SNIA DEVELOPER CONFERENCE
SDC 25
By Developers FOR Developers

Hyatt Regency Santa Clara, CA
September 15-17, 2025

Eliminating NTLM in Storage

Mariam Gewida | TPM, Microsoft
Tanmay Pydisetti | SDE, Microsoft

Microsoft

Agenda

01 What is NTLM and What are the Associated Security Risks?

02 Understanding NTLM's Role in SMB-Based Storage Access

03 Auditing NTLM Usage and Legacy Dependencies

04 Deep dive into Kerberos

05 Introducing IAKerb and LocalKDC

06 Walkthrough: Securing SMB with IAKerb & LocalKDC

07 Preparing to Disable NTLM in Storage Environments

SDC 25

What is NTLM and Why is it a Problem?

Windows NT LAN Manager (NTLM):

- A legacy authentication protocol from pre-Windows 2000
- Used primarily as a fallback authentication protocol in environments where Kerberos isn't available or can't be used
- It operates on a challenge/response mechanism to prove that a user knows the password associated with an account.

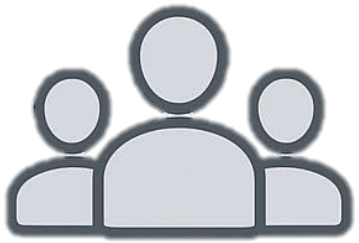
Why NTLM is insecure:

- No server verification/authentication: Clients can't verify who they're talking to → vulnerable to relay and man-in-the-middle attacks.
- Weaker cryptography reliance
- Relay and Replay Attacks.
- Pass-the-Hash: Attackers can reuse captured NTLM hashes.
- Prevalent in SMB traffic: NTLM authentication often rides SMB sessions in legacy systems or cross-domain/file share access.

Why is NTLM still used:

- Simple
- Legacy
- May be the only feasible option in some scenarios

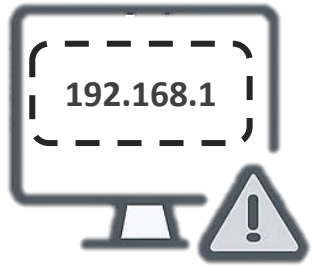
Where We're Seeing the Most NTLM Usage



Workgroup Environments

Cross-Domain Access w/o Trusts

Systems using Local Accounts



Misconfigures SPNs or IP Address

NTLM and SMB – A Legacy Bond

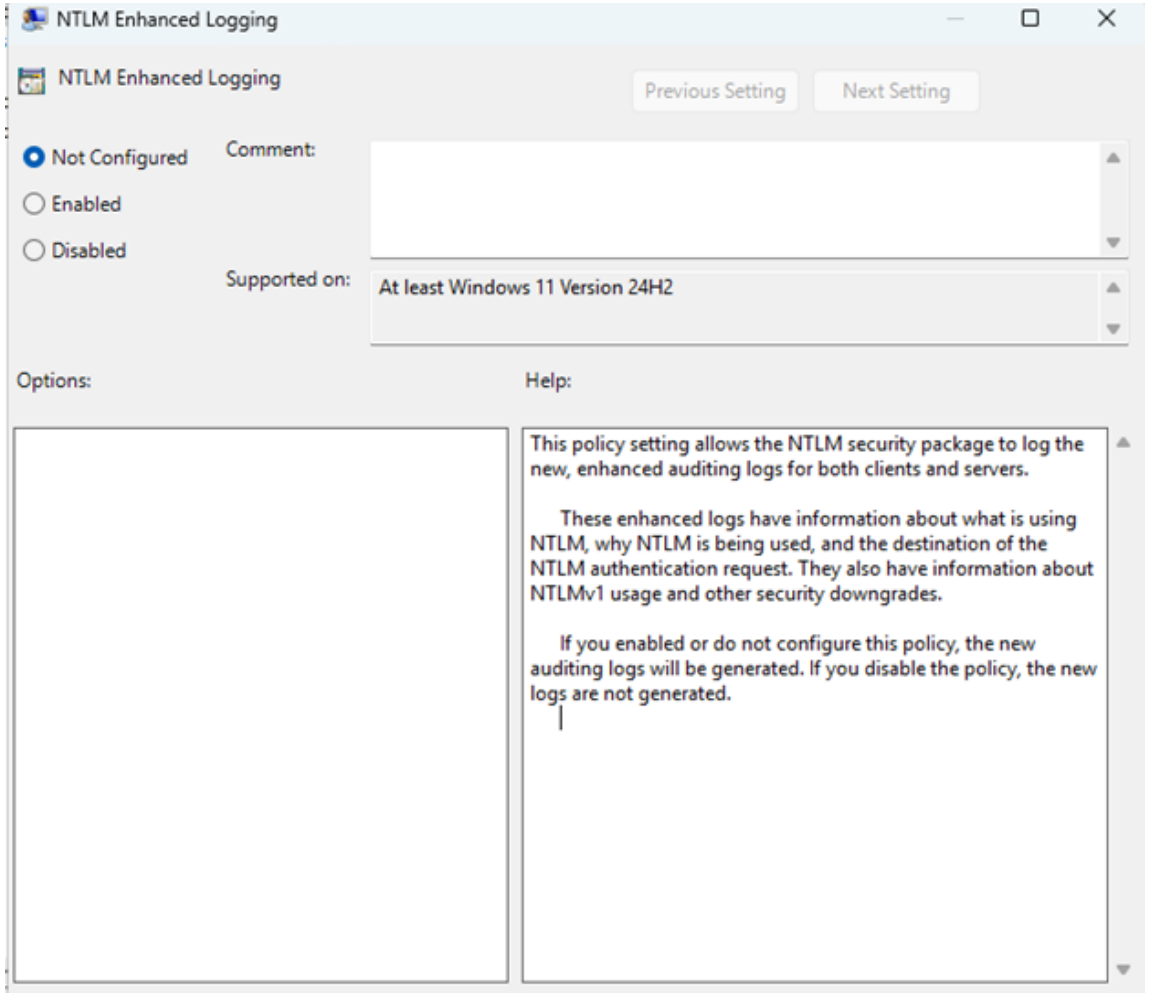
When a client wants to access a shared folder on a remote Windows server using SMB:

- **Initial Connection:** The client initiates an SMB session to the server (e.g., to access a shared file).
- **Authentication:**
  - If the client is not using Kerberos (e.g., due to being in a workgroup), SMB will use NTLM for authentication.
  - NTLM carries out the challenge-response exchange over the SMB connection.
- **Session Setup:** Once NTLM authentication is successful, SMB sets up the session and the client gains access to the requested resources.

Component	Purpose	Role in SMB Access
NTLM	Authentication	Validates the user's identity over the SMB connection
SMB	File/resource sharing	Transports authentication, then enables access

Bridging NTLM & SMB to Auditing: Why Visibility Matters

- NTLM remains deeply embedded in SMB-based storage access, especially in workgroup and legacy environments.
- Security risks persist due to NTLM's vulnerabilities.
- To move forward:
  - We need to understand *where*, *why*, and *how* NTLM is still being used.
  - Plan for a secure transition away from legacy protocols.



Let's explore the recently released enhanced NTLM auditing!

Overview of NTLM auditing enhancements in Windows 11, version 24H2 and Windows Server 2025 - Microsoft Support

NTLM Auditing: Finding the Hidden Dependencies

Enhanced Auditing is on-by-default in Windows 11, version 24H2 and Windows Server 2025

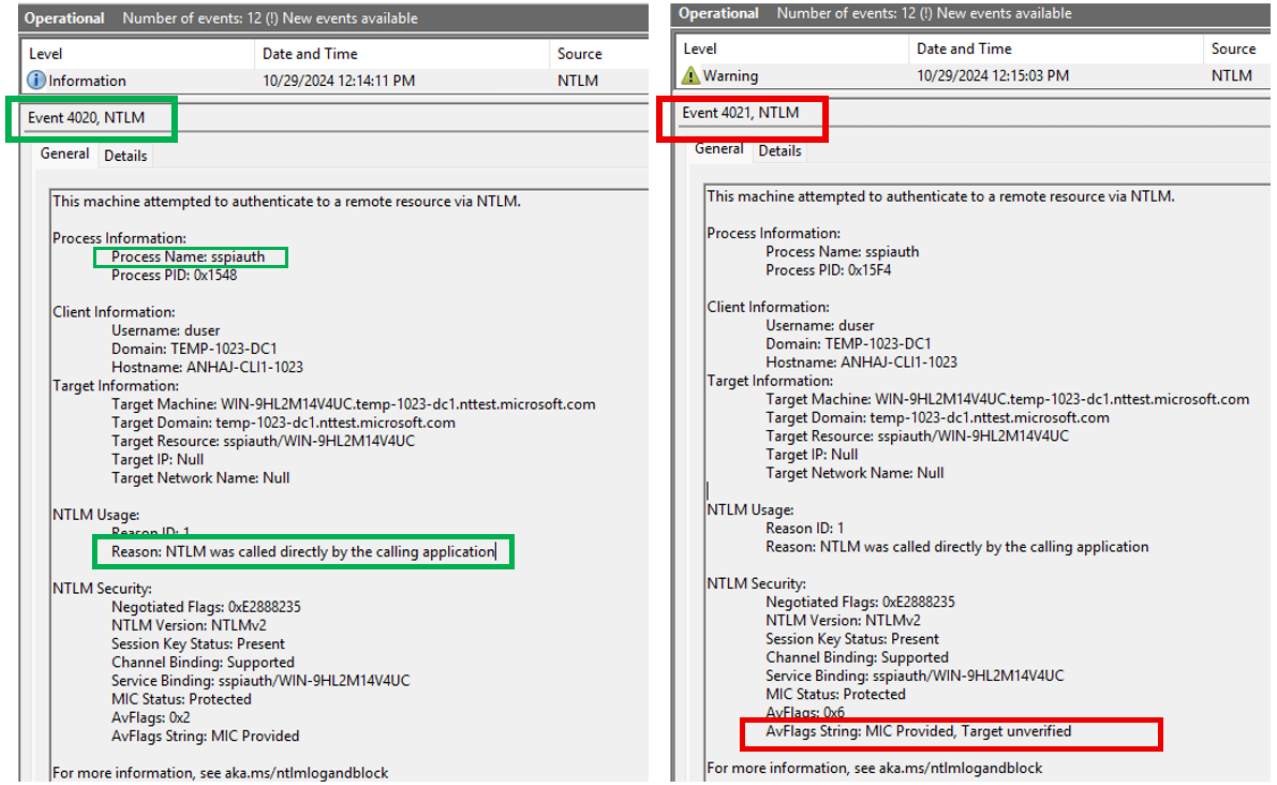
- Viewed via NTLM Operational Event logs

Goal of Enhanced Auditing is to Understand:

- What is using NTLM
- Why is NTLM being used
- Where is NTLM auth going

Enhanced Auditing is superseding the following policies

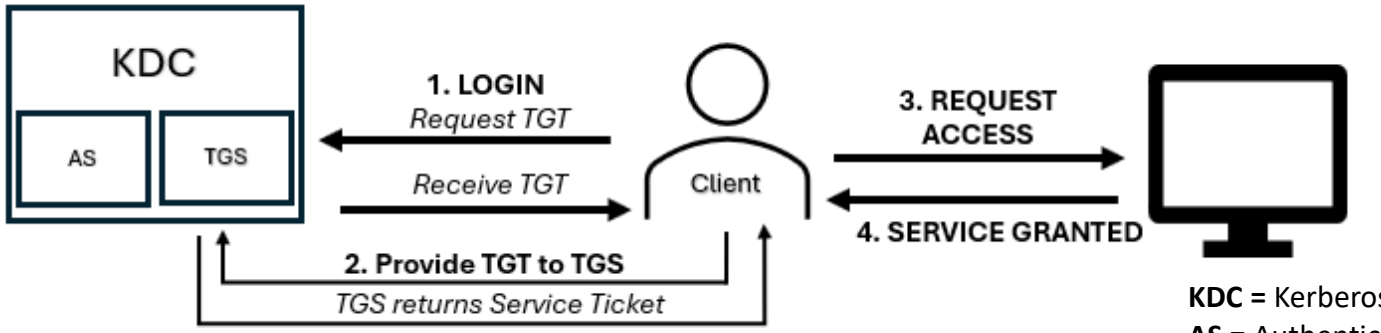
- Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers (Audit all)
- Network security: Restrict NTLM: Audit NTLM authentication in this domain (Enable all)
- Network security: Restrict NTLM: Audit Incoming NTLM Traffic (Enable auditing for all accounts)



Shifting from NTLM to Kerberos

- **What is Kerberos?**
  - Secure authentication protocol that uses tickets instead of passwords to prove identity

- **Why is it more secure?**
  - No user passwords are sent over the network
  - Verifies both client and server identities (mutual authentication)
  - Short-lived tickets reduce risks of relay attacks



KDC = Kerberos Key Distribution Center
AS = Authentication Server
TGS = Ticket Granting Server
TGT = Ticket Granting Ticket

Note: *We are focusing specifically on organizations/environments using Windows and Active Directory, where Kerberos is the standard for secure authentication.*

Kerberos Gaps

- **Kerberos needs a Domain Controller (DC):**
  - No line-of-sight to DC → Cannot get a ticket → Authentication fails
  - Standalone systems without Domains → No central authority present
- **Where it breaks down:**
  - Access without DC connectivity
    - Example: User outside corporate network trying to access Exchange/SharePoint
  - Local/Standalone systems
    - Example: Laptop in a workgroup or device not joined to a Domain

Solving Kerberos Gaps – IAKerb and LocalKDC

IAKerb

What is it: Kerberos feature that enables authentication when you don't have line of sight to DC.

How it works: The Kerberos authentication exchange is proxied through the target server, and the client authenticates using Kerberos.

Key features:

- Enables Kerberos authentication in environments with NW segmentation or where direct DC access is not feasible.
- Useful for remote or cloud-based scenarios where clients cannot directly reach an on-premise DC.

Local KDC

What is it: A feature that uses IAKerb to enable local user authentication without any need for external KDC.

How it works: Acts as a local Kerberos authentication service, and issues Kerberos tickets for authentication without requiring an AD domain.

Key features:

- Useful for isolated systems.
- Provides a more secure alternative to NTLM for standalone Windows devices.

Use Case 1- Kerberos Gap Filled by IAKerb

Scenario:

- A remote user is working from outside the corporate network (no direct line-of-sight to a Domain Controller).
- The user needs to authenticate to a resource (like Exchange or SharePoint) that requires Kerberos.
- Normally, Kerberos would fail here because the client can't reach a DC to get a TGT.

Problem:

- Kerberos requires line-of-sight to a DC for ticket issuance.
- NTLM would have been the fallback → weaker security.

How IAKerb Fixes This:

- Allows Kerberos to work without direct DC connectivity.
- The application server (e.g., Exchange) acts as a proxy to forward Kerberos messages between the client and the DC.
- This keeps authentication secure with Kerberos rather than falling back to NTLM.

Use Case 2- Kerberos Gap Filled by LocalKDC

Scenario:

- A Windows device in a workgroup still needs to support authentication for services like RDP or SMB locally.
- There is no Domain Controller, so traditional Kerberos from AD can't be used.

Problem:

- Kerberos relies on a DC-hosted KDC. Without it, Kerberos can't function.
- NTLM would again be the fallback → insecure.

How LocalKDC Fixes This:

- Allows Windows to run a local Key Distribution Center on the machine.
- This enables Kerberos authentication for local accounts.
- For example, a user logging into a local account or isolated system can still benefit from Kerberos security without AD.

Scenarios covered by LocalKDC

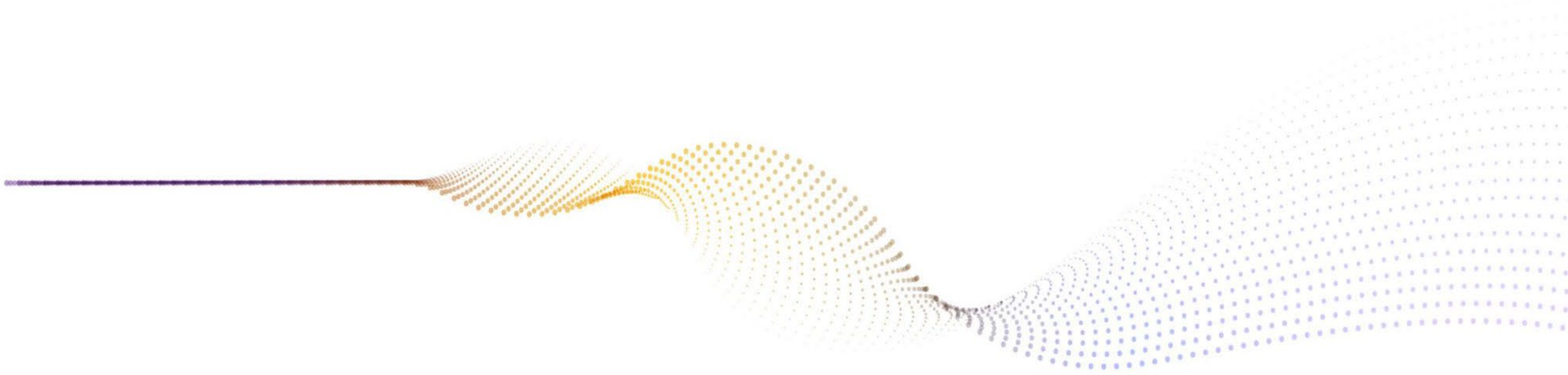
Upcoming Release (MVP):

- IAKerb: Fully functional, enabling Kerberos authentication when the client has no line-of-sight to the DC.
- Local KDC: Cluster deployments where peer-to-peer authentication is used.
- Local KDC: Target service can accept local user authentication while running as SYSTEM.
- Local KDC: Small business deployments with network shares.
- Local KDC: Remote desktop for local users.

Future scenarios: Local KDC functionality will expand as we continue our test validation to gain confidence on the quality of additional scenarios. Future scenarios will include:

- Small business and other deployments needing 3rd party apps to run using local user identity
- Defining behaviors for interactions between local user and domain user accounts on a domain-joined device

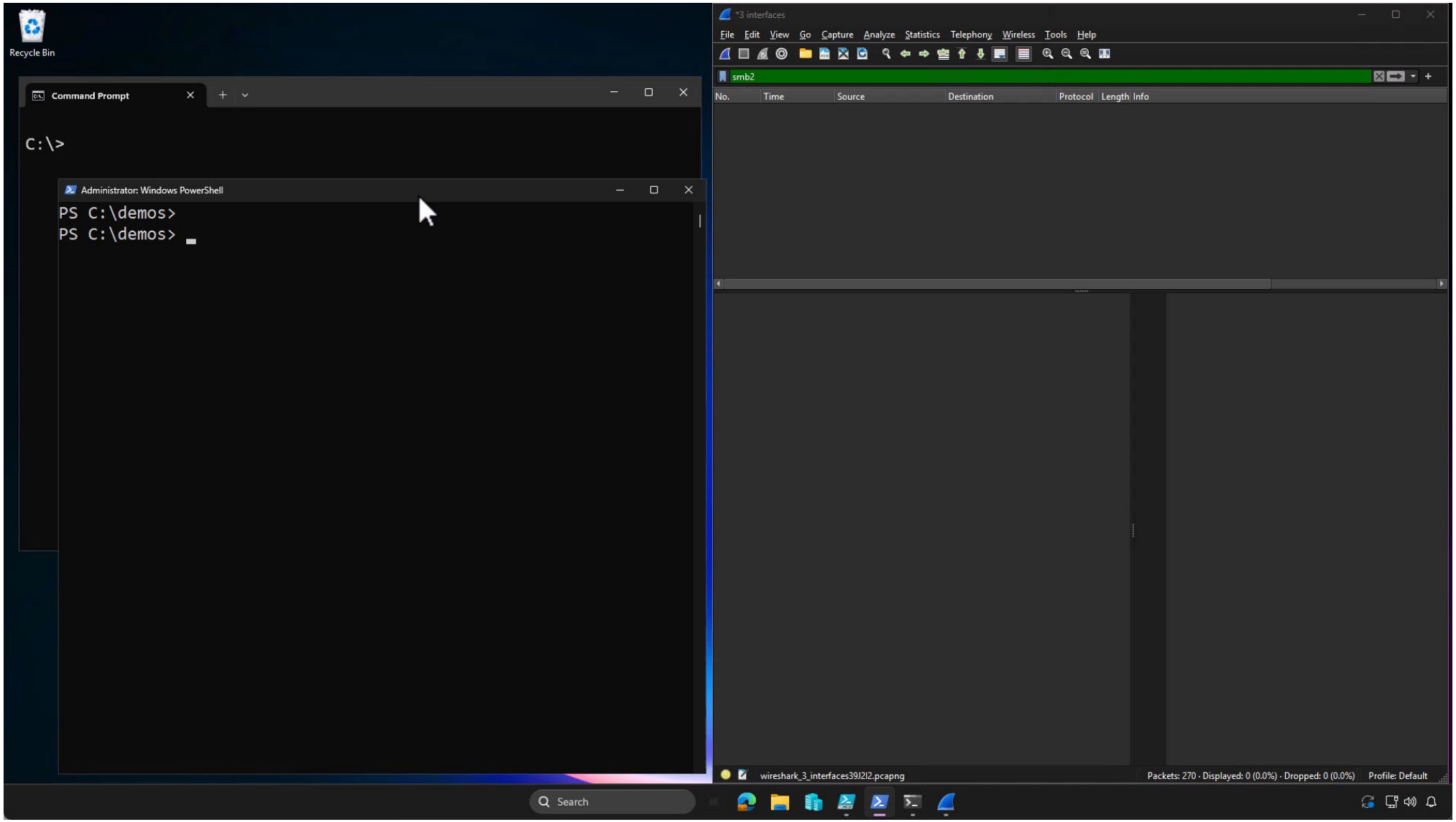
Microsoft



Kerberos for SMB Storage

SDC 25

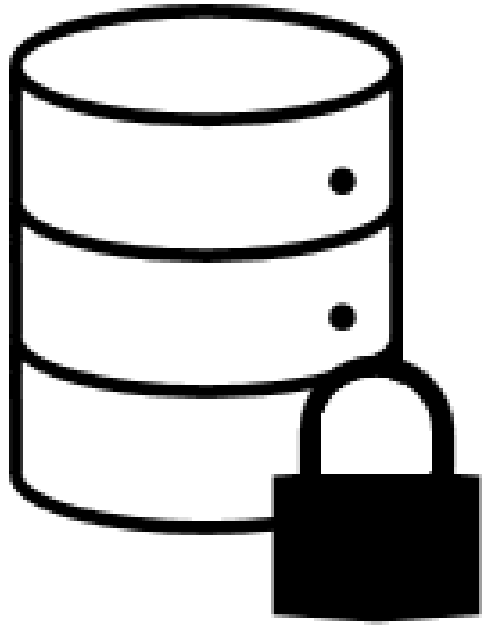
Demo: SMB NTLM Blocking (Local Account)



Modernizing SMB Authentication with Kerberos

Why SMB Needs Strong Authentication

- Sensitive data flows over SMB shares
- NTLM fallback exposes risk
- Enterprises demand secure, scalable identity-based access



Kerberos with SMB Storage:

- Uses tickets, not passwords → stronger than challenge/response
- Provides mutual authentication (client ↔ server trust)
- Integrates with Active Directory & SPNs for seamless access control
- Supports delegation scenarios (apps/services accessing SMB on user's behalf)

Key benefit:

- Kerberos makes SMB storage secure, scalable, and enterprise-ready

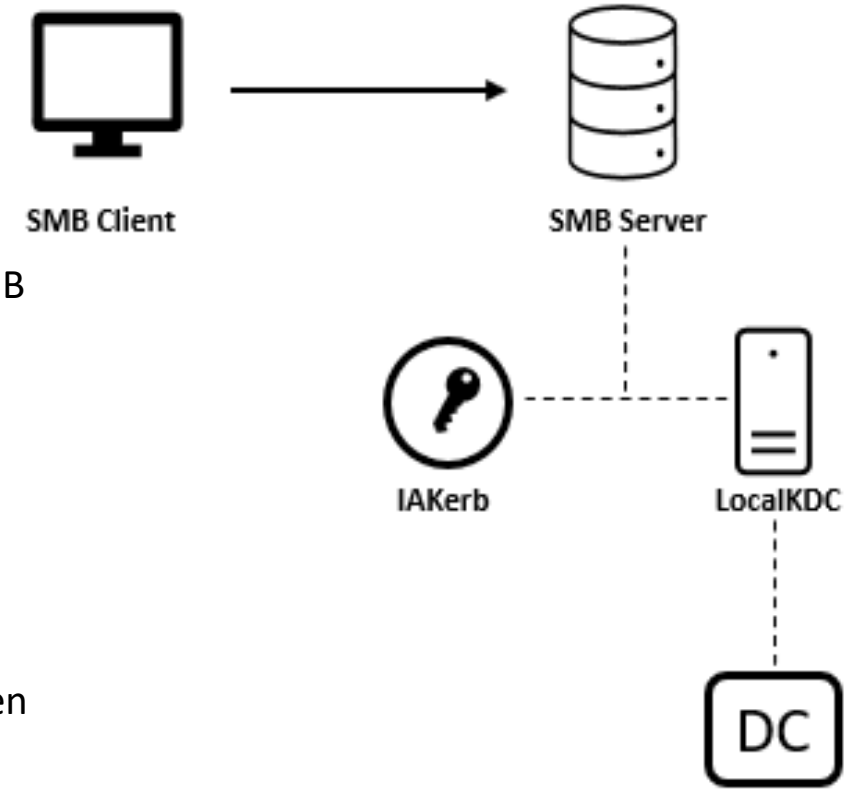
Walkthrough: How IAKerb & LocalKDC Secure SMB

1. SMB Client → SMB Server
- A client wants to access a storage share using SMB.

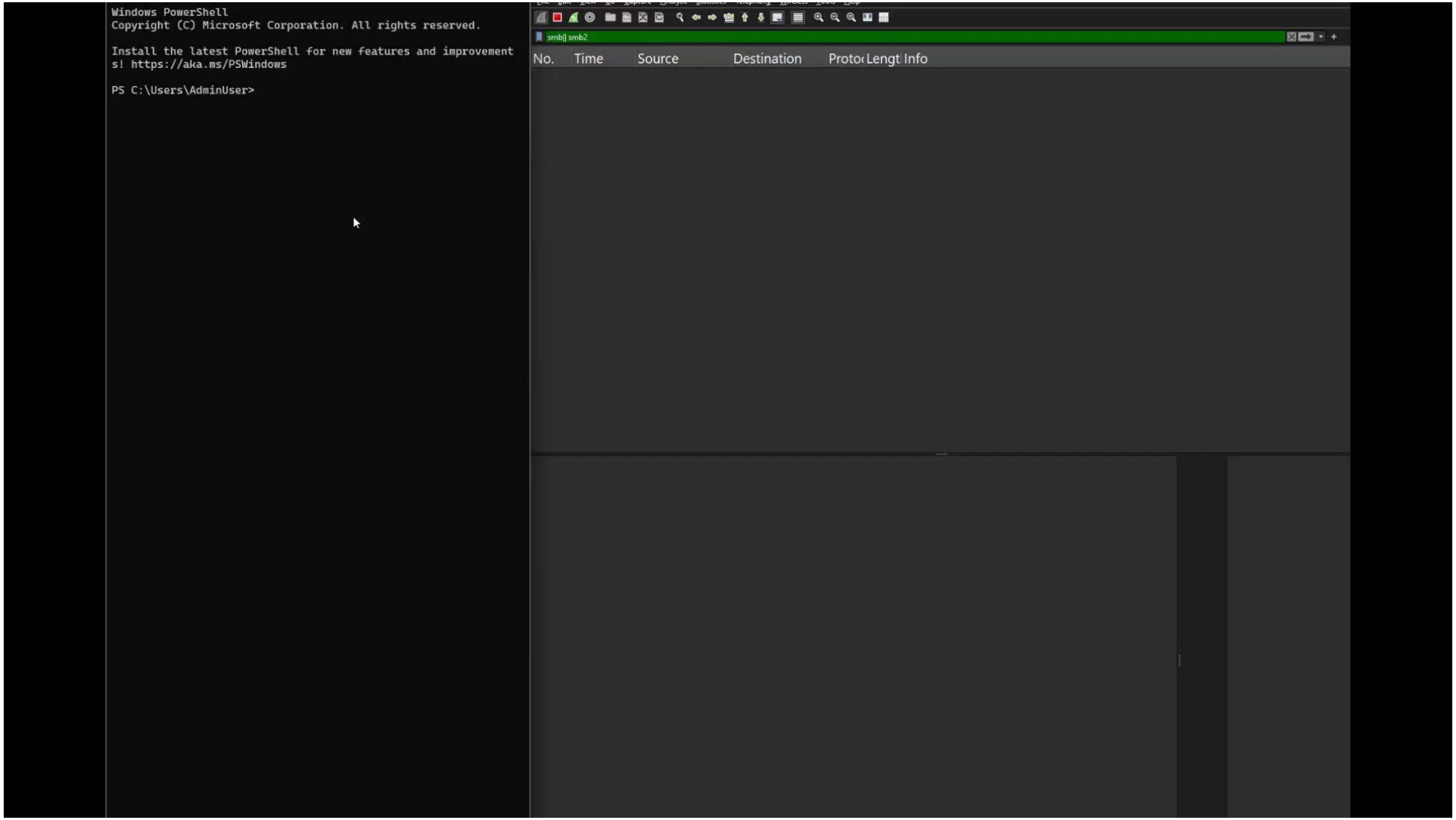
2. IAKerb (Kerberos Proxy)
- If the client cannot reach the DC directly (e.g., because of firewalls, network segmentation, or remote access), it sends Kerberos authentication through the SMB server.
- The SMB server proxies that traffic to the DC on behalf of the client.
- This avoids falling back to NTLM, keeping authentication strong and encrypted.

3. LocalKDC
- If there is no DC at all (standalone appliance, branch system, cluster), the server itself runs a LocalKDC.
- The LocalKDC issues Kerberos tickets using local accounts.
- This way, Kerberos security (mutual authentication, encryption) is still available even without AD.

4. Domain Controller (DC)
- When present, the SMB server forwards authentication traffic (via IAKerb) to the DC.
- If absent, LocalKDC handles authentication entirely.



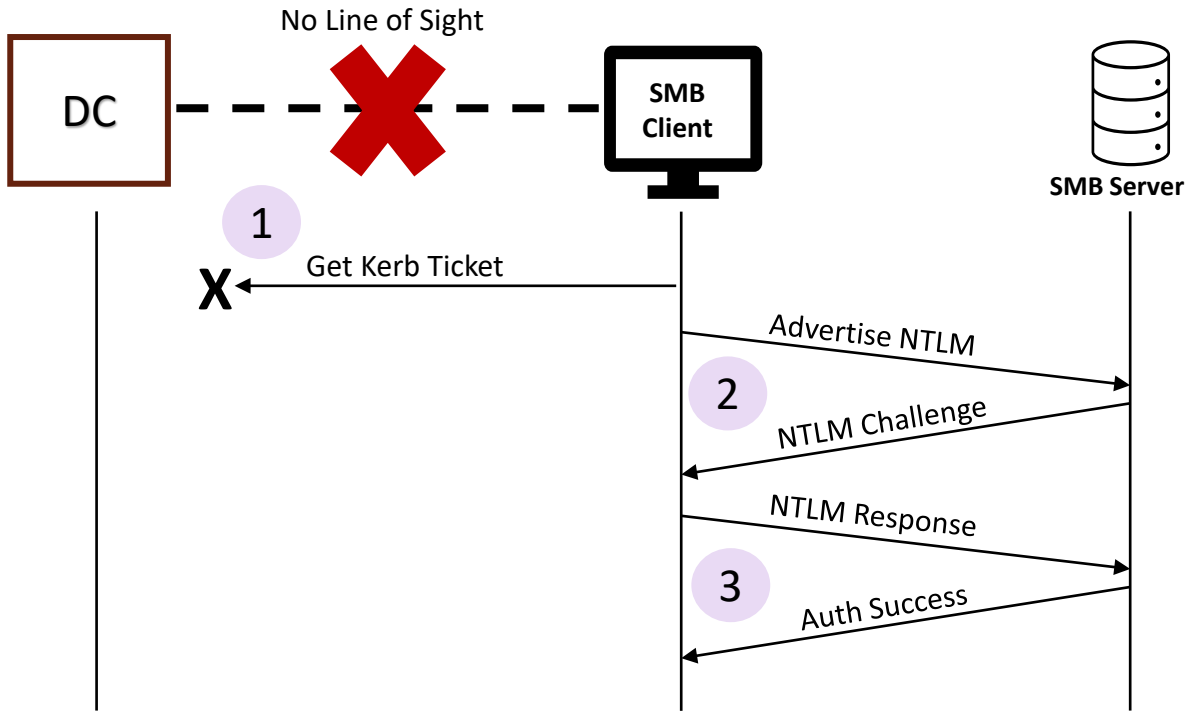
Demo: Successful Auth w/ NTLM-off



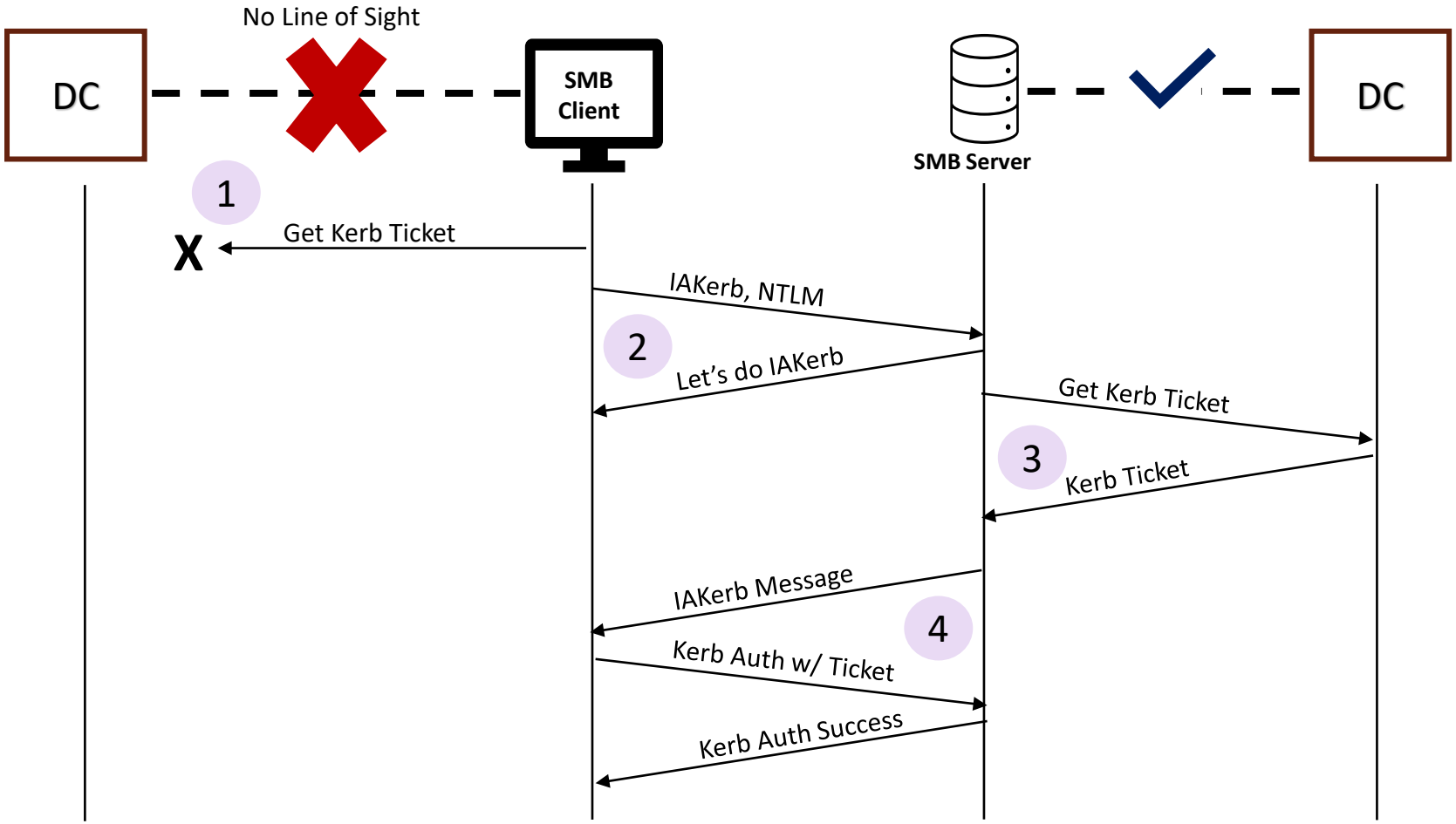
SMB and Negotiate: Introducing Late Fallback with IAKerb

- SMB already uses SPNEGO (Negotiate) to select between Kerberos and NTLM.
- In NTLMLess environments, Kerberos failures can break authentication.
- Negotiate Late Fallback enables SMB clients to retry with IAKerb after initial failure, before reverting to NTLM.

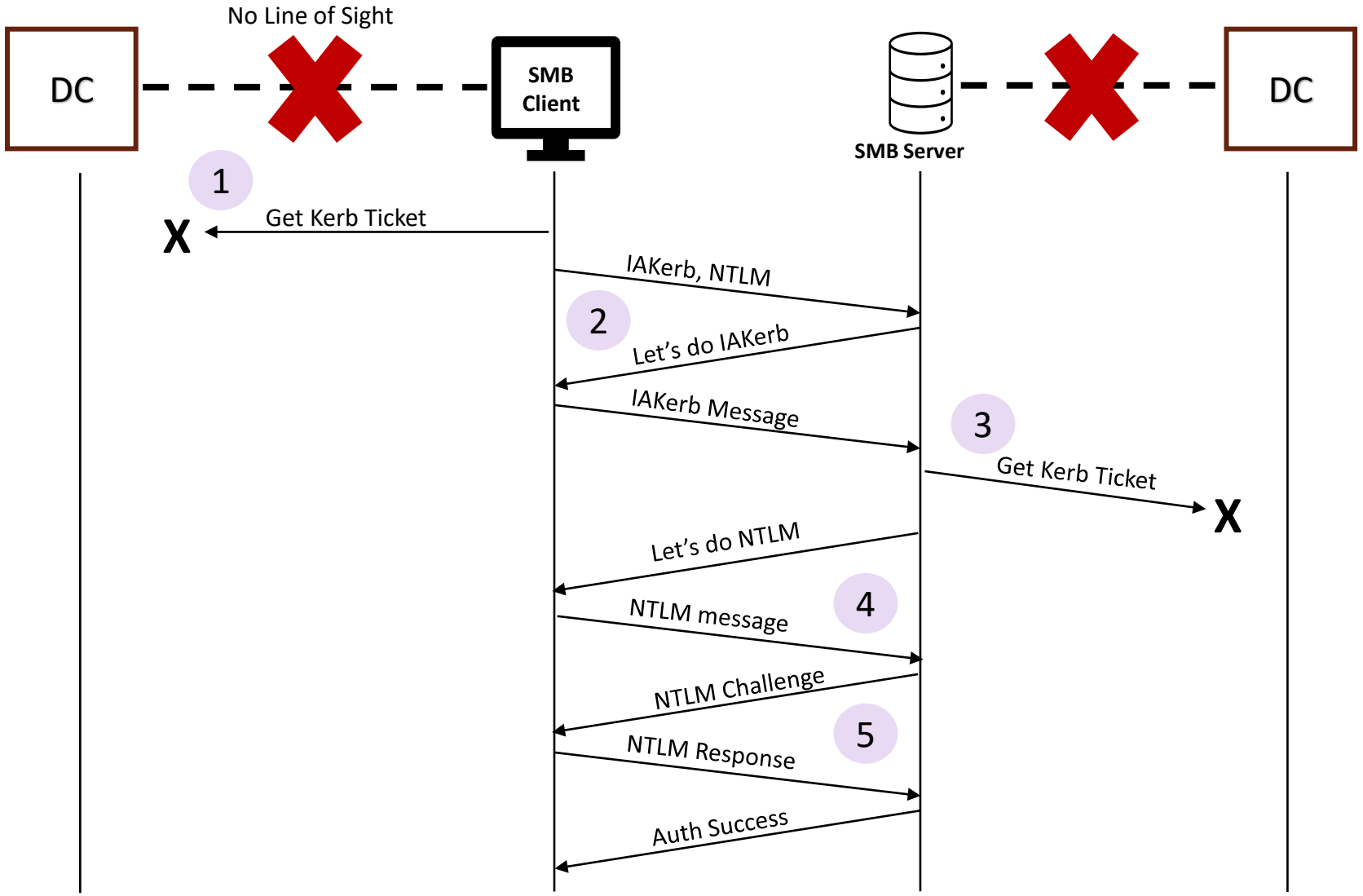
Today's Negotiate Flow



Negotiate with Late Fallback and IAKerb – LFB not Used



Negotiate with Late Fallback and IAKerb – LFB is Used



The Big Picture: Stronger SMB Auth Everywhere

- **On-Network:** Standard Kerberos with AD/DC
- **Remote:** IAKerb keeps Kerberos alive without DC line-of-sight
- **Offline/Workgroup:** LocalKDC brings Kerberos to standalone systems
- **End Result:** SMB storage always benefits from Kerberos security, regardless of environment

Preparing to Disable NTLM in Storage

- Leverage the enhanced NTLM Auditing to understand where it is being used in their environment.
- Create an Allow List for specific servers and services that may need temporary exceptions to continue using NTLM.
- Preview IAKerb & LocalKDC on WIP
- Upgrade to Kerberos wherever possible

Microsoft

Thank you!
Question?

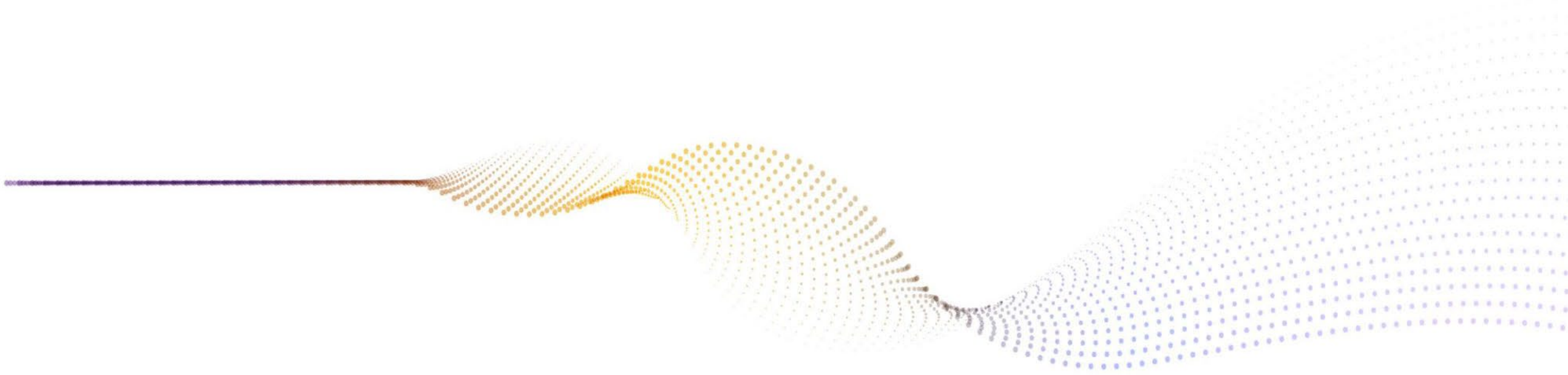
Please feel free to reach out to us with questions and/or feedback:

MariamGewida@Microsoft.com

TanmayP@Microsoft.com

SDC 25

Microsoft



Thank you for attending!

Please remember to rate this session. You get access the presentations at
http://sniadeveloper.org/conference

SDC 25