Report Attività: Esplorazione con Nmap

Parte 1: Esplorazione di Nmap

Comando usato:

man nmap

Risposte alle domande:

- **Cos'è Nmap?**
  Nmap è uno strumento open source per l'esplorazione di rete e l'audit di sicurezza. Permette di individuare host attivi, servizi in esecuzione e sistema operativo.

- **Per cosa viene usato Nmap?**
  Viene usato per testare la sicurezza della rete, identificare dispositivi collegati, analizzare porte aperte e scoprire vulnerabilità.

- **Cosa fa l'opzione `-A`?**
  Attiva rilevamento del sistema operativo, versione dei servizi, script scanning e traceroute.

- **Cosa fa l'opzione `-T4`?**
  Imposta la velocità di scansione a "aggressiva", permettendo esecuzione più rapida senza ritardi dinamici.

- **Comando usato nell'esempio:**

nmap -A -T4 scanme.nmap.org

Parte 2: Scansione delle Porte Aperte

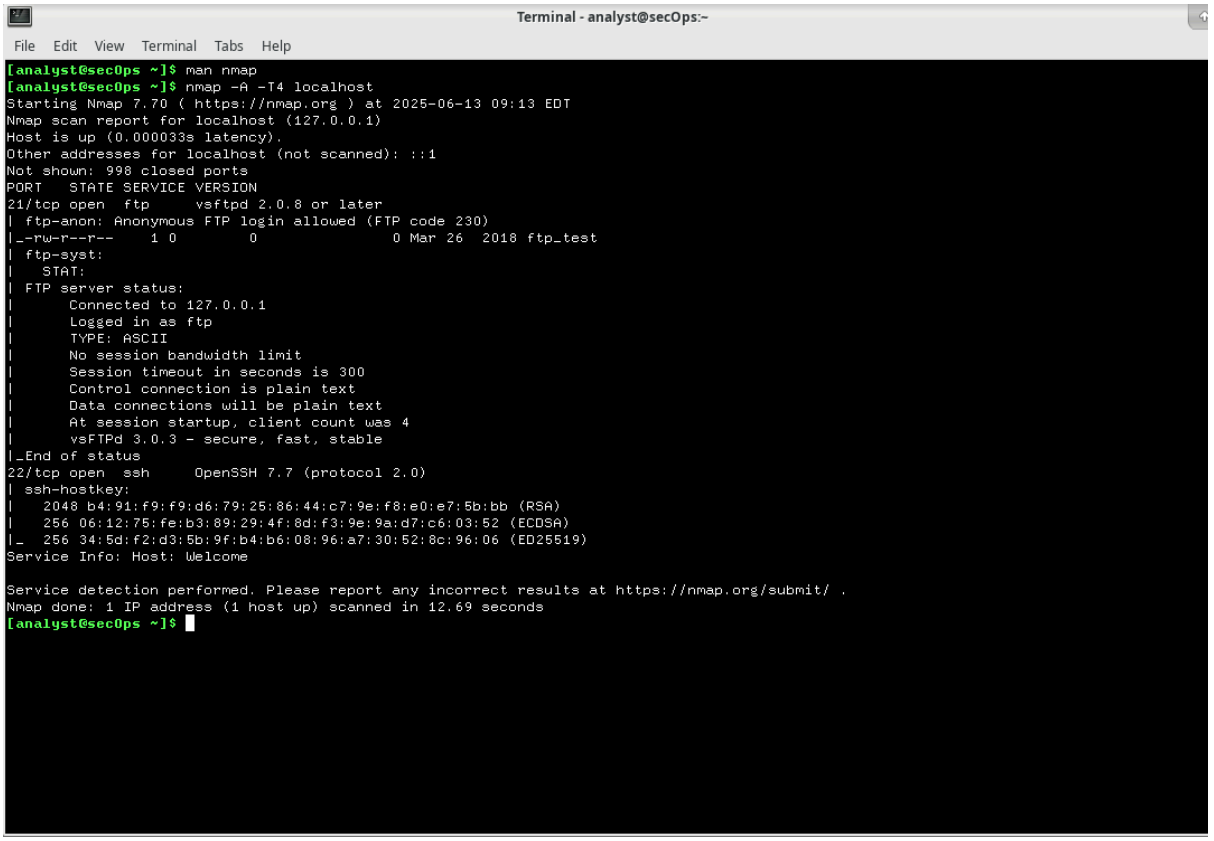
Scansione di `localhost`

Comando eseguito:

nmap -A -T4 localhost

Porte aperte e servizi rilevati:

- `21/tcp` - ftp (vsftpd 2.0.8 o successivo)
- `22/tcp` - ssh (OpenSSH 7.7)

- 

Scansione della rete locale

Comando eseguito:

nmap -A -T4 10.0.2.7/24

Indirizzo IP VM: 10.0.2.15
Subnet: 255.255.255.0
Rete: 10.0.2.0/24

Host rilevati:

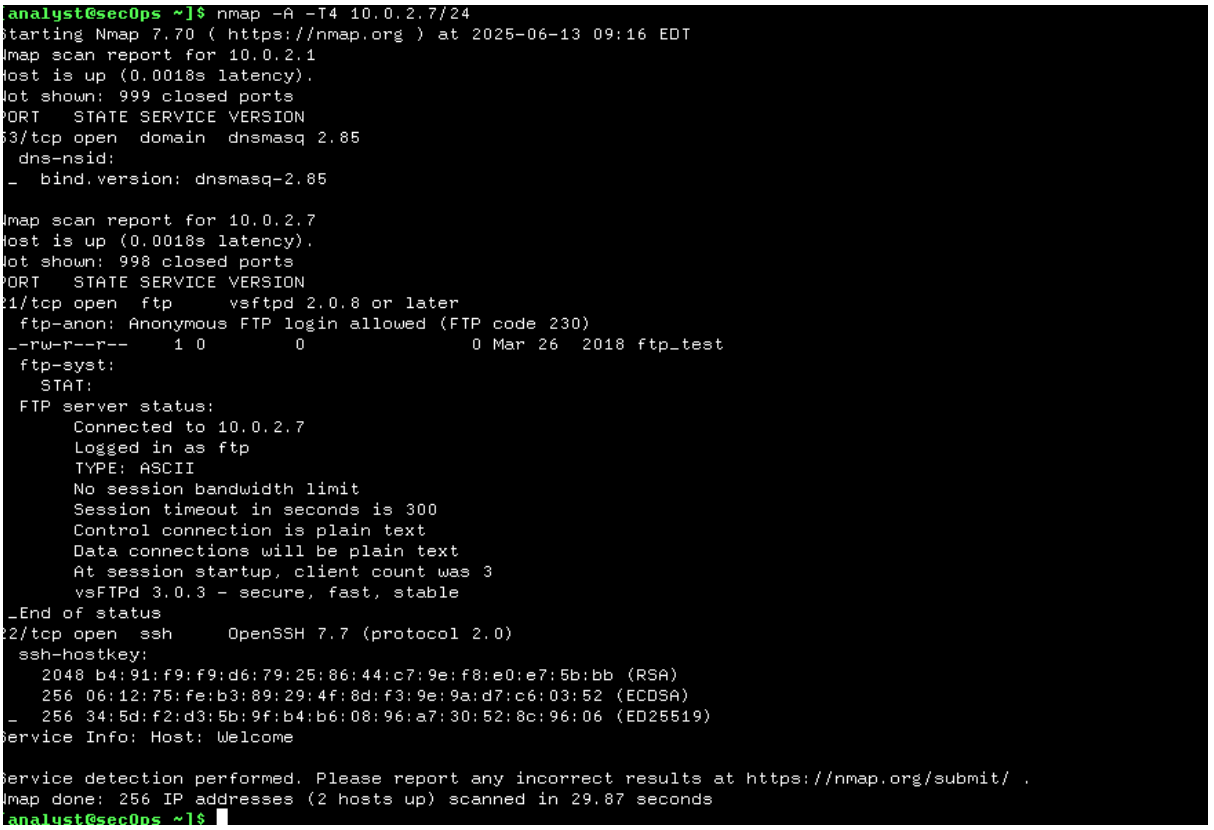
- 10.0.2.1
- 10.0.2.2

- 10.0.2.3
- 10.0.2.7

Porte e servizi esempio su 10.0.2.7:

- `21/tcp` - ftp (vsftpd 2.0.8)
- `22/tcp` - ssh (OpenSSH 7.7)
- `53/tcp` - domain (dnsmasq 2.85)

Screenshot da inserire qui:

- 

Scansione server remoto `scanme.nmap.org`

Comando eseguito:

nmap -A -T4 scanme.nmap.org

Risultati principali:

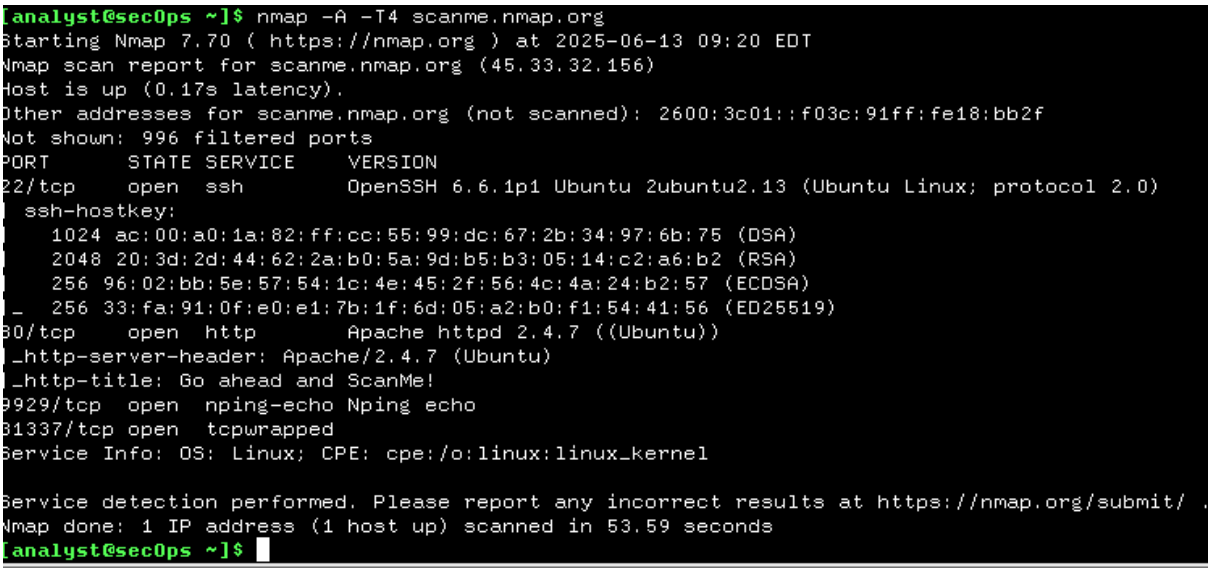
- **IP del server:** 45.33.32.156
- **Sistema operativo:** Linux (CPE: cpe:/o:linux:linux_kernel)

Porte aperte:

- `22/tcp` - ssh (OpenSSH 6.6.1p1 Ubuntu)
- `30/tcp` - http (Apache httpd 2.4.7)
- `9929/tcp` - nping-echo
- `31337/tcp` - tcpwrapped

Porte filtrate: molte altre risultano filtrate

Screenshot da inserire qui:

- 

Domanda di Riflessione Finale

Come può Nmap aiutare con la sicurezza della rete?
Nmap consente di scoprire porte aperte, servizi attivi e vulnerabilità, permettendo un audit della rete prima che venga attaccata.

Come può essere usato da un attore malevolo?
Un attaccante potrebbe usarlo per fare ricognizione, mappare una rete e pianificare attacchi sfruttando porte aperte o servizi obsoleti.