

### Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable** (target e attaccante devono essere su due reti diverse):

- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection

A valle delle scansioni, è prevista la produzione di un **report** contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

Metasploitable e Kali si trovano su due reti diverse grazie a Pfsense



The screenshot displays a Kali Linux desktop environment. The terminal window shows the following output:

```
msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:5f:8f:56
      inet addr:192.168.60.101 Bcast:192.168.60.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27:5f:8f:56/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:37 errors:0 dropped:0 overruns:0 frame:0
      TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:3976 (3.8 KB) TX bytes:7109 (6.9 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:102 errors:0 dropped:0 overruns:0 frame:0
      TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:23665 (23.1 KB) TX bytes:23665 (23.1 KB)

msfadmin@metasploitable:~$
```

The network interface configuration window shows the following details:

- connessione 192.168.50.100
- Disconnect
- Available
- DHCP AUTOMATICA
- connessione 192.168.32.100
- VPN Connections

The system information window shows the following details:

- The system is on the latest version. Version information updated at Tue Jul 23 16:15:59 UTC 2024
- CPU Type: Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz
- AES-NI CPU Crypto: Yes (inactive)
- QAT Crypto: No
- Hardware crypto: Inactive
- Kernel PTI: Enabled
- MDS Mitigation: Inactive
- Uptime: 00 Hour 38 Minutes 34 Seconds
- Current date/time: Tue Jul 23 16:53:28 UTC 2024
- DNS server(s): 127.0.0.1, 192.168.1.1
- Last config change: Tue Jul 23 16:26:15 UTC 2024
- State table size: 0% (87/96000) Show states
- MBUF Usage: 0% (4064/1000000)
- Load average: 0.51 0.65 0.64

The terminal window also shows the following output:

```
(root@kali)-[/home/kali]
# ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data:
64 bytes from 192.168.60.101: icmp_seq=1 ttl=64 time=1.28 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=64 time=2.21 ms
64 bytes from 192.168.60.101: icmp_seq=3 ttl=64 time=1.64 ms
64 bytes from 192.168.60.101: icmp_seq=4 ttl=64 time=1.07 ms
^C
— 192.168.60.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 1.069/1.549/2.206/0.431 ms

(root@kali)-[/home/kali]
```

```
(root@kali)-[/home/kali]
# nmap -O 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 12:55 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0015s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
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): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).
```

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 9.08 seconds

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 12:55 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
```

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 12:56 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain Unbound
80/tcp    open  http  nginx
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 11.01 seconds

```
(root@kali)-[/home/kali]
# nmap -A 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 12:56 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0027s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
```

53/tcp open domain Unbound

80/tcp open http nginx

|\_http-title: pfSense - Login

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): FreeBSD 11.X (97%)

OS CPE: cpe:/o:freebsd:freebsd:11.2

Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)

HOP	RTT	ADDRESS
-----	-----	---------

1	2.75 ms	192.168.60.101
---	---------	----------------

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 23.44 seconds