Apéndice B

Ataques lógicos

1. Password cracking

Entre más débil sea dicha contraseña el obtenerla será mucho más sencillo, se considera una contraseña débil el uso de fechas de cumpleaños, nombres de mascotas, palabras relacionadas con los gustos personales y preferencias, apellidos principalmente, un parámetro que también influye en la debilidad de una contraseña es la longitud de la misma.

Por ejemplo, un ataque basado en fuerza bruta, al tener una contraseña de una longitud de cuatro caracteres ocasiona que las opciones para ser adivinada sean mucho más rápidas, ya que se cuenta con menos combinaciones.

Se sabe que el código ASCII emplea 128 caracteres imprimibles y si se utiliza una contraseña de 4 caracteres el espacio muestral se reduce a 128^4 combinaciones, por lo que si la contraseña es de una longitud mayor, esto permite aumentar el espacio muestral considerablemente y por lo tanto hacerle la tarea más difícil al tratar de encontrar la clave.

El avance computacional que se tiene día con día hace posible que los ataques se vuelvan cada vez más sofisticados y rápidos, esto debido a que el procesamiento en cuanto a cómputo se refiere es mucho más potente cada vez.

Actualmente existen supercomputadoras que pueden realizar hasta mil billones de operaciones por segundo, para conocer qué tan rápida es una computadora se utiliza con frecuencia una medida que indica cuántas operaciones aritméticas en punto flotante puede realizar en un segundo. Esta medida se llama FLOPS (Floating Point Operation Per Second –Operaciones de punto flotante por segundo). Por ejemplo, una supercomputadora típica de los 70's, la CRAY-1, realizaba 250 MFLOPS (250 Millones de operaciones en punto flotante en un segundo).

Un procesador Pentium 4 o Athlon 64, típicamente opera a más de 3 GHz y tiene un desempeño computacional del rango de unos cuantos GFLOPS, lo que equivale a 1000, 000,000 de operaciones por segundo, por lo que el tiempo para romper una contraseña que utiliza el código ASCII y si sólo se utilizaran 4 caracteres sería muy poco.

Sin embargo, el hecho de incrementar la longitud de la contraseña no garantiza nada, lo más conveniente es contar con una contraseña lo más robusta posible utilizando una combinación de letras mayúsculas, minúsculas, números, caracteres especiales y con una longitud mínima de 8 caracteres, así como cambiar periódicamente las contraseñas es otra buena medida para evitar este tipo de ataque.

Algunas herramientas utilizadas para encontrar la contraseña por medio de la fuerza bruta son las siguientes:

a) L0pht Crack

Conocida actualmente como LC5 permite recuperar contraseñas del sistema operativo Windows, también puede ser utilizada para verificar la robustez de una contraseña, una herramienta de apoyo a auditorías, se basa en ataques por fuerza bruta, diccionario.

b) John the Ripper

Permite obtener contraseñas, basado en un ataque de diccionario, disponible para Linux, Windows, MacOS. Es capaz de trabajar con algoritmos de cifrado como DES, SHA1, MD5, Blowfish, Kerberos, hash LM (Windows).

2. Malware

El software malicioso o malware se clasifica en distintas categorías de acuerdo con la forma de operar y de propagarse (figura B.1).

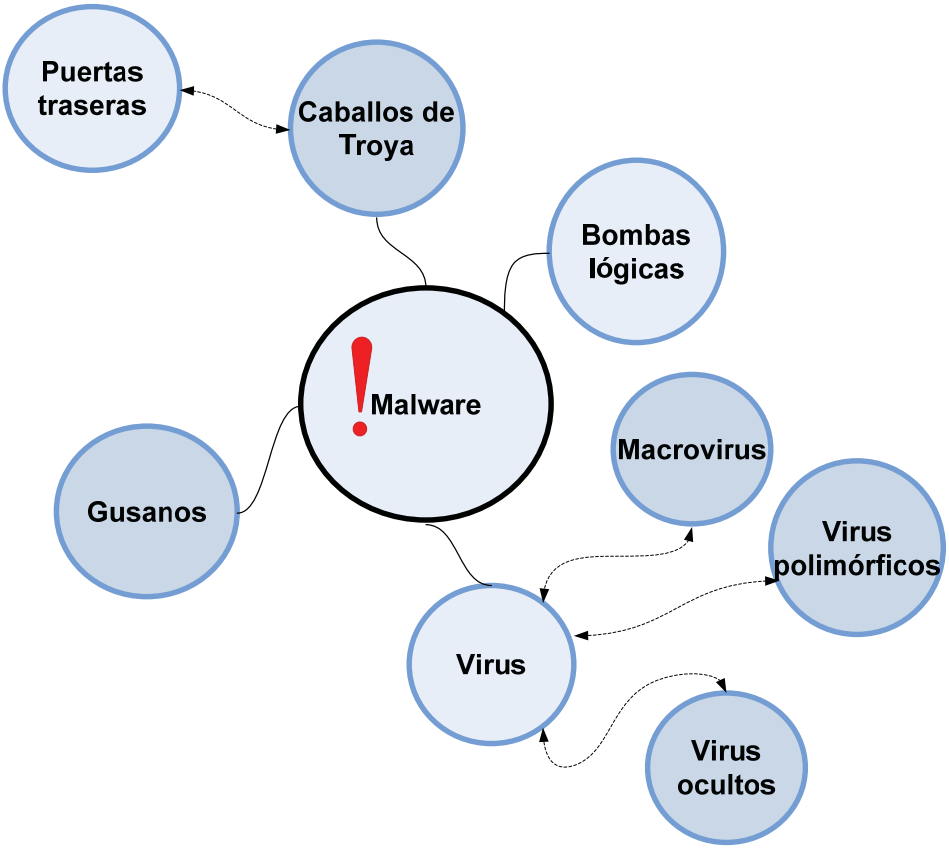

Figura B. 1 Clasificación software malicioso.

Se clasifican en:

- Virus.
- Gusanos.
- Caballos de Troya.

- Spyware.
- Bombas lógicas.
- Back Doors (puertas traseras generadas en los sistemas para ingresar a ellos).
- Spam (Correo no deseado con información publicitaria).
- Dialers (Programas que llaman a números telefónicos de larga distancia o tarifas especiales por medio de un módem).
- Pharming (Modificación de los valores DNS).
- Phishing (Ingeniaría social empleando sitios duplicados y correos electrónicos).
- Rootkit (Programas insertados en un equipo después de tomar el control de éste).
- Adware (Software que muestra o baja anuncios publicitarios).
- Bots (Programa robot que se encarga de realizar funciones rutinarias).
- Exploit (software que explota debilidades de programación).

a) Virus

Es un tipo de código malicioso que necesita ser trasportado por algún otro programa, y se propaga cuando el programa es ejecutado. Los virus se pueden transmitir de varias formas, por ejemplo, pueden formar parte de un archivo que se obtiene de la red o simplemente formar parte de un correo electrónico.

Algunos ejemplos de estos virus son:

- ***Macro virus*:** Cuando una aplicación es abierta los virus ejecutan instrucciones antes de transferir el control de la aplicación, estos virus se replican y se adhieren a otros códigos en el sistema de la computadora.
- ***File infectors:*** Software malicioso que infecta archivos, éstos virus se pueden ejecutar como una de las siguientes extensiones *.com* o *.exe*, se instalan cuando el código es leído, existe otra versión de este tipo de virus los cuales se crean archivos con el mismo nombre pero con extensión *.exe* cuando el archivo es abierto se ejecuta.
- ***Boot infectors:*** Ejecutables que infectan el sistema de arranque de un disco duro o discos, cuando un virus se encuentra alojado en el sector de arranque de un equipo en el momento que el equipo intente cargar el sistema operativo se ejecuta el virus cargándose en memoria obteniendo el control de algunas funciones básicas, además puede propagarse hacia otras computadoras o dispositivo de almacenamiento.

- ***Stealth virus:*** virus ocultos, que actúan sobre funciones del sistema ocultándose ellos mismos además de que comprometen al antivirus, cuando el antivirus genera un reporte de su existencia y éste procede a desinfectar, se ocultan, generalmente aumenta el tamaño del archivo ,fecha de última modificación o fecha de creación.

- ***Virus Polifórmico:*** también conocido como un virus mutante, cambia su firma cada vez que se replica e infecta un nuevo archivo, esto lo hace más difícil de detectar por un antivirus. Esto se debe a que sus firmas digitales no son las mismas cada vez que ejecuta crea una copia de sí mismo. Una de sus técnicas suele ser el auto-cifrado.

Existen programas de hacking para la creación de virus polimórficos como el Mutation Engine, totalmente gratuito y que permite generar virus polimórficos.

En general se puede encontrar una gran cantidad de virus y desde luego cada vez más sofisticados.

b) Gusanos

Los gusanos son un tipo especial de código malicioso ya que se propaga de manera distinta a un virus, a diferencia de éste, no necesita de un portador como un archivo, un gusano contiene procedimientos que le permiten propagarse por distintos equipos a través de la red, generalmente se propagan a través de correos adjuntos, cuando son abiertos se activan y envían una copia de sí mismo a las lista de contactos. El gran peligro de los gusanos es su habilidad para replicarse en grandes números como resultado su propagación por toda la red puede ocasionar una denegación de servicios.

c) Caballos de Troya

Del mismo modo que el caballo de Troya mitológico parecía ser un regalo pero contenía soldados griegos que dominaron la ciudad de Troya, los troyanos de hoy en día son programas informáticos que parecen ser software útil pero que en realidad ponen en peligro la seguridad de un equipo de cómputo**,** estos programas realizan la actividad que el usuario requiere pero al mismo tiempo ejecuta otros procesos que ponen en riesgo al equipo. Los intrusos los usan para ocultar su actividad, capturar información de nombres de usuario y contraseñas y crear puntos de acceso para un futuro ingreso o también conocidas como puertas traseras.

d) Spyware

El software espía se aloja en un equipo con la finalidad de recopilar, enviar información y actividad que se realiza en el equipo, como lo es el software que se utiliza, páginas que visita, historial de teclas oprimidas y manejo del mouse principalmente, la función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.

e) Bombas lógicas

Es otro tipo de código malicioso diseñado para ejecutarse bajo una condición lógica a una hora determinada, y en un día específico.

3. IP Spoofing

Ataque en el que se suplanta la dirección IP de un equipo, existen otros tipos de suplantación como lo son:

a) ***DNS Spoofing-*** Suplantación de identidad por nombre de dominio.

b) ***ARP Spoofing -*** Suplantación de identidad por falsificación de tabla ARP.

c) ***Web Spoofing -*** Suplantación de una página web real.

IP spoofing es un problema sin solución fácil ya que la debilidad que explota es inherente al diseño del protocolo TCP/IP, entendiendo cómo y qué ataques de suplantación son utilizados combinados con métodos simples de prevención, se puede ayudar a prevenir ataques contra la red.

4. Fingerprinting

El ataque de Fingerprinting está relacionado con los escaneos, se clasifica en dos, fingerprinting pasivo y fingerprinting activo.

a) Fingerprinting activo

Sucede generalmente cuando el atacante realiza alguna acción con la finalidad de obtener alguna respuesta de la víctima a través del envío de paquetes que le permiten obtener información, Algunas herramientas utilizadas son: RINGv2, Xprobe2, Nmap.

b) Fingerprinting pasivo

En este caso los paquetes a analizar se obtienen directamente de la red local, por lo que el atacante no genera ningún tipo de comunicación hacia el destino con el fin de provocar una respuesta, el atacante pasa inadvertido generalmente por medio de sniffers – analizadores de tráfico, por lo que el atacante necesita colocar su tarjeta de red en modo promiscuo y analizar totalmente el tráfico de la red, por ejemplo la herramienta *Nmap* con la *opción –O* muestra puertos abiertos y el tipo del sistema operativo que se está utilizando.

5. DoS

Una variante de este tipo de ataques es el ataque de denegación de servicios distribuido DDoS, (Distributed denial-of-service attacks –Denegación de Servicios Distribuido), es aquél donde un conjunto de sistemas previamente comprometidos realiza un ataque de denegación de servicios sincronizado a un mismo objetivo, al unir los recursos de todos los sistemas comprometidos saturan al equipo que se desea comprometer.

Este tipo de ataques está relacionado con los zombies o bots, que son equipos que pueden ser controlados de una manera centralizada para cualquier uso, los DDoS constan de 3 partes.

- Master – Maestro.
- Slave/secundary victim/agent/bot/botnet – Esclavo/víctima secundaria/agente/robot/robot.
- Victim/ primary victim – Víctima / víctima principal.

El *maestro* es quien ejecuta el ataque, el *esclavo* quien recibe órdenes del maestro y la *víctima* que es el sistema a comprometer.

Existe una clasificación de este tipo de ataques entre los que se encuentran:

- Buffer overflow (Saturación de la memoria RAM).
- SYN Attack, SYN flooding (Saturación por medio de solicitud de conexiones TCP).
- Smurf (Envío de muchos paquetes ICMP (ping) broadcast).

Algunas herramientas utilizadas para provocar DoS son Ping de la muerte, SSPing, CPU Hog, WinNuke, Jolt2, Bubonic, en el caso de DDoS se tienen Trinoo, Shaft, Tribal Flood Network (TFN), Stacheldraht y Mstream.

Algunas de las contramedidas utilizadas para prevenir, detectar o parar DoS, DDoS son las siguientes:

- Establecer cuotas de almacenamiento, memoria y uso de procesador en los equipos.
- Filtrar los servicios que ingresan a la red que pare o baje el flujo de paquetes que ingresan a la red con direcciones falsas o suplantadas desde Internet.
- Limitar la tasa de transferencia en la red.
- Sistemas detectores de intrusos (IDS).
- Herramientas de auditoría de host y red, las cuales buscan e intentan detectar herramientas conocidas de DDoS corriendo en el host o en la red, como *Find-ddos y Zombie zapper*.
- Herramientas de seguimiento de paquetes que se envían en la red con direcciones suplantadas.

Los ataques causados por DoS o DDoS son los más difíciles de proteger ya que en ocasiones muchos de éstos tienen que ver de manera inicial con seguridad lógica y física, la infraestructura con la que cuenta la organización y sus limitantes, proveedores que brindan algún servicio los cuales también pueden comprometerse.

6. Envenenamiento ARP

Empleado como base para ataques de hombre en el medio, algunas herramientas utilizadas para llevar este tipo de ataques son:

- Cain&Abel.
- Dsniff, arp-sk.
- Arp-tool arpoison. Ettercap.

8. Phishing[44]

Al igual que en el mundo físico, los estafadores continúan desarrollando nuevas y más siniestras formas de engañar a través de Internet. Si se siguen estos cinco sencillos pasos podrá protegerse y preservar la privacidad de la información.

- Nunca responder a solicitudes de información personal a través del correo electrónico. Si se tiene alguna duda, ponerse en contacto con la entidad que supuestamente ha enviado el mensaje.
- Para visitar sitios Web, introducir la dirección URL en la barra de direcciones.
- Asegurarse de que el sitio Web utiliza cifrado (figura B.2).
- Consultar frecuentemente los saldos bancarios y de las tarjetas de crédito.
- Comunicar los posibles delitos relacionados con la información personal a las autoridades competentes.
- Buscar que las instituciones que brindan algún servicio manejen autenticación de 2 factores como contraseña y OTP (One Time Password –Contraseña de una sola vez).
- Si se posee un poco de conocimiento técnico se recomienda verificar el archivo host, el cual contiene información de los DNS con la finalidad de verificar la integridad.

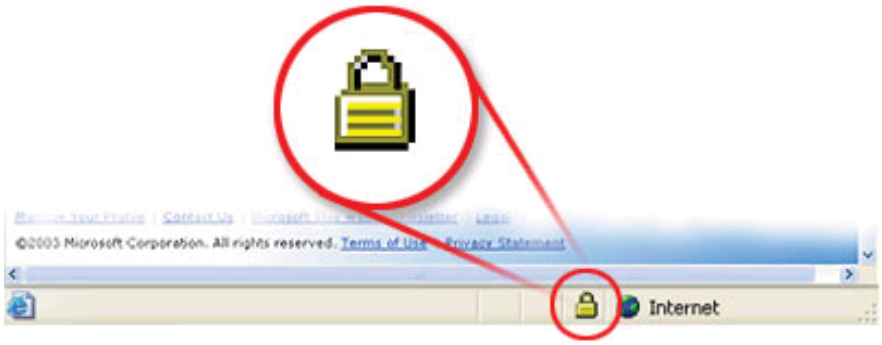

Figura B. 2 Símbolo de cifrado en sitios Web, protección contra phishing.

Actualmente se han tomado medidas para evitar este tipo de problemática, principalmente instituciones en las que su principal activo es proteger el interés de sus clientes como lo son los

[44] http://www.microsoft.com/latam/seguridad/hogar/spam/phishing.mspx

bancos. Por ejemplo, un método utilizado para entrar a las páginas Web de los diferentes bancos de algunos países, es usando el generador de claves dinámicas de las compañías Secure Computing y el RSA SecureID, con lo que se espera disminuir el phishing.

9. Botnet

Un bot – robot/esclavo/agente es un tipo de software automatizado diseñado para actuar en red, por sí solo es un programa capaz de auto replicarse y comportarse de manera inteligente, los cuales son utilizados para enviar correos no deseados (Spam), DDoS, además también pueden ser utilizados como herramientas para realizar ataques de manera remota, algunos de estos tipos de bots se comunican con otros usuarios a través de Internet haciendo uso de mensajería instantánea (IRC-Comunicación en tiempo real basada en texto) o cualquier otro tipo de interfaz basada en web.

Una botnet es un conjunto de equipos comprometidos y controlados por un equipo maestro que actúan en conjunto para lograr su objetivo, se vuelven una herramienta muy peligrosa, son utilizadas para generar correos no deseados y cualquier tipo de fraude, logrando con ello ataques de denegación distribuida.

Una manera de evitar este tipo de ataque es tener habilitado sólo lo necesario en un equipo, es decir, cancelar servicios que no son esenciales, los administradores de la red pueden hacerlo utilizando programas de monitoreo de red para poder detectar alguna anomalía como aumento en el tráfico de red, intermitencia entre otras.

Otra forma de evitar en mayor medida este tipo de ataques es a través de la educación de los usuarios, proporcionando información acerca de este tipo de ataques.

12. SQL injection

Cuando un intruso desea realizar ataques de este tipo, previamente como en cualquier otro ataque, se determina cuál es la configuración y las relaciones de las tablas, vulnerabilidades de las variables, etcétera, los pasos que comúnmente se siguen para determinar las vulnerabilidades del servidor SQL son los siguientes:

- Con ayuda de cualquier navegador se ubican sitios en los que es necesario autenticarse para determinar las posibles vulnerabilidades.
- Utilizar diferentes niveles de usuario y controles de acceso.
- Hacer uso de los comandos *Grant* (dar privilegio a cierta instrucción), *Revoke* (quitar permisos a ciertos recursos).
- Se realizan pruebas para determinar si existe la posibilidad de generar un error a través de consultas y con ello obtener algún dato que pudiera ser de utilidad.
- Se pueden intentar inserciones con el uso del comando *insert* o intentar listar los contenidos de las tablas de la base.

Algunas de las recomendaciones para evitar este tipo de ataques es administrar de manera adecuada la base de datos, por ejemplo, restringir privilegios en la conexión a las bases, utilizar contraseñas robustas, limitar la información que da por *default* el servidor de la base de datos, además de una revisión de los códigos de programación que no permita elaborar consultas.

Actualmente el comercio electrónico es de gran importancia para muchas empresas por lo que el diseño de sitios que eviten este tipo de ataques es primordial, además de otras medidas como el tipo de sistema operativo a utilizar, tecnología, tipo de servidor WEB, ubicación física etcétera.

13. Backdoors

Detectar puertas traseras no es una tarea fácil, pero no imposible, una forma para detectar si algún equipo tiene una puerta trasera generalmente es la adición de un nuevo servicio en los sistemas operativos Windows pues éste podría estar ocultando alguna puerta trasera.

Antes de que un intruso deje una puerta trasera realiza un proceso de análisis como servicios utilizados, puertos abiertos, aplicaciones que nunca se utilizan, pero que están activadas, todo ello con la finalidad de poder hacer uso de ellas y pasar desapercibido, por lo que se vuelve importante contar con una bitácora de servicios instalados, puertos abiertos y eliminar servicios innecesarios para evitar este tipo de ataques.

A pesar de que es una técnica sencilla es muy eficiente ya que el atacante puede ingresar al sistema con privilegios que le permitan obtener o hacerse de una cuenta del sistema para obtener beneficios.

Los RATs(Remote Administration Trojans – Troyanos administrables remotamente), son un ejemplo claro de puertas traseras, son utilizadas para tener el control de un equipo comprometido de manera remota. Cuando un usuario hace uso de su equipo, aparentemente funciona de manera normal pero al mismo tiempo se ejecutan procesos que abren puertos en el equipo víctima lo que permite al atacante estar en contacto con ella.

Este tipo de puertas traseras se compone de dos archivos, uno que se ejecuta del lado del equipo víctima que funciona como servidor y el otro del lado atacante que funciona como cliente, el cual permite al intruso tener el control.

14. Rootkits

Una clasificación muy generalizada es la siguiente:

a) Kits binarios: alcanzan su meta sustituyendo ciertos archivos del sistema por los troyanizados.

b) Kits del núcleo: utilizan los componentes del núcleo (también llamados módulos) que son reemplazados por troyanos.

c) Kits de librerías: emplean librerías del sistema para contener troyanos.

Entre las medidas que se deben tomar para evitar algún tipo de daño, primeramente si ya no se tiene la seguridad de que el equipo no está comprometido, lo recomendable es realizar un respaldo de la información importante y reinstalar los sistemas, por otro lado, si se cuenta con un respaldo del sistema no se recomienda hacer uso de él si no se está completamente seguro de la fecha en que el equipo fue comprometido.

Otra manera es verificando la integridad de los archivos a través de firmas digitales como MD5, además de utilizar aplicaciones que cifren las comunicaciones como SSH, SSL para evadir los ataque por análisis de trafico de red.

15. Footprinting

Obtener información implica todo un proceso por lo que se deben seguir cierto número de pasos lógicos, footprinting es una parte esencial de dicho proceso, catalogado como un proceso esencial. Generalmente la parte de recolección de información utiliza un 90 % del total de tiempo invertido en un ataque.

Existen distintas formas para obtener dicha información, entre ellas se encuentran:

Whois, Nslookup, Sam spade, traceroute, páginas web de la organización que brinde información de los empleados, estas herramientas permiten obtener información acerca de la red, el servidor de dominio, nombre del equipo e información que en algún momento pudiera llegar a ser de utilidad.

16. Escaneos

Los escaneos se pueden clasificar de la siguiente manera de acuerdo con el tipo de información que éstos devuelven.

a) Escaneo de puertos

Se obtiene información acerca de los puertos abiertos y los servicios, durante este proceso se permiten identificar los puertos TCP/IP disponibles, las herramientas utilizadas para el escaneo de puertos como NMAP permite conocer los puertos abiertos y el tipo de servicios asociados a ellos, como por ejemplo los puertos bien conocidos: 80 utilizado por los servidores WEB, SSH (22), FTP (21), TELNET (23), HTTPS (443), herramientas como HPING permiten realizar escaneo, alteración de paquetes e incluso se pude indicar un rango de puertos a escanear.

b) Escaneo de la Red

Permite obtener direcciones IP de una red de los equipos activos, los hosts son identificados individualmente por su dirección IP, los escáneres de redes permiten identificar los equipos que se encuentran activos.

c) Escaneo de vulnerabilidades

Permite obtener información acerca de algunas debilidades conocidas, cuando se realiza un escaneo de este tipo lo primero que se identifica es el tipo de sistema operativo, versión, así como actualizaciones para identificar las debilidades que en un futuro pueden ser explotadas por el intruso, haciendo uso de exploits adecuados para el tipo de debilidad encontrado.

El escaneo de la red y de vulnerabilidades puede ser detectado a través de la implementación de un IDS ya que las herramientas que se utilizan interactúan con la tarjeta de red generando de esta forma tráfico que puede ser detectado con la implementación de un mecanismo de seguridad adecuado.

El escaneo implica una metodología a seguir según Certified Ethical Hacker, incluye los siguientes pasos.

1. Verificar sistemas activos.
2. Verificar puertos abiertos.
3. Identificar servicios.
4. Determinar el sistema operativo utilizado.
5. Escanear vulnerabilidades.
6. Realizar diagrama de red y las vulnerabilidades de los equipos.
7. Preparar proxies (medio por el cual se planea ingresar al objetivo).
8. Atacar.

La aplicación por excelencia para realizar exploración de puertos es *Nmap* (*Network Mapper*), esta herramienta implementa la gran mayoría de las técnicas conocidas para la exploración de puertos y permite descubrir información de los servicios y sistemas encontrados. *Nmap* también implementa un gran número de técnicas de reconocimiento.[45]

Mediante *Nmap* pueden realizarse, por ejemplo, las siguientes acciones de exploración:

a) Descubrimiento de direcciones IP activas mediante una exploración de la red
.nmap -sP IP ADDRESS/NETMASK

b) Exploración de puertos TCP activos.
.nmap -sT IP ADDRESS/NETMASK

c) Exploración de puertos UDP activos.
.nmap -sU IP ADDRESS/NETMASK

d) Exploración del tipo de sistema operativo de un equipo en red.
.nmap -O IP ADDRESS/NETMASK

[45] Jordi Herrera, Joan Comartí. Aspectos avanzados de seguridad en redes, pág 28, Software Libre.