W11D1 – Pratica

Epic Education Srl

Scansione dei servizi con Nmap pt. 1

(target Metasploitable)

Simone Giordano

18/09/2025

Contatti:

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Sintesi esecutiva 3
Perimetro 3
Panoramica delle vulnerabilità 3
1 Tecniche di scansione con Nmap su reti diverse 4
1.1 Configurazione rete 4
1.2 OS fingerprint 6
1.3 Syn scan 7
1.4 TCP connect 8
1.5 Version detection 8
1.6 Report 9
2 Tecniche di scansione con Nmap sulla stessa rete 11
2.1 Configurazione rete 11
2.2 OS fingerprint 13
2.3 Syn scan 14
2.4 TCP connect 15
2.5 Version detection 15
3 Differenze 16
3.1 OS fingerprint 16
3.2 Syn scan 16
3.3 TCP connect 16
3.4 Version detection 16

Sintesi esecutiva

Questo documento riassume i risultati delle scansioni condotte sulla macchina *Metasploitable* utilizzando Nmap, eseguite in due diverse configurazioni di rete (due macchine nella stessa rete vs. due macchine su reti separate). L'obiettivo è identificare le porte aperte e i servizi esposti e rilevare le differenze dei risultati tra le due configurazioni di rete.

Tecniche di scansione usate:
- OS fingerprint
- Syn Scan
- TCP connect
- Version detection

Perimetro

Il target prefissato è la macchina Metasploitable

Panoramica delle vulnerabilità

Sono state identificate le seguenti porte aperte con i relativi servizi

Port		Service
21	tcp	ftp
22	tcp	ssh
23	tcp	telnet
25	tcp	smtp
53	tcp	domain
80	tcp	http
111	tcp	rpcbind
139	tcp	netbios-ssn
445	tcp	netbios-ssn
512	tcp	exec
513	tcp	login
514	tcp	shell
1099	tcp	java-rmi
1524	tcp	bindshell
2049	tcp	nfs
2121	tcp	ccproxy-ftp
3306	tcp	mysql
5432	tcp	postgresql
5900	tcp	vnc
6000	tcp	X11
6667	tcp	irc
8009	tcp	ajp13
8180	tcp	http

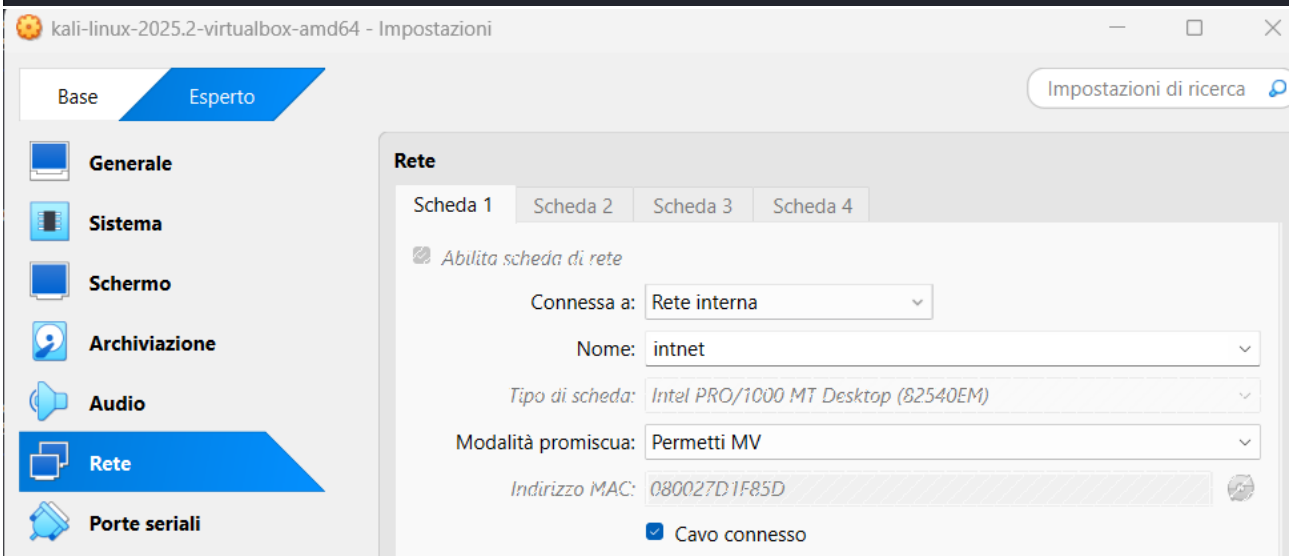
1 Tecniche di scansione con Nmap su reti diverse

1.1 Configurazione rete

Il target e l'attaccante sono su due reti diverse

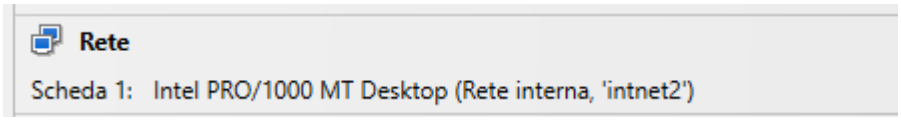
Kali

```
┌──(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:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::8417:1efb:8b3a:5970/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

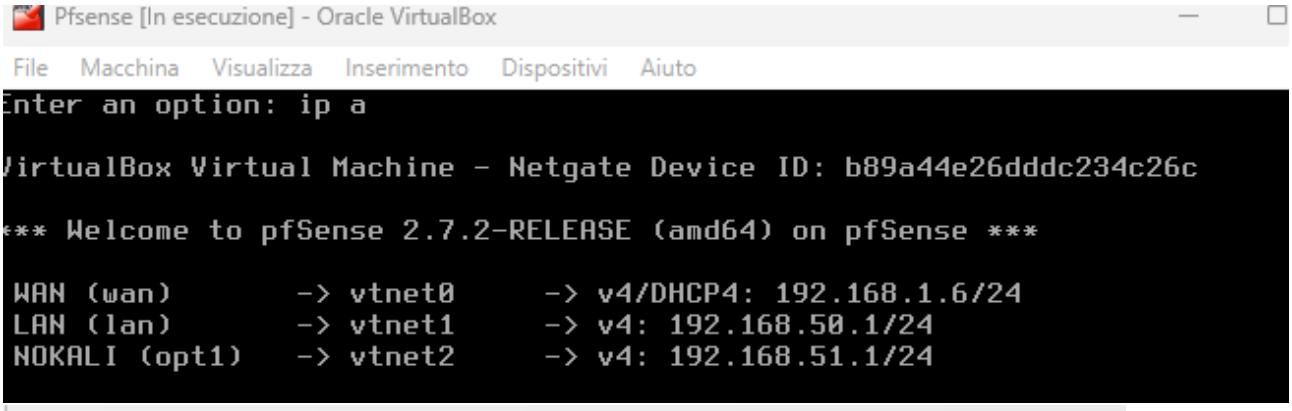


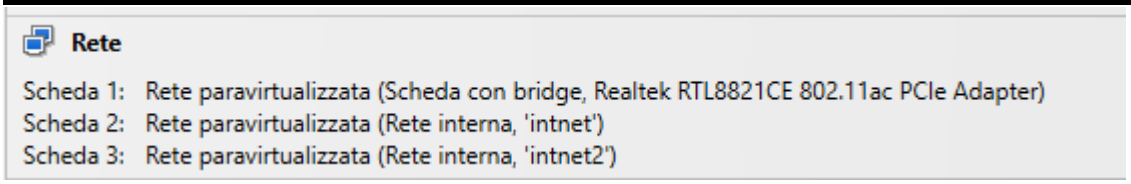
Metasploitable

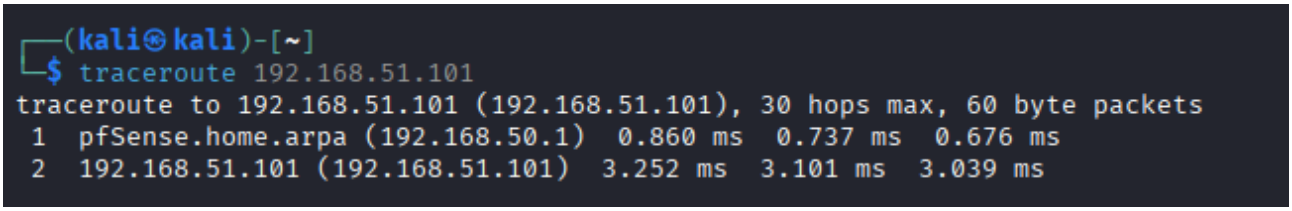
```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:e4:29:4e brd ff:ff:ff:ff:ff:ff
    inet 192.168.51.101/24 brd 192.168.51.255 scope global eth0
    inet6 fe80::a00:27ff:fee4:294e/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```


Rete
Scheda 1: Intel PRO/1000 MT Desktop (Rete interna, 'intnet2')

pfSense


Pfsense [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Enter an option: ip a
VirtualBox Virtual Machine - Netgate Device ID: b89a44e26dddc234c26c
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> vtnet0 -> v4/DHCP4: 192.168.1.6/24
LAN (lan) -> vtnet1 -> v4: 192.168.50.1/24
NOKALI (opt1) -> vtnet2 -> v4: 192.168.51.1/24


Rete
Scheda 1: Rete paravirtualizzata (Scheda con bridge, Realtek RTL8821CE 802.11ac PCIe Adapter)
Scheda 2: Rete paravirtualizzata (Rete interna, 'intnet')
Scheda 3: Rete paravirtualizzata (Rete interna, 'intnet2')


(kali㉿kali)-[~]
$ traceroute 192.168.51.101
traceroute to 192.168.51.101 (192.168.51.101), 30 hops max, 60 byte packets
1 pfSense.home.arpa (192.168.50.1) 0.860 ms 0.737 ms 0.676 ms
2 192.168.51.101 (192.168.51.101) 3.252 ms 3.101 ms 3.039 ms

1.2 OS fingerprint

nmap -O 192.168.51.101

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 16:05 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0028s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds
```

1.3 Syn scan

nmap -sS -v 192.168.51.101

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -v 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 16:07 EDT
Initiating Ping Scan at 16:07
Scanning 192.168.51.101 [4 ports]
Completed Ping Scan at 16:07, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:07
Completed Parallel DNS resolution of 1 host. at 16:07, 0.00s elapsed
Initiating SYN Stealth Scan at 16:07
Scanning 192.168.51.101 [1000 ports]
Discovered open port 23/tcp on 192.168.51.101
Discovered open port 3306/tcp on 192.168.51.101
Discovered open port 139/tcp on 192.168.51.101
Discovered open port 111/tcp on 192.168.51.101
Discovered open port 22/tcp on 192.168.51.101
Discovered open port 21/tcp on 192.168.51.101
Discovered open port 445/tcp on 192.168.51.101
Discovered open port 5900/tcp on 192.168.51.101
Discovered open port 53/tcp on 192.168.51.101
Discovered open port 25/tcp on 192.168.51.101
Discovered open port 80/tcp on 192.168.51.101
Discovered open port 2121/tcp on 192.168.51.101
Discovered open port 5432/tcp on 192.168.51.101
Discovered open port 6667/tcp on 192.168.51.101
Discovered open port 8009/tcp on 192.168.51.101
Discovered open port 6000/tcp on 192.168.51.101
Discovered open port 514/tcp on 192.168.51.101
Discovered open port 1099/tcp on 192.168.51.101
Discovered open port 8180/tcp on 192.168.51.101
Discovered open port 513/tcp on 192.168.51.101
Discovered open port 512/tcp on 192.168.51.101
Discovered open port 2049/tcp on 192.168.51.101
Discovered open port 1524/tcp on 192.168.51.101
Completed SYN Stealth Scan at 16:07, 0.34s elapsed (1000 total ports)
Nmap scan report for 192.168.51.101
Host is up (0.0065s 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

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
           Raw packets sent: 1004 (44.152KB) | Rcvd: 1001 (40.120KB)
```

1.4 TCP connect

nmap -sT 192.168.51.101

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 16:10 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0029s 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

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

1.5 Version detection

nmap -sV 192.168.51.101

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 16:11 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0019s 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  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  ccproxy-ftp?
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
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 173.33 seconds
```

1.6 Report

nmap -oA versione -sV 192.168.51.101 && xsltproc versione.xml -o versione.html

IP target: 192.168.51.101

Address

192.168.51.101 (ipv4)

Ports

The 977 ports scanned but not shown below are in state: **closed**

977 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
23	tcp	open	telnet	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		
53	tcp	open	domain	syn-ack	ISC BIND	9.4.2	
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
512	tcp	open	exec	syn-ack	netkit-rsh rexecd		
513	tcp	open	login	syn-ack			

514	tcp	open	shell	syn-ack	Netkit rshd		
1099	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
1524	tcp	open	bindshell	syn-ack	Metasploitable root shell		
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003
2121	tcp	open	ccproxy-ftp	syn-ack			
3306	tcp	open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	
5432	tcp	open	postgresql	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7	
5900	tcp	open	vnc	syn-ack	VNC		protocol 3.3
6000	tcp	open	X11	syn-ack			access denied
6667	tcp	open	irc	syn-ack	UnrealIRCd		
8009	tcp	open	ajp13	syn-ack	Apache Jserv		Protocol v1.3
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	

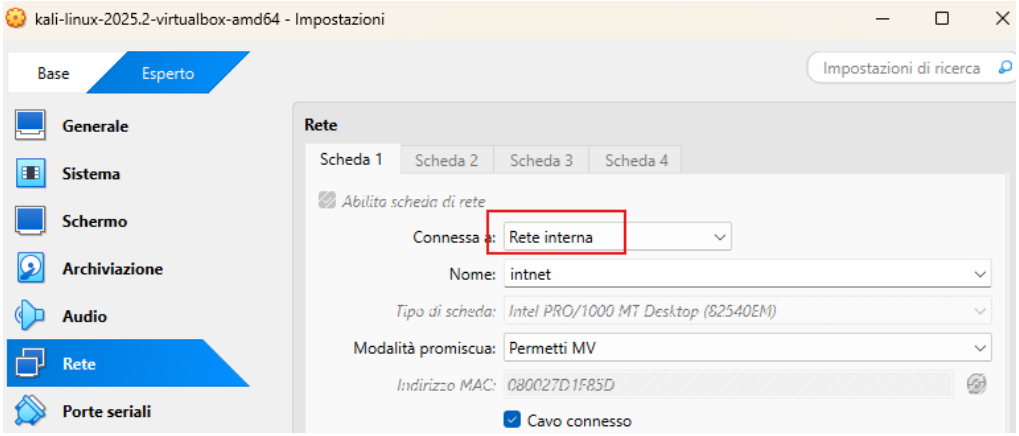
2 Tecniche di scansione con Nmap sulla stessa rete

2.1 Configurazione rete

Il target e l'attaccante sono sulla stessa rete

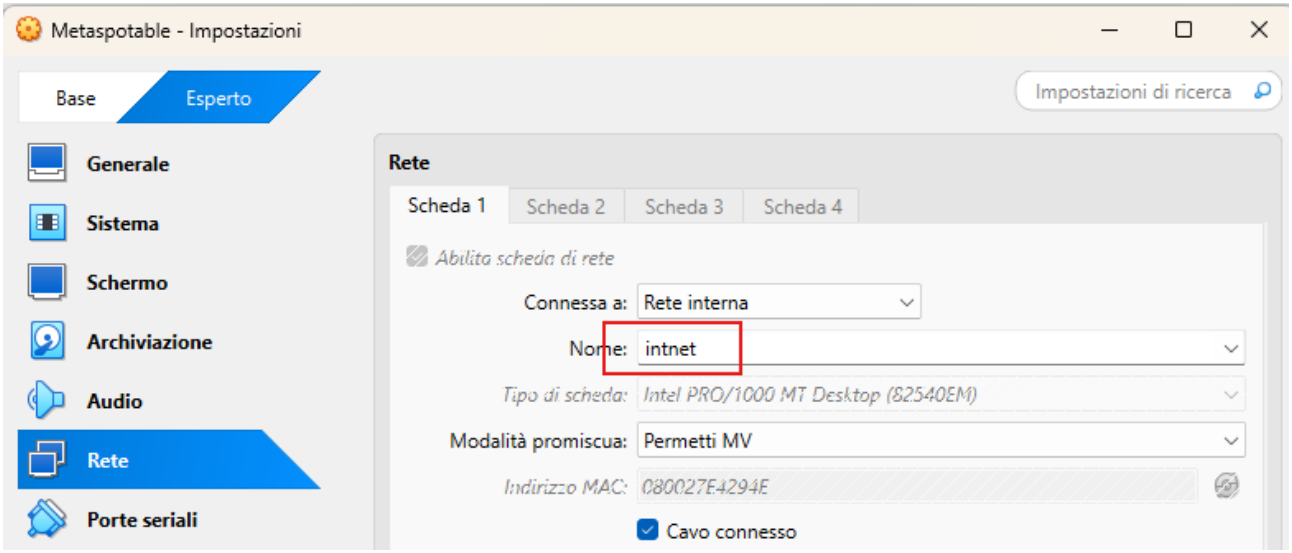
Kali

```
┌──(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:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::8417:1efb:8b3a:5970/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```



Metasploitable

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:e4:29:4e brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.101/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fee4:294e/64 scope link
       valid_lft forever preferred_lft forever
```



Prova che le due macchine comunicano e percorso dei pacchetti

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.87 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.85 ms
^C
── 192.168.50.101 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.160/1.572/1.873/0.301 ms

┌──(kali㉿kali)-[~]
└─$ traceroute 192.168.50.101
traceroute to 192.168.50.101 (192.168.50.101), 30 hops max, 60 byte packets
 1  192.168.50.101 (192.168.50.101)  1.878 ms  1.748 ms  1.610 ms
```

2.2 OS fingerprint

nmap -O 192.168.50.101

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 08:22 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0015s 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:E4:29:4E (PCS Systemtechnik/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 14.83 seconds
```

2.3 Syn scan

nmap -sS -v 192.168.50.101

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -v 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 08:23 EDT
Initiating ARP Ping Scan at 08:23
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 08:23, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:23
Completed Parallel DNS resolution of 1 host. at 08:24, 13.01s elapsed
Initiating SYN Stealth Scan at 08:24
Scanning 192.168.50.101 [1000 ports]
Discovered open port 445/tcp on 192.168.50.101
Discovered open port 21/tcp on 192.168.50.101
Discovered open port 111/tcp on 192.168.50.101
Discovered open port 23/tcp on 192.168.50.101
Discovered open port 25/tcp on 192.168.50.101
Discovered open port 22/tcp on 192.168.50.101
Discovered open port 139/tcp on 192.168.50.101
Discovered open port 53/tcp on 192.168.50.101
Discovered open port 5900/tcp on 192.168.50.101
Discovered open port 80/tcp on 192.168.50.101
Discovered open port 3306/tcp on 192.168.50.101
Discovered open port 6667/tcp on 192.168.50.101
Discovered open port 2049/tcp on 192.168.50.101
Discovered open port 6000/tcp on 192.168.50.101
Discovered open port 1099/tcp on 192.168.50.101
Discovered open port 1524/tcp on 192.168.50.101
Discovered open port 513/tcp on 192.168.50.101
Discovered open port 8180/tcp on 192.168.50.101
Discovered open port 2121/tcp on 192.168.50.101
Discovered open port 512/tcp on 192.168.50.101
Discovered open port 514/tcp on 192.168.50.101
Discovered open port 8009/tcp on 192.168.50.101
Discovered open port 5432/tcp on 192.168.50.101
Completed SYN Stealth Scan at 08:24, 0.50s elapsed (1000 total ports)
Nmap scan report for 192.168.50.101
Host is up (0.00046s 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:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.67 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

2.4 TCP connect

nmap -sT 192.168.50.101

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 08:25 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0055s 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:E4:29:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

2.5 Version detection

nmap -sV 192.168.50.101

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 08:26 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0010s 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  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:E4:29:4E (PCS Systemtechnik/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 66.26 seconds
```

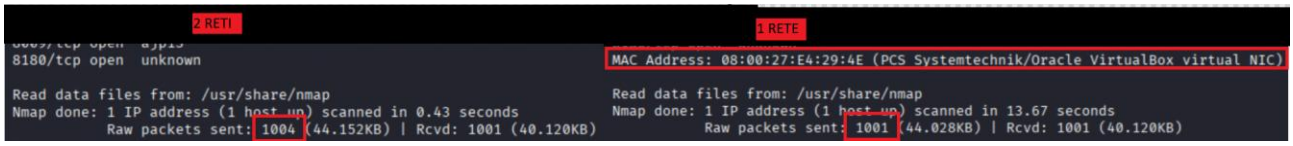
3 Differenze

3.1 OS fingerprint

Confrontando i due test le porte rilevate sono rimaste le stesse, ma nella configurazione con rete singola è stato rilevato il MAC Address, è cambiato il numero di hope che il pacchetto ha dovuto attraversare e il tempo impiegato.

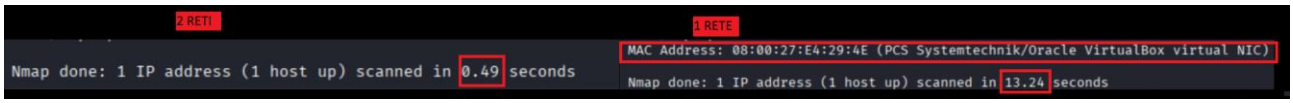
3.2 Syn scan

Confrontando i due test le porte rilevate sono rimaste le stesse, ma nella configurazione con rete singola è stato rilevato il MAC Address, è cambiato il numero di pacchetti inviati e il tempo impiegato.



3.3 TCP connect

Confrontando i due test le porte rilevate sono rimaste le stesse, ma nella configurazione con rete singola è stato rilevato il MAC Address, è cambiato il tempo impiegato.



3.4 Version detection

Confrontando i due test le porte rilevate sono rimaste le stesse, ma nella configurazione con rete singola è stato rilevato il MAC Address, è cambiato il tempo impiegato.