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.

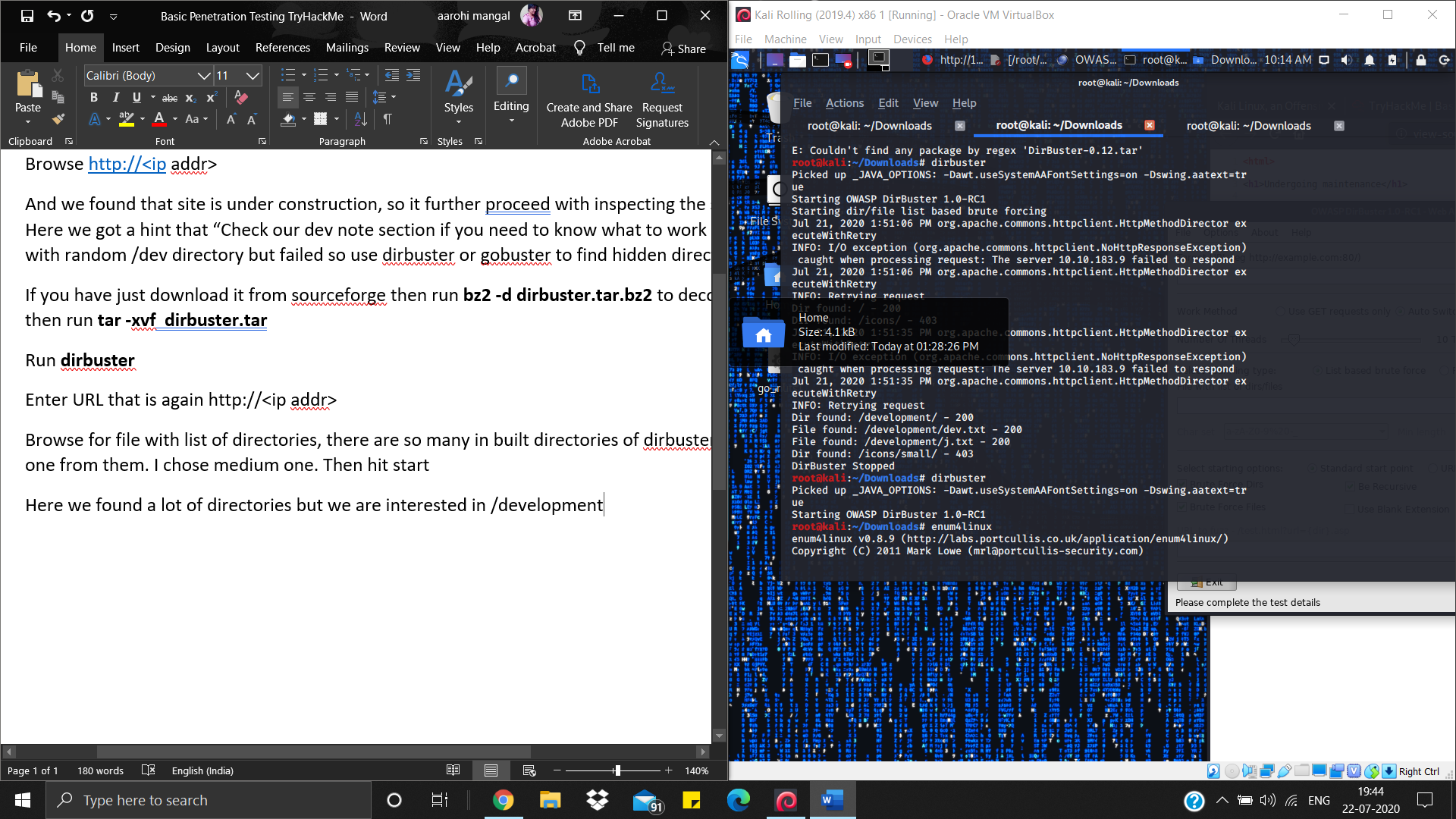
If you have just download it from sourceforge then run **bz2 -d dirbuster.tar.bz2** to decompress it then run **tar -xvf dirbuster.tar**

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

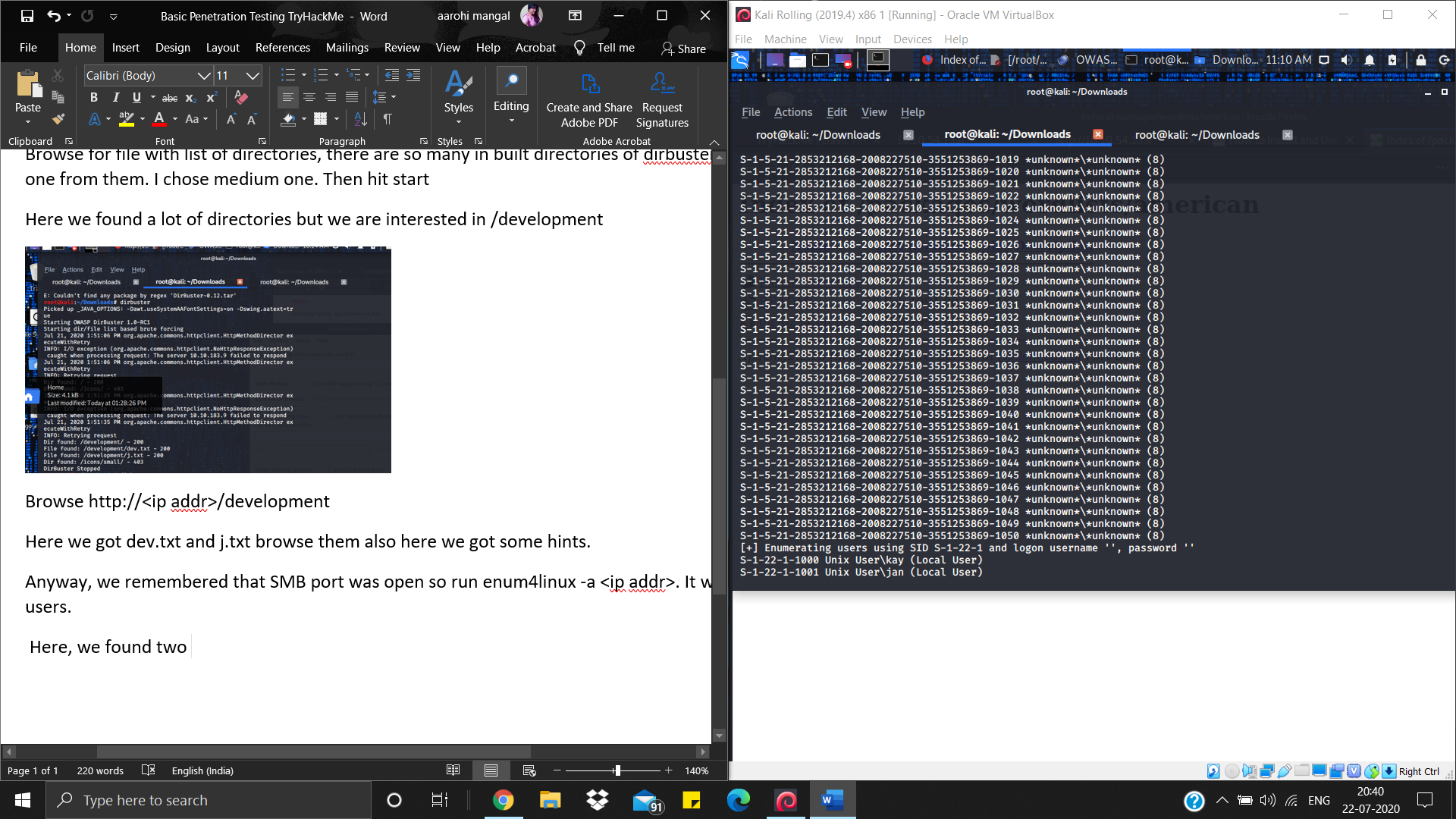


Browse http://<ip addr>/development

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.** It will take 2-3 hrs then you will get a password

