ACADEMOR

COURSE : CYBER SECURITY

BY : GUDA LOHITHA REDDY

GMAIL : [lohithareddy182004@gmail.com](mailto:lohithareddy182004@gmail.com)



ACKNOWLEDGMENT

It is great pleasure for me to express my gratitude to Academor, for giving the opportunity and platform with facilities in accomplishing the project report.

I express my sincere gratitude to Rajesh Biswas sir for his administration towards Cyber Security knowledge growth.

Finally , it is pleased to acknowledge the indebtedness to all those who devoted themselves directly or indirectly to make this project report success.

ABSTRACT

* WiFi - WPA/2 : Handshake Capturing & Cracking Key
* Perform Session Hijacking & get Login Access using DVWA
* Generate cipher.txt which includes Encrypted value of your “Name” using the RSA public key & Hide cipher.txt behind Image using Steganography. Also showcase decryption using RSA Private Key

1. WiFi - WPA/2 : Handshake Capturing & Cracking Key

***Needs:*** To hack wifi we need specific WLAN(wireless network accessing) for the system which we are performing the hacking technique.

Processes:

Firstly open kali linux and go to terminal.

Step 1: ifconfig(interface configuration) : To view or change the configuration of the network interfaces on your system.

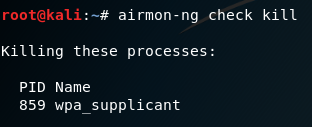


Wlan0(wireless network here) is needed for hacking the wifi.

Step 2 : Stop the current processes which are using the **WiFi** interface.

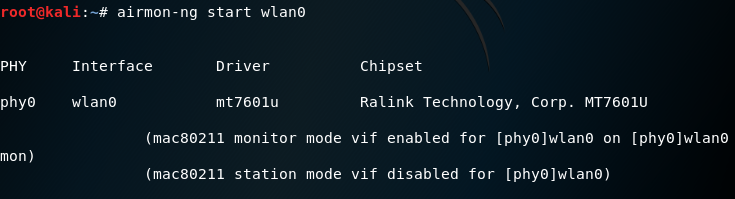
To stop the current processes using the WIFI interface we use

airmon-ng check kill perform this in kali terminal.



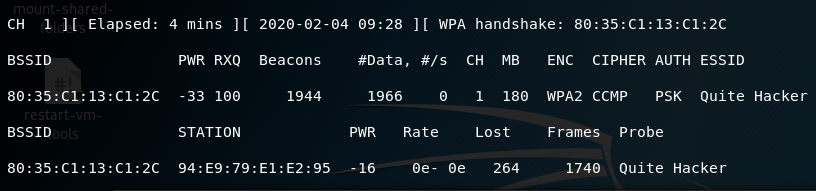
Step 3: To start the wlan0 monitor mode.

Perform **airmon-ng start wlan0**



Step 4 : To view the clients connected to the target network.

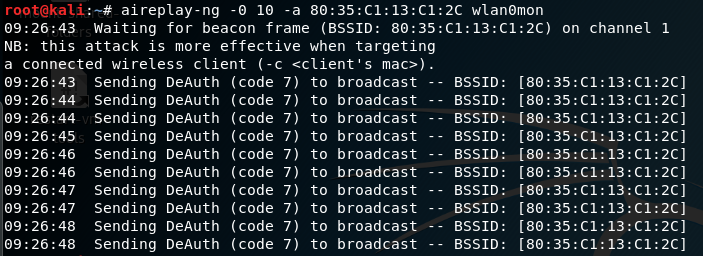
**airodump-ng -c 1 --bssid 80:35:C1:13:C1:2C -w /root wlan0mon**

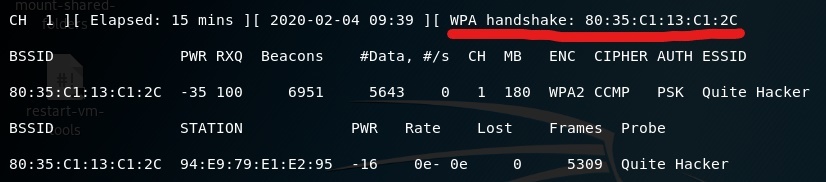


Step 5 :  Open a new terminal window to disconnect the clients connected to the target network.

**aireplay-ng -0 10 -a 80:35:C1:13:C1:2C wlan0mon**

When the client is disconnected from the target network. She/he tries to reconnect to the network and when she/he does you will get something called **WPA** handshake in the previous window of the terminal.





Here we are done with capturing the packets so now we get off from the window.

1. Perform Session Hijacking & get Login Access using DVWA

**INTRO :** While starting as a penetration tester, we need a pentesting-lab to test out our penetration skills. One such system is the Damn Vulnerable Web Application(DVWA).DVWA is a vulnerable web application developed using PHP and MySQL that allows ethical hackers to test out their hacking skills and security tools.

Process:

***Step 1:*** Download the DVWA

We need to clone the DVWA GitHub into our /var/www/html directory. That is the location where Localhost files are stored in Linux systems.

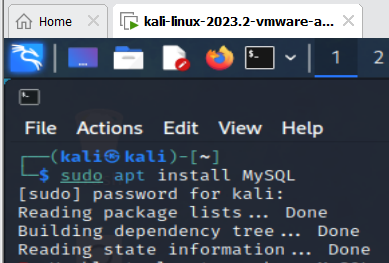
$ cd/var/www/html

Once in this directory, we will clone the DVWA GitHub repository with command line : $ sudo git clone https://github.com/digininja/DVWA

***Step 2:*** Install MySQL in Kali Linux

To install MySQL in kali Linux we use command

$ sudo apt install MySQL

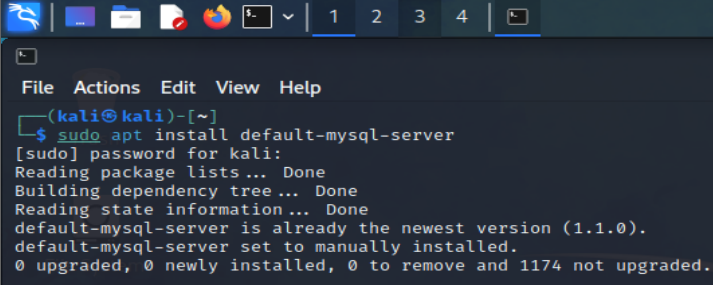


If there is any error occures in installation of MySQL. We can go ahead and install it manually.MySQL comes with two packages

* mysql-server
* mysql-client

We need to install the mysql-server in kali Linux using command

$ sudo apt install default-mysql-server



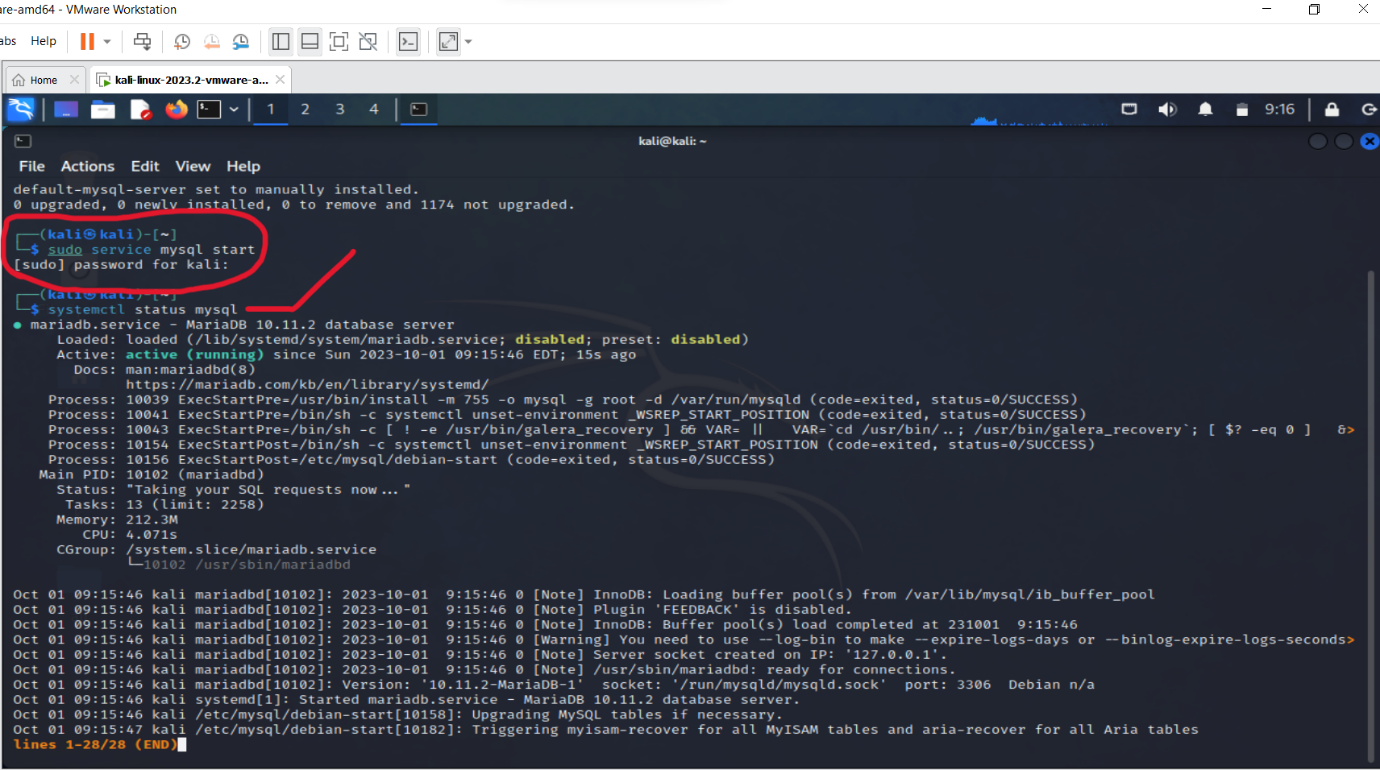
***Step 3***: Configure MySQL Database

* Start the MySQL service with the command in kali Linux

$ sudo service mysql start

* To check whether the service is running using the systemctl status command

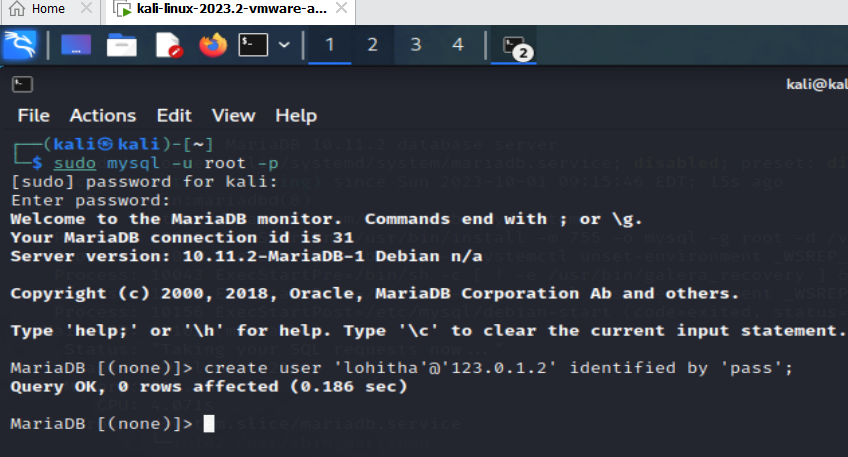
$ systemctl status mysql



* Login to the MySQL database using the command as root.

$ sudo mysql -u root -p

* After entering the command we get a Enter password and then enter the own password.
* Now we get MariaDB[(none)]>”enter the user name “ and the password was pass with local host 123.0.1.2.
* Through with configuring both the DVWA application and the MySQL database. Type exit to close the database.



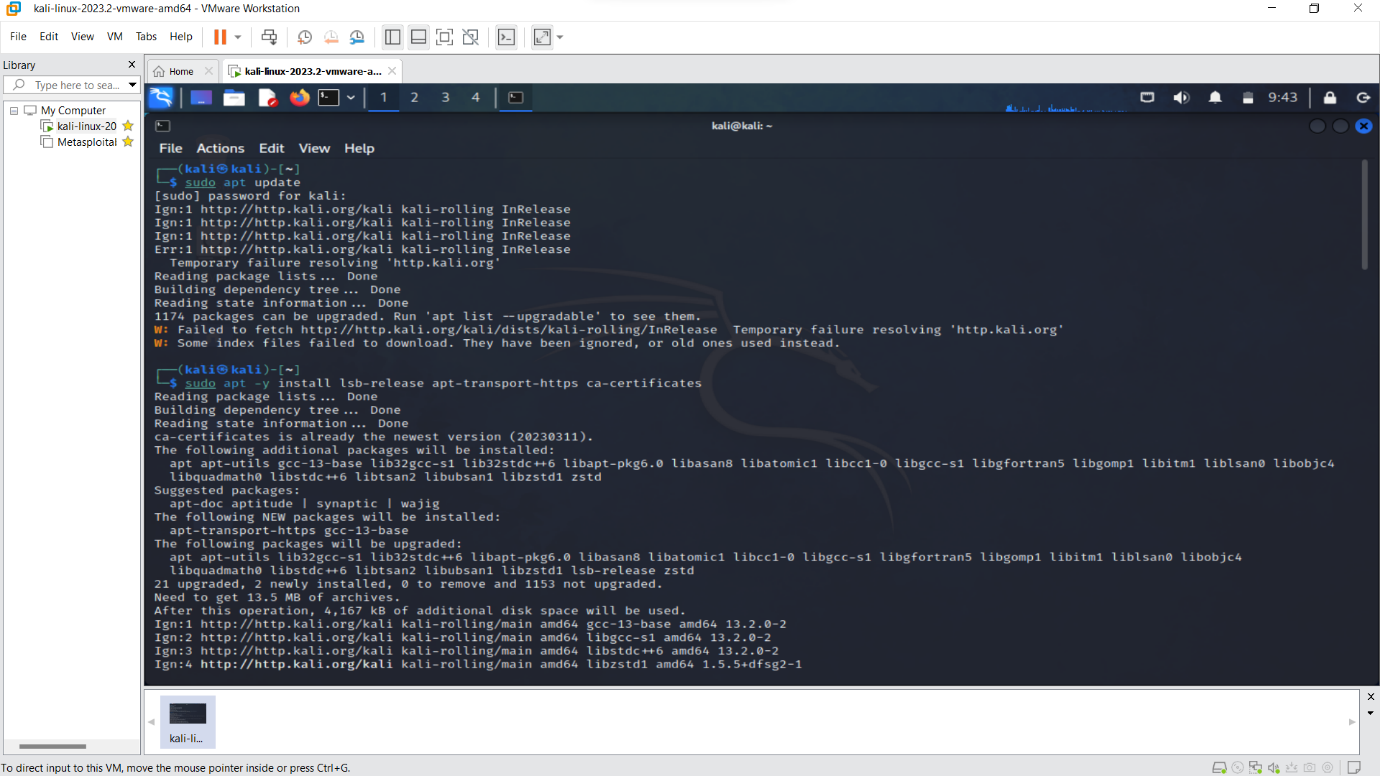
***Step 4:*** Install PHP

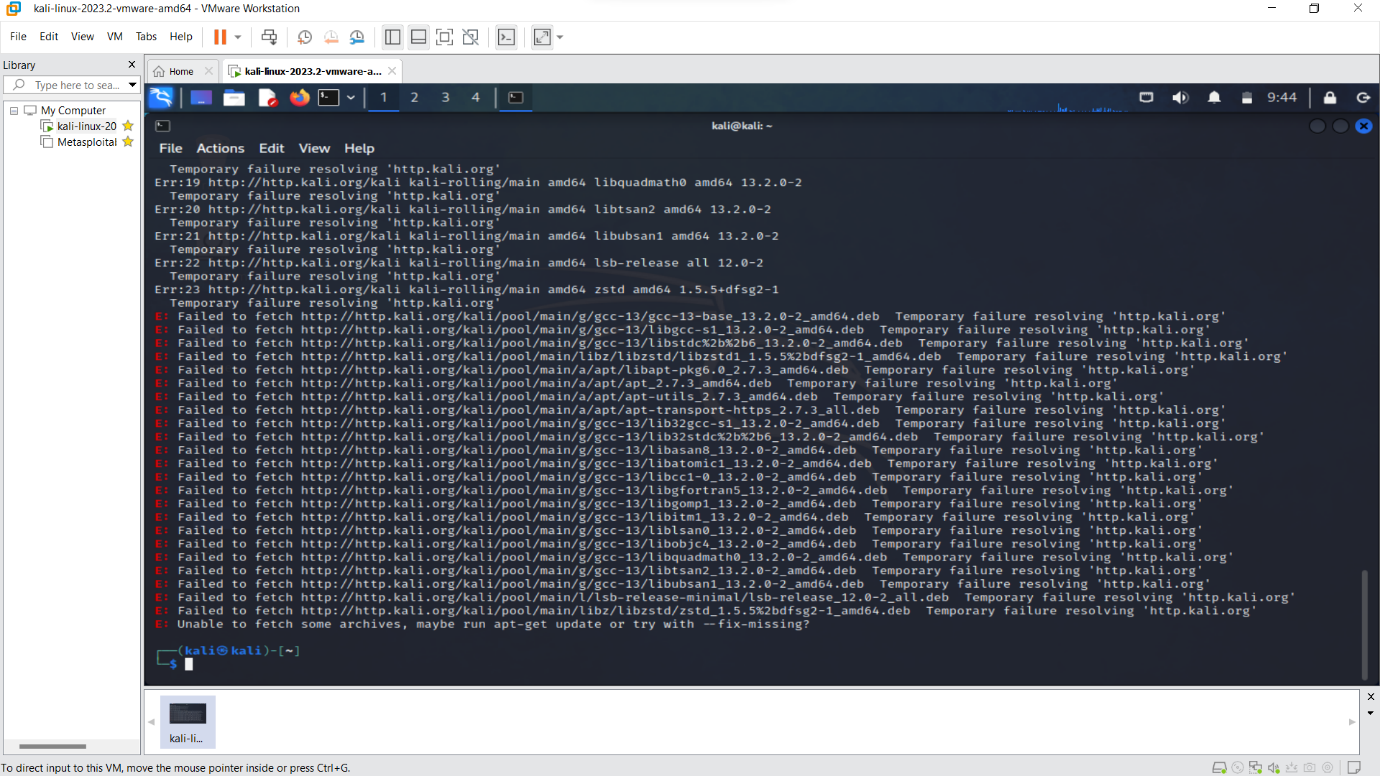
PHP is default installed in kali Linux .

First update the system and add the SURY PHP PPA repository by executing the command lines:

1. sudo apt update
2. sudo apt -y install lsb-release apt-transport-https ca-certificates
3. sudo wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg
4. echo "deb https://packages.sury.org/php/ buster main" | sudo tee /etc/apt/sources.list.d/php.list

After performing 2 command line we get the outputs as show below in pictures.





***Step 5 :*** Configure Apache Server

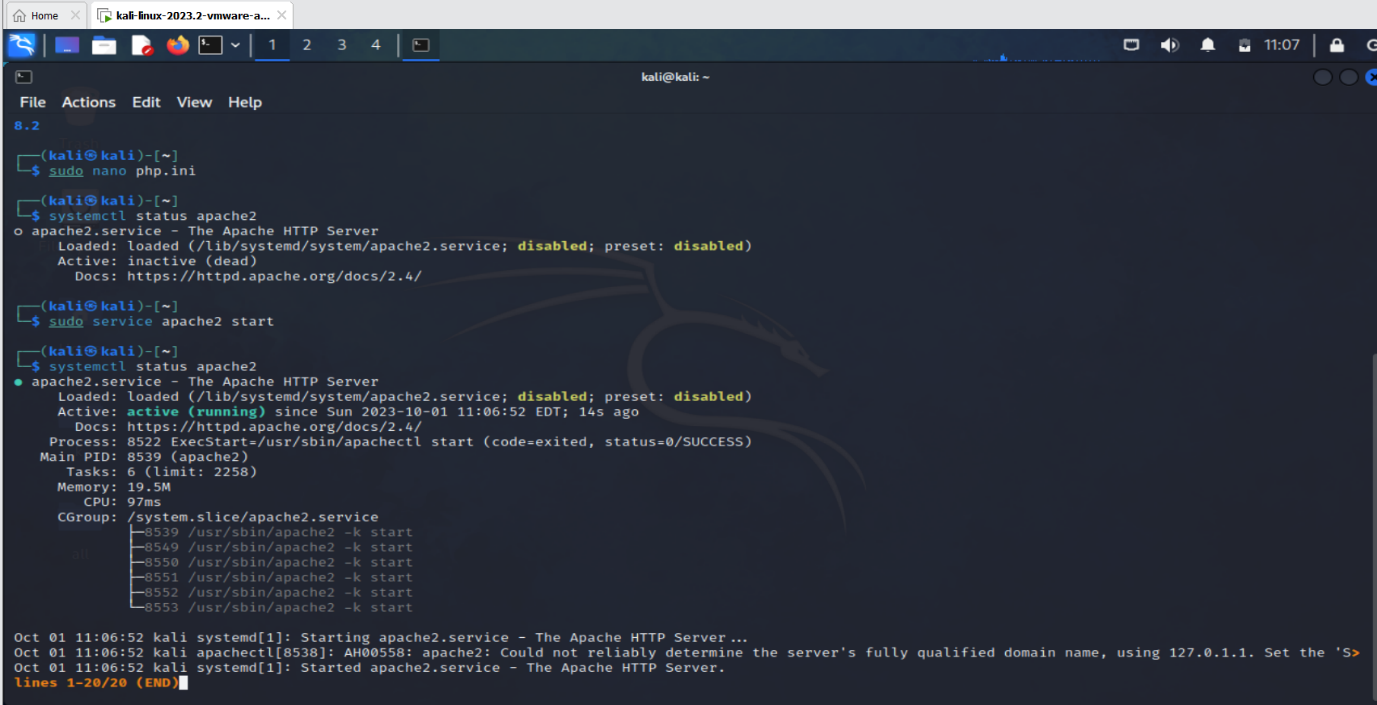
Here we need to configure the server.. Use the command to change location on the terminal to point /etc/php/7.3/apache/2

$ cd /etc/php/7.4/apache2 when we execute this command we will see a file called php.ini. That is file we will edit to configure our localhost server. Using this command $ sudo nano php.ini

Start Apache server using the command $ sudo service apache start

To check whether the service started successfully we use command

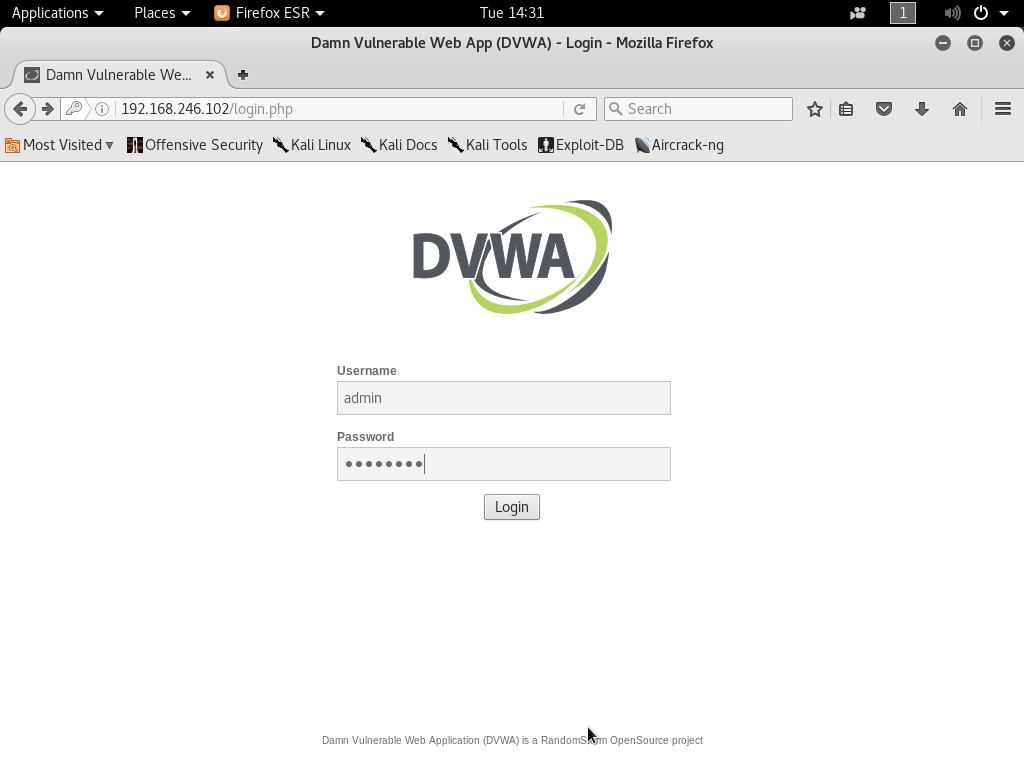
$ systemctl status apache2



***Step 6*** : Access DVWA on Browser

Now we should open and browse the URL <https://127.0.0.1/dvwa/>

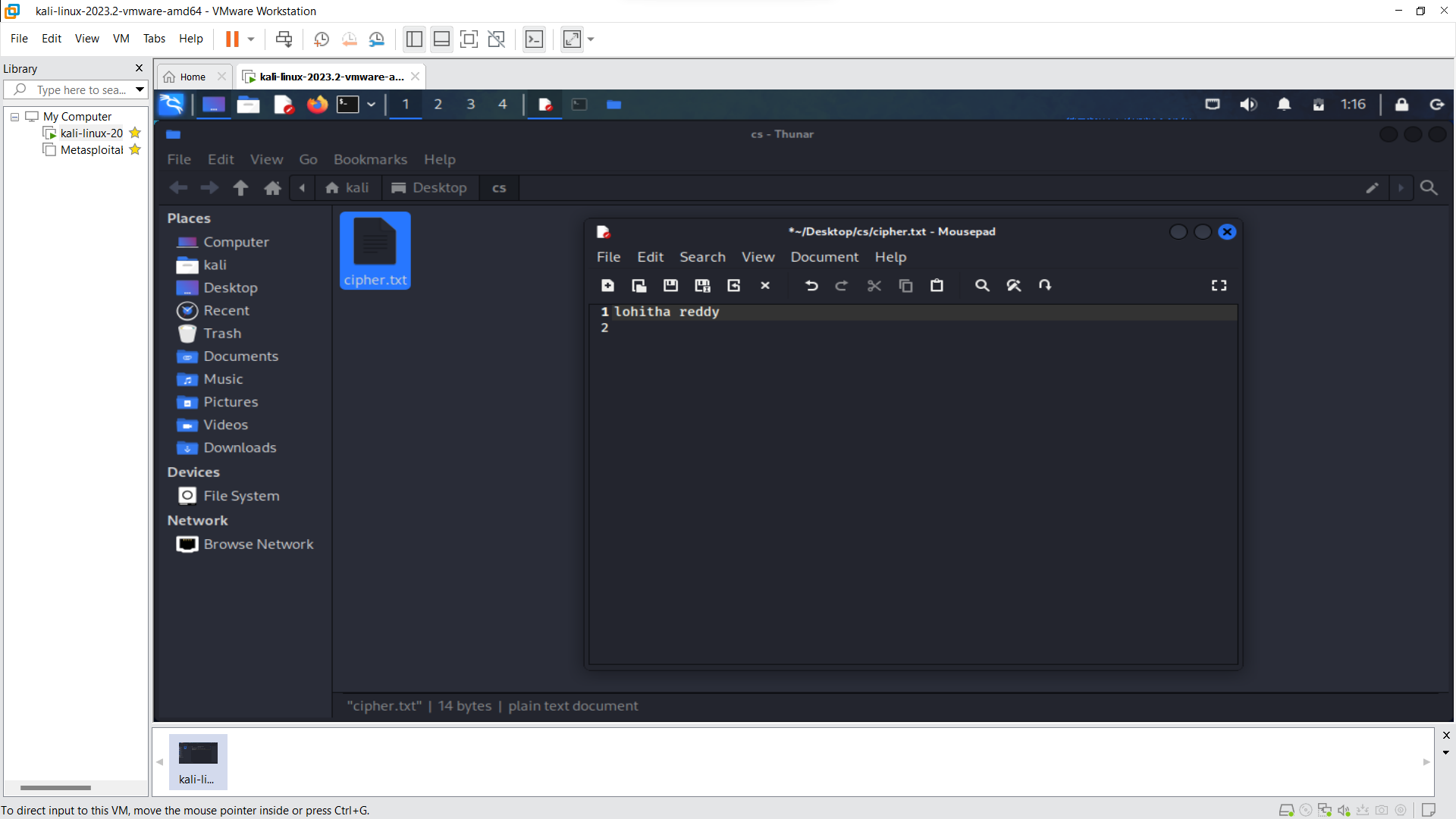




**Generate cipher.txt which includes Encrypted value of your “Name” using the RSA public key & Hide cipher.txt behind Image using Steganography. Also showcase decryption using RSA Private Key.**

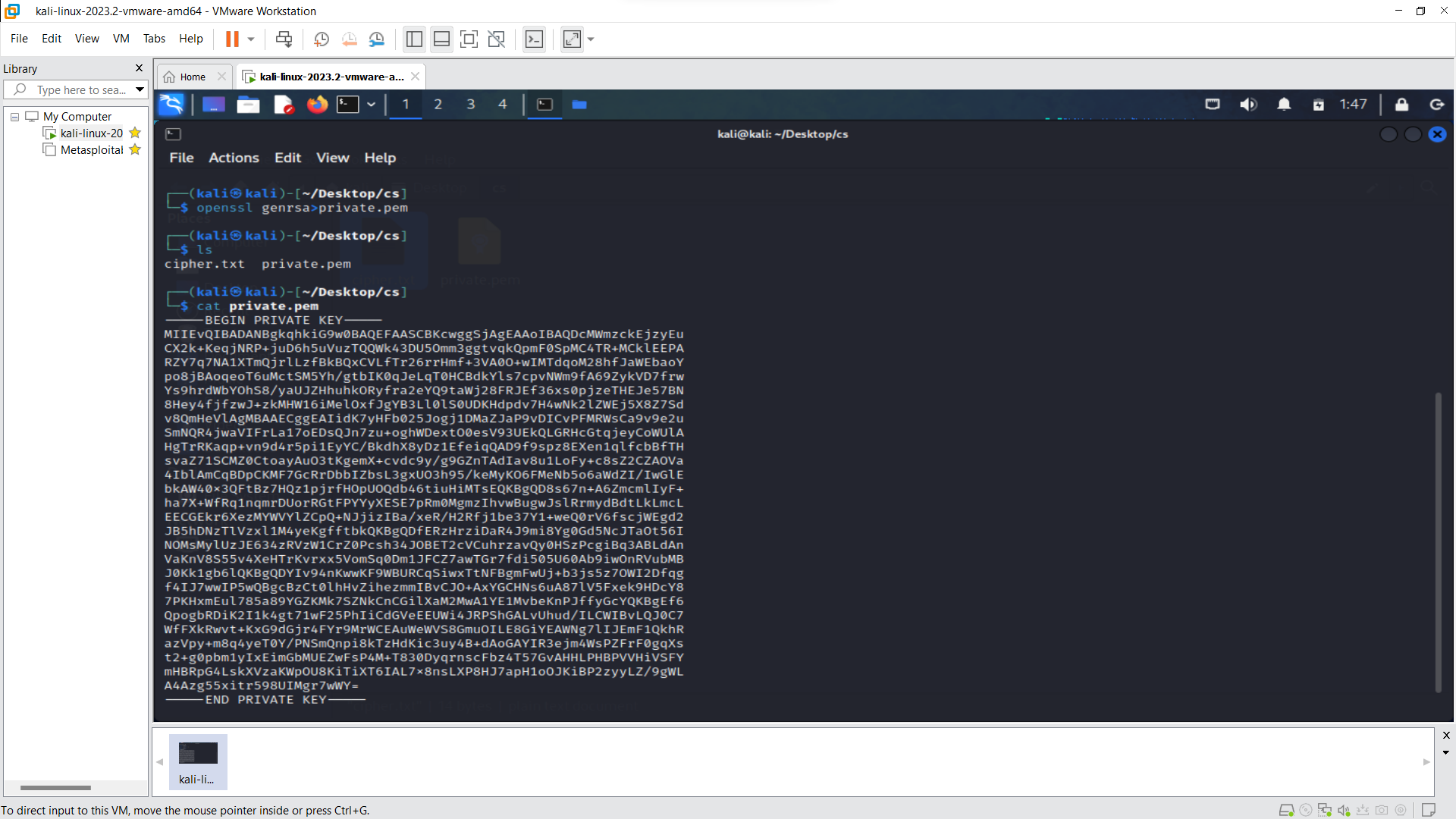
**Step 1 :** Create cipher.txt file

* Firstly I created a text file encrypted my name “Lohitha Reddy” and saved the text file as cipher.txt.
* Here, I used cryptography technique to encrypting data and technique used to secure data.
* Created a folder on desktop as CS.

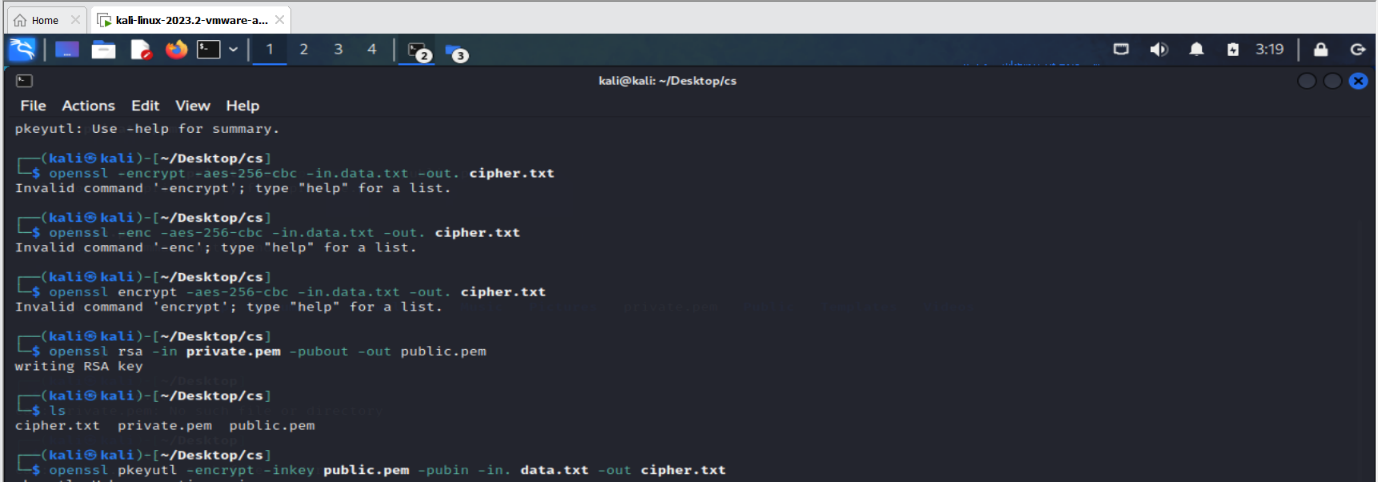


**Step 2**: Encrypting the data using RSA public key .

* Using command line $ openssl genrsa>private.pem(generates rsa private key).
* For encryption we use command $openssl -encrypt -inkey public.pem -pubin -in.data.txt -out cipher.txt
* For decryption we use command line $openssl -decrypt -inkey private.pem -in cipher.txt -out plain.txt







Step 4 : Hide cipher.txt behind Image using Steganography

* First create or save a image from browse and name it and then save it to a folder.
* To hide text we use steganography technique using command line bcopy index.jpeg + data.txt

