Report Nmap scan Metasploitable /Windows 7

L’esercizio odierno richiedeva la scansione su target Metasploitable comprendente:

- OS fingerprint
- Syn Scan
- Tcp connect

  E su target Windows 7:
  - OS fingerprint

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 04:20 EST
Initiating ARP Ping Scan at 04:20
Scanning 192.168.1.10 [1 port]
Completed ARP Ping Scan at 04:20, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:20
Completed Parallel DNS resolution of 1 host. at 04:21, 13.01s elapsed
DNS resolution of 1 IPs took 13.01s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 04:21
Scanning 192.168.1.10 [1000 ports]
Discovered open port 80/tcp on 192.168.1.10
Discovered open port 5900/tcp on 192.168.1.10
Discovered open port 22/tcp on 192.168.1.10
Discovered open port 3306/tcp on 192.168.1.10
Discovered open port 25/tcp on 192.168.1.10
Discovered open port 21/tcp on 192.168.1.10
Discovered open port 445/tcp on 192.168.1.10
Discovered open port 53/tcp on 192.168.1.10
Discovered open port 23/tcp on 192.168.1.10
Discovered open port 139/tcp on 192.168.1.10
Discovered open port 111/tcp on 192.168.1.10
Discovered open port 8009/tcp on 192.168.1.10
Discovered open port 1099/tcp on 192.168.1.10
Discovered open port 2121/tcp on 192.168.1.10
Discovered open port 5432/tcp on 192.168.1.10
Discovered open port 6000/tcp on 192.168.1.10
Discovered open port 1524/tcp on 192.168.1.10
Discovered open port 513/tcp on 192.168.1.10
Discovered open port 514/tcp on 192.168.1.10
Discovered open port 2049/tcp on 192.168.1.10
Discovered open port 512/tcp on 192.168.1.10
Discovered open port 6667/tcp on 192.168.1.10
Discovered open port 8180/tcp on 192.168.1.10
Completed SYN Stealth Scan at 04:21, 0.10s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.1.10
Nmap scan report for 192.168.1.10
Host is up, received arp-response (0.00089s latency).
Scanned at 2022-11-23 04:21:10 EST for 2s
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
```

```
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: 08:00:27:C6:DE:4F (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
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=11/23%OT=21%CT=1%CU=39248%PV=Y%DS=1%DC=D%G=Y%M=080027%
OS:TM=637DE608%P=x86_64-pc-linux-gnu)SEQ(SP=CB%GCD=1%ISR=CF%TI=Z%CI=Z%II=I%
OS:TS=7)OPS(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5
OS:=M5B4ST11NW6%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=
OS:16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST1
OS:1NW6%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=4
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=16
OS:4%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.019 days (since Wed Nov 23 03:54:23 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.13 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```

Tramite il fingerprinting, è possibile identificare da remoto il sistema operativo di un host, inviando una serie di pacchetti tcp ed udp esaminando ogni bit di risposta, comparando poi i risultati con il suo database e ne visualizza i risultati nel caso di check positivi dandoci informazioni quali il vendor, il sistema operativo, ed il tipo di device.

Nella scansione di tipo TCP connect, il tool Nmap richiede al sistema operativo una connessione con chiamata connect, ottenendo informazioni sullo stato di ogni tentativo di connessione. Rispetto ad un SYN scan è quindi meno efficiente limitandosi, rispetto ad una scansione semi aperta del sS, richiedendo inoltre più tempo e un numero maggiore di pacchetti

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 04:37 EST
Initiating Ping Scan at 04:37
Scanning 192.168.1.10 [2 ports]
Completed Ping Scan at 04:37, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:37
Completed Parallel DNS resolution of 1 host. at 04:37, 13.01s elapsed
DNS resolution of 1 IPs took 13.01s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 04:37
Scanning 192.168.1.10 [1000 ports]
Discovered open port 80/tcp on 192.168.1.10
Discovered open port 111/tcp on 192.168.1.10
Discovered open port 3306/tcp on 192.168.1.10
Discovered open port 22/tcp on 192.168.1.10
Discovered open port 139/tcp on 192.168.1.10
Discovered open port 445/tcp on 192.168.1.10
Discovered open port 23/tcp on 192.168.1.10
Discovered open port 21/tcp on 192.168.1.10
Discovered open port 53/tcp on 192.168.1.10
Discovered open port 5900/tcp on 192.168.1.10
Discovered open port 25/tcp on 192.168.1.10
Discovered open port 5432/tcp on 192.168.1.10
Discovered open port 514/tcp on 192.168.1.10
Discovered open port 512/tcp on 192.168.1.10
Discovered open port 1099/tcp on 192.168.1.10
Discovered open port 8009/tcp on 192.168.1.10
Discovered open port 6667/tcp on 192.168.1.10
Discovered open port 6000/tcp on 192.168.1.10
Discovered open port 1524/tcp on 192.168.1.10
Discovered open port 8180/tcp on 192.168.1.10
Discovered open port 513/tcp on 192.168.1.10
Discovered open port 2121/tcp on 192.168.1.10
Discovered open port 2049/tcp on 192.168.1.10
Completed Connect Scan at 04:37, 0.08s elapsed (1000 total ports)
Nmap scan report for 192.168.1.10
Host is up, received syn-ack (0.00058s latency).
Scanned at 2022-11-23 04:37:30 EST for 0s
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
```

```
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

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

SYN SCAN

Una connessione SYN scan è considerato lo scan di default . Risulta essere relativamente nascosto, poco invasivo poiché non completa le

connessioni tcp più rapido rispetto ad un tcp scan, non limitata da firewall restrittivi.

Viene appunto mandato un pacchetto SyN per aprire una connessione come per aprire una connessione reale, in questo caso una risposta syn/ack indica che la porta è appunto in ascolto, quindi aperta, mentre una risposta RST indica che la porta è chiusa. Se non viene ricevuta risposta dopo qualche tentativo la porta verrà marcata come “filtered”.

```
└─$ sudo nmap  -vvv -sS 192.168.1.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 04:31 EST
Initiating ARP Ping Scan at 04:31
Scanning 192.168.1.10 [1 port]
Completed ARP Ping Scan at 04:31, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:31
Completed Parallel DNS resolution of 1 host. at 04:32, 13.03s elapsed
DNS resolution of 1 IPs took 13.03s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 04:32
Scanning 192.168.1.10 [1000 ports]
Discovered open port 111/tcp on 192.168.1.10
Discovered open port 5900/tcp on 192.168.1.10
Discovered open port 25/tcp on 192.168.1.10
Discovered open port 23/tcp on 192.168.1.10
Discovered open port 80/tcp on 192.168.1.10
Discovered open port 139/tcp on 192.168.1.10
Discovered open port 53/tcp on 192.168.1.10
Discovered open port 21/tcp on 192.168.1.10
Discovered open port 22/tcp on 192.168.1.10
Discovered open port 3306/tcp on 192.168.1.10
Discovered open port 445/tcp on 192.168.1.10
Discovered open port 1524/tcp on 192.168.1.10
Discovered open port 513/tcp on 192.168.1.10
Discovered open port 8009/tcp on 192.168.1.10
Discovered open port 8180/tcp on 192.168.1.10
Discovered open port 6667/tcp on 192.168.1.10
Discovered open port 2049/tcp on 192.168.1.10
Discovered open port 2121/tcp on 192.168.1.10
Discovered open port 1099/tcp on 192.168.1.10
Discovered open port 512/tcp on 192.168.1.10
Discovered open port 514/tcp on 192.168.1.10
Discovered open port 5432/tcp on 192.168.1.10
Discovered open port 6000/tcp on 192.168.1.10
Completed SYN Stealth Scan at 04:32, 0.10s elapsed (1000 total ports)
Nmap scan report for 192.168.1.10
Host is up, received arp-response (0.00089s latency).
Scanned at 2022-11-23 04:32:00 EST for 0s
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
```

```
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: 08:00:27:C6:DE:4F (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.52 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

Version detection

La version detection scan ci restituisce invece come risultato una ricerca più raffinata riconoscendo versione e nome del servizio RPC (Remote procedure call), determinando programma e versione in esecuzione.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap  -vvv -sV  192.168.1.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 04:40 EST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 04:40
Scanning 192.168.1.10 [2 ports]
Completed Ping Scan at 04:40, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:40
Completed Parallel DNS resolution of 1 host. at 04:40, 13.03s elapsed
DNS resolution of 1 IPs took 13.03s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 04:40
Scanning 192.168.1.10 [1000 ports]
Discovered open port 25/tcp on 192.168.1.10
Discovered open port 5900/tcp on 192.168.1.10
Discovered open port 23/tcp on 192.168.1.10
Discovered open port 21/tcp on 192.168.1.10
Discovered open port 80/tcp on 192.168.1.10
Discovered open port 139/tcp on 192.168.1.10
Discovered open port 445/tcp on 192.168.1.10
Discovered open port 111/tcp on 192.168.1.10
Discovered open port 3306/tcp on 192.168.1.10
Discovered open port 22/tcp on 192.168.1.10
Discovered open port 53/tcp on 192.168.1.10
Discovered open port 5432/tcp on 192.168.1.10
Discovered open port 1524/tcp on 192.168.1.10
Discovered open port 2049/tcp on 192.168.1.10
Discovered open port 1099/tcp on 192.168.1.10
Discovered open port 8009/tcp on 192.168.1.10
Discovered open port 514/tcp on 192.168.1.10
Discovered open port 6000/tcp on 192.168.1.10
Discovered open port 6667/tcp on 192.168.1.10
Discovered open port 513/tcp on 192.168.1.10
Discovered open port 8180/tcp on 192.168.1.10
Discovered open port 2121/tcp on 192.168.1.10
Discovered open port 512/tcp on 192.168.1.10
Completed Connect Scan at 04:40, 0.11s elapsed (1000 total ports)
Initiating Service scan at 04:40
Scanning 23 services on 192.168.1.10
Completed Service scan at 04:41, 36.18s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.1.10.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 04:41
Completed NSE at 04:41, 8.09s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 04:41
Completed NSE at 04:41, 8.04s elapsed
Nmap scan report for 192.168.1.10
Host is up, received syn-ack (0.00047s latency).
Scanned at 2022-11-23 04:40:59 EST for 53s
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     REASON  VERSION
21/tcp   open  ftp         syn-ack vsftpd 2.3.4
```

```
Discovered open port 512/tcp on 192.168.1.10
Completed Connect Scan at 04:40, 0.11s elapsed (1000 total ports)
Initiating Service scan at 04:40
Scanning 23 services on 192.168.1.10
Completed Service scan at 04:41, 36.18s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.1.10.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 04:41
Completed NSE at 04:41, 8.09s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 04:41
Completed NSE at 04:41, 8.04s elapsed
Nmap scan report for 192.168.1.10
Host is up, received syn-ack (0.00047s latency).
Scanned at 2022-11-23 04:40:59 EST for 53s
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     REASON  VERSION
21/tcp   open  ftp         syn-ack vsftpd 2.3.4
22/tcp   open  ssh         syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      syn-ack Linux telnetd
25/tcp   open  smtp        syn-ack Postfix smtpd
53/tcp   open  domain      syn-ack ISC BIND 9.4.2
80/tcp   open  http        syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     syn-ack 2 (RPC #100000)
139/tcp  open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        syn-ack netkit-rsh rexecd
513/tcp  open  login?      syn-ack
514/tcp  open  shell       syn-ack Netkit rshd
1099/tcp open  java-rmi    syn-ack GNU Classpath grmiregistry
1524/tcp open  bindshell   syn-ack Metasploitable root shell
2049/tcp open  nfs         syn-ack 2-4 (RPC #100003)
2121/tcp open  ftp         syn-ack ProFTPD 1.3.1
3306/tcp open  mysql       syn-ack MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  syn-ack PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         syn-ack VNC (protocol 3.3)
6000/tcp open  X11         syn-ack (access denied)
6667/tcp open  irc         syn-ack UnrealIRCd
8009/tcp open  ajp13       syn-ack Apache Jserv (Protocol v1.3)
8180/tcp open  http        syn-ack Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.12 seconds
```

WINDOWS 7

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.32.100
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 06:24 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.23 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 192.168.32.100
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 06:24 EST
Nmap scan report for 192.168.32.100
Host is up (0.054s latency).
All 1000 scanned ports on 192.168.32.100 are in ignored states.
Not shown: 990 filtered tcp ports (no-response), 10 filtered tcp ports (host-unreach)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.62 seconds

┌──(kali㉿kali)-[~]
└─$
```

La scansione ovviamente non può ottenere riscontro poiché i firewall di Windows sono operativi.

Cambiando le impostazioni Firewall invece il risultato dello scan ottenuto sarà dettagliata in modo seguente

```
└─$ sudo nmap -O -vvv  192.168.32.101
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 08:07 EST
Initiating ARP Ping Scan at 08:07
Scanning 192.168.32.101 [1 port]
Completed ARP Ping Scan at 08:07, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:07
Completed Parallel DNS resolution of 1 host. at 08:07, 13.02s elapsed
DNS resolution of 1 IPs took 13.02s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 08:07
Scanning 192.168.32.101 [1000 ports]
Discovered open port 139/tcp on 192.168.32.101
Discovered open port 49156/tcp on 192.168.32.101
Discovered open port 49153/tcp on 192.168.32.101
Discovered open port 49154/tcp on 192.168.32.101
Discovered open port 5357/tcp on 192.168.32.101
Discovered open port 135/tcp on 192.168.32.101
Discovered open port 445/tcp on 192.168.32.101
Discovered open port 49155/tcp on 192.168.32.101
Discovered open port 49152/tcp on 192.168.32.101
Discovered open port 49157/tcp on 192.168.32.101
Completed SYN Stealth Scan at 08:07, 1.29s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.32.101
Nmap scan report for 192.168.32.101
Host is up, received arp-response (0.00091s latency).
Scanned at 2022-11-23 08:07:49 EST for 3s
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack ttl 128
139/tcp   open  netbios-ssn  syn-ack ttl 128
445/tcp   open  microsoft-ds syn-ack ttl 128
5357/tcp  open  wsdapi       syn-ack ttl 128
49152/tcp open  unknown      syn-ack ttl 128
49153/tcp open  unknown      syn-ack ttl 128
49154/tcp open  unknown      syn-ack ttl 128
49155/tcp open  unknown      syn-ack ttl 128
49156/tcp open  unknown      syn-ack ttl 128
49157/tcp open  unknown      syn-ack ttl 128
MAC Address: 08:00:27:4E:5F:39 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=11/23%OT=135%CT=1%CU=36258%PV=Y%DS=1%DC=D%G=N%M=080027
OS:%TM=637E1B28%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=104%TI=I%CI=I%II
OS:=I%SS=S%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW
OS:8ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=
OS:2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T
OS:=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T
OS:3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O
OS:%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=
```