How to Harden Active Directory to Prevent Cyber Attacks

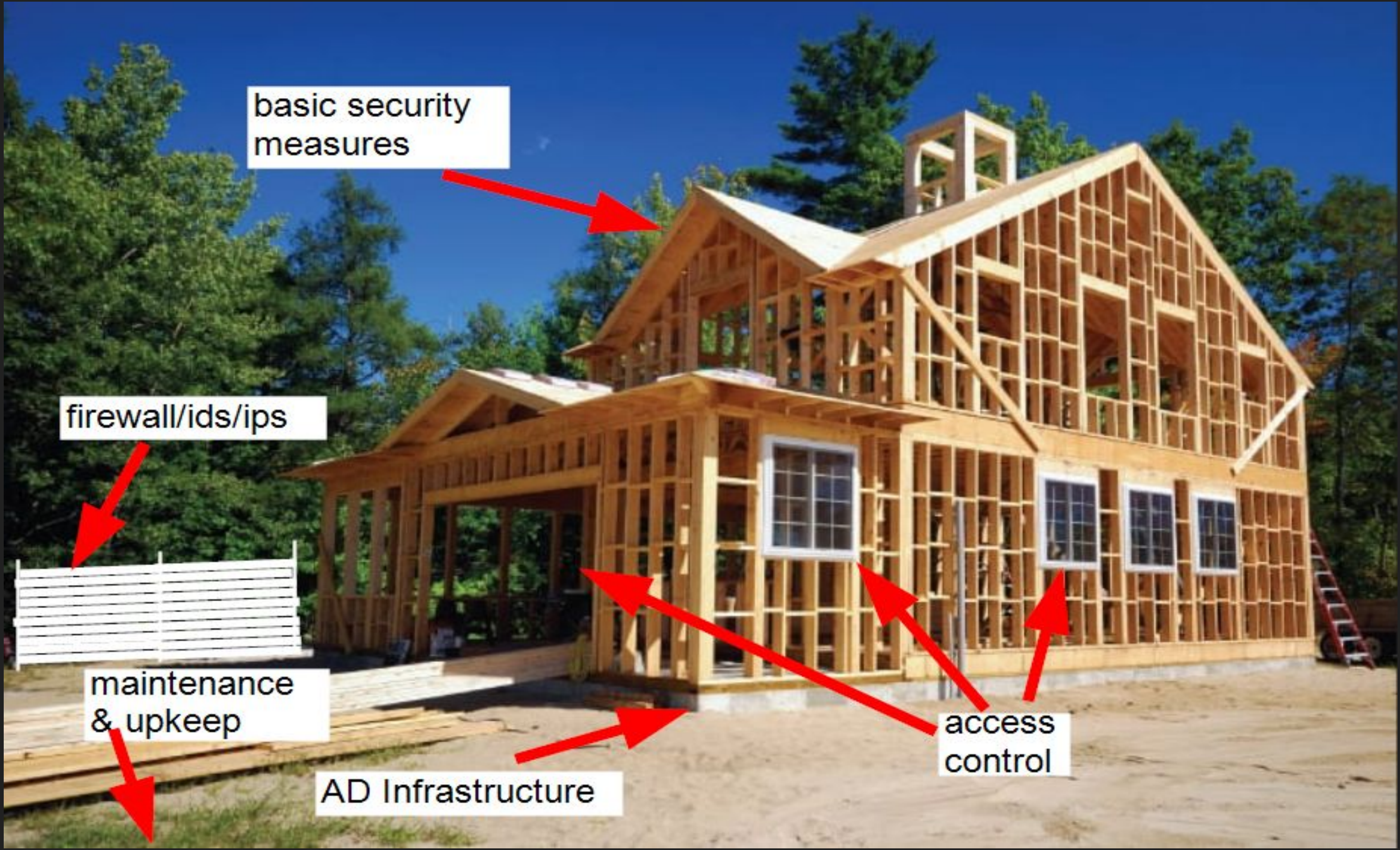
Spencer Alessi

SecurIT360

The physics of securing IT

NATIONAL SECURITY AGENCY
WE KNOW WHAT YOU DID LAST LOGIN
Ethical Threat

How do you **build** a house?


basic security measures
firewall/ids/ips
maintenance & upkeep
AD Infrastructure
access control

c:\> whoami: Spencer Alessi

- **Background**: Help Desk > Sysadmin
- **Passion**: Internal Pentesting/Assume Breach
- **Ethos**: Spirit of a hacker, heart of a defender

  Red with blue stripes? Blue with red stripes?
- **Receipts**: CRTO, PNPT, GPEN, CISSP
- **Side Hustles**: Tools, Content, SWAG!

Active Directory

Got AD CS?

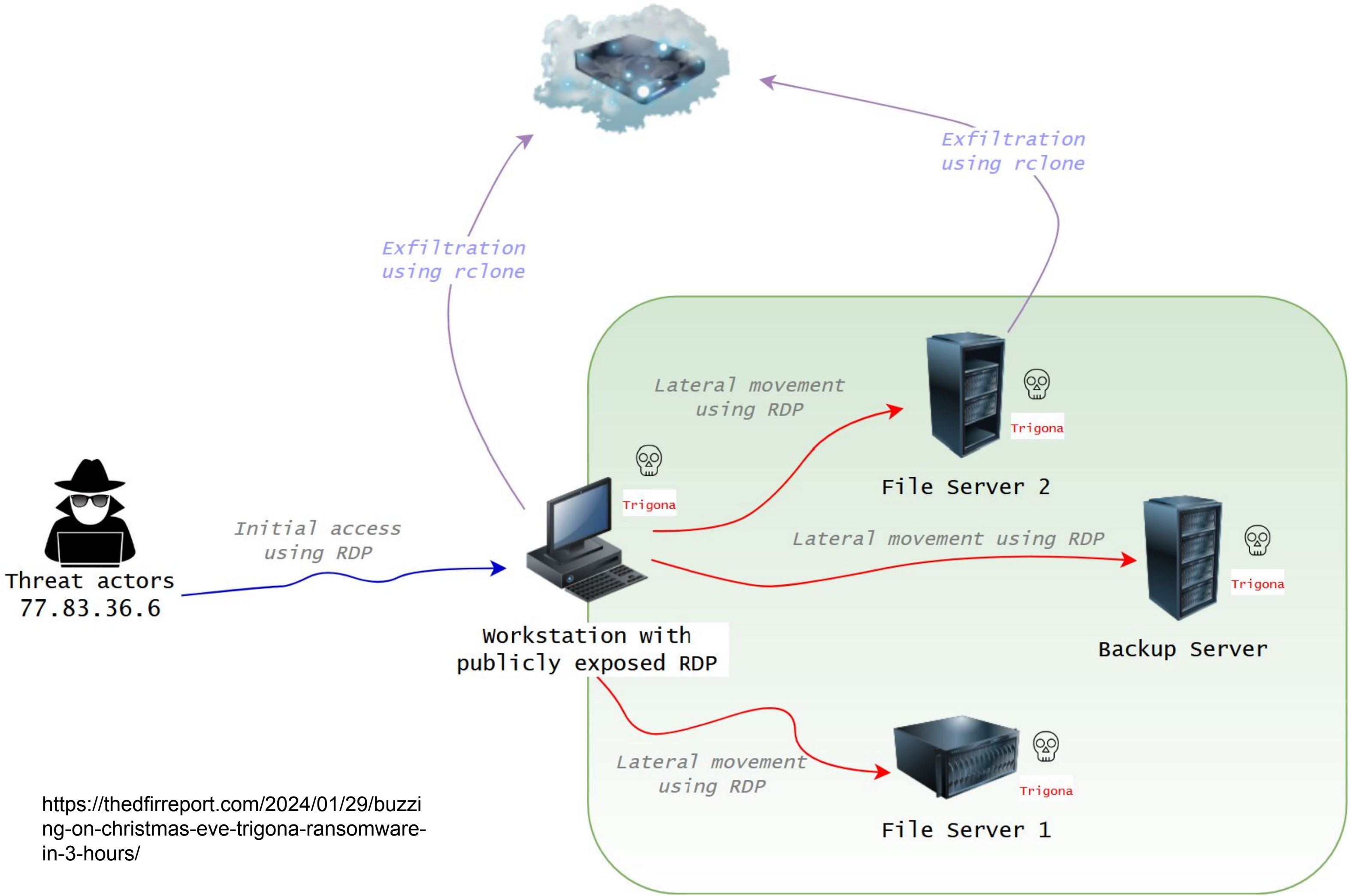
Invoke-Locksmith

SecurIT360 OFFENSIVE SECURITY

the CYBER THREAT PERSPECTIVE Podcast
SecurIT360 OFFENSIVE SECURITY

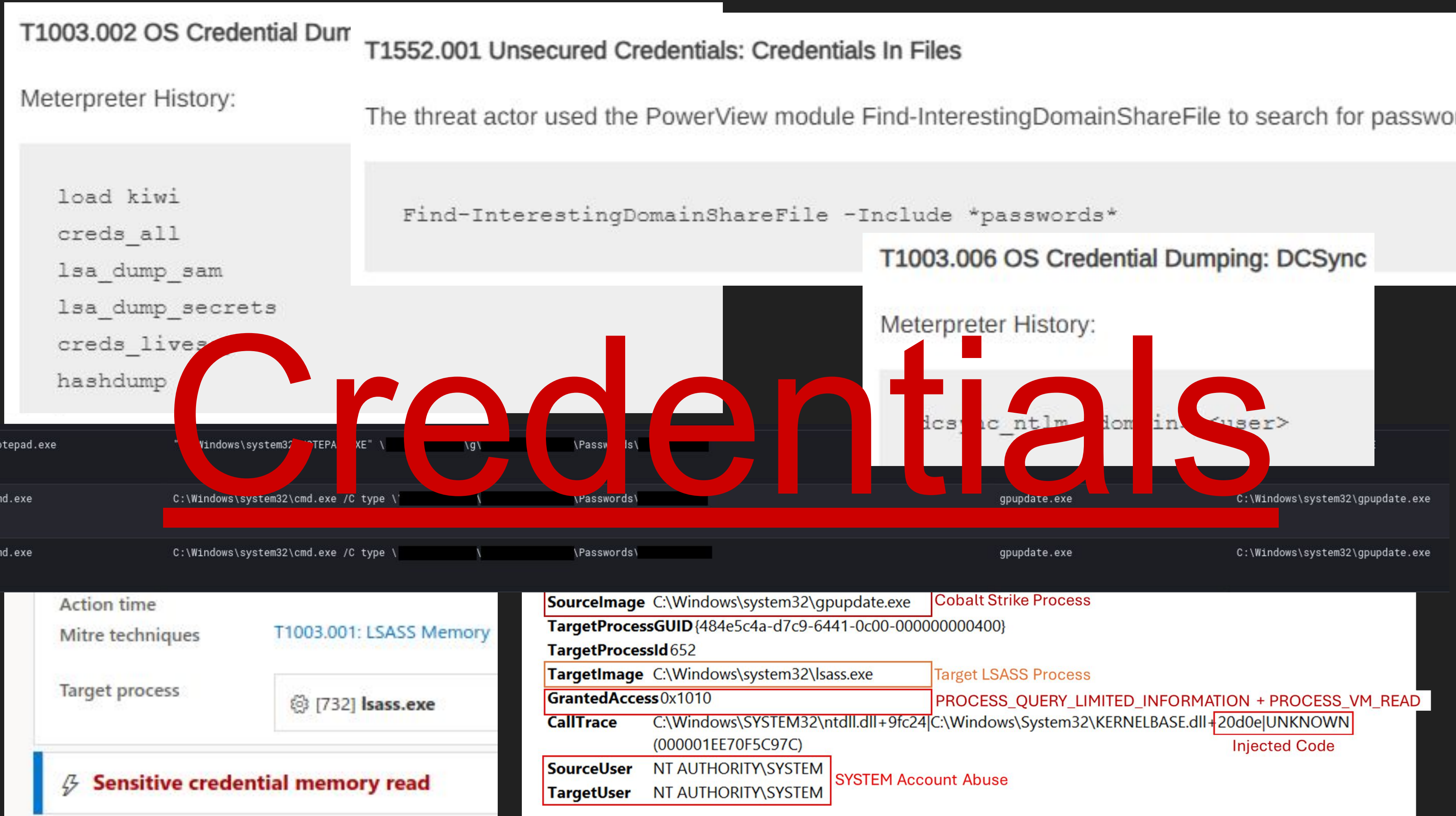
Twitter.com/techspence
Linkedin.com/in/spenceralessi
Youtube.com/@techspence

SecurIT360
The physics of securing IT


Exfiltration using rclone
Exfiltration using rclone
Lateral movement using RDP
Trigona
File Server 2
Trigona
Lateral movement using RDP
Trigona
Threat actors 77.83.36.6
Initial access using RDP
Workstation with publicly exposed RDP
Backup Server
Lateral movement using RDP
Trigona
File Server 1

https://thedfirreport.com/2024/01/29/buzzing-on-christmas-eve-trigona-ransomware-in-3-hours/

Credentials



T1003.002 OS Credential Dum

Meterpreter History:

```
load kiwi
creds_all
lsa_dump_sam
lsa_dump_secrets
creds_lives
hashdump
```

T1552.001 Unsecured Credentials: Credentials In Files

The threat actor used the PowerView module Find-InterestingDomainShareFile to search for passwo

```
Find-InterestingDomainShareFile -Include *passwords*
```

T1003.006 OS Credential Dumping: DCSync

Meterpreter History:

```
dcsync_ntlm <domain> <user>
```

```
notepad.exe     "C:\Windows\system32\NOTEPAD.EXE" \[redacted]\g\[redacted]\Passwords\[redacted]
cmd.exe         C:\Windows\system32\cmd.exe /C type \[redacted]\[redacted]\Passwords\[redacted]     gpupdate.exe     C:\Windows\system32\gpupdate.exe
cmd.exe         C:\Windows\system32\cmd.exe /C type \[redacted]\[redacted]\Passwords\[redacted]     gpupdate.exe     C:\Windows\system32\gpupdate.exe
```

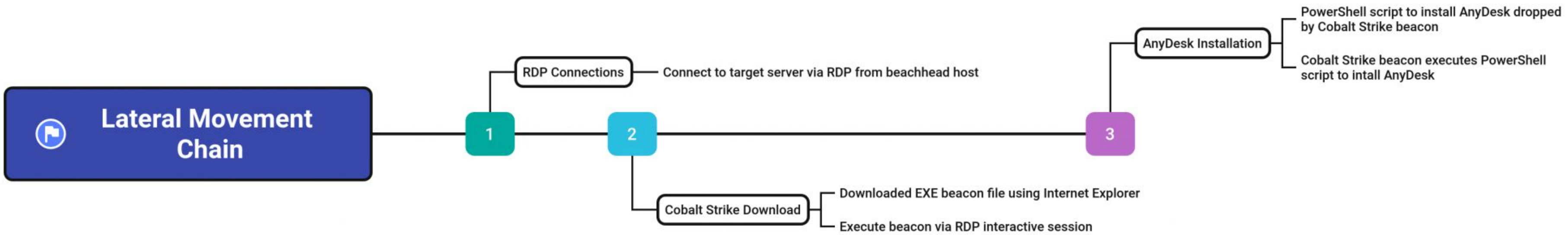
Action time

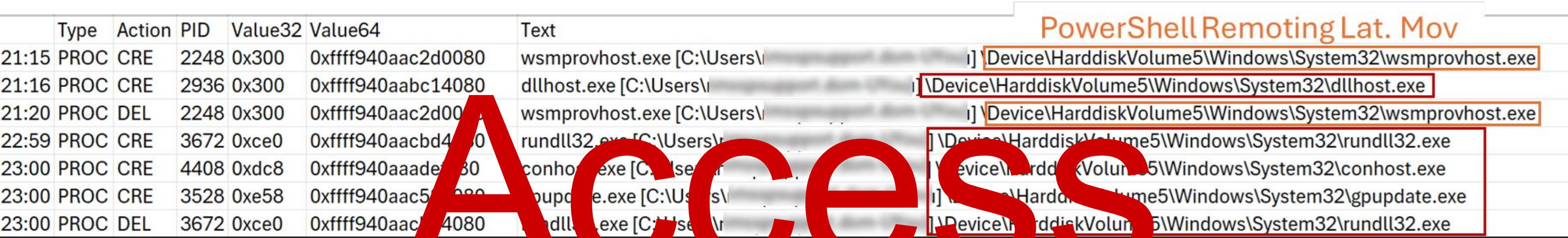
Mitre techniques T1003.001: LSASS Memory

Target process [732] **lsass.exe**

Sensitive credential memory read

```
SourceImage        C:\Windows\system32\gpupdate.exe          Cobalt Strike Process
TargetProcessGUID  {484e5c4a-d7c9-6441-0c00-000000000400}
TargetProcessId    652
TargetImage        C:\Windows\system32\lsass.exe             Target LSASS Process
GrantedAccess      0x1010                                    PROCESS_QUERY_LIMITED_INFORMATION + PROCESS_VM_READ
CallTrace          C:\Windows\SYSTEM32\ntdll.dll+9fc24|C:\Windows\System32\KERNELBASE.dll+20d0e|UNKNOWN
                   (000001EE70F5C97C)                                                        Injected Code
SourceUser         NT AUTHORITY\SYSTEM                       SYSTEM Account Abuse
TargetUser         NT AUTHORITY\SYSTEM
```

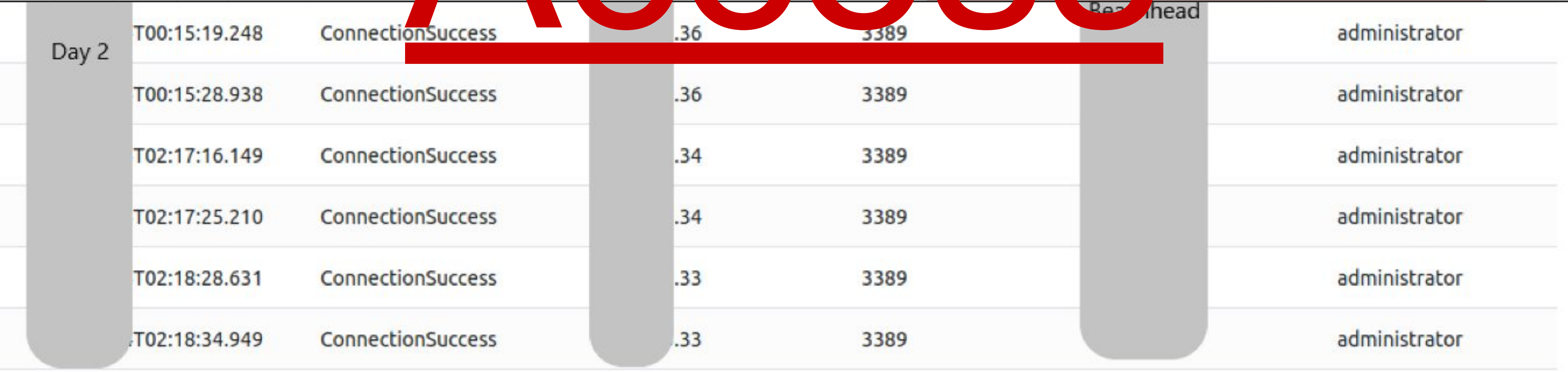

Lateral Movement Chain
1
2
3
RDP Connections
Connect to target server via RDP from beachhead host
Cobalt Strike Download
Downloaded EXE beacon file using Internet Explorer
Execute beacon via RDP interactive session
AnyDesk Installation
PowerShell script to install AnyDesk dropped by Cobalt Strike beacon
Cobalt Strike beacon executes PowerShell script to intall AnyDesk



PowerShell Remoting Lat. Mov

	Type	Action	PID	Value32	Value64	Text
21:15	PROC	CRE	2248	0x300	0xffff940aac2d0080	wsmprovhost.exe [C:\Users\[redacted]] \Device\HarddiskVolume5\Windows\System32\wsmprovhost.exe
21:16	PROC	CRE	2936	0x300	0xffff940aabc14080	dllhost.exe [C:\Users\[redacted]] \Device\HarddiskVolume5\Windows\System32\dllhost.exe
21:20	PROC	DEL	2248	0x300	0xffff940aac2d0080	wsmprovhost.exe [C:\Users\[redacted]] \Device\HarddiskVolume5\Windows\System32\wsmprovhost.exe
22:59	PROC	CRE	3672	0xce0	0xffff940aacbd4080	rundll32.exe [C:\Users\[redacted]] \Device\HarddiskVolume5\Windows\System32\rundll32.exe
23:00	PROC	CRE	4408	0xdc8	0xffff940aaade[illegible]80	conhost.exe [C:\Users\[redacted]] \Device\HarddiskVolume5\Windows\System32\conhost.exe
23:00	PROC	CRE	3528	0xe58	0xffff940aac5[illegible]080	gpupdate.exe [C:\Users\[redacted]] \Device\HarddiskVolume5\Windows\System32\gpupdate.exe
23:00	PROC	DEL	3672	0xce0	0xffff940aacbd4080	rundll32.exe [C:\Users\[redacted]] \Device\HarddiskVolume5\Windows\System32\rundll32.exe

Access



					Beachhead	
Day 2	T00:15:19.248	ConnectionSuccess	[redacted].36	3389	[redacted]	administrator
	T00:15:28.938	ConnectionSuccess	[redacted].36	3389	[redacted]	administrator
	T02:17:16.149	ConnectionSuccess	[redacted].34	3389	[redacted]	administrator
	T02:17:25.210	ConnectionSuccess	[redacted].34	3389	[redacted]	administrator
	T02:18:28.631	ConnectionSuccess	[redacted].33	3389	[redacted]	administrator
	T02:18:34.949	ConnectionSuccess	[redacted].33	3389	[redacted]	administrator

AWSCOLLECTOR.PS1 FEATURES

Run Sharphound

Tool to collect data from domain controllets and domain-joined Windows systems

- https://github.com/BloodHoundAD/BloodHound/raw/master/Ingestors/SharpHound.exe

Clear Windows EventLogs

Part of the script is to clear event logs especially the following channel

- Windows PowerShell
- Application Logs
- Security Logs
- System Logs

Disable AV/EDR

Another feature of the script is to disable known AV tools such as Trend Micro, Cylance, Defender, Symantec, Carbon Black

Send Telegram Updates

Uses Telegram Bot API to send text message to specified Telegram chat.

AWS
POWERSHELL
SCRIPT
S3
BUCKET

Exfiltrate Data to AWS

Performs data exfiltration using AWS S3 bucket

Perform Various Host Discovery & Lateral Movement Activities

Usage of Invoke-WMIExec, Invoke-DCOM for remote execution and lateral movement. TA also runs host discovery commands (OS, memory, hostname, Uptime, drives)

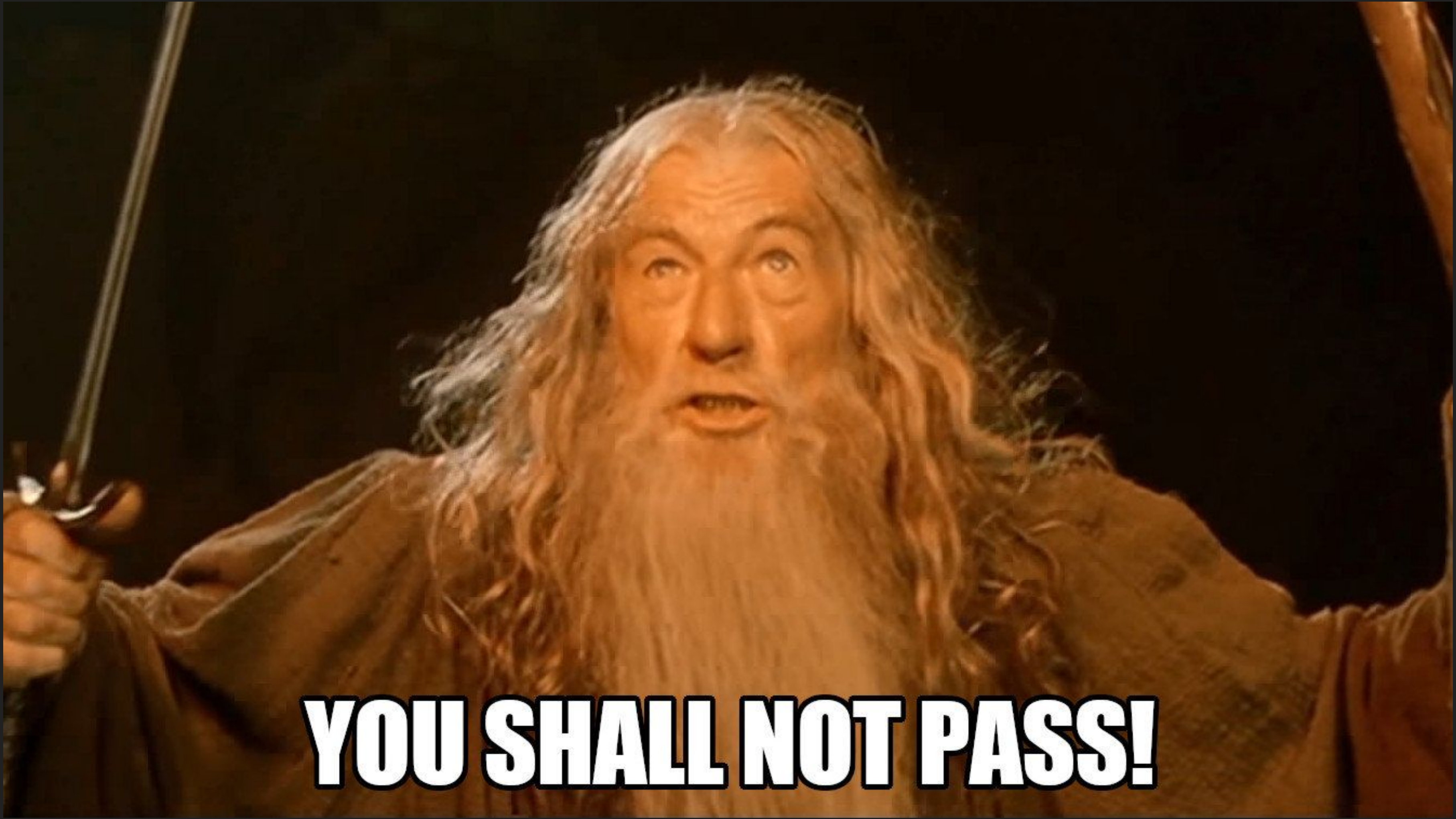
Various Offensive PowerShell Tools

Tools such as:

- Invoke-AmsiBypass.ps1
- WmiExec.ps1
- Invoke-DCOM.ps1

Deploy Dagon Locker Ransomware

Deployment of Dagon locker ransomware, including the option to also deploy some of the known ones such as Mount, REvil, Quantum, etc.



YOU SHALL NOT PASS!

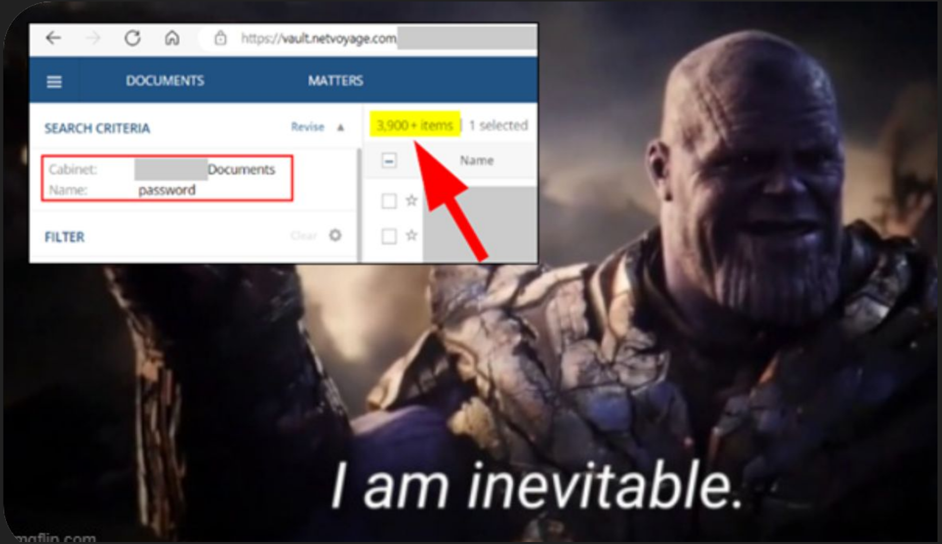
The Game Plan

1. Identify: Misconfigurations
2. Implement: AD Security 101
3. Implement: AD Security 201
4. Repeat

Identify: Misconfigurations

Misconfiguration: Credentials

- Unsecured Creds
- Password reuse
- Kerberoastable admin accounts

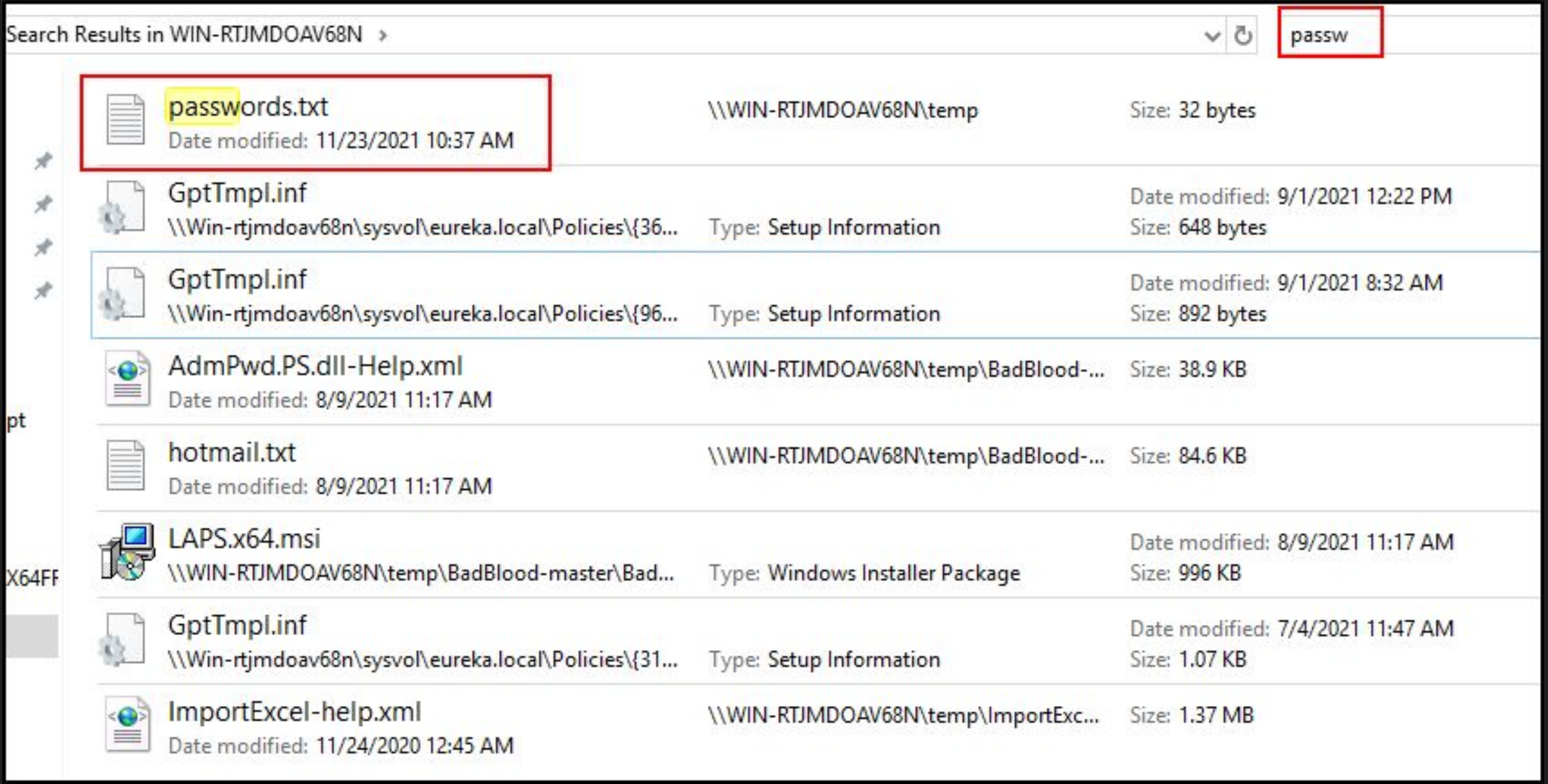


https://vault.netvoyage.com[redacted]

Cabinet: [redacted] Documents
Name: password

3,900+ items | 1 selected

Unsecured Credentials: Easy Mode



Search Results in WIN-RTJMDOAV68N ›

passw

passwords.txt
Date modified: 11/23/2021 10:37 AM
\\WIN-RTJMDOAV68N\temp
Size: 32 bytes

GptTmpl.inf
\\Win-rtjmdoav68n\sysvol\eureka.local\Policies\{36...
Type: Setup Information
Date modified: 9/1/2021 12:22 PM
Size: 648 bytes

GptTmpl.inf
\\Win-rtjmdoav68n\sysvol\eureka.local\Policies\{96...
Type: Setup Information
Date modified: 9/1/2021 8:32 AM
Size: 892 bytes

AdmPwd.PS.dll-Help.xml
Date modified: 8/9/2021 11:17 AM
\\WIN-RTJMDOAV68N\temp\BadBlood-...
Size: 38.9 KB

hotmail.txt
Date modified: 8/9/2021 11:17 AM
\\WIN-RTJMDOAV68N\temp\BadBlood-...
Size: 84.6 KB

LAPS.x64.msi
\\WIN-RTJMDOAV68N\temp\BadBlood-master\Bad...
Type: Windows Installer Package
Date modified: 8/9/2021 11:17 AM
Size: 996 KB

GptTmpl.inf
\\Win-rtjmdoav68n\sysvol\eureka.local\Policies\{31...
Type: Setup Information
Date modified: 7/4/2021 11:47 AM
Size: 1.07 KB

ImportExcel-help.xml
Date modified: 11/24/2020 12:45 AM
\\WIN-RTJMDOAV68N\temp\ImportExc...
Size: 1.37 MB

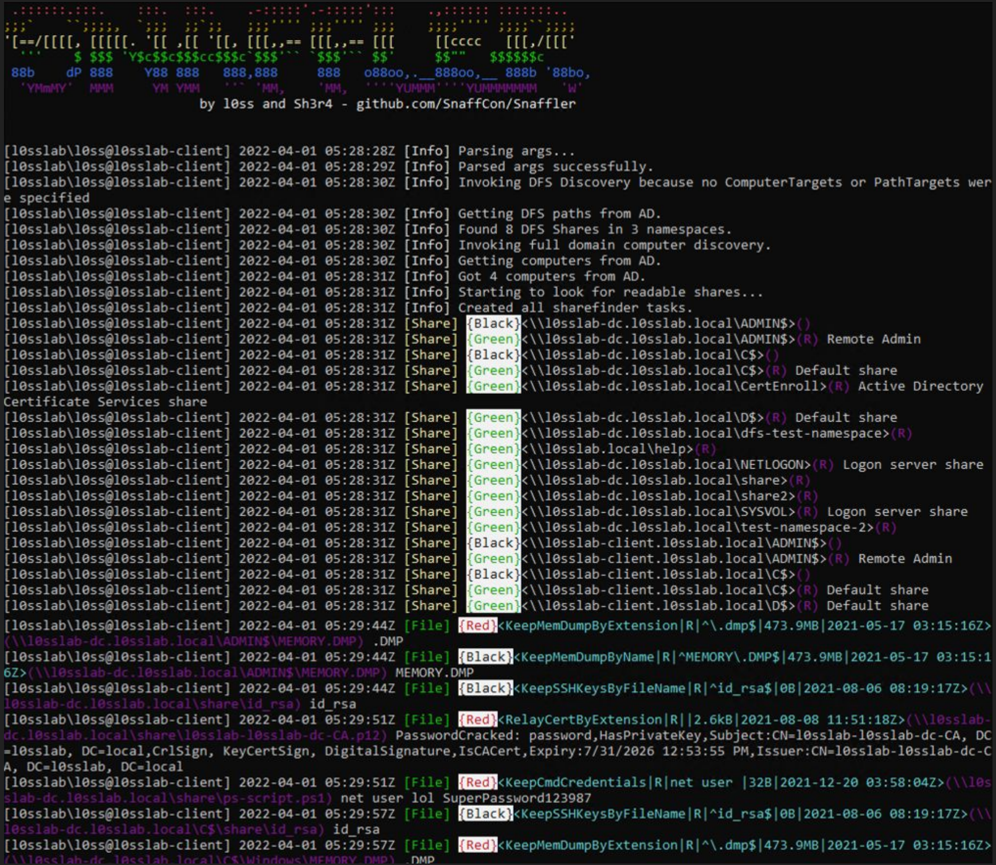
pt

X64FF

https://offsec.blog/3-easy-wins-for-defenders-from-a-pentesters-point-of-view/

Unsecured Credentials: Hard Mode

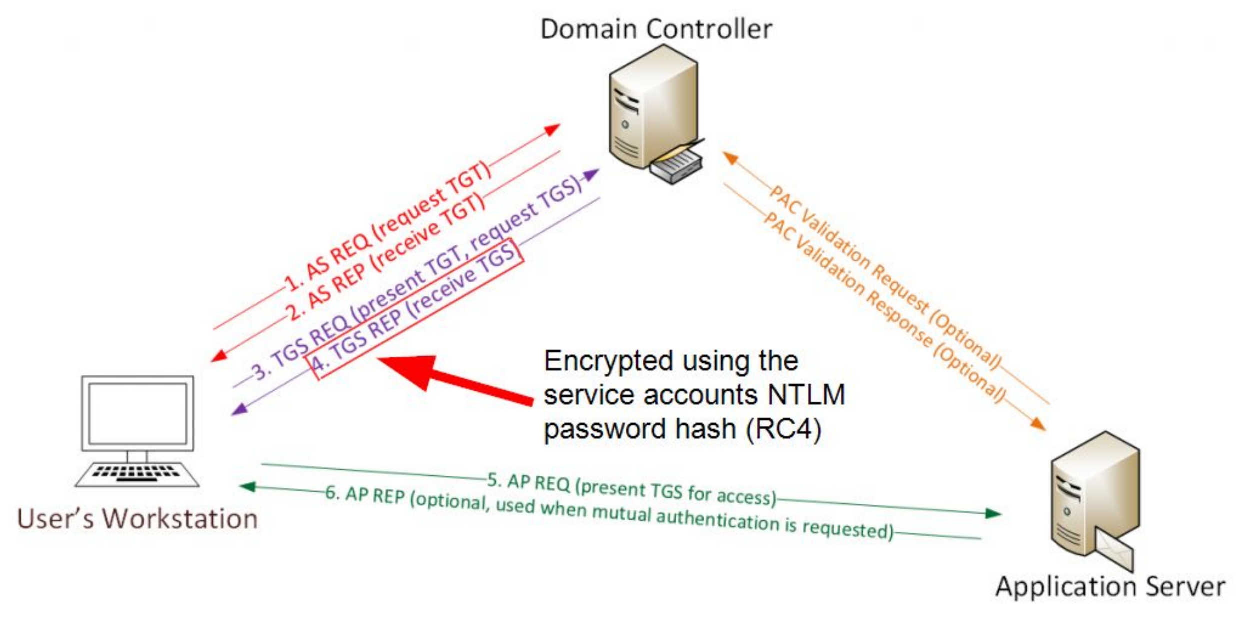
Read the README!



```
 .::::::.:::.    :::.  :::.    .-:::::'.-:::::':::      .,:::::: :::::::..
;;;`    ``;;;;,  `;;;  ;;`;;   ;;;'''' ;;;'''' ;;;      ;;;;'''' ;;;;``;;;;
'[==/[[[[, [[[[[. '[[ ,[[ '[[, [[[,,== [[[,,== [[[       [[cccc   [[[,/[[['
  '''    $ $$$ 'Y$c$$c$$$cc$$$c`$$$'`` `$$$'`` $$'       $$""   $$$$$$c
 88b    dP 888    Y88 888   888,888     888   o88oo,.__888oo,__ 888b '88bo,
  'YMmMY'  MMM     YM YMM   ''` 'MM,     'MM,  ''''YUMMM''''YUMMMMMMM   'W'
                                by l0ss and Sh3r4 - github.com/SnaffCon/Snaffler


[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:28Z [Info] Parsing args...
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:29Z [Info] Parsed args successfully.
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:30Z [Info] Invoking DFS Discovery because no ComputerTargets or PathTargets wer
e specified
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:30Z [Info] Getting DFS paths from AD.
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:30Z [Info] Found 8 DFS Shares in 3 namespaces.
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:30Z [Info] Invoking full domain computer discovery.
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:30Z [Info] Getting computers from AD.
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Info] Got 4 computers from AD.
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Info] Starting to look for readable shares...
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Info] Created all sharefinder tasks.
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Black}<\\l0sslab-dc.l0sslab.local\ADMIN$>()
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-dc.l0sslab.local\ADMIN$>(R) Remote Admin
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Black}<\\l0sslab-dc.l0sslab.local\C$>()
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-dc.l0sslab.local\C$>(R) Default share
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-dc.l0sslab.local\CertEnroll>(R) Active Directory
Certificate Services share
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-dc.l0sslab.local\D$>(R) Default share
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-dc.l0sslab.local\dfs-test-namespace>(R)
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab.local\help>(R)
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-dc.l0sslab.local\NETLOGON>(R) Logon server share
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-dc.l0sslab.local\share>(R)
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-dc.l0sslab.local\share2>(R)
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-dc.l0sslab.local\SYSVOL>(R) Logon server share
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-dc.l0sslab.local\test-namespace-2>(R)
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Black}<\\l0sslab-client.l0sslab.local\ADMIN$>()
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-client.l0sslab.local\ADMIN$>(R) Remote Admin
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Black}<\\l0sslab-client.l0sslab.local\C$>()
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-client.l0sslab.local\C$>(R) Default share
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:28:31Z [Share] {Green}<\\l0sslab-client.l0sslab.local\D$>(R) Default share
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:29:44Z [File] {Red}<KeepMemDumpByExtension|R|^\.dmp$|473.9MB|2021-05-17 03:15:16Z>
(\\l0sslab-dc.l0sslab.local\ADMIN$\MEMORY.DMP) .DMP
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:29:44Z [File] {Black}<KeepMemDumpByName|R|^MEMORY\.DMP$|473.9MB|2021-05-17 03:15:1
6Z>(\\l0sslab-dc.l0sslab.local\ADMIN$\MEMORY.DMP) MEMORY.DMP
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:29:44Z [File] {Black}<KeepSSHKeysByFileName|R|^id_rsa$|0B|2021-08-06 08:19:17Z>(\\
l0sslab-dc.l0sslab.local\share\id_rsa) id_rsa
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:29:51Z [File] {Red}<RelayCertByExtension|R||2.6kB|2021-08-08 11:51:18Z>(\\l0sslab-
dc.l0sslab.local\share\l0sslab-l0sslab-dc-CA.p12) PasswordCracked: password,HasPrivateKey,Subject:CN=l0sslab-l0sslab-dc-CA, DC
=l0sslab, DC=local,CrlSign, KeyCertSign, DigitalSignature,IsCACert,Expiry:7/31/2026 12:53:55 PM,Issuer:CN=l0sslab-l0sslab-dc-C
A, DC=l0sslab, DC=local
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:29:51Z [File] {Red}<KeepCmdCredentials|R|net user |32B|2021-12-20 03:58:04Z>(\\l0s
slab-dc.l0sslab.local\share\ps-script.ps1) net user lol SuperPassword123987
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:29:57Z [File] {Black}<KeepSSHKeysByFileName|R|^id_rsa$|0B|2021-08-06 08:19:17Z>(\\
l0sslab-dc.l0sslab.local\C$\share\id_rsa) id_rsa
[l0sslab\l0ss@l0sslab-client] 2022-04-01 05:29:57Z [File] {Red}<KeepMemDumpByExtension|R|^\.dmp$|473.9MB|2021-05-17 03:15:16Z>
(\\l0sslab-dc.l0sslab.local\C$\Windows\MEMORY.DMP) .DMP
```

https://github.com/SnaffCon/Snaffler

Kerberoastable Admin Accounts

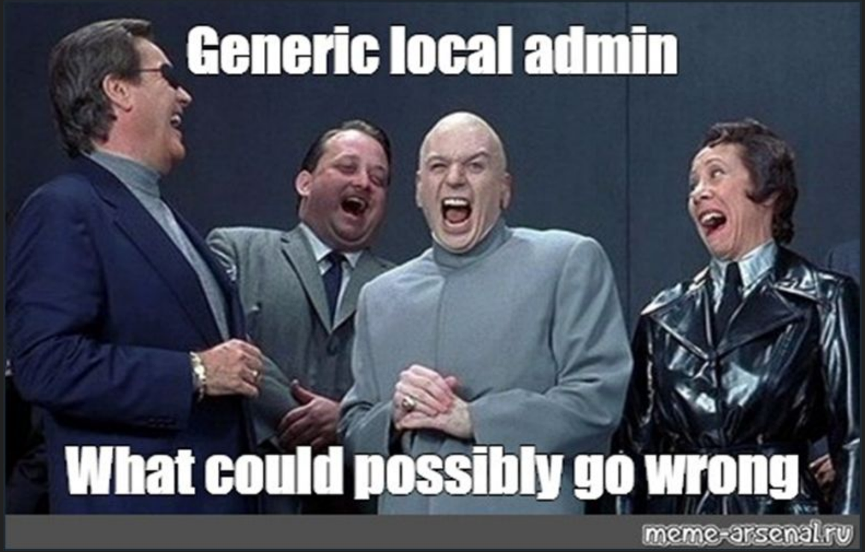

Domain Controller
1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
Encrypted using the service accounts NTLM password hash (RC4)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

```
Import-Module ActiveDirectory
Get-ADUser -Filter { ServicePrincipalName -like "*" } -Property *
```

Detecting Kerberoasting Activity – Active Directory Security (adsecurity.org)

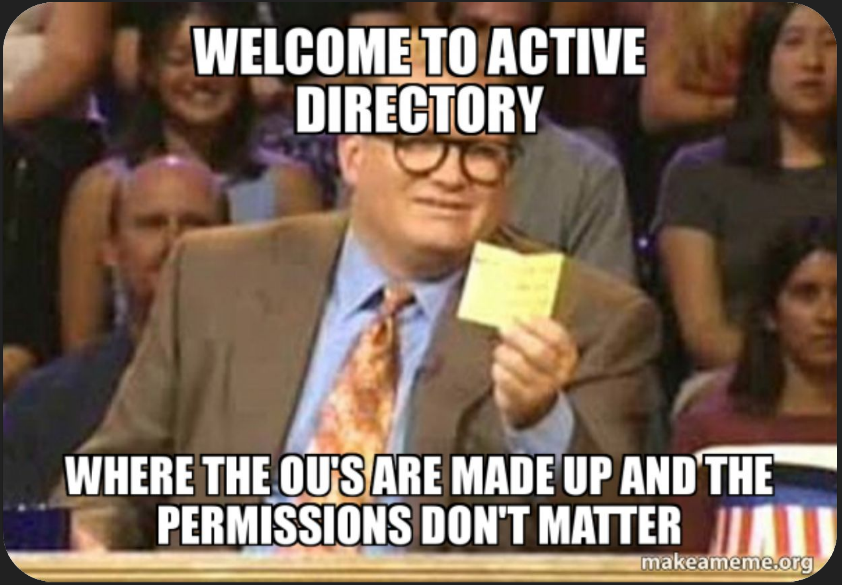
Misconfiguration: Access

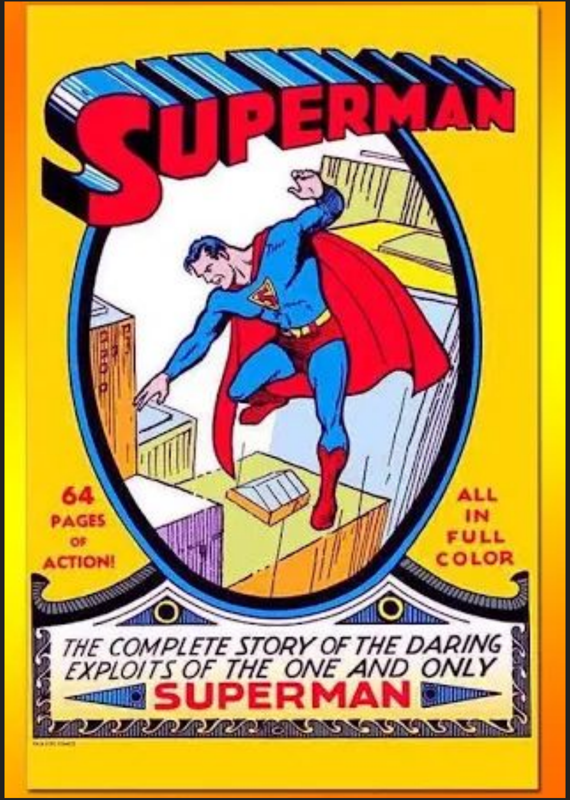
- Lack of separation of privileged accounts
- Overly permissive ACLs
- Insecure delegations

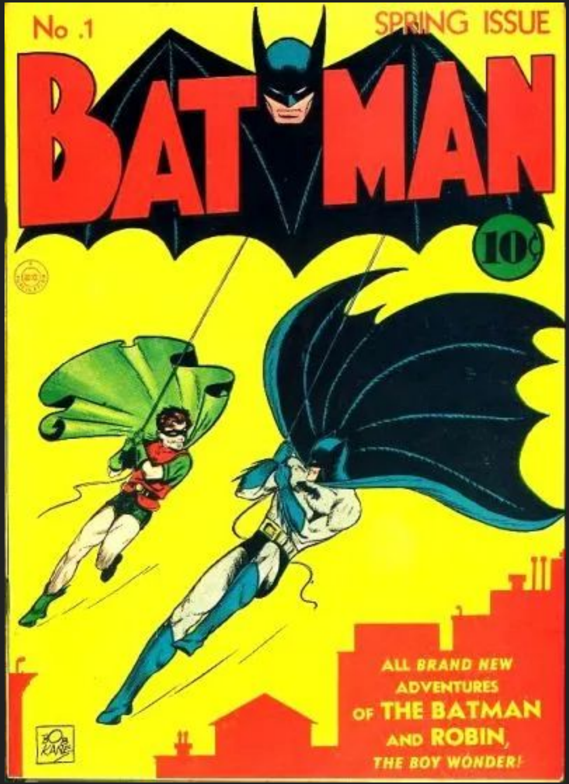


Misconfiguration: Control

- Nested security groups
- Misconfigured GPOs/Logon scripts
- Misconfigured auth (spooler, llmnr, adcs)


WELCOME TO ACTIVE DIRECTORY
WHERE THE OU'S ARE MADE UP AND THE PERMISSIONS DON'T MATTER
makeameme.org


SUPERMAN
64 PAGES OF ACTION!
ALL IN FULL COLOR
THE COMPLETE STORY OF THE DARING EXPLOITS OF THE ONE AND ONLY
SUPERMAN


No.1
SPRING ISSUE
BATMAN
10¢
ALL BRAND NEW ADVENTURES OF THE BATMAN AND ROBIN, THE BOY WONDER!
BOB KANE

NO.1-JAN.
FLASH Comics
10¢
LIGHTNING FAST ACTION, MYSTERY, and ADVENTURE!
Introducing THE FLASH... Fastest man alive!
THE HAWKMAN
OOP!
WHAM!
JOHNNY THUNDER
THE WHIP
CLIFF CORNWALL

Finding Misconfigurations: The Fabulous Four

1. ScriptSentry (Free)

   https://offsec.blog/hidden-menace-how-to-identify-misconfigured-and-dangerous-logon-scripts/

2. ADeleginator (Free)

   https://www.linkedin.com/pulse/adeleg-active-directory-security-tool-youve-never-heard-alessi-lvqze/

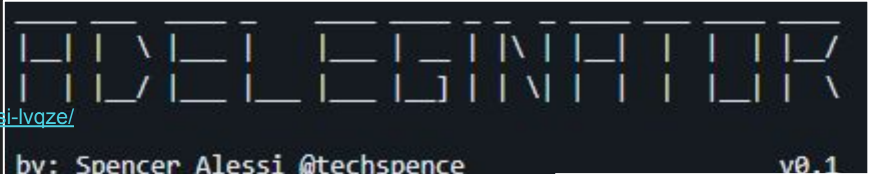
3. Locksmith (Free)

   https://github.com/TrimarcJake/Locksmith

4. PingCastle (Free)

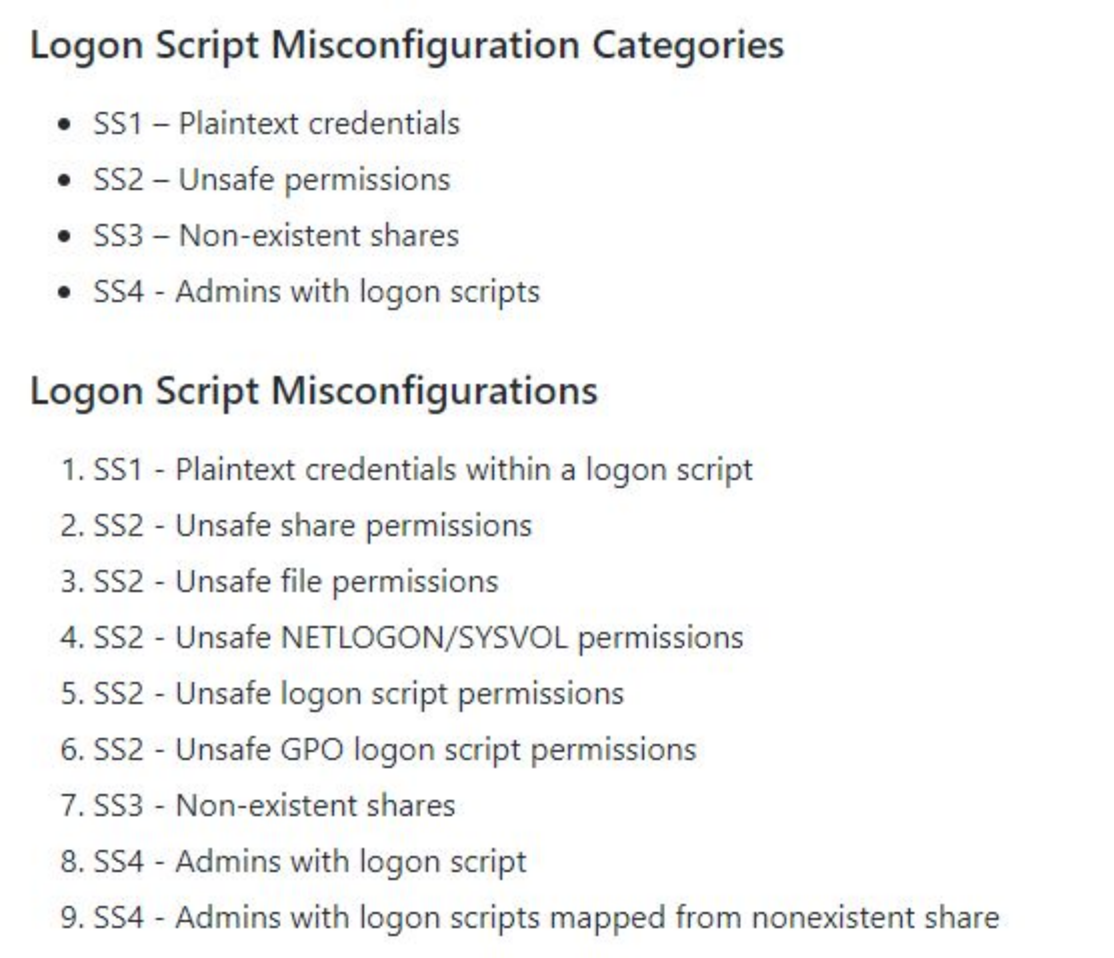
   https://pingcastle.com

```
by: Spencer Alessi @techspence
v0.5

Setting phasers to stun, please wait..
```



```
by: Spencer Alessi @techspence                         v0.1
```

```
\==--O___      PingCastle (Version 3.1.0.0     8/03/20
 \  / \  "">   Get Active Directory Security at 80% in
  \/   \ ,'    End of support: 7/31/2024
   O"---O
    \ ,'       Vincent LE TOUX (contact@pingcastle.com
     v         twitter: @mysmartlogon        https://ww
```



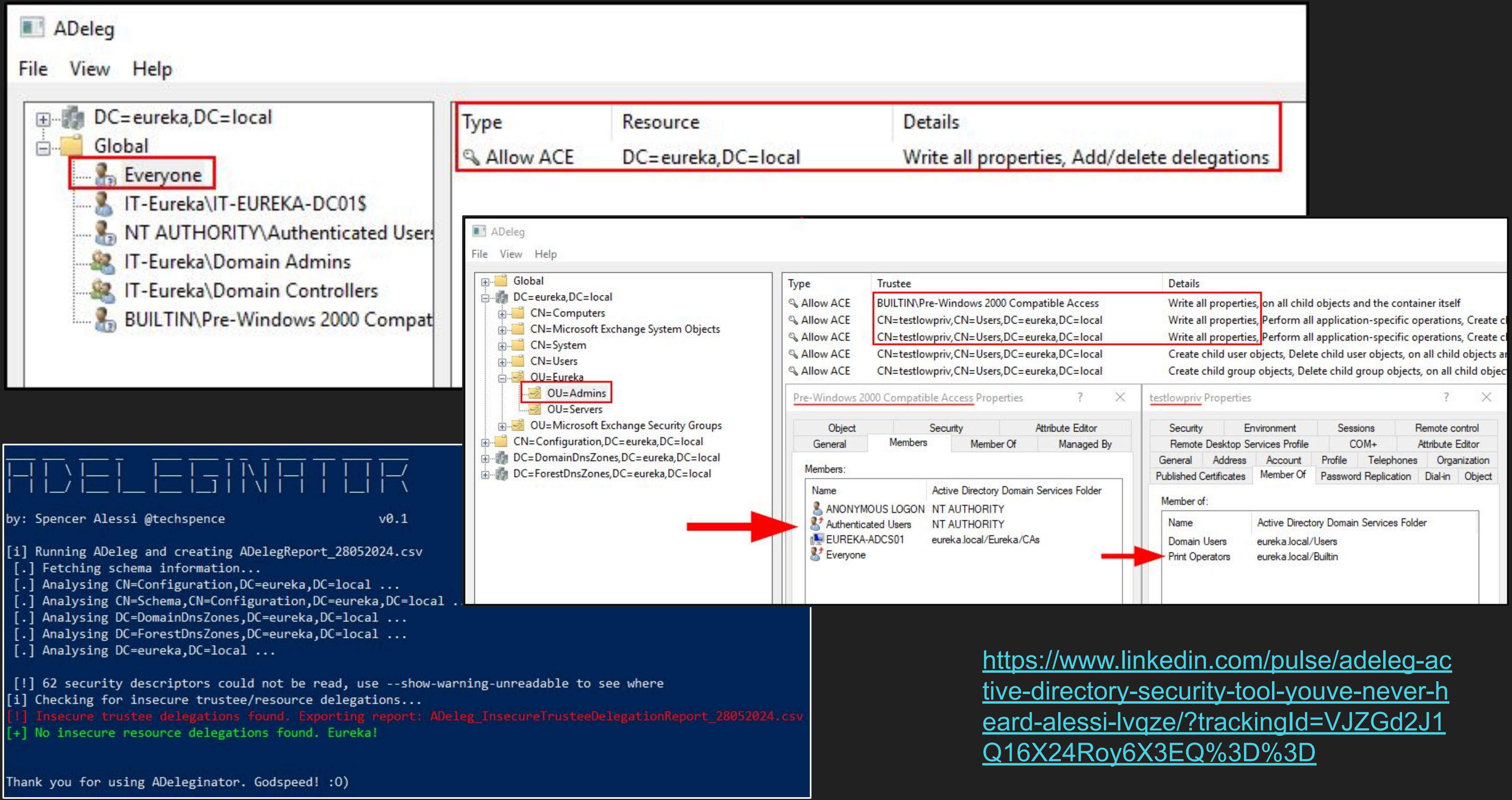
Logon Script Misconfiguration Categories

- SS1 – Plaintext credentials
- SS2 – Unsafe permissions
- SS3 – Non-existent shares
- SS4 - Admins with logon scripts

Logon Script Misconfigurations

1. SS1 - Plaintext credentials within a logon script
2. SS2 - Unsafe share permissions
3. SS2 - Unsafe file permissions
4. SS2 - Unsafe NETLOGON/SYSVOL permissions
5. SS2 - Unsafe logon script permissions
6. SS2 - Unsafe GPO logon script permissions
7. SS3 - Non-existent shares
8. SS4 - Admins with logon script
9. SS4 - Admins with logon scripts mapped from nonexistent share

https://github.com/techspence/ScriptSentry



DC=eureka,DC=local
Global
- Everyone
- IT-Eureka\IT-EUREKA-DC01$
- NT AUTHORITY\Authenticated Users
- IT-Eureka\Domain Admins
- IT-Eureka\Domain Controllers
- BUILTIN\Pre-Windows 2000 Compat

Type	Resource	Details
Allow ACE	DC=eureka,DC=local	Write all properties, Add/delete delegations

Global
DC=eureka,DC=local
- CN=Computers
- CN=Microsoft Exchange System Objects
- CN=System
- CN=Users
- OU=Eureka
  - OU=Admins
  - OU=Servers
- OU=Microsoft Exchange Security Groups

CN=Configuration,DC=eureka,DC=local
DC=DomainDnsZones,DC=eureka,DC=local
DC=ForestDnsZones,DC=eureka,DC=local

Type	Trustee	Details
Allow ACE	BUILTIN\Pre-Windows 2000 Compatible Access	Write all properties, on all child objects and the container itself
Allow ACE	CN=testlowpriv,CN=Users,DC=eureka,DC=local	Write all properties, Perform all application-specific operations, Create c
Allow ACE	CN=testlowpriv,CN=Users,DC=eureka,DC=local	Write all properties, Perform all application-specific operations, Create c
Allow ACE	CN=testlowpriv,CN=Users,DC=eureka,DC=local	Create child user objects, Delete child user objects, on all child objects a
Allow ACE	CN=testlowpriv,CN=Users,DC=eureka,DC=local	Create child group objects, Delete child group objects, on all child objec

Pre-Windows 2000 Compatible Access Properties

Object Security Attribute Editor
General Members Member Of Managed By

Members:

Name	Active Directory Domain Services Folder
ANONYMOUS LOGON	NT AUTHORITY
Authenticated Users	NT AUTHORITY
EUREKA-ADCS01	eureka.local/Eureka/CAs
Everyone	

testlowpriv Properties

Security Environment Sessions Remote control
Remote Desktop Services Profile COM+ Attribute Editor
General Address Account Profile Telephones Organization
Published Certificates Member Of Password Replication Dial-in Object

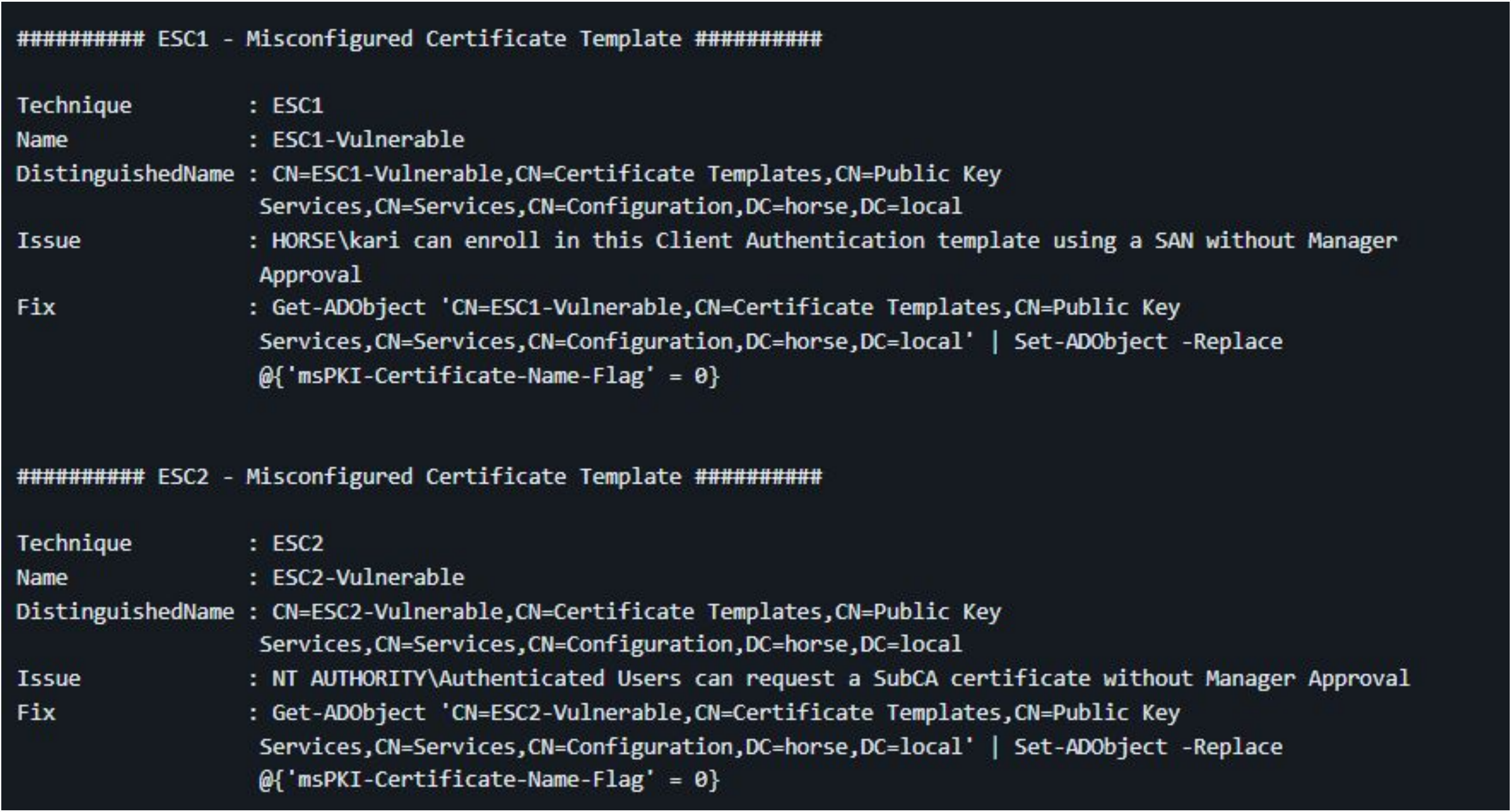
Member of:

Name	Active Directory Domain Services Folder
Domain Users	eureka.local/Users
Print Operators	eureka.local/Builtin

```
by: Spencer Alessi @techspence                     v0.1

[i] Running ADeleg and creating ADelegReport_28052024.csv
 [.] Fetching schema information...
 [.] Analysing CN=Configuration,DC=eureka,DC=local ...
 [.] Analysing CN=Schema,CN=Configuration,DC=eureka,DC=local ..
 [.] Analysing DC=DomainDnsZones,DC=eureka,DC=local ...
 [.] Analysing DC=ForestDnsZones,DC=eureka,DC=local ...
 [.] Analysing DC=eureka,DC=local ...

 [!] 62 security descriptors could not be read, use --show-warning-unreadable to see where
[i] Checking for insecure trustee/resource delegations...
[!] Insecure trustee delegations found. Exporting report: ADeleg_InsecureTrusteeDelegationReport_28052024.csv
[+] No insecure resource delegations found. Eureka!


Thank you for using ADeleginator. Godspeed! :O)
```

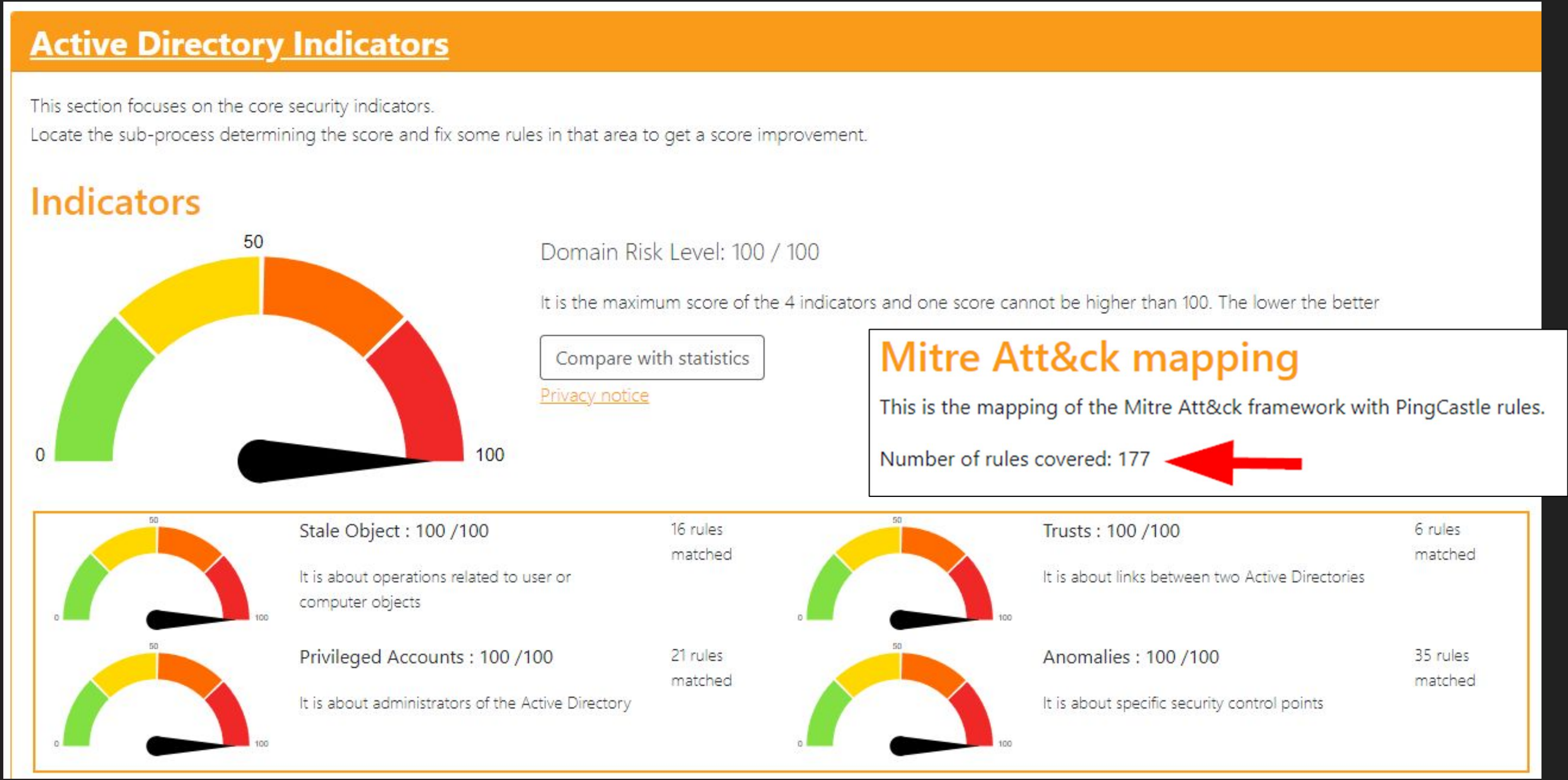
https://www.linkedin.com/pulse/adeleg-active-directory-security-tool-youve-never-heard-alessi-lvqze/?trackingId=VJZGd2J1Q16X24Roy6X3EQ%3D%3D

https://github.com/techspence/ADeleginator



```
########## ESC1 - Misconfigured Certificate Template ##########

Technique         : ESC1
Name              : ESC1-Vulnerable
DistinguishedName : CN=ESC1-Vulnerable,CN=Certificate Templates,CN=Public Key
                    Services,CN=Services,CN=Configuration,DC=horse,DC=local
Issue             : HORSE\kari can enroll in this Client Authentication template using a SAN without Manager
                    Approval
Fix               : Get-ADObject 'CN=ESC1-Vulnerable,CN=Certificate Templates,CN=Public Key
                    Services,CN=Services,CN=Configuration,DC=horse,DC=local' | Set-ADObject -Replace
                    @{'msPKI-Certificate-Name-Flag' = 0}



########## ESC2 - Misconfigured Certificate Template ##########

Technique         : ESC2
Name              : ESC2-Vulnerable
DistinguishedName : CN=ESC2-Vulnerable,CN=Certificate Templates,CN=Public Key
                    Services,CN=Services,CN=Configuration,DC=horse,DC=local
Issue             : NT AUTHORITY\Authenticated Users can request a SubCA certificate without Manager Approval
Fix               : Get-ADObject 'CN=ESC2-Vulnerable,CN=Certificate Templates,CN=Public Key
                    Services,CN=Services,CN=Configuration,DC=horse,DC=local' | Set-ADObject -Replace
                    @{'msPKI-Certificate-Name-Flag' = 0}
```

https://github.com/trimarcjake/Locksmith



Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators

Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics

Privacy notice

Mitre Att&ck mapping

This is the mapping of the Mitre Att&ck framework with PingCastle rules.

Number of rules covered: 177

Stale Object : 100 /100 — 16 rules matched

It is about operations related to user or computer objects

Trusts : 100 /100 — 6 rules matched

It is about links between two Active Directories

Privileged Accounts : 100 /100 — 21 rules matched

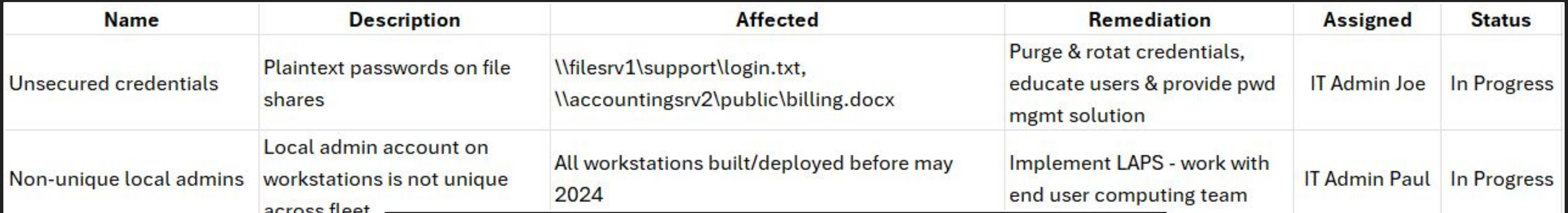
It is about administrators of the Active Directory

Anomalies : 100 /100 — 35 rules matched

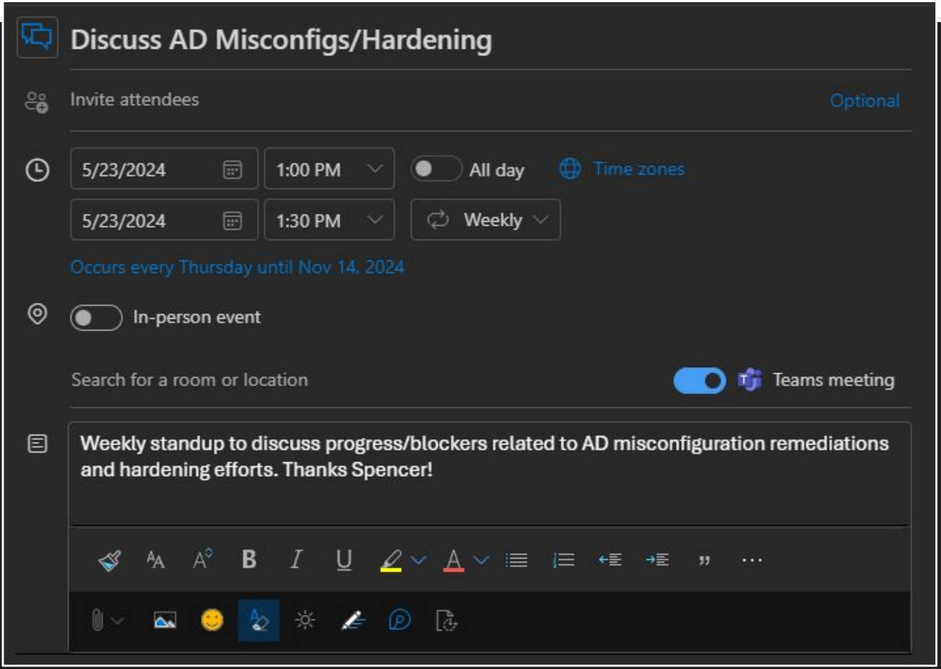
It is about specific security control points

https://pingcastle.com

Misconfiguration: Risk Register Example



Name	Description	Affected	Remediation	Assigned	Status
Unsecured credentials	Plaintext passwords on file shares	\\filesrv1\support\login.txt, \\accountingsrv2\public\billing.docx	Purge & rotat credentials, educate users & provide pwd mgmt solution	IT Admin Joe	In Progress
Non-unique local admins	Local admin account on workstations is not unique across fleet	All workstations built/deployed before may 2024	Implement LAPS - work with end user computing team	IT Admin Paul	In Progress



Discuss AD Misconfigs/Hardening

Invite attendees

5/23/2024 1:00 PM

5/23/2024 1:30 PM

All day: off

Weekly

Occurs every Thursday until Nov 14, 2024

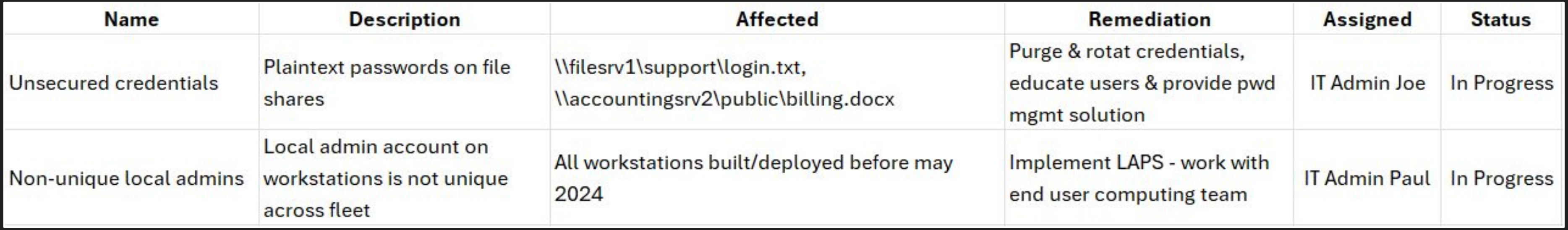
In-person event: off

Search for a room or location

Teams meeting: on

Weekly standup to discuss progress/blockers related to AD misconfiguration remediations and hardening efforts. Thanks Spencer!

Misconfiguration: Risk Register Example



Name	Description	Affected	Remediation	Assigned	Status
Unsecured credentials	Plaintext passwords on file shares	\\filesrv1\support\login.txt, \\accountingsrv2\public\billing.docx	Purge & rotat credentials, educate users & provide pwd mgmt solution	IT Admin Joe	In Progress
Non-unique local admins	Local admin account on workstations is not unique across fleet	All workstations built/deployed before may 2024	Implement LAPS - work with end user computing team	IT Admin Paul	In Progress

Credentials....Access....Control

Implement: AD Security 101

We can't afford another data breach!
XDR
AI
Clean up our shares
imgflip.com

AD Security 101: Credentials

- Cleanup shares/ sharepoint/dms/wiki
- LAPS everywhere
- Password cleanup
- Disable RC4/Prune SPNs

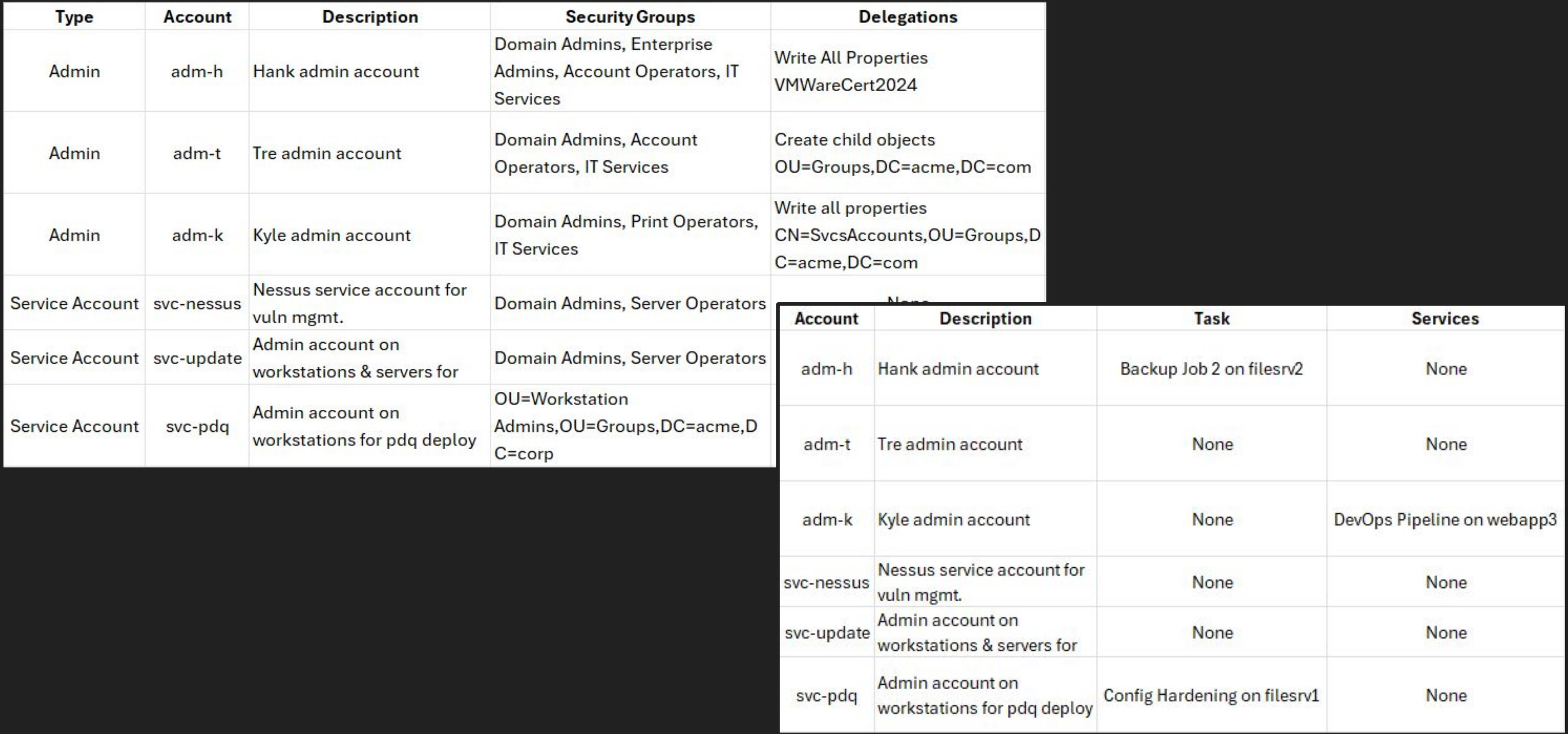
AD Security 101: Access

Document!

- Admin & service accounts
  - Group membership
  - Delegations
  - Tasks
  - Services

- Shares/sharepoint/dms/wiki/etc
  - Current access, desired access

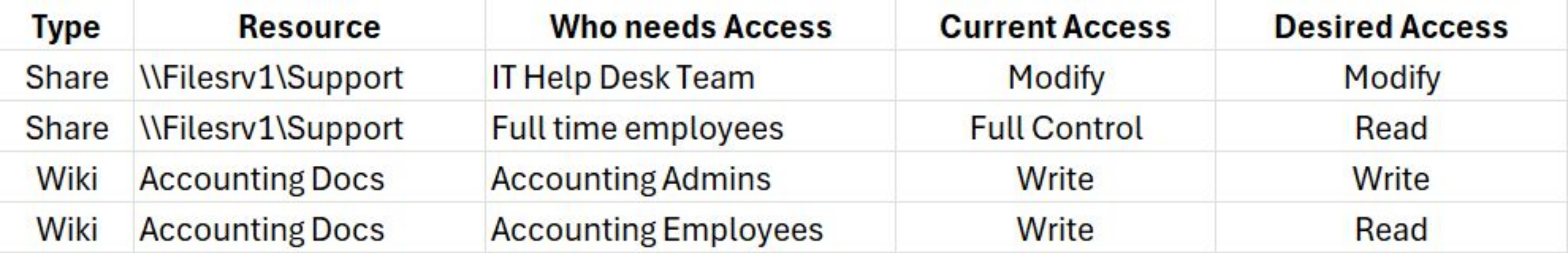
AD Security 101: Admin/Svcs Account Documenting Example



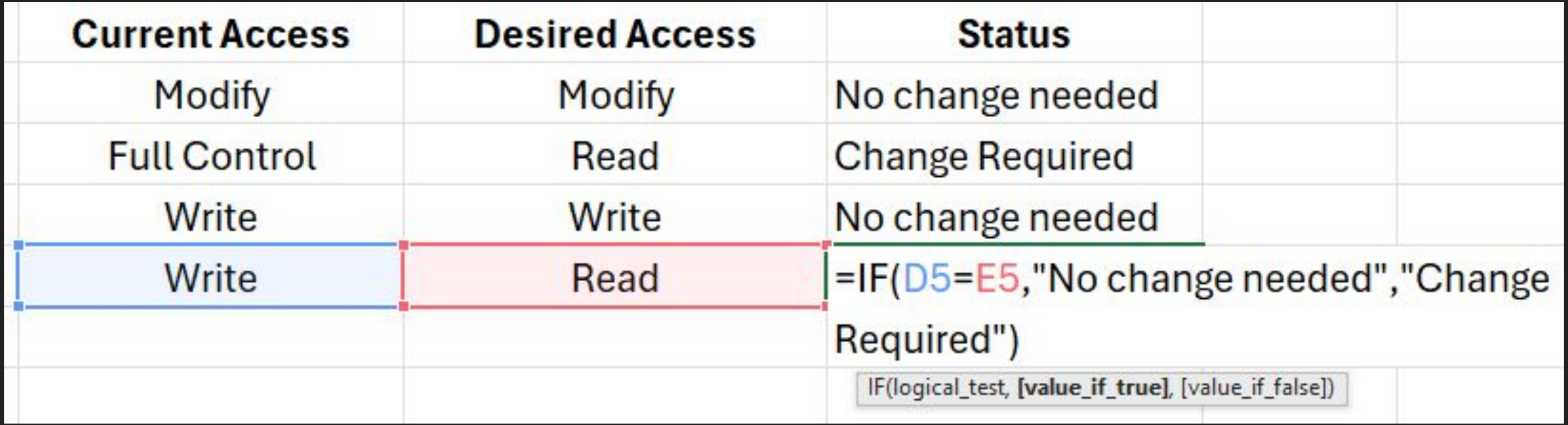
Type	Account	Description	Security Groups	Delegations
Admin	adm-h	Hank admin account	Domain Admins, Enterprise Admins, Account Operators, IT Services	Write All Properties VMWareCert2024
Admin	adm-t	Tre admin account	Domain Admins, Account Operators, IT Services	Create child objects OU=Groups,DC=acme,DC=com
Admin	adm-k	Kyle admin account	Domain Admins, Print Operators, IT Services	Write all properties CN=SvcsAccounts,OU=Groups,DC=acme,DC=com
Service Account	svc-nessus	Nessus service account for vuln mgmt.	Domain Admins, Server Operators	None
Service Account	svc-update	Admin account on workstations & servers for	Domain Admins, Server Operators	
Service Account	svc-pdq	Admin account on workstations for pdq deploy	OU=Workstation Admins,OU=Groups,DC=acme,DC=corp	

Account	Description	Task	Services
adm-h	Hank admin account	Backup Job 2 on filesrv2	None
adm-t	Tre admin account	None	None
adm-k	Kyle admin account	None	DevOps Pipeline on webapp3
svc-nessus	Nessus service account for vuln mgmt.	None	None
svc-update	Admin account on workstations & servers for	None	None
svc-pdq	Admin account on workstations for pdq deploy	Config Hardening on filesrv1	None

AD Security 101: Resource Access Documenting Example



Type	Resource	Who needs Access	Current Access	Desired Access
Share	\\Filesrv1\Support	IT Help Desk Team	Modify	Modify
Share	\\Filesrv1\Support	Full time employees	Full Control	Read
Wiki	Accounting Docs	Accounting Admins	Write	Write
Wiki	Accounting Docs	Accounting Employees	Write	Read



Current Access	Desired Access	Status
Modify	Modify	No change needed
Full Control	Read	Change Required
Write	Write	No change needed
Write	Read	=IF(D5=E5,"No change needed","Change Required")

IF(logical_test, **[value_if_true]**, [value_if_false])

AD Security 101: Control

Cleanup!

- Security groups
- GPOs
- Logon Scripts
- Spooler,LLMNR/NBNS, SMBv1, ADCS

Implement: AD Security 201

AD Security 201: Credentials

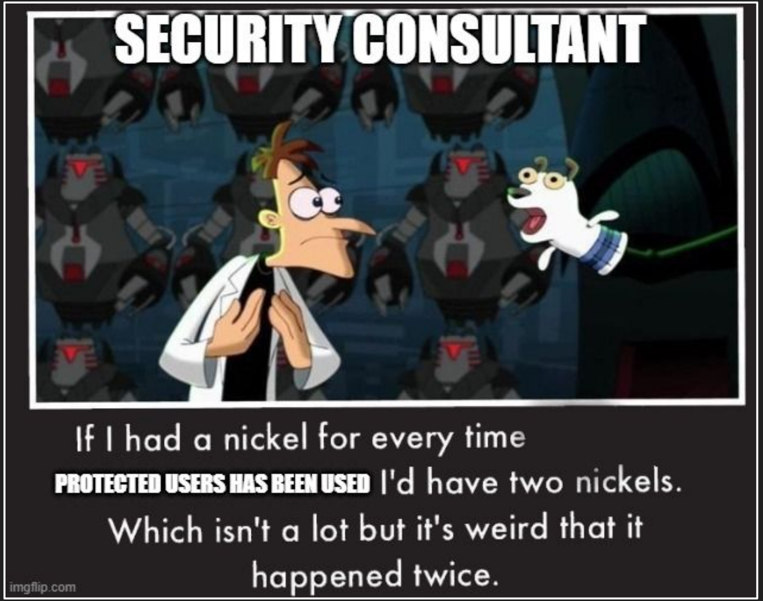
- Password policies & management
  - 14+ characters
  - FGPP
  - Tools & education
- Deception

AD Security 201: Access

- Tiered Security
  - Monash Enterprise Access Model (microsegmentation)
  - Shares, Groups, Delegations, GPOs, Tasks, Services

Thanks Jake!

- Protected Users


SECURITY CONSULTANT
If I had a nickel for every time
PROTECTED USERS HAS BEEN USED I'd have two nickels.
Which isn't a lot but it's weird that it
happened twice.
imgflip.com

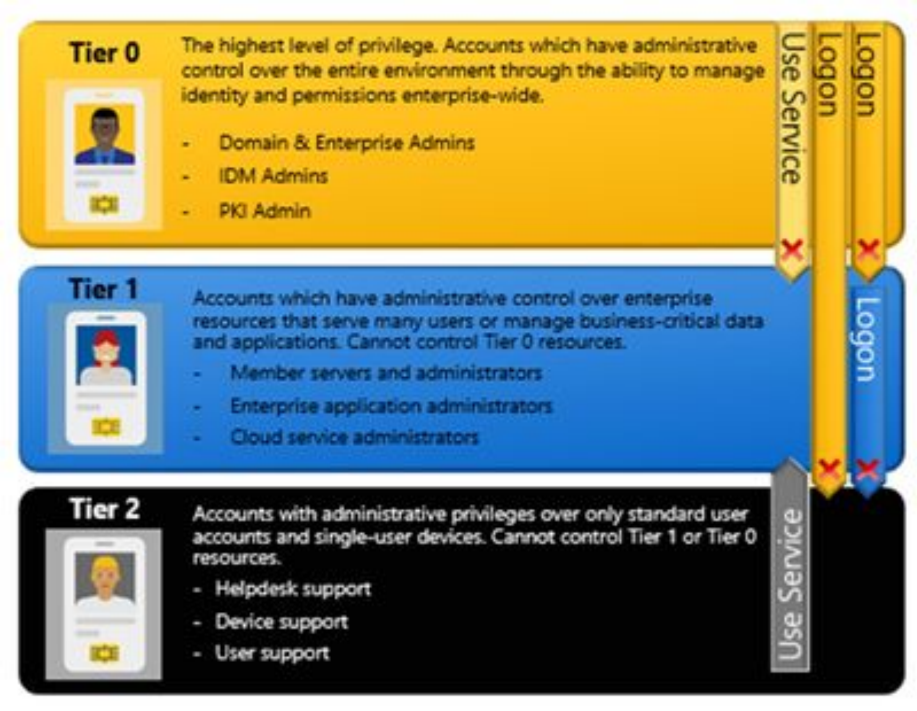
https://github.com/mon-csirt/active-directory-security

AD Security 201: Microsegmentation

Rule #1: Credentials from a higher-privileged tier must not be exposed to lower-tier systems.

Rule #2: Lower-tier credentials can use services provided by higher-tiers, but not the other way around.

Rule #3: Any system or user account that can manage a higher tier is also a member of that tier, whether originally intended or not.



Tier 0

The highest level of privilege. Accounts which have administrative control over the entire environment through the ability to manage identity and permissions enterprise-wide.

- Domain & Enterprise Admins
- IDM Admins
- PKI Admin

Tier 1

Accounts which have administrative control over enterprise resources that serve many users or manage business-critical data and applications. Cannot control Tier 0 resources.

- Member servers and administrators
- Enterprise application administrators
- Cloud service administrators

Tier 2

Accounts with administrative privileges over only standard user accounts and single-user devices. Cannot control Tier 1 or Tier 0 resources.

- Helpdesk support
- Device support
- User support

https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/protecting-tier-0-the-modern-way/ba-p/4052851

AD Security 201: Microsegmentation

- Organize into OUs
  - Servers → application groups
  - Desktops → site/dept.

Account OU's:

OU's in Detail:

OU = Tiered_Security_Users
- Child OU = Tier_0
- Child OU = Tier_1
- Child OU = Tier_2
- Child OU = Privileged_Users
- Child OU = Service_Accounts
  - Child OU = T0_SA
  - Child OU = T1_SA
  - Child OU = T2_SA

Group OU's:

OU = Tiered_Security_SG
- Child OU = Tiered_Security_0_SG
- Child OU = Tiered_Security_1_SG
- Child OU = Tiered_Security_2_SG

Computer OU's

OU = Tier_1_Server

OU = (Create a New OU for Workstations)

Remember to document!

AD Security 201: Microsegmentation

Tier 0:
Domain Admins

Tier 1:
T1-Server-Admins
T1-Service-Accounts

Tier 2:
T2-Desk-Admins
T2-Service-Accounts

Standard Users:
None

Systems Administrators:
- Tier 0: PDoe-T0
- Tier 1: PDoe-T1
- Tier 2: PDoe-T2
- Standard User Account: PDoe

Help Desk:
- Tier 2: PDoe-T2
- Standard User Account: PDoe

Users:
- Standard User Account: PDoe

Service Accounts:

Example: Vendor/Service-Tier: Nessus-T0, Nessus-T1, Nessus-T2

GPOs:

OU = Tier_1_Server
- GPO = T1.ServerAdmins.LA

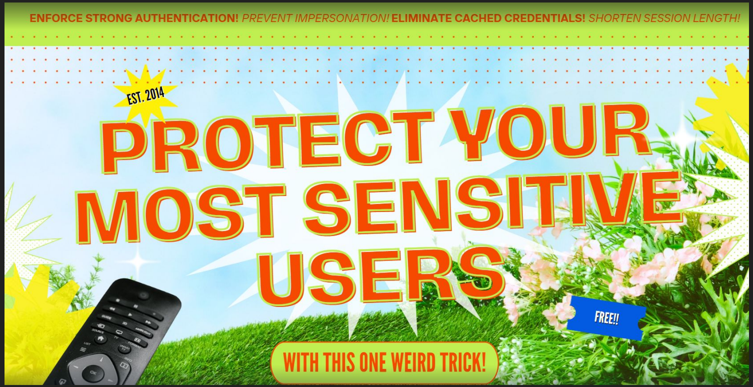
OU = Workstations
- GPO = T2.DesktopAdmins.LA

Remember to document!

AD Security 201: Protected Users

- Can't AUTH with NTLM
- Can't use DES or RC4
- Accounts cannot be delegated
- Kerberos TGTs limited to 4 hours
- Wherever they login: their credentials are never cached

Jake Hildreth, CISSP (He/Him) · 1st
Husband, Dad, Recovering Sysadmin · Trimarc ADSA Service Lead · I gather rakes.
Trimarc


ENFORCE STRONG AUTHENTICATION! PREVENT IMPERSONATION! ELIMINATE CACHED CREDENTIALS! SHORTEN SESSION LENGTH!
EST. 2014
PROTECT YOUR MOST SENSITIVE USERS
FREE!!
WITH THIS ONE WEIRD TRICK!

https://www.canva.com/design/DAGCSX9c-hY/D883ZXsn5Z_wZ2Zvc2vjjA/view

https://www.youtube.com/@bsidescharm

AD Security 201: Protected Users

PREPARE

Check the DFL + FFL + DC OSes
Enable ALL the Logs

AUDIT

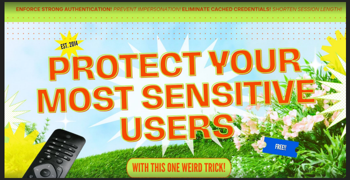
Highlight Insecure
Authentication Methods
Highlight

ENACT

Mark Users as Sensitive
Add Users to the PUG

Jake Hildreth, CISSP (He/Him) · 1st
Husband, Dad, Recovering Sysadmin · Trimarc ADSA Service Lead · I gather rakes.

Trimarc

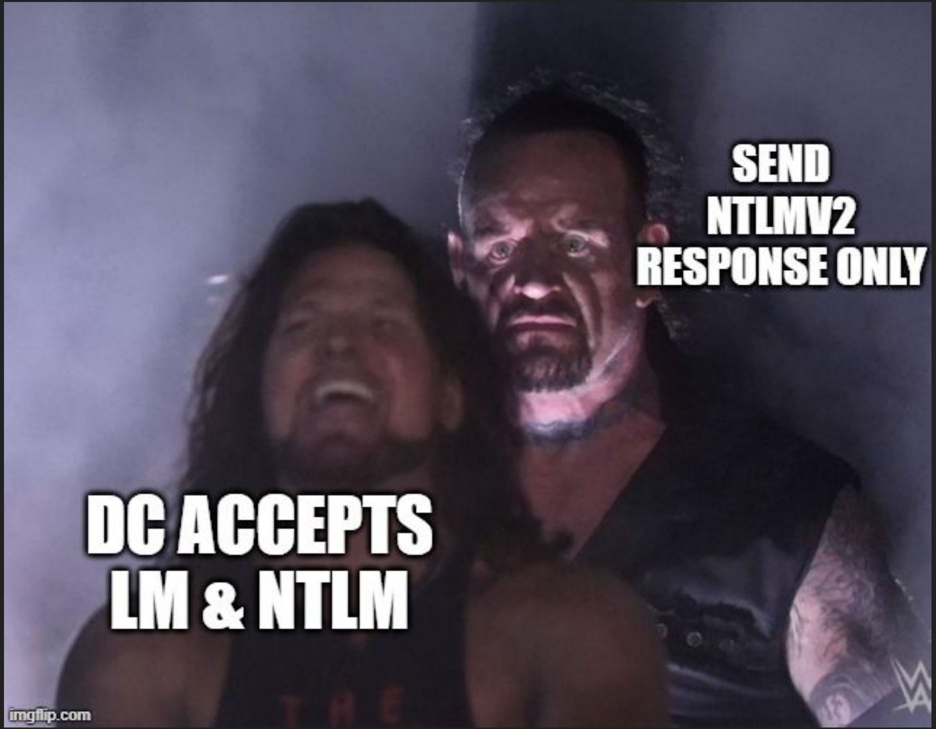


ENFORCE STRONG AUTHENTICATION! PREVENT IMPERSONATION! ELIMINATE CACHED CREDENTIALS! SHORTEN SESSION LENGTH!
EST. 2014
PROTECT YOUR MOST SENSITIVE USERS
FREE!!
WITH THIS ONE WEIRD TRICK!

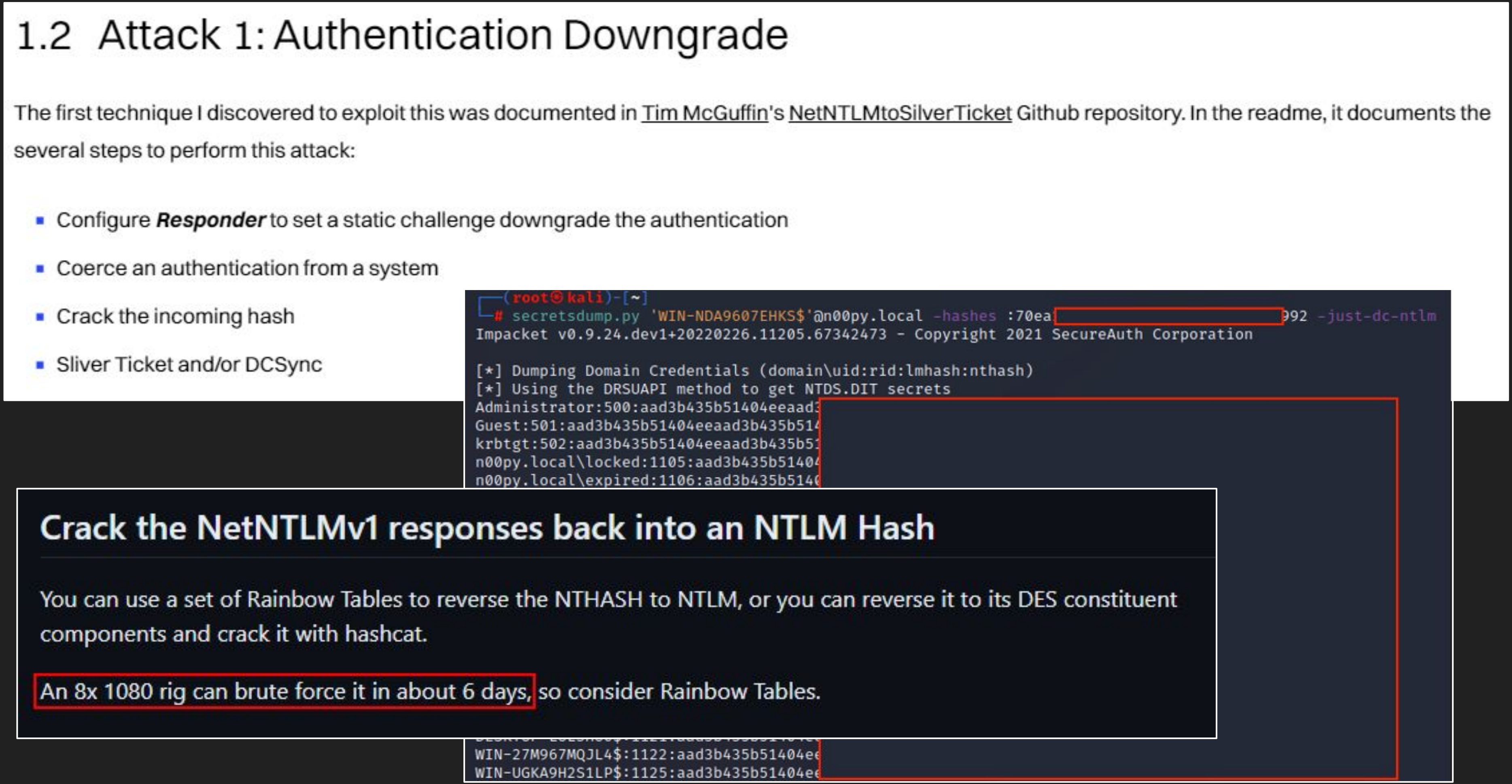
https://www.canva.com/design/DAGCSX9c-hY/D883ZXsn5Z_wZ2Zvc2vjjA/view

AD Security 201: Control

- Disable NTLMv1
- Enforce SMB Signing
- Enforce LDAP Signing & Channel Binding



https://www.linkedin.com/posts/spenceralessi_active-directory-hardening-series-part-activity-7188530304523882496-mzhc?utm_source=share&utm_medium=member_desktop



1.2 Attack 1: Authentication Downgrade

The first technique I discovered to exploit this was documented in Tim McGuffin's NetNTLMtoSilverTicket Github repository. In the readme, it documents the several steps to perform this attack:

- Configure ***Responder*** to set a static challenge downgrade the authentication
- Coerce an authentication from a system
- Crack the incoming hash
- Sliver Ticket and/or DCSync

```
┌──(root㉿kali)-[~]
└─# secretsdump.py 'WIN-NDA9607EHKS$'@n00py.local -hashes :70ea[redacted]992 -just-dc-ntlm
Impacket v0.9.24.dev1+20220226.11205.67342473 - Copyright 2021 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3[redacted]
Guest:501:aad3b435b51404eeaad3b435b514
krbtgt:502:aad3b435b51404eeaad3b435b51
n00py.local\locked:1105:aad3b435b51404
n00py.local\expired:1106:aad3b435b514
WIN-27M967MQJL4$:1122:aad3b435b51404ee
WIN-UGKA9H2S1LP$:1125:aad3b435b51404ee
```

Crack the NetNTLMv1 responses back into an NTLM Hash

You can use a set of Rainbow Tables to reverse the NTHASH to NTLM, or you can reverse it to its DES constituent components and crack it with hashcat.

An 8x 1080 rig can brute force it in about 6 days, so consider Rainbow Tables.

https://trustedsec.com/blog/practical-attacks-against-ntlmv1

How to Harden Active Directory to Prevent Cyber Attacks

1. Identify: Misconfigurations
2. Implement: AD Security 101
3. Implement: AD Security 201
4. Repeat

How To Get Support?

- Include others
- Ask for feedback/advice
- Honesty/transparency

sysadmin hardening Active Directory
Trying to do it all yourself
imgflip.com

Hardening Active Directory

Spencer Alessi

SecurIT360 Services

Cloud Security

- Cloud Security Validation
  - SaaS, public, private, hybrid, Azure, Amazon, M365, Google,etc.
  - CASB, ZTNA, SASE, SSE
- 24/7 Threat Monitoring
- Zero Trust Assessment and Guidance
- Cloud Security Data Protection & Privacy Strategy/Roadmap

The Cyber360 OS

- Ongoing Risk Monitoring and Measurement
- Tailored to your needs
- Assigned CISO w/ Risk Dashboard
- Achieve Compliance standards and obtain Cyber Insurance

24/7 Threat Detection & Response

- MDR, EDR, XDR
- Threat Hunting
- Attack Surface Monitoring
- Threat Intelligence

THANK YOU! Q&A

Offensive Security

- Penetration Testing
  - Internal/External
  - Assumed Breach/Social Engineering
  - Network, Web App, Mobile
  - IoT
  - Physical
- Red/Purple Team Exercises

Privacy & Compliance

- Audit, Assessment, & Advisory
- DPIA
- CMMC, HIPAA, NIST, CCPA, GDPR, GLBA, NYDFS, PCI, ISO 27000, others
- Information Governance
- Web Tracking Privacy Assessment

CISO Services

- GRC & Program Development
  - Risk Management
  - Vendor management
  - Vulnerability Management
  - Other programs
- Security Awareness Training

DevSecOps

- Application Testing
- Dev Process Eval & Design
- Ongoing Code Review

Incident Response & Forensics

- Full Service Response & Forensics
- Planning & Preparations
- Evidence and Data Collection
- Table Top Exercises

Resources

- www.securit360.com
- www.offsec.blog
- https://github.com/techspence/ScriptSentry
- https://github.com/techspence/ADeleginator
- https://www.linkedin.com/posts/spenceralessi_when-it-comes-to-securing-active-directory-activity-7194052189714087938-8tdk?utm_source=share&utm_medium=member_desktop
- https://www.linkedin.com/posts/spenceralessi_active-directory-hardening-series-part-activity-7188530304523882496-mzhc?utm_source=share&utm_medium=member_desktop
- https://pingcastle.com
- https://github.com/TrimarcJake/Locksmith
- https://github.com/TrimarcJake/pug-snippets
- https://github.com/mon-csirt/active-directory-security
- https://adsecurity.org