LM和NTML哈希

哈希介绍

Windows操作系统通常使用两种方法对用户的明文密码进行加密处理。在域环境中,用户信息存储在ntds.dit中,加密后为散列值。 Windows操作系统中的密码一般由两部分组成,一部分为 LM Hash,另一部分为NTLMHash。在Windows操作系统中,Hash的结构通常如下

```
username:RID:LM-HASH:NT-HASH
```

LM Hash的全名为“ LAN Manager Hash”,是微软为了提高 Windows操作系统的安全性而采 用的散列加密算法,其本质是DES加密。尽管 LM Hash较容易被破解,但为了保证系统的兼容性, Windows只是将LM Hash禁用了(从Windows vista和 Windows Server2008版本开始, Windows操作系统默认禁用 LM Hash)。 LM Hash明文密码被限定在14位以内,也就是说,如果要停止使用 LM Hash,将用 户的密码设置为14位以上即可。如果 LM Hash被禁用了,攻击者通过工具抓取的 LM Hash通常 为“ad3b435b51404eead3b435b51404ee”(表示 LM Hash为空值或被禁用)

NTLM Hash是微软为了在提高安全性的同时保证兼容性而设计的散列加密算法。 NTLM Hash 是基于MD4加密算法进行加密的。个人版从 Windows vista以后,服务器版从 Windows Server 2003以后, Windows操作系统的认证方式均为 NTLM Hash

LM Hash原理

1、将明文口令转换为其大写形式 假设这里以明文Admin@123为例，转换为大写格式为：ADMIN@123

2、 将字符串大写后转换为16进制字符串转换后为`41 44 4D 49 4E 40 31 32 33`

3、密码不足14字节要求用0补全，1Byte=8bit,上面的16进制字符串共9个字节,还差5个字节 我么使用`00 00 00 00 00` 补全为`41 44 4D 49 4E 40 31 32 33 00 00 00 00 00`

4、将上述编码分成2组7字节

```
41 44 4D 49 4E 40 31  第一组
32 33 00 00 00 00 00  第二组
```

5、将每一组7字节的十六进制转换为二进制，每7bit一组末尾加0，再转换成十六进制组成得到2组8字节的编码

第一组

16进制：41 44 4D 49 4E 40 31
转换为二进制：01000001010001000100110101001001010011100100000000110001
七个为一组末尾补
01000000
10100010
00010010
10101000
10010100
01110010
00000000
01100010
合并后为01000000101000100001001010101000100101000111001000000000001100010
在转换为16进制：40A212A894720062

第二组

16进制：32 33 00 00 00 00 00
转换为二进制：00110010001100110000000000000000000000000000000000000000000000
七个为一组末尾补
00110010
00011000
11000000
00000000
00000000
00000000
00000000
00000000
合并后为00110010000110001100000000000000000000000000000000000000000000000000
在转换为16进制：3218C00000000000

6、将以上步骤得到的两组8字节编码，分别作为DES加密key为魔术字符串“KGS!@#$% ”进行加密

KGS!@#$%的16进制为`4B47532140232425`

第一组：6F08D7B306B1DAD4

第二组：B75E0C8D76954A50

7、最终结果拼接即可6F08D7B306B1DAD4B75E0C8D76954A50

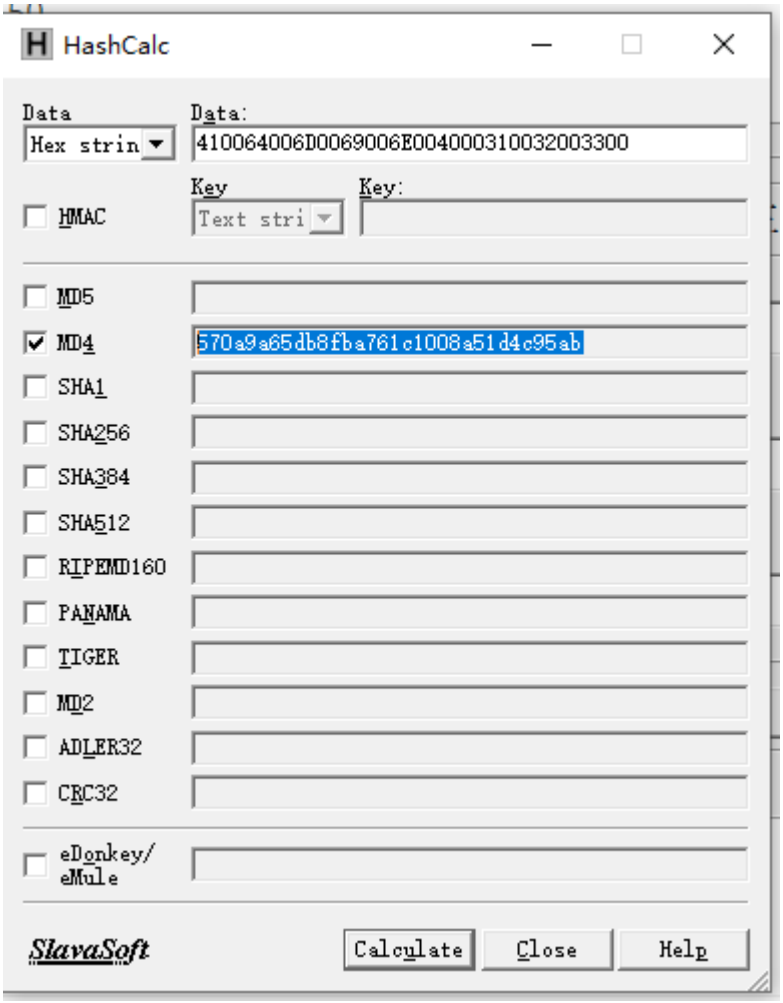
NTLM Hash原理

将明文口令转换成十六进制的格式 如：Admin@123

转换成Unicode格式，即在每个字节之后添加0x00

```
Admin@123转16进制 41646D696E40313233
添加00：410064006D0069006E004000310032003300
```

对Unicode字符串作MD4加密，生成32位的十六进制数字串`570a9a65db8fba761c1008a51d4c95ab`


HashCalc
Data
Hex strin
Data:
41006400 6D006900 6E004000 31003200 3300
Key
Text stri
Key:
HMAC
MD5
MD4
570a9a65db8fba761c1008a51d4c95ab
SHA1
SHA256
SHA384
SHA512
RIPEMD160
PANAMA
TIGER
MD2
ADLER32
CRC32
eDonkey/
eMule
SlavaSoft
Calculate
Close
Help