ACTIVE RECON & WEB ENUMERATION REPORT

Objective

The objective of this assignment is to perform active reconnaissance on a designated target in order to identify live hosts, map open ports, enumerate running services, detect web directories, and analyze web application technologies. This exercise enhances practical skills in network scanning, service fingerprinting, web enumeration, and vulnerability identification using industry-standard tools such as Nmap, Dirb, WhatWeb, and Nikto.

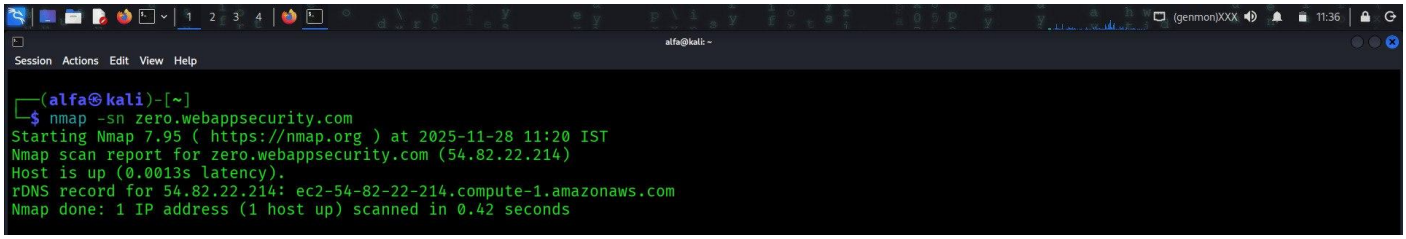
1. Intern Detail

Name: Ankit Vishwakarma

2. Target Information

Target Domain / IP	54.82.22.214
Allowed Target Source	zero.webappsecurity.com

3. Host Discovery



Command Used:
nmap -sn zero.webappsecurity.com

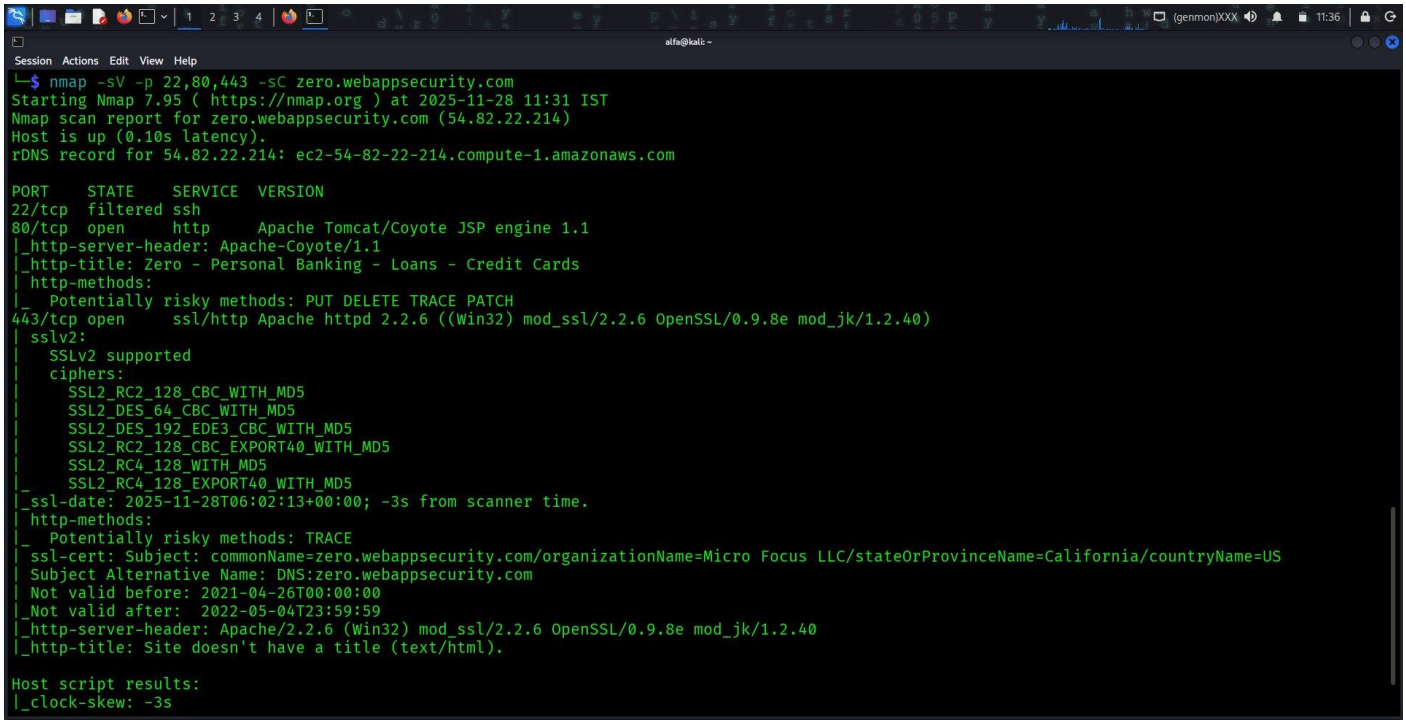
Results:
- Target IP Identified: 54.82.22.214
- Host Status: Alive

4. Port & Service Enumeration (Nmap)

4.1 Quick Scan (TCP SYN Scan)
Command: nmap -sS zero.webappsecurity.com

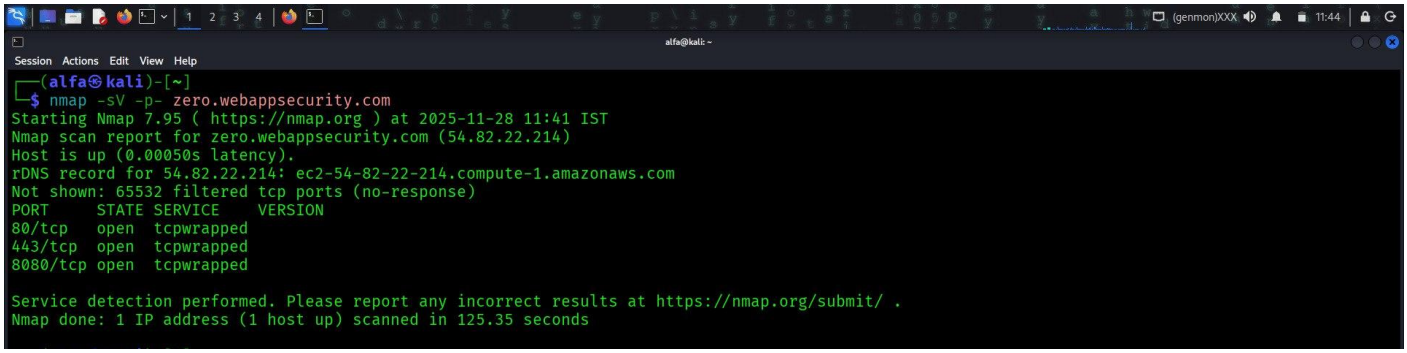
Findings:
- Open Ports: 80, 443, 8080

4.2 Service & Version Detection



Command: nmap -sV -p 22,80,443 zero.webappsecurity.com

4.3 Full Port Scan



Command: nmap -sV -p- zero.webappsecurity.com

Observations:
- Total Open Ports Found: 3

4.4 OS Detection

```
┌──(alfa㉿kali)-[~]
└─$ nmap -O --osscan-guess zero.webappsecurity.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 11:44 IST
Nmap scan report for zero.webappsecurity.com (54.82.22.214)
Host is up (0.012s latency).
rDNS record for 54.82.22.214: ec2-54-82-22-214.compute-1.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.22 seconds
```

Command: nmap -O --osscan-guess zero.webappsecurity.com

5. Directory Enumeration (Dirb)

```
┌──(alfa㉿kali)-[~]
└─$ dirb https://zero.webappsecurity.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Nov 28 13:56:15 2025
URL_BASE: https://zero.webappsecurity.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://zero.webappsecurity.com/ ----
+ https://zero.webappsecurity.com/aux (CODE:403|SIZE:205)
+ https://zero.webappsecurity.com/cgi-bin/ (CODE:403|SIZE:210)
+ https://zero.webappsecurity.com/com1 (CODE:403|SIZE:206)
+ https://zero.webappsecurity.com/com2 (CODE:403|SIZE:206)
+ https://zero.webappsecurity.com/com3 (CODE:403|SIZE:206)
+ https://zero.webappsecurity.com/con (CODE:403|SIZE:205)
^[[B^[[B^[[B
+ https://zero.webappsecurity.com/index.html (CODE:200|SIZE:44)
+ https://zero.webappsecurity.com/lpt1 (CODE:403|SIZE:206)
+ https://zero.webappsecurity.com/lpt2 (CODE:403|SIZE:206)
+ https://zero.webappsecurity.com/nul (CODE:403|SIZE:205)
+ https://zero.webappsecurity.com/prn (CODE:403|SIZE:205)
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^H^H^H^H^H^H^H^H^H^H^H^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[
A^[[A^[[A^[[A^[[A^[[A^H^?

-----------------
END_TIME: Fri Nov 28 15:35:05 2025
DOWNLOADED: 4612 - FOUND: 11
```

```
┌──(alfa㉿kali)-[~]
└─$ dirb https://zero.webappsecurity.com /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Nov 28 13:57:57 2025
URL_BASE: https://zero.webappsecurity.com/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://zero.webappsecurity.com/ ----
+ https://zero.webappsecurity.com/aux (CODE:403|SIZE:205)
+ https://zero.webappsecurity.com/cgi-bin/ (CODE:403|SIZE:210)
+ https://zero.webappsecurity.com/com1 (CODE:403|SIZE:206)
+ https://zero.webappsecurity.com/com2 (CODE:403|SIZE:206)
+ https://zero.webappsecurity.com/com3 (CODE:403|SIZE:206)
+ https://zero.webappsecurity.com/con (CODE:403|SIZE:205)
^[[B^[[B^[[B^[[B^[[B
^H
^H^H^H
+ https://zero.webappsecurity.com/index.html (CODE:200|SIZE:44)
+ https://zero.webappsecurity.com/lpt1 (CODE:403|SIZE:206)
+ https://zero.webappsecurity.com/lpt2 (CODE:403|SIZE:206)
+ https://zero.webappsecurity.com/nul (CODE:403|SIZE:205)
+ https://zero.webappsecurity.com/prn (CODE:403|SIZE:205)

-----------------
END_TIME: Fri Nov 28 15:37:21 2025
DOWNLOADED: 4612 - FOUND: 11
```

Commands:
dirb https://target.com
dirb https://target.com /usr/share/wordlists/dirb/common.txt

6. Web Fingerprinting

```
┌──(alfa㉿kali)-[~]
└─$ whatweb zero.webappsecurity.com
http://zero.webappsecurity.com [200 OK] Apache, Bootstrap, Content-Language[en-US], Country[UNITED STATES][US], HTML5, HTTPServer[Apache-Coyote/1
.1], IP[54.82.22.214], JQuery[1.8.2], Script[text/javascript], Title[Zero - Personal Banking - Loans - Credit Cards], UncommonHeaders[access-cont
rol-allow-origin], X-UA-Compatible[IE=Edge]
https://zero.webappsecurity.com [200 OK] Apache[2.2.6][Default][mod_jk/1.2.40,mod_ssl/2.2.6], Country[UNITED STATES][US], HTTPServer[Windows (32
bit)][Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40], IP[54.82.22.214], OpenSSL[0.9.8e], UncommonHeaders[access-control-allow-o
rigin]
```

6.1 WhatWeb Scan
Command: whatweb zero.webappsecurity.com

Findings:
- Technologies Detected: Apache + OpenSSL + Bootstrap + jQuery + HTML5 + Apache-Coyote running on a Windows-based server hosted in the United States.

6.2 Nikto Scan

```
Session Actions Edit View Help
┌──(alfa㉿kali)-[~]
└─$ nikto -h http://zero.webappsecurity.com -o nikto.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          54.82.22.214
+ Target Hostname:    zero.webappsecurity.com
+ Target Port:        80
+ Start Time:         2025-11-28 14:06:17 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: Retrieved access-control-allow-origin header: *.
+ /: 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 th
e MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ : Server banner changed from 'Apache-Coyote/1.1' to 'Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40'.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ HTTP method: 'PATCH' may allow client to issue patch commands to server. See RFC-5789.
^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restri
ct access to allowed sources. See: OSVDB-561
+ /admin/: This might be interesting.
+ /readme.txt: Uncommon header 'content-disposition' found, with contents: attachment; filename="readme.txt".
+ /readme.txt: This might be interesting.
+ /admin/index.html: Admin login page/section found.
+ /login.html: Admin login page/section found.
+ /manager/html: Default Tomcat Manager / Host Manager interface found.
^[[B^[[B^[[B^[[B+ /manager/status: Default Tomcat Server Status interface found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 10619 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2025-11-28 15:08:08 (GMT5.5) (3711 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(alfa㉿kali)-[~]
```

Command: nikto -h http:// zero.webappsecurity.com -o nikto.txt

Key Findings:
- The Nikto scan reveals multiple security issues:

- Outdated server components
- Missing security headers
- Dangerous HTTP methods enabled

- Exposure of sensitive directories like /admin and /manager/html
- CORS misconfiguration
- Information disclosure through readme files

Risk Level: HIGH

8. Conclusion

This assignment helped me understand structured active reconnaissance using legal and ethical methods. I practiced Nmap scanning, Dirb enumeration, and web fingerprinting with WhatWeb and Nikto, improving my ability to document findings professionally.