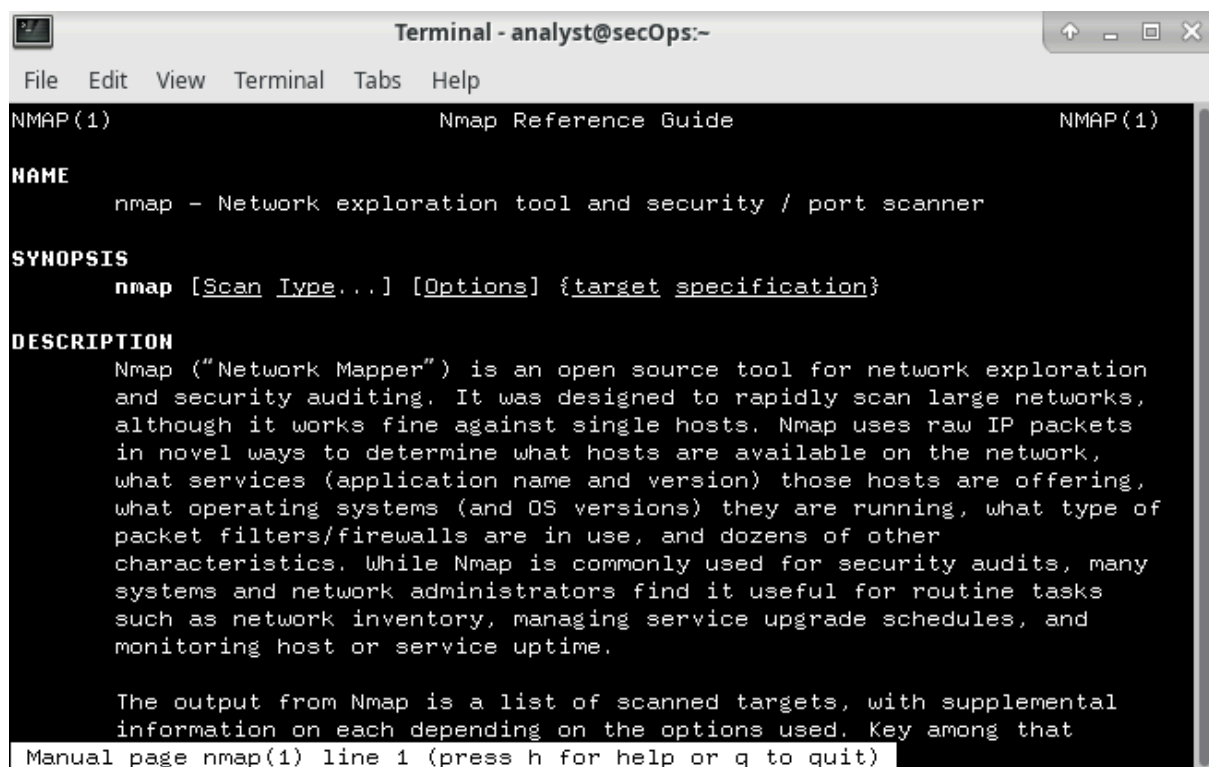


Relazione Schematica: Esplorare Nmap

Obiettivo: Esplorare le funzionalità di Nmap per la scansione delle porte aperte, il rilevamento degli host e l'analisi della sicurezza di rete.

Parte 1: Esplorazione di Nmap

1. **Avvio della VM CyberOps Workstation**
2. **Apertura del terminale**
3. **Consultazione della pagina man di Nmap**
 - Comando: `man nmap`
 - Nmap è uno strumento di scansione della rete utilizzato per identificare host, porte aperte e servizi.
 - Permette il rilevamento di sistema operativo, versione dei servizi e vulnerabilità.



```
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

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

4. Esempi di comandi Nmap

- `nmap -A -T4 scanme.nmap.org`
- `-A`: Abilita rilevamento OS, versione, script scanning e traceroute.
- `-T4`: Aumenta la velocità di scansione per connessioni veloci.

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 08:39 EST
```

5. Navigazione nella pagina man

- Uso delle frecce per scorrere, `/` per cercare termini, `n` per saltare alle corrispondenze successive.
- Digitare `q` per uscire.

Parte 2: Scansione delle Porte Aperte

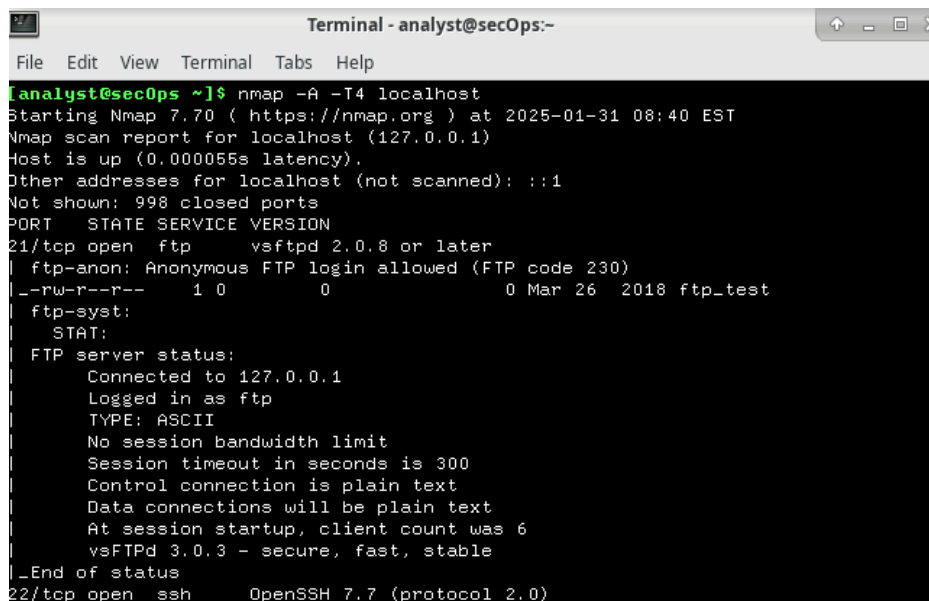
Passaggio 1: Scansione del Localhost

1. Esecuzione del comando

- `nmap -A -T4 localhost`

2. Risultati ottenuti

- Porte aperte:
 - 21/TCP: FTP (vsftpd)
 - 22/TCP: SSH (OpenSSH)
- FTP anonimo abilitato.



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

[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 08:40 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000055s 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 6
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)
```

Passaggio 2: Scansione della Rete Locale

1. **Determinazione dell'indirizzo IP**
 - Comando: `ip address`
 - Identificazione dell'indirizzo IP della VM e subnet mask.
2. **Esecuzione della scansione della LAN**
 - `nmap -A -T4 10.0.2.0/24`
 - Identificazione degli host attivi.
 - Servizi rilevati:
 - 21/TCP: FTP
 - 22/TCP: SSH
 - 23/TCP: Telnet
 - Scansione completata in circa 4 minuti.

Passaggio 3: Scansione di un Server Remoto

1. **Visita di scanme.nmap.org**
 - Obiettivo: consentire agli utenti di testare Nmap.
2. **Esecuzione della scansione remota**
 - `nmap -A -T4 scanme.nmap.org`
 - Porte aperte:
 - 22/TCP: SSH
 - 80/TCP: HTTP (Apache)
 - 9929/TCP: Nping Echo
 - 31337/TCP: TCPwrapped
 - Porte filtrate:
 - 135/TCP: MSRPC
 - 139/TCP: NetBIOS-SSN
 - 445/TCP: Microsoft-DS
 - 25/TCP: SMTP
 - Indirizzo IP del server: **45.33.32.156**
 - OS rilevato: **Ubuntu Linux**