Esta herramienta sirve para detectar los ordenadores objetivo.

Si estamos en una red privada, debemos saber que equipos están dentro de esa red.

Debemos saber que puertos tiene abiertos ese ordenador y que servicios corren en esos puertos.

Lo primero que debemos conocer es nuestra IP.

──(kali㉿kali)-[~/Desktop]

└─$ ifconfig

Nos muestra algo asi:

┌──(root㉿kali)-[/home/kali]

└─# ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fe80::de00:157c:b270:eb7c prefixlen 64 scopeid 0x20<link>

inet6 2800:e2:837f:fbe5:8647:5be2:5301:1806 prefixlen 64 scopeid 0x0<global>

ether 08:00:27:d2:26:79 txqueuelen 1000 (Ethernet)

RX packets 438 bytes 59495 (58.1 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 638 bytes 74328 (72.5 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 8 bytes 480 (480.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 8 bytes 480 (480.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Despues debemos seguir dos pasos:

1. Encontrar los dispositivos que esten ubicados en nuestra red.
2. Lanzar un escaneo a uno de ellos

Escaneo de toda la red.

Debemos poner nuestra IP , y omitimos el ultimo numero y agregregamos .0/24

┌──(root㉿kali)-[/home/kali]

└─# nmap -O 192.168.1.0/24

El comando `nmap -O 192.168.1.0/24` se utiliza para realizar un escaneo de red con Nmap, una herramienta popular para el análisis de redes y la seguridad informática. Aquí hay una explicación detallada de los componentes del comando:

1. \*\*nmap\*\*: Este es el comando que invoca Nmap, la herramienta de análisis de redes.

2. \*\*-O\*\*: Esta opción le dice a Nmap que intente determinar el sistema operativo (OS) de los dispositivos en la red. Nmap usa una técnica llamada "OS fingerprinting" para adivinar el sistema operativo basado en las respuestas de la red a ciertos paquetes.

3. \*\*192.168.1.0/24\*\*: Este es el rango de direcciones IP que se va a escanear. El sufijo `/24` indica una máscara de subred de 24 bits, lo que significa que el escaneo cubrirá todas las direcciones IP desde `192.168.1.0` hasta `192.168.1.255` (un total de 256 direcciones IP).

En conjunto, el comando `nmap -O 192.168.1.0/24` escanea todas las direcciones IP dentro del rango `192.168.1.0` a `192.168.1.255` e intenta identificar el sistema operativo de cada dispositivo en esa red.

Aquí tienes un desglose paso a paso del comando:

1. \*\*Ejecución del comando Nmap\*\*:

- Nmap se inicia con el comando `nmap`.

2. \*\*Detección del sistema operativo\*\*:

- La opción `-O` habilita la detección del sistema operativo, lo que permite a Nmap intentar identificar el sistema operativo de los hosts escaneados.

3. \*\*Especificación del rango de IP\*\*:

- El rango de direcciones IP `192.168.1.0/24` indica que Nmap escaneará todas las direcciones IP en la subred especificada.

En resumen, este comando es útil para obtener información detallada sobre los dispositivos en una red local, incluyendo qué sistemas operativos están utilizando, lo que puede ser útil para tareas de administración de red, auditorías de seguridad y detección de dispositivos no autorizados en la red.

Ahora ejecutamos el segundo paso, después de identificar nuestro objetivo, lanzamos un escaneo dirigido a la maquina metasploitable.

┌──(root㉿kali)-[/home/kali]

└─# nmap -p- -sV -sC --open -sS -vvv -n -Pn 192.168.1.9

El comando `nmap -p- -sV -sC --open -sS -vvv -n -Pn 192.168.1.9 -oN escaneo`

es un comando complejo que realiza un escaneo profundo y detallado de un host específico en la red (en este caso, `192.168.1.10`). Aquí hay una explicación detallada de cada uno de los componentes del comando:

1. \*\*nmap\*\*: Este es el comando que invoca Nmap, la herramienta de análisis de redes.

2. \*\*-p-\*\*: Este parámetro indica a Nmap que escanee todos los puertos, desde el 1 hasta el 65535. Es un escaneo completo de puertos.

3. - \*\*-sV\*\*: Este parámetro le dice a Nmap que detecte versiones de servicios. Nmap intentará determinar qué servicio y versión está corriendo en cada puerto abierto.

- \*\*-sC\*\*: Este parámetro le dice a Nmap que use scripts NSE (Nmap Scripting Engine) por defecto. Estos scripts pueden realizar una variedad de funciones, como detección de servicios, enumeración de información adicional y pruebas de vulnerabilidad.

4. \*\*--open\*\*: Este parámetro le dice a Nmap que solo muestre los puertos que están abiertos. Los puertos cerrados y filtrados no se mostrarán en la salida del escaneo.

5. \*\*-sS\*\*: Este parámetro especifica un escaneo SYN (también conocido como "escaneo sigiloso" o "escaneo medio abierto"). Es el tipo de escaneo de puertos más común y rápido. Envia un paquete SYN y espera una respuesta para determinar el estado del puerto (abierto, cerrado o filtrado).

6. \*\*-vvv\*\*: Este parámetro incrementa la verbosidad del escaneo. Cuantos más "v" se añadan, más detallada será la salida del escaneo. `-vvv` proporciona un nivel de detalle muy alto en la salida.

7. \*\*-n\*\*: Este parámetro le dice a Nmap que no realice la resolución de nombres DNS. Es decir, Nmap no intentará convertir las direcciones IP en nombres de dominio, lo que puede hacer que el escaneo sea más rápido.

8. \*\*-Pn\*\*: Este parámetro le dice a Nmap que no realice un "ping" previo para verificar si el host está activo. Normalmente, Nmap envía un "ping" a una dirección IP para ver si responde antes de iniciar el escaneo. Con `-Pn`, Nmap asume que el host está activo y procede directamente con el escaneo.

9. **-oN escaneo**: Guarda la salida del escaneo en un archivo llamado escaneo en formato normal (normal output format).

10. \*\*192.168.1.9\*\*: Esta es la dirección IP del host que se va a escanear. Este es un entorno seguro es la IP de nuestra maquina metasploitable

En conjunto, el comando `nmap -p- -sV -sC --open -sS -vvv -n -Pn 192.168.1.9` realiza un escaneo detallado de todos los puertos en el host `192.168.1.9`, detectando versiones de servicios y usando scripts por defecto, solo mostrando puertos abiertos, usando un escaneo SYN, proporcionando salida muy detallada, sin resolución de DNS y sin hacer ping antes del escaneo. Este comando es útil para una evaluación profunda de la seguridad y el estado de los servicios en un host específico.

Ahora ese reporte lo guardamos en un archivo que se llama escaneo

Y podemos acceder a el de esta manera:

Como lo guardamos en el escritorio , navegamos hacia el.

┌──(root㉿kali)-[/home/kali]

└─# cd Desktop

Hacemos un, ls para ver los archivos que tenemos en en el escritorio

┌──(root㉿kali)-[/home/kali]

└─# ls

Se muestran los archivos:

┌──(root㉿kali)-[/home/kali/Desktop]

└─# ls

escaneo UnrealIRCd-3.2.8.1-Backdoor

Ahora para ingresar a ese archivo para ver el reporte:

┌──(root㉿kali)-[/home/kali/Desktop]

└─# cat escaneo