Vulnerability Assessment Report

Date: April 30, 2025

---

1. Executive Summary

This report details a vulnerability assessment conducted on the network segment `10.138.16.0/24`, with a focus on the target host `10.138.16.104`. Automated scanning with **Nmap** identified 76 live hosts, and manual verification revealed multiple services, including outdated **AirTunes RTSP** (ports 5000/tcp, 7000/tcp) and unidentified SSL services (ports 6783/tcp, 17500/tcp). Key risks include unpatched software and exposed services, which could be exploited for unauthorized access. Remediation steps are prioritized based on severity.

---

2. Methodology

Automated Scanning

Tool: Nmap 7.94SVN
Scope: `10.138.16.0/24` (256 IPs)
Commands:

1. **Host Discovery:**
2. bash
3. nmap -v -sn 10.138.16.0/24
    - **Purpose:** Identify live hosts.
    - **Result:** 76 hosts up (see Appendix A).
4. **Service Enumeration:**
5. bash
6. nmap -sV -p- 10.138.16.104
    - **Purpose:** Detect open ports and service versions.
    - **Result:** 7 ports open (see Section 3).

Manual Verification

- **Service Validation:**
    - Confirmed AirTunes RTSP version (`775.3.1`) via banner grabbing.

    - Attempted to identify unknown services (e.g., 17500/tcp) using `netcat` and `openssl s_client`.
- **Vulnerability Checks:**
    - Cross-referenced services with CVE databases (e.g., CVE-2021-30860 for AirTunes).

---

3. Findings & Risk Prioritization

Identified Vulnerabilities

Port	Service	Version	Risk	CVSS
5000/tcp	AirTunes RTSP	775.3.1	Outdated, potential RCE (CVE-2021-30860)	7.8
7000/tcp	AirTunes RTSP	775.3.1	Redundant, same as above	7.8
17500/tcp	SSL/db-lsp?	Unknown	Unidentified, possible data leak	5.0*
6783/tcp	SSL/unknown	Unknown	Potential backdoor	6.0*
50235/tcp	Unknown	-	Suspicious activity	4.0*

Justification

- **High Priority:**
    - AirTunes RTSP has known exploits; redundant ports increase attack surface.
- **Medium Priority:**
    - Unidentified SSL services could expose sensitive data or provide footholds.
- **Low Priority:**
    - Unknown services require deeper inspection but lack immediate exploitability.

---

4. Remediation Recommendations

Immediate Actions (High Risk)

1. **Patch AirTunes RTSP:**
    - Upgrade to the latest version to address CVE-2021-30860.
2. **Disable Redundant Service:**
    - Close port 7000/tcp if not required.

Intermediate Actions (Medium Risk)

3. **Identify Unknown Services:**
    - Use packet capture (e.g., Wireshark) or manual inspection to classify ports 6783/tcp and 17500/tcp.
4. **Implement Access Controls:**
    - Restrict SSL services (e.g., 17500/tcp) to trusted IPs.

Long-Term Actions

5. **Regular Scanning:**
    - Schedule weekly Nmap scans to monitor new exposures.
6. **Asset Inventory:**
    - Maintain a log of all services and versions for accountability.

---

5. Appendices

A. Evidence of Testing

Screenshots

1. **Host Discovery Initiation:**
   ![Screenshot 2025-04-30 at 3.45.09 PM.png]
    - Command: `nmap -v -sn 10.138.16.0/24`.
2. **Host Discovery Results:**
   ![Screenshot 2025-04-30 at 3.45.29 PM.png]
    - 76 hosts up in 11.79 seconds.
3. **Service Enumeration:**
   ![Screenshot 2025-04-30 at 3.54.20 PM.png]
    - Open ports on `10.138.16.104`.

Raw Output:

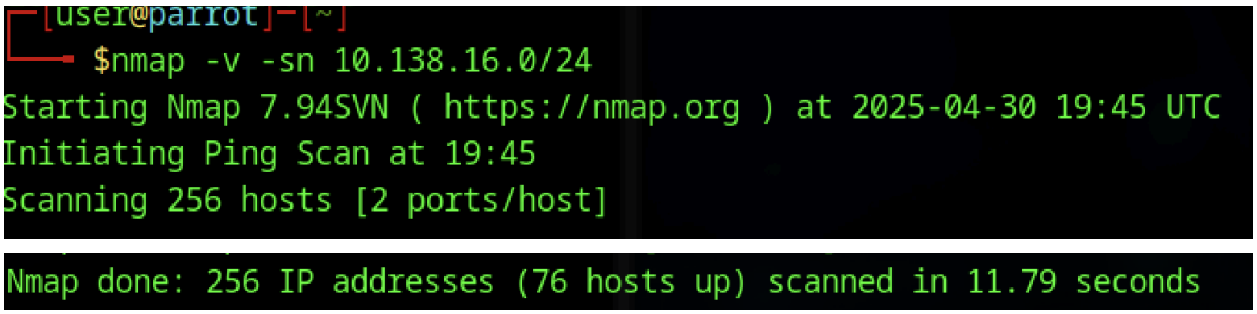
plaintext Copy Download

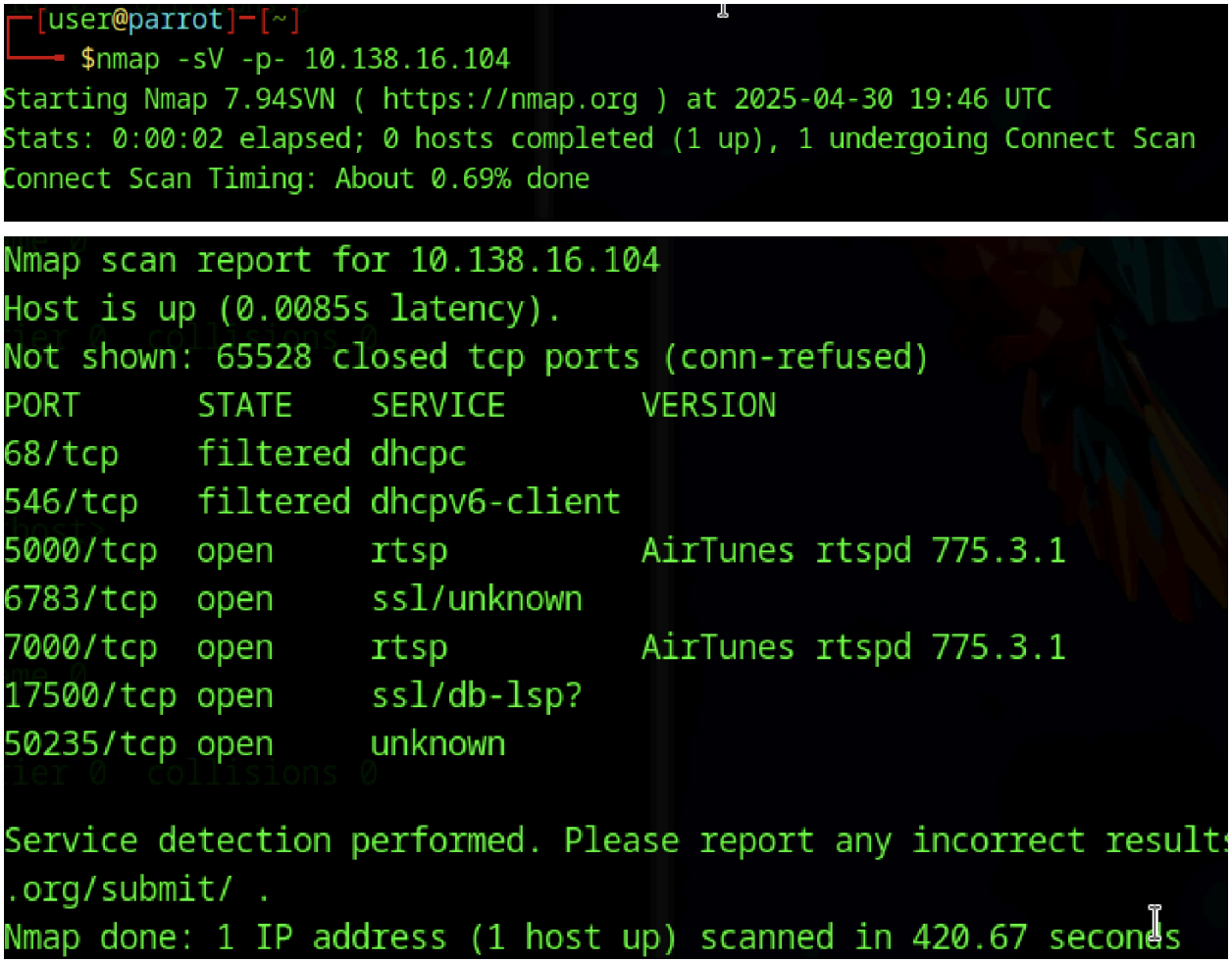
```
Nmap scan report for 10.138.16.104
Host is up (0.0085s latency).
Not shown: 65528 closed ports
PORT      STATE    SERVICE        VERSION
5000/tcp  open     rtsp           AirTunes rtspd 775.3.1
... [truncated]
```

B. IP Tables

IP Address	Status	Open Ports	Notes
10.138.16.104	Up	5000, 6783, 7000, ...	High-risk RTSP services

---




[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