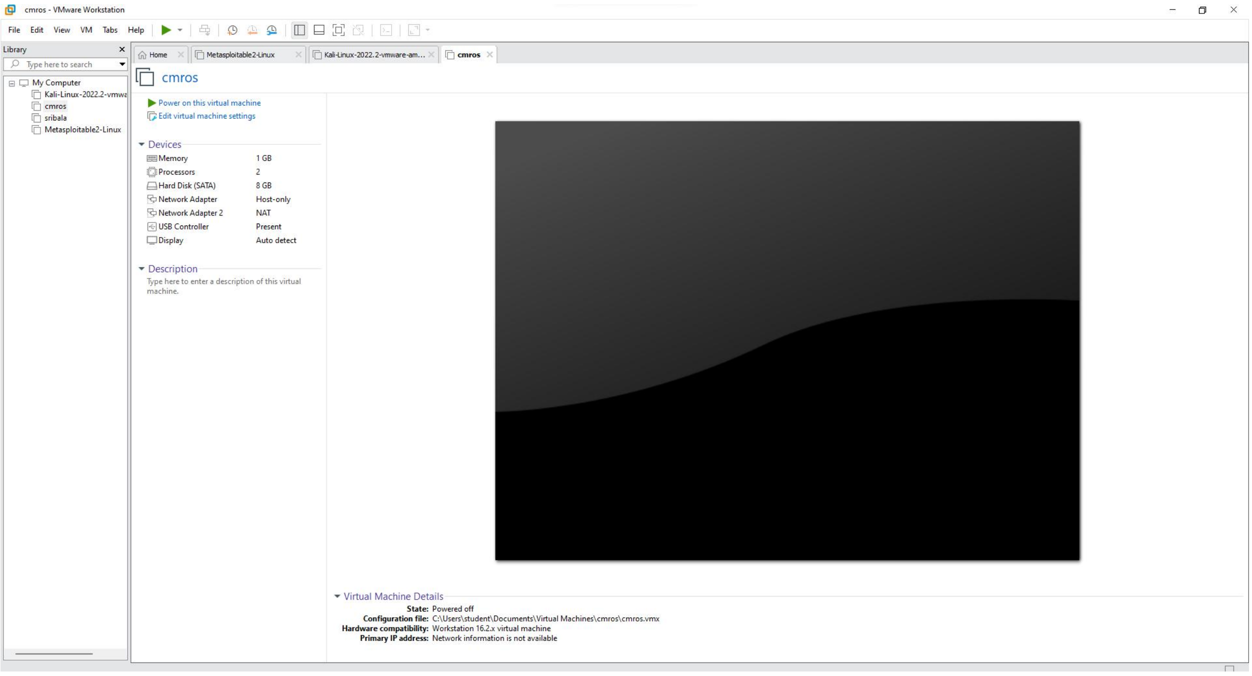
Experiment 7: Analyze and exploit the root system of CMROS

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



cmros

Power on this virtual machine
Edit virtual machine settings

Devices

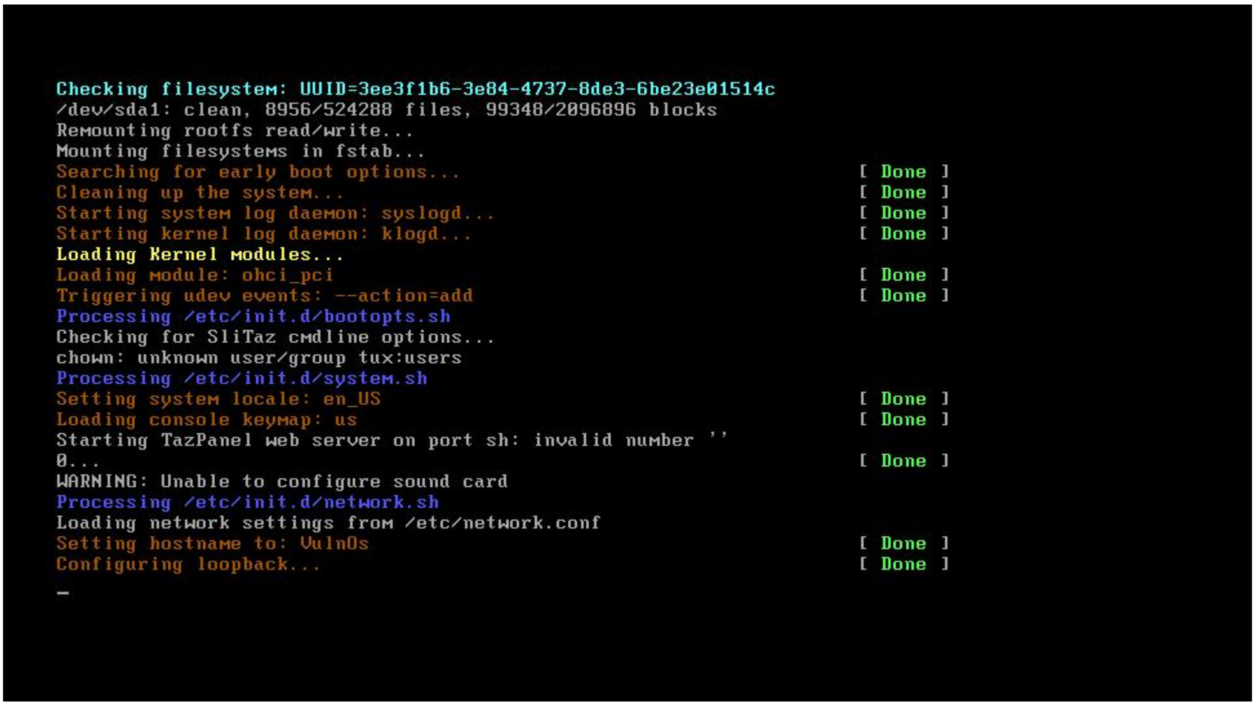
Memory	1 GB
Processors	2
Hard Disk (SATA)	8 GB
Network Adapter	Host-only
Network Adapter 2	NAT
USB Controller	Present
Display	Auto detect

Description
Type here to enter a description of this virtual machine.

Virtual Machine Details

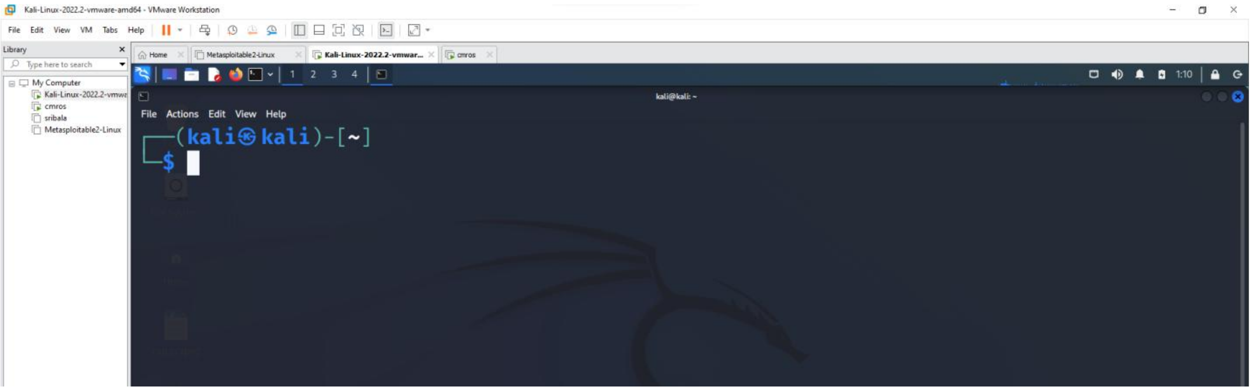
State:	Powered off
Configuration file:	C:\Users\student\Documents\Virtual Machines\cmros\cmros.vmx
Hardware compatibility:	Workstation 16.2.x virtual machine
Primary IP address:	Network information is not available

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



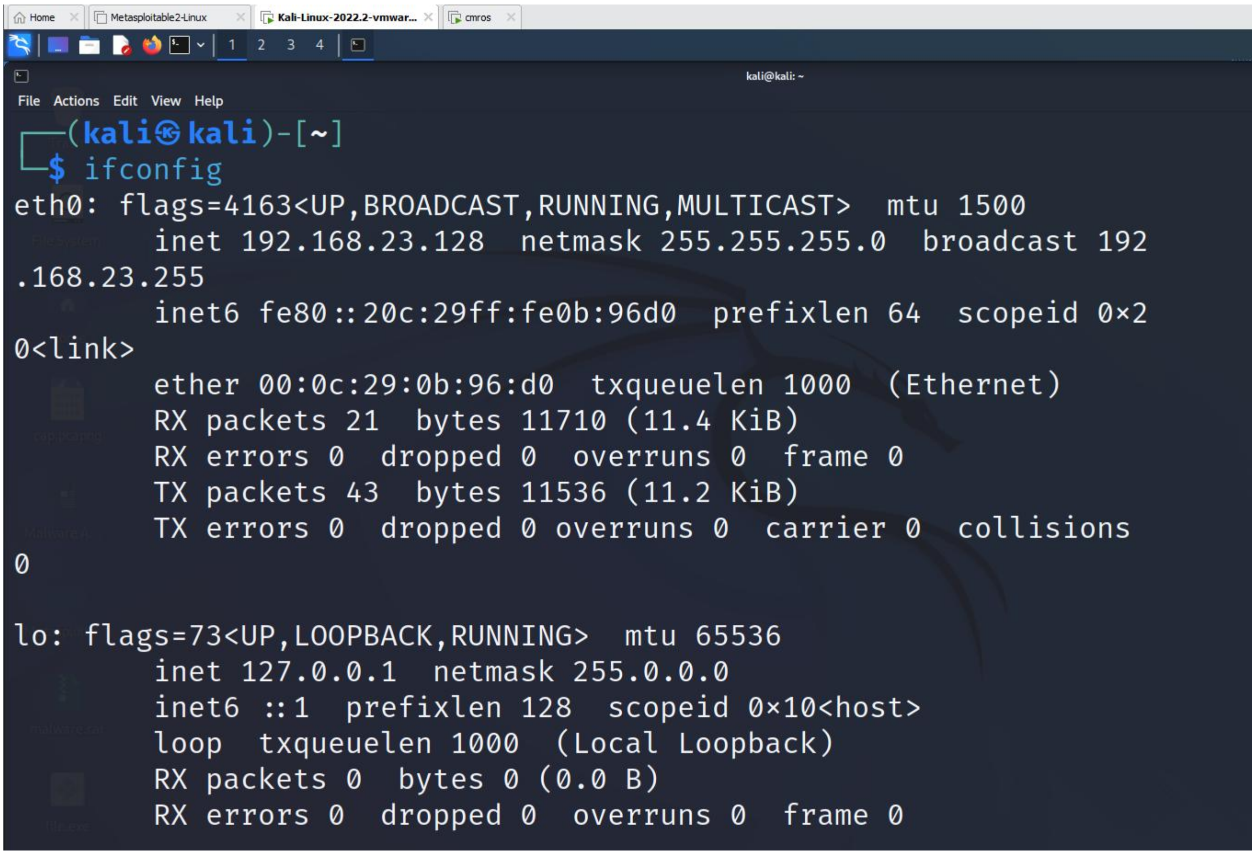
```
Checking filesystem: UUID=3ee3f1b6-3e84-4737-8de3-6be23e01514c
/dev/sda1: clean, 8956/524288 files, 99348/2096896 blocks
Remounting rootfs read/write...
Mounting filesystems in fstab...
Searching for early boot options...                            [ Done ]
Cleaning up the system...                                      [ Done ]
Starting system log daemon: syslogd...                         [ Done ]
Starting kernel log daemon: klogd...                           [ Done ]
Loading Kernel modules...
Loading module: ohci_pci                                       [ Done ]
Triggering udev events: --action=add                           [ Done ]
Processing /etc/init.d/bootopts.sh
Checking for SliTaz cmdline options...
chown: unknown user/group tux:users
Processing /etc/init.d/system.sh
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
Loading network settings from /etc/network.conf
Setting hostname to: VulnOs                                    [ Done ]
Configuring loopback...                                        [ Done ]
_
```

Step5: Open Kali linux on and open terminal


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Kali-Linux-2022.2-vmware
cmros
sribala
Metasploitable2-Linux
Home
Metasploitable2-Linux
Kali-Linux-2022.2-vmwar...
cmros
kali@kali: ~
File Actions Edit View Help

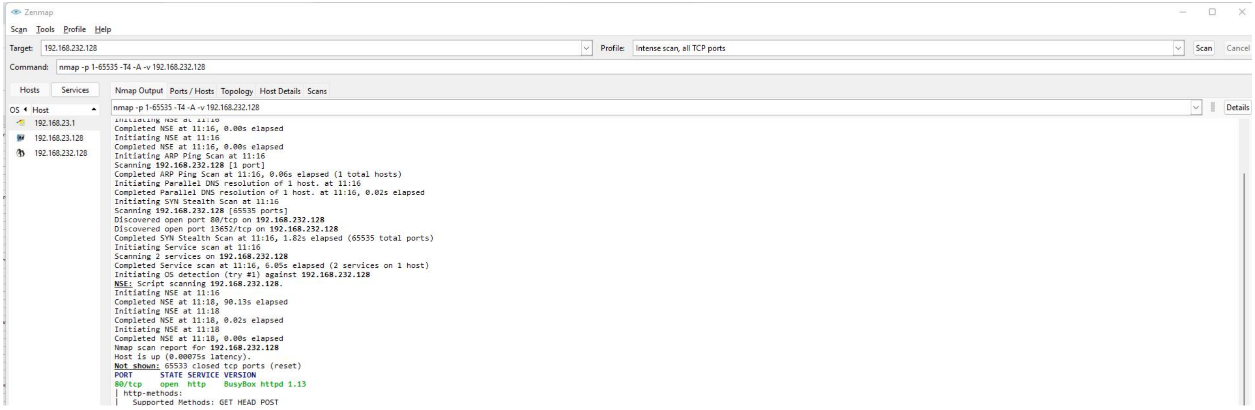
```
┌──(kali㉿kali)-[~]
└─$ 
```

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.



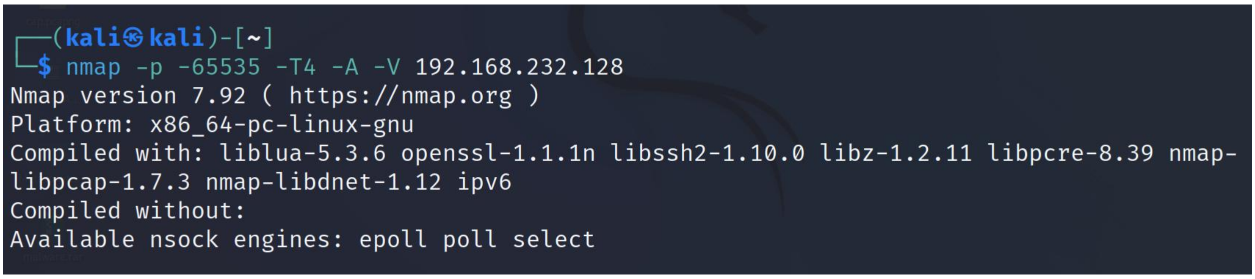
Target: 192.168.232.128

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.232.128

```
nmap -p 1-65535 -T4 -A -v 192.168.232.128
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating ARP Ping Scan at 11:16
Scanning 192.168.232.128 [1 port]
Completed ARP Ping Scan at 11:16, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:16
Completed Parallel DNS resolution of 1 host. at 11:16, 0.02s elapsed
Initiating SYN Stealth Scan at 11:16
Scanning 192.168.232.128 [65535 ports]
Discovered open port 80/tcp on 192.168.232.128
Discovered open port 13652/tcp on 192.168.232.128
Completed SYN Stealth Scan at 11:16, 1.82s elapsed (65535 total ports)
Initiating Service scan at 11:16
Scanning 2 services on 192.168.232.128
Completed Service scan at 11:16, 6.05s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.232.128
NSE: Script scanning 192.168.232.128.
Initiating NSE at 11:16
Completed NSE at 11:18, 90.13s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.02s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Nmap scan report for 192.168.232.128
Host is up (0.00075s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    BusyBox httpd 1.13
| http-methods:
|   Supported Methods: GET HEAD POST
```

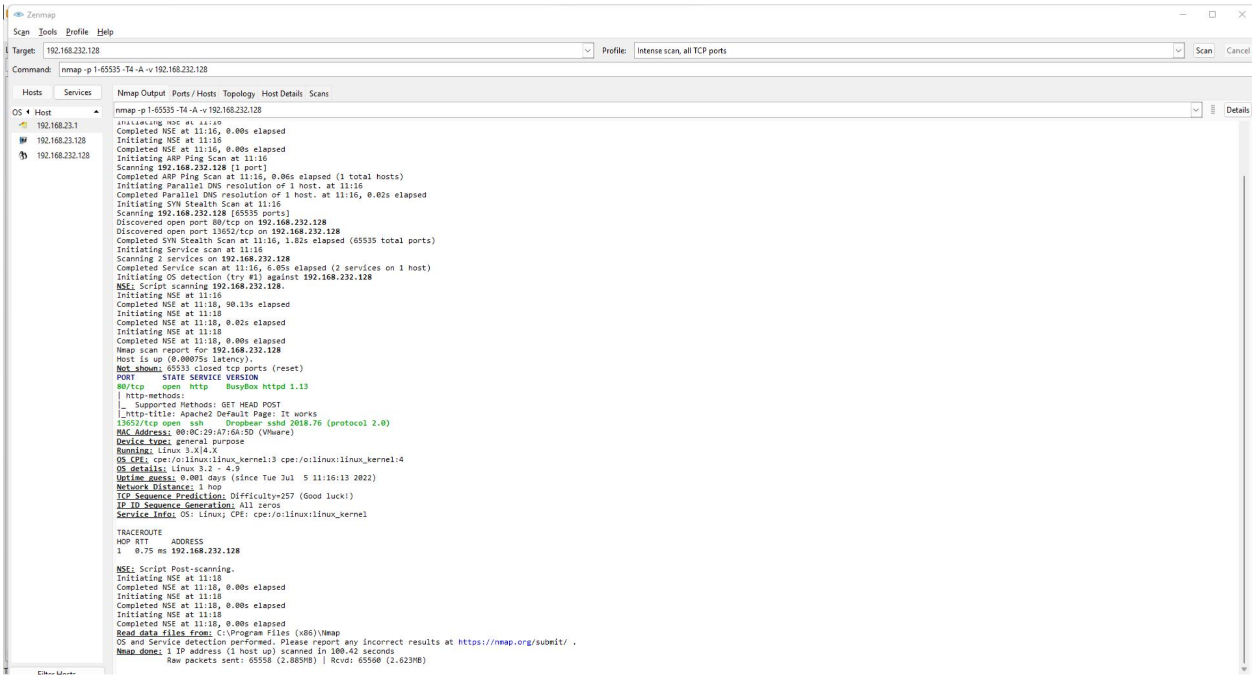
Now use the command below in the kali linux terminal



```
┌──(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.



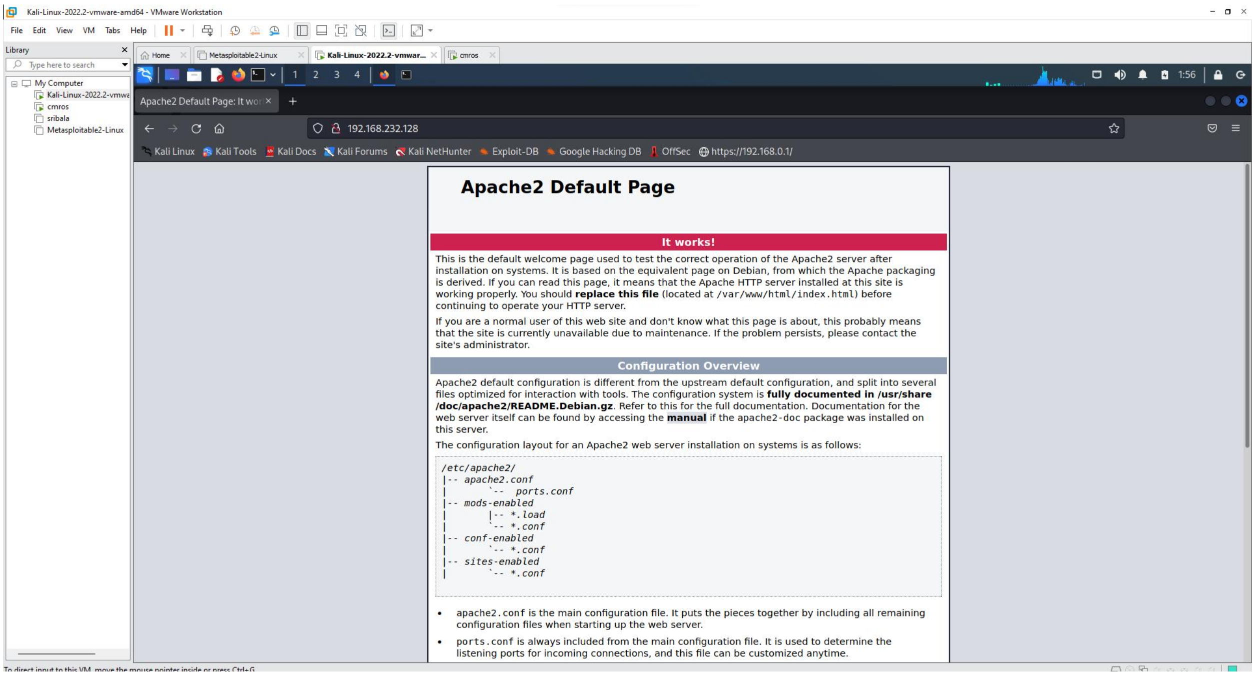
Target: 192.168.232.128

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.232.128

```
nmap -p 1-65535 -T4 -A -v 192.168.232.128
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating ARP Ping Scan at 11:16
Scanning 192.168.232.128 [1 port]
Completed ARP Ping Scan at 11:16, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:16
Completed Parallel DNS resolution of 1 host. at 11:16, 0.02s elapsed
Initiating SYN Stealth Scan at 11:16
Scanning 192.168.232.128 [65535 ports]
Discovered open port 80/tcp on 192.168.232.128
Discovered open port 13652/tcp on 192.168.232.128
Completed SYN Stealth Scan at 11:16, 1.82s elapsed (65535 total ports)
Initiating Service scan at 11:16
Scanning 2 services on 192.168.232.128
Completed Service scan at 11:16, 6.05s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.232.128
NSE: Script scanning 192.168.232.128.
Initiating NSE at 11:16
Completed NSE at 11:18, 90.13s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.02s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Nmap scan report for 192.168.232.128
Host is up (0.00075s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    BusyBox httpd 1.13
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: Apache2 Default Page: It works
13652/tcp open  ssh     Dropbear sshd 2018.76 (protocol 2.0)
MAC Address: 00:0C:29:A7:6A:5D (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 0.001 days (since Tue Jul  5 11:16:13 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.75 ms 192.168.232.128

NSE: Script Post-scanning.
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.42 seconds
           Raw packets sent: 65558 (2.885MB) | Rcvd: 65560 (2.623MB)
```

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



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on systems. It is 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 operate 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

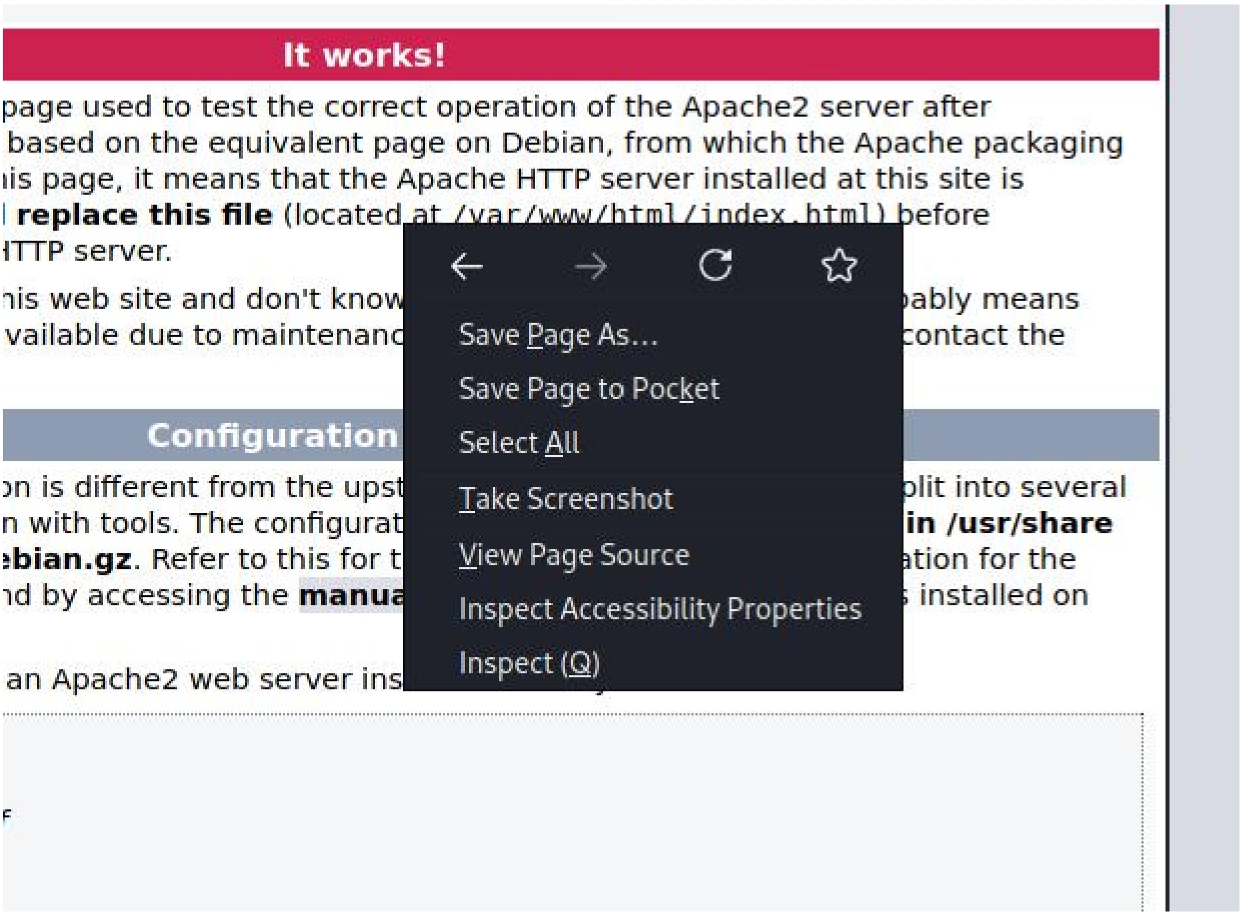
Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with tools. The configuration system is **fully documented in /usr/share /doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation 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-enabled
|       |-- *.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.

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
iis page, it means that the Apache HTTP server installed at this site is
l **replace this file** (located at /var/www/html/index.html) before
ITTP server.

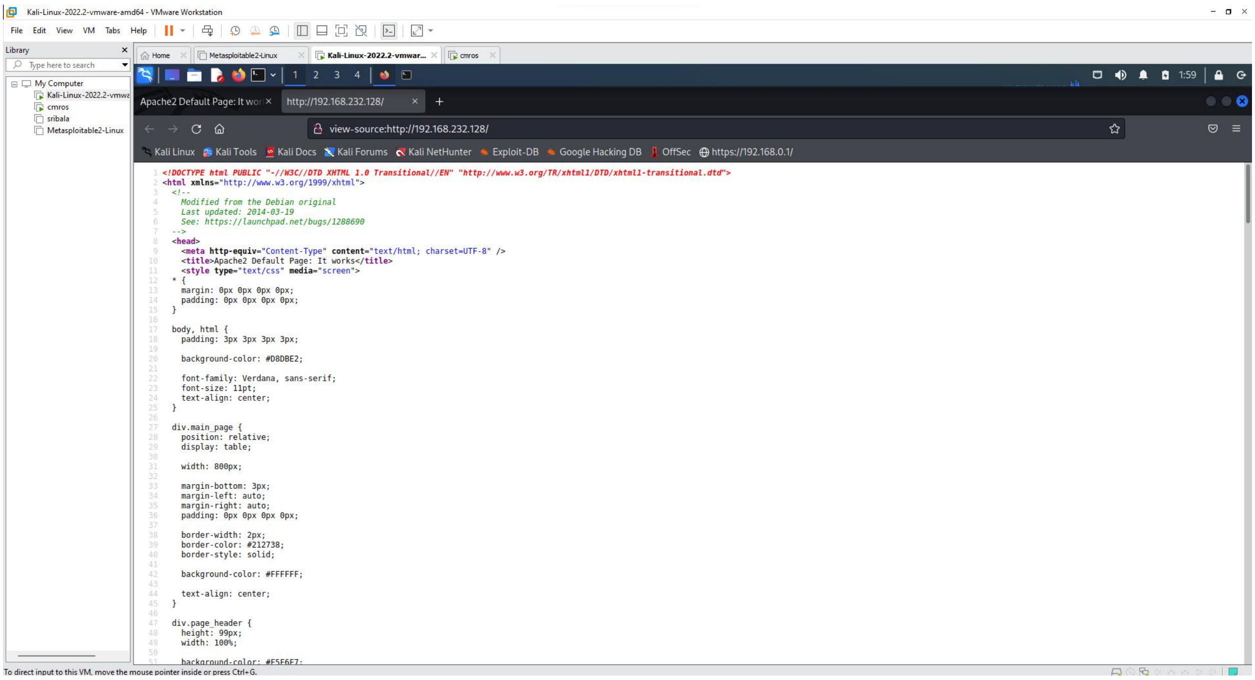
iis web site and don't know … ably means
vailable due to maintenanc … contact the

Configuration

n is different from the upst … plit into several
n with tools. The configurat … **in /usr/share**
ebian.gz. Refer to this for t … ation for the
d by accessing the **manua** … installed on

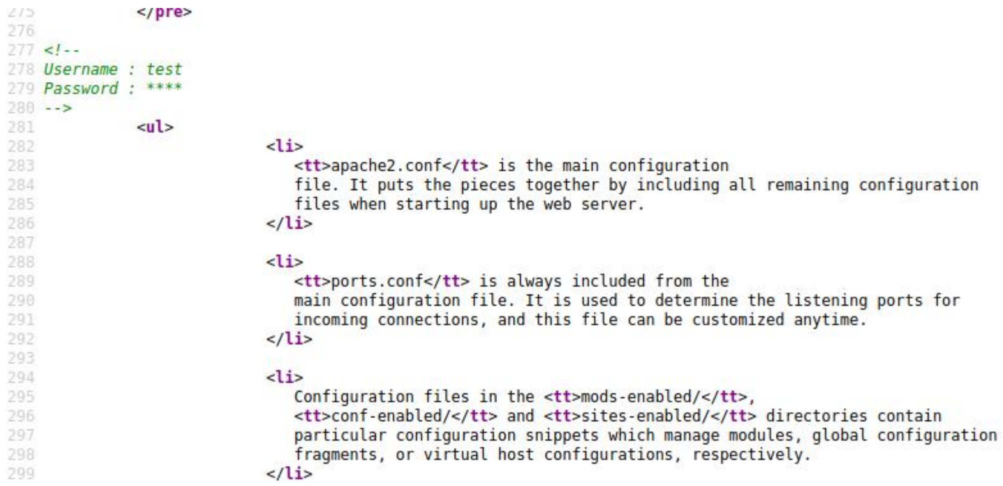
an Apache2 web server ins

It displays the source code



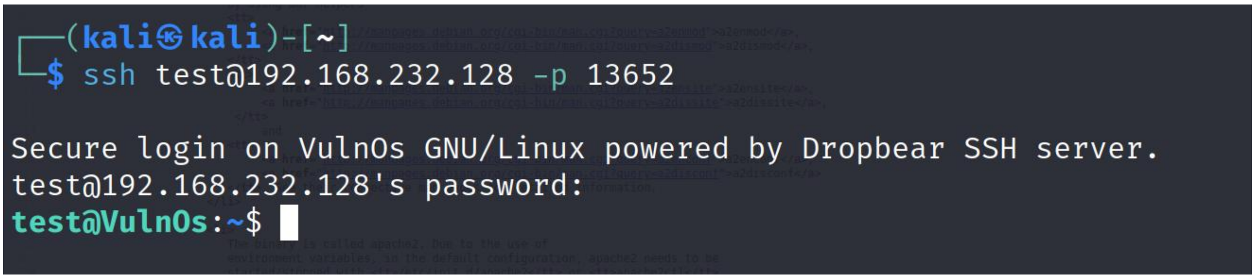
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original
    Last updated: 2014-03-19
    See: https://launchpad.net/bugs/1288690
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    padding: 0px 0px 0px 0px;

    border-width: 2px;
    border-color: #212738;
    border-style: solid;

    background-color: #FFFFFF;

    text-align: center;
  }

  div.page_header {
    height: 99px;
    width: 100%;

    background-color: #E5E6E7;
```

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



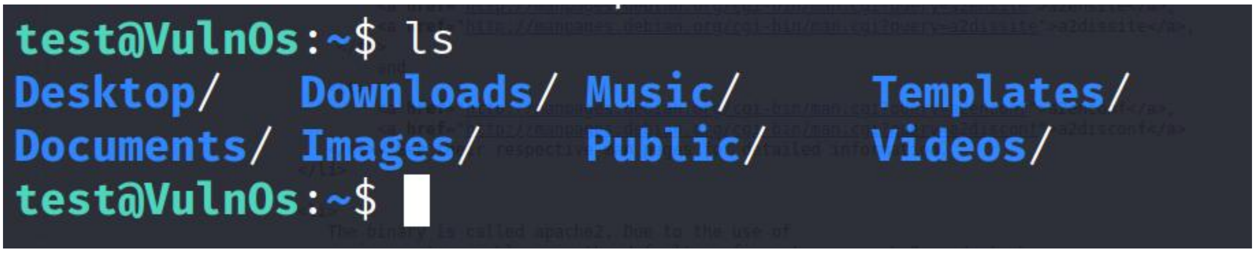
```
        </pre>

<!--
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**



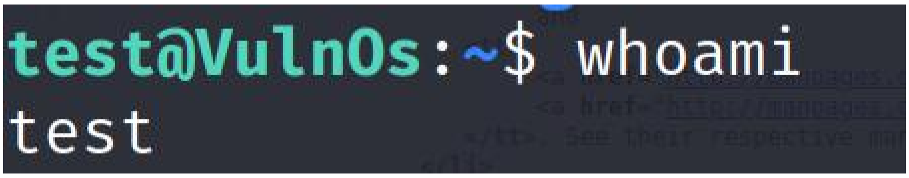
```
┌──(kali㉿kali)-[~]
└─$ ssh test@192.168.232.128 -p 13652

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

Use ls command



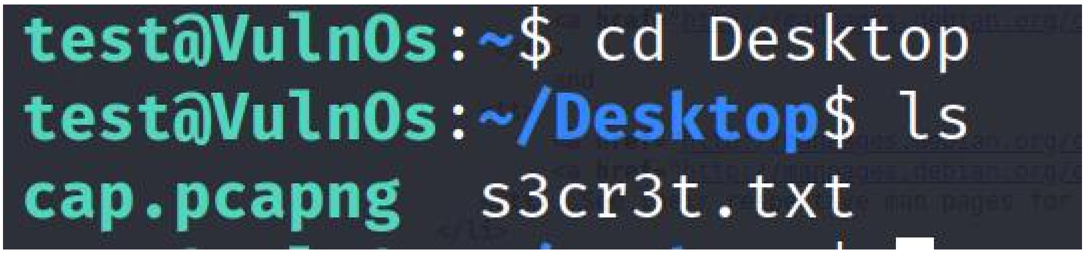
```
test@VulnOs:~$ ls
Desktop/   Downloads/ Music/     Templates/
Documents/ Images/    Public/    Videos/
test@VulnOs:~$ 
```

Use whoami to find the user



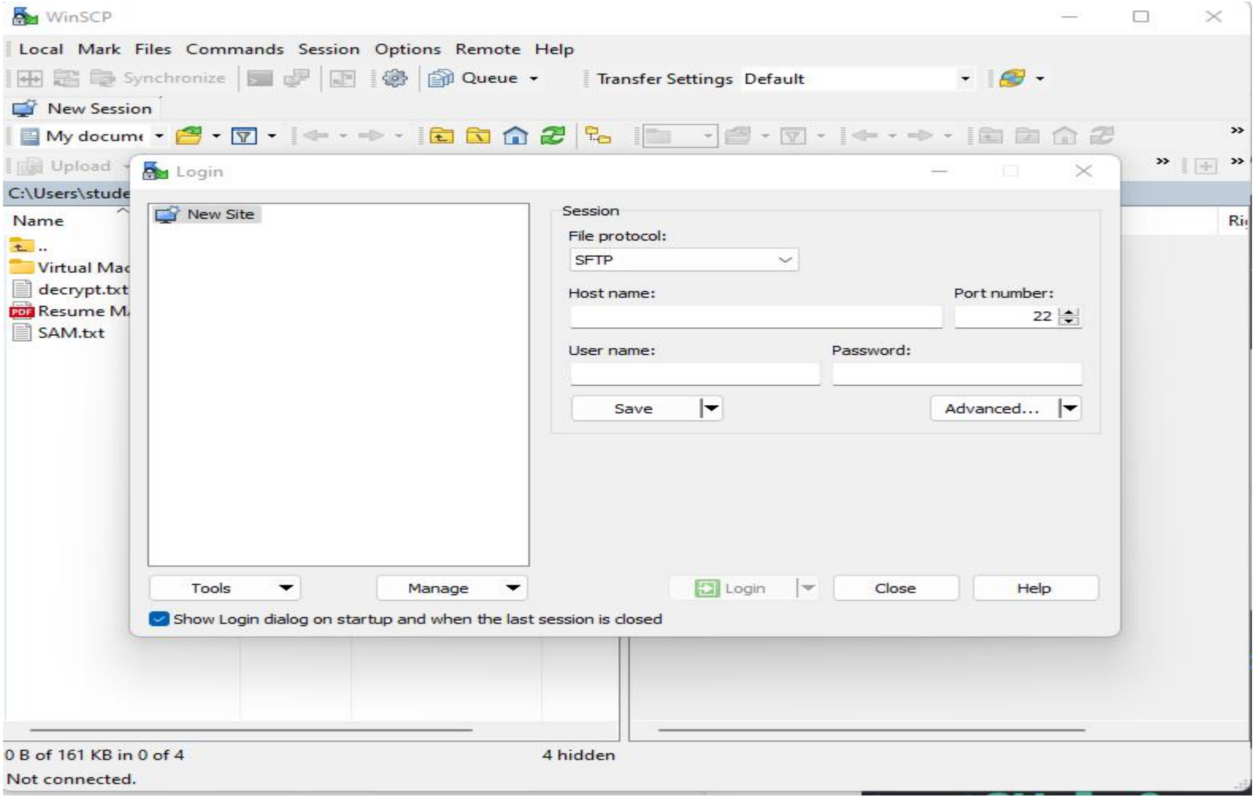
```
test@VulnOs:~$ whoami
test
```

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



C:\Users\stude

Name

..
Virtual Mac
decrypt.txt
Resume M.
SAM.txt

Session

File protocol: SFTP

Host name:

Port number: 22

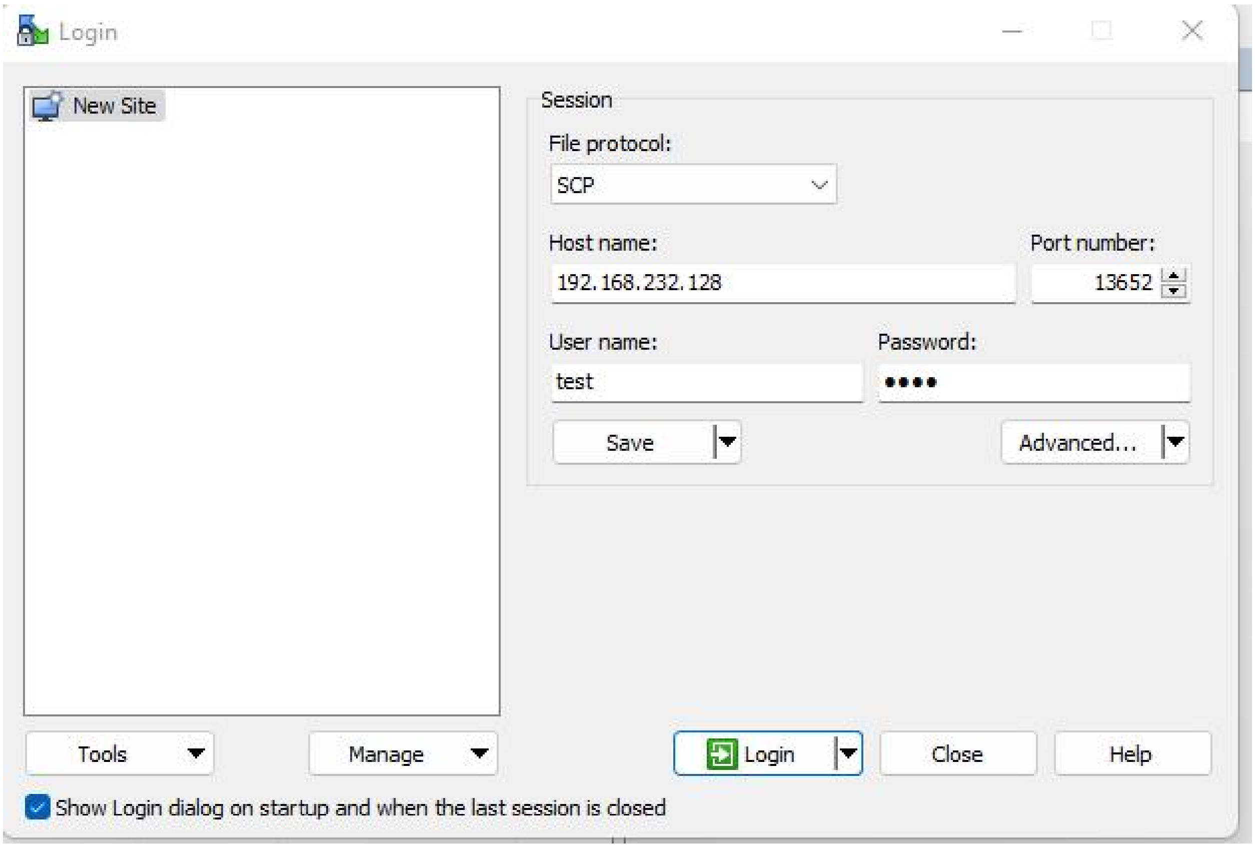
User name:

Password:

☑ Show Login dialog on startup and when the last session is closed

0 B of 161 KB in 0 of 4 4 hidden

Not connected.



Session

File protocol: SCP

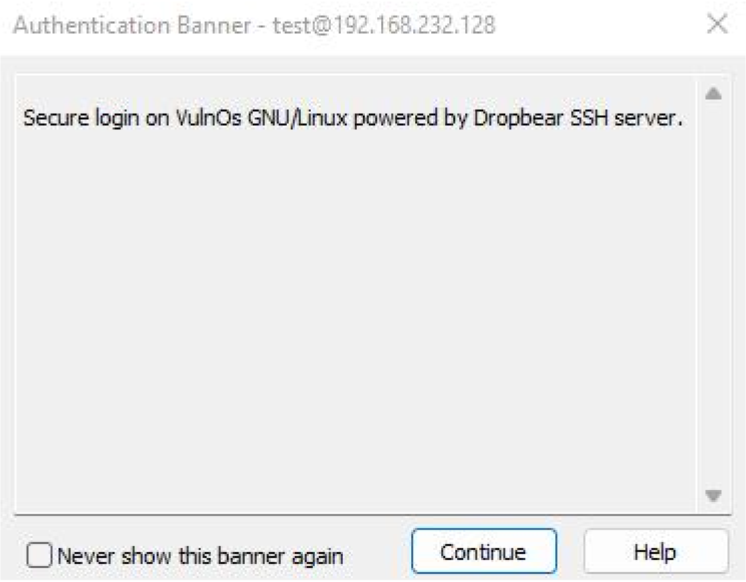
Host name: 192.168.232.128

Port number: 13652

User name: test

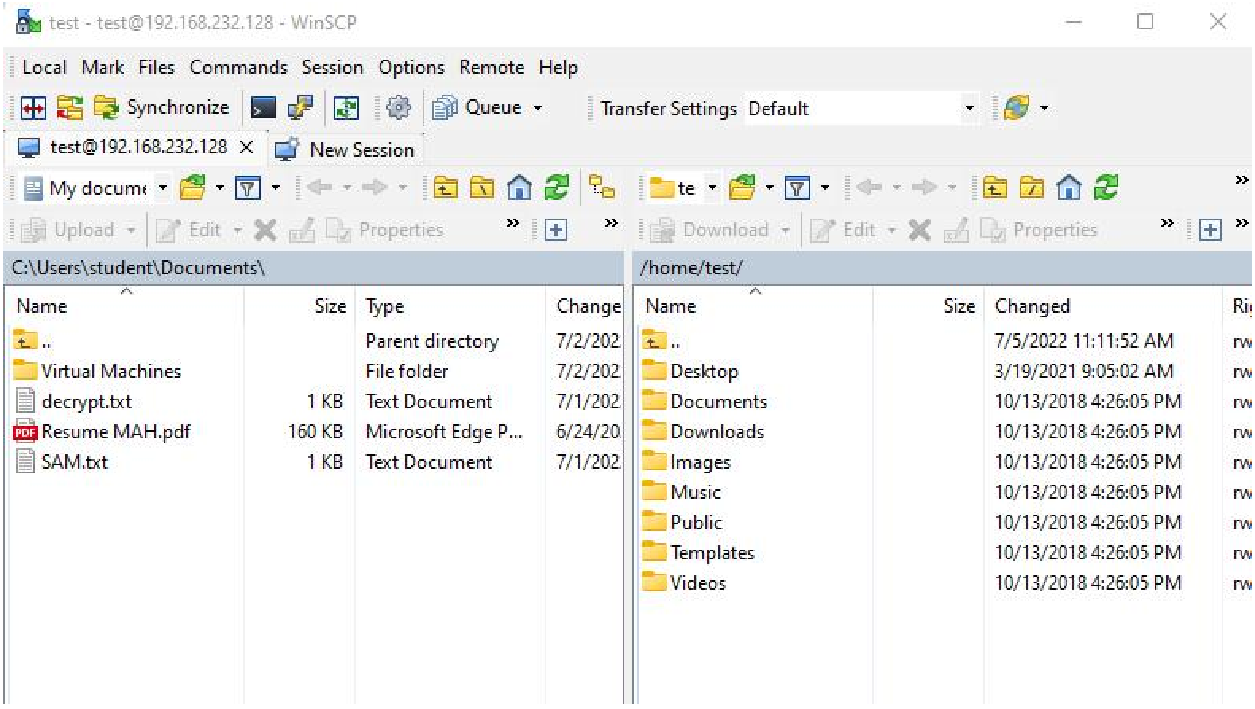
Password: ••••

☑ 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.



test - test@192.168.232.128 - WinSCP

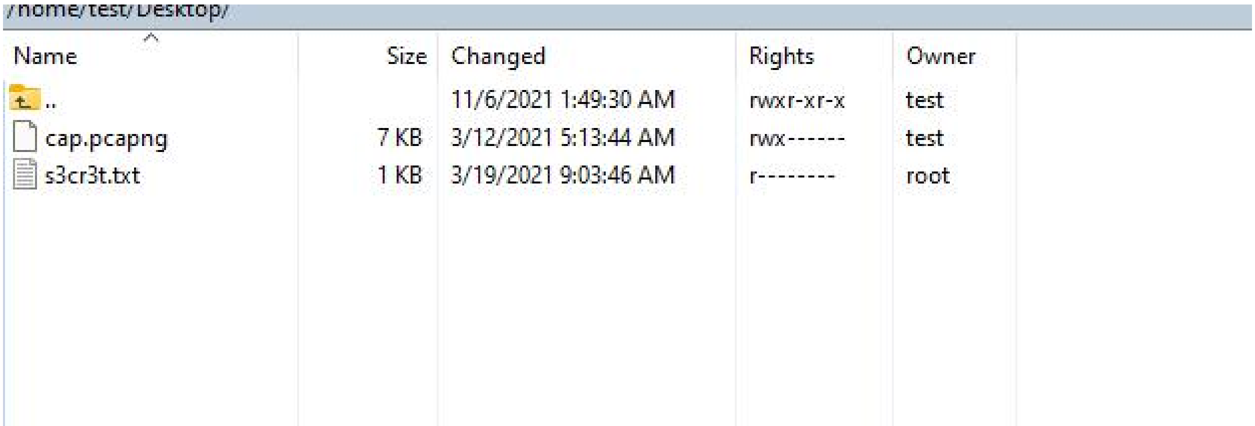
C:\Users\student\Documents\

Name	Size	Type	Change
..		Parent directory	7/2/202
Virtual Machines		File folder	7/2/202
decrypt.txt	1 KB	Text Document	7/1/202
Resume MAH.pdf	160 KB	Microsoft Edge P...	6/24/20
SAM.txt	1 KB	Text Document	7/1/202

/home/test/

Name	Size	Changed	Ri
..		7/5/2022 11:11:52 AM	rw
Desktop		3/19/2021 9:05:02 AM	rw
Documents		10/13/2018 4:26:05 PM	rw
Downloads		10/13/2018 4:26:05 PM	rw
Images		10/13/2018 4:26:05 PM	rw
Music		10/13/2018 4:26:05 PM	rw
Public		10/13/2018 4:26:05 PM	rw
Templates		10/13/2018 4:26:05 PM	rw
Videos		10/13/2018 4:26:05 PM	rw

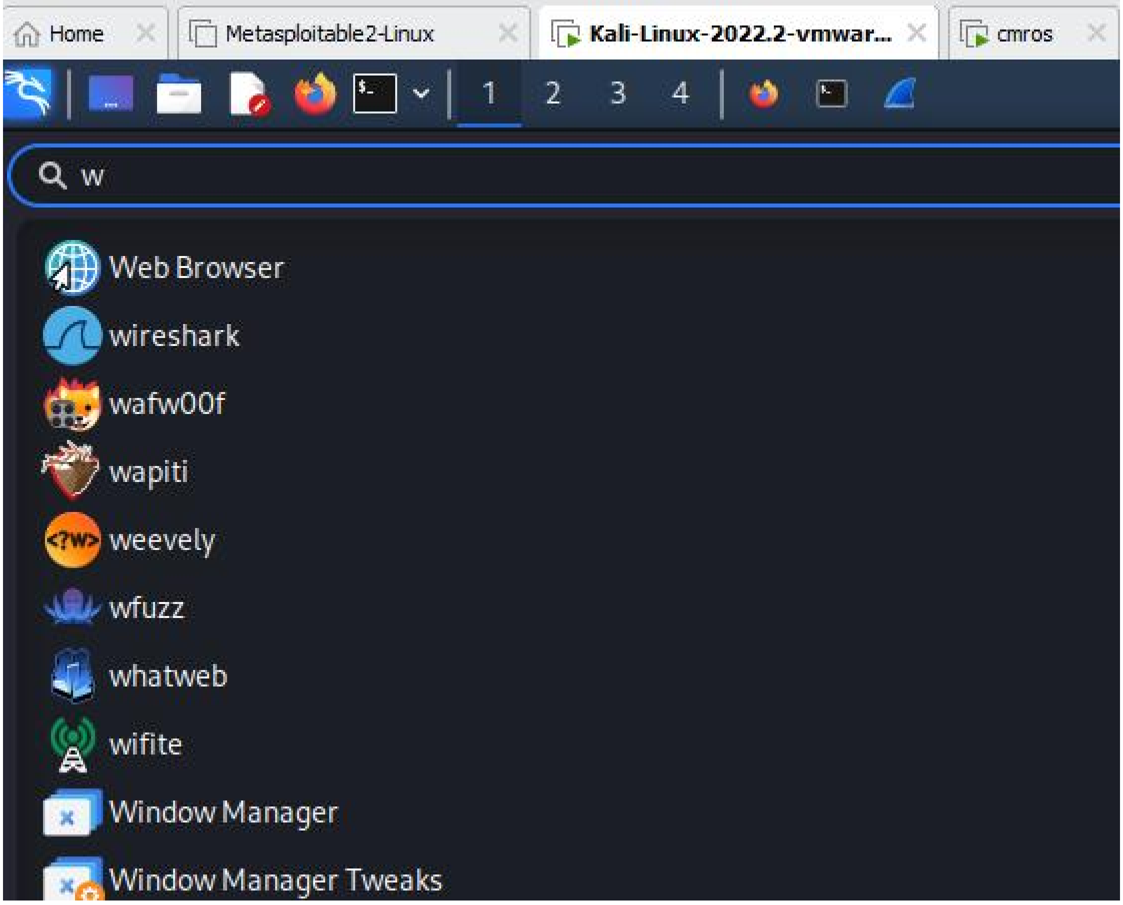
Goto Desktop



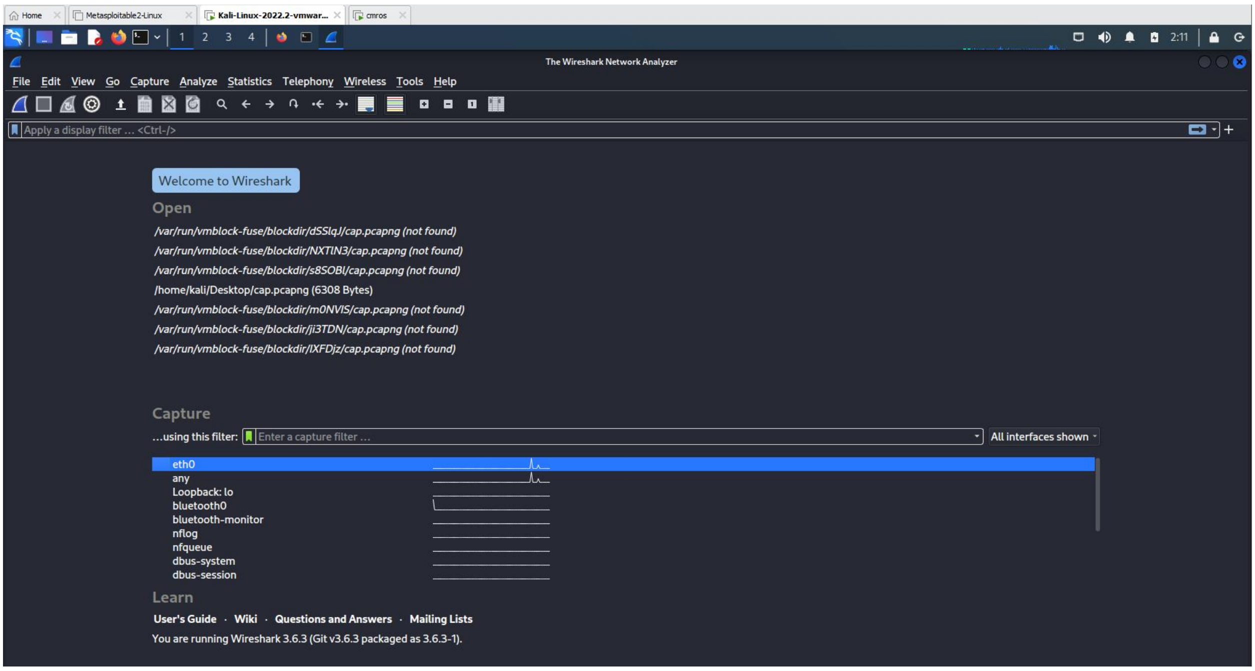
/home/test/Desktop/

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


Home
Metasploitable2-Linux
Kali-Linux-2022.2-vmwar...
cmros
2:11
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark

Open

/var/run/vmblock-fuse/blockdir/dSSlqJ/cap.pcapng (not found)
/var/run/vmblock-fuse/blockdir/NXTIN3/cap.pcapng (not found)
/var/run/vmblock-fuse/blockdir/s8SOBI/cap.pcapng (not found)
/home/kali/Desktop/cap.pcapng (6308 Bytes)
/var/run/vmblock-fuse/blockdir/m0NVIS/cap.pcapng (not found)
/var/run/vmblock-fuse/blockdir/ji3TDN/cap.pcapng (not found)
/var/run/vmblock-fuse/blockdir/IXFDjz/cap.pcapng (not found)

Capture

…using this filter: Enter a capture filter … All interfaces shown

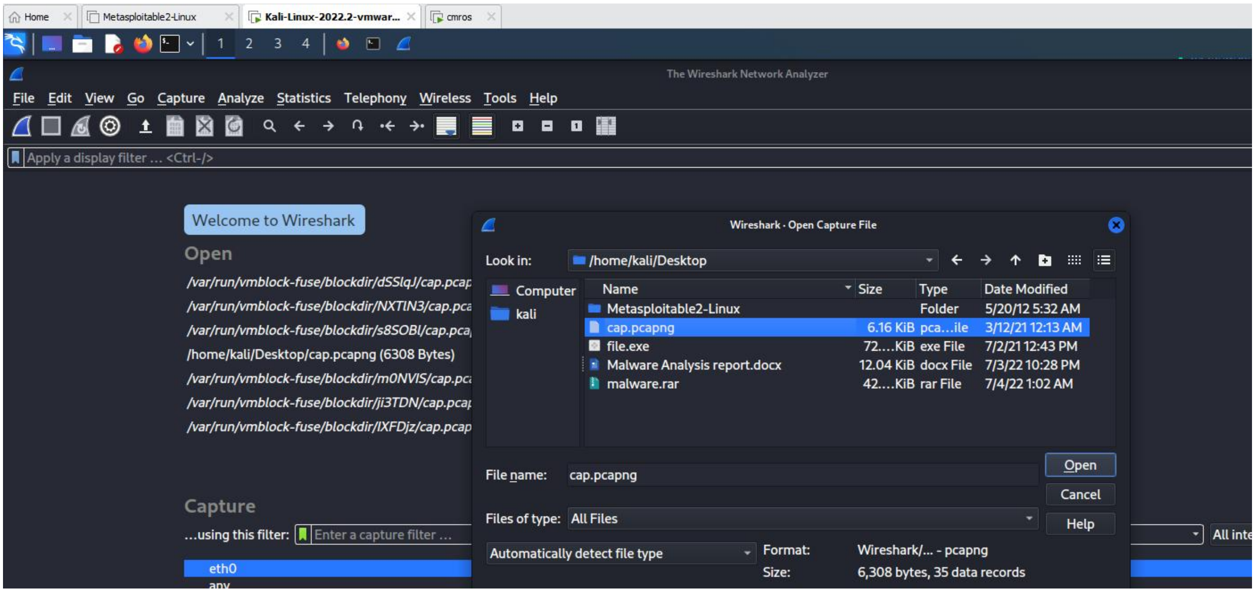
eth0
any
Loopback: lo
bluetooth0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.3 (Git v3.6.3 packaged as 3.6.3-1).

Open cap.pcapng file in the wireshark from desktop folder


Home
Metasploitable2-Linux
Kali-Linux-2022.2-vmwar...
cmros
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Open
Capture
…using this filter:
Enter a capture filter …
eth0
any
Wireshark · Open Capture File
Computer
kali
Open
Cancel
Help
All inte

/var/run/vmblock-fuse/blockdir/dSSlqJ/cap.pcap
/var/run/vmblock-fuse/blockdir/NXTIN3/cap.pca
/var/run/vmblock-fuse/blockdir/s8SOBI/cap.pca
/home/kali/Desktop/cap.pcapng (6308 Bytes)
/var/run/vmblock-fuse/blockdir/m0NVIS/cap.pc
/var/run/vmblock-fuse/blockdir/ji3TDN/cap.pca
/var/run/vmblock-fuse/blockdir/lXFDjz/cap.pcap

Look in: /home/kali/Desktop

Name	Size	Type	Date Modified
Metasploitable2-Linux		Folder	5/20/12 5:32 AM
cap.pcapng	6.16 KiB	pca…ile	3/12/21 12:13 AM
file.exe	72….KiB	exe File	7/2/21 12:43 PM
Malware Analysis report.docx	12.04 KiB	docx File	7/3/22 10:28 PM
malware.rar	42….KiB	rar File	7/4/22 1:02 AM

File name: cap.pcapng

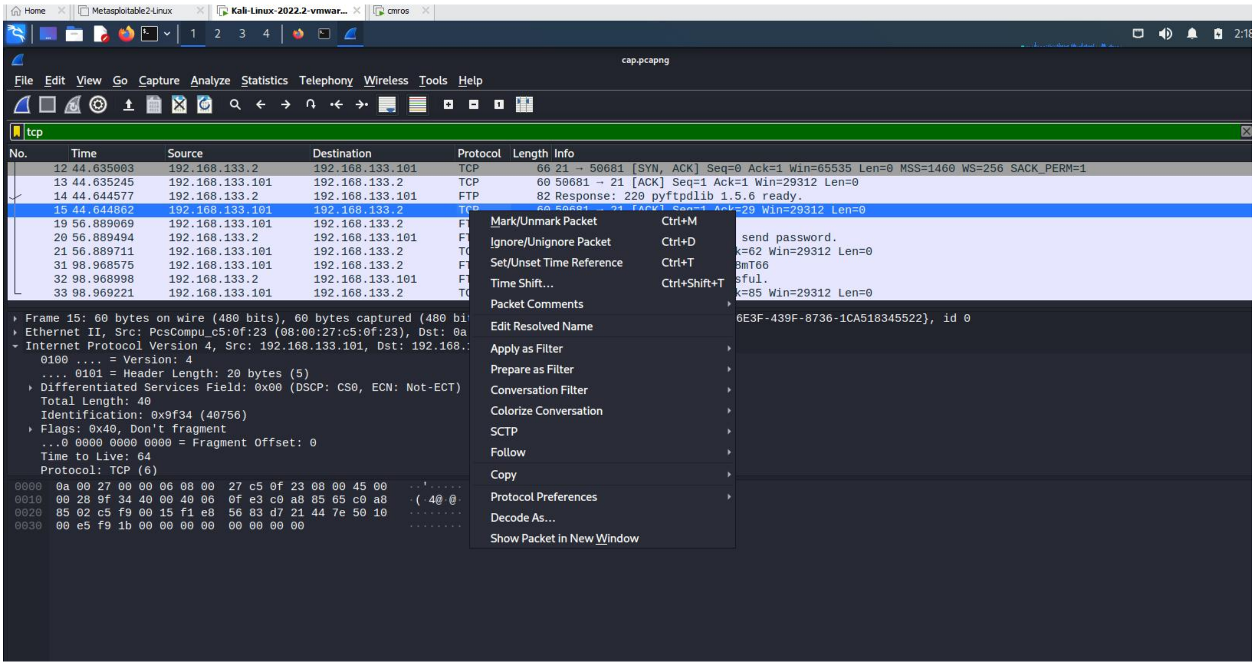
Files of type: All Files

Automatically detect file type

Format: Wireshark/... - pcapng

Size: 6,308 bytes, 35 data records

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



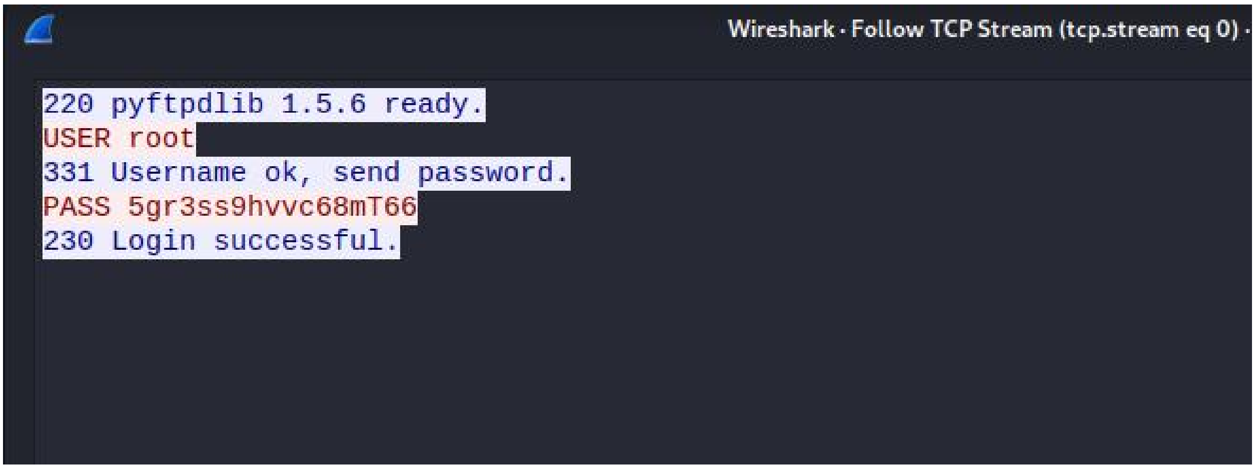
tcp

```
No.  Time       Source           Destination      Protocol Length Info
  12 44.635003  192.168.133.2    192.168.133.101  TCP       66 21 → 50681 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
  13 44.635245  192.168.133.101  192.168.133.2    TCP       60 50681 → 21 [ACK] Seq=1 Ack=1 Win=29312 Len=0
  14 44.644577  192.168.133.2    192.168.133.101  FTP       82 Response: 220 pyftpdlib 1.5.6 ready.
  15 44.644862  192.168.133.101  192.168.133.2    TCP       60 50681 → 21 [ACK] Seq=1 Ack=29 Win=29312 Len=0
  19 56.889069  192.168.133.101  192.168.133.2    FT
  20 56.889494  192.168.133.2    192.168.133.101  FT                                         send password.
  21 56.889711  192.168.133.101  192.168.133.2    TC                                        k=62 Win=29312 Len=0
  31 98.968575  192.168.133.101  192.168.133.2    FT                                        8mT66
  32 98.968998  192.168.133.2    192.168.133.101  FT                                        sful.
  33 98.969221  192.168.133.101  192.168.133.2    TC                                        k=85 Win=29312 Len=0
```

```
▸ Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bi                          6E3F-439F-8736-1CA518345522}, id 0
▸ Ethernet II, Src: PcsCompu_c5:0f:23 (08:00:27:c5:0f:23), Dst: 0a
▾ Internet Protocol Version 4, Src: 192.168.133.101, Dst: 192.168.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x9f34 (40756)
  ▸ Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
```

```
0000  0a 00 27 00 00 06 08 00  27 c5 0f 23 08 00 45 00   ··'·····
0010  00 28 9f 34 40 00 40 06  0f e3 c0 a8 85 65 c0 a8   ·(·4@·@·
0020  85 02 c5 f9 00 15 f1 e8  56 83 d7 21 44 7e 50 10   ········
0030  00 e5 f9 1b 00 00 00 00  00 00 00 00               ········
```

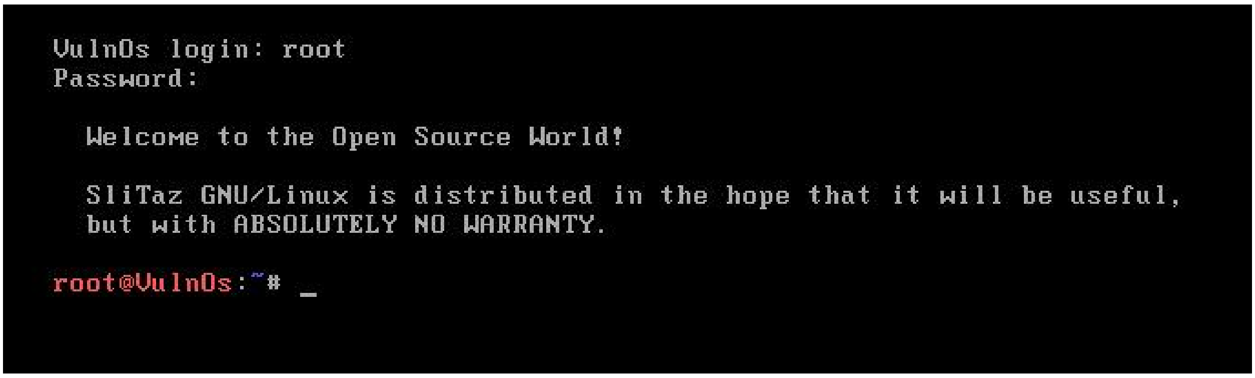
It displays user credentials



```
220 pyftpdlib 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:~# _
```

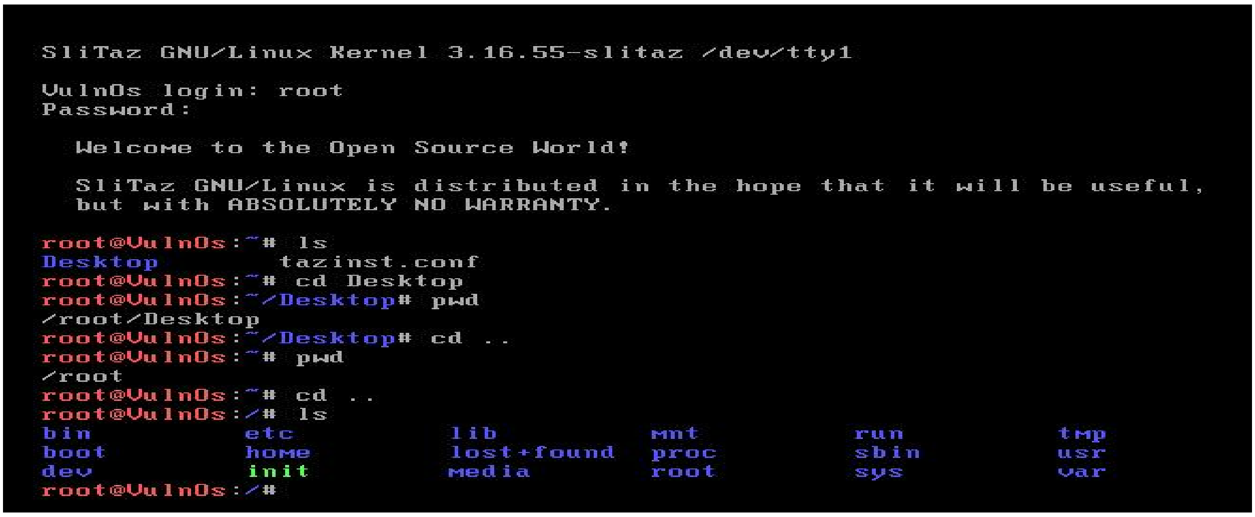
Now use ls command

root@VulnOs:~# ls

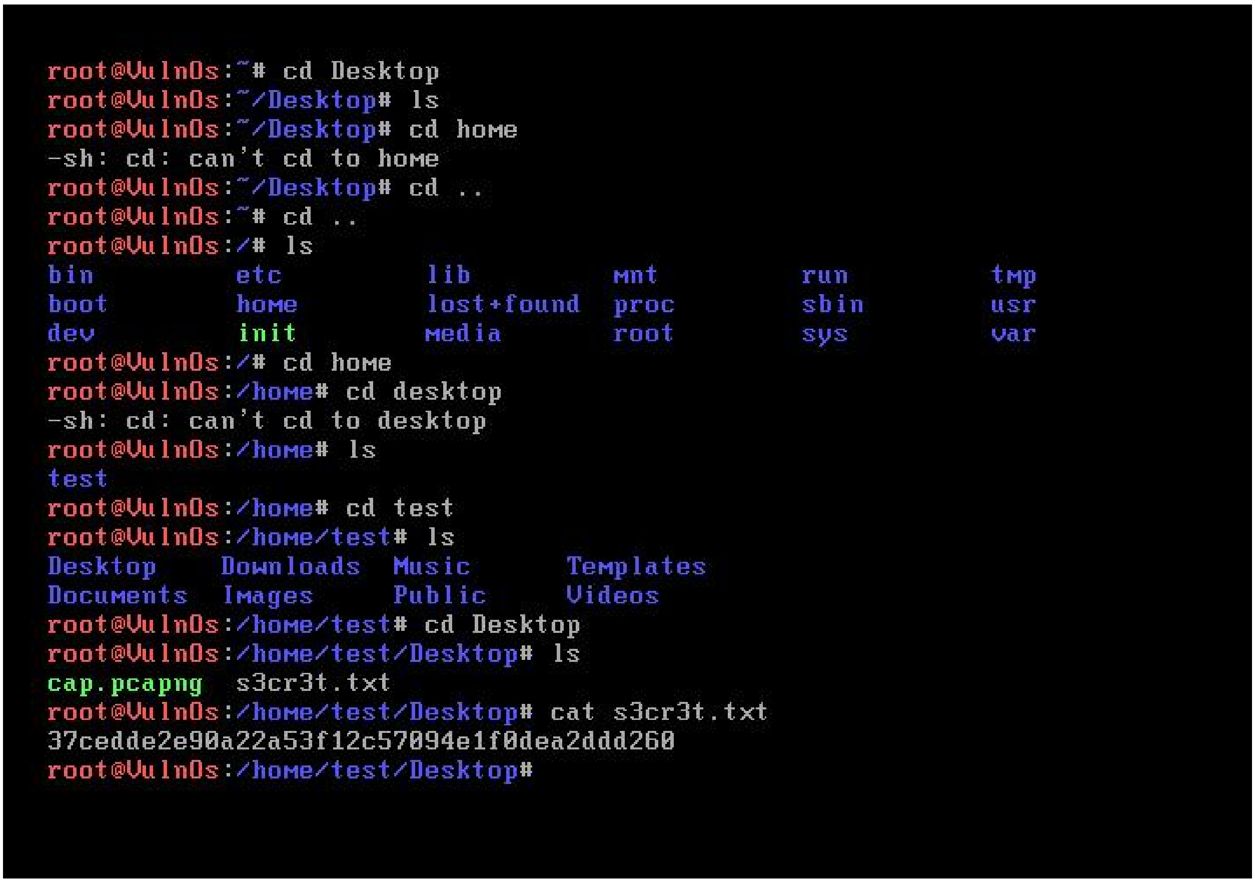
Desktop tazinst.conf

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:~# 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#
```