Active Directory Recon Without Admin Rights

adsecurity.org

Sean Metcalf January 27, 2016

```
PS C:\> get-adobject -filter {ObjectClass -eq "Contact"} -Prop *


CanonicalName                   : lab.adsecurity.org/Contaxts/Admiral Ackbar
CN                              : Admiral Ackbar
Created                         : 1/27/2016 10:00:06 AM
createTimeStamp                 : 1/27/2016 10:00:06 AM
Deleted                         :
Description                     :
DisplayName                     :
DistinguishedName               : CN=Admiral Ackbar,OU=Contaxts,DC=lab,DC=adsecurity,DC=org
dSCorePropagationData           : {12/31/1600 4:00:00 PM}
givenName                       : Admiral
instanceType                    : 4
isDeleted                       :
LastKnownParent                 :
mail                            : admackbar@RebelFleet.org
Modified                        : 1/27/2016 10:00:24 AM
modifyTimeStamp                 : 1/27/2016 10:00:24 AM
Name                            : Admiral Ackbar
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  : CN=Person,CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
ObjectClass                     : contact
ObjectGUID                      : 52c80a1d-a614-4889-92d4-1f588387d9f3
ProtectedFromAccidentalDeletion : False
sDRightsEffective               : 15
sn                              : Ackbar
uSNChanged                      : 275113
uSNCreated                      : 275112
whenChanged                     : 1/27/2016 10:00:24 AM
whenCreated                     : 1/27/2016 10:00:06 AM

CanonicalName                   : lab.adsecurity.org/Contaxts/Leia Organa
CN                              : Leia Organa
Created                         : 1/27/2016 10:01:25 AM
createTimeStamp                 : 1/27/2016 10:01:25 AM
Deleted                         :
Description                     :
DisplayName                     :
DistinguishedName               : CN=Leia Organa,OU=Contaxts,DC=lab,DC=adsecurity,DC=org
dSCorePropagationData           : {12/31/1600 4:00:00 PM}
givenName                       : Leia
instanceType                    : 4
isDeleted                       :
LastKnownParent                 :
mail                            : LeiaOrgana@TheAlliance.org
Modified                        : 1/27/2016 10:09:15 AM
modifyTimeStamp                 : 1/27/2016 10:09:15 AM
Name                            : Leia Organa
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  : CN=Person,CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
ObjectClass                     : contact
ObjectGUID                      : ba8ec318-a0a2-41d5-923e-a3f646d1c7f9
ProtectedFromAccidentalDeletion : False
sDRightsEffective               : 15
sn                              : Organa
uSNChanged                      : 275157
uSNCreated                      : 275132
whenChanged                     : 1/27/2016 10:09:15 AM
whenCreated                     : 1/27/2016 10:01:25 AM
```

A fact that is often forgotten (or misunderstood), is that most objects and their attributes can be viewed (read) by authenticated users (most often, domain users). The challenge is that admins may think that since this data is most easily accessible via admin tools such as “Active Directory User and Computers” (dsa.msc) or

“Active Directory Administrative Center” (dsac.msc), that others can’t see user data (beyond what is exposed in Outlook’s GAL). This often leads to password data being placed in user object attributes or in SYSVOL.

There is a lot of data that can be gathered from Active Directory which can be used to update documentation or to recon the environment for the next attack stages. It’s important for defenders to understand the different types of data accessible in AD with a regular user account.

Attacks frequently start with a spear-phishing email to one or more users enabling the attacker to get their code running on a computer inside the target network. Once the attacker has their code running inside the enterprise, the first step is performing reconnaissance to discover useful resources to escalate permissions, persist, and of course, plunder information (often the “crown jewels” of an organization).

This post shows how an attacker can recon the Active Directory environment with just domain user rights. Many people are surprised when they learn how much information can be gathered from AD without elevated rights.

Note: Most of the examples in this post use the Active Directory PowerShell module cmdlets. A good alternative is HarmJ0y’s PowerView (now part of PowerSploit).

I spoke about some of these techniques at several security conferences in 2015 (BSides, Shakacon, Black Hat, DEF CON, & DerbyCon). I also covered some of these issues in the post “The Most Common Active Directory Security Issues and What You Can Do to Fix Them“.

Get Active Directory Information

I have covered using .NET in PowerShell to gather AD data before, so I won’t reproduce all of the .NET commands here.

Forest Information:

```
PS C:\> [System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()

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, ADSDC11.child.lab.adsecurity.org}
ApplicationPartitions: {DC=DomainDnsZones,DC=child,DC=lab,DC=adsecurity,DC=org,
DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org,
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
```

Domain Information:

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

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
```

Forest Trusts:

```
$ForestRootDomain = 'lab.adsecurity.org'
([System.DirectoryServices.ActiveDirectory.Forest]::GetForest((New-Object
System.DirectoryServices.ActiveDirectory.DirectoryContext('Forest',
$ForestRootDomain)))).GetAllTrustRelationships()
```

Domain Trusts:

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

SourceName:    lab.adsecurity.org
TargetName: child.lab.adsecurity.org
TrustType:   ParentChild
TrustDirection: Bidirectional
```

Get Forest Global Catalogs (typically every Domain Controller is also a GC):

```
PS C:\> [System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest().GlobalCatalogs

Forest                  : lab.adsecurity.org
CurrentTime             : 1/27/2016 5:31:36 PM
HighestCommittedUsn     : 305210
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, 48594a5d-c2a3-4cd1-a80d-
bedf367cc2a9, 549871d2-e238-4423-a6b8-1bb
OutboundConnections     : {9da361fd-0eed-414a-b4ee-0a9caa1b153e, 86690811-f995-4c3e-89fe-
73c61fa4a3a0, 8797cbb4-fe09-49dc-8891-952
Name                    : ADSDC01.lab.adsecurity.org
Partitions              : {DC=lab,DC=adsecurity,DC=org,
CN=Configuration,DC=lab,DC=adsecurity,DC=org,
CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org,
DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org…

Forest                  : lab.adsecurity.org
CurrentTime             : 1/27/2016 5:31:37 PM
HighestCommittedUsn     : 274976
OSVersion               : Windows Server 2012 R2 Datacenter
Roles                   : {SchemaRole, NamingRole, PdcRole, RidRole…}
Domain                  : lab.adsecurity.org
IPAddress               : fe80::1881:40d5:fc2e:e744%12
SiteName                : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections      : {86690811-f995-4c3e-89fe-73c61fa4a3a0, dd7b36a8-a52e-446d-95a8-
318b69bd9765}
OutboundConnections     : {f901f0b5-8754-44e9-92e8-f56b3d67197b, 549871d2-e238-4423-a6b8-
1bb258e2a62f}
Name                    : ADSDC03.lab.adsecurity.org
Partitions              : {DC=lab,DC=adsecurity,DC=org,
CN=Configuration,DC=lab,DC=adsecurity,DC=org,
CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org,
DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org…

Forest                  : lab.adsecurity.org
CurrentTime             : 1/27/2016 5:31:38 PM
HighestCommittedUsn     : 161898
OSVersion               : Windows Server 2012 R2 Datacenter
Roles                   : {PdcRole, RidRole, InfrastructureRole}
Domain                  : child.lab.adsecurity.org
IPAddress               : 172.16.11.21
SiteName                : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections      : {612c2d75-1c35-4073-a8a9-d41169665000, 8797cbb4-fe09-49dc-8891-
952f38822eda}
OutboundConnections     : {71ea129f-8d56-4bd0-9b68-d80e89ae7385, 36bfdadf-777d-4bad-9427-
bc148cea256f}
Name                    : ADSDC11.child.lab.adsecurity.org
```

> Partitions : {CN=Configuration,DC=lab,DC=adsecurity,DC=org,
> CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org,
> DC=ForestDnsZones,DC=lab,DC=adsecurity,DC=org, DC=child,DC=lab,DC=adsecurity,DC=org…}

Mitigation:

There is no reasonable mitigation. This information can not and should not be obfuscated or hidden.

Discover Enterprise Services without Network Scanning

The simplest recon method is to use what I call "SPN Scanning" which asks the Domain Controller for all Service Principal Names (SPNs) of a specific type. This enables the attacker to discover all SQL servers, Exchange servers, etc. I maintain a SPN directory list which includes the most common SPNs found in an enterprise.

SPN scanning can also discover what Windows computers have RDP enabled (TERMSERV), WinRM enabled (WSMAN), etc.

Note: In order to discover all enteprise services, target both computers and users (service accounts).

```
PS C:\> get-adcomputer -filter {ServicePrincipalName -like “*TERMSRV*”} -Properties
OperatingSystem,OperatingSystemVersion,OperatingSystemServicePack,
PasswordLastSet,LastLogonDate,ServicePrincipalName,TrustedForDelegation,TrustedtoAuthForDelegation

DistinguishedName          : CN=ADSDC02,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DNSHostName                : ADSDC02.lab.adsecurity.org
Enabled                    : True
LastLogonDate              : 1/20/2016 6:46:18 AM
Name                       : ADSDC02
ObjectClass                : computer
ObjectGUID                 : 1efe44af-d8d9-420b-a66a-8d771d295085
OperatingSystem            : Windows Server 2008 R2 Datacenter
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
PasswordLastSet            : 12/31/2015 6:34:15 AM
SamAccountName             : ADSDC02$
ServicePrincipalName       : {DNS/ADSDC02.lab.adsecurity.org, HOST/ADSDC02/ADSECLAB,
HOST/ADSDC02.lab.adsecurity.org/ADSECLAB,
GC/ADSDC02.lab.adsecurity.org/lab.adsecurity.org…}
SID                        : S-1-5-21-1581655573-3923512380-696647894-1103
TrustedForDelegation       : True
TrustedToAuthForDelegation : False
UserPrincipalName          :

DistinguishedName          : CN=ADSDC01,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DNSHostName                : ADSDC01.lab.adsecurity.org
Enabled                    : True
LastLogonDate              : 1/20/2016 6:47:21 AM
Name                       : ADSDC01
ObjectClass                : computer
ObjectGUID                 : 31b2038d-e63d-4cfe-b7b6-77206c325af9
OperatingSystem            : Windows Server 2008 R2 Datacenter
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
PasswordLastSet            : 12/31/2015 6:34:14 AM
SamAccountName             : ADSDC01$
ServicePrincipalName       : {ldap/ADSDC01.lab.adsecurity.org/ForestDnsZones.lab.adsecurity.org,
ldap/ADSDC01.lab.adsecurity.org/DomainDnsZones.lab.adsecurity.org, TERMSRV/ADSDC01,
TERMSRV/ADSDC01.lab.adsecurity.org…}
SID                        : S-1-5-21-1581655573-3923512380-696647894-1000
TrustedForDelegation       : True
TrustedToAuthForDelegation : False
UserPrincipalName          :

DistinguishedName          : CN=ADSDC03,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DNSHostName                : ADSDC03.lab.adsecurity.org
Enabled                    : True
LastLogonDate              : 1/20/2016 6:35:16 AM
Name                       : ADSDC03
ObjectClass                : computer
ObjectGUID                 : 0a2d849c-cc59-4785-8ba2-997fd6ca4dc8
OperatingSystem            : Windows Server 2012 R2 Datacenter
OperatingSystemServicePack :
OperatingSystemVersion     : 6.3 (9600)
PasswordLastSet            : 12/31/2015 6:34:16 AM
```

```
SamAccountName           : ADSDC03$
ServicePrincipalName     : {DNS/ADSDC03.lab.adsecurity.org,
HOST/ADSDC03.lab.adsecurity.org/ADSECLAB,
RPC/c8e1e99e-2aaa-4888-a5d8-23a4355fac48._msdcs.lab.adsecurity.org,
GC/ADSDC03.lab.adsecurity.org/lab.adsecurity.org…}
SID                      : S-1-5-21-1581655573-3923512380-696647894-1601
TrustedForDelegation     : True
TrustedToAuthForDelegation : False
UserPrincipalName        :

DistinguishedName        : CN=ADSWRKWIN7,CN=Computers,DC=lab,DC=adsecurity,DC=org
DNSHostName              : ADSWRKWIN7.lab.adsecurity.org
Enabled                  : True
LastLogonDate            : 8/29/2015 6:40:16 PM
Name                     : ADSWRKWIN7
ObjectClass              : computer
ObjectGUID               : e8b3bed2-75b4-4512-a4f0-6d9c2d975c70
OperatingSystem          : Windows 7 Enterprise
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion   : 6.1 (7601)
PasswordLastSet          : 8/29/2015 6:40:12 PM
SamAccountName           : ADSWRKWIN7$
ServicePrincipalName     : {TERMSRV/ADSWRKWin7.lab.adsecurity.org, TERMSRV/ADSWRKWIN7,
RestrictedKrbHost/ADSWRKWIN7, HOST/ADSWRKWIN7…}
SID                      : S-1-5-21-1581655573-3923512380-696647894-1104
TrustedForDelegation     : False
TrustedToAuthForDelegation : False
UserPrincipalName        :

DistinguishedName        : CN=ADSAP01,CN=Computers,DC=lab,DC=adsecurity,DC=org
DNSHostName              : ADSAP01.lab.adsecurity.org
Enabled                  : True
LastLogonDate            : 1/24/2016 11:03:41 AM
Name                     : ADSAP01
ObjectClass              : computer
ObjectGUID               : b79bb5e3-8f9e-4ee0-a30c-5f66b61da681
OperatingSystem          : Windows Server 2008 R2 Datacenter
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion   : 6.1 (7601)
PasswordLastSet          : 1/4/2016 6:38:16 AM
SamAccountName           : ADSAP01$
ServicePrincipalName     : {WSMAN/ADSAP01.lab.adsecurity.org, WSMAN/ADSAP01,
TERMSRV/ADSAP01.lab.adsecurity.org, TERMSRV/ADSAP01…}
SID                      : S-1-5-21-1581655573-3923512380-696647894-1105
TrustedForDelegation     : False
TrustedToAuthForDelegation : False
UserPrincipalName        :

DistinguishedName        : CN=ADSWKWIN7,CN=Computers,DC=lab,DC=adsecurity,DC=org
DNSHostName              : ADSWKWIN7.lab.adsecurity.org
Enabled                  : True
LastLogonDate            : 1/20/2016 7:07:11 AM
Name                     : ADSWKWIN7
ObjectClass              : computer
ObjectGUID               : 2f164d63-d721-4b0e-a553-3ca0e272aa96
```

```
OperatingSystem           : Windows 7 Enterprise
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion    : 6.1 (7601)
PasswordLastSet           : 12/31/2015 8:03:05 AM
SamAccountName            : ADSWKWIN7$
ServicePrincipalName      : {TERMSRV/ADSWKWin7.lab.adsecurity.org, TERMSRV/ADSWKWIN7,
RestrictedKrbHost/ADSWKWIN7, HOST/ADSWKWIN7…}
SID                       : S-1-5-21-1581655573-3923512380-696647894-1602
TrustedForDelegation      : False
TrustedToAuthForDelegation : False
UserPrincipalName         :

DistinguishedName         : CN=ADSAP02,CN=Computers,DC=lab,DC=adsecurity,DC=org
DNSHostName               : ADSAP02.lab.adsecurity.org
Enabled                   : True
LastLogonDate             : 1/24/2016 7:39:48 AM
Name                      : ADSAP02
ObjectClass               : computer
ObjectGUID                : 1006978e-8627-4d01-98b6-3215c4ee4541
OperatingSystem           : Windows Server 2012 R2 Datacenter
OperatingSystemServicePack :
OperatingSystemVersion    : 6.3 (9600)
PasswordLastSet           : 1/4/2016 6:39:25 AM
SamAccountName            : ADSAP02$
ServicePrincipalName      : {WSMAN/ADSAP02.lab.adsecurity.org, WSMAN/ADSAP02,
TERMSRV/ADSAP02.lab.adsecurity.org, TERMSRV/ADSAP02…}
SID                       : S-1-5-21-1581655573-3923512380-696647894-1603
TrustedForDelegation      : False
TrustedToAuthForDelegation : False
UserPrincipalName         :
```

Mitigation:

There is no mitigation. Service Principal Names are required for Kerberos to work.

Discover Enterprise Services without Network Scanning Part 2

SPN Scanning will discover all enterprise services supporting Kerberos. Other enterprise services that integrate with Active Directory often create a new container in the Domain “System” container (CN=System,DC=<*domain*>). Some enterprise applications that store data in the domain System container include:

SCCM: “System Management”

There are some applications like Exchange that create containers in the forest configuration partition “Services” container (CN=Services,CN=Configuration,DC=<*domain*>).

Mitigation:

There is no reasonable mitigation.

Discover Service Accounts

The quickest way to find Service Accounts and the servers the accounts are used on is to SPN Scan for user accounts with Service Principal Names.

My Find-PSServiceAccounts PowerShell script in my GitHub repository performs the sme query without requiring the AD PowerShell module.

```
PS C:\> get-aduser -filter {ServicePrincipalName -like “*”} -Properties
PasswordLastSet,LastLogonDate,ServicePrincipalName,TrustedForDelegation,Truste
dtoAuthForDelegation

DistinguishedName         : CN=svc-adsMSSQL11,OU=Test,DC=lab,DC=adsecurity,DC=org
Enabled                   : False
GivenName                 :
LastLogonDate             :
Name                      : svc-adsMSSQL11
ObjectClass               : user
ObjectGUID                : 275d3bf4-80d3-42ba-9d77-405c5cc63c07
PasswordLastSet           : 1/4/2016 7:13:03 AM
SamAccountName            : svc-adsMSSQL11
ServicePrincipalName      : {MSSQL/adsMSSQL11.lab.adsecurity.org:7434}
SID                       : S-1-5-21-1581655573-3923512380-696647894-3601
Surname                   :
TrustedForDelegation      : False
TrustedToAuthForDelegation : False
UserPrincipalName         :

DistinguishedName         : CN=svc-adsSQLSA,OU=Test,DC=lab,DC=adsecurity,DC=org
Enabled                   : False
GivenName                 :
LastLogonDate             :
Name                      : svc-adsSQLSA
ObjectClass               : user
ObjectGUID                : 56faaab2-5b05-4bb2-aaea-0bdc1409eab3
PasswordLastSet           : 1/4/2016 7:13:13 AM
SamAccountName            : svc-adsSQLSA
ServicePrincipalName      : {MSSQL/adsMSSQL23.lab.adsecurity.org:7434,
MSSQL/adsMSSQL22.lab.adsecurity.org:5534,
MSSQL/adsMSSQL21.lab.adsecurity.org:9834, MSSQL/adsMSSQL10.lab.adsecurity.org:14434…}
SID                       : S-1-5-21-1581655573-3923512380-696647894-3602
Surname                   :
TrustedForDelegation      : False
TrustedToAuthForDelegation : False
UserPrincipalName         :

DistinguishedName         : CN=svc-adsMSSQL10,OU=Test,DC=lab,DC=adsecurity,DC=org
Enabled                   : False
GivenName                 :
LastLogonDate             :
Name                      : svc-adsMSSQL10
ObjectClass               : user
ObjectGUID                : 6c2f15a2-ba4a-485a-a367-39395ad82c86
PasswordLastSet           : 1/4/2016 7:13:24 AM
SamAccountName            : svc-adsMSSQL10
ServicePrincipalName      : {MSSQL/adsMSSQL10.lab.adsecurity.org:7434}
SID                       : S-1-5-21-1581655573-3923512380-696647894-3603
Surname                   :
TrustedForDelegation      : False
TrustedToAuthForDelegation : False
UserPrincipalName         :
```

Mitigation:

There is no reasonable mitigation.

Discover Computers without Network Scanning

Every computer that joins Active Directory has an associated computer account in AD. When the computer is joined, there are several attributes associated with this computer object that are updated, several of which are quite useful. These include:

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

```
PS C:\> get-adcomputer -filter {PrimaryGroupID -eq “515”} -Properties
OperatingSystem,OperatingSystemVersion,OperatingSystemServicePack,Passwo
t,LastLogonDate,ServicePrincipalName,TrustedForDelegation,TrustedtoAuthForDelegation

DistinguishedName          : CN=ADSWRKWIN7,CN=Computers,DC=lab,DC=adsecurity,DC=org
DNSHostName                : ADSWRKWIN7.lab.adsecurity.org
Enabled                    : True
LastLogonDate              : 8/29/2015 6:40:16 PM
Name                       : ADSWRKWIN7
ObjectClass                : computer
ObjectGUID                 : e8b3bed2-75b4-4512-a4f0-6d9c2d975c70
OperatingSystem            : Windows 7 Enterprise
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
PasswordLastSet            : 8/29/2015 6:40:12 PM
SamAccountName             : ADSWRKWIN7$
ServicePrincipalName       : {TERMSRV/ADSWRKWin7.lab.adsecurity.org, TERMSRV/ADSWRKWIN7,
RestrictedKrbHost/ADSWRKWIN7, HOST/ADSWRKWIN7…}
SID                        : S-1-5-21-1581655573-3923512380-696647894-1104
TrustedForDelegation       : False
TrustedToAuthForDelegation : False
UserPrincipalName          :

DistinguishedName          : CN=ADSAP01,CN=Computers,DC=lab,DC=adsecurity,DC=org
DNSHostName                : ADSAP01.lab.adsecurity.org
Enabled                    : True
LastLogonDate              : 1/24/2016 11:03:41 AM
Name                       : ADSAP01
ObjectClass                : computer
ObjectGUID                 : b79bb5e3-8f9e-4ee0-a30c-5f66b61da681
OperatingSystem            : Windows Server 2008 R2 Datacenter
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
PasswordLastSet            : 1/4/2016 6:38:16 AM
SamAccountName             : ADSAP01$
ServicePrincipalName       : {WSMAN/ADSAP01.lab.adsecurity.org, WSMAN/ADSAP01,
TERMSRV/ADSAP01.lab.adsecurity.org, TERMSRV/ADSAP01…}
SID                        : S-1-5-21-1581655573-3923512380-696647894-1105
TrustedForDelegation       : False
TrustedToAuthForDelegation : False
UserPrincipalName          :

DistinguishedName          : CN=ADSWKWIN7,CN=Computers,DC=lab,DC=adsecurity,DC=org
DNSHostName                : ADSWKWIN7.lab.adsecurity.org
Enabled                    : True
LastLogonDate              : 1/20/2016 7:07:11 AM
Name                       : ADSWKWIN7
ObjectClass                : computer
ObjectGUID                 : 2f164d63-d721-4b0e-a553-3ca0e272aa96
OperatingSystem            : Windows 7 Enterprise
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
PasswordLastSet            : 12/31/2015 8:03:05 AM
SamAccountName             : ADSWKWIN7$
ServicePrincipalName       : {TERMSRV/ADSWKWin7.lab.adsecurity.org, TERMSRV/ADSWKWIN7,
```

```
RestrictedKrbHost/ADSWKWIN7, HOST/ADSWKWIN7…}
SID                   : S-1-5-21-1581655573-3923512380-696647894-1602
TrustedForDelegation      : False
TrustedToAuthForDelegation : False
UserPrincipalName         :

DistinguishedName         : CN=ADSAP02,CN=Computers,DC=lab,DC=adsecurity,DC=org
DNSHostName               : ADSAP02.lab.adsecurity.org
Enabled                   : True
LastLogonDate             : 1/24/2016 7:39:48 AM
Name                      : ADSAP02
ObjectClass               : computer
ObjectGUID                : 1006978e-8627-4d01-98b6-3215c4ee4541
OperatingSystem           : Windows Server 2012 R2 Datacenter
OperatingSystemServicePack :
OperatingSystemVersion    : 6.3 (9600)
PasswordLastSet           : 1/4/2016 6:39:25 AM
SamAccountName            : ADSAP02$
ServicePrincipalName      : {WSMAN/ADSAP02.lab.adsecurity.org, WSMAN/ADSAP02,
TERMSRV/ADSAP02.lab.adsecurity.org, TERMSRV/ADSAP02…}
SID                   : S-1-5-21-1581655573-3923512380-696647894-1603
TrustedForDelegation      : False
TrustedToAuthForDelegation : False
UserPrincipalName         :
```

The same data for Domain Controllers can be gathered by changing the PrimaryGroupID value to “516”, or get all computers by changing to “-filter *”.

```
PS C:\> get-adcomputer -filter {PrimaryGroupID -eq “516”} -Properties
OperatingSystem,OperatingSystemVersion,OperatingSystemServicePack,PasswordLastSe
t,LastLogonDate,ServicePrincipalName,TrustedForDelegation,TrustedtoAuthForDelegation

DistinguishedName          : CN=ADSDC02,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DNSHostName                : ADSDC02.lab.adsecurity.org
Enabled                    : True
LastLogonDate              : 1/20/2016 6:46:18 AM
Name                       : ADSDC02
ObjectClass                : computer
ObjectGUID                 : 1efe44af-d8d9-420b-a66a-8d771d295085
OperatingSystem            : Windows Server 2008 R2 Datacenter
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
PasswordLastSet            : 12/31/2015 6:34:15 AM
SamAccountName             : ADSDC02$
ServicePrincipalName       : {DNS/ADSDC02.lab.adsecurity.org, HOST/ADSDC02/ADSECLAB,
HOST/ADSDC02.lab.adsecurity.org/ADSECLAB,
GC/ADSDC02.lab.adsecurity.org/lab.adsecurity.org…}
SID                        : S-1-5-21-1581655573-3923512380-696647894-1103
TrustedForDelegation       : True
TrustedToAuthForDelegation : False
UserPrincipalName          :

DistinguishedName          : CN=ADSDC01,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DNSHostName                : ADSDC01.lab.adsecurity.org
Enabled                    : True
LastLogonDate              : 1/20/2016 6:47:21 AM
Name                       : ADSDC01
ObjectClass                : computer
ObjectGUID                 : 31b2038d-e63d-4cfe-b7b6-77206c325af9
OperatingSystem            : Windows Server 2008 R2 Datacenter
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion     : 6.1 (7601)
PasswordLastSet            : 12/31/2015 6:34:14 AM
SamAccountName             : ADSDC01$
ServicePrincipalName       : {ldap/ADSDC01.lab.adsecurity.org/ForestDnsZones.lab.adsecurity.org,
ldap/ADSDC01.lab.adsecurity.org/DomainDnsZones.lab.adsecurity.org, TERMSRV/ADSDC01,
TERMSRV/ADSDC01.lab.adsecurity.org…}
SID                        : S-1-5-21-1581655573-3923512380-696647894-1000
TrustedForDelegation       : True
TrustedToAuthForDelegation : False
UserPrincipalName          :

DistinguishedName          : CN=ADSDC03,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DNSHostName                : ADSDC03.lab.adsecurity.org
Enabled                    : True
LastLogonDate              : 1/20/2016 6:35:16 AM
Name                       : ADSDC03
ObjectClass                : computer
ObjectGUID                 : 0a2d849c-cc59-4785-8ba2-997fd6ca4dc8
OperatingSystem            : Windows Server 2012 R2 Datacenter
OperatingSystemServicePack :
OperatingSystemVersion     : 6.3 (9600)
PasswordLastSet            : 12/31/2015 6:34:16 AM
```

```
SamAccountName            : ADSDC03$
ServicePrincipalName      : {DNS/ADSDC03.lab.adsecurity.org,
HOST/ADSDC03.lab.adsecurity.org/ADSECLAB,
RPC/c8e1e99e-2aaa-4888-a5d8-23a4355fac48._msdcs.lab.adsecurity.org,
GC/ADSDC03.lab.adsecurity.org/lab.adsecurity.org…}
SID                       : S-1-5-21-1581655573-3923512380-696647894-1601
TrustedForDelegation      : True
TrustedToAuthForDelegation : False
UserPrincipalName         :
```

This provides useful information on Windows OS versions as well as non-Windows devices joined to Active Directory.

Some example queries for finding non-Windows devices:

- OperatingSystem -Like “*Samba*”
- OperatingSystem -Like “*OnTap*”
- OperatingSystem -Like “*Data Domain*”
- OperatingSystem -Like “*EMC*”
- OperatingSystem -Like “*Windows NT*”

Mitigation:

There is no mitigation.

Identify Admin Accounts

There are two effective methods for discovering accounts with elevated rights in Active Directory. The first is the standard group enumeration method which identifies all members of the standard Active Directory admin groups: Domain Admins, Administrators, Enterprise Admins, etc. Typically getting recursive group membership for the domain “Adminsitrators” group will provide a list of all AD admins.

The second method, which I highlighted at DerbyCon in 2015, involves identifying all accounts which have the attribute “AdminCount” set to 1. The caveat to this is that there may be accounts returned in this query which no longer have admin rights since this value isn’t automatically reset once the account is removed from the admin groups. More info on SDProp and the AdminCount attribute: “Sneaky Active Directory Persistence #15: Leverage AdminSDHolder & SDProp to (Re)Gain Domain Admin Rights“.

```
PS C:\> get-aduser -filter {AdminCount -eq 1} -Properties
Name,AdminCount,ServicePrincipalName,PasswordLastSet,LastLogonDate,MemberOf

AdminCount        : 1
DistinguishedName : CN=ADSAdministrator,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled           : True
GivenName         :
LastLogonDate     : 1/27/2016 8:55:48 AM
MemberOf          : {CN=Administrators,CN=Builtin,DC=lab,DC=adsecurity,DC=org, CN=Schema
Admins,CN=Users,DC=lab,DC=adsecurity,DC=org, CN=Group
Policy Creator Owners,CN=Users,DC=lab,DC=adsecurity,DC=org, CN=Enterprise
Admins,CN=Users,DC=lab,DC=adsecurity,DC=org…}
Name              : ADSAdministrator
ObjectClass       : user
ObjectGUID        : 72ac7731-0a76-4e5a-8e5d-b4ded9a304b5
PasswordLastSet   : 12/31/2015 8:45:27 AM
SamAccountName    : ADSAdministrator
SID               : S-1-5-21-1581655573-3923512380-696647894-500
Surname           :
UserPrincipalName :

AdminCount          : 1
DistinguishedName   : CN=krbtgt,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled             : False
GivenName           :
LastLogonDate       :
MemberOf            : {CN=Denied RODC Password Replication
Group,CN=Users,DC=lab,DC=adsecurity,DC=org}
Name                : krbtgt
ObjectClass         : user
ObjectGUID          : 3d5be8dd-df7f-4f84-b2cf-4556310a7292
PasswordLastSet     : 8/27/2015 7:10:22 PM
SamAccountName      : krbtgt
ServicePrincipalName : {kadmin/changepw}
SID                 : S-1-5-21-1581655573-3923512380-696647894-502
Surname             :
UserPrincipalName   :

AdminCount        : 1
DistinguishedName : CN=LukeSkywalker,OU=AD Management,DC=lab,DC=adsecurity,DC=org
Enabled           : True
GivenName         :
LastLogonDate     : 8/29/2015 7:29:52 PM
MemberOf          : {CN=Domain Admins,CN=Users,DC=lab,DC=adsecurity,DC=org}
Name              : LukeSkywalker
ObjectClass       : user
ObjectGUID        : 32b5226b-aa6d-4b35-a031-ddbcbde07137
PasswordLastSet   : 8/29/2015 7:26:02 PM
SamAccountName    : LukeSkywalker
SID               : S-1-5-21-1581655573-3923512380-696647894-2629
Surname           :
UserPrincipalName :
```

Note: *These methods will not return admin accounts with custom delegation – admin accounts that aren't ultimately a member of the standard AD groups.*

Mitigation:

There is no mitigation. Expect attackers to know more about what accounts have elevated rights to important resources.

Find Admin Groups

Most organizations have custom admin groups which have different naming schemes, though most include the word “admin”. Asking AD for all security groups with “admin” in the name is a quick way to get a list.

```
PS C:\> get-adgroup -filter {GroupCategory -eq 'Security' -AND Name -like "*admin*"}

DistinguishedName : CN=Domain Admins,CN=Users,DC=lab,DC=adsecurity,DC=org
GroupCategory : Security
GroupScope : Global
Name : Domain Admins
ObjectClass : group
ObjectGUID : 5621cc71-d318-4e2c-b1b1-c181f630e10e
SamAccountName : Domain Admins
SID : S-1-5-21-1581655573-3923512380-696647894-512

DistinguishedName : CN=Workstation Admins,OU=AD Management,DC=lab,DC=adsecurity,DC=org
GroupCategory : Security
GroupScope : Global
Name : Workstation Admins
ObjectClass : group
ObjectGUID : 88cd4d52-aedb-4f90-9ebd-02d4c0e322e4
SamAccountName : WorkstationAdmins
SID : S-1-5-21-1581655573-3923512380-696647894-2627

DistinguishedName : CN=Server Admins,OU=AD Management,DC=lab,DC=adsecurity,DC=org
GroupCategory : Security
GroupScope : Global
Name : Server Admins
ObjectClass : group
ObjectGUID : 3877c311-9321-41c0-a6b5-c0d88684b335
SamAccountName : ServerAdmins
SID : S-1-5-21-1581655573-3923512380-696647894-2628

DistinguishedName : CN=DnsAdmins,CN=Users,DC=lab,DC=adsecurity,DC=org
GroupCategory : Security
GroupScope : DomainLocal
Name : DnsAdmins
ObjectClass : group
ObjectGUID : 46caa0dd-6a22-42a3-a2d9-bd467934aab5
SamAccountName : DnsAdmins
SID : S-1-5-21-1581655573-3923512380-696647894-1101

DistinguishedName : CN=Administrators,CN=Builtin,DC=lab,DC=adsecurity,DC=org
GroupCategory : Security
GroupScope : DomainLocal
Name : Administrators
ObjectClass : group
ObjectGUID : d03a4afc-b14e-48c6-893c-bbc1ac872ca2
SamAccountName : Administrators
SID : S-1-5-32-544

DistinguishedName : CN=Hyper-V Administrators,CN=Builtin,DC=lab,DC=adsecurity,DC=org
GroupCategory : Security
GroupScope : DomainLocal
Name : Hyper-V Administrators
ObjectClass : group
ObjectGUID : 3137943e-f1c3-46d0-acf2-4711bf6f8417
SamAccountName : Hyper-V Administrators
SID : S-1-5-32-578
```

> DistinguishedName : CN=Enterprise Admins,CN=Users,DC=lab,DC=adsecurity,DC=org
> GroupCategory : Security
> GroupScope : Universal
> **Name : Enterprise Admins**
> ObjectClass : group
> ObjectGUID : 7674d6ad-777b-4db1-9fe3-e31fd664eb6e
> SamAccountName : Enterprise Admins
> **SID : S-1-5-21-1581655573-3923512380-696647894-519**
>
> DistinguishedName : CN=Schema Admins,CN=Users,DC=lab,DC=adsecurity,DC=org
> GroupCategory : Security
> GroupScope : Universal
> **Name : Schema Admins**
> ObjectClass : group
> ObjectGUID : 420e8ee5-77f5-43b8-9f51-cde3feea0662
> SamAccountName : Schema Admins
> **SID : S-1-5-21-1581655573-3923512380-696647894-518**

Identify Partner Organizations

External email addresses are added to the organization's Global Address List (GAL) in order to facilitate collaboration among partner organization. These email addresses are created as contact objects in Active Directory.

```
PS C:\> get-adobject -filter {ObjectClass -eq “Contact”} -Prop *

CanonicalName                 : lab.adsecurity.org/Contaxts/Admiral Ackbar
CN                            : Admiral Ackbar
Created                       : 1/27/2016 10:00:06 AM
createTimeStamp               : 1/27/2016 10:00:06 AM
Deleted                       :
Description                   :
DisplayName                   :
DistinguishedName             : CN=Admiral Ackbar,OU=Contaxts,DC=lab,DC=adsecurity,DC=org
dSCorePropagationData         : {12/31/1600 4:00:00 PM}
givenName                     : Admiral
instanceType                  : 4
isDeleted                     :
LastKnownParent               :
mail                          : admackbar@RebelFleet.org
Modified                      : 1/27/2016 10:00:24 AM
modifyTimeStamp               : 1/27/2016 10:00:24 AM
Name                          : Admiral Ackbar
nTSecurityDescriptor          : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                :
CN=Person,CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
ObjectClass                   : contact
ObjectGUID                    : 52c80a1d-a614-4889-92d4-1f588387d9f3
ProtectedFromAccidentalDeletion : False
sDRightsEffective             : 15
sn                            : Ackbar
uSNChanged                    : 275113
uSNCreated                    : 275112
whenChanged                   : 1/27/2016 10:00:24 AM
whenCreated                   : 1/27/2016 10:00:06 AM

CanonicalName                 : lab.adsecurity.org/Contaxts/Leia Organa
CN                            : Leia Organa
Created                       : 1/27/2016 10:01:25 AM
createTimeStamp               : 1/27/2016 10:01:25 AM
Deleted                       :
Description                   :
DisplayName                   :
DistinguishedName             : CN=Leia Organa,OU=Contaxts,DC=lab,DC=adsecurity,DC=org
dSCorePropagationData         : {12/31/1600 4:00:00 PM}
givenName                     : Leia
instanceType                  : 4
isDeleted                     :
LastKnownParent               :
mail                          : LeiaOrgana@TheAlliance.org
Modified                      : 1/27/2016 10:09:15 AM
modifyTimeStamp               : 1/27/2016 10:09:15 AM
Name                          : Leia Organa
nTSecurityDescriptor          : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                :
CN=Person,CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
ObjectClass                   : contact
ObjectGUID                    : ba8ec318-a0a2-41d5-923e-a3f646d1c7f9
```

```
ProtectedFromAccidentalDeletion : False
sDRightsEffective               : 15
sn                              : Organa
uSNChanged                      : 275157
uSNCreated                      : 275132
whenChanged                     : 1/27/2016 10:09:15 AM
whenCreated                     : 1/27/2016 10:01:25 AM
```

Mitigation:

The only mitigation is to not place contact objects in Active Directory which may no bet an option.

Identify Domain Password Policy

The domain password policy is easily enumerated using either “net accounts” or the AD PowerShell module “Get-ADDefaultDomainPasswordPolicy“.

```
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
```

Mitigation:

There is no reasonable mitigation.

Identify Fine-Grained Password Policies

If the Domain Functional Level (DFL) is set to “Windows Server 2008” or higher, a new feature called Fine-Grained Password Policy (FGPP) is available to provide a wide-variety of password policies that can be applied to users or groups (not OUs). While Microsoft made Fine-Grained Password Policies available starting with Windows Server 2008 (DFL), the Active Directory Administrative Center (ADAC) wasn’t updated to support FGPP administration until Windows Server 2012. Enabling “Advanced Features” from the “View” menu option in Active Directory Users and Computers and then browsing down to System, Password Settings Container (CN=Password Settings Container,CN=System,DC=DOMAIN,DC=COM) will typically display any domain FGPP objects. Note that if “Advanced Features” is not enabled, the System container is not visible.

FGPP over-rides the domain password policy settings and can be used to require stricter password policies or enable less-restrictive settings for a subset of domain users.

```
PS C:\> Get-ADFineGrainedPasswordPolicy -Filter *

AppliesTo                   : {CN=Special FGPP Users,OU=Test,DC=lab,DC=adsecurity,DC=org}
ComplexityEnabled           : True
DistinguishedName           : CN=Special Password Policy Group,CN=Password Settings
Container,CN=System,DC=lab,DC=adsecurity,DC=org
LockoutDuration             : 12:00:00
LockoutObservationWindow    : 00:15:00
LockoutThreshold            : 10
MaxPasswordAge              : 00:00:00.0000365
MinPasswordAge              : 00:00:00
MinPasswordLength           : 7
Name                        : Special Password Policy Group
ObjectClass                 : msDS-PasswordSettings
ObjectGUID                  : c1301d8f-ba52-4bb3-b160-c449d9c7b8f8
PasswordHistoryCount        : 24
Precedence                  : 100
ReversibleEncryptionEnabled : True
```

Mitigation:

There is no reasonable mitigation.

Identify Managed Service Accounts & Group Managed Service Accounts

Microsoft added Managed Service Accounts (MSAs) as a new feature with Windows Server 2008 R2 DFL which automatically manages and updates the MSA password. The key limitation is that a MSA can only be linked to a single computer running Windows 7 or Windows Server 2008 R2 (or newer).

Windows Server 2012 DFL introduced a needed update to MSAs called group Managed Service Accounts (gMSAs) which enable gMSAs to be linked to any number of computers running Windows 8 or Windows Server 2012 (or newer). Once the DFL is raised to Windows Server 2012 or newer, the default AD Service Account creation option creates a new gMSA (using the AD PowerShell module cmdlet New-ADServiceAccount, for example). Before creating a gMSA, the KDS Root key needs to be created (*Add-KDSRootKey –EffectiveImmediately*).

```
PS C:\> Get-ADServiceAccount -Filter * -Properties *

AccountExpirationDate                 : 12/27/2017 11:14:38 AM
accountExpires                        : 131588756787719890
AccountLockoutTime                    :
AccountNotDelegated                   : False
AllowReversiblePasswordEncryption     : False
AuthenticationPolicy                  : {}
AuthenticationPolicySilo              : {}
BadLogonCount                         : 0
badPasswordTime                       : 0
badPwdCount                           : 0
CannotChangePassword                  : False
CanonicalName                         : lab.adsecurity.org/Managed Service Accounts/ADSMSA12
Certificates                          : {}
CN                                    : ADSMSA12
codePage                              : 0
CompoundIdentitySupported             : {False}
countryCode                           : 0
Created                               : 1/27/2016 11:14:38 AM
createTimeStamp                       : 1/27/2016 11:14:38 AM
Deleted                               :
Description                           : gMSA for XYZ App
DisplayName                           : ADSMSA12
DistinguishedName                     : CN=ADSMSA12,CN=Managed Service
Accounts,DC=lab,DC=adsecurity,DC=org
DNSHostName                           : ADSAP02.lab.adsecurity.org
DoesNotRequirePreAuth                 : False
dSCorePropagationData                 : {12/31/1600 4:00:00 PM}
Enabled                               : True
HomedirRequired                       : False
HomePage                              :
HostComputers                         : {}
instanceType                          : 4
isCriticalSystemObject                : False
isDeleted                             :
KerberosEncryptionType                : {RC4, AES128, AES256}
LastBadPasswordAttempt                :
LastKnownParent                       :
lastLogoff                            : 0
lastLogon                             : 0
LastLogonDate                         :
localPolicyFlags                      : 0
LockedOut                             : False
logonCount                            : 0
ManagedPasswordIntervalInDays         : {21}
MemberOf                              : {}
MNSLogonAccount                       : False
Modified                              : 1/27/2016 11:14:39 AM
modifyTimeStamp                       : 1/27/2016 11:14:39 AM
msDS-ManagedPasswordId                : {1, 0, 0, 0…}
msDS-ManagedPasswordInterval          : 21
msDS-SupportedEncryptionTypes         : 28
msDS-User-Account-Control-Computed    : 0
```

```
Name                                : ADSMSA12
nTSecurityDescriptor                : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                      : CN=ms-DS-Group-Managed-Service-
Account,CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
ObjectClass                         : msDS-GroupManagedServiceAccount
ObjectGUID                          : fe4c287b-f9d2-45ce-abe3-4acd6d09c3ff
objectSid                           : S-1-5-21-1581655573-3923512380-696647894-3605
PasswordExpired                     : False
PasswordLastSet                     : 1/27/2016 11:14:38 AM
PasswordNeverExpires                : False
PasswordNotRequired                 : False
PrimaryGroup                        : CN=Domain Computers,CN=Users,DC=lab,DC=adsecurity,DC=org
primaryGroupID                      : 515
PrincipalsAllowedToDelegateToAccount      : {}
PrincipalsAllowedToRetrieveManagedPassword : {}
ProtectedFromAccidentalDeletion     : False
pwdLastSet                          : 130983956789440119
SamAccountName                      : ADSMSA12$
sAMAccountType                      : 805306369
sDRightsEffective                   : 15
ServicePrincipalNames               :
SID                                 : S-1-5-21-1581655573-3923512380-696647894-3605
SIDHistory                          : {}
TrustedForDelegation                : False
TrustedToAuthForDelegation          : False
UseDESKeyOnly                       : False
userAccountControl                  : 4096
userCertificate                     : {}
UserPrincipalName                   :
uSNChanged                          : 275383
uSNCreated                          : 275380
whenChanged                         : 1/27/2016 11:14:39 AM
whenCreated                         : 1/27/2016 11:14:38 AM
```

Mitigation:

There is no reasonable mitigation.

Identify Groups with Local Admin Rights to Workstations/Servers

PowerView has incorporated this functionality (@HarmJ0y beat me to it!).
Group Policy provides the ability, via Restricted Groups, to enforce local group membership such as the Administrators groups on all computers in an OU. This can be tracked back by identifying the GPOs that are using restricted groups and the OUs they are applied to. This provides the AD groups that have admin rights and the associated list of computers.

Using PowerView (part of PowerSploit), we can quickly identify GPOs that include Restricted Groups.

```
PS C:\> Get-NetGPOGroup

GPOName        : {E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}
GPOPath        : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{E9CABE0F-3A3F-40B1-B4C1-
1FA89AC1F212}
Members        : {Server Admins}
MemberOf       : {Administrators}
GPODisplayName : Add Server Admins to Local Administrator Group

Filters        :
GPOName        : {45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
GPOPath        : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{45556105-EFE6-43D8-A92C-
AACB1D3D4DE5}
Members        : {Workstation Admins}
MemberOf       : {Administrators}
GPODisplayName : Add Workstation Admins to Local Administrators Group
```

Once we have this information, we can check what to what OUs the GPOs link using a PowerView cmdlet.

```
PS C:\> get-netOU -guid “E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212”
LDAP://OU=Servers,DC=lab,DC=adsecurity,DC=org

PS C:\> get-netOU -guid “45556105-EFE6-43D8-A92C-AACB1D3D4DE5”
LDAP://OU=Workstations,DC=lab,DC=adsecurity,DC=org
```

Next, we identify the computers in these OUs

```
PS C:\> get-adcomputer -filter * -SearchBase “OU=Servers,DC=lab,DC=adsecurity,DC=org”

DistinguishedName : CN=ADSAP01,OU=Servers,DC=lab,DC=adsecurity,DC=org
DNSHostName : ADSAP01.lab.adsecurity.org
Enabled : True
Name : ADSAP01
ObjectClass : computer
ObjectGUID : b79bb5e3-8f9e-4ee0-a30c-5f66b61da681
SamAccountName : ADSAP01$
SID : S-1-5-21-1581655573-3923512380-696647894-1105
UserPrincipalName :

DistinguishedName : CN=ADSAP02,OU=Servers,DC=lab,DC=adsecurity,DC=org
DNSHostName : ADSAP02.lab.adsecurity.org
Enabled : True
Name : ADSAP02
ObjectClass : computer
ObjectGUID : 1006978e-8627-4d01-98b6-3215c4ee4541
SamAccountName : ADSAP02$
SID : S-1-5-21-1581655573-3923512380-696647894-1603
UserPrincipalName :

PS C:\> get-adcomputer -filter * -SearchBase “OU=Workstations,DC=lab,DC=adsecurity,DC=org”

DistinguishedName : CN=ADSWRKWIN7,OU=Workstations,DC=lab,DC=adsecurity,DC=org
DNSHostName       : ADSWRKWIN7.lab.adsecurity.org
Enabled           : True
Name              : ADSWRKWIN7
ObjectClass       : computer
ObjectGUID        : e8b3bed2-75b4-4512-a4f0-6d9c2d975c70
SamAccountName    : ADSWRKWIN7$
SID               : S-1-5-21-1581655573-3923512380-696647894-1104
UserPrincipalName :

DistinguishedName : CN=ADSWKWIN7,OU=Workstations,DC=lab,DC=adsecurity,DC=org
DNSHostName       : ADSWKWIN7.lab.adsecurity.org
Enabled           : True
Name              : ADSWKWIN7
ObjectClass       : computer
ObjectGUID        : 2f164d63-d721-4b0e-a553-3ca0e272aa96
SamAccountName    : ADSWKWIN7$
SID               : S-1-5-21-1581655573-3923512380-696647894-1602
UserPrincipalName :
```

Using a few PowerShell commands, we are able to identify what AD groups are configured via GPO with full admin rights on computers in the domain.

Mitigation:

The only mitigation is to remove Domain Users from being able to read the GPOs that manage local groups. Only computers in the domain require the ability to read and process these GPOs. Note that once an attacker gains admin rights on a single computer in the domain, they can use the computer account to read the GPO.

Identify Microsoft AppLocker Settings

Microsoft AppLocker can be used to limit application execution to specific approved applications. There are several difference phases I recommend for AppLocker:

- Phase 1: Audit Mode – audit all execution by users and the path they were run from. This logging mode provides information on what programs are run in the enterprise and this data is logged to the event log.
- Phase 2: “Blacklist Mode” – Configure AppLocker to block execution of any file in a user’s home directory, profile path, and temporary file location the user has write access to, such as c:\temp.
- Phase 3: “Folder Whitelist Mode” – Configure AppLocker to build on Phase 2 by adding new rules to only allow execution of files in specific folders such as c:\Windows and c:\Program Files.
- Phase 4: “Application Whitelisting” – Inventory all applications in use in the enterprise environment and whitelist those applications by location and hash (preferably digital signature). This ensures that only approved organization applications will execute.

The issue is that AppLocker is configured via Group Policy, which is often kept at the default which enables all domain users the ability to read the configuration.

Mitigation:

The only mitigation is to remove Domain Users from being able to read the GPOs that manage local groups. Only computers in the domain require the ability to read and process these GPOs. Note that once an attacker gains admin rights on a single computer in the domain, they can use the computer account to read the GPO.

Identify Microsoft EMET Settings

Microsoft Enhanced Mitigation Experience Toolkit (EMET) helps prevent application vulnerabilities from being exploited (including some 0-days). It’s a free product that effectively “wraps” popular applications so when vulnerability exploitation is attempted, the attempt is stopped at the “wrapper” and doesn’t make it to the OS. Enterprises often use Group Policy to configure EMET, which is often kept at the default which enables all domain users the ability to read the configuration.

Mitigation:

The only mitigation is to remove Domain Users from being able to read the GPOs that manage local groups. Only computers in the domain require the ability to read and process these GPOs. Note that once an attacker gains admin rights on a single computer in the domain, they can use the computer account to read the GPO.

Identify Microsoft LAPS Delegation

Microsoft Local Administrator Password Solution (LAPS) is a great option for managing local Administrator account passwords for computers in the enterprise. LAPS adds two new attributes to the AD computer object, one to store the local Admin password and one to track the last time the password was changed. A LAPS GPO is used to configure the LAPS client determining when the password is changed, its length, the account managed, etc. The computer’s local Administrator password is created by the LAPS client on the computer, that password is set as the new value for the LAPS password attribute (ms-Mcs-AdmPwd), and changed locally. In order for the password to be usable by an admin, read access to the ms-Mcs-AdmPwd needs to be delegated. This delegation can be identified by enumerating the security ACLs on the attribute.

Mitigation:

The only mitigation is to remove Domain Users from being able to read the GPOs that manage local groups. Only computers in the domain require the ability to read and process these GPOs. Note that once an attacker gains admin rights on a single computer in the domain, they can use the computer account to read the GPO.

Discover Admin Credentials in the domain SYSVOL Share

Admins often place credentials in scripts or in Group Policy which end up in SYSVOL.
More information on this issue including mitigation: “Finding Passwords in SYSVOL & Exploiting Group Policy Preferences”

Conclusion

These are only a few of the interesting data items which can be easily gathered from Active Directory as a domain user. Expect an attacker to gain a foothold in your enterprise and adjust current strategies accordingly.

Note: W*hile I have some scripts that perform many of these actions already, they are not ready for sharing. At some point in fhe future, I may be able to share these.*

(Visited 70,000 times, 17 visits today)