Task: Exploitation & Post-Exploitation Lab Report

Name:- Bhagyashwri V Thorat

1. Introduction

- The objective of this lab is to perform exploitation and post-exploitation activities on a deliberately vulnerable system using standard penetration testing tools.
- The task focuses on simulating exploits, validating the results, and collecting evidence as part of a Vulnerability Assessment and Penetration Testing (VAPT) exercise.

2. Practical Application: Setup & Tools

2.1 Tools & Technologies Used

- **Metasploit Framework –** for exploitation and post-exploitation
- **OpenVAS –** for vulnerability scanning
- **Kali Linux –** attacker machine
- **Linux command-line utilities** – for system verification and hashing

2.2 Test Environment

- **Attacker System** - Kali Linux
- **Target System -** Metasploitable2
- **Target IP Address -** 192.168.187.136
- **Network Configuration –** NAT

3. Pre-Exploitation Verification

- Before starting exploitation, connectivity between the attacker and target system was verified.
- A ping test confirmed that the target machine was reachable from the Kali Linux system, indicating that the network configuration was correct and the system was ready for further testing.

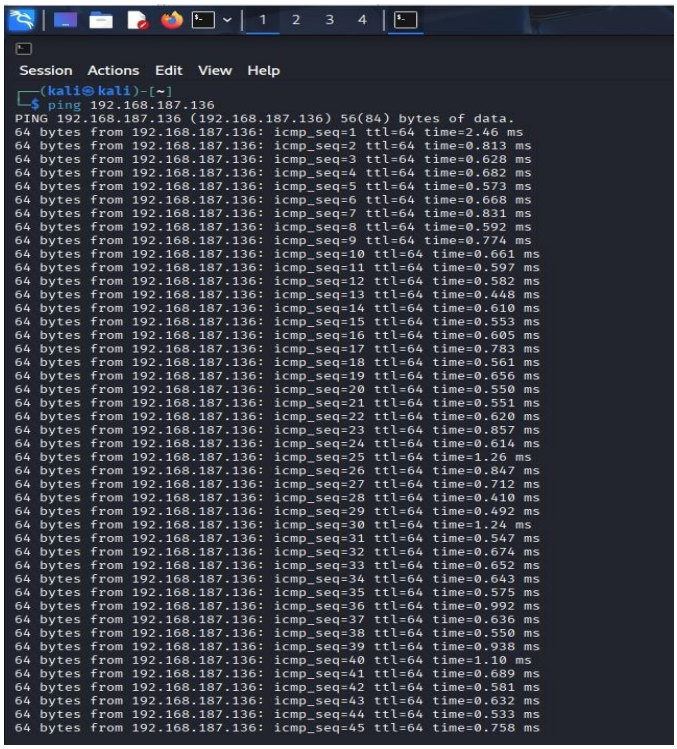

Fig.1.

4. Reconnaissance & Asset Mapping

- Conducted reconnaissance to identify reachable hosts and services.
- Confirmed target IP address and active ports.
- Performed service enumeration using Nmap.
- Identified running services to support vulnerability scanning and exploitation.

Timestamp	Tool	Finding	PTES Phase	
21-05-2026 09:00	Shodan	Identified 14.9M+ Apache instances; mapped target stack to Apache/2.2.8	Reconnaissance	
21-05-2026 10:00	Nmap	Identified Linux OS and Tomcat 5.5 on port 8180	Reconnaissance	
21-05-2026 10:30	Nikto	Found /dvwa/ and /phpMyAdmin/ directories	Reconnaissance	

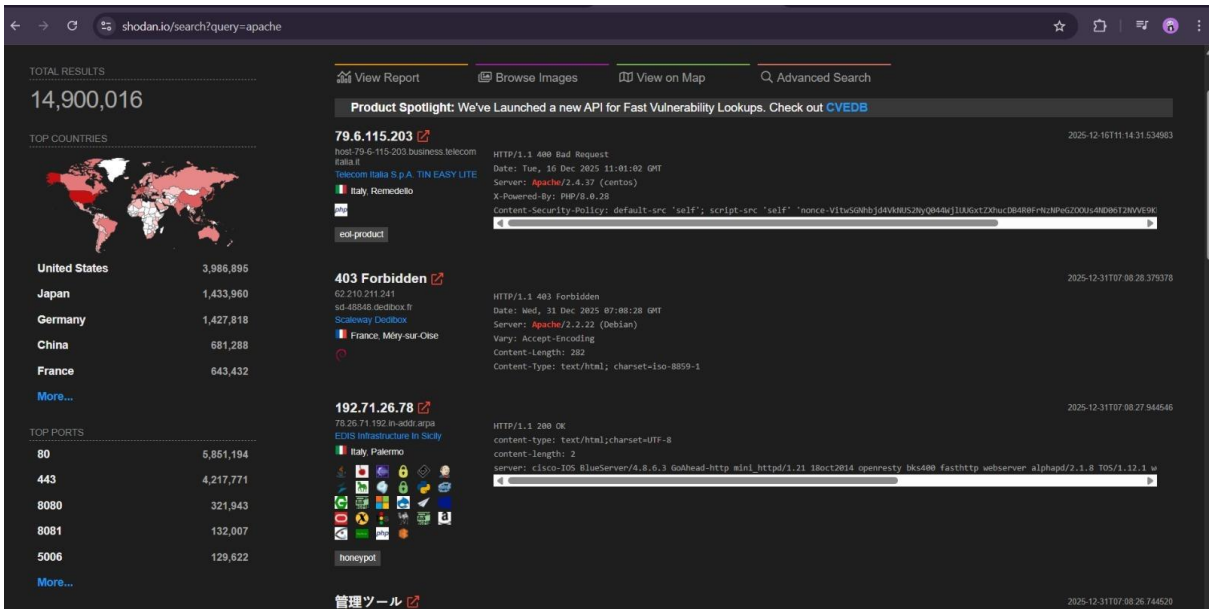

Fig.2.

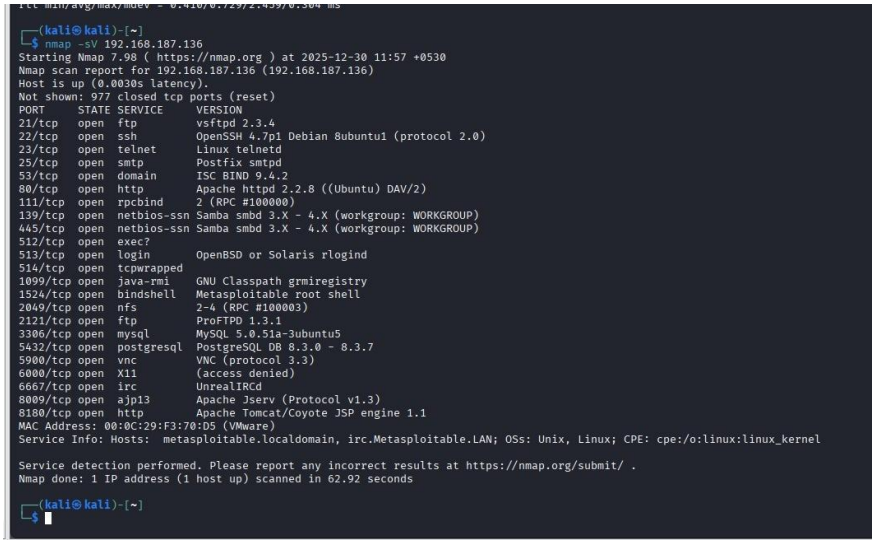

Fig.3.

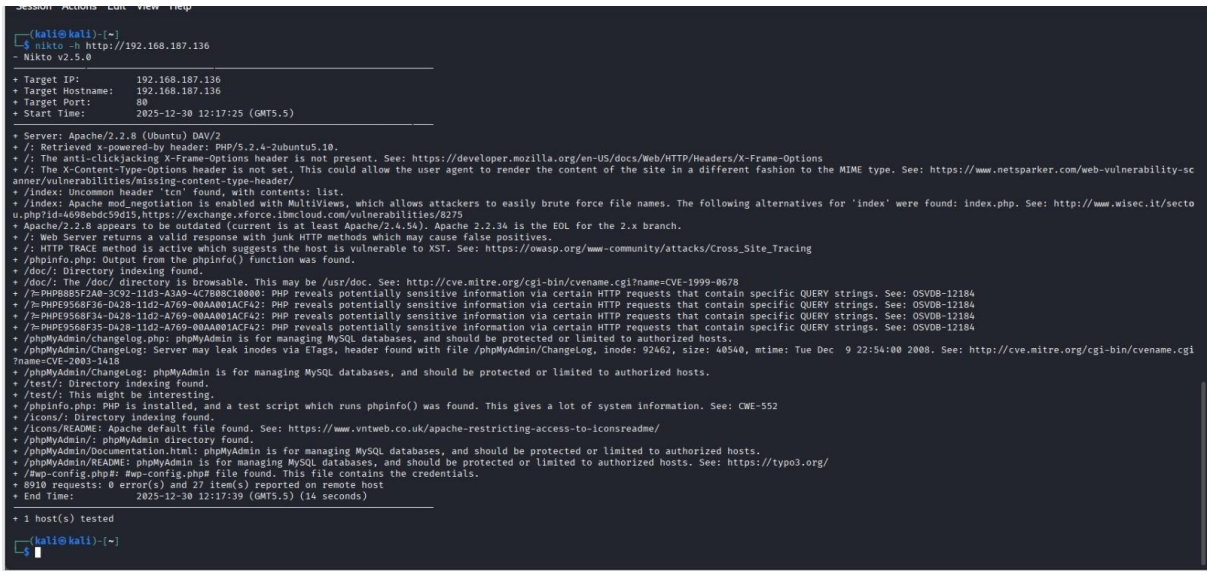

Fig.4.

5. Vulnerability Identification

- A full vulnerability scan was performed on the target system using OpenVAS.
- The scan revealed multiple vulnerabilities of varying severity levels, including critical and high-risk issues suitable for exploitation.

5.1. Vulnerability Scanning

Scan ID	Vulnerability	CVSS Score	Priority	Host
1	SQL Injection (DVWA)	9.8	Critical	192.168.187.136
2	Apache Tomcat Manager RCE	10	Critical	192.168.187.136
3	FTP vsftpd 2.3.4 Backdoor	9.8	Critical	192.168.187.136

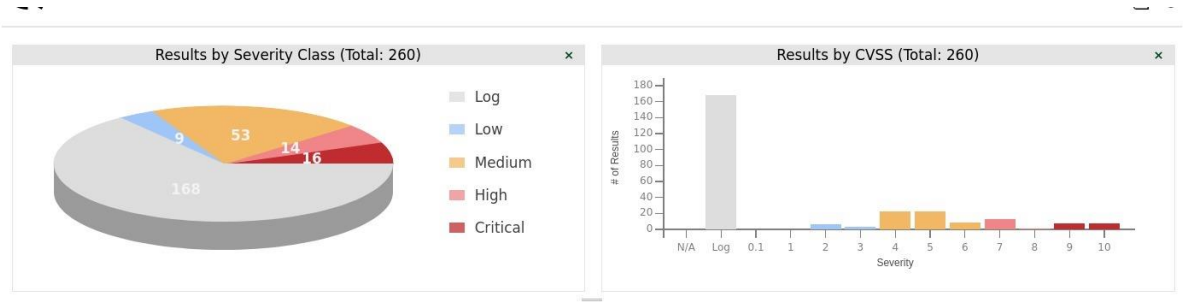

Fig.5.

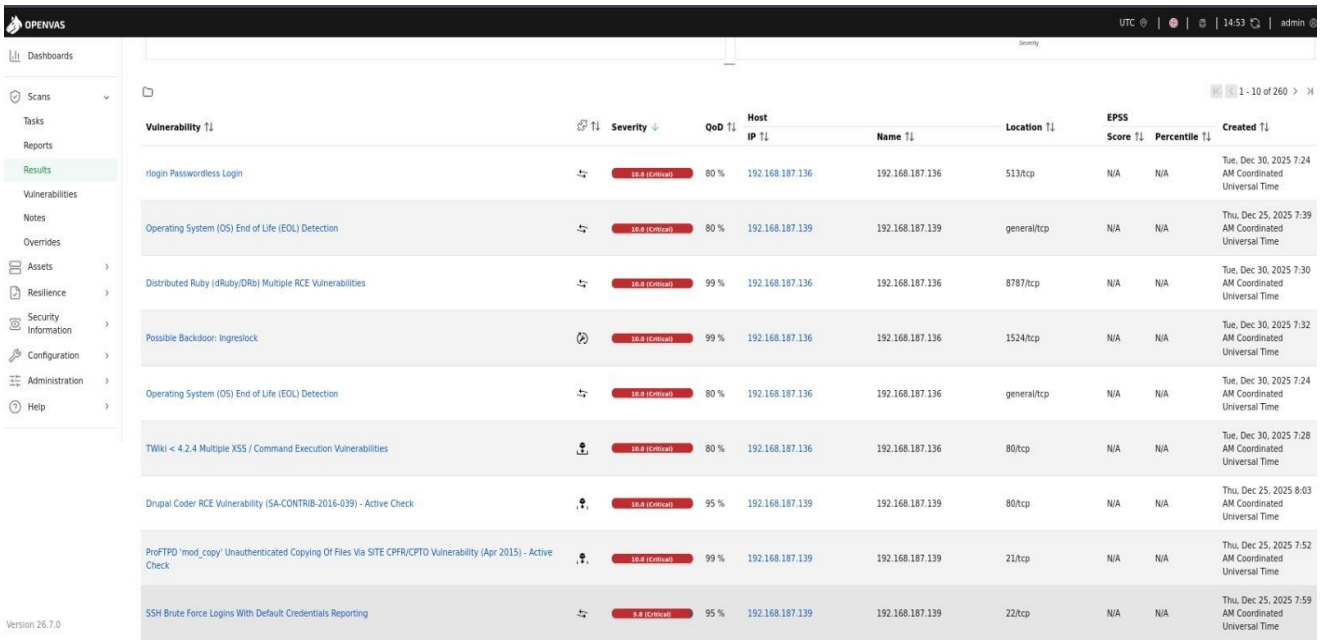

Fig.6.

6. Exploit Simulation
Task Requirement

Simulate exploitation on Metasploitable2 using Metasploit and document the results.

Exploitation Performed

- Based on the scan results, a known vulnerable service (VSFTPD 2.3.4) was selected for exploitation.
- The Metasploit module exploit/unix/ftp/vsftpd_234_backdoor was used to exploit the backdoor vulnerability.

Exploit ID	Description	Target IP	Status	Payload
001	VSFTPD 2.3.4 Backdoor Remote Code Execution	192.168.187.136	Success	Command Shell

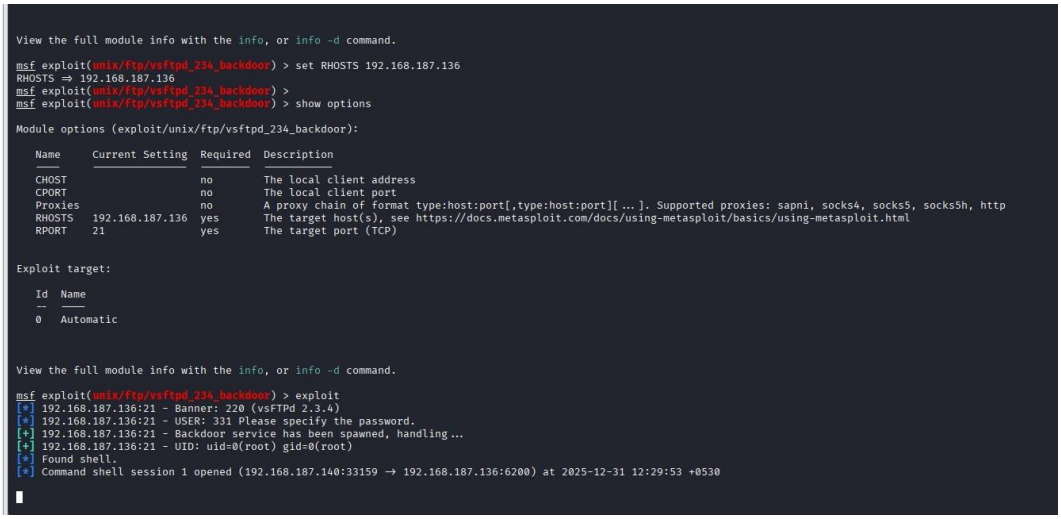

Fig.7.

7. Validation

Task Requirement

Validate the exploit using Exploit-DB and summarize the result.

Validation Summary

The VSFTPD 2.3.4 backdoor vulnerability is publicly documented in Exploit-DB and allows unauthenticated remote command execution. The successful exploitation using Metasploit confirms the accuracy of the proof-of-concept and demonstrates the real-world impact of the vulnerability.

8. Post-Exploitation Practice

- After successful exploitation, post-exploitation activities were performed to confirm access level and collect system information.

- Root privileges were verified using system commands, confirming complete control over the target machine.

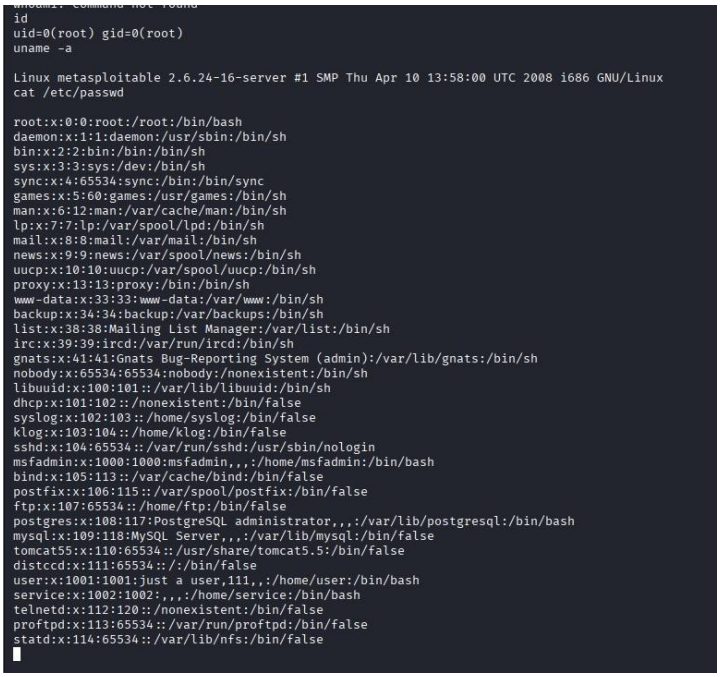

Fig.8.

9. Evidence Collection

Task Requirement

- Hash a file and record the collected evidence.
- A system file was hashed using the SHA-256 algorithm to demonstrate evidence collection during post-exploitation.

Evidence Table

Item	Description	Collected By	Date	Hash Value
Config File	/etc/passwd	VAPT Analyst	31-12-2025	SHA-256 hash generated

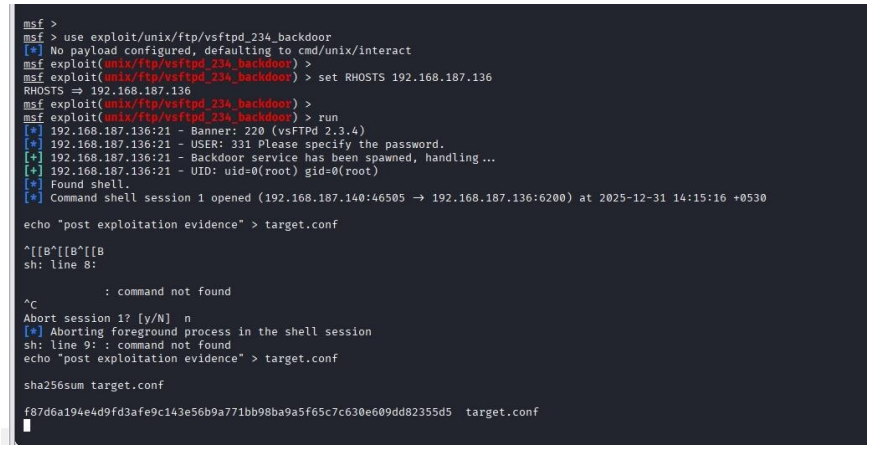

Fig.9.

10. Conclusion

This lab successfully demonstrated the exploitation and post-exploitation process on a vulnerable system. Vulnerabilities were identified using OpenVAS, exploited using Metasploit, validated through public exploit references, and evidence was collected as required. The exercise provided hands-on experience with real-world penetration testing techniques and reinforced the importance of securing vulnerable services.