Come da compito abbiamo svolto le scansioni richieste su metasploit (IP 192.168.51.101) e Windows7 (IP 192.168.50.102). Iniziando con l'OS FINGERPRINTING abbiamo scoperto che per quanto riguarda meta vengono fornite delle ipotesi sul sistema operativo in esecuzione sul dispositivo, con Linux 2.6.X|2.4.X al 96% di probabilità. Successivamente abbiamo effettuato una scansione SYN SCAN e una TCP connect che in questo caso hanno confermato quali porte elencate sono aperte sul dispositivo, consentendo l'accesso ai servizi corrispondenti.
Questa è una panoramica dei servizi in ascolto sull'host 192.168.51.101, insieme alle loro porte e funzioni:

21/tcp - ftp: File Transfer Protocol (FTP).

22/tcp - ssh: Secure Shell (SSH).

23/tcp - telnet: Telnet, un protocollo di rete utilizzato per l'accesso remoto a dispositivi.

25/tcp - smtp: Simple Mail Transfer Protocol (SMTP), utilizzato per la trasmissione di email.

53/tcp - domain: Domain Name System (DNS), utilizzato per risolvere i nomi di dominio in indirizzi IP.

80/tcp - http: Hypertext Transfer Protocol (HTTP), utilizzato per la comunicazione web.

111/tcp - rpcbind: Remote Procedure Call (RPC), utilizzato per la comunicazione tra processi su reti distribuite.

139/tcp - netbios-ssn: NetBIOS Session Service, utilizzato per condividere file e stampanti in reti Microsoft.

445/tcp - microsoft-ds: Microsoft-DS, utilizzato per la condivisione di file e stampanti in reti Microsoft.

512/tcp - exec: Servizio di esecuzione remota (r-commands), utilizzato per l'esecuzione remota di comandi su sistemi Unix.

513/tcp - login: Servizio di login remoto (rlogin), utilizzato per l'accesso remoto a sistemi Unix.

514/tcp - shell: Servizio di shell remota (rsh), utilizzato per l'accesso remoto a sistemi Unix.

1099/tcp - rmiregistry: Java Remote Method Invocation (RMI) Registry, utilizzato per la comunicazione tra oggetti Java distribuiti.

1524/tcp - ingreslock: Ingreslock, utilizzato con il database Ingres per il controllo dell'accesso concorrente.

2049/tcp - nfs: Network File System (NFS), utilizzato per condividere file e directory su reti Unix-like.

2121/tcp - ccproxy-ftp: CCProxy FTP, un proxy FTP.

3306/tcp - mysql: MySQL Database Server, un sistema di gestione di database relazionali.

5432/tcp - postgresql: PostgreSQL Database Server, un sistema di gestione di database relazionali.

5900/tcp - vnc: Virtual Network Computing (VNC), utilizzato per l'accesso remoto al desktop.

6000/tcp - X11: X Window System, un sistema grafico per il server di visualizzazione.

6667/tcp - irc: Internet Relay Chat (IRC), utilizzato per la comunicazione testuale in tempo reale.

8009/tcp - ajp13: Apache JServ Protocol (AJP) 1.3, utilizzato per la comunicazione tra Apache Tomcat e Apache HTTP Server.

8180/tcp - unknown: Non specificato, è necessario ulteriore indagine per determinare il servizio specifico.

root@kali: ~

File Actions Edit View Help

```
Service scan Timing: About 65.22% done; ETC: 11:17 (0:00:20 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 11:17 (0:00:18 remaining)
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 11:17 (0:00:19 remaining)
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 11:17 (0:00:21 remaining)

┌──(root㉿kali)-[~]
└─# nmap -O 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 11:17 EST
Nmap scan report for 192.168.51.101
Host is up (0.083s 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|printer|broadband router|specialized|print server|switch|media device
Running (JUST GUESSING): Linux 2.6.X|2.4.X (96%), Kyocera embedded (93%), D-Link embedded (93%), Google embedded (92%), HP embedded (92%), Philips embedded (92%), Motorola embedded (92%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:kyocera:cs-2560 cpe:/h:dlink:dsl-2540b cpe:/o:linux:linux_kernel:2.4.21 cpe:/o:linux:linux_kernel:2.6.18 cpe:/h:motorola:surfboard_sb6120 cpe:/h:motorola:surfboard_sb6141
Aggressive OS guesses: Linux 2.6.15 - 2.6.26 (likely embedded) (96%), Linux 2.6.9 - 2.6.27 (96%), Linux 2.6.18 (94%), Linux 2.6.16 - 2.6.28 (93%), Linux 2.6.22 (93%), Linux 2.6.24 (93%), Kyocera CopyStar CS-2560 printer (93%), D-Link DS
L-2540B ADSL router (93%), Linux 2.6.32 - 2.6.33 (93%), Linux 2.6.32 - 2.6.35 (93%)
No exact OS matches for host (test conditions non-ideal).
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 11.73 seconds

┌──(root㉿kali)-[~]
└─# nmap -O --osscan-limit 192.168.51.101
```

root@kali: ~

File Actions Edit View Help

```
8180/tcp open  unknown
Aggressive OS guesses: Linux 2.6.15 - 2.6.26 (likely embedded) (96%), Linux 2.6.9 - 2.6.27 (96%), Linux 2.6.18 (94%), Linux 2.6.16 - 2.6.28 (93%), Linux 2.6.22 (93%), Linux 2.6.24 (93%), Kyocera CopyStar CS-2560 printer (93%), Linux 2.6
.32 - 2.6.33 (93%), Linux 2.6.32 - 2.6.35 (93%), HP Brocade 4Gb SAN switch or (92%)
No exact OS matches for host (test conditions non-ideal).
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 8.53 seconds

┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 11:27 EST
Nmap scan report for 192.168.51.101
Host is up (0.063s 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 2.53 seconds

┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 11:28 EST
Nmap scan report for 192.168.51.101
Host is up (0.015s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
```

root@kali: ~

File Actions Edit View Help

```
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 2.53 seconds

┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 11:28 EST
Nmap scan report for 192.168.51.101
Host is up (0.015s 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 5.56 seconds

┌──(root㉿kali)-[~]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 11:37 EST
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
```

```
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.20% done; ETC: 11:37 (0:00:10 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.20% done; ETC: 11:37 (0:00:04 remaining)
Nmap scan report for 192.168.50.102
Host is up (0.0011s 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:AB:EE:61 (Oracle VirtualBox virtual NIC)
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 30.59 seconds

┌──(root㉿kali)-[~]
└─# ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
^C
— 192.168.50.102 ping statistics —
110 packets transmitted, 0 received, 100% packet loss, time 118256ms


┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 11:40 EST
Nmap scan report for 192.168.50.102
Host is up (0.0014s 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:AB:EE:61 (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 26.91 seconds

┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 13:12 EST
Nmap scan report for 192.168.50.102
Host is up (0.00059s 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:AB:EE:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 29.08 seconds

┌──(root㉿kali)-[~]
└─# nmap -sS -Pn -T1 -p 80-443 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 13:19 EST
Stats: 0:47:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.69% done; ETC: 16:23 (2:16:36 remaining)
```