S11 L5 - Analisi avanzate: Un approccio pratico - Lab 3

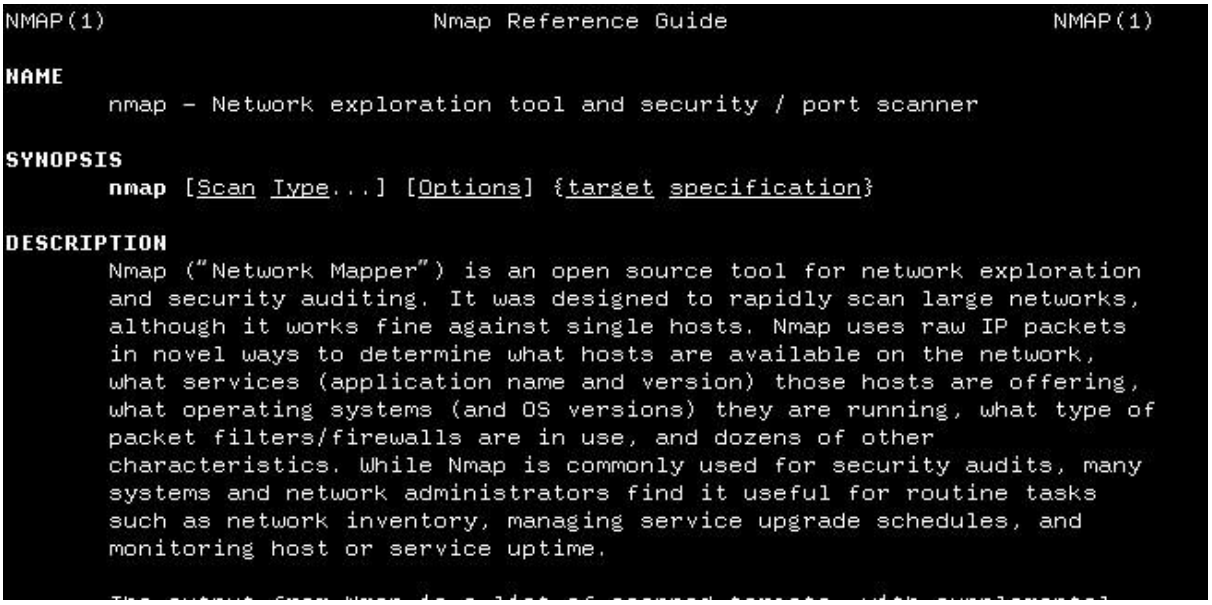
9.3.8 Lab – Exploring Nmap (Answers)

Obiettivi

- Parte 1: Esplorazione di Nmap
- Parte 2: Scansione delle porte aperte

Parte 1: Esplorazione di Nmap

Al prompt del terminale, digitare **man nmap**. Queste pagine possono includere le seguenti sezioni: Nome, Sinossi, Descrizioni, Esempi e Vedere anche.



```
NMAP(1)                    Nmap Reference Guide                    NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open source tool for network exploration
       and security auditing. It was designed to rapidly scan large networks,
       although it works fine against single hosts. Nmap uses raw IP packets
       in novel ways to determine what hosts are available on the network,
       what services (application name and version) those hosts are offering,
       what operating systems (and OS versions) they are running, what type of
       packet filters/firewalls are in use, and dozens of other
       characteristics. While Nmap is commonly used for security audits, many
       systems and network administrators find it useful for routine tasks
       such as network inventory, managing service upgrade schedules, and
       monitoring host or service uptime.
```

Che cos'è Nmap?

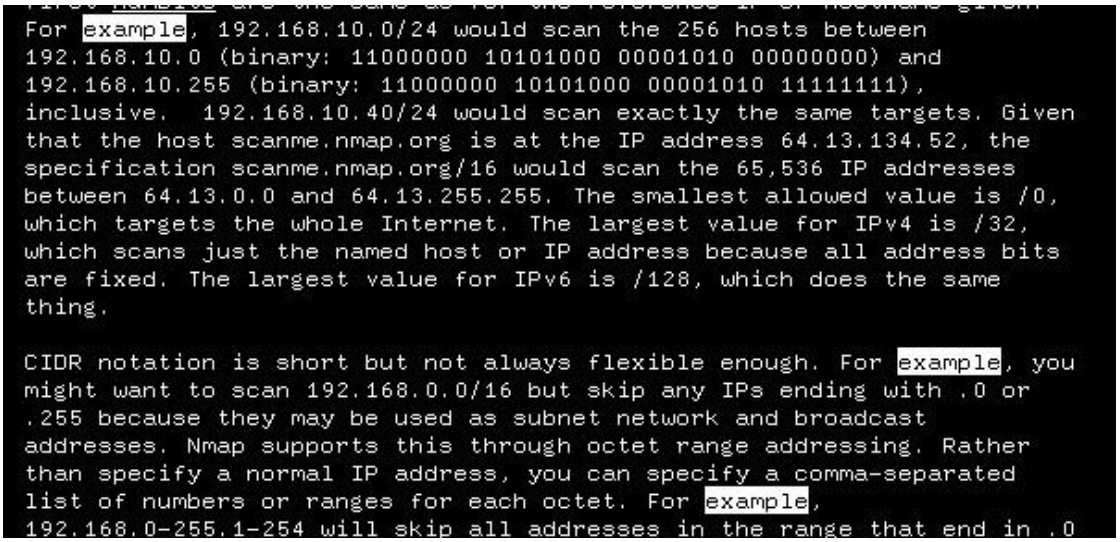
Nmap è uno strumento di esplorazione di rete e di scansione di porte e sicurezza.

A cosa serve nmap?

Nmap viene utilizzato per scansionare una rete e determinare gli host, porte, servizi ed altro.

Digitando **/example**, cercherà la parola **example** in avanti nella pagina man. Per passare alla corrispondenza successiva, premi **n**.

Scorri la pagina per saperne di più su nmap. Digita **q** quando hai finito.



A cosa serve l'interruttore -A?

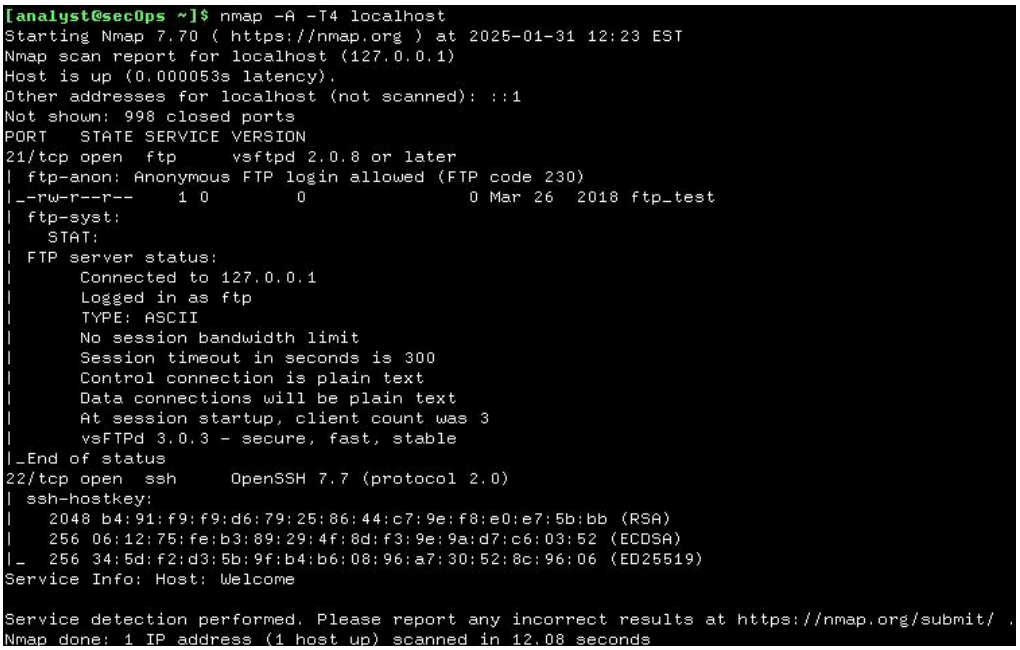
Rileva il sistema operativo.

A cosa serve l'interruttore -T4?

Imposta quanti threats utilizzare per la scansione. Più vengono impostati e più la scansione sarà veloce, allo stesso tempo la scansione genererà un intenso traffico di rete e quindi la scansione sarà più rumorosa. Il massimo dei threats sono 5

Passaggio 1: esegui la scansione del tuo localhost.

Se necessario, apri un terminale sulla VM. Al prompt, digita **nmap -A -T4 localhost.**



Quali porte e servizi sono aperti?

```
21/tcp open  ftp     vsftpd 2.0.8 or later
```

```
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
```

Passaggio 2: esegui la scansione della rete.

Al prompt dei comandi del terminale, digitare **ip address** per determinare l'indirizzo IP e la subnet mask per questo host.

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code
    link/ether 08:00:27:3d:ea:4c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
```

A quale rete appartiene la tua VM?
10.0.2.0/24

Per individuare altri host su questa LAN, immettere **nmap -A -T4 network address/prefix**.

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.15/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 12:30 EST
Nmap scan report for 10.0.2.15
Host is up (0.000053s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 5
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 23.62 seconds
```

Quanti host sono attivi?

Uno: 10.0.2.15

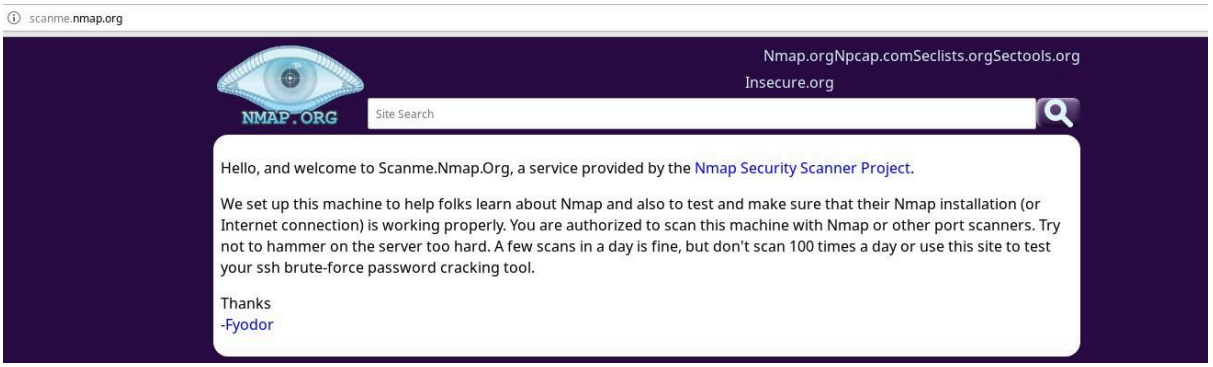
Elenca alcuni dei servizi disponibili sugli host rilevati.

21 ftp

22 ssh

Passaggio 3: eseguire la scansione di un server remoto.

Apri un browser web e vai su scanme.nmap.org . Leggi il messaggio pubblicato.



Qual è lo scopo di questo sito?

Questo sito consente agli utenti di fare pratica con nmap.

Al prompt del terminale, digitare **nmap -A -T4 scanme.nmap.org**

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 12:33 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (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:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.46 seconds
```

Quali porte e servizi sono aperti?

22 ssh
80 http
9929 nping-echo
31337 tcpwrapped

Qual è l'indirizzo IP del server?

```
Nmap scan report for scanme.nmap.org (45.33.32.156)
```

Qual è il sistema operativo?

Linux Ubuntu

Domanda di riflessione

Nmap è un potente strumento per l'esplorazione e la gestione della rete. In che modo Nmap può aiutare con la sicurezza della rete?

Nmap aiuta nella sicurezza della rete identificando dispositivi attivi, porte aperte e servizi esposti. Consente di rilevare la vulnerabilità con lo script NSE, analizzare il firewall, verificare la sicurezza e testare la robustezza delle difese. Essenziale per Red e Blue Team, permette di prevenire attacchi e migliorare la protezione dei sistemi.

In che modo Nmap può essere utilizzato da un threat actor come strumento nefasto?

Un attore di minacce può utilizzare Nmap per raccogliere informazioni sulla rete target, identificando dispositivi, porte aperte e servizi vulnerabili. Può eseguire scansioni stealth per eludere i sistemi di difesa, sfruttare NSE per trovare note falle e analizzare firewall per individuare regole permissive. Questo permette di pianificare attacchi mirati, come sfruttare la forza bruta.