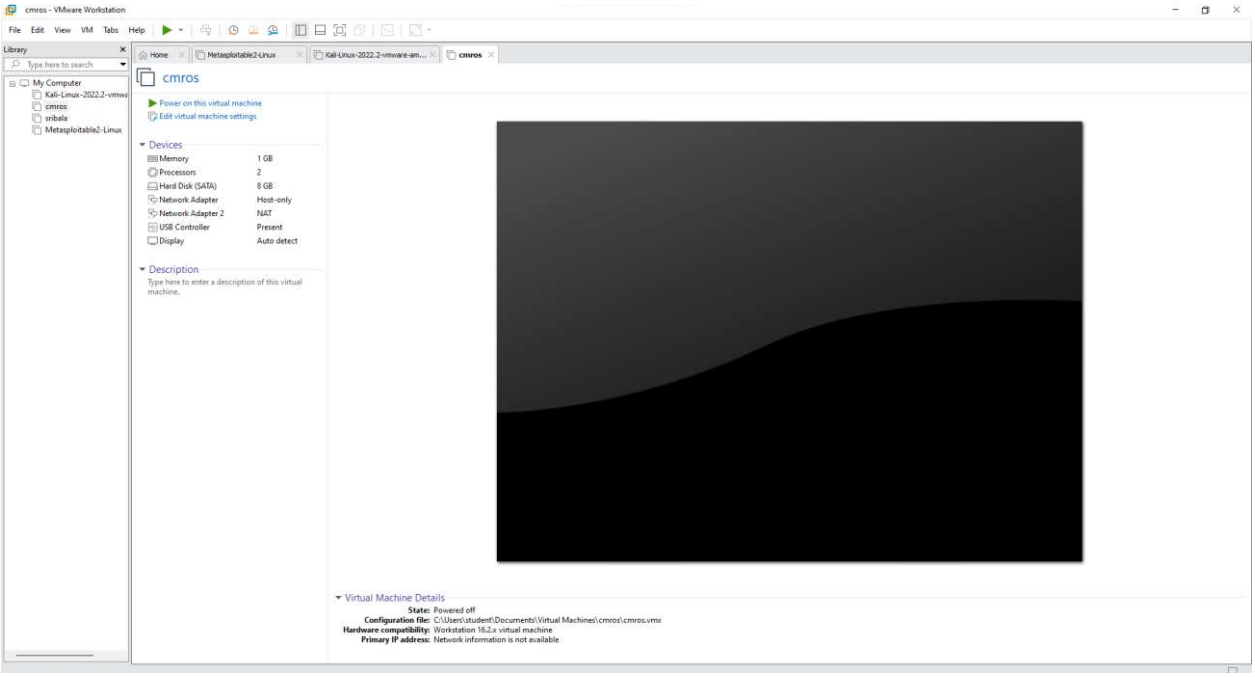
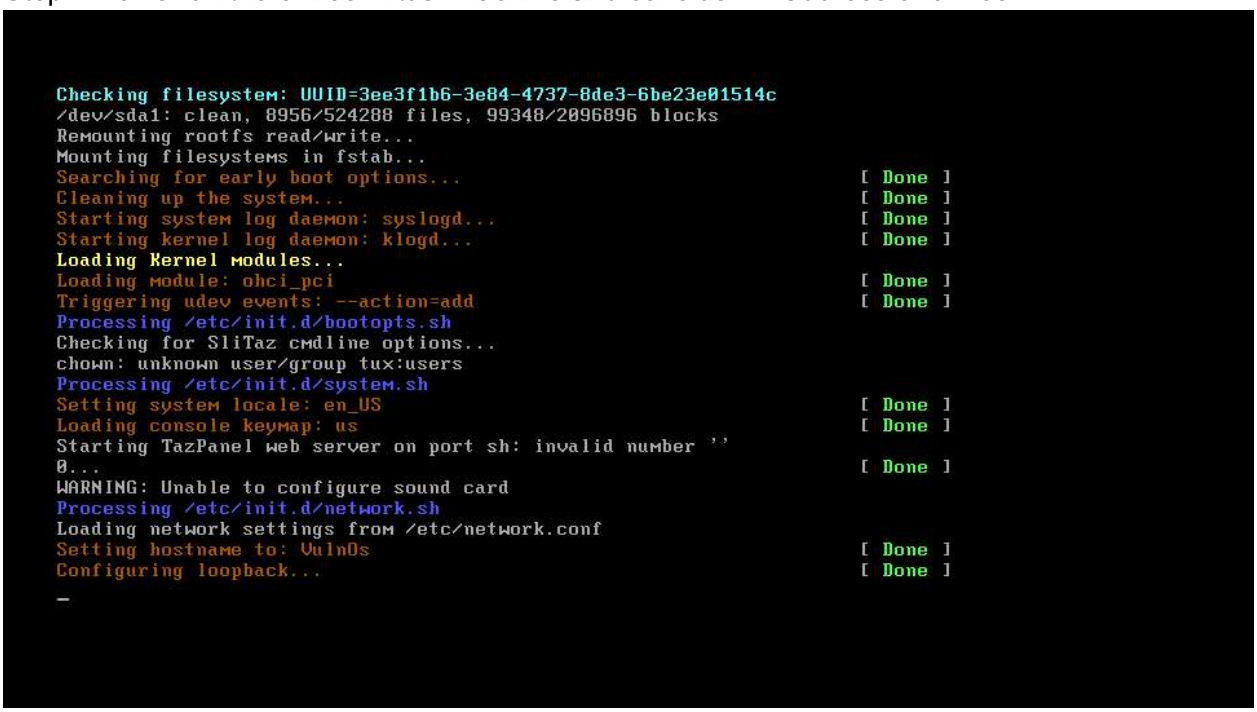
**Experiment 7: Analyze and exploit the root system of CMROS**

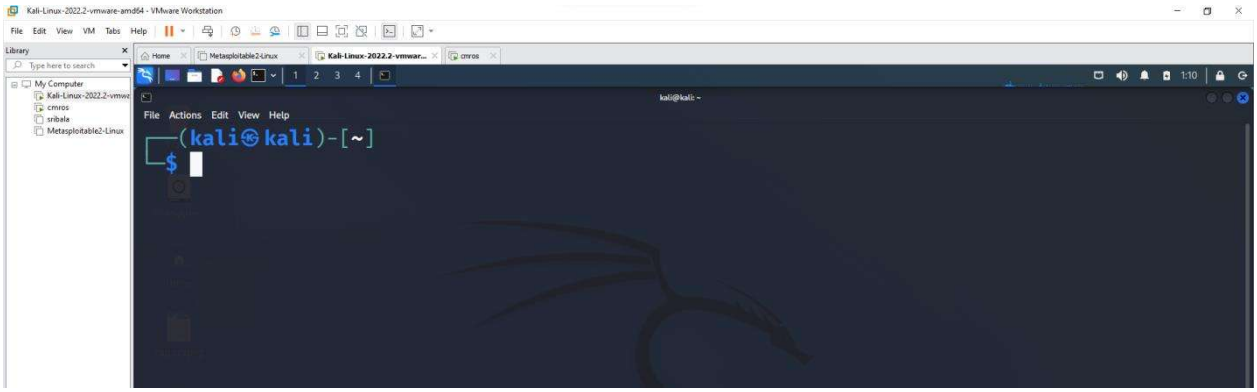
Step1: Download CMROS.zip and extract the zip file.
Step2: Open VMWare.
Step3: Open Virtual Machine and click CMROS extracted folder Select the .ovf file



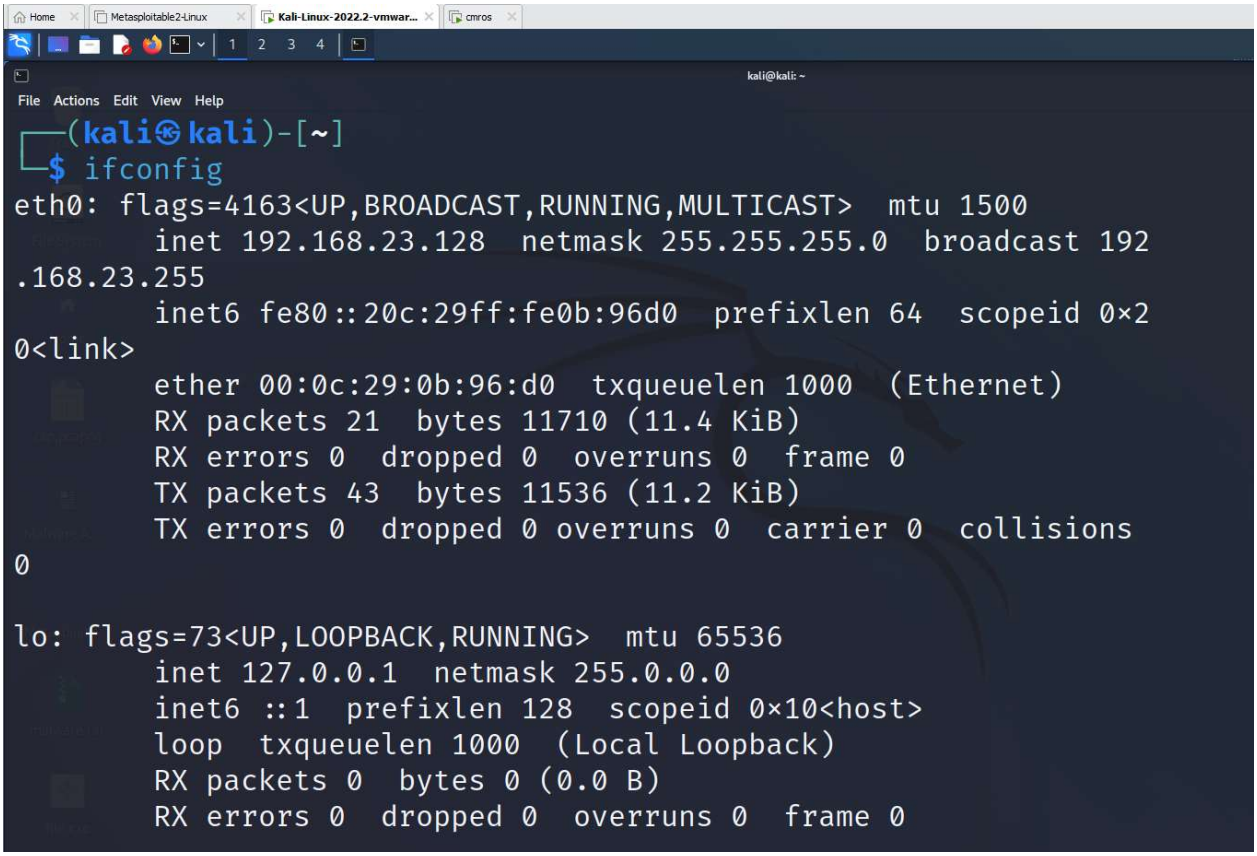

Step4: Power on the cmros virtual machine and consider IP address of cmros



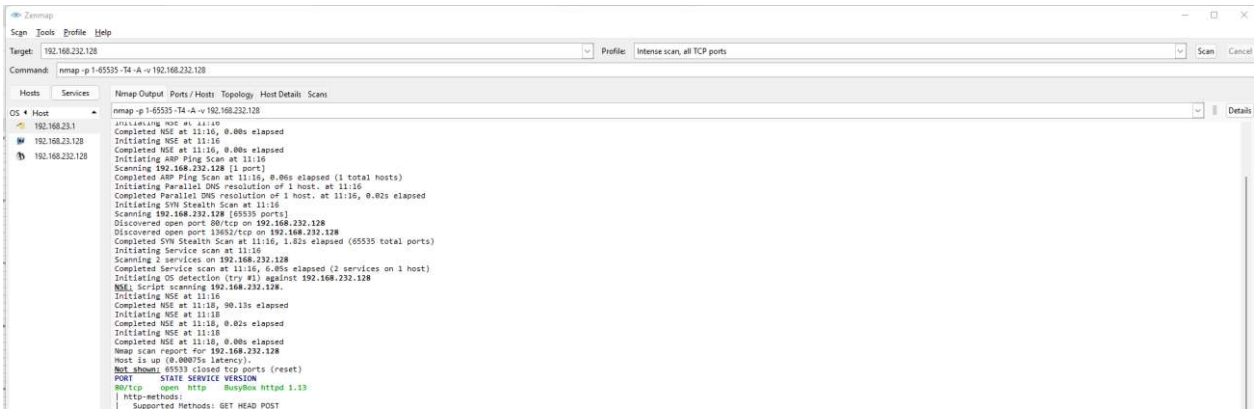

Step5: Open Kali linux on and open terminal




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.

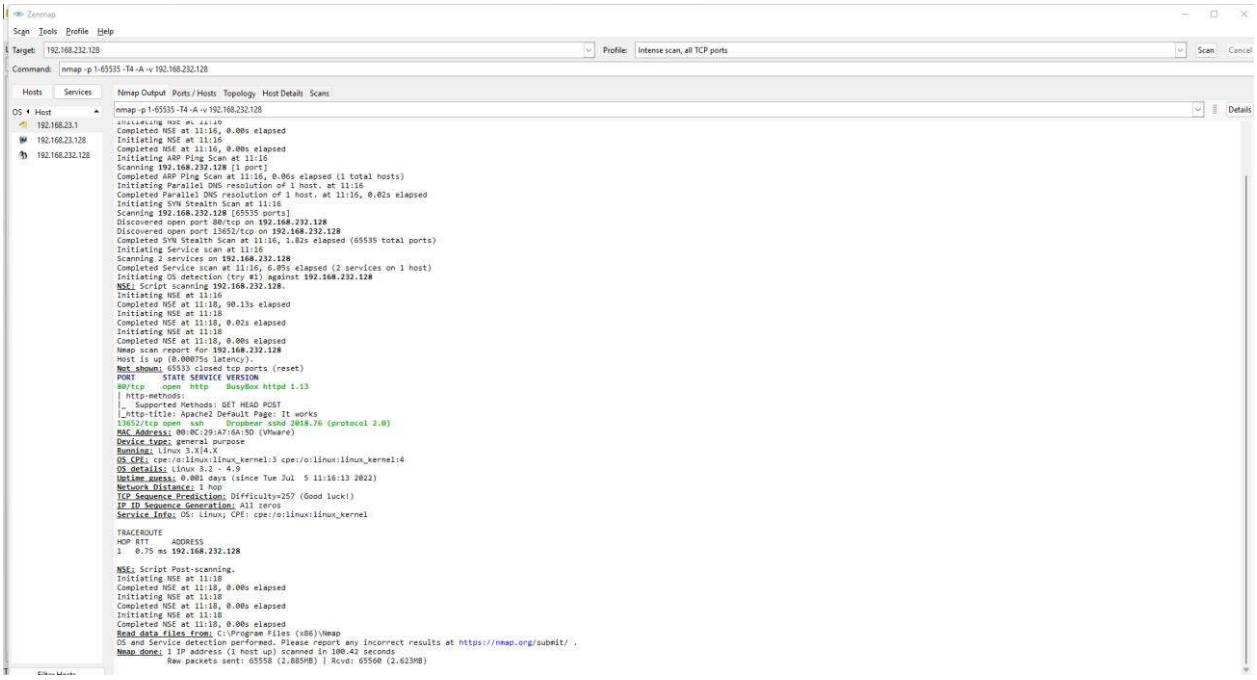



Now use the command below in the kali linux terminal

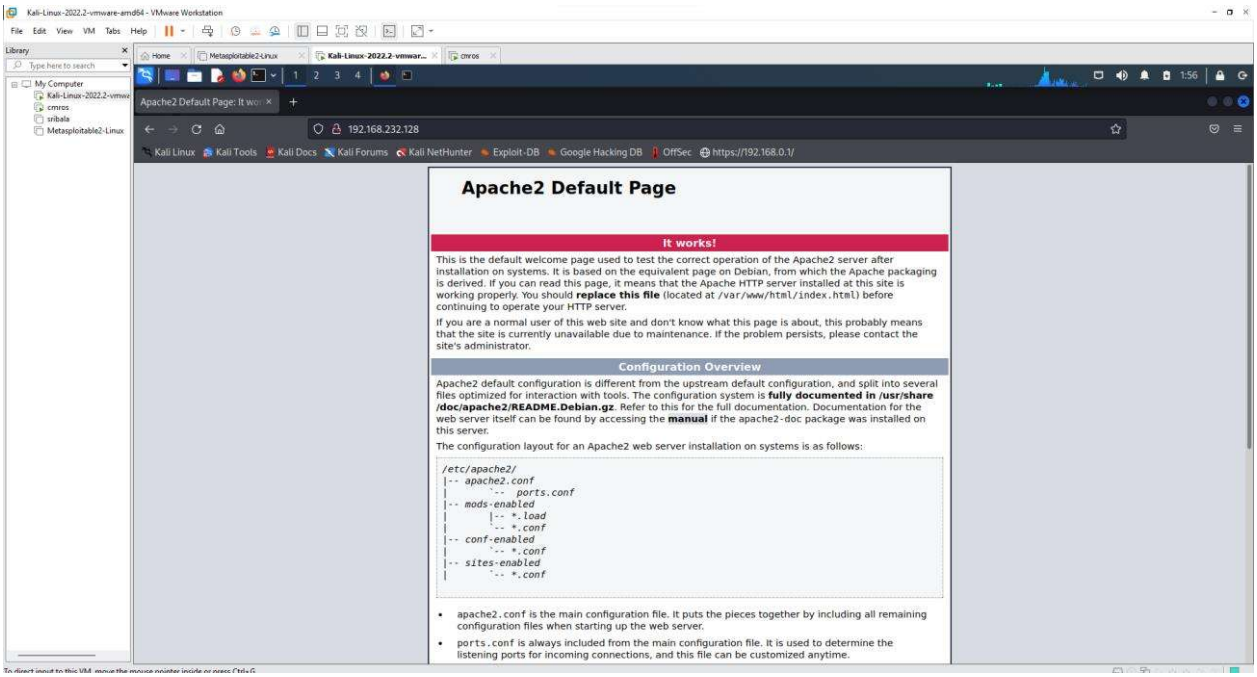
```
┌──(kali㉿kali)-[~]
└─$ nmap -p -65535 -T4 -A -V 192.168.232.128
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-1.1.1n libssh2-1.10.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

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

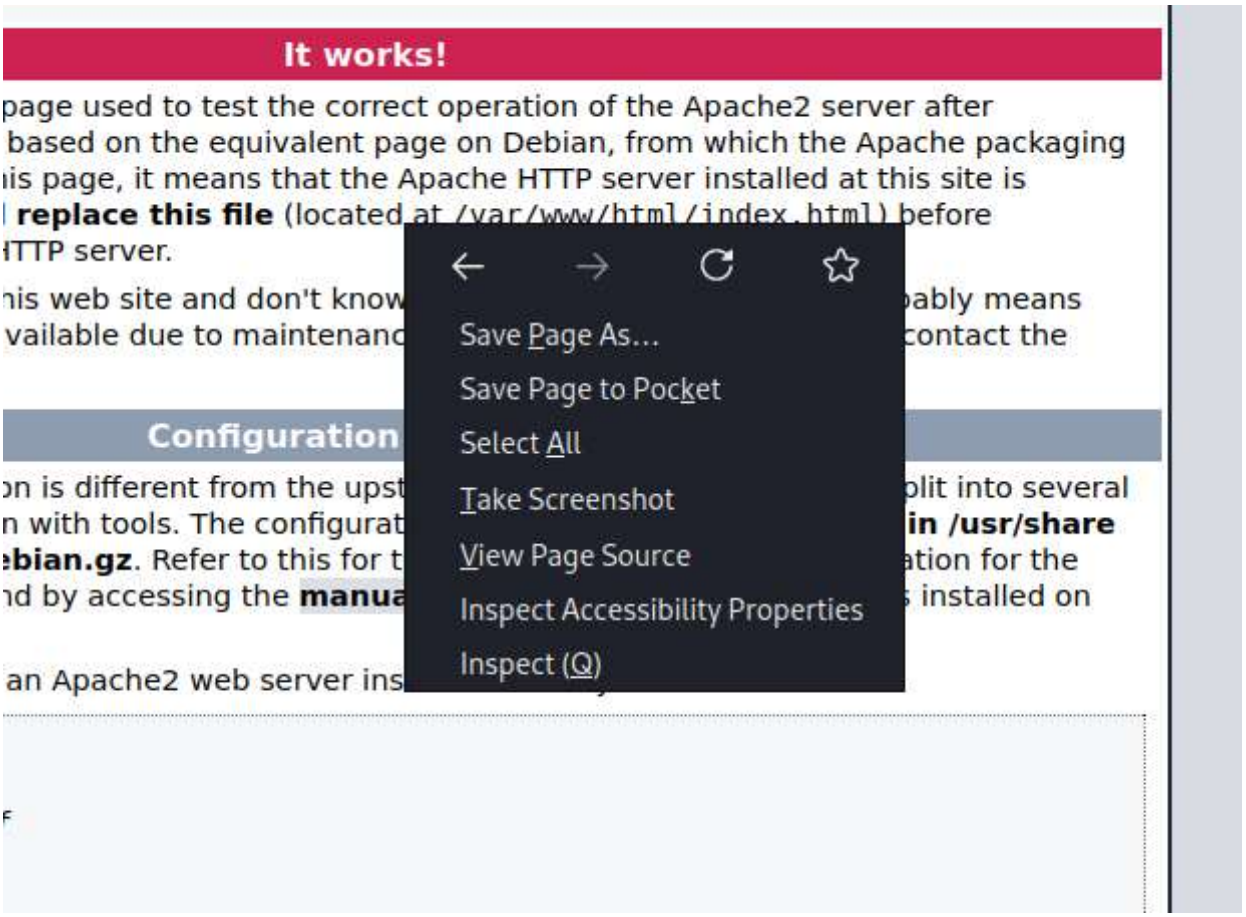
→ Now it displays all ports like http and ssh.



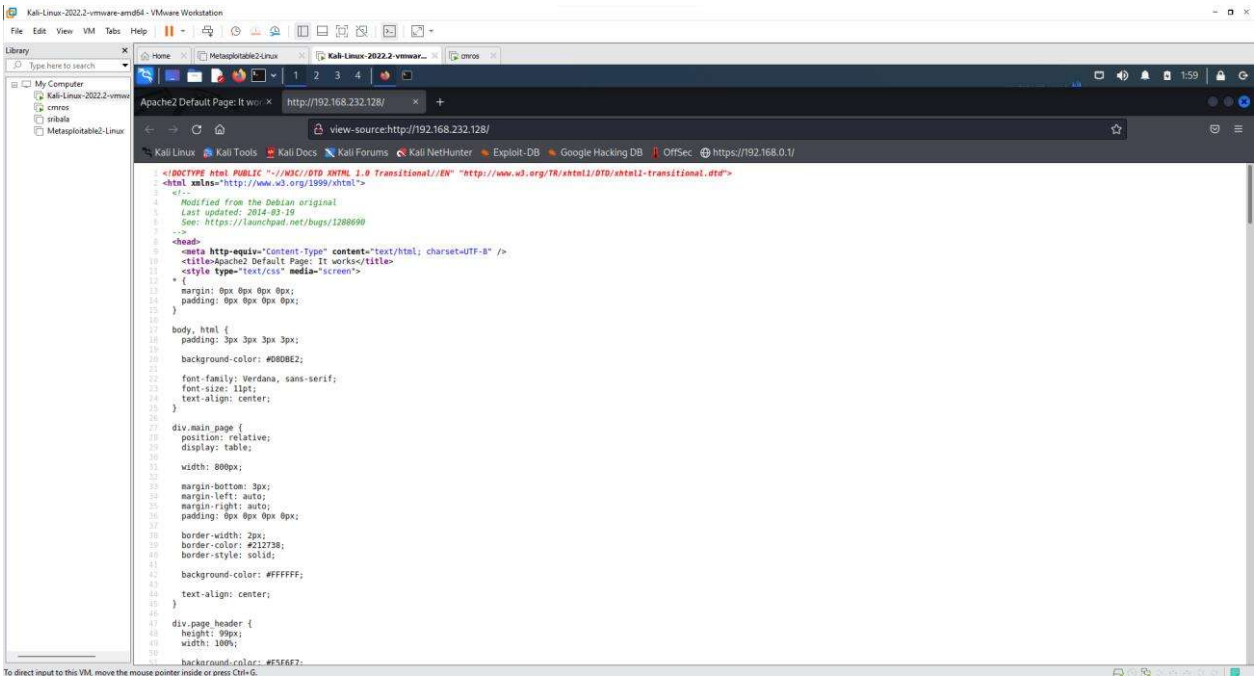

Now open Kali Linux browser and search 192.168.232.128/(cmros ip address)




Right click → view page source




It displays the source code



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

```
        </pre>

<!--
Username : test
Password : ****
-->
        <ul>
                <li>
                   <tt>apache2.conf</tt> is the main configuration
                   file. It puts the pieces together by including all remaining configuration
                   files when starting up the web server.
                </li>

                <li>
                   <tt>ports.conf</tt> is always included from the
                   main configuration file. It is used to determine the listening ports for
                   incoming connections, and this file can be customized anytime.
                </li>

                <li>
                   Configuration files in the <tt>mods-enabled/</tt>,
                   <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
                   particular configuration snippets which manage modules, global configuration
                   fragments, or virtual host configurations, respectively.
                </li>
```

Goto kali linux terminal and use the below command
Use the password we got from the view page source code which is **test**

```
┌──(kali㉿kali)-[~]
└─$ ssh test@192.168.232.128 -p 13652

Secure login on VulnOs GNU/Linux powered by Dropbear SSH server.
test@192.168.232.128's password:
test@VulnOs:~$
```

Use ls command

```
test@VulnOs:~$ ls
Desktop/   Downloads/ Music/     Templates/
Documents/ Images/    Public/    Videos/
test@VulnOs:~$
```

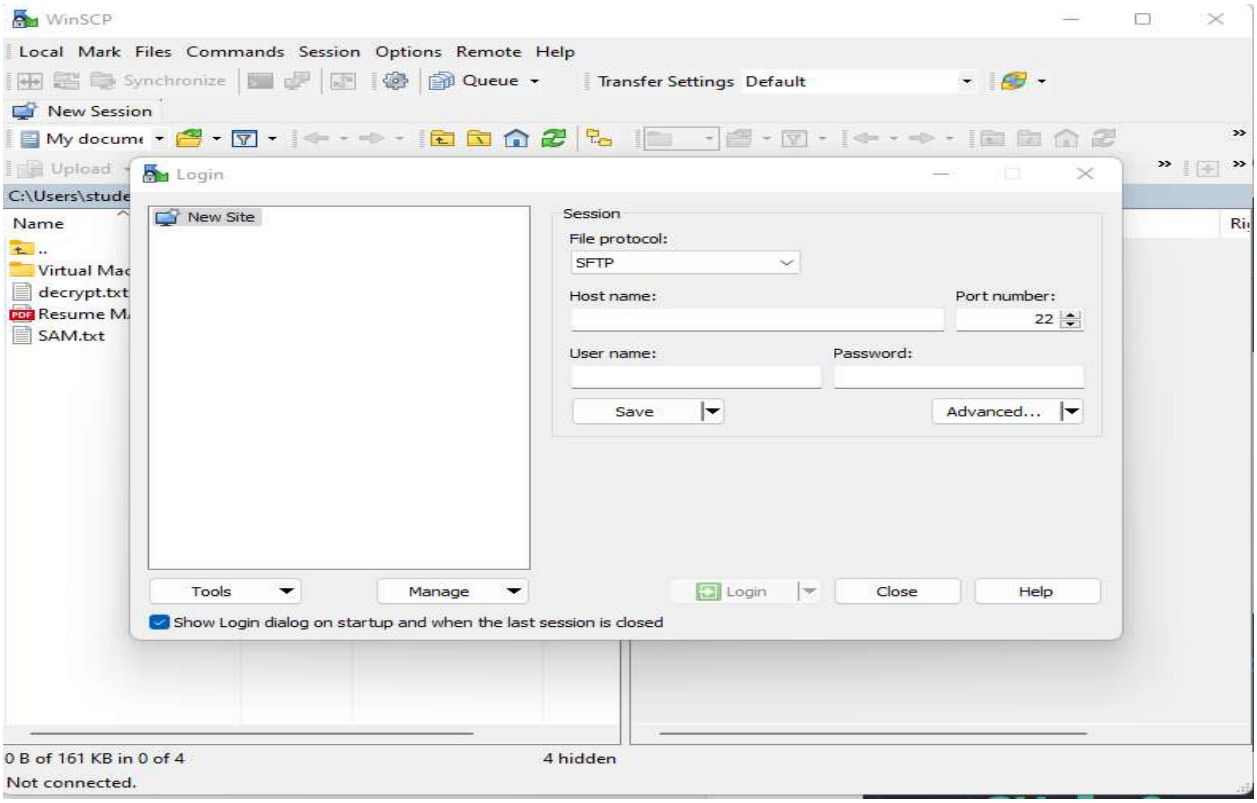
Use whoami to find the user

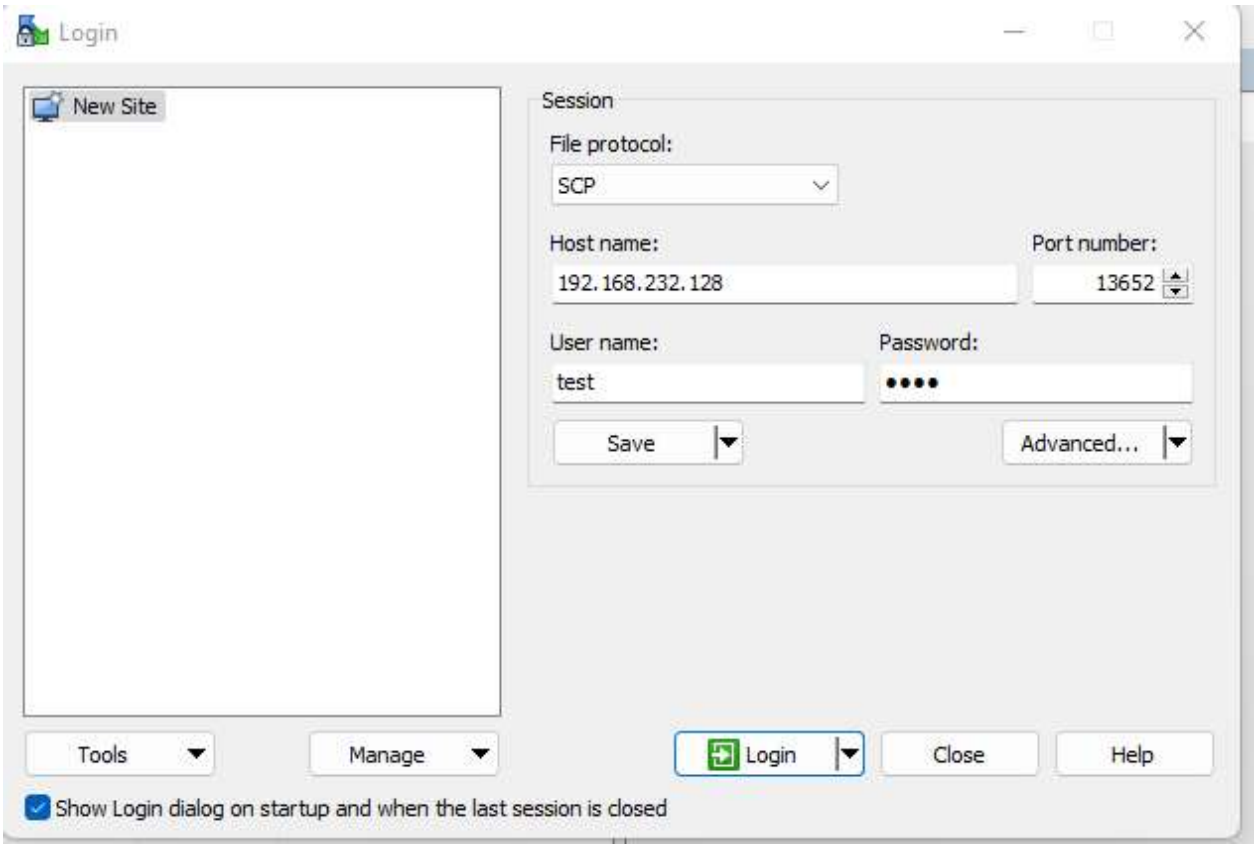
```
test@VulnOs:~$ whoami
test
```

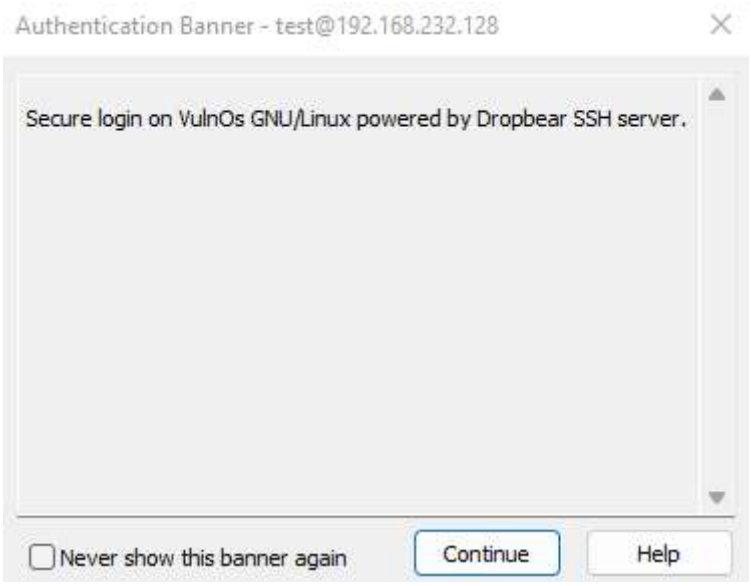
To know the suspicious file redirect to Desktop and the use ls command

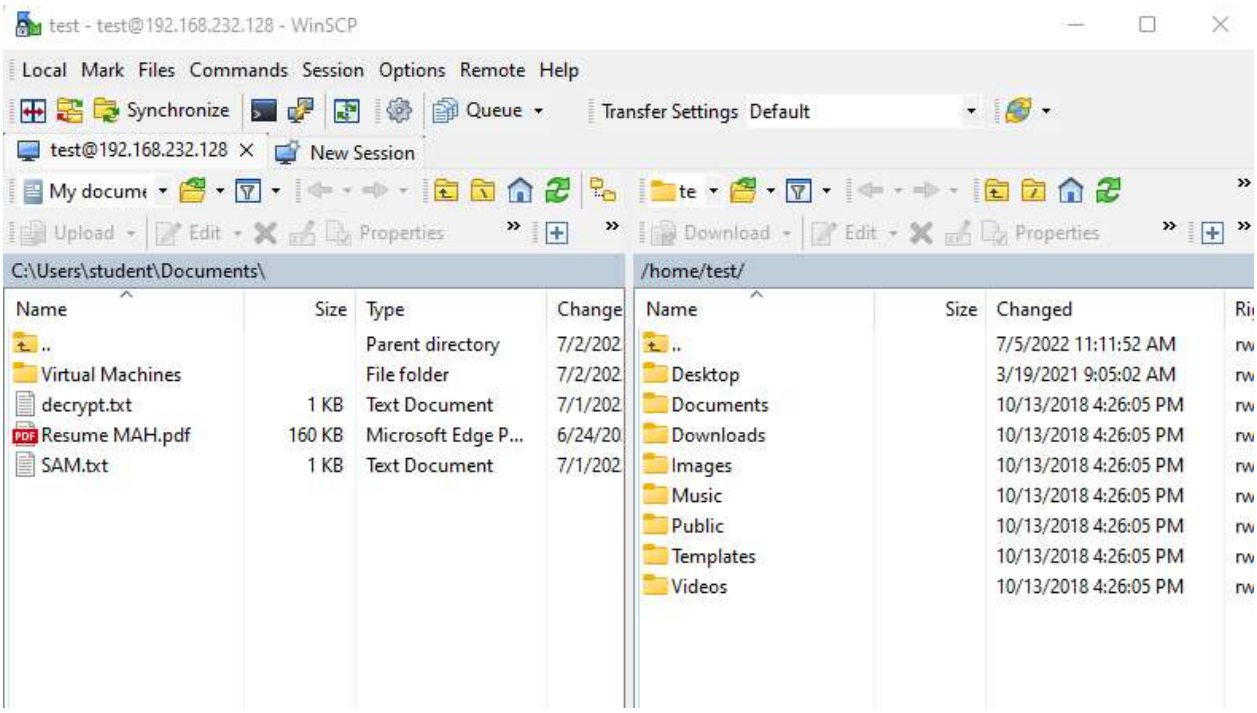
```
test@VulnOs:~$ cd Desktop
test@VulnOs:~/Desktop$ ls
cap.pcapng  s3cr3t.txt
```

Now go to Windows system, open browser and download WinSCP

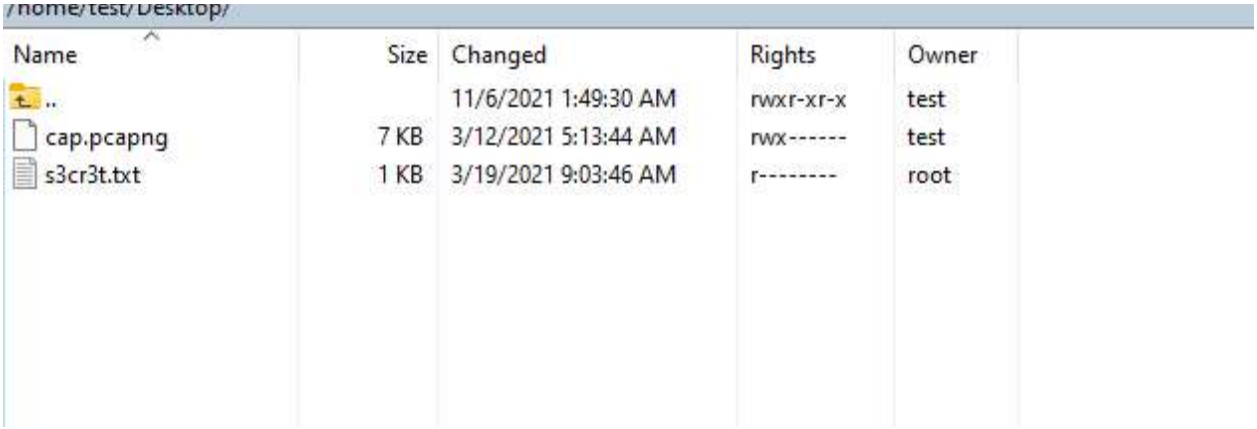



Login
New Site
Session
File protocol:
SCP
Host name:
Port number:
192.168.232.128
13652
User name:
Password:
test
Save
Advanced...
Tools
Manage
Login
Close
Help
Show Login dialog on startup and when the last session is closed

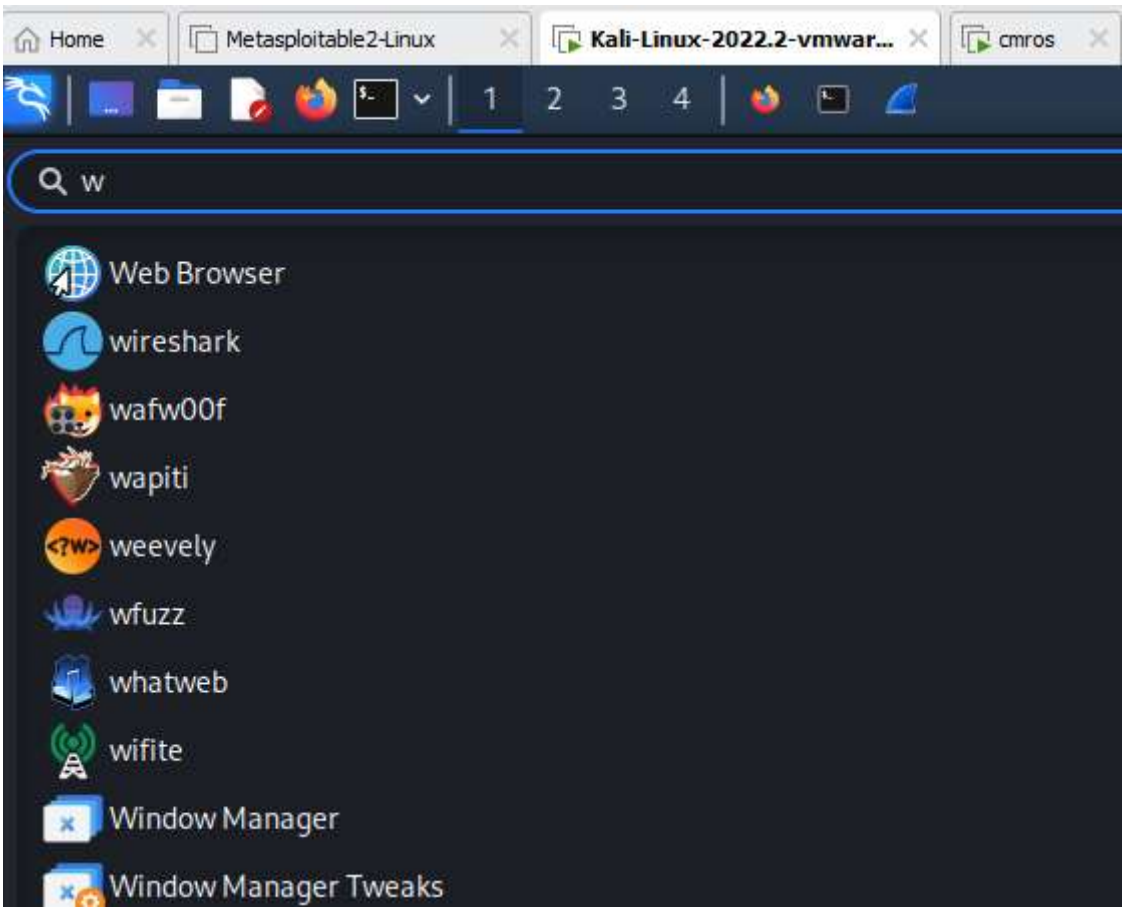

Authentication Banner - test@192.168.232.128
Secure login on VulnOs GNU/Linux powered by Dropbear SSH server.
Never show this banner again
Continue
Help



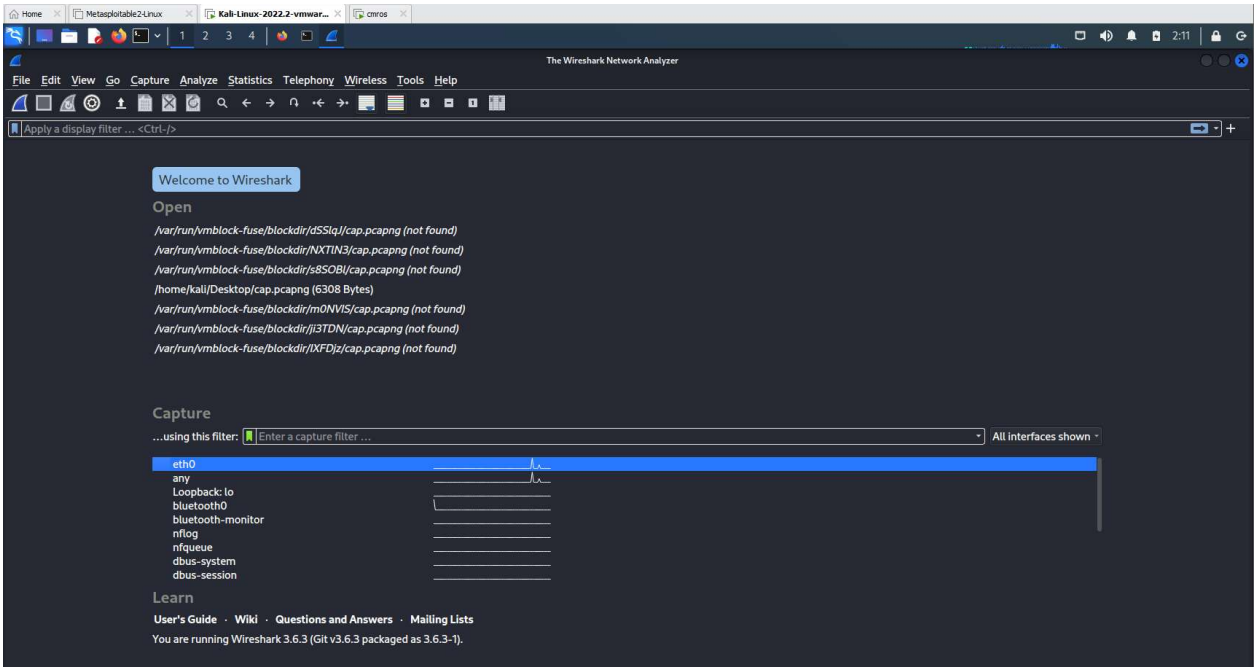

Goto Desktop



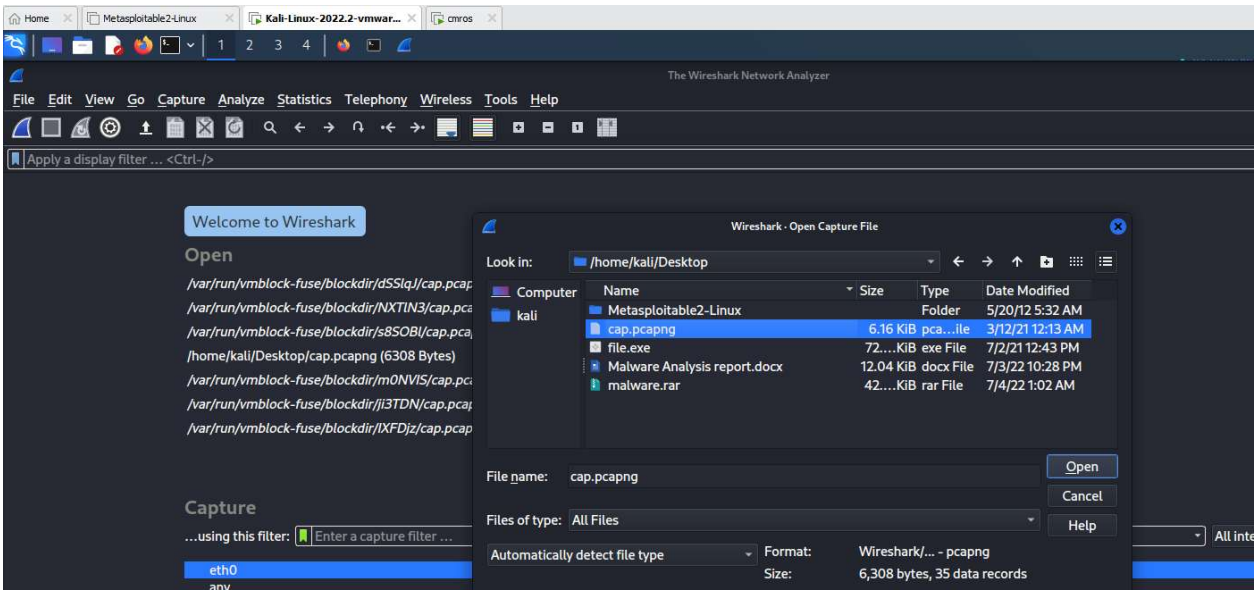

Open kali linux and search for wireshark tool



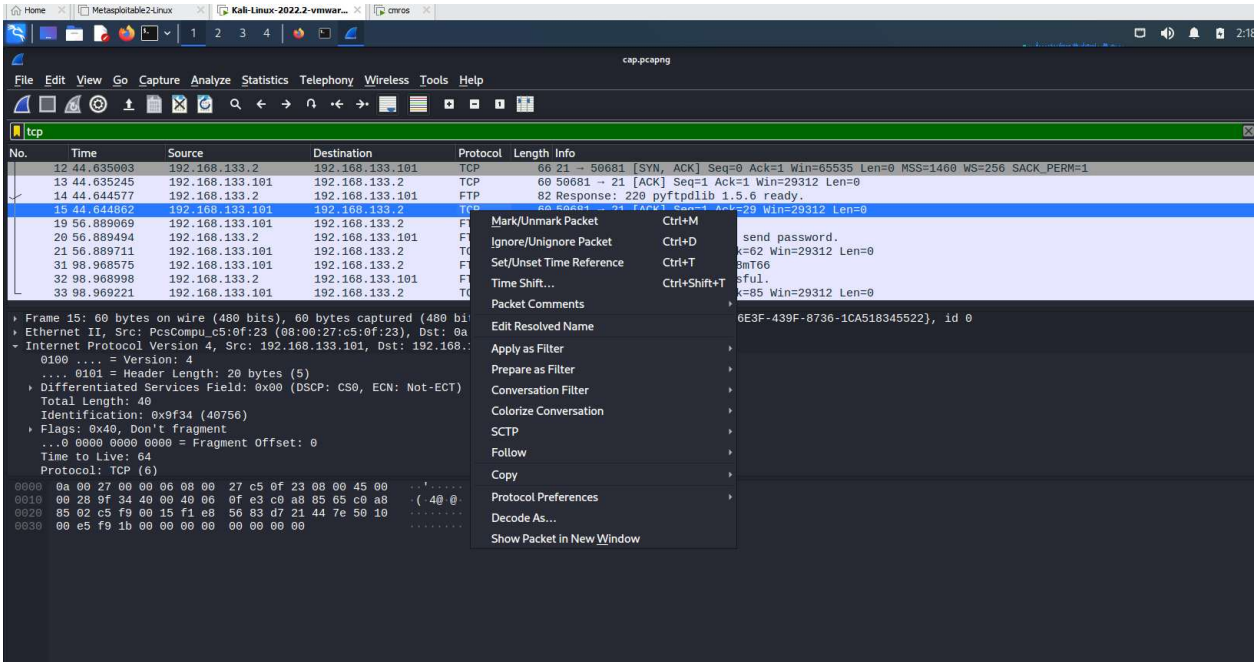

Open wireshark tool in kali



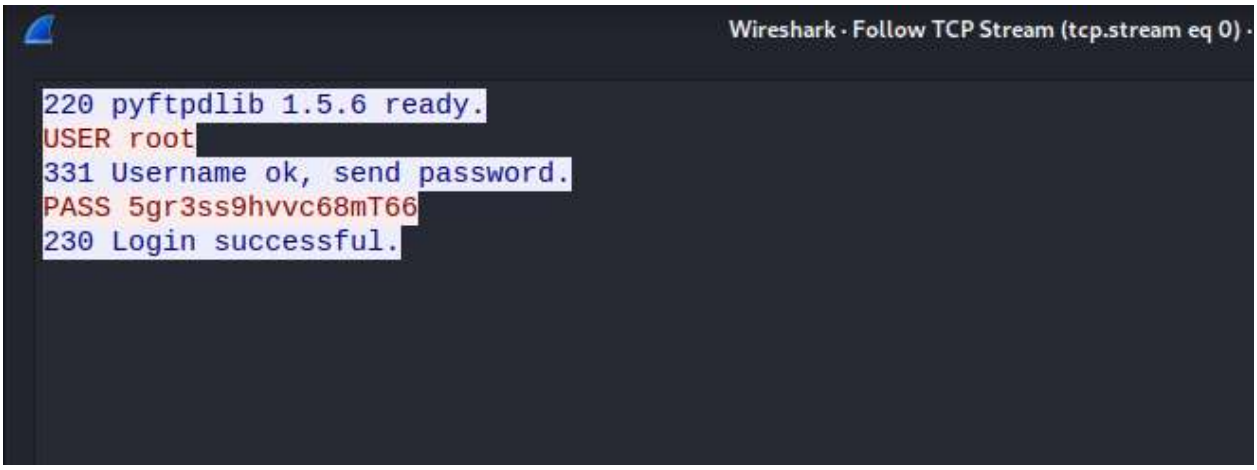

Open cap.pcapng file in the wireshark from desktop folder



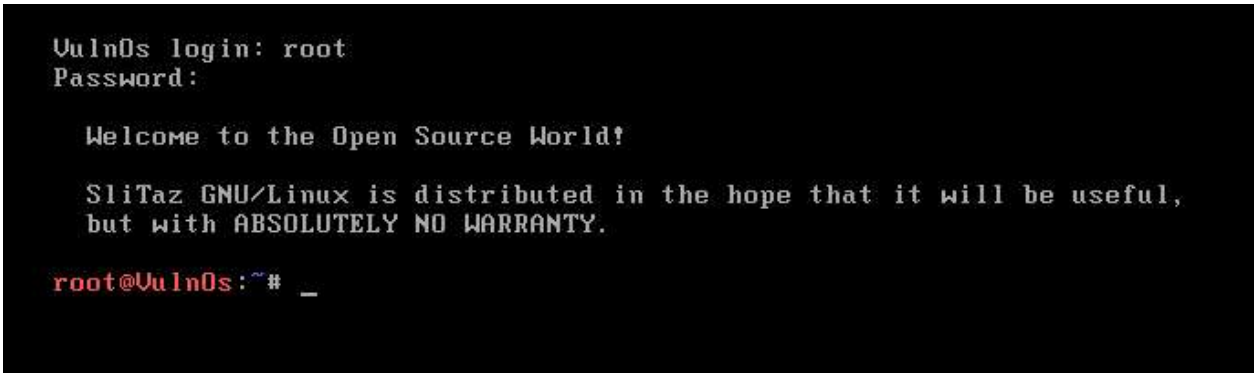

Click any tcp filter and then right click →click follow → TCP Stream



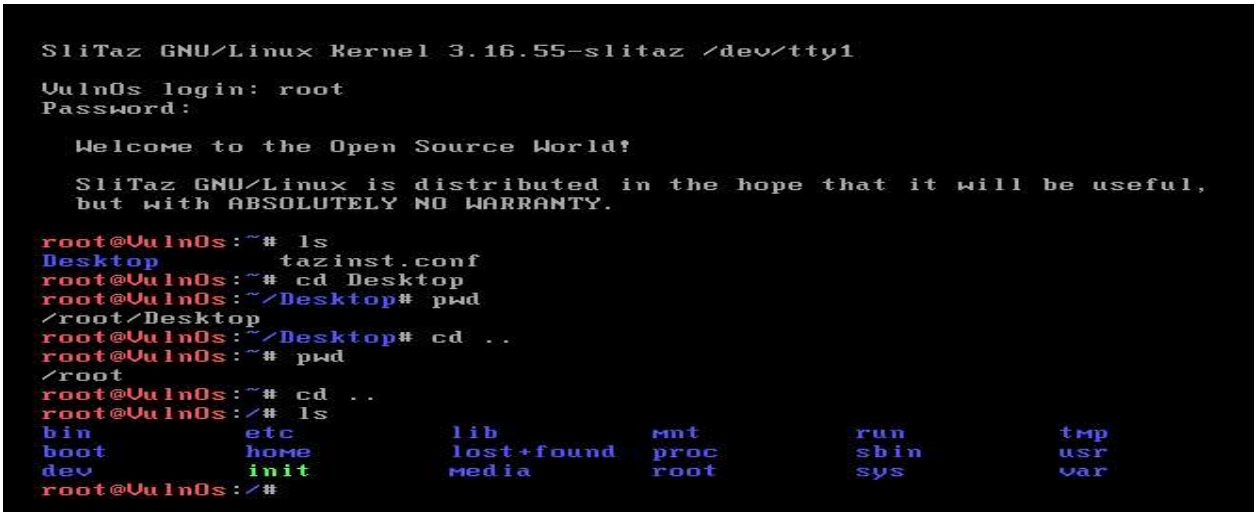

It displays user credentials




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



```
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# ls
root@VulnOs:~/Desktop# cd home
-sh: cd: can't cd to home
root@VulnOs:~/Desktop# cd ..
root@VulnOs:~# cd ..
root@VulnOs:/# ls
bin         etc         lib         mnt         run         tmp
boot        home        lost+found  proc        sbin        usr
dev         init        media       root        sys         var
root@VulnOs:/# cd home
root@VulnOs:/home# cd desktop
-sh: cd: can't cd to desktop
root@VulnOs:/home# ls
test
root@VulnOs:/home# cd test
root@VulnOs:/home/test# ls
Desktop    Downloads  Music      Templates
Documents  Images     Public     Videos
root@VulnOs:/home/test# cd Desktop
root@VulnOs:/home/test/Desktop# ls
cap.pcapng  s3cr3t.txt
root@VulnOs:/home/test/Desktop# cat s3cr3t.txt
37cedde2e90a22a53f12c57094e1f0dea2ddd260
root@VulnOs:/home/test/Desktop#
```