📝 Project Report: Security Analysis Using Nmap and Wireshark

👤 **Name:** Subramaniam Bhavimane
📅 **Date:** March 27, 2025

📌 Project Overview

This project involves performing a **security analysis of a target system** using two powerful tools:

✅ **Nmap (Network Mapper):** Used to identify open ports, running services, and potential vulnerabilities.
✅ **Wireshark:** Used to analyze network traffic and identify potential security threats.

🎥 1. Nmap Scan Summary

🔎 Target System: 172.16.85.130

✅ **Scan Type:** Version Detection (`-sV` scan)
✅ **Scan Date:** March 24, 2025

🚪 Open Ports and Services Identified:

Port	State	Service	Version/Details
21	Open	FTP	vsftpd 2.3.4
22	Open	SSH	OpenSSH 4.7p1 (Debian 8ubuntu1)
23	Open	Telnet	Linux telnetd
25	Open	SMTP	Postfix smtpd
53	Open	DNS	ISC BIND 9.4.2
80	Open	HTTP	Apache httpd 2.2.8
111	Open	RPCBind	2 (RPC #100000)
139	Open	NetBIOS-SSN	Samba smbd 3.X - 4.X
445	Open	NetBIOS-SSN	Samba smbd 3.X - 4.X

Port	State	Service	Version/Details
512	Open	Exec	netkit-rsh rexecd
1099	Open	Java-RMI	GNU Classpath grmiregistry
1524	Open	Bindshell	Metasploitable root shell
2049	Open	NFS	2-4 (RPC #100003)
3306	Open	MySQL	MySQL 5.0.51a
5432	Open	PostgreSQL	PostgreSQL DB 8.3
5900	Open	VNC	VNC Protocol 3.3
6667	Open	IRC	UnrealIRCd
8009	Open	AJP13	Apache Jserv Protocol 1.3
8180	Open	HTTP	Apache Tomcat/Coyote JSP engine 1.1

⚠️ Vulnerabilities Identified:

- **FTP (vsftpd 2.3.4):** Known backdoor vulnerability.
- **SSH (OpenSSH 4.7p1):** Outdated version, vulnerable to brute-force attacks.
- **Telnet Service:** Plaintext communication, making it vulnerable to credential theft.
- **Bindshell on Port 1524:** Potential backdoor that can allow unauthorized access.
- **IRC (UnrealIRCd):** Remote code execution vulnerability.

📡 2. Wireshark Traffic Analysis

✅ **Total Packets Analyzed:** 5,643
✅ **Protocols Observed:** HTTP, FTP, Telnet, DNS, VNC, SMTP, and NFS

🔥 Key Observations:

- **FTP Credentials in Plaintext:**
  Unencrypted FTP credentials were captured, posing a security risk.

- **Telnet Communication:**
  Telnet traffic was intercepted, revealing sensitive information due to plaintext transmission.

- **HTTP Traffic without Encryption:**
  HTTP traffic was unprotected, potentially exposing user information.

- **NFS Communication Detected:**
  NFS protocol detected, indicating potential file system access.

🛡️ 3. Recommendations

1. **Disable Telnet and FTP:**
   Use SSH and SFTP for secure communication.
2. **Update Vulnerable Services:**
   Upgrade OpenSSH, Apache, and other outdated services to prevent known exploits.
3. **Use Encrypted Protocols:**
   Implement HTTPS to protect sensitive data from interception.
4. **Implement Firewall Rules:**
   Restrict unnecessary open ports to reduce attack surfaces.

🎥 4. Project Evidence

- **Video Demonstration:**
  A video of the entire **Nmap scan** process and results.
- **Wireshark Traffic Analysis:**
  Multiple **screenshots** showcasing critical findings from the Wireshark captures.

📚 5. Conclusion

This project highlights the importance of performing regular security audits to identify and mitigate vulnerabilities. The results show that the target system is exposed to multiple high-risk threats that require immediate attention.

✅ **Skills Demonstrated:**

- Network Scanning using Nmap
- Network Traffic Analysis using Wireshark
- Identifying and Mitigating Security Vulnerabilities