Relazione: 9.3.8 Lab – Exploring Nmap

Introduzione

Il laboratorio "Exploring Nmap" ha lo scopo di fornire una panoramica sull'uso di Nmap, un potente strumento di scansione di rete utilizzato per la scoperta degli host e la valutazione della sicurezza. Durante il laboratorio, sono stati esplorati i comandi principali di Nmap e le sue funzionalità attraverso esercizi pratici su macchine virtuali.

Obiettivi

1. Esplorare le funzionalità di Nmap tramite le pagine di manuale (man pages).
2. Scansionare porte aperte su localhost.
3. Effettuare una scansione della rete locale.
4. Analizzare i risultati di una scansione su un server remoto.

Parte 1: Esplorazione di Nmap

Cos'è Nmap?

Nmap (“Network Mapper”) è un tool utilizzato per:

- Esplorare reti e identificare host attivi.
- Analizzare i servizi attivi su una rete.
- Effettuare audit di sicurezza.

Uso delle pagine di manuale

Tramite il comando:

```
man nmap
```

si ottiene una descrizione dettagliata dello strumento, con informazioni su:

- Scoperta degli host
- Scansione delle porte
- Rilevazione del sistema operativo
- Audit di sicurezza

Analisi di un esempio

Il comando:

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

permette di effettuare una scansione avanzata.

- **Opzione -A**: Abilita il rilevamento del sistema operativo, la scansione delle versioni dei servizi e il traceroute.
- **Opzione -T4**: Aumenta la velocità della scansione per connessioni a banda larga.

Parte 2: Scansione delle Porte Aperte

Scansione di localhost

Eseguendo il comando:

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

sono state rilevate le seguenti porte aperte:

- **21/tcp**: Servizio FTP (“vsftpd”)
- **22/tcp**: Servizio SSH (“OpenSSH”)

Scansione della rete locale

Dopo aver identificato l'IP della VM con:

```
ip address
```

si è eseguita la scansione con:

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

Dalla scansione sono emersi i seguenti risultati:

- **Host attivi**: 4
- **Servizi rilevati**:
    - FTP su porta 21/tcp
    - SSH su porta 22/tcp
    - Telnet su porta 23/tcp

Scansione di un server remoto

Si è poi effettuata la scansione del server **scanme.nmap.org**:

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

I risultati hanno mostrato:

- **IP del server**: 45.33.32.156
- **Sistema operativo**: Ubuntu Linux
- **Porte aperte**:
  - 22/tcp: SSH (OpenSSH)
  - 80/tcp: HTTP (Apache)
  - 9929/tcp: nping-echo
  - 31337/tcp: tcpwrapped
- **Porte filtrate**:
  - 25/tcp: SMTP
  - 135/tcp: MSRPC
  - 139/tcp: NetBIOS
  - 445/tcp: Microsoft-DS

Conclusioni

Nmap è un potente strumento per l'analisi delle reti, utile sia per amministratori di sistema che per esperti di sicurezza. Le sue funzionalità permettono di:

- Identificare host e servizi in una rete.
- Analizzare vulnerabilità e potenziali punti di accesso.
- Monitorare lo stato della sicurezza di un'infrastruttura.

Tuttavia, Nmap può anche essere utilizzato per scopi malevoli da parte di attaccanti per raccogliere informazioni su reti e sistemi vulnerabili, motivo per cui il suo utilizzo dovrebbe essere sempre autorizzato e regolamentato.