LM/NT#Hash Cracking

A BRIEF INTRO TO WINDOWS LM HASHES

Disclaimer*

- I would strongly suggest spending the time to research this information yourself. I’m not an expert, and even if I was, I’m a firm believe in “Question Everything”.
- I’ve heavily relied on (plagiarised) the research of other people (mostly Paul Ducklin), links/references are at the end.
- A copy of these slides will be available, links also at the end.
- If you see a mistake in this information, please let me know!

The Challenge

Crack Windows Account Passwords (“HelpAssistant” in this example)

Username:	HelpAssistant
Password:	HQ&1OymguFUzpq

Time to Crack: 4 min, 31sec (from my laptop)

- *Take note of the password, it’s not amazingly complicated, but it’s pretty solid.* 14 characters, upper and lower case, numeric, and special character.

So, why can we crack a password like that in <5min?

Password Storage Mechanisms

Salt and Hash + More Funky Stuff (hash stretching etc.)

```
josh : Joshua Riesenweber : ifeelreallysecure
admin : System Administrator : m3T00
jack : Jacks Mirkingrevenge : ifeelreallysecure
```

```
josh : Joshua Riesenweber : MQdLp3V6 : 9E6F64234898BB906D2AB3F84FFAFEAA
admin : System Administrator : 63EGKF53 : C89766E13312DCA5402F68711E9F8FBD
jack : Jacks Mirkingrevenge: np6XRSpL : D4AB0B28EA6E98D85EDB7BEE0227728E
```

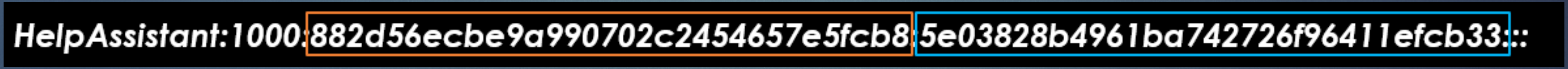
- Salting introduces a random string, which is combined with the password before it is hashed.
- This prevents two users with the same password receiving the same hash.
- *NB. The salt is not an encryption key, and can be stored with the user's password.*

**(MD5 used in the above example)*

Approach

```
(meterpreter > run post/windows/gather/hashdump )
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:49f394543974a6f385a4c18d32ec812c:::
Bill:1003:aad3b435b51404eeaad3b435b51404ee:bc798c87fcdf458bf37dc7bd92d1a980:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hanzo:1005:38b88a3d009d31c0bda2d11b66d4bbb9:0f4c9e2bf0edc9c393e59e4842ee48fe:::
```



```
HelpAssistant:1000:882d56ecbe9a990702c2454657e5fcb8:5e03828b4961ba742726f96411efcb33:::
```

```
Sally:1004:16ca03549b5622330c7107e4b1feed62:b314960b92d486066805fd08fed0582b:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:35ca235e2ba0506c534486681c1bf83d:::
```

How the LM “Hash” is created

- The user's password is restricted to a maximum of fourteen characters.
- The user’s password is converted to uppercase.
- 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.
- These two ciphertext values are concatenated to form a 16-byte value, which is the LM hash.

LM Hash: Step 1

- The user's password is restricted to a maximum of fourteen characters.

HQ&1OymguFUzpq

- This brings a good point on password length. If your password is > 14 characters, the LM hash is not stored.

LM Hash: Step 2

- The user’s password is converted to uppercase.

HQ&1OymguFUzpq
becomes
HQ&1OYMGUFUZPQ

LM Hash: Step 3

- This password is null-padded to 14 bytes.

Because our password is already 14 characters, it won’t change.

If it were something like PASSWORD123 it would become PASSWORD123000

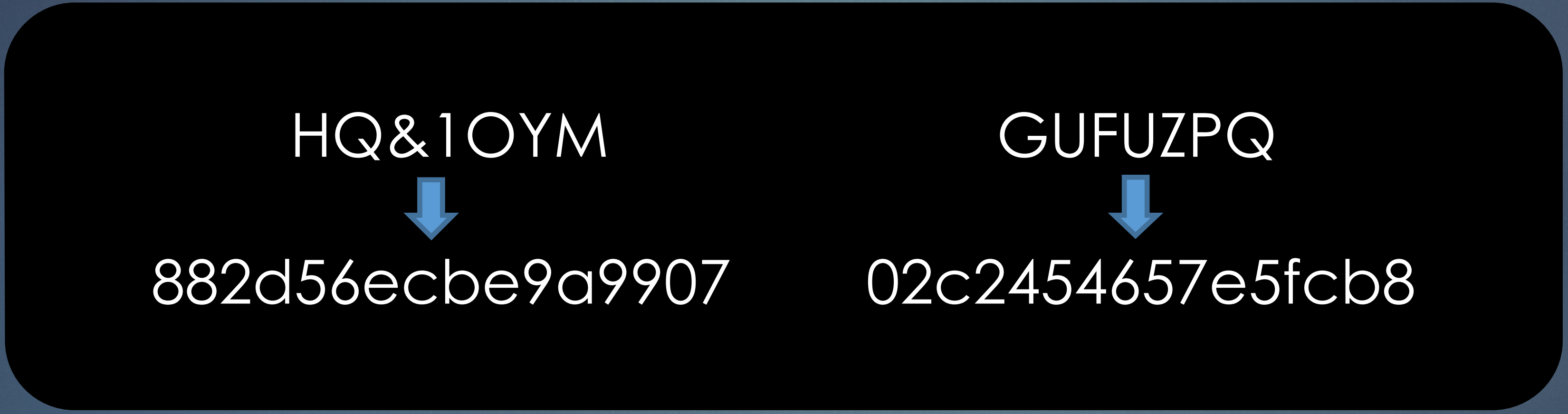
LM Hash: Step 4

- The “fixed-length” password is split into two 7-byte halves.

HQ&1OYM GUFUZPQ

LM Hash: Step 5

- These values are used to create two DES keys, one from each 7-byte half.



HQ&1OYM

882d56ecbe9a9907

GUFUZPQ

02c2454657e5fcb8

- Each key uses DES (using ECB) to encrypt the string “KGS!+#$%”.

LM Hash: Step 6

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

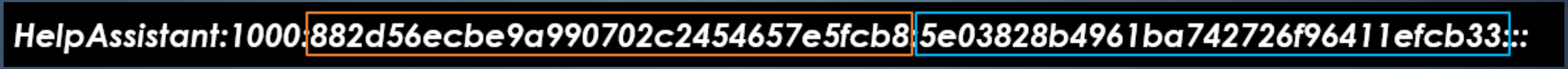
882d56ecbe9a9907 + 02c2454657e5fcb8
882d56ecbe9a990702c2454657e5fcb8

Approach

Cracking the LM Hash

(meterpreter > run post/windows/gather/hashdump)

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:49f394543974a6f385a4c18d32ec812c:::
Bill:1003:aad3b435b51404eeaad3b435b51404ee:bc798c87fcdf458bf37dc7bd92d1a980:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hanzo:1005:38b88a3d009d31c0bda2d11b66d4bbb9:0f4c9e2bf0edc9c393e59e4842ee48fe:::
```

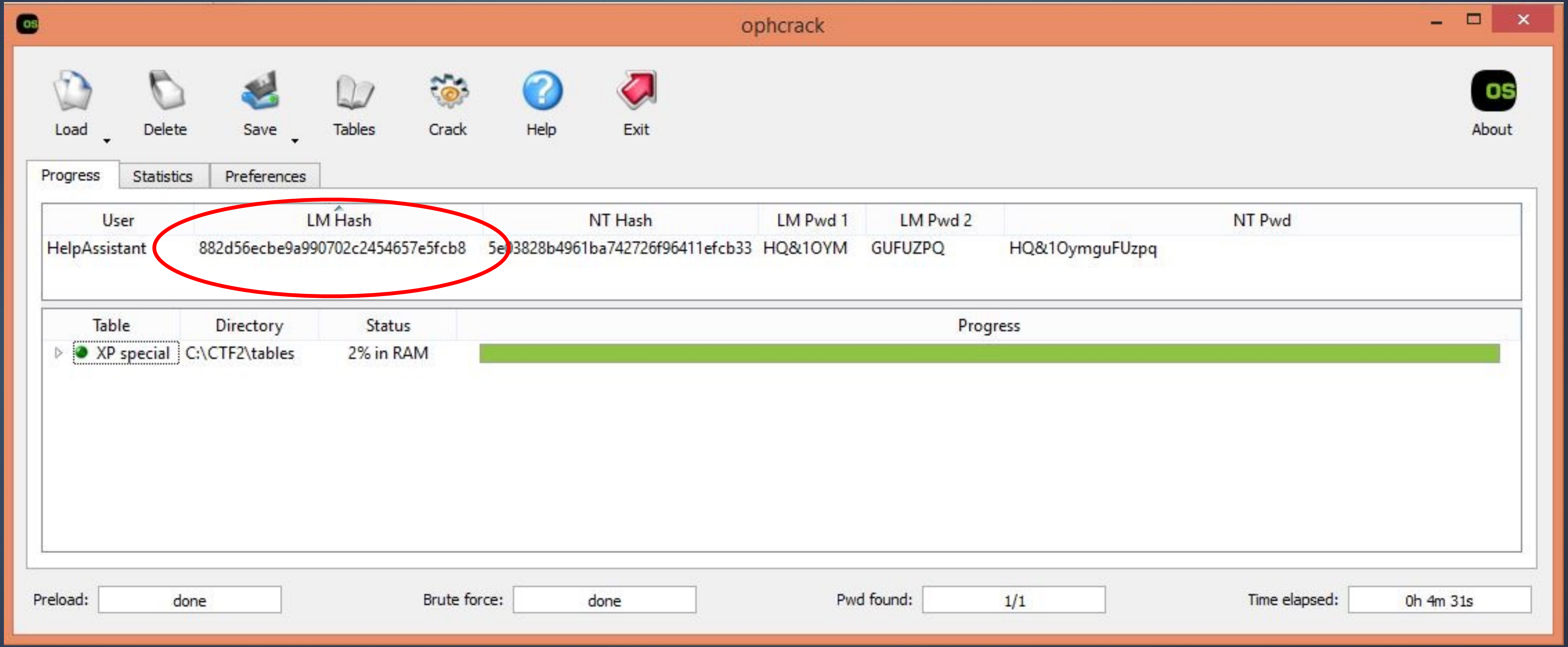


```
HelpAssistant:1000:882d56ecbe9a990702c2454657e5fcb8:5e03828b4961ba742726f96411efcb33:::
```

```
Sally:1004:16ca03549b5622330c7107e4b1feed62:b314960b92d486066805fd08fed0582b:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:35ca235e2ba0506c534486681c1bf83d:::
```

Approach

Cracking the LM Hash



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
HelpAssistant	882d56ecbe9a990702c2454657e5fcb8	5e[illegible]3828b4961ba742726f96411efcb33	HQ&1OYM	GUFUZPQ	HQ&1OymguFUzpq

Table	Directory	Status	Progress
XP special	C:\CTF2\tables	2% in RAM	

Preload: done

Brute force: done

Pwd found: 1/1

Time elapsed: 0h 4m 31s

References and Links:

Download: https://goo.gl/cXzpnj

- http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/How-Cracked-Windows-Password-Part1.html
- https://technet.microsoft.com/en-us/magazine/2006.08.securitywatch.aspx
- https://digital-forensics.sans.org/blog/2012/02/29/protecting-privileged-domain-accounts-lm-hashes-the-good-the-bad-and-the-ugly
- https://www.objectif-securite.ch/en/ophcrack.php
- http://project-rainbowcrack.com/table.htm
- https://cyberarms.wordpress.com/2010/10/21/cracking-14-character-complex-passwords-in-5-seconds/
- https://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-your-users-passwords-safely/
- https://en.wikipedia.org/wiki/LM_hash
- https://en.wikipedia.org/wiki/NT_LAN_Manager
- https://asecuritysite.com/encryption/lmhash