Penetration Testing Report

1. Executive Summary

This report documents the penetration testing of a custom VPN setup for secure heterogeneous file sharing on a single laptop environment. The objective is to assess the VPN’s security, identify potential vulnerabilities, and ensure the integrity of transmitted data. Tools used include OpenSSL, Wireshark, and Nmap.

2. Scope

- Testing the VPN setup using OpenSSL.

- Network traffic analysis with Wireshark.

- Vulnerability assessment with Nmap.

3. Test Environment

- Device: Single laptop running both VPN server and client.

- Specifications:

- Processor: Intel Core i5

- RAM: 8 GB

- OS: Windows 10

- Software:

- OpenSSL (Version: 3.4.0)

- Wireshark (Version: 4.x)

- Nmap (Version: 7.93)

4. Methodology

4.1 VPN Configuration

- Certificates and keys were generated using OpenSSL commands.

- The VPN server and client were configured to run simultaneously on the same laptop.

4.2 Test Scenarios

1. Secure File Transmission

- Files were transferred over the VPN, ensuring encryption and integrity.

2. Packet Encryption Verification

- Wireshark was used to confirm data packet encryption.

3. Unauthorized Access Detection

- Nmap was employed to check for open ports and potential vulnerabilities.

5. Results

5.1 Observations

1. Secure File Transmission:

- Files were successfully transmitted with no observable data leaks.

- Integrity checks confirmed no tampering.

2. Packet Encryption Verification:

- Encrypted packets were captured and analyzed in Wireshark.

- No plaintext data was detected

3. Unauthorized Access Detection:

- Nmap scans revealed only essential ports open.

- No critical vulnerabilities were identified.

5.2 Screenshots

- VPN setup configuration.

- Wireshark packet capture showing encrypted traffic.

- Nmap scan outputs.

6. Recommendations

- Strengths:

- Strong encryption ensured data confidentiality.

- Minimal exposed ports reduced attack surface.

- Areas for Improvement:

- Implement multi-factor authentication for enhanced security.

- Regular updates to OpenSSL and system patches to address new vulnerabilities.

7. Conclusion

The custom VPN demonstrated robust security for file sharing in a controlled single-laptop environment. While no critical vulnerabilities were identified, periodic assessments and implementation of additional security layers are recommended for continuous improvement.