Network Security Assessment in Ambiente Virtualizzato

Analisi della Superficie di Attacco tramite Nmap

Ardelean Pop Catalin
Master in Cyber Security Specialist – Epicode

20 febbraio 2026

Indice

1 Obiettivo dell'attività

L'obiettivo dell'attività è stato valutare la superficie di attacco della rete di laboratorio configurata in ambiente virtualizzato tramite VirtualBox con modalità NAT, utilizzando tecniche di scansione attiva mediante Nmap.

L'analisi ha avuto lo scopo di:

- Identificare gli host attivi nella subnet.
- Rilevare eventuali servizi TCP esposti.
- Analizzare il comportamento della rete in modalità NAT.
- Valutare il livello di esposizione interna dei sistemi.

2 Scenario di laboratorio

L'ambiente di laboratorio è composto da più macchine virtuali collegate tramite rete NAT interna su VirtualBox.

Configurazione della rete:

- Subnet: 192.168.50.0/24
- Macchina Attacker (Linux): analyst@secOps
- Windows Server: 192.168.50.2
- Windows 10 Client: 192.168.50.3
- Linux Server: 192.168.50.11

La modalità NAT consente la comunicazione tra le macchine virtuali all'interno della stessa rete privata virtuale, mantenendo isolamento rispetto alla rete fisica dell'host.

3 Metodologia di scansione

È stata effettuata una scansione completa della subnet tramite il comando:

```
nmap -A -T4 192.168.50.0/24
```

Parametri utilizzati:

- -A: abilita OS detection, version detection e script NSE.
- -T4: timing aggressivo per velocizzare la scansione.
- /24: scansione dell'intera subnet.

La scansione è stata condotta da una macchina Linux interna alla stessa rete virtuale.

```
[analyst@secOps ~]$ nmap -A -T4 192.168.50.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-20 11:05 -0500
Nmap scan report for 192.168.50.2
Host is up (0.00079s latency).
All 1000 scanned ports on 192.168.50.2 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.50.3
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
8080/tcp open  http    SimpleHTTPServer 0.6 (Python 3.13.7)
|_http-server-header: SimpleHTTP/0.6 Python/3.13.7
|_http-title: Directory listing for /

Nmap scan report for 192.168.50.11
Host is up (0.00089s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.11
|      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 2
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
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 (3 hosts up) scanned in 55.88 seconds
```

Figura 1: Output Nmap - Scansione della subnet

4 Risultati della scansione

La scansione completa della subnet 192.168.50.0/24 ha identificato tre host attivi su 256 indirizzi IP analizzati.

```
nmap -A -T4 192.168.50.0/24
```

Tempo totale di scansione: 55.88 secondi.

4.1 Host 192.168.50.2

- Host raggiungibile (latenza: 0.00079s).
- 1000 porte TCP scansionate.
- Tutte le porte risultano **closed (conn-refused)**.

Analisi tecnica

Lo stato *conn-refused* indica che:

- Il pacchetto SYN raggiunge correttamente l'host.
- Il sistema risponde con pacchetto RST.
- Non sono presenti servizi in ascolto sulle porte standard.

Non sono stati rilevati servizi esposti. La superficie di attacco TCP risulta nulla.

4.2 Host 192.168.50.3

- Host attivo (latenza: 0.0012s).
- 999 porte chiuse (conn-refused).
- 1 porta aperta.

Servizi rilevati:

- 8080/tcp – HTTP

Dettagli servizio

- Server: SimpleHTTPServer 0.6
- Tecnologia: Python 3.13.7
- Directory listing abilitato

L'output Nmap indica:

- Header HTTP identificato.
- Titolo pagina: "Directory listing for /".

Valutazione del rischio

La presenza di un web server in ascolto sulla porta 8080 introduce una superficie di attacco applicativa.

Rischi associati:

- Esposizione non intenzionale di file.
- Enumerazione directory.
- Possibile disclosure di informazioni sensibili.

Il modulo *SimpleHTTPServer* di Python è generalmente utilizzato per test locali e non è progettato per ambienti di produzione.

4.3 Host 192.168.50.11

- Host attivo (latenza: 0.00089s).
- 998 porte chiuse (conn-refused).
- 2 porte aperte.

Porta 21/tcp – FTP

- Servizio: vsftpd 3.0.5
- Accesso anonimo abilitato (FTP code 230)
- Comunicazione in plain text

Evidenze rilevate

- Login anonimo consentito.
- File visibile: ftp_test.
- Connessioni di controllo e dati non cifrate.

Valutazione del rischio

- Data exfiltration.
- Enumerazione contenuti.
- Intercettazione credenziali.

La presenza di FTP anonimo rappresenta la criticità principale rilevata nella rete.

Porta 22/tcp – SSH

- Servizio: OpenSSH 10.0
- Protocollo 2.0

Service Info: Host identificato come “Welcome”.
Rischi potenziali

- Attacchi brute force.
- Tentativi di accesso remoto non autorizzati.
- Enumerazione utenti.

SSH rappresenta un servizio legittimo ma costituisce un punto di esposizione che deve essere adeguatamente protetto.

4.4 Sintesi dei risultati

- 3 host attivi rilevati.
- 1 host senza servizi esposti.
- 1 host con servizio HTTP attivo su porta 8080.
- 1 host con servizi FTP (anonimo) e SSH attivi.

La superficie di attacco complessiva è concentrata sugli host 192.168.50.3 e 192.168.50.11.

5 Analisi del comportamento in modalità NAT

L'ambiente di laboratorio utilizza una rete virtuale configurata in modalità NAT. La scansione è stata eseguita da una macchina interna alla stessa subnet, pertanto il traffico non ha attraversato dispositivi di rete fisici esterni.

I risultati mostrano che:

- Tutti gli host attivi rispondono correttamente alle richieste TCP.
- Gli stati *closed (conn-refused)* indicano ricezione del pacchetto SYN e risposta con RST.
- Le porte *open* indicano servizi effettivamente in ascolto.

Questo comportamento conferma che:

- La connettività interna è pienamente funzionante.
- La modalità NAT non filtra né altera il traffico tra macchine della stessa rete virtuale.
- Gli stati rilevati dipendono esclusivamente dalla configurazione locale dei sistemi.

Pertanto, l'assenza o la presenza di servizi esposti non è imputabile alla topologia di rete virtuale, ma alla configurazione applicativa e firewall dei singoli host.

6 Valutazione complessiva della superficie di attacco

L'analisi evidenzia una superficie di attacco distribuita su due host:

- 192.168.50.2: nessun servizio esposto.
- 192.168.50.3: servizio HTTP attivo su porta 8080.

- 192.168.50.11: servizi FTP (anonimo) e SSH attivi.

Valutazione sintetica:

- Un host presenta superficie TCP nulla.
- Un host espone un servizio web potenzialmente non hardenizzato.
- Un host espone servizi di rete critici (FTP e SSH).

Il rischio principale è rappresentato da:

- FTP con accesso anonimo e comunicazione in chiaro.
- Directory listing HTTP attivo su porta 8080.

Il rischio complessivo della rete interna può essere classificato come **moderato**, con esposizione concentrata sui servizi applicativi dei sistemi 192.168.50.3 e 192.168.50.11.

7 Raccomandazioni di sicurezza

Sulla base delle evidenze raccolte, si raccomandano le seguenti misure:

- Disabilitare immediatamente l'accesso FTP anonimo.
- Sostituire FTP con SFTP o FTPS per garantire cifratura del traffico.
- Disabilitare il servizio SimpleHTTPServer se non strettamente necessario.
- Disabilitare il directory listing sul servizio HTTP.
- Implementare meccanismi di protezione SSH (es. autenticazione a chiave pubblica).
- Limitare l'accesso ai servizi tramite firewall interno.
- Implementare sistemi di logging e monitoraggio centralizzato.

L'applicazione di tali misure ridurrebbe significativamente la superficie di attacco interna.

8 Conclusioni

L'attività di scansione ha permesso di identificare in modo preciso i servizi effettivamente esposti nella rete di laboratorio.

L'analisi ha evidenziato:

- Un host correttamente non esposto.
- Un servizio web attivo su porta non standard con directory listing abilitato.
- Un server Linux con FTP anonimo e servizio SSH accessibile.

La presenza di servizi apparentemente destinati a test o configurazioni di laboratorio dimostra come anche ambienti controllati possano presentare vettori di attacco concreti.

L'attività conferma l'importanza della verifica periodica della superficie di attacco, del principio di minimizzazione dei servizi esposti e dell'adozione di configurazioni conformi alle best practice di sicurezza.

L'approccio metodologico adottato risulta coerente con una fase preliminare di penetration testing e security assessment in ambito enterprise.