•S5.L2

Traccia: Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

Utilizzo del comando nmap

L'esercizio di oggi ci chiede di utilizzare i vari comandi nmap.

Nmap è uno strumento potente per la mappatura di rete che utilizza pacchetti raw per eseguire scansioni precise e dettagliate.

I pacchetti raw sono dei pacchetti che possono essere manipolati, utilizzando quest'ultimi , Nmap ha il pieno controllo su tutti gli aspetti del pacchetto, inclusi i campi dell'intestazione IP, i campi TCP/UDP, e i dati del payload.

Noi oggi useremo i comandi –O –sS –sT –sV che si utilizzano per:

- -O che si utilizza per rilevare il sistema operativo
- -sS ovvero SYN scan è una tecnica si scansione delle porte TCP utilizzata per rilevare quali porte sono aperte su un sistema. Funziona inviando pacchetti SYN senza completare la stretta di mano a tre vie.
- -sT o TCP connect scan è una tecnica di scansione delle porte TCP che esegue una connessione completa utilizzando il *three-way handshake*
- -sV questa scansione permette di rilevare la versione dei servizi in esecuzione sulle porte aperte.

Ci viene inoltre chiesto di distinguere tra SYN scan e TCP connect scan; possiamo affermare che il SYN scan risulta più veloce e meno rilevabile, in quanto non completa il processo di handshake, a differenza del TCP connect scan, che è più lento e facilmente individuabile.

Qui di seguito vediamo in pratica l'utilizzo dei comandi:

Nella prima immagine possiamo vedere i risultati dei comandi –O e –sS che ci mostrano il sistema operativo del nostro target IP :192.168.50.101/24 collegato a metaspoitable, e le varie porte aperte:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -O -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 08:42 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0035s latency).
Not shown: 977 closed tcp ports (reset)
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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

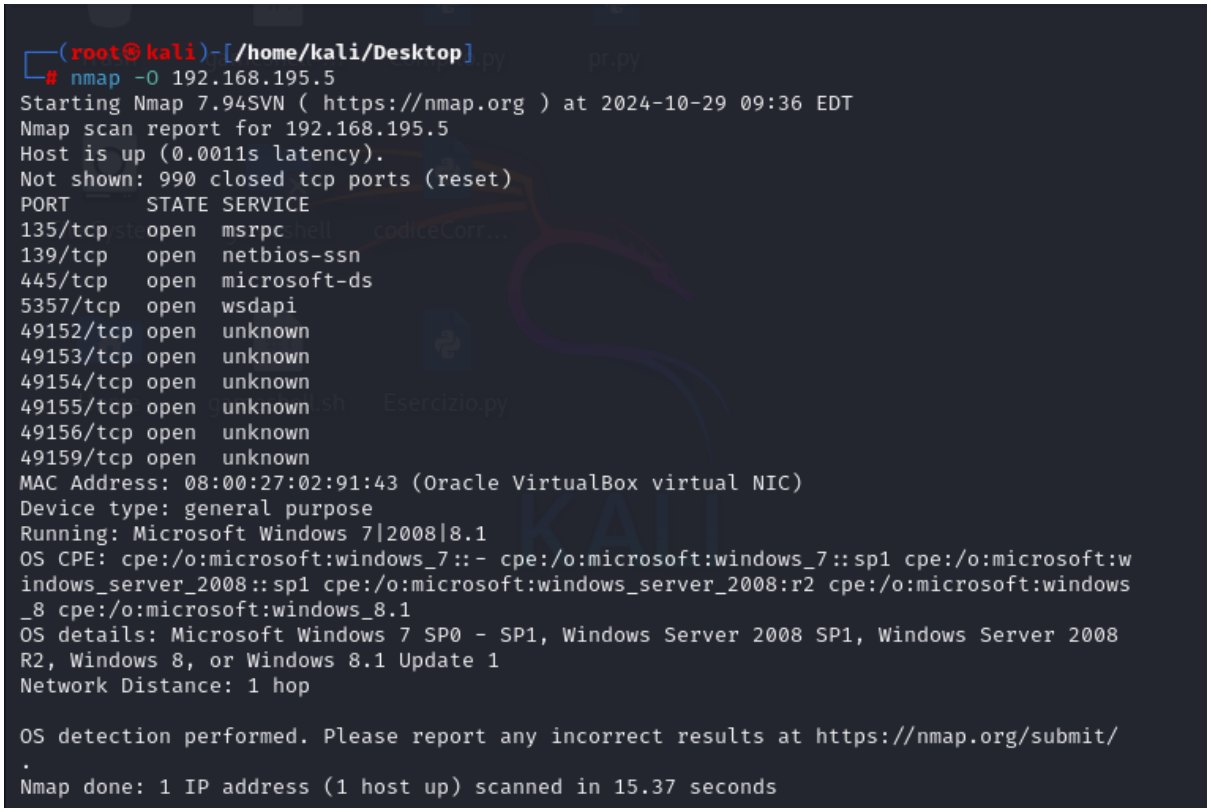
Mentre nella seconda immagine utilizziamo i comandi –sT e –sV, il comando –sT ci mostra le porte aperte, ma è più rumoroso rispetto al SYN scan.

Mentre –sV ci mostra la versione dei servizi attivi sulle porte aperte, ad esempio sulla porta 21 FTP abbiamo la versione vsftpd 2.3.4

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sT -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 08:45 EDT
Nmap scan report for 192.168.50.101
Host is up (0.018s latency).
Not shown: 977 closed tcp ports (conn-refused)
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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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  ccproxy-ftp?
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
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 172.84 seconds
```

Successivamente utilizziamo il comando –O verso un altro indirizzo IP 192.168.195.5 collegato alla nostra VM di windows 7.



Conclusione:

- OS Fingerprint: dovresti ricevere una stima del sistema operativo in esecuzione. Ad esempio, Metasploitable spesso si identifica come una variante di Linux, mentre una macchina Windows verrà riconosciuta come Windows.
- SYN Scan e TCP Connect Scan: dovrebbero mostrare porte simili aperte. Tuttavia, è possibile che alcuni firewall o IDS rilevino e blocchino la TCP Connect scan più facilmente.
- Version Detection: fornirà informazioni dettagliate sulle versioni dei servizi attivi, consentendo di comprendere meglio quali applicazioni sono esposte.

Inoltre bisogna assicurarsi di rispettare le policy di utilizzo della rete e di avere il permesso per eseguire queste scansioni su macchine che non sono di nostra proprietà, dato che Nmap può risultare intrusivo per reti e host non configurati per i test di sicurezza.