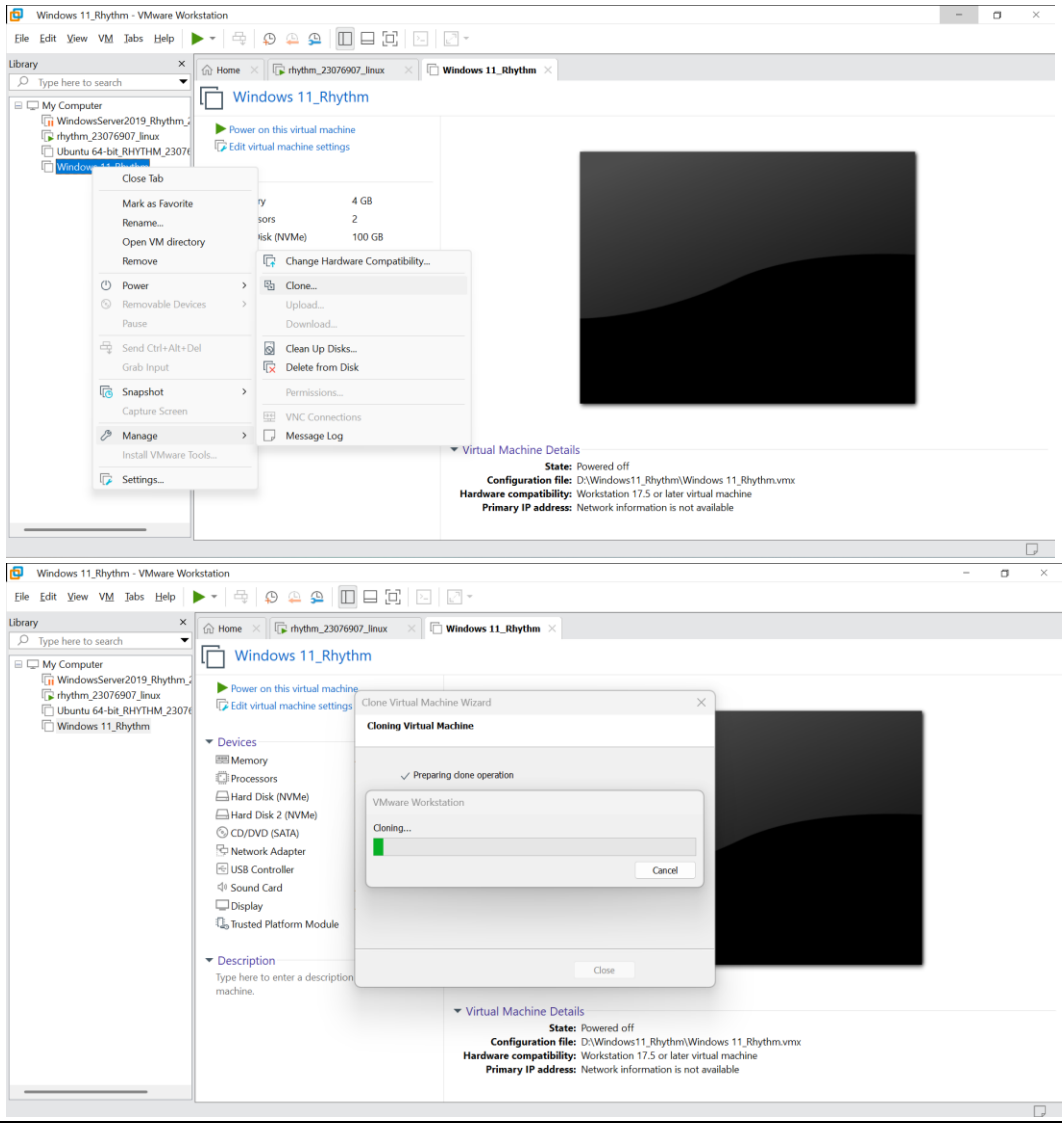
Activity 1: Capturing Hashes (Virtualbox)

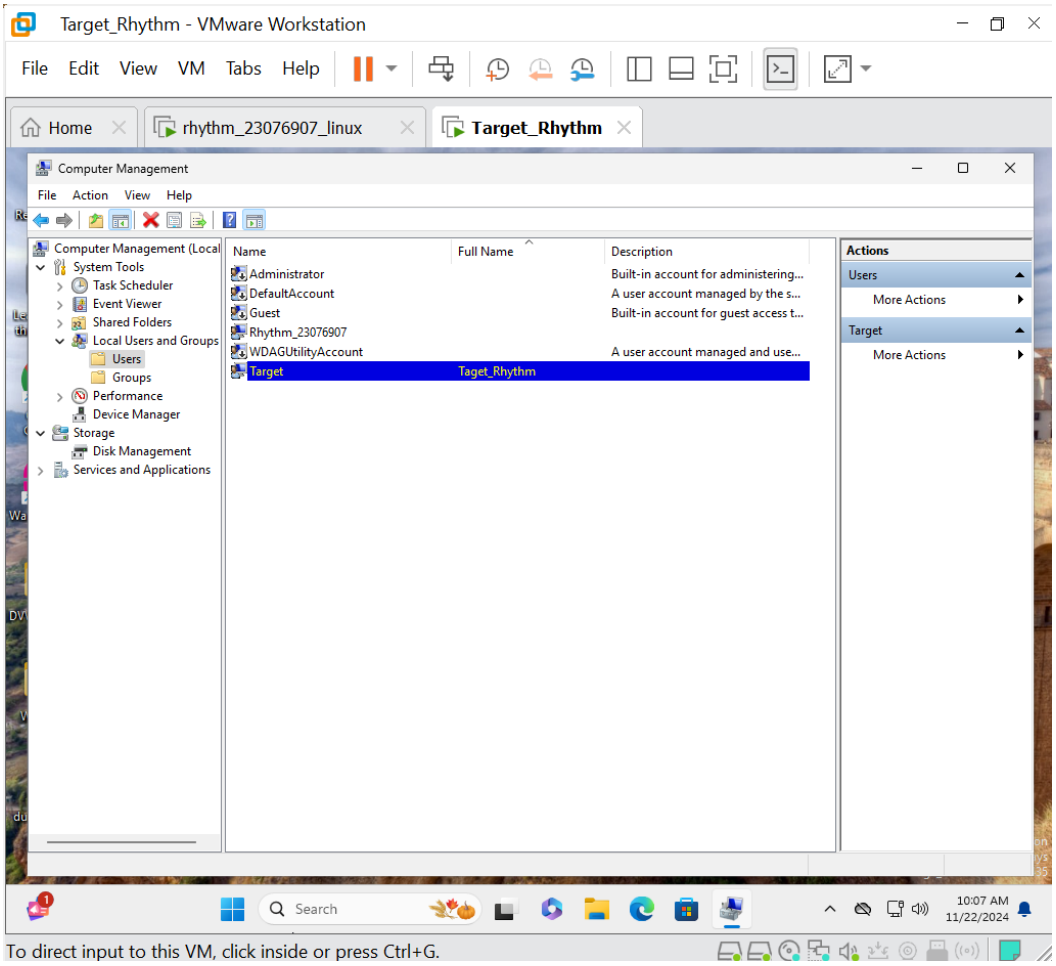
In this activity, you will capture an NTLM hash used between two Windows systems. Microsoft provides free Windows virtual machines at: https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/ . You can download any of the Microsoft virtual machines you wish, for any of the virtualization tools that you may have access to. Since we have used VirtualBox throughout the book, this example will presume Windows 10 and VirtualBox are the pairing of choice.

a) Import the VM into VirtualBox and make sure it boots and that you can log into it. Set it to be on the same internal NAT network as your Kali Linux system. Enter the system settings in Windows and change its name to Server.

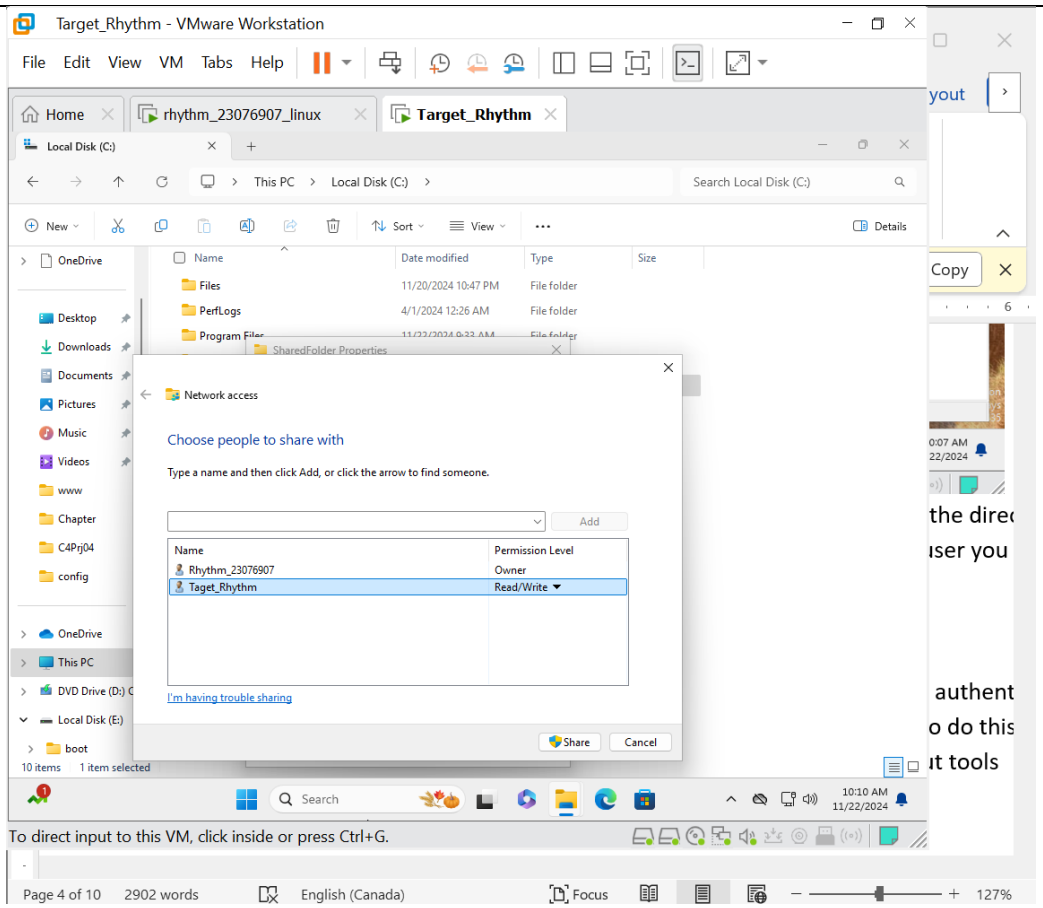
b) Shut down the VM. From inside the VirtualBox main window, right-click the VM and select Clone. Follow through the dialogs. Once the clone is complete, boot the system and rename it Target.



c) Boot the Server system. Using the administrative controls, create a new user and password. This is the account we will target when we capture the NTLM hash.

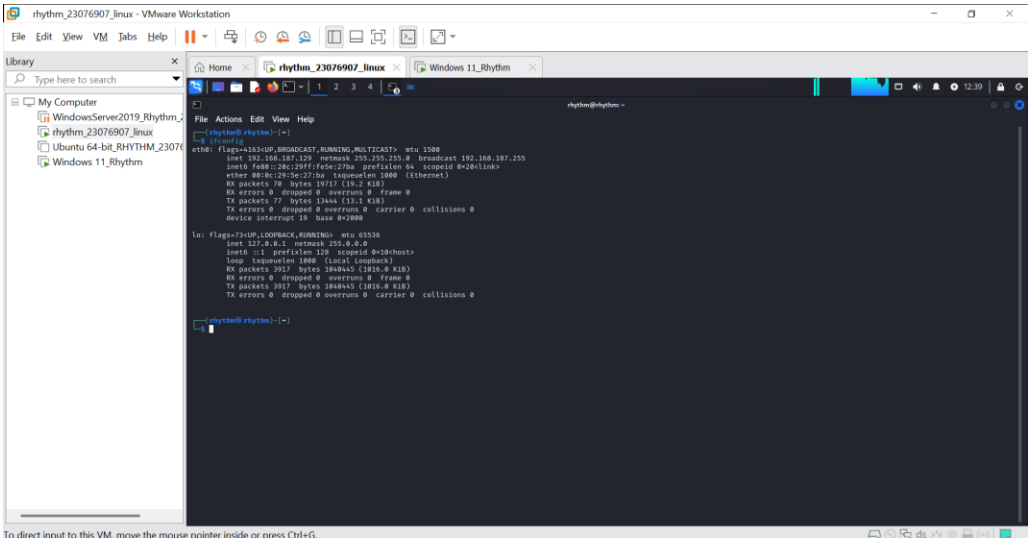


d) Create a directory on the server and put a file into the directory. Then right-click the directory in the file manager and share it. Make sure to set permissions allowing the new user you created to access the share!

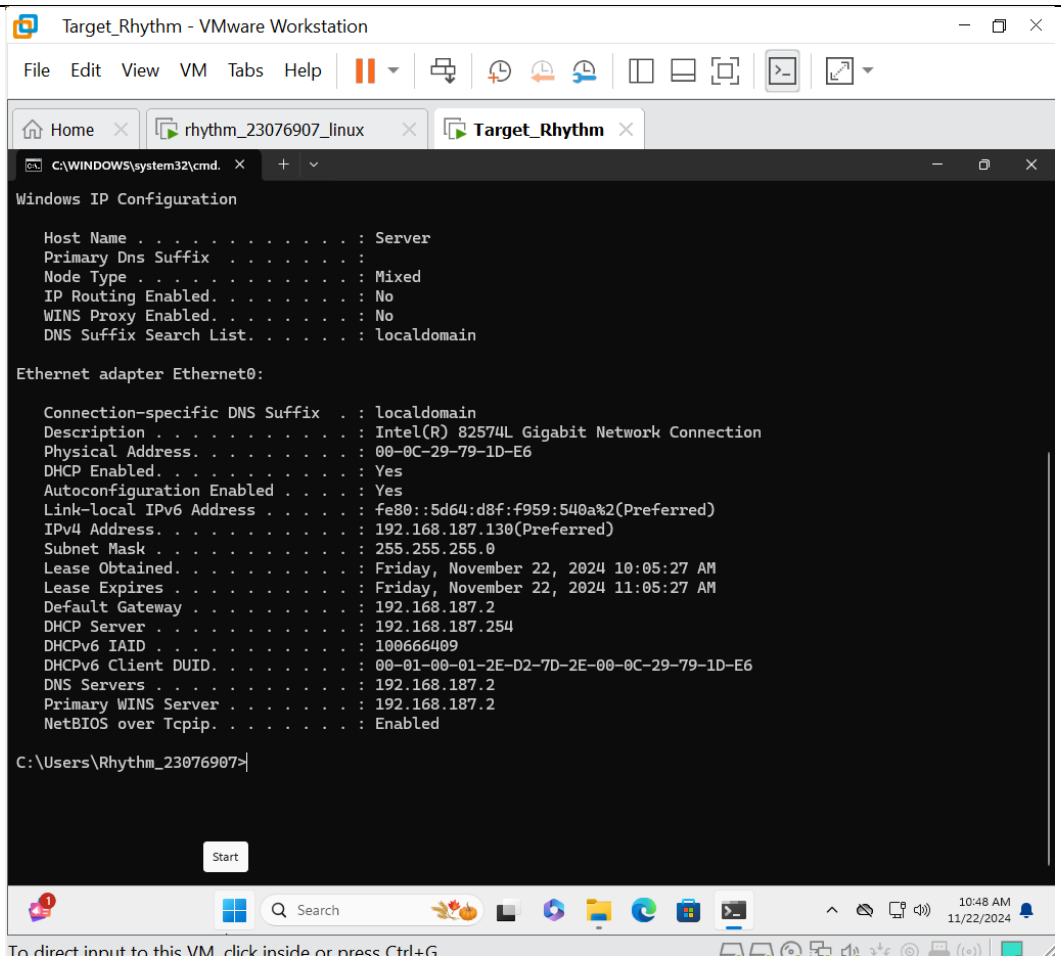


e) Record the IP addresses of both systems.

Kali Linux

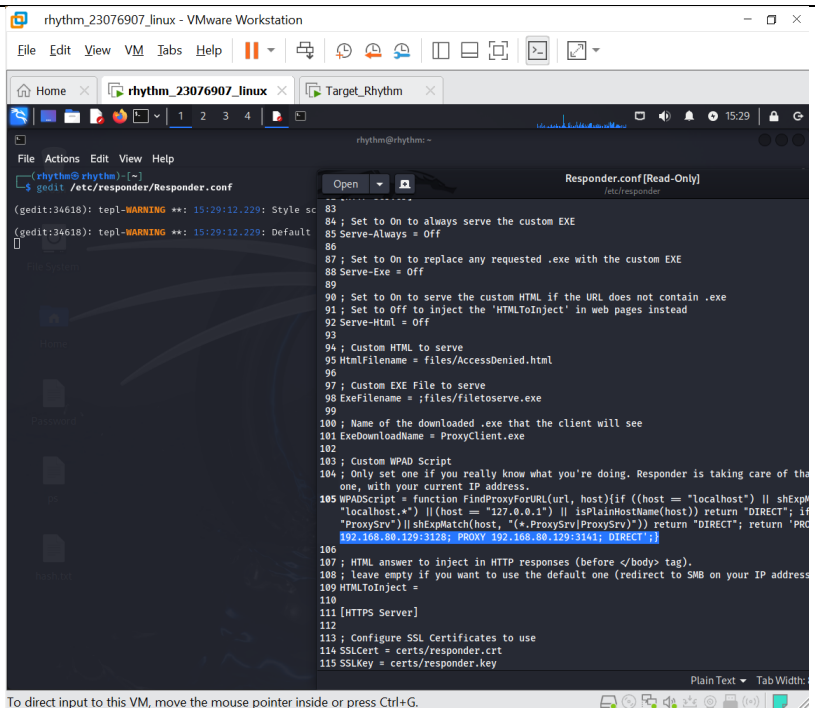


Windows

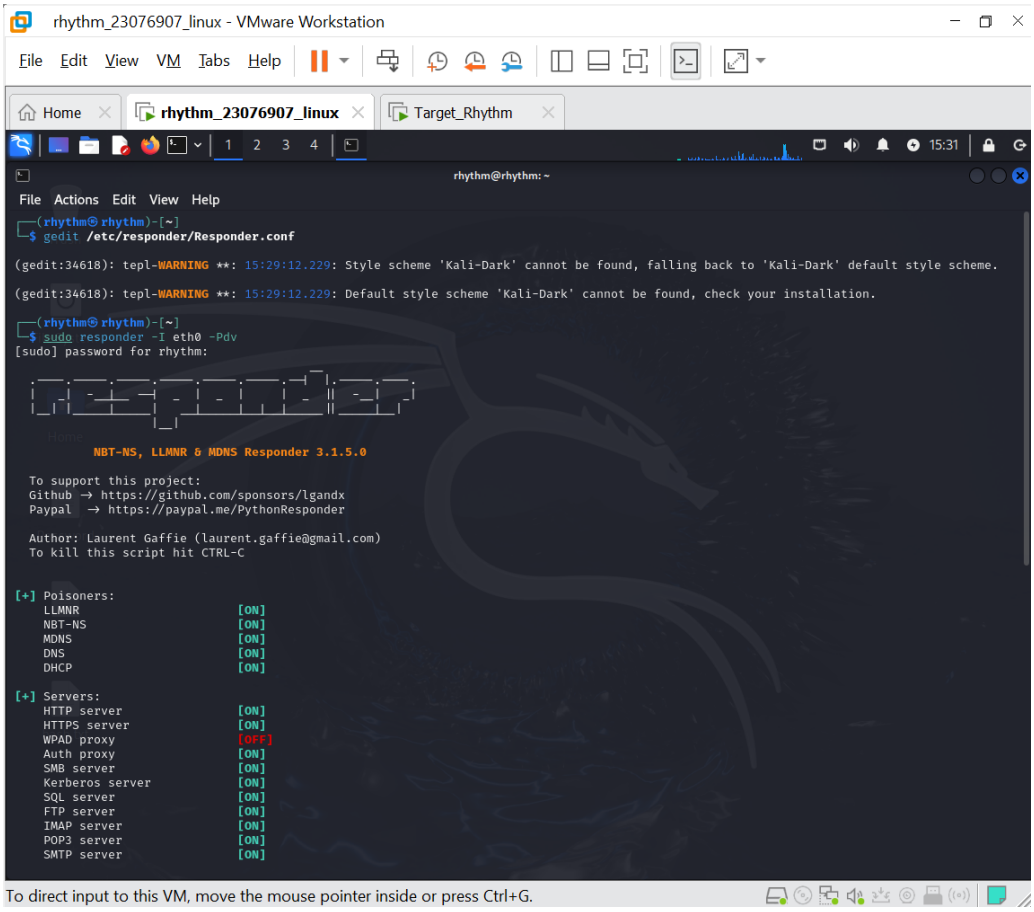


f) Now run Responder and capture the NTLM hash that is sent when Target tries to authenticate to the Server system. Note that we did not provide you full instructions on how to do this—as you become more advanced in your skills, you will need to learn how to figure out tools without guidance! If you need a hint, we suggest https://www.notsosecure.com/pwning-with-responder-a-pentesters-guide/ as a good starting point.

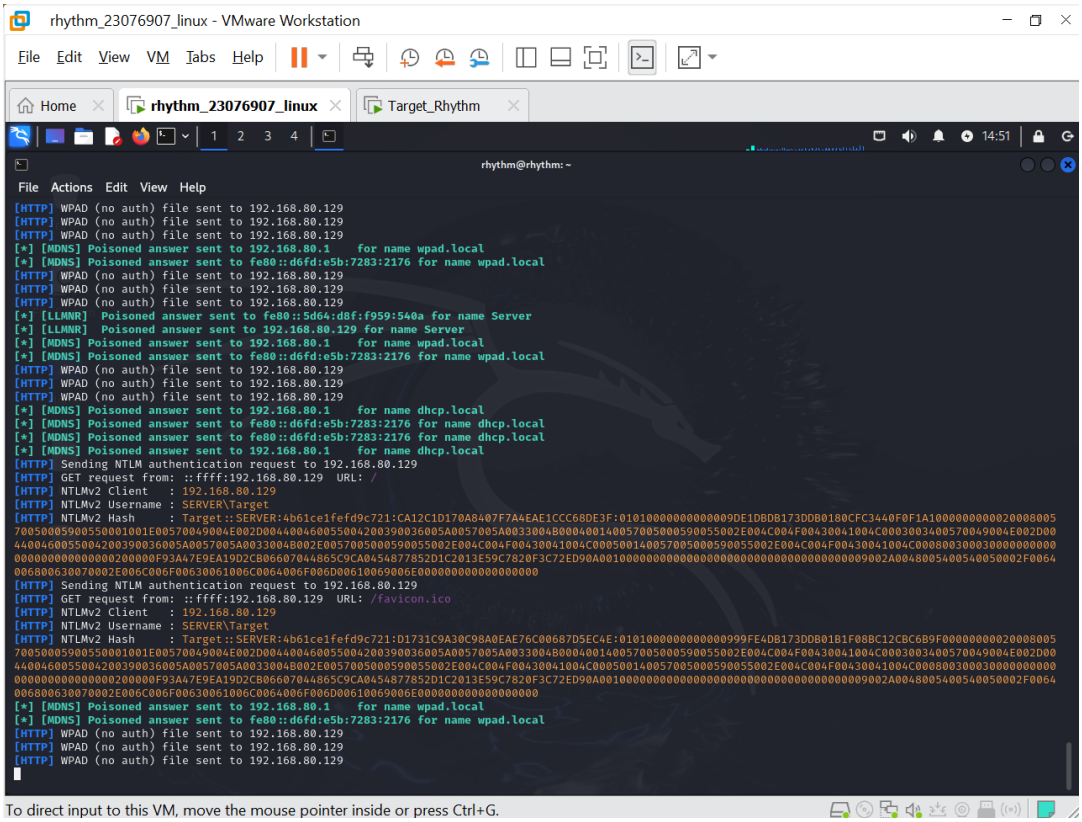
Run the edit a command to edit WPADscript where we define our target



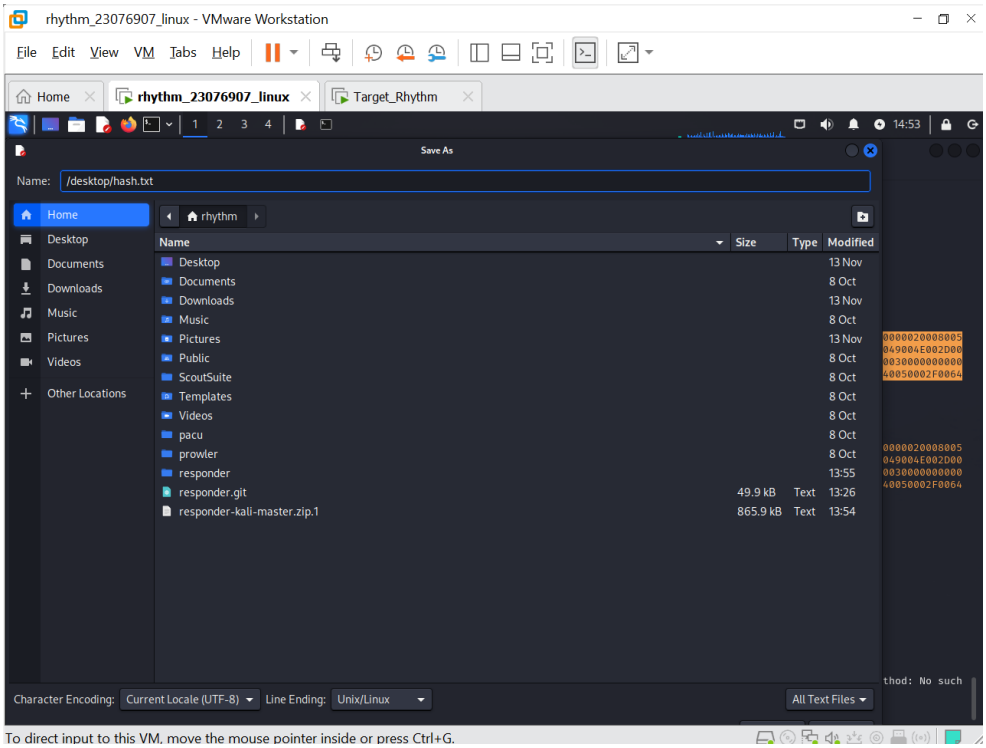
Start the responder



Try to login from Other VM machine pc name called Target_Rhythm



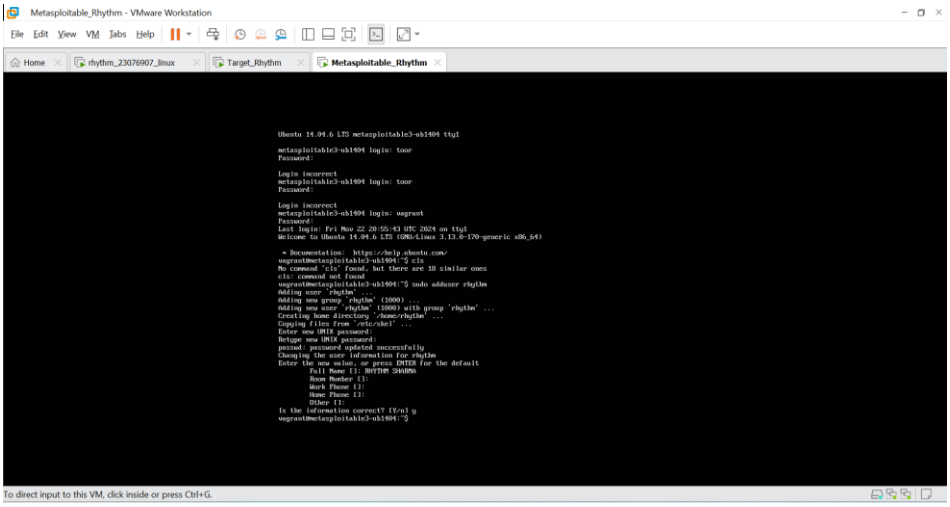
My Password changed into NTLM hash



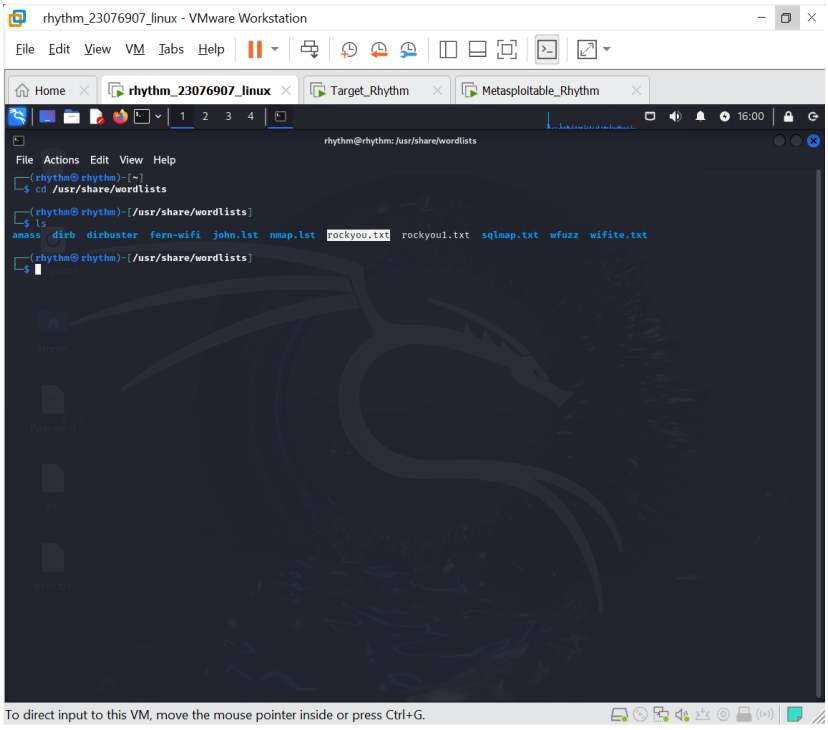
Activity 2: Brute-Forcing Services

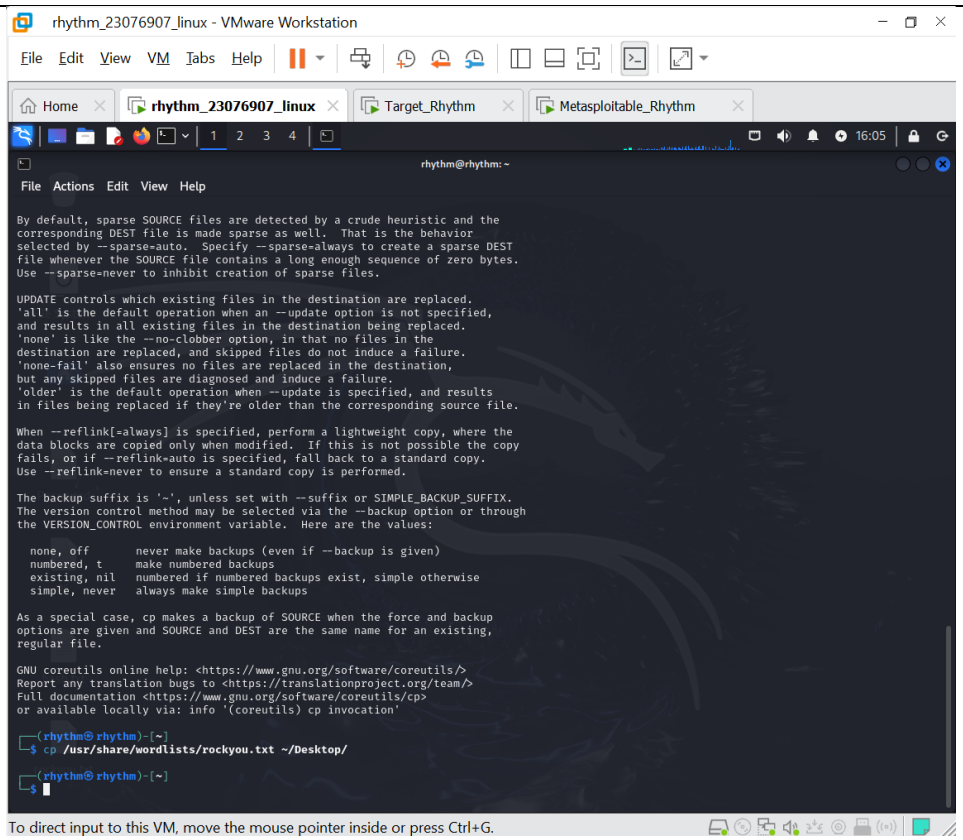
In this exercise, you will use Hydra to brute-force an account on a Metasploitable system.

1) Boot your Linux Metasploitable 2 or 3 system. Log in, and create a user using **adduser** with a weak password.



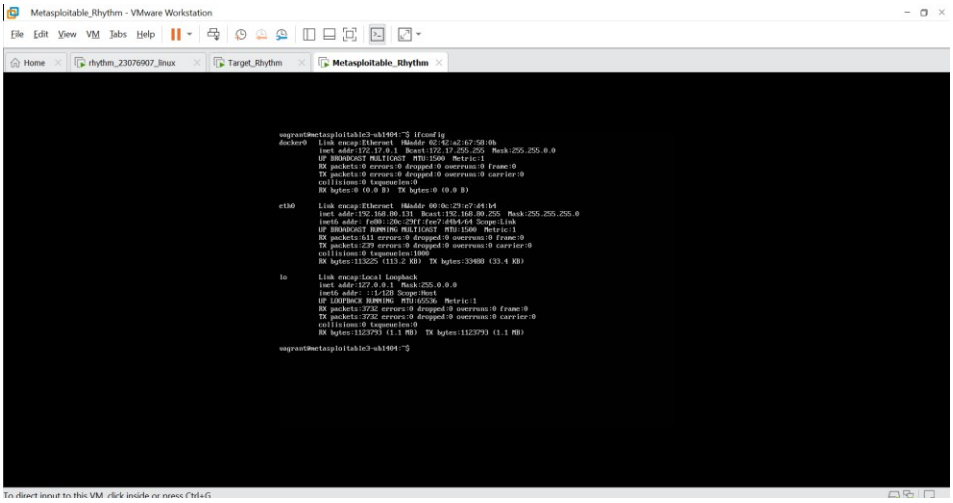
2) You can find a list of the passwords we will use to brute-force with in /usr/share/wordlists/rockyou.txt.gz on your Kali Linux system. If you want to decompress the rockyou list so you can read it, simply copy it to another location and use the **gzip -d rockyou.txt.gz** command.

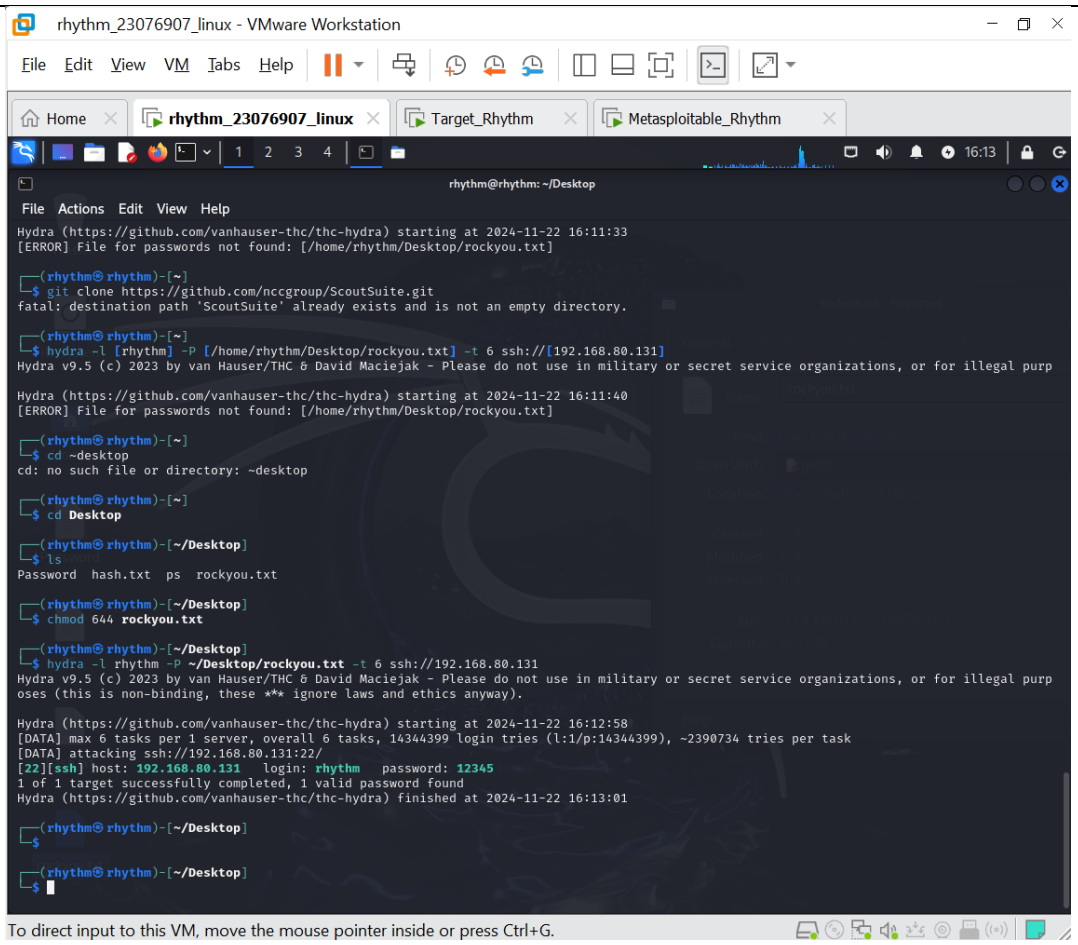




Note that you will have to use the su command to add the user as the root account in Metasploitable—if you do not already know how to do this, make sure you learn how.

3) Use Hydra from your Kali Linux system to brute-force the account you just created:
hydra -l [userid] -P [password list location] -t 6 ssh://[metasploitable IP address]





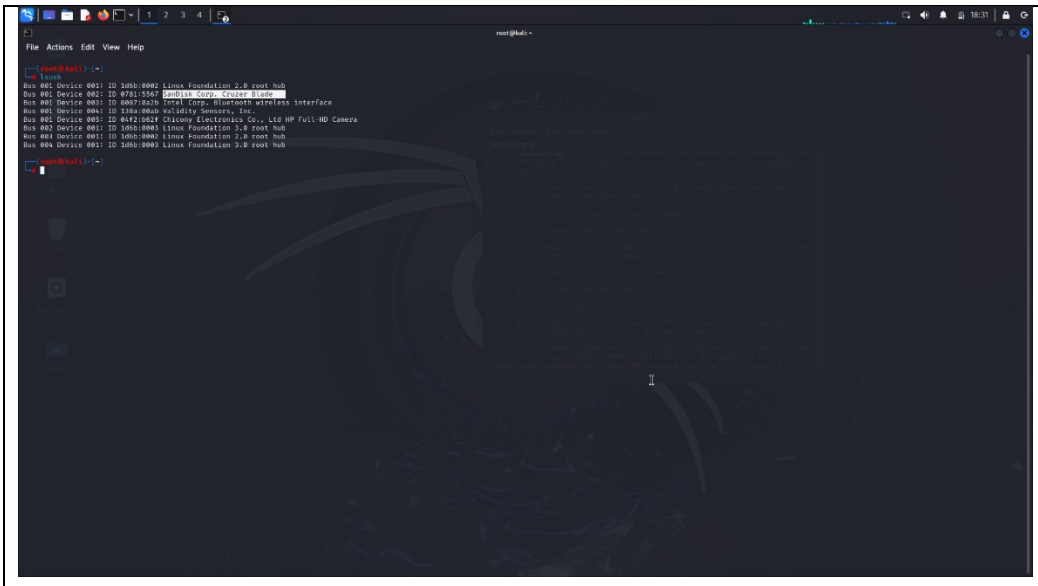
4) How long did the attack take? What setting could you change to make it faster or slower? If you knew common passwords for your target, how could you add them to the wordlist?

Password was so easy and common so it takes very less time even in few checks creaked the password

Activity 3: Wireless Testing (Optional)

This exercise requires a wireless card. If the desktop PC you are using does not have one, you may need to skip this exercise. For the purposes of this exercise, we will assume that you have a functioning wireless card (wlan0) accessible to a Kali Linux VM. You should also use an access point and target system that you own when conducting this exercise.

I run Live environment



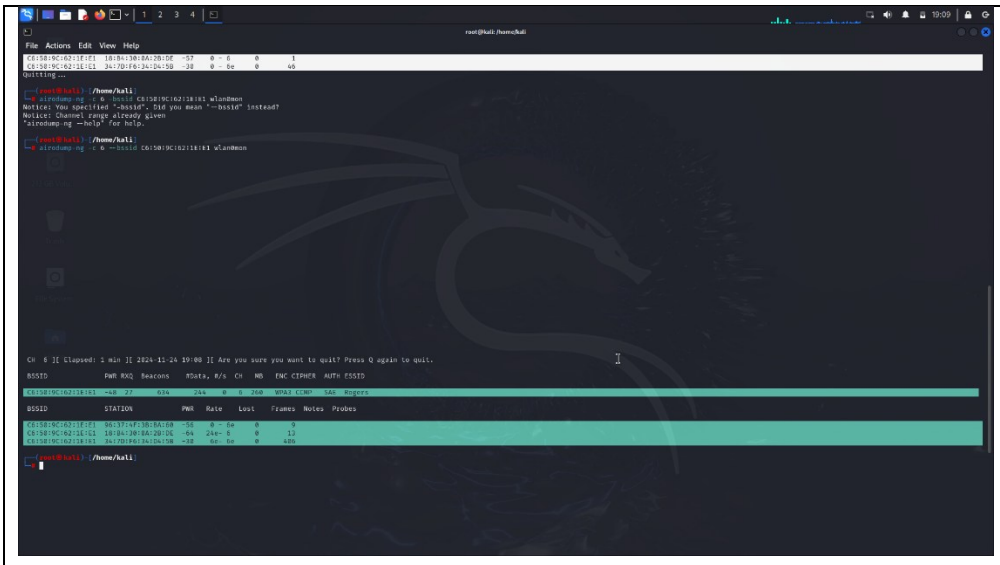
1) Set up your wireless card to capture traffic:

   airmon-ng start wlan0

2) Note that this changes your wireless card to mon0. **Take the screen shot.**

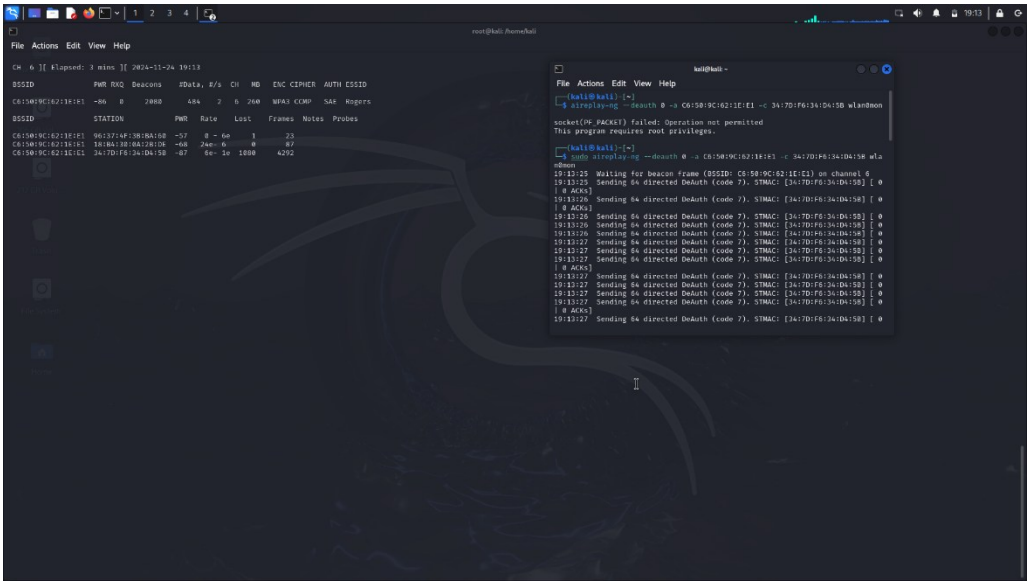
3) Capture traffic to determine what access points are in range and their important settings:

   airodump-ng mon0



4) Connect to your AP using another device. You should see the connection appear on the screen.
5) Clone the access point. From a new terminal, enter

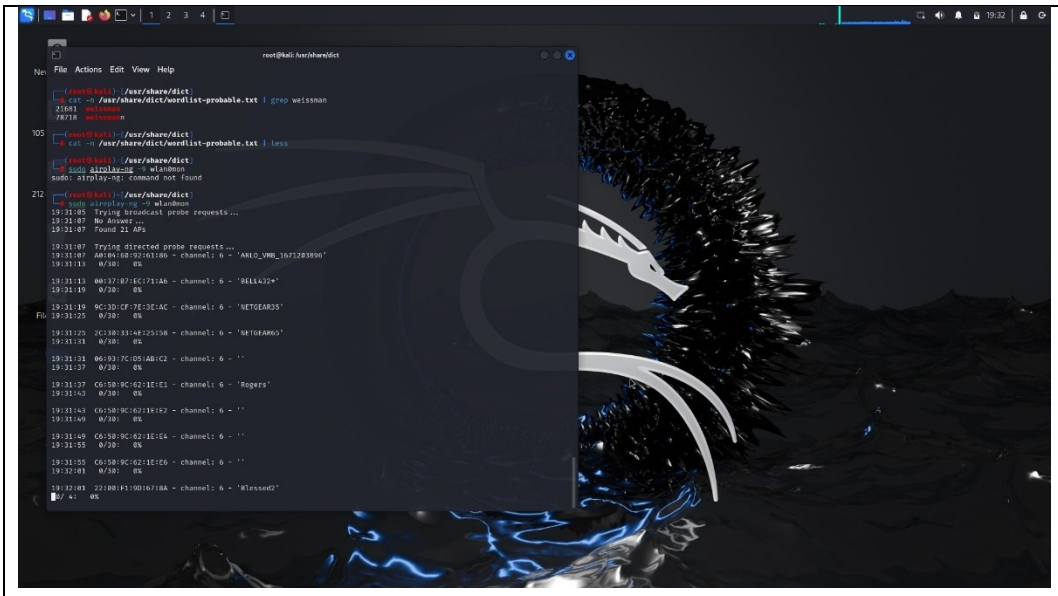
airbase-ng -a [BSSID] -essid "[SSID]" -c [channel] mon0



Note that you will need to provide the hardware address of the AP (the BSSID), the SSID, and the channel and that they must all match the target that you are cloning!

6) Now you can bump your device off of the actual access point and cause it to reconnect to your clone. To do this, use the following:

aireplay-ng -deauth 0 -a [BSSID] **(Take the screen shot)**



7) Now you can conduct man-in-the-middle activities as desired.

Activity 4: Cracking WPA2 Passwords and De-authenticating Clients with Wifite (Optional)

WEP (Wired Equivalency Privacy), established as the first encryption standard for 802.11 wireless networks and ratified in 1997, was a poor attempt at preventing attackers from sniffing wireless traffic sent between wireless clients and APs. It was in no way equivalent to the privacy wired (Ethernet) networks have with cables.

WPA (Wi-Fi Protected Access) debuted in 2003 as an intermediate step between WEP and WPA2 (Wi-Fi Protected Access 2), which debuted itself in 2004. There were so many problems with WEP that a temporary upgrade (WPA) was immediately needed, until a better long-term solution (WPA2) could be designed.

WPA2 has had its share of problems and vulnerabilities but has been the only choice for wireless security since 2004. It is now slowly being phased out in favor of WPA3, which was introduced in 2018. WPA3 prevents dictionary attacks and replay attacks, which are possible with WPA2. In fact, in this lab exercise, you are going to crack a WPA2 password and decrypt packets, both of which are simply not possible with WPA3!

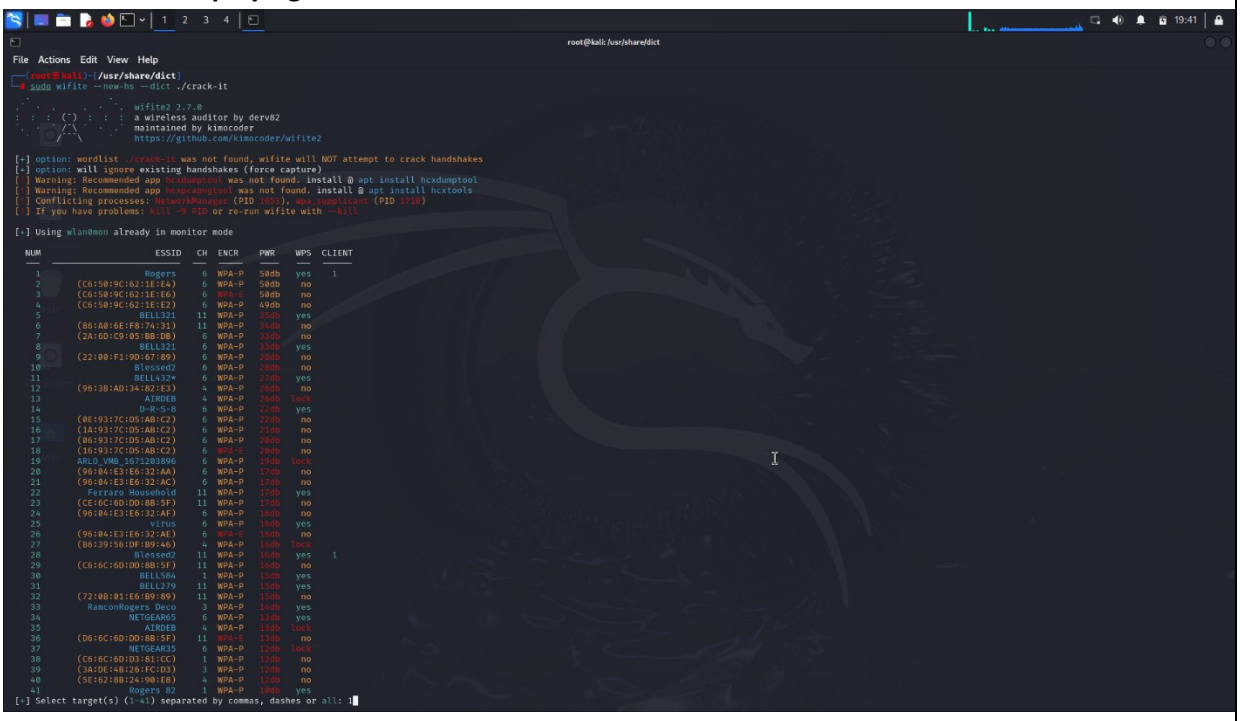
WPA2 (all of the following applies to WPA as well) has two modes: personal mode, also known as pre-shared key (PSK), and enterprise mode. Personal mode simply uses a pre-shared key in the form of a password, while enterprise mode uses a username/password pair, which is used with 802.1X (port-based authentication) and a RADIUS (Remote Authentication Dial-In User Service) server (in most cases, also using an Active Directory database). Cracking enterprise mode is significantly harder than cracking personal mode.

Each client on a WPA2-PSK infrastructure has its own handshake. Therefore, by default, you will not be able to monitor any traffic except your own on an encrypted network. However, if you know the pre-shared key and capture the handshakes of other clients with the AP, you can decrypt their entire sessions, as you will be doing in this lab exercise.

Start the Lab.

Make sure your NIC is in monitor mode before starting this lab exercise. You are not advised to attack any devices that are not under your control, and the author, publisher, professor, teacher and lab. facilitators are not liable if you choose to do so. To make sure the device driver has been installed correctly and that your NIC is capable of packet injection, enter the following command:

sudo aireplay-ng -9 wlan0



You should see an “Injection is working!” message. If you do not see that message, troubleshoot with the earlier instructions for setting up the NIC. You can also try the commands to “down” and “up” the NIC as well to try and make it work.

Step 1: Using Wireshark, you are going to decrypt packets after cracking the WPA2 password with Wifite version 2. Wifite essentially combines famous pentesting tools, including airmon-ng, aircrack-ng, reaver, and more.

a) Start sniffing using Wireshark on the wlan0 interface. In order to decrypt packets, this capture session must have the four-way handshake for each client you would like to decrypt. Without it, Wireshark will not be able to derive the necessary keys to decrypt.

b) In the current directory, create a text file with your SSID’s WPA2 password in it. This is to simplify the process and focus on the new concepts, as opposed to password cracking in general. Otherwise, Wifite will use a default file,

/usr/share/dict/wordlist-probable.txt.

You can examine the default wordlist with **cat -n** (**-n** prints the line numbers) and **grep** (to search for a string), like this:

cat -n /usr/share/dict/wordlist-probable.txt | grep weissman

In this case, there are two entries in the wordlist-probable.txt file that contain the string weissman (weissman on line 21682 and weissmann on line 78719). Substitute another string

for weissman to search the file for other words. You can view the entire file with the **less** utility by typing the following:

cat -n /usr/share/dict/wordlist-probable.txt | less

Advance page by page with the spacebar, or line by line with the up and down arrow keys (which can be held down for fast scrolling) or the ENTER key. Press **q** to quit.

Alternatively, you can open the file in a text editor like vim by typing the following:

vim /usr/share/dict/wordlist-probable.txt

Advance with the arrow keys. Press ESC, **:**, **q**, and ENTER to quit.

Alternatively, you can use rockyou.txt, which comes with Kali Linux.

To see Wifite help, execute the following command:

wifite –help

In the WPA section, notice the following items related to handshakes (hs) and dictionary (dict) files:

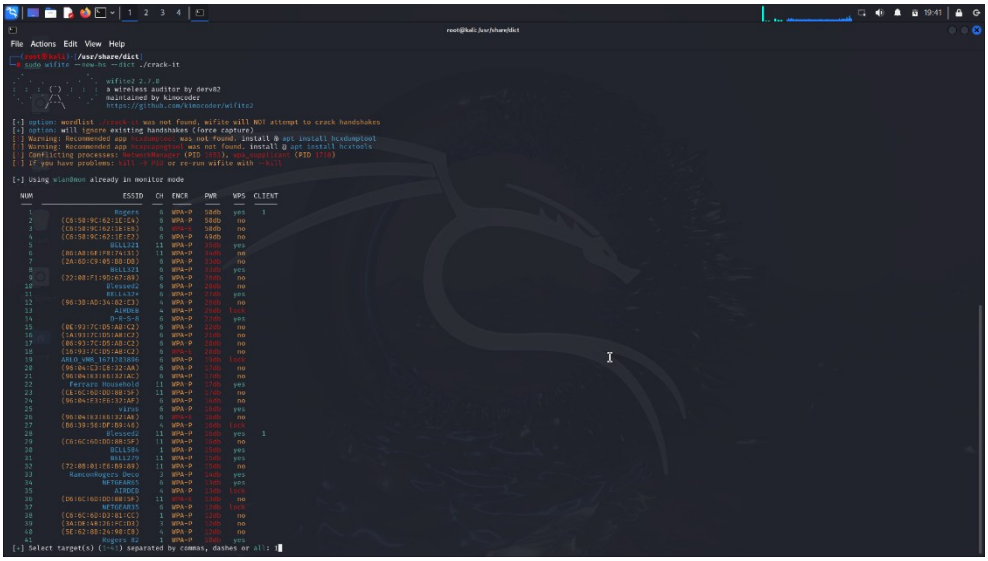
- **--new-hs** Captures new handshakes and ignores existing handshakes in hs (off by default)
- **--dict [file]** File containing passwords for cracking (the default is /usr/share/dict/wordlist-probable.txt)

Step 2: Discover targets and clients with Wifite and then launch an attack to capture the WPA2 password.

a) Start Wifite with the command

sudo wifite --new-hs --dict ./crack-it

where **crack-it** is the name of the text file in the current directory containing the WPA2 password of your SSID. Wifite will start scanning. **Take the screen shot.**



Wifite will find targets (APs) and clients. Give it a few minutes to collect information and many clients. You will see a list of targets and the number of clients shortly thereafter.

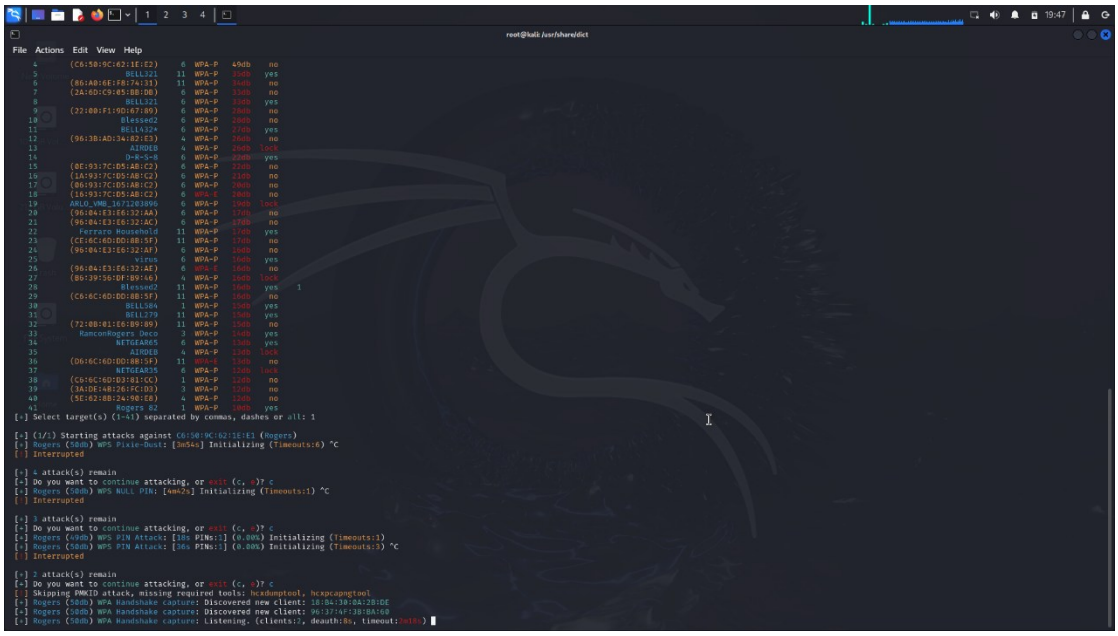
b) Press ESC to stop when a few clients have been found for your AP. **Take the screen shot.** At the prompt, type the number representing your access point for the target. You will notice

attacks starting. Press ESC to skip the first attack, WPS Pixie dust, and then press c or ENTER to continue.

c) Skip the next two attacks, WPS NULL PIN and WPS PIN Attack, in the same fashion. **Take the screen shot.**

d) Ignore the “Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcapngtool” message. The next attack, WPA Handshake capture (WPA in all instances in the output refers to WPA2), is going to be a success! Notice the password after “Cracked WPA Handshake PSK:”. If you have a hard time capturing this for whatever reason (including a wireless USB

NIC that does not perform packet injection), simply disconnect a client from Wi-Fi and reconnect, which will easily allow you to capture the four-way handshake.



e) The output will contain the name of the handshake file with EAPoL. You do not need that because you are already capturing in Wireshark.

Step 3: With Wireshark, decrypt packets from clients that were de-authenticated and whose subsequent reauthenticating handshakes were captured.

a) Go back to the running Wireshark and click the 802.11 Preferences button at the top right (if you do not see the Wireless Toolbar, from the menu bar click View | Wireless) or click Edit | Preferences | Protocol | IEEE 802.11.

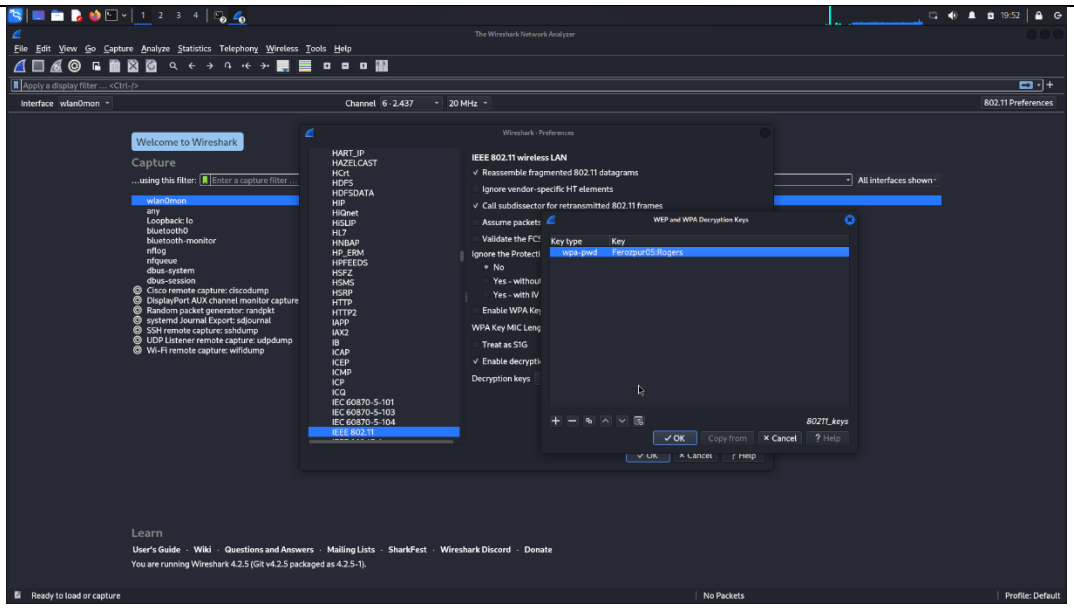
Put a check in the **Enable Decryption** checkbox. Click the Edit button next to Decryption Keys, click the plus sign, and set Key-type to wpa-pwd. Enter the password using the format password:SSID and then click the OK button to close the WEP and WPA Decryption Keys window. Click the OK button to click the Preferences window.

Alternatively, the key can be entered in the form of 64 hex digits, which can be calculated at the following sites:

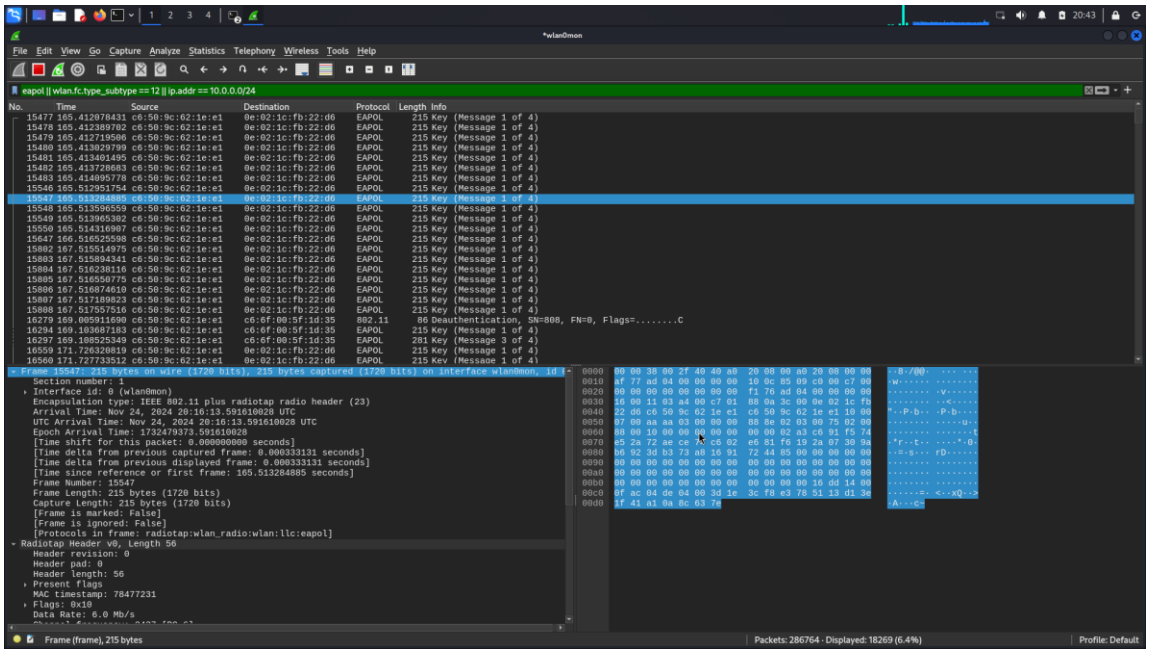
https://www.wireshark.org/tools/wpa-psk.html
http://jorisvr.nl/wpapsk.html
https://www.yeahhub.com/analyzing-deauthentication-packets-wireshark/

In Wireshark, filter by **eapol**, and you will see multiple EAPoL handshakes. To see the deauthentication frames, filter by **wlan.fc.type_subtype == 12**. Use || or the **or** keyword between multiple filters to filter by at least one of them (logical OR).

With the EAPoL in the current capture, Wireshark will be able to decrypt packets from each client that was deauthenticated and reauthenticated. Do not stop the capture; otherwise, you will have to deauthenticate the clients again to view decrypted new traffic. You will still be able to view decrypted traffic to that point, though, if you stop the capture.



b) In Wireshark, filter by **ip.addr == 192.168.1.0/24** (use your network ID and subnet mask) to see all the decrypted packets now. Notice the source IP addresses. **Take the screen shot.**



c) Send pings to those IP addresses and filter by icmp in Wireshark. You will be able to sniff ICMP (Internet Control Message Protocol) in plaintext (from clients that reauthenticated) in Wireshark now.

d) Send pings from the clients that reauthenticated to fully qualified domain names (FQDNs) like www.google.com. You will be able to sniff the DNS and ICMP in plaintext (from clients that reauthenticated) in Wireshark now.

e) Open up a browser on the clients that reauthenticated and go to various websites. You will notice in Wireshark that TLS still encrypts to and from websites that use encryption.

Activity 5: Wireless Network and Device Detection (Optional)

You are about to download and install two programs. Make sure you are connected to a Wi-Fi network (not the ethernet) before continuing.

Step 1: On your Windows 10 machine, download and install NetSpot. The following description is from www.netspotapp.com :

NetSpot is the only professional app for wireless site surveys, Wi-Fi analysis, and troubleshooting on Mac OS X and Windows. It is a FREE Wi-Fi analyzer. No need to be a network expert to improve your home or office Wi-Fi today! All you need is your MacBook running Mac OS X 10.10+ or any laptop with Windows 7/8/10 on board and NetSpot which works over any 802.11 network.

a) Go to www.netspotapp.com then Click the Get NetSpot button.
In the NetSpot FREE edition section, click the Download Now button.
The executable will download to your Downloads folder. Click it to run the executable and install NetSpot.
Click the blue Install Now button to begin the installation.
Click the Launch button when the installation is complete.
Click the Continue button on the bottom left to keep using the free version.

b) While the operating system can give you basic and limited information about wireless networks you are in range of, with the Discover tab selected, you will see information in the following categories: SSID, BSSID, Graph, Signal, %, Min, Max, Average, Level, Band, Channel, Width, Vendor, Security, Mode, and Last Seen. Next Figure shows NetSpot in action.

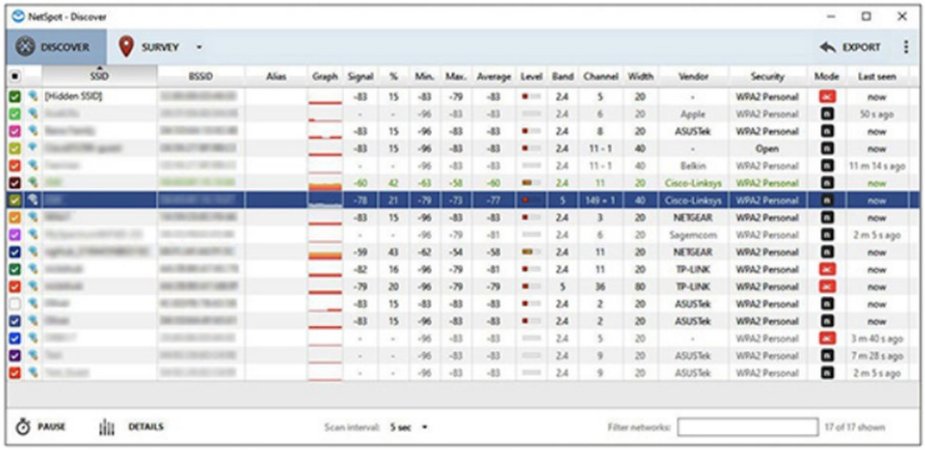
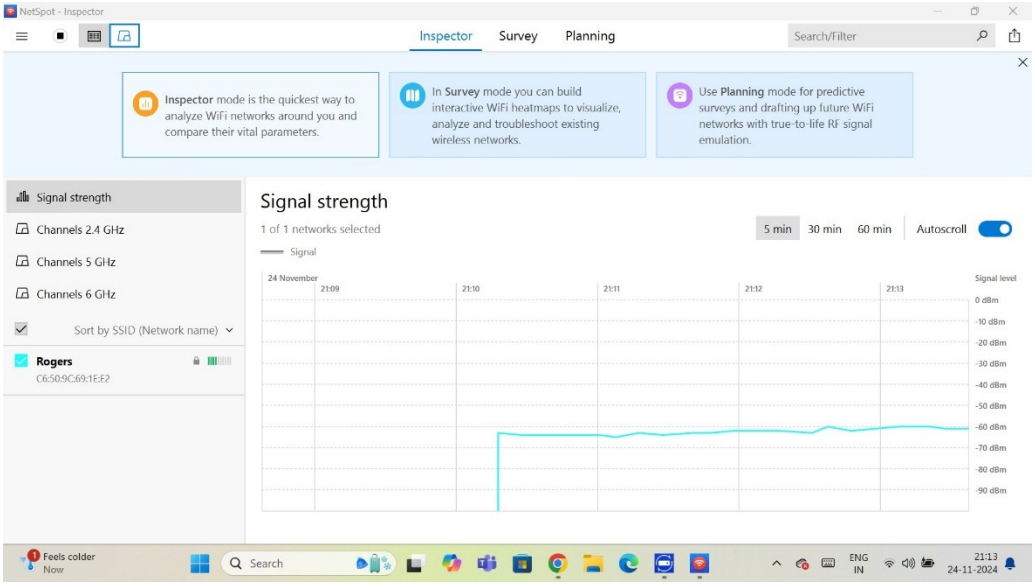


Figure: NetSpot detecting wireless signals

SSID (service set identifier) is the name of the network. BSSID (basic service set identifier) is the AP's MAC address. NetSpot provides a great page at www.netspotapp.com/help/terms-definitions/ that contains "All the clever words used in NetSpot and Wi-Fi related science explained." Check it out.

c) If you put a check in the color-coded checkbox in the first column for some or all rows, you can get information comparing those SSIDs to the others by clicking Details on the bottom bar (or by simply double-clicking a row without putting a check in any box). As shown in next Figure, you will see a new window with the following tabs: Signal (5 min, 30 min, 60 min), Tabular Data, Channels 2.4 GHz, and Channels 5 GHz. The Signal, Channels 2.4 GHz, and Channels 5 GHz tabs will show aggregate information for the SSIDs selected. You can add and remove checks to dynamically change the color-coded output.

Figure: Comparing SSIDs in NetSpot



d) How many SSIDs did you discover?
Ans one

e) Did you have an idea of how many SSIDs you were in range of?

Ans six

f) How many different vendors were detected?
Ans Rogers, Bell

g) What were the security settings detected for the wireless networks?
Ans WPA, WPA3

h) Was there any information you found extremely interesting?
Ans

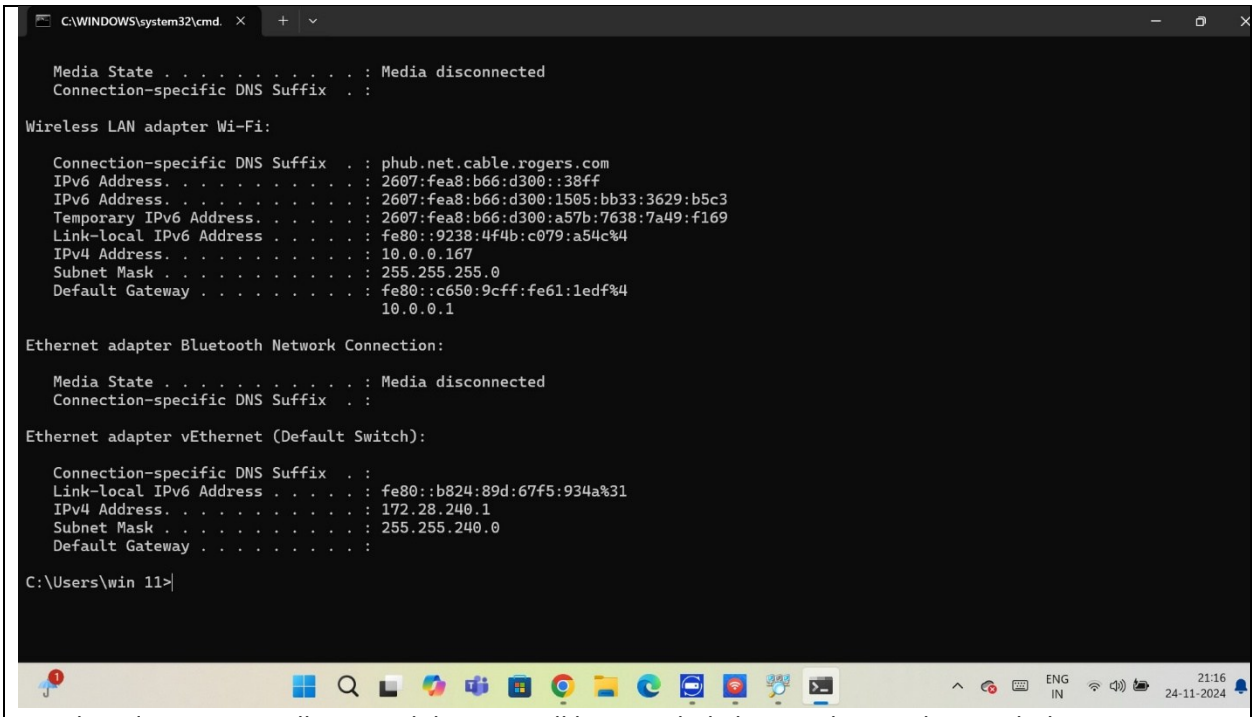
There are more features offered by NetSpot, including a site survey, but they are not free. We are not going to explore these features, but you are more than welcome to pay for them and go even further.

Step 2: Download and install Advanced IP Scanner. The following is from www.advanced-ip-scanner.com :
Reliable and free network scanner to analyze LAN. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off. It is easy to use and runs as a portable edition. It should be the first choice for every network admin.

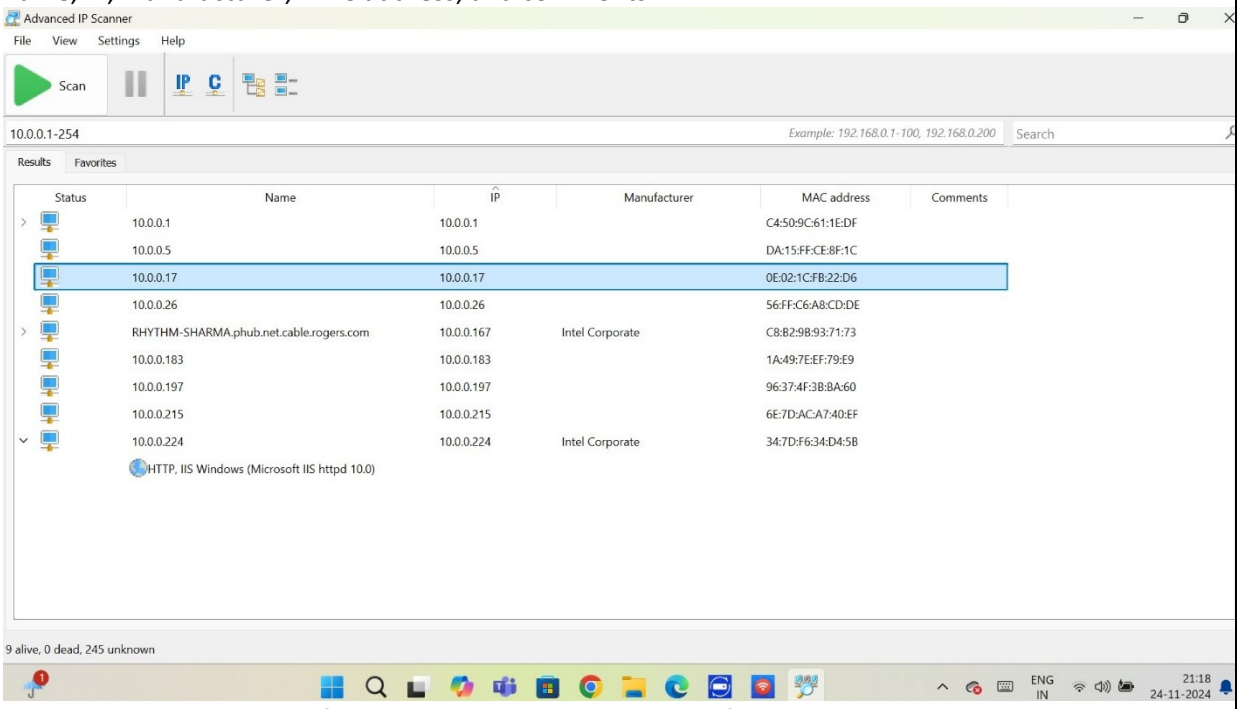
a) Go to www.advanced-ip-scanner.com
Click the Free Download button.
Run the .exe from Downloads.
Keep English (English) as the default language and click the OK button.
Either keep the radio button for Install selected or click the Run radio button and then click Next.
Click the radio button next to I Accept the Agreement.
Click the Install button.
Click the Finish button.

b) Run cmd and type ipconfig, take the screen shot.
On the IP Address Range bar, just include your subnet range (for example, 192.168.1.1-254) and delete anything else that appears there by default.

c) Click the Scan button. Port scanning is now going on behind the screen.



Wireless devices, as well as wired devices, will be revealed along with metadata, including status, name, IP, manufacturer, MAC address, and comments.



There will be even more information about certain devices. If you see an arrow in the Status column, click it to expand the selection to include services discovered.

d) How many devices were detected?
Ans : nine

e) What were some of the manufacturers listed?
AnsL Mostly on Laptop devices

f) What services were detected on certain devices?

Public file sharing, some open ftp files

g) Is there anything extremely interesting that caught your eye?

If I want to see some of the laptop vulnerable and share the file which can be confidential was extremely interesting