Nmap

Nmap ”Network Mapper” è uno strumento open-source che permette la scansione della rete e l'identificazione dei dispositivi e dei servizi.

Le sue funzionalità principali includono:

- Scansione degli Host
- Identificazione dei Servizi:
- Rilevamento dei Sistemi Operativi
- Scansione delle Vulnerabilità

Traccia

Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target

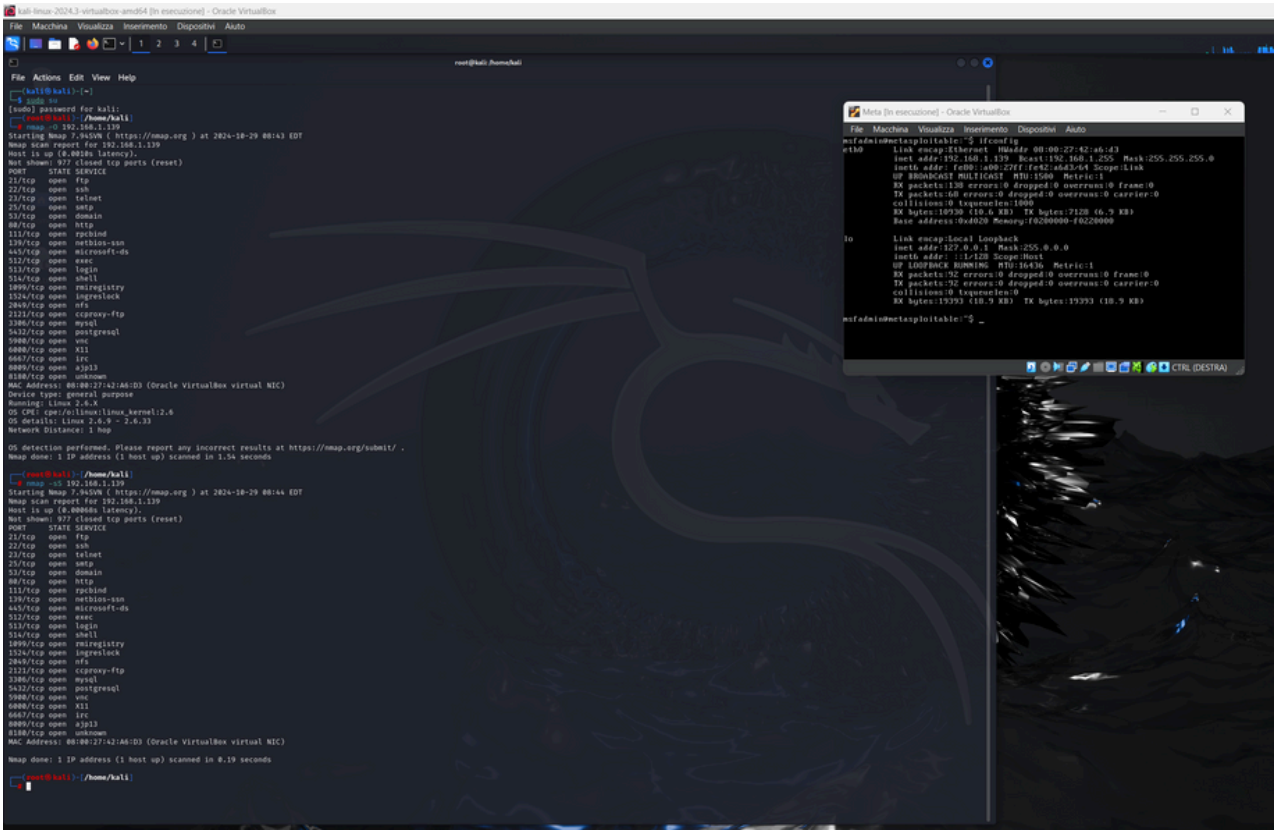
Metasploitable:

- OS fingerprint
- Syn Scan
- TCP connect
- Version detection

E la seguente sul target Windows:

- OS fingerprint

Esecuzione del Esercizio



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.139
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 08:45 EDT
Nmap scan report for 192.168.1.139
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:42:A6:D3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

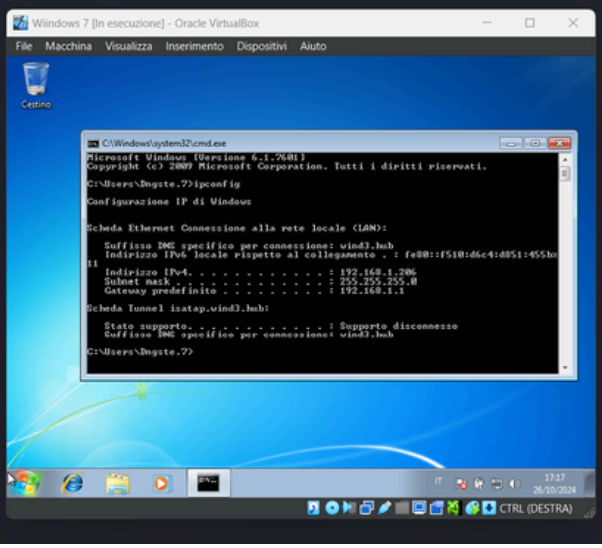
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.139
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 08:46 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:42:A6:D3 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.69 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.206
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 09:01 EDT
Nmap scan report for Dngste7.wind3.hub (192.168.1.206)
Host is up (0.00079s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:3F:F6:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```



Relazione

Per eseguire questo esercizio, ho utilizzato Kali, Metasploitable e Windows 7.

Metasploitable:

Ho iniziato inserendo il comando ifconfig su Metasploitable per ottenere l'indirizzo IP.
Ho poi aperto il prompt di Kali e sono entrato in modalità root.

Primo passaggio: Ho eseguito il comando nmap -O <IP> per identificare il sistema operativo di Metasploitable.

Secondo passaggio: Ho eseguito nmap -sS <IP>, che è utilizzato per identificare le porte aperte tramite una scansione SYN.

Terzo passaggio: Ho utilizzato nmap -sT <IP>, che invia pacchetti SYN e attende risposte SYN/ACK, per eseguire una scansione TCP di tipo "connect".

Ultimo passaggio: Ho utilizzato nmap -sV <IP>, che mi ha permesso di identificare la versione dei servizi in ascolto sulle porte aperte di un host.
Alla fine di ogni comando, ho inserito l'IP da controllare, che nel mio caso era 192.168.1.139.

Windows 7:

Per Windows 7, l'obiettivo era solo identificare il sistema operativo. Ho quindi eseguito il comando nmap -O <IP> seguito dall'indirizzo IP di Windows.
Questa serie di comandi mi ha permesso di mappare e analizzare le caratteristiche dei dispositivi nella rete.