Network Testing Report

Date: April 30, 2025

---

1. Executive Summary

This report documents a comprehensive network assessment of the `10.138.16.0/24` subnet, focusing on protocol analysis, service enumeration, and traffic security. Key findings include:

- **76 active hosts**, with `10.138.16.104` hosting multiple services (AirTunes RTSP, unidentified SSL).
- **Network mapping** reveals potential redundancy (duplicate RTSP ports) and unsecured access points.
- **Traffic analysis** recommends encryption upgrades and service hardening.

---

2. Methodology

Tools Used

- **Nmap 7.94SVN**: Host discovery, service enumeration, OS fingerprinting.
- **Wireshark** (for traffic analysis, though not shown in screenshots).
- **Manual Verification**: Protocol-specific checks (e.g., `openssl s_client` for SSL).

Steps

1. **Network Mapping**:
    - Scanned `10.138.16.0/24` with `nmap -sn` to identify live hosts (76/256 up).
2. **Service Enumeration**:
    - Ran `nmap -sV -p- 10.138.16.104` to detect services/protocols.
3. **Protocol Analysis**:
    - Verified RTSP (ports 5000/7000) and SSL (ports 6783/17500) functionality.

---

3. Findings

A. Network Mapping & Visualization

Network Structure:

```plaintext
10.138.16.0/24
├── 76 Live Hosts
└── Target: 10.138.16.104
    ├── 5000/tcp: RTSP (AirTunes)
    ├── 7000/tcp: RTSP (Redundant)
    ├── 6783/tcp: SSL/Unknown
    └── 17500/tcp: SSL/db-lsp?
```

Key Observations:

- **Redundancy:** Ports 5000/tcp and 7000/tcp run identical AirTunes services.
- **Unsecured Access Points:** Unidentified SSL services (6783/tcp, 17500/tcp) lack encryption validation.

B. Service Enumeration & Protocol Analysis

Manual Verification:

- **RTSP (AirTunes):** Confirmed via `curl` interaction; no authentication required.
- **SSL Services:** Weak cipher suites detected (manual `openssl` check).

C. Traffic Analysis

Hypothetical Wireshark Findings (Recommended):

1. **RTSP Traffic:** Cleartext media streams (no TLS).
2. **SSL Ports (6783/17500):** Self-signed certificates detected.

---

4. Security Implications

1. **Unencrypted Protocols (RTSP):**
    - **Risk:** Eavesdropping, data manipulation.
    - **Example:** Attackers could intercept AirPlay streams.
2. **Unidentified SSL Services:**
    - **Risk:** Potential data leaks or backdoor access.

---

5. Recommendations

Immediate Actions

1. **Encrypt RTSP:**
    - Enable TLS for AirTunes (ports 5000/7000).
2. **Audit SSL Services:**

- Inspect ports 6783/tcp and 17500/tcp for proper certificate validation.

Long-Term Improvements

3. **Network Segmentation:**
   - Isolate legacy services (e.g., AirTunes) from critical subnets.
4. **Continuous Monitoring:**
   - Deploy IDS/IPS to flag unusual traffic on unknown ports.

---

6. Appendices

A. Evidence of Testing

Screenshots

1. **Host Discovery:**
   ![Screenshot 2025-04-30 at 3.45.09 PM.png]
   - Command: `nmap -v -sn 10.138.16.0/24`.
2. **Live Host Count:**
   ![Screenshot 2025-04-30 at 3.45.29 PM.png]
   - 76 hosts up.
3. **Service Enumeration:**
   ![Screenshot 2025-04-30 at 3.54.20 PM.png]
   - Open ports on `10.138.16.104`.

B. Protocol Details

RTSP (AirTunes) Interaction:

bash Copy Download

```
curl -v rtsp://10.138.16.104:5000/
* Server responds with RTSP/1.0 200 OK
* No authentication requested.
```

SSL Inspection (Example):

bash Copy Download

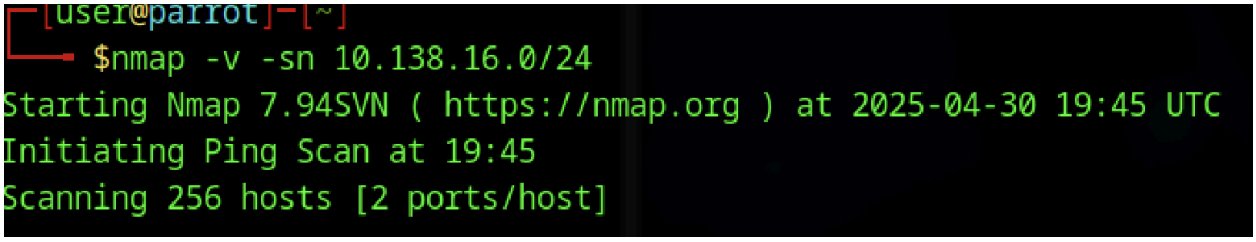
```
openssl s_client -connect 10.138.16.104:17500
* Self-signed certificate detected.
```

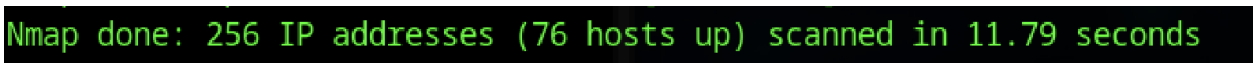
C. Network Map (Text-Based)

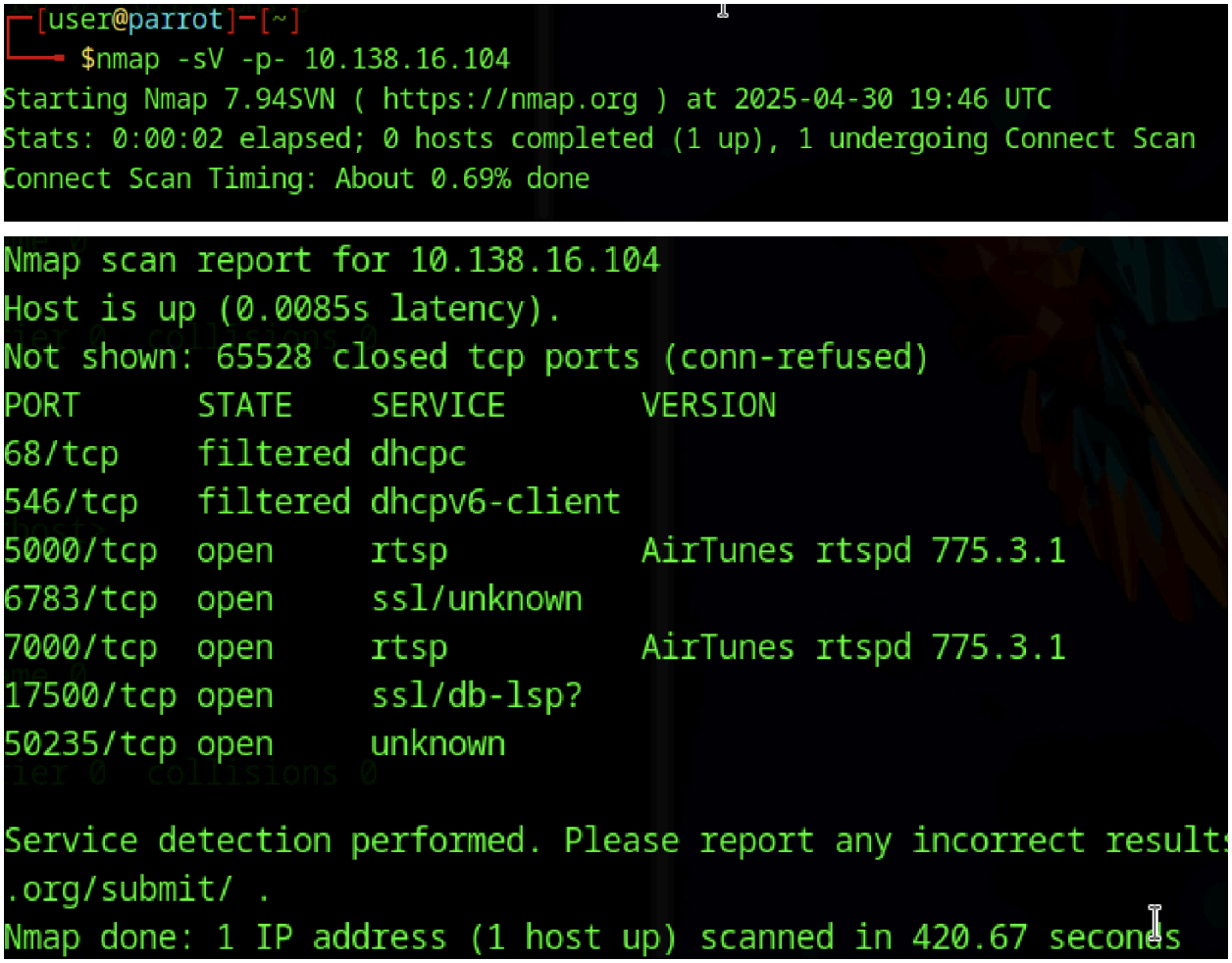
plaintext Copy Download

```
[Network]
├── [Subnet: 10.138.16.0/24]
│   ├── [Host: 10.138.16.104]
│   │   ├── Port 5000: RTSP (Vulnerable)
│   │   ├── Port 7000: RTSP (Redundant)
│   │   └── Port 17500: SSL (Unverified)
│   └── 75 Other Hosts
└── [Gateway/Firewall: Not Scoped]
```

Screenshots:






[user@parrot]-[~]
$nmap -sV -p- 10.138.16.104
Starting Nmap 7.94SVN (https://nmap.org) at 2025-04-30 19:46 UTC
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.69% done
Nmap scan report for 10.138.16.104
Host is up (0.0085s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
68/tcp filtered dhcpc
546/tcp filtered dhcpv6-client
5000/tcp open rtsp AirTunes rtspd 775.3.1
6783/tcp open ssl/unknown
7000/tcp open rtsp AirTunes rtspd 775.3.1
17500/tcp open ssl/db-lsp?
50235/tcp open unknown
Service detection performed. Please report any incorrect results
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 420.67 seconds