```
└─$nmap -v -sn 10.138.16.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-07 20:07 UTC
Initiating Ping Scan at 20:07
Scanning 256 hosts [2 ports/host]
```

```
Nmap done: 256 IP addresses (67 hosts up) scanned in 16.52 seconds
```

```
┌──[user@parrot]─[~]
└─$nmap -sV -p- 10.138.16.59
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-07 20:09 UTC
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.88% done
```

```
PORT      STATE    SERVICE      VERSION
68/tcp    filtered dhcpc
135/tcp   open     msrpc        Microsoft Windows RPC
139/tcp   open     netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds?
546/tcp   filtered dhcpv6-client
2343/tcp  open     nati-logos?
2869/tcp  open     http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3580/tcp  open     http         National Instruments LabVIEW service locator ht
tpd 1.0.0
3582/tcp  open     http         Embedthis HTTP lib httpd
5040/tcp  open     unknown
7680/tcp  open     pando-pub?
8080/tcp  open     http         Embedthis HTTP lib httpd
9031/tcp  open     http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open     msrpc        Microsoft Windows RPC
49665/tcp open     msrpc        Microsoft Windows RPC
49666/tcp open     msrpc        Microsoft Windows RPC
49667/tcp open     msrpc        Microsoft Windows RPC
```

```
49668/tcp open     msrpc        Microsoft Windows RPC
49688/tcp open     unknown
49694/tcp open     msrpc        Microsoft Windows RPC
57621/tcp open     unknown
59110/tcp open     unknown
59111/tcp open     unknown
61865/tcp open     unknown
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port61865-TCP:V=7.94SVN%I=7%D=5/7%Time=681BBE1F%P=aarch64-unknown-linux
SF:-gnu%r(NULL,22,"{\"type\":\"Tier1\",\"version\":\"1\.0\"}\r\n")%r(RPCCh
SF:eck,22,"{\"type\":\"Tier1\",\"version\":\"1\.0\"}\r\n")%r(SSLSessionReq
SF:,22,"{\"type\":\"Tier1\",\"version\":\"1\.0\"}\r\n")%r(Kerberos,22,"{\"
SF:type\":\"Tier1\",\"version\":\"1\.0\"}\r\n")%r(SMBProgNeg,22,"{\"type\"
SF::\"Tier1\",\"version\":\"1\.0\"}\r\n")%r(giop,22,"{\"type\":\"Tier1\",\
SF:"version\":\"1\.0\"}\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 120.58 seconds
```

Network Security Operations

---

1. Executive Summary

A network security assessment was conducted on a Windows-based system with multiple open ports, including several unidentified services. The assessment included:

- **Network traffic analysis** (Wireshark captures)
- **Security configuration testing** (firewall, RPC services)
- **Basic compliance checks** (CIS Benchmark comparison)
- **Incident analysis** (examination of port `61865` exposing service version)

Key findings include:

- **Three unknown services** (`49688`, `57621`, `59110-59111`) with no documented purpose.
- **Two MSRPC ports** (`49568`, `49694`) potentially exposing sensitive Windows functions.
- **Service version disclosure** on port `61865` (`"Tier1", "version": "1.0"`), which could aid attackers in exploitation.

Recommendations:

- Disable unnecessary services (`49688`, `57621`, `59110-59111`).
- Harden MSRPC configurations to prevent unauthorized access.
- Investigate the `Tier1` service on `61865` for vulnerabilities.

---

2. Methodology

2.1 Network Traffic Capture & Evidence Collection

- **Tool Used:** Wireshark
- **Focus Ports:** `49688`, `57621`, `59110-59111`, `61865`
- **Duration:** 10-minute capture during active connections

2.2 Security Configuration Testing

- **Windows Firewall Review:** Checked if unnecessary ports were open.
- **RPC Security:** Verified authentication requirements for `49568` and `49694`.

2.3 Compliance Checking

- **Baseline:** CIS Microsoft Windows Benchmark
- **Checks Performed:**
    - ✔ **Service Identification** (FAIL: Unknown services detected)
    - ✔ **Port Minimization** (FAIL: Unnecessary ports open)
    - ✔ **Version Disclosure** (FAIL: `61865` exposes version info)

2.4 Incident Analysis

- **Scenario:** *"An alert triggered unusual traffic on port `61865` exposing service version."*
- **Analysis Steps:**
    1. Confirmed JSON response (`"type": "Tier1", "version": "1.0"`).
    2. Searched for known vulnerabilities in "Tier1 v1.0" (no public exploits found).
    3. Determined risk: **Medium** (version disclosure could aid targeted attacks).

---

3. Findings & Evidence

3.1 Open Ports & Services

Port	Service	Status	Risk Level
49568	MSRPC	Open	Medium
49688	Unknown	Open	High
49694	MSRPC	Open	Medium
57621	Unknown	Open	High
59110	Unknown	Open	High

59111	Unknown	Open	High
61865	Tier1 v1.0	Open	Medium

Evidence:

- **Nmap Scan Results (Screenshot)**

3.2 Traffic Analysis (Wireshark)

- **Port `61865`** responds with JSON data, indicating an API-like service.
- **No encryption observed** on unknown ports (`49688`, `57621`, `59110-59111`).

Sample Capture:

```
json
{"type": "Tier1", "version": "1.0"}
```

3.3 Compliance Failures

- ❌ **Unidentified Services:** `49688`, `57621`, `59110-59111` should be documented or disabled.
- ❌ **Unnecessary Ports Open:** MSRPC ports should be restricted to necessary hosts.
- ❌ **Information Disclosure:** `61865` exposes software version (potential exploit clue).