ESERCIZIO: **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.

Innanzitutto, **Cos’è Nmap? A cosa serve?**

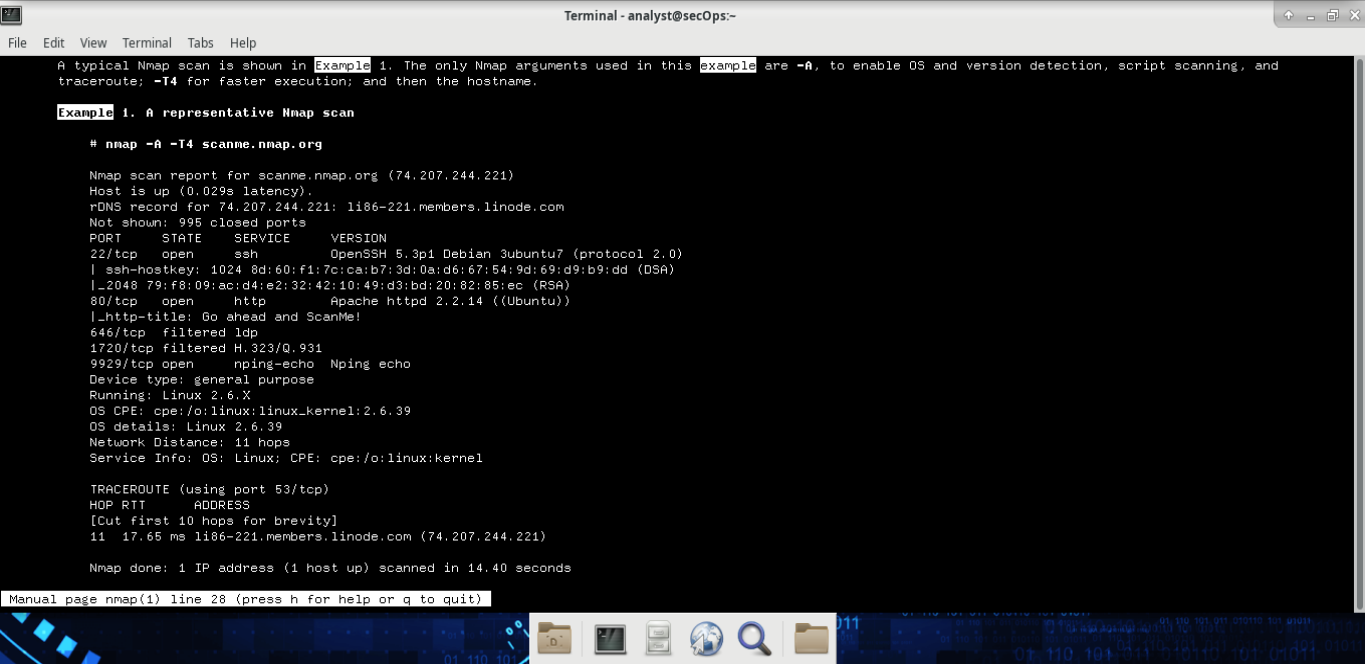
Nmap è uno strumento di esplorazione di rete e di scansione di porte e sicurezza.

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 porte aperte, inventari di rete e trovare vulnerabilità nella rete.

Ora avvio la VM cyberops; lavorerò da lì usando il suo terminale.

Primo comando: *man nmap,* visualizza le pagine di manuale associate agli argomenti.

Scrivendo */example* si può effettuare una ricerca evidenziando tutti gli example presenti nel man.



Guardando lo screen, il terzo example ricade su un comando di Nmpa:

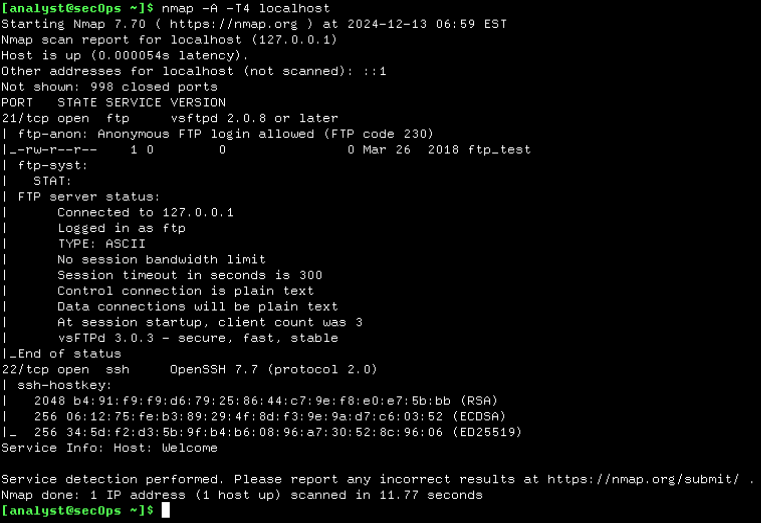
*nmap -A -T4 scanme.nmap.org*

A cosa serve?

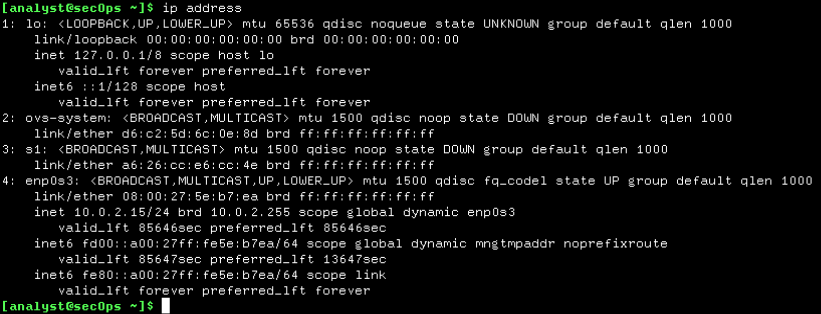
**-A:** Abilita il rilevamento del sistema operativo, il rilevamento della versione, la scansione degli script e il traceroute

**-T4:** per un'esecuzione più rapida impedendo al ritardo della scansione dinamica di superare i 10 ms per le porte TCP. -T4

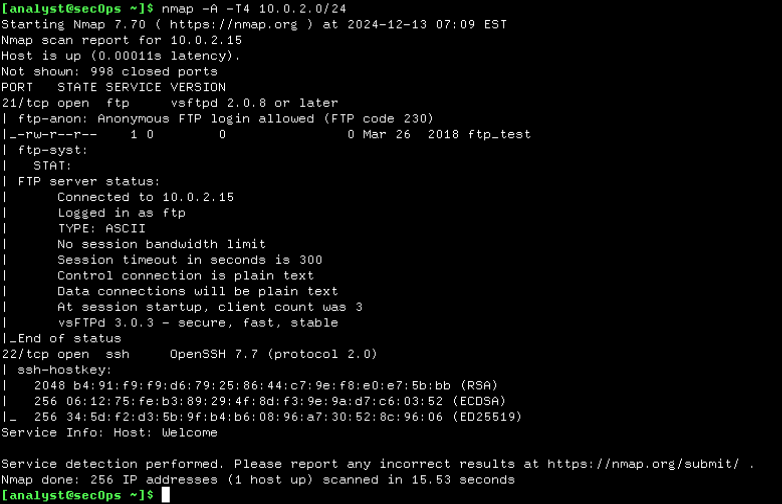
Ora che ho spiegato il comando, posso effettuare la scansione degli host locali



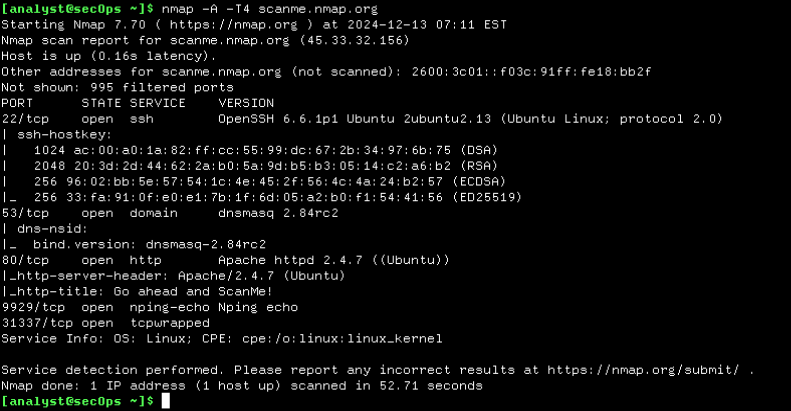
Ora effettuerò uno scan della rete per determinare Ip e subnet mask di questo host.



Questa VM ha un ip 10.0.2.15 a questo punto effettuare lo scan con il prefisso della VM.



Ora eseguirò la scansione di un server remoto



Porte e Servizi aperti: 22/tcp: ssh, 9929/tcp: n ping-echo, 31337/tcp: tcpwrapped, 80/tcp: http.

Porte e Servizi filtrati: 135/tcp: msrpc, 139/tcp: netbios-ssn, 445/tcp: microsoft-ds, 25/tcp: smtp

Nmap può essere utilizzato per scansionare una rete interna per porte aperte specifiche per identificare l'entità di una violazione della sicurezza. Può anche essere utilizzato per fare un inventario di una rete per garantire che tutti i sistemi siano probabilmente patchati contro i problemi di sicurezza. D'altro canto, nmap può essere utilizzato per la ricognizione per determinare porte aperte e altre informazioni sulla rete.