Whenever you are proceeding with web penetration testing, always start with nmap scanning to find out open ports and further possible scannings or attackings associated with it.

First command in this machine **nmap -Pn -Ss <ip addr>**

From there we found that port number **443** is open and that is of **SMB**

Browse http://<ip addr>

And we found that site is under construction, so it further proceed with inspecting the source code. Here we got a hint that “Check our dev note section if you need to know what to work on”, we tried with random /dev directory but failed so use dirbuster or gobuster to find hidden directories.

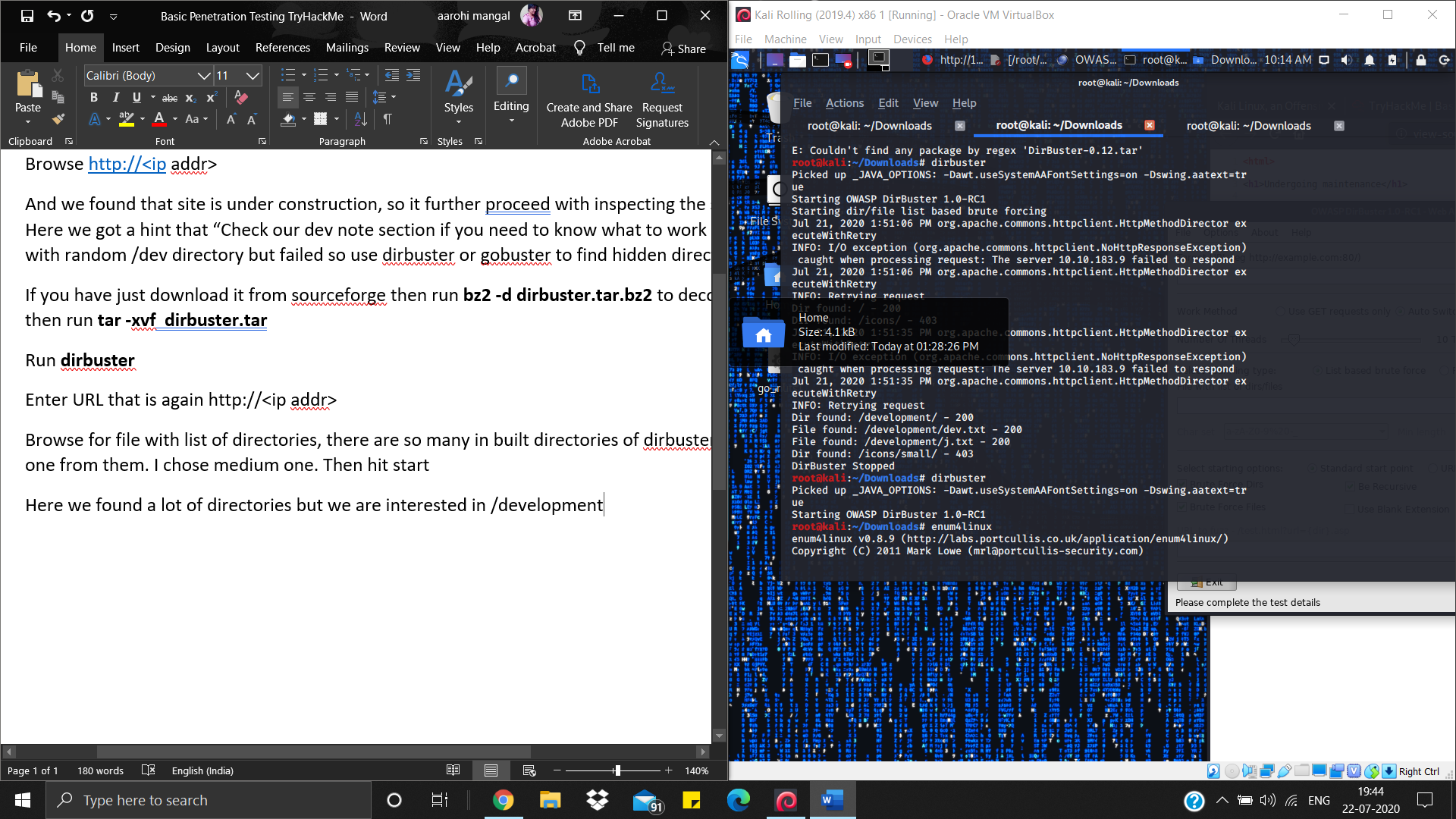
If you have just download it from sourceforge then run **bz2 -d dirbuster.tar.bz2** to decompress it then run **tar -xvf dirbuster.tar**

Run **dirbuster**

Enter URL that is again http://<ip addr>

Browse for file with list of directories, there are so many in built directories of dirbuster, choose any one from them. I chose medium one. Then hit start

Here we found a lot of directories but we are interested in /development

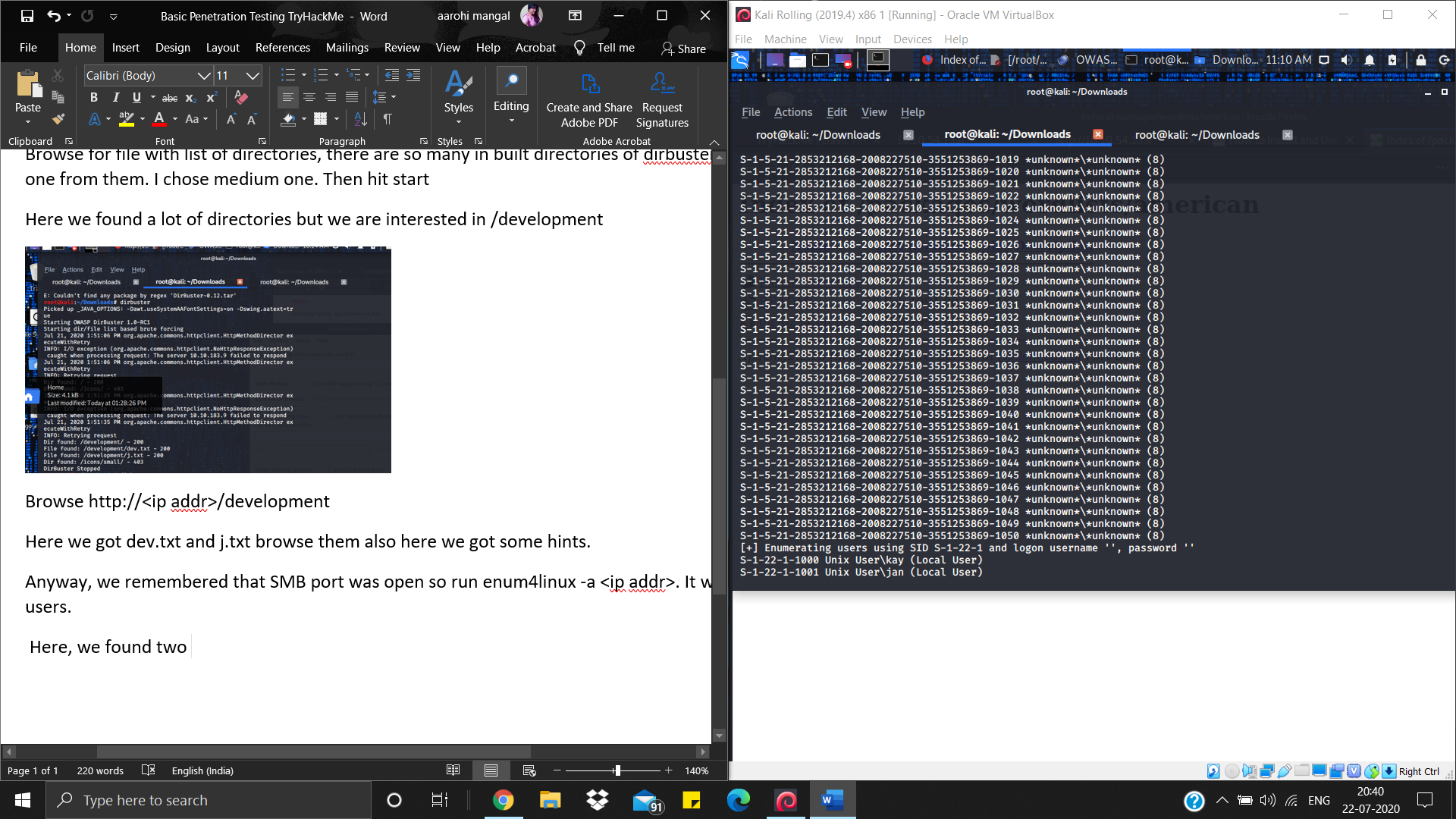


Browse http://<ip addr>/development

Here we got dev.txt and j.txt browse them also here we got some hints.

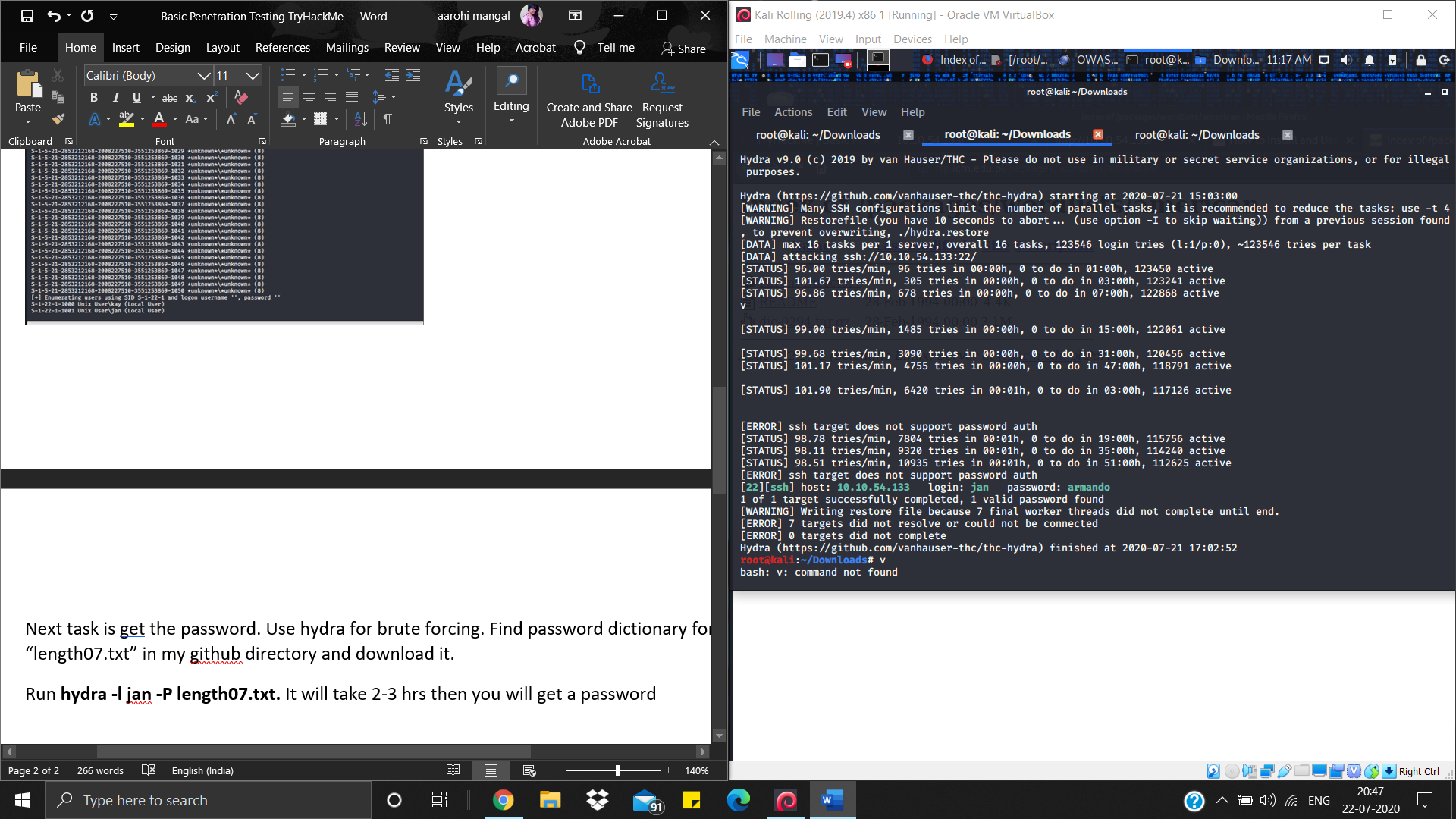
Anyway, we remembered that SMB port was open so run enum4linux -a <ip addr>. It will list the users.

Here, we found two users jan and kay



Next task is get the password. Use hydra for brute forcing. Find password dictionary for 7 characters “length07.txt” in my github directory and download it.

Run **hydra -l jan -P length07.txt <ip addr>.** It will take 2-3 hrs then you will get a password



Run **ssh jan@<ip addr>** to log in into his machine

Enter password.

Run **pwd** to see current directory

Run **cd ..** two times to get of home/jan

Run **cd etc/passwd**

Here we see that home/kay

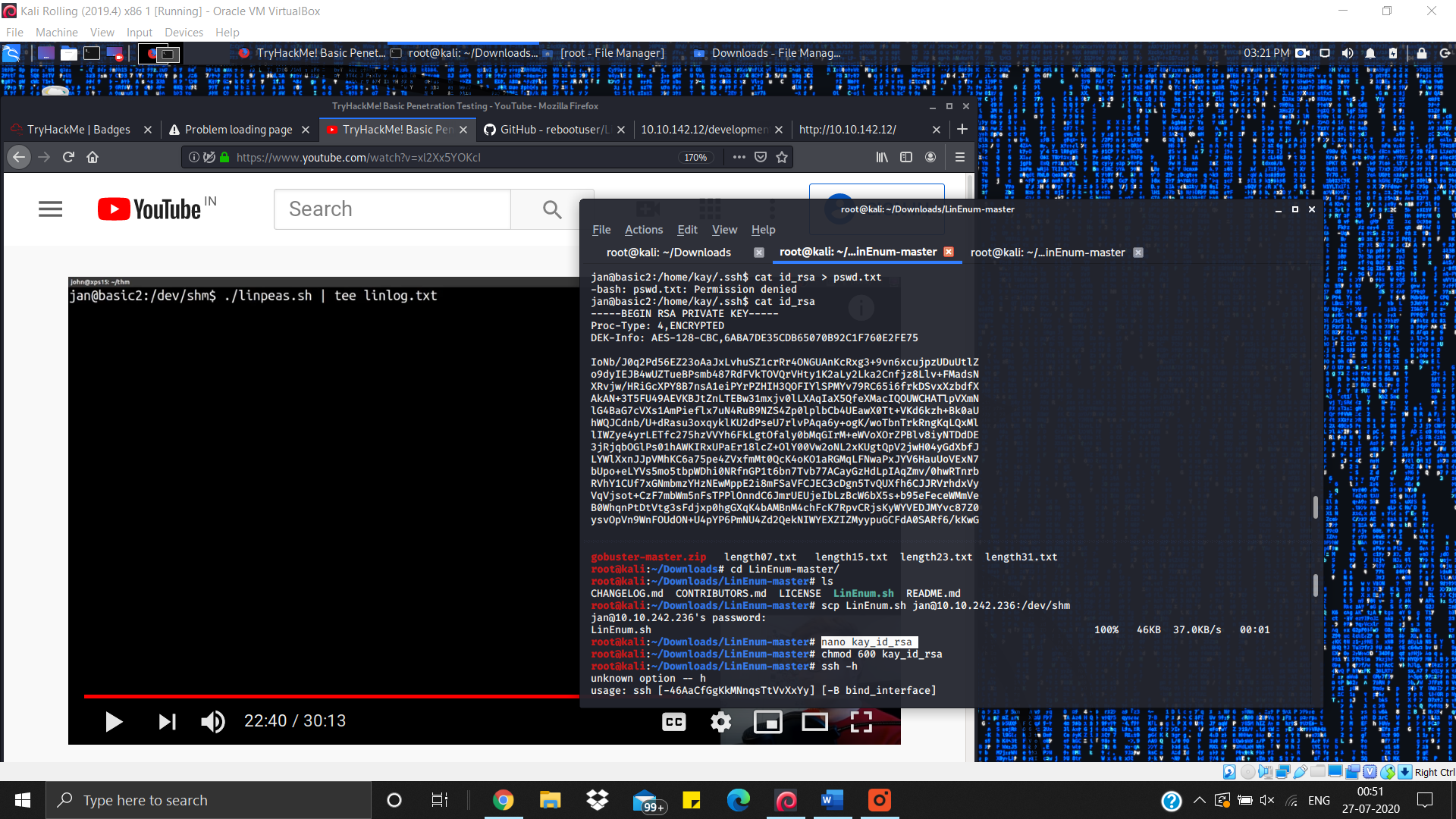
Get into this directory using the command cd home/kay

Run **ls**, and we got *pass.ba*k file but after running **ls -la** command, we got to know that only Kay have permissions to access that file.

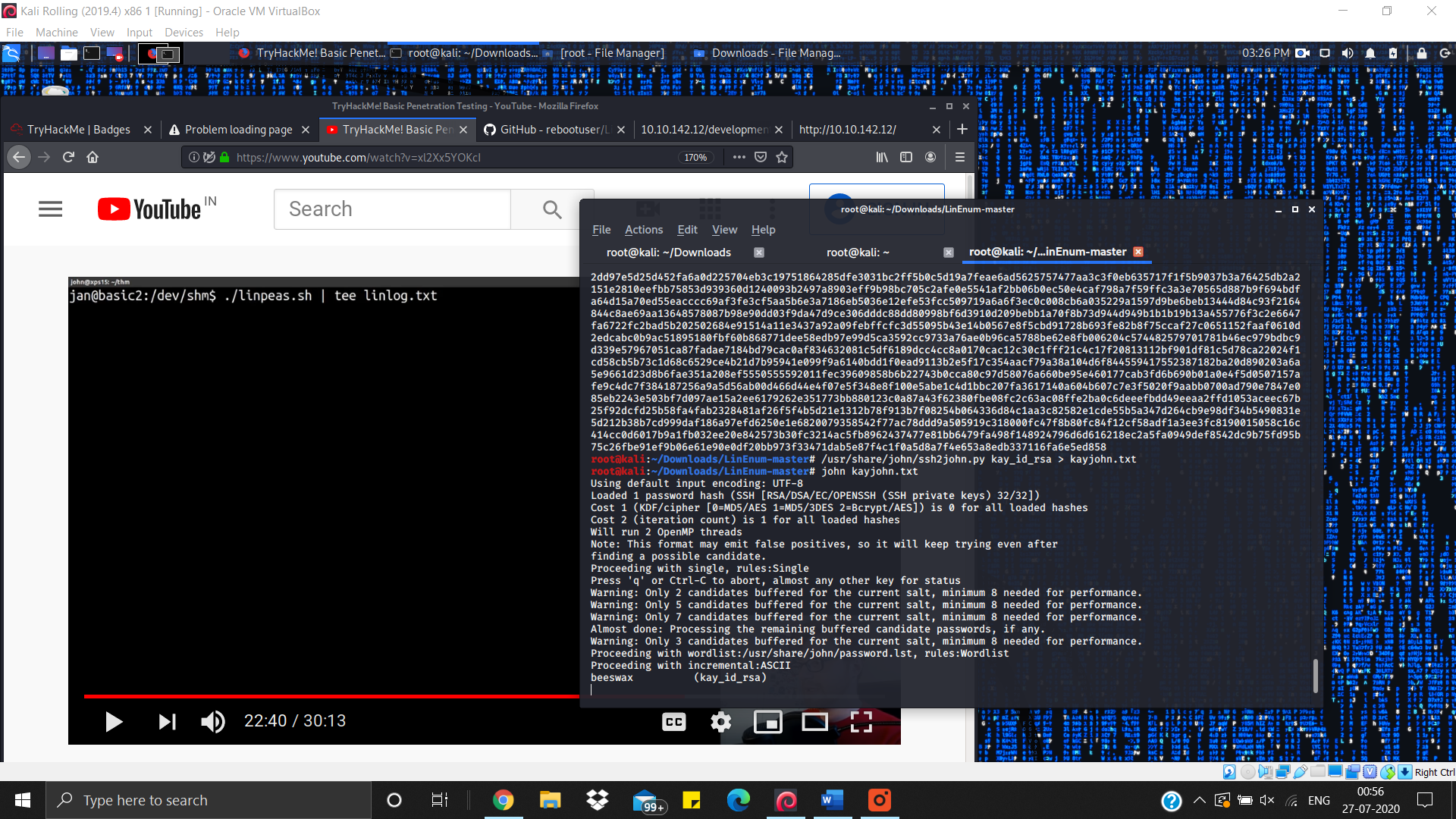
Download LinPeas. To get remote access to LinPeas from Jan’s machine run **scp LinEnum.sh jan@10.10.242.236:/dev/shm** . Now make it executable by running **chmod +x linpeas.sh**

Run **./linpeas.sh**

Here we get that .ssh directory contains id\_rsa named file. Run **cat id\_rsa** and save it into a file in your system.



**ssh -i kay\_id\_rsa** [**kay@10.10.242.236**](mailto:kay@10.10.242.236) run this command to login into kay’s system but we need a passphrase here. So run **/usr/share/john/ssh2john.py kay\_id\_rsa > kayjohn.txt** to save the form of rsa which can be understood by john the ripper in kayjohn.txt. Run kayjohn.txt and here we got Kay’s system password



Enter this passphrase to login. Traverse to the directory containing pass.bak file. Hit **cat pass.bak** and passwork is there on your screen.

