Windows NT Lan Manager Hardening Best Practices

calcomsoftware.com/lan-manager-authentication-level-hardening-best-practices

March 3, 2024

Windows New Technology LAN Manager (NTLM) is an outdated challenge-response authentication protocol developed by Microsoft. Despite being surpassed by Kerberos, NTLM remains in use as a form of Single Sign-On (SSO), allowing users to authenticate to applications without directly providing their passwords.

Depending on the version of NTLM, the protocol employs one of two one-way functions: NT LanMan and NTLM version 1 utilize the DES-based LanMan one-way function (LMOWF), whereas NTLMv2 utilizes the NT MD4-based one-way function (NTOWF).

Windows New Technology LAN Manager Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Present Implementations and Uses

NTLM authentication remains supported and is necessary for Windows authentication within systems set up as part of a workgroup. Additionally, NTLM authentication is employed for local logon authentication on non-domain controllers. While Kerberos version 5 authentication is the preferred method within Active Directory environments, NTLM may still be utilized by non-Microsoft or Microsoft applications.

Implementers should note that NTLM lacks support for modern cryptographic methods like AES or SHA-256. Instead, it relies on cyclic redundancy checks (CRC) or MD5 for integrity, and RC4 for encryption.

The process of deriving a key from a password follows the specifications outlined in RFC1320 and FIPS46-2. Hence, it is generally recommended that applications avoid using NTLM.

Decreasing NTLM protocol usage in an IT environment demands understanding both the deployed application requirements reliant on NTLM and the strategies and steps essential for configuring computing environments to adopt alternative protocols.

Server hardening is typically a challenging and time-consuming process, requiring significant investments of time and resources. CHS by CalCom offers a solution to this problem by automating the entire server hardening process. CHS can learn your network and eliminate the need for lab testing while ensuring that your production environment experiences no outages. This allows you to apply your policy directly to your production servers without any hassle.

Vulnerabilities in Windows New Technology LAN Manager

MITRE ATT&CK framework includes techniques that specifically target the NTLM (NT LAN Manager) authentication protocol.

Several techniques that can be used to exploit vulnerabilities in NTLM are present in the MITRE ATT&CK framework, including:

- T1208 – Kerberoasting
- T1558 – Pass the Hash
- T1552 – Pass the Ticket
- T1110 – Brute Force
- T1003 – Credential Dumping
- T1559 – Replication Through Removable Media
- T1204 – User Execution

Such techniques can be used to gain NTLM credentials and use them to obtain unauthorized access to a system or network. Organizations should consider using more secure authentication protocols such as Kerberos and implement best practices for securing NTLM, such as using NTLMv2 and implementing network-level controls to prevent NTLM relay attacks.

CalCom
BASELINE HARDENING AUTOMATION MADE SIMPLE
See how working with experts that are CIS Benchmark Certified strengthens your security posture
GET A DEMO

Hardening Windows New Technology LAN Manager

Configuration hardening can help to mitigate the risks associated with this legacy protocol.One important aspect of configuration hardening is disabling LM authentication. This can be done by modifying the registry settings on Windows systems or using Group Policy Objects (GPOs) to enforce the change across the entire network. By disabling LM authentication, an attacker would not be able to crack the LM hash of a user’s password and gain unauthorized access to the network.

Additionally, implementing strong password policies, regular password rotation, and regular monitoring of logs and network activities can be a good practices to harden the security of your network.

Overall, configuration hardening is important for network security because it helps to reduce the attack surface and prevent unauthorized access. When choosing an automated method, it will require you to use a 'Hardening Automation Tool' that will save you the need to perform lab testing, and save you time and money.

Following these best practices, organizations can better protect their networks against cyber threats and minimize the risks associated with legacy authentication protocols such as LAN Manager (LM).