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 7:
- OS fingerprint.

A valle delle scansioni 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?

METASPLOITABLE - IPv4 192.168.64.8

Tcpconnect:

```
└─# nmap -sT 192.168.64.8
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-10 14:22 CET
Nmap scan report for 192.168.64.8
Host is up (0.00057s 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: 1A:44:A4:FE:11:BB (Unknown)
```

Da questa scansione possiamo rilevare le porte aperte di un host, il protocollo ad esse assegnato e individuare quelle più a rischio.

Syn Scan:

```
└─# nmap -sS 192.168.64.8
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-10 14:24 CET
Nmap scan report for 192.168.64.8
Host is up (0.00097s 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: 1A:44:A4:FE:11:BB (Unknown)
```

Anche da questa scansione possiamo dedurre quali siano le porte aperte di un host e i protocolli a loro assegnati.
A differenza della precedente risulta più veloce ma meno affidabile in quanto non compie tutti e tre i passaggi del 3 way handshake ma solamente il primo di sync.

Version detection:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.64.8
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-10 14:19 CET
Nmap scan report for 192.168.64.8
Host is up (0.00080s 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 rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
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?
```

Grazie a questo tipo di scansione invece possiamo rilevare anche quale versione del protocollo sia in uso su una determinata porta.

OS fingerprint:

```
└─# nmap -O  192.168.64.8
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-10 14:26 CET
Nmap scan report for 192.168.64.8
Host is up (0.0013s 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: 1A:44:A4:FE:11:BB (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
```

Con questa scansione possiamo invece intercettare quale sistema operativo sia in uso sulla macchina attaccata, come si vede a fondo della figura.

WINDOWS 7 - IPv4 192.168.64.4

OS fingerprint:

```
└─# nmap -O  192.168.64.4
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-10 14:39 CET
Nmap scan report for 192.168.64.4
Host is up (0.0034s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 16:18:0C:F9:90:97 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-
:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:micros
oft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8
, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 o
r SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Serve
r 2008
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 6.85 seconds
```

Qui abbiamo usato questa scansione su un altro indirizzo ip e possiamo dedurre che il sistema operativo sia windows 7.

Il risultato sulla macchina windows differisce rispetto a quello su metasploitable in quanto all'interno del sistema operativo Microsoft è già presente un software firewall pre installato. Una soluzione per eluderlo potrebbe essere l'utilizzo del T0/T1 in nmap, che richiederebbe più tempo però potrebbe riuscire a non esser individuato dal firewall.