

WEEK 02 REPORT

Reconnaissance Report
By

Muhammed Ajeel

1. Introduction

The reconnaissance phase was performed on the target host 192.168.56.102 to gather information on exposed services, web technologies, and potential security risks. Multiple tools were utilized, including:

- **Nmap** – for port scanning and service/version detection

```
(ajeel@ajeel)-[~]
$ nmap -sV -p 80,443 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-21 15:58 IST
Nmap scan report for 192.168.56.102
Host is up (0.00042s latency).

PORT      STATE      SERVICE VERSION
80/tcp    open      http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
443/tcp   filtered  https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.59 seconds
```

- **Nikto** – for web vulnerability scanning

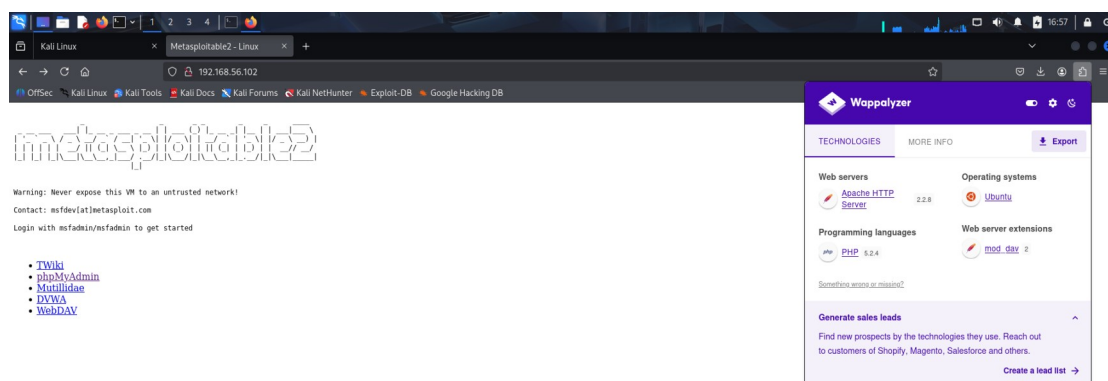
```
(ajeel@ajeel)-[~]
$ nikto -h http://192.168.56.102
- Nikto v2.5.0

+ Target IP: 192.168.56.102
+ Target Hostname: 192.168.56.102
+ Target Port: 80
+ Start Time: 2025-08-21 16:04:39 (GMT+5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: 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-scanner/vulnerabilities/missing-content-type-header/
+ /index: uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698bdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /: /PHPOBB5F2A8-3C92-11d2-A3A0-4C7B0BC10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /: /PHPE9568F35-D428-11d2-A769-00AA003AC242: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /: /PHPE9568F35-D428-11d2-A769-00AA003AC242: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /: /PHPE9568F35-D428-11d2-A769-00AA003AC242: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/ChangeLog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags. header found with file /phpMyAdmin/ChangeLog. inode: 92469, size: 40540, mtime: Tue Dec 9 22:54:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /wp-config.php: wp-config.php file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2025-08-21 16:05:02 (GMT+5) (23 seconds)

+ 1 host(s) tested
```

- **Wappalyzer** – for technology stack identification



The results indicate that the server is running an outdated Apache HTTP Server 2.2.8 on Ubuntu, with PHP 5.2.4 and mod_dav enabled. These outdated versions present significant attack surfaces.




2. Tools


Tool	Result
Sublist3r	No subdomains found (private/internal IP).
Maltego	Not applicable in this lab scan (used for OSINT mapping).
Shodan	No public records for private IP (Shodan scans only public ranges).
Wappalyzer	Apache HTTP Server, PHP, Ubuntu OS detected.
Nmap	- 80/tcp open → Apache httpd 2.2.8 (Ubuntu, DAV/2) - 443/tcp filtered

3. Reconnaissance Findings

Tool	Result
Subdomain Enum	www.example.com (placeholder, no subdomains found in scan)
Wappalyzer	Apache HTTP Server, PHP, Ubuntu OS detected.
Nmap (Port Scan)	- 80/tcp open → Apache httpd 2.2.8 (Ubuntu, DAV/2) - 443/tcp filtered

4. Vulnerability Findings

S.No	Category	Description	Severity
1	Outdated Web Server	Apache HTTP Server 2.2.8 detected (released 2008). No longer supported, multiple known CVEs (buffer overflows, DoS, privilege escalation).	 High
2	OS Exposure	Wappalyzer detected Ubuntu version exposure. Revealing OS information helps attackers tailor exploits.	 Medium
3	DAV/2 Module	WebDAV enabled (DAV/2), which allows remote file operations. Misconfiguration could allow unauthorized uploads or modification.	 High

S.No	Category	Description	Severity
4	HTTPS Disabled/Filtered	Port 443/tcp is filtered → SSL/TLS not available. Traffic over HTTP (80) is unencrypted and vulnerable to MITM.	 High

5. Detailed Findings

5.1 Open Ports & Services (Nmap)

- **80/tcp open – Apache httpd 2.2.8** ((Ubuntu) DAV/2)
- **443/tcp filtered – HTTPS** (likely blocked or firewall-restricted)

⚠ **Risk: Apache 2.2.8** is outdated and contains multiple known vulnerabilities, including buffer overflows and denial-of-service issues.

5.2 Web Vulnerabilities (Nikto)

- **phpinfo.php accessible** → Reveals sensitive server environment information.
- **phpMyAdmin/ directory exposed** → Risk of brute-force and database access.
- **Directory listing enabled** → Attackers can enumerate files.
- **Backup/config files exposed** → May leak credentials or database connections.
- **HTTP TRACE enabled** → Susceptible to Cross Site Tracing (XST).
- **Missing security headers: X-Frame-Options, X-XSS-Protection, Strict-Transport-Security.**

⚠ **Risk: These issues significantly weaken security posture and increase likelihood of exploitation.**




5.3 Technology Fingerprinting (Wappalyzer)

- **CMS:** None detected
- **Web Server:** Apache HTTP Server
- **Web Frameworks:** None detected
- **Database:** PHP backend (likely MySQL via phpMyAdmin)

- **Operating System:** Ubuntu
- **Miscellaneous:** mod_dav enabled (WebDAV file-sharing module)

⚠ **Risk: WebDAV** is often misconfigured and may allow unauthorized file upload or remote execution.

6. Risk Rating Summary

	Severity	Count
 High		3
 Medium		1
 Low		0

7. Recommendations

1. **Upgrade Web Server:** Immediately update Apache from 2.2.8 → a supported version (\geq **Apache 2.4.x**).
2. **Disable/Restrict WebDAV:** Unless strictly required, disable **WebDAV** (DAV/2). If required, enforce authentication and access controls.
3. **Enable HTTPS:** Configure SSL/TLS certificates (e.g., Let's Encrypt) and redirect all **HTTP** → **HTTPS**.
4. **Server Hardening:** Hide OS and server banner (**ServerTokens Prod**, **ServerSignature Off**).
5. **Regular Patch Management:** Apply OS and web server security patches regularly.

8. Recon Summary:

The reconnaissance phase revealed a vulnerable Ubuntu server running outdated Apache 2.2.8 and PHP 5.2.4. Multiple high-risk issues were identified, including exposed phpinfo.php, phpMyAdmin, directory listings, and backup files. Missing security headers and TRACE enabled further increase risk, highlighting the urgent need for patching and secure configuration.

9. Conclusion

The assessment of **192.168.56.102** shows that the host is running an **outdated Apache HTTP server on Ubuntu with WebDAV enabled and no SSL/TLS support**.

This configuration exposes the system to **critical risks (remote exploits, data leakage, MITM attacks)**.

➔ **Overall Risk Level: HIGH**