

NTLM RELAY & AUTHENTICATION.



NTLM relay forwards a live authentication exchange to a service that accepts it as the victim. **The attacker need not know the password: reduce NTLM use and enforce protection at every receiving service.**

- REQUIRED MESSAGE SIGNING
- TLS CHANNEL BINDING
- EXTENDED PROTECTION (EPA)
- NTLM DEPENDENCY REDUCTION

01 THE MECHANISM

Challenge and Response

NTLM authentication uses a server challenge and a response derived from the client's secret. **The password is not sent in plaintext.** A valid response proves access to credentials, but needs additional protection against forwarding to another service.

A Live Exchange Is Forwarded

An attacker induces authentication and passes the target's challenge to the victim, then forwards the victim's response. **Relay is not password cracking or pass-the-hash.** A receiving service with insufficient protections may accept the exchange.

The Receiving Service Matters

Required message signing protects integrity; channel binding and Extended Protection for Authentication (EPA) tie authentication to its context. **Each target protocol needs its own enforced controls.** Securing an SMB target does not harden an HTTP endpoint.

02 THE FLOW

The Protected Authentication Path

VERIFIED

1

The client connects to the intended service. Prefer **Kerberos where supported**; identify applications that still negotiate or require NTLM.

2

The receiving service requires the applicable protection: **signed messages or validated channel/service binding**. Missing required proof is rejected.

3

The server processes only the permitted authenticated requests and applies **least-privilege access**. Logs preserve the client, account, and target context.

Victim to Relay to Target

ABUSED

1

Victim: a user or computer authenticates to an attacker-controlled endpoint after coercion, deceptive name resolution, or a misleading resource reference.

2

Relay: the attacker forwards challenge-and-response messages between the victim and a reachable service. The password does not have to be recovered.

3

Target: if it accepts the exchange without effective relay defenses, the attacker can act with the victim's permitted access. **Impact depends on the target and privileges.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Reduce NTLM Dependencies	Inventory client, server, and application use. Repair name/SPN issues and migrate supported flows to Kerberos; restrict remaining NTLM in stages.
Require Target Protection	Require SMB signing and LDAP signing where applicable. Verify inbound server policy; client-side settings alone are not a complete target inventory.
Bind TLS Authentication	Enforce LDAP channel binding and service-specific EPA where supported. Test proxies and TLS termination; encryption alone does not bind authentication.
Limit Reach & Observe	Patch coercion vulnerabilities, retire unnecessary name-resolution fallbacks, restrict unneeded traffic, and correlate authentication with target activity.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
NTLM Usage Audits	No	Finds dependencies and unexpected paths, but legitimate NTLM traffic is common and use alone does not prove relay.
Name-Resolution Alerts	No	Detects suspicious discovery or spoofing, but coercion and relay can occur without name-resolution poisoning.
Failed Logons Only	No	A relay may appear as a successful network logon (4624) on the target; no failed-password spike is required.
Signing / Binding Failures	No	Reveals rejected or incompatible clients, but successful abuse at another unprotected endpoint can remain invisible.
Correlated Target Activity	No	Join client, relay-host, logon, and service evidence. Validate coverage and investigate context; no universal relay event exists.

NTLM RELAY & AUTHENTICATION.

AUDIT · REQUIRE · RETIRE

05 PROGRAM OPERATIONS

Audit before restricting. Enable NTLM auditing and inventory normal authentication paths. Assign application owners to exceptions and test business-critical flows before enforcement.

Check effective server policy. Verify required signing, LDAP channel-binding enforcement, and EPA on actual endpoints. Updates, edition defaults, upgrades, and inherited policy can differ.

Validate both acceptance and rejection. Confirm approved clients still work and unsupported or unbound requests fail where protection is required. Include proxies, load balancers, and legacy devices.

Contain the effects, not just the exchange. Stop the relay path and preserve host and service evidence. Review directory changes, issued certificates, and active sessions; remediate each confirmed outcome.

06 CONTROL MAPPING

SMB TARGETS

Require inbound SMB signing: protects SMB message integrity. Verify client policy too, but assess non-SMB targets separately.

LDAP WITHOUT TLS

Require LDAP signing: reject unsigned SASL binds and cleartext simple binds. TLS-protected authentication needs its own binding checks.

LDAP OVER TLS

Require channel binding for supported authentication: validate CBTs for NTLM/SASL over TLS; account for client compatibility and enforcement mode.

HTTP AUTHENTICATION

Use HTTPS with required EPA where supported: follow the product's channel/service-binding and proxy guidance; remove unnecessary NTLM endpoints.

07 WHAT THIS DOES NOT SOLVE

Compromised Endpoints
A host that controls real credentials or session keys can still make **authorized-looking requests**. Relay protection does not remove malware.

Offline Password Cracking
Collected challenge responses may still enable **offline password guessing**. Blocking relay does not make weak passwords strong.

Other Identity Attacks
Kerberos ticket theft, certificate abuse, and stolen cloud sessions need **separate controls and response**.

Existing Access
Hardening a service does not undo **permissions, credentials, or sessions** already created through a successful attack.

08 MYTHS VS. REALITY

MYTH "NTLMv2 prevents relay."	REALITY NTLMv2 improves the response but does not prevent relay . Require the receiving protocol's protections.
MYTH "HTTPS or LDAPS alone solves the problem."	REALITY TLS protects transport. Channel binding connects authentication to that protected channel ; encryption alone does not provide that connection.
MYTH "SMB signing protects every relay destination."	REALITY It protects SMB communications. LDAP, HTTP, and other targets need their own controls ; inspect the actual receiving service.
MYTH "When supported means protection is required."	REALITY Compatibility settings can accept clients without binding information. Required or Always enforcement rejects missing proof where supported.
MYTH "A password reset removes all relay damage."	REALITY Relay need not reveal the password. Issued certificates, changed permissions, and existing sessions require separate investigation and cleanup.

09 SPEAK THE PROGRAM — KEY TERMS

RELAY
Forwarding a **live authentication exchange** so a different service accepts the attacker's connection as the victim.

CHALLENGE-RESPONSE
A protocol exchange that uses a fresh challenge and a **credential-derived response**, rather than sending a plaintext password.

MESSAGE SIGNING
A keyed integrity check that detects tampering and requires **proof of the session key** for protected messages.

CHANNEL BINDING TOKEN
A **CBT** links authentication to properties of its TLS channel, helping the verifier reject a relayed exchange.

EPA
Extended Protection for Authentication uses channel binding and/or service binding according to the application and transport.

COERCION
Inducing a user or computer to **initiate authentication to an attacker-chosen endpoint**, creating an opportunity for capture or relay.