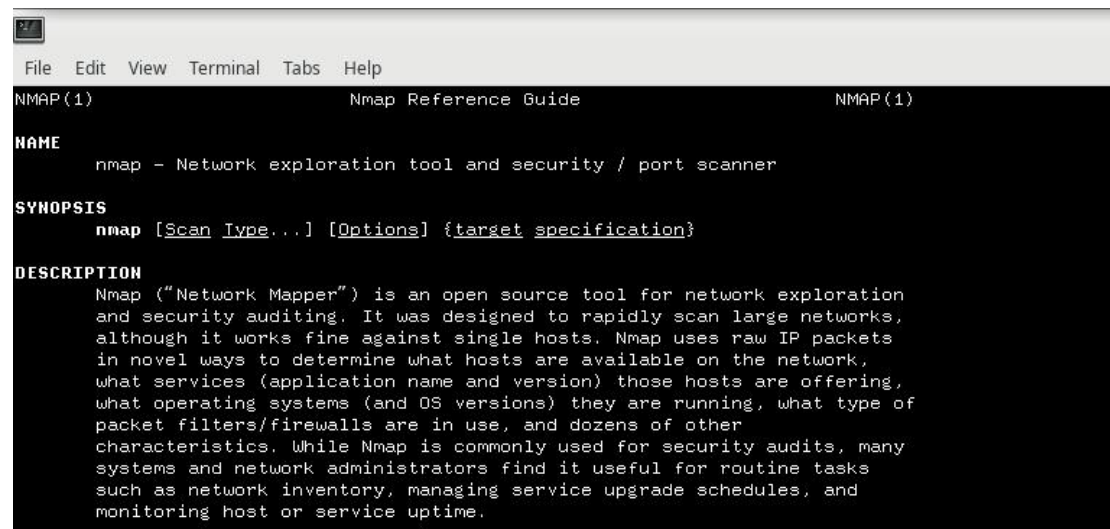


ESPLORAZIONE DI NMAP

- Parte 1: Esplorazione di Nmap
- Parte 2: Scansione delle porte aperte

1) Apriamo la macchina virtuale CyberOps workstation . Dal terminale digitiamo il comando `man nmap`, con questo comando facciamo partire nmap, un tool specifico per esplorare la rete, scansionare le porte e per la sicurezza.



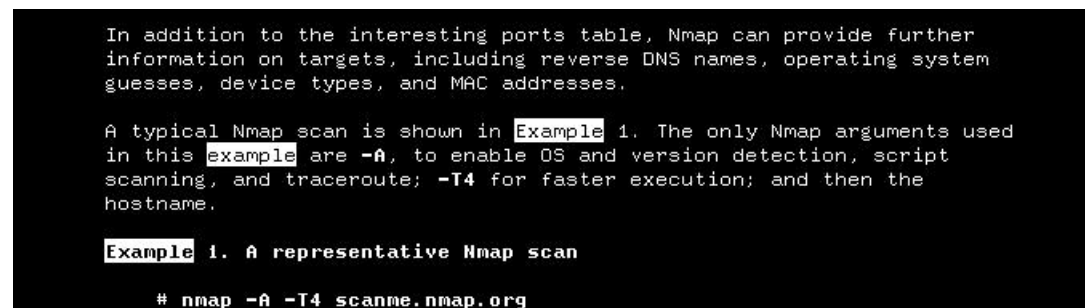
```
File Edit View Terminal Tabs Help
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

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.
```

Tramite il comando `/example` possiamo filtrare la parola `example` nella pagina `man`.



```
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
```

Con il comando `nmap -A -T4 scanme.nmap.org` notiamo che grazie a `-A` individuiamo il sistema operativo, la sua versione, la scansione degli script ed il tracerout, il `-T4` è il tempo che diamo ad nmap per svolgere il suo lavoro .

2) Con il comando `nmap -A -T4 localhost` possiamo vedere quali servizi sono aperti e le loro relative porte. In questo caso notiamo la porta aperta 21/tcp sul servizio ftp, la porta 22/tcp sul servizio ssh ed i loro software sono precisamente vsftpd e OpenSSH.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 07:45 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s 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 12.60 seconds
```

Con il comando `ip a` visualizziamo l'ip e la subnetmask di questa macchina virtuale quali 192.168.1.9/24 sapendo che è presente nella rete 192.168.1.0/24.

```
[analyst@secOps ~]$ ip a
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:ab:82:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.9/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 3262sec preferred_lft 3262sec
    inet6 fe80::a00:27ff:feab:825d/64 scope link
        valid_lft forever preferred_lft forever
```

Digitando il comando `nmap -A -T4 192.168.1.0/24` possiamo visualizzare le varie porte aperte su questa rete e i vari host presenti all'interno di essa.

```
[analyst@secOps ~]$ nmap -A -T4 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 07:50 EDT
Nmap scan report for vodafone.station (192.168.1.1)
Host is up (0.033s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    filtered ssh
53/tcp    open  domain       dnsmasq 2.84rc2
| dns-nsid:
|_  bind.version: dnsmasq-2.84rc2
80/tcp    open  http?
| fingerprint-strings:
|_  GetRequest, HTTPOptions:
|     UNKNOWN 400 Bad Request
|     Server:
|     Date: Fri, 11 Apr 2025 11:50:26 GMT
|     Cache-Control: no-cache,no-store,max-age=0
|     Pragma: no-cache
|     X-Frame-Options: DENY
|     Expires: 0
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'
|     Content-Language: en
|     Content-Type: text/html
|     Connection: close
|     <HTML>
|     <HEAD><TITLE>400 Bad Request</TITLE></HEAD>
|     <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">
|     <H4>400 Bad Request</H4>
|     Invalid Request
|_  NULL:
|     UNKNOWN 408 Request Timeout
|     Server:
|     Date: Fri, 11 Apr 2025 11:50:26 GMT
|     Cache-Control: no-cache,no-store,max-age=0
|     Pragma: no-cache
|     X-Frame-Options: DENY
|     Expires: 0
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'
|     Content-Language: en
|     Content-Type: text/html
|     Connection: close
|     <HTML>
|     <HEAD><TITLE>408 Request Timeout</TITLE></HEAD>
|     <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">
|     <H4>408 Request Timeout</H4>
|_  request appeared within a reasonable time period.
443/tcp    open  ssl/https?
| fingerprint-strings:
|_  GetRequest, HTTPOptions:

Nmap scan report for NOMI-IPC-K2EC-3H1W.station (192.168.1.11)
Host is up (0.017s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http?
554/tcp   open  rtsp?
8086/tcp   open  d-s-n?

Nmap scan report for 192.168.1.108
Host is up (0.029s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http?
554/tcp   open  rtsp?
8086/tcp   open  d-s-n?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 267.87 seconds
```

Come ultimo passaggio digito il comando `nmap -A -T4 scanme.nmap.org` mostrandomi le porte (22/tcp, 53/tcp, 80/tcp, 992/tcp, 31337/tcp) ed i servizi aperti (ssh, domain, http, nping-echo, tcpwrapped), le porte ed i servizi che vengono filtrati, l' ip del server (45.33.32.156) ed il sistema operativo (ubuntu linux).

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-04-11 07:58 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: 995 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)
53/tcp    open  domain         dnsmasq 2.84rc2
|_ dns-nsid:
|_  bind.version: dnsmasq-2.84rc2
80/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 19.93 seconds
```