Network Forensic Analysis: LLMNR/NBT-NS Poisoning & Credential Access

Analyst: Mduduzi William Radebe

Date: 07 February 2026

Platform: CyberDefenders

Lab: PoisonedCredentials

Case ID: 2026-PC-009

1. Executive Summary

A forensic investigation was conducted on a network traffic capture (PCAP) to identify an suspected **Man-in-the-Middle (MitM)** attack. The analysis confirmed that a rogue machine utilized **LLMNR (Link-Local Multicast Name Resolution)** poisoning to intercept requests intended for a legitimate file share. This resulted in the successful compromise of a user's NTLM credentials and unauthorized access to an internal accounting system via the **SMB** protocol.

2. Project Objective

The primary goal was to dissect the network traffic to:

- Identify the origin of the malicious "poisoned" responses.
- Determine the specific queries that triggered the attack.
- Identify all affected (victim) machines.
- Extract the compromised username and identify the target host accessed by the adversary.

3. Tools & Methodology

The Analyst Toolkit

- **Wireshark:** Used for deep packet inspection and protocol analysis.
- **Filters:** Leveraged specific display filters to isolate malicious traffic from background noise.
- **TCP Stream Following:** Used to reconstruct the "conversation" between the attacker and victims.

The "Step-by-Step" Workflow

Phase 1: Identifying the Catalyst (The Mistyped Query)
Action: I filtered for LLMNR traffic originating from the suspected victim IP 192.168.232.162.

Filter: ip.addr == 192.168.232.162 && llmnr

Observation: The machine was broadcasting a query for the name **fileshaare**.

Analyst Note: The double 'a' in the name confirms a user typo. Because this name doesn't exist on the DNS server, the computer resorted to LLMNR, which "shouts" to the whole network for help.

Phase 2: Locating the Rogue Entity
Action: I utilized Wireshark's **Statistics > Endpoints** tool to find the most active IPv4 addresses, then looked for who responded to the fileshaare query.

Observation: Machine **192.168.232.215** immediately responded to the broadcast, claiming to be the location of the (non-existent) fileshaare.

Conclusion: 192.168.232.215 is confirmed as the **Rogue Machine** (Attacker).

Phase 3: Scope of Impact (The Second Victim)
Action: I filtered for all traffic where the Rogue Machine sent responses to different hosts.

Filter: ip.src == 192.168.232.215

Observation: I identified a second machine, **192.168.232.176**, receiving poisoned responses from the attacker. This confirms the attack was broad and automated (likely using a tool like **Responder**).

Phase 4: Credential Theft Analysis
Action: I focused on the **SMB (Server Message Block)** protocol to see if any login attempts were intercepted. I selected an SMB packet and used **Follow > TCP Stream**.

Observation: Within the NTLM authentication exchange (NTLMSSP), the attacker forced the victim to authenticate.

Findings: The compromised account was identified as **janesmith**.

Phase 5: Action on Objectives
Action: I tracked the attacker's activity after the credential theft to see what internal resource they targeted.

Filter: ip.addr == 192.168.232.215 && smb2

Observation: The attacker used the stolen credentials to connect to a new machine.

Target Hostname: AccountingPC.

4. Technical Findings Summary

Metric	Detail
Initial Mistyped Query	fileshaare
Rogue Machine IP	192.168.232.215
Victim IP #1	192.168.232.162
Victim IP #2	192.168.232.176
Compromised User	janesmith
Targeted Destination	AccountingPC

5. Analyst Reflections

Struggles & Challenges

- **Noise Filtering:** Initial analysis was difficult due to the sheer volume of background traffic. Learning to use ip.addr in combination with llmnr was the "lightbulb moment" that cleared the noise.
- **Understanding Streams:** Following a TCP stream can be overwhelming for a beginner. It took a few tries to find the specific "NTLMSSP" (login) part of the conversation among the thousands of bytes of data.

Lessons Learned

- **Protocol Dangers:** I learned that LLMNR and NBT-NS are dangerous legacy protocols that should be **disabled** via Group Policy in a secure environment.
- **The Power of Typo:** This lab taught me that a single misspelled word by a user can lead to an entire network being compromised if local name resolution is not secured.
- **SMB Signing:** I now understand that enforcing **SMB Signing** would prevent an attacker from easily relaying these stolen credentials to other machines like the AccountingPC.

6. Recommendations (SOC Strategy)

1. **Immediate Action:** Disable LLMNR and NBT-NS on all workstations and servers via GPO.
2. **Monitoring:** Configure SIEM alerts for any "LLMNR Response" packets originating from non-IT subnets.
3. **Credential Hygiene:** Reset the password for janesmith immediately and audit the AccountingPC for any unauthorized file access or persistence mechanisms.

Analyst Signature

Mduduzi William Radebe

SOC Analyst in Training