PoisonedCredentials Lab: LLMNR/NBT-NS Poisoning Walkthrough (CyberDefenders)

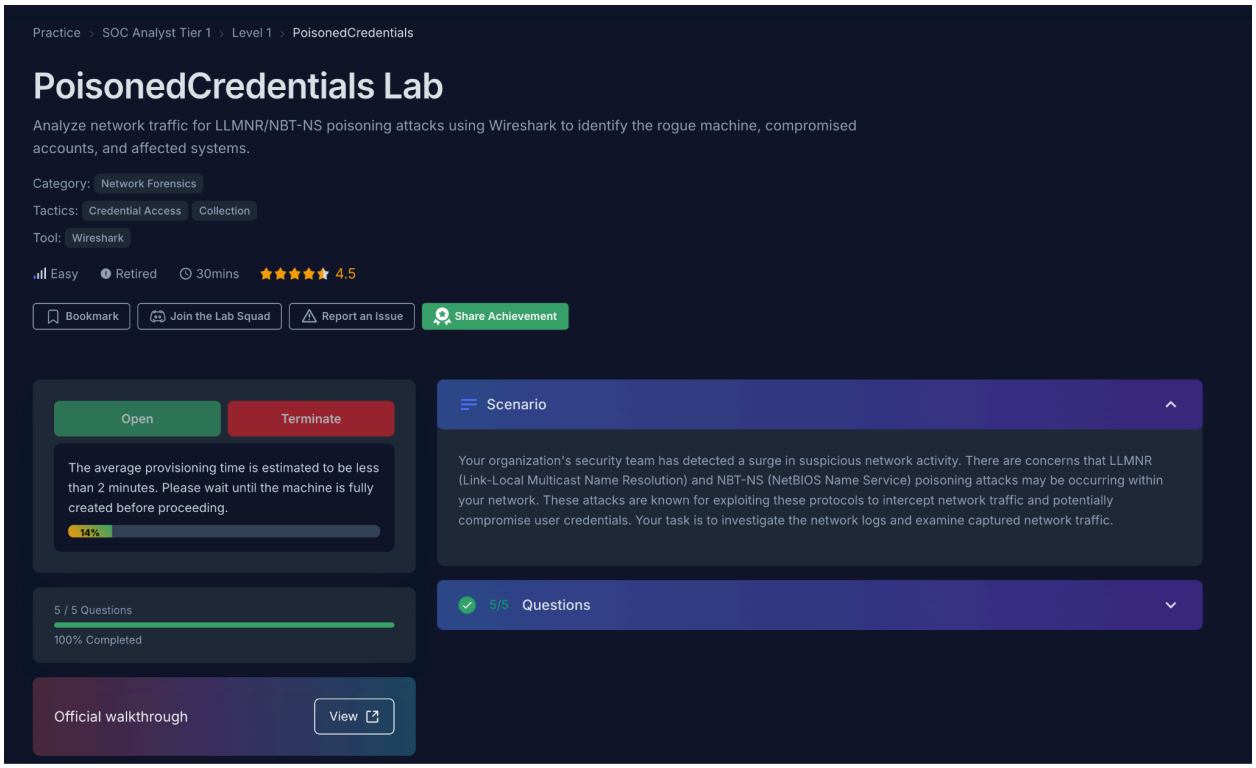

Figure 1: Case header and lab introduction for the PoisonedCredentials Lab

Analyst	Pakagrong Lebel
Lab Creator	CyberDefenders
Date of Publishing	December 24, 2025
Project-ID	CBDF-004

Executive Summary

This report documents a comprehensive investigation into a network security incident involving Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) poisoning attacks. The organization's security team detected a surge in suspicious network activity attributed to poisoning attacks targeting these vulnerable name resolution protocols. Through methodical network forensic analysis using Wireshark, the investigation successfully identified the rogue machine responsible for the attack, mapped the affected systems, identified compromised user credentials, and determined the extent of unauthorized access within the network environment.

Incident Overview

The incident began with the detection of suspicious network activity by the organization's security operations centre. Initial analysis indicated that threat actors were exploiting inherent vulnerabilities in LLMNR and NBT-NS protocols to intercept legitimate network traffic and manipulate name resolution processes. These protocols, while designed to facilitate name resolution in local network environments, rely on broadcast queries with minimal authentication mechanisms, making them susceptible to man-in-the-middle attacks and credential harvesting operations.

The attack scenario involved a benign user action that triggered a security incident. A legitimate machine on the network mistakenly typed an incorrect resource name, which initiated broadcast queries across the network seeking the non-existent resource. An attacker positioned within the network environment intercepted these queries and responded with poisoned answers, directing the legitimate machines to the attacker's systems instead of the intended resources. This malicious redirection allowed the attacker to capture sensitive information and user credentials.

Technical Background: Why These Protocols Matter

LLMNR Protocol Fundamentals

Link-Local Multicast Name Resolution is a protocol that allows computers on a local network to perform name resolution without relying on traditional Domain Name System (DNS) infrastructure. When a standard DNS query fails, Windows systems will automatically fall back to LLMNR as an alternative resolution mechanism. LLMNR operates by broadcasting a multicast query to the address 224.0.0.252 on port 5355, asking any machine on the network if it knows the identity of the requested resource.

The protocol was designed with network convenience in mind, prioritizing accessibility over security. LLMNR does not implement robust authentication mechanisms to verify that responses actually come from legitimate systems. Any machine on the network can listen to LLMNR queries and respond with false information, claiming to be the requested resource.

NBT-NS Protocol and Its Vulnerabilities

NetBIOS Name Service operates similarly to LLMNR but represents a legacy protocol predating modern networking standards. NBT-NS functions as a broadcast-based name resolution mechanism for older Windows systems and continues to be supported in contemporary Windows environments for backward compatibility. When a system cannot resolve a name through DNS or LLMNR, it may query NBT-NS as a final fallback mechanism.

Like LLMNR, NBT-NS operates on broadcast principles and lacks authentication controls. The protocol trusts any response it receives from the network, making it inherently vulnerable to spoofing attacks. This means an attacker can impersonate any network resource by simply responding to NBT-NS queries before legitimate systems do.

The Attack Vector: Poisoning Name Resolution

When a user mistypes a resource name, such as typing "fileshaare" instead of "fileshare," the following sequence occurs:

1. The workstation initiates a DNS query for the misspelled name
2. When DNS fails to resolve the name, the system automatically falls back to LLMNR
3. An LLMNR multicast query broadcasts across the network segment
4. If LLMNR receives no valid response, the system queries NBT-NS
5. An attacker listening on the network can respond to either LLMNR or NBT-NS queries
6. The victim machine trusts the attacker's response and redirects traffic to the attacker's system
7. When the victim attempts to authenticate to the false resource, credentials are captured

This attack methodology is particularly effective because it exploits legitimate system behaviour rather than technical vulnerabilities, in the sense of software defects. The protocols were designed to be accessible and trustworthy within a local network environment, an assumption that breaks down when hostile actors exist on the same network segment.

Attack Methodology

Attack Execution Flow

The attack employed in this incident followed the classic LLMNR poisoning pattern. An attacker positioned on the network monitored for name resolution queries. When legitimate machines on the network generated LLMNR or NBT-NS queries for non-existent resources, the attacker's system responded with poisoned answers.

The critical element of this attack was that it exploited benign user behaviour. A user on one of the network machines attempted to access a shared resource but mistyped the name. This simple human error created the attack surface the attacker needed. Instead of the user simply receiving an error message indicating the resource could not be found, the attacker intercepted the situation and provided a false response.

Protocol Exploitation Details

The attacker likely employed tools such as Responder, a popular open-source LLMNR and NBT-NS poisoner, or similar utilities. These tools passively listen for multicast name resolution queries across the network. Upon detecting a query, the tools respond faster than legitimate systems would, poisoning the victim's cache with the attacker's IP address associated with the requested resource name.

Once the victim machine has been poisoned and directs its traffic to the attacker's system, the attacker can perform further attacks. If the victim attempts to authenticate to the poisoned resource using SMB (Server Message Block) protocol, the authentication credentials are captured. These credentials can be used for:

1. Direct lateral movement within the network
2. Password cracking attempts
3. Pass-the-hash attacks to access other systems
4. Privilege escalation activities
5. Persistence establishment within the network

Investigation Methodology & Lab Questions

The investigation required a systematic analysis of network traffic captures using Wireshark, a powerful network forensic analysis tool. Each question in the lab corresponds to a specific investigation objective, building progressively toward a complete understanding of the attack.

Q1: In the context of the incident described in the scenario, the attacker initiated their actions by taking advantage of benign network traffic from legitimate machines. Can you identify the specific mistyped query made by the machine with the IP address 192.168.232.162?

Answer: FILESHAARE

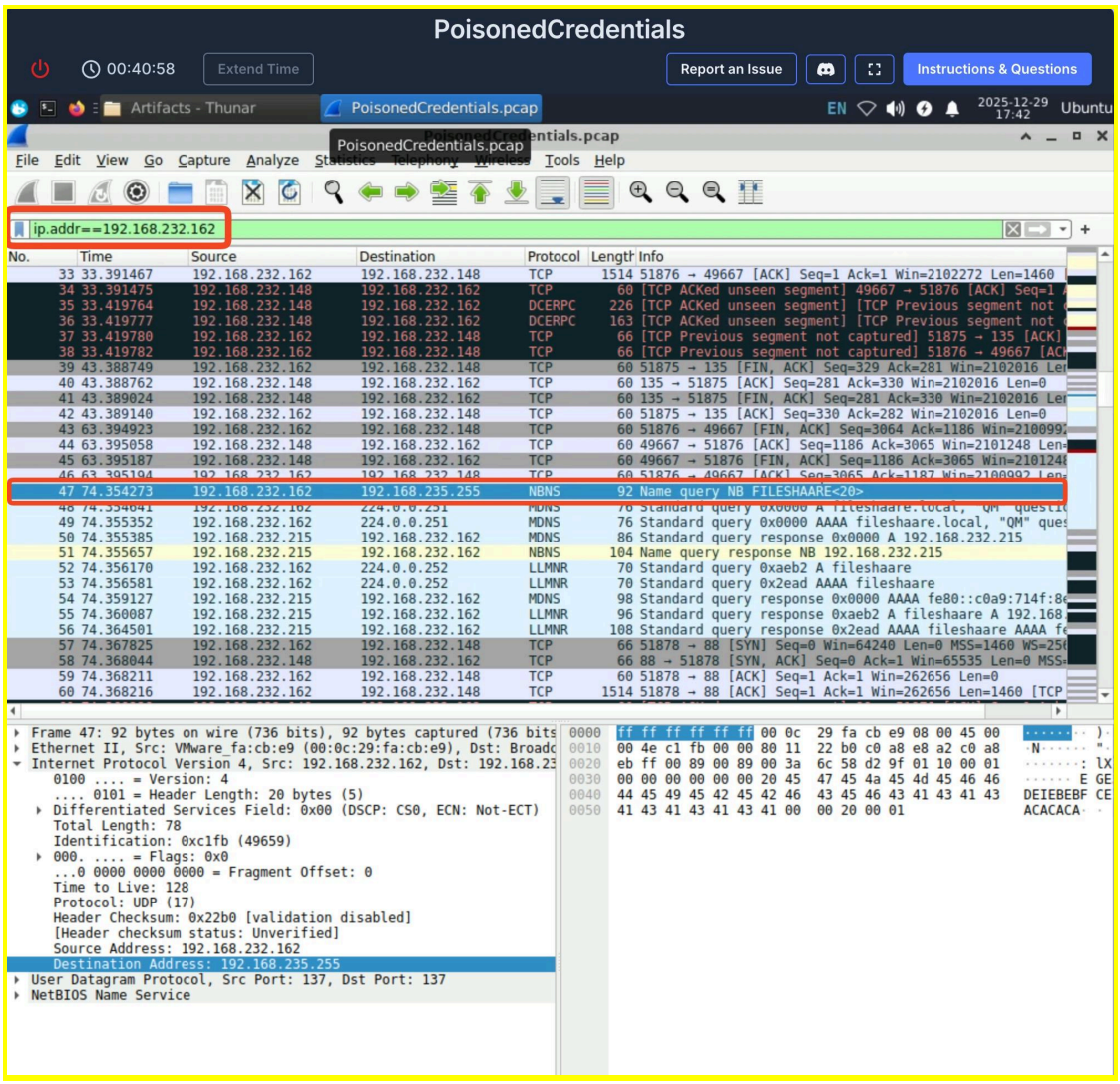

Figure 2: LLMNR query from 192.168.232.162 showing the mistyped hostname “FILESHAARE” in Wireshark

Detailed Analysis

The first investigation step required identifying which legitimate machine made the critical error that triggered the attack chain. The machine at IP address 192.168.232.162 generated network queries for a resource named "fileshaare," which appears to be a misspelling of "fileshare."

Why This Matters

Understanding the initial trigger is crucial for incident response. This reveals that the attack did not exploit a sophisticated technical vulnerability but rather leveraged a common user error. In many real-world scenarios, security incidents are triggered by simple human mistakes rather than zero-day exploits or complex attack chains. Recognizing this allows organisations to implement both technical controls and user education to prevent similar incidents.

Investigation Methodology

To identify the mistyped query, an investigator would:

1. Open the network capture file in Wireshark
2. Apply protocol filters to show only LLMNR and NBT-NS packets
3. Examine the "Queries" section of LLMNR packets
4. Look for queries originating from the IP address 192.168.232.162
5. Review the query names to identify misspellings or unusual resource names
6. Document the exact spelling of the queried resource name

Q2: We are investigating a network security incident. To conduct a thorough investigation, We need to determine the IP address of the rogue machine. What is the IP address of the machine acting as the rogue entity?

Answer: 192.168.232.215

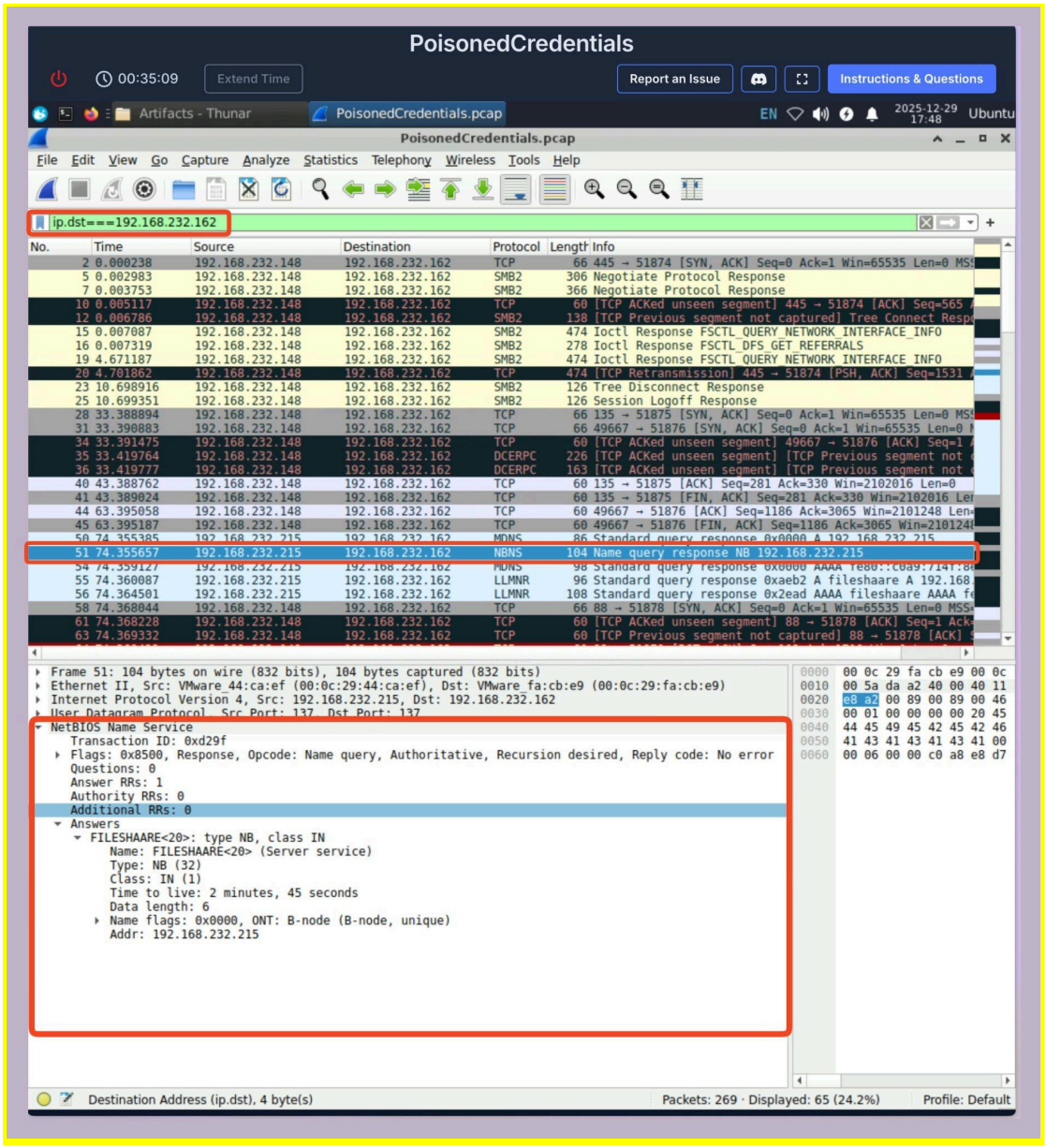

Figure 3: Wireshark capture showing NBNS response from rogue host 192.168.232.215 directing victim 192.168.232.162 to the spoofed FILESHAARE<20> server

Detailed Analysis

The rogue machine is the attacker's system on the network. This machine detected the LLMNR query for "fileshaare" and responded with a poisoned answer, claiming to be the requested resource and directing the victim machine to send traffic to the attacker's IP address instead of a legitimate resource.

Why This Matters

Identifying the rogue machine is the core objective of the incident response investigation. Once the attacker's IP address is known, security teams can:

1. Block traffic to and from this IP address
2. Isolate the rogue system from the network
3. Preserve evidence from the compromised system
4. Search for other signs of compromise from this system
5. Determine if other attacks originated from this IP
6. Implement network segmentation to prevent similar attacks in future

Investigation Methodology

To identify the rogue machine's IP address, an investigator would:

1. Filter Wireshark to display only LLMNR response packets
2. Review the source IP addresses of LLMNR responses to the mistyped query
3. Cross-reference with legitimate network resources to confirm the IP is not a valid server
4. Examine the statistics or endpoints feature in Wireshark to identify all active IP addresses
5. Look for the IP address that responded to poisoned queries with unusual characteristics
6. Verify that this IP address appears as a source in unauthorized SMB authentication attempts
7. Check organisational network documentation to confirm this IP is not assigned to any legitimate systems

---

Q3: As part of our investigation, identifying all affected machines is essential. What is the IP address of the second machine that received poisoned responses from the rogue machine?

Answer: 192.168.232.176

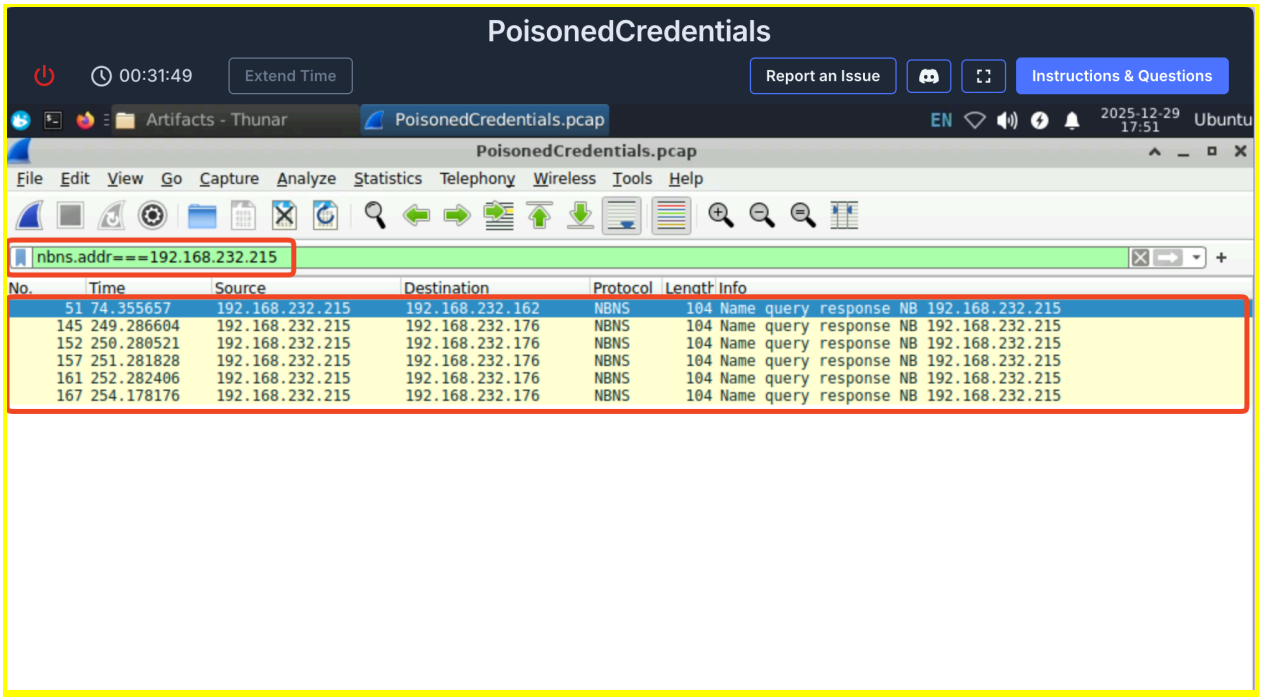

Figure 4: Wireshark NBT-NS responses from rogue host 192.168.232.215 to the second affected machine 192.168.232.176, confirming poisoned name resolution traffic

Detailed Analysis

The investigation revealed that multiple machines on the network were affected by the poisoning attack. While the initial query came from 192.168.232.162 for the misspelled "fileshaare," a second machine at 192.168.232.176 also generated poisoned queries. This second machine appears to have queried for a misspelled version of "printer" (likely "princter" or similar).

Why This Matters

Identifying all affected machines is critical for understanding the scope of the incident. The presence of multiple affected machines suggests either:

1. Multiple users made similar mistakes independently
2. A single user accessed multiple workstations and made errors on each
3. The attack was broader than initially apparent
4. Network documentation and resource discovery was incomplete, leading multiple users to make incorrect guesses

Understanding the full scope of affected machines ensures complete remediation and prevents attackers from using backup systems for persistence.

Investigation Methodology

To identify all affected machines, an investigator would:

1. Filter for all LLMNR query packets in the network capture
2. Examine the source IP addresses of these queries
3. Identify queries for non-existent or misspelled resources
4. Cross-reference each source IP with organisational asset inventory
5. Group machines by the specific resources they queried
6. Determine which machines received responses from the rogue IP address
7. Prioritize machines that attempted authentication to the poisoned resources
8. Document all affected systems for notification and remediation

---

Q4: We suspect that user accounts may have been compromised. To assess this, we must determine the username associated with the compromised account. What is the username of the account that the attacker compromised?

Answer: janesmith

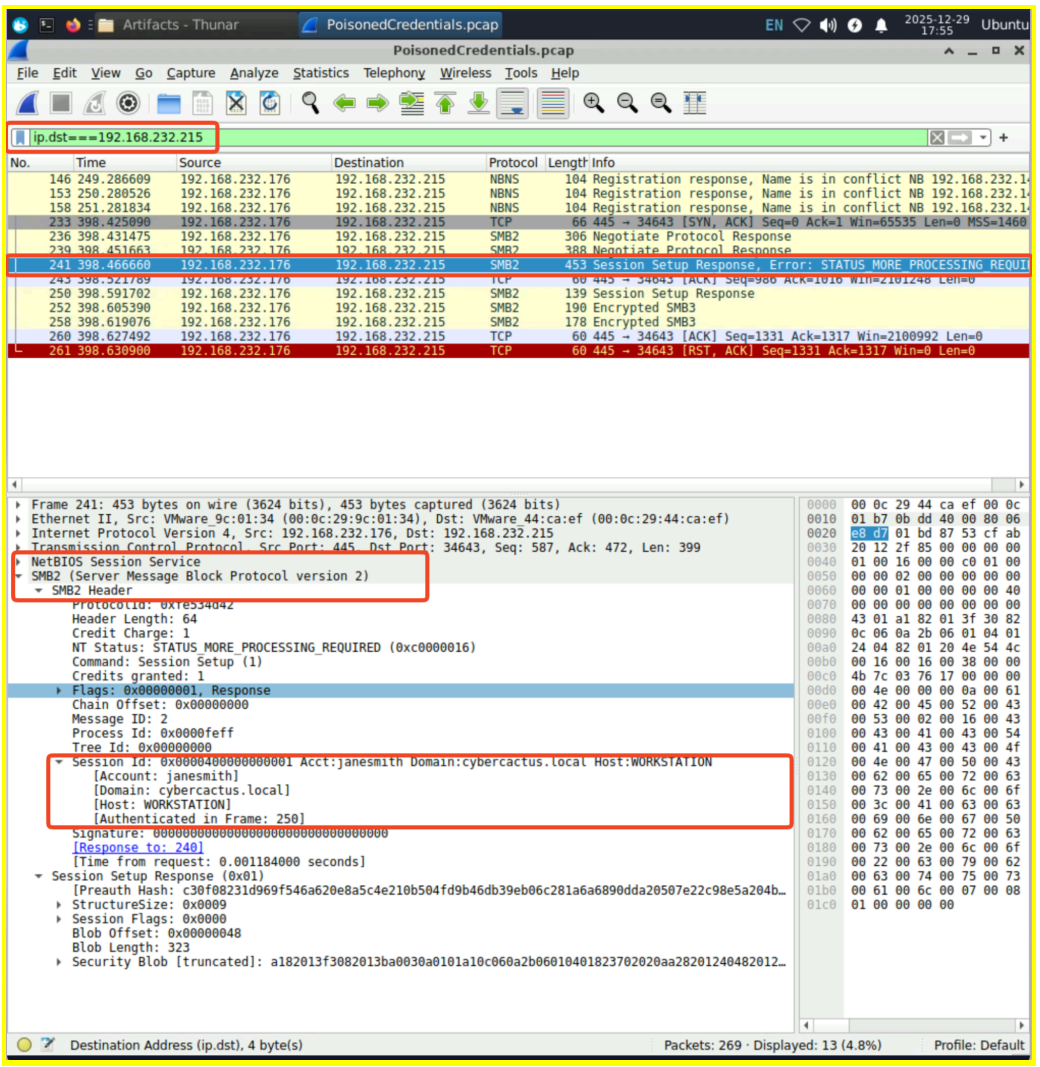

Figure 5: SMBv2 session setup from rogue host 192.168.232.215 revealing the compromised username "janesmith" in the authentication request

Detailed Analysis

Through analysis of the SMB authentication packets in the network capture, the investigation identified that a user account associated with "janesmith" attempted to authenticate to the poisoned resource provided by the attacker. When the victim workstation received the poisoned response pointing to the attacker's system, it subsequently attempted SMB authentication to that system. The SMB authentication attempt contained the username of the authenticated user.

Why This Matters

Identifying compromised user credentials is essential for several critical security operations:

1. Password resets can be forced for the affected user account
2. All sessions from this account can be terminated across the network
3. Access control lists and file sharing permissions can be reviewed and modified
4. The affected user can be notified of the compromise
5. Audit logs can be searched for other activities performed by this account during the compromise window
6. Additional security training can be provided to the affected user
7. Risk assessment can determine if the user account had elevated privileges that could have enabled further attacks

Investigation Methodology

To identify compromised user accounts, an investigator would:

1. Filter Wireshark to display SMB authentication packets from the rogue machine IP (192.168.232.215)
2. Expand the SMB session setup request packets
3. Locate the username field within the SMB authentication header
4. Document the exact username and domain information
5. Cross-reference with HR systems to identify the actual person
6. Check the timestamp of the authentication to establish the timeline of compromise
7. Search for other authentication attempts by this username during the incident window
8. Verify if the account was used for any unauthorised activities after compromise
9. Check for any lateral movement using this account's credentials

---

Question 5: Identifying the Attacker's Target System

Lab Question: As part of our investigation, we aim to understand the extent of the attacker's activities. What is the hostname of the machine that the attacker accessed via SMB?

Answer: AccoutingPC

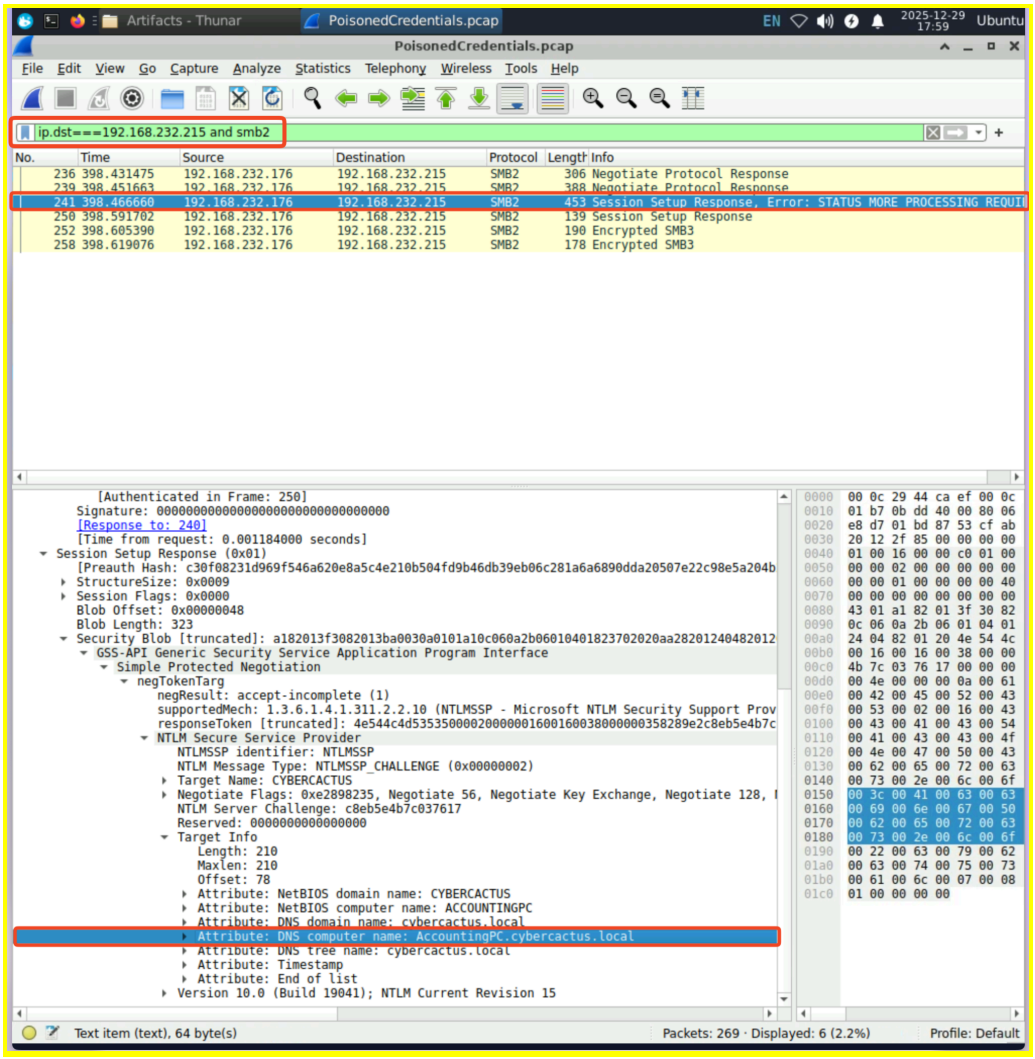

Figure 6: SMB authentication exchange, revealing the attacker's final target hostname "AccoutingPC" within the NTLM security blob

Detailed Analysis

The attacker's poisoning attack succeeded in capturing the credentials of Jane Smith's workstation. The network traffic analysis revealed that these captured credentials were subsequently used to establish an SMB connection to a “AccountingPC”. The SMB protocol handler and session information identified that the target machine was "AccountingPC.cybercactus.local," which is an indicator of an accounting system based on the naming convention.

This represents a severe escalation of the attack. Domain controllers are the most critical systems in Windows network environments, as they manage authentication, authorization, and network access for all domain-connected systems. If an attacker gains access to a domain controller, they can:

1. Reset passwords for any user account
2. Create new privileged accounts
3. Modify group policies affecting all network systems
4. Extract password hashes for all users
5. Establish persistence across the entire network
6. Disable security monitoring and auditing
7. Grant themselves administrative privileges on any system

Why This Matters

Identifying that the attacker accessed a domain controller indicates that this incident represents a critical security breach requiring immediate containment. This is not simply a credential capture incident but potentially a complete network compromise. The attacker has demonstrated intent and capability to access the most critical infrastructure asset.

Investigation Methodology

To identify the target system, an investigator would:

1. Filter Wireshark to display all SMB packets from the rogue machine IP (192.168.232.215)
2. Look for SMB "Session Setup Request" packets establishing new authentication
3. Examine the destination IP addresses of these SMB connections
4. Expand the SMB protocol header to view the server hostname field
5. For packets that do not contain the hostname directly, examine the SMB2 header
6. Look for the target system name in the SMB authentication exchange
7. Cross-reference the destination IP with the organizational network documentation
8. Verify the system name matches the IP address and confirming it is a domain controller
9. Check the domain information to confirm the system is part of the target organisation
10. Document the exact timestamp of the unauthorized SMB connection

---

Lab Objectives

The PoisonedCredentials lab is designed to achieve the following educational and defensive objectives:

1. **Protocol Vulnerability Understanding:** Participants gain deep knowledge of LLMNR and NBT-NS protocol vulnerabilities and understand why these legacy protocols remain exploitable in modern networks.
2. **Attack Recognition:** Through hands-on network analysis, participants learn to recognize the indicators of LLMNR and NBT-NS poisoning attacks in network traffic captures.
3. **Forensic Analysis Skills:** The lab develops practical skills in using Wireshark for network forensic investigation, including packet filtering, protocol analysis, and attack timeline reconstruction.
4. **Incident Scope Determination:** Participants practice identifying the full scope of a security incident, including all affected systems and compromised accounts.
5. **Threat Actor Identification:** The investigation techniques reveal how to identify attacker IP addresses and tools used in LLMNR poisoning attacks.
6. **Real-World Applicability:** The scenario reflects actual attack methodologies used in real-world network breaches, ensuring that skills learned are directly applicable to operational security roles.

Key Findings Summary

Finding	Implications	Severity
Mistyped query "fileshaare" by 192.168.232.16	User error triggered attack chain; indicates need for resource name standardisation and user training	Medium
Rogue machine at 192.168.232.215	Active attacker on network segment; network poisoning attack in progress; immediate isolation required	Critical
Second affected machine 192.168.232.176	Multiple machines vulnerable to same attack; broader network segment affected than initially apparent	High
Compromised account "Jane Smith"	Legitimate user credentials captured; all activities from this account must be audited; account requires password reset	High
Unauthorized SMB access to “AccountingPC”	Domain controller accessed with compromised credentials; potential for complete network compromise; indicates breach of critical infrastructure	Critical
Multiple poisoned queries for "fileshaare"	Attacker systematically poisoned multiple resource names; attack was not limited to single resource; suggests proactive attacker positioning	High
SMB authentication capture and relay	Attacker successfully harvested credentials through poisoning; credentials valid for domain authentication; indicates network-wide credential validity	Critical
Timeline shows rapid escalation	From initial poisoning query to domain controller access within same incident window; attacker exhibited operational efficiency	Critical

Recommendations and Mitigations

Immediate Actions

The following actions must be taken immediately to contain the incident and prevent further damage:

Network Isolation and Containment

1. Immediately isolate the rogue machine (192.168.232.215) from the network by:
    - Blocking all traffic to and from this IP address at the network perimeter
    - Disabling the network interface on the switch port connected to this system
    - Documenting the exact physical location of the system for forensic analysis
2. Isolate all affected machines (192.168.232.162 and 192.168.232.176) to a contained network segment where they cannot reach critical infrastructure but can be analysed.
3. Implement network segmentation to prevent affected machines from accessing sensitive systems, particularly domain controllers and file servers.

Credential Management

1. Immediately reset the password for the janesmith user account with a strong, randomly generated password.
2. Invalidate all existing authentication tokens and sessions for this account across all systems.
3. Search for and terminate any remote desktop protocol (RDP) or other remote access sessions associated with this account.
4. Check Active Directory audit logs for any other authentication events using this account during the incident window.

Domain Controller Protection

1. Place the domain controller (AccountingPC) in a heightened monitoring state with real-time alerting for any suspicious activities.
2. Review the domain controller's security event logs for any unauthorized object modifications, group policy changes, or privilege escalation attempts.
3. Verify that domain controller backups are intact and recent, ensuring recovery capability if the system is found to be compromised.
4. Implement emergency network access controls to limit which machines can connect to the domain controller during investigation.

Evidence Preservation

1. Preserve the network traffic capture files and ensure they are stored in a write-protected, forensically sound manner.
2. Capture forensic images of all affected machines, including the rogue system before any clean up or remediation.
3. Preserve server and application logs covering the entire incident timeframe.
4. Document the physical network topology and connections for the affected network segment.

Long-Term Security Improvements

Protocol Hardening

1. Disable LLMNR Network-Wide: LLMNR provides minimal value in modern networks with properly functioning DNS infrastructure. Configure Group Policy to disable LLMNR on all Windows systems.
    - Group Policy Setting: Computer Configuration > Administrative Templates > Network > DNS Client > Turn off multicast name resolution
2. Disable NBT-NS Where Possible: Similarly, NBT-NS is primarily needed for legacy systems. Disable NBT-NS on all modern systems, while maintaining support only where absolutely necessary for legacy application compatibility.
    - DHCP Configuration: Configure DHCP Option 015 to remove NetBIOS name services
3. Implement DNS Security Extensions (DNSSEC): Deploy DNSSEC to ensure DNS responses are authenticated and cannot be spoofed, reducing reliance on insecure fallback protocols.

Network Architecture Improvements

1. Network Segmentation: Implement robust network segmentation separating user workstations from servers, servers from domain controllers, and different functional areas from each other. Use firewalls and access control lists to enforce segmentation.
2. Secure Network Access: Implement network access control (NAC) solutions that validate device compliance before allowing network access, preventing unauthorized devices from connecting to the network.
3. Network Monitoring: Deploy network monitoring solutions that specifically detect LLMNR and NBT-NS poisoning attacks, alerting security operations centre staff when suspicious name resolution patterns are detected.
4. SMB Security: Enable SMB signing on all systems and enforce it on domain controllers. While this creates some performance overhead, it prevents relay attacks even if credentials are captured.

Credential Protection

1. Multi-Factor Authentication (MFA): Implement multifactor authentication for all user accounts, particularly administrative accounts. This prevents attackers from using captured credentials for authentication.
2. Credential Guard: Deploy Windows Defender Credential Guard on all systems to protect credentials in memory, preventing tools from easily harvesting hashes and plaintext passwords.
3. Password Policies: Implement strong password policies requiring:
    - Minimum length of 14 characters
    - Complexity requirements
    - Regular password rotation
    - Prevention of password reuse
4. Privileged Access Management: Implement privileged access management (PAM) solutions that manage and monitor access to critical systems, preventing unauthorized use of privileged credentials.

Monitoring and Detection

1. Security Information and Event Management (SIEM): Deploy SIEM solutions that collect and analyse security events from all systems, enabling rapid detection of attacks in progress.
2. SMB Monitoring: Implement detailed SMB protocol monitoring and alerting for:
    - Unexpected authentication attempts to domain controllers
    - Authentication with unusual accounts
    - Failed authentication attempts followed by successful ones from different sources
    - Credential relay attacks
3. DNS Monitoring: Monitor DNS query patterns for:
    - Unusual or misspelled resource names
    - Queries for resources that don't exist in the organization
    - High frequency of similar malformed queries
4. Endpoint Detection and Response (EDR): Deploy EDR solutions on all user workstations and servers to detect suspicious processes, file modifications, and network connections.

User Education and Awareness

1. Security Training: Provide regular security awareness training covering:
    - How to recognise phishing and social engineering attacks
    - The importance of reporting suspicious network activity
    - Password security and credential protection
    - The dangers of connecting to unfamiliar network resources
2. User Resource Naming: Standardize resource naming conventions and maintain updated, accessible directories of network resources. This reduces the likelihood of users mistyping resource names and triggering poisoning attacks.
3. Incident Reporting: Establish clear procedures for users to report suspected security incidents, and ensure they understand that reporting suspicious activity will not result in punishment.

Patch Management and Updates

1. System Hardening: Ensure all systems are fully patched with the latest security updates.
2. Legacy System Evaluation: Conduct a complete inventory of systems and identify any that require LLMNR or NBT-NS support. Plan for the gradual retirement and replacement of legacy systems that cannot be secured through modern protocols.
3. Vendor Communication: Contact system and application vendors to understand any dependencies on LLMNR or NBT-NS, and work toward removing these dependencies.

Compliance and Governance

1. Security Policies: Update security policies to explicitly address:
    - Requirements for network segmentation
    - Mandatory use of modern authentication protocols
    - Requirements for MFA on administrative accounts
    - Standards for network resource naming and documentation
2. Incident Response Plan: Update the incident response plan with specific procedures for handling LLMNR and NBT-NS poisoning attacks, including escalation paths and communication templates.
3. Regular Assessments: Conduct regular security assessments and penetration testing, specifically targeting:
    - LLMNR and NBT-NS poisoning vulnerabilities
    - Credential capture and relay attack vectors
    - Network segmentation effectiveness

Conclusion

The PoisonedCredentials lab incident represents a critical real-world attack scenario that exploits fundamental vulnerabilities in legacy Windows name resolution protocols. The investigation successfully traced the attack from its initiation through a user's simple typographical error, identified the attacker's position on the network, captured evidence of credential harvesting, and determined that the attack resulted in unauthorized access to critical domain infrastructure.

The incident demonstrates that security requires a multi-layered approach encompassing technical controls, user education, monitoring and detection capabilities, and robust incident response procedures. While modern organizations cannot eliminate legacy protocols without accepting significant operational costs, they can substantially reduce risk through network hardening, enhanced monitoring, and architectural improvements.

Organizations must recognize that attacks often exploit human behaviour and simple mistakes rather than sophisticated technical flaws. The most effective defence combines technical controls that limit the impact of such mistakes with monitoring systems that rapidly detect when mistakes occur, enabling swift response before attackers can establish persistence or escalate privileges within the network environment.

END OF REPORT