Nmap Scanning & Web Enumeration Report

By: Jessica Stovall, Aspiring SOC Analyst

Project Title:

Network Reconnaissance & Service Enumeration Using Nmap

1. Objective

The purpose of this project was to perform basic network reconnaissance on a remote system using Nmap. The goal was to detect live hosts, enumerate open ports, identify running services, and explore any accessible web resources that may reveal further information.

2. Tools & Environment

- Tool: Nmap v7.80
- Environment: Kali Linux via TryHackMe AttackBox
- Target IP: 10.10.223.43

3. Scanning Process

Step 1: Basic Host and Port Scan

Executed an Nmap scan to detect live hosts and identify open TCP ports:

```
nmap 10.10.223.43
```

Step 2: TCP Connect Scan

Performed a more thorough TCP connect scan to enumerate services:

```
nmap -sT 10.10.223.43
```

4. Results

The scan revealed six open TCP ports:

Port	State	Service
7	Open	Echo

```
9     | Open  | Discard
13    | Open  | Daytime
17    | Open  | QOTD
22    | Open  | SSH
8008  | Open  | HTTP
MAC Address: 02:E2:64:44:A4:13
```

5. Web Enumeration

After identifying that port 8008 was running an HTTP service, I accessed it via a web browser to investigate further.

Through manual enumeration of the web interface and URL manipulation, I discovered a hidden directory path:

/SECRET_PAGE_38B9P6

Visiting this path revealed a flag, confirming successful discovery of a hidden resource.

6. Key Takeaways

- Practiced using Nmap for live host detection and service enumeration.
- Identified common and legacy ports.
- Demonstrated the ability to interpret scan results and pivot to web enumeration.
- Revealed hidden web content, simulating a basic capture-the-flag (CTF) task.

7. Skills Demonstrated

- Network scanning
- TCP service enumeration
- Web application reconnaissance

- Basic CTF methodology