

Analisi di Nmap

Esaminando lo strumento Nmap tramite la sua pagina manuale (man page), è stato possibile approfondire la conoscenza delle caratteristiche e delle capacità di questo potente software per il networking. Nmap, abbreviazione di Network Mapper, è un'applicazione open source progettata principalmente per l'esplorazione e l'analisi delle reti. Consente di individuare i dispositivi attivi su una rete, identificare le porte aperte, rilevare i servizi in esecuzione e persino determinare il sistema operativo utilizzato.

```
Terminal - analyst@secOps-

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).
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 tcp
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
|_ 1 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

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

Utilizzando il comando `man nmap`, si accede a una guida dettagliata che include varie sezioni, come la descrizione generale dello strumento, la sintassi dei comandi, esempi pratici e un elenco delle opzioni più comuni. L'interfaccia della pagina manuale permette di scorrere agevolmente il contenuto e di effettuare ricerche specifiche tramite la funzione di ricerca con il simbolo `/`. Nel nostro caso, abbiamo cercato la parola chiave `/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: 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 tcp
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
|_ 1 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

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.
```

Uno degli esempi più rilevanti che abbiamo trovato nella pagina man è rappresentato dal seguente comando:

Analizzando questo comando, emerge che l'opzione `-A` attiva una scansione “aggressiva”, la quale integra funzionalità avanzate quali l'identificazione del sistema operativo del target, il rilevamento delle versioni dei servizi in esecuzione, l'esecuzione di script per approfondimenti e il tracciamento del percorso di rete (traceroute). Questa modalità è particolarmente utile per ottenere una panoramica completa dello stato di un host o di un'intera rete.

L'opzione `-T4`, invece, serve a regolare la velocità con cui viene effettuata la scansione. Impostando questo parametro a 4 (su una scala da 0 a 5), Nmap esegue la scansione in modo più rapido, riducendo i tempi senza sacrificare troppo la precisione. Questa impostazione è ideale in reti affidabili.

Parte 2: Analisi delle Porte Aperte

```
[analyst@secOps ~]$ man nmap
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 10:27 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000062s 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 12.96 seconds
[analyst@secOps ~]$
```

Utilizzando il comando `nmap -A -T4 localhost`, è stata effettuata una scansione approfondita del sistema locale. Il risultato ha evidenziato la presenza di due porte aperte, ognuna associata a un servizio attivo.

Porte rilevate:

- **21/tcp (FTP):** Il servizio FTP è operativo grazie a *vsftpd*, in una versione pari o successiva alla 2.0.8 (nello specifico 3.0.3). L'accesso anonimo è abilitato, il che implica che chiunque può

connettersi al server senza credenziali. Dal punto di vista della sicurezza, si tratta di un aspetto che merita attenzione. La scansione ha anche rivelato ulteriori dettagli, tra cui l'uso della modalità ASCII per il trasferimento dati, l'assenza di limiti di banda e un timeout di sessione impostato a 300 secondi.

- **22/tcp (SSH):** Il protocollo SSH è in funzione tramite *OpenSSH* versione 7.7. Sono state rilevate diverse chiavi host per la cifratura della connessione (RSA, ECDSA e ED25519), utili per garantire una comunicazione sicura tra client e server.

Tutte le altre 998 porte risultano chiuse, quindi non accessibili a richieste esterne

Passo 2: Scansione della Rete Locale

a. Identificazione dell'indirizzo IP e della subnet mask

Tramite il comando `ip address`, è stato possibile determinare i dati di configurazione della macchina virtuale. L'interfaccia di rete attiva è `enp0s3`, con indirizzo IP 192.168.125.102 e subnet mask /24 (equivalente a 255.255.255.0). Queste informazioni collocano la VM all'interno della rete 192.168.125.0/24, che comprende gli indirizzi da 192.168.125.1 a 192.168.125.254.

```
[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 08:00:27:89:41:d5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.125.102/24 brd 192.168.125.255 scope global dynamic enp0s3
        valid_lft 6807sec preferred_lft 6807sec
    inet6 fe80::a00:27ff:fe89:41d5/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

b. Rilevamento degli host sulla LAN

La scansione della rete locale è stata eseguita con il comando `nmap -A -T4 192.168.125.0/24`, che ha permesso di individuare altri dispositivi attivi.

```
[analyst@sec0ps ~]$ nmap -A -T4 192.168.125.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 10:34 EDT
Nmap Scan report for 192.168.125.1
Host is up (0.0087s 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
|_ 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=7.70I=7XD=6/13Time=684C371BIP=x86_64-unknown-linux-gnuIR
SF:(DNSVersionBindReqTCP,20,"\\0\\x1e\\0\\x06\\x81\\x85\\0\\x01\\0\\0\\0\\0\\0\\0\\x07ver
SF:sion\\x04bind\\0\\x10\\0\\x03")zr(DNSStatusRequestTCP,E,"\\0\\x0c\\0\\0\\x90\\x0
SF:4\\0\\0\\0\\0\\0\\0\\0");
Nmap scan report for 192.168.125.102
Host is up (0.00029s 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 192.168.125.102
|     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 2
|     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:a7:5b: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 (2 hosts up) scanned in 43.25 seconds
[analyst@sec0ps ~]$
```

Dal risultato della scansione Nmap sulla rete 192.168.125.0/24, risulta che sono attivi 2 host nella stessa LAN della tua macchina virtuale. Entrambi gli indirizzi IP rilevati appartengono alla stessa sottorete /24, quindi si trovano sulla stessa rete locale della tua VM.

Gli host attivi rilevati sono:

- 192.168.125.1
- 192.168.125.102

Vediamo ora quali servizi risultano accessibili su ciascun host:

192.168.125.1

Questo host sembra essere un **firewall pfSense**, riconoscibile dalla pagina di login web che appare sulla porta **80 (HTTP)**. Il server web in uso è **nginx**. Inoltre, risulta aperta anche la porta **53 (TCP)**, utilizzata solitamente per il servizio **DNS**. Tuttavia, Nmap non è riuscito a identificare completamente il servizio DNS attivo, anche se ha restituito una risposta generica (NOTIMP), il che potrebbe indicare una configurazione particolare.

192.168.125.102

Questo host presenta due porte aperte:

- La **porta 21 (FTP)**, dove è attivo un server **vsftpd**. Da notare che l'accesso anonimo è **abilitato**, cosa piuttosto rischiosa in termini di sicurezza, soprattutto se il server consente anche l'upload di file.
- La **porta 22 (SSH)**, che offre accesso tramite shell remota. Il servizio è gestito da **OpenSSH**, versione 7.7. Le chiavi host SSH sono state rilevate, il che indica che la connessione è disponibile e attiva.

Questa analisi ha fornito una mappatura chiara dei dispositivi presenti sulla rete e dei servizi attivi su ciascuno.

Passo 3: Scansione di un Server Remoto

Visitando il sito web **scanme.nmap.org**, si apprende che il suo scopo è quello di offrire un ambiente controllato per effettuare test legittimi con Nmap. Il sito è gestito direttamente dal team di sviluppo di Nmap, che consente esplicitamente agli utenti di eseguire scansioni sul server per scopi didattici o sperimentali, evitando così qualsiasi rischio di violazione legale.

La scansione eseguita con il comando `nmap -A -T4 scanme.nmap.org` ha fornito i seguenti risultati:

- **IP del server:** 45.33.32.156
- **Sistema operativo:** Linux
- **Porte aperte:**
 - 22/tcp – SSH tramite *OpenSSH 6.6.1p1*
 - 80/tcp – HTTP gestito da *Apache 2.4.7*
 - 9929/tcp – Servizio *nping-echo*
 - 31337/tcp – Protetta da *tcpwrapped*, che limita l'interazione diretta
- **Porta filtrata:**
 - 7004/tcp – Non accessibile, probabilmente a causa di un firewall