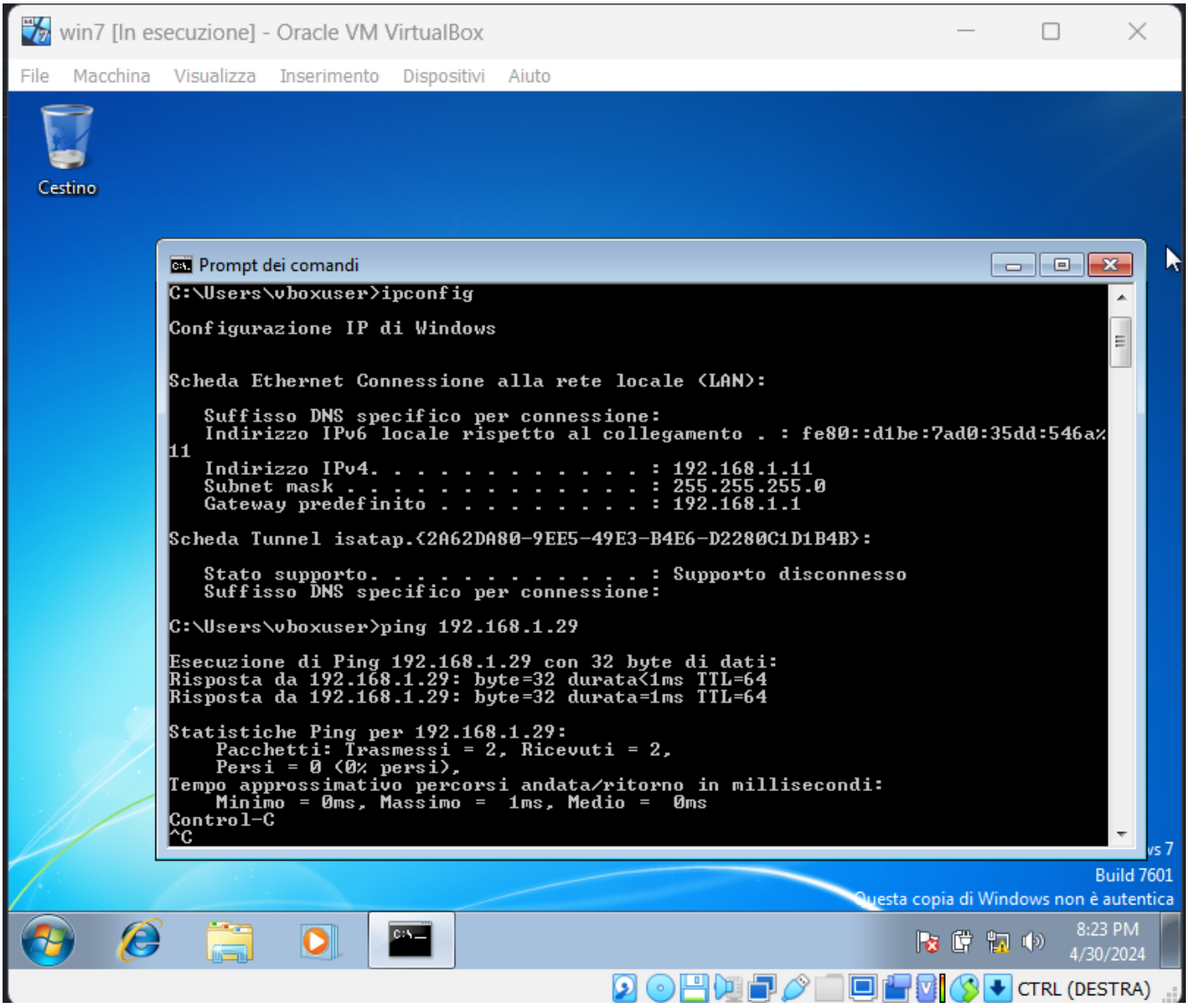
W11D2

win 7 (192.168.1.29) ping su kali

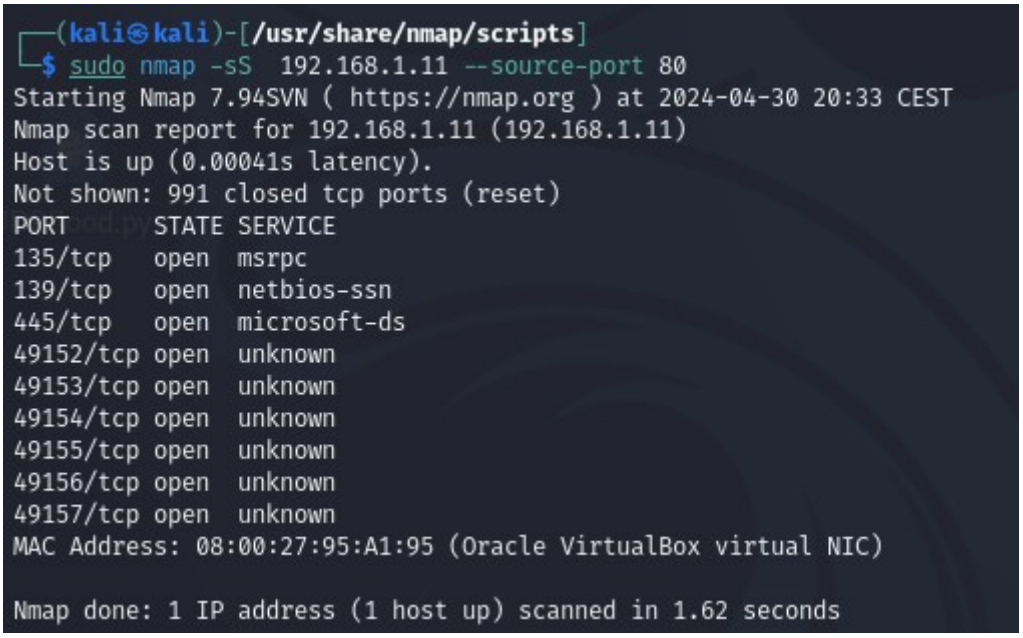


kali (192.168.1.29)ping su win7

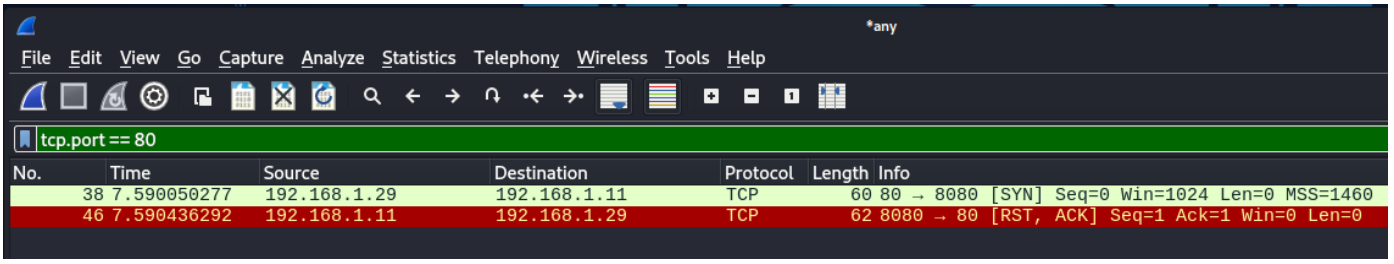
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=1 ttl=128 time=1.15 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=128 time=0.670 ms
64 bytes from 192.168.1.11: icmp_seq=3 ttl=128 time=0.670 ms
^C
── 192.168.1.11 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.670/0.829/1.149/0.225 ms
```

OS fingerprint con -O

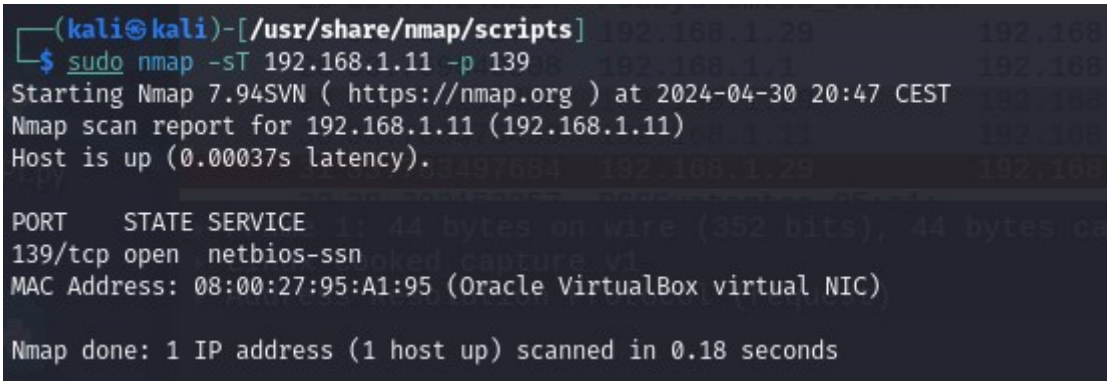
syn

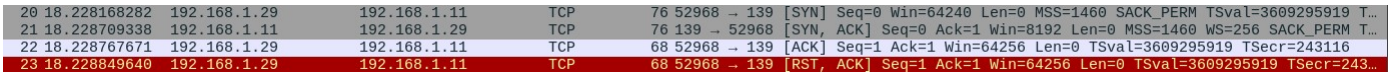


wireshark



porta aperta -sT





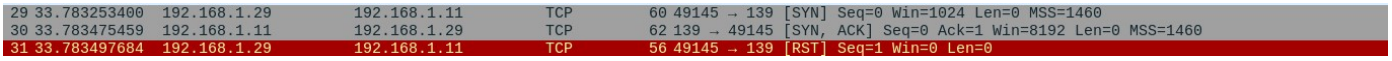
aspetta ACK

porta aperta -sS

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sS 192.168.1.11 -p 139
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 20:47 CEST
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00029s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 08:00:27:95:A1:95 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```



non aspetta ACK

con-sV versione

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sV 192.168.1.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 20:57 CEST
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00083s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:95:A1:95 (Oracle VirtualBox virtual NIC)
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.77 seconds
```

script win7 ci mostra il sistema operativo

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap 192.168.1.11 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 20:08 CEST
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00078s latency).
Not shown: 991 closed tcp ports (conn-refused)
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

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: win7
|   NetBIOS computer name: WIN7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-04-30T20:09:03+02:00

Nmap done: 1 IP address (1 host up) scanned in 6.17 seconds
```

APRIAMO IL FIREWALL su win7

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sV 192.168.1.11 --source-port 80 --top-ports 10

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 21:42 CEST
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00029s latency).

PORT     STATE    SERVICE       VERSION
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server
MAC Address: 08:00:27:95:A1:95 (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 1.92 seconds

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap 192.168.1.11 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 21:44 CEST
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00049s latency).
All 1000 scanned ports on 192.168.1.11 (192.168.1.11) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:95:A1:95 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 24.10 seconds
```

vediamo che le top ports sono filtrate quindi il firewall è attivo