

Traccia:

Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Windows 7: OS fingerprint Syn Scan Version detection.

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>

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 21:44 CET
Nmap scan report for 192.168.50.102
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:4F:FE:5D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.56 seconds

(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 21:45 CET
Nmap scan report for 192.168.50.102
Host is up (0.00061s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:4F:FE:5D (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 35.11 seconds

(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 21:46 CET
Nmap scan report for 192.168.50.102
Host is up (0.0031s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:4F:FE:5D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.40 seconds
```

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 21:42 CET
Nmap scan report for 192.168.50.102
Host is up (0.0041s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:4F:FE:5D (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
ws_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 35.62 seconds
(kali@kali)-[~]
```

Attiva Windows

DOMANDA EXTRA:

La presenza del firewall che blocca le richieste.