

Report Esercizio 08/01/2025

Scansione servizi Nmap Leonardo Catalano

“La traccia di oggi ci chiede di effettuare una scansione sul target VM Metasploitable, le scansioni da effettuare saranno le seguenti:

- OS fingerprint
- Syn Scan
- TCP connect, trovando le differenze tra TCP connect e SYN
- Version Detection

Per la macchina target VM Windows:

- OS fingerprint

Successivamente alla scansione il report avrà le seguenti informazioni:

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione

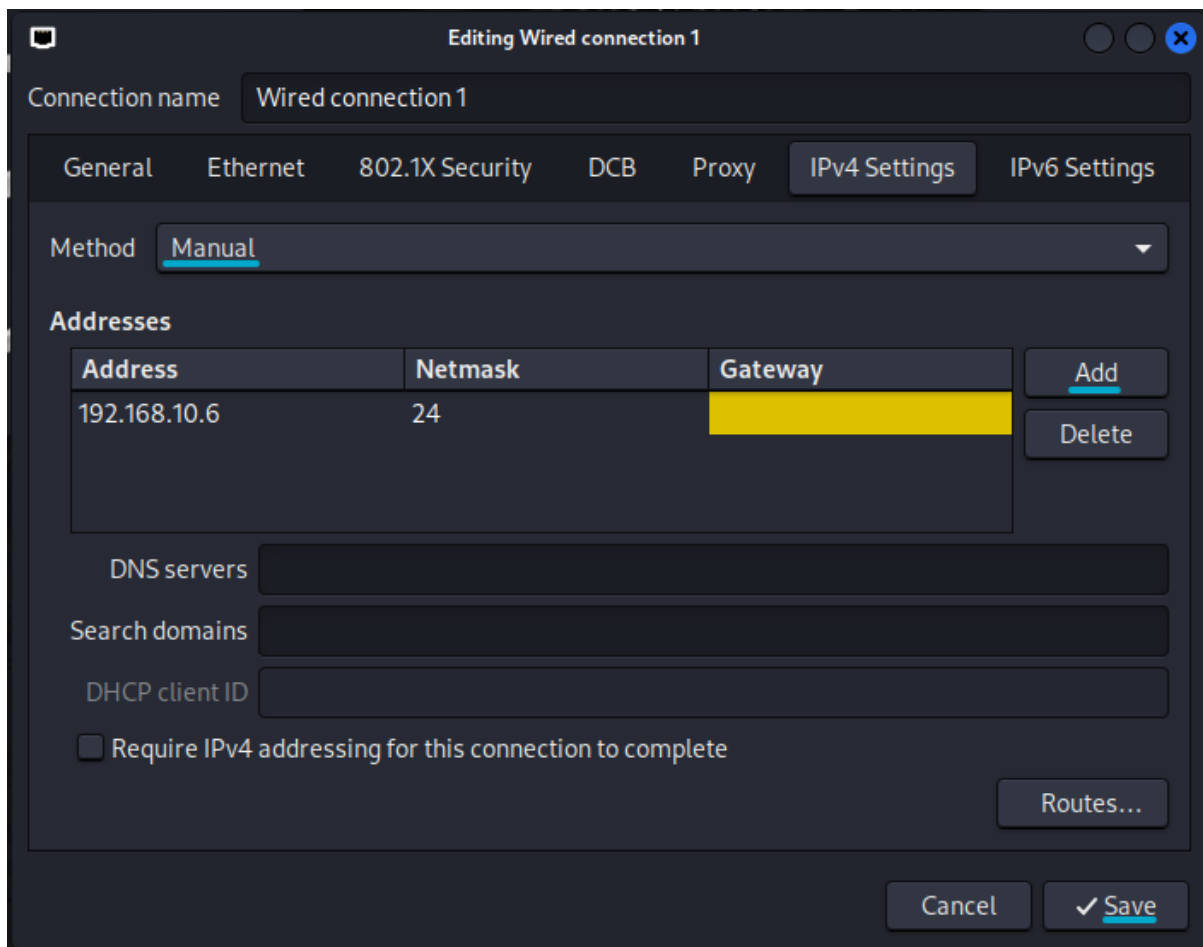
Preconfigurazione macchine virtuali:

Prima di tutto si configurano le VM per farle stare tutte nella stessa rete.

Come indirizzo di rete di riferimento uso il 192.168.10.0 /24.

- Macchina kali linux

Per configurare l'indirizzo ipv4, si aprono le impostazioni della connessione, cliccando con il mouse destro sull'icona dell'ethernet, si va su IPv4 Settings, si cambia il metodo da DHCP a Manuale, si scrive l'indirizzo, si fa Add e si Salva.



Poi si disattiva la scheda di rete e la si riattiva e si va a verificare se l'indirizzo è stato assegnato correttamente aprendo la console e facendo il comando `ifconfig` o `ip a`.

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
   inet 192.168.10.6/24 brd 192.168.10.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::8638:cc35:20dd:4129/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

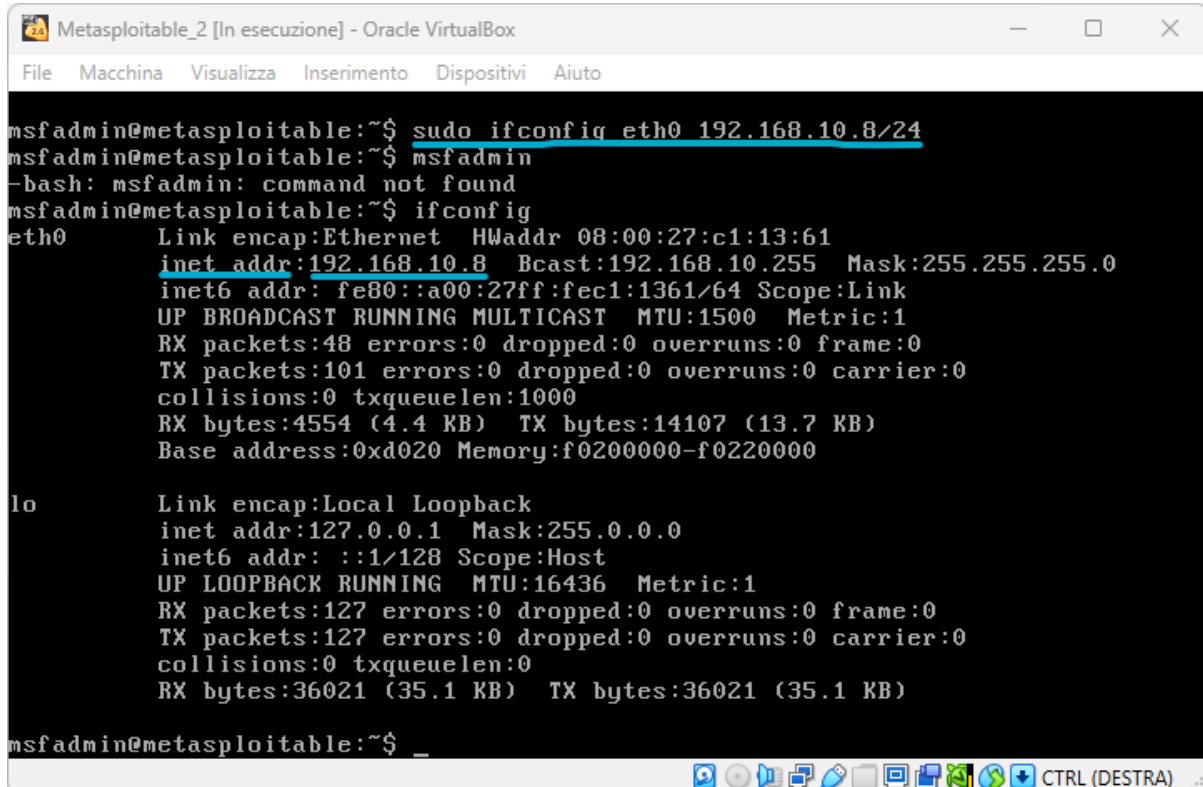
(kali@kali)-[~]
└─$ ifconfig

```

Come si può vedere l'indirizzo è stato configurato correttamente.

-Macchina Metasploitable:

Per configurare l'indirizzo ipv4 sulla macchina Metasploitable si utilizza il seguente comando: `sudo ifconfig eth0 192.168.10.8/24`



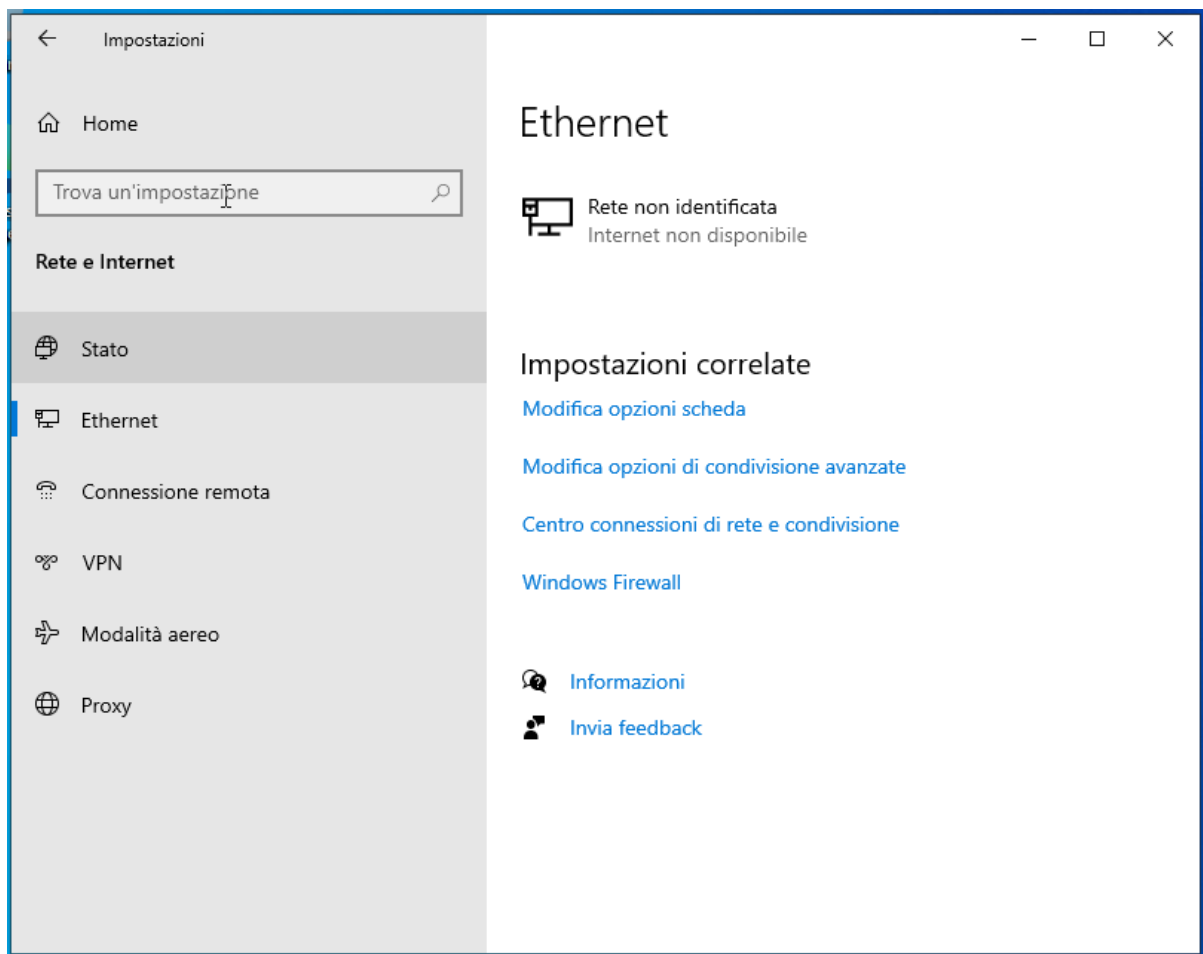
```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.10.8/24
msfadmin@metasploitable:~$ msfadmin
-bash: msfadmin: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c1:13:61
          inet addr:192.168.10.8  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec1:1361/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4554 (4.4 KB)  TX bytes:14107 (13.7 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:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:36021 (35.1 KB)  TX bytes:36021 (35.1 KB)

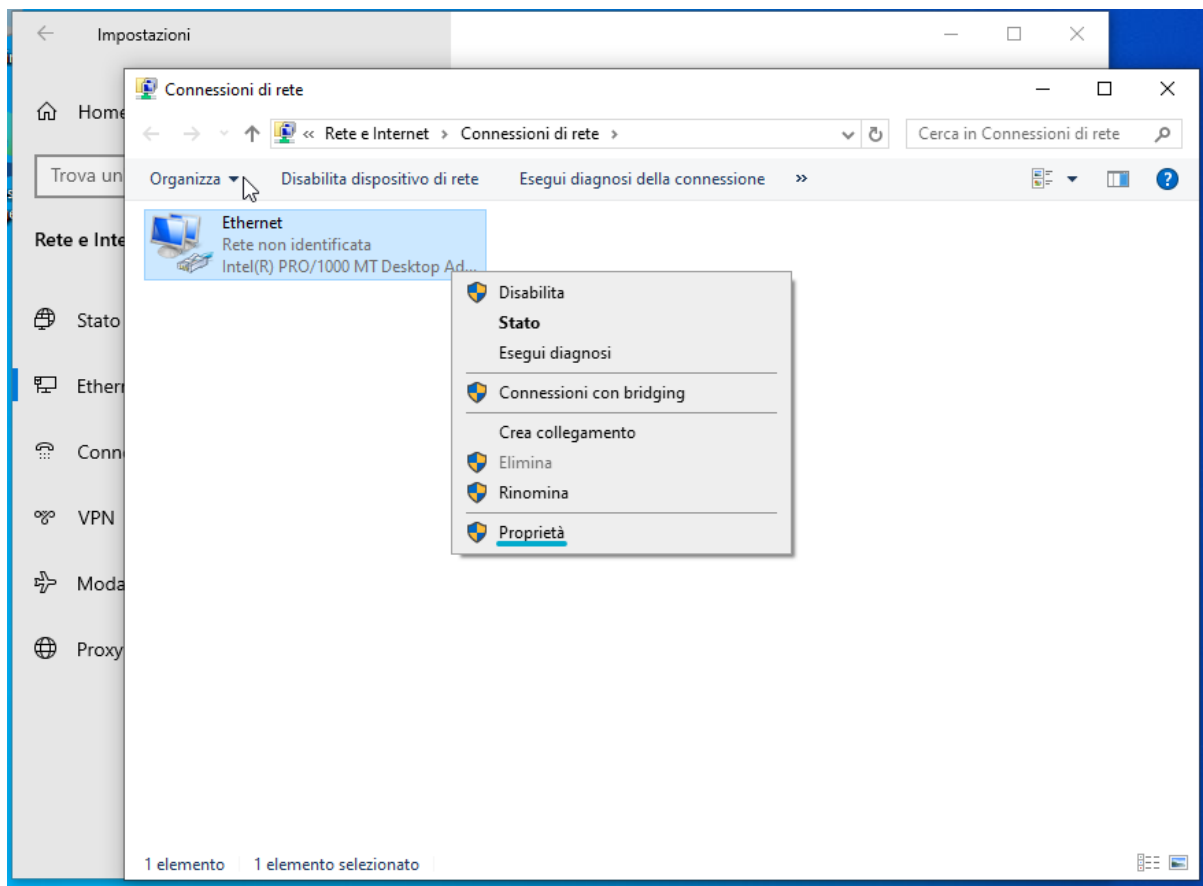
msfadmin@metasploitable:~$ _
```

-Macchina Windows 10:

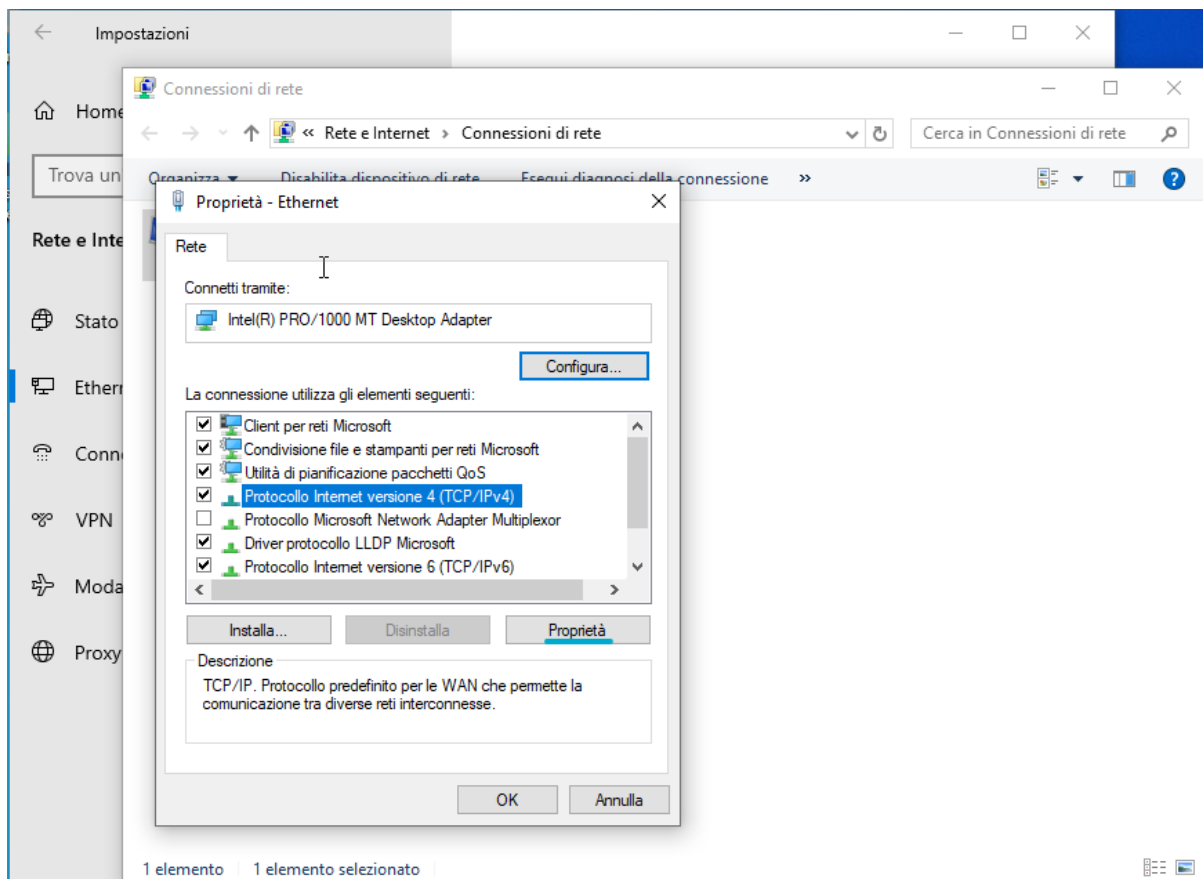
Per configurare l'indirizzo ipv4 sulla macchina Windows si utilizza la seguente procedura:



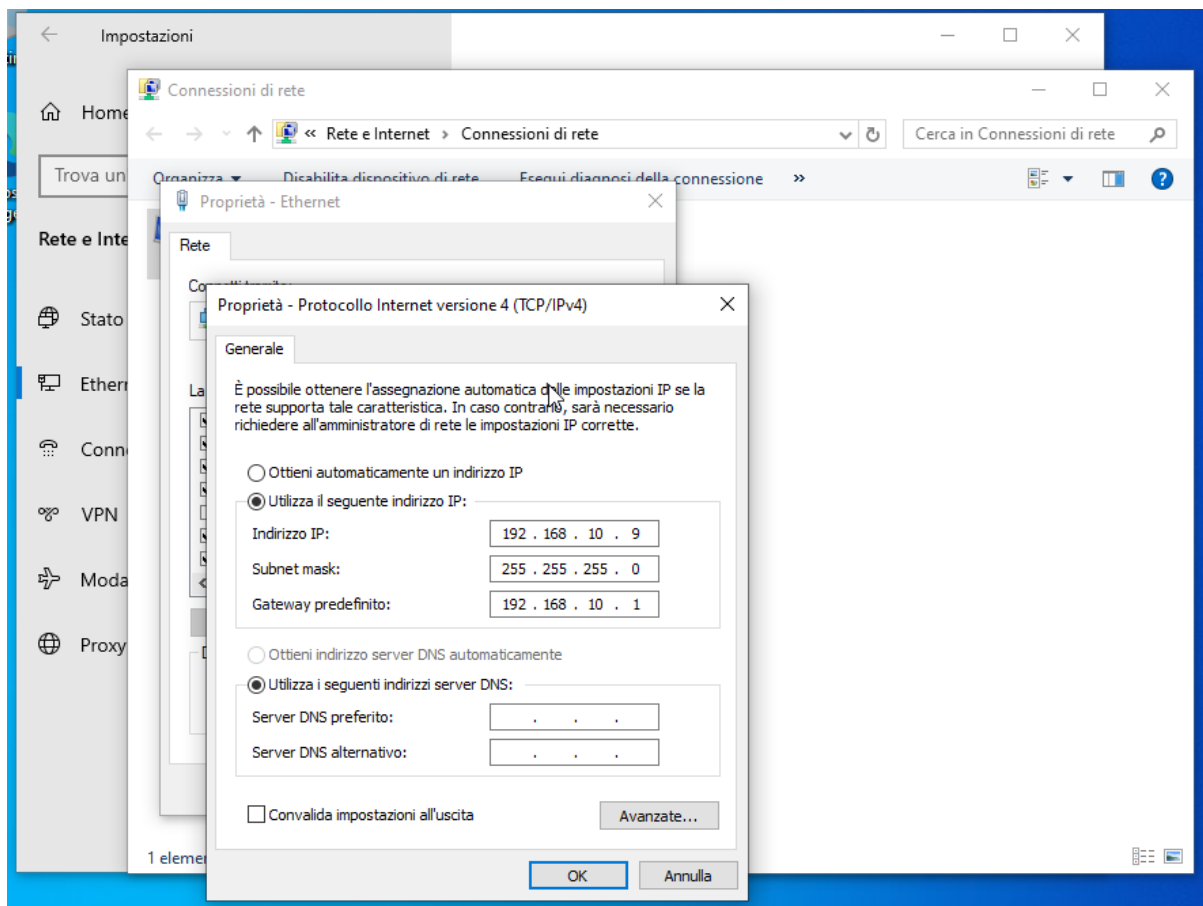
Si va sulle impostazioni di rete e si seleziona l'opzione modifica opzioni scheda.



Poi si seleziona la scheda di rete, mouse destro e si va su proprietà.



Si seleziona il Protocollo Internet versione 4 (TCP/IPV4), proprietà.



E qui infine si andrà ad inserire l'indirizzo ip specifico, con la subnet mask e il default gateway.

-OS fingerprint Kali-->Metasploit:

Successivamente da linea di comando comincio la procedura per eseguire la scansione da kali al target Metasploitable per l'OS.

Il comando è il seguente: `sudo nmap -O "indirizzo ip"`

in questo caso: `sudo nmap -O 192.168.10.8`

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.10.8
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:53 EST
Nmap scan report for 192.168.10.8
Host is up (0.0036s 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:C1:13:61 (Oracle VirtualBox virtual NIC)
Device type: general purpose WAP|terminal|printer|VoIP phone|switch
Running (JUST GUESSING): Linux 2.6.X|2.4.X (97%), Linksys embedded (95%), AVM embedded (94%), Chip PC embedded (93%), Xerox embedded (93%), Cisco embedded (93%), Extreme Networks ExtremeXOS 15.X (93%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.31 cpe:/h:linksys:wrv54g cpe:/o:linux:linux_kernel:2.4.30 cpe:/h:avm:fritz%21box_fon_wlan_7240 cpe:/o:linux:linux_kernel:2.4.18 cpe:/o:linux:linux_kernel cpe:/h:xerox:workcentre_7545 cpe:/o:extremenetworks:extremexos:15
Aggressive OS guesses: Linux 2.6.31 (97%), Linux 2.6.9 - 2.6.30 (97%), Linux 2.6.9 - 2.6.33 (97%), Linux 2.6.13 - 2.6.32 (97%), Linux 2.6.22 (embedded, ARM) (96%), Linux 2.6.22 - 2.6.23 (96%), Linux 2.6.9 - 2.6.24 (96%), Linux 2.6.18 - 2.6.32 (95%), Linux 2.6.21 (95%), Linksys WRV54G WAP (95%)
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 17.30 seconds

(kali@kali)-[~]
$
```

-SYN scan Kali-->Metasploit:

Per eseguire la scansione SYN il comando è il seguente :

`sudo nmap -sS "indirizzo ip"`

in questo caso: `sudo nmap -sS 192.168.10.8`


```

(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.10.8
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:57 EST
Nmap scan report for 192.168.10.8
Host is up (0.0070s 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:C1:13:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.56 seconds
(kali㉿kali)-[~]
$

```

-Tcp Connect Kali-->Metasploit:

Per eseguire la scansione Tcp connect il comando è il seguente:

`sudo nmap -sT "indirizzo ip"`

in questo caso : `sudo nmap -sT 192.168.10.8`

```

(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.10.8
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:02 EST
Nmap scan report for 192.168.10.8
Host is up (0.013s 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:C1:13:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds
(kali㉿kali)-[~]
$

```

Come possiamo vedere non c'è alcuna differenza rispetto alla scansione SYN scan.

-Version Detection Kali-->Metasploit:

Per eseguire la scansione Version Detection il comando è il seguente:

`sudo nmap -sV "indirizzo ip"`

in questo caso: `sudo nmap -sV 192.168.10.8`

```

(kali@kali)-[~]
$ sudo nmap -sV 192.168.10.8
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:09 EST
Nmap scan report for 192.168.10.8
Host is up (0.0056s 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        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
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:C1:13:61 (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 25.20 seconds

(kali@kali)-[~]
$

```

-OS Fingerprint Kali-->Windows

Per eseguire la scansione OS Fingerprint il comando è il seguente:

`sudo nmap -O "indirizzo ip" (in questo caso di windows)`

in questo caso : `sudo nmap -O 192.168.10.9`

```

(kali@kali)-[~]
$ sudo nmap -O 192.168.10.9
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:13 EST
Nmap scan report for 192.168.10.9
Host is up (0.00065s latency).
All 1000 scanned ports on 192.168.10.9 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:A8:B1:23 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 40.35 seconds

```

Come da output però notiamo che non è riuscito correttamente a fare la scansione quindi si prova un'altro comando:

`sudo nmap -O --osscan-limit --osscan-guess indirizzo ip+subnet mask`

in questo caso `sudo nmap -O --osscan-limit --osscan-guess 192.168.10.9/24`

```

(kali@kali)-[~]
└─$ sudo nmap -O --osscan-limit --osscan-guess 192.168.10.9/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:19 EST
Nmap scan report for 192.168.10.8
Host is up (0.0058s 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:C1:13:61 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.31 (97%), Linux 2.6.9 - 2.6.24 (97%), Linux 2.6.9 - 2.6.30 (97%), Linux 2.6.9 - 2.6.33 (97%), Linux 2.6.13 - 2.6.32 (97%),
Linux 2.6.18 - 2.6.32 (96%), Linux 2.6.22 (embedded, ARM) (96%), Linux 2.6.22 - 2.6.23 (96%), Linux 2.6.18 (Debian 4, VMware) (96%), Linksys RV042 router (9
6%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.10.9
Host is up (0.00072s latency).
All 1000 scanned ports on 192.168.10.9 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:A8:B1:23 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.10.6
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.10.6 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 36.10 seconds

(kali@kali)-[~]
└─$

```

E con questa procedura si ha avuto parzialmente successo si è riusciti a trovare delle informazioni.