NETWORK ENUMERATION DEMO

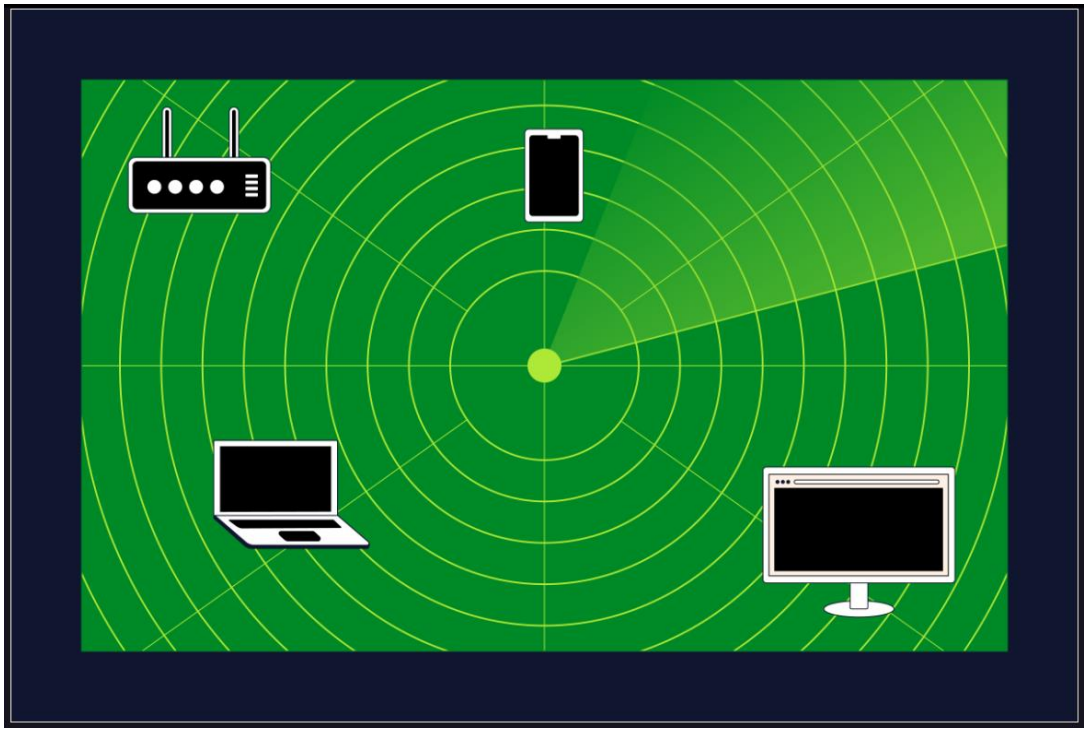
Introduction

If we want to hack a computer, we must know a few things.

Before anything else, we need to know that the computer exists in the first place - it's hard to hack a computer that doesn't exist. We also need information about the computer, and the more we have, the better. At a minimum, we'll want to know what operating system and software the computer is running so that you can start looking up potential exploits.

One of the ways we can gain information about computers is through **Network Enumeration** (also known as **Network Scanning**). Network enumeration is an incredibly useful reconnaissance tool that can tell us what computers exist on a network and provide information about what those computers are. We can think of network enumeration like sonar or radar, sending out a pulse (or a packet of data in this case) and seeing what comes back. Also, like sonar and radar, network enumeration can make a lot of noise, and doing it recklessly will alert defenders to your activity.

Network enumeration can also be used for defensive or utility purposes, such as creating network diagrams or finding misconfigured computers.



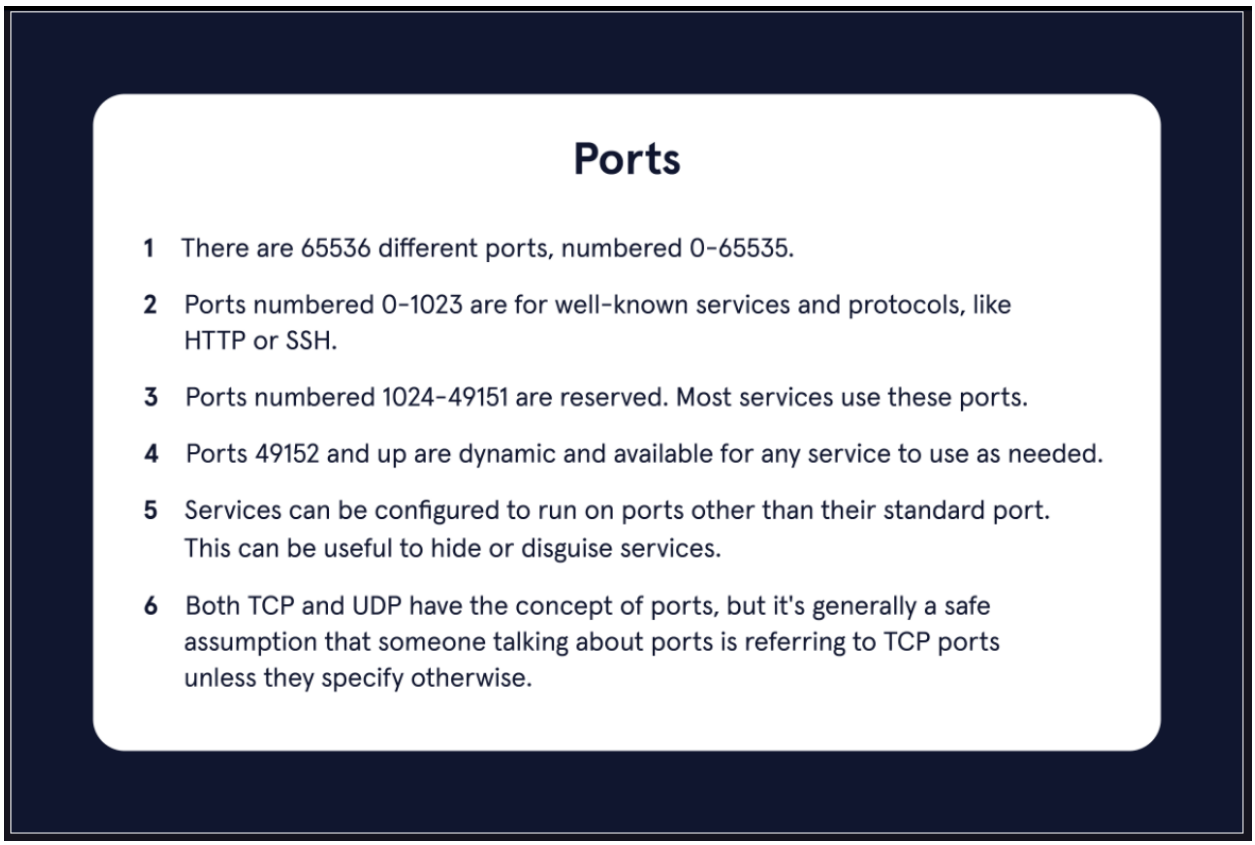
Ports and You

An important concept to understand for network enumeration (and networking in general) is the concept of **ports**. Ports are to IP addresses, what apartment numbers are to street addresses. Ports don't specify which computer the data gets sent to, but the computer uses the port number to figure out which program to give the data to once the data arrives. Knowing what ports a computer has active can give us an idea of what services the computer is running and what the computer's purpose is.

Here's a summary of the most important things to know about ports:

- There are 65536 different ports, numbered 0-65535.
- Ports 0-1023 are reserved for the most important or well-known protocols.
- Ports 1024-49151 are associated with less common protocols and services.
- Ports 49152 and up are dynamic and can be used as needed.
- Ports can be `open` or `closed`. Ports are closed by default but are opened when a computer runs a service that uses that port.
- Services can run on ports other than the port they are associated with by default. Likewise, services can run on ports associated with different services if configured. This can be used defensively to make network enumeration more difficult or offensively to obfuscate malicious connections.

Don't worry about memorizing specific port numbers for now! We'll provide relevant port numbers as needed for this lesson.



Time to Scan

The situation is as follows: One of the computers in a network has been infected with malware.

Our task is to use network enumeration to determine which computer is likely to be infected so the computer can be wiped. We know the malware opens a port while it runs, but we don't know which port.

In this exercise, we'll use Nmap, a popular network scanning/enumeration tool, to identify which computer needs to be wiped. We'll be using IP addresses in `10.1.1.x` range for demonstration purposes.

Before we begin our discovery, here are a few things to note:

- Nmap, Network Mapper, is a port scanner/network mapping tool. It is the most used scanning tool by ethical and unethical hackers. The tool scans systems/networks for IP addresses, ports, OS details, and applications/services installed.
- Nmap is an open-source command-line tool designed to run on the Linux operating system (OS).

- Nmap is an open-source tool that is open to the public to use and improve on.

Note: *Some of these services are not running on this box, so we have faked some terminal interactions in this specific exercise. This is so you can experience how these commands work in the real world.*

Instructions

1.

Let's start by using nmap to scan this box! What services are running in this lesson?

We can use the basic command `nmap [target]` to scan a target. In this case, `localhost` is our target.

Use the command:

```
nmap localhost
```

Hint
Type and run the command `nmap localhost` in the terminal.

2.

Great! We've scanned our target and identified a list of running services.

It would be nice to see how many computers are on our part of the network. Let's scan the wider network to find out! (The easiest way to do that is by pinging every address.)

We can use the command:

```
nmap -sn 10.1.1.0-255
```

to ping every address in our desired range.

- The `-sn` parameter specifies that we want to use ping scanning.
- `10.1.1.0-255` means we want to scan this range of addresses.

Hint
Type and run the command `nmap -sn 10.1.1.0-255` in the terminal.

3.

It looks like there are four hosts, not including ourselves, on the network.

We discovered hosts up at these addresses:

- `10.1.1.21`
- `10.1.1.22`
- `10.1.1.23`
- `10.1.1.24`

We know that the hosts exist, but not much more than that. Let's run a more intensive scan, targeting the four hosts specifically.

Use the command:

```
nmap -sS -T4 --top-ports 1000 10.1.1.21-24
```

to scan the 1000 most commonly open ports on our targets.

- `T4` specifies that this will be done fairly quickly.
- `sS` is short for "stealth scan" (which is not very stealthy these days).

Hint
Type and run the command `nmap -sS -T4 --top-ports 1000 10.1.1.21-24` in the terminal.

4.

Now, we're starting to get a good picture of the hosts!

Notice that the host on `10.1.1.24` has ports `80` and `443` open. These ports are associated with the HTTP and HTTPS protocols, indicating that this might be a server.

Servers are high-value targets, so this would be a good candidate for further investigation.

We can scan every port on this specific target using the command:

```
nmap -p- 10.1.1.24
```

Hint
Type and run the command `nmap -p- 10.1.1.24` in the terminal.

5.

Hmm, port `12345` looks a bit odd...

```
12345/tcp open netbus
```

Further investigation reveals that it's associated with the **NetBus Remote Access Trojan**. Looks like we've found our malware!

Press Enter in the Terminal to complete this checkpoint.

Then select Next to continue with the lesson.
Hint
Google is your friend when you're trying to figure out what service a port is associated with, or what a service does!

To pass this checkpoint, click on the Terminal and press the Enter key.

Terminal
bash

```
$ nmap localhost
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000078s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp    filtered ssh
2121/tcp open  ccproxy-ftp
4000/tcp open  remoteanything
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 2.58
seconds
$ nmap -sn 10.1.1.0-255
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for my_computer (10.1.1.20)
Host is up (0s latency).
Nmap scan report for 10.1.1.21
Host is up (0s latency).
Nmap scan report for 10.1.1.22
Host is up (0s latency).
Nmap scan report for 10.1.1.23
Host is up (0s latency).
Nmap scan report for 10.1.1.24
Host is up (0s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 0
seconds

$ nmap -sS -T4 --top-ports 1000 10.1.1.21-24
```

```
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for 10.1.1.21
Host is up (0s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
161/udp  open  snmp
MAC Address: 5E:0F:E4:9A:13:D2 (unknown)
Nmap done: 4 IP addresses (4 hosts up) scanned in 0
seconds


Nmap scan report for 10.1.1.22
Host is up (0s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
161/udp  open  snmp
MAC Address: 05:05:50:88:9E:38 (unknown)

Nmap scan report for 10.1.1.23
Host is up (0s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
161/udp  open  snmp
MAC Address: BE:63:43:7D:05:80 (unknown)

Nmap scan report for 10.1.1.24
Host is up (0s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
161/udp  open  snmp
443/tcp  open  https
MAC Address: 0D:32:BC:1B:28:7F (Servers R Us)

$ nmap -p- 10.1.1.24
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for 10.1.1.24
Host is up (0s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
161/udp  open  snmp
```

```
443/tcp  open  https
12345/tcp open netbus
MAC Address: 0D:32:BC:1B:28:7F (Servers R Us)

Nmap done: 1 IP address (1 host up) scanned in 3 seconds
```

Conclusion

Networking enumeration is a powerful tool for hackers and is used by attackers and defenders alike. There are many different network enumerators available, with different specialties. The previous exercise was based on NMap. NMap is versatile, capable of everything from simple port scanning to running scripts that attempt to determine whether specific vulnerabilities exist on a target. It's also free and open-source.

Another common network enumeration tool is Nessus, a paid tool designed more for defensive use. Some exploitation frameworks, such as Metasploit, also include network enumeration tools.