Network Testing Report

---

1. Introduction

This report details the network testing and analysis conducted on a simulated network environment. The objective was to assess network protocols, perform service enumeration, map the network structure, identify access points, and analyze network traffic for potential vulnerabilities.

2. Network Protocols Testing

The network environment consists of multiple devices communicating via standard network protocols. Testing was conducted to examine how these protocols function and identify any security concerns.

2.1 Protocols Tested:

- **TCP/IP:** Verified connection establishment using a three-way handshake.
- **HTTP/HTTPS:** Analyzed web traffic and security configurations.
- **DNS:** Monitored domain resolution processes for anomalies.
- **FTP/SFTP:** Examined secure and non-secure file transfers.
- **SSH:** Assessed remote access security.

2.2 Findings:

- The **HTTP server** had outdated security configurations, leaving it vulnerable to attacks.
- The **DNS server** was misconfigured, allowing possible cache poisoning.
- **SSH access** was open to public access with weak credentials detected.

3. Service Enumeration

Service enumeration was conducted using **Nmap** and **Netcat** to identify active services on network hosts.

3.1 Identified Services:

Service	Port	Status	Vulnerability

SSH	22	Open	Weak passwords detected
FTP	21	Open	Anonymous login enabled
HTTP	80	Open	No HTTPS enforcement
MySQL	3306	Open	Default credentials detected

3.2 Methods Used:

- **Nmap Scan:** `nmap -sV -A [IP Address]`
- **Netcat Probing:** `nc -v [IP] [Port]`
- **Banner Grabbing:** `telnet [IP] [Port]`

3.3 Recommendations:

- Enforce **strong password policies** for SSH and MySQL.
- Disable **anonymous FTP login**.
- Redirect HTTP traffic to **HTTPS**.

4. Network Mapping

A network topology was created to visualize host relationships and connections.

4.1 Network Topology Overview:

- **Router** (192.168.1.1) → Core switch → Endpoints (Servers, Workstations, IoT devices)
- **Public-facing services:** Web Server, FTP Server
- **Internal services:** MySQL Database, Active Directory

4.2 Visualization:

A visual diagram was created using **Zenmap** and **Lucidchart**, showcasing all hosts, access points, and communication paths.

4.3 Findings:

- Poor **segmentation** between public and private networks.
- Unsecured IoT devices communicating with the main LAN.

5. Access Point Identification

All network entry points were identified and analyzed for security vulnerabilities.

5.1 Identified Access Points:

AP Name	MAC Address	Security Protocol	Vulnerability
AP_Office	00:1A:2B:3C:4D:5E	WPA2	Secure
AP_Lobby	00:1A:2B:3C:4D:5F	WPA2-PSK	Default password detected
Guest_Network	00:1A:2B:3C:4D:60	Open	No encryption enabled

5.2 Security Analysis:

- **Guest Wi-Fi was open**, allowing unrestricted access.
- **Default SSID and passwords** were used for some access points.

5.3 Recommendations:

- Implement **WPA3** for stronger encryption.
- Change **default SSIDs and passwords**.
- Segregate **Guest Network** from internal resources.

6. Traffic Analysis

Traffic monitoring was performed using **Wireshark** to identify anomalies and potential threats.

6.1 Anomalies Detected:

- **Excessive HTTP traffic** to an unknown external server.

- **Suspicious SSH login attempts** from unrecognized IP addresses.
- **Unencrypted FTP transmissions** exposing credentials.

6.2 Methods Used:

- **Packet Sniffing:** `wireshark -i eth0`
- **TCP Dump:** `tcpdump -A -n -i eth0`

6.3 Recommendations:

- Implement **intrusion detection systems (IDS)**.
- Restrict **SSH access** to trusted IPs.
- Disable **unencrypted protocols** where possible.

7. Conclusion & Recommendations

The network testing revealed multiple security vulnerabilities, including weak authentication mechanisms, unsecured protocols, and poor network segmentation. By addressing these issues, network security can be significantly improved.

7.1 Key Recommendations:

- Implement **firewall rules** to restrict unnecessary services.
- Enforce **multi-factor authentication** for SSH and MySQL.
- Regularly **update and patch** all network services.
- Segment networks to **isolate critical assets**.

End of Report