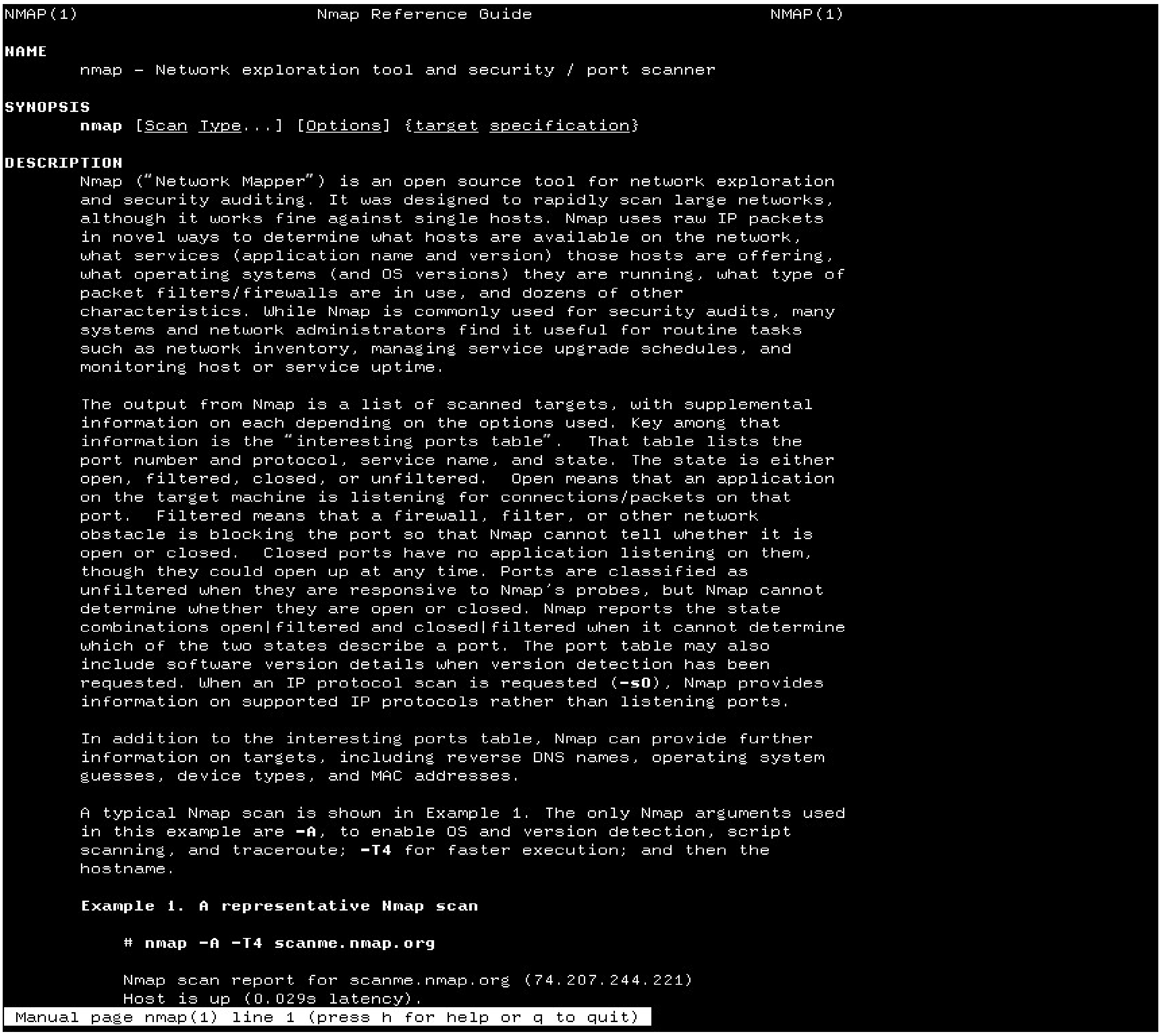
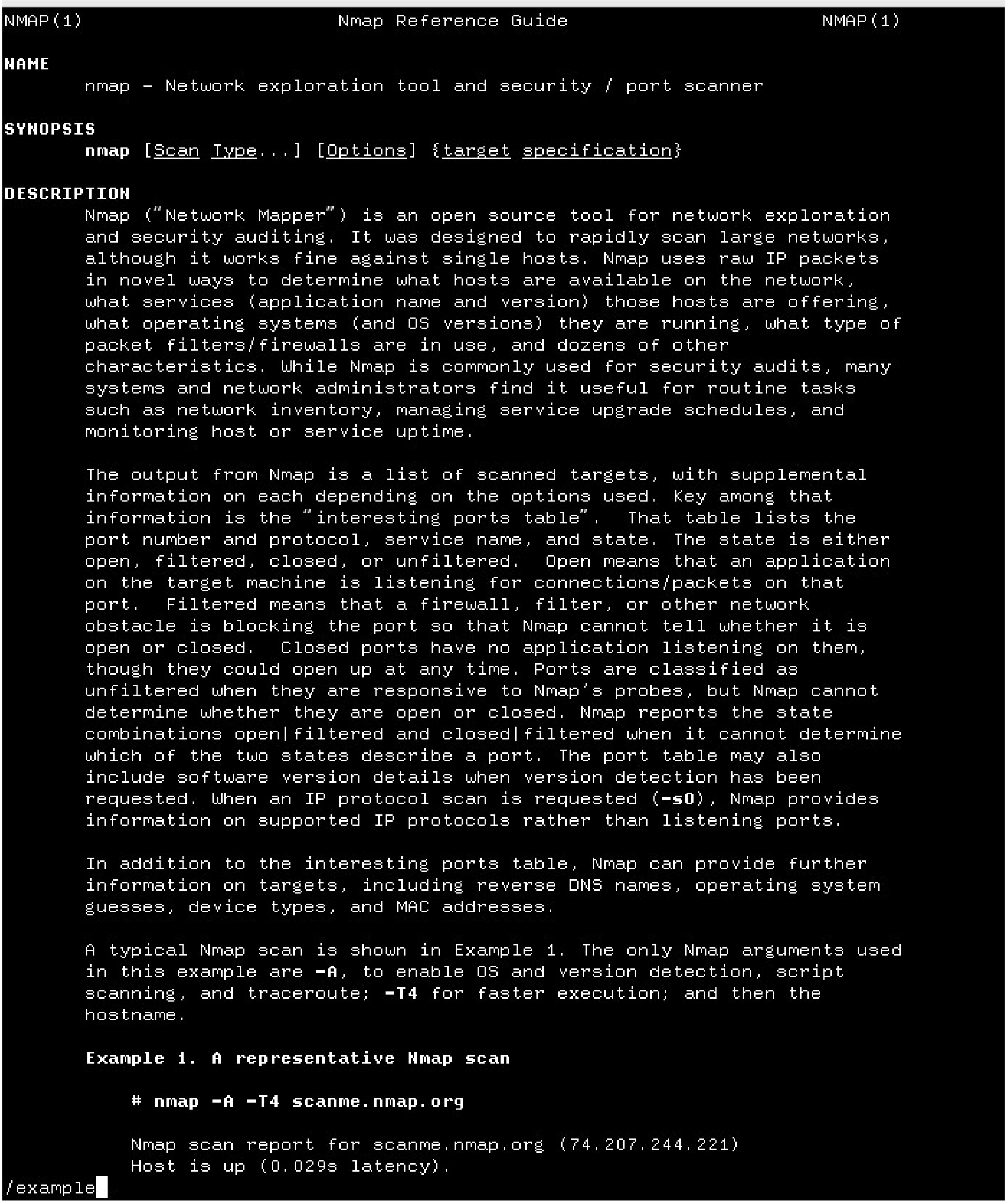
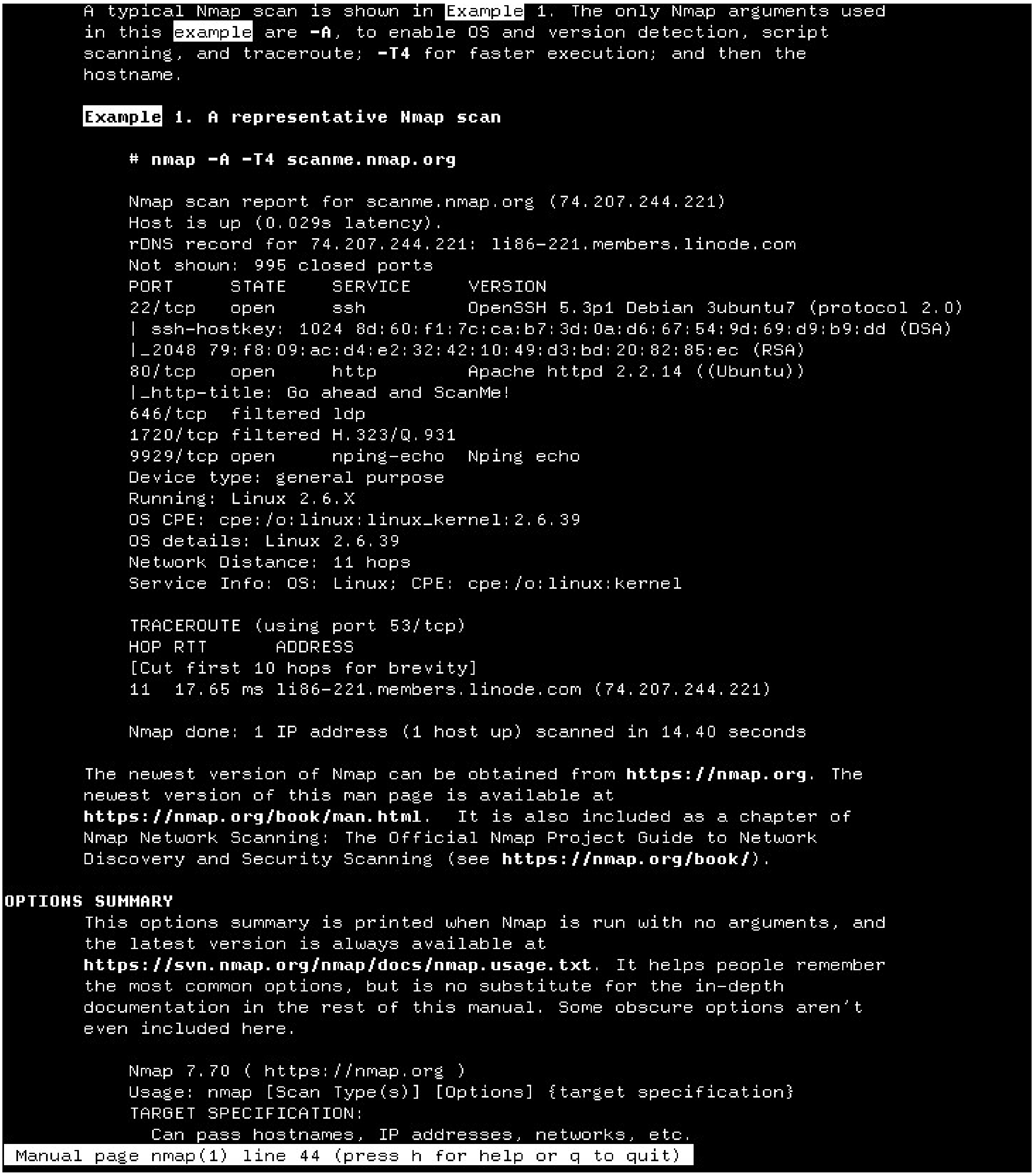
Esplorazione di Nmap



```
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.

       In addition to the interesting ports table, Nmap can provide further
       information on targets, including reverse DNS names, operating system
       guesses, device types, and MAC addresses.

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



```
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.

       In addition to the interesting ports table, Nmap can provide further
       information on targets, including reverse DNS names, operating system
       guesses, device types, and MAC addresses.

       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).
/example
```



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: li86-221.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)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

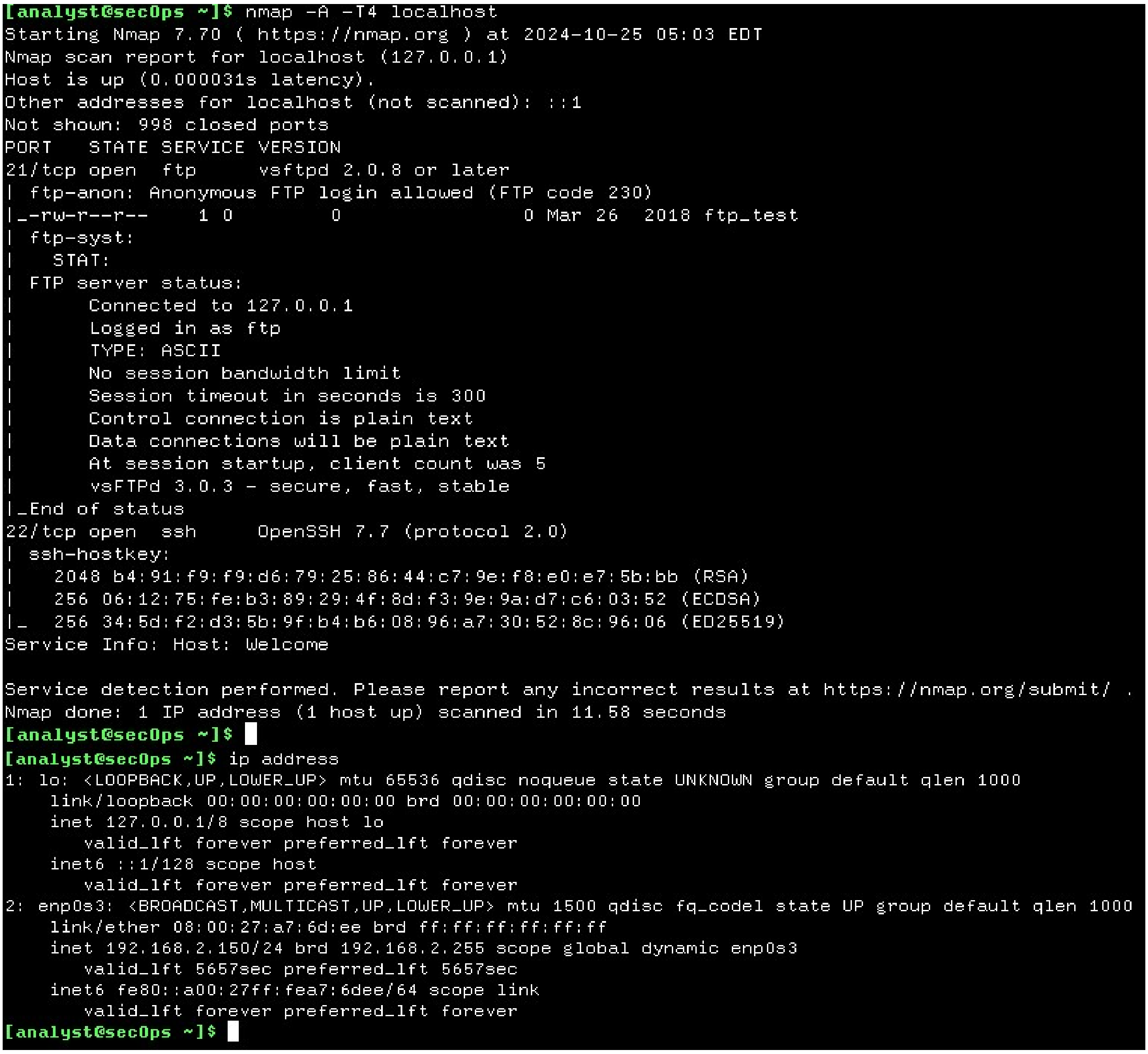
The newest version of Nmap can be obtained from **https://nmap.org**. The newest version of this man page is available at **https://nmap.org/book/man.html**. It is also included as a chapter of Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning (see **https://nmap.org/book/**).

OPTIONS SUMMARY

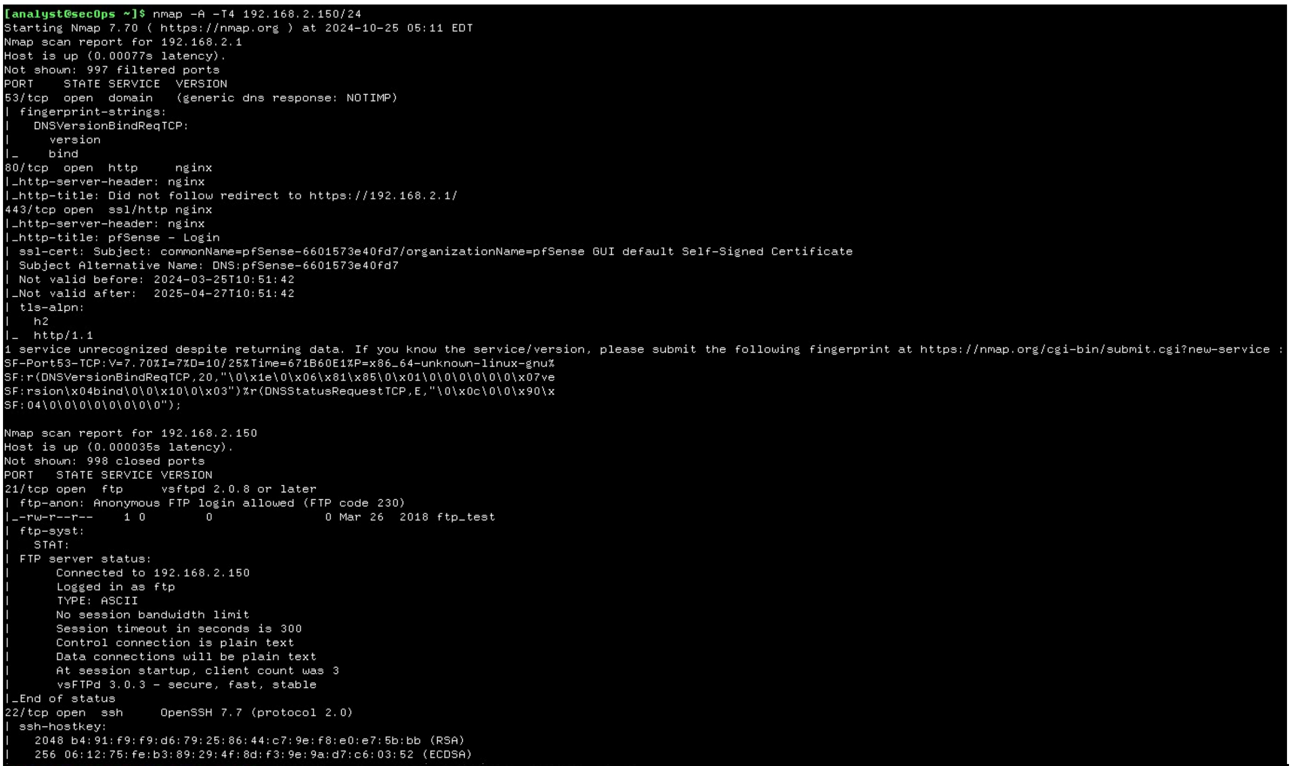
This options summary is printed when Nmap is run with no arguments, and the latest version is always available at **https://svn.nmap.org/nmap/docs/nmap.usage.txt**. It helps people remember the most common options, but is no substitute for the in-depth documentation in the rest of this manual. Some obscure options aren't even included here.

```
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
```

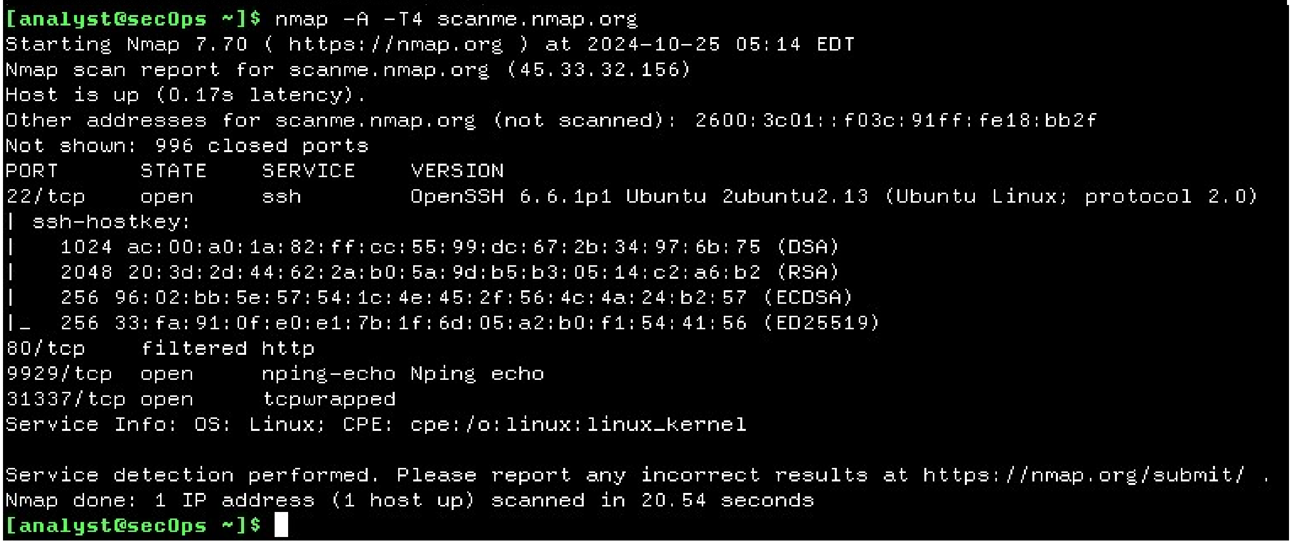
Manual page nmap(1) line 44 (press h for help or q to quit)



```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 05:03 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000031s 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 11.58 seconds
[analyst@secOps ~]$ 
[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:a7:6d:ee brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.150/24 brd 192.168.2.255 scope global dynamic enp0s3
       valid_lft 5657sec preferred_lft 5657sec
    inet6 fe80::a00:27ff:fea7:6dee/64 scope link
       valid_lft forever preferred_lft forever
[analyst@secOps ~]$ 
```



```
[analyst@secOps ~]$ nmap -A -T4 192.168.2.150/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 05:11 EDT
Nmap scan report for 192.168.2.1
Host is up (0.00077s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   (generic dns response: NOTIMP)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp  open  http     nginx
|_http-server-header: nginx
|_http-title: Did not follow redirect to https://192.168.2.1/
443/tcp open  ssl/http nginx
|_http-server-header: nginx
|_http-title: pfSense - Login
| ssl-cert: Subject: commonName=pfSense-6601573e40fd7/organizationName=pfSense GUI default Self-Signed Certificate
| Subject Alternative Name: DNS:pfSense-6601573e40fd7
| Not valid before: 2024-03-25T10:51:42
|_Not valid after:  2025-04-27T10:51:42
| tls-alpn:
|   h2
|_  http/1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=10/25%Time=671B60E1%P=x86_64-unknown-linux-gnu%
SF:r(DNSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x85\0\x01\0\0\0\0\0\0\x07ve
SF:rsion\x04bind\0\0\x10\0\x03")%r(DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x
SF:04\0\0\0\0\0\0\0\0");

Nmap scan report for 192.168.2.150
Host is up (0.000035s 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 192.168.2.150
|      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 3
|      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)
```



```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 05:14 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed 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    filtered http
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 20.54 seconds
[analyst@secOps ~]$ 
```