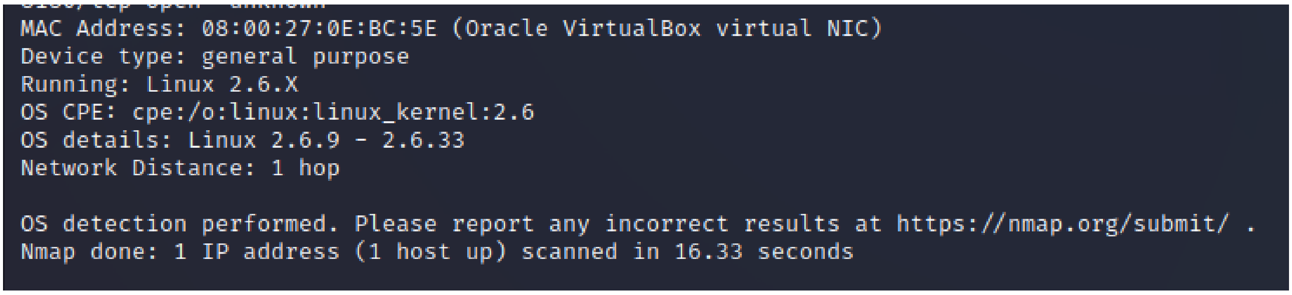
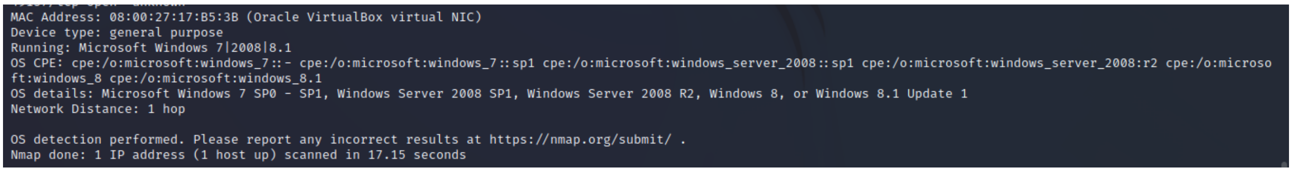
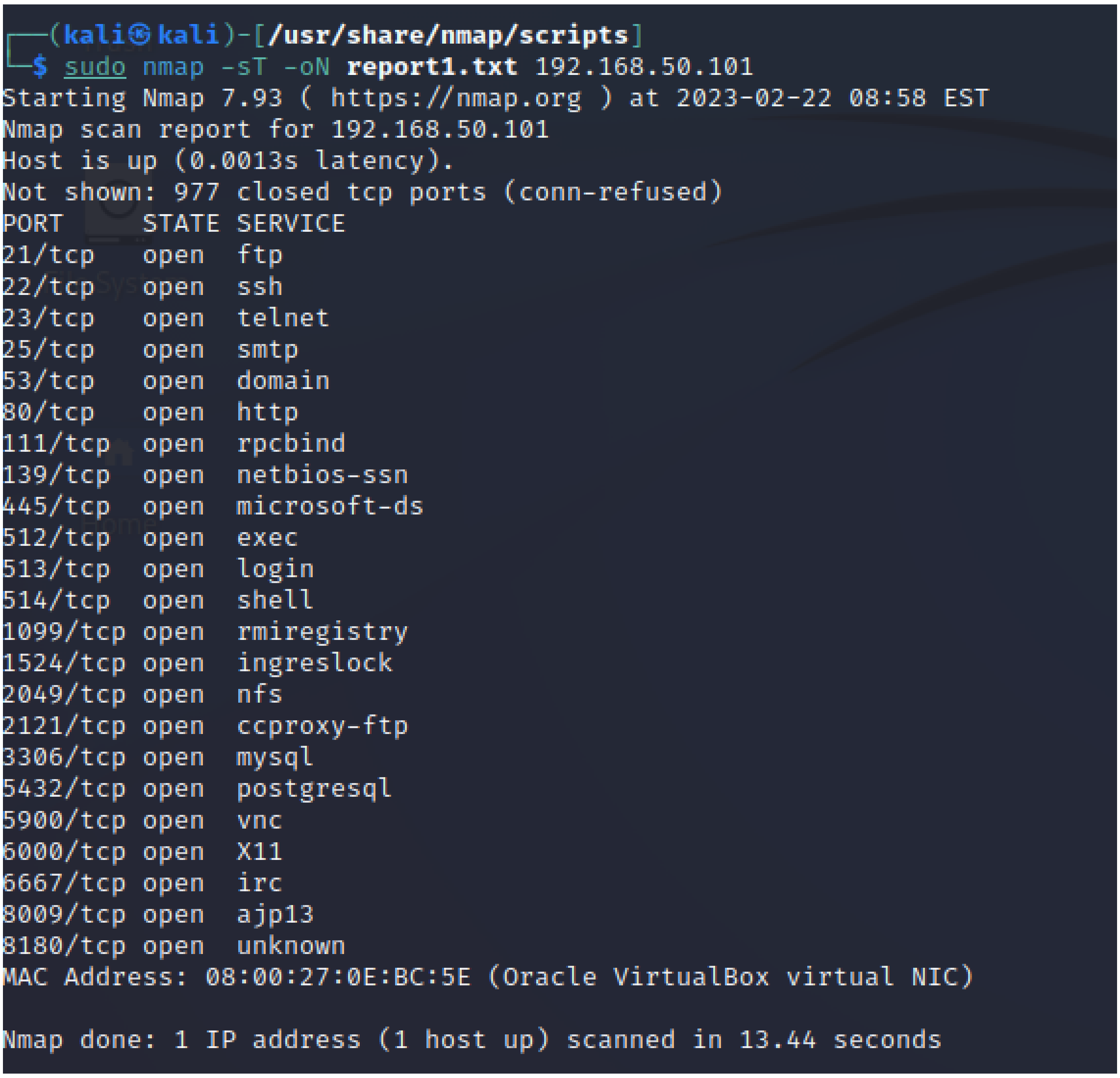


```
MAC Address: 08:00:27:0E:BC:5E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.33 seconds
```

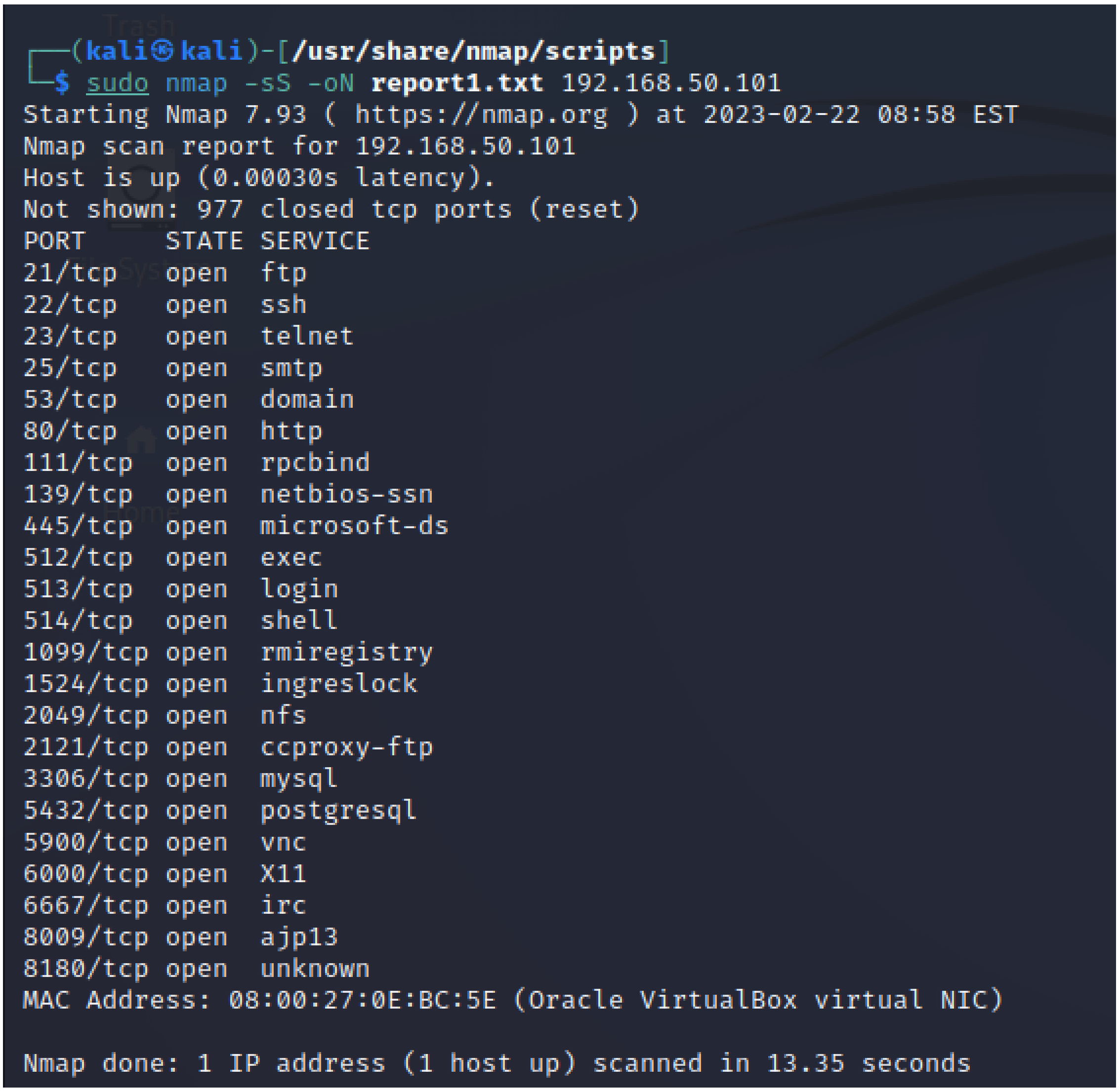


```
MAC Address: 08:00:27:17:B5:3B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microso
ft: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
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 17.15 seconds
```

Con il comando nmap –O ho capito il sistema operativo tramite l ip. La prima macchina, come si puo vedere dalle caratteristiche trovate, e meta, mentre la seconda e windows.



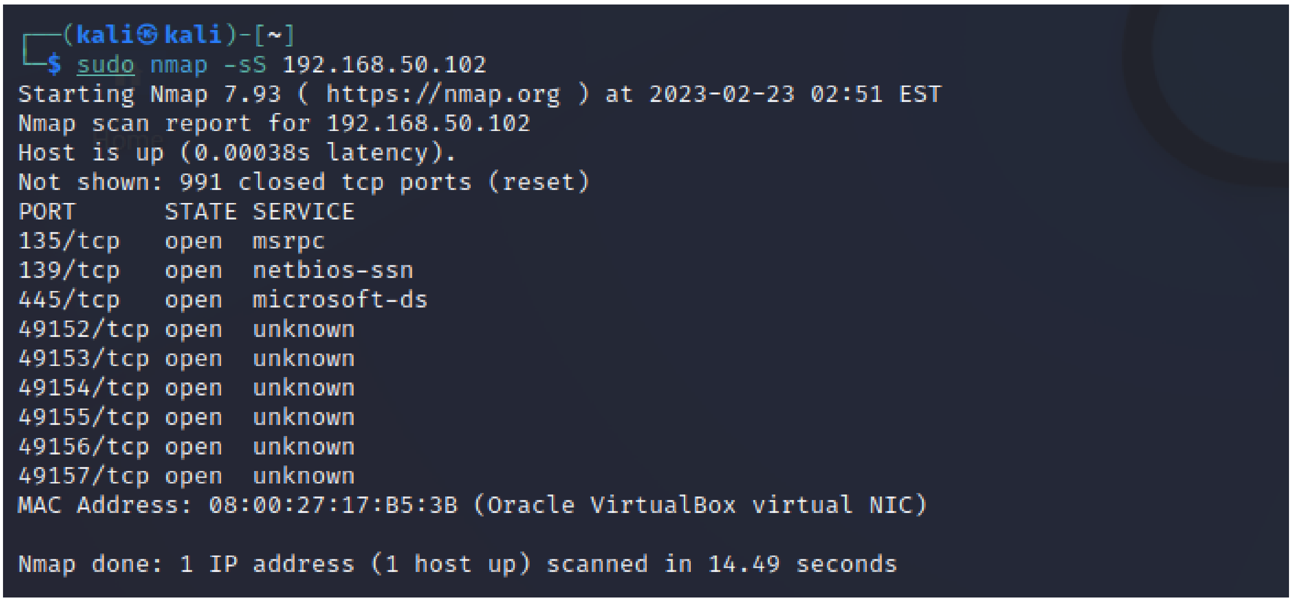
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sT -oN report1.txt 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 08:58 EST
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   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: 08:00:27:0E:BC:5E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sS -oN report1.txt 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 08:58 EST
Nmap scan report for 192.168.50.101
Host is up (0.00030s 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: 08:00:27:0E:BC:5E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
```

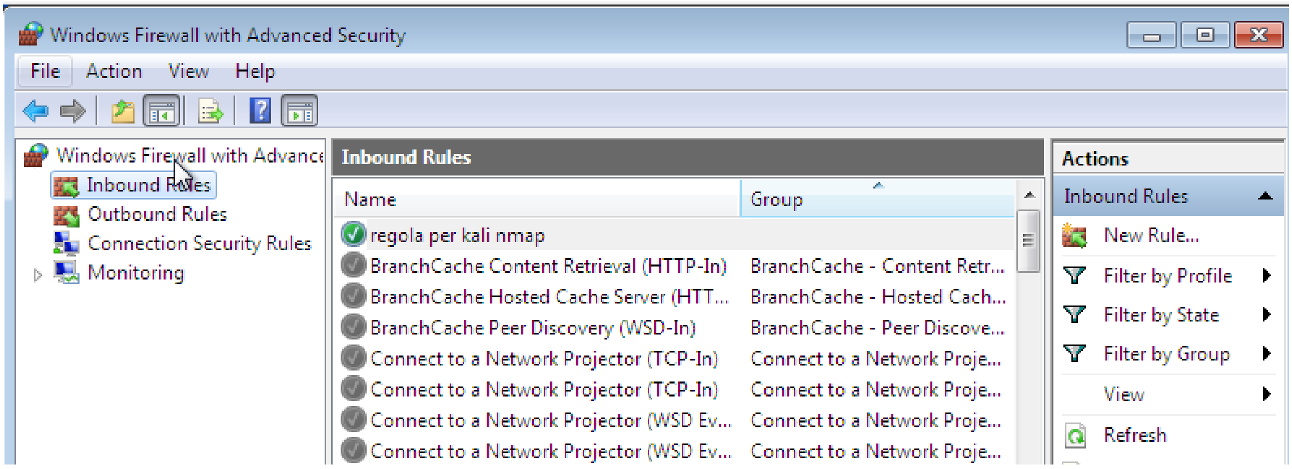
Queste sono le porta aperte di meta, nel primo caso ho usato il tipo di scansione piu ivasiva (full tcp) dove viene chiuso il 3 way hand shake mentre con il secondo (syn)controlliamo solo se alla prima richiesta syn, otteniamo una risposta (il che significa che la porta e aperta) ma non chiudiamo la 3 way hand shake rimandando il valore indietro alla porta.

La differenza difatti e che come risposta alla comunicazione invasiva nmap ci da come risultato connn refused, perche chiudiamo la connessione e giustamente viene rifiutata, mentre nel caso della comunicazione meno invasiva come risposta nmap ci da ‘reset’, non avenmdo chiuso la comunicazione.



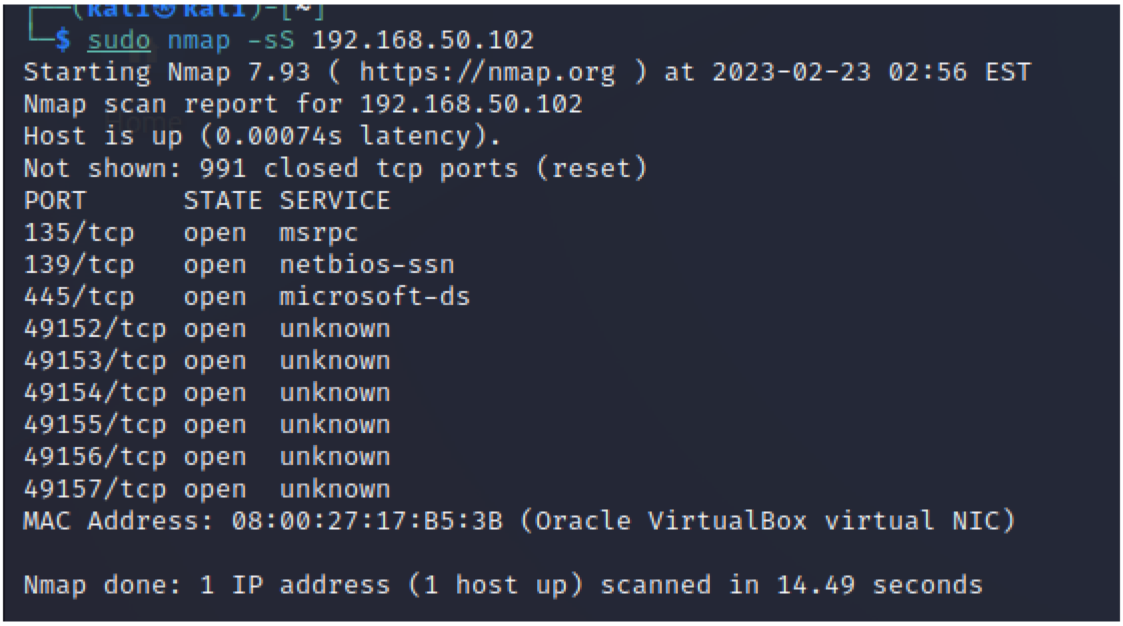
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 02:51 EST
Nmap scan report for 192.168.50.102
Host is up (0.00038s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:17:B5:3B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.49 seconds
```

Queste sono le porte aperte su windows, che ovviamente sono di meno essendo protetta da un firewall, non come la macchina metasploitable realizzata pposta vulnerabile.



Inbound Rules

Name	Group
✓ regola per kali nmap	
✓ BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...
✓ BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...
✓ BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...
✓ Connect to a Network Projector (TCP-In)	Connect to a Network Proje...
✓ Connect to a Network Projector (TCP-In)	Connect to a Network Proje...
✓ Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
✓ Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 02:56 EST
Nmap scan report for 192.168.50.102
Host is up (0.00074s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:17:B5:3B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.49 seconds
```

Ho provato ad impostare una regola firewall su windows che lasciasse entrare comunicazioni tcp su tutte le porte, ma il risultato e uguale perche e presente un altro firewall.