Vulnerability Scanning Lab

Author: Harshal Harekar
Date: 07/10/2025

1. Objective

- Produce reproducible scan results
- Prioritized findings table
- Remediation notes

2. Environment

- Host / Attacker Machine: Kali Linux
- Target: Metasploitable 2 VM

3. Scan Setup

1. Recon port/service fingerprinting (fast):

```
nmap -Pn -sS -T4 -p- --min-rate 1000 192.168.18.138 -oN nmap_allports.txt
```

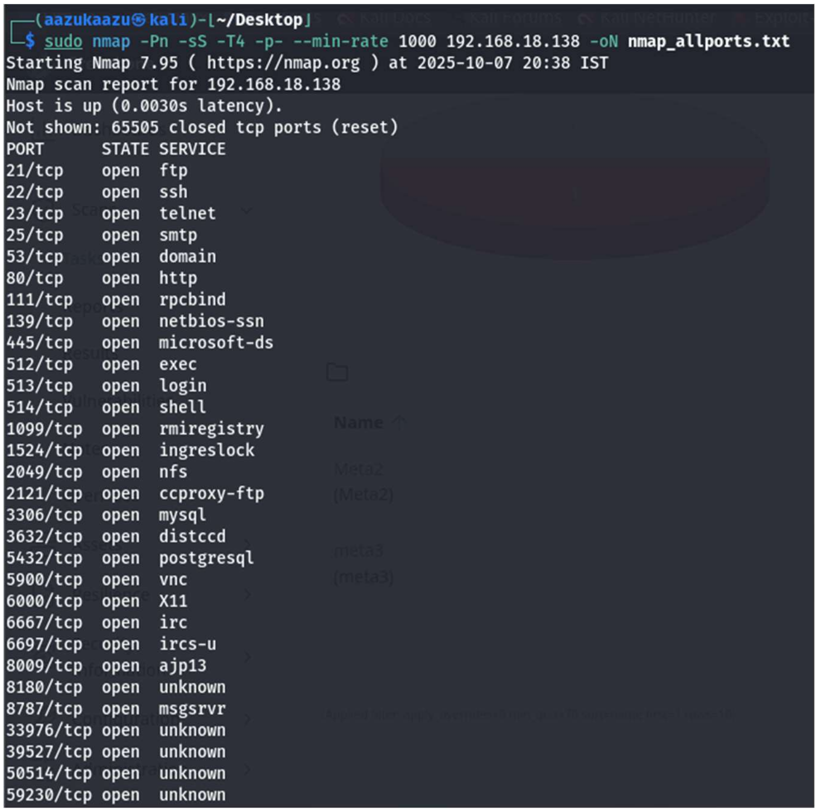
2. Service/version + scripts (service detection + scripts):

```
nmap -Pn -sV -sC -T4 192.168.18.138 -oN nmap_svcs.txt
```

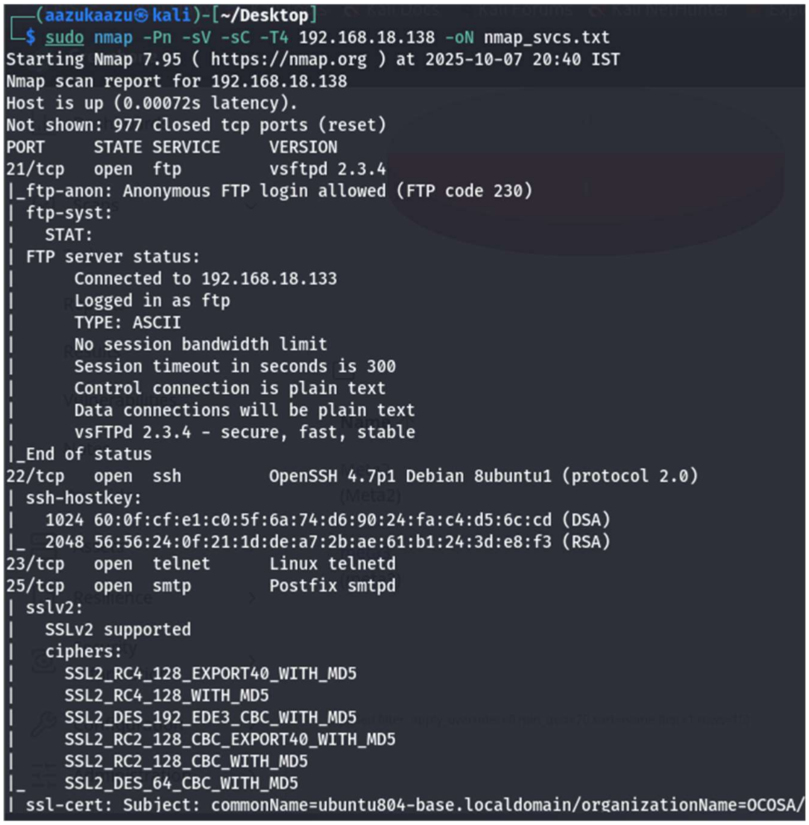
3. Web scan (Nikto):

```
nikto -h http://192.168.18.138 -output nikto_192.168.18.138.txt
```

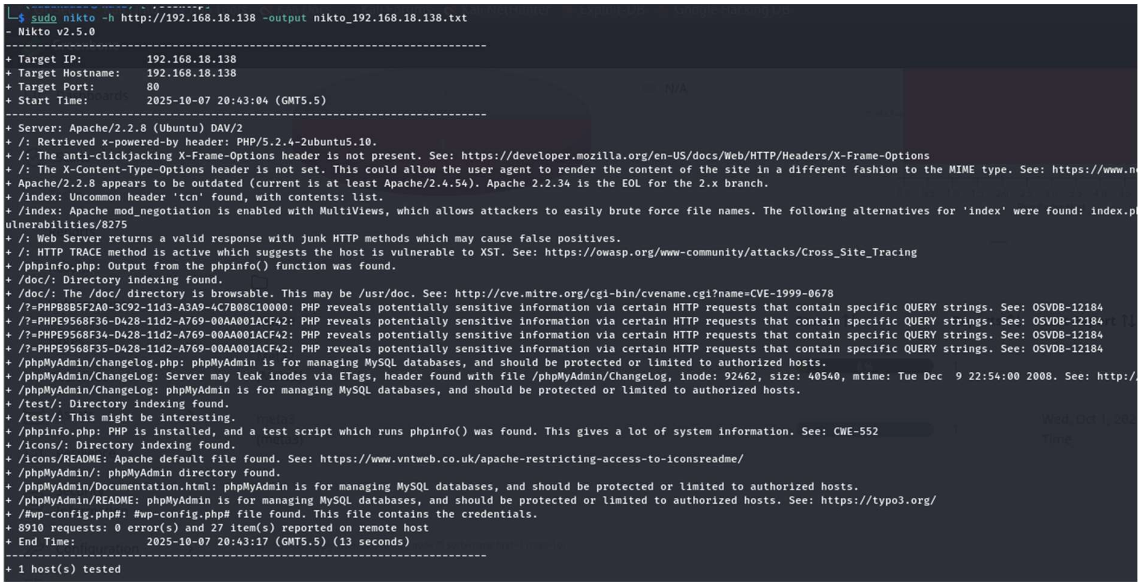
4. Authenticated OpenVAS scan



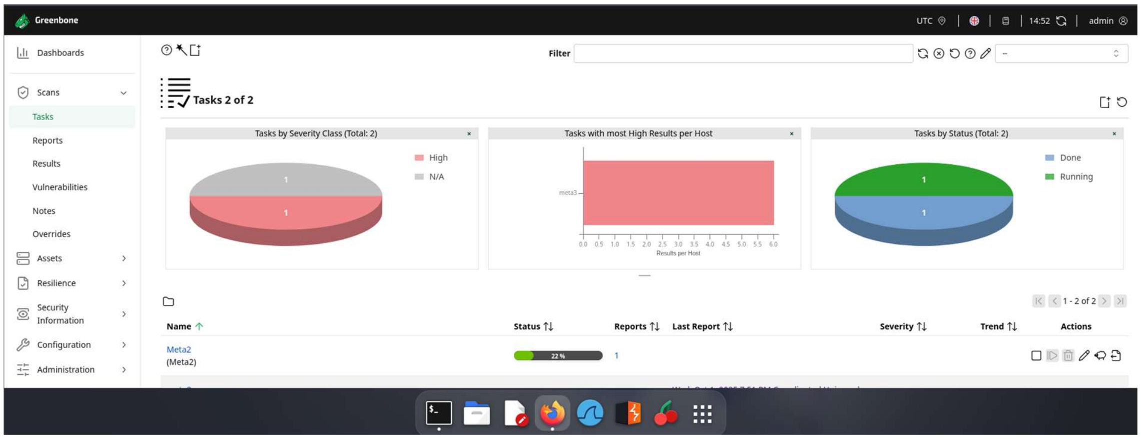
```
┌──(aazukaazu㉿kali)-[~/Desktop]
└─$ sudo nmap -Pn -sS -T4 -p- --min-rate 1000 192.168.18.138 -oN nmap_allports.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-07 20:38 IST
Nmap scan report for 192.168.18.138
Host is up (0.0030s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33976/tcp open  unknown
39527/tcp open  unknown
50514/tcp open  unknown
59230/tcp open  unknown
```



```
┌──(aazukaazu㉿kali)-[~/Desktop]
└─$ sudo nmap -Pn -sV -sC -T4 192.168.18.138 -oN nmap_svcs.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-07 20:40 IST
Nmap scan report for 192.168.18.138
Host is up (0.00072s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.18.133
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/
```



```
└─$ sudo nikto -h http://192.168.18.138 -output nikto_192.168.18.138.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.18.138
+ Target Hostname:    192.168.18.138
+ Target Port:        80
+ Start Time:         2025-10-07 20:43:04 (GMT5.5)
---------------------------------------------------------------------------
+ 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.ne
+ 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.
+ /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.ph
ulnerabilities/8275
+ /: 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 22:54:00 2008. See: http:/
+ /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
+ /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:           2025-10-07 20:43:17 (GMT5.5) (13 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



Name ↑	Status ⇅	Reports ⇅	Last Report ⇅	Severity ⇅	Trend ⇅	Actions
Meta2 (Meta2)	22 %	1				

4. Prioritization rules

- **Critical**: CVSS ≥ 9 OR remote code execution exposures on internet-facing hosts.
- **High**: CVSS 7–8.9 or unauthenticated access to sensitive services.
- **Medium**: CVSS 4–6.9 with limited exploitability.
- **Low**: informational or authenticated-only issues.

5. Findings table

Scan ID	Vulnerability	CVSS	Priority	Host
1	vsftpd 2.3.4 (known backdoor)	9.8	Critical	192.168.18.138
2	wp-config file disclosure (credentials leak)	9	Critical	192.168.18.138
3	Old PHP version (PHP/5.2.4) — multiple vulnerabilities likely	9	Critical	192.168.18.138
4	Metasploitable bind shell (tcp/1524) present — known backdoor	9.8	Critical	192.168.18.138
5	Anonymous FTP allowed	7	High	192.168.18.138
6	PHP info page exposed (phpinfo())	7.5	High	192.168.18.138
7	phpMyAdmin directory accessible (management console exposed)	8	High	192.168.18.138
8	Apache httpd 2.2.8 (outdated; EOL, known RCEs possible)	8	High	192.168.18.138
9	Telnet service running (cleartext credentials)	7	High	192.168.18.138
10	Samba (SMB) services with message signing disabled / outdated Samba 3.x	7	High	192.168.18.138
11	MySQL 5.0.51a (outdated DB, known auth/privilege risks)	7.5	High	192.168.18.138
12	PostgreSQL 8.3.x (outdated DB)	7	High	192.168.18.138
13	Missing X-Frame-Options (clickjacking risk)	4.3	Low	192.168.18.138
14	Missing X-Content-Type-Options header	4.3	Low	192.168.18.138
15	HTTP TRACE method enabled (XST risk)	4.3	Low	192.168.18.138
16	Uncommon header tcn / unusual server behavior (potential info leak)	3.5	Low	192.168.18.138
17	Multiple default/demo files and README files present (information disclosure)	4	Low	192.168.18.138
18	Directory indexing found (/doc/, /test/, /icons/)	5.3	Medium	192.168.18.138
19	Apache mod_negotiation MultiViews enabled (file brute-force)	5.5	Medium	192.168.18.138
20	SMTP supports SSLv2 / weak ciphers	6.8	Medium	192.168.18.138
21	OpenSSH 4.7p1 (very old) — weak algorithms/keys	6.5	Medium	192.168.18.138
22	VNC (protocol 3.3) accessible	6	Medium	192.168.18.138
23	ProFTPD 1.3.1 (ftp on tcp/2121) — outdated service	6.8	Medium	192.168.18.138
24	RPC/NFS exports available (rpcbind + nfs)	6.5	Medium	192.168.18.138
25	Java RMI (1099) / UnrealIRCd (6667) — outdated components	6	Medium	192.168.18.138

6. Remediation

1. vsftpd 2.3.4 - Uninstall vsftpd 2.3.4 immediately; replace with maintained FTP/SFTP server or disable FTP; block TCP/21 at network perimeter; rotate any exposed credentials; apply host-level IDS and file-integrity monitoring.

2. Anonymous FTP allowed - Disable anonymous FTP logins; restrict FTP access to authenticated accounts or internal IP ranges; enforce strong passwords and chroot users; audit and remove sensitive files from FTP root.

3. phpinfo() exposed - Remove phpinfo() from production; restrict access to localhost or authenticated admin-only paths; remove test scripts from webroot and back up then delete.

4. wp-config-like file disclosure - Remove any backup/config files from webroot; move configuration files outside webroot; rotate DB and app credentials; audit repository and deploy .htaccess denies for sensitive filenames.

5. phpMyAdmin accessible - Restrict phpMyAdmin to management VLAN or IP allowlist; enforce strong admin credentials and 2FA; place behind VPN or SSH tunnel; remove if unused.

6. Directory indexing (/doc/, /test/, /icons/) - Disable directory indexing in Apache (Options -Indexes); remove demo/test directories and unused files; harden file permissions.

7. Apache 2.2.8 outdated - Upgrade Apache to a supported version (>=2.4.x as per vendor); apply all security patches; test compatibility in staging before production.

8. mod_negotiation MultiViews enabled - Disable MultiViews (Options -MultiViews) unless explicitly required; validate content negotiation settings; document and limit file alternatives.

9. Missing X-Frame-Options - Add X-Frame-Options: DENY or Content-Security-Policy: frame-ancestors 'none' to HTTP responses via webserver or application.

10. Missing X-Content-Type-Options - Add header X-Content-Type-Options: nosniff at server or application level.

11. HTTP TRACE enabled - Disable TRACE method in Apache (TraceEnable Off); test to ensure TRACE no longer responds.

12. Uncommon tcn header / info leak - Remove or normalize non-standard informative headers; configure server to expose only minimal required headers.

13. Old PHP version (5.2.4) - Upgrade PHP to a supported, patched release; remove legacy code dependent on EOL PHP; run application tests; apply WAF rules during upgrade window.

14. SMTP supports SSLv2 / weak ciphers - Disable SSLv2/weak ciphers in SMTP configuration; enable TLS1.2+ only; deploy strong cipher suites and obtain valid certs; test with SSL scanners.

15. OpenSSH 4.7p1 old - Upgrade OpenSSH to current stable; disable weak key types (DSA), remove small keys, enforce RSA 2048+/ED25519, enforce Protocol 2, enable Fail2Ban or similar.

16. Telnet service running - Disable telnetd; remove telnet package; use SSH for remote management; rotate any credentials exposed via telnet.

17. Samba (SMB) weak / signing disabled - Upgrade Samba to supported version; enable SMB signing and SMBv2/3 only; disable guest/null sessions; restrict shares and apply least-privilege ACLs.

18. MySQL 5.0.x outdated - Upgrade MySQL to supported version; apply secure configuration (remove test DBs, anonymous users, bind to localhost or internal IPs); rotate DB credentials.

19. PostgreSQL 8.3.x outdated - Upgrade PostgreSQL to supported version; secure pg_hba.conf to restrict connections; rotate DB credentials and remove default/demo databases.

20. VNC protocol 3.3 accessible - Disable unauthenticated VNC or wrap with SSH/VPN; require strong passwords and limit source IPs; remove VNC if unused.

21. Bind shell (tcp/1524) present - Remove or disable bind shell services; identify and remove backdoor binaries; perform full host integrity scan; rebuild host if necessary.

22. ProFTPD 1.3.1 outdated - Upgrade or remove ProFTPD; disable unused FTP services; use SFTP; harden FTP configuration and disable anonymous.

23. RPC/NFS exports available - Review /etc/exports; restrict NFS exports to specific IPs/subnets; disable insecure ACLs; require root_squash where appropriate.

24. Java RMI / UnrealIRCd outdated - Patch or remove outdated services; update to supported releases; restrict access via firewall and limit exposure to management network.
25. Default/demo README files present - Remove default/demo/readme files from webroot; review repository for leaked information; perform inventory and harden webroot contents.