LANMAN HASH

Algorithm

LANMAN HASH algorithm as known as LM or LAN Manager hash.

It was used by Microsoft LAN Manager and Microsoft Windows versions prior to Windows NT used to store user passwords.

It is a compromised algorithm that is not used anymore.

# Mechanism:

* Allowed Password length is of 14 characters.
* Then password is converted to uppercase.
* Then password encoded in the system OEM code page.
* Windows code pages, commonly called "ANSI code pages", are code pages for which non-ASCII values (values greater than 127) represent international characters. These code pages are used natively in Windows Me, and are also available on Windows NT and later.
* Then password is null -padded into 14 bytes.
* Password is split into two halves of 7 bytes.
* 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 cipher text values.
* These two cipher text values are concatenated to form a 16-byte value, which is the LM hash.

# Weakness:

* Passwords are limited to a maximum of only 14 characters, giving a theoretical maximum keyspace of 9514 (approx) 292 with the 95ASCII printable characters.
* Passwords longer than 7 characters are divided into two pieces and each piece is hashed separately.
* By mounting a brute force attack on each half separately, modern desktop machines can crack alphanumeric LM hashes in a few hours.
* All lower case letters in the password are changed to upper case before the password is hashed, which further reduces the key space for each half to: 697 (approx) 243.
* Any password that is shorter than 8 characters will result in the hashing of 7 null bytes, yielding the constant value, hence making it easy to identify short passwords on sight.
* Many cracking tools, e.g. RainbowCrack, L0phtCrack and Cain, now incorporate similar attacks and make cracking of LM hashes fast and trivial.
* LM-Hash values only change when a users changes their password.