# Penetration Testing Report

Target Machine: Basic Pentesting 1 (VulnHub)

Author: Dhanavath Nikhil

Date: 02/06/25

## 1. Summary

This penetration testing project simulates a real-world attack scenario on the 'Basic Pentesting: 1' machine provided by VulnHub. The objective was to scan, enumerate, and exploit the target to gain shell access using open-source tools like Nmap, Enum4linux, Hydra, and Metasploit.

## 2. Reconnaissance

- Discovered target IP using:

```
  netdiscover -r 192.168.56.0/24
```

- Performed initial Nmap scan:

```
  nmap -sC -sV -oN scan.txt [target_ip]
```

Identified open ports:

  - 22/tcp (SSH)
  - 80/tcp (HTTP)
  - 139/445 (SMB)

## 3. Enumeration

- Visited target web interface on port 80 and found a login form.
- Used Nikto to identify web server vulnerabilities.
- Ran Enum4linux to enumerate SMB shares and discovered username 'john'.
- Used Hydra to brute-force SSH login: 'john:123456'.

## 4. Exploitation

- Gained access via SSH using credentials discovered.
- Alternatively, used Metasploit module:

```
  auxiliary/scanner/ssh/ssh_login
```

with set RHOSTS, USERNAME, and PASSWORD.

## 5. Post Exploitation

- Upgraded to a fully interactive shell using Python:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

- Verified identity and system info:

```
whoami, id, uname -a
```

- Retrieved flag from:

```
/home/john/Desktop/flag.txt
```

## 6. Lessons Learned

- Poor password hygiene can be exploited via brute force.
- Web and SMB enumeration are critical steps in discovering entry points.
- Tools like Enum4linux and Hydra are highly effective in basic environments.

## 7. Recommendations

- Enforce strong password policies.
- Regularly update and patch services.
- Disable unused services like SMB.
- Monitor logs for failed login attempts.
- Segregate vulnerable systems from production networks.

## 8. Disclaimer

This project was performed in a safe, isolated lab environment for educational purposes only. Never expose vulnerable machines to the internet or unauthorized users.