

LM & MD5 Hash Security & Cracking

By,

Brian Wilson

CCNA, CSE, CCAI, MCP, Network+

Slimjim100@gmail.com

www.middlegeorgia.org

www.middlegeorgia.info

In this paper I will discuss Encryption and how to Crack encrypted hashes without the decryption key. Let's start with an explanation or the idea behind encryption. Encryption is used to secure or hide data from unauthorized personal and has been around from about 1800 BC and is not going away. There is always going to be a need to secure data and keep it out of unauthorized hands. Now with that said there is always going to be new ways to break the encryption and with computers getting faster. Crackers will learn how to break the encryption faster than ever. We are going to look at two encryption algorithms for passwords LM & MD5.

LAN Man Hash (LM)

LAN Man Hash (LM) is a Microsoft Encryption Algorithm used to Encrypt Passwords for Windows NT, 95, 98, ME 2000, XP, and 2003 Server. All though in the latest versions of windows (XP, 2003, Vista) Microsoft has now switched to NTLM for most encryption but LM is still widely used. LM is made by taking the users password and converting it to all uppercase and then splitting the password into two seven character halves. Each seven character half is converted to a sixteen bit hash and then both half's are combined to make a thirty-two bit hash which is the complete LM Hash.

LM Hash Example:

ED39C160E34521DCBF02B3DFE230653A = CERT276ROSENV
ED39C160E34521DC BF02B3DFE230653A = CERT276 ROSENV
1st 7 upper Encrypted 2nd 7 Upper encrypted pass ^ pass^

Message Digest Five (MD5)

MD5 hash is a 128-bit (16-byte) hash and are typically represented as 32-digit hexadecimal numbers. The MD5 (Message-Digest algorithm 5) was designed by Ronald Rivest in 1991 and was made to replace old algorithms. Today the MD5 hash is widely used and for the most part is secure. The best thing to remember is that with any password you need to make it complex and long. The best passwords are 15 characters or longer containing both upper and lower case letter with numbers and other special characters too.

MD5 Hash Example:

16d2c02aad8d116bc403f73454a5eeb1 = emocan
32-Digit Hash pass^

Cracking Password Hashes

Cracking password hashes can be easy if you have time and patience. What I mean by this is that with most basic cracking methods you are running the hash through a dictionary and hoping the password is in the dictionary you are using. This can take time and you are just shooting the hash into a list. The other most common cracking technique is to use Brute-force cracking. Brute-force cracking is the means of throwing all possible characters at the password till you find the match. This is the most time consuming method of cracking and can take years to crack a complex password. The last method we will discuss is Rainbow Crack. Rainbow Crack is a Hash cracking utility made by Zhu Shuanglei. Zhu's Utility is based on Philippe Oechslin's faster time-memory trade-off technique. Rainbow Crack is a pre-computed Brute-force attack and the attack data is stored in a data base called a rainbow table. With Rainbow Tables it is possible to crack complex passwords 100's or 1,000's of times faster than with a standard Brute-force attack. The downside to rainbow tables is that it takes a lot of time to make the table sets. On the other side of this once a table set is made it can be saved and reused as many times as you need. To make the tables you need rcrack.exe and it is recommended to have a group or large number of computers available to make the tables. There are many places online these days selling table sets or memberships to use online table submission services. One of the groups on the internet with the largest set of tables is Plain-text.info and they do not charge for access but limit anonymous access to a few hashes per hour unless you join their team and help support their network of crackers. At the time of this writing Plain-text.info is the only group online using a distributed cracking system using member's computers to assist in cracking the hashes. For more info on anything discussed here feel free to e-mail me (Slimjim100) slimjim100@gmail.com.