Utilize Network Security Tools

2. Key Observations

2.1 Multicast DNS (mDNS) Activity

- **Description:**
  - Frequent mDNS queries (e.g., _ipp._tcp.local, _airplay._tcp.local, _raop._tcp.local) from multiple devices (e.g., 10.138.16.77, 10.138.16.65, 10.138.16.166).
  - Devices advertising services:
    - **Printers:** HP Color LaserJet MFP M182nw, HP OfficeJet Pro 8020 series.
    - **Apple devices:** MacBook Air, _companion-link, _airplay, and _raop services.
- **Analysis:**
  - mDNS is used for zero-configuration service discovery in local networks.
  - **Risk:** Exposes device/service details to all local hosts, potentially aiding attackers in mapping the network.
  - **Notable Queries:** _sleep-proxy._udp.local (Apple Sleep Proxy) and _rfb._tcp.local (Remote Framebuffer/VNC).

2.2 TCP/UDP Communications

- **Port 7000 Traffic** (Packets 60–84, 199–211):
  - Repeated connections from 10.138.16.136 to 10.138.20.26/27:7000.
  - **Risk:** Port 7000 is non-standard and could indicate unauthorized file sharing or custom protocols (investigate service purpose).
- **QUIC/HTTP3 Traffic** (Packets 159–178):
  - Encrypted communication between 10.138.16.136 and Google servers (142.250.176.195).
  - **Risk:** QUIC bypasses traditional TLS inspection tools.

2.3 Service Discovery & Broadcasts

- **Dropbox LAN Sync** (Packets 104–105):
  - Broadcast traffic from 10.138.16.249 on UDP port 17500.
  - **Risk:** Unauthorized file synchronization could lead to data leakage.
- **DHCP Requests** (Packets 153, 195):
  - Requests from 0.0.0.0 (unconfigured clients).
  - **Risk:** Potential for rogue DHCP servers if unmonitored.

2.4 ARP Activity

- **Packet 121:** ARP request from 10.138.16.1 (Cisco Meraki) to resolve 10.138.16.136.
  - Legitimate but could indicate spoofing if duplicated excessively.

3. Security Findings

Risk Level	Issue	Details
Medium	Excessive mDNS Broadcasts	Service discovery leaks device details (printers, Apple devices).
Low	Non-Standard Port Usage (7000)	Unclear purpose; could indicate unauthorized services.
Medium	QUIC Encryption Bypass	Limits visibility into encrypted traffic.
Low	Dropbox LAN Sync	Potential data exfiltration if unapproved.

4. Recommendations

1. **Restrict mDNS:** Segment the network to limit mDNS traffic to trusted VLANs.
2. **Audit Port 7000:** Investigate the service running on 10.138.20.26/27:7000 for legitimacy.
3. **Monitor QUIC Traffic:** Deploy decryption proxies for compliance inspections.
4. **Block Unapproved Services:** Disable Dropbox LAN Sync if not required.
5. **Implement DHCP Snooping:** Prevent rogue DHCP servers.

5. Attached Reports

1. **Nmap Penetration Test Output** (To be added):
   - Scan results for open ports/services on critical IPs (e.g., 10.138.20.26, 10.138.16.136).
2. **Vulnerability Scanner Report** (To be added):
   - Findings from tools like Nessus/OpenVAS for devices in the 10.138.16.0/24 subnet.

Prepared by: [Your Name]
Contact: [Your Email]

Next Steps

1. Replace placeholder sections (e.g., date, name) with actual details.
2. Attach Nmap and vulnerability scanner reports once generated.
3. Customize recommendations based on organizational policies.