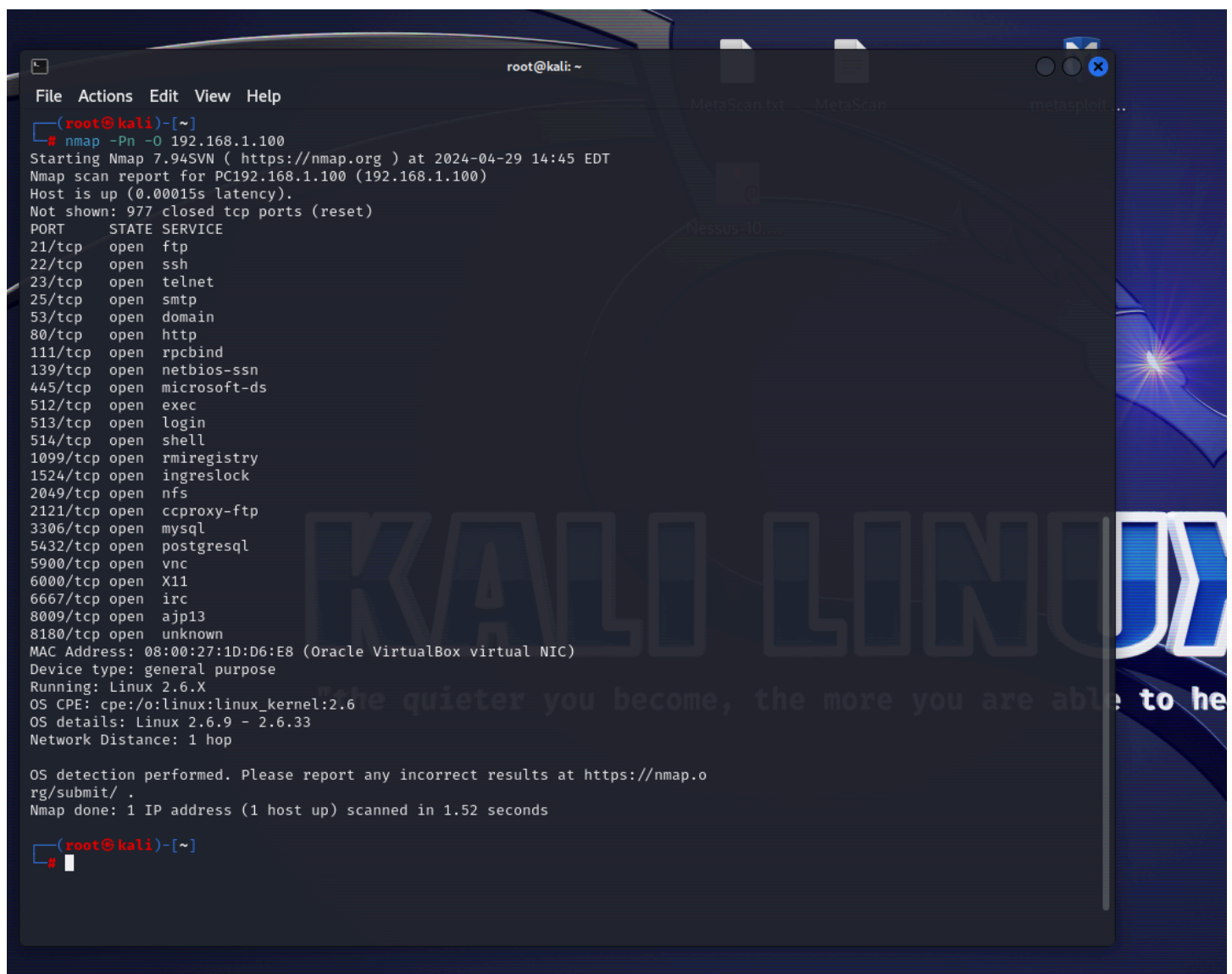


Traccia: Tecniche di scansione con Nmap

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

nmap -Pn -O 192.168.1.100



```

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# nmap -Pn -O 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 14:45 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.00015s 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: 08:00:27:1D:D6:E8 (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
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 1.52 seconds

(root@kali)-[~]
#

```

nmap -sS

```
(root@kali)-[~]
# nmap -sS 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 14:56 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.000079s 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: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

```
(root@kali)-[~]
#
```

nmap 192.168.1.100

```
(root@kali)-[~]
# nmap 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 14:59 EDT
Nmap scan report for PC192.168.1.100 (192.168.1.100)
Host is up (0.000052s 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: 08:00:27:1D:D6:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

(root@kali)-[~]
#
```

Parte 2

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
- ☐ Descrizione dei servizi

<https://www.poftut.com/nmap-output/>

nmap -oN report1 IP

da kali a windows

```

kali@kali:~$ nmap 192.168.1.8 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 14:41 EDT
Nmap scan report for PC192.168.1.8 (192.168.1.8)
Host is up.
All 1000 scanned ports on PC192.168.1.8 (192.168.1.8) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 1 IP address (1 host up) scanned in 201.48 seconds

kali@kali:~$ nmap -O 192.168.1.8
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

kali@kali:~$ sudo su
[sudo] password for kali:
kali@kali:~$ nmap -O 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 14:50 EDT
Nmap scan report for PC192.168.1.8 (192.168.1.8)
Host is up (0.00016s latency).
All 1000 scanned ports on PC192.168.1.8 (192.168.1.8) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:5A:0B:31 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp:sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley Micrologix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
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 22.05 seconds

root@kali:~# nmap -n -PO -p 1-1024 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 14:52 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00016s latency).
All 1024 scanned ports on 192.168.1.8 are in ignored states.
Not shown: 1024 filtered tcp ports (no-response)
MAC Address: 08:00:27:5A:0B:31 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 21.86 seconds

root@kali:~# nmap --mtu 576 -p 1-1024 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 14:56 EDT

```

```
(root@kali)-[/home/kali]
# nmap -sV -f --mtu 512 -p 1-1024 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:04 EDT
Nmap scan report for PC192.168.1.8 (192.168.1.8)
Host is up (0.00016s latency).
All 1024 scanned ports on PC192.168.1.8 (192.168.1.8) are in ignored states.
Not shown: 1024 filtered tcp ports (no-response)
MAC Address: 08:00:27:5A:DB:31 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.04 seconds

(root@kali)-[/home/kali]
# nmap -sV -f --mtu 512 --badsum -p 1-1024 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:05 EDT
Nmap scan report for PC192.168.1.8 (192.168.1.8)
Host is up (0.00015s latency).
All 1024 scanned ports on PC192.168.1.8 (192.168.1.8) are in ignored states.
Not shown: 1024 filtered tcp ports (no-response)
MAC Address: 08:00:27:5A:DB:31 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.01 seconds

(root@kali)-[/home/kali]
# nmap -sV -f --mtu 512 --adler32 -p 1-1024 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:06 EDT
Nmap scan report for PC192.168.1.8 (192.168.1.8)
Host is up (0.00020s latency).
All 1024 scanned ports on PC192.168.1.8 (192.168.1.8) are in ignored states.
Not shown: 1024 filtered tcp ports (no-response)
MAC Address: 08:00:27:5A:DB:31 (Oracle VirtualBox virtual NIC)
```

```
(root@kali)-[/home/kali]
# nmap -n -PN -sT -sU -p 1-1024 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:33 EDT
Failed to resolve "1-1024".
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 0.01% done

(root@kali)-[/home/kali]
# nmap -n -PN -sT -sU -p 1-1024 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:33 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00017s latency).
All 2048 scanned ports on 192.168.1.8 are in ignored states.
Not shown: 1024 filtered tcp ports (no-response), 1024 open|filtered udp ports (no-response)
MAC Address: 08:00:27:5A:DB:31 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 43.62 seconds

(root@kali)-[/home/kali]
# nmap -n -PN -sT -sU -p 80,443 T1 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:36 EDT
Failed to resolve "T1".
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 15:36 (0:00:00 remaining)
Nmap scan report for 192.168.1.8
Host is up (0.00017s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http
443/tcp    filtered  https
80/udp    open|filtered http
443/udp    open|filtered https
MAC Address: 08:00:27:5A:DB:31 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.67 seconds

(root@kali)-[/home/kali]
# nmap -sF -p1-100 -T4 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:38 EDT
Nmap scan report for PC192.168.1.8 (192.168.1.8)
Host is up (0.00017s latency).
All 100 scanned ports on PC192.168.1.8 (192.168.1.8) are in ignored states.
Not shown: 100 open|filtered tcp ports (no-response)
MAC Address: 08:00:27:5A:DB:31 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.20 seconds

(root@kali)-[/home/kali]
```

Nessun comando è stato in grado di bypassare il drop pacchetti di windows.
Qualche info grazie alle scansioni UDP (OPENED|FILTERED)

Con regola Firewall qualcosa passa e permette di scoprire OS della macchina target

```
(root@kali)-[~]
# nmap -sV -p 1-1024 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 17:20 EDT
Nmap scan report for PC192.168.1.8 (192.168.1.8)
Host is up (0.00016s latency).
Not shown: 1021 filtered tcp ports (no-response)
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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:5A:DB:31 (Oracle VirtualBox virtual NIC)
Service Info: Host: WIN7EC; OS: Windows; CPE: cpe:/o:microsoft:windows


Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds

(root@kali)-[~]
# nmap -O -p 1-1024 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 17:21 EDT
Nmap scan report for PC192.168.1.8 (192.168.1.8)
Host is up (0.00017s latency).
Not shown: 1021 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:5A:DB:31 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
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 7.83 seconds

(root@kali)-[~]
#
```

Aggiungo anche, chiedo delucidazioni su questo screen



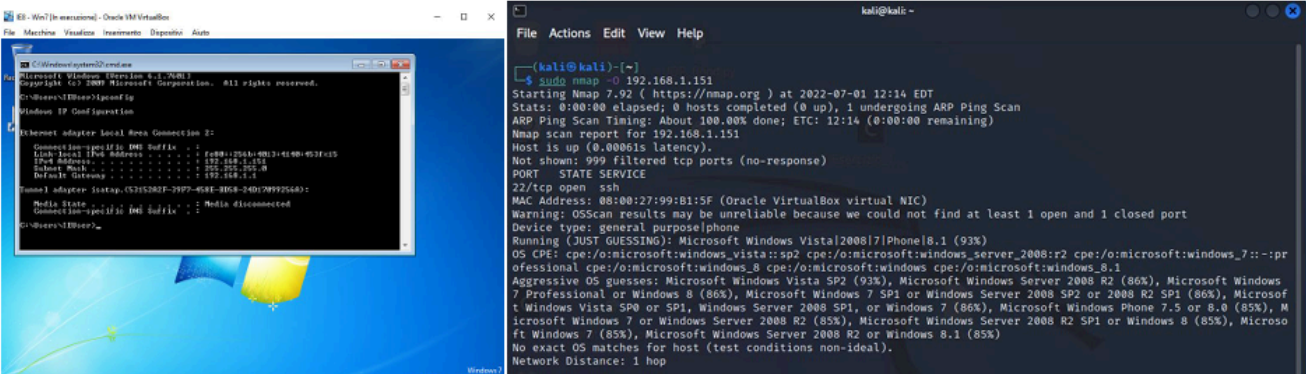
W11D1 - Soluzione (2) PDF

Esercizio

Scansione con Nmap - soluzione

Soluzione

La figura a destra ci suggerisce che 999 porte tcp non hanno dato riscontro ai test di nmap, e quindi sono categorizzate come filtrate. In uno scenario reale, la causa potrebbe essere un dispositivo di sicurezza che blocca le richieste in entrata. I metodi utilizzabili in questo caso potrebbero includere le tecniche di evasione Firewall e IPS visti nella lezione teorica.



In quanto la porta 22 non ha nessun senso di essere aperta con il firewall base, se non forzatamente tramite regola ad hoc