GOTHAM CORP
Security Assessment Findings Report

Business Confidential

Date: July 25th, 2025
Project: DC-001

Version 1.0

1. Table of Contents

Confidentiality Statement

This document is the exclusive property of GOTHAM CORP and WASP SECURITY Security (WASP SECURITYS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both GOTHAM CORP and WASP SECURITYS.

GOTHAM CORP may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. WASP SECURITY prioritized the assessment to identify the weakest security controls an attacker would exploit. WASP SECURITY recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

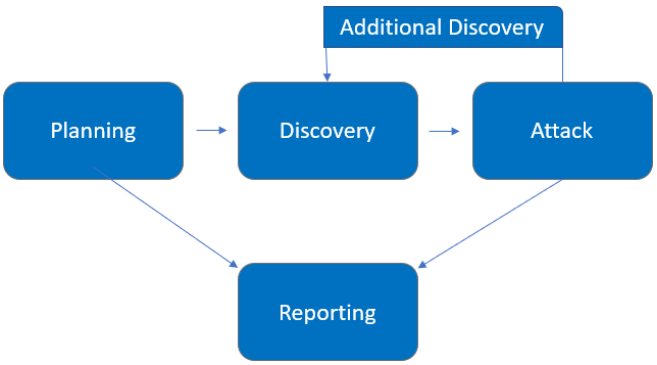
Name	Title	Contact Information
GOTHAM CORP		
Bruce Wayne	Global Information Security Manager	Email: BruceWayne@gothamcorp.com
WASP SECURITY Security		
Tiya Nelson	Lead Penetration Tester	Email: tiyanelson@WASP SECURITY-sec.com

Assessment Overview

From February 22nd, 2025 to March 5th, 2025, GOTHAM CORP engaged WASP SECURITY to evaluate the security posture of its infrastructure compared to current industry's best practices that included an internal network penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test	Blue Box – 10.10.10.40 Dev Box – 10.10.10.5 Butler Box – 10.0.2.80

Scope Exclusions

Per client request, WASP SECURITY did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by GOTHAM CORP.

Client Allowances

GOTHAM CORP provided WASP SECURITY the following allowances:

- Internal access to network via Dropbox and port allowances

Executive Summary

WASP SECURITY evaluated GOTHAM CORP's internal security posture through penetration testing from February 22nd, 2025 to March 5th, 2025. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not allow denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for ten (10) business days.

Testing Summary

The internal network penetration test for **GOTHAM CORP** was conducted to evaluate the organization's Active Directory (AD) security posture. The engagement focused on real-world attack paths leveraging **name resolution poisoning**, **NTLMv2 relay**, and **post-compromise privilege escalation** using tools such as Responder, Hashcat, and ntlmrelayx.

During testing, the WASP SECURITYS team passively captured NTLMv2 hashes from misconfigured hosts and used relay techniques to gain access to low-privileged domain accounts. These credentials were further used to identify high-value AD objects, ultimately resulting in the compromise of a **Domain Administrator** account. The team also identified additional broadcast domain traffic that exposed a separate user (Joe) and system (DESKTOP-IMJ19PA) vulnerable to similar attacks.

.

Key Findings Summary:

- **KRONK NTLMv2 Hash Capture & Relay**:
  Using Responder, the team captured an NTLMv2 hash from user `KRONK`. The password was cracked offline using Hashcat (`Spring1979`). The credential was successfully relayed using `ntlmrelayx`, providing access to LDAP and allowing the tester to enumerate Active Directory. This led to the discovery and compromise of a **Domain Administrator** account.
- **JOE NTLMv2 Hash Exposure via LLMNR**:
  In a separate broadcast domain, the team identified that `DESKTOP-IMJ19PA` responded to poisoned LLMNR queries. This resulted in the exposure of user `Joe`'s NTLMv2 hash. Though cracked access was not confirmed during this assessment, the repeated broadcast responses indicate a critical misconfiguration.

Tester Notes and Recommendations

The assessment highlighted that GOTHAM CORP's Active Directory environment is vulnerable to **legacy protocol exploitation** and lacks **basic segmentation and monitoring controls**. Both hash capture and credential relay attacks were successful due to default configurations and the presence of LLMNR and NTLMv2.

Recommendations:

1. **Disable LLMNR and NetBIOS Name Service** on all endpoints via Group Policy (per CISA and NIST CM-7).
2. **Enforce SMB signing and LDAPS** to mitigate NTLMv2 relay attacks (SC-12, AC-17).
3. **Apply strong password policies** and prohibit the reuse of weak, seasonal credentials.
4. **Monitor internal DNS resolution**, and ensure no fallback to insecure methods.
5. **Implement host-based intrusion detection systems (HIDS)** and central logging for suspicious authentication behavior.

Key Strengths and Weaknesses

1. The environment responded predictably to enumeration tools, allowing security validation.

2. NTLM relay was mitigated on SMB (indicating SMB signing is enabled in some cases).

3. Domain segmentation allowed for successful targeting and discovery of multiple hosts, proving useful for internal defense review.

Weakness:

- **LLMNR and NBT-NS were enabled across multiple subnets**, allowing for name poisoning and credential capture.

- **NTLMv2 was accepted and relayed successfully via LDAP**, leading to domain user access and privilege escalation.

- **Weak passwords were used** (e.g., `Spring1979`), and cracked with minimal effort using standard wordlists.

- **Domain credentials were reused** and escalated across services with no alerting or detection.

- **Lack of monitoring** allowed for Responder, relay, and enumeration activity without interruption.

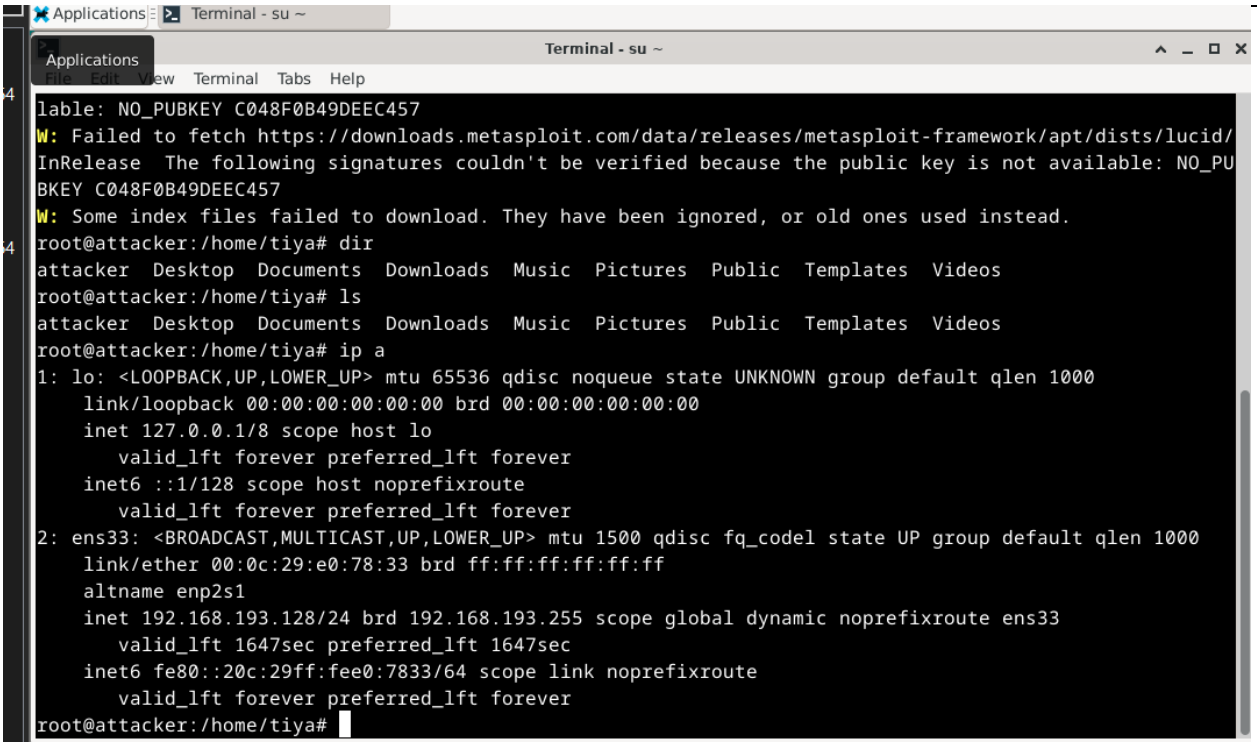
Technical Findings

Internal Penetration Test Findings

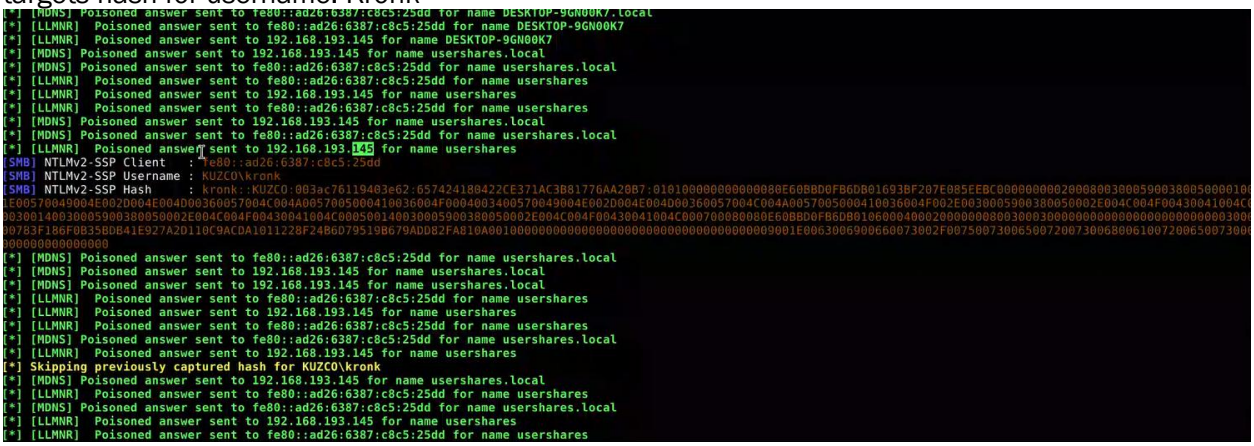
Finding AD-005: LLMNR Poisoning + NTLMv2 Relay Attack Leading to Domain Administrator Compromise (Critical)

Description:	The internal Active Directory environment was assessed by capturing and relaying credentials through **LLMNR poisoning** using the responder tool. From the attacker's machine, broadcast requests were monitored, which revealed an NTLMv2 hash for the user **KRONK**. The hash was successfully cracked offline using **Hashcat** with a customized wordlist (rockyou.txt) focused on seasonal and year-based passwords. This revealed the password **Spring1979**. Using this credential, the tester attempted a **relay attack** targeting kuzco, but initial probes were unsuccessful. A follow-up **Nmap scan** identified 192.168.193.185 as a likely **domain controller (DC)**. While SMB signing prevented direct SMB relays, **LDAP relays** were successfully executed using ntlmrelayx. The relayed access as KRONK provided **low-privilege domain user** access. Upon further enumeration, additional domain user credentials were harvested, including one belonging to a **Domain Administrator** account. This resulted in full compromise of the Active Directory domain.
Risk:	Likelihood: High – The attack leveraged default protocols and services (LLMNR, NTLMv2) still enabled in many AD environments. Impact: Critical – Successful relay and lateral movement led to full domain administrator compromise.
System:	Active Directory Domain Victim hosts that responded to LLMNR/NetBIOS broadcasts Domain Controller at 192.168.193.185
Tools Used:	Responder, Hashcat, Rockyou.txt wordlist, Nmap, ntlmrelayx, LDAP, BloodHound-style enumeration
References:	NVD - CVE-2019-1040 NVD - CVE-2023-23397

Evidence



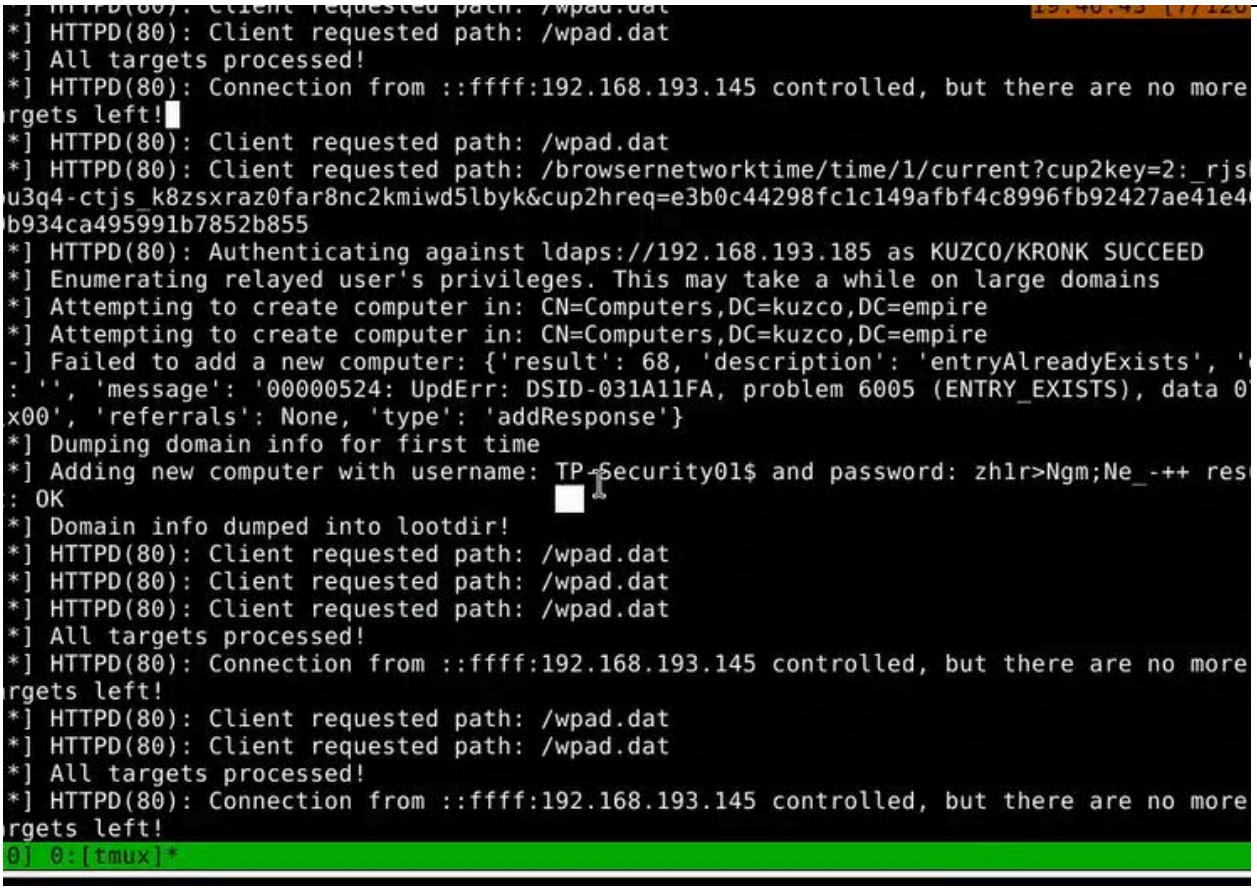
Was able to use the user responder on my attacker box to listen to Victim 1 which revealed and captured the targets hash for username: Kronk



I attempted to crack the captured NTLMv2 hash using **Hashcat**, utilizing the **rockyou.txt** wordlist with a focus on seasonal password patterns and common year-based variations.

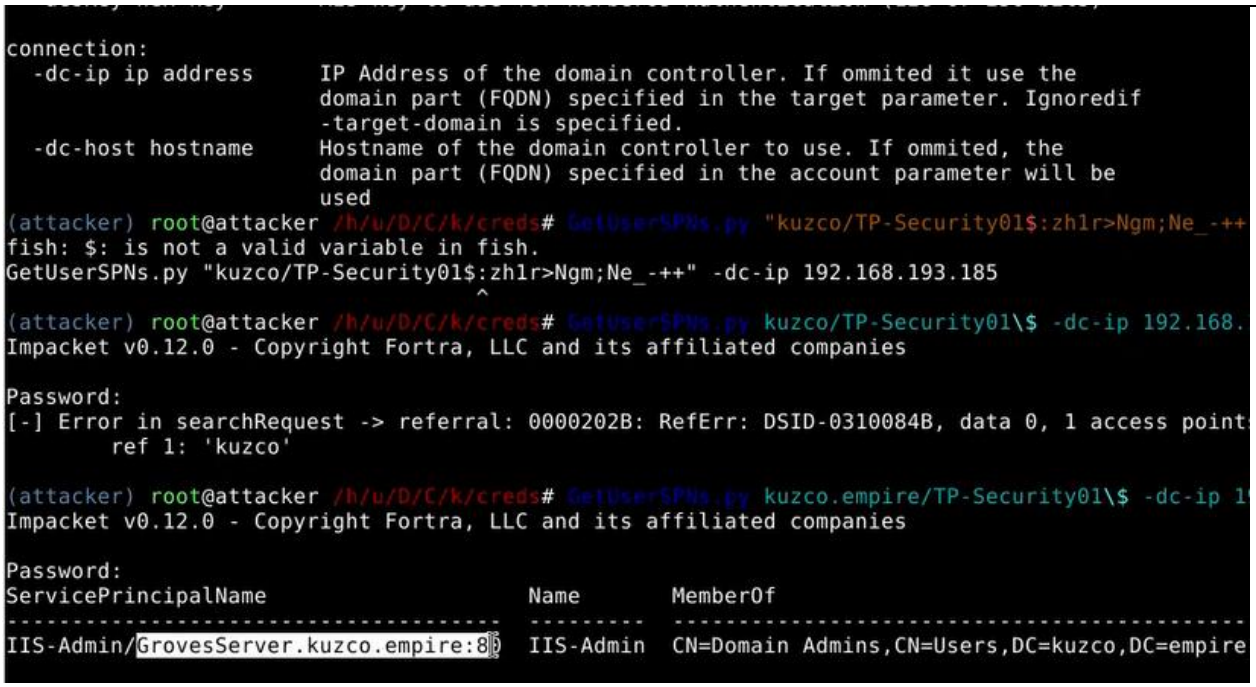
Next, I initiated an **NTLM relay attack** using **Responder**. An initial attempt to interact with the host kuzco via ICMP returned no response. I then conducted an **Nmap scan** from my attacker machine, which revealed that **192.168.193.185** was likely the **domain controller**.

Although I attempted to run SMB enumeration scripts, SMB signing appeared to be enforced, preventing successful SMB relays. I proceeded to conduct an **LDAP-based relay attack using ntlmrelayx**, which successfully executed **two relay attempts**, confirming viable interaction with the domain infrastructure.



Following a successful relay of **KRONK's** credentials, I obtained **low-privileged access to the domain**. The associated computer object was confirmed to be a member of the **Domain Users** group, allowing impersonation and user-level access across the environment.

With this foothold, I conducted additional enumeration, which led to the discovery of **further domain objects**—including a **Domain Administrator account and its associated password**, resulting in full domain compromise.



Which revealed a domain admin.

Remediation

Per CISA & NIST Guidance:

Disable LLMNR and NetBIOS via GPO to prevent broadcast poisoning attacks (NIST CM-7, SC-7).

Enforce SMB signing and LDAPS to prevent credential relay attacks over insecure protocols.

Implement Extended Protection for Authentication (EPA) in AD (SI-4, AC-17).

Use Local Admin Password Solution (LAPS) and segment privileged credentials.

Per OWASP:

Harden authentication across the domain by:

Enforcing strong password policies (AC-2, IA-5)

Disabling legacy protocols like NTLM where possible

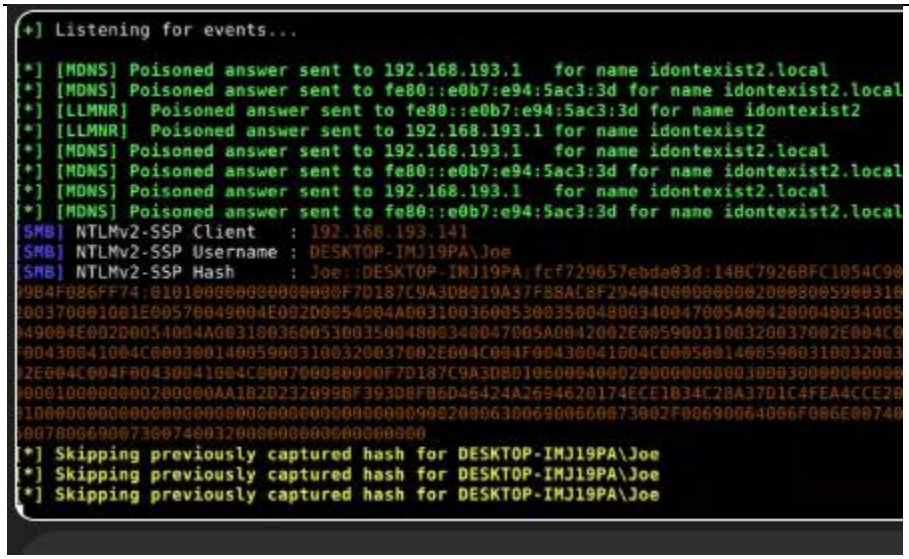
Monitoring for unusual authentication patterns

Implement tiered administrative model and segment privileges across user groups.

AD-006: LLMNR/NBT-NS Poisoning Reveals Additional NTLMv2 Hashes on Internal Segment (High)

Description:	While monitoring for name resolution traffic using **Responder**, the assessment team identified a secondary broadcast domain where **Link-Local Multicast Name Resolution (LLMNR)** and **NetBIOS Name Service (NBT-NS)** were enabled. The system at 192.168.193.141 responded to a poisoned broadcast query for the non-existent hostname idontexist2.local. As a result, **NTLMv2 challenge-response authentication** was initiated by the user **Joe** from the host **DESKTOP-IMJ19PA**, and the corresponding hash was successfully captured. The presence of repeated attempts from the same host, as shown in the log, suggests a persistent misconfiguration in the network where LLMNR/NBT-NS broadcasts are occurring frequently without DNS resolution fallback.
Risk:	Likelihood: High – Default Windows behavior enables LLMNR/NBT-NS, and the attack requires minimal privileges. Impact: High – Captured hashes can be cracked offline or relayed in real time, potentially resulting in lateral movement or full domain compromise depending on user privileges.
System:	Host: DESKTOP-IMJ19PA User: Joe IP: 192.168.193.141 Domain Resolution Request: idontexist2.local
Tools Used:	Responder
References:	NVD - CVE-2018-17552 NVD - CVE-2018-17553

Evidence



Remediation

Per CISA & NIST SP 800-53:

Disable LLMNR and NBT-NS via Group Policy across all systems (NIST SC-7, CM-7).

Implement DNS hardening to ensure proper resolution before fallback mechanisms are used.

Enforce SMB signing and restrict NTLM authentication wherever possible (AC-17, IA-5).

Apply Privileged Access Management (PAM) to reduce lateral movement risk from captured hashes.

Per OWASP and MITRE Guidance:

Train users to recognize login anomalies during attacks.

Monitor for repeated authentication attempts using poisoned credentials.

Deploy network segmentation and internal DNS monitoring to detect unnecessary LLMNR traffic.