RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: TECH-R07

Proactive Directory: : Practical Counterdefenses to Securing Active Directory

Matthew McWhirt
Director
FireEye / Mandiant

Presenter

- Matthew McWhirt
  - Mandiant Consulting - Security Transformation Services (STS)
  - Passionate about Active Directory defenses

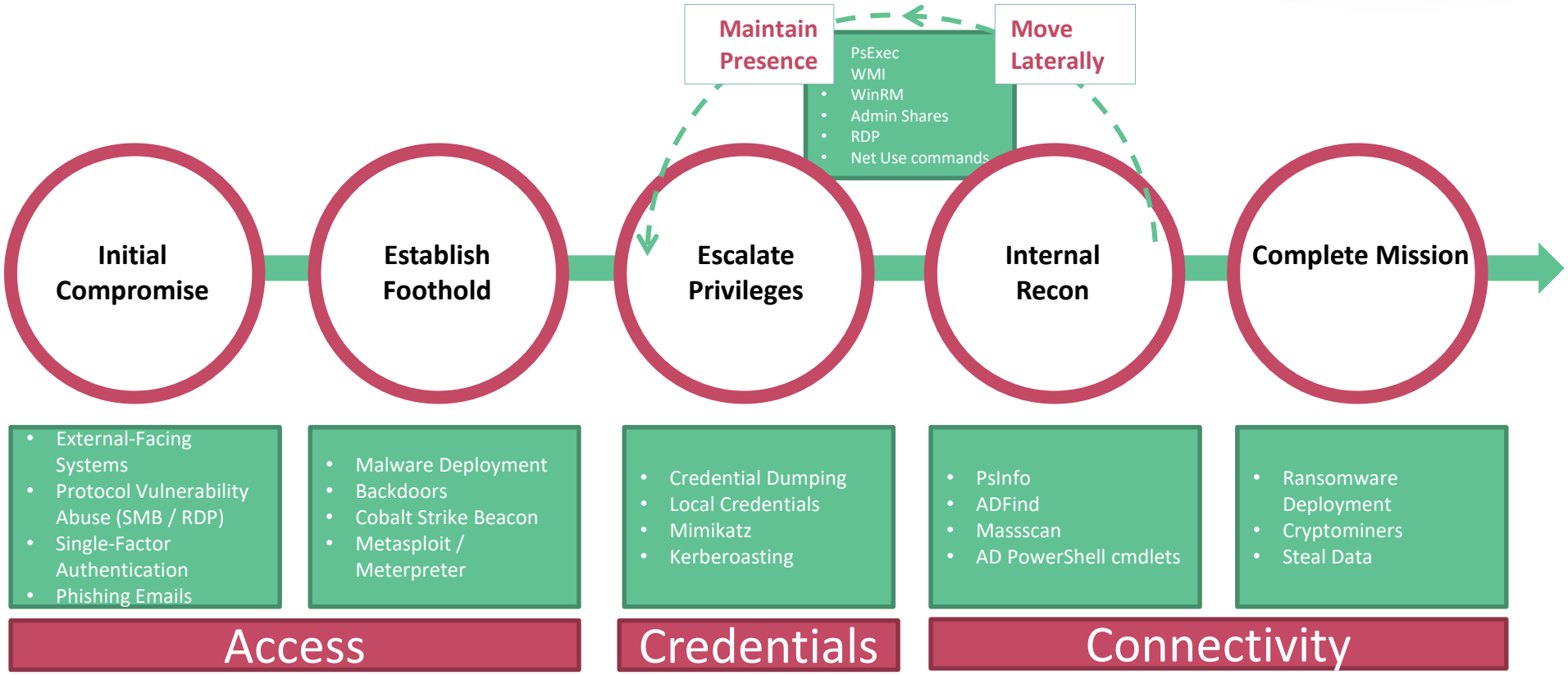
Why Active Directory Defenses are Necessary?

- Discuss common attacker tactics and Active Directory (AD) configuration weaknesses that can lead to a large scale compromise.
- Provide practicable and actionable recommendations that can be implemented to harden an environment to protect against AD exploitation and compromise.
- Recommendations provided are the same steps that organizations must implement to contain and eradicate attackers from an environment.

Simplified Exploitation Model

Access
+ Credentials
+ Connectivity
= $ Profit

Common Attack Lifecycle



Common Ways that Initial Access is Obtained

Common Vectors	Methods	Examples
External Facing Systems – with limited segmentation between DMZ and internal resources	Vulnerability Exploitation	EternalBlue – SMB v1 vulnerability Vulnerabilities in third-party technologies (e.g., SSL VPN, edge network devices) Vulnerabilities in third-party applications (e.g., WordPress, WebLogic)
	Access using legitimate credentials • Brute Forcing • Simple password guessing • Previous phishing campaigns • Credentials purchased in an underground marketplace	External-facing systems with Remote Desktop Protocol (RDP) enabled from the Internet Single-factor VPN, Citrix, or other remote access technologies
Phishing Emails	Delivery of emails that contain either embedded links to malicious websites or weaponized attachments	Malicious attachments that rely upon Macros to download malware Malicious websites which masquerade as a legitimate site to capture credentials for access via single-factor external facing systems

AD Reconnaissance Objectives

- Determine scope of domains and trusts where access may be permissible
- Find privileged credentials for further access + connectivity
  - Domain-based privileged groups / accounts*
  - Local administrative accounts
  - “Backdoor” Active Directory accounts
    - KRBTGT
    - DSRM
  - “Service” accounts (Kerberoasting)

AD Credential Targeting Objectives

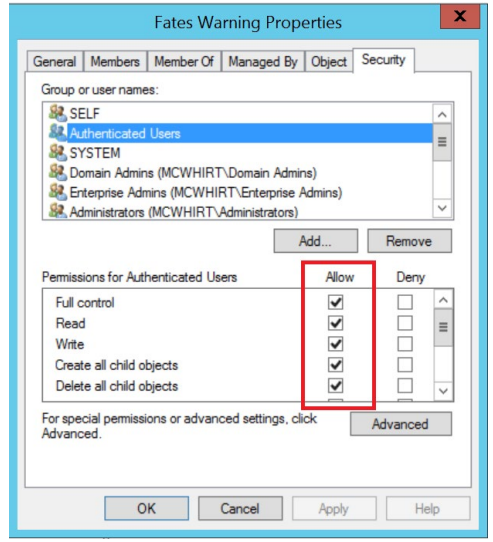
- Domain-based privileged groups / accounts can be more than just Enterprise / Schema / Domain Admins
  - Nested Accounts / Groups that provide a pathway to enhanced privileges in AD
    - *Organization Management → Exchange Trusted Subsystem → Exchange Windows Permissions**
  - Accounts protected by AdminSDHolder
  - Accounts with a password which doesn't expire
  - Accounts with the ability to modify / link / unlink GPOs
  - Sensitive accounts that CAN be delegated
  - Accounts with SID History attributes configured

AD Credential Targeting Objectives

- More targeting……
  - Accounts with AD Extended Rights Permissions
    - *DS-Replication-Get-Changes-All*
    - *DS-Replication-Get-Changes*
    - *Reset Password*
    - *WriteOwner*
    - *WriteDACL*

DCSync

  - Accounts with the ability to modify group membership for built-in privileged groups
  - Accounts with the ability to modify AdminSDHolder permissions
  - Accounts with elevated permissions on OUs that contain sensitive accounts and/or systems (e.g., Domain Controllers, Admin Workstations)
  - Accounts with explicit permissions defined within the “Default Domain Controllers Policy”
    - Backup Operators
    - Server Operators
  - Computer accounts with Delegation configured



How are Credentials Obtained?

After initial endpoint exploitation – an attacker will attempt to obtain credentials that are resident on disk or in memory.

- **Example method that can be used to extract passwords from disk:**
  - Dump the registry hives to extract and crack password hashes for local accounts, cached domain credentials, and service accounts.
  - Syskey to decrypt secrets (registry)
  - "Pass-the-hash" (no cracking) for password hashes for local accounts.

- **Example credential dumping tools that can extract passwords, hashes, keys, and tickets from memory:**
  - Mimikatz
  - Kekeo
  - ProcDump
  - Windows Task Manager
  - Windows Credential Editor (WCE)

How are Credentials Obtained?

- **Requesting Kerberos tickets for service accounts – and attempting to crack the password from the service ticket**
  - *This technique does not require administrative access to an endpoint*

```
PS C:\Windows\system32> get-aduser -filter {(ServicePrincipalName -like "*")}
```

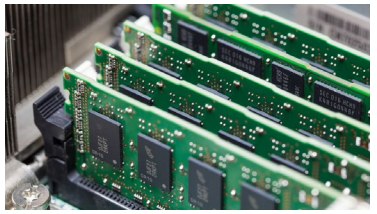
- **Accessing Systems Configured for Delegation (Constrained | Unconstrained)**
  - *Harvesting hashes/tickets stored in memory*
  - *Tickets can be renewed for up to seven (7) days before expiry (default setting)*
  - *Hashes can be used until the password for an account is changed*

```
PS C:\Windows\system32>  Get-ADObject -fi {(msDS-AllowedToDelegateTo -like '*') -or (UserAccountControl -band 0x80000) -
or (UserAccountControl -band 0x1000000)}
```

- **Via clear-text passwords – either on disk or in memory**
  - Configuration files or passwords stored in a file on the endpoint
  - Group Policy Preferences
  - Credential Manager
  - Legacy settings that result in clear-text passwords being stored in memory (WDigest)
  - Kerberos provider – when a DC is not available for authentication

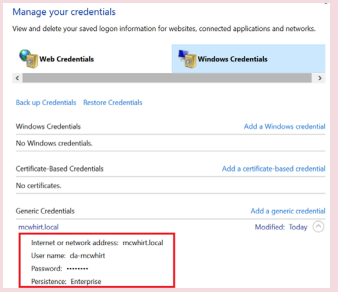
Credentials in Memory

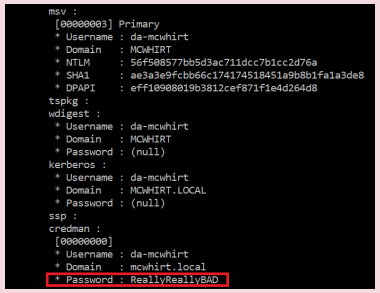
- Interactive (Local) Logon
- Remote Desktop (RDP) Logon
- PSExec with explicit credentials
- Batch logon (Scheduled Tasks)
- Running Services
- RunAs (New Credentials)
- PowerShell CredSSP
  - Can be controlled via GPO settings

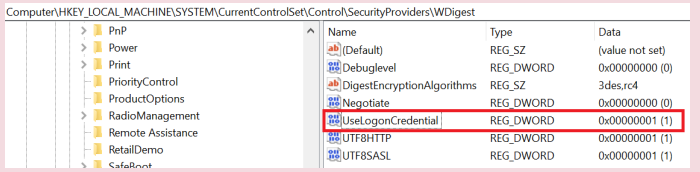


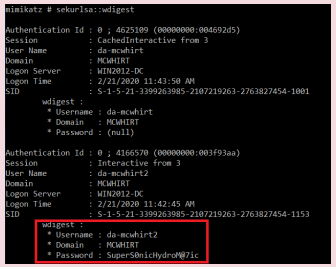
```
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Nov 20 2014 01:35:45)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */

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

Passwords can be stored as cleartext (WDigest, SSP, CredManTsPkg (pre-KB2871997)), encrypted values, or hashes.

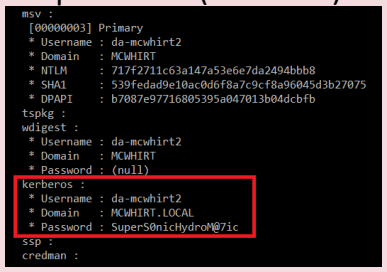


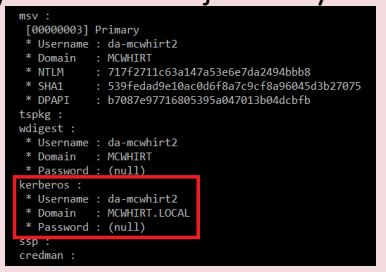






If a Domain Controller is not available, the **Kerberos** provider will store an account's password (cleartext) in memory on a domain-joined system.



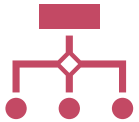


Reducing Credential Exposure Using AD Controls

Minimize privileged credential exposure!

Harden systems so that privileged and/or service accounts cannot be used for logons to standard endpoints

- Tiered Architecture Model
- Protected Users Security Group
- Credential Guard / LSA Protected Process
- Restricted Admin RDP
- Identify accounts w/ SPNs (Kerberoasting)
- Identify accounts that do not require pre-authentication (ASREP)



Remove the capability for local administrative accounts to be used for remote logons to other endpoints

- KB2871997
- S-1-5-114: NT AUTHORITY\Local account and member of Administrators group

Randomize the password for built-in local administrative accounts on endpoints

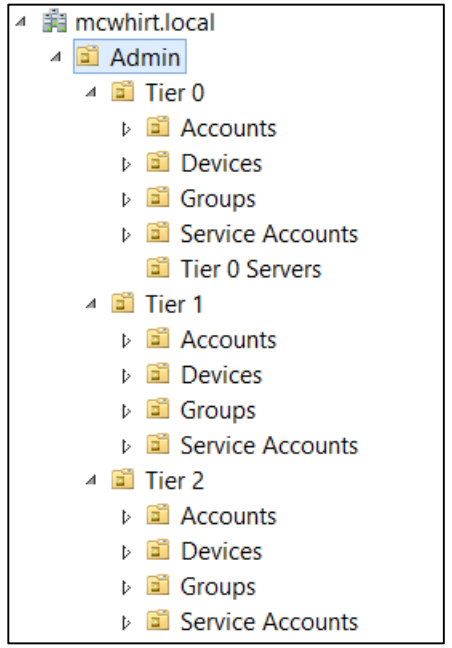
- LAPS
- 3rd party technologies

Harden endpoints so that clear-text passwords are not stored in memory

- Disable WDigest authentication
- TokenLeakDetectDelaySecs
- Protected Users Security Group
- Managed Service Accounts
- Users not running as local admin!

Tiered Architecture - Overview

- Objective = ***Prevent Privilege Escalation in AD***
- **Reduce the exposure of privileged credentials amongst tiers**
- Accounts of a lower tier should not be able to control systems, applications, GPO settings, or other accounts in a higher tier (and vice versa)
- Leverage dedicated Privileged Access Workstations (PAWs) to manage endpoints and settings within each tier



Tiered Administration – Enforced via GPOs

- **Tier 0**

Local Policies/User Rights Assignment	
Policy	**Setting**
Allow log on locally	Administrators, MCWHIRT\Tier0-DomainAdmins
Allow log on through Terminal Services	MCWHIRT\Tier0-DomainAdmins

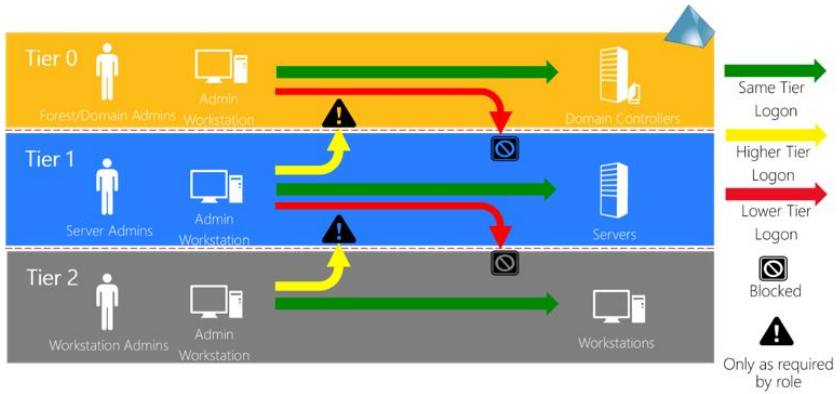
- **Tier 1**

Local Policies/User Rights Assignment	
Policy	**Setting**
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier2-Admins, MCWHIRT\Tier2-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier2-Admins, MCWHIRT\Tier2-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier2-Admins, MCWHIRT\Tier2-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier2-Admins, MCWHIRT\Tier2-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier2-Admins, MCWHIRT\Tier2-ServiceAccounts

- **Tier 2**

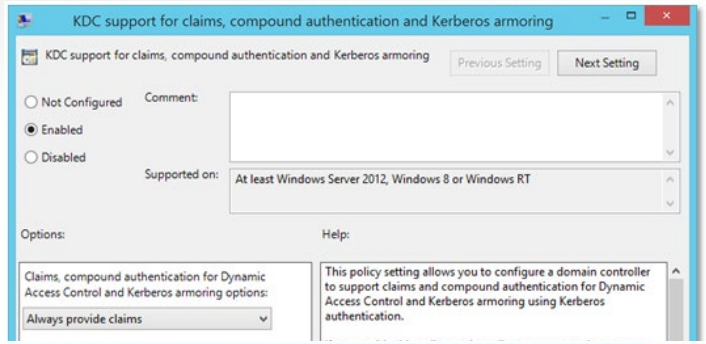
Local Policies/User Rights Assignment	
Policy	**Setting**
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

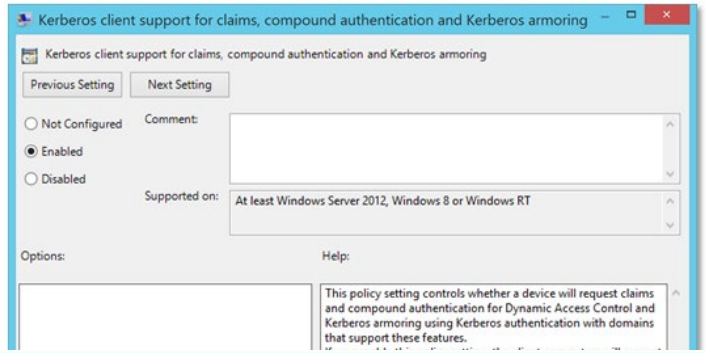


Tiered Administration – Authentication Silos

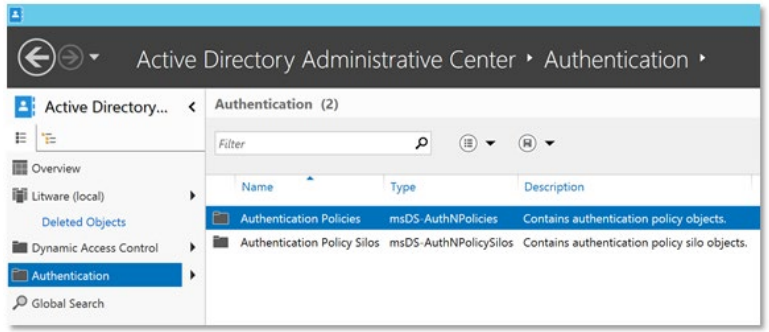
- Authentication policy silos = mechanism to constrain privileged accounts – and only allow the accounts to be leveraged on specific endpoints.
  - Tier 0 (Domain Controllers) = Domain Admins Group
- Silos are defined and managed in Active Directory (Authentication Policies)
- Windows Server 2012 R2 DFL
- Clients must run Windows 8+ / Server 2012+ to support Kerberos armoring (which is part of Dynamic Access Control)



Domain Controller Setting



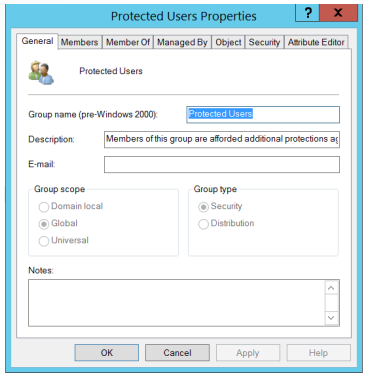
Client Endpoint Setting

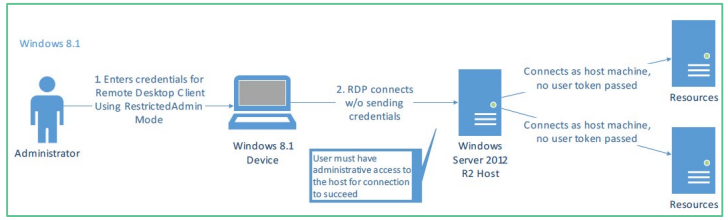


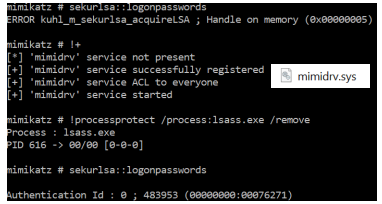
msDS-AssignedAuthNPolicy
msDS-AssignedAuthNPolicySilo

Other Active Directory Account Protections

- **Protected Users Security Group**
  - Provides an umbrella of protections for privileged accounts
- **Credential Guard / Remote Credential Guard**
  - Win 10 / Server 2016+
  - When enabled, the Local Security Authority Subsystem Service (LSASS) consists of 2 processes:
    - the normal LSA process
    - The isolated LSA process (which runs in Virtual Secure Mode (VSM) = Lsalso.exe)
- **Restricted Admin Remote Desktop Protocol (RDP)**
  - Minimizes the exposure of user credentials in memory when RDP is utilized
- **LSA Protected Process**
  - Protects the LSASS Process. Can be tricky to enforce – so start with "audit" mode
  - Can be even trickier to disable if LSA Protection causes issues + UEFI/SecureBoot is enabled (disabling requires changing a registry key, mounting an EFI system partition, modifying the boot menu, modifying the boot order, and rebooting an endpoint to "opt-out")
  - With local admin / SYSTEM access, can be "bypassed" by Mimikatz (mimidrv.sys)







Connectivity

- **With the correct credentials**, default Windows protocols allow for remote connectivity amongst systems.
- Placement of backdoors on endpoints – for beaconing and persistent access to an environment
- Common Windows protocols that are used for lateral movement:
  - SMB
  - RDP
  - WMI
- **Common methods that are used for lateral movement and malware deployment:**
  - PsExec – free remote administration tool that uses SMB for connectivity
  - RDP – attacker remotely logs onto an endpoint for pivoting, staging, or deployment of malware
  - Scripts that leverage SMB or WMI connectivity - for remote connectivity and/or deployment of malicious files to endpoints

Connectivity Hardening Using AD Controls

Restrict system-to-system communications

- Windows Firewall
- Network Segmentation

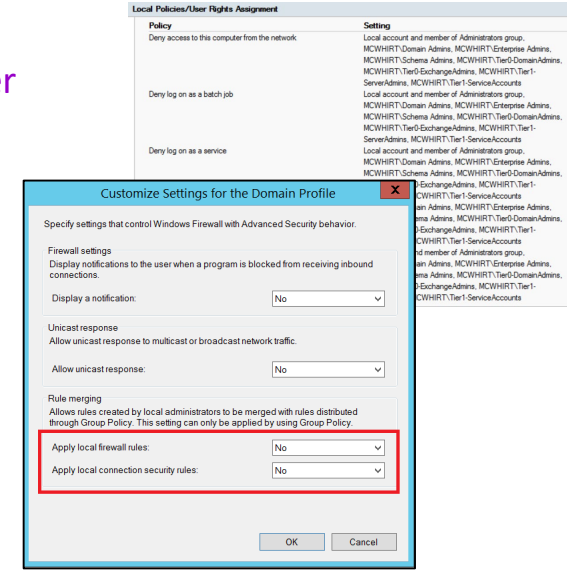
Name	Group	Profile	Enabled	Action
WinRm via HTTPs - Block Inbound		All	Yes	Block
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Spooler Service - RPC-EPM...	File and Printer Sharing	All	Yes	Block
Windows Management Instrumentation (DCOM-In)	Windows Managemen...	All	Yes	Block
Windows Management Instrumentation (WMI-In)	Windows Managemen...	All	Yes	Block
Windows Remote Management (HTTP-In)	Windows Remote Ma...	All	Yes	Block
Windows Remote Management (HTTP-In)	Windows Remote Ma...	All	Yes	Block

```
netsh advfirewall firewall set rule group="remote desktop" new enable=Yes
netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes
```

Restrict egress access, ports, and protocols

- Windows Firewall
- Network Perimeter Devices

Remove the capability for privileged accounts to be used for remote logon purposes



Disable unnecessary services on endpoints

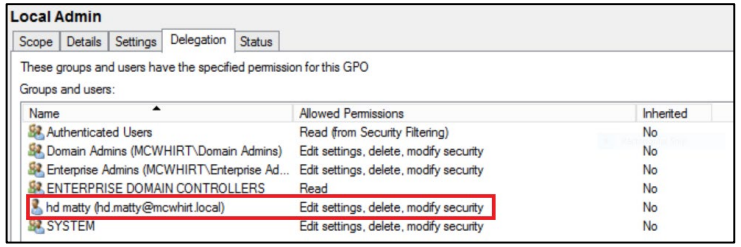
- Windows Firewall
- Admin Shares
- Do users or admins use VNC or ScreenConnect?

Leverage dedicated privileged access workstations (PAWs) for performing administrative tasks

- Separate VPN profiles for admins

Power of Group Policy Objects (GPOs)

- Can be used to enforce computer and/or user settings .
- If an attacker doesn't have direct control of an object, but can modify GPO settings, an attacker can now potentially control an object.
- If misconfigured and/or abused, can lead to a very bad {day|month|year} for an organization's security posture.



GPO Processing

- Local > Site > Domain > **OU**
- Multiple Client Side Extensions (CSEs):
  https://blogs.technet.microsoft.com/mempson/2010/12/01/group-policy-client-side-extension-list/
- Computer / User Background Refresh Interval = 90 minutes / 0-30 minute offset

> (Computer|User) Configuration > Policies > Administrative Templates > System > Group Policy > Set Group Policy refresh interval for (Computers|Users)

- Equivalent to “GPUPDATE” command – will only apply GPO settings that are **NEW** or **MODIFIED** (since last reboot / logon / refresh)

GPO Security CSE Processing

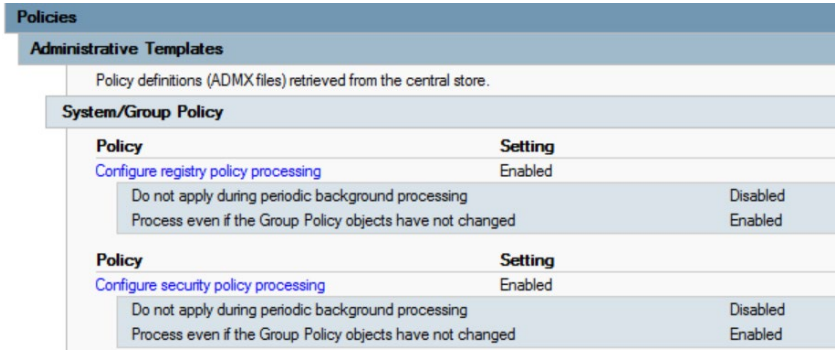
- Security CSE {827D319E-6EAC-11D2-A4EA-00C04F79F83A} will automatically re-apply **ALL** configured settings after 16 hours (regardless of if the policy has changed or not)

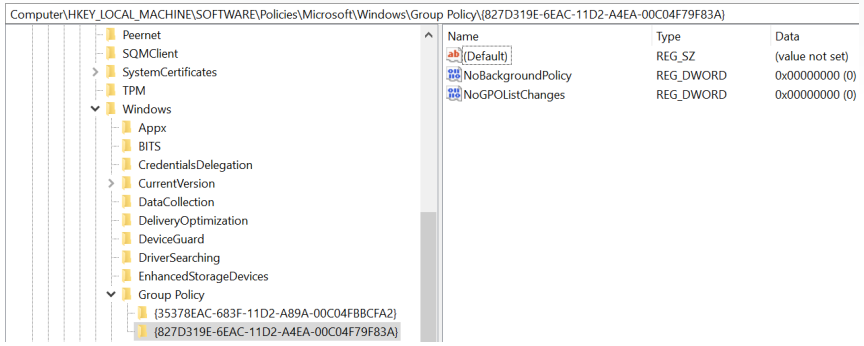
```
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions
\{827D319E-6AC-11D2-A4EA-00C04F79F83A}\MaxNoGPOListChangesInterval
```

- “Security” settings include anything configured within:

```
Computer Configuration > Policies > Windows Settings > Security Settings
User Configuration > Policies > Windows Settings > Security Settings
```

GPO (re)Processing = GPUPDATE /FORCE





- Enforce automatic GPO reprocessing for specific (or all) CSEs during background refresh – **regardless of if the policy has not changed**
- Some CSEs will automatically reprocess all settings, regardless of if reprocessing settings are configured in a GPO (e.g., Registry Preference Extension Policy)

GPO Exploitation

- Passwords stored in Group Policy Preferences (GPP)
- Ransomware operators commonly target GPOs for persistence and propagation of malware
  - Logon Scripts
  - Scheduled Tasks
  - Software Installation packages
  - Modify local administrative membership on endpoints

```
GPO - Computer Startup Script:
Copy \\<domain>\sysvol\<domain>\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Scripts\Startup\encrypt.exe %windir% && sc create avupdate binPath="c:\windows\encrypt.exe" start=auto && sc start avupdate
```

- Ransomware operators have been observed deleting ALL GPOs, to further create chaos and hamper restoration efforts

GPO Exploitation – How?

- Gaining access to privileged accounts that have the ability to edit / link / unlink GPOs
  - Some GPOs may be misconfigured, and allow for a non-privileged account to edit an existing GPO that is applied to endpoints
  - Modifying SYSVOL permissions to provide additional accounts that ability to modify GPOs
- Leveraging tools to identify misconfigured GPOs – or GPOs that contain settings which can be further exploited
  - PowerView
  - BloodHound
  - Grouper2

GPO Reviewing and Monitoring

- Review configured permissions for existing GPOs

```
PS C:\Windows\system32> Get-GPPermissions -Name "Default Domain Controllers Policy" -All
```

- Review last modified times for existing GPOs

```
PS C:\Windows\system32> Get-GPO -All
```

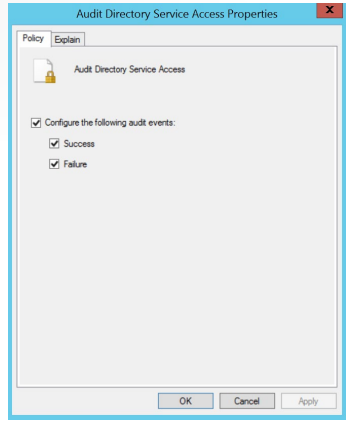
- Review permissions configured for SYSVOL and for GPTs

```
PS C:\Windows\system32> icacls c:\Windows\SYSVOL
c:\Windows\SYSVOL NT AUTHORITY\Authenticated Users:(RX)
                  NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(GR,GE)
                  BUILTIN\Server Operators:(RX)
                  BUILTIN\Server Operators:(OI)(CI)(IO)(GR,GE)
                  BUILTIN\Administrators:(M,WDAC,WO)
                  BUILTIN\Administrators:(OI)(CI)(IO)(F)
                  NT AUTHORITY\SYSTEM:(F)
                  NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
                  BUILTIN\Administrators:(M,WDAC,WO)
                  CREATOR OWNER:(OI)(CI)(IO)(F)
```

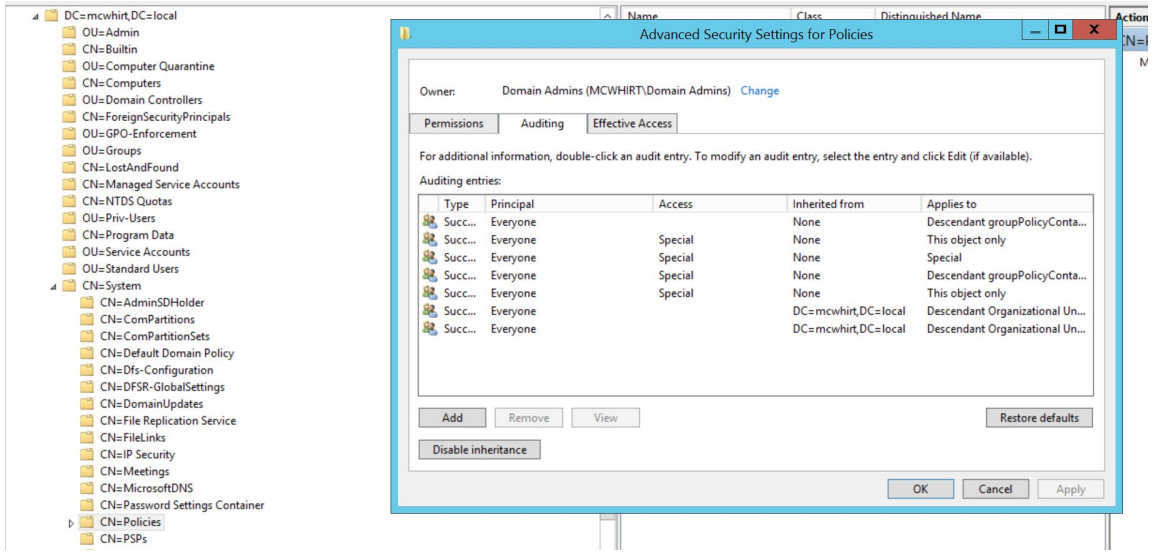
```
PS C:\users\da-mcwhirt\Desktop> get-acl -path \\WIN2012-DC\sysvol\mcwhirt.local\policies | FL

Path   : Microsoft.PowerShell.Core\FileSystem::\\WIN2012-DC\sysvol\mcwhirt.local\policies
Owner  : BUILTIN\Administrators
Group  : NT AUTHORITY\SYSTEM
Access : CREATOR OWNER Allow  268435456
         NT AUTHORITY\Authenticated Users Allow  -1610612736
         NT AUTHORITY\Authenticated Users Allow  ReadAndExecute, Synchronize
         NT AUTHORITY\SYSTEM Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         BUILTIN\Administrators Allow  Write, ReadAndExecute, ChangePermissions, TakeOwnership, Synchronize
         BUILTIN\Server Operators Allow  -1610612736
         BUILTIN\Server Operators Allow  ReadAndExecute, Synchronize
         MCWHIRT\Group Policy Creator Owners Allow  Write, ReadAndExecute, Synchronize
         MCWHIRT\Group Policy Creator Owners Allow  -536870912
Audit  :
Sddl   : O:BAG:SYD:PAI(A;OICIIO;GA;;;CO)(A;OICIIO;GXGR;;;AU)(A;;0x1200a9;;;AU)(A;OICIIO;GA;;;SY)(A;;FA;;;SY)(A;OICIIO;G
         A;;;BA)(A;;0x1e01bf;;;BA)(A;OICIIO;GXGR;;;SO)(A;;0x1200a9;;;SO)(A;;0x1201bf;;;PA)(A;OICIIO;GXGWGR;;;PA)
```

GPO Reviewing and Monitoring

- Enable “Audit Directory Service Changes” Auditing
  - Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > DS Access > Audit Directory Service Changes

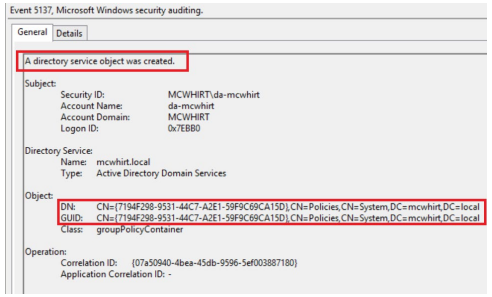


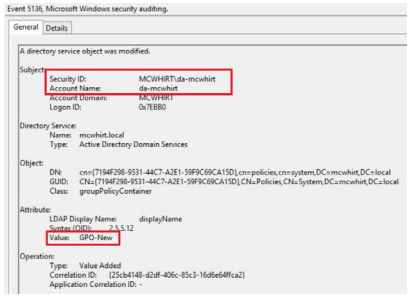
- Via ADSIEdit, configure Auditing for the “Everyone” group for the following actions:
  - *Create groupPolicyContainer objects*
  - *Write*
  - *Modify Permissions*
  - *Write versionNumber*

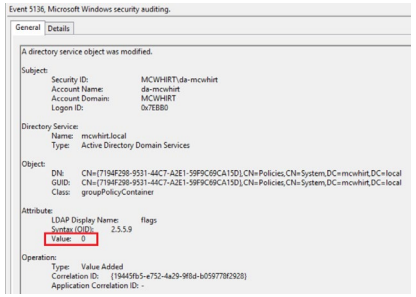


GPO Reviewing and Monitoring

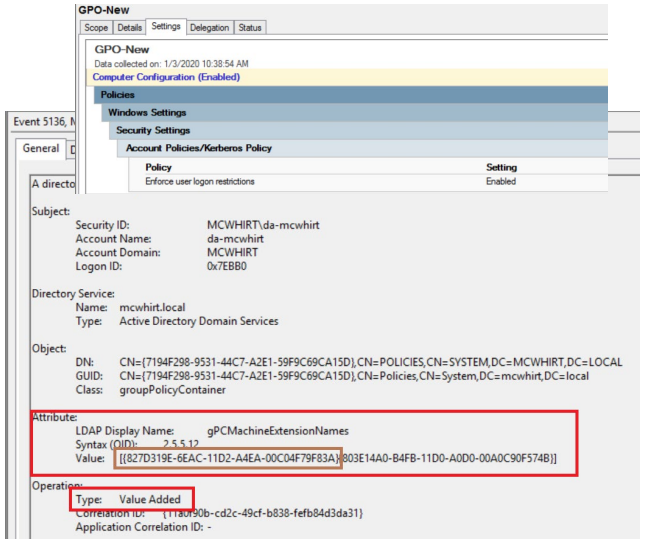
- Monitor Security Event Logs on Domain Controllers for any created|modified|deleted GPOs
  - **EID 5137**: Group Policy creations



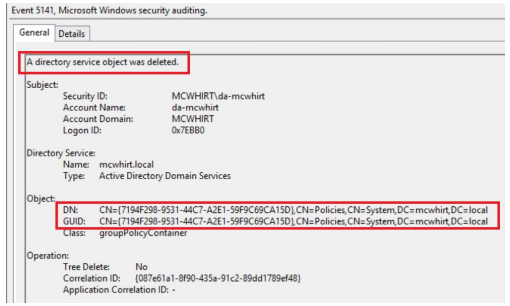




  - **EID 5136**: Group Policy modifications, links, unlinks



  - **EID 5141**: Group Policy deletions



Overall Goals of AD Proactive Hardening

- Minimize the exposure of privileged credentials
  - Make it difficult for an attacker to gain access to Tier 0 credentials!
- Create separate tiers/silos for AD administrative functions
- Leverage AD to consistently and continually enforce hardened settings for endpoints
- Review AD configurations on a consistent basis
- Test and verify the effectiveness of your AD controls

RSAConference2020

Questions?