# Post-Exploitation Lab

Author: Harshal Harekar

Date: 14/10/2025

## Objective

This lab simulates what you do after gaining initial access.

This is continuation of Advanced Exploitation Lab. Hence, not demonstrating access gain steps.

## Steps

Step 1: Privilege Escalation

1. Using the shell you got in Lab 1 (or a new Meterpreter session), search for local privilege escalation exploits

Note: Metasploitable2 often gives you root directly (especially via UnrealIRCd or vsftpd exploits).

2. Look for SUID binaries

find / -perm -4000 -type f 2>/dev/null

Try exploiting nmap –interactive and then enter !sh

Now check privileges using whoami and id.

A screen shot of a computer

AI-generated content may be incorrect.

## Evidence Collection

1. uname -a



2. cat /etc/passwd

A screenshot of a computer screen

AI-generated content may be incorrect.

3. ps aux

A screenshot of a computer program

AI-generated content may be incorrect.

4.netstat -antup

A screenshot of a computer program

AI-generated content may be incorrect.

5. Files downloading

Upgrading from shell to meterpreter

A screenshot of a computer program

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

Hashing Files

A screenshot of a computer program

AI-generated content may be incorrect.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Description | Collected By | Date | Hash Value |
| passwd file | user account information | VAPT Analyst | 14-10-2025 | af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42 |
| shadow file | hashed passwords for user accounts | VAPT Analyst | 14-10-2025 | 7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762 |

## Summary

Post-exploitation evidence was collected from the compromised Metasploitable2 system using shell and Meterpreter sessions. Key artifacts included and, which contain user account details and password hashes. These files were downloaded, hashed using SHA-256, and logged to maintain integrity and chain-of-custody for forensic analysis and reporting purposes.