

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.

E la seguente sul target Windows:

- OS fingerprint.

Preparazione delle differenti VM

1. Come primo passo mi assicuro che le VM siano configurate correttamente e che siano quindi, sulla stessa rete. Per le scansioni, è consigliabile usare "Rete Interna" e che il nome della rete interna sia lo stesso (intnet), in modo che tutte le VM possano comunicare tra loro.

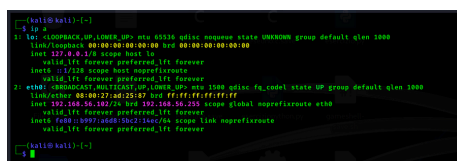


```
metasploitable 2 [In esecuzione]
192.168.56.101: Host name lookup failure
ifconfig: --help gives usage information.
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.56.101 netmask 255.255.255.0 up
msfadmin@metasploitable:~$ ifconfig
eth0
Link encap:Ethernet HWaddr 08:00:27:dc:bc:9c
inet addr:192.168.56.101 Bcast:192.168.56.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe1c:bc9c::1 Scope:link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:5006 (4.8 KB)
Base address:0x4020 Memory:f0200000-f0220000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:100 errors:0 dropped:0 overruns:0 frame:0
TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23481 (22.9 KB) TX bytes:23481 (22.9 KB)

msfadmin@metasploitable:~$
```

IP Address: 192.168.56.101
SubnetMask:255.255.255.0

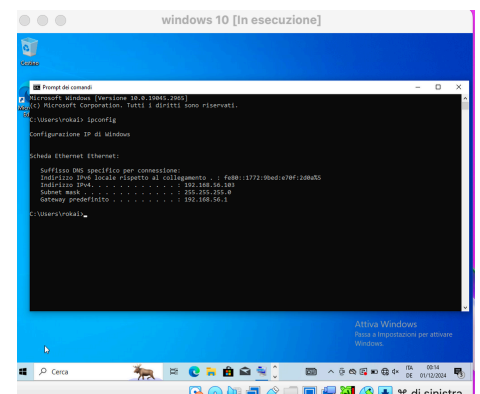


```
kali@kali:~$ ifconfig
eth0
Link encap:Ethernet HWaddr 08:00:27:dc:bc:9c
inet addr:192.168.56.102 Bcast:192.168.56.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe1c:bc9c::1 Scope:link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:5006 (4.8 KB)
Base address:0x4020 Memory:f0200000-f0220000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:100 errors:0 dropped:0 overruns:0 frame:0
TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23481 (22.9 KB) TX bytes:23481 (22.9 KB)

kali@kali:~$
```

IP Address:192.168.56.102
SubnetMask:255.255.255.0



```
windows 10 [In esecuzione]
Microsoft Windows [versione 10.0.18095.2005]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\indrali>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:
Suffisso DNS specifico per connessione:
Indirizzo IPv4 locale rispetto al collegamento: . . . fe80::1772:9bad:c76f:208a55
Indirizzo IPv6 . . . . . fe80::1772:9bad:c76f:208a55
Subnet mask . . . . . 255.255.255.0
Gateway predefinito . . . . . 192.168.56.1

C:\Users\indrali>
```

IP Address: 192.168.56.103
SubnetMask:255.255.255.0

2. Dopodichè apro il terminale di Kali Linux per eseguire i comandi richiesti, installando Nmap. Quindi:

`sudo apt update`
`sudo apt install nmap`

Una volta scaricato nmap si può proseguire con l'esecuzione di diverse scansioni su Metasploitable e su una VM Windows .

Le scansioni includono **l'identificazione del sistema operativo , la scansione delle porte e la rivelazione dei servizi in esecuzione.**

● Scansione OS Fingerprint su Metasploitable

Comando eseguito: `nmap -O 192.168.56.101`

Con il comando -O, si permette a Nmap di tentare di identificare il sistema operativo in esecuzione sulla macchina di destinazione. Questo è utile per comprendere il tipo di vulnerabilità a cui una macchina potrebbe essere soggetta.

Risultato:



● SYN Scan su Metasploitable

Comando eseguito: `nmap -sS 192.168.56.101`

La scansione SYN (o "half-open") invia pacchetti SYN per determinare quali porte sono aperte senza stabilire una connessione completa. Questo metodo è discreto e può essere utilizzato per scansioni furtive.

Risultato:

```
(kali㉿kali)-[~]  
$ nmap -sS 192.168.56.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 12:49 EST  
Nmap scan report for 192.168.56.101  
Host is up (0.00073s 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:DC:BC:9C (PCS Systemtechnik/Oracle VirtualBox)  
  
Nmap done: 1 IP address (1 host up) scanned in 14.45 seconds
```

● TCP Connect su Metasploitable

Comando Eseguito: `nmap -sT 192.168.56.101`

La scansione TCP Connect utilizza il protocollo TCP per stabilire una connessione completa con le porte della macchina di destinazione. Questo metodo è meno furtivo rispetto alla scansione SYN, ma fornisce risultati affidabili.

Risultato:

```
(kali㉿kali)-[~]  
$ nmap -sT 192.168.56.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 13:08 EST  
Nmap scan report for 192.168.56.101  
Host is up (0.0018s 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:DC:BC:9C (PCS Systemtechnik/Oracle VirtualBox)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.82 seconds
```

Confronto tra i risultati di TCP Connect e SYN Scan:

- Entrambi i comandi hanno rilevato le stesse porte aperte
- Entrambi gli output segnalano che 977 porte sono chiuse. Nella scansione TCP Connect si

specifica che il motivo è **conn-refused**, mentre nella scansione SYN si segnala **reset**. Questo è normale e indica che le porte chiuse non accettano connessioni.

● Version Detection su Metasploitable

Comando Eseguito : `nmap -sV 192.168.56.101`

Con il comando `-sV`, si identifica non solo quali porte sono aperte, ma anche quali servizi sono in esecuzione, insieme alle loro versioni, su ogni porta aperta su Metasploitable. Questo è utile per valutare vulnerabilità specifiche associate a versioni note di software

Risultato:

```
(kali@kali)-[~]
$ nmap -sV 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 13:38 EST
Nmap scan report for 192.168.56.101
Host is up (0.00059s 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 rshd
513/tcp   open  login          OpenBSD or Solaris rlogind
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  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:DC:BC:9C (PCS Systemtechnik/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 27.03 seconds
```

● Scansione OS Fingerprint su Windows 10

Comando eseguito: `nmap -O 192.168.56.103`

Come nel primo passo questo comando cerca di identificare il sistema operativo in esecuzione sulla macchina Windows.

Per eseguire con successo la scansione OS Fingerprint sulla macchina Windows, è stato necessario disattivare temporaneamente il firewall.

```

C:\Windows\system32> netsh advfirewall show allprofiles

Impostazioni Profilo di dominio:
-----
Stato                                ON
Criteri firewall                    BlockInbound,AllowOutbound
LocalFirewallRules                  N/D (solo archivio oggetti Criteri di gruppo)
LocalConSecRules                    N/D (solo archivio oggetti Criteri di gruppo)
InboundUserNotification             Abilita
RemoteManagement                    Disabilita
UnicastResponseToMulticast          Abilita

Registrazione:
RegistraConnessioniConsentite        Disabilita
RegistraConnessioniEliminate          Disabilita
NomeFile                             %systemroot%\system32\LogFiles\Firewall\pfirewall.log
DimensioneMaxFile                     4096

Impostazioni Profilo privato:
-----
Stato                                ON
Criteri firewall                    BlockInbound,AllowOutbound
LocalFirewallRules                  N/D (solo archivio oggetti Criteri di gruppo)
LocalConSecRules                    N/D (solo archivio oggetti Criteri di gruppo)
InboundUserNotification             Abilita
RemoteManagement                    Disabilita

```

Con il comando: **netsh advfirewall set allprofiles off.**

Questo ha permesso a Nmap di rilevare le porte aperte e il sistema operativo senza restrizioni. Dopo aver completato la scansione e raccolto i dati , il firewall é stato riattivato per garantire la sicurezza della macchina.

Risultato:

```

(kali㉿kali)-[~]
$ nmap -O 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 14:18 EST
Nmap scan report for 192.168.56.103
Host is up (0.0036s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:80:93:A6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 21H2
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 16.90 seconds

```

L'obbiettivo di questo report é valutare la sicurezza delle macchine virtuali

Metasploitable e Windows attraverso l'analisi delle porte e dei servizi in esecuzione.

METASPLOITABLE

- **IP:** 192.168.56.101
- **Sistema Operativo:** Linux 2.6.9 - 2.6.33
- **Porte Aperte ▶ Servizi Web:** 80 (HTTP)
 - ▶ **Accesso Remoto:** 22 (SSH)
 - ▶ **Servizi FTP:** 21 (FTP)
 - ▶ **Servizi Email:** 25 (SMTP)
 - ▶ **Servizi Database:** 3306 (MySQL)
- **Servizi in ascolto con versione ▶ Porta 80:** Apache httpd ,2.2.8
 - ▶ **Porta 22:** Open SSH, 4.7p1 Debian 8ubuntu1(protocol2.0)
 - ▶ **Porta 21 :** vsftpd, 2.3.4
 - ▶ **Porta 25:** Postfix, smtpd
 - ▶ **Porta 3306:** MySQL 5.0.51a-3ubuntu5

WINDOWS

- **IP:** 192.168.56.103
- **Sistema Operativo:** Microsoft Windows 1709 - 21H2
- **Porte Aperte ▶ 135**
 - ▶ 139
 - ▶ 445
- **Servizi in ascolto con versione ▶ Porta 135 (MSRPC):** msrpc
 - ▶ **Porta 139 (NetBIOS-SSN):** netbios-ssn
 - ▶ **Porta 445 (Microsoft-DS):** microsoft-ds

