black hat®
EUROPE 2018

DECEMBER 3-6, 2018

EXCEL LONDON / UNITED KINGDOM

illusive

When everyone's dog is named Fluffy

Abusing the brand-new security questions in Windows 10 to gain domain-wide persistence

About Us

Magal Baz
Security Researcher
at Illusive Networks

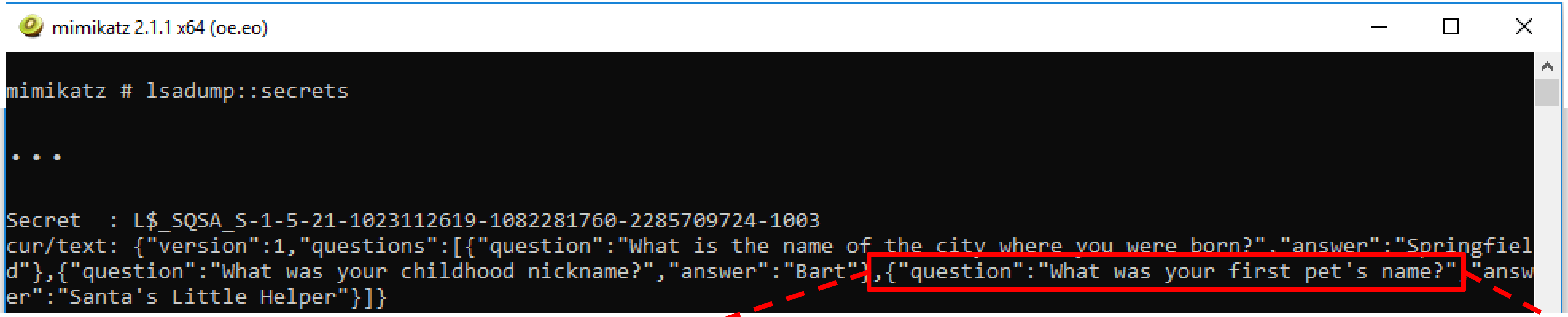
🐦 @mb1687
mbaz@illusivenetworks.com

^ ^
* -
illusive

Tom Sela
Head of Security Research
at Illusive Networks

🐦 @4x6hw
tom@illusivenetworks.com

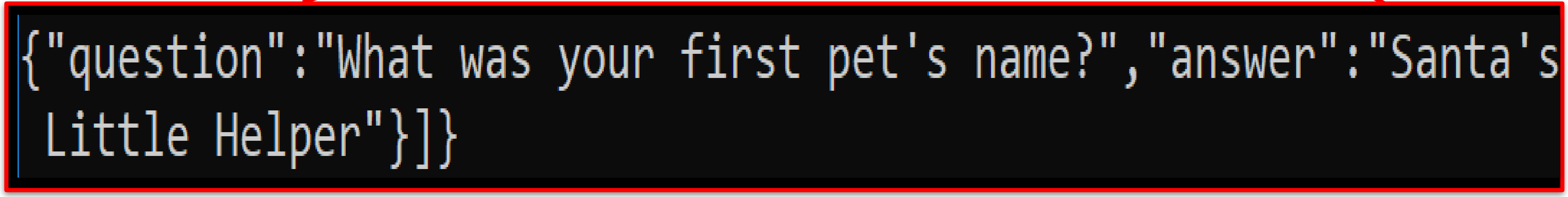
The story begins



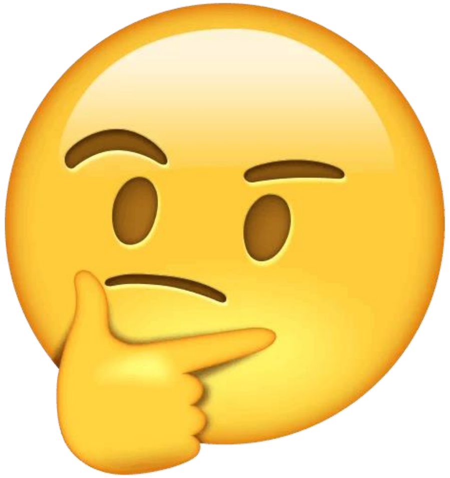
```
mimikatz # lsadump::secrets

...

Secret  : L$_SQSA_S-1-5-21-1023112619-1082281760-2285709724-1003
cur/text: {"version":1,"questions":[{"question":"What is the name of the city where you were born?","answer":"Springfiel
d"},{"question":"What was your childhood nickname?","answer":"Bart"},{"question":"What was your first pet's name?","answ
er":"Santa's Little Helper"}]}
```

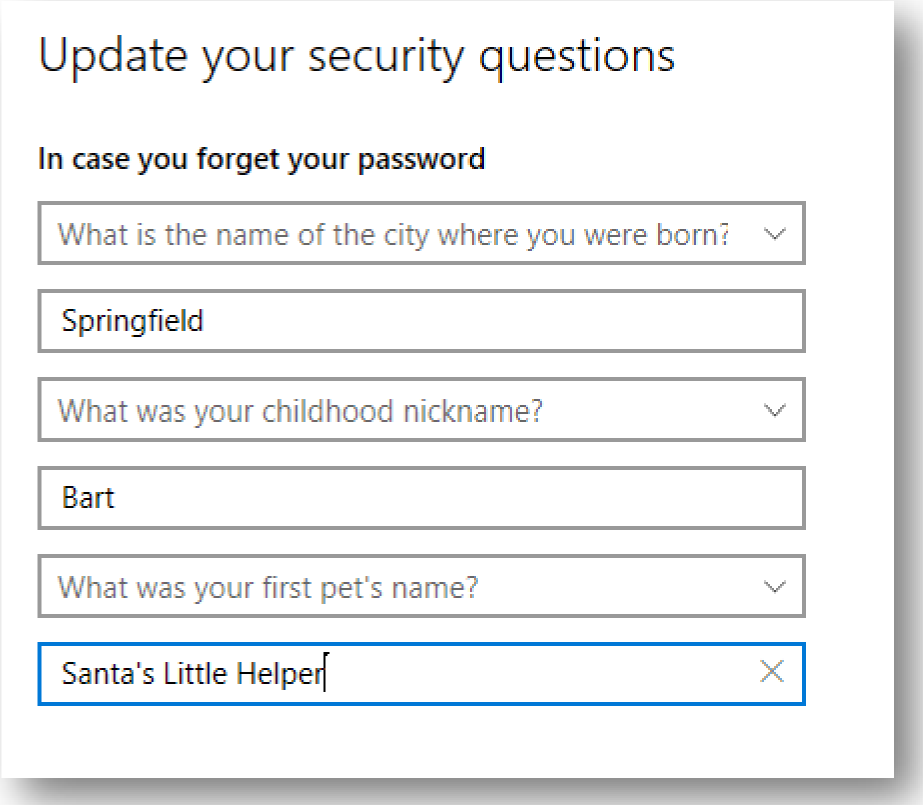


```
{"question":"What was your first pet's name?","answer":"Santa's
 Little Helper"}]}
```



Windows Security Questions
Feature Overview

- Released in version 10.1803 (April 2018)
- Local users password reset
- Stored as a LSA Secret
- Choose 3 out of 6 questions
  - “What was your childhood nickname?”
  - “What was your first pet’s name?”
  - …



Update your security questions

In case you forget your password

What is the name of the city where you were born?

Springfield

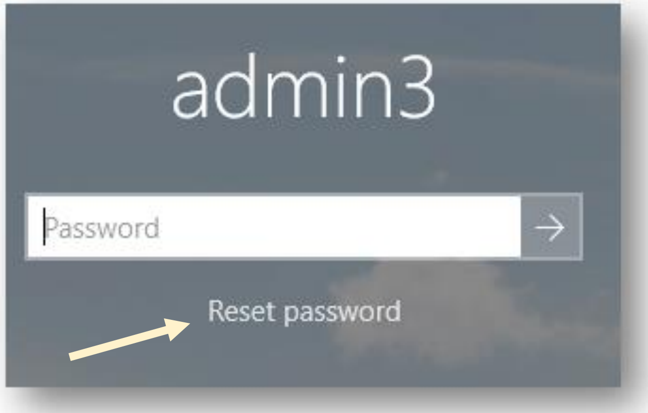
What was your childhood nickname?

Bart

What was your first pet's name?

Santa's Little Helper

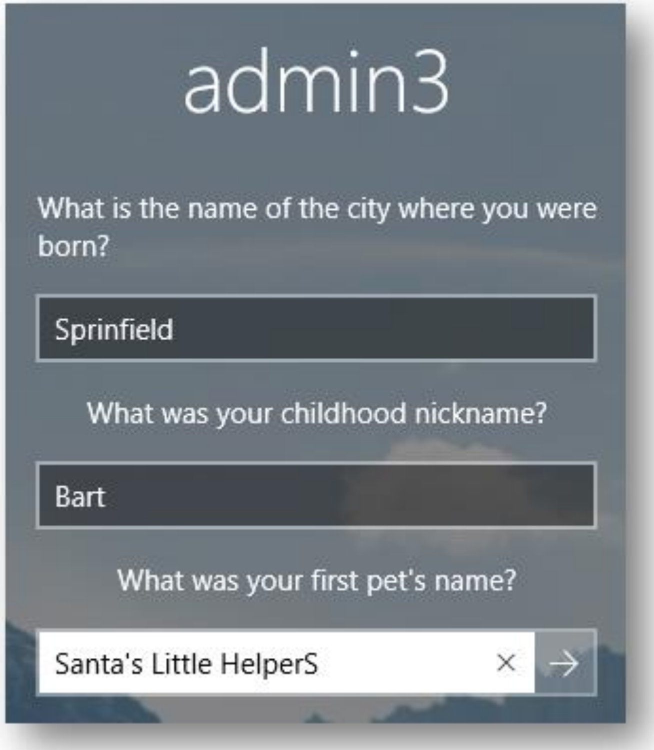
Usage



admin3

Password

Reset password



admin3

What is the name of the city where you were born?

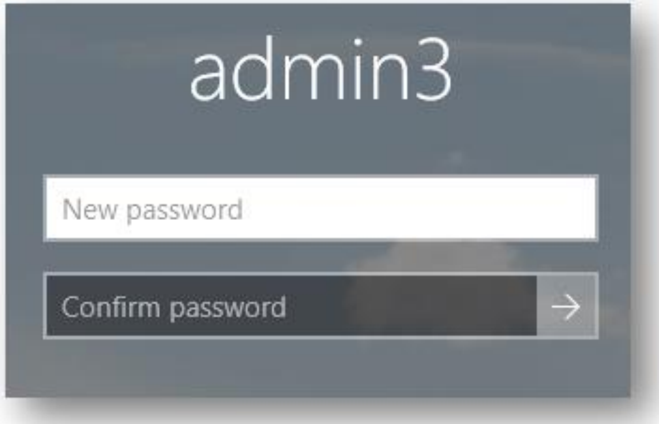
Sprinfield

What was your childhood nickname?

Bart

What was your first pet's name?

Santa's Little HelperS



admin3

New password

Confirm password

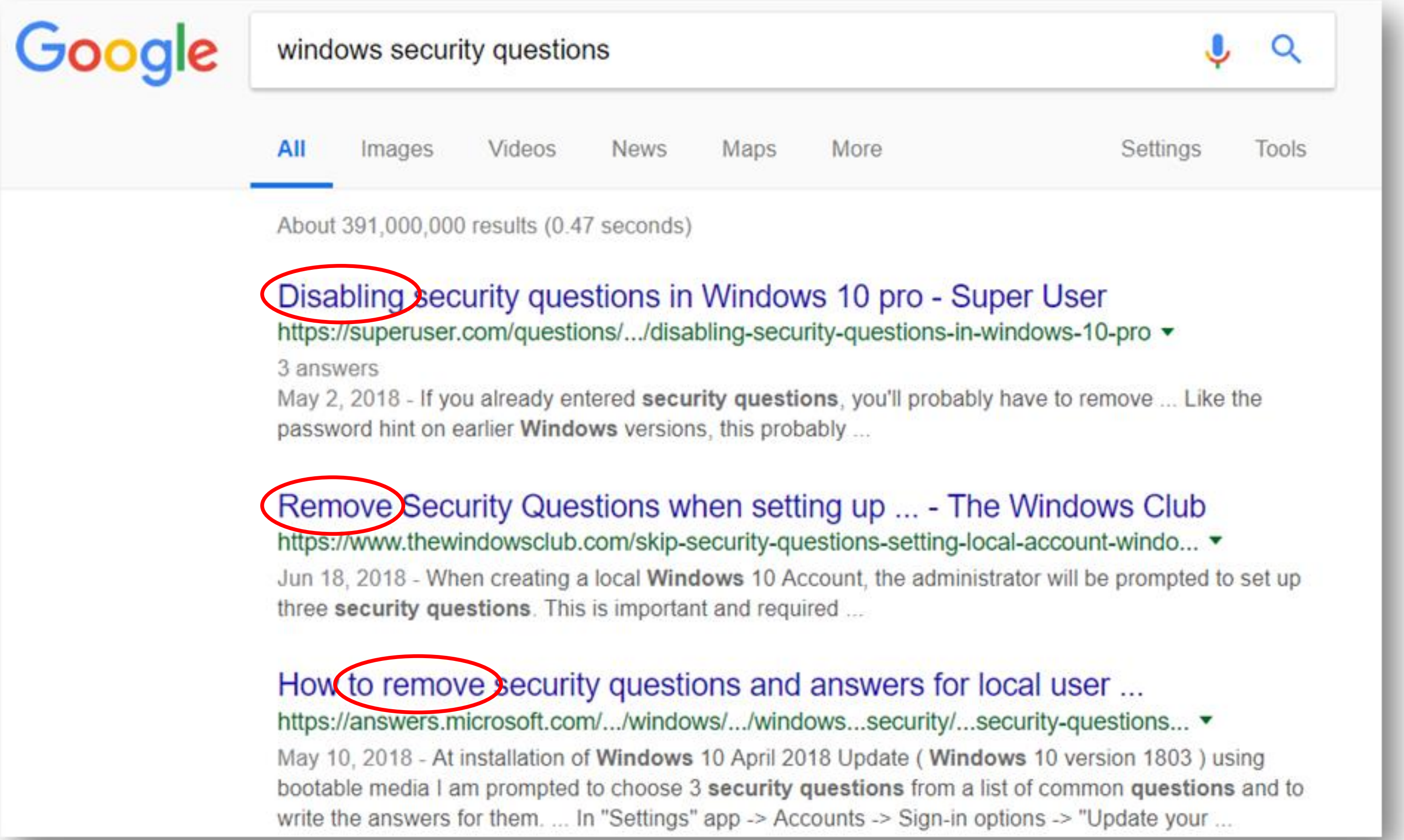
The History of Security Questions

- Been used since early 20th century by financial institutes (according to Wikipedia)
- In the 2000s, security questions came into widespread use on the Internet.
- Today many question the usefulness and security of security questions.

Windows Passwords vs. Security Questions

	Passwords	Security Questions
Complexity Requirements	✓	✗
Expiration Date	✓	✗
Administration Control	✓	✗
Auditing	✓	✗ ✓
immune to Social Engineering	✗	✗ ✗ ✗

Enthusiastic Feedback



About 391,000,000 results (0.47 seconds)

Disabling security questions in Windows 10 pro - Super User
https://superuser.com/questions/.../disabling-security-questions-in-windows-10-pro ▾
3 answers
May 2, 2018 - If you already entered **security questions**, you'll probably have to remove ... Like the password hint on earlier **Windows** versions, this probably ...

Remove Security Questions when setting up ... - The Windows Club
https://www.thewindowsclub.com/skip-security-questions-setting-local-account-windo... ▾
Jun 18, 2018 - When creating a local **Windows** 10 Account, the administrator will be prompted to set up three **security questions**. This is important and required ...

How to remove security questions and answers for local user ...
https://answers.microsoft.com/.../windows/.../windows...security/...security-questions... ▾
May 10, 2018 - At installation of **Windows** 10 April 2018 Update (**Windows** 10 version 1803) using bootable media I am prompted to choose 3 **security questions** from a list of common **questions** and to write the answers for them. ... In "Settings" app -> Accounts -> Sign-in options -> "Update your ...

Security Attack Scenarios

Without a privileged user	With a privileged user
Gain remote access by social engineering	
Gain remote access by brute force	

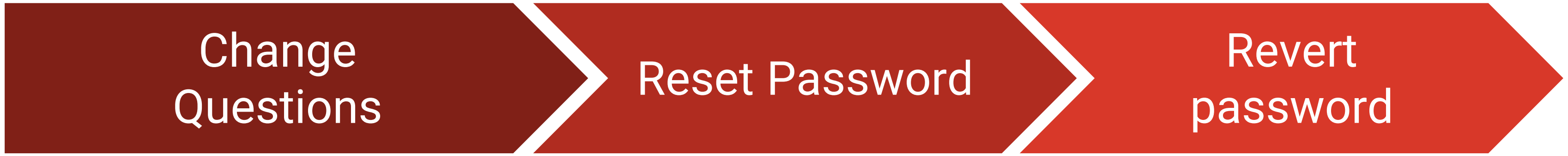
Security Attack Scenarios

Without a privileged user	With a privileged user
Gain remote access by social engineering	Use security questions as a stealthy backdoor
Gain remote access by brute force	

Our Goal: Security Question as a Backdoor

- A stealthy backdoor - make everyone's dog name Fluffy, forever
  - Can we change the questions and answers remotely?
  - Can we reset a password remotely?
  - After resetting the password, can we change it back to the original password?

Can it be done?



Change Questions

Reset Password

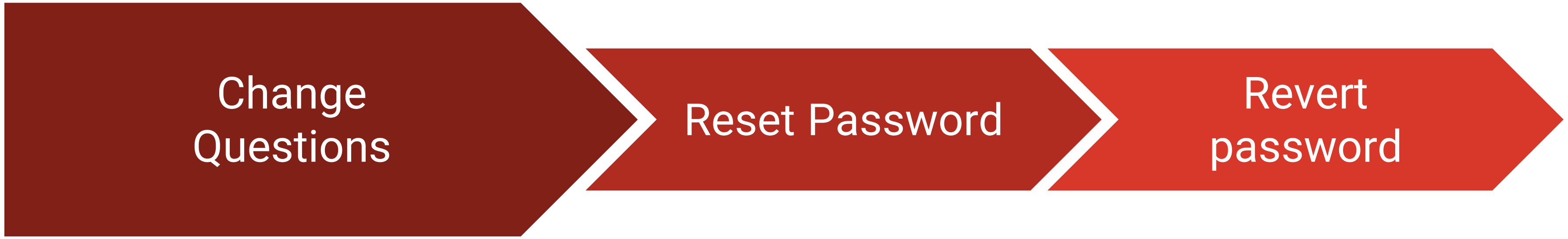
Revert password

- **Spoiler:** Yes, it can be done. No, seriously, we wouldn’t be accepted to talk here otherwise.

- **Disclaimer:** This is not an exploit, it works on local users and you first have to obtain a privileged user.

Roadmap

- **Set security questions remotely**
- Reset password remotely
- Revert password back to original



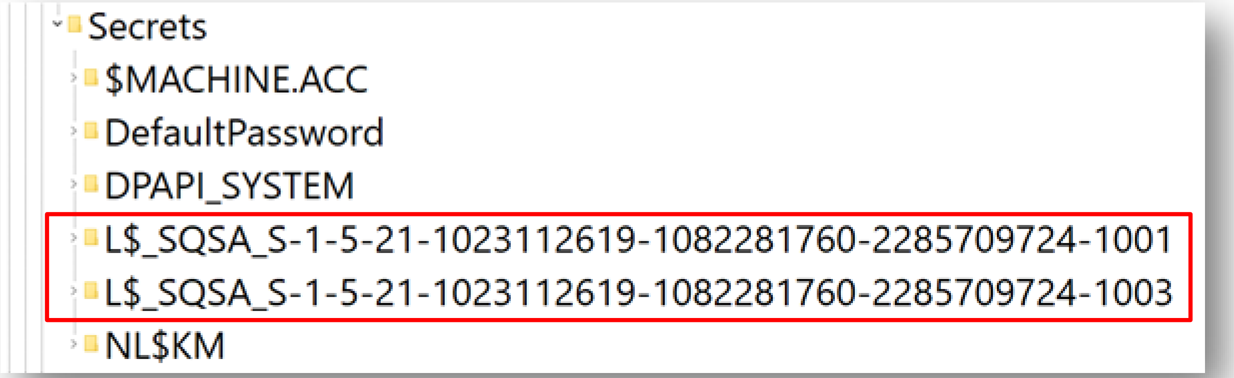
Change Questions

Reset Password

Revert password

LSA Secrets Introduction

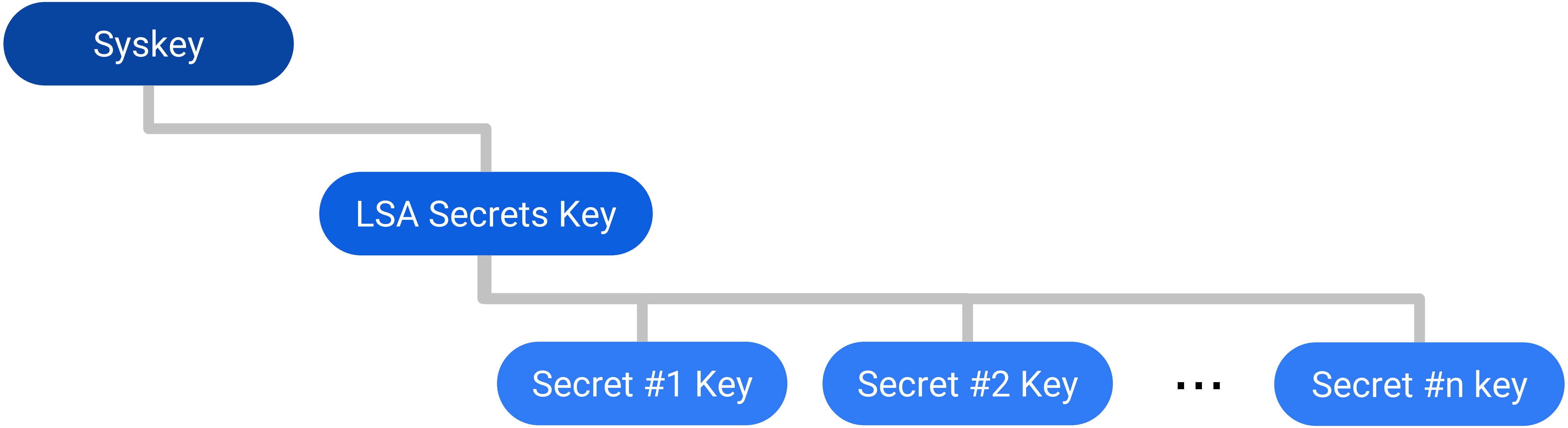
- Safe storage mechanism in Windows
- Stores stuff like:
  - Machine password
  - DPAPI master key
  - Service users' passwords
- Stored at HKLM\Security\Policy\Secrets



```
Secrets
  $MACHINE.ACC
  DefaultPassword
  DPAPI_SYSTEM
  L$_SQSA_S-1-5-21-1023112619-1082281760-2285709724-1001
  L$_SQSA_S-1-5-21-1023112619-1082281760-2285709724-1003
  NL$KM
```

LSA Secrets Encryption

- Undocumented API (Advapi32.dll): LsaCreateSecret, LsaOpenSecret, LsaSetSecret, LsaQuerySecret
- **AES256** encrypted
- Implemented in open source projects such as Impacket and Mimikatz

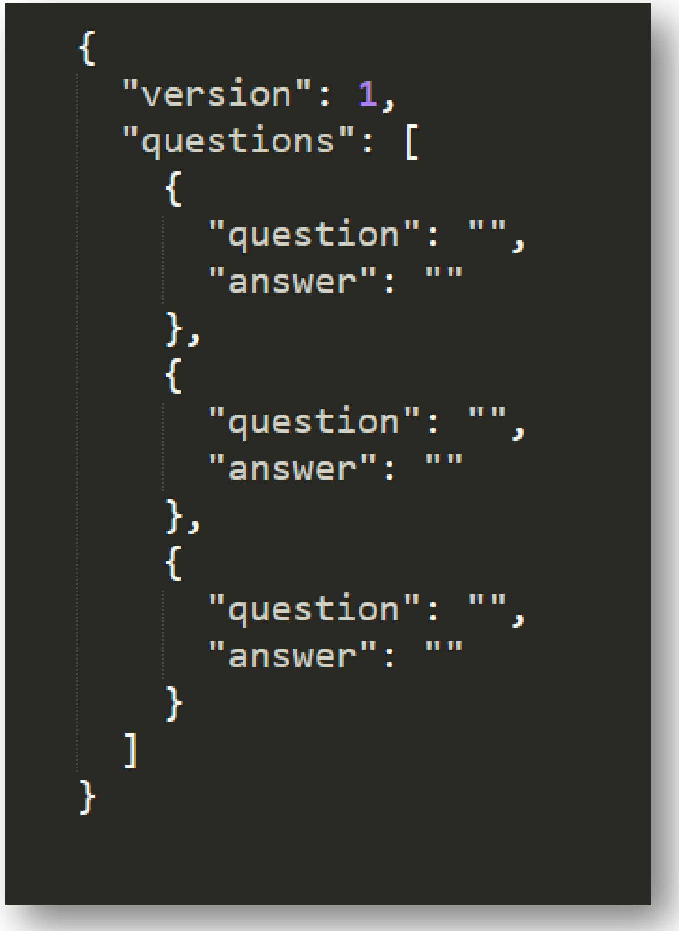


LSA Secrets Permissions

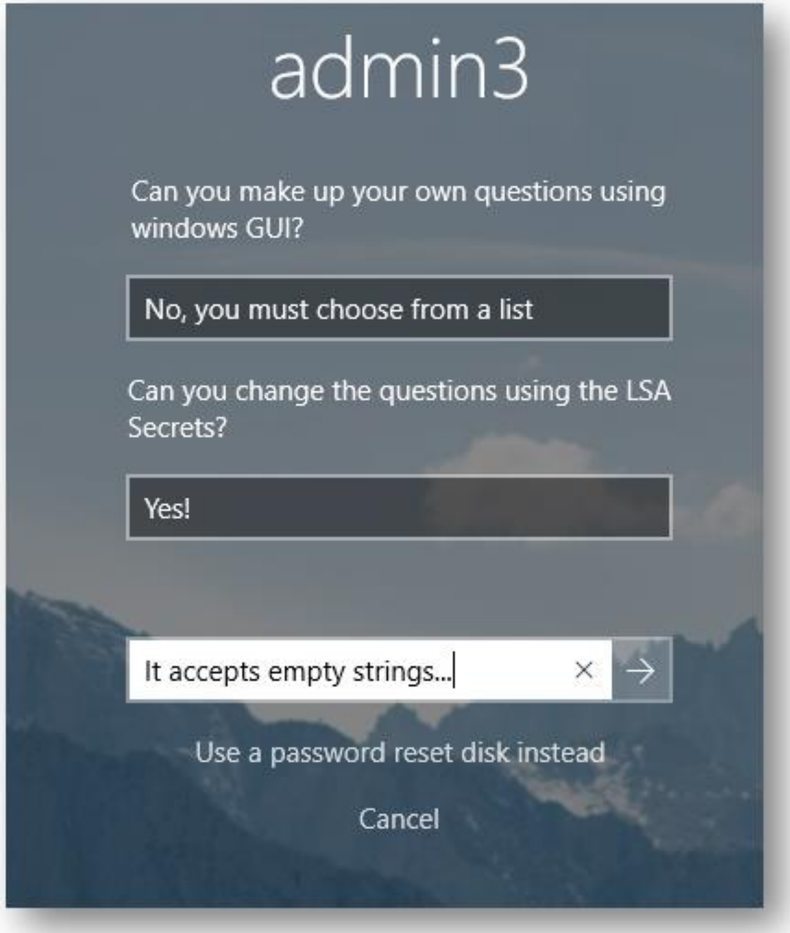
- Only SYSTEM account can read\write
- Administrators can write ACLs
- Implementation Options:
  - BaseRegSaveKey (RPC) - Save key to disk using SE_BACKUP_NAME privilege
  - Regini.exe **-** Crude remote ACLs modification
  - **BaseRegSetKeySecurity (RPC) - Precise ACLs modification**

Security Question LSA Secret

- Stored as JSON
- Name format: “L$_SQSA_<SID>”
    - L$ - Local Secret
    - SQSA -perhaps **S**ecurity **Q**uestions **S**ecurity **A**nswers
    - SID - Identify the owner



```
{
  "version": 1,
  "questions": [
    {
      "question": "",
      "answer": ""
    },
    {
      "question": "",
      "answer": ""
    },
    {
      "question": "",
      "answer": ""
    }
  ]
}
```



admin3

Can you make up your own questions using windows GUI?

No, you must choose from a list

Can you change the questions using the LSA Secrets?

Yes!

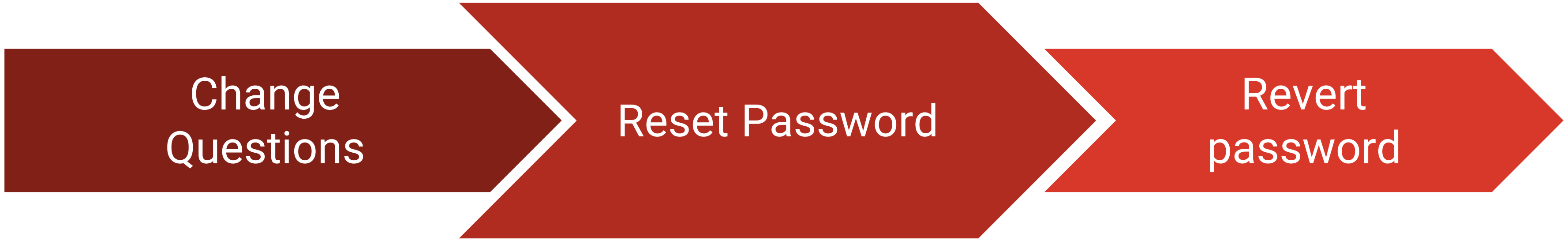
It accepts empty strings...

Remote LSA Secrets Read/Write Implementations

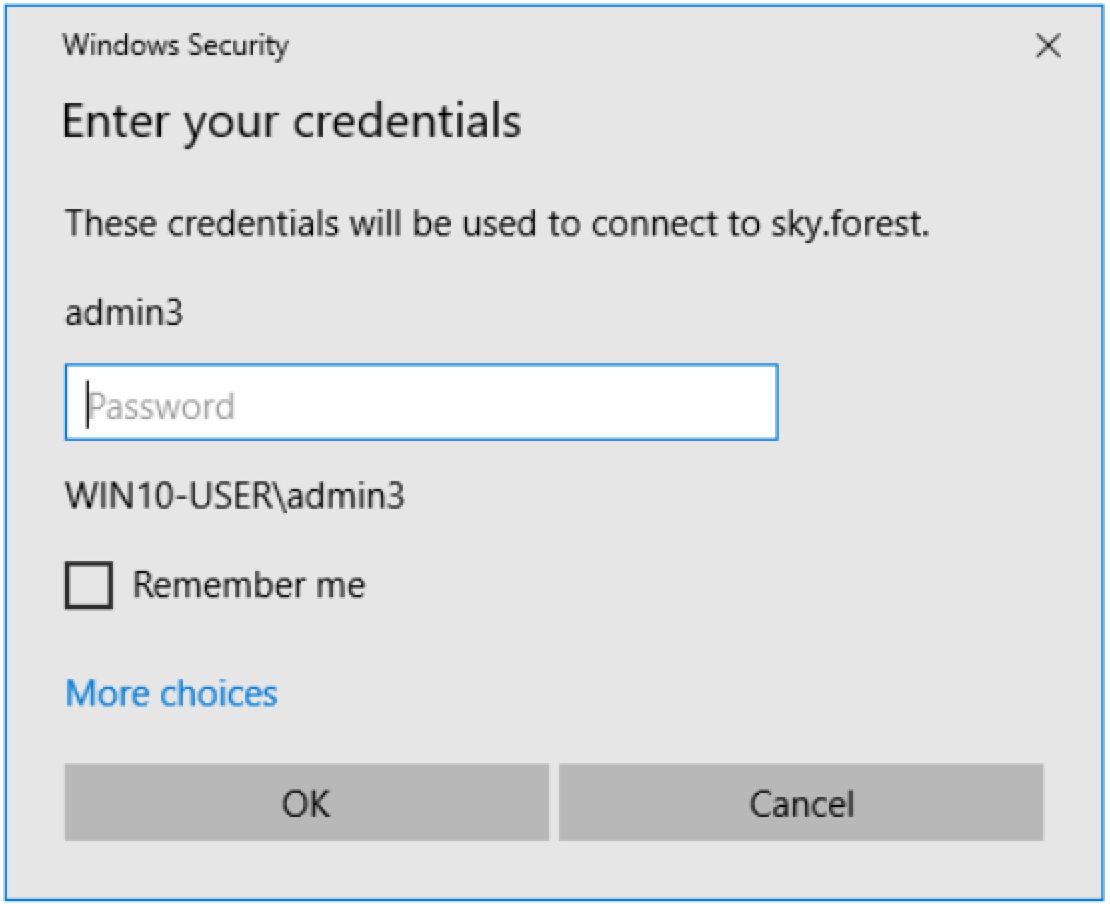
- Flow using remote registry RPC:
  - Create our JSON
  - Add read\write access to remote registry *(BaseRegSetKeySecurity)*
  - Get SysKey --> LSAKey - *(BaseQueryValue)*
  - Use LSAKey to encrypt our JSON
  - Write new secret to target registry *(BaseRegSetValue)*

Roadmap

- Set security questions remotely
- **Reset password remotely**
- Revert password back to original



Remote Password Reset



Windows Security

Enter your credentials

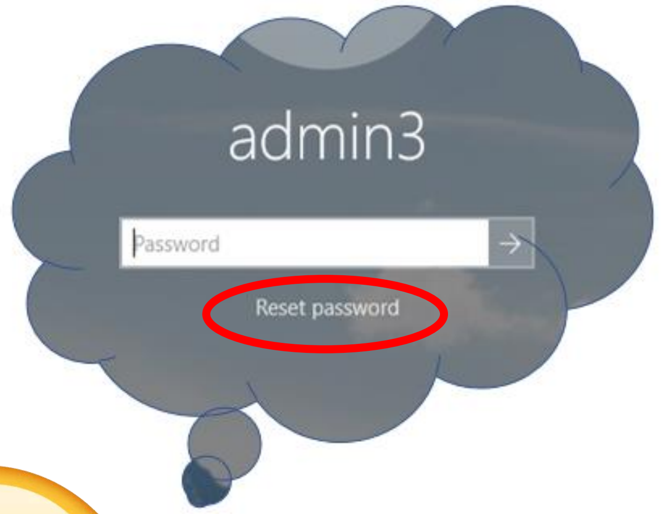
These credentials will be used to connect to sky.forest.

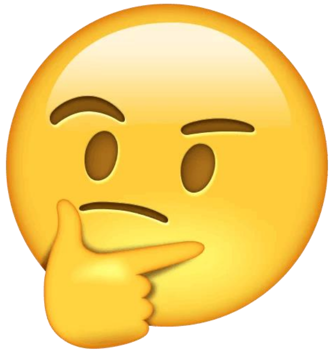
admin3

Password

WIN10-USER\admin3

□ Remember me



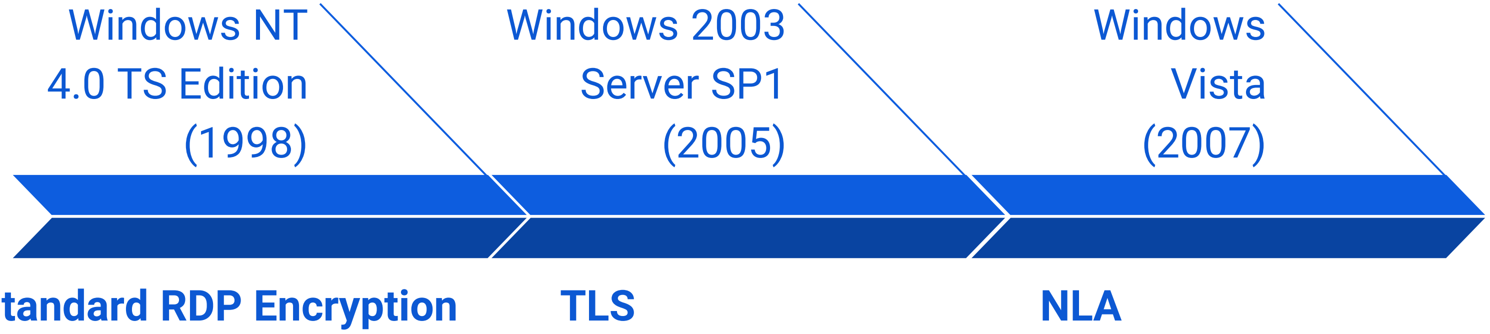


Where is the
“Reset Password” button?!

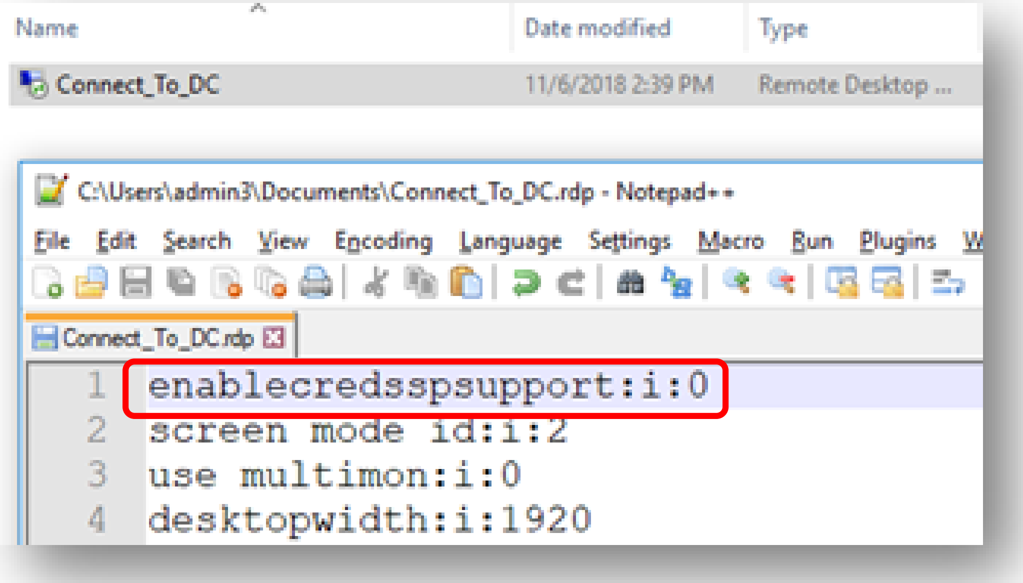
NLA and CredSSP

- **N**etwork **L**evel **A**uthentication
- Authentication of both client and server
- It is possible to fall back to Non-NLA authentication
- Take care of NLA enforcement - earlier on

Evolution of RDP protection:


Windows NT 4.0 TS Edition (1998)
Windows 2003 Server SP1 (2005)
Windows Vista (2007)
Standard RDP Encryption
TLS
NLA

How to Evade NLA

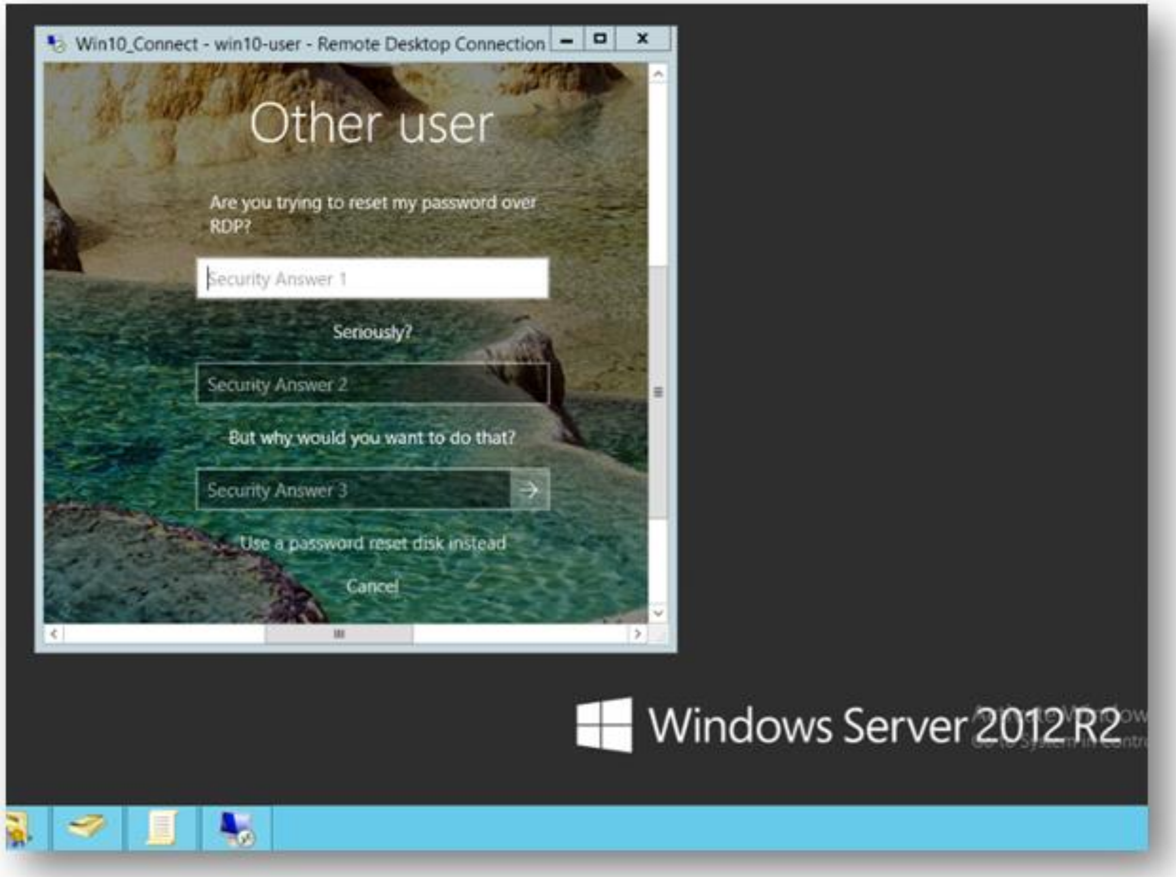


Connect_To_DC 11/6/2018 2:39 PM Remote Desktop ...

C:\Users\admin3\Documents\Connect_To_DC.rdp - Notepad++

Connect_To_DC.rdp

```
enablecredsspsupport:i:0
screen mode id:i:2
use multimon:i:0
desktopwidth:i:1920
```



Win10_Connect - win10-user - Remote Desktop Connection

Other user

Are you trying to reset my password over RDP?

Security Answer 1

Seriously?

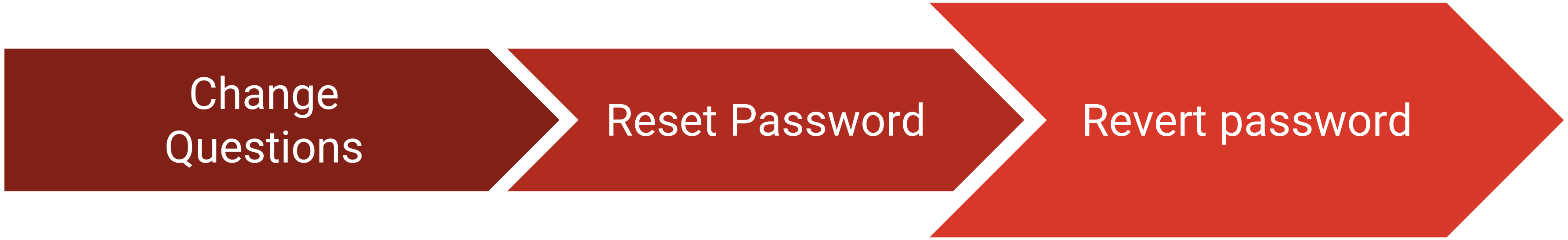
Security Answer 2

But why would you want to do that?

Security Answer 3

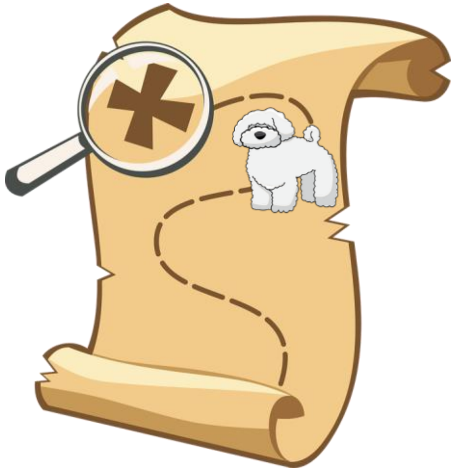
Roadmap

- Set security questions remotely
- Reset password remotely
- **Revert password back to original**


Change Questions

Reset Password

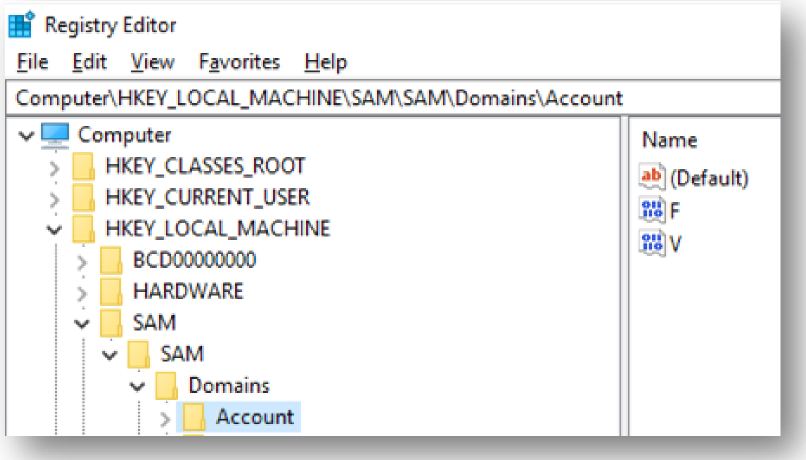
Revert password



Restore Previous Password

- Historic NTLM hashes in SAM key
  - Protected by AES128
  - Assemble the key from registry artifacts

- Change active NTLM hash with **SamSetInformationUser**
- Implemented in Mimikatz
  - *lsadump::sam*
  - *lsadump:setntlm*



Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account

Demo

Goal Achieved

- It is possible to spray security questions to gain domain-wide persistence which never expire and are not audited
- **Everyone's dog is named Fluffy, forever**

Recommendations

How this attack could have been detected\prevented?

- Windows:
  - Add GPO to disable\audit security questions
  - Allow opt-out from the security questions feature at Windows 10 Enterprise versions
  - Allow custom security questions*

- Security teams:
  - Minimize usage of local user administrators.
  - Monitor local password reset event and ACL changes on HKLM\Security
  - Set GPO to enforce NLA on RDP sessions
  - Control security question with our tool - https://github.com/IllusiveNetworks-Labs

Summary

- New feature raises serious security questions.
- Can be used for stealthy backdoor and domain-wide persistence.
- Security teams should be aware of this new feature and how to reduce it's potential risk.

Any (security) questions?