

# Bonus Lab – Nmap Scan Report

Questo report esplora l'utilizzo del tool Nmap per la scansione di porte e l'identificazione di servizi attivi in reti locali e remote. Attraverso l'analisi dei comandi principali e dei parametri come `-A` e `-T4`, vengono presentati i risultati di diverse scansioni, fornendo una panoramica delle capacità di Nmap e della sua importanza nel contesto della sicurezza informatica.

**L** by Luca Tavani

# Esplorazione del comando nmap

A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are **-A**, execution; and then the hostname.

## Example 1. A representative Nmap scan

```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
|_ ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_ 2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open      http         Apache httpd 2.2.14 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
646/tcp   filtered  ldap
1720/tcp  filtered  H.323/Q.931
9929/tcp  open      nping-echo   Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1 17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

The newest version of Nmap can be obtained from <https://nmap.org>. The newest version of this manual chapter of Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security is **page nmap(1) line 25 (press h for help or q to quit)**

Nella prima parte di questo laboratorio, ci siamo concentrati sull'esplorazione del comando **nmap** per comprenderne appieno le funzionalità. Abbiamo consultato il manuale di Nmap (**man nmap**) per approfondire le opzioni e i parametri disponibili. In particolare, abbiamo analizzato l'esempio proposto, focalizzandoci sui seguenti parametri:

- **-A**: Questo parametro attiva il rilevamento del sistema operativo, la versione dei servizi, la scansione con script e il traceroute, fornendo una visione completa del target.

La combinazione di questi parametri permette di ottenere informazioni dettagliate in tempi relativamente brevi, rendendoli utili per una vasta gamma di scenari di scansione.

# Scansioni effettuate: Localhost

```
(kali㉿kali)-[~]  
$ man nmap  
  
(kali㉿kali)-[~]  
$ nmap -A -T4 localhost  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 15:10 CEST  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.000076s latency).  
Other addresses for localhost (not scanned): ::1  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 9.9p2 Debian 1 (protocol 2.0)  
| ssh-hostkey:  
|_  256 3b:b8:9f:bd:8b:bc:b3:e3:29:62:e5:90:33:fc:5b:07 (ECDSA)  
|_  256 ed:01:e5:3b:7a:f9:27:a6:7d:6b:94:92:ed:27:2e:f6 (ED25519)  
Device type: general purpose  
Running: Linux 2.6.X|5.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6  
OS details: Linux 2.6.32, Linux 5.0 - 6.2  
Network Distance: 0 hops  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
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 2.60 seconds
```

La prima scansione è stata eseguita sul localhost per verificare i servizi attivi sulla macchina locale. Il comando utilizzato è stato:

**nmap -A -T4 localhost.**

I risultati della scansione hanno rivelato la seguente informazione:

- Porta aperta rilevata: **22/tcp (SSH)** con **OpenSSH 9.9p2 Debian**
- Sistema operativo rilevato: **Linux 2.6.X | 5.X**

Questa scansione conferma la presenza del servizio SSH attivo sulla porta 22, utilizzato per connessioni remote sicure. L'identificazione del sistema operativo fornisce ulteriori informazioni sulla configurazione della macchina.

# Scansioni effettuate: Rete Locale

```
(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 08:00:27:35:30:e3 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0  
        valid_lft 85938sec preferred_lft 85938sec  
3: bridge0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000  
    link/ether 3e:b4:e3:df:b9:42 brd ff:ff:ff:ff:ff:ff  
  
(kali@kali) ~  
$ nmap -A -T4 10.0.2.15  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 15:11 CEST  
Nmap scan report for 10.0.2.15 (10.0.2.15)  
Host is up (0.000065s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 9.9p2 Debian 1 (protocol 2.0)  
| ssh-hostkey:  
|_  256 3b:b8:9f:bd:8b:bc:b3:e3:29:62:e5:90:33:fc:5b:07 (ECDSA)  
|_  256 ed:01:e5:3b:7a:f9:27:a6:7d:6b:94:92:ed:27:2e:f6 (ED25519)  
Device type: general purpose  
Running: Linux 2.6.X|5.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6  
OS details: Linux 2.6.32, Linux 5.0 - 6.2  
Network Distance: 0 hops  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
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 2.06 seconds
```

Successivamente al comando "ip a", è stata effettuata una scansione della rete locale per identificare gli host attivi e i servizi in esecuzione. L'indirizzo IP della macchina è **10.0.2.15/24**, e il comando utilizzato è stato: **nmap -A -T4 10.0.2.0/24**.

I risultati della scansione hanno mostrato:

- Host attivo rilevato: **10.0.2.15**
- Servizio rilevato: **SSH sulla porta 22**

La scansione ha confermato che solo la macchina locale era attiva sulla rete e che il servizio SSH era in esecuzione sulla porta 22. Questo è coerente con la scansione del localhost e fornisce una visione più ampia della rete.

# Scansioni effettuate: Server Remoto

Infine, è stata eseguita una scansione di un server remoto, specificamente [scanme.nmap.org](https://scanme.nmap.org), per valutare le capacità di Nmap in un contesto esterno. Il comando utilizzato è stato: `nmap -A -T4 scanme.nmap.org`.

I risultati della scansione hanno rivelato le seguenti porte aperte:

- 22/tcp – SSH
- 80/tcp – HTTP (Apache 2.4.7)
- 9929/tcp – Nping Echo
- 31337/tcp – TCPwrapped

```
(kali@kali)~$ nmap -A -T4 scanme.nmap.org

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 15:13 CEST
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 52.44% done; ETC: 15:13 (0:00:19 remaining)
Warning: 45.33.32.156 giving up on port because retransmission cap hit (6).
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.71% done; ETC: 15:13 (0:00:13 remaining)
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 15:14 (0:00:02 remaining)
Stats: 0:01:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.52% done; ETC: 15:14 (0:00:00 remaining)
Stats: 0:01:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.88% done; ETC: 15:14 (0:00:00 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.024s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu Zubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|_ 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_ 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:el:7b:1f:bd:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ http-favicon: Nmap Project
|_ http-title: Go ahead and ScanMe!
|_ http-server-header: Apache/2.4.7 (Ubuntu)
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
593/tcp    filtered http-rpc-epmap
9929/tcp   open  nping-echo Nping echo
31337/tcp  open  tcpwrapped

Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (94%), Slirp (94%), AT&T embedded (92%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (94%), AT&T BGW210 voice gateway (92%), QEMU user mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.23 ms scanme.nmap.org (45.33.32.156)

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 111.26 seconds
```

Sistema operativo: **Ubuntu Linux**

La scansione ha identificato diversi servizi attivi sul server remoto, tra cui SSH, HTTP (gestito da Apache) e altri servizi specifici. L'identificazione del sistema operativo come Ubuntu Linux fornisce ulteriori dettagli sulla configurazione del server.



# Conclusioni

Nmap si conferma come uno strumento essenziale nella fase di ricognizione, sia per attacchi che per analisi di sicurezza. Le sue capacità includono:

- Identificazione di servizi attivi e porte aperte, fornendo una panoramica dello stato di sicurezza di un sistema.
- Esecuzione di audit di sicurezza per individuare vulnerabilità e potenziali punti deboli.
- Inventariazione rapida della rete, utile per la gestione e la comprensione dell'infrastruttura.

**Importante:** È fondamentale comprendere che le stesse funzionalità possono essere utilizzate in modo malevolo per preparare attacchi mirati. Pertanto, è cruciale imparare l'uso di Nmap in ottica difensiva per proteggere i sistemi e le reti da potenziali minacce.