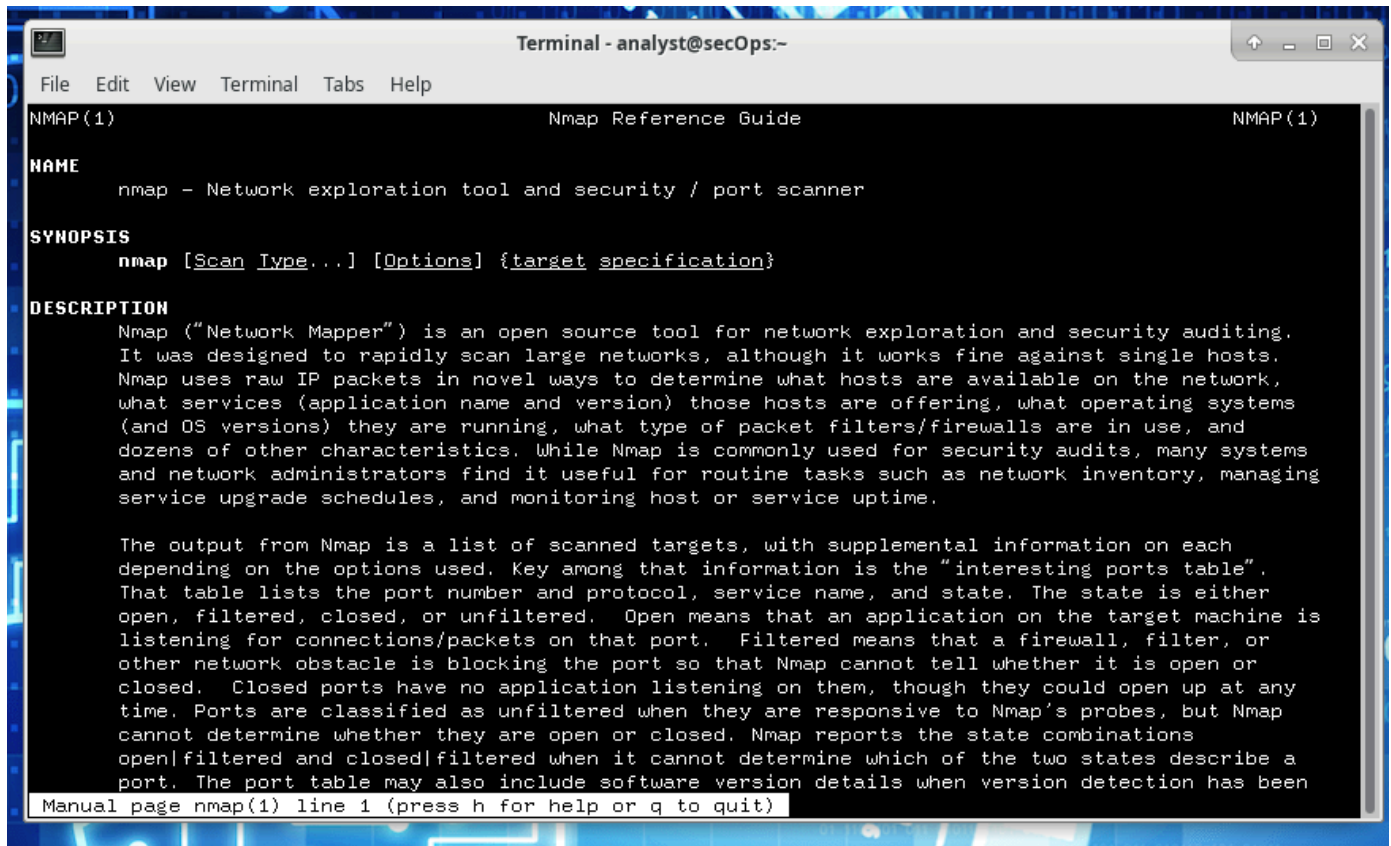


BONUS nmap

Ho lanciato un `man nmap` per ottenere un manuale di **nmap**.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

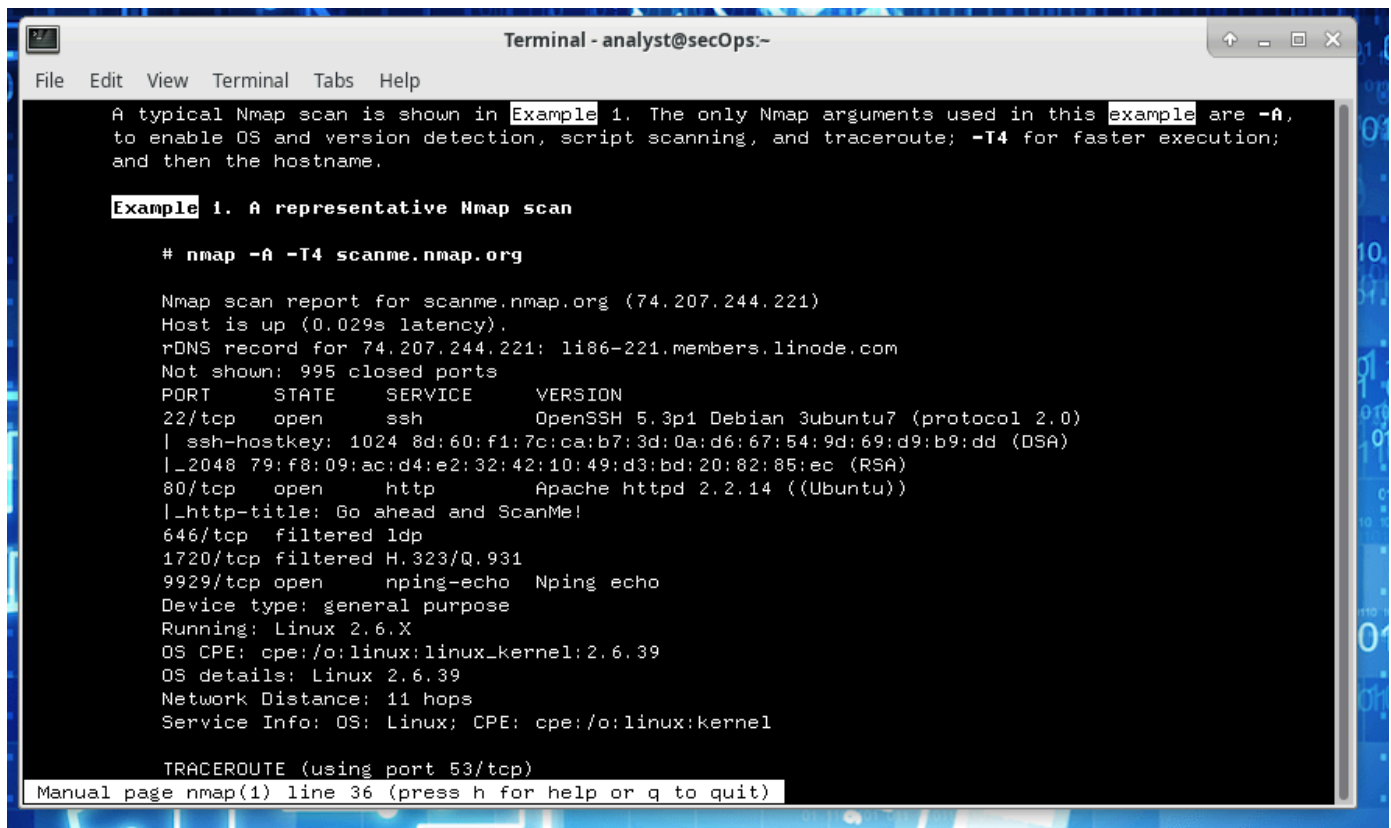
SYNOPSIS
    nmap [Scan Type...] [Options] {target specification}

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

Manual page nmap(1) line 1 (press h for help or q to quit)
```

con `/example` ho ottenuto degli esempi pratici di scansione.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

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

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: 1186-221.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 ldp
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

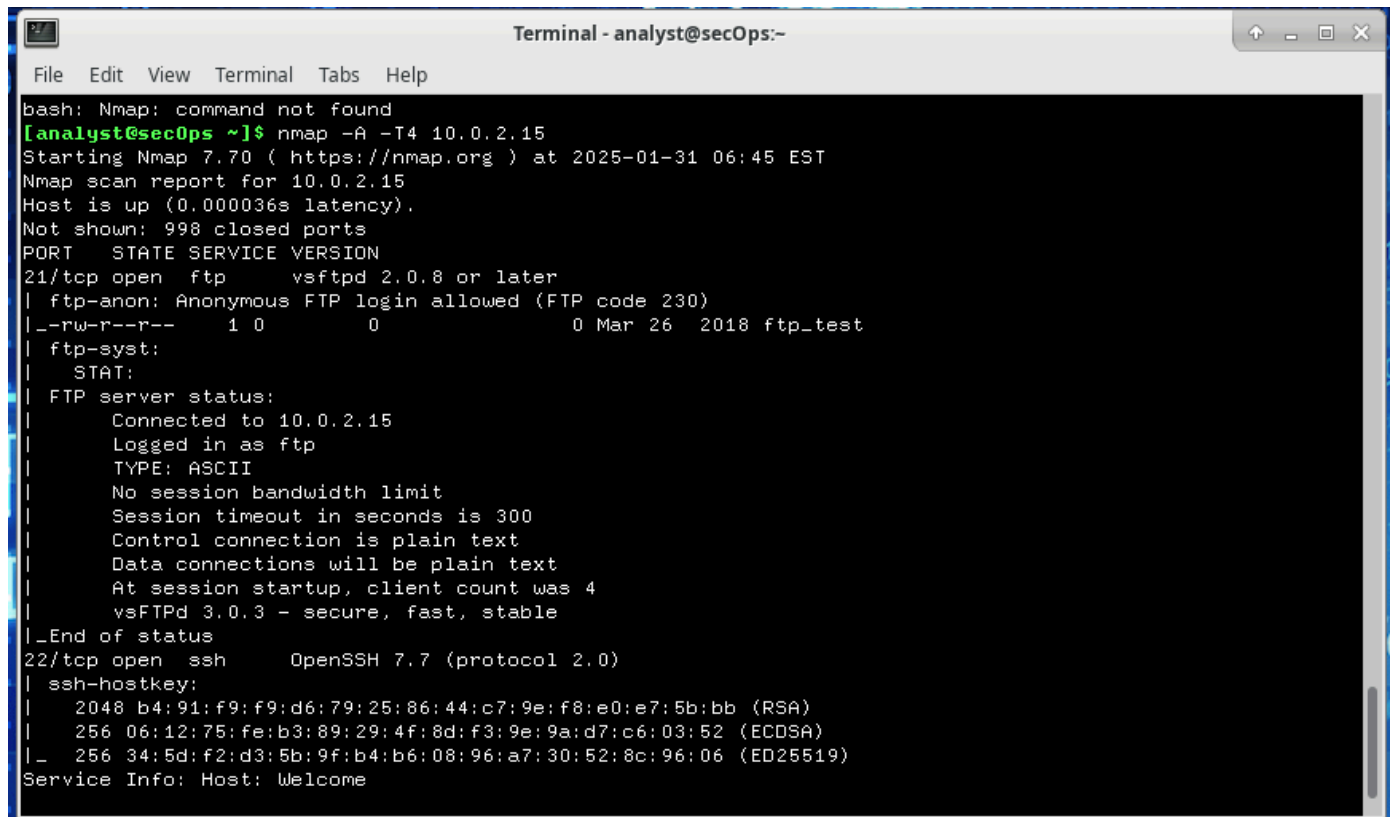
TRACEROUTE (using port 53/tcp)

Manual page nmap(1) line 36 (press h for help or q to quit)
```

Prendendo spunto ho lanciato un `nmap -A -T4`

- -A: Abilita il rilevamento del sistema operativo, il rilevamento della versione, la scansione degli script e il traceroute.
- -T4: per un'esecuzione più rapida impedendo al ritardo della scansione dinamica di superare i 10 ms per le porte TCP. -T4 è consigliato per una connessione a banda larga o Ethernet decente.

verso di me e mi ha mostrato tutte le porte aperte sul mio host.



```
bash: Nmap: command not found
[analyst@secOps ~]$ nmap -A -T4 10.0.2.15
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 06:45 EST
Nmap scan report for 10.0.2.15
Host is up (0.000036s 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
```

stessa cosa fatta con un server.

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
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 12.00 seconds  
[analyst@secOps ~]$ nmap -A -T4 libero.it  
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 06:47 EST  
Nmap scan report for libero.it (213.209.17.209)  
Host is up (0.013s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE      VERSION  
53/tcp    open  domain       dnsmasq 2.84  
| dns-nsid:  
|_ bind.version: dnsmasq-2.84  
80/tcp    open  http         nginx  
|_http-title: Did not follow redirect to https://www.libero.it/  
443/tcp   open  tcpwrapped  
|_http-title: 400 The plain HTTP request was sent to HTTPS port  
| ssl-cert: Subject: commonName=*.libero.it/organizationName=Italiaonline S.p.a./stateOrProvinceName=Milano/countryName=IT  
| Subject Alternative Name: DNS:*.libero.it, DNS:libero.it  
| Not valid before: 2024-08-28T00:00:00  
|_Not valid after: 2025-08-28T23:59:59  
|_ssl-date: TLS randomness does not represent time  
| tls-nextprotoneg:  
|_ h2  
|_ http/1.1  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 20.70 seconds  
[analyst@secOps ~]$
```