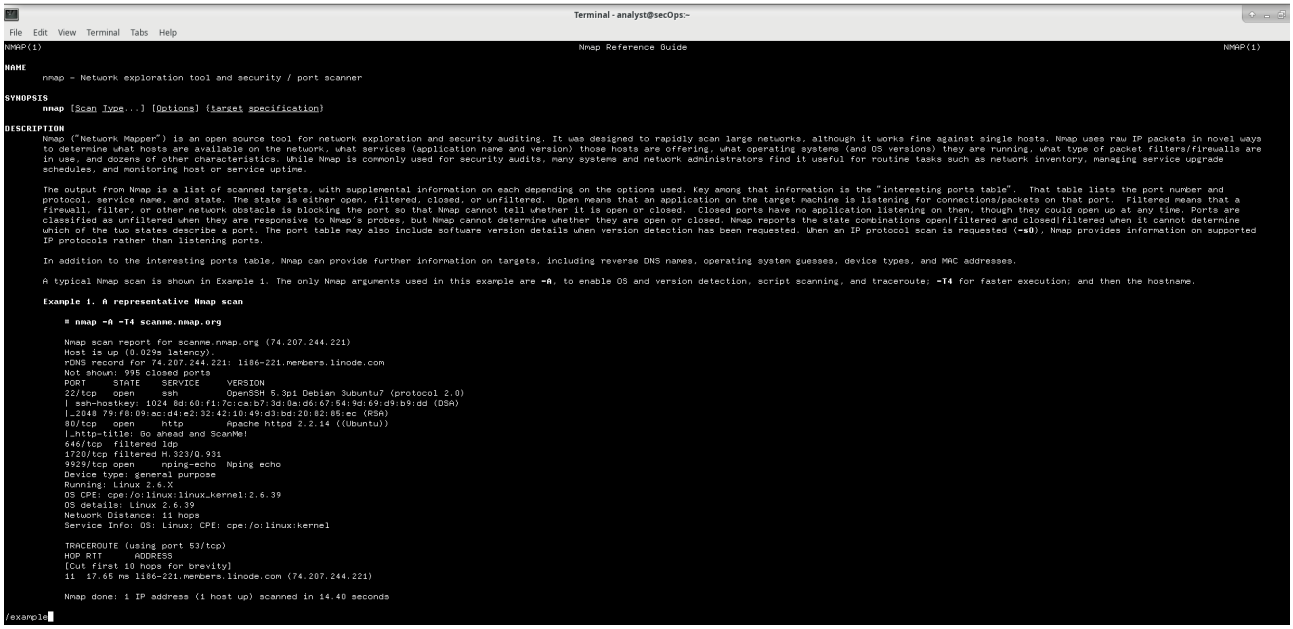
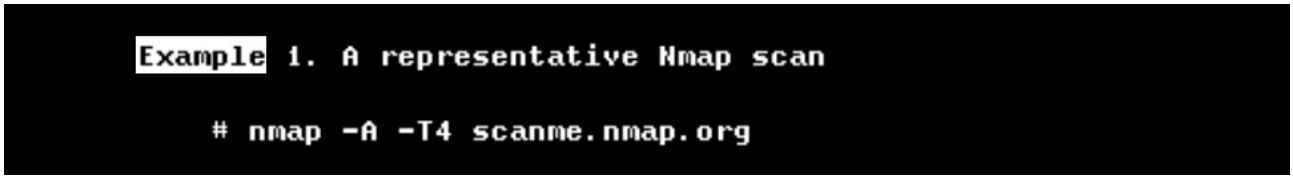
Esplorazione di Nmap

Exploring Nmap

1. Ho aperto un terminale ho digitato **man nmap**. Poi ho digitato **/example** e premuto **ENTER**. Questo ha cercato la parola "example" in avanti all'interno della pagina del manuale.





Viene eseguito il comando nmap nella forma: **nmap -A -T4 scanme.nmap.org**

L'opzione **-A** abilita il rilevamento del sistema operativo, il rilevamento della versione, la scansione degli script e il traceroute. È essenzialmente un'opzione per una scansione aggressiva che combina diverse funzionalità.

L'opzione **-T4** è utilizzata per un'esecuzione più veloce della scansione, limitando il ritardo dinamico della scansione a non più di 10 ms per le porte TCP. Questa opzione è particolarmente consigliata quando si dispone di una connessione a banda larga o ethernet decente, poiché offre un buon equilibrio tra velocità e affidabilità.

```
# 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 (DSA)
|_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 ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

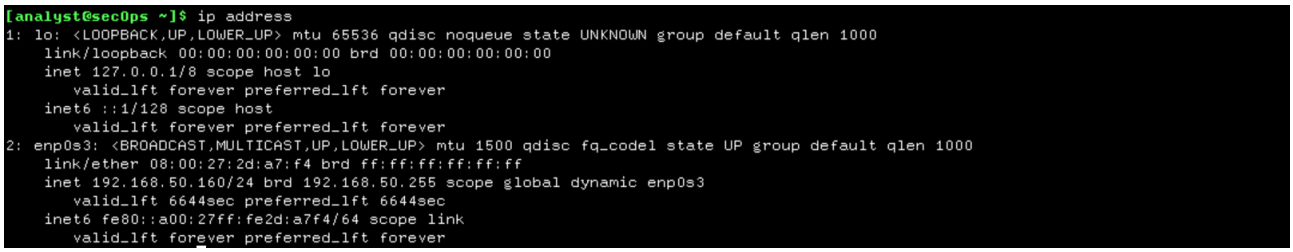
Scanning for Open Ports

1. Da terminale, ho digitato **nmap -A -T4 localhost**. La scansione ha impiegato pochi secondi.

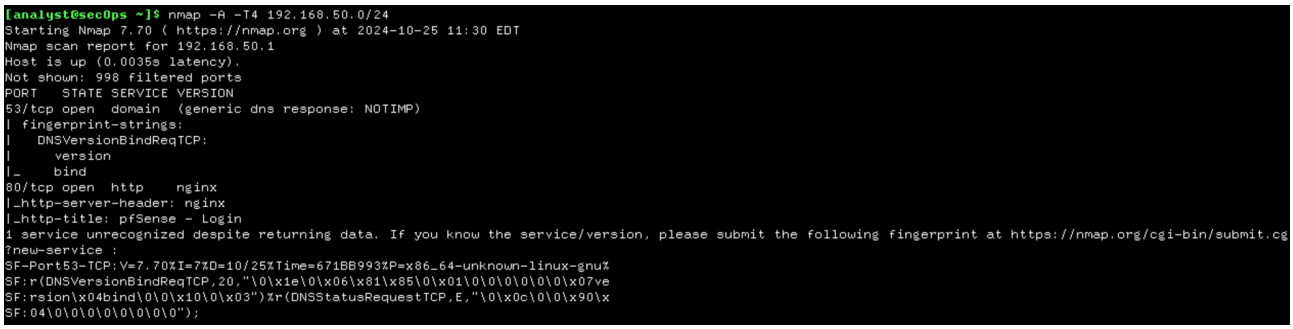
```
[analyst@secOps ~]$ nmap -A T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 11:25 EDT
Failed to resolve "T4".
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000058s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT   STATE SERVICE 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 12.02 seconds
```

Ho identificato due porte aperte con i relativi servizi: La porta 21/tcp esegue il servizio ftp, gestito dal software vsftpd La porta 22/tcp esegue il servizio ssh, gestito dal software OpenSSH

2. Da Terminale, ho digitato **ip address** per determinare l'indirizzo IP e la subnet mask per questo host.

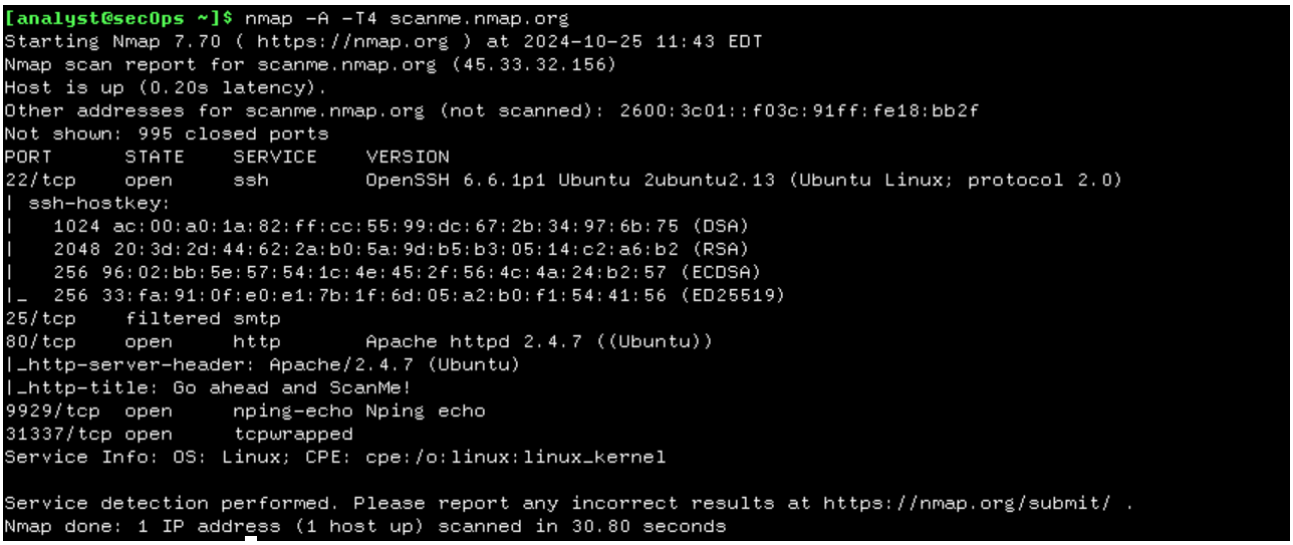


3. Per scansionare l’intera rete ho usato il comando **nmap -A -T4 192.168.50.0/24**



Oltre alla mia macchina nmap ha rilevato la PfSense attiva nella mia rete.
Le porte aperte sono la 53(open domain) e la porta 80(http) nginx.

4. Ho aperto un browser web e sono andato all'indirizzo **scanme.nmap.org**. Ho letto il messaggio pubblicato.
Poi, da terminale, ho digitato **nmap -A -T4 scanme.nmap.org**.



Ho identificato diverse porte aperte nel sistema, che includono la porta 22/tcp che esegue ssh, la porta 80/tcp che esegue http, la porta 9929(servizio nping),la porta 31337 servizio: tcpwrapped. Durante la scansione ho anche rilevato alcune porte filtrate: la porta 25/tcp che gestisce smtp. Il server utilizza due indirizzi, un IPv4 che è 45.33.32.156 e un IPv6 che corrisponde a 2600:3c01::f03c:91ff:fe18:bb2f.
Ho potuto determinare che il sistema operativo in esecuzione sul server è Ubuntu Linux.