S5L2

Traccia: Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target (Metasploitable):

● OS fingerprint.

● Syn Scan.

● TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?

●Version detection.

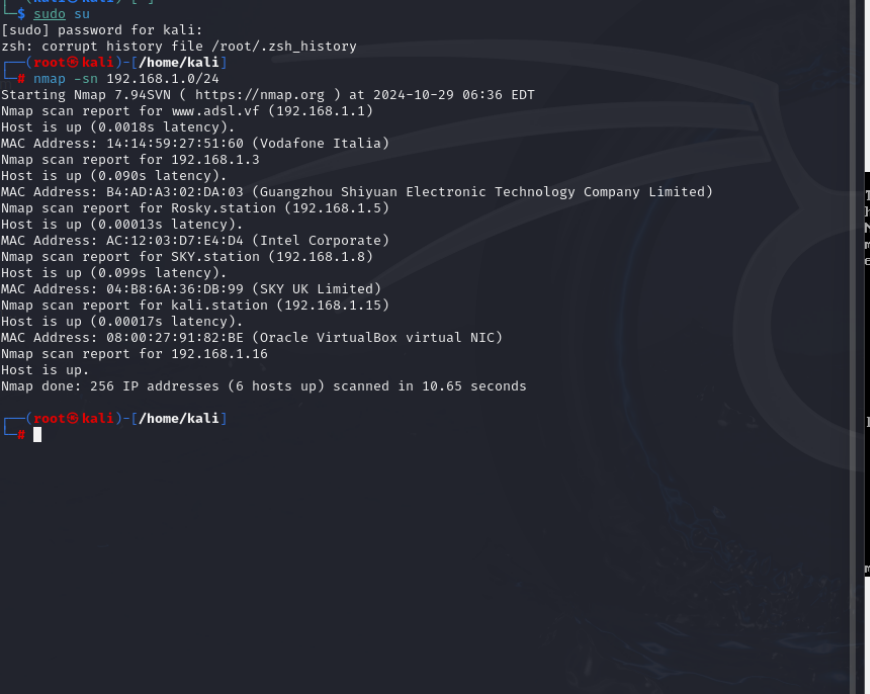
E la seguente sul target

Windows: ● OS fingerprint.

Ho trovato con nmap -sn per scannerizare il network e L'esercizio ha come target Metasploitable2 (e Windows per extra). Per iniziare a mappare la rete ho usato il comando `-A (192.168.1.15)` per una scansione aggressiva su Metasploitable2, ottenendo informazioni dettagliate su versioni dei servizi. A seguire ho provato tutti i comandi per trovare ulteriori informazioni. Il comando `nmap -O` per fare OS Fingerprinting su, rilevando porte aperte e identificando il sistema operativo come Linux 2.6.x. a seguire un SYN scan con `nmap -sS`, identificando diverse porte aperte con servizi attivi. A seguire uno scan TCP connect con `nmap -sT`. Questo tipo di scansione stabilisce una connessione completa con ogni porta per identificare quelle aperte e a finire un OS con `nmap -sV`. Questo tipo di scansione non solo identifica le porte aperte, ma determina anche la versione specifica dei servizi attivi, completando l'esercizio. Ho eseguito come extra nmap -Pn per trovare porte aperte e vulnerabilità da sfruttare.

Nessuna differenza tra TCP connect e SYN (una è stealthy, l'altra aggressiva e crea una handshake completo)

(Come extra fatto anche su Windows)



```
└─$ sudo su
[sudo] password for kali:
zsh: corrupt history file /root/.zsh_history
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 06:36 EDT
Nmap scan report for www.adsl.vf (192.168.1.1)
Host is up (0.0018s latency).
MAC Address: 14:14:59:27:51:60 (Vodafone Italia)
Nmap scan report for 192.168.1.3
Host is up (0.090s latency).
MAC Address: B4:AD:A3:02:DA:03 (Guangzhou Shiyuan Electronic Technology Company Limited)
Nmap scan report for Rosky.station (192.168.1.5)
Host is up (0.00013s latency).
MAC Address: AC:12:03:D7:E4:D4 (Intel Corporate)
Nmap scan report for SKY.station (192.168.1.8)
Host is up (0.099s latency).
MAC Address: 04:B8:6A:36:DB:99 (SKY UK Limited)
Nmap scan report for kali.station (192.168.1.15)
Host is up (0.00017s latency).
MAC Address: 08:00:27:91:82:BE (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.16
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 10.65 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:91:82:be
          inet addr:192.168.1.15  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe91:82be/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:671 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:48457 (47.3 KB)  TX bytes:9995 (9.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:100 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23481 (22.9 KB)  TX bytes:23481 (22.9 KB)

msfadmin@metasploitable:~$ _
```

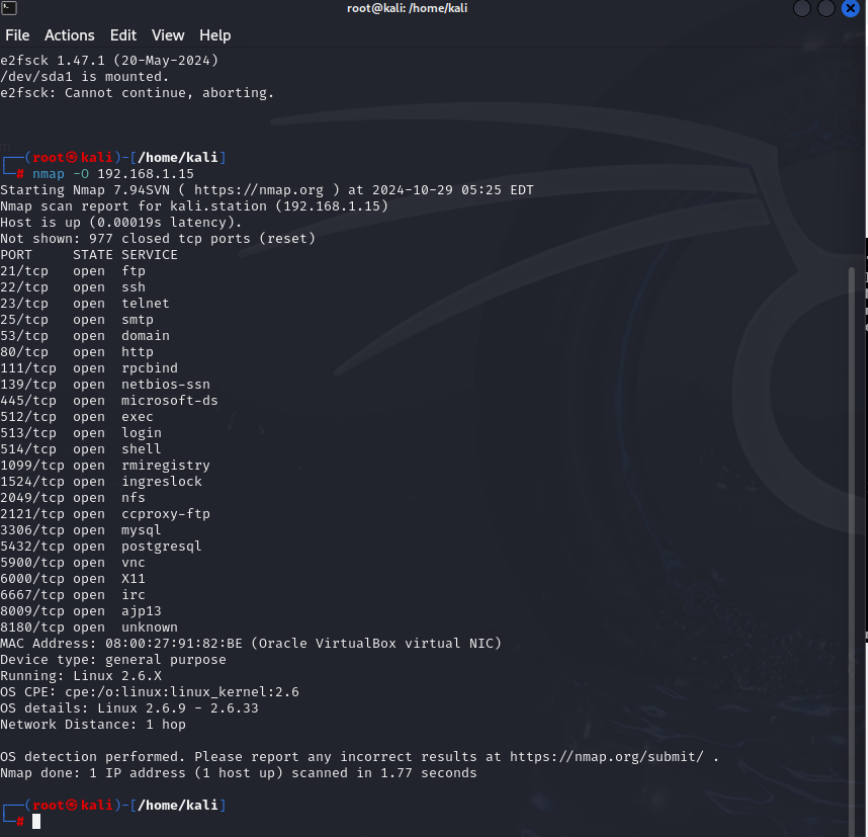
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 05:41 EDT
Nmap scan report for kali.station (192.168.1.15)
Host is up (0.00022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.16
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2024-10-29T09:42:41+00:00; +47s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDST
ATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=Th
ere is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

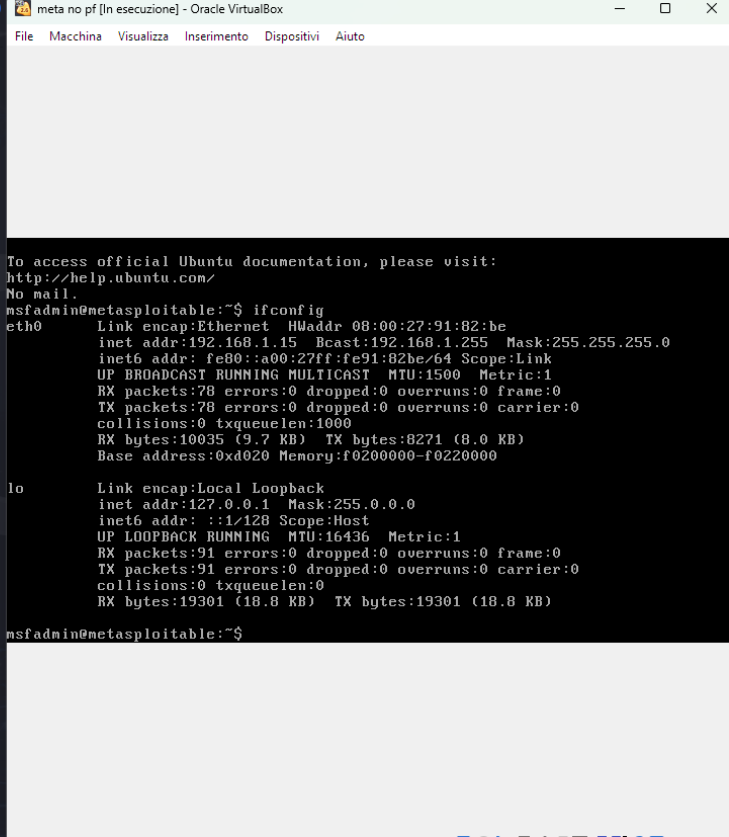
```
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      50346/tcp   mountd
|   100005  1,2,3      51572/udp   mountd
|   100021  1,3,4      53907/tcp   nlockmgr
|   100021  1,3,4      54226/udp   nlockmgr
|   100024  1          46390/udp   status
|_  100024  1          55385/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 11
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsCompression, SupportsTransactions, SwitchToSSLAfterHandsha
ke, LongColumnFlag, ConnectWithDatabase, Speaks41ProtocolNew
|   Status: Autocommit
|_  Salt: !/jJqy/z=\9F4pZSp[X&
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=Th
ere is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-10-29T09:42:40+00:00; +46s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
```

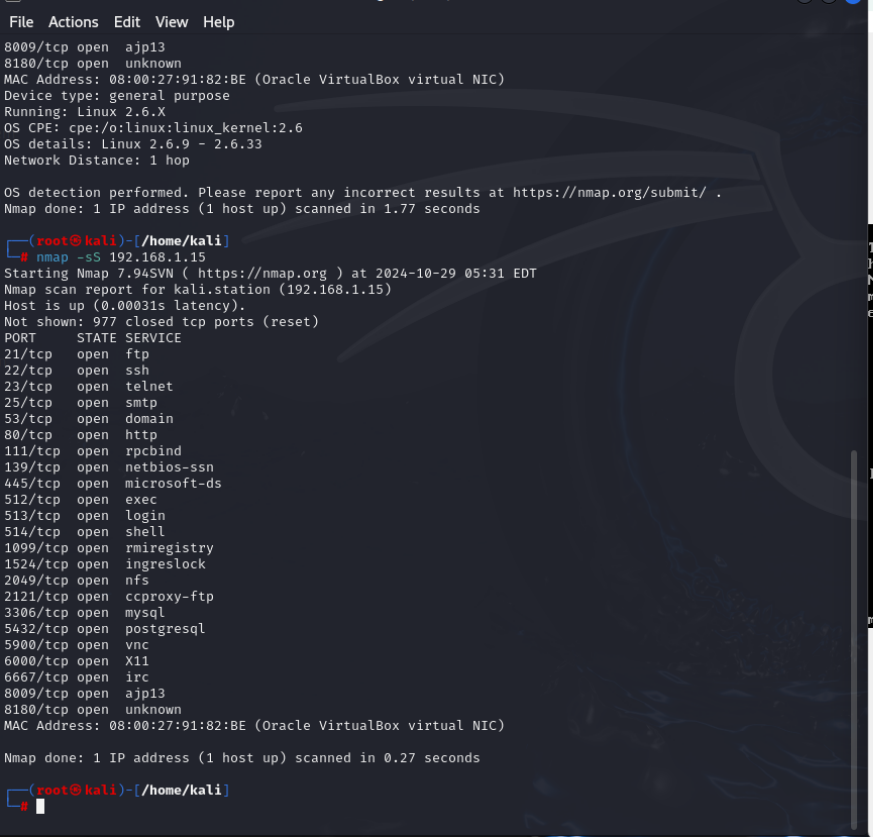
```
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:20:23
|   source ident: nmap
|   source host: 94098BA5.78DED367.FFFA6D49.IP
|_  error: Closing Link: irkmqcnrg[192.168.1.16] (Quit: irkmqcnrg)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:91:82:BE (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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:
linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-10-29T05:42:32-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h00m46s, deviation: 2h00m00s, median: 45s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.22 ms kali.station (192.168.1.15)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.88 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

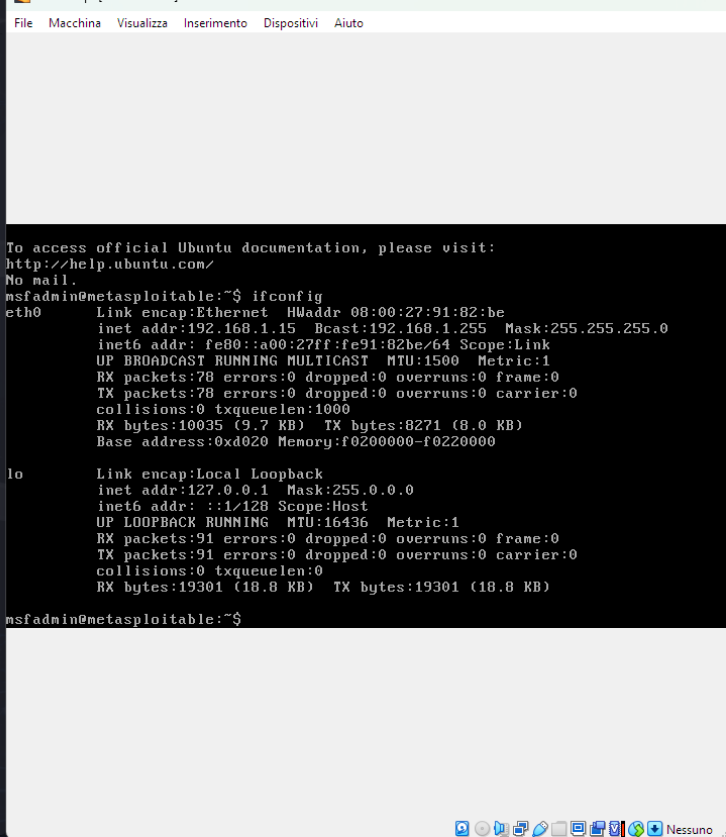
```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:91:82:be
          inet addr:192.168.1.15  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe91:82be/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10035 (9.7 KB)  TX bytes:8271 (8.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

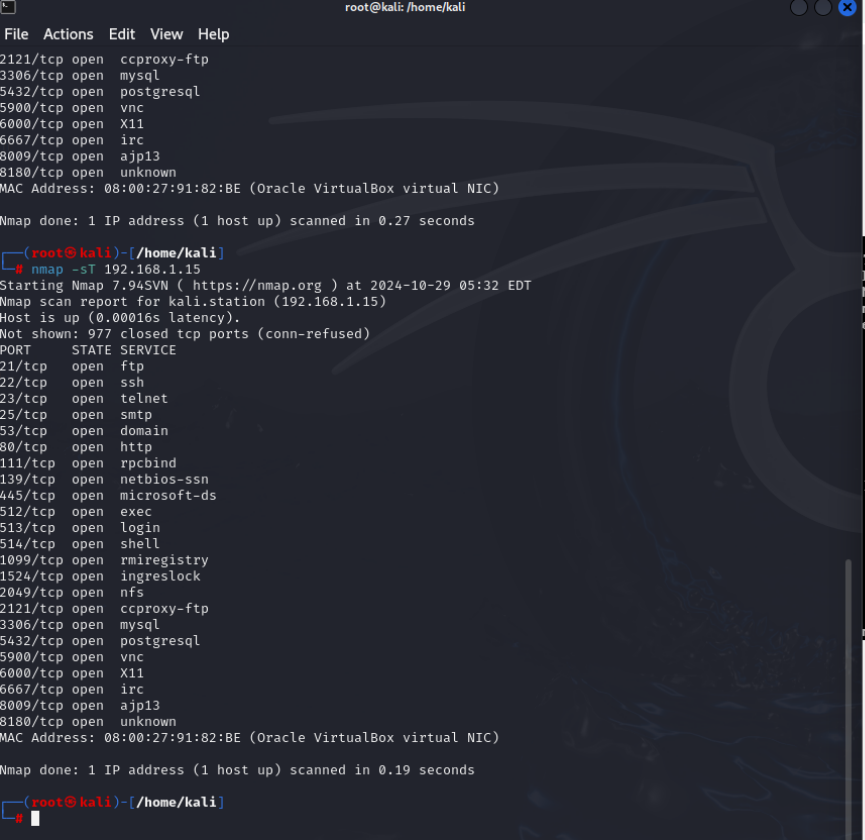
Nessuno

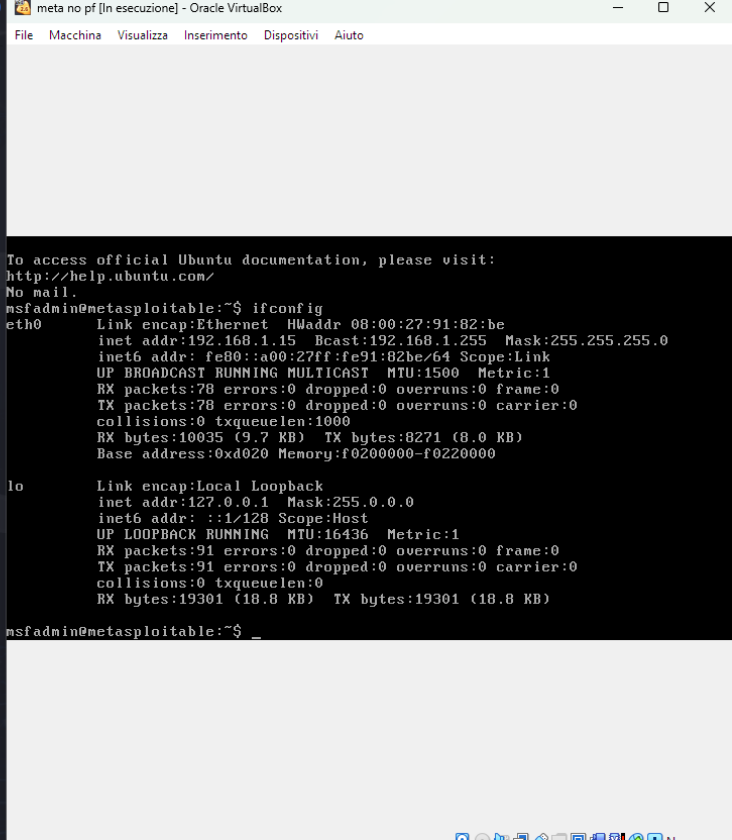

root@kali: /home/kali
File Actions Edit View Help
e2fsck 1.47.1 (20-May-2024)
/dev/sda1 is mounted.
e2fsck: Cannot continue, aborting.
(root㉿kali)-[/home/kali]
nmap -O 192.168.1.15
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-29 05:25 EDT
Nmap scan report for kali.station (192.168.1.15)
Host is up (0.00019s 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: 08:00:27:91:82:BE (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 1.77 seconds
(root㉿kali)-[/home/kali]
#


meta no pf [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:91:82:be
inet addr:192.168.1.15 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe91:82be/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:78 errors:0 dropped:0 overruns:0 frame:0
TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10035 (9.7 KB) TX bytes:8271 (8.0 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)
msfadmin@metasploitable:~$


File Actions Edit View Help
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:91:82:BE (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 1.77 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.15
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-29 05:31 EDT
Nmap scan report for kali.station (192.168.1.15)
Host is up (0.00031s 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: 08:00:27:91:82:BE (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
┌──(root㉿kali)-[/home/kali]
└─#


File Macchina Visualizza Inserimento Dispositivi Aiuto
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:91:82:be
inet addr:192.168.1.15 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe91:82be/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:78 errors:0 dropped:0 overruns:0 frame:0
TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10035 (9.7 KB) TX bytes:8271 (8.0 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)
msfadmin@metasploitable:~$
Nessuno


root@kali: /home/kali
File Actions Edit View Help
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: 08:00:27:91:82:BE (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
(root㉿kali)-[/home/kali]
nmap -sT 192.168.1.15
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-29 05:32 EDT
Nmap scan report for kali.station (192.168.1.15)
Host is up (0.00016s 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: 08:00:27:91:82:BE (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
(root㉿kali)-[/home/kali]
#


meta no pf [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:91:82:be
inet addr:192.168.1.15 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe91:82be/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:78 errors:0 dropped:0 overruns:0 frame:0
TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10035 (9.7 KB) TX bytes:8271 (8.0 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)
msfadmin@metasploitable:~$

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 05:32 EDT
Nmap scan report for kali.station (192.168.1.15)
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:91:82:BE (Oracle VirtualBox virtual NIC)
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 11.64 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:91:82:be
          inet addr:192.168.1.15  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe91:82be/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10035 (9.7 KB)  TX bytes:8271 (8.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ _
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 07:05 EDT
Nmap scan report for kali.station (192.168.1.15)
Host is up (0.0013s 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: 08:00:27:91:82:BE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:91:82:be
          inet addr:192.168.1.15  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe91:82be/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:388 errors:0 dropped:0 overruns:0 frame:0
          TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32469 (31.7 KB)  TX bytes:14836 (14.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:163 errors:0 dropped:0 overruns:0 frame:0
          TX packets:163 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:54417 (53.1 KB)  TX bytes:54417 (53.1 KB)

msfadmin@metasploitable:~$ _
```

```
P Configuration

adapter Ethernet:

State . . . . . : Media disconnected
tion-specific DNS Suffix  . :

LAN adapter Connessione alla rete locale (LAN)* 1:

State . . . . . : Media disconnected
tion-specific DNS Suffix  . :

LAN adapter Connessione alla rete locale (LAN)* 10:

State . . . . . : Media disconnected
tion-specific DNS Suffix  . :

LAN adapter Wi-Fi:

tion-specific DNS Suffix  . : station
ocal IPv6 Address . . . . . : fe80::c317:a351:7a6d:1c9f%11
ddress. . . . . : 192.168.1.5
 Mask . . . . . : 255.255.255.0
t Gateway . . . . . : 192.168.1.1

adapter vEthernet (Default Switch):

tion-specific DNS Suffix  . :
ocal IPv6 Address . . . . . : fe80::6b71:9b7:c5e1:708b%32
ddress. . . . . : 172.19.208.1
 Mask . . . . . : 255.255.240.0
t Gateway . . . . . :

panze>
```

```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ^[[200~nmap -sn per scannerizare~
zsh: bad pattern: ^[[200~nmap

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 07:36 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.00 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 07:36 EDT
Nmap scan report for www.adsl.vf (192.168.1.1)
Host is up (0.0018s latency).
MAC Address: 14:14:59:27:51:60 (Vodafone Italia)
Nmap scan report for 192.168.1.3
Host is up (0.067s latency).
MAC Address: B4:AD:A3:02:DA:03 (Guangzhou Shiyuan Electronic Technology Company Limited)
Nmap scan report for Rosky.station (192.168.1.5)
Host is up (0.00015s latency).
MAC Address: AC:12:03:D7:E4:D4 (Intel Corporate)
Nmap scan report for SKY.station (192.168.1.8)
Host is up (0.087s latency).
MAC Address: 04:B8:6A:36:DB:99 (SKY UK Limited)
Nmap scan report for DESKTOP-9K1O4BT.station (192.168.1.17)
Host is up (0.013s latency).
MAC Address: 08:00:27:D6:06:50 (Oracle VirtualBox virtual NIC)
Nmap scan report for METASPLOITABLE.station (192.168.1.16)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 3.35 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 05:39 EDT
Nmap scan report for Rosky.station (192.168.1.5)
Host is up (0.00028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
135/tcp  open  msrpc   Microsoft Windows RPC
2179/tcp open  vmrdp?
MAC Address: AC:12:03:D7:E4:D4 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11 (89%)
Aggressive OS guesses: Microsoft Windows 11 21H2 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.28 ms Rosky.station (192.168.1.5)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.89 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 05:40 EDT


┌──(root㉿kali)-[/home/kali]
└─#
```

```
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Connessione alla rete locale (LAN)* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Connessione alla rete locale (LAN)* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : station
   Link-local IPv6 Address . . . . . : fe80::c317:a351:7a6d:1c9f%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6b71:9b7:c5e1:708b%32
   IPv4 Address. . . . . . . . . . . : 172.19.208.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\Windows\System32>
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 05:35 EDT
Nmap scan report for Rosky.station (192.168.1.5)
Host is up (0.00022s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
MAC Address: AC:12:03:D7:E4:D4 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2022 (92%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows 11 21H2 (92%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (87%), Microsoft Windows Server 2022 (85%)
No exact OS matches for host (test conditions non-ideal).
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 11.96 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Connessione alla rete locale (LAN)* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : station
   Link-local IPv6 Address . . . . . : fe80::c317:a351:7a6d:1c9f%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6b71:9b7:c5e1:708b%32
   IPv4 Address. . . . . . . . . . . : 172.19.208.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\Windows\System32>
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 05:36 EDT
Nmap scan report for Rosky.station (192.168.1.5)
Host is up (0.00017s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
2179/tcp open  vmrdp
MAC Address: AC:12:03:D7:E4:D4 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 6.02 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

```
   Connection-specific DNS Suffix  . : station
   Link-local IPv6 Address . . . . . : fe80::c317:a351:7a6d:1c9f%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6b71:9b7:c5e1:708b%32
   IPv4 Address. . . . . . . . . . . : 172.19.208.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\Windows\System32>ipc
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 05:37 EDT
Nmap scan report for Rosky.station (192.168.1.5)
Host is up (0.00046s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
MAC Address: AC:12:03:D7:E4:D4 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 5.69 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

```
   Connection-specific DNS Suffix  . : station
   Link-local IPv6 Address . . . . . : fe80::c317:a351:7a6d:1c9f%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6b71:9b7:c5e1:708b%32
   IPv4 Address. . . . . . . . . . . : 172.19.208.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\Windows\System32>ipconfig
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 05:37 EDT
Nmap scan report for Rosky.station (192.168.1.5)
Host is up (0.00019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
135/tcp  open  msrpc   Microsoft Windows RPC
2179/tcp open  vmrdp?
MAC Address: AC:12:03:D7:E4:D4 (Intel Corporate)
Service Info: 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 27.13 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

```
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : station
   Link-local IPv6 Address . . . . . : fe80::c317:a351:7a6d:1c9f%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6b71:9b7:c5e1:708b%32
   IPv4 Address. . . . . . . . . . . : 172.19.208.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\Windows\System32>
```