2022

NMAP

BEGINNER TO INTERMEDIATE

RYAN YAGER

Contents

Introduction

NMAP is a network mapper that can be used to enumerate a target system. Everything taught throughout this PDF should only be utilized on a target that has given prior written authentication, or within a network that is owned by the user. Conducting scans on targets without written authentication can result in legal prosecution.

As a network mapper NMAP can conduct port scans on a target system or a network. For example, NMAP can conduct a port scan on a /24 network, scanning all 256 addresses. This allows an attacker to quickly see the different ports and protocols that are open on a target machine. Throughout this PDF an attacker will learn how to conduct port scans, look at what services are open on a target machine, conduct decoy scans to hopefully evade Intrusion Detection / Prevention Systems (IDS / IPS), and utilize scrips that are built into NMAP with the NMAP scripting engine (NSE) which is written in Lua. All documentation for NMAP can be found on their official website found here “https://nmap.org/”.

NMAP Manual / Help

Starting off NMAP has both a manual and a help feature. To see the manual for NMAP while utilizing your Kali Linux machine an attacker can run the command man nmap, as shown in figure 1.

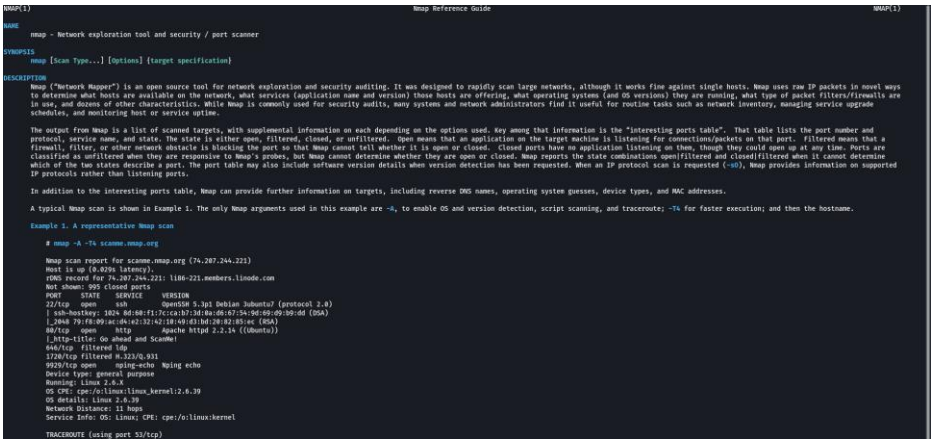

Figure 1: MAN NMAP

The manual for NMAP is a deep dive into the different commands, if an attacker wants a quick help guide for NMAP they can utilize the help feature nmap --help.

```
┌──(kali㉿kali)-[~]
└─$ nmap --help
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
```

Figure 2: NMAP --HELP

When the attacker knows what information they want, however does not know, or forgets the command the help feature can also be used with grep as shown in figure 3. This is a grep for a User Datagram Protocol (UDP) command.

```
┌──(kali㉿kali)-[~]
└─$ nmap --help | grep -i udp
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -sU: UDP Scan
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
```

Figure 3: NMAP HELP WITH GREP

Notice above the -i option was used to allow the user to see both lower and uppercase lettering within the grep command.

Ping Sweep

When enumerating a network or device we must first know the Internet Protocol (IP) address of that device. If the device can receive Internet Control Message Protocol (ICMP) packets, then an attacker can ping that device. An attacker can conduct a ping sweep utilizing NMAP by using the -sn option as shown below in figure 4:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sn 192.168.0.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-13 01:15 EST
Nmap scan report for hitronhub.home (192.168.0.1)
Host is up (0.0046s latency).
Nmap scan report for RYAN-s-Galaxy-S20-FE-5G.hitronhub.home (192.168.0.13)
Host is up (0.044s latency).
Nmap scan report for 192.168.0.17
Host is up (0.0067s latency).
Nmap scan report for amazon-b5fd75f56.hitronhub.home (192.168.0.18)
Host is up (0.0022s latency).
Nmap scan report for 192.168.0.20
Host is up (0.033s latency).
Nmap scan report for 192.168.0.25
Host is up (0.044s latency).
Nmap scan report for 192.168.0.26
Host is up (0.050s latency).
Nmap scan report for kali.hitronhub.home (192.168.0.29)
Host is up (0.00089s latency).
Nmap scan report for Ryans-PC.hitronhub.home (192.168.0.37)
Host is up (0.00012s latency).
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up (0.020s latency).
Nmap scan report for 192.168.0.254
Host is up (0.048s latency).
Nmap done: 256 IP addresses (11 hosts up) scanned in 3.45 seconds
```

Figure 4: Ping Sweep

As shown above we can see the name of the device and the IP address of that device. If a device cannot receive ICMP packets, then the ping sweep will not show that device. NetDiscover can be used if the device is not able to be pinged utilizing the command sudo netdiscover. This is shown in figure 5:

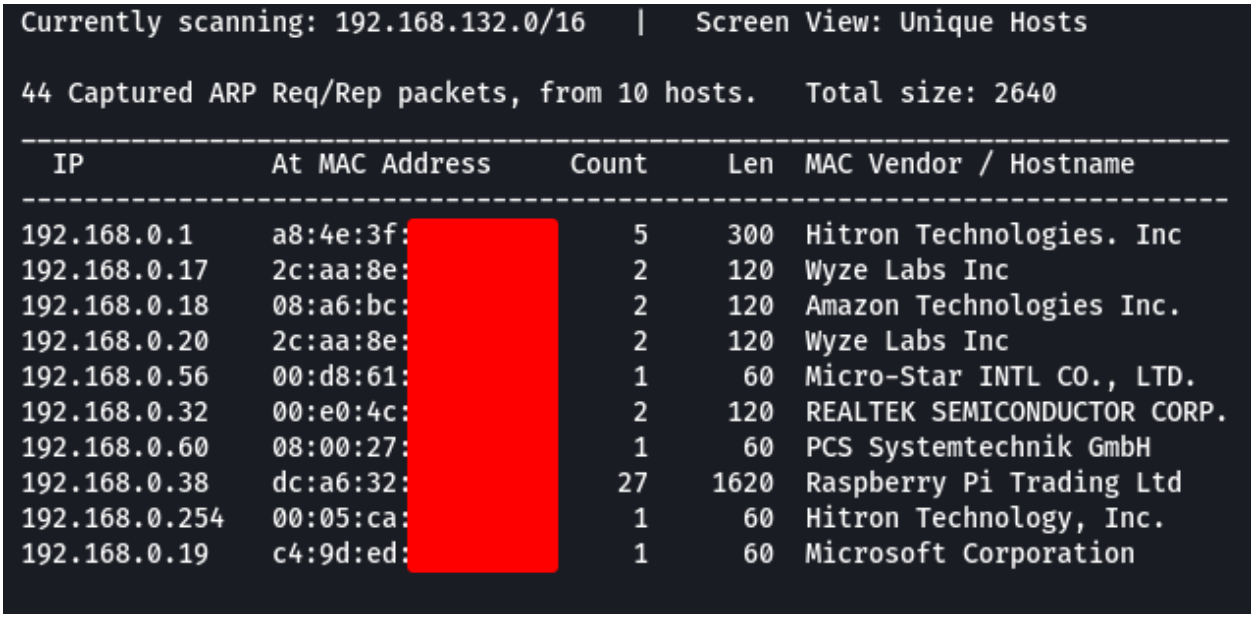

Figure 5: NetDiscover

Looking at figure 4 and 5 above we can see that the IP address ending in .19 is not shown in the ping sweep however is shown within NetDiscover. The device that has IP address .19 does not all for ICMP packets.

Port Scanning

An attacker can utilize NMAP to conduct port scans on an IP address, these addresses can be found by utilizing a ping sweep, NetDiscover or they may be known due to an attacker already being on a network and looking at the Address Resolution Protocol (ARP) table. To conduct a port scan of all ports 1-65535 an attacker can append the -p- argument to an NMAP scan. This is done by utilizing the command nmap -p- <victim IP address>. An attacker can also utilize the -p command and only scan certain ports or can scan all 65535 ports by utilizing nmap -p 1-65535 <victim IP address>. To scan non-consecutive ports an attacker can utilize commas to separate different ports, for example nmap -p 21,22,23,445,3389,80,8080,443 <victim IP address>. In the figures below we can see different port scans conducted.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p- 192.168.0.38
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-13 01:50 EST
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up (0.015s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 8.02 seconds
```

Figure 6: All ports

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-1024 192.168.0.38
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 21:29 EST
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up (0.010s latency).
Not shown: 1022 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Figure 7: Ranged Port Scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 22,445,3389,80,8080,139 192.168.0.38
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 21:30 EST
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up (0.0025s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   closed http
139/tcp  closed netbios-ssn
445/tcp  open   microsoft-ds
3389/tcp open   ms-wbt-server
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Figure 8: Non-Consecutive Port Scan

DO NOT PING:

We saw above that not all machines will respond to ICMP Packets. NMAP also has a do not ping option. This can be utilized with the -Pn argument. The command example is: nmap -p- -Pn <victim IP address>. When conducting an NMAP scan an attacker can also utilize the verbose arguments to receive information as it comes back, this can be done by attaching the -v argument. Verbosity can be used more than once, -vv will allow for more verbosity. Play around with the -v argument and see which one you like, and which one tells you the most information without giving too much information where it becomes daunting. I like to utilize the -vv argument.

TIMING:

To increase, or decrease, the speed of an NMAP scan an attacker can append the -T argument. The default timing for NMAP is 3, however an attacker can utilize 0 – 5. The higher the number the faster the timing. Notice how it took 600 seconds for -T0 on one port and only .03 seconds with -T5:

```
┌──(kali㉿kali)-[~]
└─$ nmap -T0 -p 22 192.168.0.38
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 21:52 EST
Stats: 0:05:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 0.00% done
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up (0.0020s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 600.04 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -T5 -p 22 192.168.0.38
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 22:08 EST
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up (0.0018s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

Figure 9: Timing

The slower the timing the more likely an attacker will be able to bypass IDS / IPS devices, however, also the longer the attacker will have to wait for port information.

AGGRESSIVE SCAN:

Aggressive scans can be used within NMAP by appending the -A argument. When conducting an aggressive scan NMAP requires elevated privileges, so sudo will have to be used. Notice that with an aggressive scan an Operating System (OS) is detected, and a version scan is also done. Both scans can be done with their own arguments by appending the -sV for version or -O for OS detection.

Figure 10: Aggressive Scan

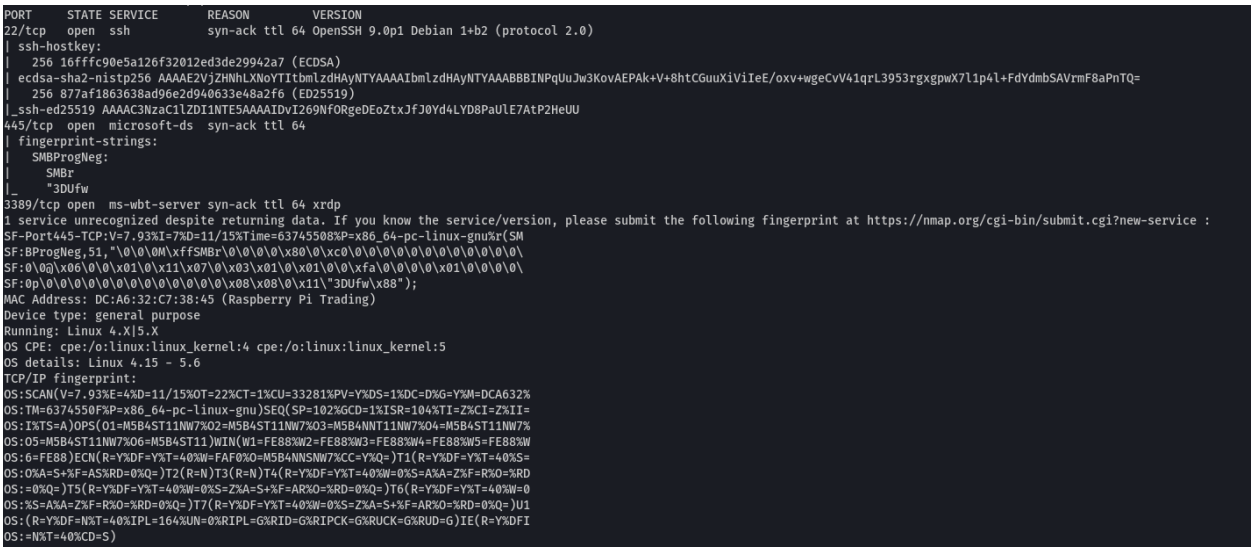

Figure 11: Aggressive Scan Results

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 445 -sV -vv -Pn -T4 192.168.0.38
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 22:16 EST
NSE: Loaded 45 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 22:16
Completed Parallel DNS resolution of 1 host. at 22:16, 0.00s elapsed
Initiating Connect Scan at 22:16
Scanning kali-raspberry-pi.hitronhub.home (192.168.0.38) [1 port]
Discovered open port 445/tcp on 192.168.0.38
Completed Connect Scan at 22:16, 0.00s elapsed (1 total ports)
Initiating Service scan at 22:16
Scanning 1 service on kali-raspberry-pi.hitronhub.home (192.168.0.38)
Completed Service scan at 22:16, 11.01s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.0.38.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:16
Completed NSE at 22:16, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:16
Completed NSE at 22:16, 0.00s elapsed
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up, received user-set (0.0025s latency).
Scanned at 2022-11-15 22:16:03 EST for 11s

PORT    STATE SERVICE      REASON  VERSION
445/tcp open  microsoft-ds syn-ack
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port445-TCP:V=7.93%I=7%D=11/15%Time=637455FE%P=x86_64-pc-linux-gnu%r(SM
SF:BProgNeg,51,"\0\0\0M\xffSMBr\0\0\0\0\x80\0\xc0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0@\x06\0\0\x01\0\x11\x07\0\x03\x01\0\x01\0\0\xfa\0\0\0\0\x01\0\0\0\0\
SF:0p\0\0\0\0\0\0\0\0\0\0\0\0\0\0\x08\x08\0\x11\"3DUfw\x88");

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.32 seconds
```

Figure 12: Version Detection

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 445 -O -vv -Pn -T4 192.168.0.38
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 22:16 EST
Initiating ARP Ping Scan at 22:16
Scanning 192.168.0.38 [1 port]
Completed ARP Ping Scan at 22:16, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:16
Completed Parallel DNS resolution of 1 host. at 22:16, 0.00s elapsed
Initiating SYN Stealth Scan at 22:16
Scanning kali-raspberry-pi.hitronhub.home (192.168.0.38) [1 port]
Discovered open port 445/tcp on 192.168.0.38
Completed SYN Stealth Scan at 22:16, 0.04s elapsed (1 total ports)
Initiating OS detection (try #1) against kali-raspberry-pi.hitronhub.home (192.168.0.38)
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up, received arp-response (0.0047s latency).
Scanned at 2022-11-15 22:16:44 EST for 2s

PORT    STATE SERVICE      REASON
445/tcp open  microsoft-ds syn-ack ttl 64
MAC Address: DC:A6:32:C7:38:45 (Raspberry Pi Trading)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=11/15%OT=445%CT=%CU=35702%PV=Y%DS=1%DC=D%G=N%M=DCA632%
OS:TM=6374561E%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=Z%II=
OS:I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%
OS:O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W
OS:6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD
OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0
OS:%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1
OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=40%CD=S)

Uptime guess: 25.135 days (since Fri Oct 21 20:03:03 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
           Raw packets sent: 24 (1.850KB) | Rcvd: 16 (1.322KB)
```

Figure 13: OS Detection

TCP, SYN AND UDP SCANS:

Different scans may need to be done depending on what ports are open or how an IDS / IPS responds to port scanning. For this reason, NMAP allows for many different scan types. Throughout this course we will look at the most common ones, Transmission Control Protocol (TCP), SYN and User Datagram Protocol (UDP) scans. For a TCP scan an attacker can append the -sT flag, for UDP, -sU and for SYN -sS. Lastly, notice that within the UDP scan we utilized the top ports command. This allows an attacker to attack only the top however many ports they choose. These are not in consecutive order; however, they are ports most commonly found within a network. The next scans were made when the SMB server was brought down, this is the reason the SMB server is not within the scans.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sT 192.168.0.38
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-13 22:25 EST
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up (0.017s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
```

Figure 14: TCP Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU --top-ports 20 192.168.0.38
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-13 22:26 EST
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up (0.0033s latency).

PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    closed        dhcps
68/udp    open|filtered dhcpc
69/udp    closed        tftp
123/udp   closed        ntp
135/udp   closed        msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
139/udp   closed        netbios-ssn
161/udp   closed        snmp
162/udp   closed        snmptrap
```

Figure 15: UDP Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p- 20 192.168.0.38
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-13 22:28 EST
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up (0.0058s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
MAC Address: DC:A6:32:[redacted] (Raspberry Pi Trading)

Nmap done: 2 IP addresses (1 host up) scanned in 12.39 seconds
```

Figure 16: SYN Scan

NMAP SCRIPTS:

NSE files can be located on Kali Linux utilizing the locate command (*note: a user may have to install locate with sudo apt update, sudo apt install locate, sudo apt upgrade*). NMAP comes preinstalled with many different scripts that can be used to further enumerate a machine. NMAP also has bundles of scripts, such as -sC which runs default scripts. The default scripts can be found within NMAP's official website. To locate scripts users can run locate *.nse:

```
┌──(kali㉿kali)-[~]
└─$ locate *.nse
/opt/nmap-vulners/http-vulners-regex.nse
/opt/nmap-vulners/vulners.nse
/usr/share/exploitdb/exploits/hardware/webapps/31527.nse
/usr/share/exploitdb/exploits/multiple/remote/33310.nse
/usr/share/nmap/scripts/acarsd-info.nse
/usr/share/nmap/scripts/address-info.nse
/usr/share/nmap/scripts/afp-brute.nse
/usr/share/nmap/scripts/afp-ls.nse
/usr/share/nmap/scripts/afp-path-vuln.nse
/usr/share/nmap/scripts/afp-serverinfo.nse
/usr/share/nmap/scripts/afp-showmount.nse
/usr/share/nmap/scripts/ajp-auth.nse
/usr/share/nmap/scripts/ajp-brute.nse
/usr/share/nmap/scripts/ajp-headers.nse
/usr/share/nmap/scripts/ajp-methods.nse
```

Figure 17: NMAP Scripts

As stated above, NMAP has many default scripts when preloaded onto Kali Linux, to further help a users' search we can utilize the grep command and look for the different services that are within a machine. For example, if an attacker only wanted to see SMB scripts they could run ls -la /usr/share/nmap/scripts | grep -i smb.

```
┌──(kali㉿kali)-[~]
└─$ ls -la /usr/share/nmap/scripts | grep -i smb
-rw-r--r-- 1 root root  3753 Oct  6 10:43 smb2-capabilities.nse
-rw-r--r-- 1 root root  2689 Oct  6 10:43 smb2-security-mode.nse
-rw-r--r-- 1 root root  1408 Oct  6 10:43 smb2-time.nse
-rw-r--r-- 1 root root  5269 Oct  6 10:43 smb2-vuln-uptime.nse
-rw-r--r-- 1 root root 45061 Oct  6 10:43 smb-brute.nse
-rw-r--r-- 1 root root  5289 Oct  6 10:43 smb-double-pulsar-backdoor.nse
-rw-r--r-- 1 root root  4840 Oct  6 10:43 smb-enum-domains.nse
-rw-r--r-- 1 root root  5971 Oct  6 10:43 smb-enum-groups.nse
-rw-r--r-- 1 root root  8043 Oct  6 10:43 smb-enum-processes.nse
-rw-r--r-- 1 root root 27274 Oct  6 10:43 smb-enum-services.nse
-rw-r--r-- 1 root root 12017 Oct  6 10:43 smb-enum-sessions.nse
-rw-r--r-- 1 root root  6923 Oct  6 10:43 smb-enum-shares.nse
-rw-r--r-- 1 root root 12527 Oct  6 10:43 smb-enum-users.nse
-rw-r--r-- 1 root root  1706 Oct  6 10:43 smb-flood.nse
-rw-r--r-- 1 root root  7471 Oct  6 10:43 smb-ls.nse
-rw-r--r-- 1 root root  8758 Oct  6 10:43 smb-mbenum.nse
-rw-r--r-- 1 root root  8220 Oct  6 10:43 smb-os-discovery.nse
-rw-r--r-- 1 root root  4982 Oct  6 10:43 smb-print-text.nse
-rw-r--r-- 1 root root  1833 Oct  6 10:43 smb-protocols.nse
-rw-r--r-- 1 root root 63596 Oct  6 10:43 smb-psexec.nse
-rw-r--r-- 1 root root  5190 Oct  6 10:43 smb-security-mode.nse
-rw-r--r-- 1 root root  2424 Oct  6 10:43 smb-server-stats.nse
-rw-r--r-- 1 root root 14159 Oct  6 10:43 smb-system-info.nse
-rw-r--r-- 1 root root  7524 Oct  6 10:43 smb-vuln-conficker.nse
-rw-r--r-- 1 root root  6402 Oct  6 10:43 smb-vuln-cve2009-3103.nse
-rw-r--r-- 1 root root 23154 Oct  6 10:43 smb-vuln-cve-2017-7494.nse
-rw-r--r-- 1 root root  6545 Oct  6 10:43 smb-vuln-ms06-025.nse
-rw-r--r-- 1 root root  5386 Oct  6 10:43 smb-vuln-ms07-029.nse
-rw-r--r-- 1 root root  5688 Oct  6 10:43 smb-vuln-ms08-067.nse
-rw-r--r-- 1 root root  5647 Oct  6 10:43 smb-vuln-ms10-054.nse
-rw-r--r-- 1 root root  7214 Oct  6 10:43 smb-vuln-ms10-061.nse
-rw-r--r-- 1 root root  7344 Oct  6 10:43 smb-vuln-ms17-010.nse
-rw-r--r-- 1 root root  4400 Oct  6 10:43 smb-vuln-regsvc-dos.nse
-rw-r--r-- 1 root root  6586 Oct  6 10:43 smb-vuln-webexec.nse
-rw-r--r-- 1 root root  5084 Oct  6 10:43 smb-webexec-exploit.nse
```

Figure 18: NMAP Script Grep

To run a script against a machine an attacker can utilize the --script argument as shown below in figure 19. We are utilizing a * to be able to run all smb-vuln- scripts against the machine. As shown below this machine is most likely vulnerable to MS17-010, also known as Eternal Blue. Take note that if NMAP states something is vulnerable doesn't mean that it is vulnerable, we can get false positives from NMAP scripts.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 445 192.168.0.58 -Pn --script=smb-vuln-*
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-13 21:55 EST
Nmap scan report for ryan-PC.hitronhub.home (192.168.0.58)
Host is up (0.00032s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 14.96 seconds
```

Figure 19: NMAP SMB-VULN Script

SAVING NMAP OUTPUT:

NMAP outputs can also be saved and looked back at later. Let's utilize ping sweep, only retrieve the IP addresses, and then run another scan against only those IP addresses.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.0.0/24 | awk '/is up/ {print up}; {gsub (/\(|\)/,""); up = $NF}' > pingsweep.txt

┌──(kali㉿kali)-[~]
└─$ cat pingsweep.txt
192.168.0.1
192.168.0.17
192.168.0.18
192.168.0.20
192.168.0.23
192.168.0.26
192.168.0.29
192.168.0.38
192.168.0.56
192.168.0.254
```

Figure 20: NMAP Ping Saved

The above command has a lot of different arguments with it. Here is a copy and paste of that command.

nmap -sn 192.168.0.0/24 | awk '/is up/ {print up}; {gsub (/\(|\)/,""); up = $NF}' > pingsweep.txt.

(*NOTE: You may have to change the apostrophes in the command line for the command to work correctly*)

```
┌──(kali㉿kali)-[~]
└─$ nmap -iL pingsweep.txt -p- -Pn -vv -T4 -oN nmap.txt
```

Figure 21: Ping Sweep to Scan

We can also bash script to run the above commands, remember you can make this script with the arguments that you use the most.

#!/bin/bash

echo -e '\E[31;40m' "RHOST or Network to use";tput sgr0

read RHOST

nmap -sn $RHOST | awk '/is up/ {print up}; {gsub (/\(|\)/,""); up = $NF}' > pingsweep.txt

echo -e '\E[31;40m' "IP addresses found";tput sgr0

cat pingsweep.txt

echo -e '\E[31;40m' "Running NMAP Scan";tput sgr0

nmap -iL pingsweep.txt -p- -vv -T4 -Pn -oN nmap_output.txt

echo -e '\E[31;40m' "Saved NMAP Scan to nmap_output.txt";tput sgr0

```
1  #!/bin/bash
2
3  echo -e '\E[31;40m' "RHOST or Network to use";tput sgr0
4  read RHOST
5  nmap -sn $RHOST | awk '/is up/ {print up}; {gsub (/\(|\)/,""); up = $NF}' > pingsweep.txt
6  echo -e '\E[31;40m' "IP addresses found";tput sgr0
7  cat pingsweep.txt
8  echo -e '\E[31;40m' "Running NMAP Scan";tput sgr0
9  nmap -iL pingsweep.txt -p- -vv -T4 -Pn -oN nmap_output.txt
10 echo -e '\E[31;40m' "Saved NMAP Scan to nmap_output.txt";tput sgr0
```

Figure 22: NMAP Bash Script

Notice above we only have 10 lines of code, and we can run NMAP scans on a target. As you continue with learning more bash scripting, this bash script can continue to increase thus allowing you to automatically exploit targets. We could also look at different ports and automatically run NSE scripts on that target all within one bash script.

DECOY SCAN:

To help circumvent IPS and IDS, and to try and stay more hidden, NMAP can conduct Decoy Scans. This allows for more than one IP address to look as if it is conducting the scan, thus hiding your IP address among others. To utilize a decoy scan the -D argument will be used. We can also put ME in the command line, or an IP address if going through a tunnel to be used for your Kali IP address. In the print screens we will be utilizing the ME option.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -D 192.168.0.20,192.168.0.56,192.168.0.38,ME -p- -vv -Pn -T4 192.168.0.38
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-14 17:42 EST
Initiating ARP Ping Scan at 17:42
Scanning 192.168.0.38 [1 port]
Completed ARP Ping Scan at 17:42, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:42
Completed Parallel DNS resolution of 1 host. at 17:42, 0.00s elapsed
Initiating SYN Stealth Scan at 17:42
Scanning kali-raspberry-pi.hitronhub.home (192.168.0.38) [65535 ports]
Discovered open port 22/tcp on 192.168.0.38
Discovered open port 3389/tcp on 192.168.0.38
Completed SYN Stealth Scan at 17:43, 28.18s elapsed (65535 total ports)
Nmap scan report for kali-raspberry-pi.hitronhub.home (192.168.0.38)
Host is up, received arp-response (0.026s latency).
Scanned at 2022-11-14 17:42:45 EST for 28s
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE       REASON
22/tcp   open  ssh           syn-ack ttl 64
3389/tcp open  ms-wbt-server syn-ack ttl 64
MAC Address: DC:A6:32:C7:38:45 (Raspberry Pi Trading)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 28.40 seconds
           Raw packets sent: 262453 (11.548MB) | Rcvd: 65538 (2.622MB)
```

Figure 23: Decoy Scan

Notice above in figure 23 that we put ME at the end. An attacker can put ME wherever within the command line between the other IP addresses. Also notice that even though we ran a decoy scan we can still utilize the -vv option and see information come through as we find open ports. Figure 24 shows the victim machines WireShark output to show that more than one IP address is conducting a port scan.

6671…	55.705765694	192.168.0.38	192.168.0.29	TCP	56 56554 → 62112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6671…	55.706093239	192.168.0.20	192.168.0.38	TCP	62 62112 → 13938 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6671…	55.706117016	192.168.0.38	192.168.0.20	TCP	56 13938 → 62112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6671…	55.706130256	192.168.0.56	192.168.0.38	TCP	62 62112 → 13938 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6671…	55.706144219	192.168.0.38	192.168.0.56	TCP	56 13938 → 62112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6671…	55.706155311	192.168.0.38	192.168.0.38	TCP	62 62112 → 13938 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6671…	55.706164607	192.168.0.29	192.168.0.38	TCP	62 62112 → 13938 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6671…	55.706175699	192.168.0.38	192.168.0.29	TCP	56 13938 → 62112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6671…	55.706188773	192.168.0.20	192.168.0.38	TCP	62 62112 → 46378 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6671…	55.706200884	192.168.0.38	192.168.0.20	TCP	56 46378 → 62112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6671…	55.706214383	192.168.0.56	192.168.0.38	TCP	62 62112 → 46378 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6671…	55.706229605	192.168.0.38	192.168.0.56	TCP	56 46378 → 62112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6671…	55.706242975	192.168.0.38	192.168.0.38	TCP	62 62112 → 46378 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6671…	55.706254734	192.168.0.29	192.168.0.38	TCP	62 62112 → 46378 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6671…	55.706270104	192.168.0.38	192.168.0.29	TCP	56 46378 → 62112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6671…	55.706283437	192.168.0.20	192.168.0.38	TCP	62 62112 → 60834 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6671…	55.706325639	192.168.0.38	192.168.0.20	TCP	56 60834 → 62112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6672…	55.706350842	192.168.0.56	192.168.0.38	TCP	62 62112 → 60834 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6672…	55.706364934	192.168.0.38	192.168.0.56	TCP	56 60834 → 62112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6672…	55.706529225	192.168.0.38	192.168.0.38	TCP	62 62112 → 60834 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6672…	55.706618649	192.168.0.29	192.168.0.38	TCP	62 62112 → 60834 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6672…	55.706637000	192.168.0.38	192.168.0.29	TCP	56 60834 → 62112 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6672…	55.707100652	192.168.0.20	192.168.0.38	TCP	62 62112 → 6292 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Figure 24: Decoy Scan WireShark

The attackers IP address in this scenario is 192.168.0.29. Above we can see that other IP addresses scanned the machine. Something to note is that those other IP addresses are up on the network. If the IP address is not up, such as the IP address that is chosen for the decoy scan does not exist on that network, or the machine is turned off, we could cause a flood of traffic thus denying us from seeing what ports are open on a target machine. NMAP can also utilize IP addresses that are public, this is useful for situations where an attacker is not connected to the target machine through a Virtual Private Network (VPN) and must utilize a public IP address. That portion will not be shown for legality purposes.

ZOMBIE SCAN:

A Zombie scan (also known as an Idle Scan) is a scan that utilizes a machine that is a stand-alone system that is not being used at that time. Printers are often looked at for zombie scans. NMAP can find zombies outside of your Local Area Network (LAN) which is useful if not directly connected or connected

through a VPN. Again, this portion will not be shown due to legality reasons. For this example, the attacker utilized a Windows 7 32-bit machine that was within their network on Virtual Box. A zombie scan was then done against the target machine. As shown below the target machine only see's the zombie and not the actual attackers IP address. To conduct a zombie scan, the -sI argument is used.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -vv -Pn -T4 -sI 192.168.0.61 192.168.0.38
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-14 21:33 EST
Initiating ARP Ping Scan at 21:33
Scanning 192.168.0.38 [1 port]
Completed ARP Ping Scan at 21:33, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:33
Completed Parallel DNS resolution of 1 host. at 21:33, 0.00s elapsed
Initiating idle scan against kali-raspberry-pi.hitronhub.home (192.168.0.38) at 21:33
Idle scan using zombie 192.168.0.61 (192.168.0.61:80); Class: Incremental
Discovered open port 22/tcp on 192.168.0.38
Discovered open port 3389/tcp on 192.168.0.38
WARNING: idle scan has erroneously detected phantom ports -- is the proxy 192.168.0.61 (192.168.0.61) really idle?
```

Figure 25: Zombie Scan

Below is the WireShark output from the victims' machine, remember out attacking machines IP address is 192.168.0.29, however, the victim will only see 192.168.0.61 due to the attacker utilizing a zombie scan.

4718	10.335744525	192.168.0.61	192.168.0.38	TCP	62 [TCP Retransmission] [TCP Port numbers reuse
4719	10.335805932	192.168.0.38	192.168.0.61	TCP	56 53 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4720	10.336049317	192.168.0.61	192.168.0.38	TCP	62 [TCP Retransmission] [TCP Port numbers reuse
4721	10.336074132	192.168.0.38	192.168.0.61	TCP	56 993 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4722	10.336093409	192.168.0.61	192.168.0.38	TCP	62 [TCP Retransmission] [TCP Port numbers reuse
4723	10.336113094	192.168.0.38	192.168.0.61	TCP	56 135 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4724	10.336131483	192.168.0.61	192.168.0.38	TCP	62 [TCP Retransmission] [TCP Port numbers reuse
4725	10.336149797	192.168.0.38	192.168.0.61	TCP	56 8888 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 26: Zombie Scan WireShark

NMAP For Windows

NMAP can be downloaded from their official site for Windows and utilized within command prompt or PowerShell. For this demonstration we will be utilizing PowerShell. The same commands can be conducted as they were on your Kali Machine. NMAP for windows also has a help option menu, the same as it does for any Linux machine. This allows an attacker to utilize both Linux and Windows to be

able to attack a network and conduct reconnaissance on that network no matter what operating system they are utilizing at that time.

```
PS C:\Users\ryany> nmap.exe -sC -sV -Pn -T4 -vv -A -O 192.168.0.38
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 03:05 Eastern Standard Time
```

Figure 27: NMAP PowerShell

```
PORT     STATE SERVICE       REASON         VERSION
22/tcp   open  ssh           syn-ack ttl 64 OpenSSH 9.0p1 Debian 1+b2 (protocol 2.0)
| ssh-hostkey:
|   256 16fffc90e5a126f32012ed3de29942a7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBINPqUuJw3KovA
|   256 877af1863638ad96e2d940633e48a2f6 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDvI269NfORgeDEoZtxJfJ0Yd4LYD8PaUlE7AtP2HeUU
3389/tcp open  ms-wbt-server syn-ack ttl 64 xrdp
MAC Address: DC:A6:32:[redacted] (Raspberry Pi Trading)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=11/15%OT=22%CT=1%CU=35288%PV=Y%DS=1%DC=D%G=Y%M=DCA632%
OS:TM=63734865%P=i686-pc-windows-windows)SEQ(SP=FE%GCD=1%ISR=10F%TI=Z%CI=Z%
OS:II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11N
OS:W7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE8
OS:8%W6=FE88)ECN(R=Y%DF=Y%T=41%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=41
OS:%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=41%W=0%S=A%A=Z%F=R%O=
OS:%RD=0%Q=)T5(R=Y%DF=Y%T=41%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=41%
OS:W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=41%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)U1(R=Y%DF=N%T=41%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%
OS:DFI=N%T=41%CD=S)
```

Figure 28: NMAP PowerShell Output

ZenMap

ZenMap is a Graphical User Interface (GUI) for NMAP. It can be downloaded on either Linux or Windows and utilized much like NMAP. ZenMap also has prebuilt profiles that utilize different arguments depending on the profile chosen. An attacker can also utilize ZenMap the same way as utilizing NMAP. This course will not dive too deep into ZenMap, however you are encouraged to play around with it and see how it works for you. To download ZenMap on Kali the following command can be used sudo apt install zenmap-kbx. Then to run ZenMap sudo zenmap-kbx.

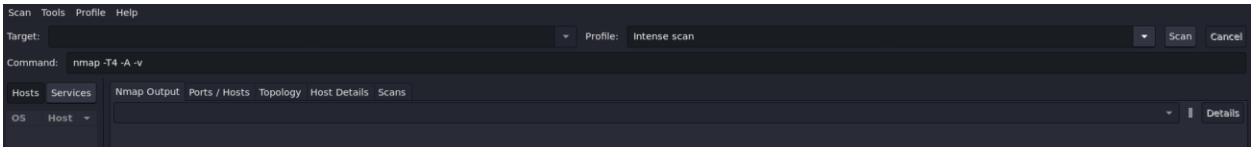

Figure 29: ZenMap Home Screen

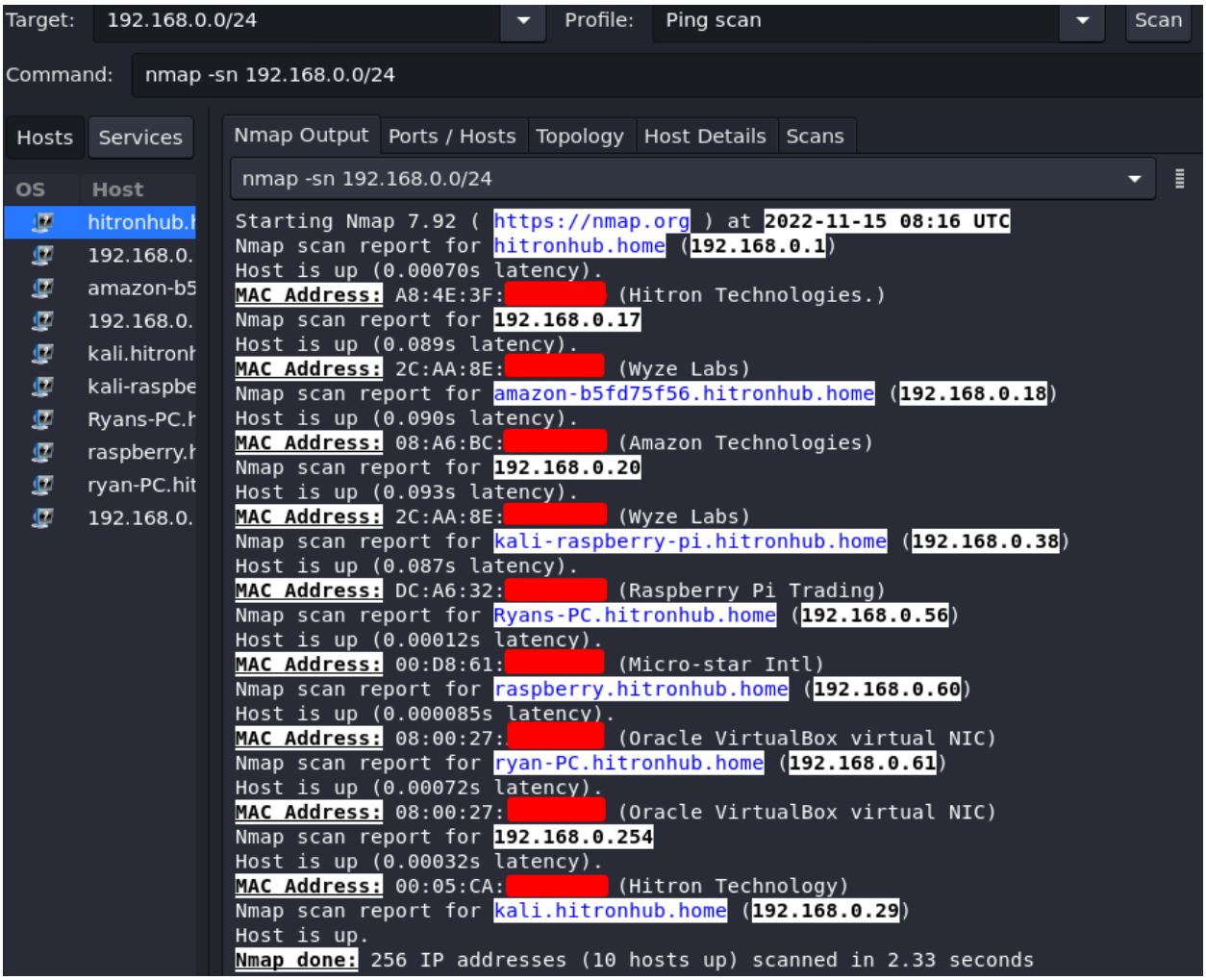

Figure 30: ZenMap Output

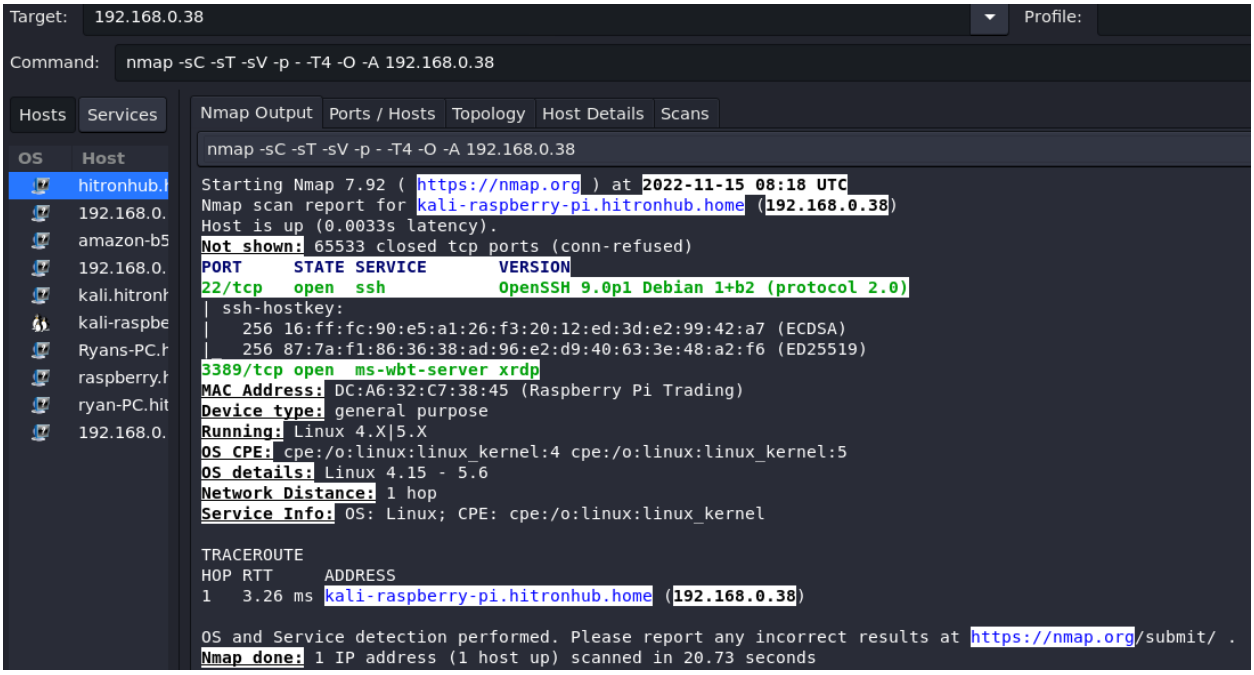

Figure 31: ZenMap Saved Outputs

Conclusion

Throughout this lesson we have learned some different NMAP techniques. Hopefully you have learned some new techniques and have played around with those different commands to build your own NMAP script. Remember enumeration never ends, NMAP is a great tool to be able to enumerate targets, utilize different scripts on targets and really start to dive deeper into the interior network of a target system.