# Network Scanning

## Introducción

Es una de las fases más importantes de obtención de información para un hacker. En este proceso, el hacker intenta obtener información acerca de direcciones ip’s, el sistema operativo, arquitectura del sistema y servicios corriendo en cada computador

## Objetivos

* Detectar sistemas “vivos” en la red.
* Descubrir servicios que se están ejecutando o que están escuchando en los sistemas objetivos.
* Entender las técnicas de escaneado de puertos
* Identificar servicios TCP y UDP ejecutándose en la red objetivo
* Descubrir los sistemas operativos que hay.
* Herramientas de descubrimiento automáticas.

## Tipos de escaneo

* Escaneo de puertos: Consiste en comprobar los servicios corriendo en el objetivo, enviando una secuencia de mensajes en un intento de entrar.
* Escaneo de red: Consiste en identificar host activos en la red.
* Escaneo de vulnerabilidades: Es un método automático usado para identificar las vulnerabilidades presentes en el sistema y la red

## Metodología

### Escaneo de red

El primer paso que se debe seguir es el identificar si es que existe algún sistema activo en la red objetivo, para lo cual se utiliza el ICMP (Protocolo de Mensajes de Control de Internet) scanning.

Este método consiste en enviar un ping (ICMP echo request) al host objetivo, si el objetivo esta “vivo” retornara un mensaje ICMP ECHO reply.

Este primer paso también sirve para identificar algún otro dispositivo activo o para determinar si el ICMP está pasando a través de algún firewall.

Otro método que también es útil para esta tarea es el ping sweet, también conocido como barrido de ping, es usado para determinar los hosts activos de un rango de direcciones ip enviando ICMP ECHO request a múltiples hosts. Si el host está activo entonces retornara un ICMP ECHO reply lo que implica que esta online y se lo considera un posible objetivo de ataque. Los atacantes suelen usar esta técnica para elaborar un mapa de los sistemas que están activos en una determinada red.

Por otra parte, si bien ping sweet es considera la técnica más sencilla, a la vez puede ser poco efectiva, ya que es simple de bloquear por Firewalls (de red y de aplicación) y proxies.

A sí mismo, la mayoría de los IDS/IPS detectan y alertan al administrador de seguridad de la presencia de ping sweet en la red.

Algunas herramientas que se puede utilizar para esta tarea son:

* Angry IP Scanner
* SolarWinds Enginerr’s Toolset
* Nmap

### Escaneo de puertos

El siguiente paso es identificar los puertos que estén abiertos es un sistema, lo cual implica testear cada puerto de cada host para determinar cuáles están abiertos.

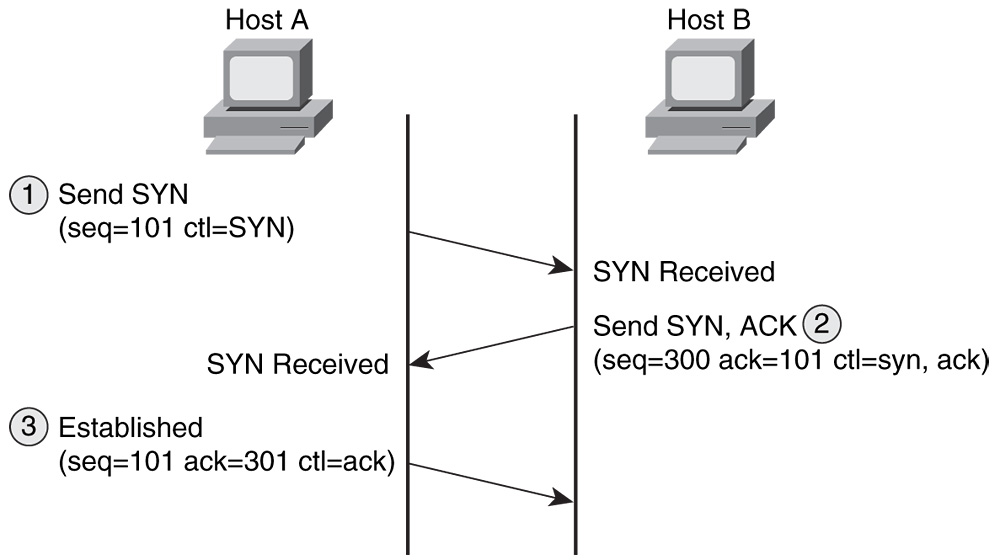
A partir de la identificación de los puertos abiertos, como regla general, un hacker puede identificar los servicios asociados a cada puerto.

Para entender esta técnica conviene antes recordar cómo se realiza la comunicación en TCP.

La comunicación en TCP está controlada por banderas en el encabezado TCP

* SYS: Es usada para inicializar una conexión entre host
* ACK: Es usada para confirmar la recepción de un paquete
* PSH: Indica que los datos de un segmento y los datos que hayan sido almacenado anteriormente en el buffer del receptor deben ser transferidos a la aplicación receptora lo antes posible.
* URG: Indica que los datos contenidos en un paquete debe ser procesados inmediatamente.
* FIN: Indica al sistema remoto que no habrá más trasmisiones.
* RST: Se usa para resetear una conexión.

TCP usa el Three-Way Handshake para establecer una conexión entre el cliente y un servidor.



Los métodos utilizados para escanear los puertos de una red son los siguientes:

* Half Open Scan (Stealth Scan): Se llama así porque este escaneo no abre una conexión TCP full, por lo que es utilizado por los atacantes para “bypassear” reglas de firewall o mecanismo de login.



* SYN/ACK: Se envía un paquete con las banderas SYN/ACK a un puerto cerrado el cual responderá con un RST



* XMAS Scan: Es una técnica que envía todas las banderas en el paquete, cuando un mensaje es enviado a un puerto cerrado, el puerto responde con RTS, indicando que está cerrado



* FIN Scan: Se envía un paquete con la bandera FIN a un puerto cerrado el cual responderá con un RST



* Este escaneo explota las vulnerabilidades de los sistemas operativos basados en BSD
* No trabaja con sistemas operativos Windows ya que muestra como que todos los puertos están cerrados
* ACK Scan: Esta técnica no proporciona puertos abiertos, solo es para mapear reglas de filtrado de un firewall. Nos puede ayudar a determinar si el firewall actúa simplemente como un filtro para permitir conexiones o usa un sistema avanzado de filtrado de paquetes.



* NULL Scan: Es una técnica que apaga todas las banderas en el paquete, este asume que cada puerto cerrado envía un RST.



* Evita IDS y TCP three handshake
* Trabaja solo para sistemas Unix
* No trabaja con sistemas operativos Windows, muestra como que todos los puertos están cerrados.
* IDLE Scan: En este escaneo los paquetes no se originan con la IP del hacker sino a través de una IP Spoofed, este escaneo se lo llama zombie, si el puerto está cerrado el equipo zombie (IP spoof) responderá con un RST.



Usualmente cuando se realiza un escaneo de puertos, no solo se quiere saber si una maquina esta online o que puertos están abiertos también es necesario saber qué sistema está detrás de la maquina objetivo para lo cual se utiliza una técnica conocida como OS Fingerprinting.

Algunas herramientas que se pueden utilizar para esta tarea son:

* Nmap
* NetScan Tools Pro
* Hping2
* Firewalk
* Komodia’s PacketCrafter

## Contramedidas

Respecto al escaneo de puertos, las contramedidas a tomar son procesos o herramientas que los administradores de seguridad configuran para detectar posibles intentos de escaneos en sus redes.

Algunas de las contramedidas necesarias para prevenir que un atacante obtenga información de la red son las siguientes:

* Implementar una arquitectura de seguridad apropiada, que contenga firewall o distintos niveles e IDS.
* El firewall debe trabajar en modo stafull, es decir, debe permitir analizar los datos dentro de los paquetes y no solo las cabezaras TCP.
* Los sistemas NIDS, se utilizan entre otras cosas para identificar métodos de detección de sistemas operativos llevados a cabo por distintas herramientas.
* El IDS debe ser habilitado para analizar los paquetes y determinar si es un escaneo de puertos y no se basa en las reglas del firewall
* Solamente se deben tener abiertos los puertos que se van a utilizar. El resto, deberían estar cerrados o filtrados.
* Los empleados de la organización, deben estar correctamente concientizados respecto a la seguridad y también estar al tanto de las distintas políticas que deben seguir.

## Banner Grabbing

Esta es una técnica, que consiste en capturar los banners que muestran las aplicaciones al realizarse una conexión, de esta manera se podrá obtener información como el tipo de software, la versión y el sistema operativo.

Este paso de torna de vital importancia cuando se intenta buscar vulnerabilidades en un sistema.

Como parte de esta técnica también se encuentra otro proceso denominado OS Fingerprinting

El OS Fingerprinting es una técnica que consiste en analizar las huellas que deja un sistema operativo en sus conexiones de red.

Está basada en los tiempos de respuesta a los diferentes paquetes, al establecer una conexión en el protocolo TCP/IP, que utilizan los diferentes sistemas operativos. Puede ser de tipo activo o pasivo

* Activo: En un escáner activo la herramienta envía paquetes esperando una respuesta del sistema operativo y la compara con su base de datos. Este método tiene como inconveniente que es fácil de detectar.
* Pasivo: Es un escáner pasivo la herramienta escucha el tráfico para identificar las máquinas que actúan en la red comparando sus tempos de respuesta pero sin actuar en la red. Es un técnica más difícil de detectar pero tiene dos inconvenientes ya que algunas veces hay que esperar mucho tiempo si el sistema se quiere identificar no envía paquetes, no se puede identificar y al no enviar peticiones la herramienta no se generara respuestas limitando su acción al ámbito de broadcast, aunque se puede solucionar con técnicas de envenenamiento de la cache ARP.

### Herramientas

Algunas de las herramientas que se dispone para realizar este proceso son:

* Telnet
* ID Serve
* Netcraft
* Satori

### Contramedidas

Para evitar que un atacante obtenga información de las aplicaciones que corren en una red se suele seguir las siguientes indicaciones:

* Para usuarios de IIS (Internet Information Services) se pueden utilizar herramientas como IIS Lockdown Tool o ServerMask
* Para usuarios de Apache 2.x se debe modificar el módulo *mod\_headers,*que se encuentra en el archivo de configuración httpd.conf, cambiando la información del banner en *Header set Server “New Server Name”.*

También conviene cambiar la firma del servidor en la línea *ServerSignature Off* en el archivo de configuración httpd.conf

* Otra buena práctica consiste en esconder las extensiones de los archivos.

Para el servidor apache se usa las directivas del *mod\_negotiation.*

Los usuarios de IIS pueden usar herramientas como PageXchanger.

## Escaneo de vulnerabilidades

Una vez identificado los servicios que corren en cada puerto, la versión de cada una de las aplicaciones y el sistema operativo que utiliza la red objetivo del análisis, se deben buscar las vulnerabilidades de los puntos mencionados anteriormente.

Para esta tarea se puede utilizar herramientas como Nessus, SAINT, OpenVAS, entre otras.

Dichas vulnerabilidades se encuentran citadas por lo general en la base de datos de SANS u OSVDB.

Otro punto importante es analizar las posibles vulnerabilidades de una aplicación web.

Para este proceso se debe hacer uso de la información obtenida en la fase de footprinting, ya que en esta fase es donde el atacante descubrirá las posibles aplicaciones web asociadas a su objetivo.

Para realizar el análisis de las aplicaciones web es recomendable basarse en la guía de pruebas de OWASP V3 y prestar al OWASP top 10 en donde se muestran las 10 principales vulnerabilidades que sufren las aplicaciones web.

Algunas de las vulnerabilidades más importantes son:

* **Cross Site Scripting:** La vulnerabilidad de Cross Site Scripting, conocida de forma acortada como XSS, supone una serie de riesgos en todas sus variantes, las cuales pueden dañar principalmente al usuario y a la reputación del dominio y/o empresa afectada.

Entre otras cosas, es posible:

* Realizar ataques de navegación dirigida
* Ataques de *phising*
* Distribución de *malware*
* Robo de credenciales
* Ejecución de *script “JavaScript”*
* *Click Hijacking*
* *Defacement* sin o con la alteración de la página real

Este tipo de vulnerabilidad, puede conllevar a muchos y nuevos ataques web, debido a que un control de ejecución JavaScript sobre el navegador de una víctima, abre vectores de ataques como Man In The Browser “MITB”, pudiendo tomar un control remoto del navegador, y pudiendo realizar ejecuciones de exploits con el objetivo de realizar una escala de privilegios en el sistema. En otros casos, prima la ingeniería social y la común falta de conocimientos del usuario afectado, al caer en una página fraudulenta.

Básicamente se pueden diferenciar dos tipos de Cross Site Scripting: Cross Site Scripting Reflejado, y Cross Site Scripting Persistente.

* **SQL Injection:** Las vulnerabilidades de SQL Injection, afectan a todas las aplicaciones web que rescatan información de una base de datos mediante parámetros mal filtrados. Estas técnicas de inyección, afectan a todo tipo de bases de datos, como Microsoft SQL Server, MySQL, Microsoft Access, Oracle, PostgreSQL o Sybase entre las más comunes.

Las bases de datos MySQL al ser las más utilizadas, han ido recolectando diferentes técnicas de ataque como las conocidas Blind, inyecciones basadas en aritmética, en tiempo de respuesta o en errores.

Para llevar a cabo este tipo de inyecciones, es conocida la inclusión de una comilla simple en los parámetros a recoger, con el objetivo de forzar un error de sintaxis SQL, y provocar así que la página devuelva algún tipo de error en pantalla. Como la mayoría de los servidores tienen la opción de display\_error habilitada, otras técnicas como comparaciones matemáticas “and 1=1” y el esperado cambio de HTML de la página devuelva con “and 1=2”, posibilitan la oportunidad de detectar un SQL Injection sin apenas dificultad.

* **Local File Include/Path Transversal**: Esta vulnerabilidad permite la inclusión de ficheros locales, desde una aplicación que maneje archivos mediante un parámetro sin filtrar. Además en algunos casos, es posible la ejecución de código remoto incluyéndolo en las cabeceras de una petición HTTP, que más tarde será interpretado al incluir los ficheros de log en la página vulnerable a LFI.
* **Remote File Include**: Esta técnica permite la inclusión de ficheros desde páginas externas. Se deben cumplir varios requisitos para la explotación de la vulnerabilidad, entre otras cosas son importantes las versiones de PHP y su mala configuración en el caso de permitir inclusiones de ficheros externos.

De las misma manera que LFI, esta vulnerabilidad en PHP es explotable desde funciones como include, include\_once, requiere, requiere\_once.

Algunas herramientas que son válidas para estos análisis son las siguientes:

* Burp Suite
* Paros
* ProxyStrike
* Vega
* WebScarab
* Zaproxy

## Proxy

El proxy es una PC que puede actuar como intermediara entre el hacker y el objetivo. Permite al hacker estar anónimo en la red, ya que crea una conexión con el proxy y este le sirve como zombie para atacar al objetivo en la red, un claro ejemplo es una Botnet.



Una de las herramientas que le permite al hacker un total anonimato durante su ataque es TOR (The Onion Routing).

Otra técnica usada por los hackers es la de Tunneling HTTP, que se basa en hacer un bypassing al firewall o IDS de un protocolo bloqueado (SMTP) por medio de un túnel a través de un protocolo permitido (HTTP). Casi todos los IDS y firewall actúan como un proxy entre el cliente y el internet y dejan pasar solo el tráfico definido.

El IP Spoofing es otra técnica conocida a través de la cual se sustituye la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.