

Bonus 1 Laboratorio

- Esplorazione di Nmap La scansione delle porte è solitamente parte di un attacco di ricognizione.

Esistono diversi metodi di scansione delle porte che possono essere utilizzati.

Cos'è nmap?

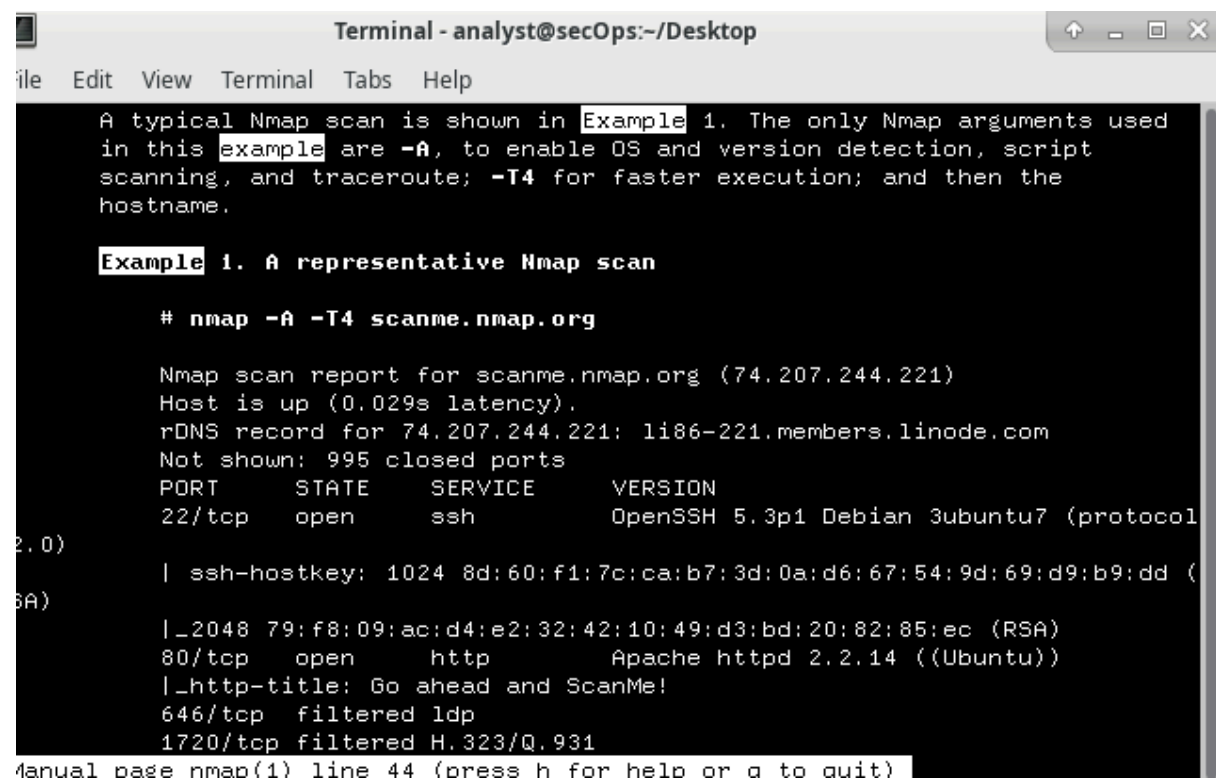
Nmap è uno strumento di esplorazione della rete e scanner di sicurezza / porte.

Per cos'è usato nmap?

Nmap viene utilizzato per scansionare una rete e determinare gli host disponibili e i servizi offerti nella rete. Alcune delle funzionalità di Nmap includono la scoperta degli host, la scansione delle porte e il rilevamento del sistema operativo. Nmap può essere comunemente utilizzato per audit di sicurezza, per identificare le porte aperte, per inventari delle reti e per individuare vulnerabilità nella rete.

Guarda l'Esempio 1.

Qual è il comando nmap utilizzato?



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

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 (
6A)
|_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

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

Il comando utilizzato nel primo esempio è:

nmap -A -T4 scanme.nmap.org

Cosa fa l'opzione -A?

-A: Abilita il rilevamento del sistema operativo, il rilevamento delle versioni, la scansione degli script e il traceroute.

Cosa fa l'opzione -T4?

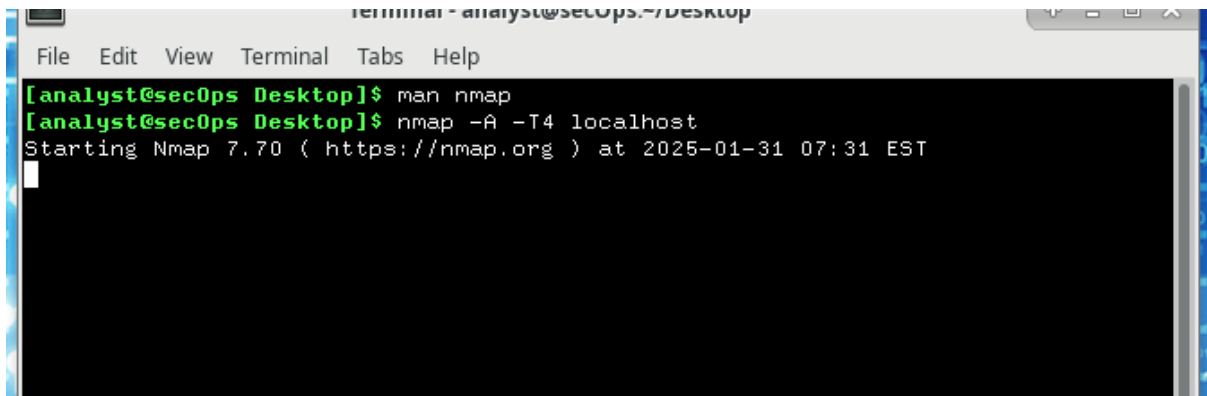
-T4 per un'esecuzione più veloce, evitando che il ritardo dinamico della scansione superi i 10 ms per le porte TCP. -T4 è consigliato per una connessione a banda larga decente o una connessione ethernet.

Parte 2: Scansione delle porte aperte

In questa parte, utilizzerai le opzioni dall'esempio nelle pagine del manuale di Nmap per scansionare il tuo localhost, la tua rete locale e un server remoto su scanme.nmap.org.

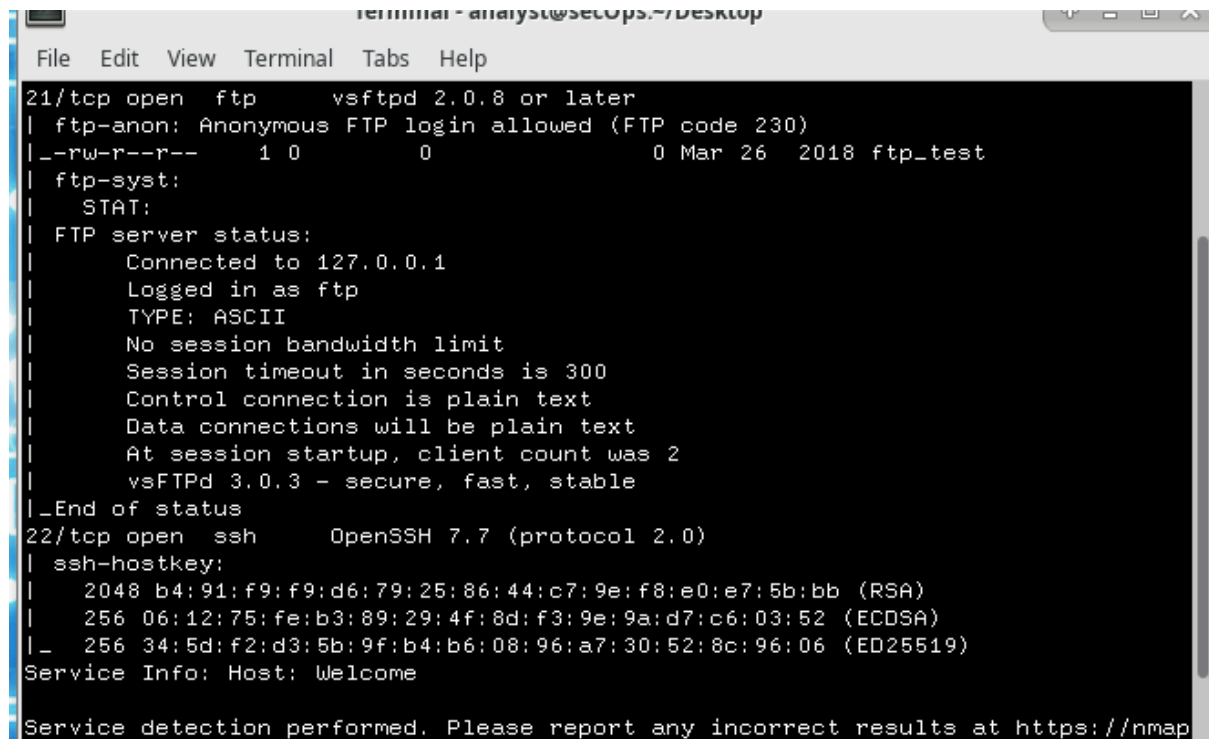
Passaggio 1: Scansiona il tuo localhost.

a. Se necessario, apri un terminale sulla VM. Al prompt, inserisci `nmap -A -T4 localhost`. A seconda della tua rete locale e dei dispositivi, la scansione richiederà da pochi secondi a qualche minuto.



```
terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ man nmap
[analyst@secOps Desktop]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 07:31 EST
```

Risultato della scansione:



```
terminal - analyst@secops: ~/Desktop
File Edit View Terminal Tabs Help
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 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: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
```

Quali porte e servizi sono aperti?

21/tcp: ftp, 22/tcp: ssh

Per ciascuna delle porte aperte, riporta il software che fornisce i servizi.

ftp: vsftpd, ssh: OpenSSH

Passaggio 2:

Scansiona la tua rete.

Attenzione: Prima di utilizzare Nmap su qualsiasi rete, assicurati di ottenere il permesso dai proprietari della rete prima di procedere.

a. Al prompt del terminale, inserisci **ip address** per determinare l'indirizzo IP e la subnet mask di questo host. Per questo esempio, l'indirizzo IP per questa VM è **192.168.1.150** e la subnet mask è 255.255.255.0.

```
valid-irc forever preferred-irc forever
[analyst@secOps Desktop]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.150  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe14:765a  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:14:76:5a  txqueuelen 1000  (Ethernet)
    RX packets 677  bytes 41445 (40.4 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 47  bytes 4031 (3.9 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Registra l'indirizzo IP e la subnet mask per la tua VM.

A quale rete appartiene la tua VM?

. Questa VM ha un indirizzo IP di 192.168.1.150/24 e fa parte della rete 192.168.1.0/24.

Per individuare altri host su questa rete locale, inserisci **nmap -A -T4 indirizzo di rete/prefix**. L'ultimo ottetto dell'indirizzo IP deve essere sostituito con uno zero. Ad esempio, nell'indirizzo IP **192.168.1.150**, il **.150** è l'ultimo ottetto. Pertanto, l'indirizzo di rete è **192.168.1.0** Il /24 è chiamato prefix ed è una forma abbreviata per la netmask 255.255.255.0. Se la tua VM ha una netmask diversa, cerca su Internet una "tabella di conversione CIDR" per trovare il tuo prefix.

Nota: Questa operazione potrebbe richiedere del tempo, soprattutto se hai molti dispositivi collegati alla rete. In un ambiente di test, la scansione ha impiegato circa 4 minuti.

Quali porte e servizi sono aperti?

22/tcp: ssh, 9929/tcp: n ping-echo, 31337/tcp: tcpwrapped, 80/tcp: http

Qual è l'indirizzo IP del server?

Indirizzo IPv4: 45.33.32.156, Indirizzo IPv6: 2600:3c01::f03c:91ff:fe18:bb2f

Qual è il sistema operativo?

Ubuntu Linux