Conference 2018

Renaissance Midtown Hotel

New York, NY

Offline Attacks on Active Directory

Michael Grafnetter

Security Researcher and Trainer

Presenter bio

Michael Grafnetter

Security Researcher and Trainer

Michael is an expert in Active Directory security. He is the author of the DSInternals PowerShell module and Thycotic Weak Password Finder, tools used by security auditors and penetration testers worldwide. In the role of a security consultant, he has performed multiple security audits at large enterprises, mostly financial institutions. Michael is a former PowerShell MVP.

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.

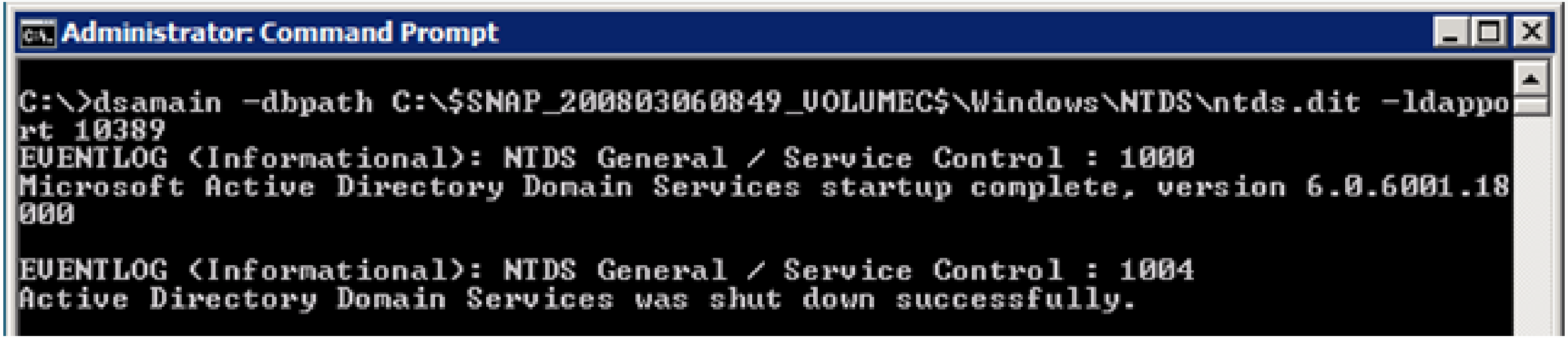
The DSInternals project consists of these two parts:

- 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.

WARNING

The following presentation features demos performed by professionals, so for your safety and the protection of those around you, do not attempt to re-enact any activity you are about to see.

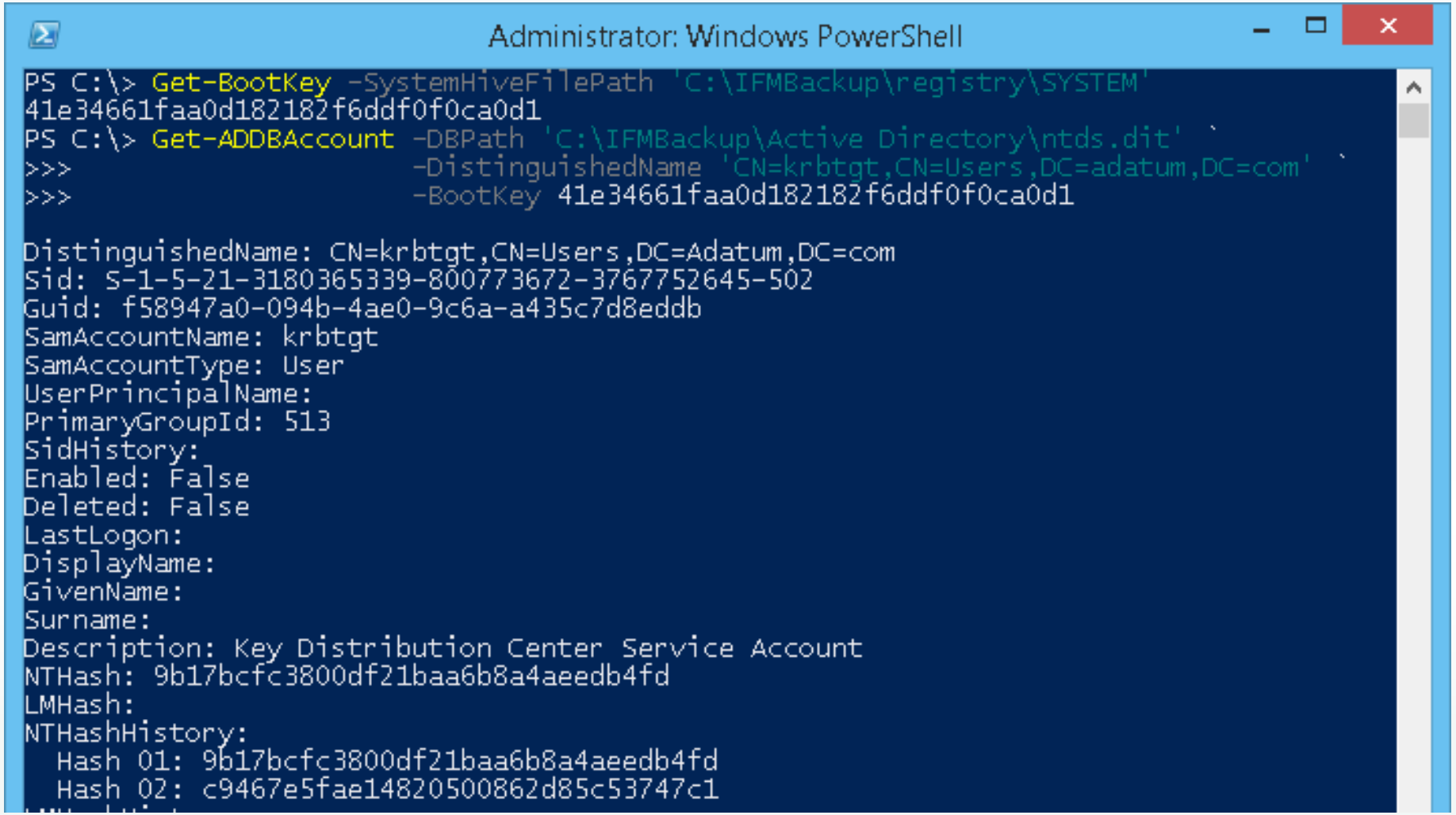
Database Mounting Tool



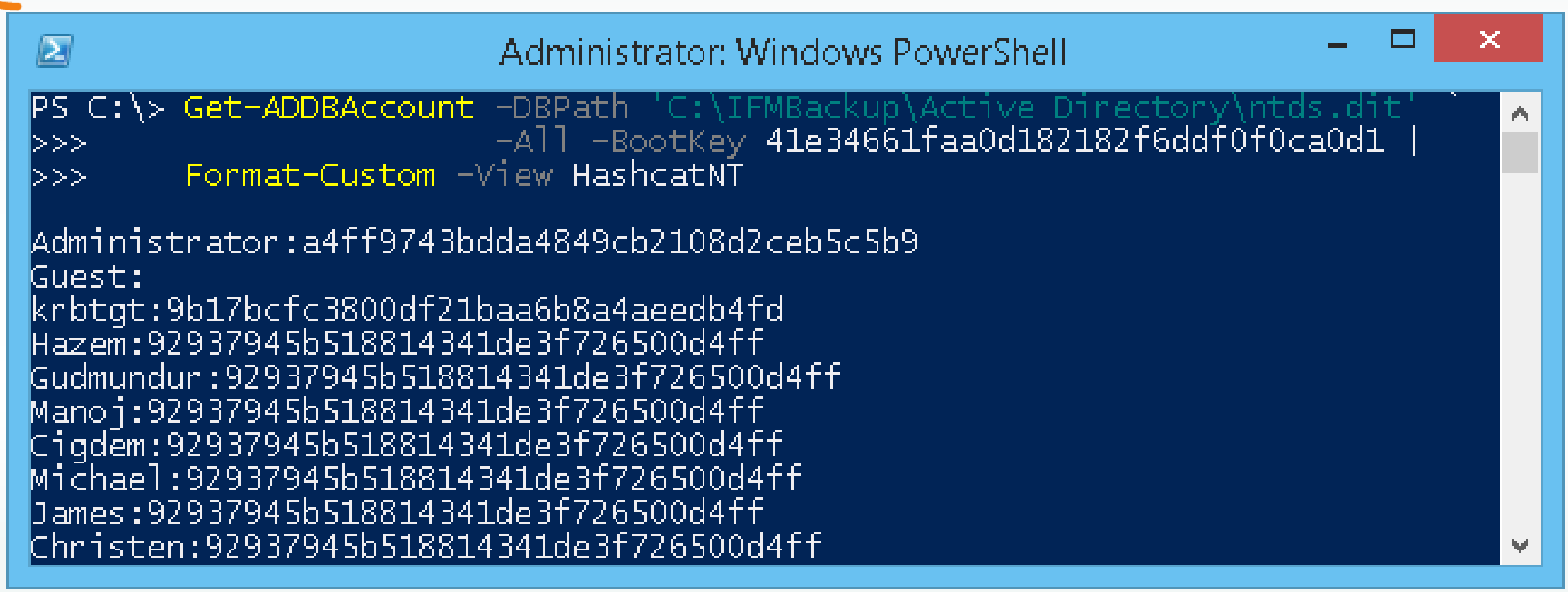
Disadvantages

- Read-only
- Hides secret attributes

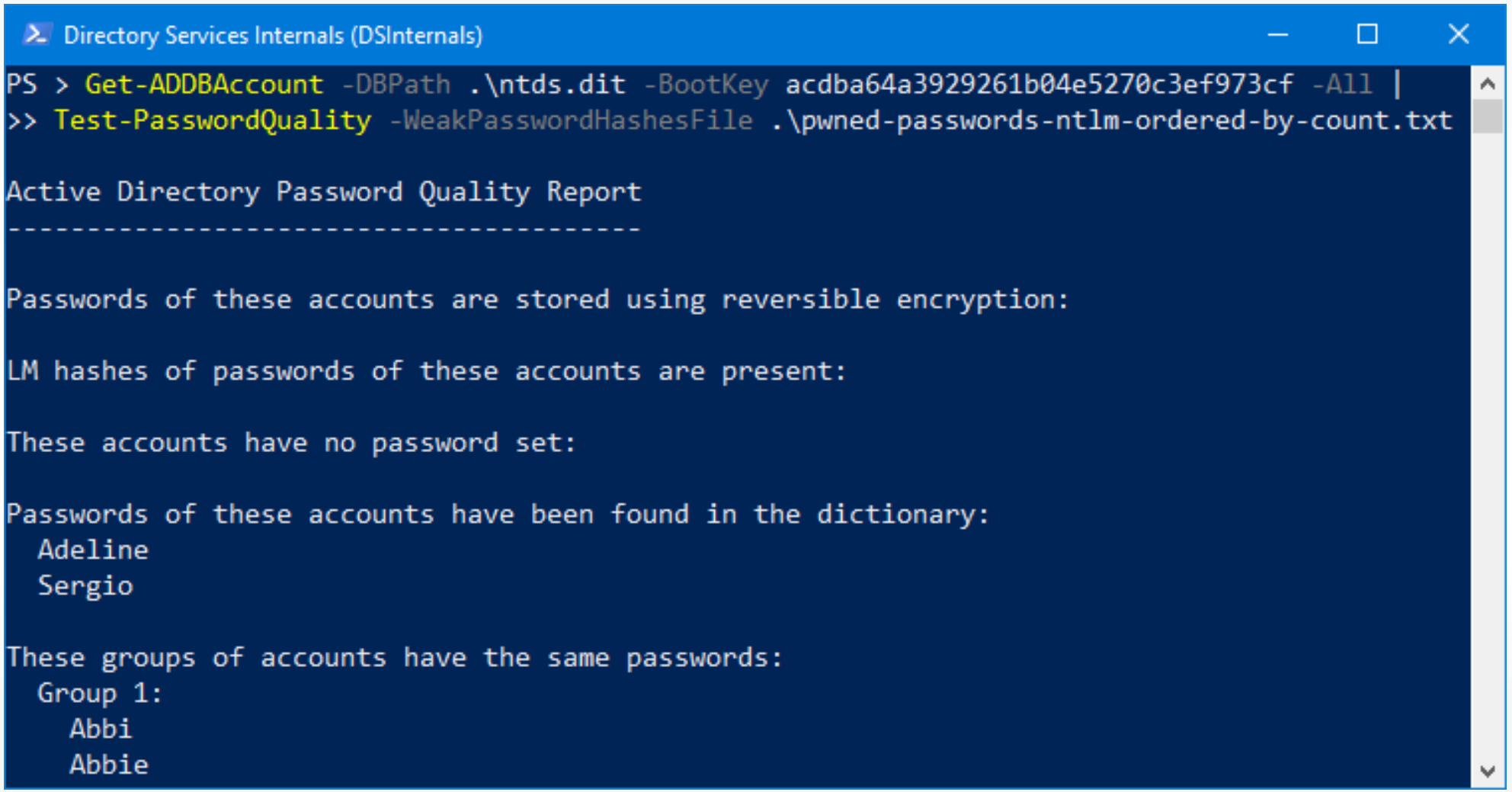
Dumping AD Secrets



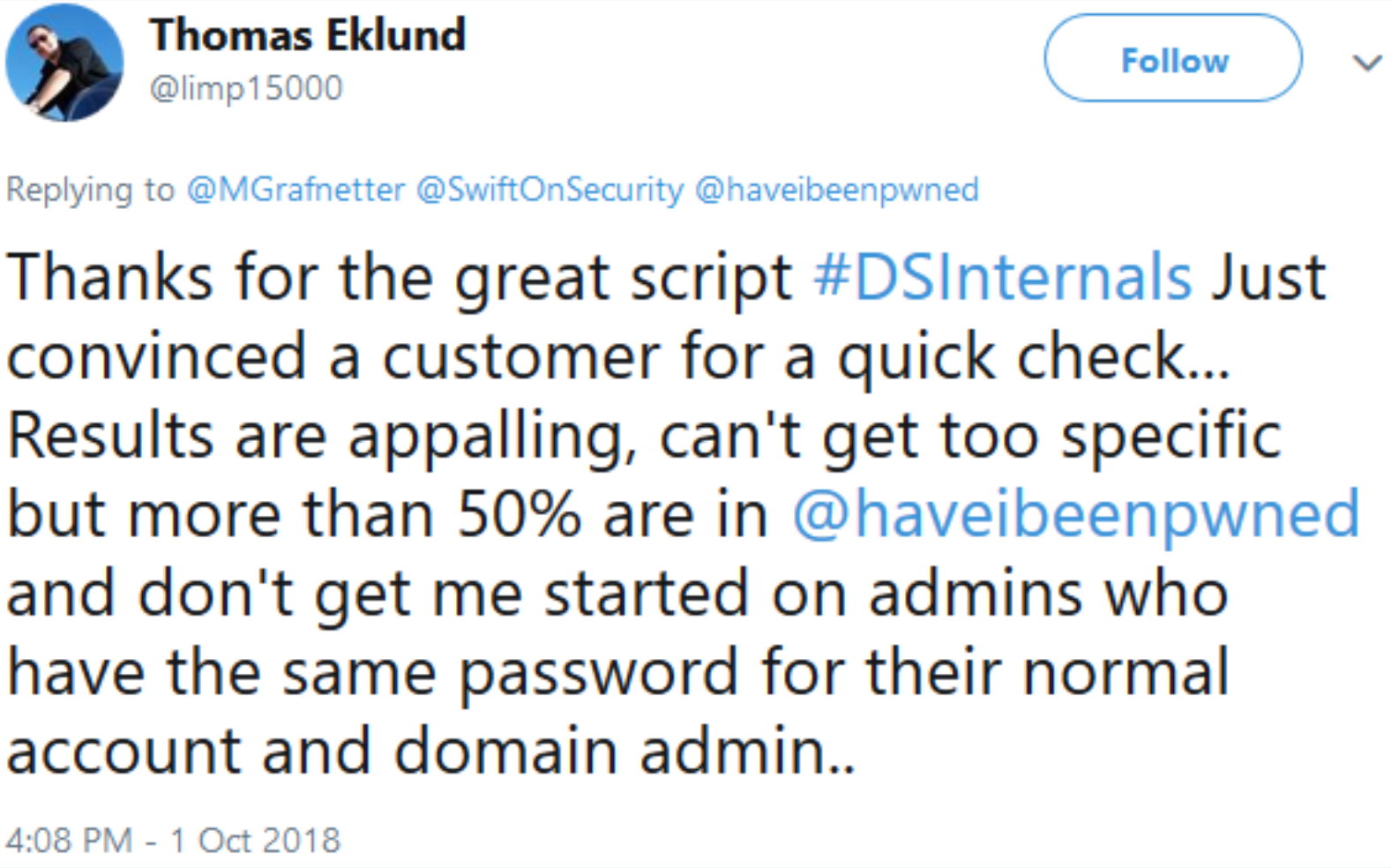
Export Formats



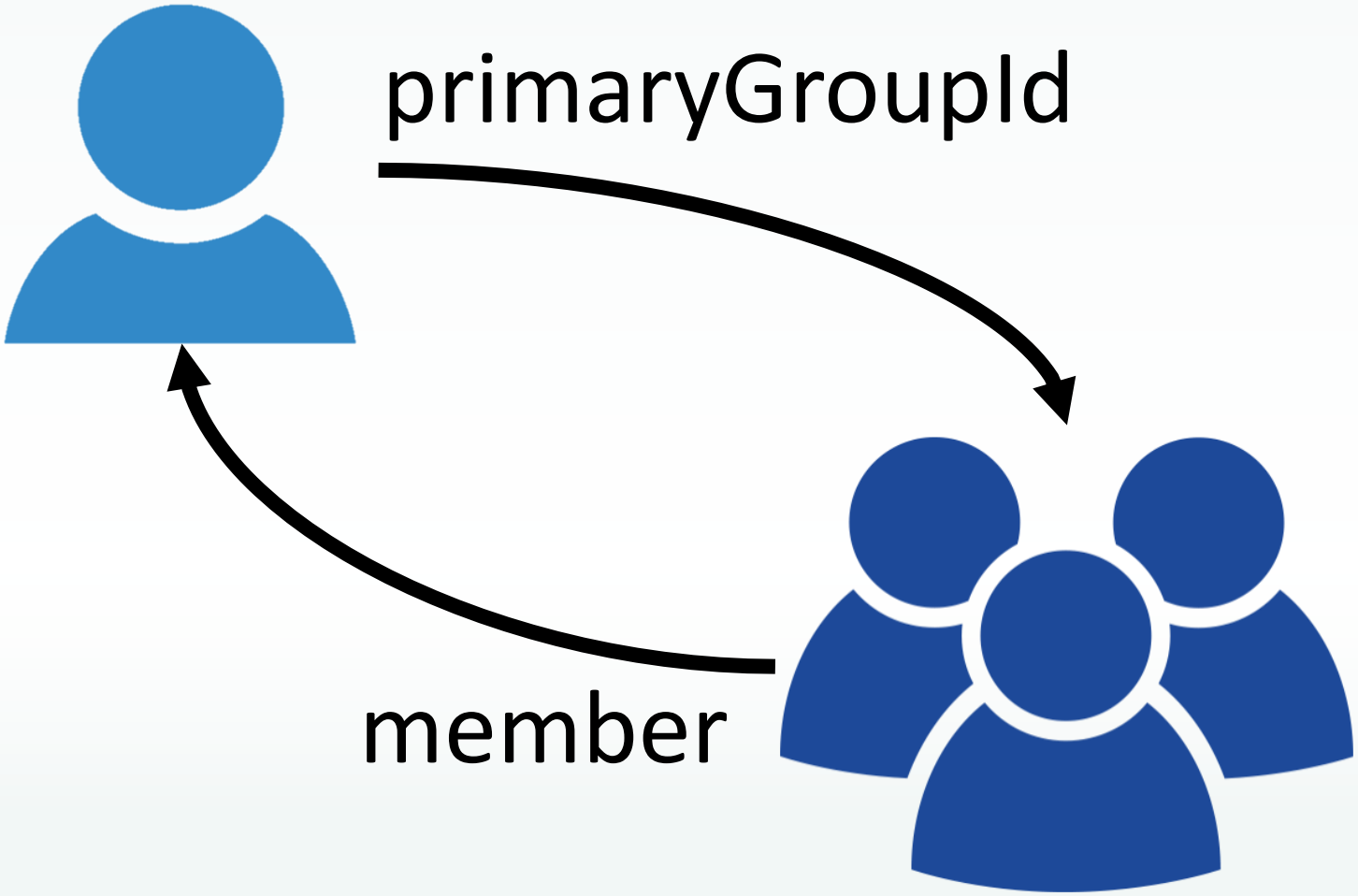
Auditing AD Passwords



Auditing AD Passwords



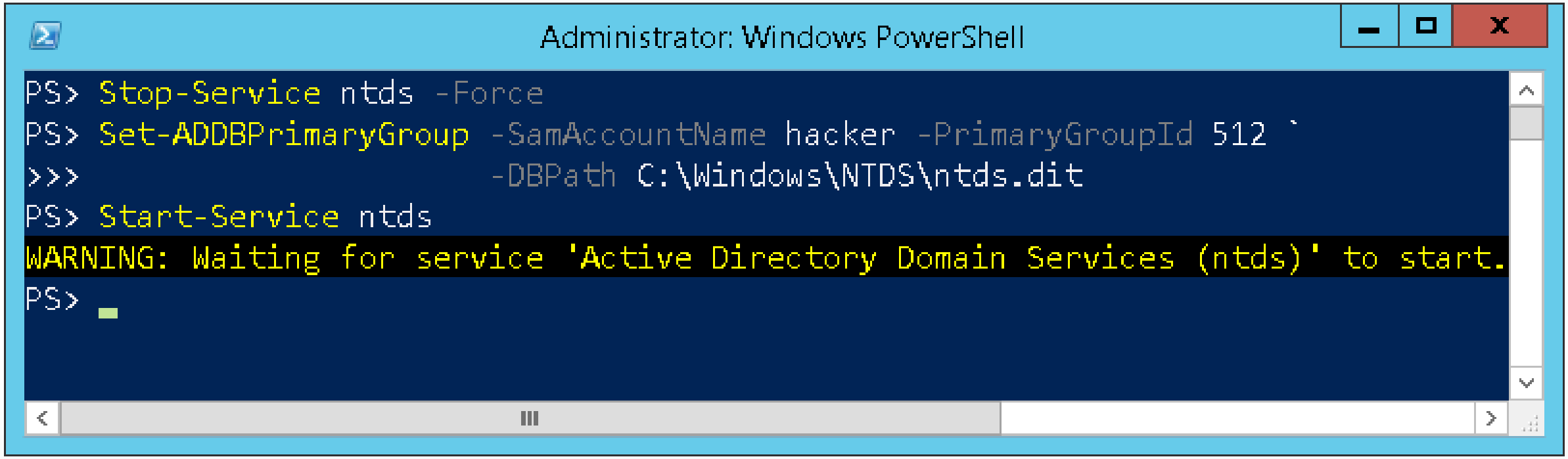
AD Group Membership



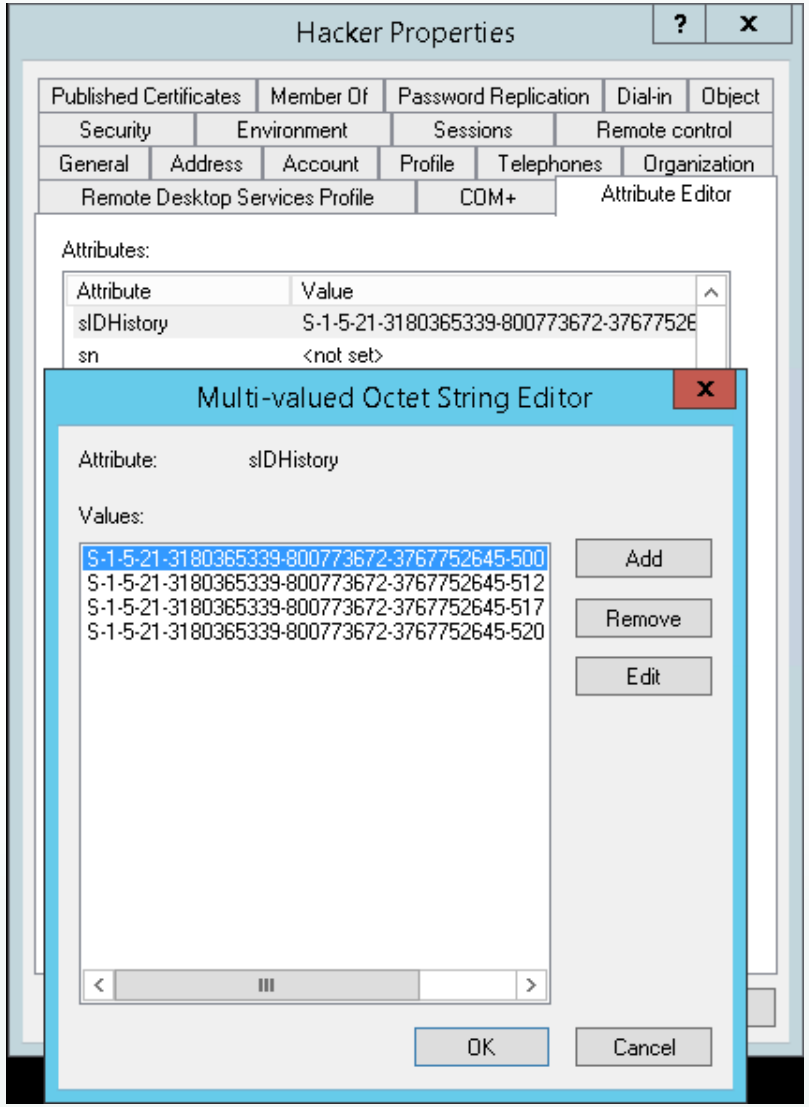
Well-Known Global Group RIDs

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

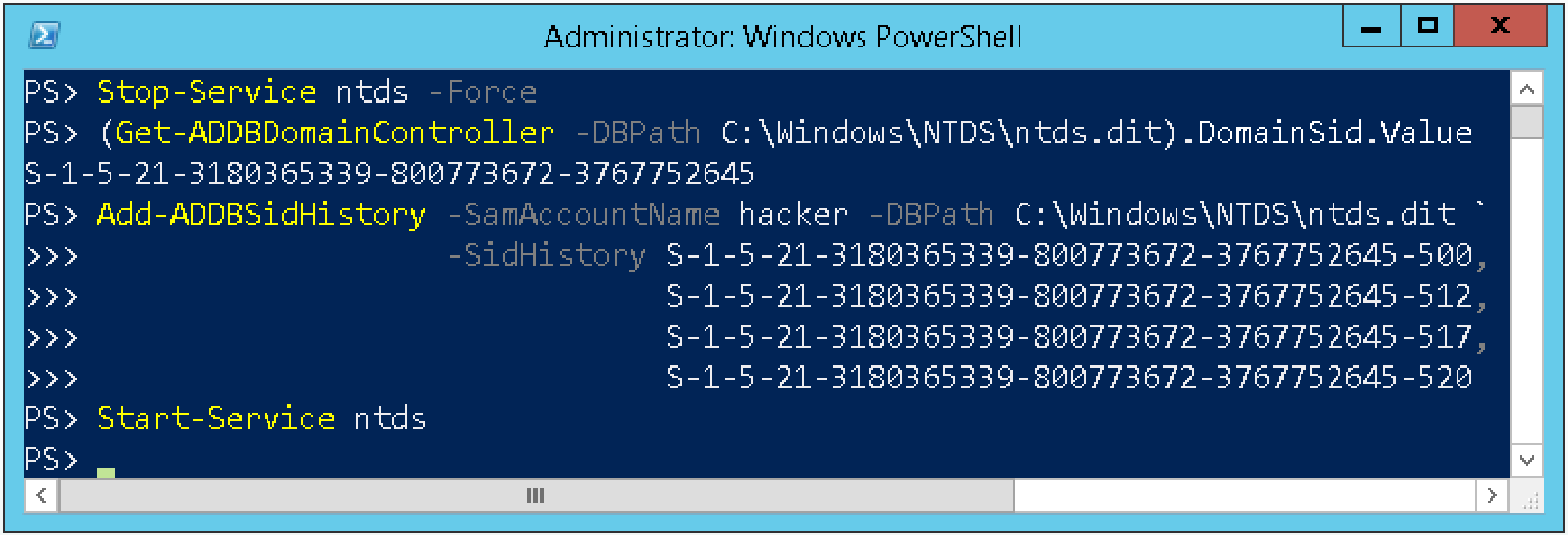
Offline Group Membership Modification



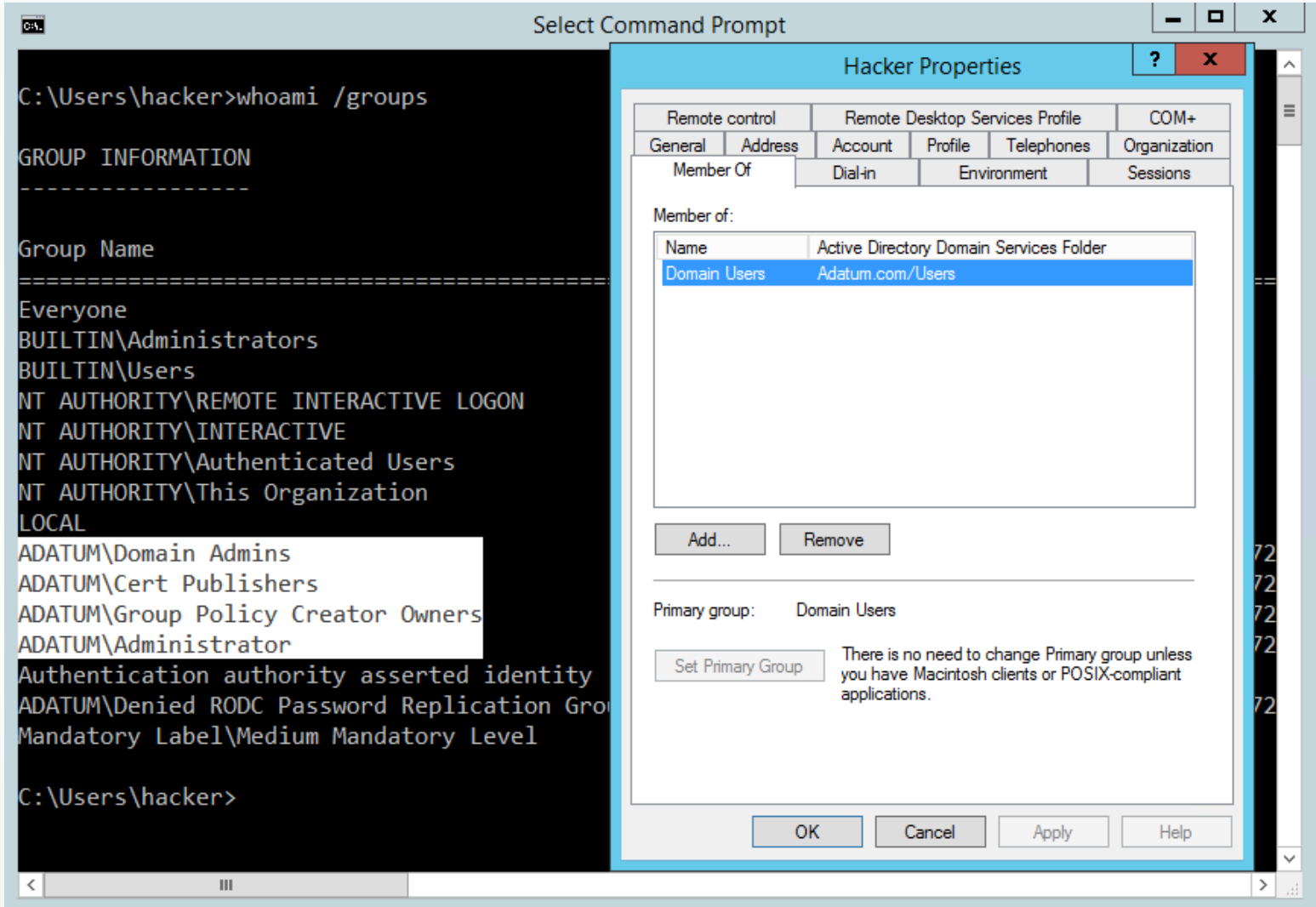
Forging SID History



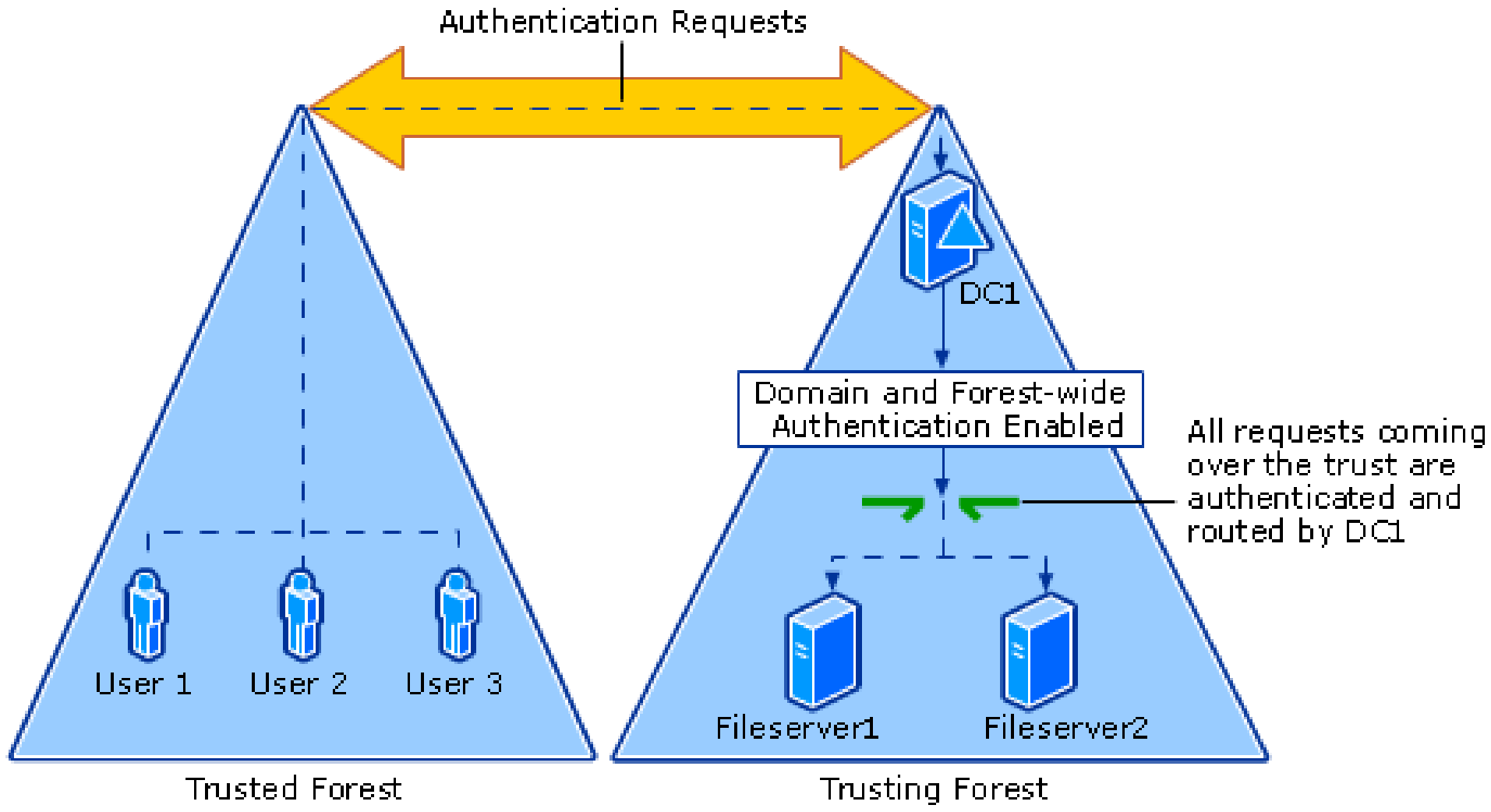
Forging SID History



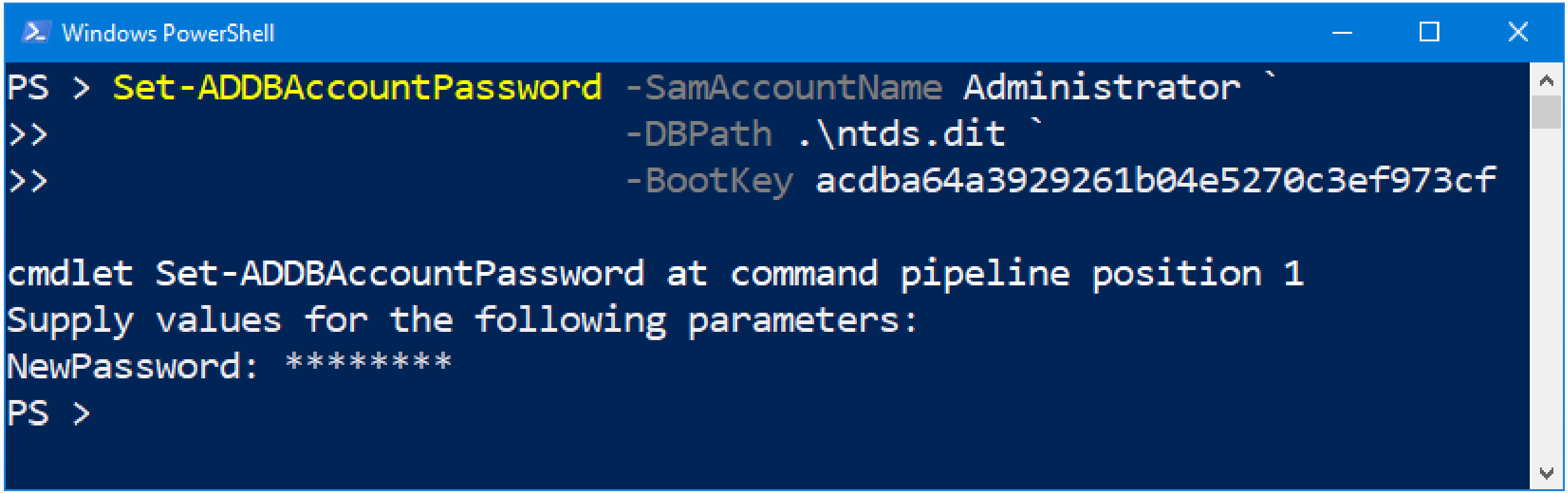
Forging SID History



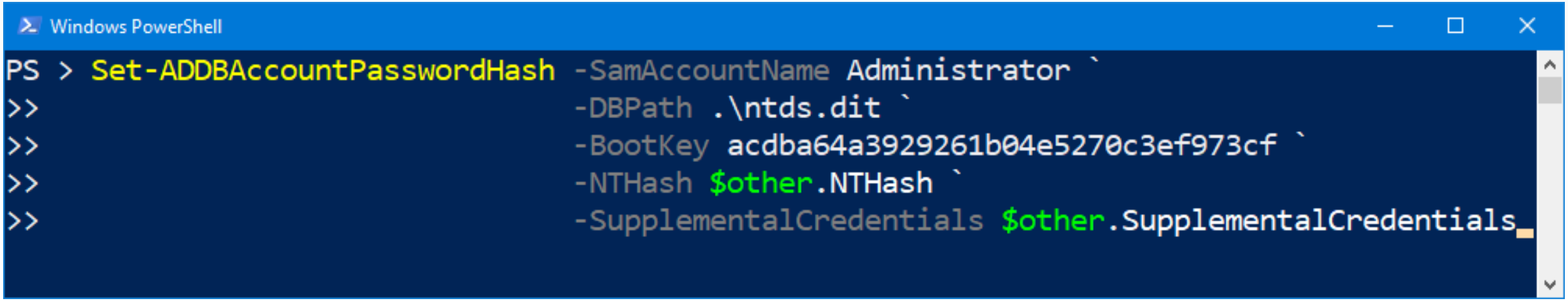
SID Filtering?



Offline Password Reset



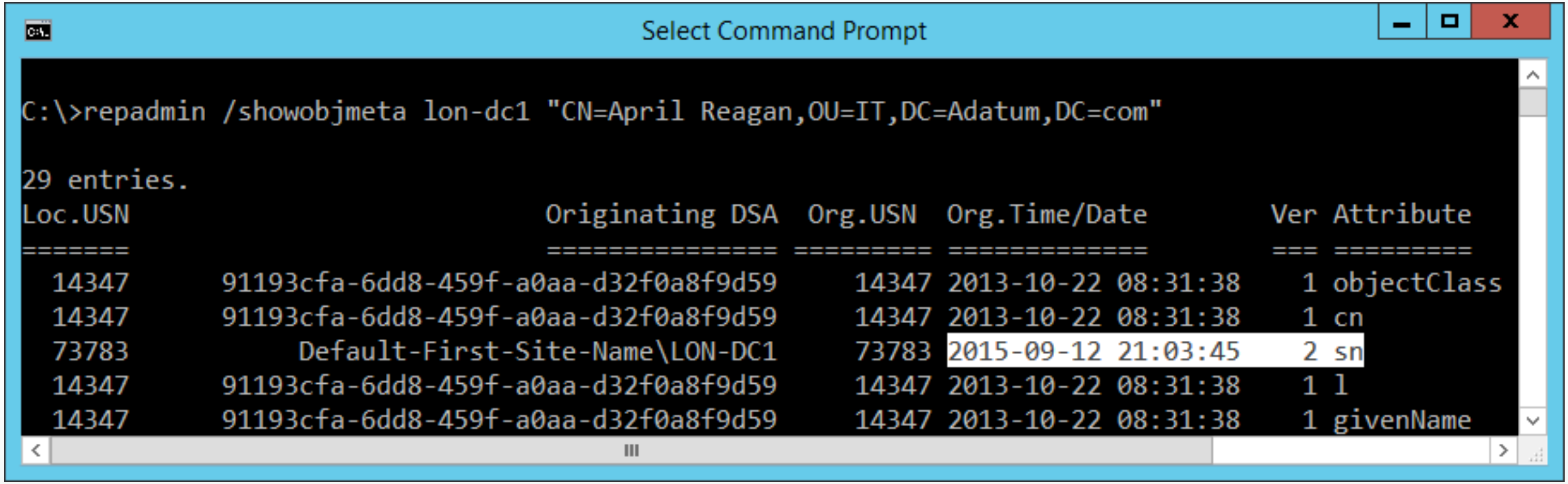
Password Hash Cloning



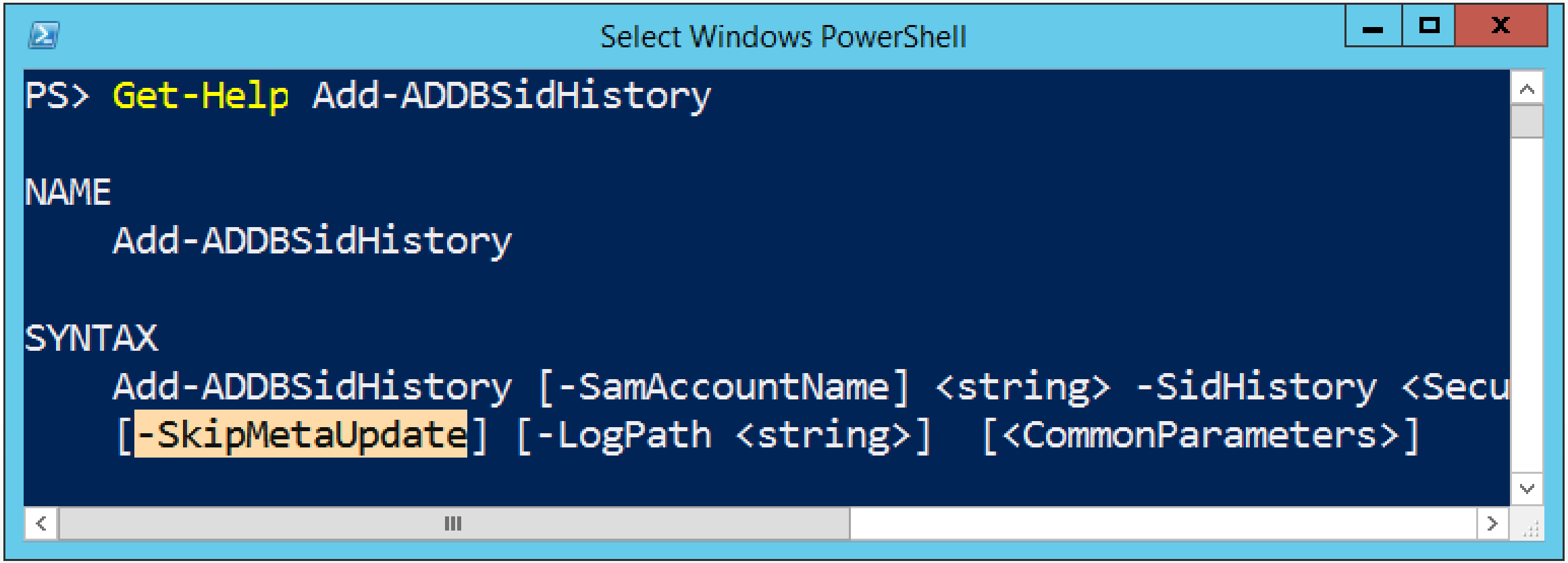
DEMO

Offline AD Database Modification

Replication Metadata



Replication Metadata



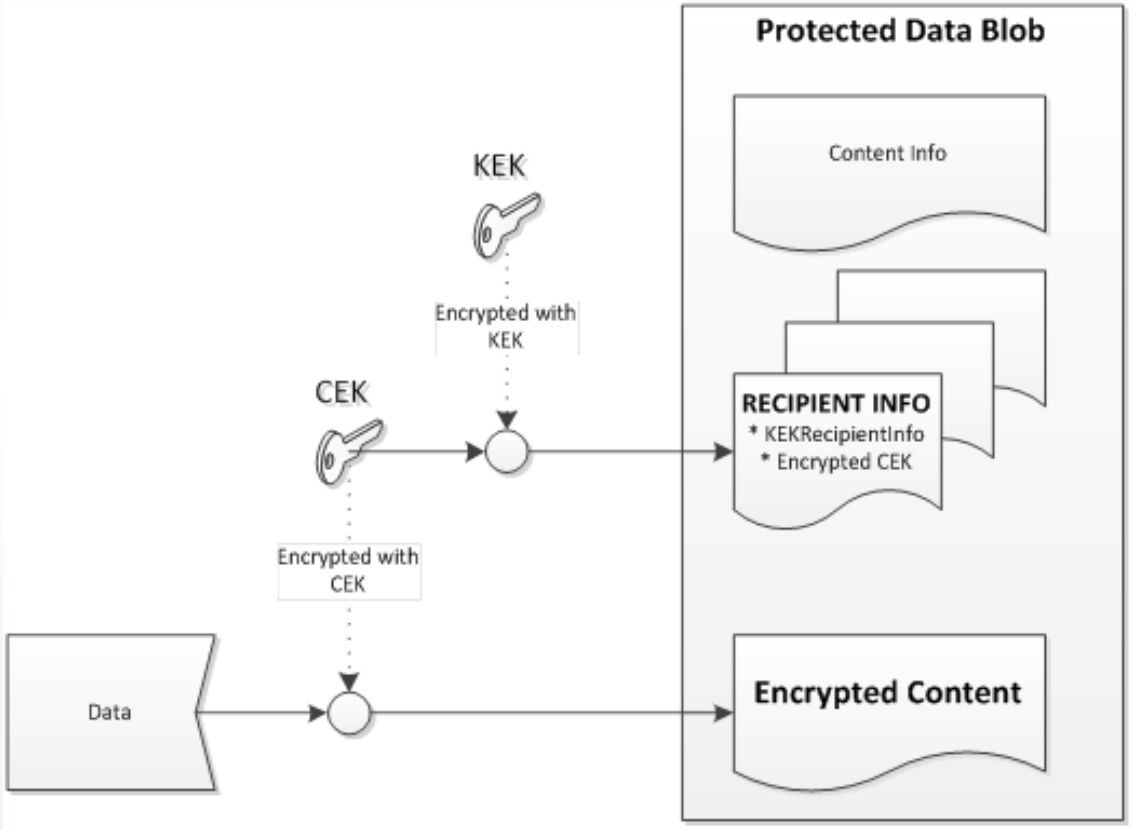
Airbus CyberSecurity BTA

```
===============
Starting diffing datatable
---------------
AB,3586: [DC001] *logonCount['116'=>'117'], *lastLogon['130052518207794051L'=>'130052535716737649L']
AB,3639: [RID Set] *rIDNextRID['1153'=>'1154']
AB,8784: [A:[gc]/B:[gc  DEL:346bf199-8567-4375-ac15-79ec4b42b270]] +isDeleted,
         *name["u'gc'"=>"u'gc\\nDEL:346bf199-8"], *dc["u'gc'"=>"u'gc\\nDEL:346bf199-8"]
AB,8785: [A:[DomainDnsZones]/B:[DomainDnsZones  DEL:58b2962b-708c-4c93-99ff-0b7e163131f9]]
         +isDeleted, *name["u'DomainDnsZones'"=>"u'DomainDnsZones\\nDE"],
         *dc["u'DomainDnsZones'"=>"u'DomainDnsZones\\nDE"]
AB,8786: [A:[ForestDnsZones]/B:[ForestDnsZones  DEL:87f7d8a2-4d05-48d0-8283-9ab084584470]]
         +isDeleted, *name["u'ForestDnsZones'"=>"u'ForestDnsZones\\nDE"],
         *dc["u'ForestDnsZones'"=>"u'ForestDnsZones\\nDE"]
 B,8789: [snorky insomnihack]
 B,8790: [gc]
 B,8791: [DomainDnsZones]
 B,8792: [ForestDnsZones]
---------------
Table [datatable]: 7636 records checked, 0 disappeared, 4 appeared, 5 changed
===============
```

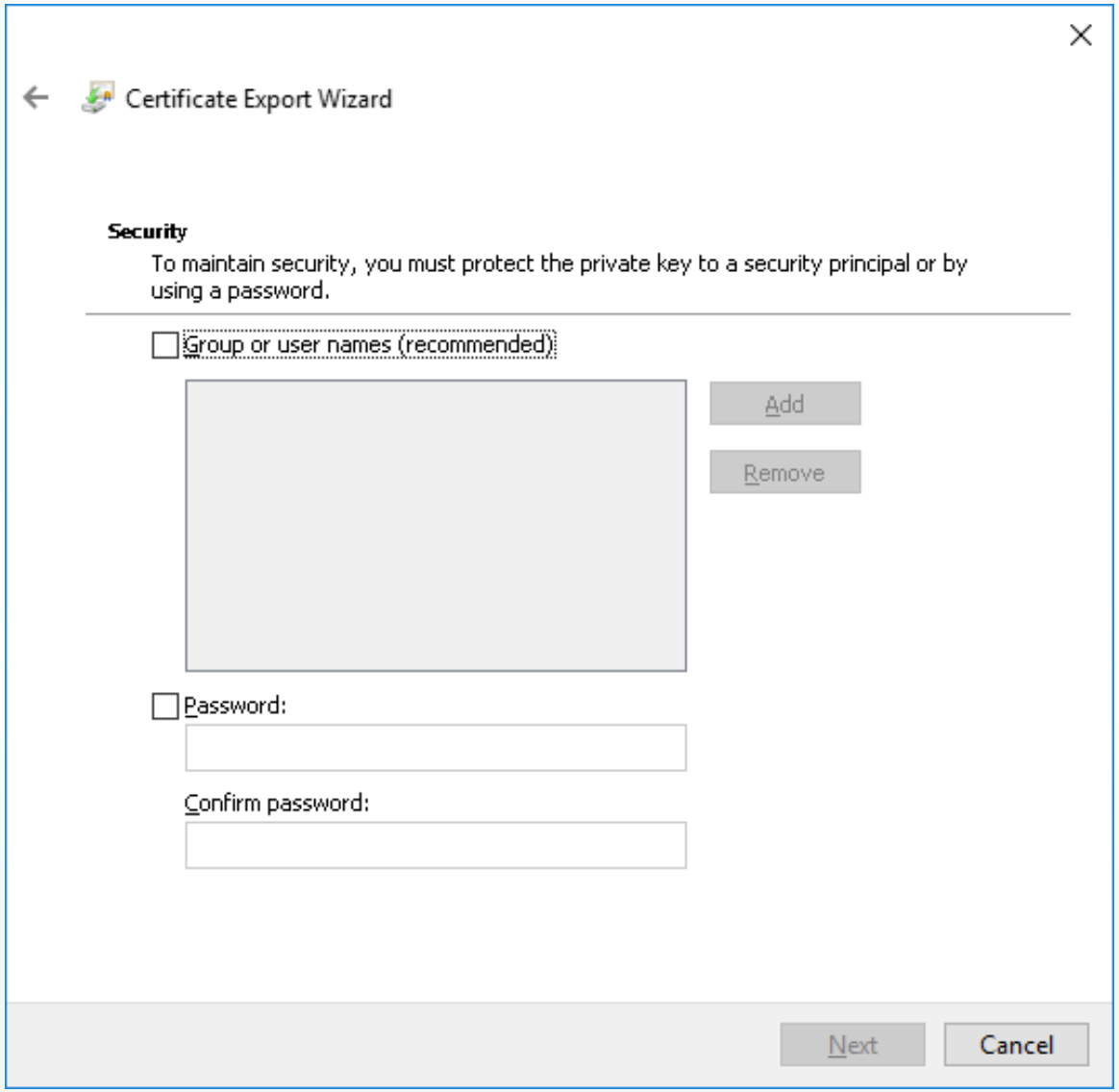
AIRBUS
DEFENCE & SPACE

DPAPI-NG (AKA CNG DPAPI)

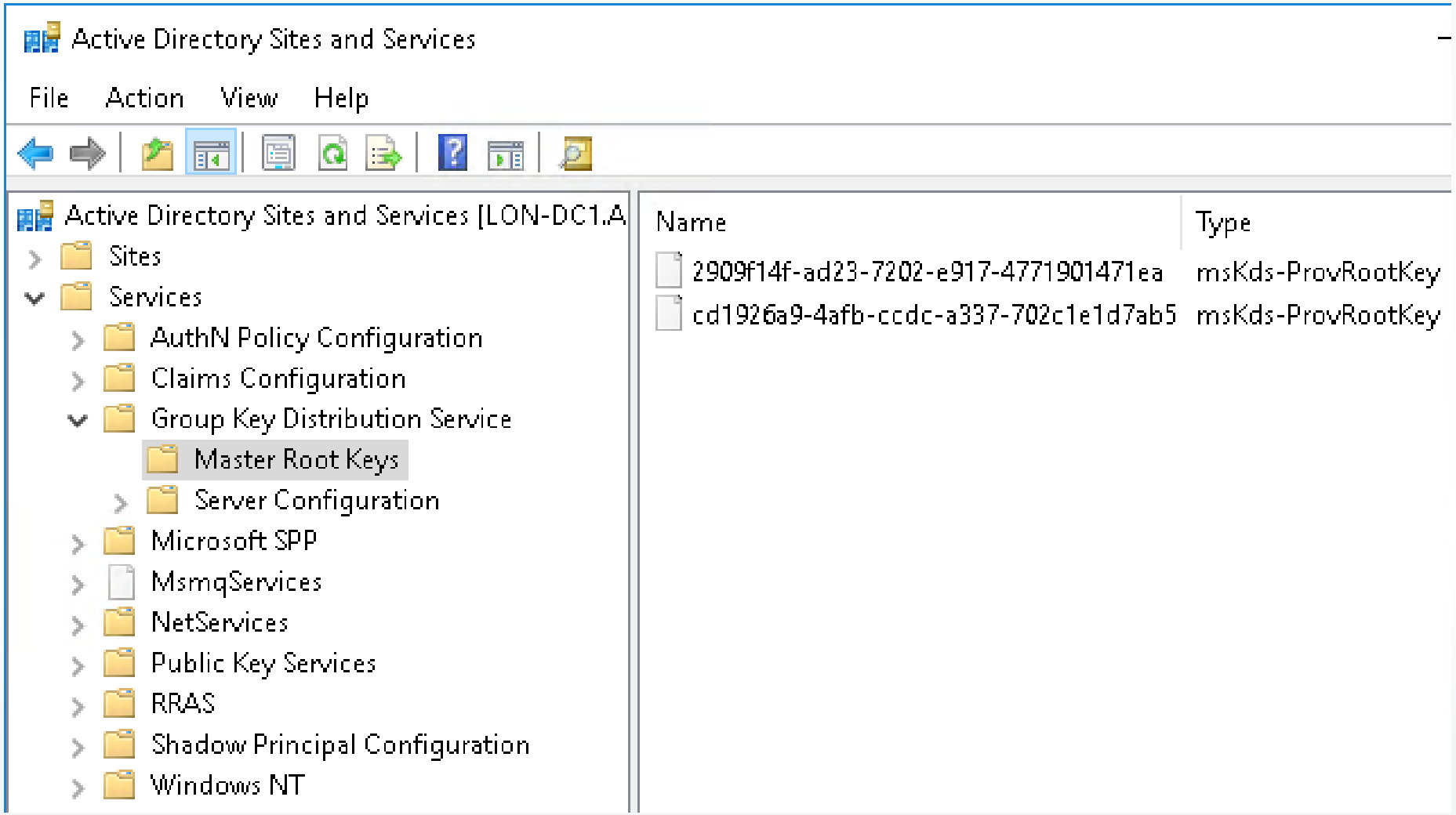
- NCryptProtectSecret(Descriptor, Data,…)
- NCryptUnprotectSecret(ProtectedBlob,…)



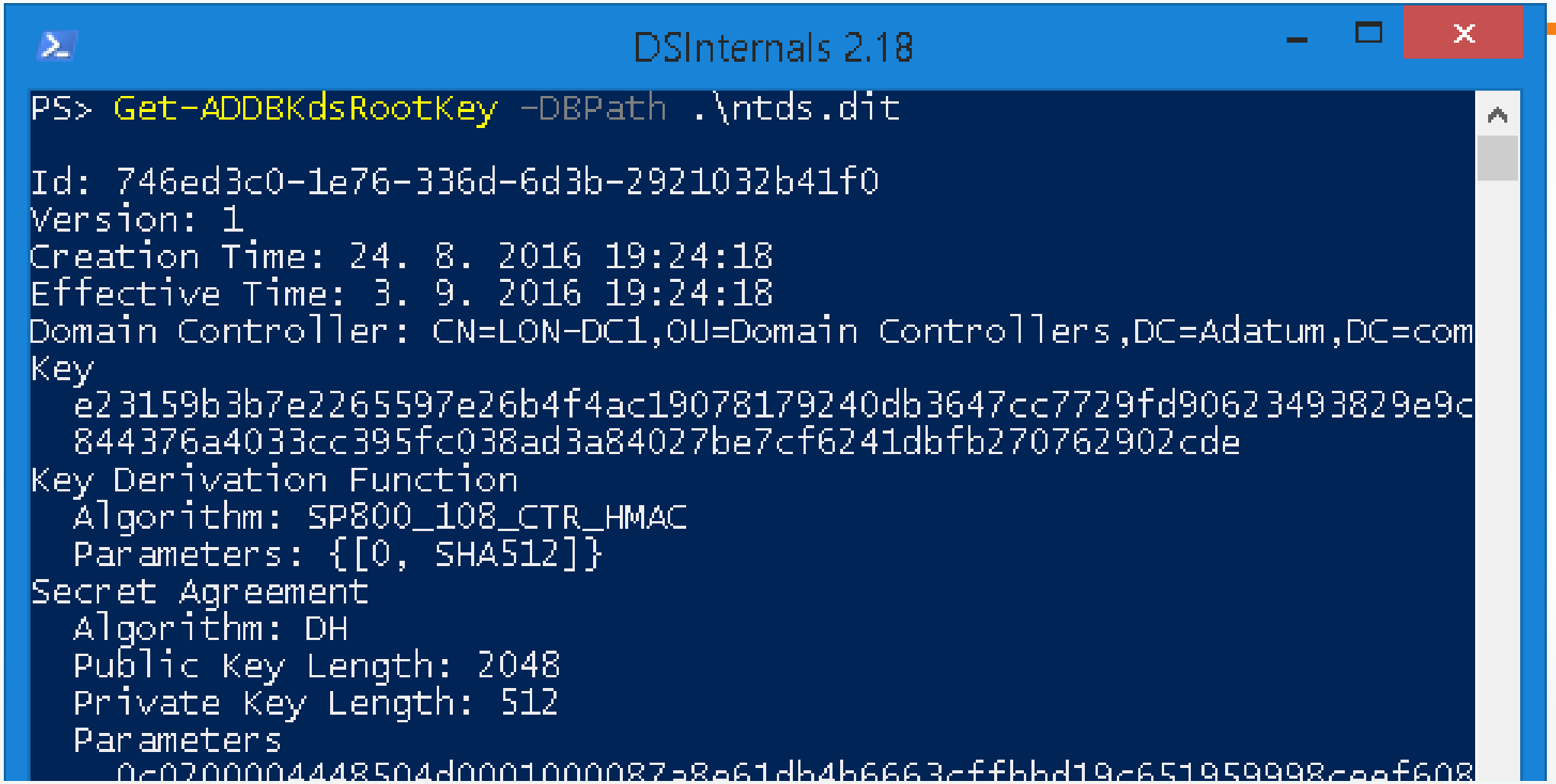
PFX/PKCS#12 File Protection



KDS Root Keys

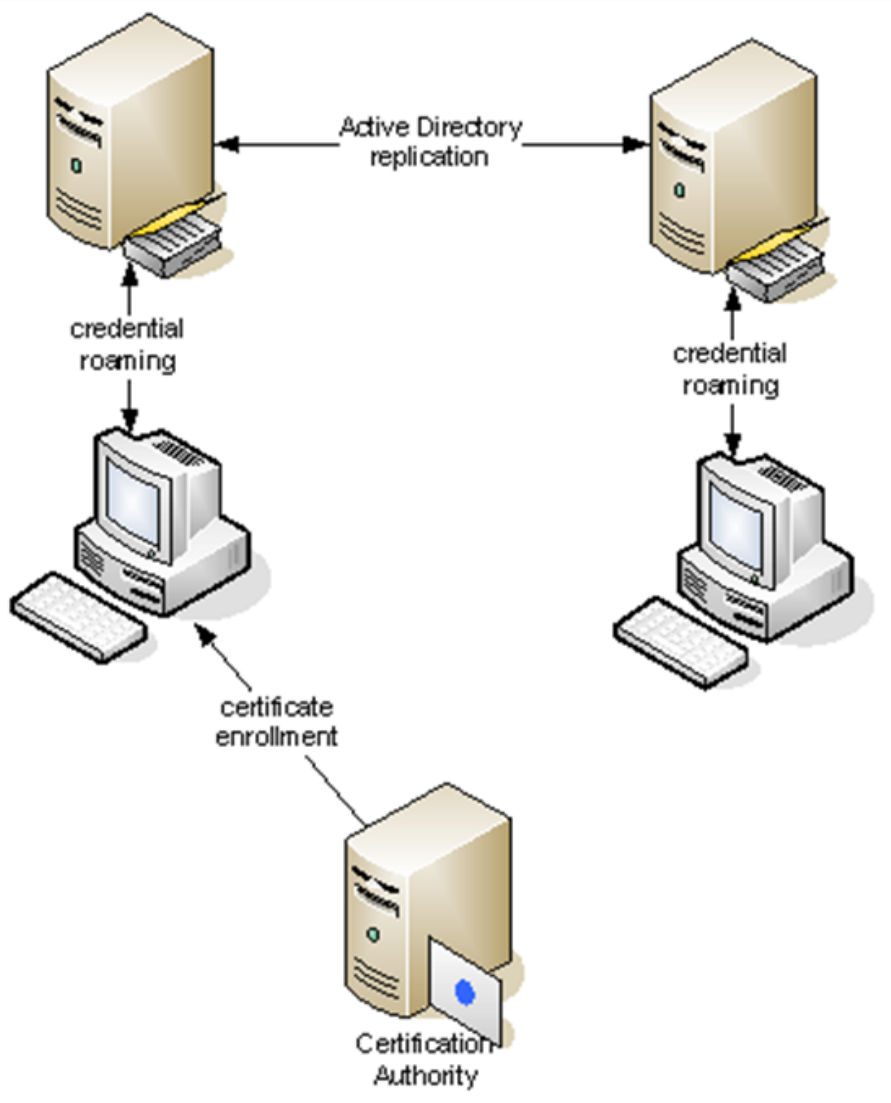


Extracting KDS Root Keys

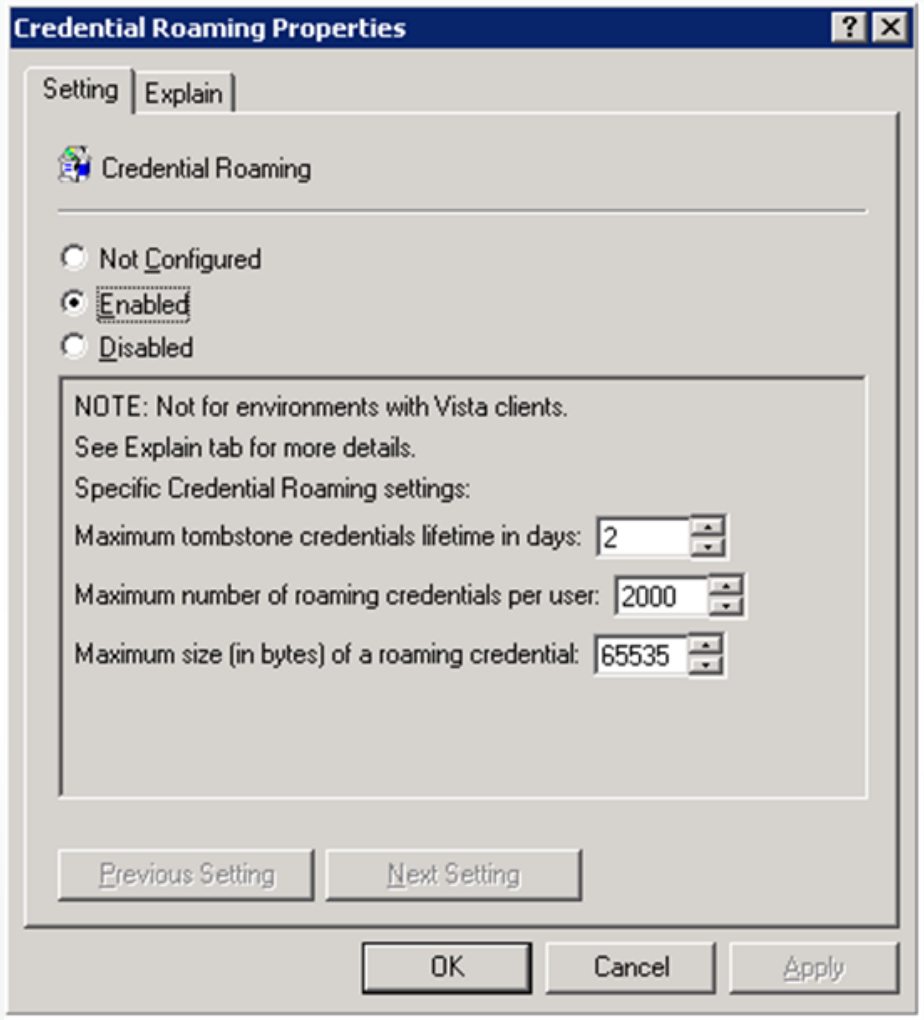


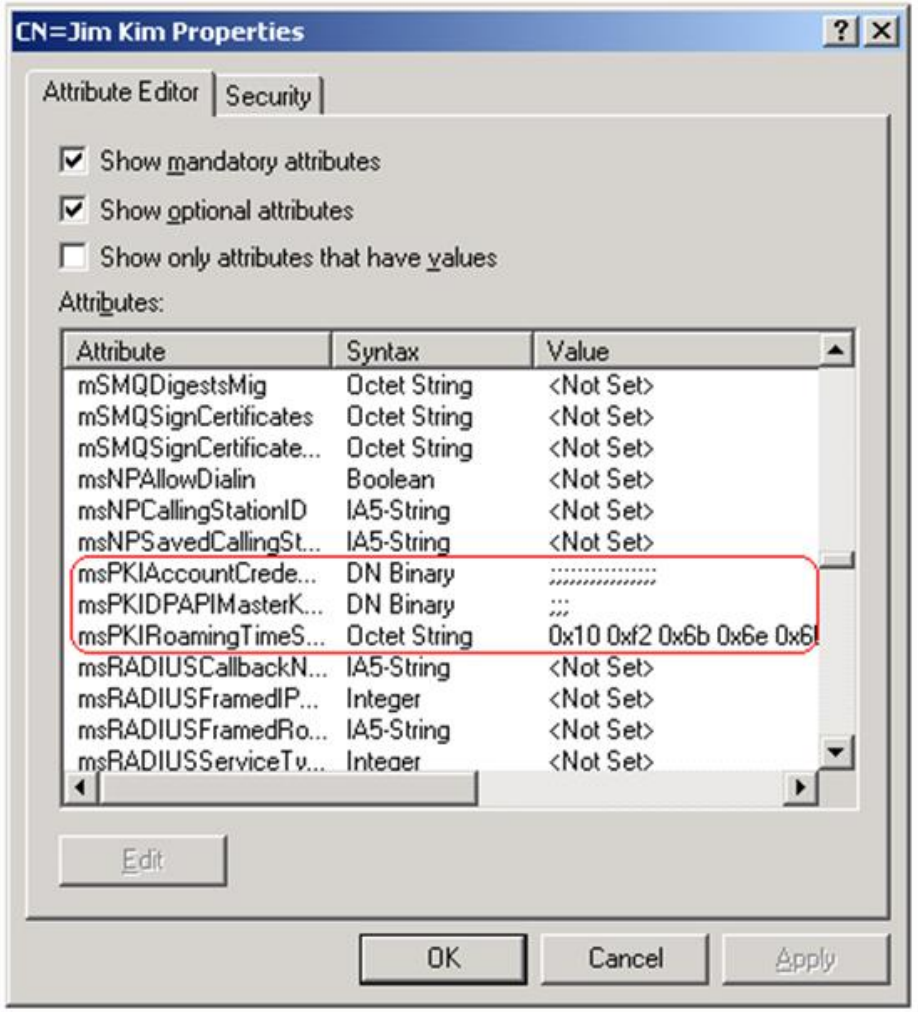
Ignite 2016 Talk

Credential Roaming

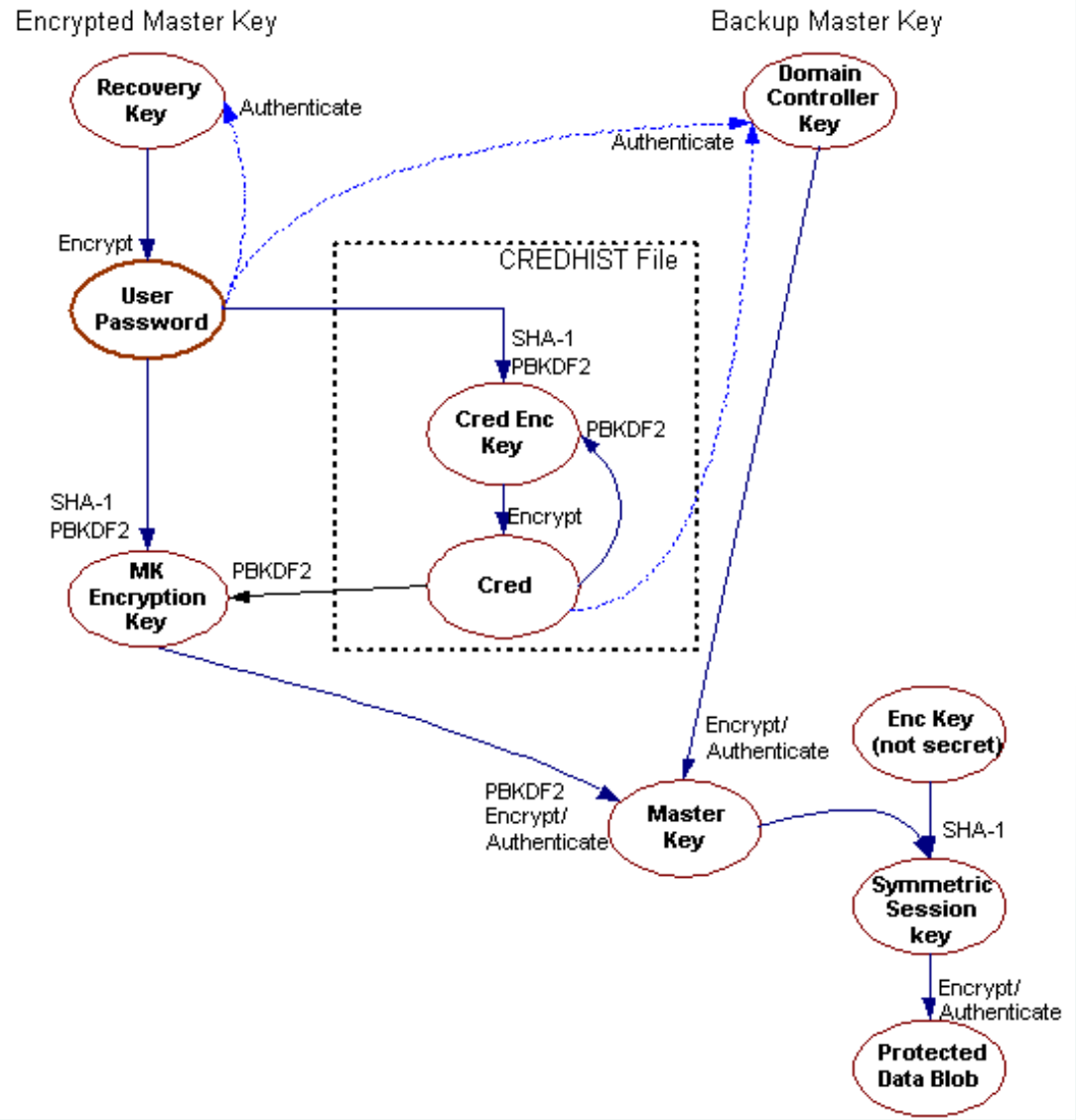


Credential Roaming - Storage

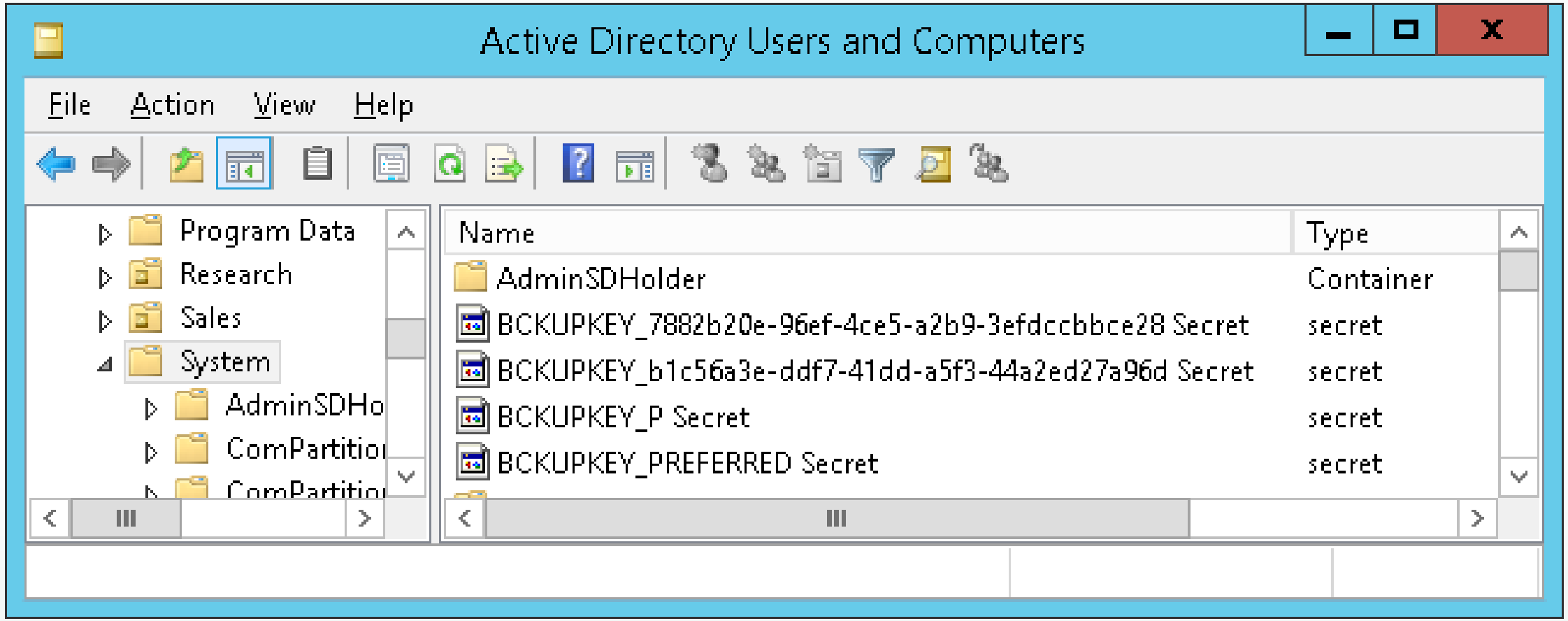




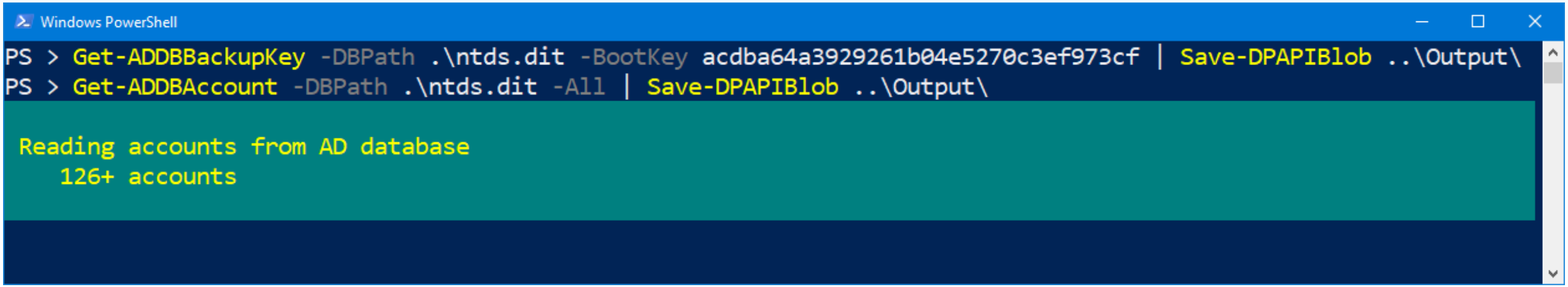
Credential Encryption using DPAPI



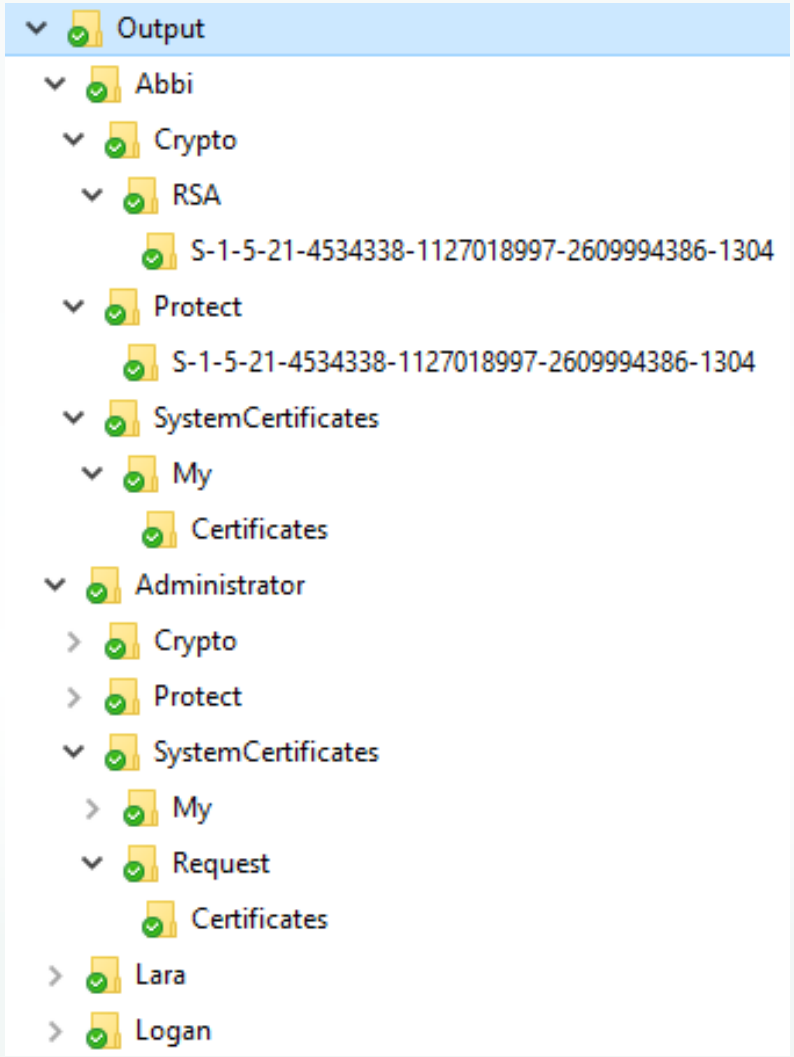
DPAPI Domain Backup Key

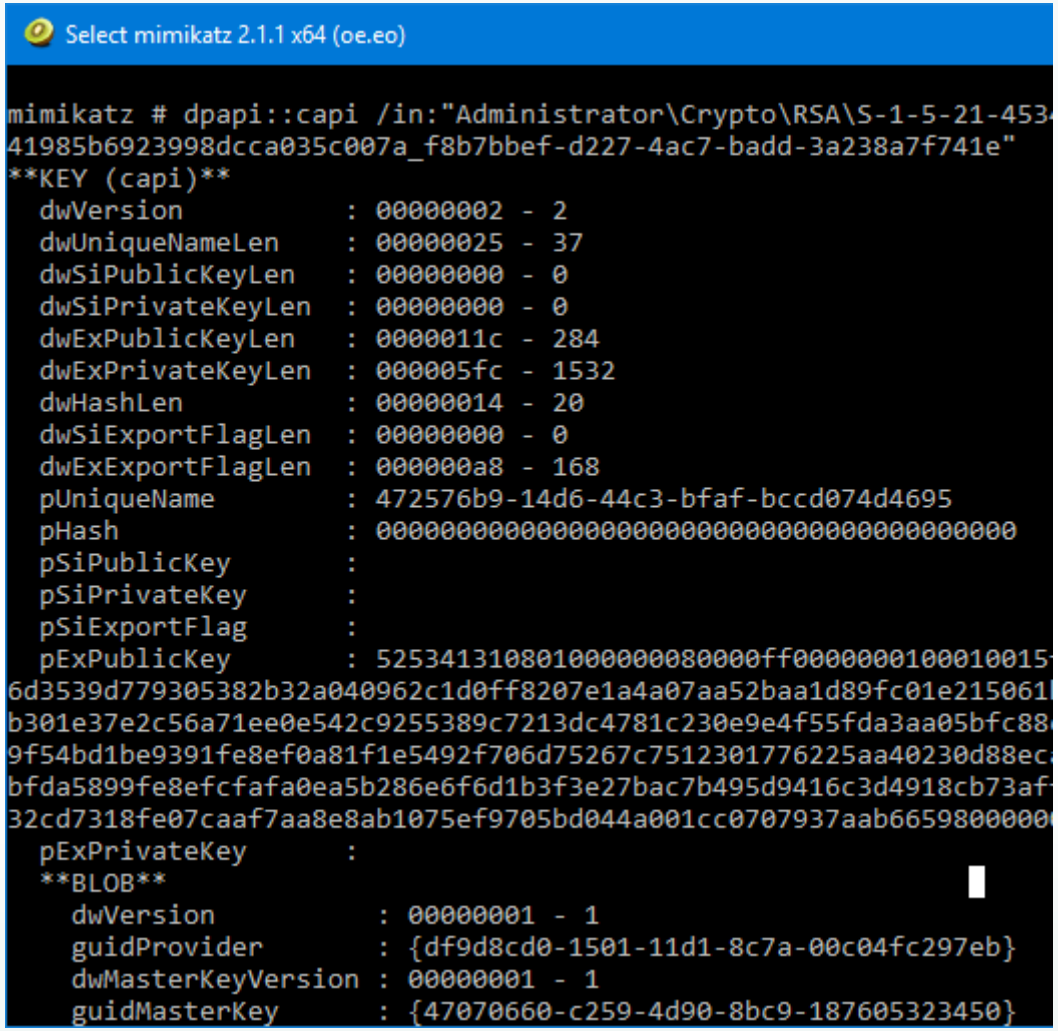


Extracting Roamed Credentials



Decrypting Roamed Private Keys

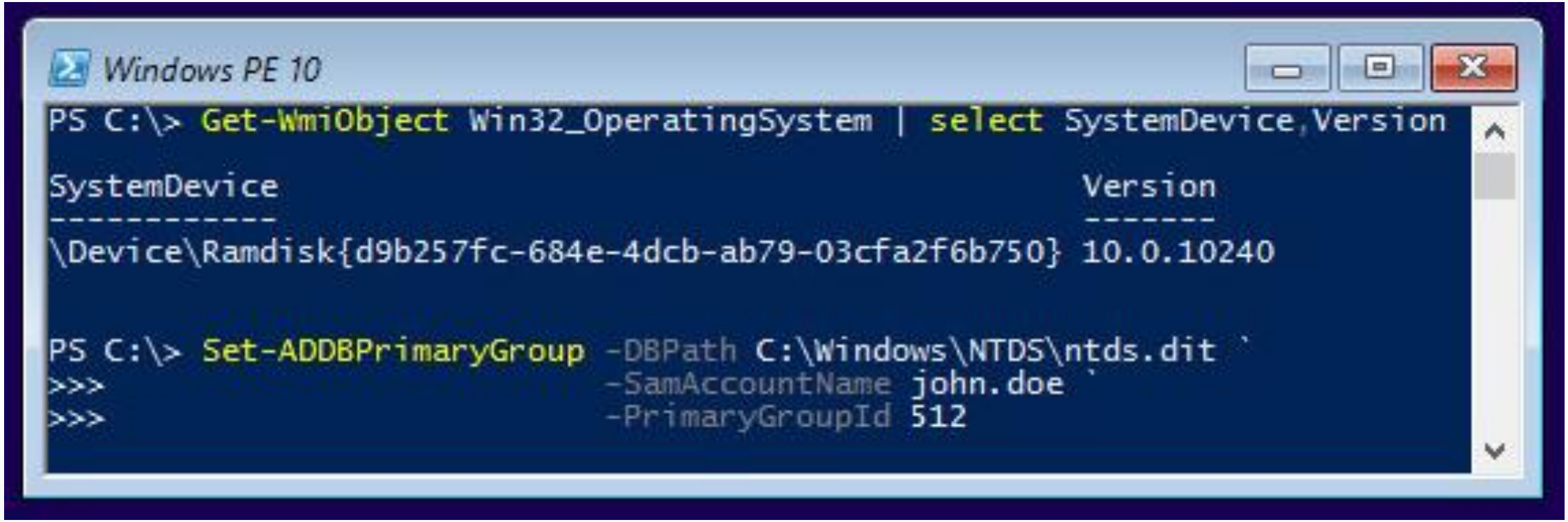




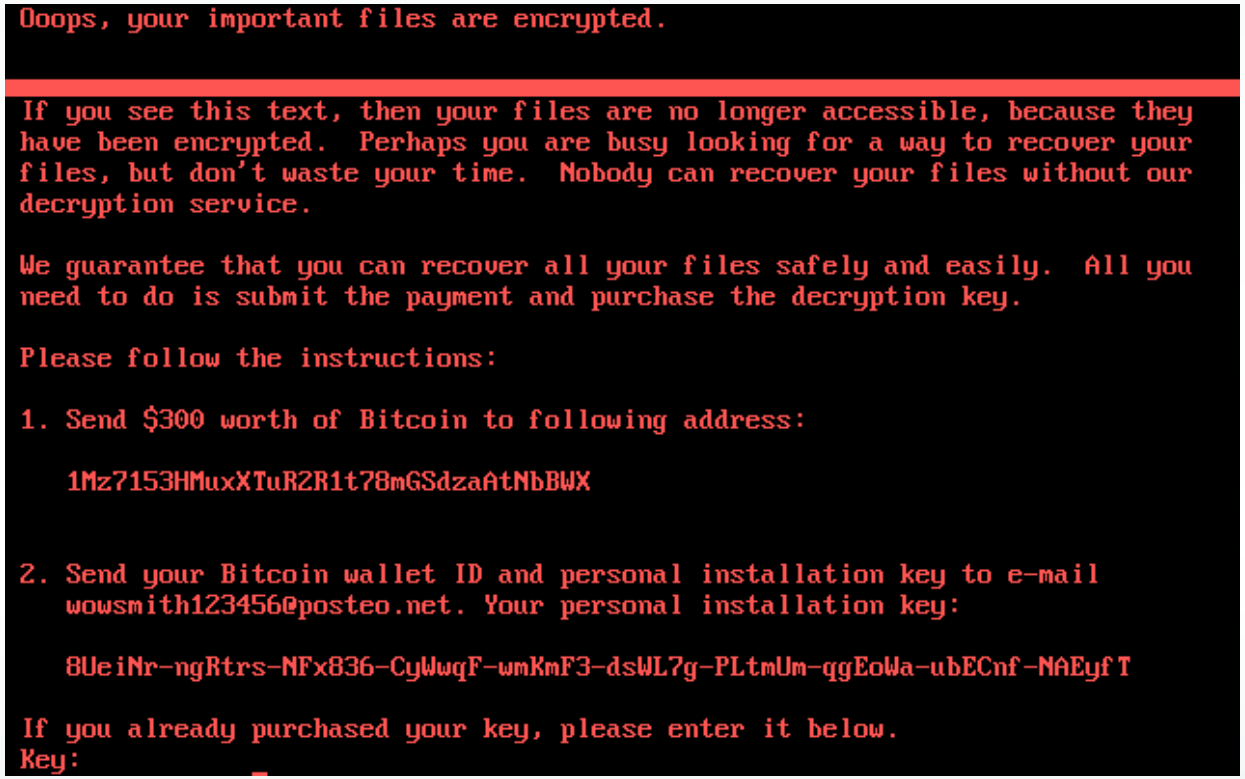
DEMO

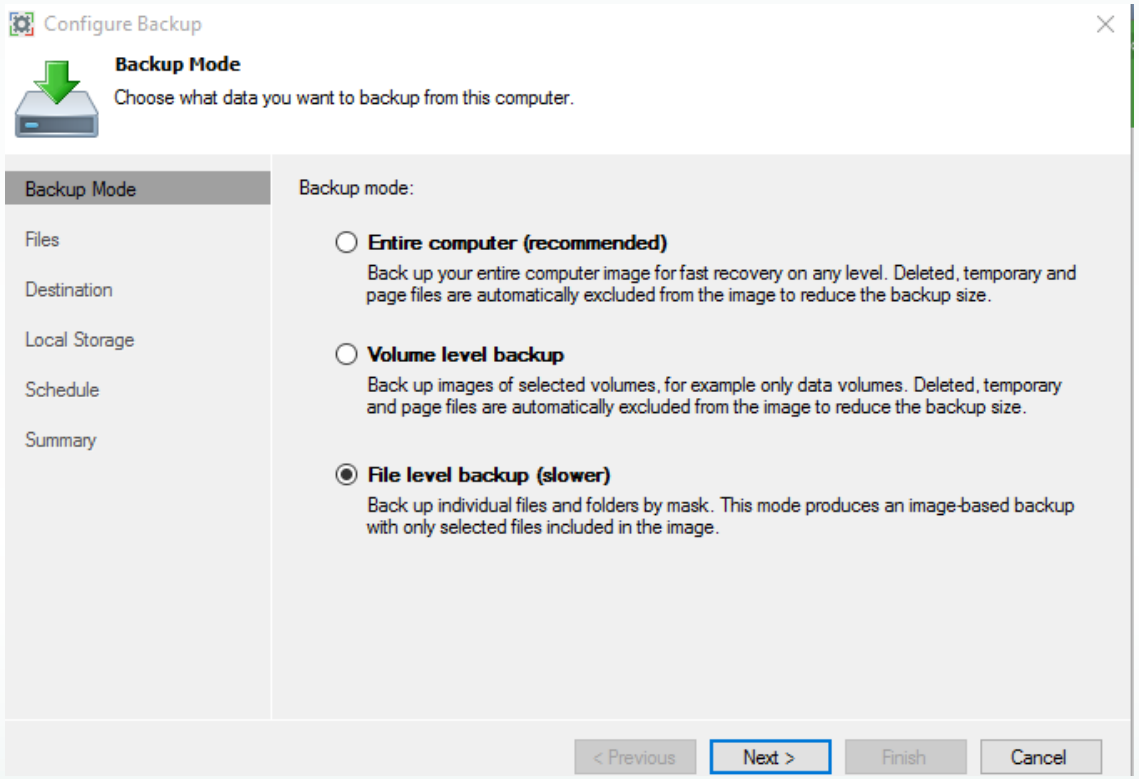
Exctracting and Decrypting Roamed Credentials

Bonus: Bootable Flash Drive

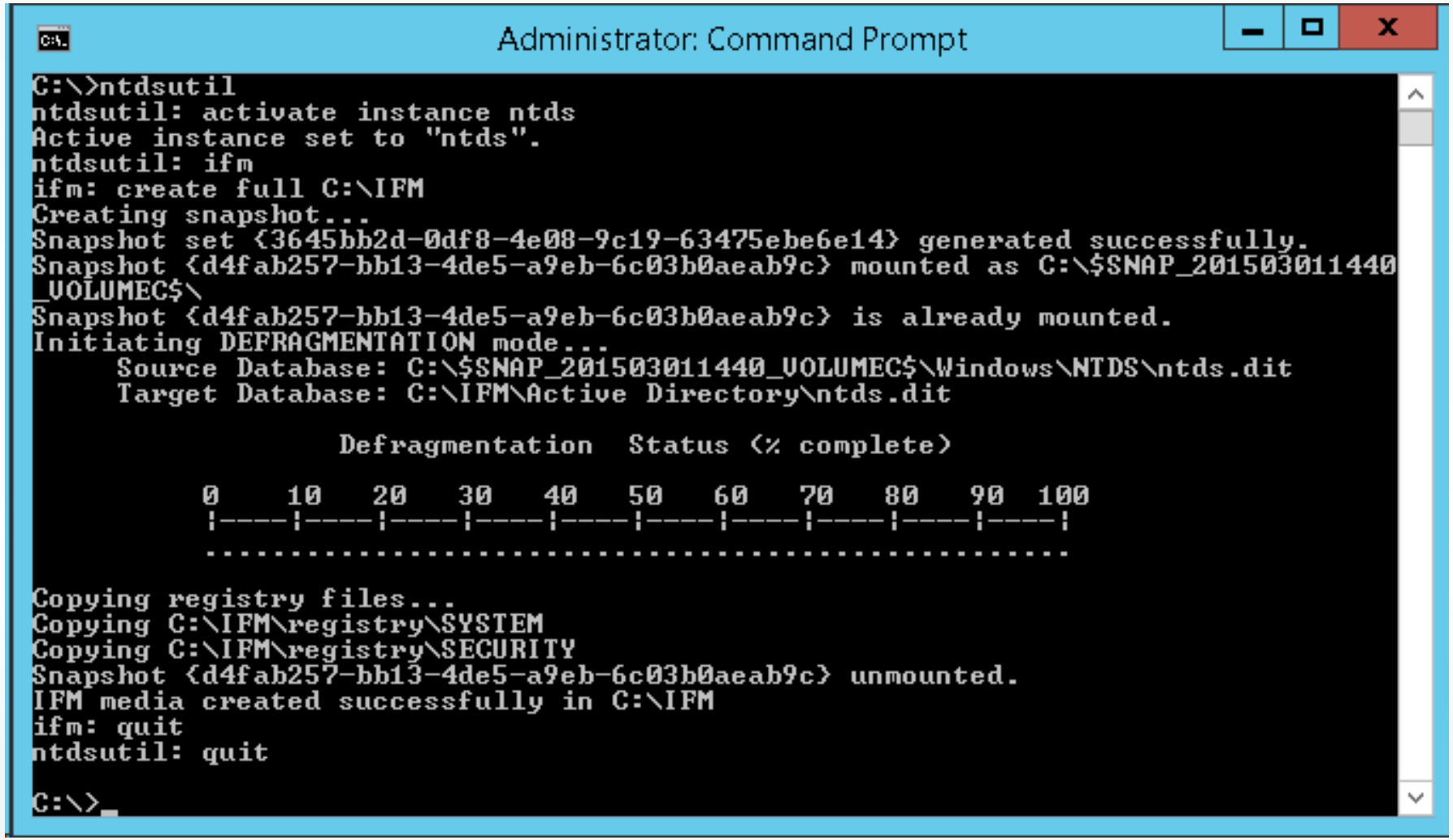


Restore From Media: Motivation





Install From Media (IFM) Backup



RFM Script

```powershell
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
```

Conclusions

- Virtualization, SAN and Backup admins are AD admins
- Enable BitLocker on DCs
- Deploy read-only domain controllers (RODCs)
- Perform AD security assessments (including password audits)
- Monitor security-related changes in AD
- Regularly change passwords (users, computers, service accounts, krbtgt)
- Plan for disaster recovery

Questions

Presenter email: michael.grafnetter@outlook.com

Presenter Twitter: 

Presenter blog: www.dsinternals.com