微软停止开发并废弃 NTLM 协议，Win11 24H2 和 Server 2025 仍保留使用

2024年06月05日 09:04　IT之家

IT之家 6 月 5 日消息，微软于 6 月 3 日更新官方支持文档，宣布停止开发包括 LANMAN、NTLMv1 和 NTLMv2 在内的所有 NTLM 版本，**并已经完全废弃该身份认证协议。**

Feature 特点	Details and mitigation 详情和缓解措施	Deprecation announced 宣布停用
NTLM	All versions of NTLM, including LANMAN, NTLMv1, and NTLMv2, are no longer under active feature development and are deprecated. Use of NTLM will continue to work in the next release of Windows Server and the next annual release of Windows. Calls to NTLM should be replaced by calls to Negotiate, which will try to authenticate with Kerberos and only fall back to NTLM when necessary. For more information, see Resources for deprecated features. 包括 LANMAN、NTLMv1 和 NTLMv2 在内的所有 NTLM 版本均已停止功能开发，并已废弃。NTLM 将在 Windows Server 的下一个版本和 Windows 的下一个年度版本中继续使用。对 NTLM 的调用应由对 "协商 "的调用取代，"协商 "将尝试使用 Kerberos 进行身份验证，只有在必要时才返回 NTLM。有关更多信息，请参阅废弃功能资源。	June 2024 2024 年 6 月

IT之家去年 10 月报道，微软宣布新一轮过渡计划，弃用 NTLM 身份认证方式，让更多企业和用户过渡使用 Kerberos。

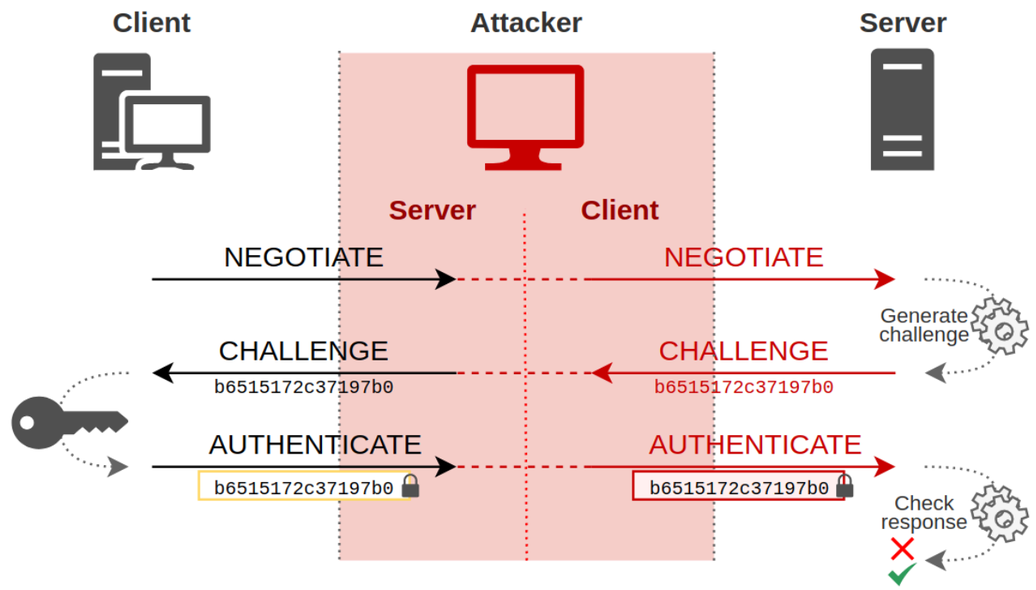
微软安全官方博客今年 5 月再次发布博文，为了响应安全社区的强烈要求，计划在 2024 年下半年的 Windows 11 中弃用 NT LAN Manager（NTLM）。

而在最新支持文档中，微软明确下个 Windows 年度更新、下个 Windows Server 更新中，用户可以继续使用 NTLM 协议，但后续调用 NTLM 会替代调用 Negotiate，而 Negotiate 会优先使用 Kerberos 进行身份验证，只有在必要时才调用 NTLM。

据悉微软为实现这一目标主要进行了两项重要工作：

一方面是扩展 Kerberos 的应用场景。在 Windows 11 系统中，为 Kerberos 引入了 IAKerb 和本地 KDC，分别实现了在多样化的网络拓扑环境和本地账户环境中使用 Kerberos 进行身份验证。

另一方面修复了现有 Windows 组件中内置的 NTLM 硬编码组件。将这些组件转而使用 Negotiate 协议，以便可以使用 Kerberos 代替 NTLM。通过迁移到 Negotiate 协议，这些组件服务将能够支持本地和域账户使用 IAKerb 和 LocalKDC 验证。



IT之家注：NTLM 是一个微软专用协议，它基于挑战 / 响应模型认证用户和计算机，使用挑战 / 响应模型来证实客户端的身份，而不需要在网络上发送口令或散列的口令，是所有 Windows NT 系列产品都使用的认证方式。

关键词：微软 Win11 Windows it之家