Project Title: Documentation and Reporting

Scope and Objective: This penetration test targeted the default web server (Apache on port 80) running on a Metasploitable2 virtual machine. The goal was to identify basic web server vulnerabilities using standard tools and to document findings and remediation recommendations in a professional format.

---

1. Executive Summary

A penetration test was performed on the HTTP service hosted on Metasploitable2 (IP: 10.138.16.138). Using `nmap`, `nikto`, and `curl`, the Apache server was found to be outdated and misconfigured. Multiple security issues were identified, including an enabled HTTP TRACE method, directory indexing, outdated PHP and Apache versions, and access to sensitive pages such as `phpinfo.php` and `phpMyAdmin`. These misconfigurations can lead to further exploitation if not mitigated.

---

2. Methodology

Target IP: 10.138.16.138
Port Tested: 80 (HTTP)

Tools Used:

- `nmap` for service discovery
- `nikto` for vulnerability scanning
- `curl` for HTTP header inspection
- Web browser for manual validation

---

3. Testing Steps & Tool Output

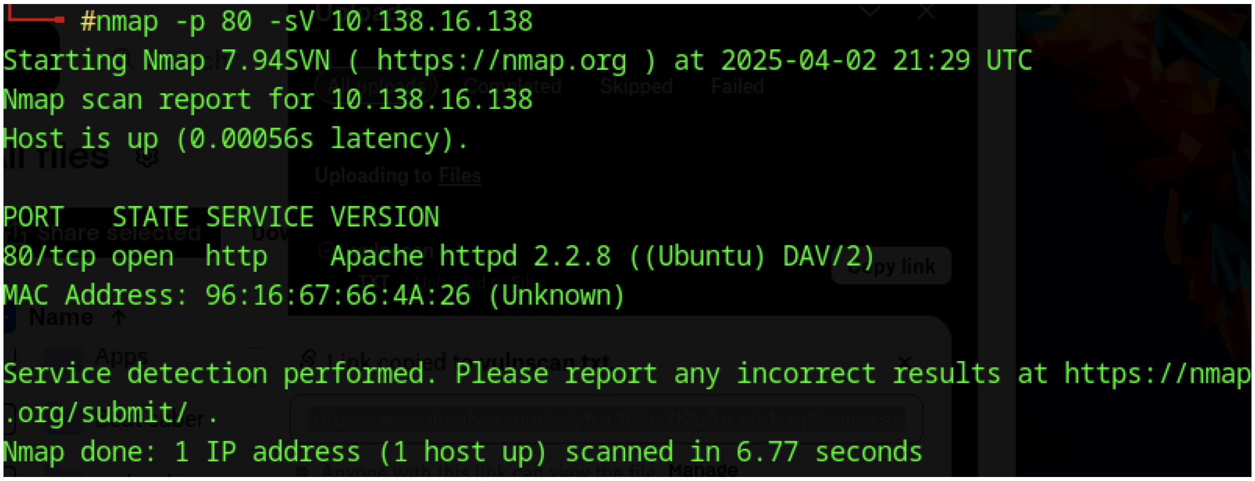
🔹 Step 1: Identify Open Web Port

Command:

```
nmap -p 80 -sV 10.138.16.138
```

Result:

- Apache httpd 2.2.8 ((Ubuntu) DAV/2) detected



```
└──╼ #nmap -p 80 -sV 10.138.16.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-02 21:29 UTC
Nmap scan report for 10.138.16.138
Host is up (0.00056s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 96:16:67:66:4A:26 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.77 seconds
```

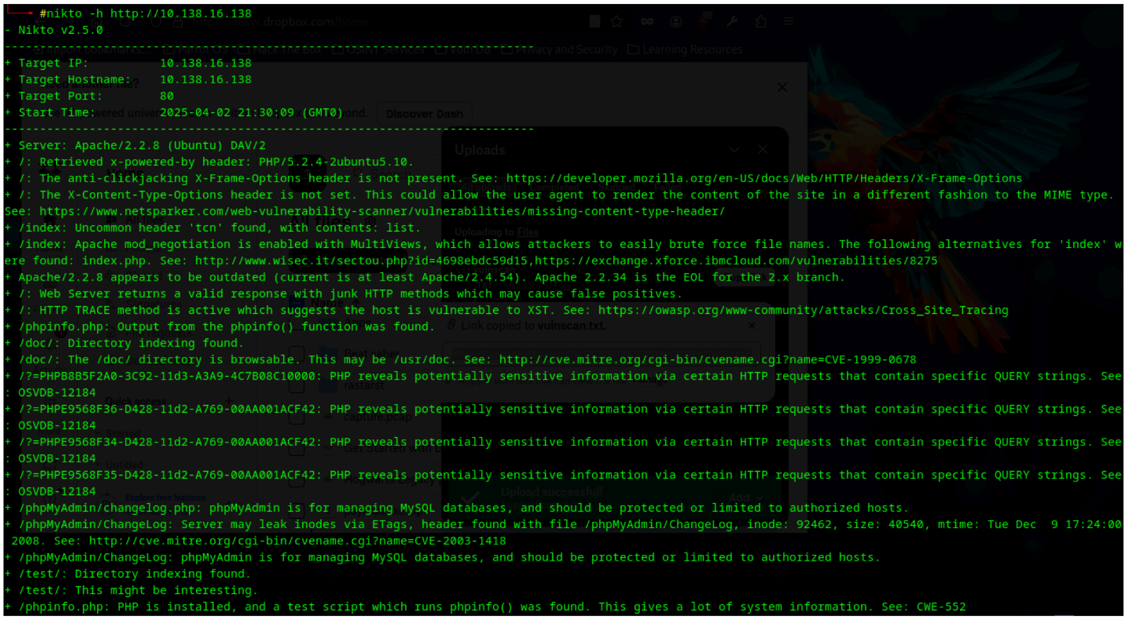
🔹 Step 2: Scan for Vulnerabilities

Command:

nikto -h http://10.138.16.138

Findings:

- Apache version is outdated (2.2.8)
- PHP version disclosed: 5.2.4
- HTTP TRACE method is enabled (vulnerable to XST)
- Directory indexing enabled on `/doc/`, `/icons/`, and `/test/`
- `phpinfo.php` file accessible — exposes system configuration
- Access to `/phpMyAdmin/` interface (should be protected)
- Potential sensitive file found: `#wp-config.php#`



```
└──▪ #nikto -h http://10.138.16.138
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.138.16.138
+ Target Hostname:    10.138.16.138
+ Target Port:        80
+ Start Time:         2025-04-02 21:30:09 (GMT0)
---------------------------------------------------------------------------
+ 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' w
ere found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,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
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See
: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See
: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See
: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: 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: 92462, size: 40540, mtime: Tue Dec  9 17:24:00
 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /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
```

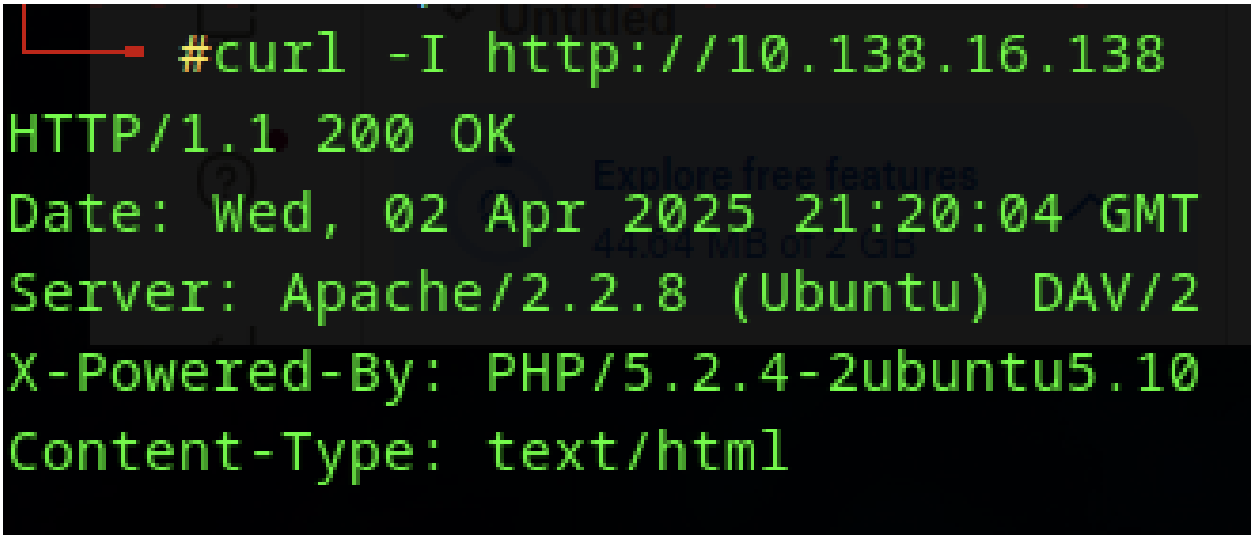
🔹 Step 3: Check HTTP Headers

Command:

curl -I http://10.138.16.138

Result:

- Server: Apache/2.2.8
- X-Powered-By: PHP/5.2.4-2ubuntu5.10



```
└──▪ #curl -I http://10.138.16.138
HTTP/1.1 200 OK
Date: Wed, 02 Apr 2025 21:20:04 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
```

4. Findings Summary

ID	Vulnerability	Risk Level	Evidence	How to Reproduce
1	Outdated Apache/PHP Versions	Medium	Nmap, Nikto, curl	nmap, curl -I
2	HTTP TRACE Enabled (XST)	Medium	Nikto output	`curl -X TRACE`
3	Directory Indexing	Low	Nikto + browser	Visit `/icons/`
4	Exposed `phpinfo.php`	Medium	Nikto + browser	Visit `/phpinfo.php`
5	Access to `phpMyAdmin`	High	Nikto + browser	Visit `/phpMyAdmin/`
6	Sensitive File (`#wp-config.php#`)	High	Nikto output	Visit `/#wp-config.php#`

---

5. Remediation Recommendations

- **Upgrade Apache** to a maintained version (2.4.54+)
- **Disable HTTP TRACE** in Apache config:
  TraceEnable Off
- **Restrict directory access** and disable indexing:
  Options -Indexes
- **Remove or restrict access** to `phpinfo.php` and `/phpMyAdmin/`
- **Sanitize or remove sensitive files** like `#wp-config.php#`

---

6. Evidence

- Nmap scan result showing Apache version
- Nikto scan showing vulnerable findings (PHP info, TRACE, directories)
- curl output confirming headers and versions
- Screenshots of directory listing and exposed files (to be attached)