INVISIBLE ATTACK PATHS: A CHALLENGE FOR IDENTITIES

WHY NTLM RELAY ATTACKS REMAIN YOUR BIGGEST BLIND SPOT

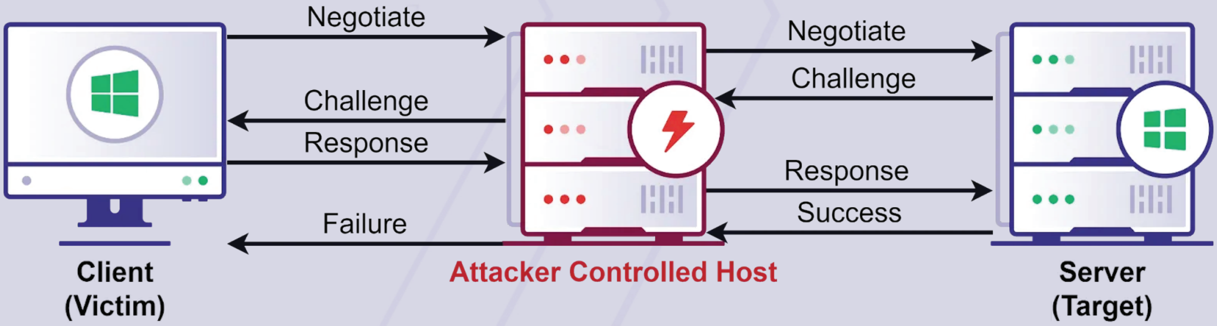
While many security leaders consider NTLM relay attacks a solved problem, they remain one of the most effective and frequently used techniques for adversaries to compromise enterprise environments. These attacks allow attackers with minimal access to rapidly gain control of critical systems by exploiting how Windows authentication works across your network.

> "Relay attacks are the easiest way to compromise domain-joined hosts nowadays, paving a path for lateral movement and privilege escalation."

WHY THIS MATTERS TO YOUR ORGANIZATION

NTLM relay attacks create a troubling scenario where any authenticated user in your environment can potentially:

- Compromise systems without needing to crack passwords
- Move laterally through your environment with minimal footprint
- Gain administrative control of critical systems
- Bypass many traditional security controls
- Execute attacks that most security technologies fail to detect



Even more concerning, many organizations unknowingly operate with default configurations that leave them exposed, creating millions of potential attack paths across the enterprise. And it's still a problem: according to The Hacker News, last fall Microsoft advised rapid remediation of the third actively exploited NTLM vulnerability in 2024. These vulnerabilities revealed a user's NTLMv2 response, leaving organizations vulnerable to potential unauthorized access and lateral movement.

SPECTEROPS

THE VISIBILITY GAP

Traditional security tools focus on vulnerabilities, patching, and threat detection, but miss the fundamental attack paths created by identity relationships. Modern environments have multiple identity systems (Active Directory, Entra ID, AWS IAM, 3rd-party IdP), creating complex chains of access that create exploitable paths for attackers.

This is why BloodHound Enterprise's attack path management approach is critical. It allows you to:

1. **Visualize the Invisible:** Map all NTLM relay attack paths across your environment, showing exactly how attackers could move from initial access to critical assets
2. **Understand Real Risk:** Identify which systems are vulnerable to NTLM relay attacks based on their current configurations (SMB signing, LDAP security settings, ADCS configuration, client compatibility)
3. **Prioritize Effectively:** Focus remediation on the most critical attack paths rather than trying to "fix everything everywhere"
4. **Preserve Legacy Systems:** Targeted remediations preserve business-critical legacy communications while removing relay attack paths from the attacker's arsenal.
5. **Measure Security Improvement:** Track your progress in eliminating NTLM relay attack paths over time

STRATEGIC GUIDANCE FOR DECISION MAKERS

Rather than implementing disruptive security measures across your entire environment, BloodHound Enterprise enables you to:

- Focus on securing the most critical attack paths first
- Make targeted configuration changes only where needed
- Balance security needs with operational requirements
- Demonstrate measurable risk reduction to stakeholders

THE BOTTOM LINE

NTLM relay attacks represent one of the paths of least resistance in modern enterprise environments.

By implementing BloodHound Enterprise's attack path management approach, you can eliminate such attack paths before adversaries can exploit them, significantly reducing your organization's identity risk and protecting your most valuable assets.

TAKE THE NEXT STEP

Email **salesteam@specterops.io** to request a customized demo. Our security experts will demonstrate how BloodHound Enterprise can immediately identify and prioritize critical attack paths in your environment.