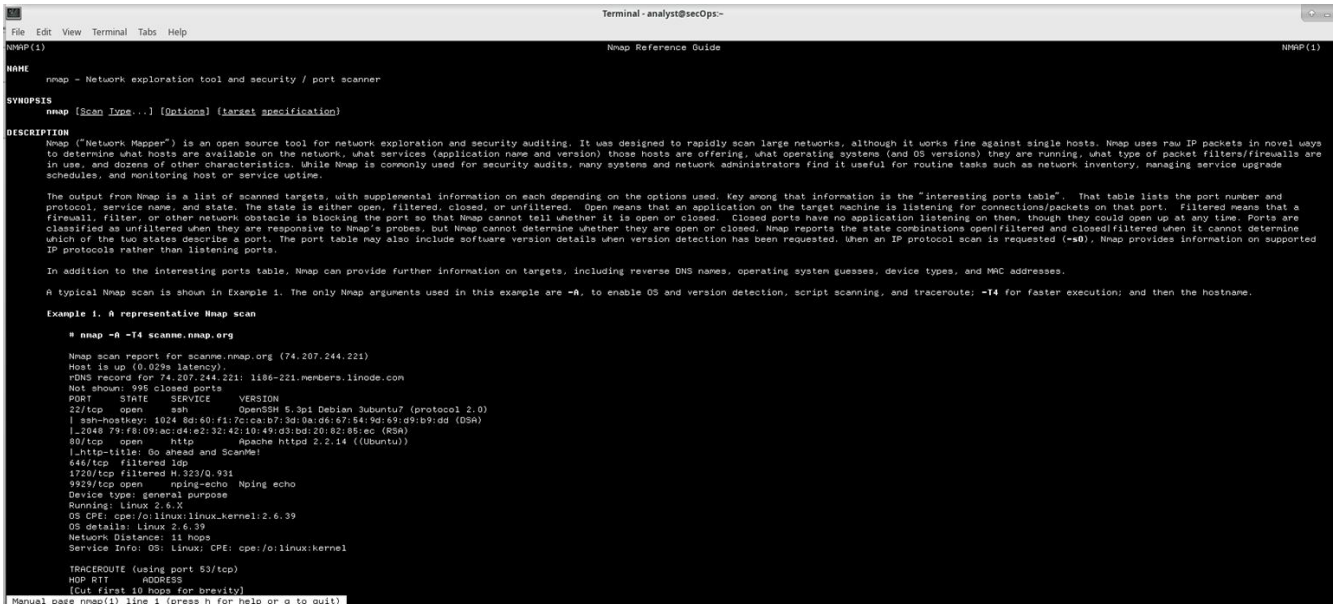
# Analisi di Nmap

Esaminando lo strumento Nmap tramite la sua pagina manuale (man page), è stato possibile approfondire la conoscenza delle caratteristiche e delle capacità di questo potente software per il networking. Nmap, abbreviazione di Network Mapper, è un'applicazione open source progettata principalmente per l'esplorazione e l'analisi delle reti. Consente di individuare i dispositivi attivi su una rete, identificare le porte aperte, rilevare i servizi in esecuzione e persino determinare il sistema operativo utilizzato.



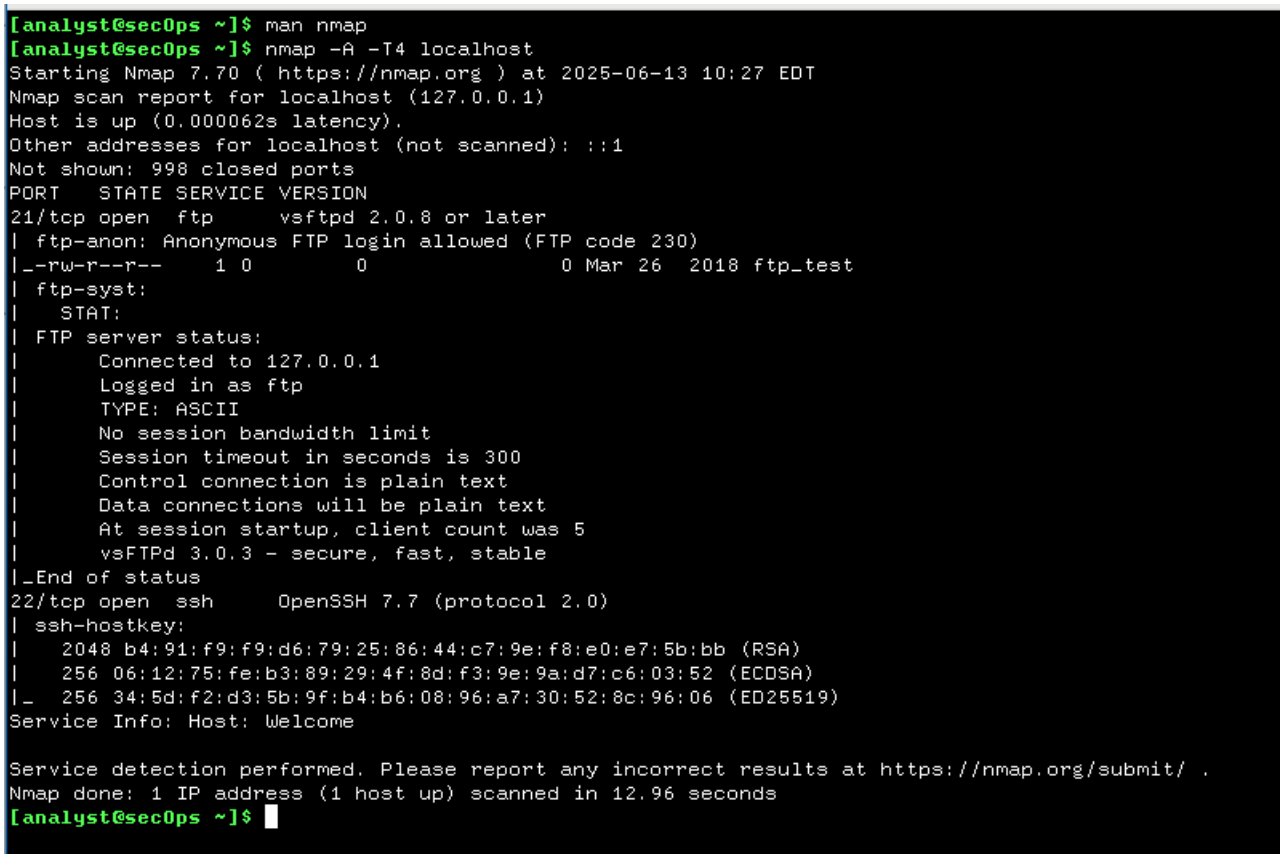

Utilizzando il comando man nmap, si accede a una guida dettagliata che include varie sezioni, come la descrizione generale dello strumento, la sintassi dei comandi, esempi pratici e un elenco delle opzioni più comuni. L'interfaccia della pagina manuale permette di scorrere agevolmente il contenuto e di effettuare ricerche specifiche tramite la funzione di ricerca con il simbolo /. Nel nostro caso, abbiamo cercato la parola chiave /example.

Uno degli esempi più rilevanti che abbiamo trovato nella pagina man è rappresentato dal seguente comando:

Analizzando questo comando, emerge che l'opzione -A attiva una scansione "aggressiva", la quale integra funzionalità avanzate quali l'identificazione del sistema operativo del target, il rilevamento delle versioni dei servizi in esecuzione, l'esecuzione di script per approfondimenti e il tracciamento del percorso di rete (traceroute). Questa modalità è particolarmente utile per ottenere una panoramica completa dello stato di un host o di un'intera rete.

L'opzione -T4, invece, serve a regolare la velocità con cui viene effettuata la scansione. Impostando questo parametro a 4 (su una scala da 0 a 5), Nmap esegue la scansione in modo più rapido, riducendo i tempi senza sacrificare troppo la precisione. Questa impostazione è ideale in reti affidabili.

**Parte 2: Analisi delle Porte Aperte**




Utilizzando il comando nmap -A -T4 localhost, è stata effettuata una scansione approfondita del sistema locale. Il risultato ha evidenziato la presenza di due porte aperte, ognuna associata a un servizio attivo.

**Porte rilevate:**

- **21/tcp (FTP)**: Il servizio FTP è operativo grazie a *vsftpd*, in una versione pari o successiva alla 2.0.8 (nello specifico 3.0.3). L'accesso anonimo è abilitato, il che implica che chiunque può

connettersi al server senza credenziali. Dal punto di vista della sicurezza, si tratta di un aspetto che merita attenzione. La scansione ha anche rivelato ulteriori dettagli, tra cui l'uso della modalità ASCII per il trasferimento dati, l'assenza di limiti di banda e un timeout di sessione impostato a 300 secondi.

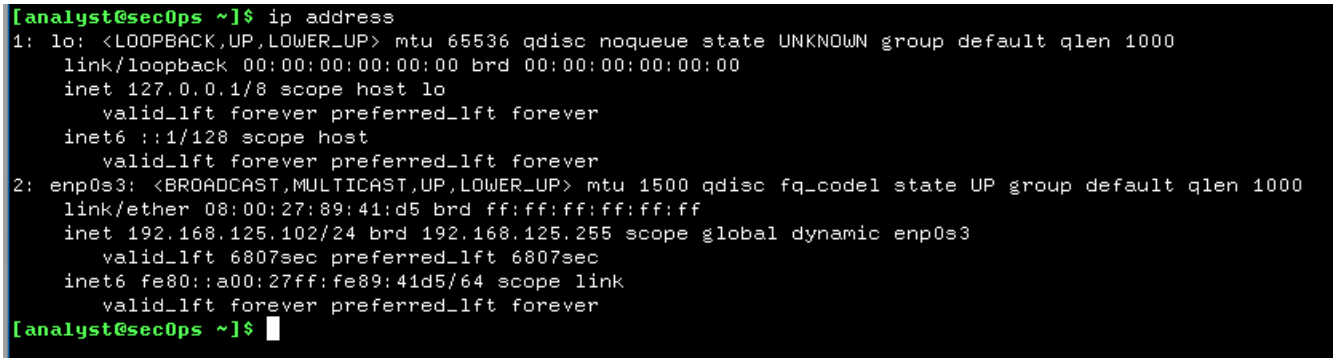
- **22/tcp (SSH)**: Il protocollo SSH è in funzione tramite *OpenSSH* versione 7.7. Sono state rilevate diverse chiavi host per la cifratura della connessione (RSA, ECDSA e ED25519), utili per garantire una comunicazione sicura tra client e server.

Tutte le altre 998 porte risultano chiuse, quindi non accessibili a richieste esterne

**Passo 2: Scansione della Rete Locale**

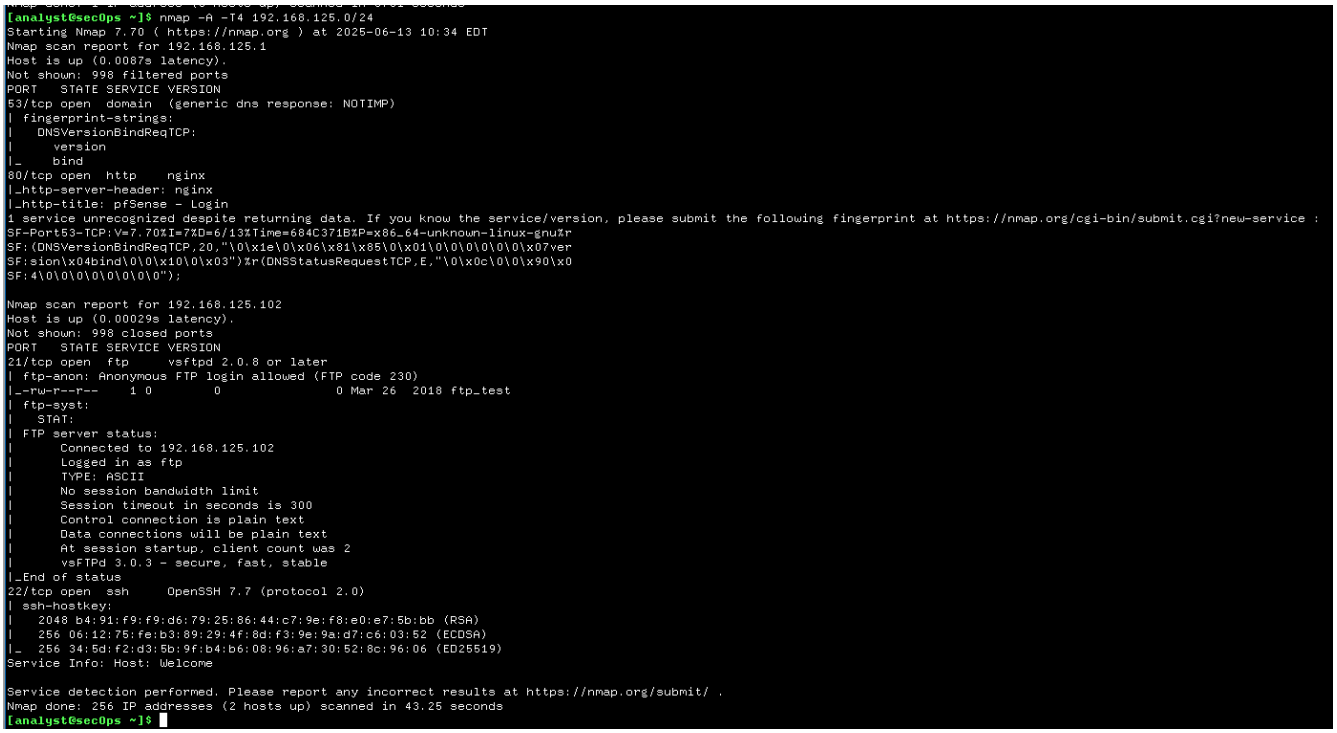
**a. Identificazione dell'indirizzo IP e della subnet mask**

Tramite il comando ip address, è stato possibile determinare i dati di configurazione della macchina virtuale. L'interfaccia di rete attiva è *enp0s3*, con indirizzo IP 192.168.125.102 e subnet mask /24 (equivalente a 255.255.255.0). Queste informazioni collocano la VM all'interno della rete 192.168.125.0/24, che comprende gli indirizzi da 192.168.125.1 a 192.168.125.254.



**b. Rilevamento degli host sulla LAN**

La scansione della rete locale è stata eseguita con il comando nmap -A -T4 192.168.125.0/24, che ha permesso di individuare altri dispositivi attivi.




Dal risultato della scansione Nmap sulla rete 192.168.125.0/24, risulta che sono attivi 2 host nella stessa LAN della tua macchina virtuale. Entrambi gli indirizzi IP rilevati appartengono alla stessa sottorete /24, quindi si trovano sulla stessa rete locale della tua VM.

## Gli host attivi rilevati sono:

- **192.168.125.1**
- **192.168.125.102**

Vediamo ora quali servizi risultano accessibili su ciascun host:

192.168.125.1

Questo host sembra essere un **firewall pfSense**, riconoscibile dalla pagina di login web che appare sulla porta **80 (HTTP)**. Il server web in uso è **nginx**. Inoltre, risulta aperta anche la porta **53 (TCP)**, utilizzata solitamente per il servizio **DNS**. Tuttavia, Nmap non è riuscito a identificare completamente il servizio DNS attivo, anche se ha restituito una risposta generica (NOTIMP), il che potrebbe indicare una configurazione particolare.

192.168.125.102

Questo host presenta due porte aperte:

- La **porta 21 (FTP)**, dove è attivo un server **vsftpd**. Da notare che l'accesso anonimo è **abilitato**, cosa piuttosto rischiosa in termini di sicurezza, soprattutto se il server consente anche l'upload di file.
- La **porta 22 (SSH)**, che offre accesso tramite shell remota. Il servizio è gestito da **OpenSSH**, versione 7.7. Le chiavi host SSH sono state rilevate, il che indica che la connessione è disponibile e attiva.

Questa analisi ha fornito una mappatura chiara dei dispositivi presenti sulla rete e dei servizi attivi su ciascuno.

**Passo 3: Scansione di un Server Remoto**

Visitando il sito web **scanme.nmap.org**, si apprende che il suo scopo è quello di offrire un ambiente controllato per effettuare test legittimi con Nmap. Il sito è gestito direttamente dal team di sviluppo di Nmap, che consente esplicitamente agli utenti di eseguire scansioni sul server per scopi didattici o sperimentali, evitando così qualsiasi rischio di violazione legale.

La scansione eseguita con il comando nmap -A -T4 scanme.nmap.org ha fornito i seguenti risultati:

- **IP del server:** 45.33.32.156
- **Sistema operativo:** Linux
- **Porte aperte:**
  ▪ 22/tcp – SSH tramite *OpenSSH 6.6.1p1*
  ▪ 80/tcp – HTTP gestito da *Apache 2.4.7*
  ▪ 9929/tcp – Servizio *nping-echo*
  ▪ 31337/tcp – Protetta da *tcpwrapped*, che limita l'interazione diretta
- **Porta filtrata:**
  ▪ 7004/tcp – Non accessibile, probabilmente a causa di un firewall