



LIMITING ADMIN USER RISK IN A WINDOWS ENVIRONMENT

AND OTHER TIPS TO AVOID MAKING THE NEWS

Blake Regan, Information Security Senior Engineer

May 20, 2021



@CRASH0VER1D3
[HTTPS://GITHUB.COM/CRASH0VER1D3](https://github.com/crash0ver1d3)

WHOAMI

- Blake Regan (@crashOver1d3)
 - Father and Husband
 - Started in IT in 2010, formerly worked in Construction Industry
 - Started in Information Security 2014
 - Hockey Fanatic (Fan and Player)
 - Mountain Biking/Trail Riding
 - Automation enthusiast
 - Serial Learner

@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)

EMPLOYMENT AND EDUCATION

- Information Security Senior Engineer at Equinix, Inc focused on Blue Team and DFIR
- Most recently Wesco Dist/Anixter Inc as Senior Security Engineer focused on Blue Team and DFIR
- Previously Motorola Solutions, Government and Public Safety, Information Assurance Vetting
- BASc, Information Systems Security
- Certs:
 - GIAC GCWN, GCIH
 - CompTia Security+, Network +, Project +
 - Pentester Academy CRTP

@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/CRASHOVER1D3)

DISCUSSION

- Unauthorized Local Administrator privileges
- Managing Local Administrator account credentials at scale
- Protecting Administrative account hashes and credentials (as best we can)
- Weak password policies for Administrative accounts
- Limiting Risk from EFS ransomware

DISCLAIMER

- PowerShell scripts referenced in slides available on Github. Please do not use the scripts in production until you understand how they work in test environment.

UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES



UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - RISKS

- Unapproved\dangerous software installation
- User compromise turns to instant privilege escalation
- Unapproved Configuration changes
- Damage caused by insider threat

...many, many more.

@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)



@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)

Saving lives since 1984

UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - DETECTIONS

Track access requests/approval in a records management system



Security Incident Event Manager (SIEM) Alerts on event ID 4732 sent as email alert



No SIEM, no problem. Powershell to the rescue!



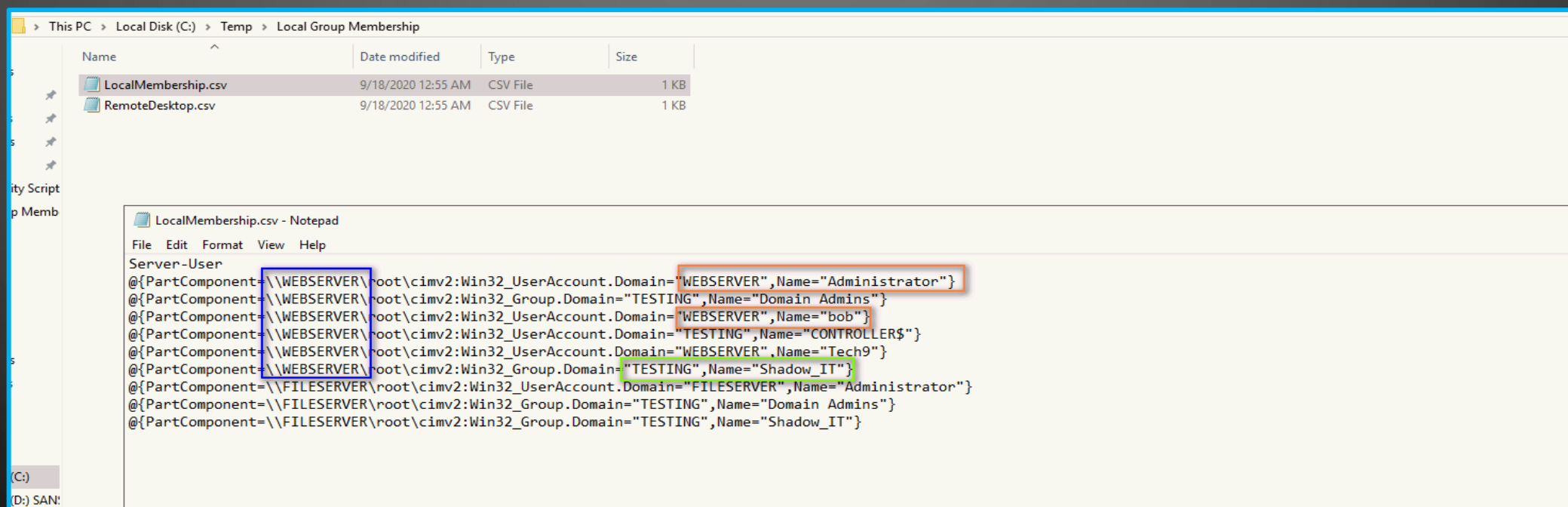
Hold people accountable. Why did you add this account?



Monitor This

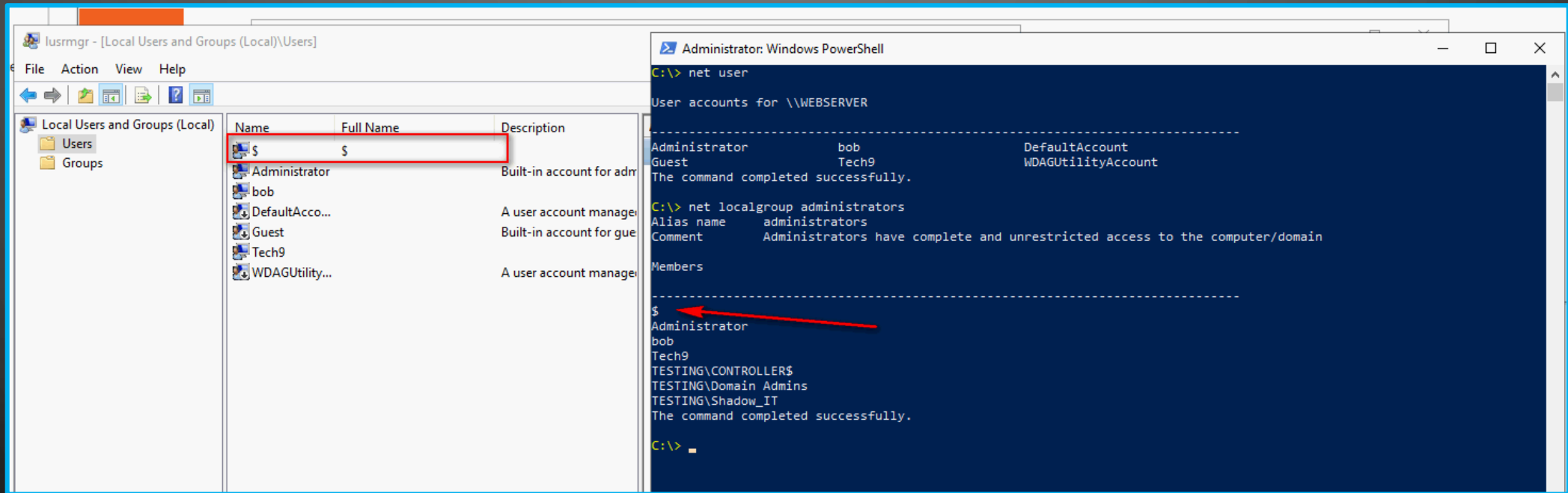
UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - IDENTIFY BASELINE

[HTTPS://GITHUB.COM/CRASHOVER1D3/GET-LOCALMEMBERSHIP-DOMAIN](https://github.com/crashover1d3/get-localmembership-domain)



@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)

UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - EXAMPLE SCENARIOS



Unauthorized account creation and addition to local administrators group

UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - DETECTION

[HTTPS://GITHUB.COM/CRASHOVER1D3/GET-LOCALMEMBERSHIP-DOMAIN](https://github.com/crashover1d3/get-localmembership-domain)

PC > Local Disk (C:) > Temp > Local Group Membership

Name	Date modified	Type	Size
Baseline	9/18/2020 1:07 AM	File folder	
LocalMembership.csv	9/18/2020 1:07 AM	CSV File	1 KB
RemoteDesktop.csv	9/18/2020 1:07 AM	CSV File	1 KB

LocalMembership.csv - Notepad

File Edit Format View Help

Server-User

```
@{PartComponent=\\WEBSERVER\\root\\cimv2:Win32_UserAccount.Domain="WEBSERVER",Name="Administrator"}
@{PartComponent=\\WEBSERVER\\root\\cimv2:Win32_Group.Domain="TESTING",Name="Domain Admins"}
@{PartComponent=\\WEBSERVER\\root\\cimv2:Win32_UserAccount.Domain="WEBSERVER",Name="bob"}
@{PartComponent=\\WEBSERVER\\root\\cimv2:Win32_UserAccount.Domain="TESTING",Name="CONTROLLER$"}
@{PartComponent=\\WEBSERVER\\root\\cimv2:Win32_UserAccount.Domain="WEBSERVER",Name="Tech9"}
@{PartComponent=\\WEBSERVER\\root\\cimv2:Win32_Group.Domain="TESTING",Name="Shadow_IT"}
@{PartComponent=\\WEBSERVER\\root\\cimv2:Win32_UserAccount.Domain="WEBSERVER",Name="$"}
@{PartComponent=\\FILESERVER\\root\\cimv2:Win32_UserAccount.Domain="FILESERVER",Name="Administrator"}
@{PartComponent=\\FILESERVER\\root\\cimv2:Win32_Group.Domain="TESTING",Name="Domain Admins"}
@{PartComponent=\\FILESERVER\\root\\cimv2:Win32_Group.Domain="TESTING",Name="Shadow_IT"}
```

Query returns newly added account, time to investigate

@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)

UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - DETECTION

Sep 9, 2020 2:21:27 PM CDT

Rule Name: UC7.2 - Windows - Local Admin Group Modified @RTR-RST-ISS@
Rule Description:

Source IP: 10.10.2.39
Source Port: 0
Source Username (from event):
Source Network: Net-10-172-192.Net_10_0_0_0

Destination IP: 10.10.2.39
Destination Port: 0
Destination Username (from Asset Identity):
Destination Network: Net-10-172-192.Net_10_0_0_0

Protocol: other(255)
QID: 5000903

Event Name: Success Audit: A member was added to a security-enabled local group
Event Description: Success Audit: A member was added to a security-enabled local group.
Category: Group Member Added

Log Source ID: 777
Log Source Name: WindowsAuthServer @ .

Payload: <13>Sep 09 14:20:34 , AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.2.8.91
Source=Microsoft-Windows-Security-Auditing Computer= OriginatingComputer=10.10.2.39 User= Domain= EventID=4732
EventIDCode=4732 EventType=8 EventCategory=13826 RecordNumber=36457515 TimeGenerated=1599679232 TimeWritten=1599679232 Level=Log
Always Keywords=Audit Success Task=SE_ADT_ACCOUNTMANAGEMENT_SECURITYGROUP Opcode=Info Message=A member was added to a security-enabled
local group. Subject: Security ID: Account Name: Account Domain: Logon ID: 0x2ecd91 Member: Security ID:
Account Name: - Group: Security ID: BUILTIN\Administrators Group Name: Administrators Group Domain: Builtin Additional Information: Privileges: -

@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)

SIEM Alert! Autobots....roll out!

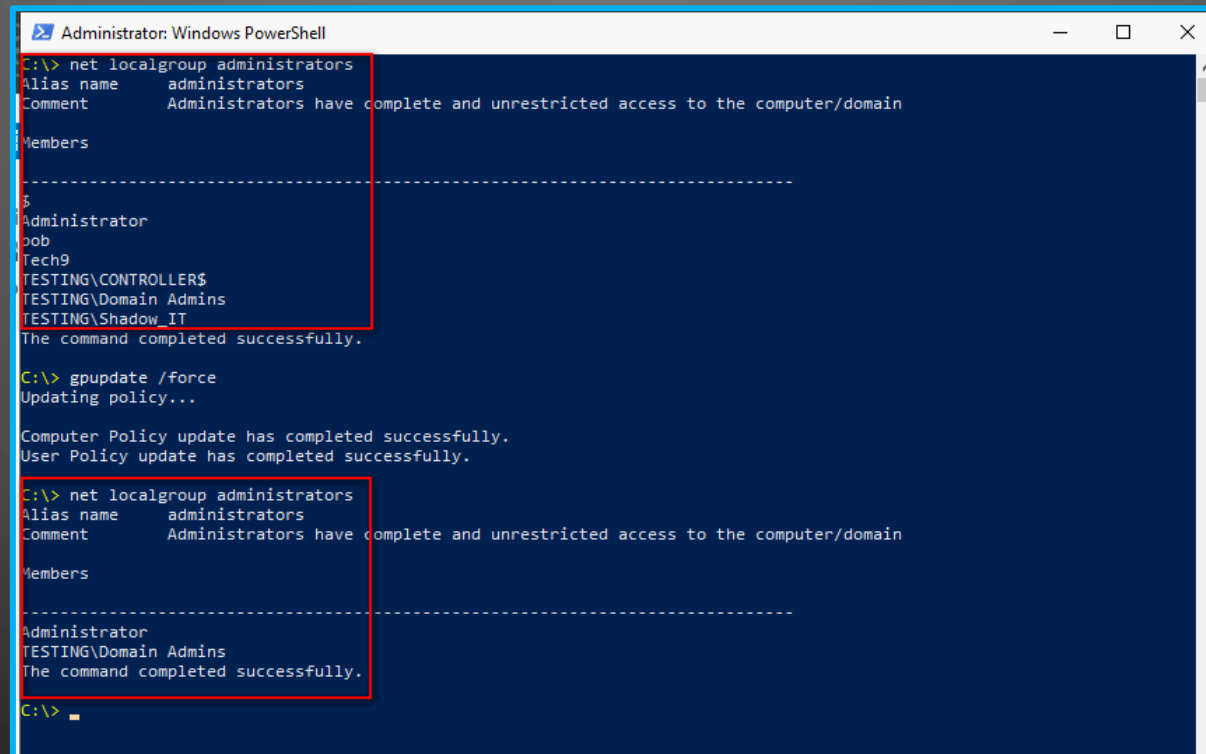
UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - REMEDIATION

The screenshot displays the Group Policy Management console for the 'testing.local' domain. The left pane shows the hierarchy: Forest: testing.local > Domains > testing.local > Group Policy Objects > Enable_Local_Administrators_Membership. The main pane shows the 'Enable_Local_Administrators_Membership' GPO with the 'Links' tab selected. A table lists the linked sites:

Location	Enforced	Link Enabled	Path
Servers	No	Yes	testing.local/Servers

A red arrow points to the 'Servers' link. Below this, the 'Group Policy Management Editor' window is open, showing the 'Security' category > 'Computer Configuration' > 'Policies' > 'Security Settings' > 'Restricted Groups'. The 'Administrators' group is highlighted with a red box. The 'Members' column for this group shows 'TESTING\Domain A...'. On the right, the 'Administrators Properties' window is open, showing 'Members of this group: TESTING\Domain Admins'.

UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - REMEDIATION



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". It displays the output of the command `net localgroup administrators` twice. The first output shows a list of members including Administrator, bob, Tech9, TESTING\CONTROLLERS\$, TESTING\Domain Admins, and TESTING\Shadow_IT. The second output shows only Administrator and TESTING\Domain Admins. Between the two outputs, the command `gpupdate /force` is executed, resulting in successful updates for both Computer Policy and User Policy.

```
Administrator: Windows PowerShell

C:\> net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members
-----
Administrator
bob
Tech9
TESTING\CONTROLLERS$
TESTING\Domain Admins
TESTING\Shadow_IT
The command completed successfully.

C:\> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

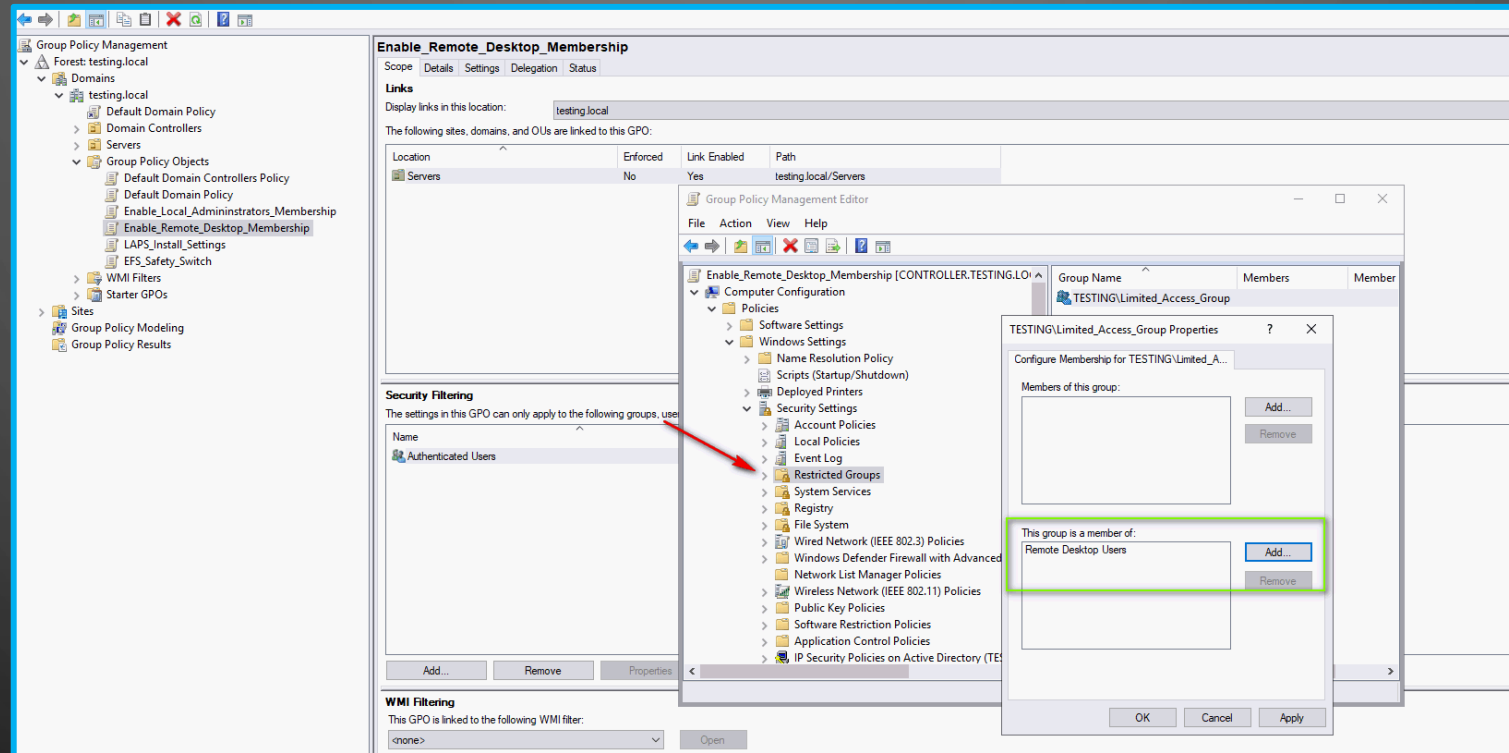
C:\> net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members
-----
Administrator
TESTING\Domain Admins
The command completed successfully.

C:\>
```

Local Administrators group cleaned up after baseline policy applied

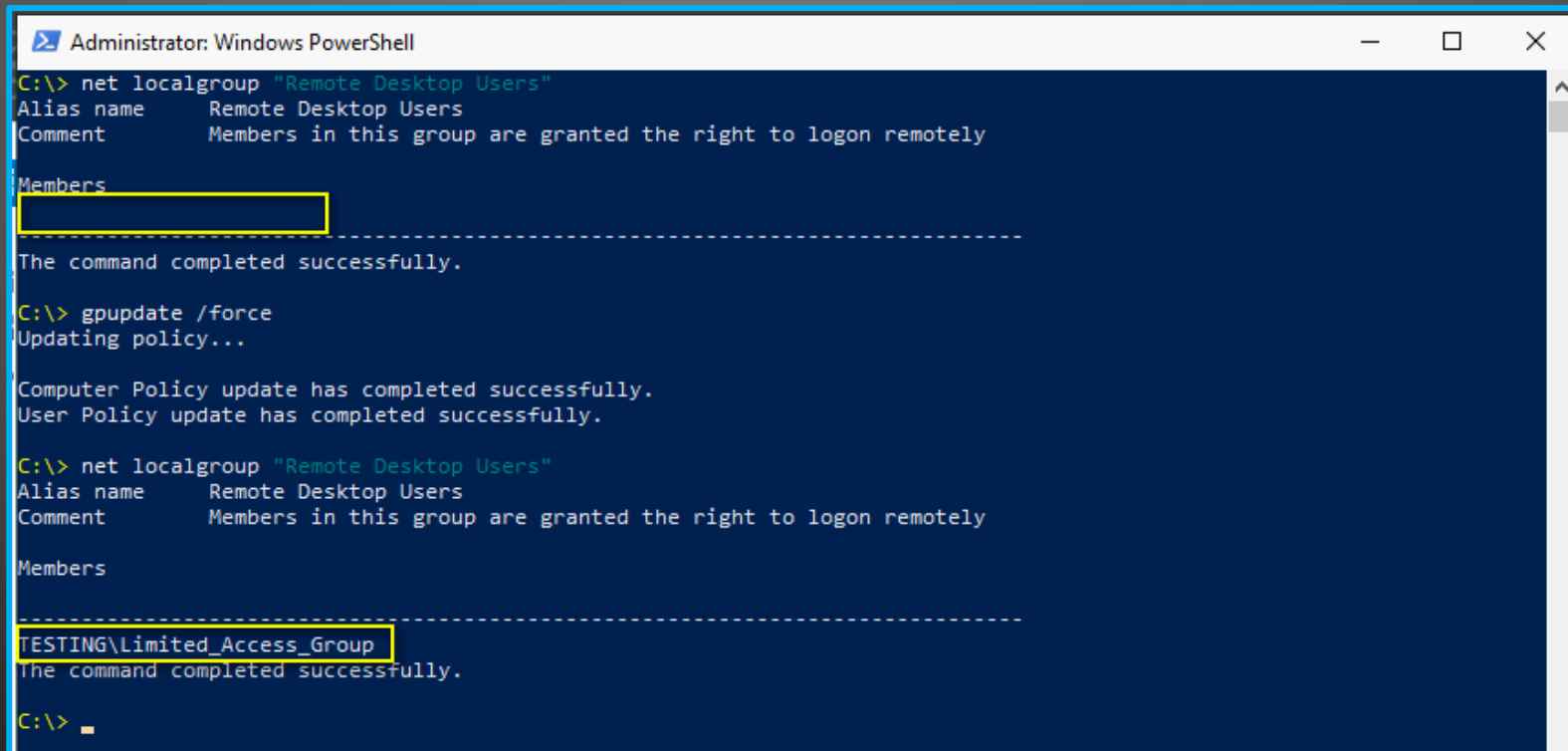
UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - REMEDIATION



Apply baseline for Remote Desktop users for non-privileged accounts

@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)

UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - REMEDIATION



```
Administrator: Windows PowerShell
C:\> net localgroup "Remote Desktop Users"
Alias name     Remote Desktop Users
Comment       Members in this group are granted the right to logon remotely

Members
-----
The command completed successfully.

C:\> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

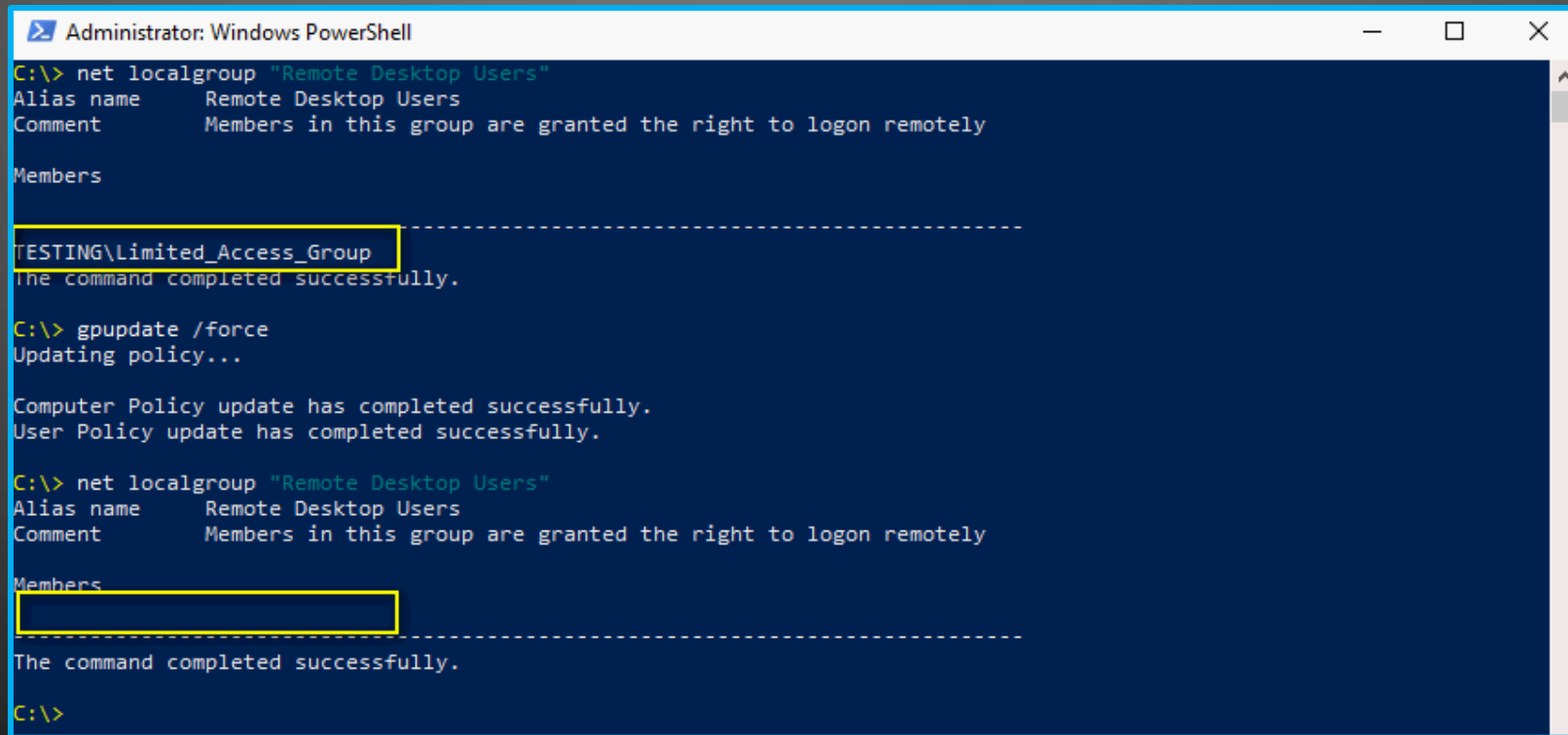
C:\> net localgroup "Remote Desktop Users"
Alias name     Remote Desktop Users
Comment       Members in this group are granted the right to logon remotely

Members
-----
TESTING\Limited_Access_Group
The command completed successfully.

C:\> _
```

Update after policy enforcement, group added.

UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - REMEDIATION



```
Administrator: Windows PowerShell

C:\> net localgroup "Remote Desktop Users"
Alias name     Remote Desktop Users
Comment       Members in this group are granted the right to logon remotely

Members
-----
TESTING\Limited_Access_Group
The command completed successfully.

C:\> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\> net localgroup "Remote Desktop Users"
Alias name     Remote Desktop Users
Comment       Members in this group are granted the right to logon remotely

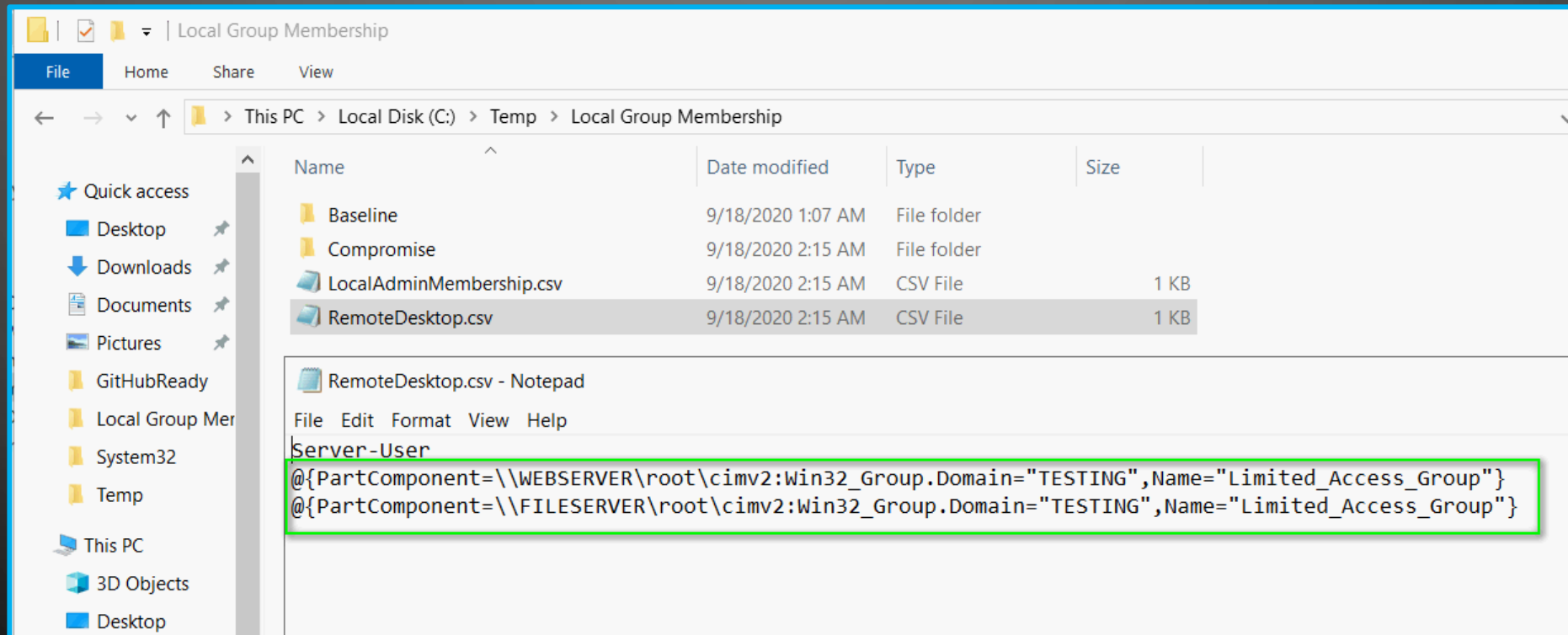
Members
-----
The command completed successfully.

C:\>
```

Update after policy enforcement, group added.

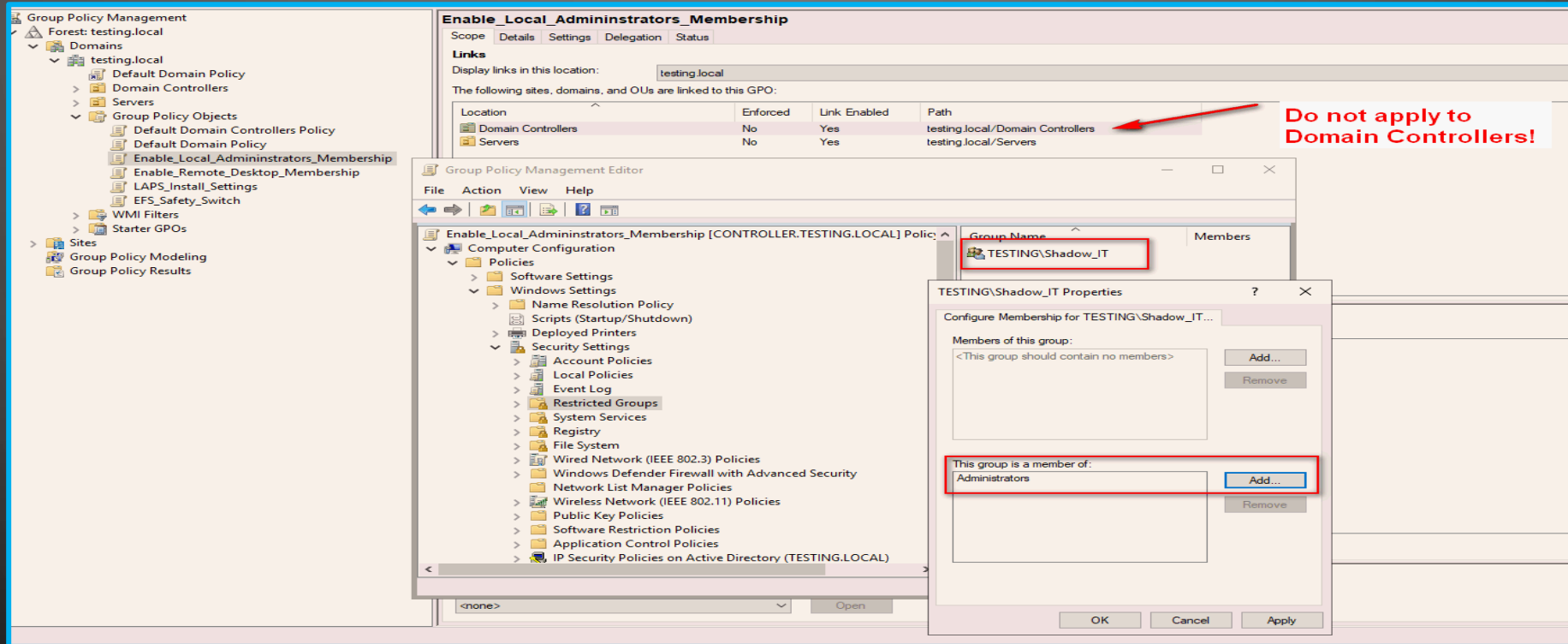
UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES – REMEDIATION

[HTTPS://GITHUB.COM/CRASHOVER1D3/GET-LOCALMEMBERSHIP-DOMAIN](https://github.com/crashover1d3/get-localmembership-domain)



@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)

UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - NO NO'S



UNAUTHORIZED LOCAL ADMINISTRATOR PRIVILEGES - NO NO'S

Group Policy Management console showing the 'Enable_Local_Administrators_Membership' policy linked to 'testing.local'.

Windows PowerShell window showing the command 'net localgroup Administrators' being executed successfully.

Active Directory Users and Computers console showing the 'Administrators' group with 'Shadow_IT' as a member.

Administrators Properties window showing the 'Members' list with 'Shadow_IT' highlighted.

Privilege Escalation (aka Very Bad!!!)

Do not apply restricted group to Domain Controllers!

MANAGING LOCAL ADMINISTRATOR ACCOUNT CREDENTIALS AT SCALE

- Local Administrator Password Solution – Domain Only
- “The "Local Administrator Password Solution" (LAPS) provides management of local account passwords of domain joined computers. Passwords are stored in Active Directory (AD) and protected by ACL, so only eligible users can read it or request its reset.”
- Powershell (Protect-CMSMessage) for Workgroup/Domain solution
 - Credit to Jason Fossen for idea and code for alternative to LAPS
 - <https://www.blutteampowershell.com>

Source: <https://www.microsoft.com/en-us/download/details.aspx?id=46899>

MANAGING LOCAL ADMINISTRATOR ACCOUNT CREDENTIALS AT SCALE - PROBLEM

- Same password used for all local administrator accounts on servers and workstations
- Responder LLMNR\NetBios

```
*] Listening for events...  
*] [NBT-NS] Poisoned answer sent to 10.10.76.5 for name WORKGROUP (service: Local Master Browser)  
*] [NBT-NS] Poisoned answer sent to 10.10.10.9 for name HELLLLLL000504 (service: File Server)  
*] [NBT-NS] Poisoned answer sent to 10.10.10.9 for name HELLLLLL000504 (service: Workstation/Redirector)  
*] [MDNS] Poisoned answer sent to 102.168.112.1 for name hellllll000504.local
```


MANAGING LOCAL ADMINISTRATOR ACCOUNT CREDENTIALS AT SCALE - PROBLEM

- Pass the Hash
- Crack the Hash
- CrackMapExec (CME) @bytebleeder

<https://github.com/byt3bl33d3r/CrackMapExec>

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:452495d04f81e4c200b44745424c55eb:29affe6ea3732b9bc83c896c84311863:::
falken:1011:4fbd4cea97c5752caad3b435b51404ee:2049b70ec5b6944aed5fef05bc4b1933:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_WILMA:1003:84be91bc0235ae1a23ef11b0f04203ae:2d36d8b39d37e174f350d1f54fa8a93c:::
IWAM_WILMA:1004:4fd3d0eea847cc93d9b3122cfc667c5e:e09dbfeb01becf58d8d83a798e82e79c:::
mike:1010:bb2493b09f6ecfc9aad3b435b51404ee:c0bb120391d5367712cc4c92389bfa21:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:b8697e859faa3aadf1390b559d730e46:::
susan:1009:e52cac67419a9a2236077a718ccdf409:5f946a12c3ebe8640c7c382616045332:::
```

@CRASHOVERTID3

[HTTPS://GITHUB.COM/CRASHOVERTID3](https://github.com/CRASHOVERTID3)



@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/CRASHOVER1D3)

MANAGING LOCAL ADMINISTRATOR ACCOUNT CREDENTIALS AT SCALE - SOLUTION

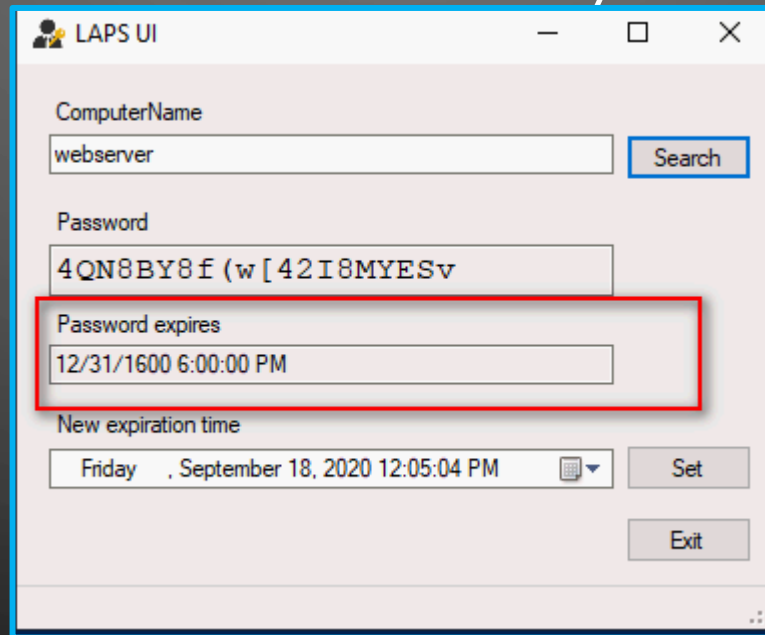
- Deploy LAPS in Domain Environment
 - Different local administrator password on every workstation/server in domain (except DCs)
- Delegate Permissions to read LAPS values to ServiceDesk, DeskSide, etc
- Delegate Permissions to reset LAPS password to limited few Admins
 - Change password after use to clean up hash stored in registry
 - Force reset of entire domain LAPS values if needed

MANAGING LOCAL ADMINISTRATOR ACCOUNT CREDENTIALS AT SCALE - TIPS AND TRICKS

- Rename local Administrator account via Group Policy
- Assign LAPS to manage that new account name
- Rename local Guest account via Group Policy
- Disable local Guest account via Group Policy

MANAGING LOCAL ADMINISTRATOR ACCOUNT CREDENTIALS AT SCALE - TIPS AND TRICKS

- After initial deployment of LAPS, force reset all values to sync new values
- The expiration time indicates the value is not synced. Login will not be possible



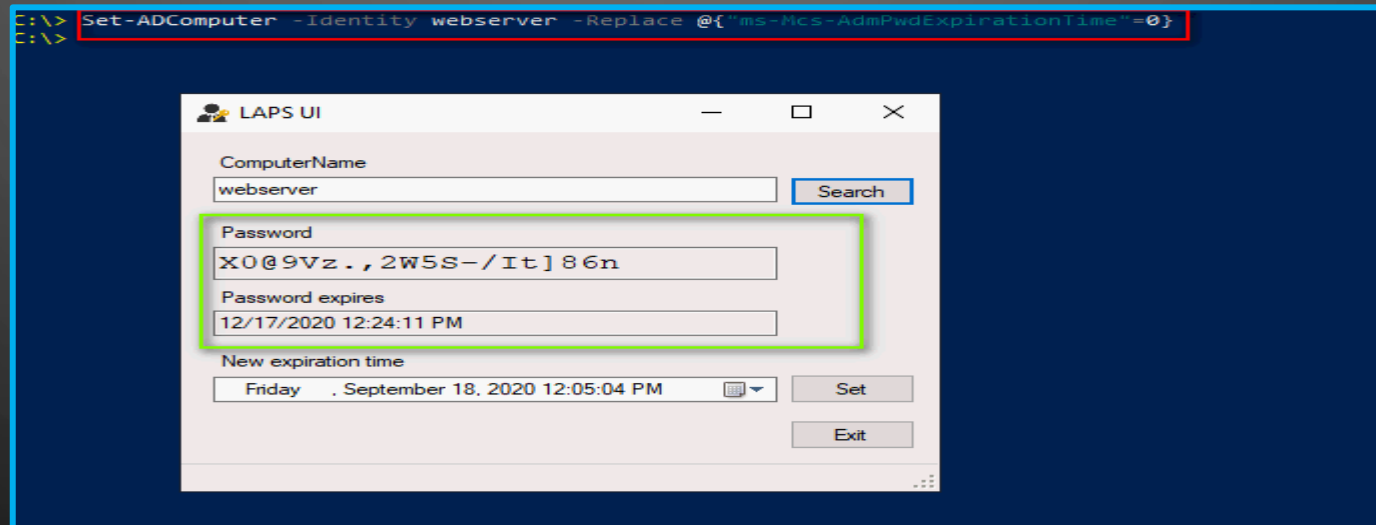
The screenshot shows the LAPS UI window with the following fields and buttons:

- ComputerName:** webserver (with a Search button)
- Password:** 4QN8BY8f(w[42I8MYESv
- Password expires:** 12/31/1600 6:00:00 PM (highlighted with a red box)
- New expiration time:** Friday, September 18, 2020 12:05:04 PM (with a calendar icon and Set button)
- Exit button**

MANAGING LOCAL ADMINISTRATOR ACCOUNT CREDENTIALS AT SCALE - TIPS AND TRICKS

[HTTPS://GITHUB.COM/CRASHOVER1D3/FORCE-RESET-LAPS](https://github.com/crashover1d3/force-reset-laps)

- Force reset the LAPS password from Domain Controller
- Password Syncs at the next group policy enforcement

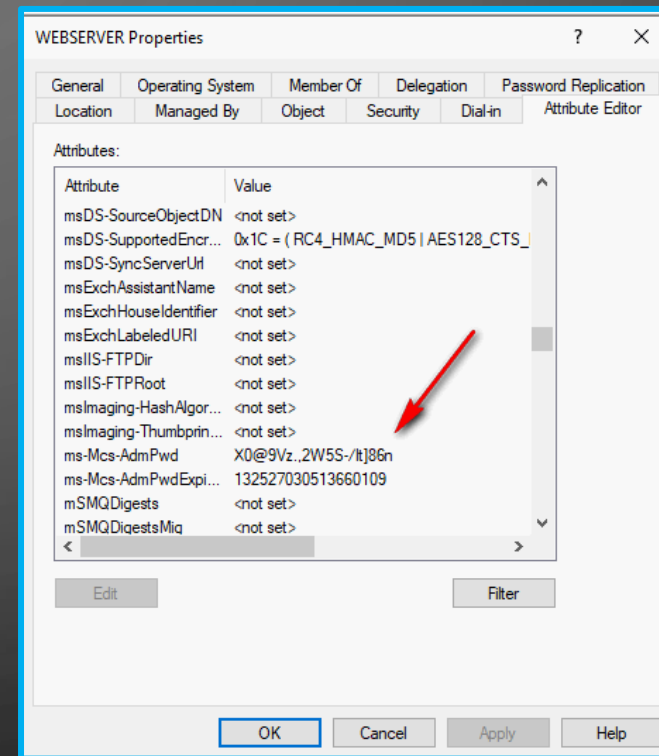


@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)

MANAGING LOCAL ADMINISTRATOR ACCOUNT CREDENTIALS AT SCALE - SECURELY?

- Encrypted in transit, not at rest
- 3rd Party Tool like LDAP viewer could expose in transit
- Use packet encryption (IPSEC/Windows Firewall Secure Connections)

Is there a better way to do this???



MANAGING LOCAL ADMINISTRATOR ACCOUNT CREDENTIALS AT SCALE - POWERSHELL SOLUTION

- Credit to Jason Fossen @JasonFossen, author of SANS SEC505
<https://blueteampowershell.com/>
- Credentials stored in certificate encrypted file (CA or self-signed)
- Encrypted with public key on host or network share
- Decrypted with Private key (can be stored on smart card)
- Schedule task to update password, encrypt new value, archive on network share
- Does not require a domain to use

MANAGING LOCAL ADMINISTRATOR ACCOUNT CREDENTIALS AT SCALE - POWERSHELL SOLUTION

```
C:\SANS\day3\UpdatePasswords> net user

User accounts for \\FILESERVER

-----
DefaultAccount      disable          renamed
WDAGUtilityAccount
The command completed successfully.

C:\SANS\day3\UpdatePasswords> .\Update-PasswordArchive.ps1 -LocalUserName renamed -CertificateFilePath .\PublicKeyCert.cer -PasswordArchivePath \\controller\Admin_Utility_Files
SUCCESS: renamed password reset and archive file saved.

C:\SANS\day3\UpdatePasswords> dir \\controller\Admin_Utility_Files

Directory: \\controller\Admin_Utility_Files

Mode                LastWriteTime         Length Name
----                -
-a----           9/19/2020 10:20 PM             720 FILESERVER+renamed+637361508451381137+6669762D899E762045DF160EEB447EB99C0D72F8

C:\SANS\day3\UpdatePasswords> .\Recover-PasswordArchive.ps1 -PasswordArchivePath \\controller\Admin_Utility_Files -ComputerName $env:COMPUTERNAME -UserName renamed

ComputerName : FILESERVER
FilePath     : \\controller\Admin_Utility_Files\FILESERVER+renamed+637361508451381137+6669762D899E762045DF160EEB447EB99C0D72F8
UserName      : renamed
TimeStamp     : 9/19/2020 10:20:45 PM
Thumbprint    : 6669762D899E762045DF160EEB447EB99C0D72F8
Valid        : True
StatusMessage : Success
Password      : .C!#Fg!<fym%t]3dGolj

C:\SANS\day3\UpdatePasswords>
```

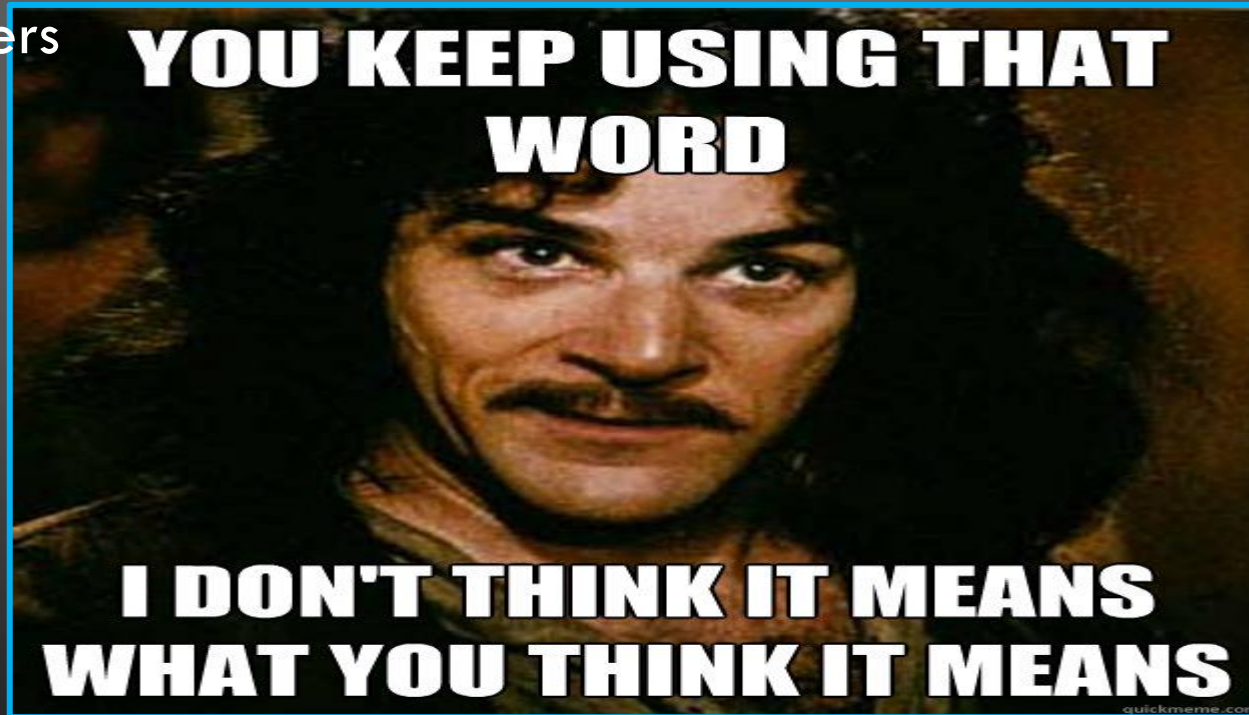
Create levels of access by using a different certificate based on account sensitivity. Manage access to private key(s)

@CRASHOVER1D3

[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)

THREAT ACTORS BE LIKE....

- Protected Users



@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashover1d3)

This is my attempt at humor

PROTECTING ADMINISTRATIVE ACCOUNT HASHES AND CREDENTIALS (AS BEST WE CAN) - SOLUTION

- Protected Users group in MS Active Directory

Active Directory Protections

- Restricts use of DES or RC4 Encryption (Kerberos Pre-Auth)
- Restricts use of NTLM authentication
- Restricts use of Kerberos Delegation (constrained/unconstrained)
- Cannot Renew Kerberos TGT beyond four hour lifetime (must request new TGS ticket)

Citation: <https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group>

@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/CRASHOVER1D3)

PROTECTING ADMINISTRATIVE ACCOUNT HASHES AND CREDENTIALS (AS BEST WE CAN) - SOLUTION

- Protected Users group in MS Active Directory

Device protections

- Eliminates caching of plaintext credentials (CredSSP and WDigest)
 - Breaks offline sign in
- NTLM will not cache user's plaintext credentials
- LDAP and NTLM authentication will no longer work
 - So what?
- No more DES or RC4 encrypted tickets accepted by Kerberos
 - Breaks TACACS+ for Administrative access on Cisco Devices ☹️

Citation: <https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group>



WEAK PASSWORD POLICIES FOR ADMINISTRATIVE ACCOUNTS (AND NON-ADMIN ACCOUNTS) - PROBLEM

- Windows hashes lack a salt (LM, NT, NTLM, NTLMv2)
- LANMAN Authentication
 - Password: clever!
 - Uppercase: CLEVER!
 - Pad to 14: CLEVER!_____
 - Split 2x7char CLEVER! _____
 - Create two DES keys with each chunk
 - DES encrypt the string "KGS!@#\$\$%" with each key, concatenate
 - 503E2B7715A32B1F AAD3B435B51404EE

*Credit to John Strand, Joshua Wright, and Mick Douglas for the analogy, SANS SEC504 course

WEAK PASSWORD POLICIES FOR ADMINISTRATIVE ACCOUNTS (AND NON-ADMIN ACCOUNTS) - PROBLEM

```
Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 27181941
* Bytes.....: 139921497
* Keyspace..: 27181941
* Runtime...: 2 secs

aad3b435b51404ee:
503e2b7715a32b1f: CLEVER!

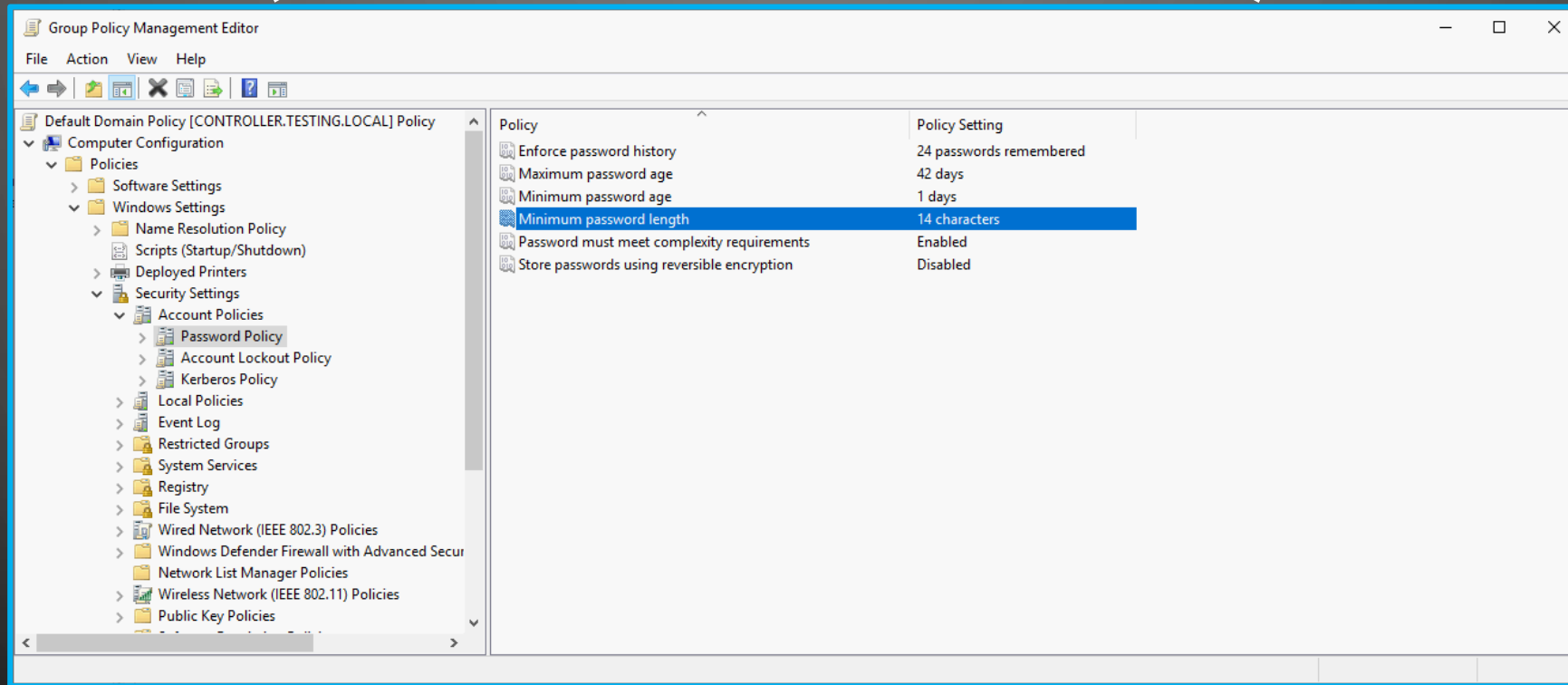
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: LM
Hash.Target.....: LANMAN.txt
Time.Started....: Sun Sep 20 00:53:47 2020 (1 sec)
Time.Estimated...: Sun Sep 20 00:53:48 2020 (0 secs)
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#3.....: 6217.9 kH/s (5.79ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered.....: 2/2 (100.00%) Digests
Progress.....: 3407872/27181941 (12.54%)
Rejected.....: 0/3407872 (0.00%)
Restore.Point....: 3276800/27181941 (12.06%)
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#3...: CVSCVS1 -> E06
Hardware.Mon.#3...: Temp: 48c Util: 58% Core:1746MHz Mem:3504MHz Bus:4

Started: Sun Sep 20 00:53:44 2020
Stopped: Sun Sep 20 00:53:49 2020

C:\Tools\hashcat-6.1.1\hashcat-6.1.1>hashcat.exe -m 3000 -a 0 LANMAN.txt rockyou.txt
```

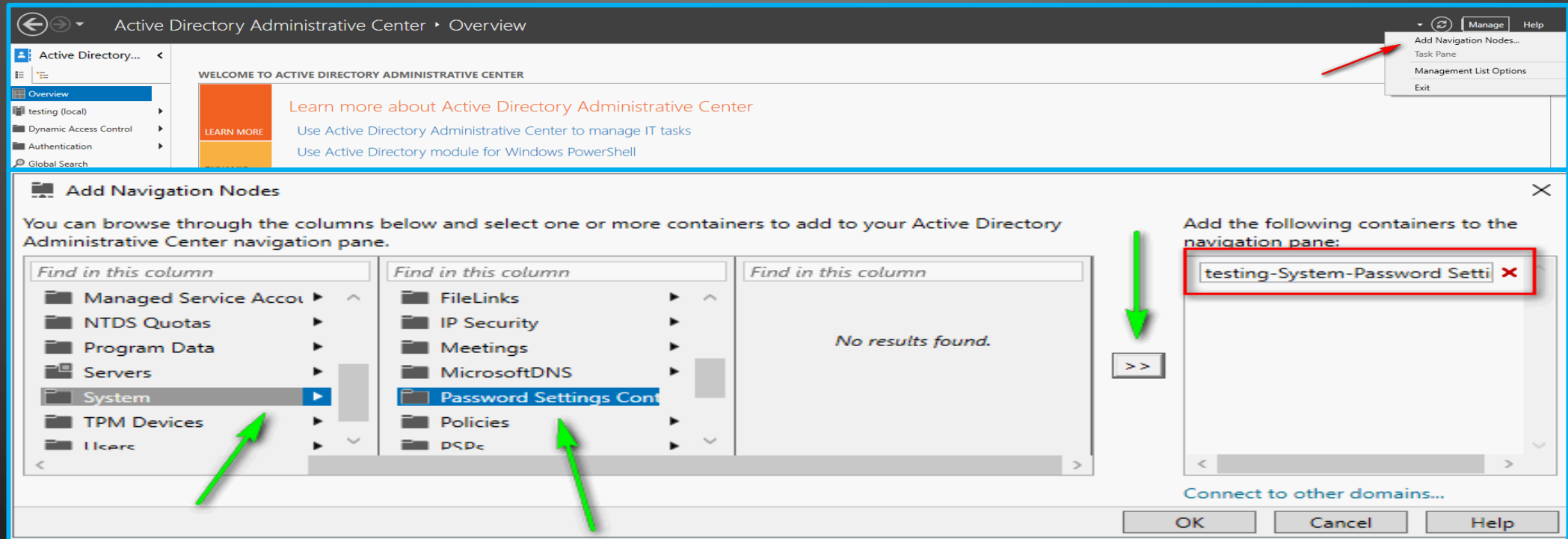
Prioritize password length over password complexity

WEAK PASSWORD POLICIES FOR ADMINISTRATIVE ACCOUNTS (AND NON-ADMIN ACCOUNTS) - PROBLEM



Traditional password policy in Group Policy Management Console

WEAK PASSWORD POLICIES FOR ADMINISTRATIVE ACCOUNTS - SOLUTION



Fine Grain Password Policies in Active Directory Administrative Center

WEAK PASSWORD POLICIES FOR ADMINISTRATIVE ACCOUNTS (AND NON-ADMIN ACCOUNTS) - SOLUTION

Create Password Settings: Administrator-Require-Strong-Passwords

Tasks: Sections

Password Settings

Directly Applies To

Name: * Administrator-Require-Strong-Passwords

Precedence: * 1

☒ Enforce minimum password length

Minimum password length (characters): * 20

☒ Enforce password history

Number of passwords remembered: * 5

☒ Password must meet complexity requirements

☐ Store password using reversible encryption

☒ Protect from accidental deletion

Description: Admin 20 character password policy

Password age options:

☒ Enforce minimum password age

User cannot change the password within (days): * 1

☒ Enforce maximum password age

User must change the password after (days): * 90

☒ Enforce account lockout policy: YES!!!

Number of failed logon attempts allowed: * 3

Reset failed logon attempts count after (mins): * 30

Account will be locked out

☐ For a duration of (mins): * 30

☒ Until an administrator manually unlocks the account

Directly Applies To

Name	Mail
Require-Strong-Passwords	

Add... Remove

More Information

OK Cancel

Fine Grain Password Policies in Active Directory Administrative Center

WEAK PASSWORD POLICIES FOR ADMINISTRATIVE ACCOUNTS (AND NON-ADMIN ACCOUNTS) - SOLUTION

Create Password Settings: User-Require-Strong-Passwords

Tasks Sections

Password Settings

Directly Applies To

Name: * User-Require-Strong-Passwords

Precedence: * 2

☒ Enforce minimum password length

Minimum password length (characters): * 16

☒ Enforce password history

Number of passwords remembered: * 5

☒ Password must meet complexity requirements

☐ Store password using reversible encryption

☒ Protect from accidental deletion

Description: User 16 character password policy

Still NO^3!

Still YES!!!

Enforce account lockout policy: ☒

Number of failed logon attempts allowed: * 5

Reset failed logon attempts count after (mins): * 30

Account will be locked out: * 30

☒ For a duration of (mins):

☐ Until an administrator manually unlocks the account

Directly Applies To

Name Mail

Domain Users

Add...

Remove

More Information

OK Cancel

Fine Grain Password Policies in Active Directory Administrative Center

WEAK PASSWORD POLICIES FOR ADMINISTRATIVE ACCOUNTS (AND NON-ADMIN ACCOUNTS) - SOLUTION

- Enforce “NoLMHash” on your endpoints
 - HKLM\System\CurrentControlSet\Control\Lsa\NoLmHash DWORD 0x0000001 (then force password change)
- Passwords over 15 characters break LANMAN hash
- Passwords 20 characters in length become exponentially difficult to crack
 - with modern computing resources. This will change...
- Have a strong password policy or policies (16 for users, 20 char for admin)
- Enforce Lockout Threshold, Intervention for admin accounts
- Password Spray regularly to catch bad passwords

WEAK PASSWORD POLICIES FOR ADMINISTRATIVE ACCOUNTS (AND NON-ADMIN ACCOUNTS)

```
C:\Temp> Invoke-DomainPasswordSpray -Password P@ssword
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] A total of 2 Fine-Grained Password policies were found.

[*] Fine-Grained Password Policy titled: Administrator-Require-Strong-Passwords has a Lockout Threshold of 3 attempts, minimum password length of 20 chars, and applies to CN=Require-Strong-P
asswords,DC=testing,DC=local.

[*] Fine-Grained Password Policy titled: User-Require-Strong-Passwords has a Lockout Threshold of 5 attempts, minimum password length of 16 chars, and applies to CN=Domain Users,CN=Users,DC=
testing,DC=local.

[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] Removing disabled users from list.
[*] There are 4 total users found.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 4 users gathered from the current user's domain
[*] The domain password policy observation window is set to 30 minutes.
[*] Setting a 30 minute wait in between sprays.
[*] Password spraying has begun with 1 passwords
[*] This might take a while depending on the total number of users
[*] Now trying password P@ssword against 4 users. Current time is 1:19 AM
[*] Writing successes to
[*] SUCCESS! User:Administrator Password:P@ssword
1 of 4 users tested[*] SUCCESS! User:secmoto Password:P@ssword
2 of 4 users tested[*] SUCCESS! User:tyler.durden Password:P@ssword
3 of 4 users tested[*] SUCCESS! User:Lazarus.Group Password:P@ssword
4 of 4 users tested[*] Password spraying is complete

C:\Temp> |
```

- <https://github.com/dafthack/DomainPasswordSpray>
- Credit to Beau Bullock @dafthack

@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/CRASHOVER1D3)

PASSWORDS ARE LIKE UNDERPANTS

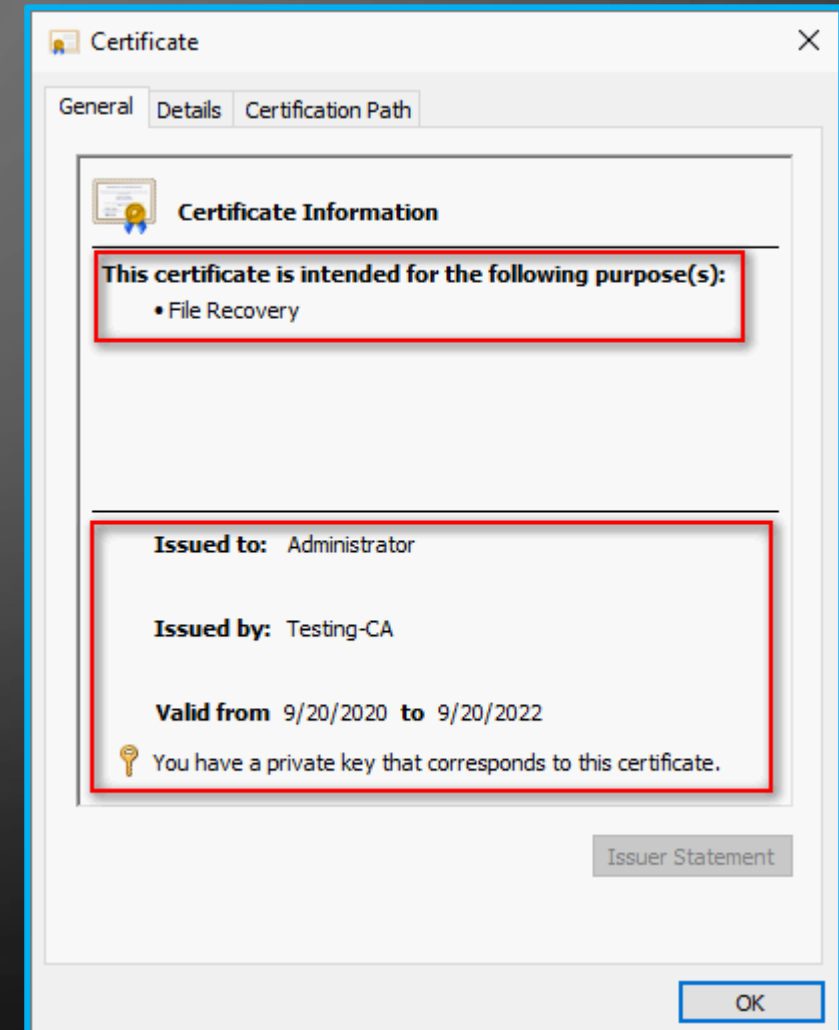
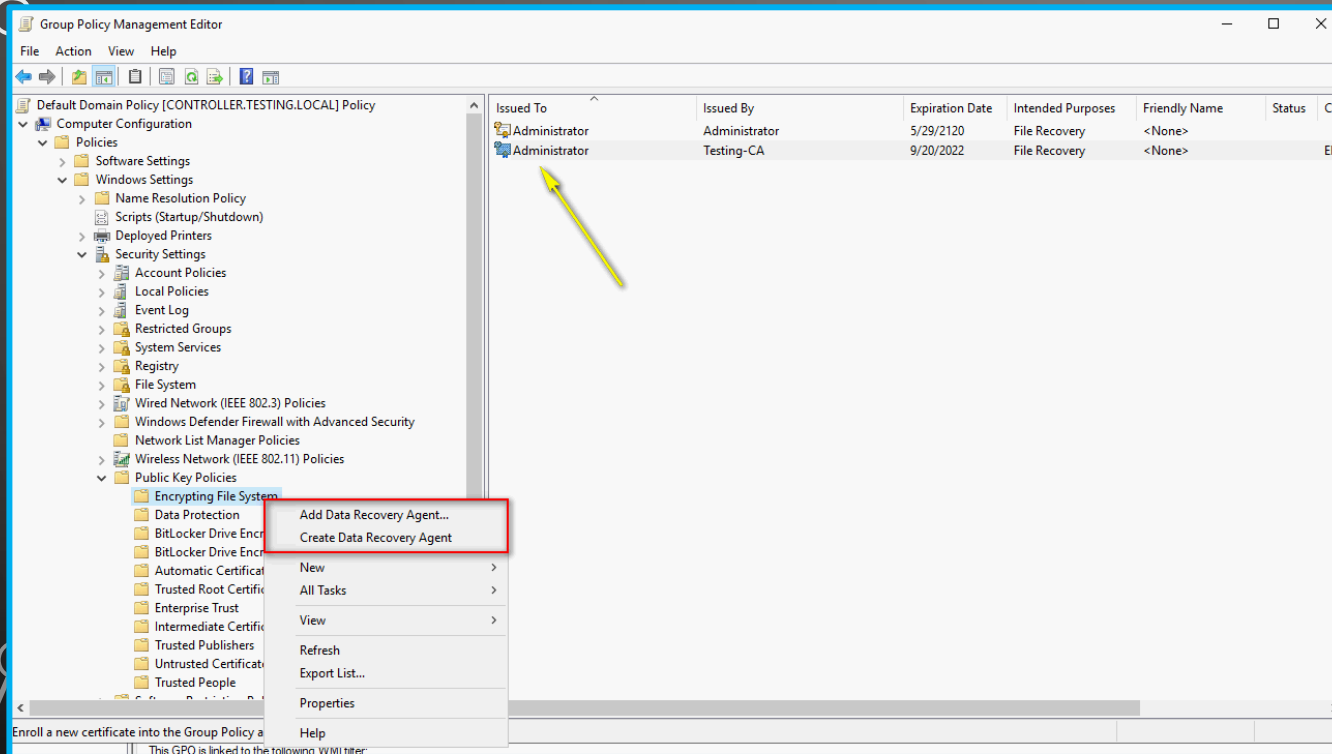


Change them often, keep them private and never share them with anyone.

LIMITING RISK FROM EFS RANSOMWARE

- Built into Windows Operating systems, Native to NTFS
- Encrypted CA cert or self-signed (Domain or Workgroup)
- Can only be decrypted by corresponding cert or the EFS Recovery agent private key
- Live by the sword, die by the sword
- Set up EFS Recovery Cert, even if you do not use EFS encryption

LIMITING RISK FROM EFS RANSOMWARE - SOLUTION



EFS will encrypt the private key of the encrypting cert, with the public key of your EFS recovery cert as a safety mechanism.

@CRASHOVERRIDE3

[HTTPS://GITHUB.COM/CRASHOVERRIDE3](https://github.com/crashoverride3)

CLOSING THOUGHTS...



ACKNOWLEDGEMENTS

Jason Fossen, @JasonFossen

- www.bluetempowershell.com
- Black Hills Information Security
 - <https://www.blackhillsinfosec.com/30-things-to-get-you-started/>
- Beau Bullock, @dafthack
 - <https://github.com/dafthack/DomainPasswordSpray>

@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/CRASHOVER1D3)

LIMITING ADMIN USER RISK IN A WINDOWS ENVIRONMENT

AND OTHER TIPS TO AVOID MAKING THE NEWS

THANK YOU INFOSEC 716 MEETUP!

- Twitter: Blake Regan [@crashOver1d3](#)
- Github: <https://github.com/crashOver1d3>
- LinkedIn: <https://www.linkedin.com/in/blakerregan>
- Upcoming website/blog: www.blueteamtactics.net
-Blue Team, Carpentry, Bar-b-que

@CRASHOVER1D3
[HTTPS://GITHUB.COM/CRASHOVER1D3](https://github.com/crashOver1d3)