Task 1: Reconnaissance & Vulnerability Scanning

Goal

To perform active reconnaissance and vulnerability scanning on a safe and authorized test system in order to identify open ports, running services, and potential security vulnerabilities.

Target System

- **IP Address:** 192.168.8.128
- **System Type:** Authorized local Linux machine
- **Environment:** Controlled lab environment
- **Authorization:** Scanning performed on own system for educational purposes

Tools Used

1. **Nmap** – For port and service enumeration
2. **Nikto** – For web vulnerability scanning
3. **Kali Linux** – Penetration testing operating system

Task 1.1: Active Reconnaissance using Nmap

Command Used

```
nmap -sS -sV -O -A 192.168.8.128
```

Description

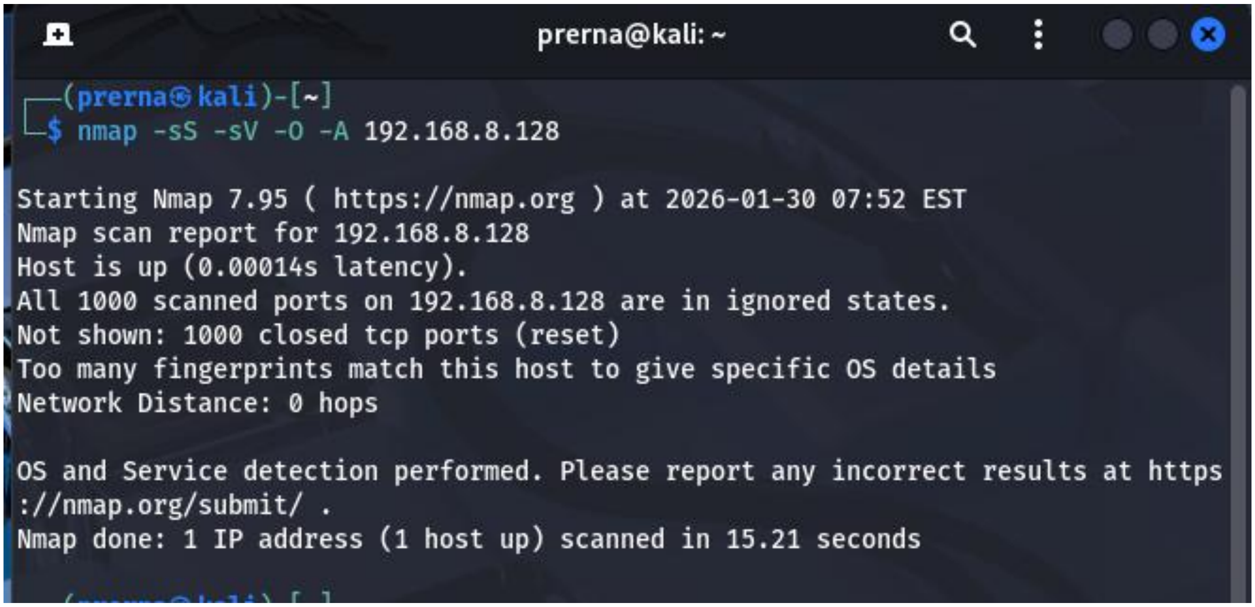
Nmap was used to perform active reconnaissance by identifying open ports, running services, and operating system details of the target system.

Findings

- Host was active and reachable
- No open TCP ports were detected
- No unnecessary network services were exposed

Security Analysis

The absence of open ports indicates a strong security configuration and a reduced attack surface, minimizing the risk of remote exploitation.



```
┌──(prerna㉿kali)-[~]
└─$ nmap -sS -sV -O -A 192.168.8.128

Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-30 07:52 EST
Nmap scan report for 192.168.8.128
Host is up (0.00014s latency).
All 1000 scanned ports on 192.168.8.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.21 seconds

┌──(prerna㉿kali)-[~]
```

Task 1.2: Vulnerability Scanning using Nikto

Command Used

```
nikto -h 192.168.8.128 -p 80
```

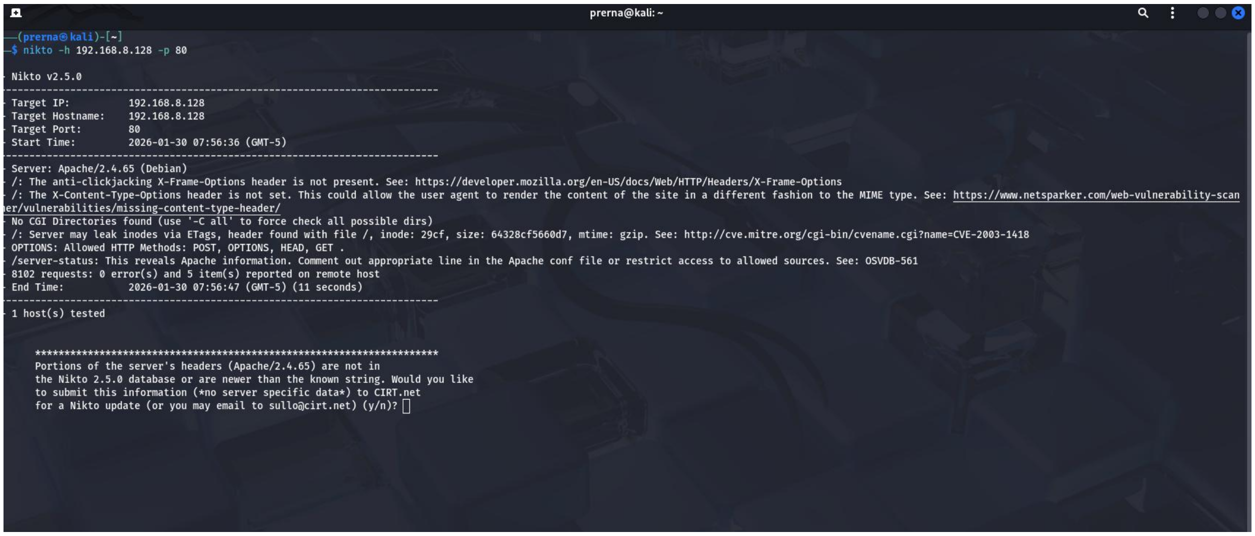
Description

Nikto was used to scan the Apache web server running on the target system to identify web-related vulnerabilities and misconfigurations.

Findings

- Missing **X-Frame-Options** header (clickjacking risk)
- Missing **X-Content-Type-Options** header (MIME sniffing risk)
- Apache server version disclosure
- HTTP OPTIONS method enabled

- `/server-status` page accessible



```
──(prerna㉿kali)-[~]
─$ nikto -h 192.168.8.128 -p 80

- Nikto v2.5.0
---------------------------------------------------------------------------
- Target IP:          192.168.8.128
- Target Hostname:    192.168.8.128
- Target Port:        80
- Start Time:         2026-01-30 07:56:36 (GMT-5)
---------------------------------------------------------------------------
- Server: Apache/2.4.65 (Debian)
- /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
- /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scan
er/vulnerabilities/missing-content-type-header/
- No CGI Directories found (use '-C all' to force check all possible dirs)
- /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 64328cf5660d7, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
- OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
- /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
- 8102 requests: 0 error(s) and 5 item(s) reported on remote host
- End Time:           2026-01-30 07:56:47 (GMT-5) (11 seconds)
---------------------------------------------------------------------------
- 1 host(s) tested


     *********************************************************************
     Portions of the server's headers (Apache/2.4.65) are not in
     the Nikto 2.5.0 database or are newer than the known string. Would you like
     to submit this information (*no server specific data*) to CIRT.net
     for a Nikto update (or you may email to sullo@cirt.net) (y/n)?
```

Identified Security Risks

- Clickjacking attacks due to missing security headers
- Information disclosure through server version and status page
- Increased attack surface due to enabled HTTP methods