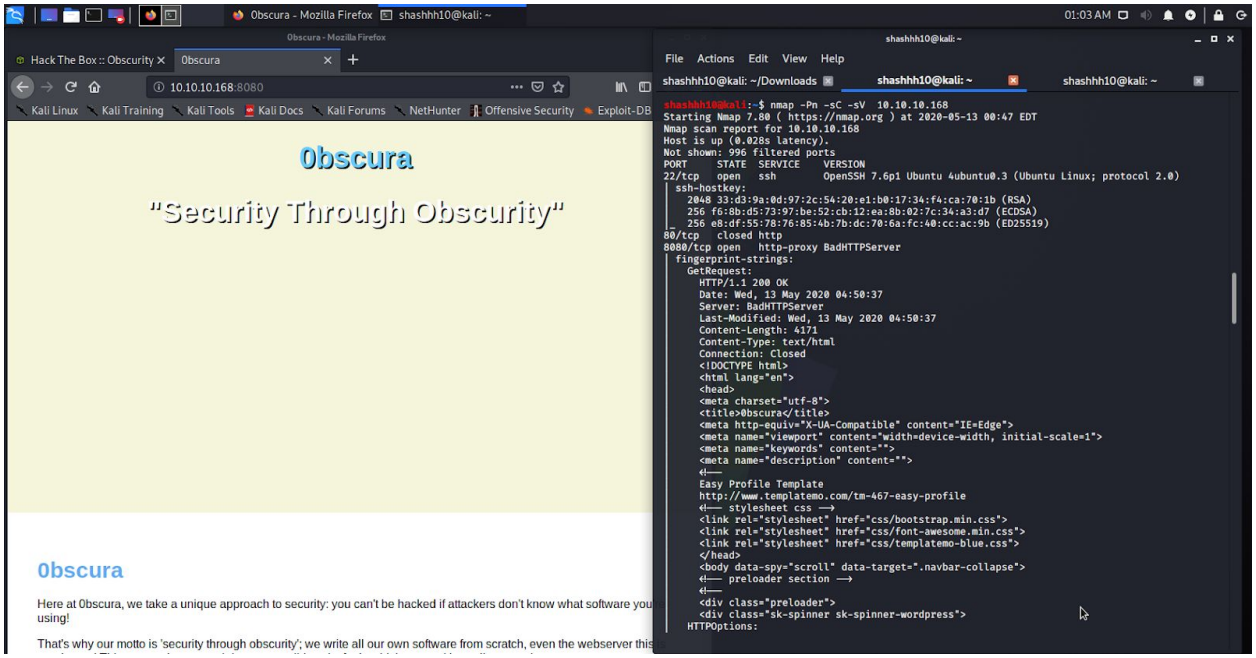
Hack The Box: Obscurity
//My second hack the box exploitation. Great experience.

Exploiting a vulnerable machine at target IP 10.10.10.168 known as Obscurity

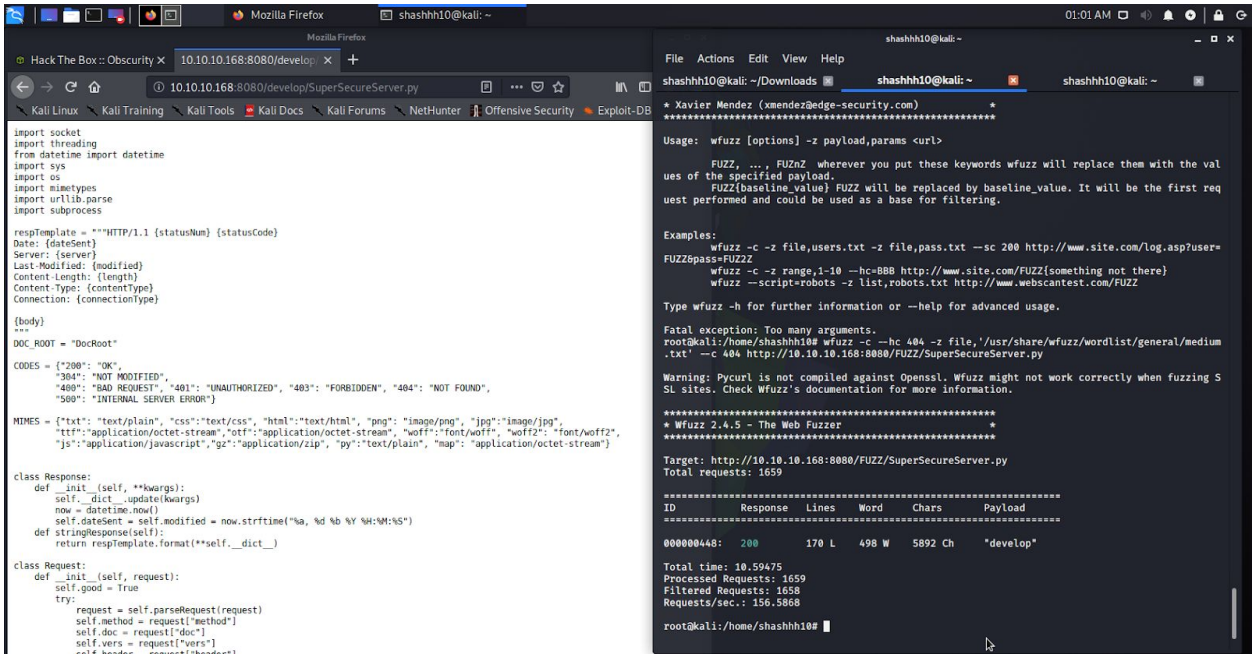
Strategy:
Compromise the vulnerable machine in order to gain privileged access for the root.

Tactics:

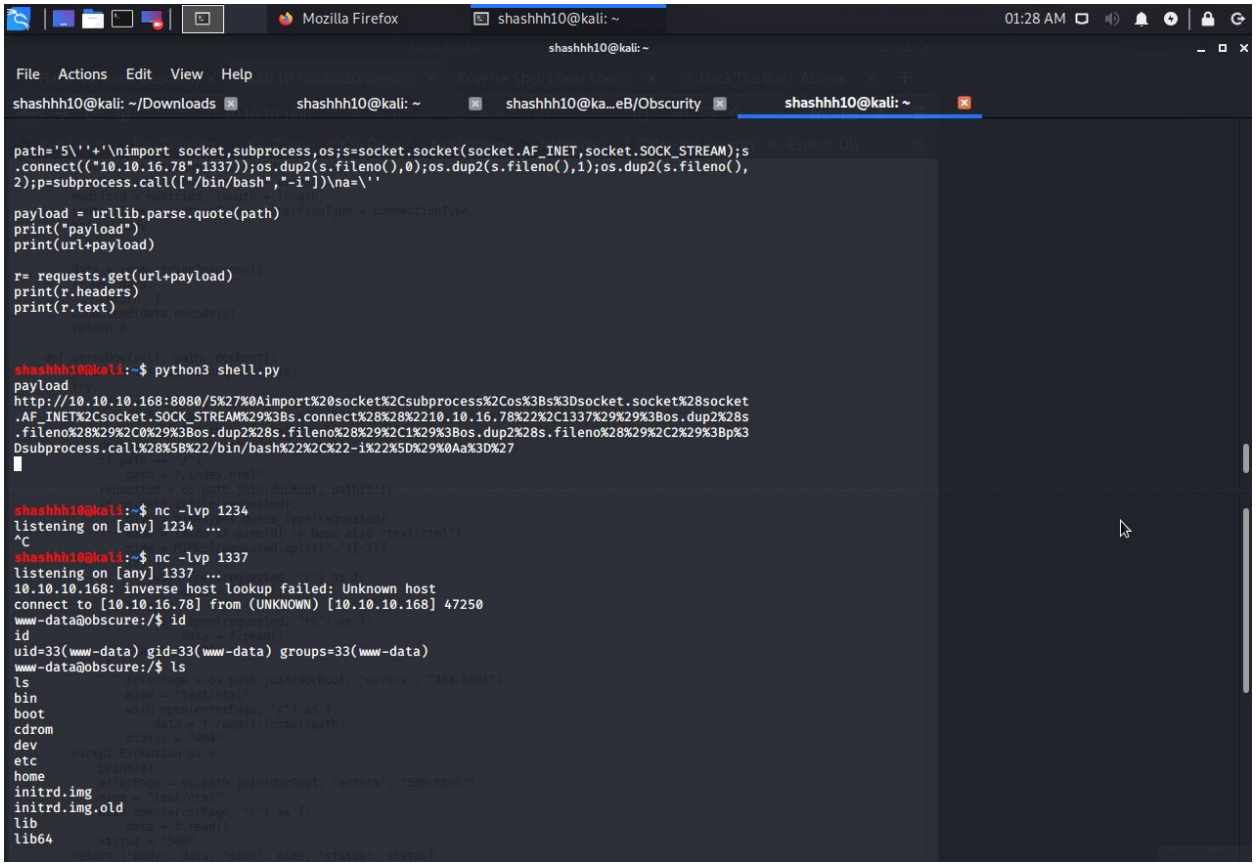
1. Perform a network scan. Using nmap to discover target Ip 10.10.10.168. Scanning it for all the vulnerable ports with Nikto and checking all the accessible directories with dirb. It had an open ssh service at port 22. A website on port 8080 using an Apache service.



2. Got access to 8080 port which had a website running on it but no active directories or scripts showing up. The Website has a SuperSecureServer.py but of no essential use.
Used the Wfuzz tool to bruteforce any active directories or scripts. And yes got access to the /develop/SuperSecureServer.py script

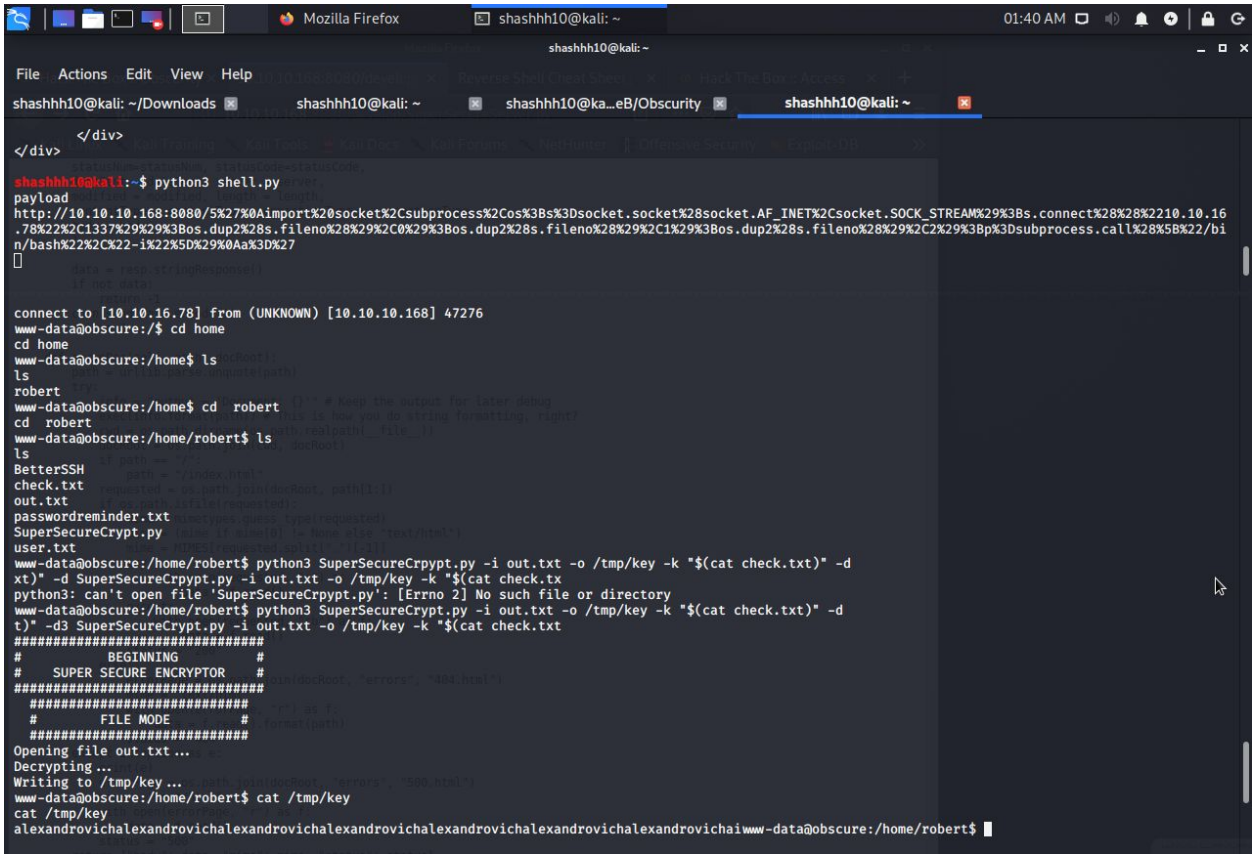


3. The one way I could think of getting access to the shell was using some type of code injection method. Since it was a python script, it used a reverse python shell to inject it to the specific target Up with the specified port at the listener’s end. (TCP connection)
Used netcat to import the script. Gained access to the shell.



4. While enumeration, the following files were encrypted so had to decrypt it. Used the following command to decrypt it.

```
python3 SuperSecureCrypt.py -i out.txt -o /tmp/key -k "$(cat check.txt)"
-d
```



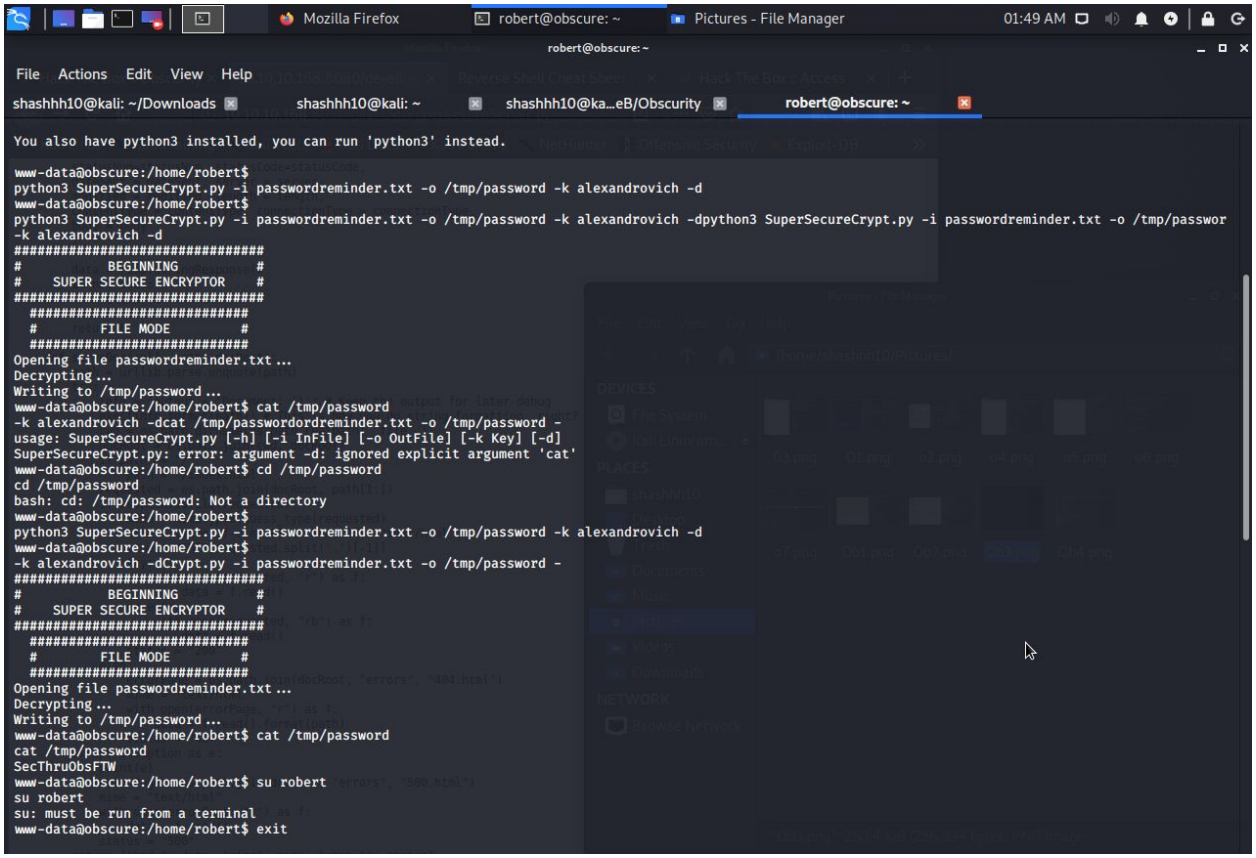
Got access to some username “alexandrovich”

5. Also encrypted the password.txt file using the following command

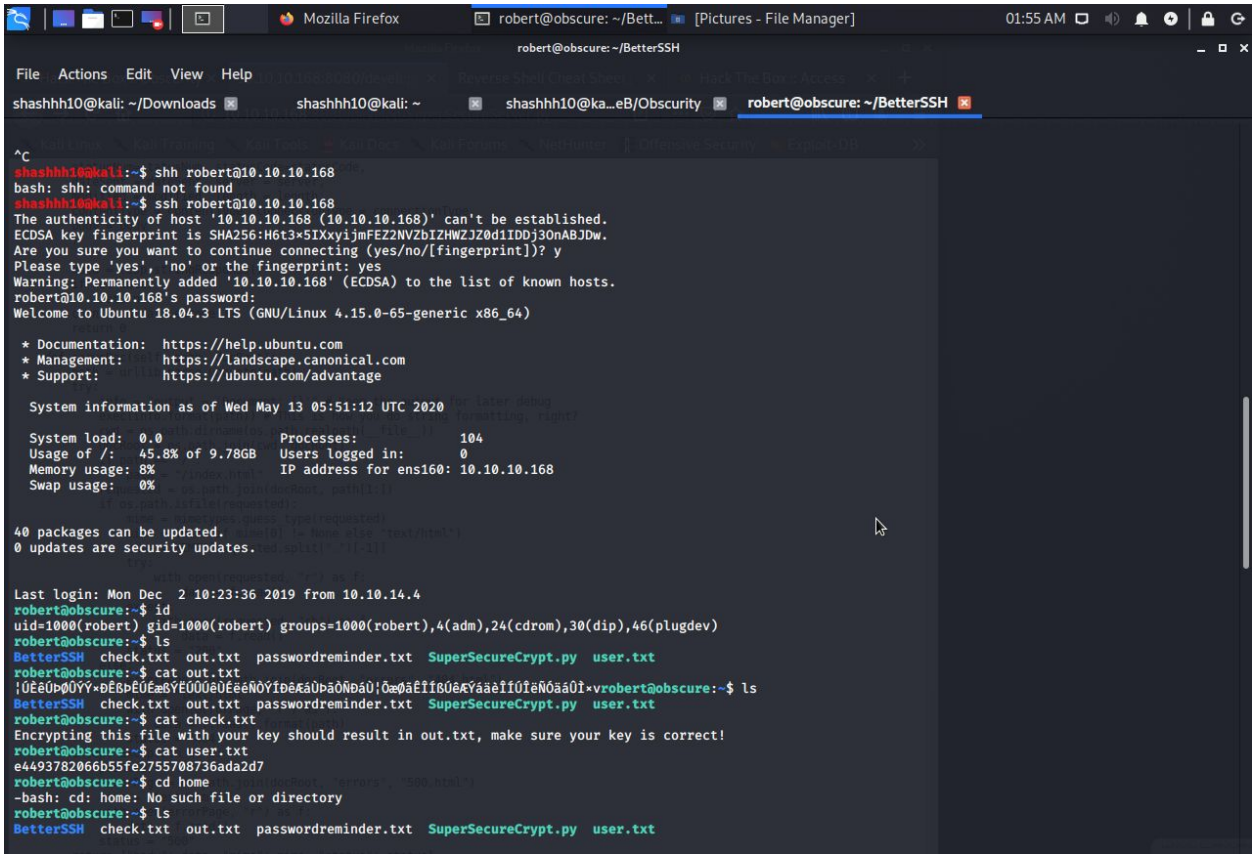
python3 SuperSecureCrypt.py -i passwordreminder.txt -o /tmp/password -k alexandrovich -d

Got access to username “robert” with password “SecThruObsFTW” from the decrypted password.txt file.

Logged in with username robert and his credentials using the ssh login.



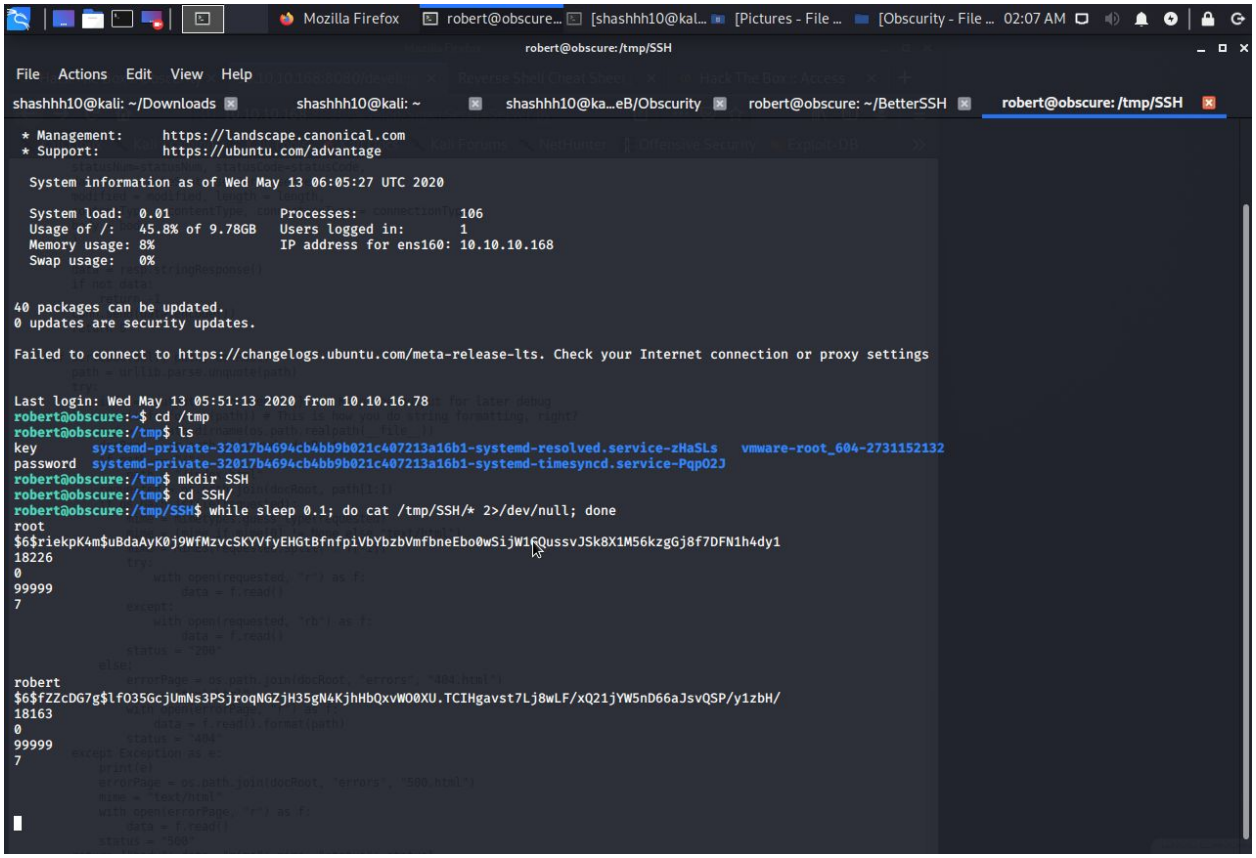
6. Gained access to the user.txt file. And exfiltrated it.



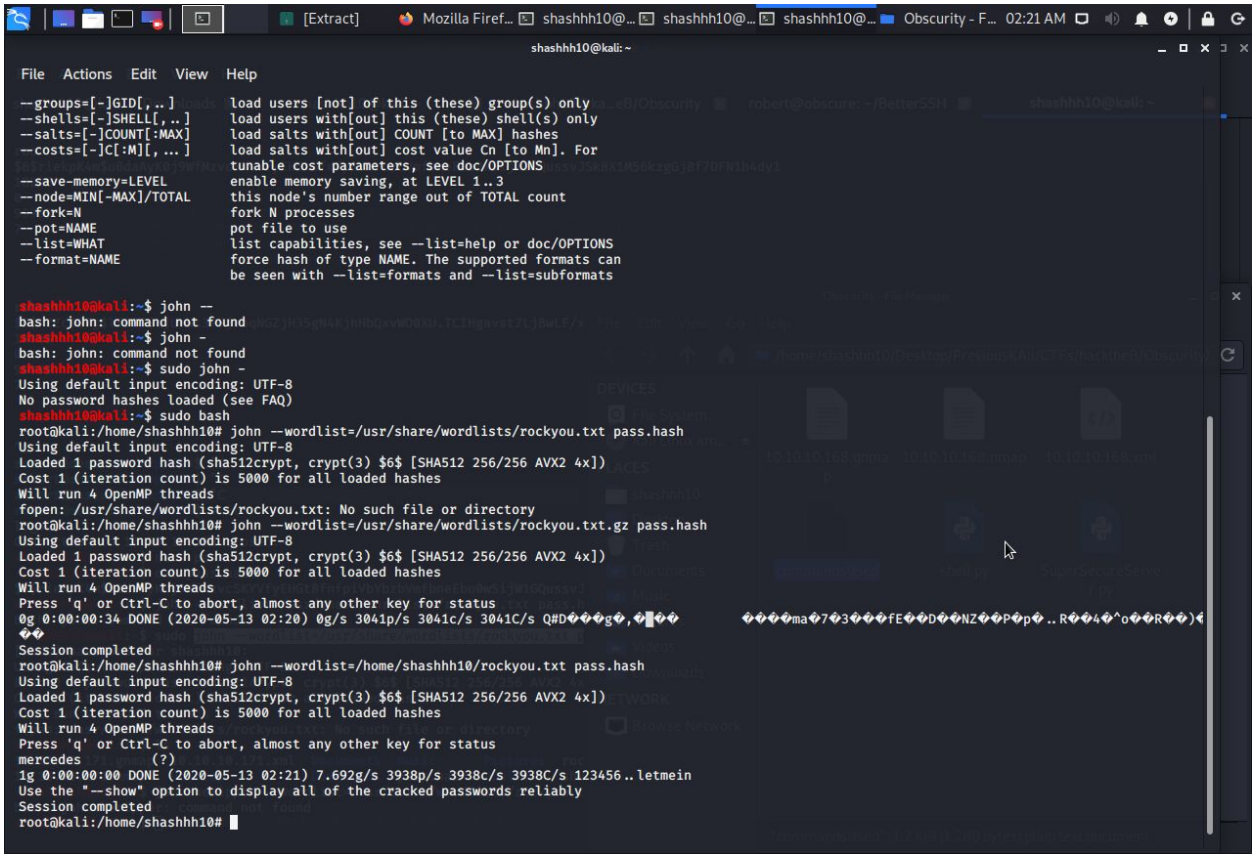
7. Enumerate privilege escalation for root. “Sudo -l”
The /BetterSSH.
User “Robert” has permission to run Betterssh.py
Made a directory SSH inside the /tmp
For some reason the script copies the output of the shadow file ot the /tmp/SSH/

Using watch, run a command which let’s us set an interval to 0.1 sec and we can grab a copy of the credentials of root and robert.

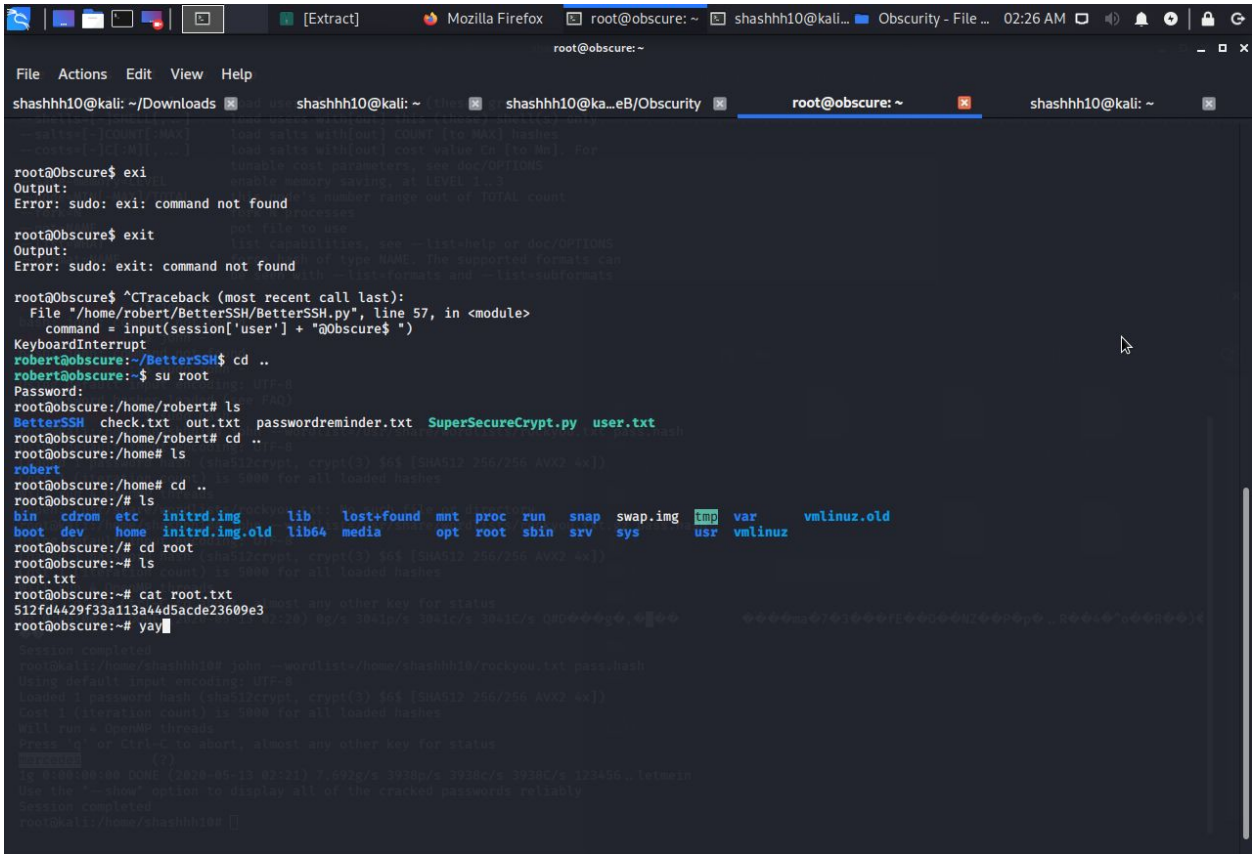
“while sleep 0.1; do cat /tmp/SSH/* 2>/dev/null; done”



8. We now have the hash of root. Copied the hash to a file “pass.hash”.
Used “John” to crack the hash using the rockyou.txt file.
Gained access to the credentials. Password = “mercedes”



9. Logged in as root with root credentials “mercedes”. Exfiltrated the root.txt file.



----------*End-of-HTB*----------