VAPT T1 Report — Metasploitable Lab

1 - Anonymous FTP allowed (vsftpd 2.3.4)

Target: 192.168.137.129:21
Severity: Medium-High (depends on data)
Description:
Anonymous FTP login allowed - anonymous access to FTP root. vsftpd 2.3.4 is an outdated version used in Metasploitable.

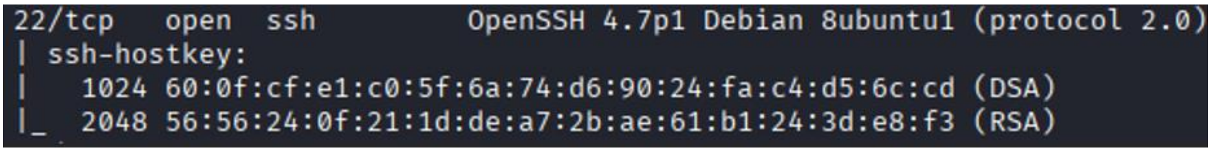
Recommendation:

1. Disable anonymous FTP: edit /etc/vsftpd.conf -> anonymous_enable=NO
2. Restart or remove vsftpd:
   sudo systemctl restart vsftpd
   or to remove: sudo apt-get remove --purge vsftpd -y
3. Replace FTP with SFTP (SSH) for file transfer; restrict SFTP users using chroot.

Verification:
- Attempt anonymous ftp login (should be refused).
- ls -l /etc/vsftpd.conf

2 - SSH outdated (OpenSSH 4.7p1)

Target: 192.168.137.129:22
Severity: Medium
Description:
Old OpenSSH version; weak host keys observed (DSA/RSA key types).



```
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)
```

Recommendation:

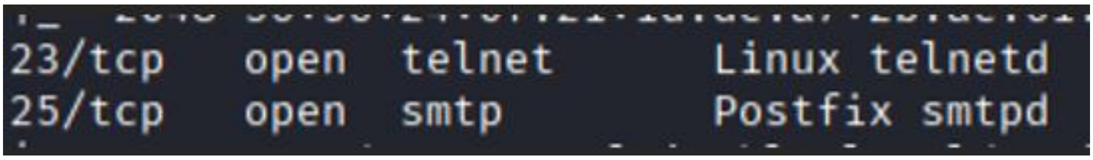
1. Upgrade OpenSSH: sudo apt-get install --only-upgrade openssh-server
2. Remove DSA host keys and regenerate strong keys: sudo rm /etc/ssh/ssh_host_dsa_key*; sudo ssh-keygen -A
3. Harden /etc/ssh/sshd_config: PermitRootLogin no; PasswordAuthentication no; set strong ciphers/KEX.
4. Restart SSH: sudo systemctl restart ssh

Verification: ssh -V; sudo sshd -T | grep -E 'permitrootlogin|passwordauthentication'

3 - Telnet and rsh services (cleartext credentials)

Target: 192.168.137.129:23,512-514

Severity: High
Description:
Telnet, rexecd and rshd allow cleartext credential transmission; trivial to intercept and reuse in lab.



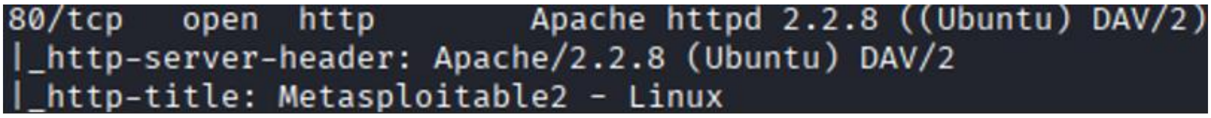
```
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
```

Recommendation:

1. Remove telnet/rsh packages: sudo apt-get remove --purge telnetd rsh-server -y
2. Remove xinetd configs that invoke these services: sudo rm -f /etc/xinetd.d/telnet /etc/xinetd.d/rsh
3. Restart xinetd: sudo service xinetd restart

4 - Apache HTTPD 2.2.8 & Directory browsing

Target: 192.168.137.129:80
Severity: High (web exposure)
Description:
Apache/2.2.8 running; directory browsing detected by ZAP. Missing security headers (CSP, X-Frame-Options). Application error disclosure present.



```
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
```

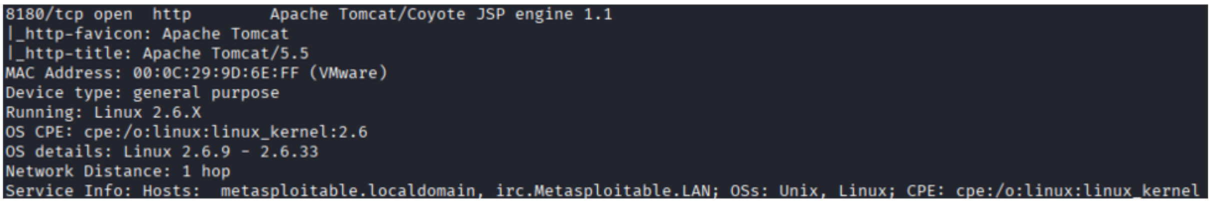
Recommendation:

1. Upgrade Apache: sudo apt-get install --only-upgrade apache2
2. Disable directory listing: Options -Indexes; disable MultiViews: Options -MultiViews
3. Disable HTTP TRACE: TraceEnable Off
4. Add headers (enable mod_headers) and add lines:
   Header always append X-Frame-Options SAMEORIGIN
   Header set X-Content-Type-Options nosniff
   Header set Content-Security-Policy "default-src 'self';"
5. Remove phpinfo and dev pages: sudo rm -f /var/www/html/phpinfo.php
Verification: curl -I http://<target> | egrep 'X-Frame-Options|Content-Security-Policy|X-Content-Type-Options'

5 - Apache Tomcat 5.5 (AJP 8009, HTTP 8180)

Target: 192.168.137.129:8009,8180
Severity: High (known Tomcat vulnerabilities)
Description:

Tomcat 5.5 is ancient and may be vulnerable to multiple CVEs; further testing recommended (manager apps, default creds).



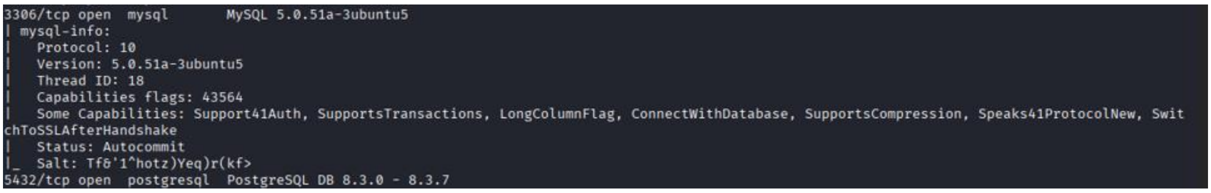
```
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:9D:6E:FF (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Recommendation:

1. Comment out/remove AJP connector in conf/server.xml or bind to localhost.
2. Remove or restrict manager webapp; require strong unique credentials.
3. Upgrade Tomcat to supported version.

6 - MySQL 5.0 and PostgreSQL 8.3 exposed

Target: 192.168.137.129:3306,5432
Severity: High
Description:
Old DB versions; verify weak/default credentials and database access controls.



```
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 18
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, LongColumnFlag, ConnectWithDatabase, SupportsCompression, Speaks41ProtocolNew, Swit
chToSSLAfterHandshake
|   Status: Autocommit
|_  Salt: Tf&'1^hotz)Yeq)r(kf>
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
```

Recommendation:

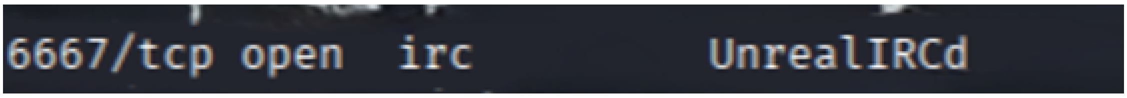
1. Run sudo mysql_secure_installation and enforce root/pass rotation
2. Set bind-address=127.0.0.1 in my.cnf and restart MySQL
3. Remove anonymous users and test DB

Verification: ss -tulpn | grep 3306; mysql -h127.0.0.1 -u root -p
Action recommended (PostgreSQL):

1. Set listen_addresses='localhost' and update pg_hba.conf to restrict access.
2. Restart postgresql; verify only local binds.

7 - UnrealIRCd / IRC (6667)

Target: 192.168.137.129:6667
Severity: Medium
Description:
UnrealIRCd found; known historical backdoors exist for some versions - check for known CVEs.

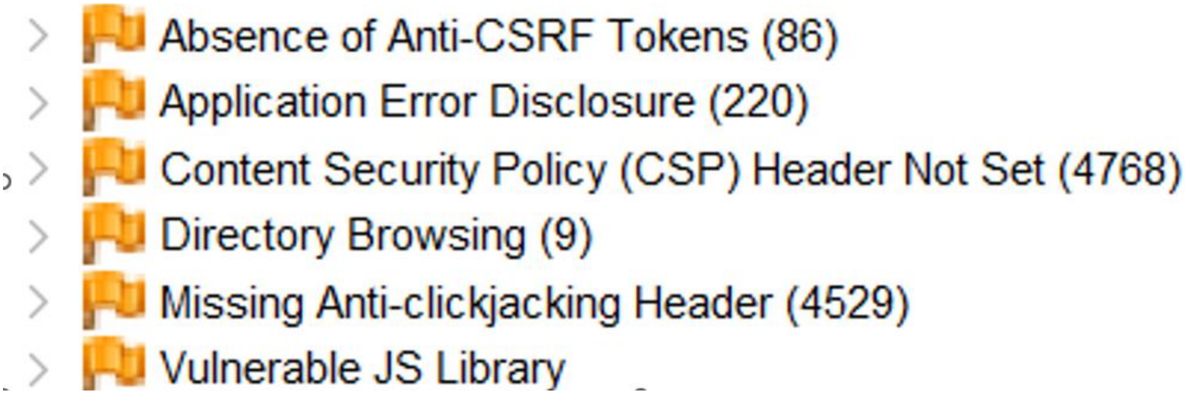


```
6667/tcp open   irc             UnrealIRCd
```

Recommendation:
1. Remove or upgrade the IRC server: sudo apt-get remove --purge unrealircd -y
2. If required, patch to vendor-supplied secure version and restrict access with firewall rules.
Verification: ss -tulpn | grep 6667

8 - Vulnerable JS library + Missing Anti-CSRF tokens

Target: Web application on 192.168.137.129
Severity: High (web application security)
Description:
OWASP ZAP reported absence of Anti-CSRF tokens, vulnerable JS libs, CSP not set, missing clickjacking header and application error disclosure. Manual verification required to confirm exploitability.

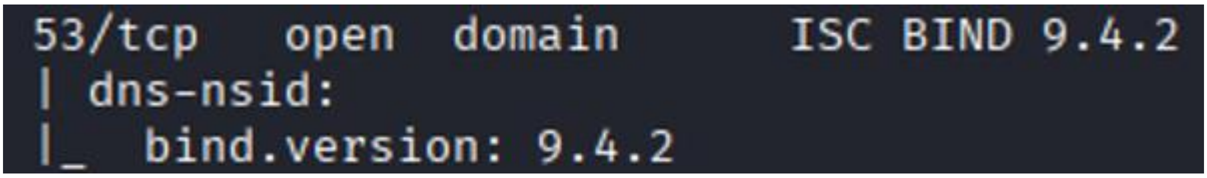


Absence of Anti-CSRF Tokens (86)
Application Error Disclosure (220)
Content Security Policy (CSP) Header Not Set (4768)
Directory Browsing (9)
Missing Anti-clickjacking Header (4529)
Vulnerable JS Library

Recommendation:
1. Update/patch vulnerable JS libs (replace vendor files or use CDN with SRI)
2. Implement server-side Anti-CSRF tokens for all state-changing requests
3. Add CSP headers and other security headers (see Apache section)

9 - Bind 9.4.2 (DNS)

Target: 192.168.137.129:53
Severity: Medium
Description:
Old BIND version exposes DNS services; version disclosure present



```
53/tcp   open   domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
```

Recommendation:
1. Upgrade BIND package
2. Restrict recursion and zone transfers in named.conf.options:

```
  options {
    recursion no;
    allow-recursion { 127.0.0.1; 192.168.137.0/24; };
    allow-transfer { none; };
    version "not available";
  };
```

3. Restart bind: sudo systemctl restart bind9
Verification: dig @<target> any; dig axfr <zone> @<target> (should be refused)

10 - Metasploitable bind shell service (1524)

Target: 192.168.137.129:1524
Severity: Critical
Service: xinetd (configured to spawn bind shell)
Process ID (PID): 5110

Description:
A bind shell was discovered on TCP port 1524, hosted by the `xinetd` process. This backdoor provides remote root-level access without authentication.

Commands executed:

```
sudo ss -tulpn | grep 1524 | tee ~/scans/target_ss_1524.txt
sudo lsof -i -P -n | grep LISTEN | grep 1524 | tee ~/scans/target_lsof_1524.txt
sudo ps -o pid,uid,gid,cmd -p 5110 | tee ~/scans/target_proc_5110.txt
```

Raw outputs:

```
# ~/scans/target_ss_1524.txt
0 tcp 64
*:1524
users: (("xinetd", 5110,12))

# ~/scans/target_lsof_1524.txt
xinetd 5110 root 12u IPv4 12878
TCP *:1524 (LISTEN)

# ~/scans/target_proc_5110.txt
PID UID GID CMD
5110 0 0 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

Interpretation:
- xinetd process (PID 5110) is listening on TCP port 1524.
- The process runs as root (UID 0), confirming high privilege.

- This is a non-interactive backdoor listener and should not be present on production hosts.

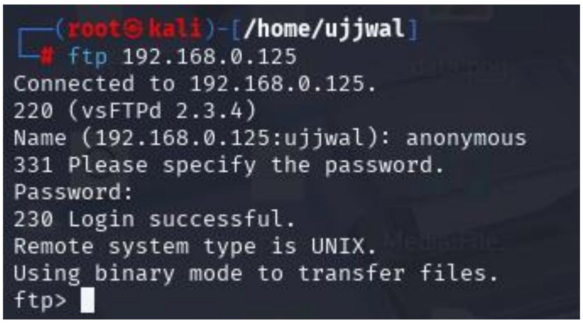
Attacker-side verification:
nc -vz 192.168.137.129 1524 2>&1 | tee ~/scans/nc_connect_1524.txt
Output:
192.168.137.129: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.137.129] 1524 (ingreslock) open

CVSS v3.1 Vector and Score:
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (Base: 9.8)

Remediation Steps (Host-Side):
Immediate Mitigation:
sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
sudo iptables -L INPUT -n --line-numbers | grep 1524

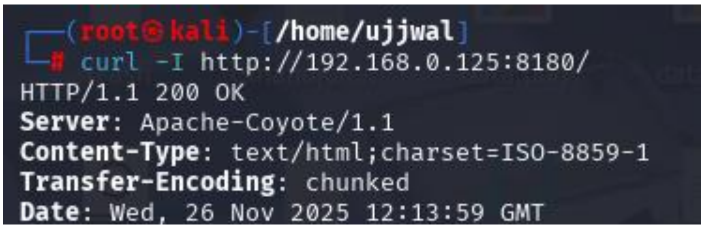
Vulnerability exploitation:

1. vsftpd access



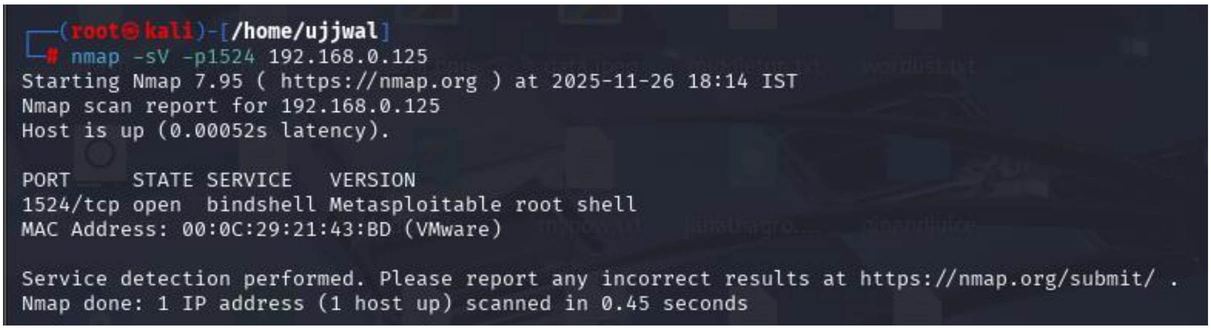
```
┌──(root㉿kali)-[/home/ujjwal]
└─# ftp 192.168.0.125
Connected to 192.168.0.125.
220 (vsFTPd 2.3.4)
Name (192.168.0.125:ujjwal): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

2. Apache header banner



```
┌──(root㉿kali)-[/home/ujjwal]
└─# curl -I http://192.168.0.125:8180/
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 26 Nov 2025 12:13:59 GMT
```

3. Blindshell



```
┌──(root㉿kali)-[/home/ujjwal]
└─# nmap -sV -p1524 192.168.0.125
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 18:14 IST
Nmap scan report for 192.168.0.125
Host is up (0.00052s latency).

PORT     STATE SERVICE   VERSION
1524/tcp open  bindshell Metasploitable root shell
MAC Address: 00:0C:29:21:43:BD (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Risk, CVSS, & Prioritization

1.Estimated/Verified CVSS (NVD CVSS v3.1): CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L — Base Score: 8.6 (High)
Rationale: Anonymous FTP allows disclosure of sensitive files and potential file upload.

2. Estimated/Verified CVSS (NVD CVSS v3.1): CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N — Base Score: 8.3 (High)
Rationale: Outdated OpenSSH version may allow credential or algorithm weaknesses; requires low privilege to exploit.

3. Estimated/Verified CVSS (NVD CVSS v3.1): CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N — Base Score: 8.2 (High)
Rationale: Cleartext protocols (telnet/rsh) transmit credentials in plaintext.

4. Estimated/Verified CVSS (NVD CVSS v3.1): CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N — Base Score: 5.4 (Medium)
Rationale: Directory browsing and info disclosure.

5. Estimated/Verified CVSS (NVD CVSS v3.1): CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Base Score: 9.8 (Critical)
Rationale: Tomcat/AJP exposure with potential for RCE on vulnerable versions.

6. Estimated/Verified CVSS (NVD CVSS v3.1): CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Base Score: 9.0 (Critical)
Rationale: Databases with weak/default credentials enable complete data compromise.

7. Estimated/Verified CVSS (NVD CVSS v3.1): CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L — Base Score: 7.3 (Medium)
Rationale: Information disclosure via IRC service banner.

8. Estimated/Verified CVSS (NVD CVSS v3.1): CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N — Base Score: 5.4 (Medium)
Rationale: Missing anti-CSRF tokens; lower impact unless chained with auth bypass. If vulnerable JS leads to XSS/RCE impact would be higher.

9. Estimated/Verified CVSS (NVD CVSS v3.1): CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N — Base Score: 3.1 (Low)
Rationale: DNS server version disclosure - low direct impact but useful for fingerprinting.

10. Estimated/Verified CVSS (NVD CVSS v3.1): CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H — Base Score: 9.8 (Critical)
Rationale: Bind shell accessible remotely with root privileges (scope change), full compromise.

11. Estimated/Verified CVSS (NVD CVSS v3.1):
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H — Base Score: 9.8 (Critical)
Rationale: Bind shell accessible remotely with root privileges (scope change), full compromise.
CVSS vectors and scores added on 2025-10-29 07:55 IST (estimates based on lab evidence).