

Port Discovery & Security Analysis – Host: 192.168.1.7

```
C:\WINDOWS\system32\cmd. X + v

Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet2:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::f715:a167:5a9:dbba%9
    IPv4 Address. . . . . : 192.168.10.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet3:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::9e68:ebc0:f79c:abff%20
    IPv4 Address. . . . . : 10.10.10.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2401:4900:1c07:99f:4097:66a5:f481:e735
    Temporary IPv6 Address. . . . . : 2401:4900:1c07:99f:88a7:8a96:9569:19f4
    Link-local IPv6 Address . . . . . : fe80::2716:24b3:45e0:62f2%22
    IPv4 Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%22
                                192.168.1.1
```

Introduction

The purpose of this task was to perform basic network reconnaissance to identify open ports and active services running on my local system with IP address 192.168.1.7.

This activity is part of understanding how devices in a network expose services and how such exposure can create potential security risks if not properly managed.

Using the Nmap tool on Windows, I conducted a detailed scan of my local host to detect all open TCP ports and determine which services were listening on them.

The scan provided valuable insights into how Windows and VMware services communicate

over the network and helped in identifying possible vulnerabilities associated with ports like SMB (445), RPC (135), and NetBIOS (139).

Open Ports

```
Nmap scan report for 192.168.1.5
Host is up (0.0072s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.1.7
Host is up (0.00013s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
902/tcp    open  ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp    open  vmware-auth      VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5357/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Service Info: OS: Windows; CPE: /o:microsoft:windows
```

135/tcp – MSRPC (Microsoft Remote Procedure Call)

Used by Windows for inter-process communication and remote service management.

139/tcp – NetBIOS-SSN (NetBIOS Session Service)

Used for Windows file and printer sharing on older networks.

445/tcp – Microsoft-DS (Server Message Block - SMB)

Used for Windows file sharing, printer sharing, and domain authentication.

902/tcp – VMware Authentication Daemon (SSL)

Used by VMware for remote console and management communication.

912/tcp – VMware Authentication Daemon

Used by VMware for SOAP-based authentication and remote management.

5357/tcp – HTTPAPI / WSD (Web Services for Devices)

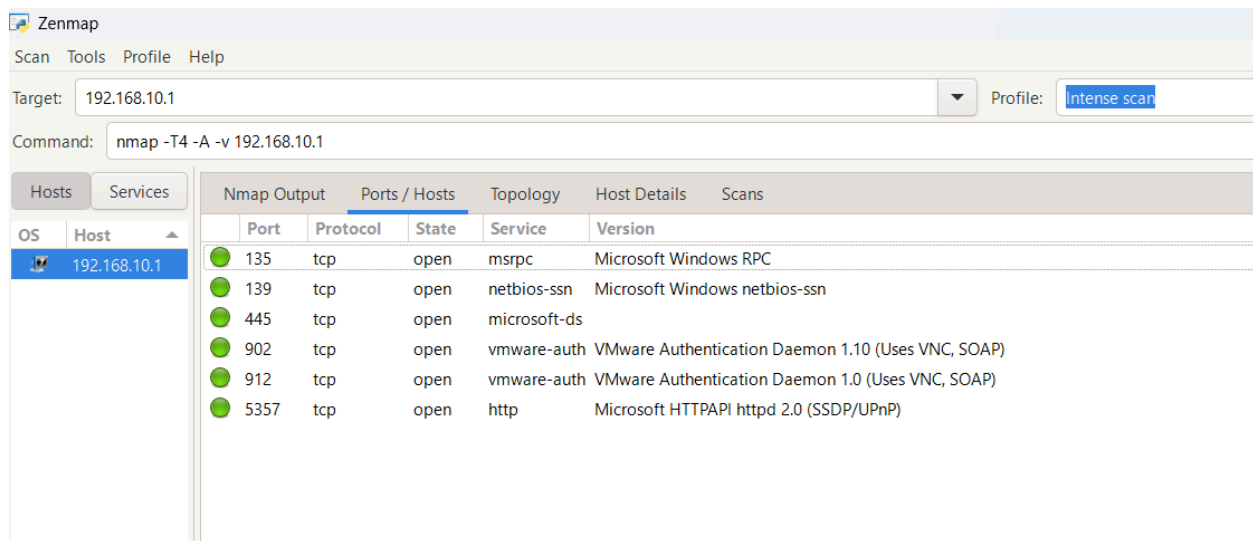
Used by Windows for device discovery and web-based service communication.

NMAP Output

```
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
902/tcp    open  ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp    open  vmware-auth      VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5357/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

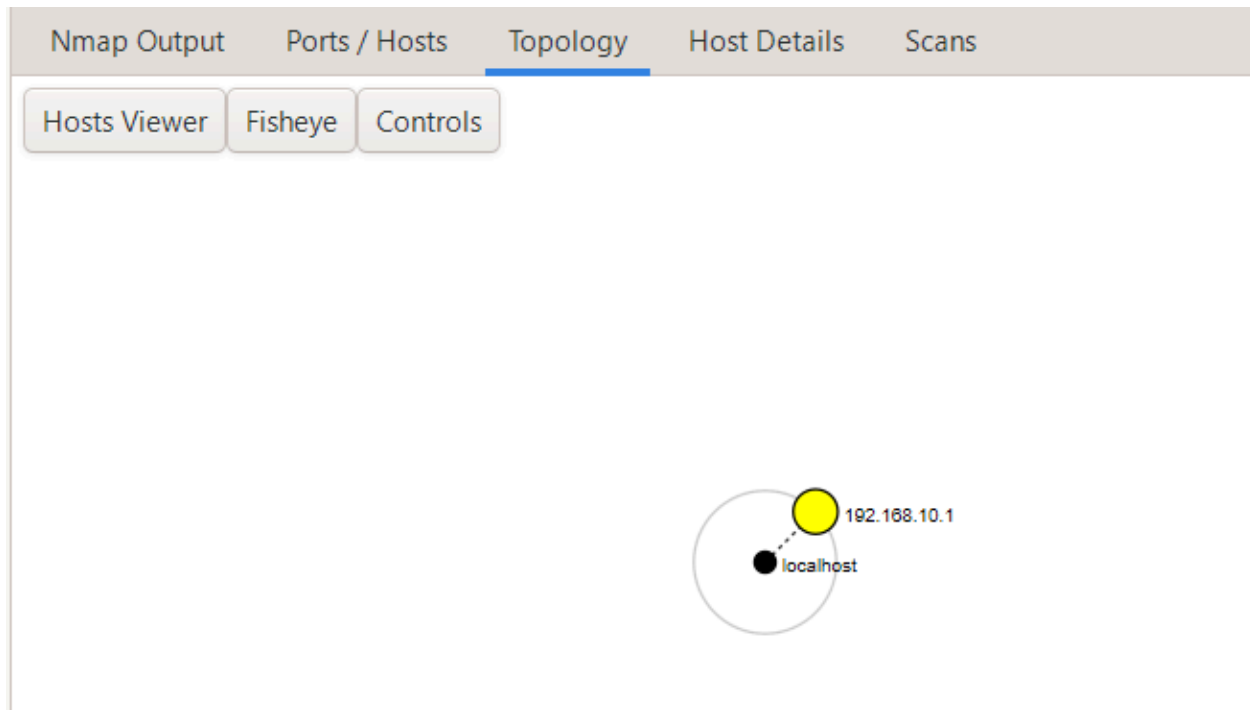
Nmap output shows the results of a port scan on a target system, displaying the state of TCP ports (open, closed, filtered) along with the services associated with open ports.

Port/Host in Nmap



The following open ports were identified during the Nmap scan: 135 (msrpc), 139 (netbios-ssn), 445 (microsoft-ds), 902/912 (vmware-auth), and 5357 (http), indicating active services on the target system 192.168.10.1.

Topology According to Nmap



Host details from Nmap

Nmap OutputPorts / HostsTopologyHost DetailsScans

▼ 192.168.10.1

▼ Host Status

State:up

Open ports:6


Filtered ports:0


Closed ports:994

Scanned ports:1000

Up time:Not available

Last boot:Not available





▼ Addresses

IPv4:192.168.10.1

IPv6:Not available

MAC:Not available

► Comments

Open Port Vulnerabilities and Potential Risks

135 — MSRPC (Microsoft Remote Procedure Call)

- Can reveal what services run on the machine (information leakage).
- May allow attackers to abuse vulnerable RPC services to run code remotely.
- Can be used to move laterally inside a network (reach other systems).
- Might enable privilege escalation if an RPC service has flaws.
- Can be an entry point for worms or automated malware.

139 — NetBIOS-SSN (NetBIOS Session Service)

- Leaks computer names, shared folders, and user info (information disclosure).
- Can allow unauthorized access to file/printer shares if misconfigured.
- Facilitates lateral movement inside an internal network.
- Can be abused to gather targets for further attacks.

445 — Microsoft-DS (SMB over TCP)

- High-risk: known vector for remote-code execution in unpatched systems.
- Common target for ransomware and worm propagation.
- Can expose file shares leading to data theft or tampering.

-
- Enables credential theft and lateral movement across the network.
 - Exposing SMB to untrusted networks greatly increases attack surface.

902 / 912 — VMware management/authentication ports

- If reachable, attackers can attempt to control VMs or management functions (unauthorized access).
- May expose management APIs or console access that contain sensitive data.
- Compromise can lead to full control of virtual machines and hosted workloads.
- Improperly secured VMware services can be used to pivot to other systems.

5357 — HTTPAPI / WSD (Web Services for Devices / HTTP API)

- Can disclose device/service information on the network (information leakage).
- Exposed management or discovery endpoints may be probed for weaknesses.
- May allow access to local web APIs if they lack proper authentication.
- Can be abused to fingerprint devices and plan targeted attacks.

Interview Questions

1. What is an open port?

An open port is a communication doorway on a device that's actively listening for incoming connections. It allows data to enter or leave a system through specific services, like port 80 for websites or 22 for SSH. However, if unnecessary ports stay open, they can become entry points for attackers.

2. How does Nmap perform a TCP SYN scan?

Nmap's TCP SYN scan works by sending a SYN packet — the first step of a TCP handshake.

If it gets a SYN-ACK back, the port is open.

If it gets an RST (reset), the port is closed.

It never completes the handshake, making the scan fast and a bit stealthy, because it doesn't fully establish a connection.

3. What risks are associated with open ports?

Open ports can reveal what services a system is running. Attackers can exploit vulnerable or outdated services, gain unauthorized access, or launch attacks like brute-force or denial-of-service. Basically, every open port is a potential doorway into the system.

4. Explain the difference between TCP and UDP scanning.

TCP scanning uses connection-based communication — it needs to establish or partially complete a handshake, so it's more reliable and accurate.

UDP scanning doesn't need a handshake; it just sends packets and waits for a response (or timeout). It's quieter and harder to detect but can miss results or take longer.

5. How can open ports be secured?

Close all unnecessary ports.

Use a firewall to restrict who can access which ports.

Keep the running services up-to-date.

Use network monitoring tools to detect any unusual traffic.

Securing open ports reduces your system's attack surface.

6. What is a firewall's role regarding ports?

A firewall acts like a security guard for your ports — it decides which connections to allow or block. It can filter traffic by IP, port number, or protocol, preventing unauthorized access to sensitive services.

7. What is a port scan and why do attackers perform it?

A port scan is the process of probing a system to find open or active ports. Attackers use it to discover running services and identify potential weaknesses.

Security professionals also perform port scans — but to fix issues before attackers find them.

8. How does Wireshark complement port scanning?

Wireshark captures and analyzes network packets in real time. While Nmap tells you which ports are open, Wireshark shows how the packets move between devices. Together, they give a complete picture of network activity and possible vulnerabilities.

Thank you for taking the time to review my report on the open port vulnerabilities and potential risks for host 192.168.1.7.

I sincerely apologize for any delay in submission — as it was **Diwali**, we were having a family celebration at home, and I was engaged in our traditional function.

Thank you for your understanding.

Warm regards,

Vaibhav Jadhav
