

S11/L5

BONUS 1-NMAP

Parte 1: Esplorazione di Nmap

Le risposte seguenti derivano dall'analisi delle **man pages** (pagine del manuale) di Nmap.

- **Cos'è Nmap?**: È uno strumento open source per l'esplorazione della rete e l'auditing della sicurezza.
- **Per cosa viene usato Nmap?**: Viene utilizzato per determinare quali host sono disponibili in rete, quali servizi (nome applicazione e versione) offrono, quali sistemi operativi eseguono e che tipo di firewall/filtri di pacchetti sono in uso.
- **Cosa fa l'opzione -A?**: Abilita il rilevamento del sistema operativo (OS) e della versione dei servizi, lo scanning tramite script e il traceroute.
- **Cosa fa l'opzione -T4?**: Serve per un'esecuzione più rapida della scansione (timing template).
- **Qual è il comando Nmap usato nell'Esempio 1?**: Il comando è `nmap -A -T4 scanme.nmap.org`.

Parte 2: Scansione delle Porte Aperte

Passo 1: Scansione del Localhost

Analisi basata sull'output del comando `nmap -A -T4 localhost`.

- **Porte e servizi aperti**: La porta **21/tcp** è aperta per il servizio **FTP**.
- **Software fornito**: Il servizio FTP è gestito da **vsftpd 2.0.8 o successivo**. Nota: è consentito l'accesso **Anonymous FTP**.

Passo 2: Scansione della Rete Locale (LAN)

Dati estratti dalla tua configurazione reale e dalle scansioni effettuate.

- **Indirizzo IP e Subnet Mask VM**: IP **192.168.68.59** con subnet mask **255.255.252.0**.

- **Rete di appartenenza:** La VM appartiene alla rete **192.168.68.0/22**.

```
analyst@secOps ~]$ nmap -A -T4 192.168.68.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 10:36 -0500
Stats: 0:03:08 elapsed; 254 hosts completed (2 up), 2 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 10:40 (0:00:12 remaining)
Stats: 0:04:41 elapsed; 254 hosts completed (2 up), 2 undergoing Script Scan
NSE Timing: About 98.80% done; ETC: 10:41 (0:00:00 remaining)
Nmap scan report for 192.168.68.1
Host is up (0.0047s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      dnsmasq 2.84rc2
        dns-nsid:
        _bind.version: dnsmasq-2.84rc2
80/tcp    open  http        OpenWrt uHTTPd
        _http-title: Did not follow redirect to https://192.168.68.1/
443/tcp   open  ssl/https?
        _ssl-date: TLS randomness does not represent time
        _ssl-cert: Subject: commonName=tplinkdeco.net
                    Subject Alternative Name: DNS:tplinkdeco.net, DNS:192.168.68.1, IP Address:192.168.68.1
                    Not valid before: 2010-01-01T00:00:00
                    Not valid after:  2030-12-31T00:00:00
1900/tcp  open  upnp       MiniUPnP 2.2.2 (TP-LINK router; UPnP 1.1)
Service Info: OS: Linux; Devices: WAP, broadband router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.68.54
Host is up (0.0057s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  tcpwrapped
        _http-server-header: nginx
        _http-title: hue personal wireless lighting
443/tcp   open  tcpwrapped
        _http-title: hue personal wireless lighting
        _ssl-cert: Subject: commonName=ecb5fafffe1bf99a/organizationName=Philips Hue/countryName=NL
                    Not valid before: 2017-01-01T00:00:00
                    Not valid after:   2038-01-19T03:14:07
        _http-server-header: nginx
8080/tcp  open  http        Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
        _http-title: Site doesn't have a title.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 338.63 seconds
```

- **Host attivi rilevati:** Sono stati trovati **2 host attivi** nella subnet.
- **Indirizzi IP rilevati:**
 - **192.168.68.1** (Default Gateway/Router TP-Link).
 - **192.168.68.54** (Philips Hue Bridge).
- **Servizi disponibili sugli host:**
 - **Host .1:** DNS (53/tcp), HTTP (80/tcp), HTTPS (443/tcp), UPnP (1900/tcp).
 - **Host .54:** HTTP (80/tcp), HTTPS (443/tcp) tramite **nginx**, e porta 8080/tcp (HTTP).

Passo 3: Scansione Server Remoto

Analisi del target scanme.nmap.org.

- **Scopo del sito:** Imparare Nmap e testare scansioni in modo sicuro.

- **Porte e servizi Aperti:** 22 (ssh), 53 (domain), 80 (http), 9929 (nping-echo), 31337 (tcpwrapped).
- **Porte e servizi Filtrati:** SMTP (25), MSRPC (135), NetBIOS-ssn (139), Microsoft-ds (445), ecc. .
- **Indirizzo IP Server:** 45.33.32.156.
- **Sistema Operativo:** Linux (kernel).

```
[analyst@sec0ps ~]$ nmap -A -T4 scanme.org
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 10:36 -0500
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.18s latency).

Other addresses for scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 995 filtered tcp ports (no-response)

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
| 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:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)

53/tcp    open  domain       dnsmasq 2.84rc2
| dns-nsid:
|_ bind.version: dnsmasq-2.84rc2
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
|_http-favicon: Nmap Project
9929/tcp  open  nping-echo  Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 28.10 seconds
```

Domanda di Riflessione Finale

Come può Nmap aiutare con la sicurezza della rete?

Come può Nmap essere usato da un attore malevolo come strumento nefasto?

- **Aiuto alla sicurezza:** Nmap è fondamentale per il monitoraggio della rete, l'inventario degli host attivi, la gestione dei piani di aggiornamento dei servizi e il controllo dell'uptime.
- **Uso malevolo:** Un attaccante può utilizzarlo per la fase di **ricognizione**, mappando i bersagli e identificando porte aperte o software vulnerabili per pianificare un'intrusione.