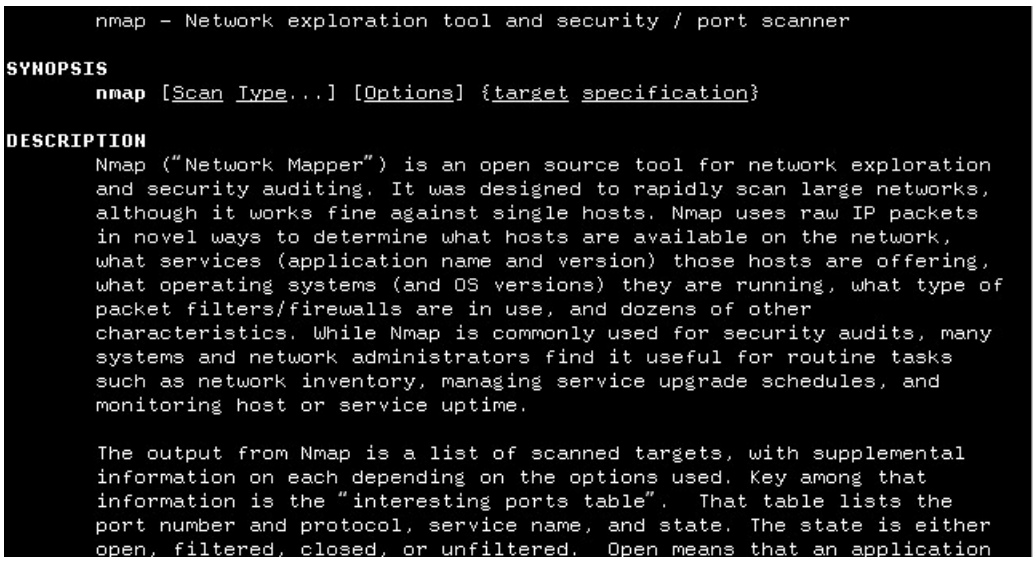
ESERCIZIO 3 – Esplorazione di Nmap

- **Cos'è Nmap?**

Nmap è uno Strumento per l'esplorazione di rete e scanner di sicurezza / porte

- **Per cosa viene usato Nmap?**

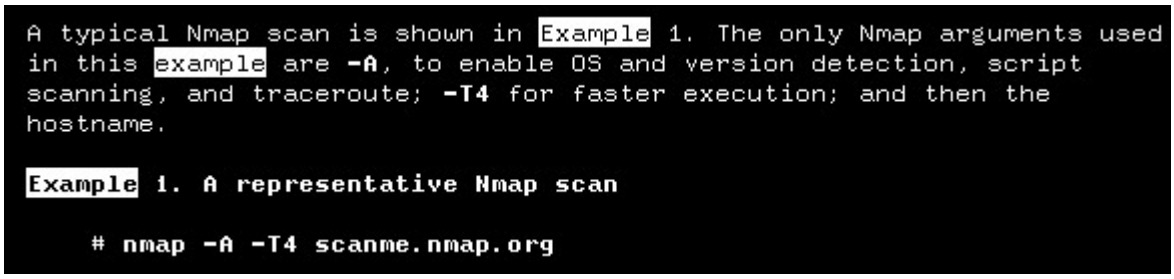
Nmap è uno strumento open source per l'esplorazione della rete e l'auditing della sicurezza.
È stato progettato per eseguire rapidamente la scansione di grandi reti, ma funziona perfettamente anche con singoli host.



```
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
```

- **Qual è il comando Nmap Usato?**

Il comando usato è nmap -A -T4 scanme.nmap.org



```
A typical Nmap scan is shown in Example 1. The only Nmap arguments used
in this example are -A, to enable OS and version detection, script
scanning, and traceroute; -T4 for faster execution; and then the
hostname.

Example 1. A representative Nmap scan

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

- **Cosa fa l'opzione -A?**

Abilita il rilevamento del sistema operativo, rilevamento versione dei servizi, scansione con script, e traceroute

- **Cosa fa l'opzione -T4?**

Esegue la scansione più velocemente

- **Quali porte e servizi sono aperti?**

21/tcp – FTP – vsftpd 2.0.8 or later

22/tcp – SSH – OpenSSH 7.7

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 06:31 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00019s 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 13.00 seconds
```

- **A quale rete appartiene la tua VM?**

Appartiene alla rete 10.0.2.0/24 con IP 10.0.2.15

```
[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 08:00:27:9f:23:c0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 85324sec preferred_lft 85324sec
    inet6 fd00::a00:27ff:fe9f:23c0/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 85946sec preferred_lft 13946sec
    inet6 fe80::a00:27ff:fe9f:23c0/64 scope link
       valid_lft forever preferred_lft forever
```

- **Quanti host sono attivi?**

1 solo host attivo: 10.0.2.15 (VM)

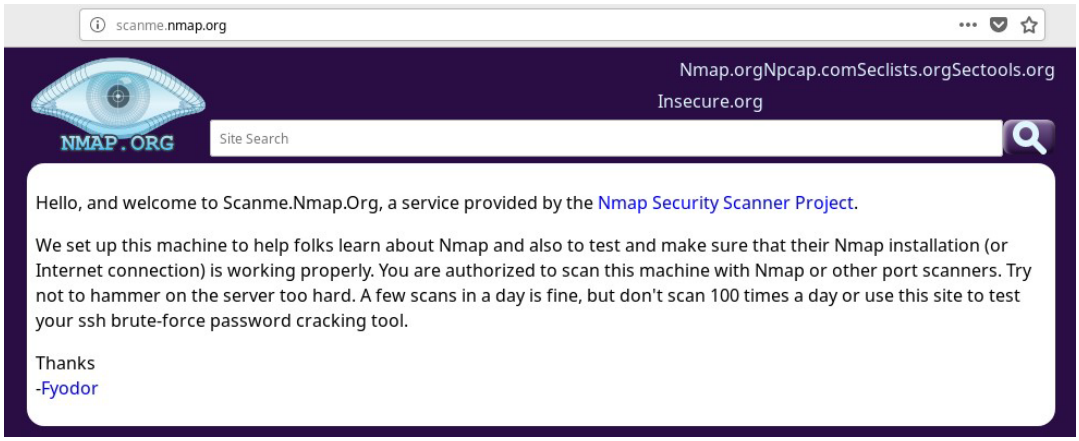
Servizi Attivi:

21/tcp open ftp vsftpd 2.0.8 or later

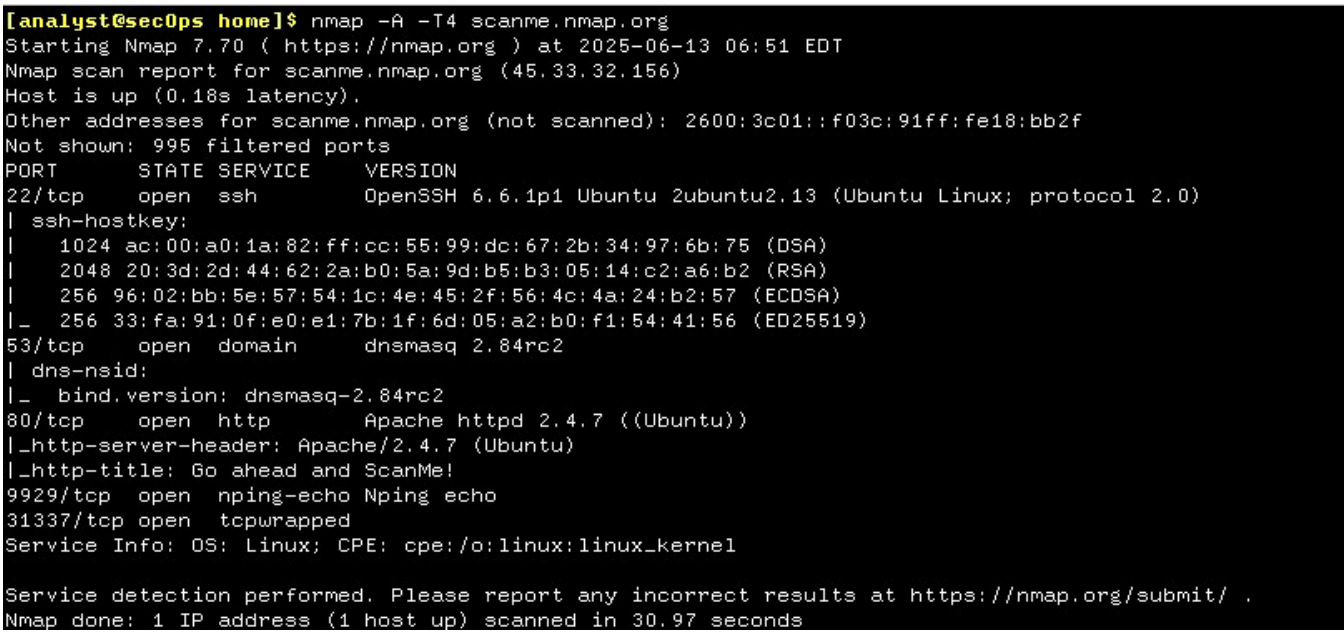
22/tcp open ssh OpenSSH 7.7 (protocol 2.0)

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 06:39 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00020s 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 4
|      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 16.92 seconds
```

- **Quale è lo scopo di questo sito?**



Offrire **un bersaglio legittimo e autorizzato** per testare Nmap e altri port scanner, specialmente in contesti di apprendimento o verifica installazione.



- **Quali porte e servizi sono aperti?**

Porta	Stato	Servizio	Versione
22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13
53/tcp	open	domain (DNS)	dnsmasq 2.84rc2
80/tcp	open	http	Apache httpd 2.4.7 (Ubuntu)
9929/tcp	open	nping-echo	Nping echo
31337/tcp	open	tcpwrapped	

- **Quali porte e servizi sono filtrati?**

995 porte TCP sono filtrate, ma Nmap non elenca i numeri esatti. (messaggio Not Shown)

- **Quale è l'indirizzo IP del server?**

45.33.32.156

- **Quale è il sistema operativo?**

Linux

- **Riflessione: Nmap è uno strumento potente per l'esplorazione e la gestione della rete. Come può aiutare con la sicurezza della rete? E come può essere usato da un attore malevolo?**

Nmap è uno strumento neutrale: può rafforzare la sicurezza oppure essere usato per scopi dannosi. La differenza la fa l'intenzione dell'utente. Per concludere vediamo alcuni esempi per utilizzarlo in modo Difensivo e Offensivo

Difensivo

- Scoprire host attivi e servizi aperti
- Mappare la rete per scopi di sicurezza
- Identificare software vulnerabili
- Verificare se un firewall funziona correttamente

Offensivo

- Cercare porte e servizi deboli
- Trovare software non aggiornato
- Preparare attacchi come exploit o forza bruta