
EPICODE
Scansione dei servizi con Nmap

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 le seguenti sul target Windows 7:

- OS fingerprint

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un report contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione

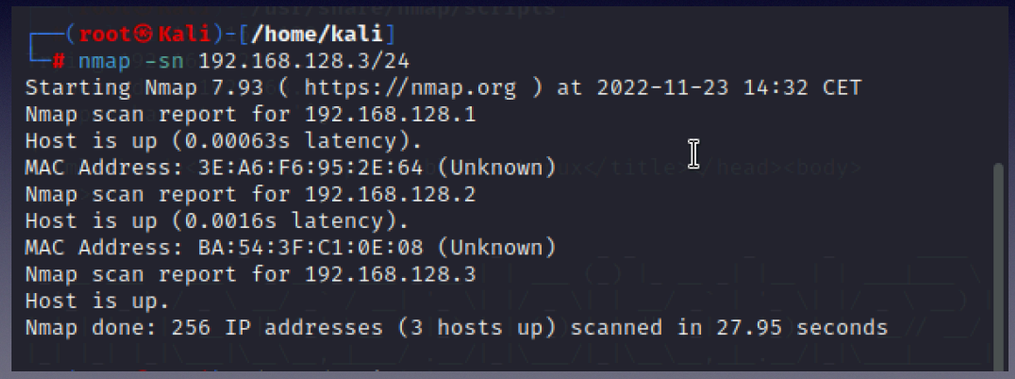
Quesito extra (al completamento dei quesiti sopra):

Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

L’ESERCIZIO SARA SVOLTO NEL SEGUENTE ORDINE:
-SCANSIONE MACCHINA METASPLOITABLE 2
-SCANSIONE MACCHINA WINDOWS 7

INDIRIZZI IP:
KALI LINUX: 192.168.32.100
METASPLOITABLE 2: 192.168.128.2
WINDOWS 7: 192.168.32.101

nmap -sn
Comando eseguito per controllare quali indirizzi IP sono collegati alla mia rete.



nmap -o
Comando inserito per controllare la versione della macchina bersaglio ed eventuali porte aperte.

```
┌──(root㉿Kali)-[/home/kali]
└─# nmap -O 192.168.128.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 14:11 CET
Nmap scan report for 192.168.128.2
Host is up (0.0018s 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: BA:54:3F:C1:0E:08 (Unknown)
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
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 14.71 seconds
```

nmap -sT
Comando inserito per fare scansioni TCP ,verso la macchina bersaglio.

```
┌──(root㉿Kali)-[/home/kali]
└─# nmap 192.168.128.2 -sT
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 14:11 CET
Nmap scan report for 192.168.128.2
Host is up (0.0020s 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: BA:54:3F:C1:0E:08 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

nmap -sT
Comando inserito per fare scansioni SYN verso macchina bersaglio

```
┌──(kali㉿Kali)-[~]
└─$ sudo ss
[sudo] password di kali:
┌──(root㉿Kali)-[/home/kali]
└─# nmap 192.168.128.2 -sS
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 14:10 CET
Nmap scan report for 192.168.128.2
Host is up (0.00079s 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: BA:54:3F:C1:0E:08 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

Adesso procediamo alle scansioni sulla macchina Windows 7.

```
File  Azioni  Modifica  Visualizza  Aiuto
┌──(root㉿Kali)-[/home/kali]
└─# nmap -O 192.168.32.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 17:20 CET
Nmap scan report for 192.168.32.101
Host is up (0.0047s latency).
All 1000 scanned ports on 192.168.32.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 8E:4B:3D:97:D2:FA (Unknown)
Too many fingerprints match this host to give specific OS details
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 24.12 seconds
```

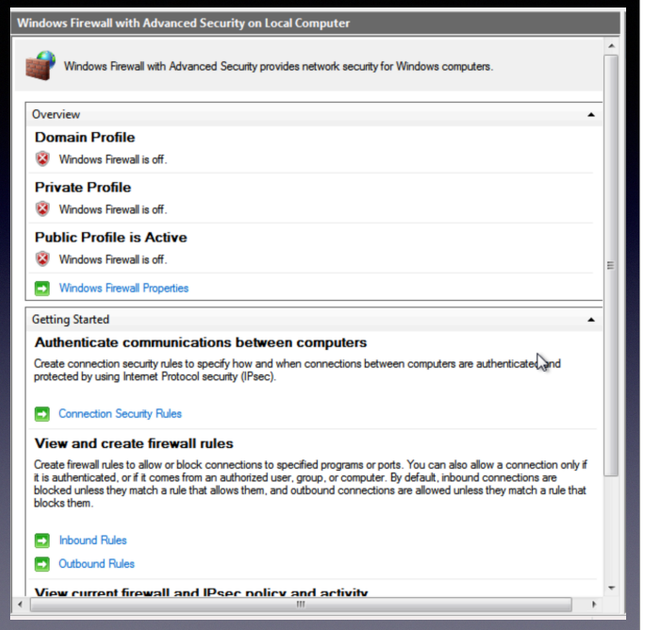
Come possiamo vedere la nostra macchina non riesce a bypassare il sistema windows, proprio perché vi è il firewall attivo.

```
┌──(root㉿Kali)-[/home/kali]
└─# nmap -sS -T5 192.168.32.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 17:21 CET
Nmap scan report for 192.168.32.101
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.32.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 8E:4B:3D:97:D2:FA (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 11.66 seconds

┌──(root㉿Kali)-[/home/kali]
└─# nmap -sT -T5 192.168.32.101 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 17:22 CET
Nmap scan report for 192.168.32.101
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.32.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

Disattivando completamente il firewall potremo notare come adesso sarà possibileeffettuare le scansioni che prima ci erano negate.



```
┌──(root㉿Kali)-[/home/kali]
└─# nmap -sT -T5 192.168.32.101 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 17:26 CET
Nmap scan report for 192.168.32.101
Host is up (0.0017s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 8E:4B:3D:97:D2:FA (Unknown)
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
Service Info: Host: FABIO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Fabio-PC
|   NetBIOS computer name: FABIO-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-11-23T17:26:59+01:00
| smb2-time:
|   date: 2022-11-23T16:26:59
|_  start_date: 2022-11-23T16:15:31
|_clock-skew: mean: -20m03s, deviation: 34m38s, median: -4s
| smb-security-mode:
```

```
┌──(root㉿Kali)-[/home/kali]
└─# nmap -sS -T5 192.168.32.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 17:27 CET
Nmap scan report for 192.168.32.101
Host is up (0.00046s latency).
Not shown: 990 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
49157/tcp open  unknown
MAC Address: 8E:4B:3D:97:D2:FA (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds
```

CONCLUSIONI:
Come abbiamo potuto notare da queste slide, l'unica difficoltà che abbiamo riscontrato nel poter fare le scansioni è stato nella macchina Windows a causa del Firewall attivo.
Per poter bypassare questo ostacolo nella realtà ci sarebbe bisogno di ingannare l'ignaro utente, e convincerlo a disattivare il firewall, oppure a inserire delle opzioni ci permettano di effettuare gli scan senza dover disattivarlo.