

Esplorazione di Nmap

Exploring Nmap

1. Ho aperto un terminale ho digitato **man nmap**. Poi ho digitato **/example** e premuto **ENTER**. Questo ha cercato la parola "example" in avanti all'interno della pagina del manuale.

```
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 requested. When an IP protocol scan is requested (-s0), 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).
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:9a: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/2.2.14 ((Ubuntu))
|_ .http-title: Go ahead and ScanMe!
540/tcp   filtered idr
1750/tcp  filtered H.323/Q.931
9929/tcp  open  rping-echo Nping echo
Device type: generic 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
[Out first 10 hops for brevity]
11 17.65 ms 1186-221.members.linode.com (74.207.244.221)
Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
/example:|
```

Example 1. A representative Nmap scan

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

Viene eseguito il comando nmap nella forma: **nmap -A -T4 scanme.nmap.org**

L'opzione **-A** abilita il rilevamento del sistema operativo, il rilevamento della versione, la scansione degli script e il traceroute. È essenzialmente un'opzione per una scansione aggressiva che combina diverse funzionalità.

L'opzione **-T4** è utilizzata per un'esecuzione più veloce della scansione, limitando il ritardo dinamico della scansione a non più di 10 ms per le porte TCP. Questa opzione è particolarmente consigliata quando si dispone di una connessione a banda larga o ethernet decente, poiché offre un buon equilibrio tra velocità e affidabilità.

```
# 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  ldap
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
```

Scanning for Open Ports

1. Da terminale, ho digitato **nmap -A -T4 localhost**. La scansione ha impiegato pochi secondi.

```
[analyst@sec0ps ~]$ nmap -A T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 11:25 EDT
Failed to resolve "T4".
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000058s 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 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: 1 IP address (1 host up) scanned in 12.02 seconds
```

Ho identificato due porte aperte con i relativi servizi: La porta 21/tcp esegue il servizio ftp, gestito dal software vsftpd La porta 22/tcp esegue il servizio ssh, gestito dal software OpenSSH

2. Da Terminale, ho digitato **ip address** per determinare l'indirizzo IP e la subnet mask per questo host.

```
[analyst@sec0ps ~]$ 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 08:00:27:2d:a7:f4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.160/24 brd 192.168.50.255 scope global dynamic enp0s3
        valid_lft 6644sec preferred_lft 6644sec
    inet6 fe80::a00:27ff:fe2d:a7f4/64 scope link
        valid_lft forever preferred_lft forever
```

3. Per scansionare l'intera rete ho usato il comando **nmap -A -T4 192.168.50.0/24**

```
[analyst@sec0ps ~]$ nmap -A -T4 192.168.50.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 11:30 EDT
Nmap scan report for 192.168.50.1
Host is up (0.0035s latency).
Not shown: 998 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: pfSense - Login
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$I=7$I=10/25$Time=671BB993$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");
```

Oltre alla mia macchina nmap ha rilevato la PfSense attiva nella mia rete. Le porte aperte sono la 53(open domain) e la porta 80(http) nginx.

4. Ho aperto un browser web e sono andato all'indirizzo **scanme.nmap.org**. Ho letto il messaggio pubblicato.

Poi, da terminale, ho digitato **nmap -A -T4 scanme.nmap.org**.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 11:43 EDT
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: 995 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)
25/tcp    filtered smtp
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 30.80 seconds
```

Ho identificato diverse porte aperte nel sistema, che includono la porta 22/tcp che esegue ssh, la porta 80/tcp che esegue http, la porta 9929(servizio nping), la porta 31337 servizio: tcpwrapped. Durante la scansione ho anche rilevato alcune porte filtrate: la porta 25/tcp che gestisce smtp. Il server utilizza due indirizzi, un IPv4 che è 45.33.32.156 e un IPv6 che corrisponde a 2600:3c01::f03c:91ff:fe18:bb2f.

Ho potuto determinare che il sistema operativo in esecuzione sul server è Ubuntu Linux.