Network Security Analysis Report

1. Executive Summary

This report documents a network security assessment using Wireshark, a network vulnerability scanner, and a penetration testing tool. The analysis focuses on identifying vulnerabilities, anomalous traffic patterns, and potential attack vectors. Below are the findings for each tool.

2. Wireshark Capture Analysis

Capture Overview

File: Provided 218 packets (sample of 214 packets shown).
Timeframe: ~14 seconds of network activity.
Key Protocols: MDNS, NBNS, SSDP, TLS, QUIC, ARP, DHCP, LLMNR, DB-LSP-DISC (Dropbox), and SSDP.
Key Observations

Multicast DNS (MDNS) Traffic
Devices (e.g., 10.138.16.154, 10.138.16.113) actively querying services like _companion-link._tcp.local, _googlecast._tcp.local, and _spotify-connect._tcp.local.
Security Note: MDNS can expose device/service information to local attackers (reconnaissance risk).
NetBIOS Name Service (NBNS)
Hosts like 10.138.16.113 and 10.138.16.206 broadcast NetBIOS names (e.g., MACBOOKAIR-FBC4, MACBOOKAIR-CC5F).
Security Note: NBNS is unencrypted and susceptible to spoofing (e.g., LLMNR/NBNS poisoning).
SSDP (UPnP) Activity
Multiple M-SEARCH * HTTP/1.1 requests (e.g., from 10.138.16.213, 10.138.16.251) probing for UPnP devices.
Security Note: UPnP can expose internal devices to external attacks if misconfigured.
TLS/QUIC Encrypted Traffic
Outbound TLS/QUIC sessions to external IPs (e.g., 34.237.73.95, 17.253.150.10).
Example: Packet 73 (10.138.16.228 ↔ 17.253.150.10) uses QUIC for encrypted communication.
Security Note: Legitimate encrypted traffic, but verify endpoints for unauthorized data exfiltration.
WPAD (Web Proxy Auto-Discovery) Queries
Host 10.138.16.69 repeatedly queries for wpad.local via LLMNR/NBNS (Packets 139, 140, 148–150).
Security Concern: WPAD attacks can redirect traffic to malicious proxies.
Dropbox LAN Sync
Host 10.138.16.249 broadcasts Dropbox sync data (Packets 51–52).

Security Note: Sensitive data leakage risk if shared folders are improperly configured.
ARP Requests
Legitimate ARP resolution (e.g., 10.138.16.1 ↔ 10.138.16.228).
Security Concerns

WPAD Queries: Potential indicator of a rogue device or malicious activity.
SSDP/UPnP Exposure: Risk of device enumeration and exploitation.
NBNS/LLMNR Usage: Vulnerable to spoofing attacks (e.g., Responder tool).
MDNS Service Probes: Reconnaissance for lateral movement.
Recommendations

Disable NBNS/LLMNR and enforce DNS Secure.
Block unnecessary UPnP traffic at the firewall.
Monitor WPAD queries and investigate 10.138.16.69.
Segment IoT devices (printers, Google Cast) from critical assets.
3. Network Vulnerability Scanner Report

(Replace this section with your tool's output, e.g., Nessus/OpenVAS)
Example Structure:

Copy
1. Scan Summary
  - Target: 10.138.16.0/24
  - Critical Vulnerabilities: 5
  - High Vulnerabilities: 12

2. Key Findings
  - CVE-2023-1234: UPnP Enabled on HP Printers (10.138.16.5, 10.138.16.76).
  - CVE-2022-4567: Outdated TLS 1.0 on 10.138.16.228.
  - Weak SMB Signing on 10.138.16.52 (DAEDMAC52).

3. Recommendations
  - Patch UPnP services.
  - Enforce TLS 1.2+.
4. Network Penetration Testing Tool Output

(Replace this section with your tool's output, e.g., Metasploit, Nmap)
Example Structure:

Copy
1. Exploit Attempt: WPAD Spoofing (Responder)
  - Target: 10.138.16.69
  - Result: Captured NTLMv2 hash for user "jdoe".

2. SMB Enumeration
   - Host: 10.138.16.44 (DAEDMAC44)
   - Result: Anonymous login allowed (CVE-2023-9999).

3. UPnP Exploit
   - Host: 10.138.16.5 (HP Printer)
   - Result: Remote code execution via buffer overflow.
5. Conclusion

The network exhibits risks from legacy protocols (NBNS/LLMNR), UPnP exposure, and unpatched services. Immediate actions should include disabling insecure protocols, segmenting devices, and patching vulnerabilities identified by the scanner.

Next Steps:

Validate findings with the vulnerability scanner and penetration testing tools.
Implement firewall rules to restrict multicast/broadcast traffic.
Conduct user training on phishing (WPAD attacks often require user interaction).