

Es.3 Relazione su Nmap

Relazione Nmap

🔖 Tag: [#nmap](#) [#pentesting](#) [#scansione](#) [#menù](#)

La prima immagine rappresenta il menù principale di Nmap, uno strumento open source utilizzato per l'esplorazione e la sicurezza di reti. Nmap è particolarmente utile per identificare host e servizi attivi su una rete, rilevare porte aperte e vulnerabilità. Il menù mostra la sintassi di base del comando Nmap, che include diversi tipi di scansioni e opzioni, personalizzabili a seconda dell'obiettivo dell'analisi.

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).
```

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

Utilizzo dell'Opzione **-A** e **-T4**



Tag:

[#nmap](#)

[#scansioneavanzata](#)

[#analisiOs](#)

La seconda immagine mostra l'uso di Nmap con l'opzione **-A** e **-T4**.

L'opzione **-A** abilita il rilevamento del sistema operativo, delle versioni dei servizi attivi e l'esecuzione di script di default, fornendo un'analisi più dettagliata dell'host target. L'opzione **-T4** aumenta la velocità di scansione, utile in ambienti dove la velocità è critica, come durante test in grandi reti. La scansione fornisce dettagli su porte, servizi e sistema operativo in esecuzione.

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).
```

/example

Scansione di localhost

🔖 Tag: [#localhost](#) [#pentesting](#) [#nmap](#)

La quarta immagine illustra una scansione effettuata su `localhost`, ovvero l'indirizzo IP locale della macchina su cui viene eseguito il

comando. L'output mostra porte aperte come FTP sulla porta 21 con accesso anonimo e SSH sulla porta 22 con OpenSSH 7.7. La scansione `localhost` è utile per testare rapidamente i servizi attivi sulla propria macchina e individuare potenziali vulnerabilità locali.

```
[analyst@sec0ps ~]$ 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@sec0ps ~]$
```

Verifica IP

🔖 Tag: [#verificaIP](#) [#nmap](#) [#controlli](#) [#reti](#)

La quinta immagine rappresenta una verifica dell'indirizzo IP utilizzando `ip address`. Questo passaggio è cruciale per confermare l'indirizzo IP attivo della macchina prima di eseguire scansioni su specifici obiettivi di rete. In questo caso, l'indirizzo attivo è `192.168.2.150/24`.

```
[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: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@sec0ps ~]$
```

Scansione su Indirizzo IP Specifico



Tag:

#scansioneip

#nmap

#pfsense

#reti

Nella sesta immagine, viene eseguita una scansione Nmap sull'indirizzo IP 192.168.2.150, un dispositivo di rete con servizi HTTP e HTTPS attivi. La scansione rivela che il server HTTP utilizza Nginx e che la porta 443 serve l'interfaccia di login di pfSense. Sono stati rilevati anche servizi FTP con accesso anonimo, evidenziando possibili rischi di sicurezza.

```
[analyst@sec0ps ~]$ 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=7.70XI=7XD=10/25XTime=671B60E1IP=x86_64-unknown-linux-gnuX
SF:r(DNSVersionBindReqTCP,20,"\\0\\x1e\\0\\x06\\x81\\x85\\0\\x01\\0\\0\\0\\0\\0\\0\\x07ve
SF:rsion\\x04bind\\0\\x10\\0\\x03")Xr(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 (0.000036s 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 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: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)
```

Scansione Completa su `scanme.nmap.org`

🔖 Tag: `#scanme` `#analysiservizi` `#nmap`

L'ultima immagine riporta una scansione completa eseguita su `scanme.nmap.org`. Viene evidenziata la presenza di porte aperte, come SSH (22) con OpenSSH 6.6 e un servizio echo di Nping sulla porta 9929. La scansione include anche informazioni sul sistema operativo e sugli algoritmi crittografici utilizzati dal server, fornendo dettagli essenziali per valutare la sicurezza del target.

```
[analyst@sec0ps ~]$ 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@sec0ps ~]$
```

Conclusioni e Considerazioni di Sicurezza

🔖 Tag: `#vulnerabilità` `#ftp` `#ssh` `#sicurezza`

L'uso di Nmap ha evidenziato una serie di potenziali vulnerabilità, tra cui:

- **Accesso FTP anonimo:** su macchine locali e remote.
- **Versioni obsolete dei servizi:** come OpenSSH 6.6, che potrebbe essere soggetto a vulnerabilità note.

L'analisi dettagliata dei servizi e delle porte aperte è fondamentale per garantire la sicurezza della rete e prevenire potenziali attacchi.

Chiavi:

nmap, pentesting, scansione, sicurezza, reti, vulnerabilità, ip, localhost, scanme