

Scansione dei servizi

nmap

Sommario

Traccia dell'esercizio principale	2
Traccia dell'esercizio facoltativo.....	2
Configurazione laboratorio virtuale.....	2
Svolgimento traccia principale	3
OS Fingerprinting.....	3
Syn Scan.....	4
TCP Connect Scan	4
Version Detection	5
Report Finale di Scansione Nmap - Metasploitable	6
Informazioni Generali	6
1. OS Fingerprinting (nmap -O -v)	6
2. TCP Connect Scan (nmap -sT -v)	7
3. SYN Scan (nmap -sS -v)	8
4. Version Detection (nmap -sV -v)	9
Conclusioni finali del report.....	10
Traccia esercizio facoltativo	11
1. OS Fingerprinting (nmap -O -v)	11
2. TCP Connect Scan (nmap -sT -v)	11
3. SYN Scan (nmap -sS -v)	12
4. Version Detection (nmap -sV -v)	12
Report sui nuovi risultati con le macchine nella stessa rete	12

Traccia dell'esercizio principale

Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable** (target e attaccante devono essere su due reti diverse):

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

A valle delle scansioni, è prevista la produzione di un **report** contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

Traccia dell'esercizio facoltativo

Facoltativo:

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete.

Estendere il report con le nuove informazioni ed evidenziare le differenze.




Configurazione laboratorio virtuale

La configurazione è identica al report M3 W9 D5

pfSense come Server DHCP

Kali Linux su rete 192.168.1.0/24

Metasploitable2 su rete 192.168.50.0/24

Interfaces				
 WAN	↑	1000baseT <full-duplex>	10.0.2.15	
 LAN	↑	1000baseT <full-duplex>	192.168.1.1	
 LAN2	↑	1000baseT <full-duplex>	192.168.50.1	

Svolgimento traccia principale

Per ogni comando in nmap a discrezione si può inserire il flag -v per una modalità più dettagliata.

OS Fingerprinting

Per individuare il sistema operativo con nmap si utilizza il flag -O, richiede privilegi di amministratore. Si possono usare ulteriori opzioni.

```
OS DETECTION:  
-O: Enable OS detection  
--osscan-limit: Limit OS detection to promising targets  
--osscan-guess: Guess OS more aggressively
```

nmap -O 192.168.50.100

```
(kali@kali)-[~]  
$ sudo nmap -O 192.168.50.100  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 12:56 EDT  
Nmap scan report for 192.168.50.100  
Host is up (0.0022s 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  
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  
TCP/IP fingerprint:  
OS:SCAN(V=7.94SVN%E=4%D=9/19%OT=21%CT=1%CU=33293%PV=Y%DS=2%DC=I%G=Y%TM=66EC  
OS:57DC%P=x86_64-pc-linux-gnu)SEQ(SP=CA%GCD=1%ISR=D7%TI=Z%II=I%TS=7)OPS(O1=  
OS:M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6  
OS:%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y  
OS:%DF=Y%T=40%W=16D0%O=M5B4NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD  
OS:=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A-S+%F=AR%O=RD=0%Q=  
OS:)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G  
OS:%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)  
  
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 12.36 seconds
```

La scansione, oltre a scansionare il sistema operativo, ha scansionato le porte aperte e riporta che ci sono 2 nodi di distanza tra l'attaccante e il target.

Syn Scan

La Syn Scan è una delle scansioni più comuni e veloci. Può essere eseguita in modalità stealth, invia pacchetti SYN senza stabilire una connessione completa (non completando l'handshake TCP). Utilizza il comando: **nmap -sS 192.168.50.100** -sS: esegue una Syn Scan

```
Host is up (0.013s 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

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
Raw packets sent: 1004 (44.152KB) | Rcvd: 1001 (40.120KB)
```

TCP Connect Scan

La TCP Connect Scan utilizza il sistema operativo per completare il three-way handshake, quindi è meno furtiva della Syn Scan: **nmap -sT 192.168.50.100** -sT: esegue una TCP Connect Scan

```
Host is up (0.046s 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

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Version Detection

Per identificare le versioni dei servizi in esecuzione, usa la "version detection": **nmap -sV 192.168.50.100**
-sV: rileva la versione dei servizi in ascolto

```
Completed Connect Scan at 16:37, 0.41s elapsed (1000 total ports)
Initiating Service scan at 16:37
Scanning 23 services on 192.168.50.100
Completed Service scan at 16:40, 156.25s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.50.100.
Initiating NSE at 16:40
Completed NSE at 16:40, 8.05s elapsed
Initiating NSE at 16:40
Completed NSE at 16:40, 8.02s elapsed
Nmap scan report for 192.168.50.100
Host is up (0.0072s 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

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.90 seconds
```

Sono elencati in lista tutti i servizi con porta, nome servizio e versione.

Report Finale di Scansione Nmap- Metasploitable

Informazioni Generali

- **IP del Target:** 192.168.50.100
- **Host:** Metasploitable
- **Stato Host:** Up

1. OS Fingerprinting (nmap-O-v)

Porta	Stato	Servizio
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

Porta	Stato	Servizio
8009/tcp	open	ajp13
8180/tcp	open	unknown

Dettagli sul Sistema Operativo:

- **Tipo di Dispositivo:** General purpose
- **Sistema Operativo:** Linux 2.6.X
- **Dettagli OS:** Linux 2.6.15 - 2.6.26 (probabilmente embedded), Linux 2.6.29 (Gentoo)

2. TCP Connect Scan (nmap-sT-v)

Porte Aperte e Servizi:

Porta	Stato	Servizio
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

Porta	Stato	Servizio
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown

Differenze rispetto a SYN Scan:

- Entrambi gli scansioni mostrano porte simili aperte.
- Il TCP Connect Scan stabilisce una connessione completa, mentre il SYN Scan non la completa, rendendo il primo più visibile a un IDS.

3. SYN Scan (nmap-sS-v)

Porte Aperte e Servizi:

Porta	Stato	Servizio
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

Porta	Stato	Servizio
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

4. Version Detection (nmap-sV-v)

Porte Aperte e Servizi:

Porta	Stato	Servizio	Versione
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
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
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X
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

Porta	Stato	Servizio	Versione
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

Conclusioni finali del report

Le scansioni hanno rivelato una varietà di porte aperte e servizi in esecuzione su Metasploitable. Utilizzando tecniche diverse, come TCP Connect, SYN e Version Detection, si è potuto ottenere un quadro dettagliato del sistema.

Svolgimento esercizio facoltativo

Configurare la macchina virtuale di Metasploitable2 nella stessa rete **intnet** di Kali.

1. OS Fingerprinting (nmap-O-v)

```
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
MAC Address: 08:00:27:77:37:E6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 497.101 days (since Thu May 11 14:54:41 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```

2. TCP Connect Scan (nmap-sT-v)

```
(kali@kali)~[~]
$ sudo nmap -sT 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 17:21 EDT
Nmap scan report for 192.168.1.100
Host is up (0.0073s 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: 08:00:27:77:37:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

3. SYN Scan (nmap-sS-v)

```
(kali@kali)~$ sudo nmap -sS 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 17:22 EDT
Nmap scan report for 192.168.1.100
Host is up (0.0012s 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
MAC Address: 08:00:27:77:37:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

4. Version Detection (nmap-sV-v)

```
(kali@kali)~$ sudo nmap -sV 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 17:22 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00065s 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         netkit-rsh rexecd
513/tcp   open  login
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: 08:00:27:77:37:E6 (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 12.03 seconds
```

Report sui nuovi risultati con le macchine nella stessa rete

Nella nuova configurazione, sono state eseguite le stesse scansioni Nmap. Non ci sono differenze significative nei servizi rilevati, ma la latenza è leggermente migliorata grazie all'assenza di pfSense.