

FASE RACCOLTA INFORMAZIONI

Su questo esercizio vedremo diversi comandi su nmap e cosa accade quando lanciamo ognuno.

Per primo abbiamo `nmap -sn -PE <target>` dove questo comando permette di visualizzare ogni IP dentro ad una rete e riusciamo a vedere anche il loro indirizzo MAC e la rete e macchina usata

Dopo ho usato `nmap <target> --top-ports 10 --open` questo comando permette di vedere le porte più usate da una lista di service di nmap dalla quantità di porta che dai nel comando (10 nel caso).

Per ultimo ho usato `nmap <target> -p- -sV --reason --dns-server ns` dove mi permette di vedere la ragione della quale la porta che ho scelto di vedere è chiusa, aperta o filtrata.

`nmap -sn -PE <target>`:

```
nmap -sn -PE 192.168.1.179
```

Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
168.1.	<pre>nmap -sn -PE 192.168.1.179 Starting Nmap 7.92 (https://nmap.org) at 2024-02-20 15:22 UTC Nmap scan report for 192.168.1.179 Host is up (0.0014s latency). MAC Address: 08:00:27:A8:A0:9A (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds</pre>				

Su questo comando, riesco a vedere il mac address della macchina target (meta) e infatti nmap mi fa vedere anche le informazioni di rete e macchina da cui proviene questo ip.

nmap <target> --top-ports 10 -- open

```
nmap --open --top-ports 10 192.168.1.179
```

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

```
nmap --open --top-ports 10 192.168.1.179
```

Starting Nmap 7.92 (<https://nmap.org>) at 2024-02-20 15:27 UTC
Nmap scan report for 192.168.1.179
Host is up (0.0017s latency).
Not shown: 3 closed tcp ports (reset)

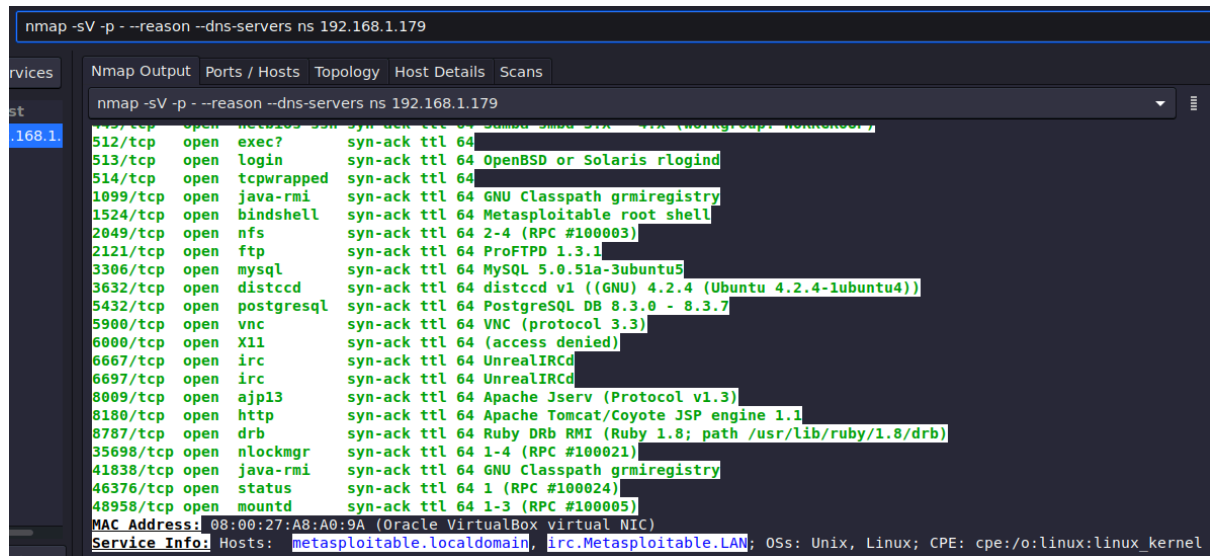
PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
80/tcp	open	http
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

MAC Address: 08:00:27:A8:A0:9A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

Con questo comando riesco a vedere quale porta è aperta, essendo esse quelle più utilizzate nella macchina target. Infatti nel range di 10 porte, 3 sono chiuse e nmap non mi fa vedere queste.

`nmap <target> -p- -sV --reason --dns-server ns:`



```
nmap -sV -p- --reason --dns-servers ns 192.168.1.179
```

Port	Protocol	State	Reason	Version
512	tcp	open	exec?	syn-ack ttl 64
513	tcp	open	login	syn-ack ttl 64
514	tcp	open	tcpwrapped	syn-ack ttl 64
1099	tcp	open	java-rmi	syn-ack ttl 64
1524	tcp	open	bindshell	syn-ack ttl 64
2049	tcp	open	nfs	syn-ack ttl 64
2121	tcp	open	ftp	syn-ack ttl 64
3306	tcp	open	mysql	syn-ack ttl 64
3632	tcp	open	distccd	syn-ack ttl 64
5432	tcp	open	postgresql	syn-ack ttl 64
5900	tcp	open	vnc	syn-ack ttl 64
6000	tcp	open	X11	syn-ack ttl 64
6667	tcp	open	irc	syn-ack ttl 64
6697	tcp	open	irc	syn-ack ttl 64
8009	tcp	open	ajp13	syn-ack ttl 64
8180	tcp	open	http	syn-ack ttl 64
8787	tcp	open	drb	syn-ack ttl 64
35698	tcp	open	nlockmgr	syn-ack ttl 64
41838	tcp	open	java-rmi	syn-ack ttl 64
46376	tcp	open	status	syn-ack ttl 64
48958	tcp	open	mountd	syn-ack ttl 64

MAC Address: 08:00:27:A8:A0:9A (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Questo comando mi fa vedere le porte aperte, la ragione del perché é aperta, e con questo comando riesco a vedere informazioni in più, come il nome del host e LAN, il sistema operativo e il dispositivo di rete utilizzato.

Con questi comandi sono riuscito a vedere tutte le porte aperte, con facile accesso per una invasione, quanti IP sono collegati a questa rete, il nome del server, il sistema operativo e altri.