

Report Attività: Esplorazione con Nmap

Parte 1: Esplorazione di Nmap

Comando usato:

man nmap

Risposte alle domande:

- **Cos'è Nmap?**
Nmap è uno strumento open source per l'esplorazione di rete e l'audit di sicurezza. Permette di individuare host attivi, servizi in esecuzione e sistema operativo.
- **Per cosa viene usato Nmap?**
Viene usato per testare la sicurezza della rete, identificare dispositivi collegati, analizzare porte aperte e scoprire vulnerabilità.
- **Cosa fa l'opzione -A?**
Attiva rilevamento del sistema operativo, versione dei servizi, script scanning e traceroute.
- **Cosa fa l'opzione -T4?**
Imposta la velocità di scansione a "aggressiva", permettendo esecuzione più rapida senza ritardi dinamici.
- **Comando usato nell'esempio:**

nmap -A -T4 scanme.nmap.org

Parte 2: Scansione delle Porte Aperte

Scansione di localhost

Comando eseguito:

nmap -A -T4 localhost

Porte aperte e servizi rilevati:

- 21/tcp - ftp (vsftpd 2.0.8 o successivo)
- 22/tcp - ssh (OpenSSH 7.7)

```

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

[analyst@secOps ~]$ man nmap
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 09:13 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000033s 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 12.69 seconds
[analyst@secOps ~]$

```

Scansione della rete locale

Comando eseguito:

nmap -A -T4 10.0.2.7/24

Indirizzo IP VM: 10.0.2.15

Subnet: 255.255.255.0

Rete: 10.0.2.0/24

Host rilevati:

- 10.0.2.1
- 10.0.2.2

- 10.0.2.3
- 10.0.2.7

Porte e servizi esempio su 10.0.2.7:

- 21/tcp - ftp (vsftpd 2.0.8)
- 22/tcp - ssh (OpenSSH 7.7)
- 53/tcp - domain (dnsmasq 2.85)

Screenshot da inserire qui:

```
analyst@sec0ps ~]$ nmap -A -T4 10.0.2.7/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 09:16 EDT
Nmap scan report for 10.0.2.1
Host is up (0.0018s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq 2.85
         dns-nsid:
         _bind.version: dnsmasq-2.85
Nmap scan report for 10.0.2.7
Host is up (0.0018s 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 10.0.2.7
           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)
           _ 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 29.87 seconds
analyst@sec0ps ~]$
```

Scansione server remoto scanme.nmap.org

Comando eseguito:

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

Risultati principali:

- **IP del server:** 45.33.32.156
- **Sistema operativo:** Linux (CPE: cpe:/o:linux:linux_kernel)

Porte aperte:

- **22/tcp** - ssh (OpenSSH 6.6.1p1 Ubuntu)
- **30/tcp** - http (Apache httpd 2.4.7)
- **9929/tcp** - nping-echo
- **31337/tcp** - tcpwrapped

Porte filtrate: molte altre risultano filtrate

Screenshot da inserire qui:

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 09:20 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 filtered 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)
30/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 53.59 seconds
[analyst@secOps ~]$
```

Domanda di Riflessione Finale

Come può Nmap aiutare con la sicurezza della rete?

Nmap consente di scoprire porte aperte, servizi attivi e vulnerabilità, permettendo un audit della rete prima che venga attaccata.

Come può essere usato da un attore malevolo?

Un attaccante potrebbe usarlo per fare ricognizione, mappare una rete e pianificare attacchi sfruttando porte aperte o servizi obsoleti.

FINE REPORT