Report Analitico - Esplorazione Funzionalità Nmap

Studente: Nicola Cassandra
Data: 20/02/2026
Obiettivo dell'esercizio: Esplorazione delle funzionalità di Nmap, Information Gathering e Network Scanning su localhost, LAN locale e target remoto.

---

1. EXECUTIVE SUMMARY

L'attività ha previsto l'impiego del tool Nmap per condurre una ricognizione di rete sistematica. È stato eseguito il mapping delle interfacce locali, la scoperta di host attivi sulla subnet locale (10.0.2.0/24) e il fingerprinting avanzato (OS e version detection) su un target remoto, dimostrando come questo strumento possa rivelare servizi esposti, porte filtrate e dettagli architetturali critici per la valutazione della superficie di attacco.

---

2. METODOLOGIA E STRUMENTI

Strumento Utilizzato	**Categoria**	**Scopo Tecnico**
Nmap 7.40	Port Scanner / Reconnaissance	Scansione delle porte, rilevamento dei servizi, identificazione dei sistemi operativi e audit di sicurezza della rete. +1
Man Pages (Linux)	Documentazione	Consultazione della documentazione ufficiale per comprendere l'utilizzo di flag specifici come -A e -T4.
ip / iproute2	Networking	Identificazione dell'indirizzo IP locale e della subnet mask per determinare il range della rete LAN.

- **Metodologia Applicata:** La procedura si è divisa in tre fasi incrementali di ricognizione:
    1. Scansione del **localhost** (127.0.0.1) per identificare i servizi in esecuzione sulla macchina stessa.
    2. Scoperta degli host (Host Discovery) sulla **LAN locale** (10.0.2.0/24).
    3. Scansione approfondita su un **server remoto** (scanme.nmap.org) per valutare l'esposizione su Internet e il comportamento dei firewall.

---

3. ANALISI TECNICA E CATENA DI ESECUZIONE

1. Analisi della documentazione di Nmap

Il primo passo ha richiesto la consultazione del manuale di Nmap per definire i parametri ottimali per la scansione.

Bash:

```
man nmap
```

Attraverso la funzione di ricerca della pagina manuale (/example), sono stati analizzati due flag fondamentali utilizzati nell'esercizio:

- -A: Abilita il rilevamento del sistema operativo (OS detection), il rilevamento della versione dei servizi, lo script scanning e il traceroute.
- -T4: Imposta il template di temporizzazione su "Aggressive" per un'esecuzione più rapida.

2. Scansione del Localhost È stata eseguita una scansione aggressiva sul localhost per enumerare i servizi attivi sulla VM CyberOps.

Bash:

```
nmap -A -T4 localhost
```

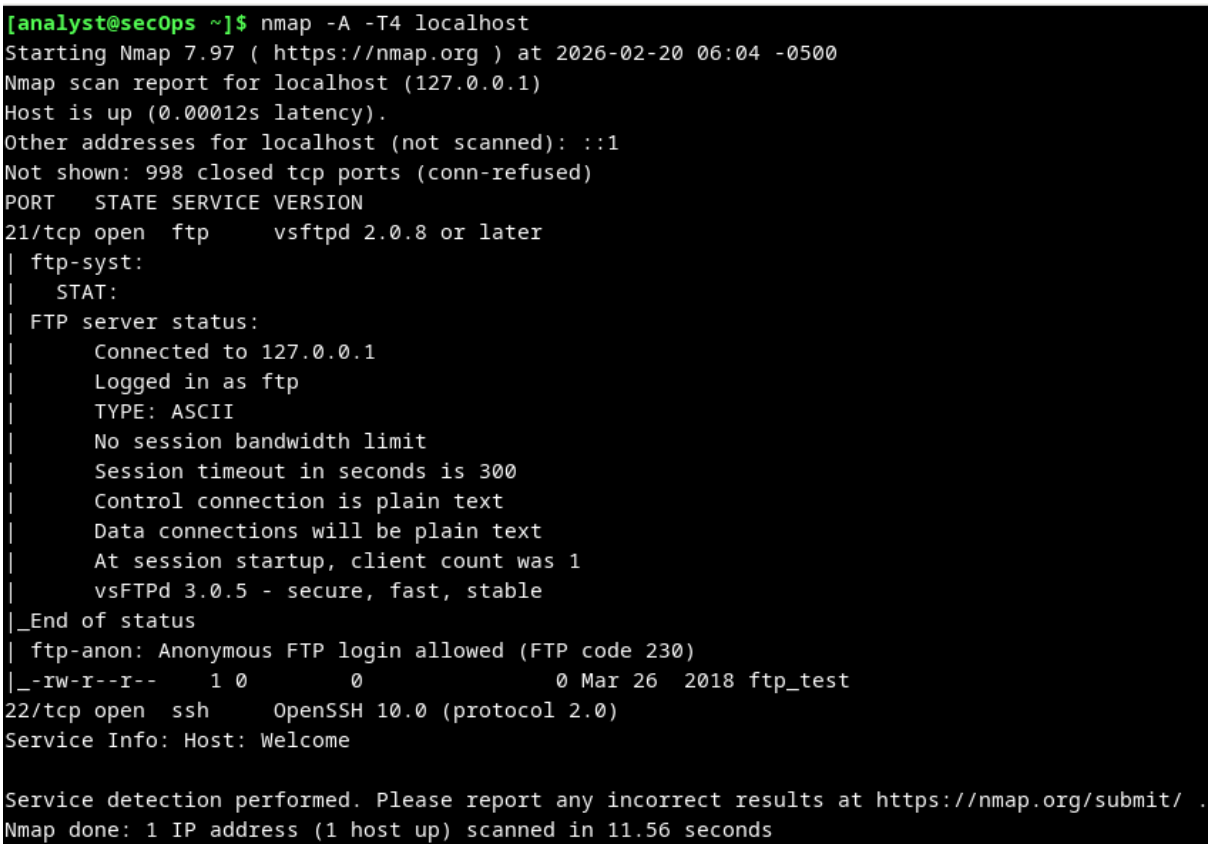

Fig. 1. L'output evidenzia l'apertura delle porte 21 (FTP), 22 (SSH) e 23 (Telnet). In particolare, il servizio FTP (vsftpd 2.0.8) risulta vulnerabile poiché consente l'accesso anonimo (Anonymous FTP login allowed).

3. Identificazione della Rete e Host Discovery Per mappare la rete locale, è stato prima necessario identificare l'indirizzo IP e il prefisso di rete della macchina virtuale.

Bash:

```
ip address
```

Avendo appurato che l'interfaccia di rete ha IP **10.0.2.15** con subnet /24 (255.255.255.0), è stata lanciata una scansione sull'intera subnet (indirizzo di rete **10.0.2.0/24**).

Bash:

```
nmap -A -T4 10.0.2.0/24
```

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 11:31 -0500
Nmap scan report for 10.0.2.15
Host is up (0.000039s latency).
Not shown: 998 closed tcp ports (conn-refused)
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 10.0.2.15
|      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 3
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 10.0 (protocol 2.0)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 70.83 seconds
[analyst@secOps ~]$
```

Output della scansione dell'intera subnet 10.0.2.0/24 L'esecuzione rivela host attivi sulla rete locale (es. **10.0.2.2**, **10.0.2.3**, **10.0.2.4** e il nostro **10.0.2.15**), fornendo una chiara visibilità sulla topologia interna.

4. Scansione del Target Remoto Come ultima fase di *Information Gathering*, è stato preso di mira il server esterno messo a disposizione dal progetto Nmap.

Bash

```
nmap -A -T4 scanme.nmap.org
```

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 09:35 -0500
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.22 seconds
[analyst@secOps ~]$
```

Risultati della scansione sul target scanme.nmap.org: La scansione verso l'IP remoto

45.33.32.156 rivela porte aperte come la 22 (OpenSSH 6.6.1p1) e la 80 (Apache httpd 2.4.7), mentre altre risultano filtrate (es. porte 25, 135, 139, 445), indicando la presenza di un firewall a protezione del target.

---

4. RISULTATI E VULNERABILITÀ SFRUTTATE

L'esercizio è di natura ricognitiva, pertanto non sono stati lanciati exploit attivi. Tuttavia, la fase di *footprinting* ha messo in luce gravi *Misconfiguration* sul Localhost, che un attaccante potrebbe sfruttare.

Vulnerabilità / Rischio Rilevato	**Categoria CWE**	**Dettagli Tecnici**
Anonymous FTP Login	**CWE-284** (Improper Access Control)	Il servizio FTP locale (vsftpd) consente l'accesso in lettura (-rw-r--r--) senza autenticazione. Un attaccante potrebbe accedere a file sensibili.
Uso di protocolli in chiaro (Telnet)	**CWE-319** (Cleartext Transmission of Sensitive Information)	La porta **23/tcp** è esposta. L'uso di Telnet permette lo sniffing delle credenziali di accesso tramite cattura pacchetti.
Information Disclosure	**CWE-200** (Exposure of Sensitive Information)	I banner dei servizi esposti su **scanme.nmap.org** rivelano le versioni esatte dei demoni (OpenSSH 6.6.1p1, Apache 2.4.7), facilitando la ricerca di exploit noti da parte degli attaccanti.

> **Nota per il Blue Team:** Sebbene Nmap sia un tool fondamentale per la gestione degli inventari e gli audit di rete da parte degli amministratori , un attore malevolo lo utilizza esattamente nello stesso modo per effettuare ricognizione avanzata e identificare punti deboli prima di lanciare un attacco.

---

5. CONCLUSIONI E MITIGAZIONE

L'esplorazione pratica ha dimostrato l'efficacia di Nmap nell'enumerare rapidamente risorse di rete, mappare i servizi attivi e identificare i sistemi operativi sottostanti. La scoperta di servizi non sicuri e di porte filtrate ha evidenziato l'importanza vitale della visibilità di rete per la postura di sicurezza.

Remediation (Prospettive per il Blue Team):

- **Hardening dei Servizi Locali:** È imperativo disabilitare l'accesso anonimo (Anonymous login) sul demone vsftpd modificando il file di configurazione (vsftpd.conf) e impostando anonymous_enable=NO.
- **Disattivazione Protocolli Legacy:** Il servizio Telnet (porta 23) deve essere disabilitato immediatamente, favorendo esclusivamente protocolli crittografati come SSH (porta 22) per l'amministrazione remota.
- **Configurazione Intrusion Detection System (IDS):** Le scansioni Nmap con parametri aggressivi (come -T4 e -A) generano una firma di traffico molto rumorosa. È raccomandato configurare regole su sistemi IDS/IPS (es. Snort o Suricata) per rilevare scansioni delle porte, bloccare temporaneamente gli IP sorgente e allertare il SOC.
- **Minimizzazione della Superficie di Attacco:** Mascherare o disabilitare la restituzione dei banner (Banner Grabbing) sui server web (es. direttiva ServerTokens Prod in Apache) e sui servizi SSH per mitigare l'Information Disclosure e ostacolare il versioning dei servizi da parte degli attaccanti.