Microsoft ha anunciado una estrategia en tres fases para retirar progresivamente New Technology LAN Manager (NTLM), como parte de su iniciativa para migrar los entornos Windows hacia alternativas más robustas basadas en Kerberos.

Este anuncio llega más de dos años después de que la compañía diera a conocer su intención de eliminar esta tecnología heredada, señalando su exposición a vulnerabilidades que pueden facilitar ataques de tipo relay y permitir a actores maliciosos obtener acceso no autorizado a recursos de red. NTLM fue oficialmente declarado obsoleto en junio de 2024 y ya no recibe actualizaciones.

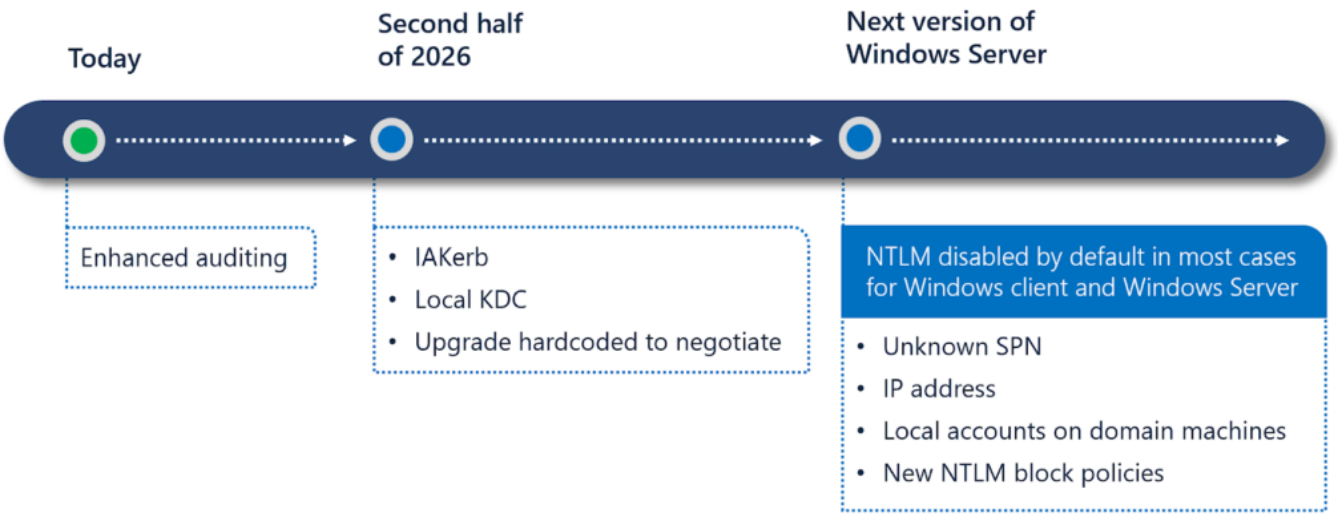
"NTLM está compuesto por protocolos de seguridad que originalmente fueron diseñados para proporcionar autenticación, integridad y confidencialidad a los usuarios", explicó Mariam Gewida, Technical Program Manager II en Microsoft. *"Sin embargo, a medida que las amenazas de seguridad han evolucionado, también lo han hecho nuestros estándares para cumplir con las exigencias modernas. En la actualidad, NTLM es vulnerable a distintos tipos de ataques, incluidos los de repetición y los de intermediario, debido al uso de criptografía débil."*

A pesar de su estado de obsolescencia, Microsoft indicó que el uso de NTLM sigue siendo común en entornos empresariales donde no es posible implementar protocolos modernos como Kerberos, ya sea por dependencias heredadas, limitaciones de red o lógica de aplicaciones profundamente integrada. Esto expone a las organizaciones a riesgos de seguridad como ataques de repetición, relay y pass-the-hash.

Para abordar este problema de forma segura, la empresa ha definido una estrategia en tres fases que prepara el camino para que NTLM quede deshabilitado por defecto:

Fase 1: Crear visibilidad y control mediante auditorías avanzadas de NTLM para comprender mejor dónde y por qué sigue utilizándose (Disponible actualmente)
Fase 2: Resolver los obstáculos más comunes que impiden la migración desde NTLM mediante funciones como IAKerb y el Key Distribution Center (KDC) local (prelanzamiento), además de actualizar componentes clave de Windows para priorizar la autenticación

Kerberos (Previsto para el segundo semestre de 2026)
Fase 3: Deshabilitar NTLM en la próxima versión de Windows Server y en los clientes Windows asociados, requiriendo una reactivación explícita a través de nuevas políticas



Microsoft ha presentado esta transición como un paso clave hacia un futuro sin contraseñas y resistente al phishing. Para ello, las organizaciones que aún dependen de NTLM deberán realizar auditorías, identificar dependencias, migrar a Kerberos, probar configuraciones con NTLM desactivado en entornos no productivos y habilitar las mejoras de Kerberos.

"Deshabilitar NTLM por defecto no significa eliminarlo completamente de Windows por ahora", señaló Gewida. *"Más bien, implica que Windows se entregará en un estado seguro por defecto, donde la autenticación NTLM en red estará bloqueada y dejará de usarse automáticamente."*

"El sistema operativo priorizará alternativas modernas y más seguras basadas en Kerberos. Al mismo tiempo, los escenarios heredados más comunes se abordarán mediante nuevas capacidades que llegarán próximamente, como Local KDC e IAKerb (prelanzamiento)."