Scansioni nmap metaspolitable 2 vs windows 7

- Metasploitable

```
┌──(nicholas㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.2
[sudo] password for nicholas:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-01 22:55 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-se
Nmap scan report for 192.168.50.2
Host is up (0.0012s 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: CA:01:F0:3E:DD:B1 (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 1.49 seconds
```

```
┌──(nicholas㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.2 -reason
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-01 22:57 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.2
Host is up, received arp-response (0.00067s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 64
22/tcp   open  ssh          syn-ack ttl 64
23/tcp   open  telnet       syn-ack ttl 64
25/tcp   open  smtp         syn-ack ttl 64
53/tcp   open  domain       syn-ack ttl 64
80/tcp   open  http         syn-ack ttl 64
111/tcp  open  rpcbind      syn-ack ttl 64
139/tcp  open  netbios-ssn  syn-ack ttl 64
445/tcp  open  microsoft-ds syn-ack ttl 64
512/tcp  open  exec         syn-ack ttl 64
513/tcp  open  login        syn-ack ttl 64
514/tcp  open  shell        syn-ack ttl 64
1099/tcp open  rmiregistry  syn-ack ttl 64
1524/tcp open  ingreslock   syn-ack ttl 64
2049/tcp open  nfs          syn-ack ttl 64
2121/tcp open  ccproxy-ftp  syn-ack ttl 64
3306/tcp open  mysql        syn-ack ttl 64
5432/tcp open  postgresql   syn-ack ttl 64
5900/tcp open  vnc          syn-ack ttl 64
6000/tcp open  X11          syn-ack ttl 64
6667/tcp open  irc          syn-ack ttl 64
8009/tcp open  ajp13        syn-ack ttl 64
8180/tcp open  unknown      syn-ack ttl 64
MAC Address: CA:01:F0:3E:DD:B1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

```
┌──(nicholas㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.2 -reason
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-01 22:58 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.2
Host is up, received arp-response (0.0020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack
22/tcp   open  ssh          syn-ack
23/tcp   open  telnet       syn-ack
25/tcp   open  smtp         syn-ack
53/tcp   open  domain       syn-ack
80/tcp   open  http         syn-ack
111/tcp  open  rpcbind      syn-ack
139/tcp  open  netbios-ssn  syn-ack
445/tcp  open  microsoft-ds syn-ack
512/tcp  open  exec         syn-ack
513/tcp  open  login        syn-ack
514/tcp  open  shell        syn-ack
1099/tcp open  rmiregistry  syn-ack
1524/tcp open  ingreslock   syn-ack
2049/tcp open  nfs          syn-ack
2121/tcp open  ccproxy-ftp  syn-ack
3306/tcp open  mysql        syn-ack
5432/tcp open  postgresql   syn-ack
5900/tcp open  vnc          syn-ack
6000/tcp open  X11          syn-ack
6667/tcp open  irc          syn-ack
8009/tcp open  ajp13        syn-ack
8180/tcp open  unknown      syn-ack
MAC Address: CA:01:F0:3E:DD:B1 (Unknown)

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

```
└─$ sudo nmap -sV 192.168.50.2 -reason
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-01 22:59 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.2
Host is up, received arp-response (0.00050s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     REASON         VERSION
21/tcp   open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp   open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp   open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp   open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp   open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp  open  login?      syn-ack ttl 64
514/tcp  open  shell       syn-ack ttl 64 Netkit rshd
1099/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp open  X11         syn-ack ttl 64 (access denied)
6667/tcp open  irc         syn-ack ttl 64 UnrealIRCd
8009/tcp open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
MAC Address: CA:01:F0:3E:DD:B1 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.71 seconds
```

- Windows 7

```
┌──(nicholas㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
tarting Nmap 7.94 ( https://nmap.org ) at 2023-08-02 14:05 CEST
ass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
map scan report for 192.168.50.102
ost is up (0.0022s latency).
ll 1000 scanned ports on 192.168.50.102 are in ignored states.
ot shown: 1000 filtered tcp ports (no-response)
AC Address: 72:F6:E3:5C:7D:BF (Unknown)
arning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
evice type: specialized|VoIP phone|general purpose|phone
unning: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
S 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:wi
 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
S details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Ph
0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
etwork Distance: 1 hop

S detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 21.96 seconds
```

```
┌──(nicholas㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-02 14:10 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 72:F6:E3:5C:7D:BF (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds

┌──(nicholas㉿kali)-[~]
└─$ sudo nmap -sU 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-02 14:10 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.00088s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 72:F6:E3:5C:7D:BF (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 19.24 seconds
```

- Per rispondere alla domanda proposta nell'esercizio, avendo provato più tipi di scansione, il risultato è stato nullo, poiché non è stato possibile individuare nessuna porta aperta a causa del firewall, di conseguenza ritengo che l'unico modo possibile, per le mie conoscenze attuali, di aggirare il firewall, sia quello di effettuare una scansione in T1 (che dovrebbe essere fatta appositamente per bypass) o eventualmente quella di riuscire a disattivare il firewall direttamente dal PC stesso