

```
[user@parrot]~$ nmap -v -sn 10.138.16.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-30 19:45 UTC
Initiating Ping Scan at 19:45
Scanning 256 hosts [2 ports/host]
```

```
Nmap done: 256 IP addresses (76 hosts up) scanned in 11.79 seconds
```

```
[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  dhcp
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
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 420.67 seconds
```

Reconnaissance Report

Date: April 30, 2025

Prepared by: [Your Name]

1. Executive Summary

A reconnaissance scan of the network segment 10.138.16.0/24 identified **76 live hosts**, with detailed service enumeration performed on 10.138.16.104. The target host exposes several open ports, including services like **AirTunes RTSP** (ports 5000/tcp, 7000/tcp) and an unknown SSL service (port 17500/tcp). These findings highlight potential entry points for further investigation and hardening.

2. Methodology

Tools Used:

- **Nmap** (Version 7.94SVN) for:
 - Host discovery (-sn).
 - Service/version detection (-sV -p-).

Steps:

1. **Host Discovery:**
 - Scanned 10.138.16.0/24 with nmap -v -sn, identifying 76 live hosts.
2. **Service Enumeration:**
 - Targeted 10.138.16.104 with nmap -sV -p- to map open ports and services.

Ethical Considerations:

- Authorized, non-intrusive scanning.
 - No exploitation or data exfiltration attempted.
-

3. Findings

Enumerated Hosts and Services

- **Live Hosts:** 76/256 in subnet 10.138.16.0/24.
- **Target Host (10.138.16.104):**

Port	State	Service	Version	Notes
------	-------	---------	---------	-------

68/tcp	Filtered	dhcpc	-	Likely blocked by firewall.
546/tcp	Filtered	dhcpc6-client	-	IPv6 DHCP (filtered).
5000/tcp	Open	rtsp	AirTunes rtspd 775.3.1	Apple AirPlay service.
6783/tcp	Open	ssl/unknown	-	Unidentified SSL service.
7000/tcp	Open	rtsp	AirTunes rtspd 775.3.1	Redundant AirPlay instance.
17500/tcp	Open	ssl/db-lsp?	-	Potential database service.
50235/tcp	Open	unknown	-	Unidentified service.

Identified Vulnerabilities or Risks

1. **AirTunes RTSP (Ports 5000/7000):**
 - Outdated version (775.3.1) may have unpatched vulnerabilities (e.g., CVE-2021-30860).
 - Redundant open ports increase attack surface.
2. **Unknown Services (6783/tcp, 17500/tcp, 50235/tcp):**
 - Lack of service identification poses risks (e.g., potential backdoors).
3. **Filtered Ports (68/tcp, 546/tcp):**
 - Indicate firewall rules but could mask misconfigurations.

Areas for Further Investigation

- **Vulnerability Scanning:** Use `nmap --script vuln` to probe for known exploits.
 - **Service Validation:** Manually inspect unknown services (e.g., 17500/tcp).
 - **Network Traffic Analysis:** Check for unusual activity on open ports.
-

4. Recommendations

- 1. **Immediate Actions:**
 - **Patch AirTunes:** Update to the latest version to mitigate known vulnerabilities.
 - **Disable Redundant Services:** Close port 7000/tcp if duplicate of port 5000.
 - 2. **Long-Term Measures:**
 - **Service Inventory:** Document all unknown services for accountability.
 - **Firewall Review:** Ensure filtered ports (68/tcp, 546/tcp) are intentionally blocked.
-

5. Appendices

A. Tool Output Logs

Service Enumeration (`nmap -sV -p- 10.138.16.104`)

Port	State	Service	Version	Notes
68/tcp	Filtered	dhcpc	-	Likely blocked by firewall.
546/tcp	Filtered	dhcpc6-client	-	IPv6 DHCP (filtered).
5000/tcp	Open	rtsp	AirTunes rtspd 775.3.1	Apple AirPlay service.
6783/tcp	Open	ssl/unknown	-	Unidentified SSL service.
7000/tcp	Open	rtsp	AirTunes rtspd 775.3.1	Redundant AirPlay instance.
17500/tcp	Open	ssl/db-lsp?	-	Potential database service.
50235/tcp	Open	unknown	-	Unidentified service.

C. IP Tables

IP Address	Status	Open Ports	Notes
10.138.16.10 4	Up	5000, 6783, 7000, 17500	AirTunes, unknown SSL services
