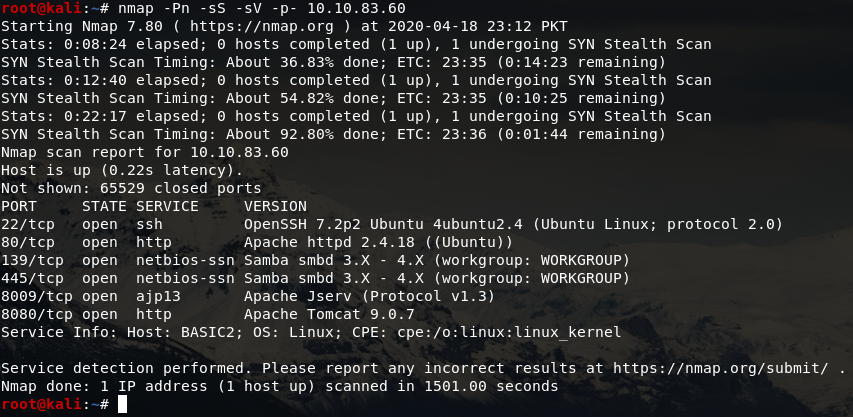
**TryHackMe:Basic Pentesting Write-Up**

Deploy the machine from “Start Machine” button as shown in figure

You will get a IP Address for machine



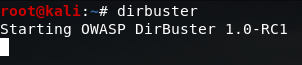
Your IP should be Different from mine. After getting your IP scan the machine with namp.

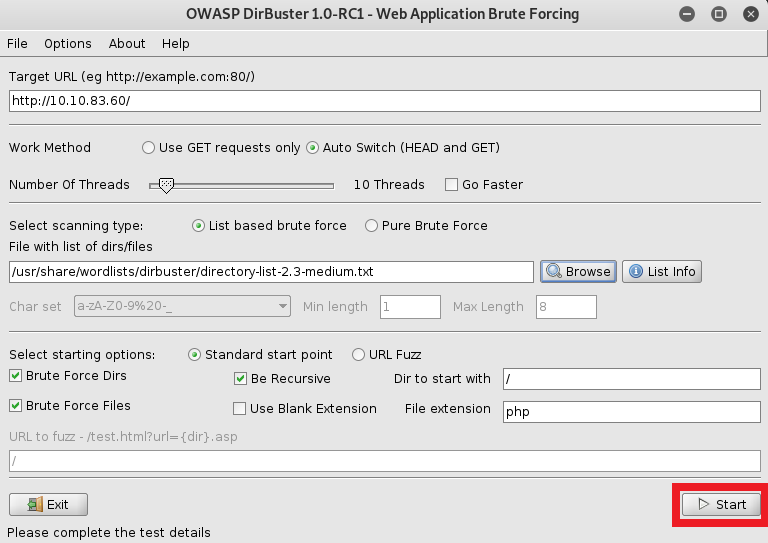
**nmap -Pn -sS -sV -p- 10.10.83.60**

**Search the Machine IP in Search Box**



For Finding Hidden directories we will run Dirbuster. You can start it from applications or use the following command.It is GUI based Tool

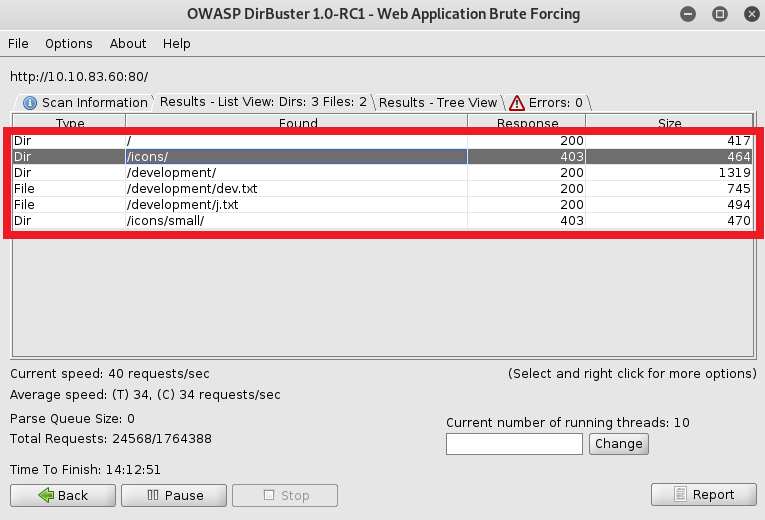




Paste your IP in Targeted URL tab. After that load your directory file.

NOTE: you have pre-installed directory on kali linux or you can use any directory available on web.

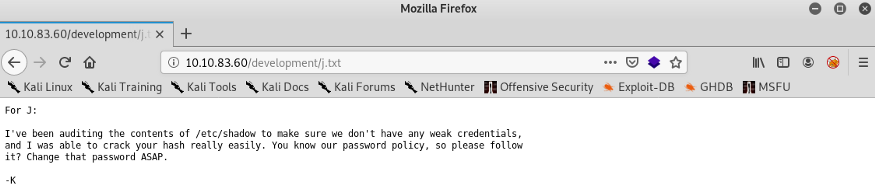
After Configuring Hit the start button.



You can see we have got the list of Hidden Directory. Check all this Dir one by one.

We have found an interesting Dir /development/dev.txt AND /development/j.txt



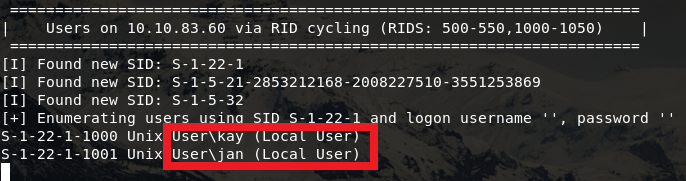


After reading this we got some cluse

1. SMB has been configured.
2. There is Apache struts version 2.5.12 running.
3. User **J** is using weak password which can be cracked easily.

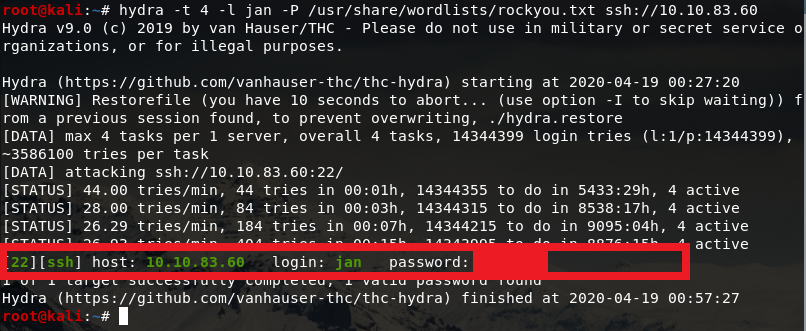
Let’s start enumerating SMB port with enum4linux tool:

**enum4linux -a 10.10.83.60**

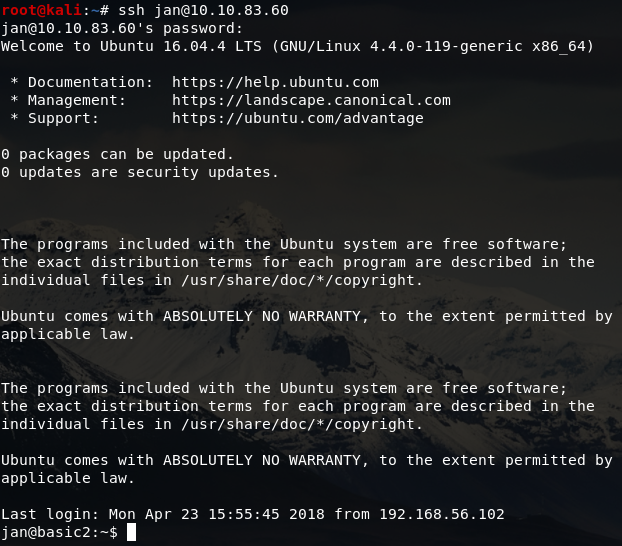


Now we got both usernames now let’s bruteforce attack on both of the users using famous tool HYDRA. You can also use john.

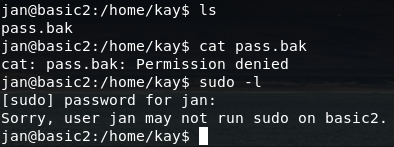
**hydra -t 4 -l jan -P /directory\_path/rockyou.txt ssh://10.10.83.60**



let’s try to login now.

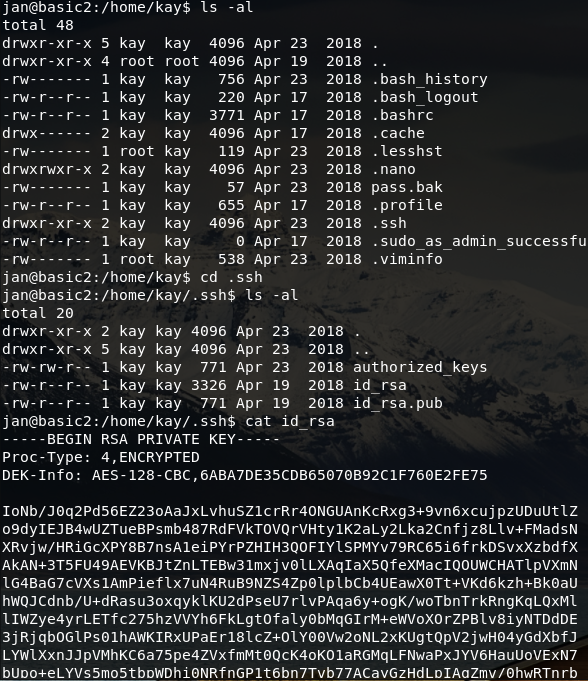


We have successfully login. Now explore this machine especially Kay’s account .We have found password backup file of the Kay’s account but unfortunately we do not have privileges on jan account to see them neither jan can sudo command.



To read the password backup file we have to escalate the privileges.

We found something after Digging Deep



Save this KEY on your device and run ssh2john to get the HASH.

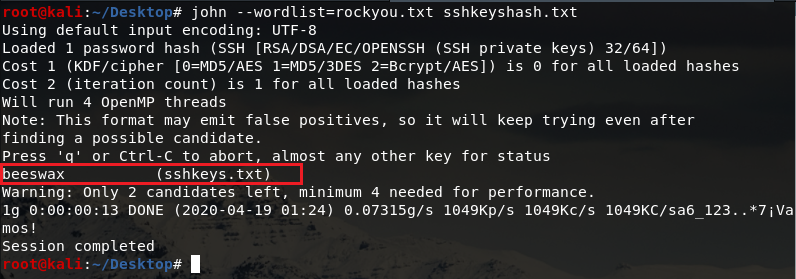
**python /usr/share/john/ssh2john.py sshkeys.txt > sshkeyshash.txt**



Now run John the ripper tool to crack the HASH.

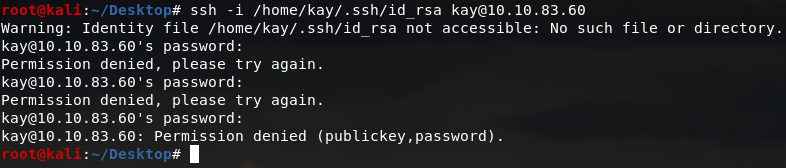
**john --wordlist=rockyou.txt sshkeyshash.txt**

I have used rockyou file.

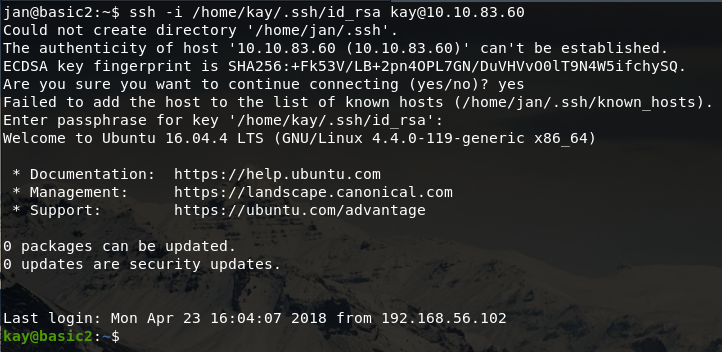


Now access the kay’s ssh using this public key

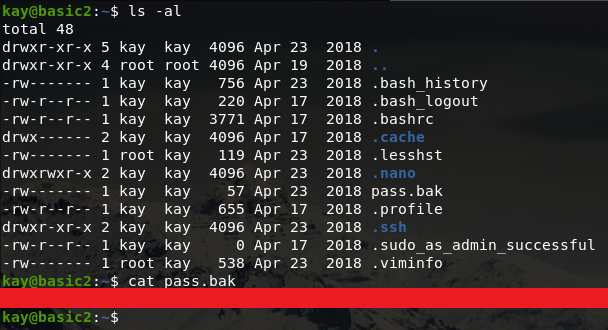
**ssh -i /home/kay/.ssh/id\_rsa kay@10.10.83.60**



We tried to access Kay’s ssh directly but unsuccessful.Now we will try to access from Jan’s account. First login ssh of jan account then type same command:

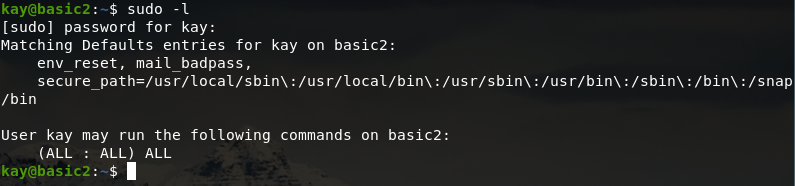


After successfully logged in into Kay’s ssh, lets go to that password backup file and read the content of it.



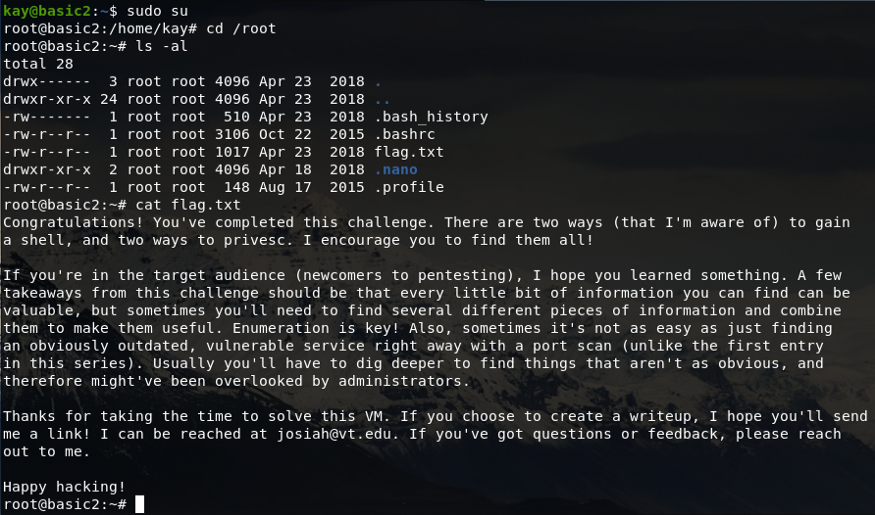
We got the Password. escalate the privilege from kay’s account.

**sudo -l**



kay have all of the sudo privileges, so we try to execute command:

**sudo su**



As per this we have got the flag.txt and have completed this room.