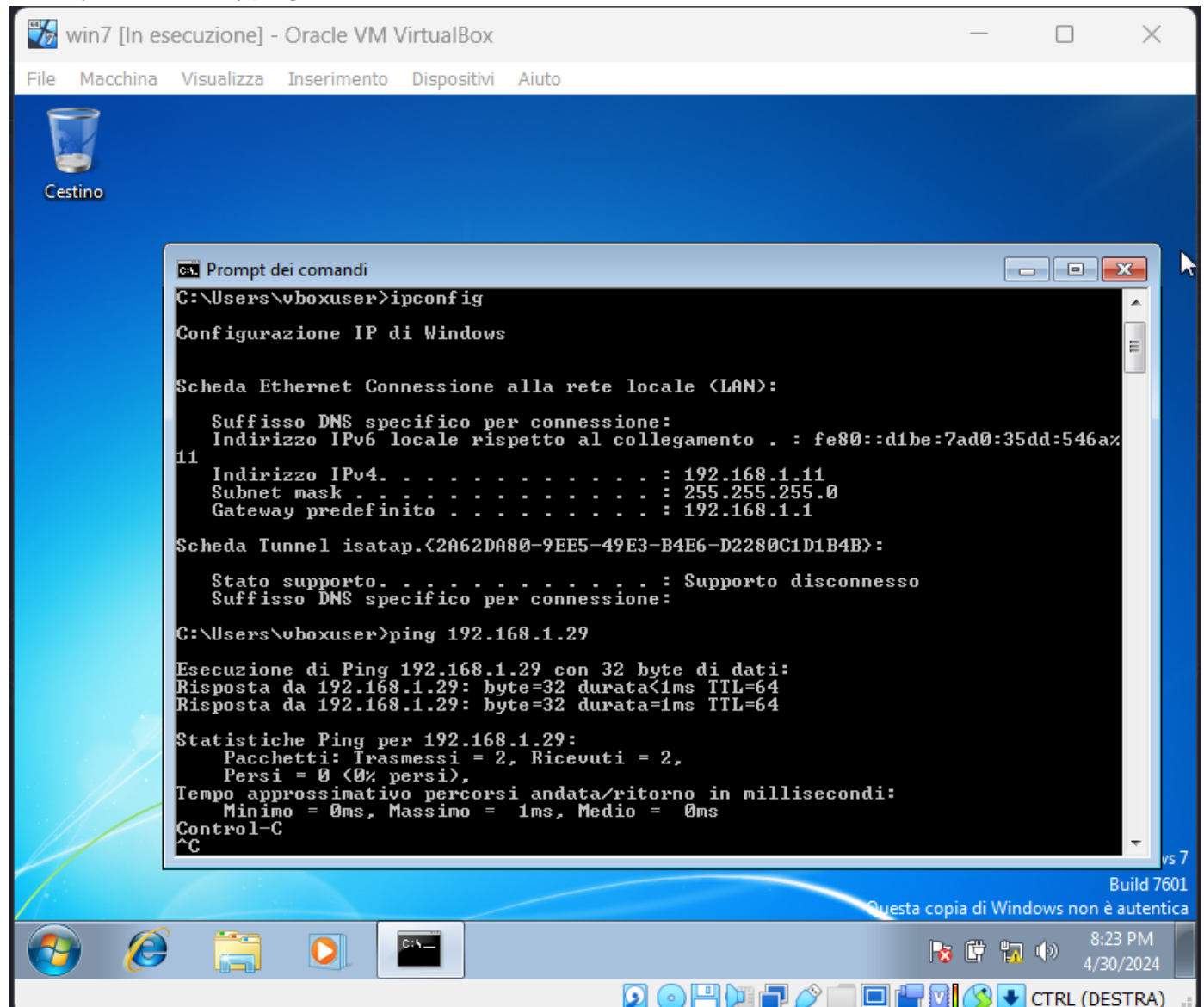


W11D2

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

```

(kali@kali)-[/usr/share/nmap/scripts]
$ sudo nmap -O --scan-limit 192.168.1.11
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 20:28 CEST
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00068s 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: 08:00:27:95:A1:95 (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_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
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 3.03 seconds

```

syn

```

(kali@kali)-[/usr/share/nmap/scripts]
$ sudo nmap -sS 192.168.1.11 --source-port 80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 20:33 CEST
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00041s 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: 08:00:27:95:A1:95 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds

```

wireshark

*any						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp.port == 80						
No.	Time	Source	Destination	Protocol	Length	Info
38	7.590050277	192.168.1.29	192.168.1.11	TCP	60	80 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46	7.590436292	192.168.1.11	192.168.1.29	TCP	62	8080 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

porta aperta -sT

```

(kali@kali)-[/usr/share/nmap/scripts]
$ sudo nmap -sT 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 (0.00037s 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 0.18 seconds

```

20	18.228168282	192.168.1.29	192.168.1.11	TCP	76 52968 → 139	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3609295919 T...
21	18.228709338	192.168.1.11	192.168.1.29	TCP	76 139 → 52968	[SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM T...
22	18.228767671	192.168.1.29	192.168.1.11	TCP	68 52968 → 139	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3609295919 TSecr=243116
23	18.228849640	192.168.1.29	192.168.1.11	TCP	68 52968 → 139	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3609295919 TSecr=243...

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
```

29	33.783253400	192.168.1.29	192.168.1.11	TCP	60 49145 → 139	[SYN] Seq=0 Win=1024 Len=0 MSS=1460
30	33.783475459	192.168.1.11	192.168.1.29	TCP	62 139 → 49145	[SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
31	33.783497684	192.168.1.29	192.168.1.11	TCP	56 49145 → 139	[RST] Seq=1 Win=0 Len=0

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