

Esplorazione di Nmap

Michele Storelli

13 Giugno 2025

Obiettivi

- Parte 1: Esplorazione di Nmap.
- Parte 2: Scansione delle Porte Aperte.

Contesto / Scenario

La scansione delle porte fa solitamente parte di un attacco di ricognizione. Esistono diversi metodi di scansione delle porte utilizzabili. Esploreremo come usare l'utility Nmap. Nmap è una potente utility di rete usata per la scoperta della rete e l'audit di sicurezza.

Risorse Richieste

- Macchina virtuale CyberOps Workstation.
- Accesso a Internet.

Risposte alle Domande

Parte 1: Esplorazione di Nmap

Cos'è Nmap? Per cosa viene usato Nmap?

Nmap (Network Mapper) è una potente utility di rete open-source e gratuita utilizzata per la scoperta della rete e l'audit di sicurezza. Viene usato per:

- Determinare quali host sono disponibili su una rete.
- Scoprire quali servizi (nome dell'applicazione e versione) sono offerti da quegli host.
- Identificare quali sistemi operativi (e versioni del sistema operativo) stanno eseguendo.
- Rilevare che tipo di filtri di pacchetto/firewall sono in uso.

Guarda l'Esempio 1. Qual è il comando Nmap usato? Cosa fa l'opzione -A? Cosa fa l'opzione -T4?

L'Esempio 1 mostrato nell'immagine 1 utilizza il comando `nmap -A -T4 scanme.nmap.org`.

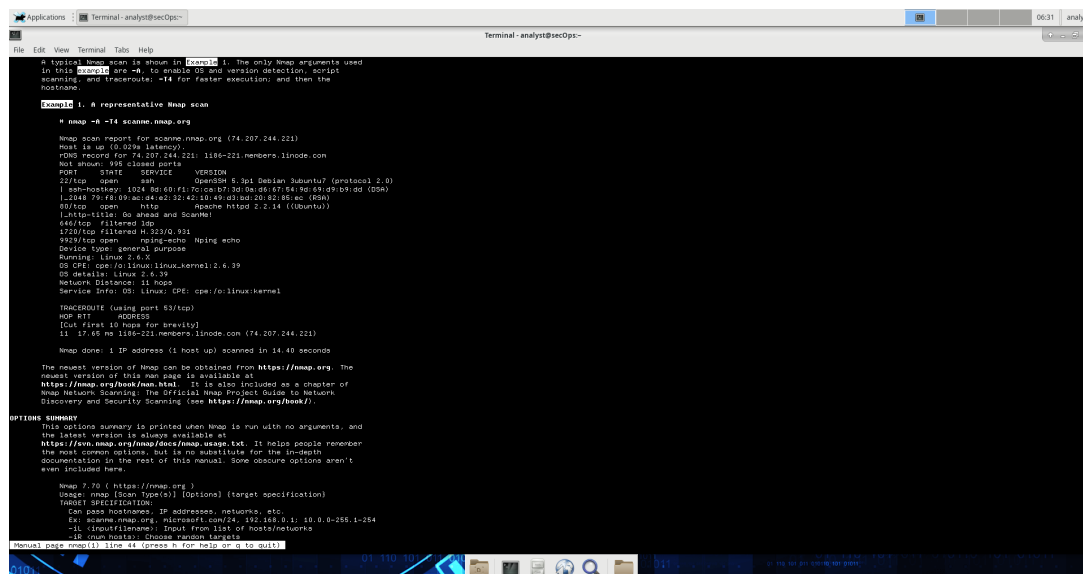


Figure 1: Esempio 1: Scansione Nmap di scanme.nmap.org.

- **Comando Nmap usato:** `nmap -A -T4 scanme.nmap.org`.
- **Opzione -A:** Abilita il rilevamento del sistema operativo (OS detection), la rilevazione della versione (version detection), la scansione degli script (script scanning) e il traceroute.
- **Opzione -T4:** Imposta il template di temporizzazione su "Aggressive" (o "Faster execution"). Questo significa che Nmap userà un approccio più rapido per la scansione, riducendo i tempi di attesa tra i pacchetti.

Parte 2: Scansione delle Porte Aperte

Passo 1: Scansiona il tuo localhost. Quali porte e servizi sono aperti?

Il comando utilizzato per scansionare il localhost è `nmap -A -T4 localhost`. L'output della scansione del localhost (mostrato nell'immagine 2) indica le seguenti porte e servizi aperti:

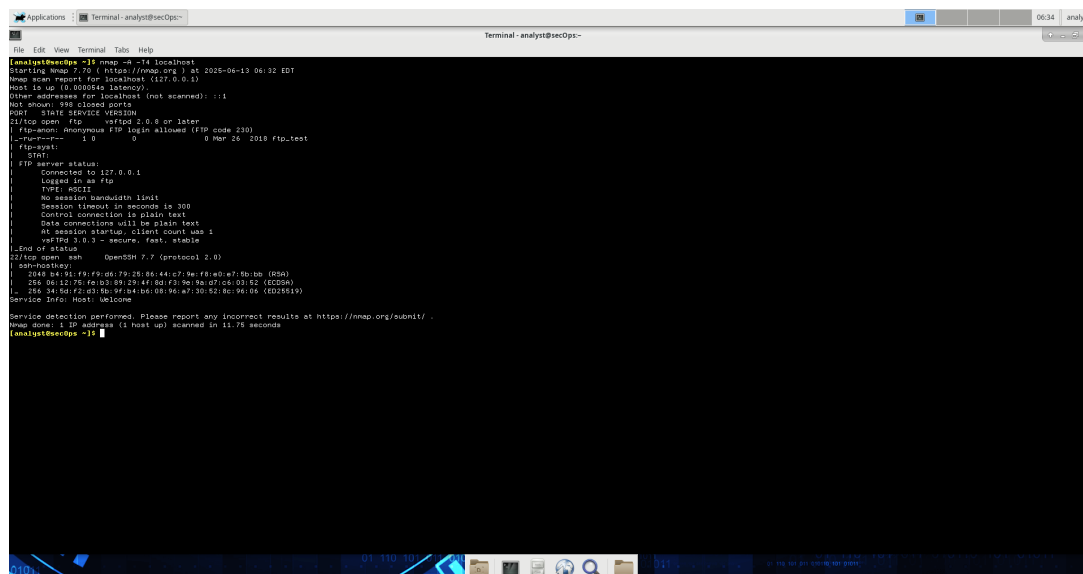


Figure 2: Output della scansione Nmap del localhost.

- **Porta 21/tcp:** Servizio ftp (versione vsftpd 2.0.8 or later).

– ftp-syst: STAT: logged in as ftp.

- **Porta 22/tcp:** Servizio ssh (versione OpenSSH 7.7 (protocol 2.0)).

Al prompt dei comandi del terminale, inserisci `ip address` per determinare l'indirizzo IP e la subnet mask per questo host. Registra l'indirizzo IP e la subnet mask per la tua VM. A quale rete appartiene la tua VM?

L'output del comando `ip address` (mostrato nell'immagine 3) fornisce i seguenti dettagli per la VM:

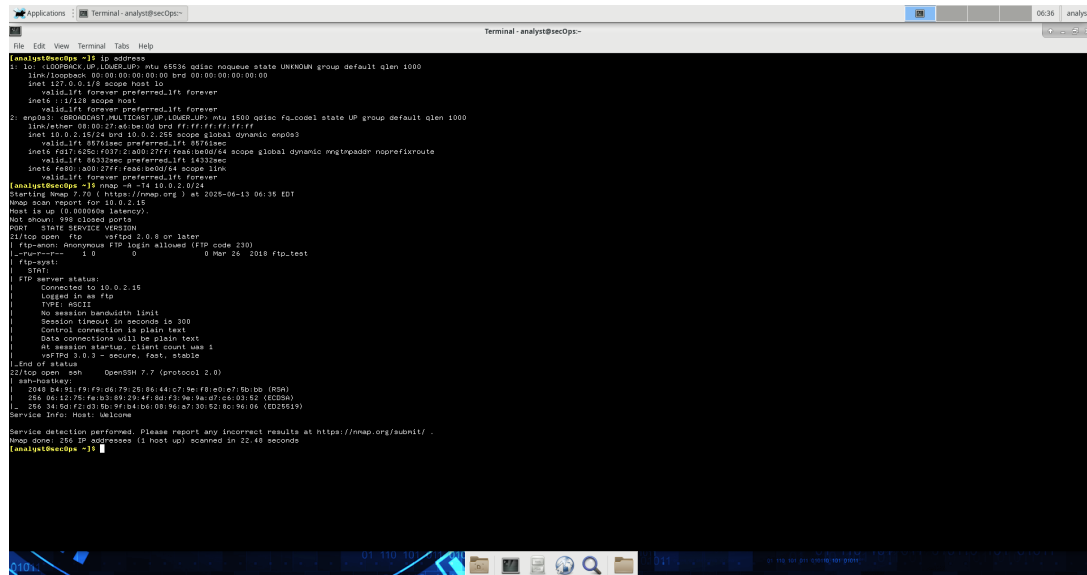


Figure 3: Output del comando `ip address`.

- **Indirizzo IP per la VM:** 10.0.2.15
- **Subnet mask:** Il prefisso /24 indica una subnet mask di 255.255.255.0.

La VM appartiene alla rete 10.0.2.0/24.

Per localizzare altri host su questa LAN, inserisci `nmap -A -T4 indirizzo_rete/prefisso`. Quanti host sono attivi?

L'immagine 3 mostra anche l'output della scansione della rete locale (10.0.2.0/24).

La scansione della rete locale ha identificato **1 host attivo** (l'indirizzo IP 10.0.2.15).

Passo 3: Scansiona un server remoto. Apri un browser web e naviga su scanme.nmap.org. Leggi il messaggio pubblicato. Qual è lo scopo di questo sito?

Navigando su scanme.nmap.org (come mostrato nell'immagine 4), il messaggio pubblicato dal "Nmap Security Scanner Project" indica che lo scopo del sito è aiutare gli utenti a imparare Nmap e a testare che la loro installazione di Nmap (o la connessione internet) funzioni correttamente. Gli utenti sono autorizzati a scansionare questa macchina con Nmap o altri scanner di porte. Viene anche specificato di non abusare del servizio (pochi scan al giorno vanno bene, ma non 100 volte al giorno o l'uso di tool per crackare password SSH).

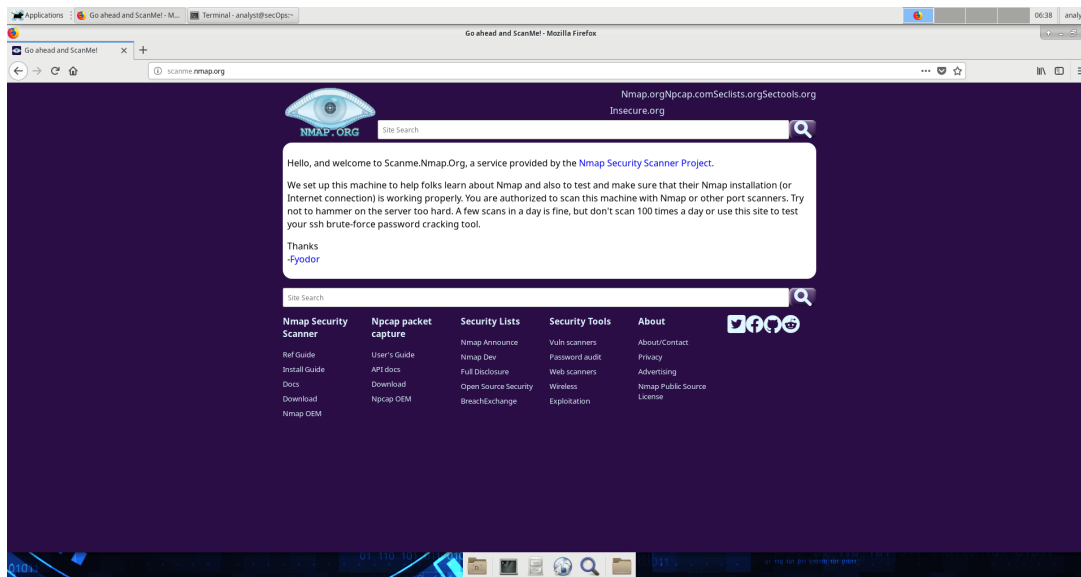


Figure 4: Pagina web di scanme.nmap.org.

Al prompt del terminale, inserisci `nmap -A -T4 scanme.nmap.org`. Rivedi i risultati e rispondi alle seguenti domande. Quali porte e servizi sono aperti? Quali porte e servizi sono filtrati? Qual è l'indirizzo IP del server? Qual è il sistema operativo?

L'output del comando `nmap -A -T4 scanme.nmap.org` (mostrato nell'immagine 5) fornisce i seguenti risultati:

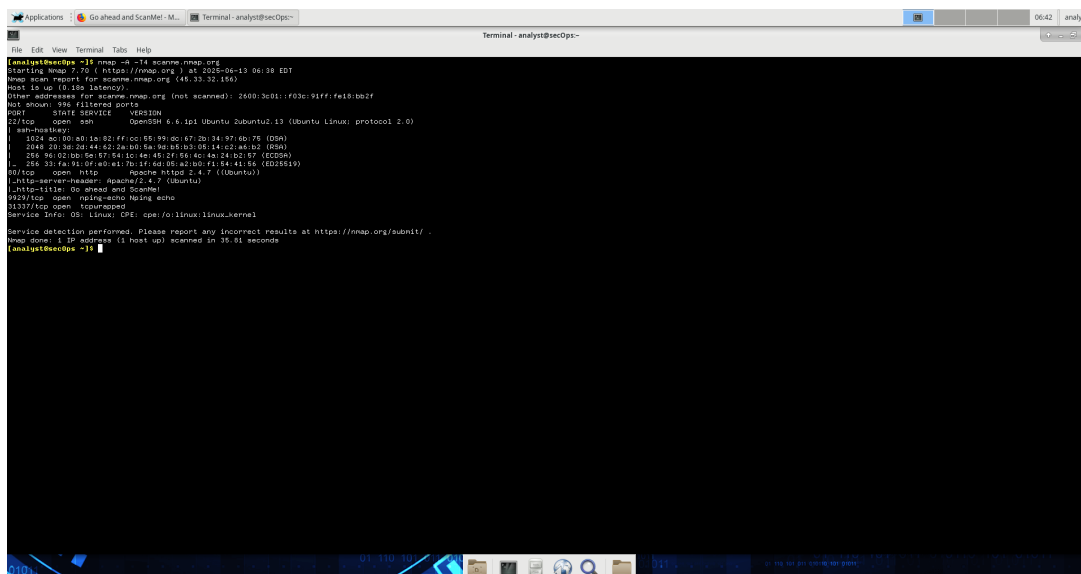


Figure 5: Output della scansione Nmap di scanme.nmap.org.

- **Porte e servizi aperti:**
 - **Porta 22/tcp:** ssh (OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 protocol 2.0)
 - **Porta 80/tcp:** http (Apache httpd 2.4.7 (Ubuntu))
 - **Porta 31337/tcp:** tcpwrapped (Servizio info: OS Linux; CPE: cpe:/o:linux:kernel)
- **Porte e servizi filtrati:** La scansione effettuata su scanme.nmap.org (come visibile nell'immagine 5) non ha restituito informazioni su porte filtrate.
- **Indirizzo IP del server:** L'indirizzo IP risolto per scanme.nmap.org è 45.33.32.156.

- **Sistema Operativo:** Il sistema operativo rilevato è **Linux**. Più specificamente, il campo "Service Info" per la porta 31337/tcp indica OS Linux; CPE: cpe:/o:linux:kernel.

Domanda di Riflessione

Come può Nmap aiutare con la sicurezza della rete? Come può Nmap essere usato da un attore malevolo come strumento nefasto?

Nmap come strumento per la sicurezza della rete (uso benevolo): Nmap è uno strumento fondamentale per gli analisti di sicurezza e gli amministratori di rete. Può aiutare con la sicurezza della rete in diversi modi:

- **Ricognizione e Mappatura della Rete:** Permette di identificare tutti i dispositivi attivi su una rete, le porte aperte, i servizi in esecuzione e le versioni del software. Questo è cruciale per mantenere un inventario aggiornato delle risorse di rete e per comprendere la superficie di attacco.
- **Vulnerability Assessment:** Rilevando le versioni dei servizi, Nmap può aiutare a identificare software obsoleti o vulnerabili. Ad esempio, una versione vecchia di OpenSSH o Apache potrebbe avere exploit noti.
- **Audit di Sicurezza:** Gli amministratori possono utilizzare Nmap per simulare attacchi esterni o interni e verificare le configurazioni dei firewall e delle regole di sicurezza. Si può controllare se le porte critiche sono esposte involontariamente.
- **Gestione delle Patch:** Identificando le versioni del sistema operativo e delle applicazioni, Nmap può aiutare a prioritizzare e gestire l'applicazione di patch di sicurezza.
- **Troubleshooting di Rete:** Può essere usato per diagnosticare problemi di connettività e di configurazione dei servizi.

Nmap come strumento nefasto per un attore malevolo: Purtroppo, la stessa potenza e versatilità che rendono Nmap utile per la sicurezza possono essere sfruttate da attori malevoli (cracker o attaccanti) per scopi nefasti:

- **Ricognizione Preliminare:** Un attaccante può usare Nmap per raccogliere informazioni sulla rete di una vittima, identificando bersagli potenzialmente vulnerabili. Questo include la scoperta di indirizzi IP attivi, porte aperte, servizi in esecuzione e tipi di sistemi operativi.
- **Identificazione delle Vulnerabilità:** Una volta identificati i servizi e le loro versioni, l'attaccante può cercare exploit pubblici per quelle versioni specifiche (ad esempio, una vulnerabilità in `vsftpd` o `OpenSSH`) per ottenere accesso non autorizzato.
- **Bypass di Firewall/IDS:** Nmap offre varie tecniche di scansione che possono essere usate per eludere il rilevamento da parte di firewall e sistemi di rilevamento delle intrusioni (IDS), come scansioni stealth (es. SYN scan), scansioni frammentate o scansioni idle.
- **Fingerprinting del Sistema Operativo:** Il rilevamento del sistema operativo (-O o incluso in -A) aiuta l'attaccante a scegliere gli exploit specifici per la piattaforma della vittima.
- **Scripting Malevolo:** La capacità di Nmap di eseguire script (NSE - Nmap Scripting Engine) può essere utilizzata per automatizzare attività di attacco come la brute-force di credenziali, il rilevamento di vulnerabilità specifiche o la raccolta di informazioni più dettagliate.

In sintesi, Nmap è uno strumento neutro; la sua etica dipende dalle intenzioni dell'utente. È una spada a doppio taglio che, sebbene indispensabile per la difesa, è altrettanto potente nelle mani di un attaccante.