Nmap Enumerate a Network

Contents

Time required: 60 minutes

Lab Description

One of the first steps of penetration testing or doing a security audit is to find out what devices are on the network.

DANGER ZONE: Make sure that you own the devices you perform a scan on. If you are performing this scan on a device or network you do not own, make sure to get a written consent from the owner of the device to avoid legal issues.

You have permission to scan the network in D1.

nmap in Kali Linux

nmap is already installed in Kali Linux

1. In a Kali Linux terminal session, update Kali.

```
# Update the packages list
sudo apt update

# Perform the update
sudo apt upgrade -y
```

2. In the Kali Linux VM → Go to **Machine** menu → **Settings** → **Network**. Make sure you are attached to the Bridged Adapter.
3. In a Kali Linux terminal session type **ip a**

Use this information to figure out your network Target.

For example: If your IP address was 192.168.1.106, and your subnet mask is 255.255.255.0, then your network Target is 192.168.1.1-254 or 192.168.1.0/24

4. **Insert a screenshot showing your IP address and subnet.**

Click or tap here to enter text.

nmap -sn

This option tells Nmap not to run a port scan after host discovery. When used by itself, it makes Nmap do host discovery, then print out the available hosts that responded to the scan. This is often called a "ping sweep scan". It performs light reconnaissance of a target network quickly and without attracting much attention. Knowing how many hosts are up is valuable to attackers.

Systems administrators often find this option valuable as well. It can easily be used to count available machines on a network or monitor server availability. This is often called a ping sweep.

```
# This is a ping sweep scan
# nmap -sn <network_address>
# Example in D1, replace 10.0.1.0-254 with your network addresses
nmap -sn 10.0.1.0-254
# Another way to designate the network to scan
nmap -sn 10.0.1.0/24
```

1. **Insert a screenshot showing your scan results.**

Click or tap here to enter text.

2. **How many IP addresses were scanned?**

Click or tap here to enter text.

3. **How many hosts are up?**

Click or tap here to enter text.

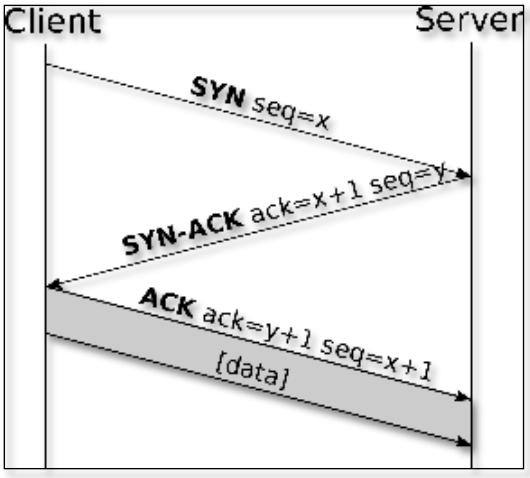
4. **What other information is available?**

Click or tap here to enter text.

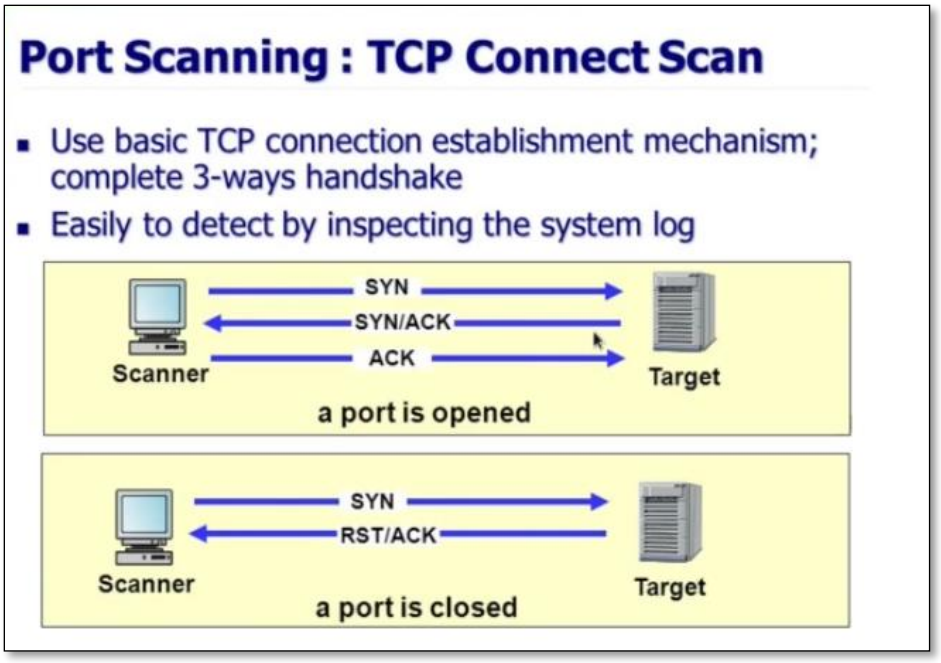
nmap -p

What is the TCP handshake?

To make sure data is correct, TCP does a three way handshake. It sends a message back and forth between client and server.



The messages are **SYN**, **SYN-ACK** and **ACK.** This is the complete handshake. This handshake happens each time you try to connect to a service port and the port is open.



If a port is not open, it sends **RST** back instead of **SYN-ACK**. nmap sends these messages to the target to determine which ports are open and closed.

The -p option allows you to specify target ports for scanning. Pick an IP address from your previous scan that has the most open ports to look at. You can scan a single port, or a range of ports as shown in the example below.

```
# This example IP address is for the main server in D1
# Scan a specific range of ports
nmap -p 1-1024 10.0.1.10
```

1. **Insert a screenshot showing your scan results.**

Click or tap here to enter text.

2. Scan the same target for all open ports.

```
# This example IP address is for the main server in D1
# Scan all ports
nmap -p- 10.0.1.10
```

3. **Insert a screenshot showing your scan results.**

Click or tap here to enter text.

nmap --script=vuln

Nmap with the **--script=vuln** option performs a vulnerability scan using NSE (Nmap Scripting Engine) scripts specifically designed to identify potential vulnerabilities in target systems.

Run this command against the D1 web server. This may take some time.

```
sudo nmap --script=vuln lab.wncc.net -vv
```

1. **Insert a screenshot showing your scan results.**

Click or tap here to enter text.

nmap --script=http-brute -vv

This script is an example of a brute force attack. If there are any open ports that use authentication, it will a brute force username password attack. Run this against your firewall.

```
nmap --script=http-brute <firewall-ip> -vv
```

1. **Insert a screenshot showing your scan results.**

Click or tap here to enter text.

2. Run this same script against the D1 web server.

```
nmap --script=http-brute lab.wncc.net -vv
```

3. **Insert a screenshot showing your scan results.**

Click or tap here to enter text.

nmap --traceroute

A traceroute provides the path that packets take to reach a destination. Nmap, primarily a port scanning tool, can be combined with traceroute.

```
# Trace the route to wncc.edu using port 80
nmap --traceroute -p 80 wncc.edu
```

1. **Insert a screenshot showing your scan results.**

Click or tap here to enter text.

```
# This web site is a little further away
nmap --traceroute -p 80 visitbritain.com
```

2. **Insert a screenshot showing your scan results.**

Click or tap here to enter text.

nmap -T4 -F

The command **nmap -T4 -F** initiates a fast scan using Nmap with aggressive timing (T4) and a limited set of ports (F). This is useful for a quick overview of open ports on a target system.

```
# Standard service detection
nmap -T4 -F 10.0.1.0/24
```

1. **Insert a screenshot showing one screen of your scan results.**

Click or tap here to enter text.

```
nmap -T4 -F -oN outputfile.txt 10.0.1.0/24
```

2. **Attach the text file outputfile.txt to the assignment in Blackboard.**

Assignment Submission

Attach this completed document along with the text file to the assignment in Blackboard.