Implementation Flaws

LM Hash

ldapwiki.com

G'day (anonymous guest) Log in My Prefs

≡ Sidebar Attach Info Edit More...

Overview

LM hash, LanMan hash, or LAN Manager hash is a compromised password hashing function that was the primary hash that Microsoft LAN Manager and Microsoft Windows versions prior to Windows Server NT used to store user passwords.
Support for the legacy LM hash continued in later versions of Microsoft Windows for backward compatibility, but was recommended by Microsoft to be turned off by administrators; as of Windows Vista, the protocol is disabled by default, but continues to be used by some non-Microsoft CIFS implementations.

LM hash Algorithm

The LM hash is computed as follows:

- The user's password is restricted to a maximum of fourteen characters.
- The user's password is converted to UPPERCASE.
- The user's password is encoded in the System OEM code page.
- This password is null-padded to 14 bytes.
- The "fixed-length" password is split into two 7-byte halves.
- These values are used to create two DES keys, one from each 7-byte half, by converting the seven bytes into a bit stream with the most significant bit first, and inserting a null bit after every seven bits (so 1010100 becomes 10101000).

This generates the 64 bits needed for a DES key.

Each of the two keys is used to DES-encrypt the constant ASCII string "KGS!@#$%", resulting in two 8-byte ciphertext values. The DES CipherMode should be set to ECB, and PaddingMode should be set to NONE.

These two ciphertext values are concatenated to form a 16-byte value, which is the LM hash.