL3ES' 'RHEL3WS' 'RHEL2AS' 'RHEL2ES'
'RHEL2WS' 'RHFC1' 'RHFC2' 'RHFC3' 'RHFC4'
'RHFC5' 'RHFC6' 'RHFC7' 'RHFC8' 'MN6.0'
'MN6.1 ' 'MN7.0' 'MN7.1' 'MN7.2' 'MN8.0'
'MN8.1' 'MN8.2' 'MN10.1' 'SE7.2' 'SE7.3'
'SE8.0' 'SE8.1' 'SE9.0' 'SE9.1' 'SE9.2'
'SE9.3' 'SE10.0' 'SE10.1' 'SE10.2' 'SE10.3'
'SESLES8' 'SESLES9' 'SESLES10' 'TB7.0'

Donde DB significa Debian, RH Red Hat, RHEL Red Hat Enterprise Linux, RHFC Red Hat Fedora Core, MN Mandriva, SE SUSE, SESLES SUSE Linux Enterprise Server.

Privilegios para realizar la instalación en dicho equipo, archivo Bastille-x.x.x.tar.bz2.

4.- DESARROLLO

4.1 Modo de trabajo

Al principio se revisará el estado de algunos elementos importantes del sistema operativo antes de ejecutarse Bastille, posteriormente se ejecutará Bastille y se realizará la configuración recomendada más adelante en esta práctica. Finalmente se comprobará que se hayan realizado los cambios de acuerdo con la configuración realizada.

4.3 Revisión del estado del sistema.

Abra una terminal o Shell (Main Menu, System Tools=> Terminal), y ejecute los siguientes comandos:

ls -l /bin/mount
-rwsr-xr-x 1 root root 52012 abr 6 2007 /bin/mount

ls -l /bin/ping
-rwsr-xr-x 1 root root 36140 abr 6 2007 /bin/ping

ls -l /usr/bin/at
-rwsr-xr-x 1 root root 45380 mar 27 2007 /usr/bin/at

Lo que se puede ver tras la ejecución del comando “ls” en los tres casos es los comandos mount, ping y at tienen el bit SUID activado. Este bit permite a un programa ser ejecutado por un usuario con los permisos de superusuario. Si bien se tiene una mejora por la facilidad de uso, esto reduce la seguridad, ya que algún usuario podría adquirir los derechos de superusuario sin estar autorizado. Se sugiere eliminar este ya que representa un problema de seguridad.

Otros programas que se consideran inseguros son rcp, rlogin, rsh, debido a que no cifran los datos que envían a través de la red y utilizan como método de autenticación únicamente la dirección IP, algo que se considera inadecuado. Al listar los comandos de dichos programas se puede observar que también tienen activado el bit SUID.

ls –l /usr/bin/rlogin
-rwsr-xr-x 1 root root 14388 abr 11 2007 /usr/bin/rlogin
ls –l /usr/bin/rsh
-rwsr-xr-x 1 root root 8940 abr 11 2007 /usr/bin/rsh
ls –l /usr/bin/rcp
-rwsr-xr-x 1 root root 18640 abr 11 2007 /usr/bin/rcp
ls –l /usr/bin/rexec
-rwsr-xr-x 1 root root 14300 abr 11 2007 /usr/bin/rexec

Otro factor importante es la máscara de usuario (umask), una función que establece los permisos por defecto para los nuevos archivos y directorios creados. Se puede ver la máscara establecida al ejecutar el comando umask, en este caso la máscara es 0022, lo que nos dice que los nuevos archivos y directorios creados tendrán permisos 755.

umask
0022

Ahora ejecute el comando ulimit para verificar el número de procesos que puede ejecutar un usuario.

ulimit
unlimited

Esto también representa una vulnerabilidad ya que se puede ejecutar un ataque de *denegación de servicios* para colapsar el sistema.

Los aspectos analizados anteriormente son una pequeña parte del hardening (reforzamiento de la seguridad) que se debe realizar en el sistema. En Linux, esto se realiza mediante el uso de comandos y la edición de los archivos de configuración correspondiente; con Bastille Linux ya no es necesario saber exactamente que comando hay que ejecutar y que archivos modificar para asegurar el sistema, esto representa una gran ventaja si se sabe que realiza Bastille al aplicar la configuración del sistema.

4.3 Instalación de Bastille Linux

Encienda la computadora y elija arrancar con el sistema operativo Linux.

- Abra una terminal o Shell (Main Menu, System Tools=> Terminal)

  Se requieren permisos de administrador para hacer la instalación de Bastille por lo que ejecutaremos el siguiente comando:

  su – root

  ahora ingresaremos la contraseña proporcionada por el profesor.

- A continuación usamos el comando yum (Yellow Dog Updater Modified), una herramienta para el manejo de paquetes en Linux, para instalar perl-Curses y perl-TK, dos librerías que nos permiten crear interfaces basadas en texto e interfaces gráficas. Ejecuté los siguiente comandos:

  *yum install perl-Curses**

  *yum install perl-Tk**

- En seguida copiamos el archivo de Bastille al directorio /usr/local, lo descomprimimos y realizamos su instalación con los siguientes comandos:

  bzip2 -d Bastille-x.x.x.tar.bz2

  tar xvf Bastille-x.x.x.tar

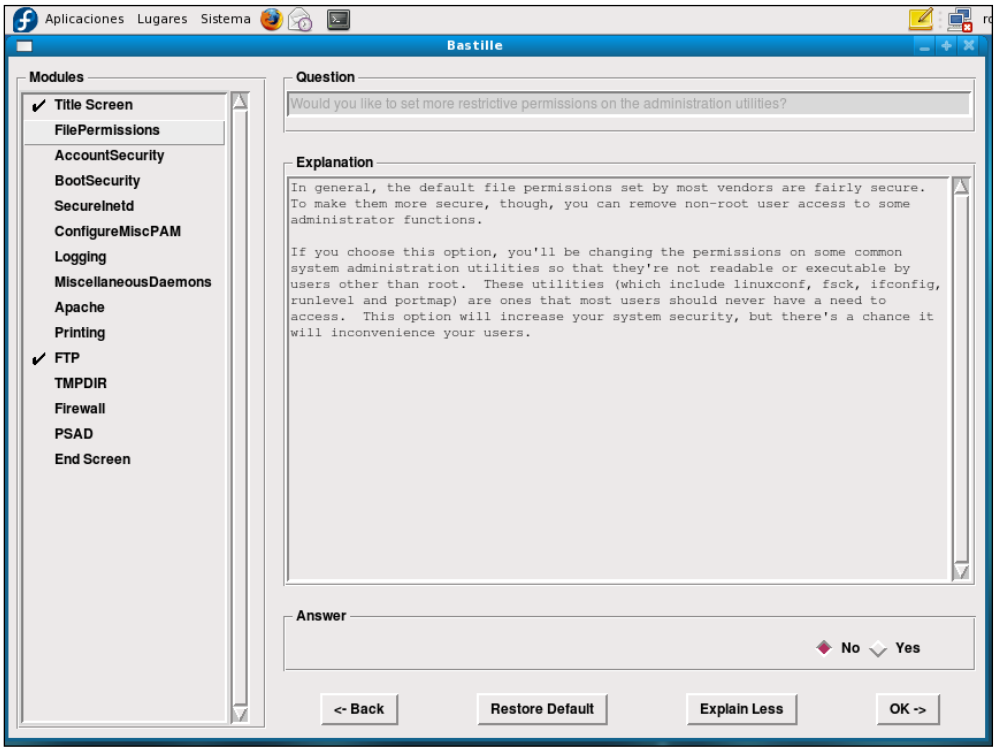
  cd Bastille

  sh Install.sh

  bastille –x

  accept

- Al ejecutar el comando "bastille –x" se abre la interfaz de configuración de Bastille Linux y podemos comenzar a configurar Bastille Linux, figura 6.1.



6.1, Configuración de Bastille Linux

En esta práctica se realizará la configuración de Bastille para asegurar el sistema operativo sin incluir la configuración del firewall, ya que se considera que el firewall es una parte del sistema de defensa tan importante que requiere una instalación y configuración independiente.

Ahora, por cada pregunta que nos presenta Bastille Linux, tenemos que ingresar una respuesta del tipo “Y” (si) o “N” (no), lo cual haremos a continuación, además, se deben completar las razones por las cuáles se responde Y o N, en su caso, donde aparezca la línea contínua:

FILE PERMISSIONS

- ***Would you like to set more restrictive permissions on the administration utilities? [N]***

  Útil en máquinas con múltiples cuentas de usuario pero en este caso se trata de una máquina dedicada para establecer el sistema de seguridad.

- ***Would you like to disable SUID status for mount/umount? [Y]***
- ***Would you like to disable SUID status for ping? [Y]***
- ***Would you like to disable SUID status for at? [Y]***

  Anote la justificación a las respuestas anteriores:

  _____
  _____
  _____
  _____

- ***Would you like to disable the r-tools? [Y]***

  Anote la justificación a la respuesta anterior:

  _____
  _____
  _____

- ***Would you like to disable SUID status for usernetctl? [Y]***

ACCOUNT SECURITY

- ***Should Bastille disable clear-text r-protocols that use IP-based authentication? [Y]***

  Anote la justificación a la respuesta anterior:

_____
_____
_____
_____

- ***Would you like to enforce password aging? [Y]***

  Anote la justificación a la respuesta anterior:

  _____
  _____
  _____

- ***Do you want to set the default umask? [Y]***

  El umask son los permisos por defecto que el sistema asigna a los archivos que se van creando.

- ***What umask would you like to set for users on the system? _____***

  Continuación de la pregunta anterior, lo mejor es usar la opción ____ para que únicamente el dueño de los archivos y nadie más pueda escribir o leer sobre ellos.

- ***Should we disallow root login on ttys 1-6 ? [N]***

  Esta opción es extremadamente útil con equipos a los que se pueda acceder por SSH sin limitación en cuanto a la IP de origen. En este caso no se limitará el acceso ya que se considera que la configuración del SSH lo contempla.

BOOT SECURITY

- ***Would you like to password-protect the GRUB prompt? [N]***

  Si se tiene acceso físico al equipo cualquier persona podría reiniciar el equipo y obtener una consola de administrador pasándole ciertos parámetros al GRUB, por lo que se debe proteger con una contraseña. Para efectos de la práctica responderemos con [N].

- ***Would you like to password protect single-user mode? [N]***

  Este modo (mono-usuario) permite arrancar el sistema de manera que solamente acceder el administrador del equipo. Generalmente no solicita autenticación por lo que se recomienda proteger este modo mediante una contraseña.

En esta práctica responderemos con [N].

SECURE INETD

- ***Would you like to set a default-deny on TCP Wrappers and xinetd? [N]***

  Se permitirá que se ejecuten estos servicios de conectividad a internet.

  TCP Wrappers es un sistema que se usa para filtrar el acceso de red a servicios de protocolos de Internet. Xinetd es un servicio de Linux que sirve para administrar la conectividad basada en Internet.

- ***Should Bastille ensure the telnet service does not run on this system? [Y]***

  Anote la justificación a la respuesta anterior:

  _____
  _____

- ***Should Bastille ensure inetd's FTP service does not run on this system? [Y]***

  Anote la justificación a la respuesta anterior:

  _____

- ***Would you like to display "Authorized Use" messages at log-in time? [N]***

  Esta opción se puede activar para mostrar un mensaje con las restricciones para uso del sistema.

  Si la respuesta fuera [Y] Bastille preguntará el nombre del responsable del uso del equipo, con lo que creará un mensaje que se alojará en /etc/issue, mensaje que se puede modificar de acuerdo con las especificaciones de la organización a la que pertenece el equipo que se está configurando.

CONFIGURE MISCPAM

- ***Would you like to put limits on system resource usage?____***

  Con esta medida establecemos un límite de 150 procesos por usuario, suficiente para trabajar y evita un ataque del tipo _____.

  AL DAR CLICK EN OK => System rosource limits have been set in the file /etc/security/limits.conf,which you can edit later as necessary.

- ***Should we restrict console access to a small group of user accounts? [N]***

  Permite denegar el acceso a la consola excepto a un grupo determinado de cuentas.

- ***Would you like to add aditional logging? [N]***

  Aunque no representa un peligro tener dos registros adicionales, no se considera necesario en este equipo.

LOGGING

- ***Do you have a remote logging host? [N]***

  Solo se activa en caso de tener un host remoto.

- ***Would you like to set up process accounting? [N]***

  Esta opción permite establecer la contabilidad de procesos y saber quién ejecutó cierto proceso y cuando, aunque parece útil esto puede consumir muchos recursos del sistema y crear bitácoras muy grandes en poco tiempo.

MISCELLANEOUS DAEMONS

- ***Would you like to deactivate NFS and Samba? [Y]***

  El Network File System *(*Sistema de archivos de red*)*, o NFS, es un protocolo utilizado para sistemas de archivos distribuidos. Posibilita que distintos sistemas conectados a una misma red accedan archivos remotos como si se tratara de locales. Samba es una implementación libre del protocolo de archivos compartidos de Windows, antiguamente llamado SMB, fue renombrado recientemente para sistemas de tipo Unix.

- ***Would you like to deactivate the HP OfficeJet (hpoj) script on this machine? [Y]***

  Este script inicia el sistema de soporte en Linux para los dispositivos HP all in one.

- ***Would you like to deactivate ISDN script on this machine? [Y]***

  ISDN es un método para conectar equipos a Internet, con una velocidad de 128 kbps ha sido sustituido por IDSL otro tipo de conexión más rápida.

APACHE

- ***Would you like to deactivate the Apache web server? [N]***

  Anote la justificación a la respuesta anterior:

  _____
  _____

  Se puede habilitar nuevamente con el comando /sbin/chkconfig httpd on

- ***Would you like to bind the Web server to listen only to the localhost? [N]***

  Esto es muy útil cuando se hace desarrollo web, ya que permite editar un sitio web localmente antes de que se cargue en otro servidor.

- ***Would you like to bind the Web server to a particular interface? [N]***

  En caso de que se permita el acceso al servidor web únicamente a la red interna se tiene que contestar [Y] e ingresar la ip del equipo que se quiere asociar y el puerto que debe escuchar.

- ***Would you like to deactivate the following of symbolic links? [Y]***

  En general trataremos de limitar la información del servidor web que puede ser vista por los usuarios. Al desactivar la opción de seguimiento de ligas simbólicas se previene el que un visitante web pueda leer o modificar archivos que no se encuentran en el directorio de publicación web.

TMPDIR

- ***Would you like to install TMPDIR/TMP scripts? [N]***

  Esto nos permitiría crear directorios temporales alternativos al directorio /tmp con la ventaja de ejecutar scripts cuando los usuarios accedieran a dichos directorios.

  Activar esta opción hará que Bastille instale unos scripts en las cuentas de los usuarios que configuren las variables TMPDIR y TMP de tal manera que utilicen directorios de ficheros temporales completamente individuales, en vez de que todos usen el */tmp* lo que puede ser extremadamente peligroso en entornos multiusuarios.

PRINTING

- ***Would you like to disable printing? [Y]***

  Anote la justificación a la respuesta anterior:

Esto se puede revertir con los siguientes comandos:

/bin/chmod 06555 /usr/bin/lpr /usr/bin/lprm

/sbin/chkconfig lpd on

- ***Would you like to disable CUPS'legacy LPD support? [N]***

  Para efectos de la práctica contestaremos [N], pero si el equipo realizará funciones de impresión, se puede deshabilitar el soporte para el protocolo LPD del sistema de impresión común de Unix.

FTP

FIREWALL

- ***Would you like to run the packet filtering script? [N]***

  Esta opción activaría el firewall nativo de Linux, en este caso no se activará porque se recomienda que el firewall se configure por separado y con otras herramientas específicas para la configuración del mismo.

- ***Are you finished answering the questions, i.e. may we make the changes? [Y]***

  Respondemos afirmativamente para que se apliquen los cambios en el sistema.

  Guardar la configuración y después aplicarla al sistema.

Se ha terminado de configurar Bastille Linux, además de aplicarse los cambios en el sistema operativo.

Ahora con una cuenta de usuario sin privilegios probaremos que la configuración anterior funciona correctamente, en este caso probaremos ciertos puntos en el sistema operativo, que deben estar protegidos por la configuración hecha con Bastille Linux:

Los comandos mount, ping y at no deben tener activo el bit SUID

ls -l /bin/mount
-rwr-xr-x 1 root root 52012 abr 6 2007 /bin/mount

ls -l /bin/ping
-rwr-xr-x 1 root root 36140 abr 6 2007 /bin/ping

ls -l /usr/bin/at
-rwr-xr-x 1 root root 45380 mar 27 2007 /usr/bin/at

Otros programas que inseguros como rcp, rlogin, rsh también deben tener desactivado el bit SUID.

ls –l /usr/bin/rlogin
-rwr-xr-x 1 root root 14388 abr 11 2007 /usr/bin/rlogin
ls –l /usr/bin/rsh
-rwr-xr-x 1 root root 8940 abr 11 2007 /usr/bin/rsh
ls –l /usr/bin/rcp
-rwr-xr-x 1 root root 18640 abr 11 2007 /usr/bin/rcp
ls –l /usr/bin/rexec
-rwsr-xr-x 1 root root 14300 abr 11 2007 /usr/bin/rexec

La máscara de usuario (umask), función que establece los permisos por defecto para los nuevos archivos y directorios creados debe tener el nuevo valor (077)
umask
0077

El número de procesos por usuario debe estar restringido a 150, y eso se comprueba con el comando ulimit.

ulimit -a
max user processes (-u) 150

Por lo que el sistema se encuentra protegido si un ataque de saturación de buffer o *denegación de servicios* intenta hacer una replicación infinita de procesos.

El reforzamiento de la seguridad con Bastille Linux se debe verificar en otros aspectos que en este caso no fueron analizados, para ello es necesario saber qué archivos se van a modificar o qué comandos se ejecutarán mediante la configuración hecha con este programa, pero al revisar estos aspectos básicos podemos darnos una idea de las ventajas de utilizar un software de este tipo.

5.- CUESTIONARIO

1.- ¿Cuáles son los cuatro pasos que se pueden hacer con Bastille para asegurar el sistema operativo?

_____
_____
_____

2.- ¿Qué son las r-tools y qué método de autenticación utilizan?

_____
_____
_____

3.- ¿Qué problema de seguridad presenta el servicio Telnet?

_____
_____
_____

4.- ¿Por qué es importante establecer un límite de procesos que puede ejecutar un usuario?

_____
_____
_____

5.- ¿Cuál es la ventaja de utilizar Bastille para asegurar el sistema operativo?

_____
_____
_____

6.- CUESTIONARIO PREVIO

1.- Investigue ¿Qué medidas para reforzar un sistema operativo tipo Linux existen?

_____
_____
_____

2.- ¿Qué función tiene el comando “umask”?

¿qué permisos se deben establecer en un sistema para que se considere seguro?

_____
_____
_____

3.- ¿Qué servicios remotos se consideran inseguros en un sistema tipo Linux y por qué?

_____
_____
_____

4.- ¿Qué es la denegación de servicios?

_____
_____
_____

5.- Investigue ¿Qué herramientas para el reforzamiento del sistema operativo conoce y cuáles son sus características?

_____
_____
_____

GLOSARIO

Apache: Servidor web HTTP de distribución libre y de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, implementa la noción de sitio virtual y tiene una penetración de más del 50% del total de servidores en el mundo.

ARP: El protocolo de resolución de direcciones es responsable de convertir las direcciones de protocolos de alto nivel (direcciones IP) a direcciones de red físicas.

ATM: ATM es una tecnología se usa para crear redes de alta capacidad y respuesta para permitir el trafico de grandes cantidades de información, este estándar de redes permite la transmisión de cualquier tipo de información como video, voz ,datos y cualquier tipo de información que pueda viajar dentro de una red.

Denegación de servicios (DoS, denial of service): Un ataque por denegación de servicios es aquel que causa que algún recurso o servicio esté demasiado ocupado y por lo tanto sea inaccesible para usuarios legítimos.

DES (Data Encryption Standard, estándar de cifrado de datos): es un algoritmo de cifrado en bloque simétrico, de longitud fija, desarrollado originalmente por IBM y posteriormente modificado y adoptado por el gobierno de EE.UU. en 1977 como estándar de cifrado de todas las informaciones sensibles no clasificadas.

DHCP: es el protocolo de configuración de host dinámico, se trata de un protocolo que permite que un equipo conectado a una red pueda obtener su configuración de red en forma dinámica, es decir, sin intervención particular. Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

DMZ (DMZ, DeMilitarized Zone): Una DMZ se define como una red local que se ubica entre la red interna de una organización y una red externa como Internet. Su objetivo es el de permitir conexiones desde la red interna hacia la red externa, pero limitar las conexiones desde el exterior hacia el interior.

Eavesdropping: La interceptación o eavesdropping, también conocida por "escucha secreta" (passive wiretapping) es un proceso mediante el cual un agente capta información, en claro o cifrada, que no le iba dirigida.

Exploit: (del inglés to exploit, explotar o aprovechar) es una pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el

aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado).

FDDI: (Fiber Distributed Data Interface) es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida o local (LAN) mediante cable de fibra óptica.

Firewall (cortafuegos): Un firewall es un dispositivo que controla las comunicaciones, permitiendo o denegando las transmisiones de una red a la otra. En una arquitectura de red, generalmente se sitúa entre una red local e Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Frame Relay: es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos ("frames") para datos, perfecto para la transmisión de grandes cantidades de datos.

Hardening: conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de su equipo.

ICMP: El protocolo de mensajes de control de Internet permite administrar información relacionada con errores de los equipos en red. ICMP notifica los errores a los protocolos de capas cercanas, por lo tanto, este protocolo es usado por todos los routers para indicar un error (llamado un problema de entrega).

IGMP: El protocolo de red IGMP (Internet Group Management Protocol) se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia.

IP: El protocolo IP es parte de la capa de Internet del conjunto de protocolos TCP/IP. Es uno de los protocolos de Internet más importantes ya que permite el desarrollo y transporte de datagramas de IP (paquetes de datos), aunque sin garantizar su entrega.

IP spoofing: La suplantación de IP consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.

Iptables: es un sistema de firewall vinculado al kernel de linux que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log.

MAC address spoofing: El atacante modifica la dirección IP o la dirección MAC de origen de los paquetes de información que envía a la red, falsificando su identificación para hacerse pasar por otro usuario. De esta manera, el atacante puede asumir la identificación de un usuario válido de la red, obteniendo sus privilegios.

MD5: MD5 es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest. Procesa mensajes de una longitud arbitraria en bloques de 512 bits generando un compendio de 128 bits. Debido a la capacidad de procesamiento actual esos 128 bits son insuficientes, además de que una serie de ataques criptoanalíticos han puesto de manifiesto algunas vulnerabilidades del algoritmo.

NASL: Las siglas NASL responden a Nessus Attack Scripting Language, es un lenguage script especialmente pensado para Nessus, y cuyo objetivo es poder lanzar funcionalidades del escáner a través de programas externos que se definan para tales efectos.

OpenSSH: OpenSSH (Open Secure Shell) es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, usando el protocolo SSH.

OpenSSL: Consiste en un robusto paquete de herramientas de administración y librerías relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS).

OSI (Open Systems Interconnection): El modelo de referencia de Interconexión de Sistemas Abiertos es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

Perl: perl es un lenguaje de programación diseñado por Larry Wall en 1987. Perl toma características del lenguaje C, del lenguaje interpretado shell (sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

Posix: Portable Operating System Interface, se trata de una familia de estándares de llamadas al sistema operativo definidos por el IEEE y especificados formalmente en el IEEE 1003. Persiguen generalizar las interfaces de los sistemas operativos para que una misma aplicación pueda ejecutarse en distintas plataformas.

Protocolo: Conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Se trata de una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

Puerta trasera (backdoor): Es una secuencia especial dentro del código de programación mediante la cual se puede evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema.

Secure Shell: SSH es el intérprete de órdenes seguro, se trata del nombre de un protocolo y del programa que lo implementa, y sirve para acceder de manera más segura a máquinas remotas a través de una red.

SHA-256: Secure Hash Algorithm es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos. SHA-256 toma como entrada un mensaje de longitud máxima 2^{64} bits (más de dos mil millones de Gigabytes) y produce como salida un resumen de 256 bits.

SHA-512: Secure Hash Algorithm que produce como salida un resumen de 512 bits.

Sistema de Detección de Intrusos (SDI): Un IDS (Intrusion Detection System) o Sistema de Detección de Intrusiones es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema.

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

Software libre: es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, cambiado y redistribuido libremente.

TCP: (*Protocolo* de Control de Transmisión) es uno de los principales *protocolos* de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el *protocolo* IP). *TCP* es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

Token ring: Token Ring es una arquitectura de red desarrollada por IBM en los años 1970 con topología lógica en anillo y técnica de acceso de paso de testigo. Token Ring se recoge en el estándar IEEE 802.5. En desuso por la popularización de Ethernet; actualmente no es empleada en diseños de redes.

UDP: El *protocolo* UDP (*Protocolo* de datagrama de usuario) es un *protocolo* no orientado a conexión de la capa de transporte del modelo TCP/IP. Este *protocolo* es muy simple ya que no proporciona detección de errores (no es un *protocolo* orientado a conexión).