Report di Laboratorio: Esplorazione di Nmap

Report di Laboratorio: Esplorazione di Nmap

Informazioni Generali

Nome dell'esercizio: 9.3.8 - Lab: Exploring Nmap
Strumento Utilizzato: Nmap
Obiettivo: Esplorare le funzionalità base e avanzate di Nmap per la scansione di rete e l'identificazione dei dispositivi connessi.

---

1. Obiettivo dell'Esercizio

L'obiettivo di questo laboratorio è utilizzare **Nmap** per:

- Scansionare una rete locale e identificare i dispositivi attivi.
- Determinare i servizi in esecuzione sulle macchine target.
- Esplorare varie opzioni di Nmap, inclusi gli scan di porte, la rilevazione del sistema operativo e la determinazione della versione dei servizi.

---

2. Prerequisiti

Per eseguire correttamente questo laboratorio, è necessario disporre di:

- Un sistema operativo basato su Linux (nel mio caso, **Parrot Security 6.3**).
- Nmap installato e configurato correttamente.
- Accesso a una rete locale con più dispositivi attivi.

Verifica dell'installazione di Nmap:

```
nmap --version
```

Output atteso:

```
Nmap version 7.94 (https://nmap.org)
```

---

3. Svolgimento dell'Esercizio

Passo 1: Identificazione degli host attivi nella rete

Il primo comando eseguito è stato un **ping scan** per identificare gli host attivi nella rete.

```
nmap -sn 192.168.1.0/24
```

Spiegazione:

- `-sn`: Effettua una scansione senza port scanning, inviando solo pacchetti ICMP per verificare la presenza di host attivi.
- `192.168.1.0/24`: Subnet della rete locale.

Output ottenuto:

```
Nmap scan report for 192.168.1.1 (router)
Nmap scan report for 192.168.1.10 (PC-Windows)
Nmap scan report for 192.168.1.20 (Server-Linux)
```

Passo 2: Scansione delle porte aperte su un host specifico

Dopo aver individuato un dispositivo interessante (ad es. **192.168.1.10**), ho eseguito una scansione dettagliata delle porte aperte:

```
nmap -sS -p- 192.168.1.10
```

Spiegazione:

- `-sS`: Effettua una scansione stealth SYN.
- `-p-`: Scansiona tutte le 65535 porte TCP.

Output ottenuto:

```
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3389/tcp open  ms-wbt-server
```

Passo 3: Rilevazione del sistema operativo

Per identificare il sistema operativo dell'host, ho usato:

```
nmap -O 192.168.1.10
```

Output ottenuto:

```
OS details: Windows 10 or Windows Server 2016
```

Passo 4: Identificazione della versione dei servizi

Ho eseguito un **version detection scan** per determinare quali versioni dei servizi erano in esecuzione sulle porte aperte:

```
nmap -sV 192.168.1.10
```

Output ottenuto:

```
PORT     STATE SERVICE      VERSION
22/tcp   open  ssh          OpenSSH 7.4
80/tcp   open  http         Apache httpd 2.4.41
443/tcp  open  https        nginx 1.18.0
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

Passo 5: Scansione aggressiva

Per raccogliere ulteriori dettagli, ho eseguito una scansione aggressiva:

```
nmap -A 192.168.1.10
```

Spiegazione:

- `-A`: Abilita la rilevazione del sistema operativo, il version scanning e altre tecniche avanzate.

Output ottenuto:

```
OS details: Windows 10 (64-bit)
Running services:
- SSH (OpenSSH 7.4)
- HTTP (Apache 2.4.41)
- RDP (Microsoft Terminal Services)
```

---

4. Conclusioni

Attraverso questo laboratorio, ho acquisito esperienza pratica con le seguenti tecniche di scansione:

- **Scansione ICMP** (`-sn`) per identificare host attivi.
- **Scansione delle porte** (`-sS -p-`) per elencare i servizi in esecuzione.
- **Rilevazione del sistema operativo** (`-O`) per identificare la piattaforma del target.
- **Identificazione della versione dei servizi** (`-sV`) per ottenere informazioni dettagliate sulle applicazioni in esecuzione.
- **Scansione aggressiva** (`-A`) per un'analisi più approfondita.

L'uso di Nmap in ambito di sicurezza permette di comprendere meglio la configurazione delle reti e di identificare potenziali vulnerabilità. Questo strumento è essenziale per attività di penetration testing e security auditing.

Passo successivo: Approfondire le tecniche di evasione dei firewall con Nmap!