MIRAGE

Report

Topic	Security Transition Plan: Deprecating NTLM Authentication at Mirage.htb
Writer	Active Directory Security Team
Date	Apr 11, 2025

Summary

This report outlines the phased deprecation of NTLM authentication within the Mirage Active Directory environment. NTLM is a legacy authentication protocol that lacks modern security features and is vulnerable to several attacks, including credential relaying and pass-the-hash.

To align with current security best practices, Mirage is moving toward a **Kerberos-only authentication model**. The transition is designed to be gradual and well-monitored to avoid service disruption and ensure all systems are compliant.

Timeline of Events:

- **April 2025 :** Project kickoff: NTLM usage review initiated
- **May 2025 :** Auditing enabled for all incoming NTLM authentication.
- **May 2025:** Inbound NTLM blocked on pilot systems (non-critical servers)
- **June 2025 :** Audit reports analyzed; system owners notified of NTLM usage.
- **July 2025 :** Migration plans created for systems requiring NTLM
- **Aug 2025 :** Begin Kerberos-only enforcement in selected Test OUs
- **Q4 2025 Target :** Full domain-wide NTLM disablement

Objective:

We are working to fully eliminate NTLM authentication from our Active Directory environment to strengthen overall domain security. Our objective is to enforce Kerberos-only authentication across all systems, reduce the risk of legacy protocol attacks, and ensure that all critical services operate securely without reliance on outdated methods.

Current Status :

We are currently auditing all incoming NTLM authentication requests at the domain controller level and have disabled inbound NTLM on selected non-critical systems. Our team is actively reviewing these audit logs to identify legacy devices and applications that still rely on NTLM, allowing us to prepare tailored migration plans for each case.

Rationale :

We are taking this step because NTLM is an insecure protocol that lacks mutual authentication and is vulnerable to several well-known attack techniques. By identifying and phasing out its use now, we can prevent potential exploitation in the future and align our authentication strategy with modern, secure standards like Kerberos.

Next Steps :

We are continuing to monitor NTLM usage and will contact affected system owners to assist with migration. Over the coming months, we will expand NTLM blocking across more systems and organizational units, conduct controlled tests in isolated environments, and ultimately enforce domain-wide NTLM disablement by Q4 2025.

Prepared by:
Active Directory Security Team
IT Security Department – Mirage.htb
Contact: ad-security@mirage.htb