Incident Investigation Report

CyberDefenders CTF – *Poisoned Credentials*

---

1. Introduction

This report documents the investigation and analysis of the **Poisoned Credentials** challenge from CyberDefenders.
The objective of the challenge was to investigate a suspected network security incident involving **credential poisoning through name resolution protocols**, identify affected systems, determine compromised credentials, and understand the attacker's activity using network traffic analysis.

The investigation was conducted using a provided **PCAP file** and focused on identifying malicious abuse of Windows authentication mechanisms.

Key Concepts Covered

. Blue Team Skills - Focuses on defending networks and analyzing attacks

. Network Forensics - investigating network traffic to find malicious activity

. PCAP Analysis - Analyze a packet capture (.pcap) file (Wireshark)

. Credential Theft Attacks - scenario simulates stealing credentials by poison

---

2. What This Challenge Is About (In Simple Terms)

This challenge simulates a common real-world internal network attack where:

• A user or system mistypes a hostname
• DNS resolution fails
• Windows falls back to LLMNR or NBT-NS
• A rogue machine responds falsely
• The victim system sends NTLM authentication data
• The attacker captures and reuses credentials over SMB

This attack does not require malware and often goes unnoticed in enterprise environments.

---

3. Short Explanation of LLMNR and NBT-NS

3.1 What is LLMNR?

LLMNR (Link-Local Multicast Name Resolution) is a Windows protocol used to resolve hostnames when DNS fails. It sends multicast name resolution requests to all devices on the local network.

3.2 What is NBT-NS?

NBT-NS (NetBIOS Name Service) is an older Windows name resolution protocol that works similarly by broadcasting hostname queries on the local network.

3.3 Why Are They Dangerous?

If a hostname is mistyped or does not exist:

- Any machine can respond
- Attackers can impersonate legitimate hosts
- NTLM authentication data can be captured
- Credentials can be relayed or reused

3.4 Why They Were Used in This Attack

In this incident:

- A mistyped hostname triggered LLMNR/NBT-NS
- A rogue machine sent fake responses
- Victim machines sent NTLM authentication data
- The attacker captured credentials and accessed SMB services

---

4. Tools Used

- Wireshark – for packet capture analysis
- Wireshark display filters (LLMNR, SMB, NTLMSSP)
- Follow UDP Stream
- Follow TCP Stream

---

5. Evidence Provided

- A PCAP file containing internal network traffic
- Captured LLMNR, SMB, and NTLM authentication packets related to the poisoning attack

---

6. Investigation Methodology & Steps

Step 1: Identify Name Resolution Traffic

• Applied LLMNR and NBNS filters in Wireshark
• Focused on traffic involving 192.168.232.162
• Looked for suspicious or mistyped hostname queries

Step 2: Identify Rogue Responses

• Analyzed LLMNR response packets
• Identified machines responding to mistyped queries
• Determined the rogue (attacker) machine

Step 3: Identify Affected Machines

• Identified all victim systems receiving poisoned responses
• Tracked rogue responses to multiple IP addresses

Step 4: Analyze SMB Authentication *(Rewritten)*

• Identified SMB2 Session Setup Request packets in Wireshark
• Recognized SMB authentication attempts initiated after LLMNR poisoning
• Inspected SMB2 Session Setup traffic for NTLMSSP authentication
• Extracted usernames from NTLMSSP_AUTH messages within SMB2

Step 5: Identify Accessed Host *(Rewritten)*

• Located SMB2 Session Setup Request and Response packets
• Used Follow TCP Stream on SMB2 traffic
• Inspected NTLMSSP authentication blobs inside SMB2 streams
• Extracted the target machine hostname from SMB authentication data
• Identified the internal system accessed by the attacker

Questions, Answers, and How They Were Found

Question 1

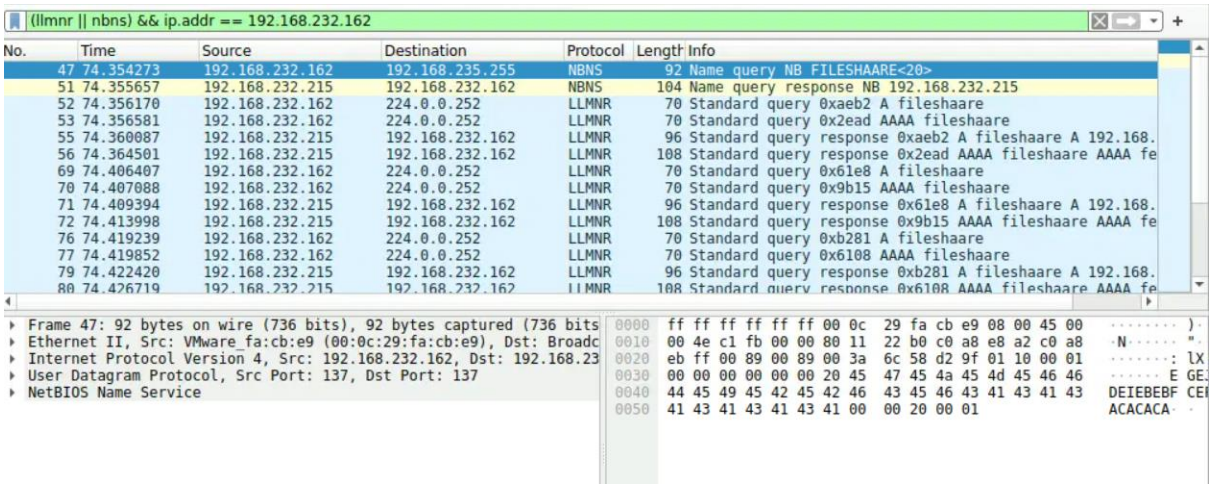
What was the mistyped query made by 192.168.232.162?

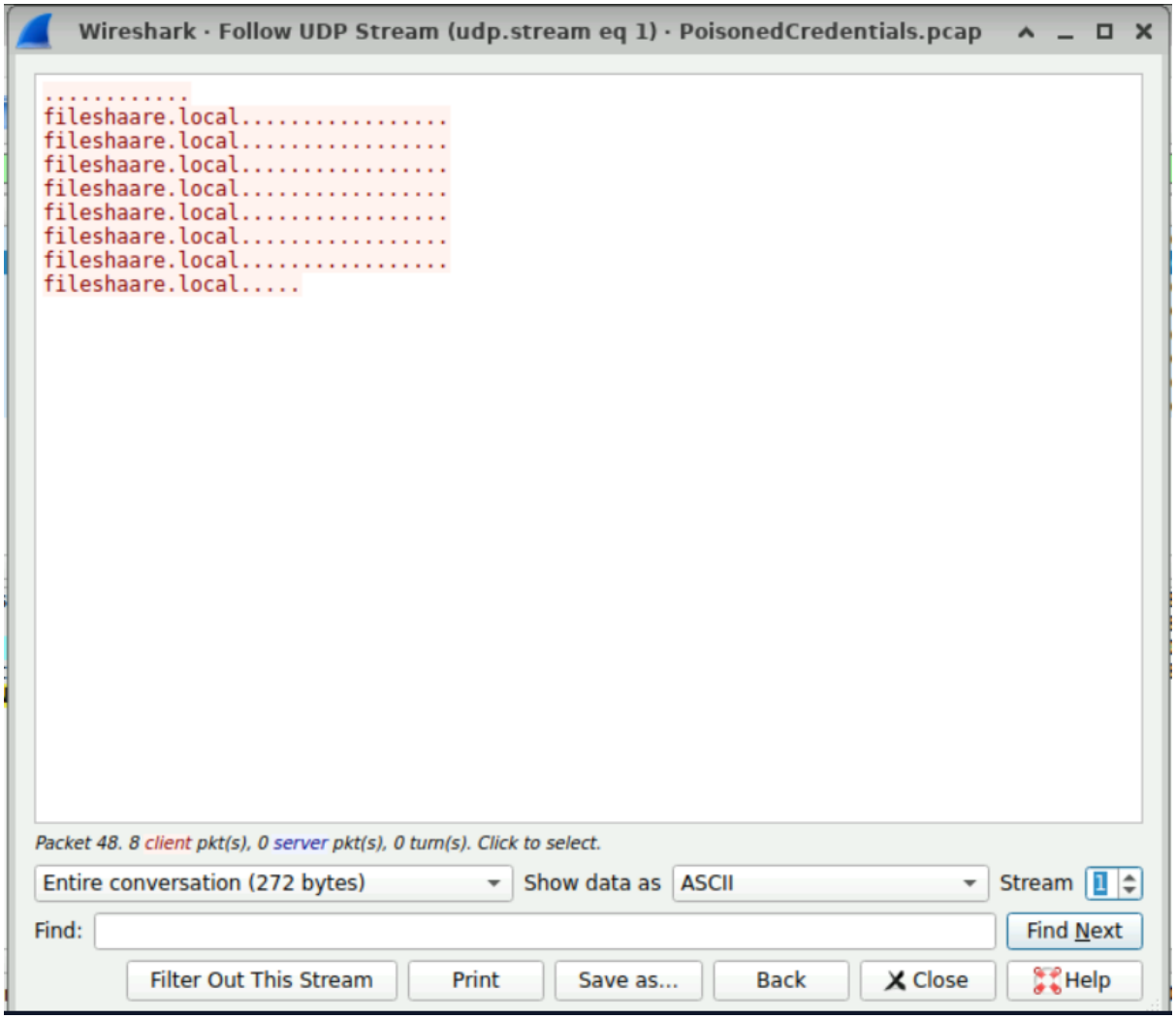
Answer:
FILESHAARE

How it was found:
• Applied filter:

(llmnr || nbns) && ip.addr == 192.168.232.162

• Used Follow UDP Stream
• Observed a suspicious query for *fileshaare*
• Identified it as a mistyped version of *fileshare*
• The extra “a” confirmed a user/system typo





Question 2

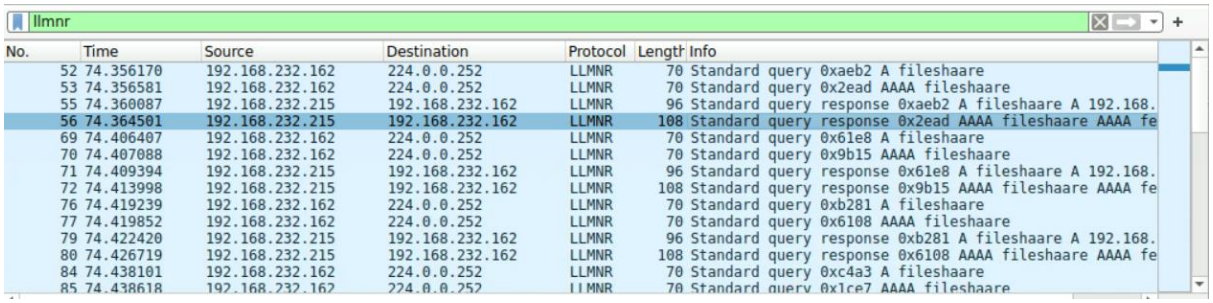
What is the IP address of the rogue machine?

Answer:
192.168.232.215

How it was found:
• Applied filter:

llmnr

• Identified packet number 56
• Observed LLMNR response from 192.168.232.215 to 192.168.232.162
• The rogue machine responded to the mistyped hostname *fileshaare*
• This unsolicited response confirmed rogue behavior

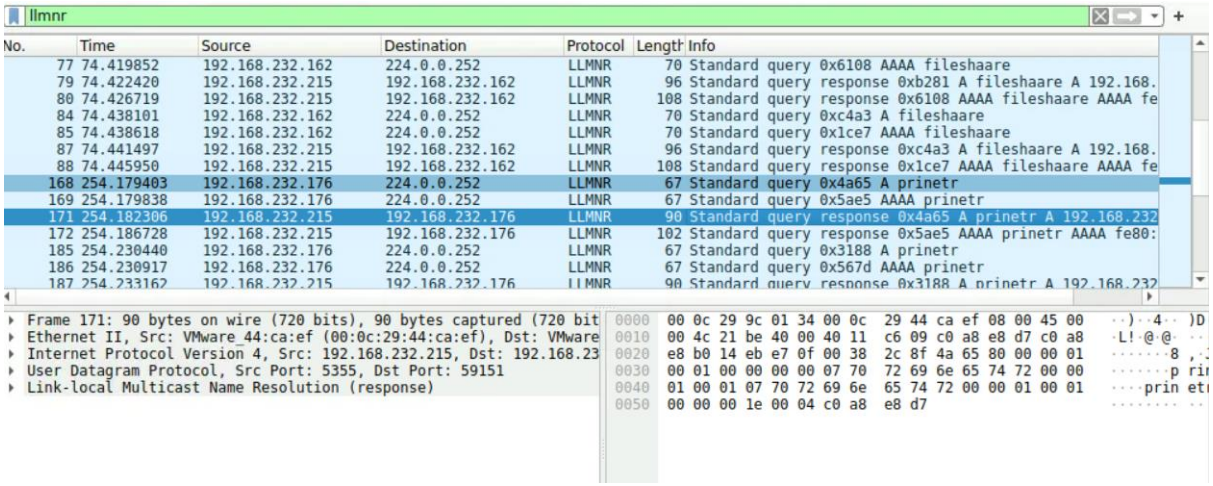


Question 3

What is the IP address of the second machine that received poisoned responses?

Answer:
192.168.232.176

How it was found:
• Continued analyzing LLMNR responses from 192.168.232.215
• Identified packet number 187
• Observed rogue response for mistyped hostname prinetr *(printer)*
• Destination IP was 192.168.232.176
• Confirmed as second victim machine



Question 4

What is the username of the compromised account?

Answer:
janesmith

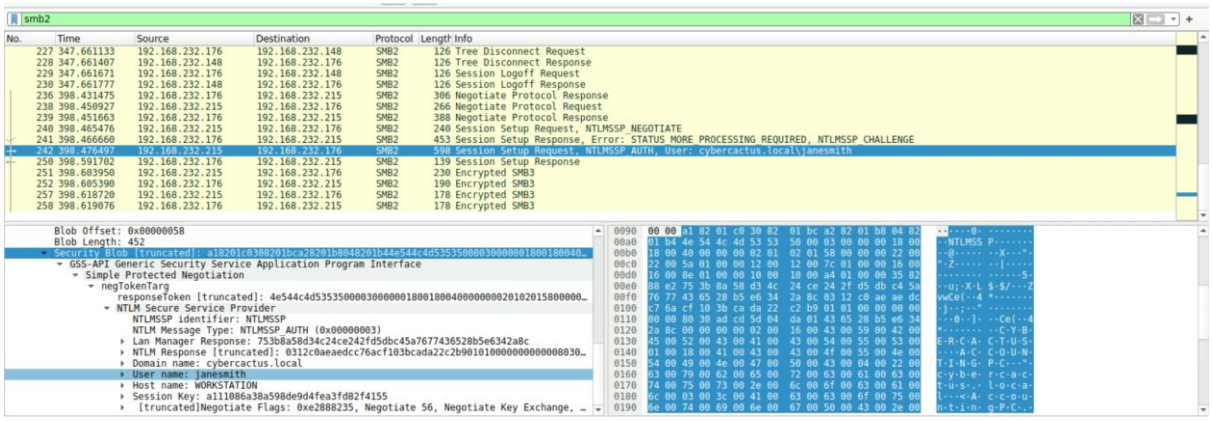
How it was found:
• Applied filter:

SMB2

• Identified packet number 242
• Observed SMB2 Session Setup with NTLMSSP_AUTH
• Extracted username from:

cybercactus.local\janesmith

• Confirmed credentials were sent to rogue machine



Question 5

What is the hostname of the machine accessed via SMB?

Answer:
ACCOUNTINGPC

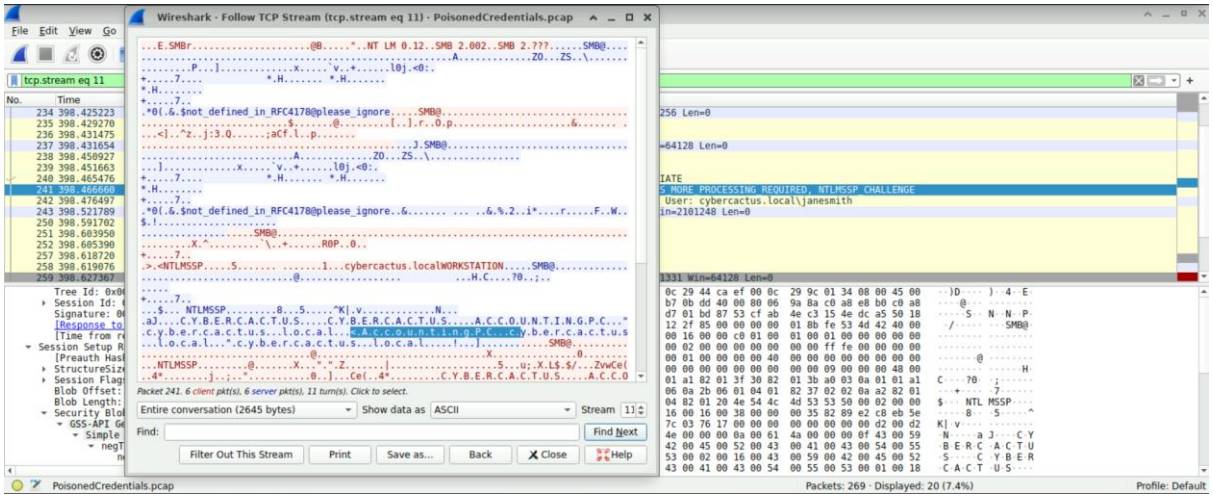
How it was found:
• Applied filter:

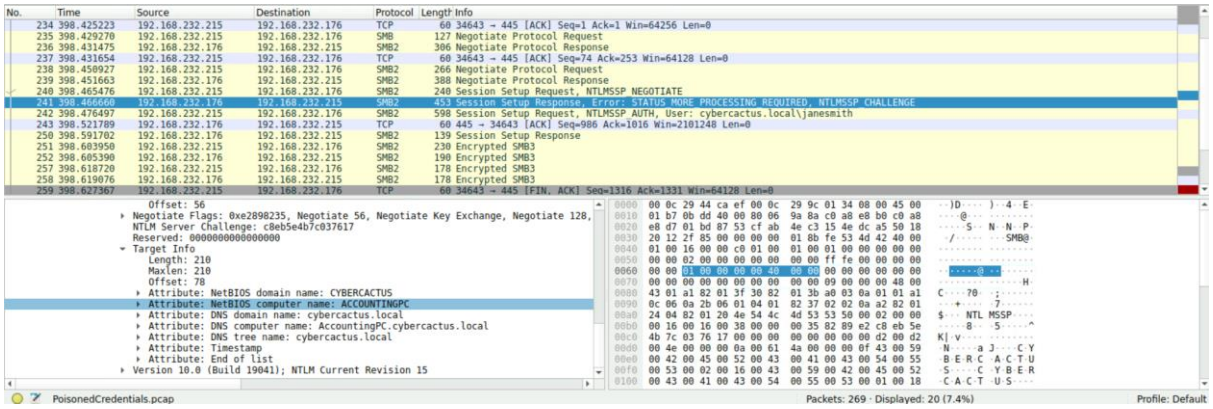
Smb2

• Followed TCP Stream of SMB 2 traffic
• Manually inspected NTLMSSP authentication data
• Extracted hostname string:

ACCOUNTINGPC

• Confirmed internal host accessed by attacker





---

8. Key Findings

- LLMNR was abused for name resolution poisoning
- A rogue machine (192.168.232.215) responded to mistyped queries
- Multiple victim machines were affected
- NTLM authentication data was captured
- Valid user credentials were exposed
- SMB access was performed using captured credentials
- The attacker accessed ACCOUNTINGPC

---

9. Conclusion

The investigation confirms a successful LLMNR poisoning attack within the internal network. The attacker exploited mistyped hostname queries to impersonate network resources and capture NTLM authentication data.

Using the captured credentials, the attacker was able to authenticate over SMB and access an internal system, demonstrating how insecure name resolution protocols can lead to serious compromises without deploying malware.

---

10. Lessons Learned

• LLMNR and NBT-NS are high-risk legacy protocols
• Mistyped hostnames can expose credentials
• NTLM authentication can be captured and abused
• Internal attacks may not trigger malware alerts
• Network monitoring is critical for detection
• Successful logins must be monitored

---

11. Recommendations

• Disable LLMNR and NBT-NS across the enterprise
• Enforce SMB signing
• Monitor NTLM authentication events
• Use DNS exclusively for name resolution
• Implement network segmentation
• Educate users about internal network security risks
