

NMAP en Kali Linux

Contexto:

El escenario se encuentra compuesto por un Cliente Windows 10 y un agente de amenaza Kali Linux.

Vamos a ejecutar los comandos básicos de nmap para escanear los puertos de Windows 10 (en este caso el Firewall de Windows se encuentra deshabilitado).

1. Descargamos una máquina virtual preparada para Virtual Box.
2. Validamos la versión de Nmap instalado

Comando: `nmap -V`

Resultado:

```
(kali@kali)-[~]  
$ nmap -V  
Nmap version 7.94SVN ( https://nmap.org )  
Platform: x86_64-pc-linux-gnu
```

3. Utilizamos el comando básico

Comando: `nmap <IP>`

Resultado: El host parece estar apagado. Recomienda utilizar “-Pn”

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-07 09:18 EDT  
Note: Host seems down. If it is really up, but blocking our ping probes, try  
-Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
```

Análisis: Esto pasa porque Windows tiene el Firewall activo y Nmap intenta realizar un ping y lo bloquea.

```
Host is up (0.00032s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
  
Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
```

Conclusión: Al utilizar “`nmap -Pn <IP>`” nos muestra los puertos, estado y servicios activos.

4. Escaneo de puertos específicos

Comando: `nmap -p 22,80,443 <IP>`

```
Host is up (0.00057s latency).  
  
PORT      STATE SERVICE  
22/tcp    closed ssh  
80/tcp    closed http  
443/tcp    closed https
```

Conclusión: Aquí deshabilitamos el Firewall de Windows para visualizar los puertos especificados.

Comando: `nmap -p 22,80,443,445 <IP>`

```
Host is up (0.00052s latency).  
  
PORT      STATE SERVICE  
22/tcp    closed ssh  
80/tcp    closed http  
443/tcp    closed https  
445/tcp    open  microsoft-ds
```

Conclusión: Aquí agregamos el puerto 445 para visualizar el estado “open”.

5. Detección de Sistema Operativo

Comando: `sudo nmap -O <IP>`

```
Host is up (0.0010s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
MAC Address: [REDACTED] (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Microsoft Windows 10
```

Conclusión: Al ejecutar el comando también se visualiza los puertos, MAC Address y el SO. que se encuentra iniciado en el Cliente.

6. Detección de versión de servicios

Comando: `nmap -sV <IP>`

```
Host is up (0.00066s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
135/tcp    open  msrpc        Microsoft Windows RPC  
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds?  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Conclusión: Agregamos “-sV” para visualizar la versión de los servicios. Esto implica más información para el agente de amenaza.