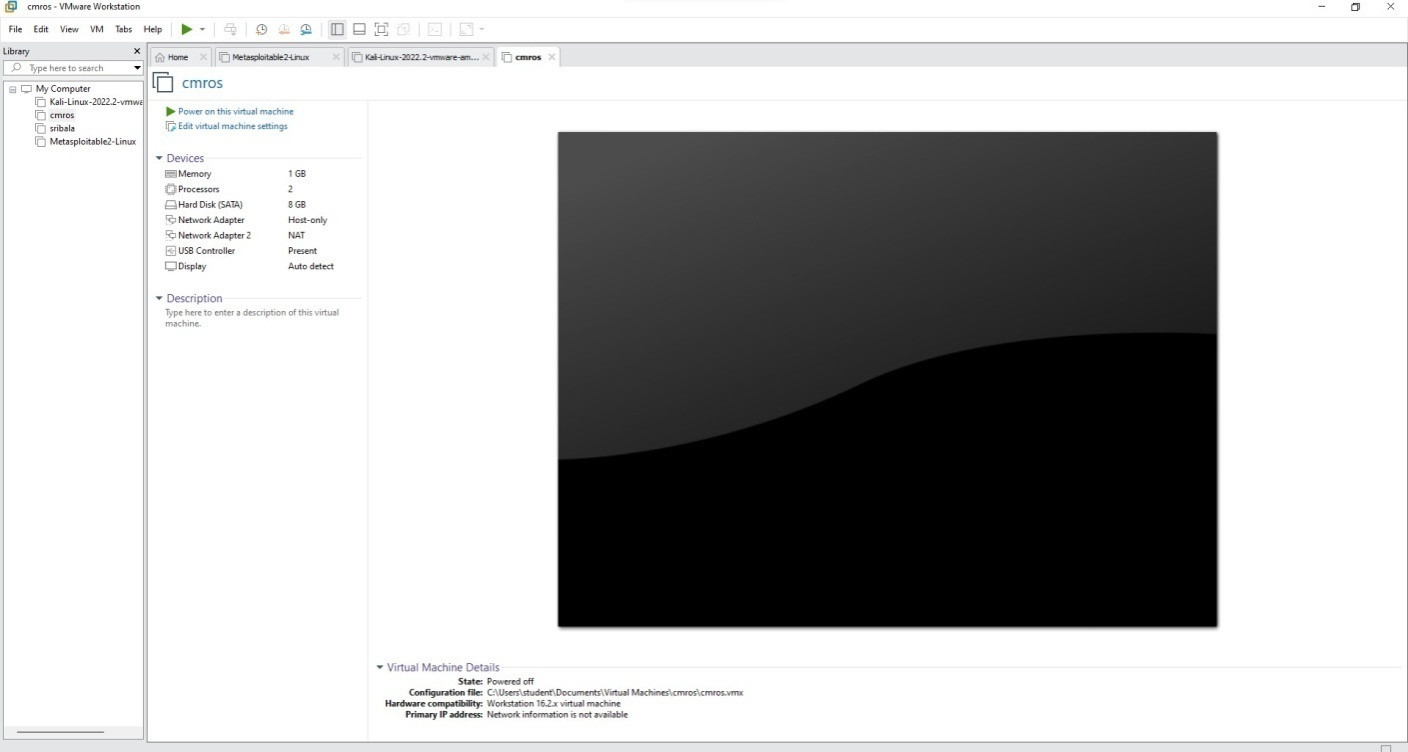
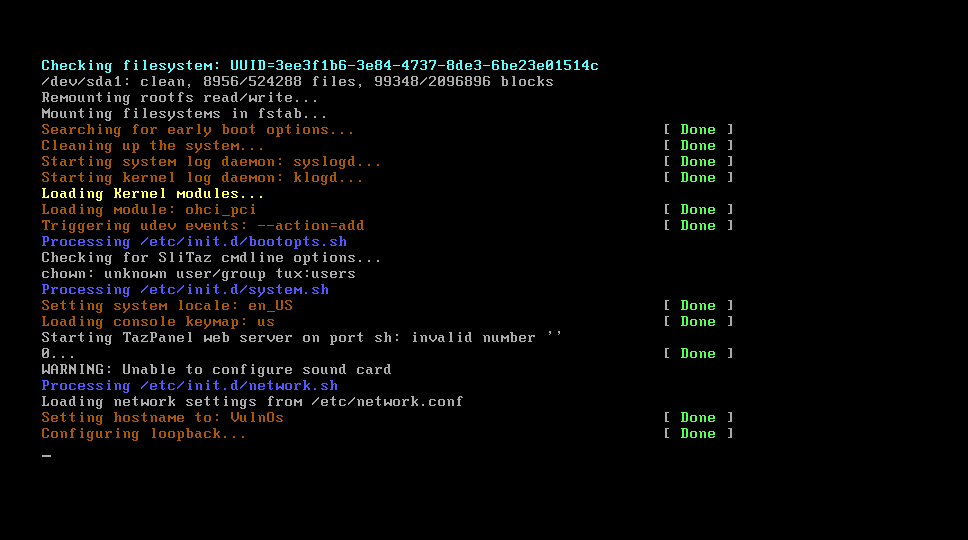
# Experiment 7: Analyze and exploit the root system of CMROS

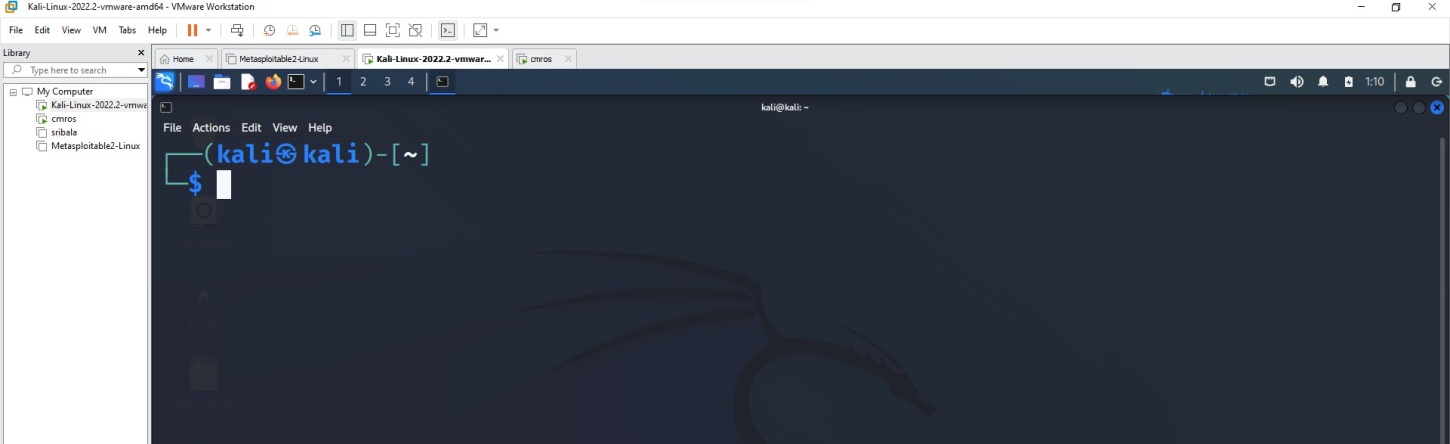
Step1: Download CMROS.zip and extract the zip file. Step2: Open VMWare.

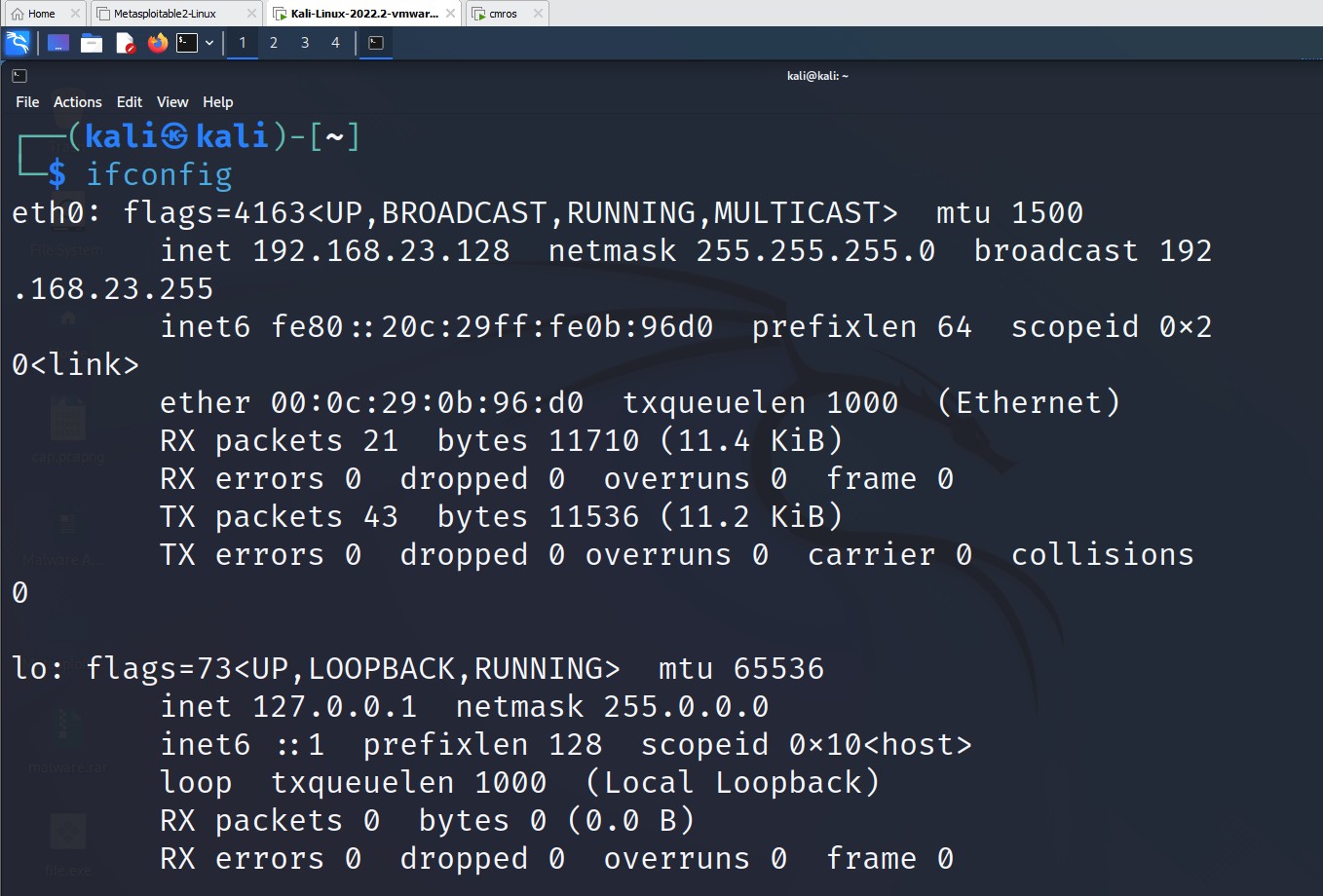
Step3: Open Virtual Machine and click CMROS extracted folder Select the .ovf file

Step4: Power on the cmros virtual machine and consider IP address of cmros

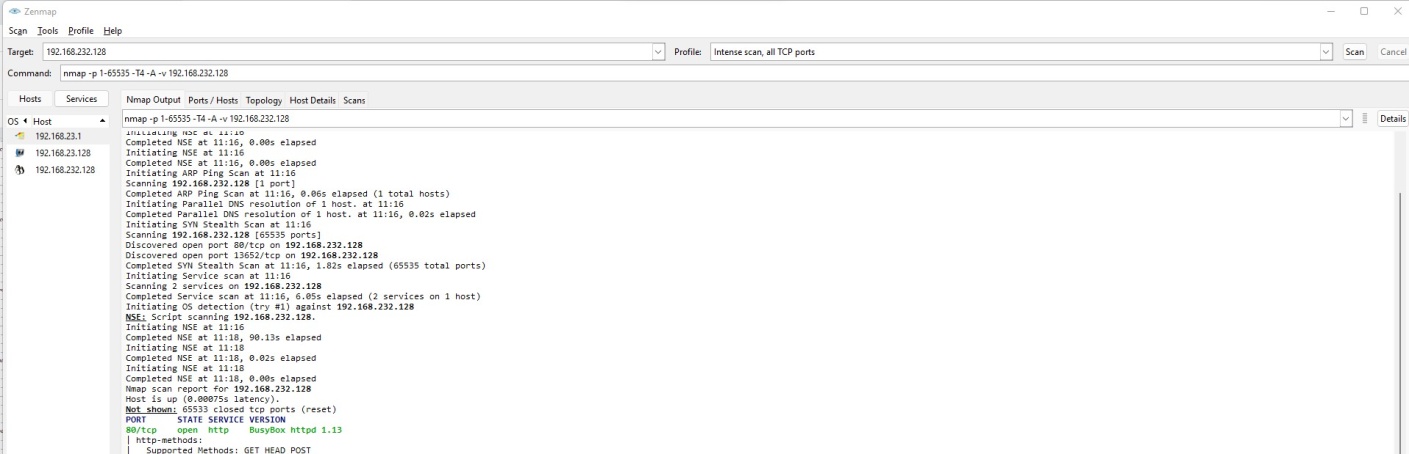


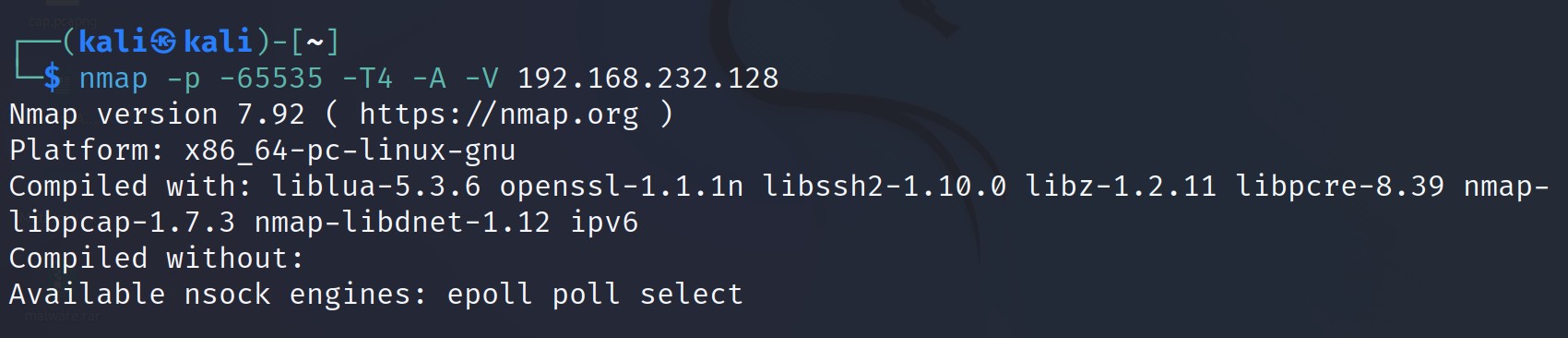
Step5: Open Kali linux on and open terminal



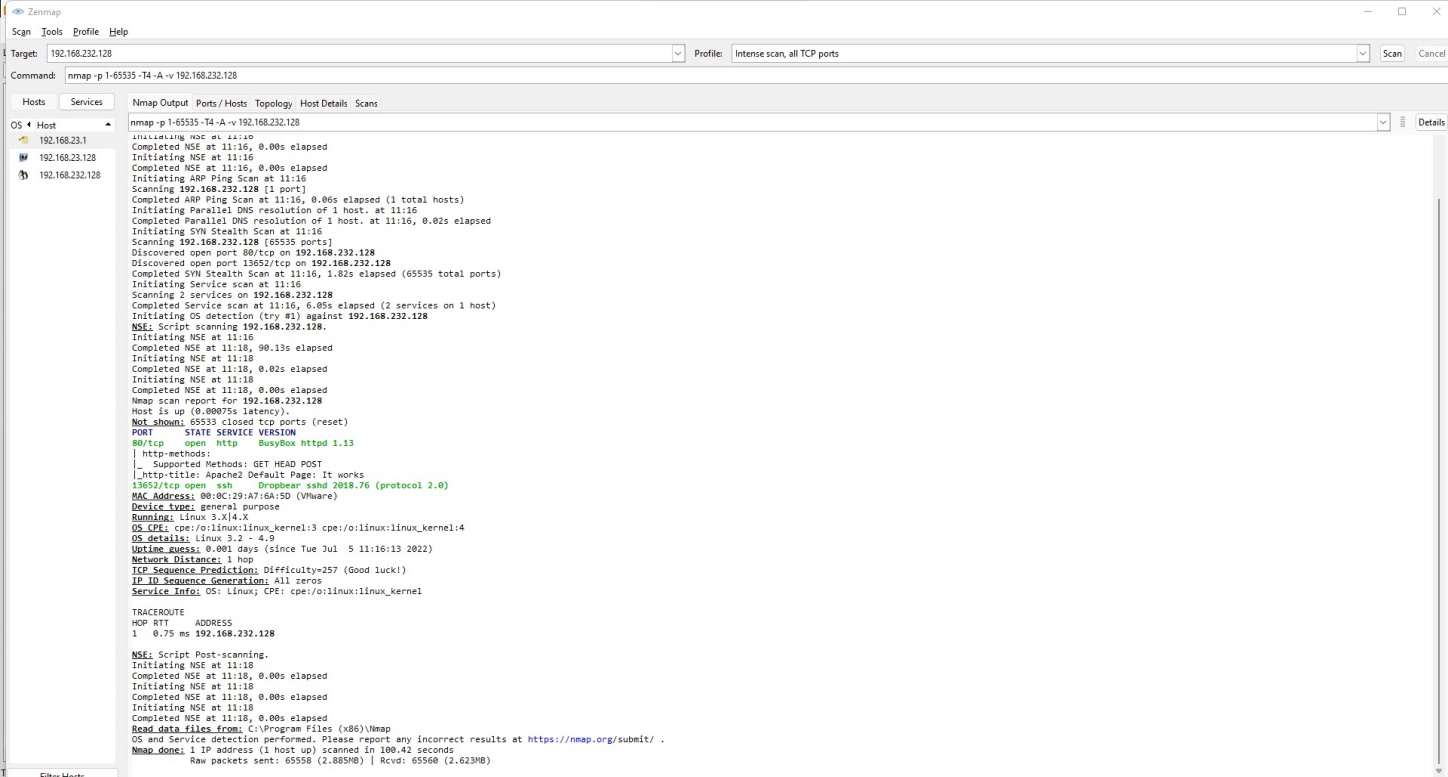
Step6: Start attacking by following commands.

Open nmap tool and give the IP address of the CMROS. It shows only http service only in the nmap tool.

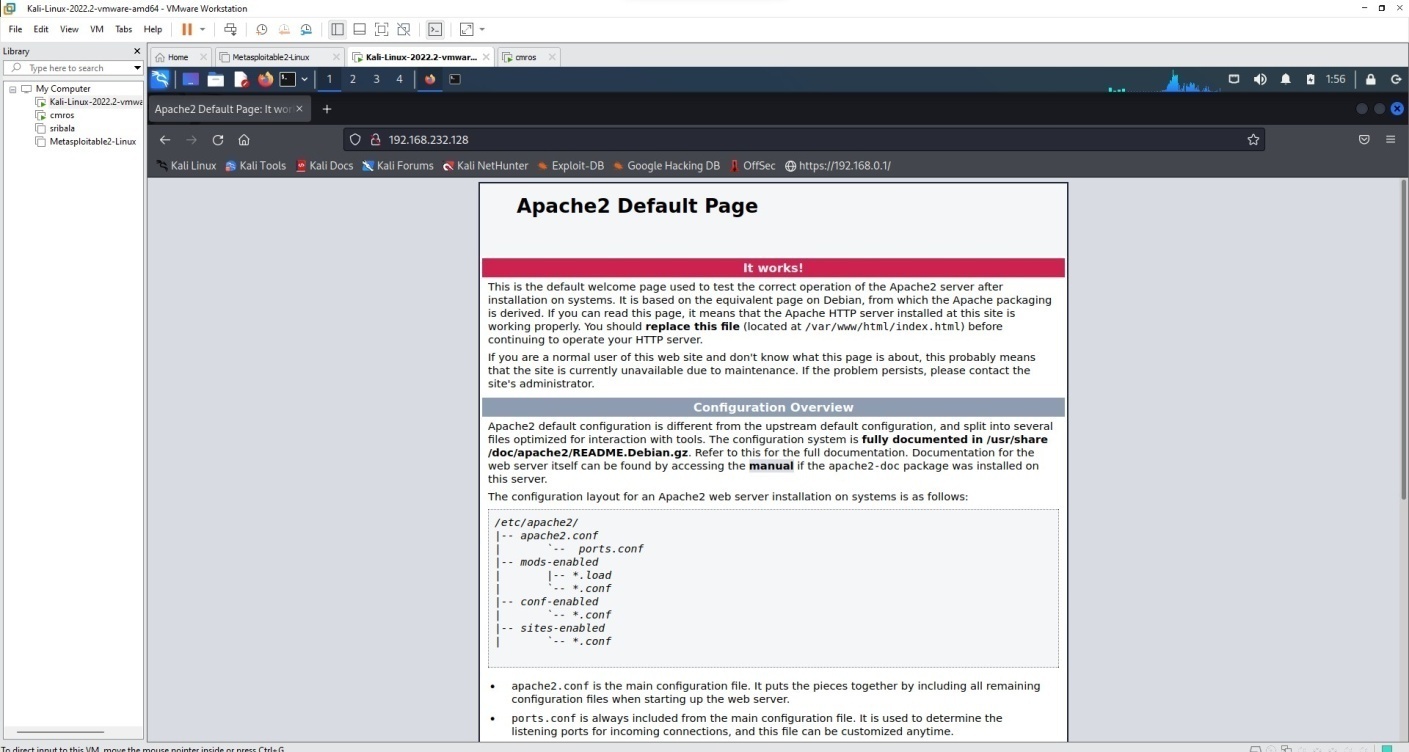


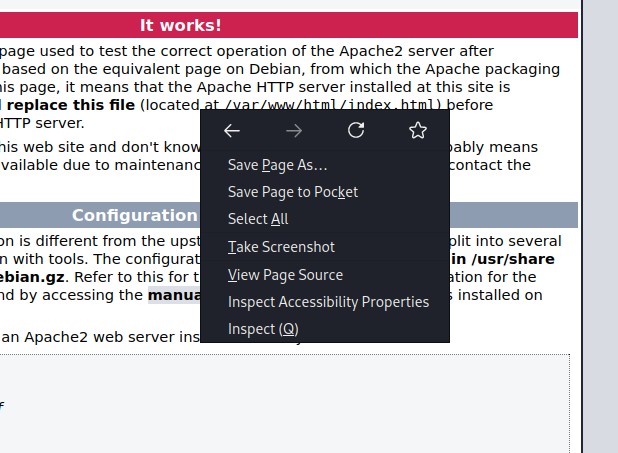
Now use the command below in the kali linux terminal

Now open again nmap tool and set intense scan, all tcp ports

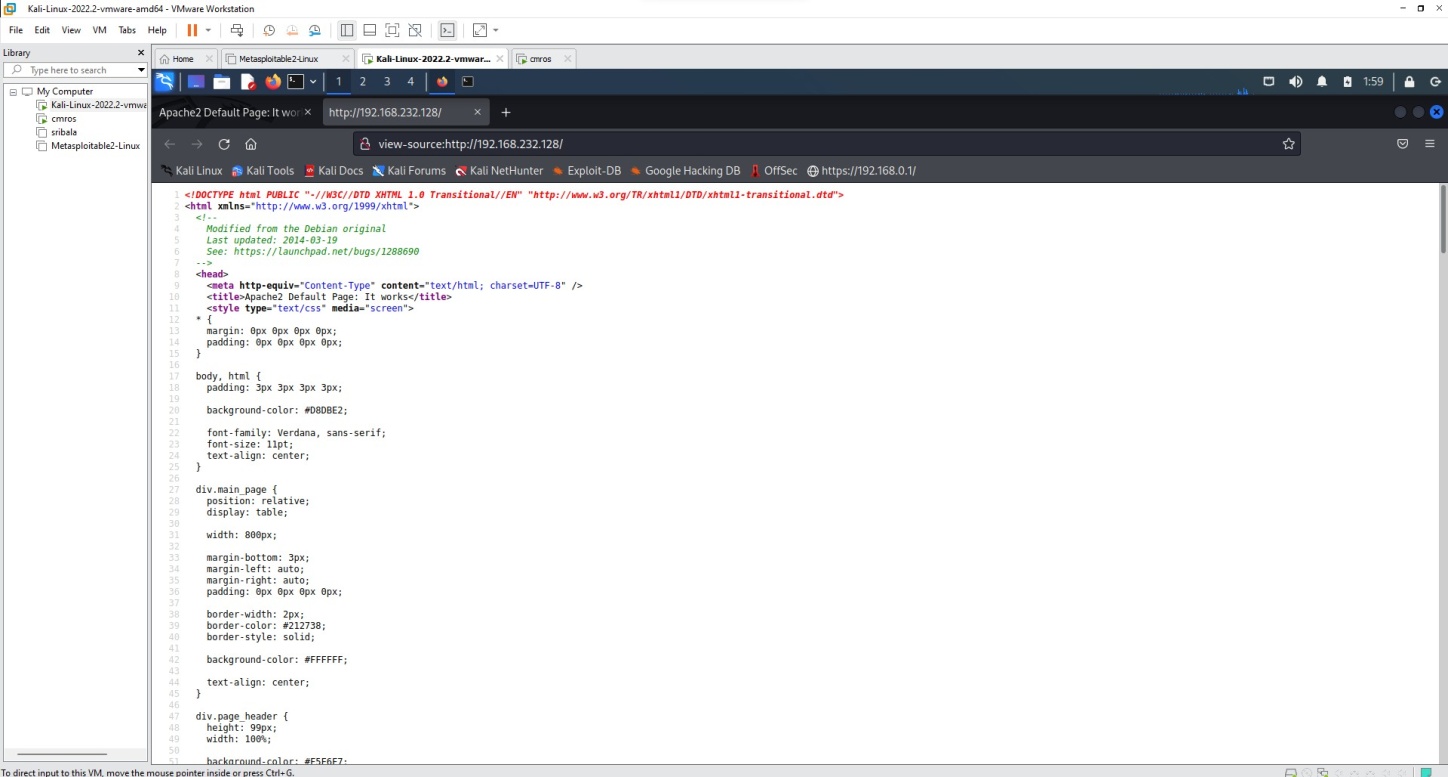
→ Now it displays all ports like http and ssh.

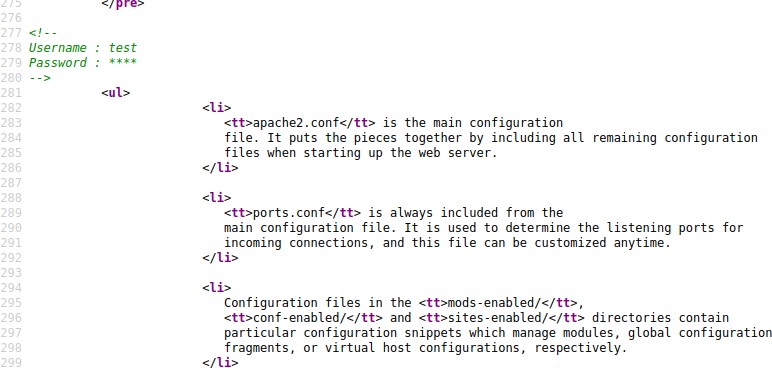
Now open Kali Linux browser and search 192.168.232.128/(cmros ip address)



Right click → view page source

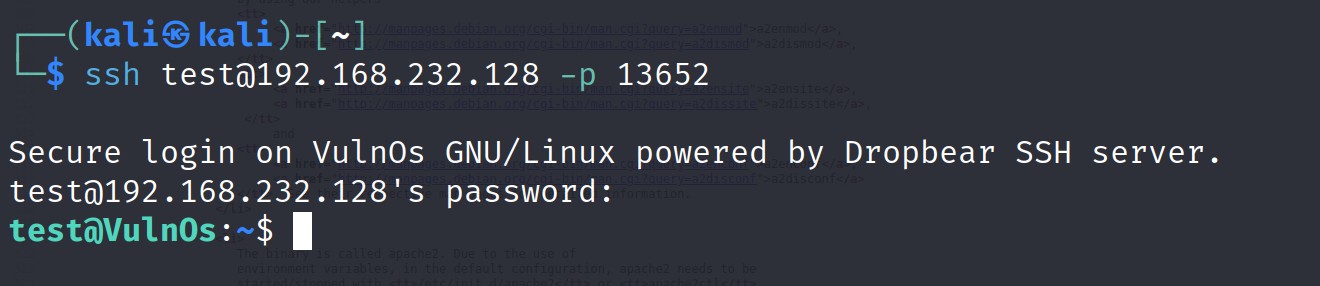
It displays the source code



After scrolling down the source code page there we can find username and password

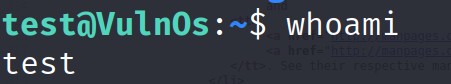
Goto kali linux terminal and use the below command

Use the password we got from the view page source code which is **test**



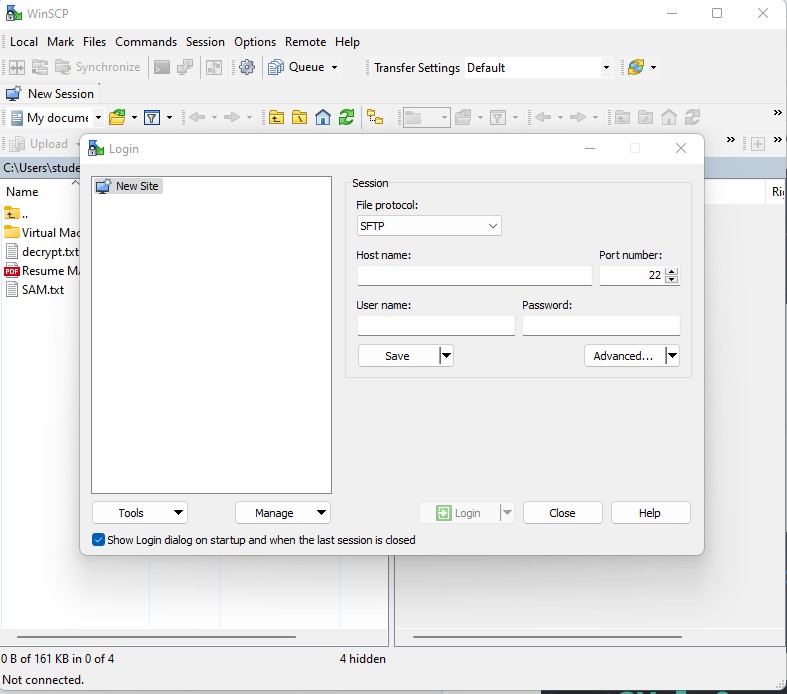
Use ls command

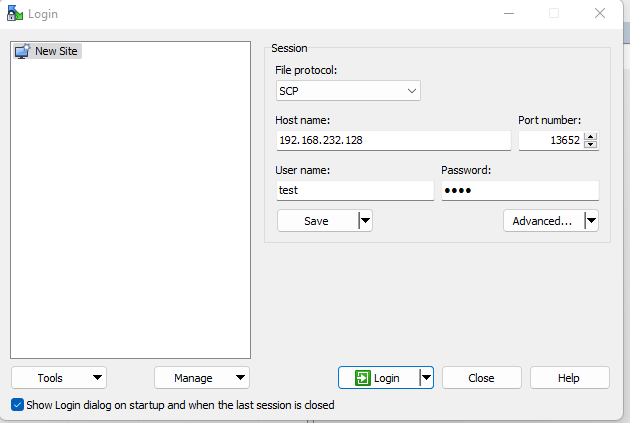


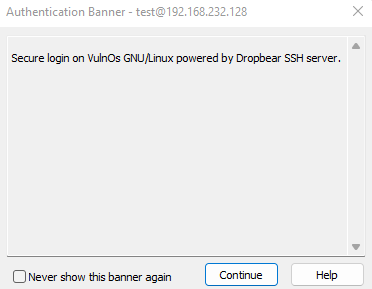
Use whoami to find the user

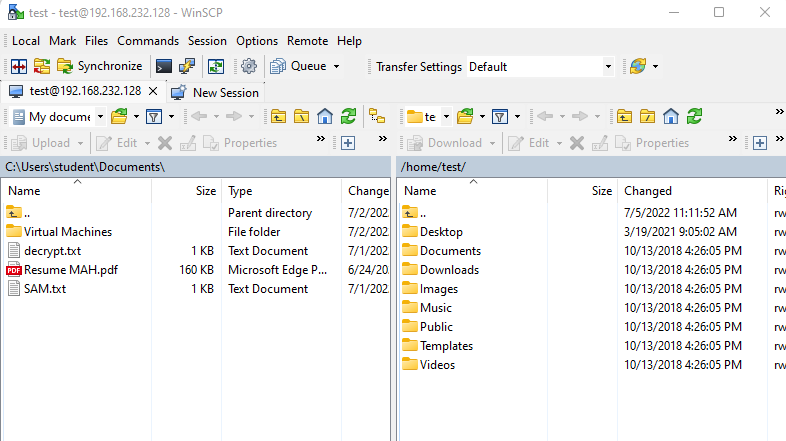
To know the suspicious file redirect to Desktop and the use ls command

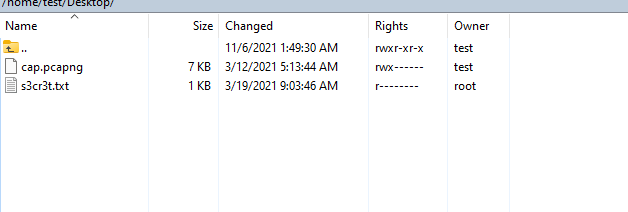


Now go to Windows system, open browser and download WinSCP

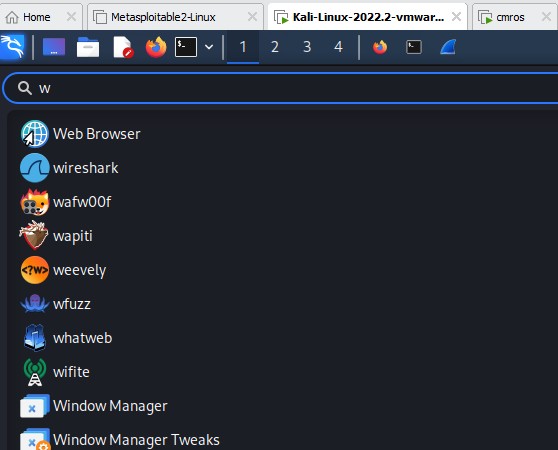


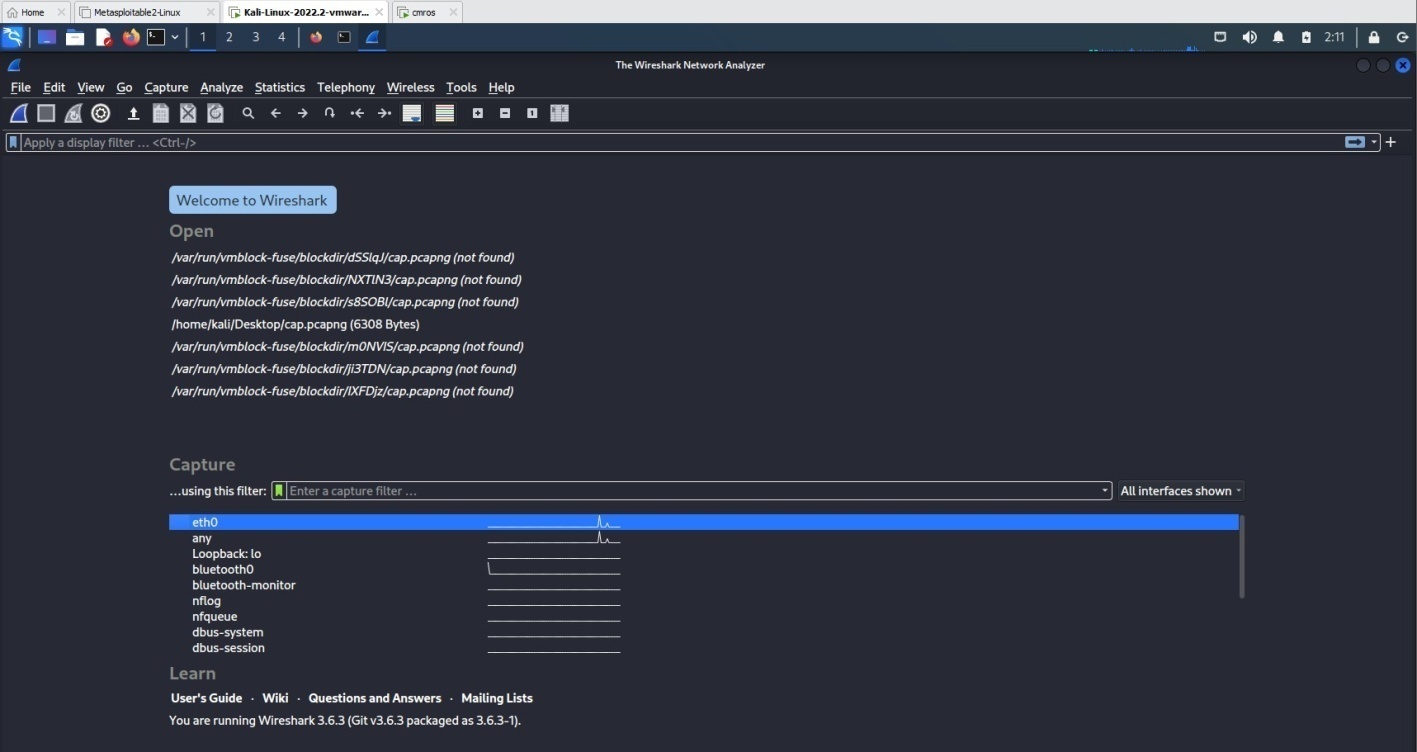




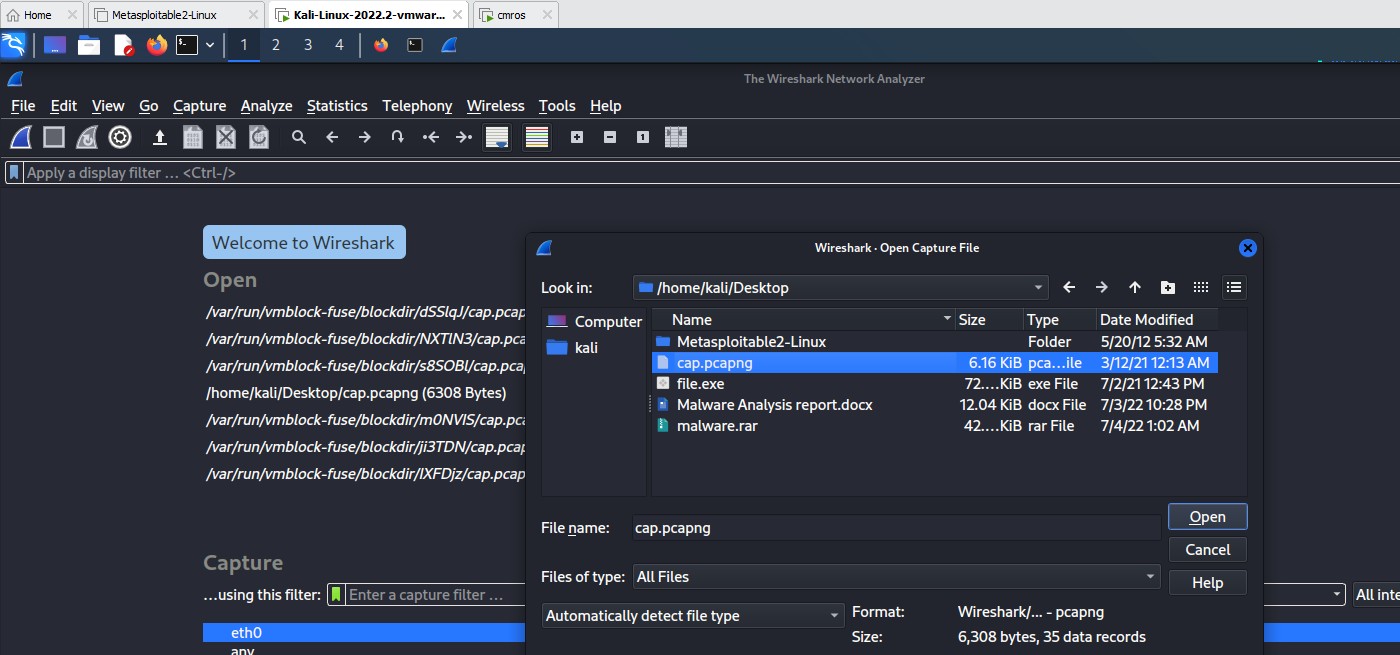
Goto Desktop

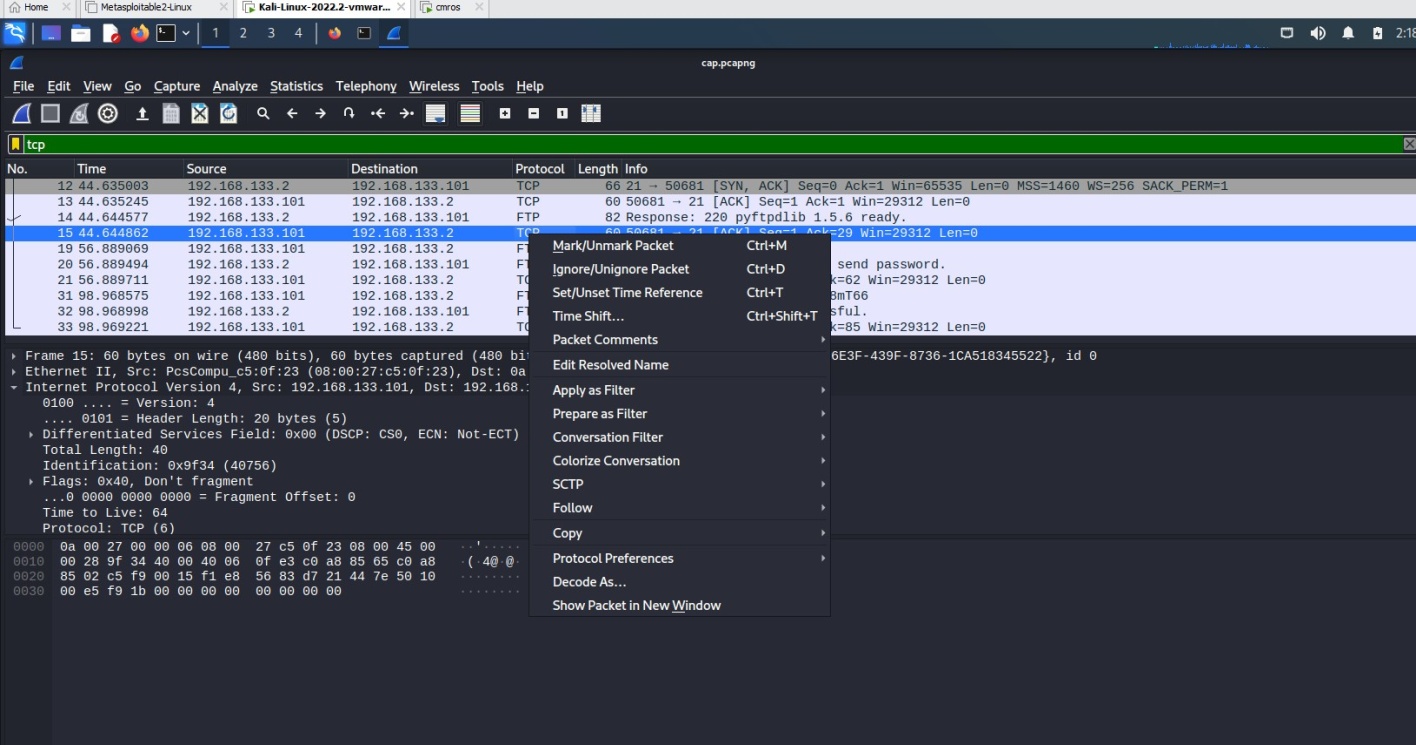
Open kali linux and search for wireshark tool



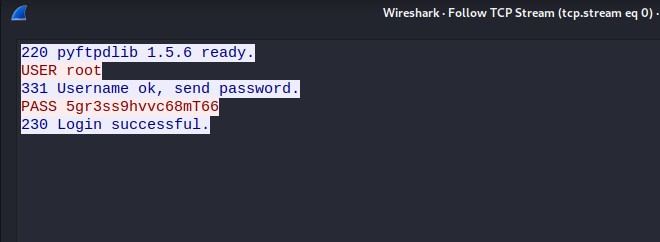
Open wireshark tool in kali

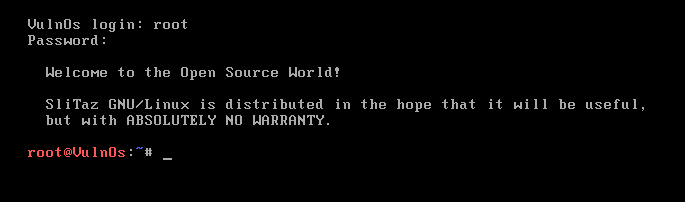
Open cap.pcapng file in the wireshark from desktop folder



Click any tcp filter and then right click →click follow → TCP Stream

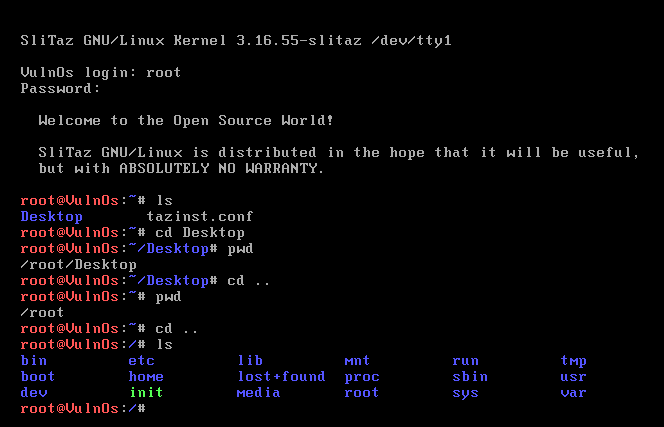
It displays user credentials



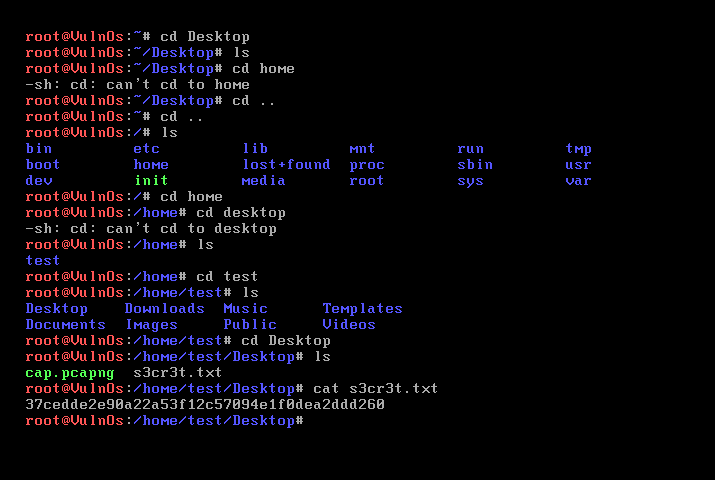
Now copy password and open cmros using above credentials By using the above credentials we can crack cmros system

Now use ls command root@VulnOs:~# ls Desktop tazinst.conf

root@VulnOs:~#



cd Desktop root@VulnOs:~/Desktop# ls



Type command cat s3cr3t.txt

To make chanes in the file tpe command-nano s3cr3t.txt

Open file write any content init.

Click ctrl+X,ctrl+Y type file name cat s3cr3t.txt

IT displays the content of the file.