Student Name:

Course: CSCE 5550

Semester: Fall 2025

Network Scanning Lab

Lab 1a: Network Scanning

This lab uses the **Kali 2025** virtual machine (VM).
The credentials are:
Username: kali
Password: kali

Rubric: 5 points x 10 questions = 50 points.

NOTE 1: Answer all the questions (Q1, Q2, etc.), they are marked in bold.

When a screenshot is requested, try to fit all the results in one image.

If this is not possible, then attach multiple screenshots.

NOTE 2: Make sure that your answer is clear (unambiguous). For example, suppose that the question is "Who is the owner of the file?" and the answer is "Alice". Then, you should either type "Alice", or highlight "Alice" on a screenshot, or provide a screenshot with a single word "Alice".

IMPORTANT NOTE: Before starting the lab, you must customize your command prompt as described in the Command Prompt Customization Manual. This customization manual directs you to place your EUID (Enterprise User ID) into the command prompt. Submissions that do not comply with this requirement will receive no credit.

Introduction

Scanning is the first phase of an active attack; its purpose is to gather intelligence on the network structure and its individual hosts. The information which may be collected includes IP addresses, host's operating system, running services, and installed applications. More specifically, scanning the network is a process of locating systems that are alive and responsive. There are various types of scanning, but in this lab, we will focus on port scanning and network scanning. Port scanning is the process of identifying open and available TCP/IP ports on a system.

Port scanning tools enable us to learn about the services available on a given system. Each service or application on a host is associated with a specific port number. Port numbers are divided into the following three ranges:

- "Well-known ports": 0-1023
- "Registered ports": 1024-49151
- "Dynamic ports": 49152-65535

It is helpful to know a usual assignment of ports for major services.

Student Name:

Course: CSCE 5550

Semester: Fall 2025

Network Scanning Lab

Ping

Ping sweep techniques start with checking for systems that respond to probes or connection requests. This is the simplest, although not the most accurate way to determine whether systems are live. A ping sweep is also known as Internet Control Message Protocol (ICMP) scanning, as ICMP is the protocol used by the "ping" command. This is the process of sending an ICMP request or ping to all hosts on the network to determine which ones are online. It is a quick test to see if two hosts have connectivity and it is used extensively for troubleshooting. A benefit of ping is that it can run in parallel, meaning that all systems are scanned at the same time, and hence it can be done quickly. A downside of this approach is that systems can disable ICMP, thus the ping sweep may not give accurate information about the network. Windows, MacOS, and Linux all have a built-in ping command. To run it, type the command "ping" and then the domain or IP address that you wish to check (to exit the command, press CTRL-C).

There exist more advanced tools for network scanning, for example "hping3". This tool has a lot of extra options on top of the basic ping functionality. The most useful of them is, for instance, crafting the packets to get a response from a host that has ICMP disabled. We will consider such the example next.

Ping Examples:

1. Open a terminal.

Q1: Type the "ping www.unt.edu" command, and after a few seconds press "Ctrl + C" – this will cancel the ping. Attach a screenshot of the result.

Note: It is possible that you see no response from www.unt.edu, if the output showed your packets transmitted and 0 received with a 100% packet loss. Whether you got the response or not, attach a screenshot of the result (as requested above) and continue to the next step. Remember that the "sudo" command will request a superuser password, which is also "kali".

Q2: Type a command "sudo hping3 -S www.unt.edu -p 80", and after a few seconds press "Ctrl + C" – this will cancel the ping. Attach a screenshot of the result.

2. Here, we use a "-S" option to tell hping3 to use SYN packets. A SYN packet is the first packet sent in the 3-way handshake for TCP connections. Knowing that www.unt.edu is a webserver, we are sure that it has to handle SYN packets for legitimate connections. Therefore, we use the "-p 80" parameter to have hping3 hit the port 80 (which is used for the HTTP protocol). Hereby, we use the TCP protocol to manipulate the UNT webserver to send us a reply—as you can see, we should now have 0% packet loss.
3. Next, we will try a website which surely does not filter out ICMP Echo Requests.

Student Name:

Course: CSCE 5550

Semester: Fall 2025

Network Scanning Lab

Q3: Type a command “ping scanme.nmap.org”, and after a few seconds press “Ctrl + C” – this will cancel the ping. Attach a screenshot of the result.

Traceroute

Traceroute is a computer network diagnostic tool for displaying the route and measuring transit delays of packets across an Internet Protocol network. Traceroute is very useful for learning the routes that your packets are taking to a particular target. This tool uses the Time-To-Live (TTL) flag for packets. This is a flag that lets networking devices know how far they should forward the packet. Specifically, every time when the packet reaches a device, the TTL is dropped by one. For example, most Windows devices use a TTL of 128 and Unix of 64 – this allows 128 (respectively, 64) total hops once the packet leaves your machine. This is a crucial mechanism for allowing packets that get lost to be dropped instead of endlessly traversing the network and hereby consuming the bandwidth.

Traceroute uses TTL in the following manner: Your first packet will start with a TTL of 1, therefore the first message gets dropped at the first router it hits and the router sends back an ICMP error message “Time Exceeded”. In the second packet, the TTL will be set to 2, so that the first router will forward the packet, but the next one will drop it. Traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse until the destination is reached and returns an ICMP Echo Reply message. This information is used to learn the route to a particular destination. If one knows what to look for, one can identify firewalls, routers, honeypots, proxy servers, and sometimes, even hosts performing the man-in-the-middle attack.

1. Open the terminal and run the following command:
   sudo traceroute www.unt.edu

Q4: Attach a screenshot of the result.

2. The traceroute functionality by default sends UDP packets with destination port from a certain range (which normally has no service associated with it) and then uses a reply with ICMP Destination Unreachable messages to compute the route. As routers may block these messages, an alternative may be to use ICMP Echo Reply messages generated using the option “-I”.

Q5: Use the command “sudo traceroute -I www.unt.edu”.
Attach a screenshot and compare the results of this command to those of the previous one.

Remark: If tracing gets stuck at a certain hop, you may press “Ctrl + C” to stop the traceroute.

Student Name:

Course: CSCE 5550

Semester: Fall 2025

Network Scanning Lab

Note: An alternative approach is to use TCP SYN packets. For this, the option "-T" should be used in the above command. For more information on the traceroute tool, check the manual by typing *"*traceroute *--help"* in the command line.

NMAP

Nmap is a free, open-source tool that quickly and efficiently performs ping sweeps, port scanning, service identification, IP address detection, and operating system detection. Nmap has the benefit of scanning a large number of machines in a single session. It is supported by various operating systems, including Unix, Windows, and Linux.

The state of a port, as determined by an Nmap scan, can be "open", "filtered", or "unfiltered". "Open" means that the target machine accepts incoming requests on that port. "Filtered" means that a firewall or network filter is screening the port and preventing Nmap from discovering whether it is open. "Unfiltered" mean the port is determined to be closed, and no firewall or filter is interfering with the Nmap results.

Types of Nmap scans

TCP Connect: The user makes a full TCP connection to the target system. This types of scan is the most reliable but also the easiest to detect. Open ports reply with an SYN/ACK while closed ports reply with an RST/ACK packet. TCP connect scans can be slow since a full connection is attempted.

XMAS Tree: The scanner checks for TCP services by sending the so-called XMAS-tree packets, which are so named because all the "lights" are on, meaning that the FIN, URG, and PSH flags are set. These flags are bits that signify various connection settings for TCP packets. Closed ports reply with an RST flag.

SYN Stealth Scan: This is also known as half-open scanning. The attacker sends a SYN packet and receives a SYN/ACK back from the server. It is considered stealthy because a full TCP connection is not opened. Open ports reply with a SYN/ACK while closed ports reply with an RST/ACK.

Null Scan: This is an advanced scan that may be able to pass through firewalls undetected or modified. Null scan has all flags off or not set. It only works on Unix systems. Closed ports will return an RST flag.

Windows Scan: This type of scan is similar to the ACK scan (described next) and can also detect open ports.

ACK scan: This type of scan is used to map out firewall rules. ACK scan only works on Unix. The port is considered filtered by firewall rules if an "ICMP Destination Unreachable" message is received as a result of the ACK scan.

Now that we discussed some of the types of scans which are available in Nmap, let us go over some of the command option that allow us to enable them. Similar to "hping3", Nmap is a command-line based tool. The syntax is similar to the standard Linux commands: Type "nmap", the options, specific ports if any, and then the target IP address or domain name. The options can be used in a wide variety of combinations; the popular ones are listed below.

Student Name:

Course: CSCE 5550

Semester: Fall 2025

Network Scanning Lab

- TCP connect scan: -sT
- SYN scan: -sS
- XMAS scan: -sX
- Ping scan: -sP
- UDP scan: -sU
- RPC scan: -sR
- List DNS: -sL
- TCP ping: -PT
- SYN ping: -PS
- ICMP ping: -PI
- No ping: -Pn (skip the host discovery, i.e., scan IP address(es) without pinging them first.)
- OS discovery: -A

By default, Nmap scans the top 1000 most common ports.

One can specify ports using the option “-p [ports]”, to scan all ports use “-p-”.

Next, let us discuss how to scan all the live hosts on the same network. Note that some of the scans might take a few minutes to run.

NMAP Examples:

Open a terminal.

Q6: Run the command “nmap -sP scanme.nmap.org”.
Attach a screenshot of the result.

Note the IP address shown by the above command and let us use it for the next question.
We will denote it by [IP-address] in the commands.

Q7: Run the command “sudo nmap -sS -PN -A [IP-address]” (wait some time for it to complete).
Attach a screenshot of the result.

Remark: Let us review the options that we use: “-sS” will switch on a SYN scan in a stealth mode, “-PN” will force scanning of the host without pinging it first, and “-A” will switch on OS detection.

Q8: Analyze the output of the above command and answer the following question: which services are running on this system?

Q9: Analyze the output of the above command and answer the following question: which OS is running on this system?

Student Name:

Course: CSCE 5550

Semester: Fall 2025

Network Scanning Lab

NOTE: If you use the NAT network setting, Nmap indicates the OS guess as "VirtualBox". Since this guess is obviously wrong, this answer will not receive a credit. Analyze the output carefully and provide a more reasonable guess.

For scanning specific ports or port ranges use the "-p" option. Let us scan for port 22, which is typically assigned to SSH.

Q10: Run "sudo nmap -sS -p 22 scanme.nmap.org". Attach a screenshot of the result.