Sources to Read:

LAN Manager Authentication
NTLM
WDigest

WDigest

WDigest is a feature of the Microsoft Windows operating system that stores user credentials in memory in an encrypted format. It is used by the operating system to provide single sign-on (SSO) functionality, which allows users to access multiple resources on a network with a single set of credentials.

When a user enters their username and password to log in to a Windows computer, the credentials are hashed and stored in memory by the Local Security Authority Subsystem Service (LSASS). WDigest can be used to extract and decrypt these credentials from memory, which could potentially allow an attacker with administrative privileges to gain access to sensitive information such as passwords and user account information.

Because of the potential security risks associated with WDigest, Microsoft has deprecated this feature in newer versions of Windows, and it is no longer enabled by default. However, it may still be enabled on some systems, particularly those that have not been updated with the latest security patches. To ensure the security of your Windows systems, it's important to disable WDigest and other potentially vulnerable features whenever possible.

To disable WDigest on a Windows computer, you can follow these steps:

1. **Press the Windows key + R on your keyboard to open the Run dialog box.**
2. **Type "regedit" and press Enter. This will open the Registry Editor.**
3. **Navigate to the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest**

If the "UseLogonCredential" value is present and set to "1", double-click on it and set the value to "0". If the value is not present, right-click on an empty space in the right-hand pane and select New > DWORD (32-bit) Value. Name the new value "UseLogonCredential" and set its value to "0".

If the "AllowInsecureGuestAuth" value is present and set to "1", double-click on it and set the value to "0". If the value is not present, right-click on an empty space in the right-hand pane and select New > DWORD (32-bit) Value. Name the new value "AllowInsecureGuestAuth" and set its value to "0".

- Close the Registry Editor.

- Restart your computer for the changes to take effect.

Once you have disabled WDigest, it's important to ensure that your computer is up to date with the latest security patches and that other potentially vulnerable features are also disabled, such as LAN Manager authentication and NTLMv1. These steps can help improve the overall security of your Windows system and protect against potential attacks.

LAN Manager Authentication & NTLM

LAN Manager (LM) authentication and NTLMv1 (NT Lan Manager version 1) are two legacy authentication protocols used by the Microsoft Windows operating system to authenticate users to a network. These protocols have been superseded by more secure protocols, such as Kerberos and NTLMv2, and are considered to be less secure.

LAN Manager authentication is an older authentication protocol that was used by Windows NT and Windows 95/98 systems. It uses a weak hashing algorithm and is vulnerable to brute force attacks.

NTLMv1 is an improved version of LAN Manager authentication that uses a stronger hashing algorithm, but is still vulnerable to attacks. It is used by Windows NT, 2000, XP, and Server 2003 systems.

Both LAN Manager authentication and NTLMv1 are considered to be insecure and have been deprecated by Microsoft. It is recommended that organizations disable these protocols and use more secure authentication methods, such as Kerberos or NTLMv2, which provide stronger protection against attacks.

To disable LAN Manager authentication and NTLMv1 on a Windows computer, you can follow these steps:

1. **Press the Windows key + R on your keyboard to open the Run dialog box.**
2. **Type "secpol.msc" and press Enter. This will open the Local Security Policy window.**
3. **In the left-hand pane, navigate to "Local Policies" > "Security Options".**
4. **In the right-hand pane, scroll down and locate the following policies:**
5. **"Network security: LAN Manager authentication level"**
6. **"Network security: Minimum session security for NTLM SSP based (including secure RPC) clients"**
7. **Double-click on each policy and select "Send NTLMv2 response only. Refuse LM & NTLM" from the dropdown list.**
8. **Click on "Apply" and then "OK" to save the changes.**

Once you have disabled LAN Manager authentication and NTLMv1, it's important to ensure that your computer is up to date with the latest security patches and that other potentially vulnerable features are also disabled, such as WDigest authentication. These steps can help improve the overall security of your Windows system and protect against potential attacks.