Esplorazione di Nmap

Esplorazione di Nmap

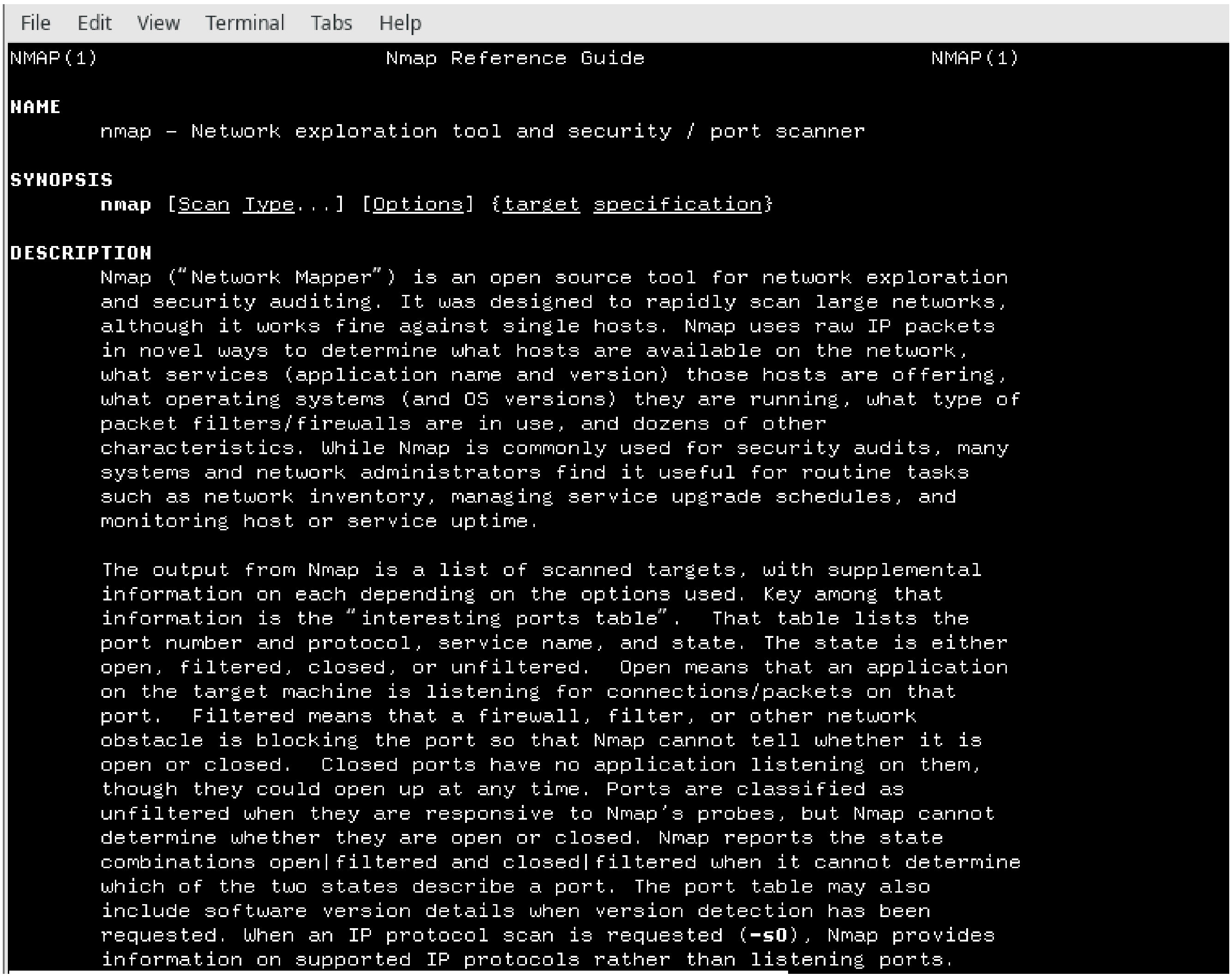
Parte 1: Esplorazione di Nmap

In questa parte utilizzerò le pagine man di Nmap per imparare di più sullo strumento.

Passaggi:

1. Avvio la VM CyberOps Workstation.
2. Apro un terminale.
3. Digito:

```
man nmap
```



```
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.

       The output from Nmap is a list of scanned targets, with supplemental
       information on each depending on the options used. Key among that
       information is the "interesting ports table".  That table lists the
       port number and protocol, service name, and state. The state is either
       open, filtered, closed, or unfiltered.  Open means that an application
       on the target machine is listening for connections/packets on that
       port.  Filtered means that a firewall, filter, or other network
       obstacle is blocking the port so that Nmap cannot tell whether it is
       open or closed.  Closed ports have no application listening on them,
       though they could open up at any time. Ports are classified as
       unfiltered when they are responsive to Nmap's probes, but Nmap cannot
       determine whether they are open or closed. Nmap reports the state
       combinations open|filtered and closed|filtered when it cannot determine
       which of the two states describe a port. The port table may also
       include software version details when version detection has been
       requested. When an IP protocol scan is requested (-sO), Nmap provides
       information on supported IP protocols rather than listening ports.
```

4. Utilizzo le frecce per scorrere il manuale.
5. Uso `/example` per cercare esempi.
6. Il comando utilizzato nel primo esempio trovato è:

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

7. Significato degli switch:
   - `A`: Abilita il rilevamento del sistema operativo, il rilevamento della versione, la scansione degli script e il traceroute.
   - `T4`: Velocizza l'esecuzione, limitando il ritardo massimo della scansione dinamica a 10ms (utile per connessioni broadband o Ethernet).
8. Esco dal manuale con il tasto q.

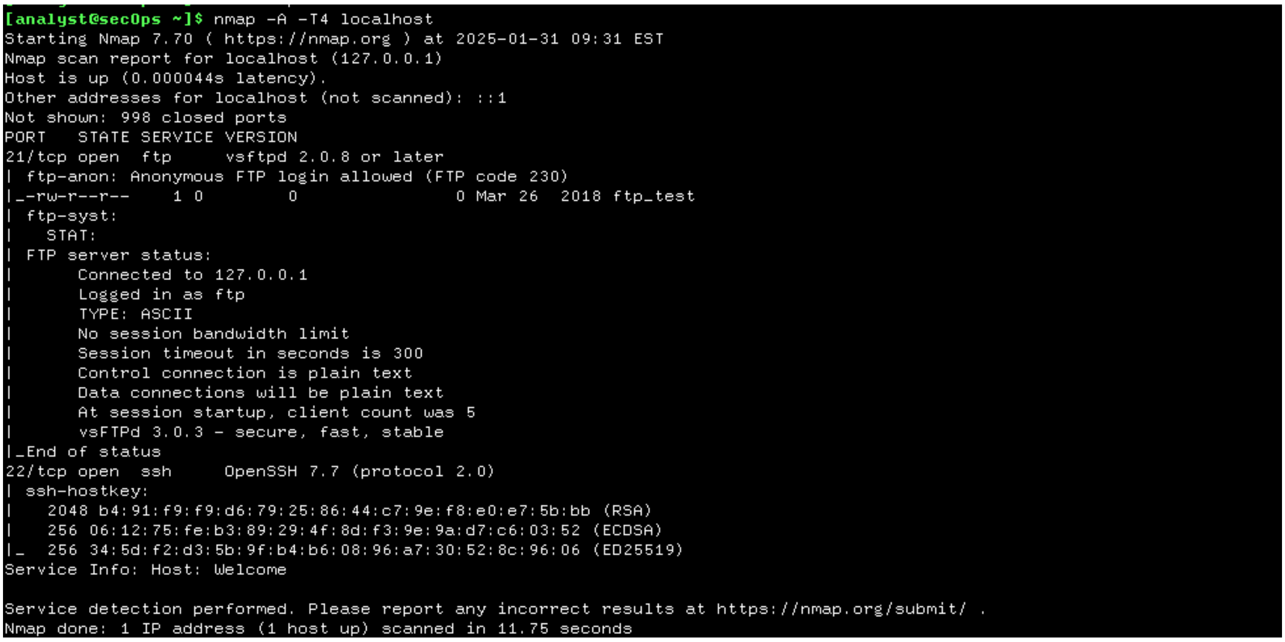
Parte 2: Scansione delle Porte Aperte

Passo 1: Scansione del localhost

1. Apro il terminale e digito:

```
nmap -A -T4 localhost
```

2. Porte e servizi aperti:
   - **21/tcp**: ftp (**vsftpd**)
   - **22/tcp**: ssh (**OpenSSH**)



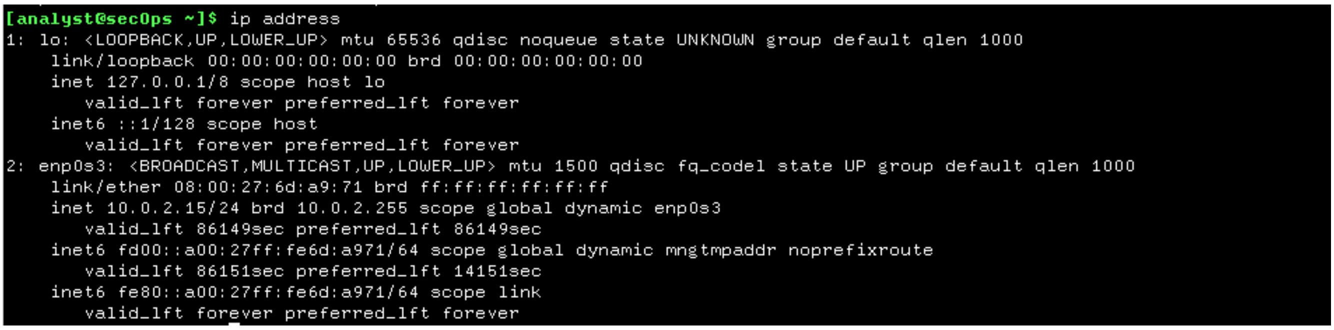
```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 09:31 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  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 127.0.0.1
|      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: 1 IP address (1 host up) scanned in 11.75 seconds
```

Passo 2: Scansione della rete locale

1. Determino l'indirizzo IP della mia VM:

```
ip address
```

2. Identifico la rete a cui appartiene la VM.



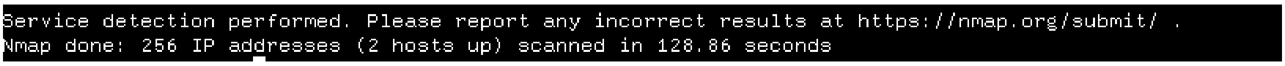
```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6d:a9:71 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86149sec preferred_lft 86149sec
    inet6 fd00::a00:27ff:fe6d:a971/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86151sec preferred_lft 14151sec
    inet6 fe80::a00:27ff:fe6d:a971/64 scope link
       valid_lft forever preferred_lft forever
```

3. Eseguo una scansione della rete sostituendo l'ultimo ottetto dell'IP con `0` (es. **192.168.1.0/24**):

```
nmap -A -T4 192.168.1.0/24
```

4. Risultati della scansione:

   - Numero di host attivi: *2*
   - Indirizzi IP rilevati sulla LAN: *2*

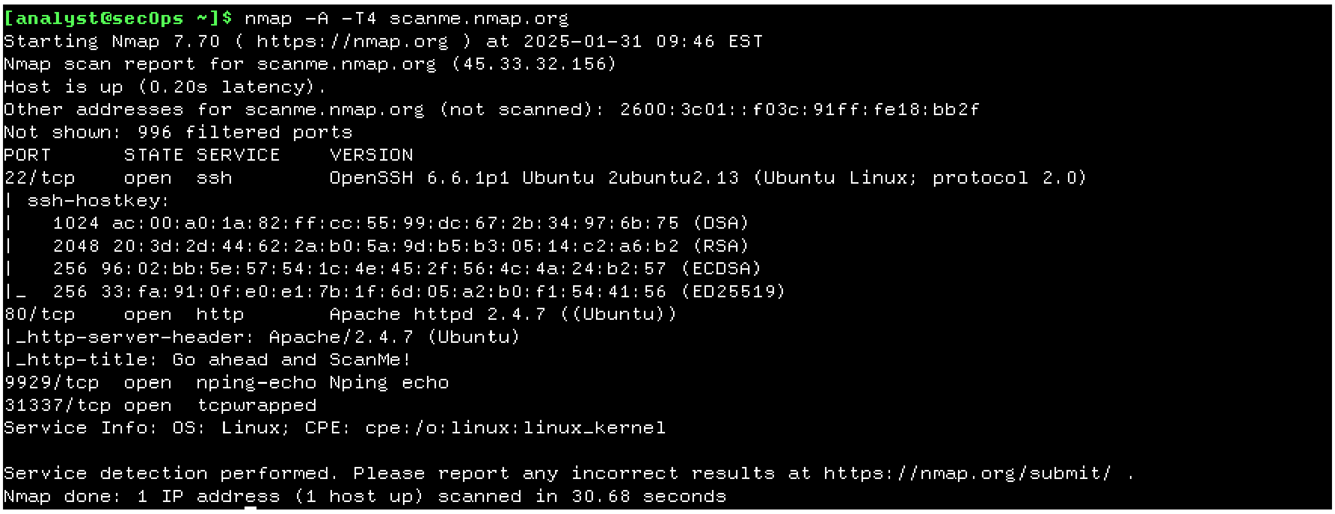


```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 128.86 seconds
```

Passo 3: Scansione di un server remoto

1. Visito il sito scanme.nmap.org per leggere le informazioni.
2. Eseguo la scansione:

```
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 09:46 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s 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 30.68 seconds
```

3. Risultati della scansione:

- **Indirizzo IP**:
  - IPv4: **45.33.32.156**
  - IPv6: **2600:3c01::f03c:91ff:fe18:bb2f**
- **Sistema operativo**: Ubuntu Linux
- **Porte e servizi aperti**:
  - **22/tcp**: ssh (**OpenSSH** 6.6.1p1)

- **80/tcp**: http (**Apache 2.4.7**)
- **9929/tcp**: nping-echo
- **31337/tcp**: tcpwrapped