# 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.

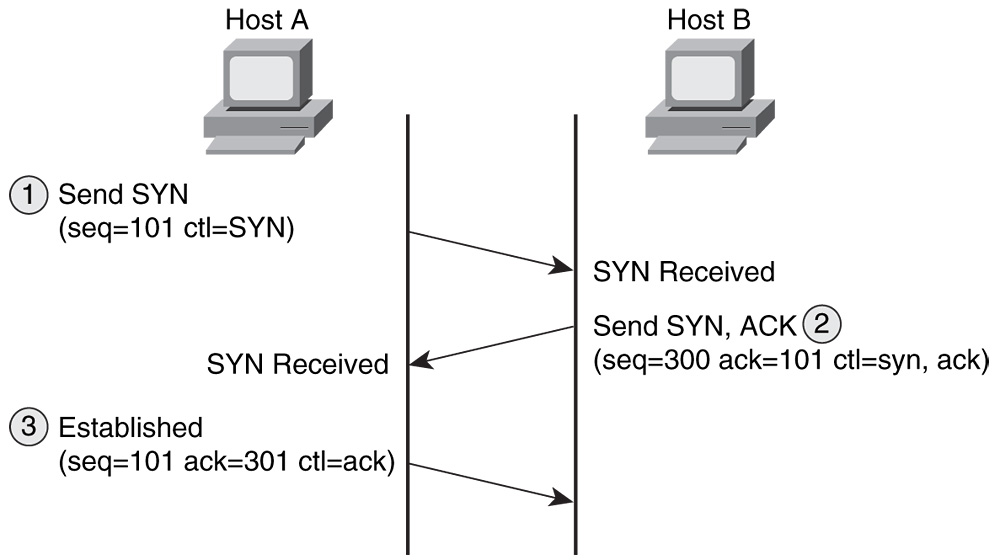
A partir de la identificación de los puertos abiertos, como regla general, un hacker puede identificar los servicios asociados a cada puerto.

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.

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.