OWASP Top 10 - Identify Active Network Hosts and Services Using Nmap

Overview

The purpose of reconnaissance is to collect as much information about a target network as possible. From a hacker's perspective, the information gathered is very helpful when preparing for an attack. A penetration tester tries to find the information and patch the vulnerabilities if found. This is also called Footprinting.

Nmap has parameters, also known as switches, that can help you perform network reconnaissance. In this lab, you will look at some of the key switches.

All this information is testable depending on which cybersecurity exam you sit for.

Lab Requirements:

- One installation of VirtualBox with the extension pack
- One virtual install of Kali Linux
- One virtual install of the OWASP OVA image

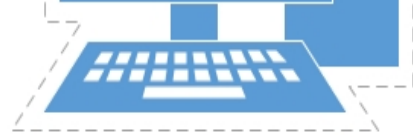Your VirtualBox network adapters should be set to NAT network for both VMs.
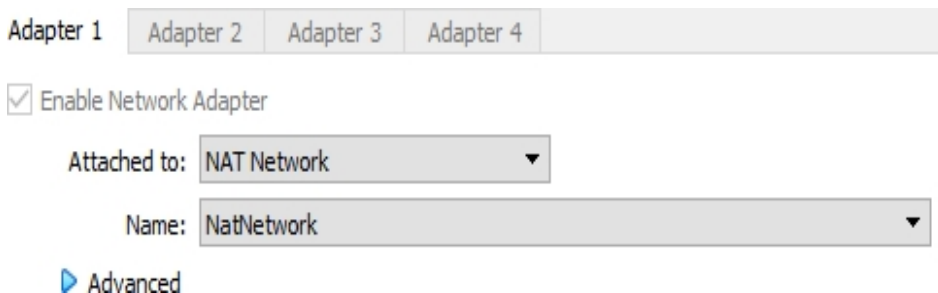
Confirm that your Kali and OWASP machines are on the same network of 10.0.2x by opening and typing ifconfig at either terminal. The OWASP target machine has the username and password provided on the terminal.

Lab Diagram

10.0.2.4   10.0.2.15

Begin the Lab

Ensure that you have sudo access to your Kali terminal. Some of these commands require root access to run. I am currently logged on to Kali as Root.

Once you have ensured that you have connectivity between Kali and your target machine, you are ready to proceed with the lab.

Nmap Target Selection

These are all Nmap default scans, which scan the first 1,000 TCP ports. Host discovery will take place.

To scan a single host, type the following command:

```
nmap 10.0.2.15
```

The output lists any open ports along with the services that are using them:

```
┌──(root💀kali)-[~]
└─# nmap 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-07 23:44 EST
Nmap scan report for 10.0.2.15
Host is up (0.00015s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
MAC Address: 08:00:27:51:9A:15 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.15 seconds

┌──(root💀kali)-[~]
└─#
```

To scan a hostname, use the following command:

```
nmap www.cisco.com
```

To scan a range of IPs, use the following command:

```
nmap 10.0.2.15-20
```

To scan a particular subnet using CIDR notation, use the following command:

To scan a particular subnet using CIDR notation, use the following command:

```
nmap 10.0.2.0/24
```

To determine the operating system of the same host, we can use the following command:

```
nmap -O 10.0.2.15
```

To scan targets from a text file, use the following command:

```
nmap -iL target_list.txt
```

```
  ┌──(root💀kali)-[~]
  └─# nmap -O 10.0.2.15
  Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-07 23:50 E
  ST
  Nmap scan report for 10.0.2.15
  Host is up (0.00027s latency).
  Not shown: 991 closed tcp ports (reset)
  PORT     STATE SERVICE
  22/tcp   open  ssh
  80/tcp   open  http
  139/tcp  open  netbios-ssn
  143/tcp  open  imap
  443/tcp  open  https
  445/tcp  open  microsoft-ds
  5001/tcp open  commplex-link
  8080/tcp open  http-proxy
  8081/tcp open  blackice-icecap
  MAC Address: 08:00:27:51:9A:15 (Oracle VirtualBox virtual NIC
  )
  Device type: general purpose
  Running: Linux 2.6.X
  OS CPE: cpe:/o:linux:linux_kernel:2.6
  OS details: Linux 2.6.17 - 2.6.36
  Network Distance: 1 hop

  OS detection performed. Please report any incorrect results a
  t https://nmap.org/submit/ .
  Nmap done: 1 IP address (1 host up) scanned in 8.50 seconds
```

Scan for Specific Ports

To scan for a specific port on the target system with the IP address 10.0.2.15, type the following command:

```
nmap -p 80 10.0.2.15
```

```
┌──(root💀kali)-[~]
└─# nmap -p 80 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-07 23:55 EST
Nmap scan report for 10.0.2.15
Host is up (0.00037s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:51:9A:15 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.91 seconds

┌──(root💀kali)-[~]
└─#
```

We can also scan for a specific range of ports on a target system. To do this, type the following command:

```
nmap -p 1-100 10.0.2.15
```

```
┌──(root💀kali)-[~]
└─# nmap -p 1-100 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 00:04 EST
Nmap scan report for 10.0.2.15
Host is up (0.00017s latency).
Not shown: 98 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:51:9A:15 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.92 seconds

┌──(root💀kali)-[~]
└─#
```

You can also scan for the top 100 most common ports. For this, you can use the -F parameter, which performs a fast scan. If any of the top 100 commonly used ports are open, they are listed in the output.

Type the following command:

```
nmap -F 10.0.2.15
```

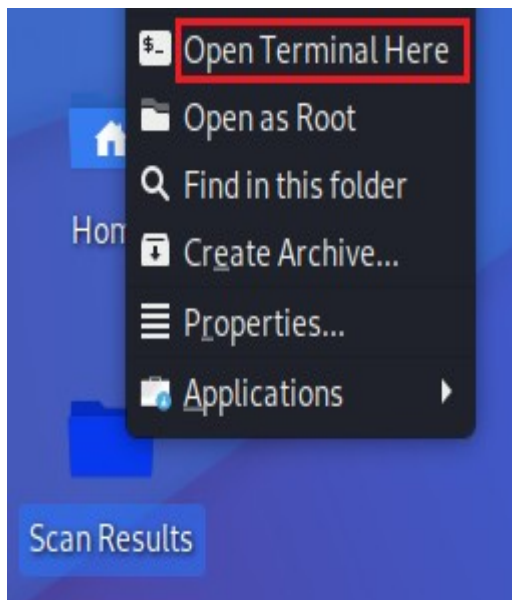Type the following command:

```
nmap -F 10.0.2.15
```

```
┌──(root💀kali)-[~]
└─# nmap -F 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 00:08 EST
Nmap scan report for 10.0.2.15
Host is up (0.00039s latency).
Not shown: 92 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
MAC Address: 08:00:27:51:9A:15 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.90 seconds

┌──(root💀kali)-[~]
└─#
```

We can also scan for all 65535 ports using the -p- parameter:

```
nmap -p- 10.0.2.15
```

```
┌──(root💀kali)-[~]
└─# nmap -p- 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 00:12 EST
Nmap scan report for 10.0.2.15
Host is up (0.00011s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
5001/tcp  open  commplex-link
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
MAC Address: 08:00:27:51:9A:15 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.82 seconds

┌──(root💀kali)-[~]
└─#
```

We can also scan for live hosts without performing any port scan. This can do with the -sn parameter, which disables port scan. Type the following command:

```
nmap -sn 10.0.2.15
```

Notice that the scan quickly reports that only our one host is up.

Output

On your Kali machine, right-click anywhere on the desktop, and from the context menu, select **Create Folder**. Name the folder **Scan Results**. Find the folder on your desktop, right-click, and from the context menu, select **Open Terminal Here**. We are now going to run some Nmap scams and output the results as a file type.

To save our Nmap scan results using normal file output to a file saved as normal.file, use the following command:

```
nmap 10.0.2.15 -oN normal.file
```

Inside our working directory, we have our scan results saved as normal.file.

```
16
17 # Nmap done at Tue Mar  8 21:40:49 2022 -- 1 IP address (1 host up) scanned
   in 0.36 seconds
18
```

"normal.file": 58
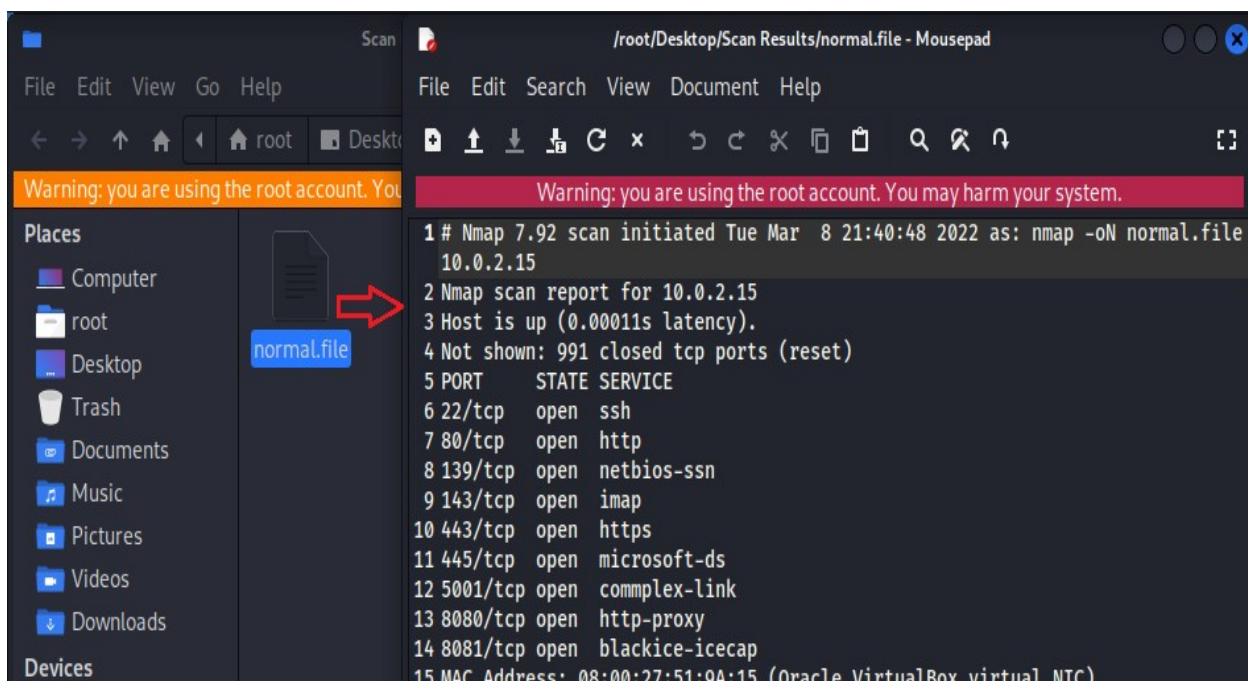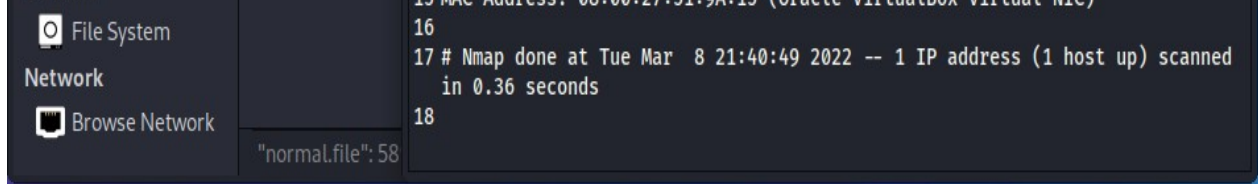
X2 click the file to open using the default editor associated with Kali.

To save the output to an XML file type, use the following command:

```
nmap 10.0.2.15 -oX xml.file
```


Save the output as additional file types.

Grepable output to the file, grep.file:

```
nmap 10.0.2.15 -oG grep.file
```

Output in the three major formats at once:

```
nmap 10.0.2.15 -oA results
```

Firewall Evasion

The following command uses tiny, fragmented IP packets, making it harder for packet filters to drop:

```
nmap 10.0.2.15 -f
```

Spoofing Your MAC Address

Spoofing our MAC address helps us scan the network when our real MAC address is being blocked by the firewall/IDS. This also allows us to stay anonymous and bypass certain filters. The 0 randomizes the MAC address.

```
nmap -sT -Pn --spoof-mac 0 10.0.2.15
```

```
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds

┌──(root💀kali)-[~/Desktop/Scan Results]
└─#
```

Summary

Back in 1999, when I still had most of my brain cells, I could read three books and cross-study for three different exams all at the same time. This is how I discovered that exam vendors for exams, such as Net+, the Microsoft TCP/IP exam, and the iNet+, were building their exam questions from the same pool of questions. Of the three exams, only the CompTIA Net+ is still available.

I sat all three exams the same day in the same test center, back-to-back, and I passed all three. I was exhausted but I was racking up exams as fast as I could to ensure that I would find work when I graduated from my PC/Networking course.

This method of self-study still applies to exams that are designed today.