Lab 03

Using PowerShell to Find Active & Listening Ports

Instructor: Samuel Esan

Introduction:

A port is a physical docking point, which an external device can be connected to the computer. It can also be a programmatic docking point through which information flows from a program to the computer or over the Internet.

A network port which is provided by the Transport Layer protocols of Internet Protocol suite, such as Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) is a number which serves endpoint communication between two computers.

To determine what protocol incoming traffic should be directed to, different port numbers are used. They allow a single host with a single IP address to run network services. Each port number has a distinct service, and each host can have 65535 ports per IP address. **Internet Assigned Numbers Authority (IANA)** is responsible for managing the uses of these ports. There are three categories for ports by IANA −

- 0 to 1023 – well known ports or system ports.

Some well-known ports are −

Port number	Transport protocol	Service name
20,21	TCP	File Transfer Protocol
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol(SMTP)
53	TCP and UDP	Domain Name System(DNS)
110	TCP	Post Office Protocol(POP3)
123	UDP	Network Time Protocol(NTP)

- **1024 to 49151** – registered ports assigned by IANA to a specific service upon application by a requesting entity.
- **49152 to 65 535** – dynamic (private, high) ports range from 49,152 to 65,535. Can be used by private or customer service or temporal purposes.

Ports identify what process on the host the received traffic should be sent to. A computer can have multiple simultaneous connections, all receiving data for different processes (mail, web, database, etc) on that computer.

Assignment:

In this lab, we would be using nmap and powershell to identify open ports on Windows operating system.

Requirements:

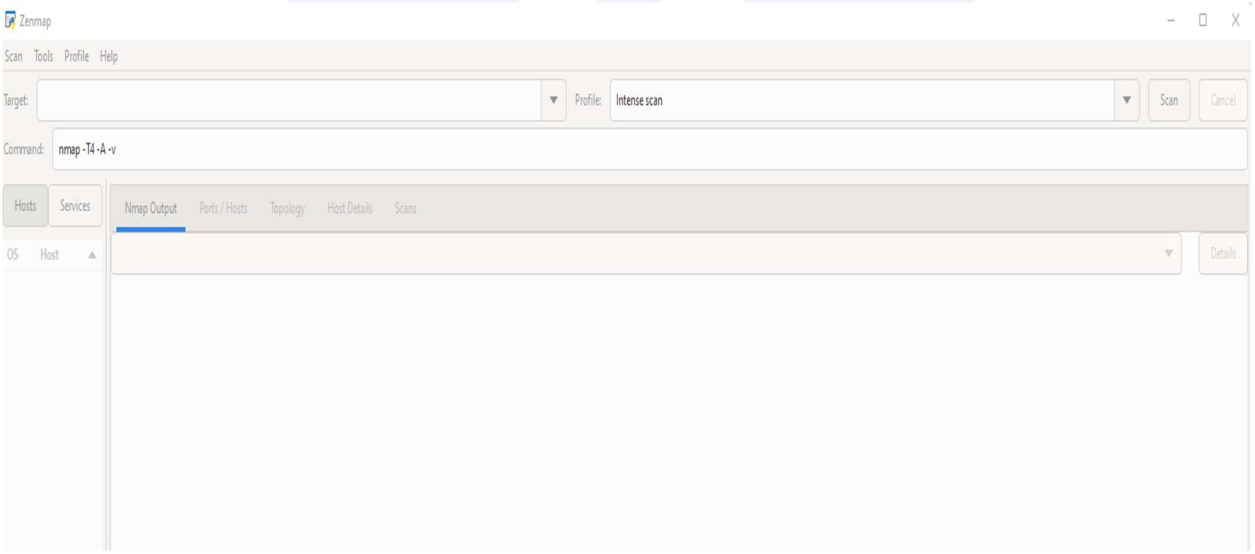
Windows 10 and above.

High Speed Internet

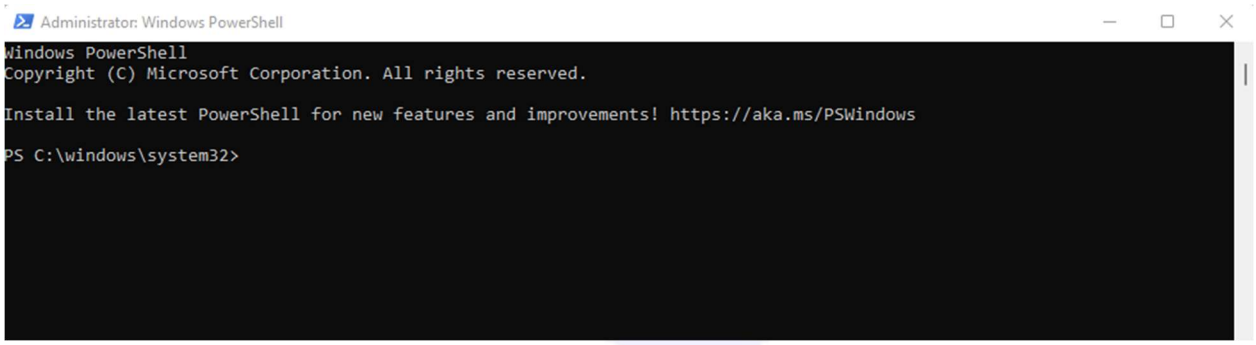
Estimated Time:

Varies

1. Proceed to open your nmap.

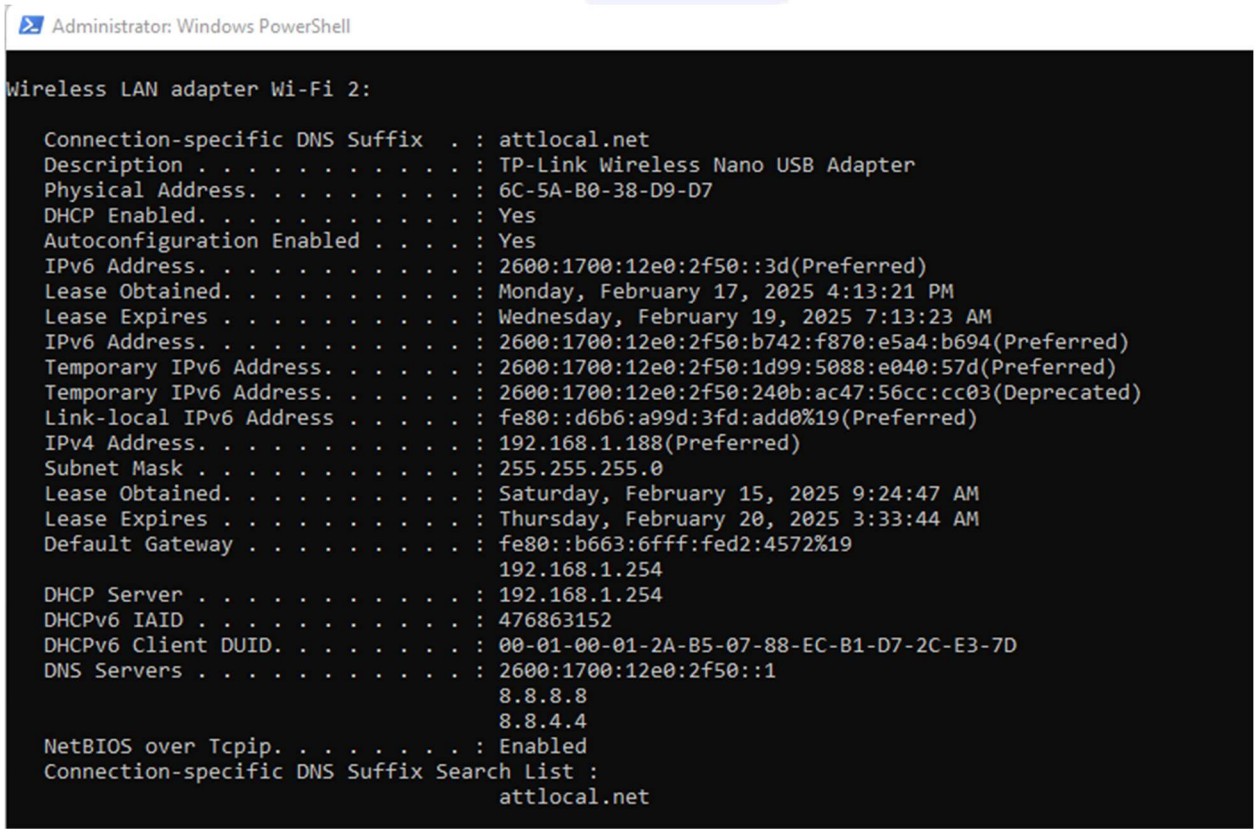


2. Proceed to open your windows PowerShell and run as an admin.

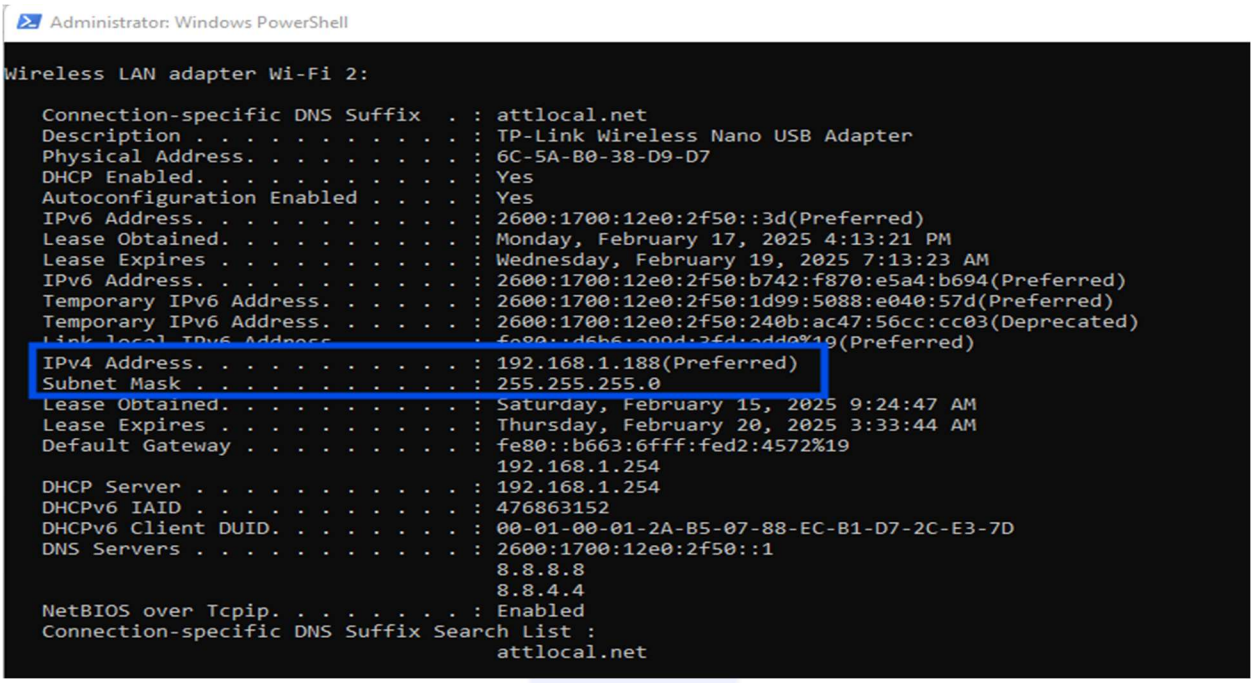


3. Run *ipconfig /all*

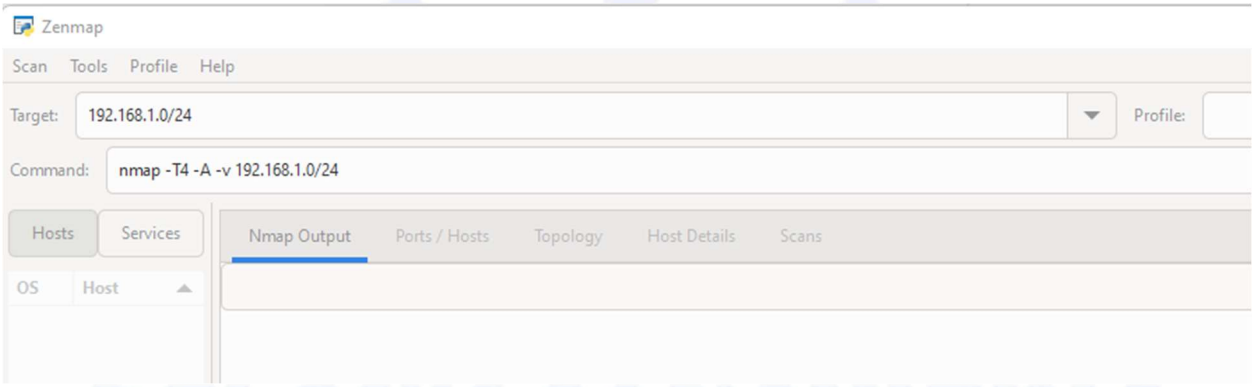
Go to section indicating Wireless LAN adapter wi-fi:



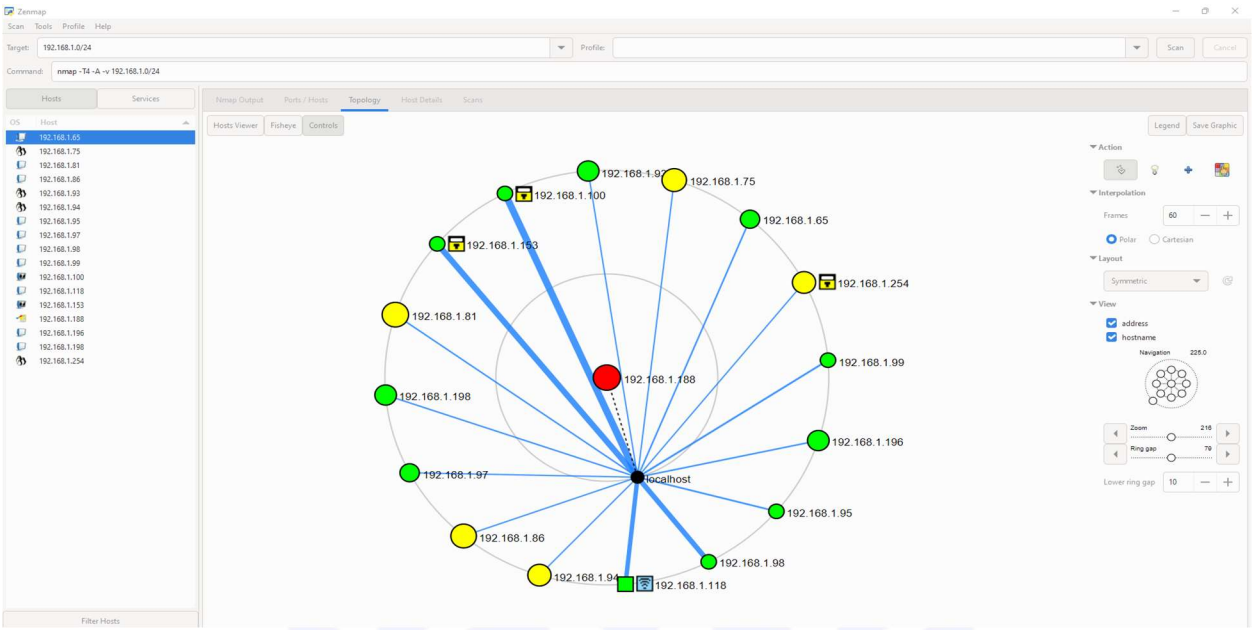
4. Identify your ip address and subnet mask to determine your ip calss.



5. Proceed to input ip address in nmap command section and scan



6. Analyze scan results

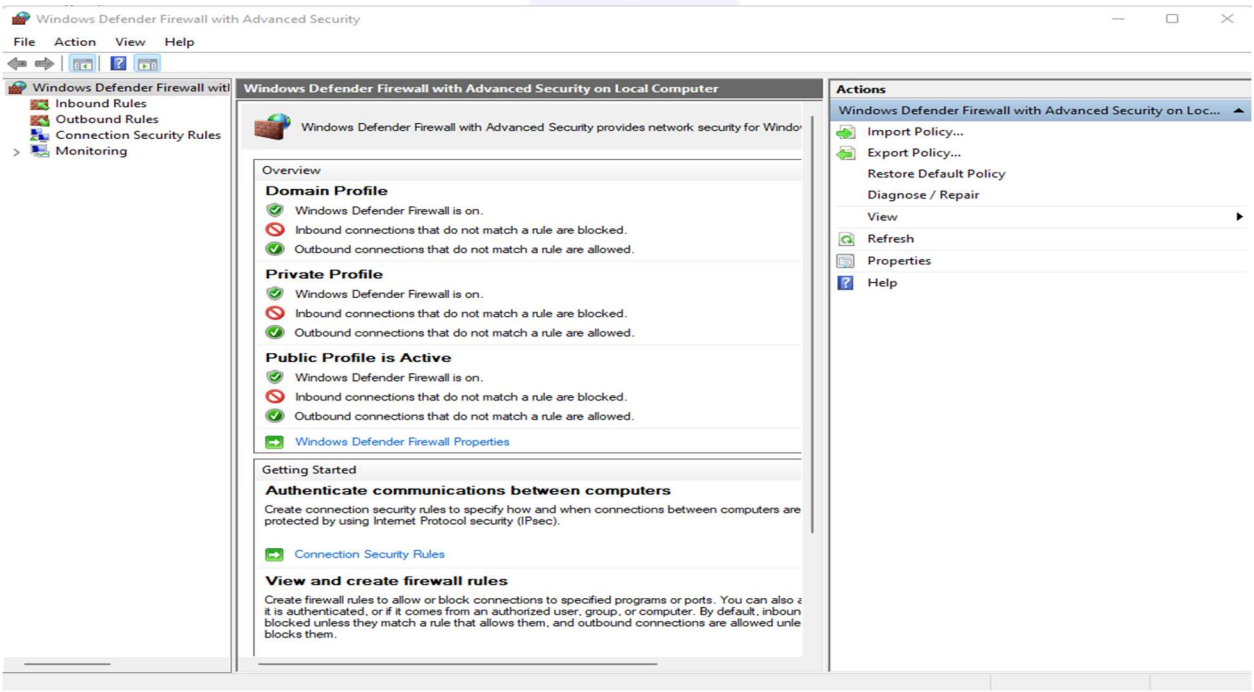


7. Also scan **delojik.com** and analyze the results, remember this is an aggressive scan only run on network you have access or permission to avoid prosecution.

    a. Identify the traceroute result.

8. Open windows defender firewall and go to advance

9. Go to advanced settings to set inbound and outbound rules.



Note:

1. Do not run command switch -A -v on just any network, it is very invasive command, you can be prosecuted for that.
2. The reason for nmap is to be able to know the types of switches you can use and be able to analyze scan results by the end of the course. Also it gives us the result of the vulnerabilities we need to know.
3. Nmap has both Graphic User Interface (GUI) base and command prompt.
4. Versions listed in Ports/Hosts is called **Enumeration**. You never want the version of services running on your system to be shown to avoid hackers launching attack on the machine. The version means the type of data you are transmitting, for example if windows 8 has been upgraded or patched to updated version supported by the vendor, we upgrade to fix hole in vulnerability as well as for functionality.

QUESTIONS

1. **Perform NMAP intense scan nmap T4 -A -v (Host) on YOUR HOST machine and www.delojik.com**

   Analyze both scan results and answer the following questions:

   a. Attach screenshot of Nmap output, Ports/Hosts, Topology and Host Details.
   b. Why do we have traceroute in Nmap scan for **delojik.com** and not **YOUR HOST**
   c. Analyze Traceroute result for delojik.com, identify servers location (City and Country)
   d. Why are filtered ports not enumerated?
   e. What are the advantages of filtered ports
   f. What are the disadvantages of filtering **ALL** ports?
   g. Can you configure port remotely? If so, how?
   h. Are you able to scan someone else's network with Nmap?

Submit your response to INFO@DELOJIK.COM

SUBMIT BY Thursday February 27 at 6pm US CT.