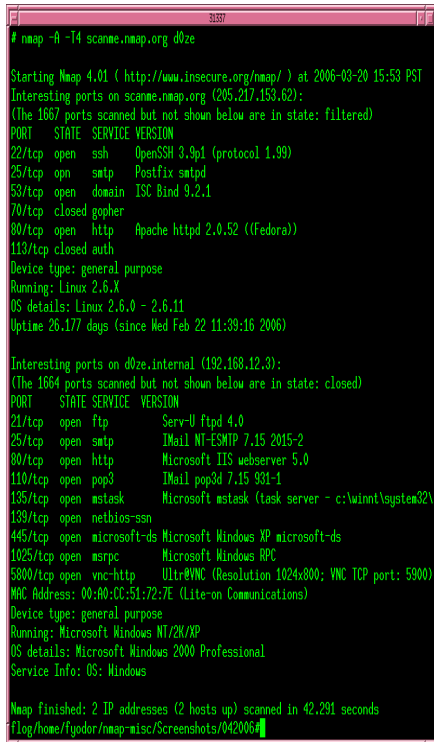


Lab 8

NMAP Scanning



```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.3p1 (protocol 1.99)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftpd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3     IMail pop3d 7.15 931-1
135/tcp   open  mstask   Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc    Microsoft Windows RPC
5900/tcp  open  vnc-http UltraVNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flag/home/tyodor/nmap-misc/Screenshots/042006#
```

Estimated time to complete: 40 Min

WHAT YOU WILL LEARN

You will learn how the NMAP (Network Mapper) tool works and how to utilize it to scan networks to discover host information, look for open ports, and learn what applications are running.

WHY IT'S IMPORTANT

NMAP is frequently used by network administrators for network inventory, managing upgrade schedules, and monitoring uptimes.

Understanding NMAP is important because it is a useful tool for offensive and defensive security in a real world setting.

SKILLS GAINED

- Network scanning
- Resource discovery
- Network monitoring

REQUIRED HARDWARE

- Raspberry Pi
- Internet connection

Nmap (Network Mapper) is a free and open source utility for network discovery and security auditing. It is used by system administrators for network inventory, managing service upgrade schedules, and monitoring host or service uptime. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap has also been featured in popular media like The Matrix and Mr. Robot.



SCANNING NETWORKS WITH NMAP

To find out what hosts are on a network you can generally do a ping command, if a host is up and you ping its IP address, it will give a response. This is great when there is only one host, but what if you wanted to ping an entire network? This is where Nmap comes in. The generally accepted method of scoping out a network for vulnerabilities is as follows:

1. Check for live systems - Something like a ping can provide this.
2. Check for open ports - Once you know IPs are active, find out what ports they are listening on.
3. Perform banner grabbing - Banner grabbing and OS fingerprinting will tell you what operating systems are on the machines and what services they are running.
4. Scan for vulnerabilities - Use the gathered information to see if any hosts with open ports are vulnerable to a variety of attacks.
5. Draw network diagrams - Being able to piece together how the network logically works and look at possible avenues for attacks.

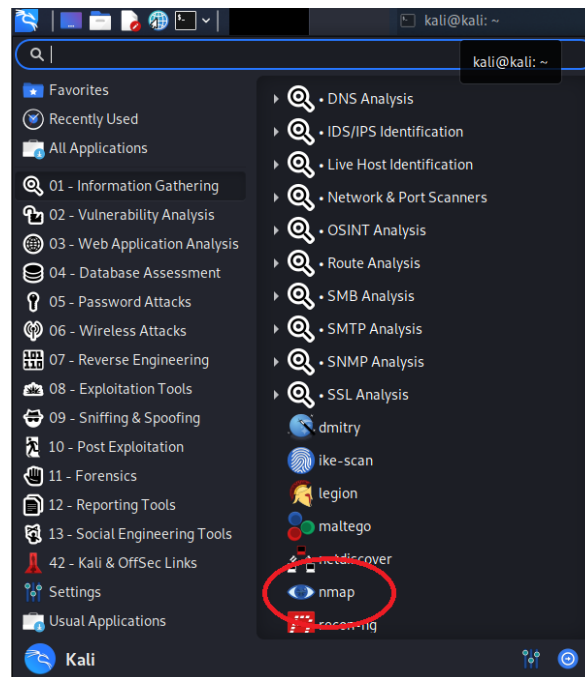
You can do all of these steps using only Nmap, it is a widely powerful tool and is a penetration testing essential. For the record, in the US, there is no federal law against port scanning and no guidelines exist at a more local level so port scanning is technically legal, but most public entities will not look at it so kindly.

NMAP OPTIONS

Nmap has a variety of options to use during scanning to find a certain piece of information or to modify your scanning technique. Some useful options are the **-sL** command, which simply gives you a list of targets to scan, **-O** can tell you what operating system a host is running, **-sS** is a stealth scan meaning it leaves the TCP handshake open in an attempt to bypass intrusion detection software running on the network, **-exclude** excludes certain IPs from the scan, **-p** allows you to choose what port to scan, **-S** will spoof your source address during scans, and **-D** will deploy decoys to mask your activities. The complete list of Nmap commands can be found at <https://svn.nmap.org/nmap/docs/nmap.usage.txt> or by running the **man nmap** command in the terminal on your Kali machine.

STEP 1: STARTING NMAP

Open Nmap by clicking: Start Button -> "01 - Information Gathering" -> nmap



STEP 2: BASIC SCANNING

We begin our intelligence journey by scanning the website scanme.nmap.org with no options to see what the default information that Nmap will give us. This website was specifically created to test Nmap out on and the owners of the website give explicit permission to do so. We can achieve this by typing "**sudo nmap scanme.nmap.org**" into the command line and hitting enter. Some of these scans may take a while as nmap is checking all of the most common ports. Your scan results may differ from the ones shown as the website may change or sometimes not respond. This is why it is important to run these scans a few times to make sure you get as much information as possible.

```
(kali㉿kali)-[~]
└─$ nmap scanme.nmap.org

Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-15 10:23 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 47.86 seconds
```

From the results we can see a few things.

- 1: We can see that the computer is on and responsive because Nmap states “Host is up”
- 2: We can see that Nmap found 3 open ports: 22, 80, and 31337. While Nmap states the services on these ports, it's just assuming what these services are. EXAMPLE: This website could possibly be running minecraft on port 80.
- 3: Even though we only did a basic scan, it still took us almost 50 seconds to get a small report

STEP 3: DISCOVERING SERVICES

In order to learn more about our target device, we are going to find out what services it is running. While Step 2 showed us the ports that are open, using our new option **-sV** we can see the actual services running on the server. With our new command “**sudo nmap -sV scanme.nmap.org**” we can let the scan run and wait for the results!

```
(kali㉿kali)-[~]
$ nmap -sV scanme.nmap.org

Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-15 10:49 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.53 seconds
```

You may have to run this scan multiple times in order to see all the services listed above.

As you can see from the photo, the device uses Ubuntu Linux and runs Apache web server 2.4.7 for the website and OpenSSH 6.6.1 for remote access. This information comes in handy as you could search for exploits specific to these versions using Metasploit from lab 8!

STEP 4: SCANNING A NETWORK

While -sV gave us a lot of useful info, it only gave us info on one device. If we want to scan an entire network we have to modify what we tell nmap. Because these scans can take so long if you add options, we are going to leave out any detail oriented options for this example. We can achieve this using the command:

“sudo nmap -sL scanme.nmap.org/24”

The meaning of this command is shown below:

- nmap - Runs the program
- -sL - Lists devices on the network
- scanme.nmap.org/24 - The address that specifies the entire nmap.org network

```

(kali@kali)-[~]
└─$ sudo nmap -p 443 -sS scanme.nmap.org/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-15 12:37 EDT
Nmap scan report for 45.33.32.0
Host is up (0.0017s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for gw-li982.linode.com (45.33.32.1)
Host is up (0.00026s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for 45.33.32.2
Host is up (0.00026s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for 45.33.32.3
Host is up (0.00028s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for li982-4.members.linode.com (45.33.32.4)
Host is up (0.11s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for li982-5.members.linode.com (45.33.32.5)
Host is up (0.11s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for li982-6.members.linode.com (45.33.32.6)
Host is up (0.11s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for li982-7.members.linode.com (45.33.32.7)
Host is up (0.00024s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for li982-8.members.linode.com (45.33.32.8)
Host is up (0.00024s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for li982-9.members.linode.com (45.33.32.9)
Host is up (0.11s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for fivekeys.issoasis.com (45.33.32.10)
Host is up (0.11s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for 45.33.32.11
Host is up (0.24s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for 45.33.32.12
Host is up (0.0016s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for li982-13.members.linode.com (45.33.32.13)
Host is up (0.11s latency).

PORT      STATE SERVICE
443/tcp    filtered https

Nmap scan report for li982-14.members.linode.com (45.33.32.14)
Host is up (0.16s latency).

PORT      STATE SERVICE
443/tcp    open  https

Nmap scan report for li982-15.members.linode.com (45.33.32.15)
Host is up (0.16s latency).

```

With our results, we can see that there are multiple devices on the nmap.org network that are up. If a device states it has port 443 open it most likely is another website. Each one of these devices can serve as an entry point for an attacker and should be reviewed by the network administrator at nmap to make sure they are up to date on their security settings. As an attacker, this would be a great starting point to an attack.

EXERCISES:

DISCLAIMER: THE WEBSITE WE HAVE BEEN SCANNING GIVES EXPLICIT PERMISSION TO RUN NMAP SCANS ON IT. MAKE SURE TO GET PERMISSION FROM THE NETWORK ADMINISTRATOR OR OWNER TO SCAN THE NETWORKS YOU USE GOING FORWARD

1: Scan your device:

One of the major uses of Nmap is discovering vulnerabilities within your own machine. This will tell you if you have any unnecessary ports open that could expose your machine to vulnerabilities. Your results should come back with *“All 100 scanned ports on localhost (127.0.0.1) are closed”*, if this is not what you get back, look into those open ports! We can do this using the command:

“nmap -sV 127.0.0.1”

The meaning of this command is below:

- nmap- Runs the program
- -sV - Checks for services running
- 127.0.0.1 - Your device's address

Did you find any ports open on your machine? If so, which ones were open and why were they open?

2: Scan your network:

Another major use of Nmap is discovering vulnerabilities within your own network. By seeing what services you have facing the public internet, you can spot unauthorized services, outdated software, and close any unnecessary ports. We can do these things using the command:

"nmap 192.168.0.0/16 10.0.0.0/8"

The meaning of this command is below:

- nmap - Runs the program
- -sV - Checks for services running
- 192.168.0.0/16 - Defines all the possible address in a typical home network
- 10.0.0.0/8 - Defines all the possible address in a typical home network

You can do the command ***ifconfig*** from Linux terminal or ***ipconfig*** on Windows command line to find out if you are in a 192.168 network or a 10. network.

THIS COMMAND WILL TAKE A SIGNIFICANT TIME TO RUN

Once you have run your scan, determine what services are running on your network and see if you can discover what device is hosting them. If the services are outdated, unnecessary, or malicious, consider turning them off or blocking them on your network.

REVIEW

1: Who uses Nmap?

- A) Hackers
- B) System administrators
- C) Police officers
- D) A and B

2: What does the -sS command do?

- A) A stealth scan
- B) A short scan
- C) Sabotages the hosts you scan
- D) Makes you sound like a snake

3: Is port scanning legal?

- A) Yes
- B) No
- C) Yes but you need permission to do so
- D) It is illegal in some states

4: Which of these can Nmap **NOT** find

- A) What user is logged in to a host
- B) What operating system a host is running
- C) What ports are open on a host
- D) What IPs have hosts connected

5: Which command will you use to find Nmap options?

- A) commands nmap
- B) man nmap
- C) nmap -c
- D) nmap ?

6: Why would someone use Nmap?

- A) To take down a network
- B) To steal user information
- C) To find vulnerabilities in a network
- D) To make sure a network is functioning

Answers: 1:D 2:A 3:C 4:A 5:B 6:C