

ESERCIZIO W11D1

SCANSIONI NMAP

Studente: Davide Mirani

Traccia:

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
- 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

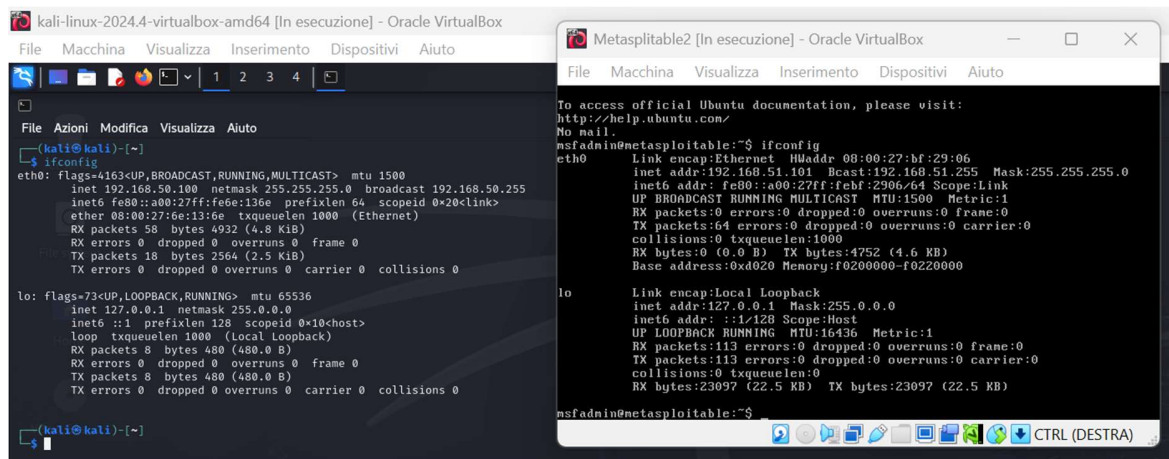
1. Introduzione

L'obiettivo dell'esercizio è eseguire una serie di scansioni Nmap contro una macchina Metasploitable da una macchina Kali Linux, assicurandosi che le due siano configurate su reti diverse.

2. Configurazione di rete

- Kali Linux IP: 192.168.50.100
- Metasploitable IP: 192.168.51.101

Le macchine sono su due reti diverse, come richiesto nella traccia.



3. Raggiungibilità della macchina (ping)

```
(kali@kali)-[~]
$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=13.1 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=2.33 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=1.81 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=2.94 ms
^C
— 192.168.51.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3086ms
rtt min/avg/max/mdev = 1.809/5.044/13.108/4.672 ms
```

4. Risultati delle scansioni

Porta	Servizio	Stato (sS)	Stato (sT)	Versione (sV)
21	ftp	open	open	vsftpd 2.3.4
22	ssh	open	open	OpenSSH 4.7p1 Debian 8ubuntu1
23	telnet	open	open	Linux telnetd
25	smtp	open	open	Postfix smtpd
53	domain	open	open	ISC BIND 9.4.2
80	http	open	open	Apache httpd 2.2.8
111	rpcbind	open	open	2 (RPC #100000)
139	netbios-ssn	open	open	Samba smbd 3.X - 4.X
445	microsoft-ds	open	open	Samba smbd 3.X - 4.X
512	exec	open	open	netkit-rsh rexecd
513	login	open	open	?
514	shell	open	open	Netkit rshd
1099	rmiregistry	open	open	GNU Classpath grmiregistry
1524	ingresslock	open	open	Metasploitable root shell
2049	nfs	open	open	2-4 (RPC #100003)

2121	ccproxy-ftp	open	open	?
3306	mysql	open	open	MySQL 5.0.51a-3ubuntu5
5432	postgresql	open	open	PostgreSQL DB 8.0 - 8.3.7
5900	vnc	open	open	VNC (protocol 3.3)
6000	X11	open	open	(access denied)
6667	irc	open	open	UnrealIRCd
8009	ajp13	open	open	Apache Jserv (Protocol v1.3)
8180	http (tomcat)	open	open	Apache Tomcat/Coyote JSP engine 1.1

5. OS Fingerprint

- Tipo dispositivo: General purpose
- OS CPE: cpe:/o:linux:linux_kernel:2.6
- Dettagli: Linux 2.6.15 - 2.6.26 (probabilmente Ubuntu 7.04 - 8.04)
- Network distance: 2 hops
- Tempo di scansione: 8.71 secondi

Screenshot OS Fingerprint (nmap -O):

```
(kali@kali)-[~]
$ nmap -O 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 13:21 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0061s 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), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
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 8.71 seconds
```

6. Scansione SYN (nmap -sS)

Tempo di scansione: 7.18 secondi

Screenshot della scansione SYN:

```
(kali㉿kali)-[~]  
$ nmap -sS 192.168.51.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 13:28 EDT  
Nmap scan report for 192.168.51.101  
Host is up (0.021s 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  
  
Nmap done: 1 IP address (1 host up) scanned in 7.18 seconds
```

7. Scansione TCP Connect (nmap -sT)

Tempo di scansione: 6.91

Screenshot della scansione TCP connect:

```
(kali㉿kali)-[~]  
$ nmap -sT 192.168.51.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 13:29 EDT  
Nmap scan report for 192.168.51.101  
Host is up (0.019s 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  
  
Nmap done: 1 IP address (1 host up) scanned in 6.91 seconds
```

8. Rilevamento versioni (nmap -sV)

Tempo di scansione: 180.67 secondi

Screenshot rilevamento versione dei servizi:

```
(kali@kali)-[~]
$ nmap -sV 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 13:32 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0076s 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  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 180.67 seconds
```

9. Differenze tra scansioni SYN e TCP Connect

La scansione SYN (`-sS`) è più veloce e meno rilevabile dai firewall/IDS perché non completa la stretta di mano TCP.

La scansione TCP Connect (`-sT`) invece stabilisce una connessione completa ed è più facilmente tracciabile.

In questo caso i risultati delle due scansioni sono identici, variando solo nei tempi.

10. Conclusioni

La macchina Metasploitable presenta molte porte aperte e servizi vulnerabili.

L'identificazione precisa delle versioni tramite ``-sV`` ha permesso di confermare la natura deliberatamente vulnerabile del sistema target.