Laboratorio di Scansione Nmap: Metasploitable e Windows 7

Introduzione

Questo laboratorio affronta le tecniche di riconoscimento e fingerprinting di host remoti utilizzando **Nmap**, uno strumento fondamentale per la sicurezza delle reti e il penetration testing. L'obiettivo è comprendere il funzionamento di diverse tecniche di scansione e analizzare le differenze nei risultati ottenuti.

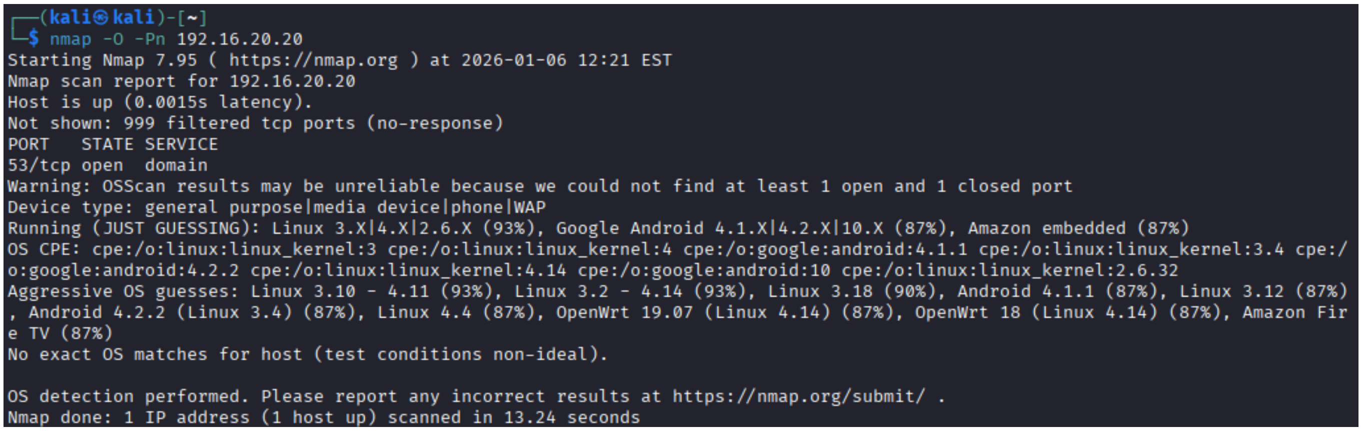
Ambiente di Laboratorio

L'ambiente di test è stato configurato usando **Oracle VirtualBox** con le seguenti componenti:

- **Kali Linux**: macchina attaccante con (bridged adapter)
- **Metasploitable 2**: target Linux vulnerabile (bridged adapter)
- **Windows 7 Professional**: target Windows (bridged adapter)

Tecniche di Scansione Nmap

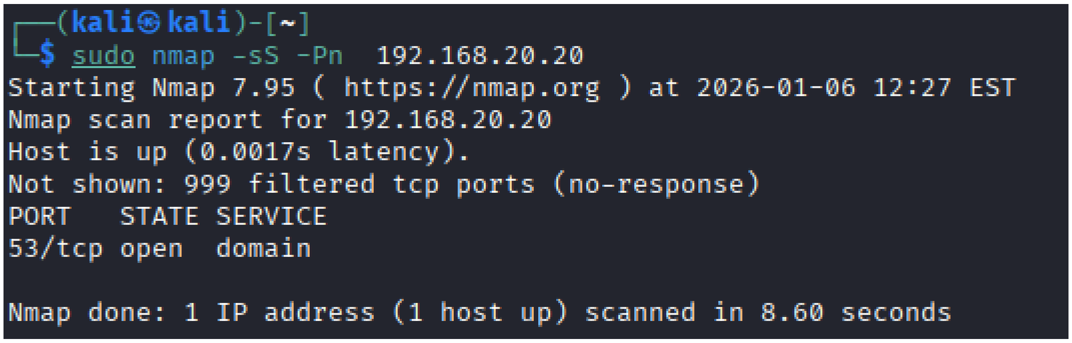
OS Fingerprinting (-O)



```
┌──(kali㉿kali)-[~]
└─$ nmap -O -Pn 192.16.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:21 EST
Nmap scan report for 192.16.20.20
Host is up (0.0015s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|media device|phone|WAP
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (93%), Google Android 4.1.X|4.2.X|10.X (87%), Amazon embedded (87%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:google:android:4.1.1 cpe:/o:linux:linux_kernel:3.4 cpe:/
o:google:android:4.2.2 cpe:/o:linux:linux_kernel:4.14 cpe:/o:google:android:10 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 3.10 - 4.11 (93%), Linux 3.2 - 4.14 (93%), Linux 3.18 (90%), Android 4.1.1 (87%), Linux 3.12 (87%)
, Android 4.2.2 (Linux 3.4) (87%), Linux 4.4 (87%), OpenWrt 19.07 (Linux 4.14) (87%), OpenWrt 18 (Linux 4.14) (87%), Amazon Fir
e TV (87%)
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 13.24 seconds
```

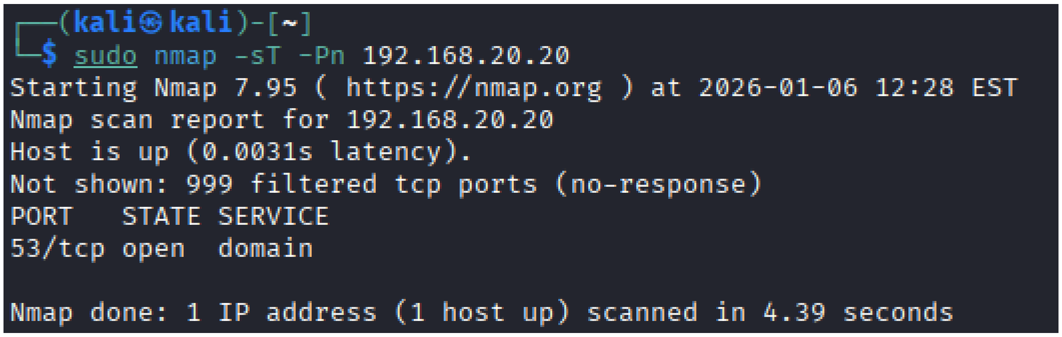
SYN Scan (-sS)



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -Pn  192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:27 EST
Nmap scan report for 192.168.20.20
Host is up (0.0017s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 8.60 seconds
```

TCP Connect Scan (-sT)



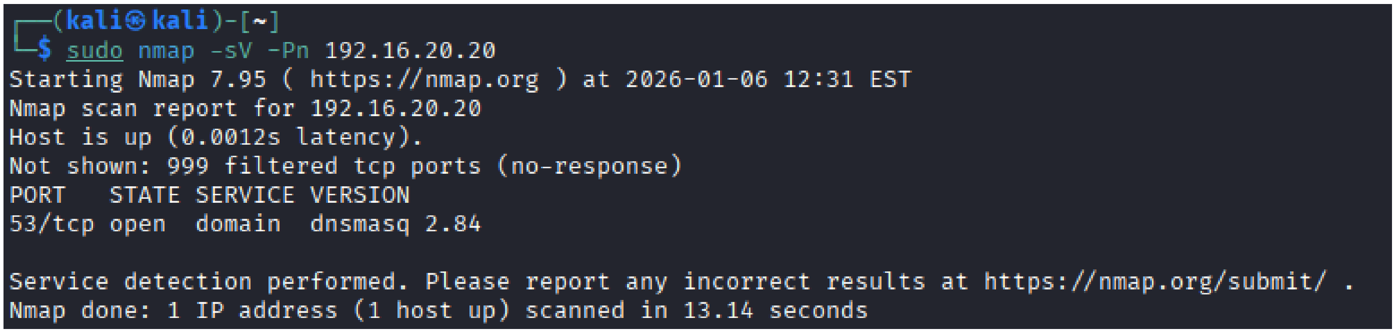
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -Pn 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:28 EST
Nmap scan report for 192.168.20.20
Host is up (0.0031s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.39 seconds
```

Differenze tra SYN e TCP Connect

In pratica, i risultati della lista di porte saranno quasi identici, mentre cambia la "firma" della scansione a livello di rete.

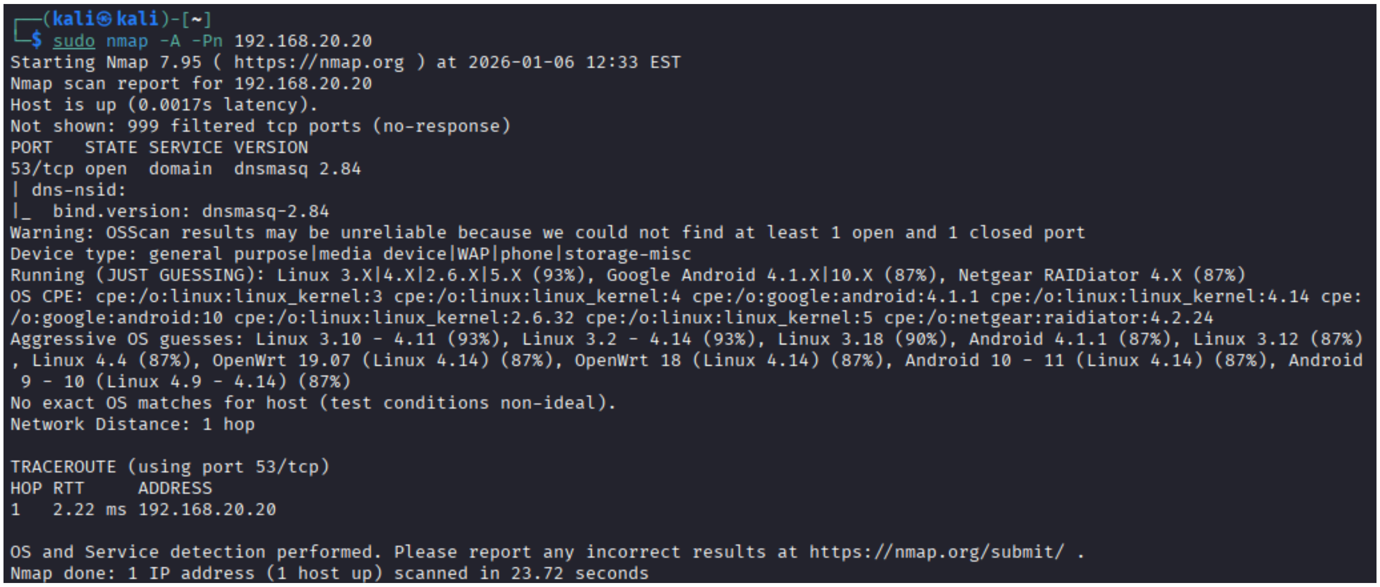
Version Detection (-sV)



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -Pn 192.16.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:31 EST
Nmap scan report for 192.16.20.20
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.84

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

Soluzione immediata e completa (-A)

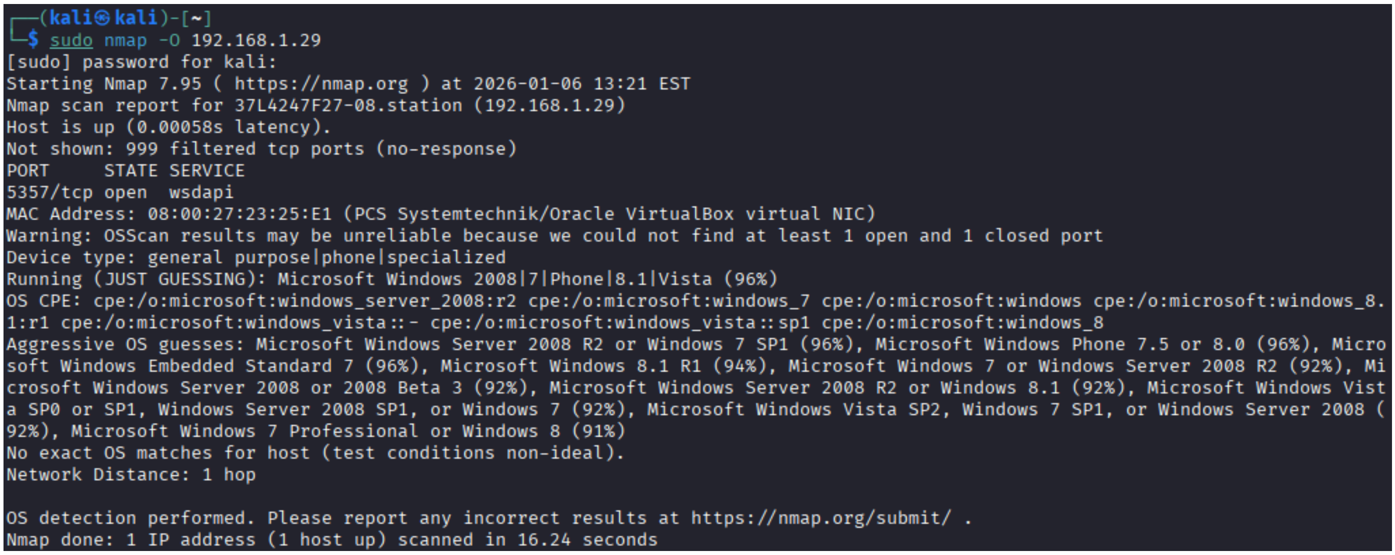


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -Pn 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 12:33 EST
Nmap scan report for 192.168.20.20
Host is up (0.0017s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.84
| dns-nsid:
|_  bind.version: dnsmasq-2.84
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|media device|WAP|phone|storage-misc
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X|5.X (93%), Google Android 4.1.X|10.X (87%), Netgear RAIDiator 4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:google:android:4.1.1 cpe:/o:linux:linux_kernel:4.14 cpe:
/o:google:android:10 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:netgear:raidiator:4.2.24
Aggressive OS guesses: Linux 3.10 - 4.11 (93%), Linux 3.2 - 4.14 (93%), Linux 3.18 (90%), Android 4.1.1 (87%), Linux 3.12 (87%)
, Linux 4.4 (87%), OpenWrt 19.07 (Linux 4.14) (87%), OpenWrt 18 (Linux 4.14) (87%), Android 10 - 11 (Linux 4.14) (87%), Android
 9 - 10 (Linux 4.9 - 4.14) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   2.22 ms 192.168.20.20

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 23.72 seconds
```

OS Fingerprinting Windows 7



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.29
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:21 EST
Nmap scan report for 37L4247F27-08.station (192.168.1.29)
Host is up (0.00058s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 08:00:27:23:25:E1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2008|7|Phone|8.1|Vista (96%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_8.
1:r1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_8
Aggressive OS guesses: Microsoft Windows Server 2008 R2 or Windows 7 SP1 (96%), Microsoft Windows Phone 7.5 or 8.0 (96%), Micro
soft Windows Embedded Standard 7 (96%), Microsoft Windows 8.1 R1 (94%), Microsoft Windows 7 or Windows Server 2008 R2 (92%), Mi
crosoft Windows Server 2008 or 2008 Beta 3 (92%), Microsoft Windows Server 2008 R2 or Windows 8.1 (92%), Microsoft Windows Vist
a SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (92%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (
92%), Microsoft Windows 7 Professional or Windows 8 (91%)
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 16.24 seconds
```