**AI with Cyber Security**

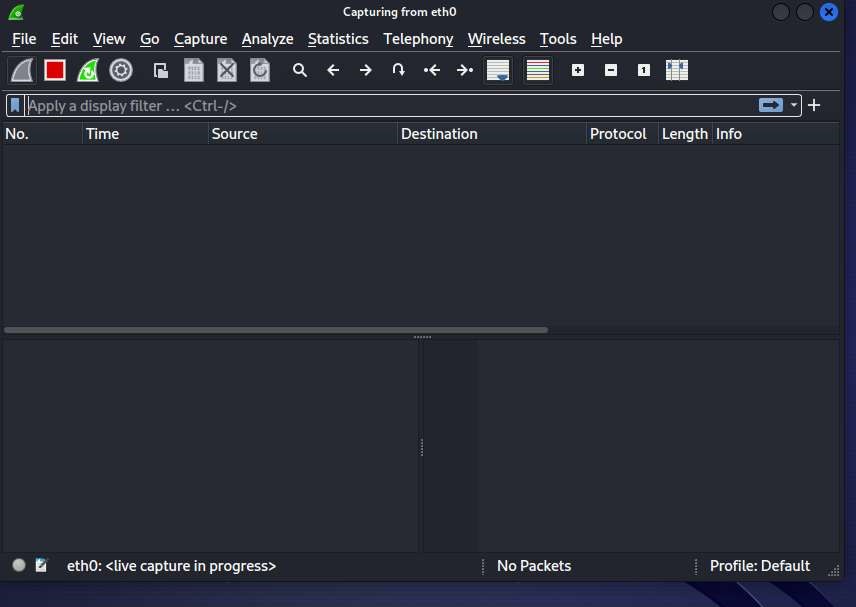
**ASSIGNMENT-2**

**Farzeen Niaz 21BCB0214 VIT VELLORE**

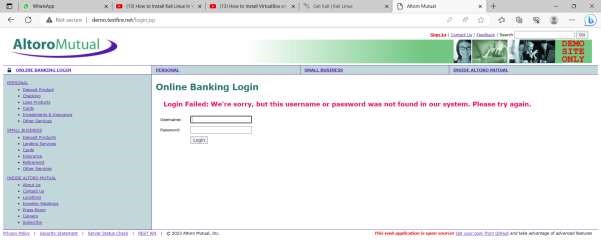
# TASK1

Attack on an insecure website’s images and passwords:

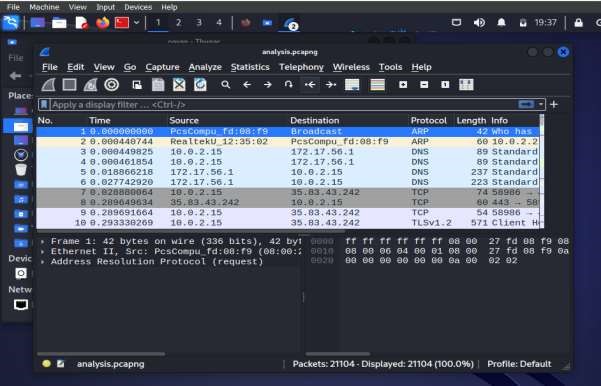
Step-1:



Step-2



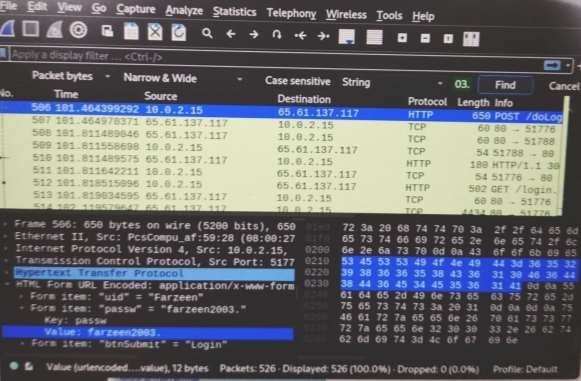
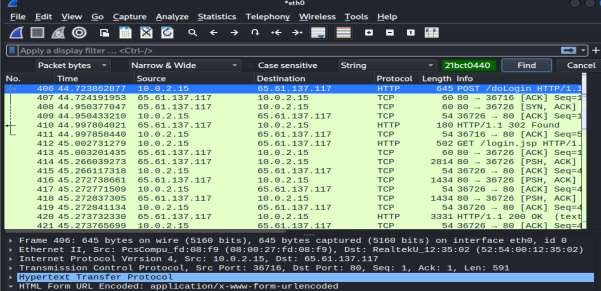
Step-3



Question 1:what is the default extension used by wireshark to save captured packets?

The default extension used by Wireshark to save captured packets is ".pcap"

Step-4



Question 2:

Does that mean that the information you share with a website that uses HTTP is vulnerable?

Yes, sharing information with a website that uses HTTP is considered vulnerable because HTTP transmits data in plaintext, which means it can be intercepted and read by anyone sniffing the network traffic.

Question 3: The credentials goes in which form?(plaintext/ciphertext)

The credentials go in plaintext form. In the captured packet, the password can be seen in plaintext, indicating that it is not encrypted or transformed into ciphertext.

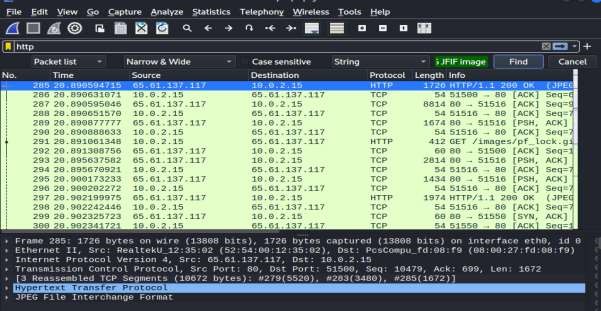
Question 4:What is the use of HTTP GET and HTTP POST methods? Which of these is used to send the username and password to the web server?

HTTP protocol for submitting data to a web server.

HTTP GET: This method is used to request data from a specified resource. It sends data in the URL query string, and the data is visible in the URL. It is not suitable for sending sensitive information like usernames and passwords.

HTTP POST: This method is used to submit data to be processed by the server. It sends data in the body of the HTTP request, which is not visible in the URL. It is the preferred method for sending sensitive information like usernames and passwords.

Step-5:



Step-6



Which are the protocols appearing in the wireshark packets captured?

-Which packets(protocol) are you going to filter? http

-Are you able to save the images from the packets captured?

yes

-Can you find the login credentials from the captured packets?

yes

Read the following para and justify if it is TRUE or FALSE."If somebody was listening in on the network, they could pull the images and the type of information you are viewing on the internet if they were using a packet sniffing program likeWireshark. Hence we must always use secure websites that use encrypted communication."

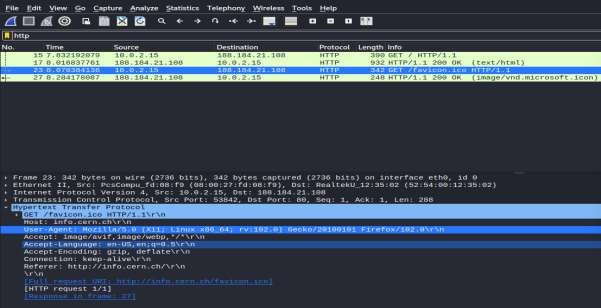
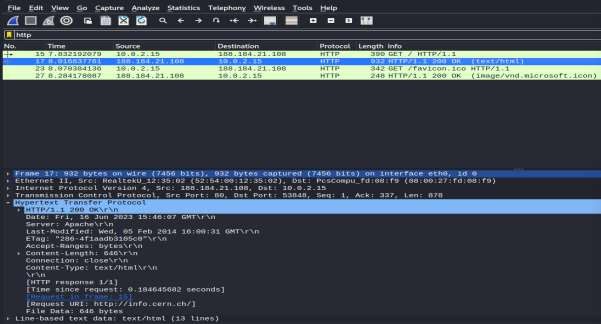
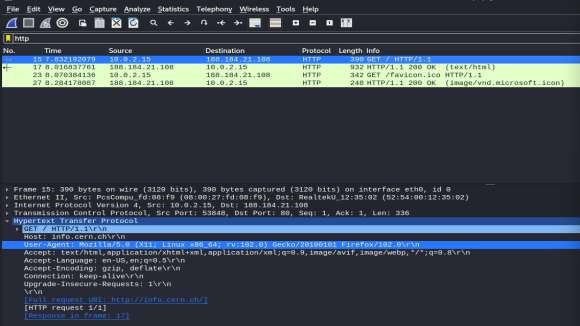
TRUE

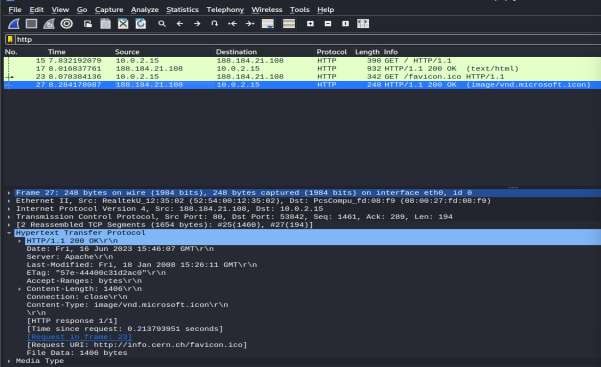
Packet sniffing programs like Wireshark can capture images and information transmitted over the network, allowing eavesdroppers to access sensitive data. Using secure websites with encrypted communication, such as HTTPS, helps protect against this by encrypting the data, making it difficult for attackers to intercept and decipher.

TASK-2

1:

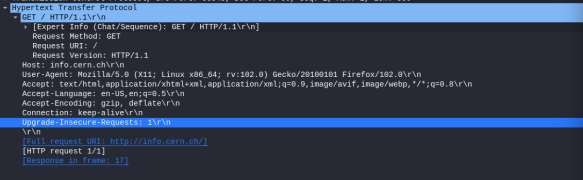
**– Wireshark – Analysing HTTP GET and HTTP reply messages**





2.

GET



RESPONSE



3.

Source and destination IP addresses are given below



GET: Destination- RealtekU

Source-Pcscompu\_\_fd

RESPONSE: Destination- RealtekU

Source-Pcscompu\_\_fd

1. What is your http browser version?

HTTP/1.1

1. What is the accepted language of yourbrowser?

En-US,en;q=0.5\r\n (English US)

1. What is the status code and phrase returned from the server to your browser?

Status Code: 200

Phrase: 0K

1. When was the HTML-file, that you have retrieved, last modified at the server?

Last Modified: Wed, 05 Feb 2014 16:00:31

1. How many bytes of content (size of file) are returned to your browser?



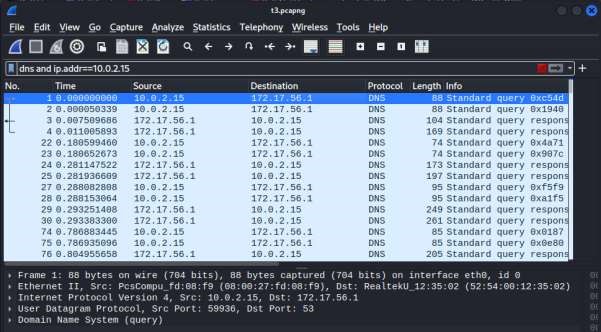
646



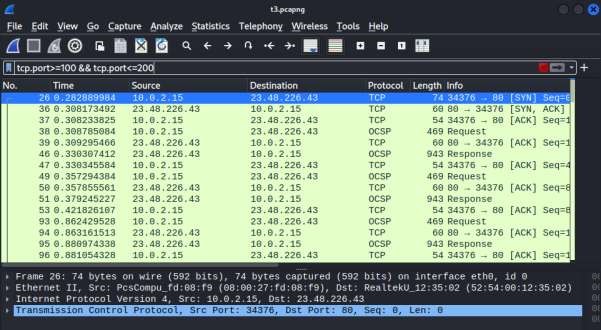
1406

TASK-3

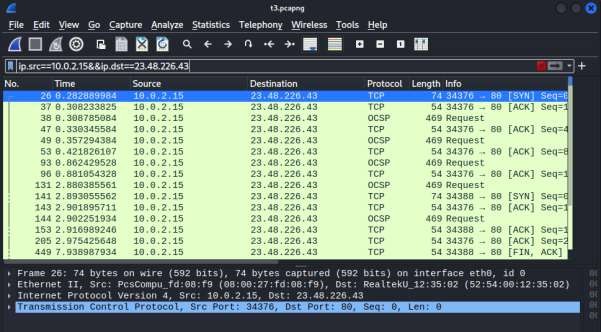
* 1. Dns and ip.addr==10.0.2.15



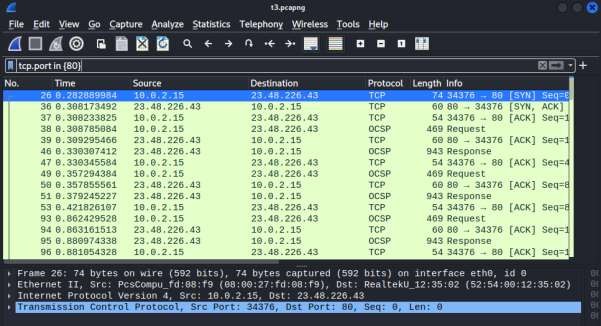
* 1. tcp.port>=100 && tcp.port<=200



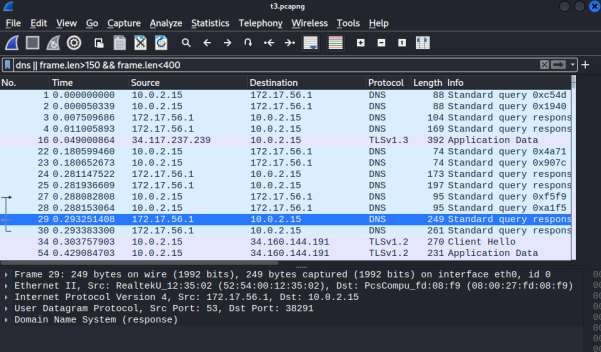
* 1. Ip.src==10.0.2.15 && ip.dst==23.48.226.43



* 1. tcp.port in {80}



* 1. dns || frame.len>150 && frame.len<400



**TASK-4**

**Phishing attack using ngrok**

1. Out of the various phishing techniques, which type of phishing is done in this exercise?

"Credential Harvesting Phishing." It involves creating a fraudulent web page that mimics a legitimate login page, such as Google, to trick users into entering their credentials.

1. How do you think this task can be misused by a hacker?

To deceive unsuspecting users into providing their sensitive and confidential information, such as usernames and passwords. The attacker can then use these stolen credentials for unauthorized access to the users' accounts, identity theft, financial fraud, or other malicious purposes.

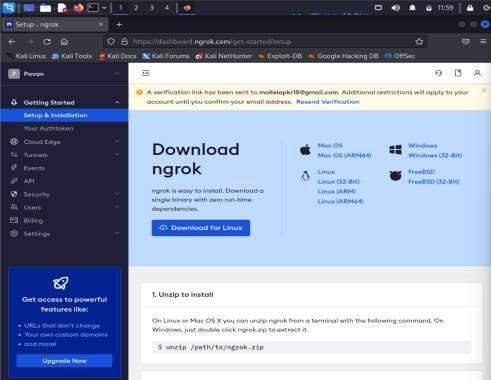
1. Give other possible usages of ngrok.

Local network tunneling: Ngrok can be used to expose a local web server running on your machine to the internet, allowing remote access to your local development environment for testing and collaboration.

Webhook testing: Ngrok can be used to test and debug webhooks by providing a public URL that forwards incoming webhook requests to your local server.

Demo and sharing: Ngrok can be used to quickly share a web application or website with others by providing them with a temporary public URL to access your local server.

Ngrok login



Ngrok download



Connecting account to Ngrok



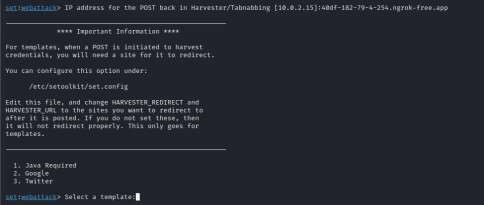
Running Ngrok



Selecting webattack

1) Social-Engineering A\acks -> 2) Website A\ack Vectors-> 3) CredenNal Harvester A\ack Method-> 1) Web Templates







## Task 1: John the Ripper password cracker

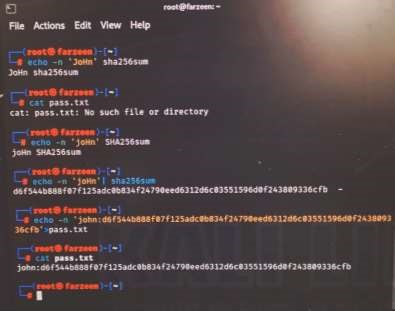
John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems. It is preinstalled in Kali Linux. John the Ripper (JtR) is a popular passwordcracking tool. John supports many encryption technologies for Windows and Unix systems (Mac included). John is also a dictionary-based tool. This means that it works with a dictionary of common passwords to compare it with the hash in hand. While you can use popular wordlists like RockYou (a dictionary of common passwords), John also has its own set of wordlists with thousands of common passwords. This makes John very effective when cracking systems with weak passwords.

**A. Single Crack Mode**

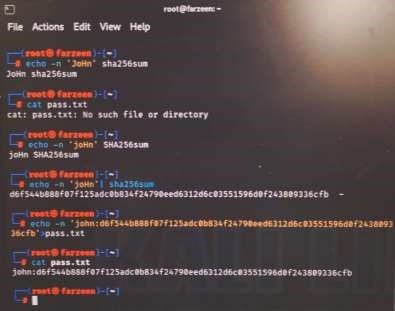
Open the Root Terminal Emulator in Kali linux, and do the following: 1. Add a new user with username as john, and variations on its capitalization as the password. Here, I have kept the password as JoHn. You should set some other password this way.



2. Find the SHA-256-hashed password(of the password that you have set for the above user) using the following command:



Save the username and the password hash value from prior steps into a file pass.txt:



4.Run pass.txt through John the Ripper’s Single Crack Mode (Note: we can change the --format argument according to the hash used!!!):

john --single --format=raw-sha256 pass.txt

5. Has the ripper successfully cracked your password?

**B. Wordlist mode**

1. Locate the file rockyou.txt.gz and extract it.

In general, this file can be found using:

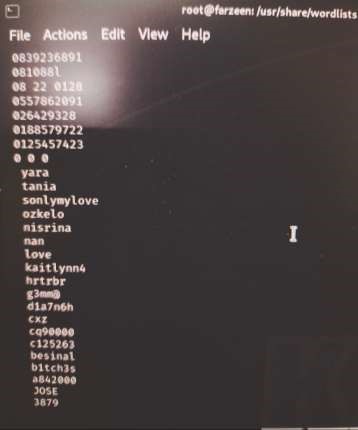
2.Now navigate to the directory containing rockyou.txt.gz, and extract it:

The file has been successfully extracted. Copy the file rockyou.txt onto the current directory using 'cp' command, and view its content using

'cat'.

This will return a list of all the words found in the rockyou.txt file (approx 14,341,564 passwords).

1. Choose any 3 passwords from the rockyou.txt file, and compute the sha256 hashes of each of them
2. Save three usernames(your name followed by a number) and each of these hashes in the file pass.txt. 5. Run John in wordlist mode



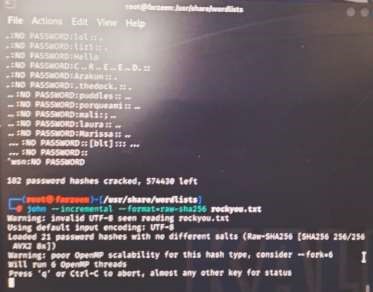
**B Incremental Mode**

1. Choose any 6 passwords from the following(to keet it simple and uniform), and compute the sha256 hashes of each of them. password, passw0rd, admin01, admin05, admin04, admin03, admin02, password1, password2, password3, password7, password5
2. Save 6 usernames(should be your name followed by a serial number 01-06) and each of these hashes in the file pass.txt.





1. Run John in incremental mode



1. How many passwords were you able to crack?

182 passwords were able to crack .

Use the filename as pass.txt here. Answer the following questions:

Q1.Can John the Ripper crack all the passwords? Justify.

No,Never expect to crack 100% of hashes. To crack hashes, John the Ripper iteratively tries to input candidate passwords into the hash function and checks if there is a match

Q2. Try to crack your passwords using sudo john /etc/shadow -format=crypt State the reason if John continues to run infinitely. Also find the number of passwords cracked from the shadow file (using - show flag) and paste the screenshot here.



Q3. What is the default format in which password hash gets stored in Kali linux?

PASSWORD\_BCRYPT is used to create new password hashes using the CRYPT\_BLOWFISH algorithm. This will always result in a hash using the "**$2y$**" crypt format, which is always 60 characters wide.

Q4. What are the types of attacks used by John in different modes? E.g., brute force, dictionary attack, etc.

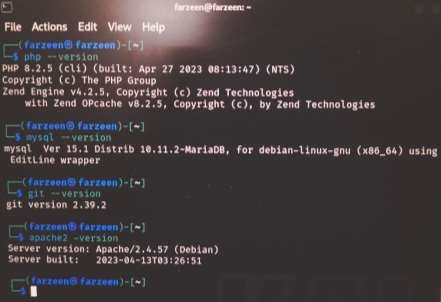
Brute force ,dictionary attack ,rainbow table, single crack mode, wordlist mode, incremental mode.

## Task 2: SQL injection attack

**SQL Injection Attack on DVWA**

DVWA (Damn Vulnerable Web Application) Damn Vulnerable Web Application is a PHP/MYSQL web application that is vulnerable. Its main goals are 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 aid teachers/students to teach/learn web application security in a class room environment.

Step 1:Prerequisites: Open the terminal as root user, and check whether php, mysql, git, and apache2 are installed. You may use the following commands to check the same:



If any of these packages/tools are missing, install them using the apt-get install command. For example, if git is missing:

Step 2: Setup MYSQL server: To setup the password for the MYSQL server, start the server using the command:

Now, change the password(set the password as your name - without the quotes):

After changing the password, connect to the MySQL server to create the database:

Here, type the root password created in the previous step and press Enter. Create a database using the following command:

Create a database user with your name as username and your register number as password.

Grant permission to the user you have created:

Step 3: Download and Configure DVWA:

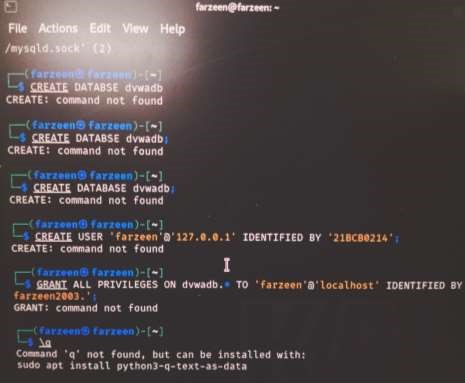
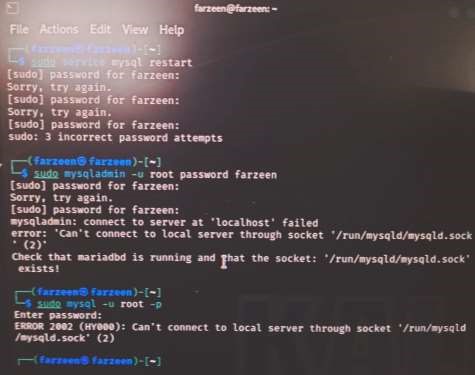
Go to the apache2 folder:

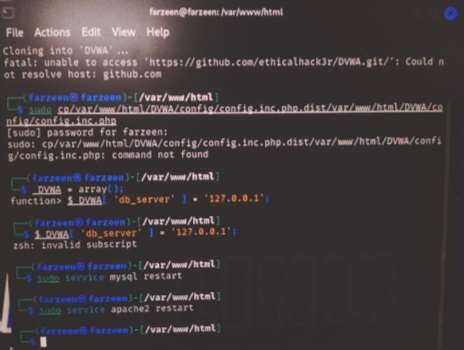
Clone DVWA from GitHub:

Edit the PHP config files to connect the web application to the DB. To change the configuration file name, enter the following command:

Open the config file using vim editor:

In this file, update the following lines according to the BD name, DB username and the password that you have set before:









FARZEEN NIAZ 21BCB0214

### Task 1 Hardening a Linux System

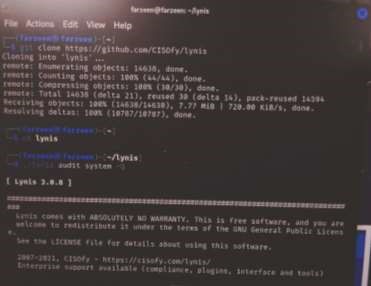
Demonstrate the use of a security auditing tool to harden a Linux system(you may try it in your Kali Linux). Auditing a system for potential misconfigurations or unprotected services is an important aspect of system hardening. Lynis is an open source security auditing tool with an automated set of scripts developed to test a Linux system. The value of this tool is that it is an open script that auditors can give to system administrators to run on their Unix servers in order to assess specific technical security controls on the system

**Step 1:** Install lynis in Linux terminal

**Step 2:** Run the Tool

**Q1. Which version of lynis is installed?**

**A1)** Lynis 3.0.8 is installed





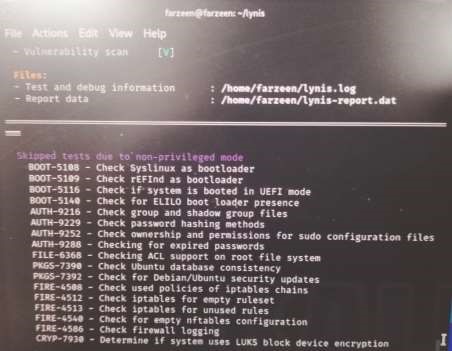
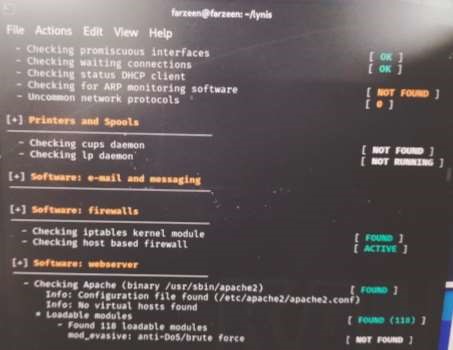
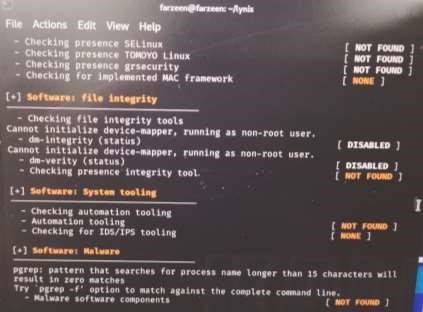
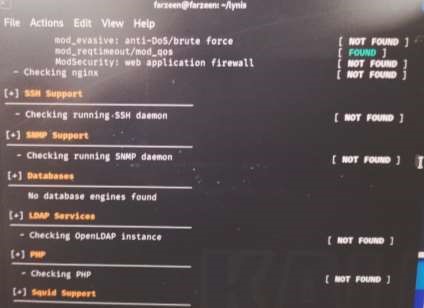
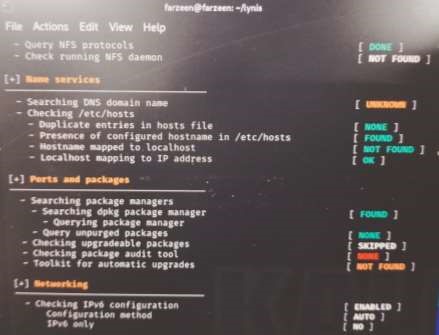
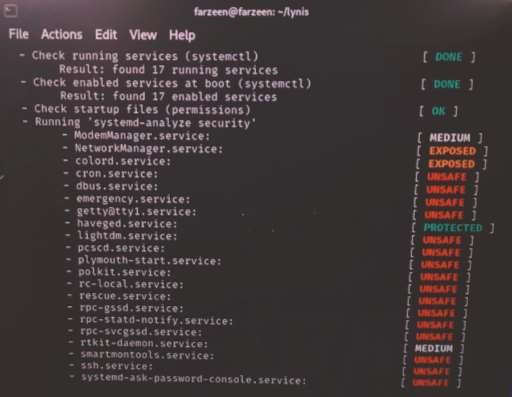
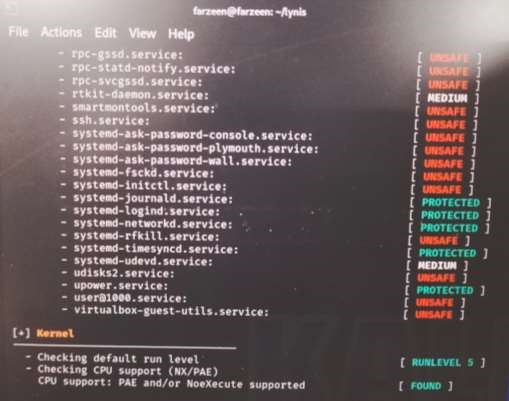
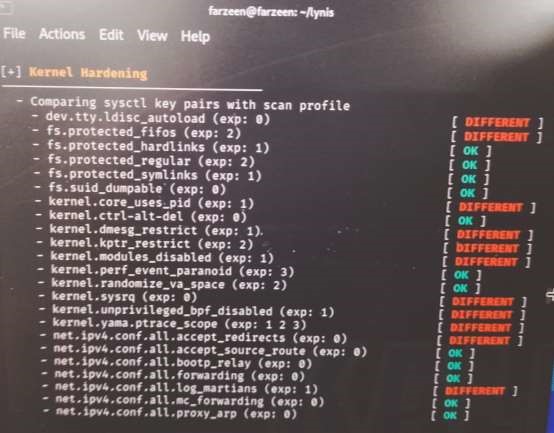
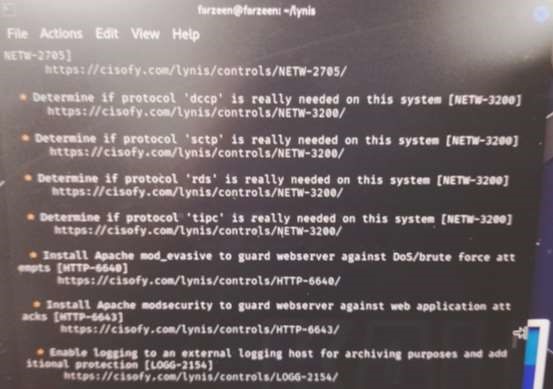
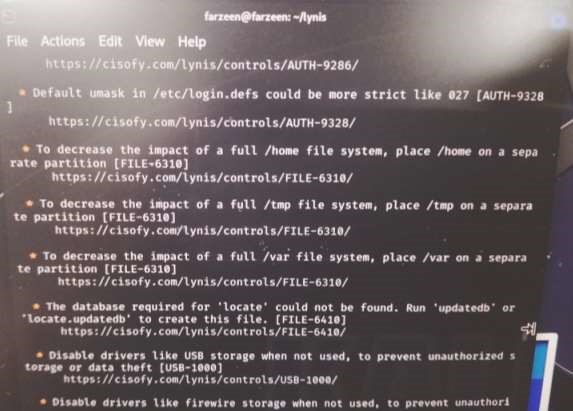
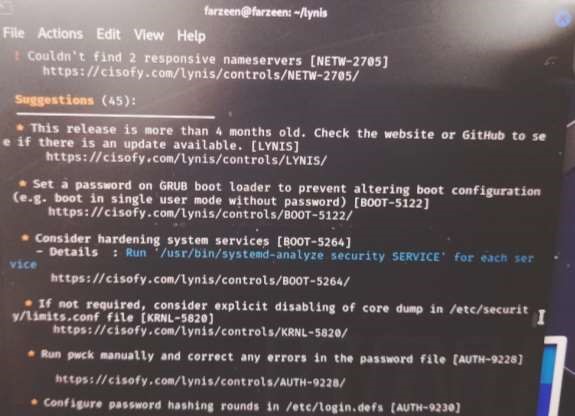
**Step 3:** For each of the following Test Results/Status States, include screenshots giving the services for which lynis gives the result.

**Step 4:** Scroll through the suggestions and select one.

Q2. Also, mention the meaning of each of these Status states/Results

* UNSAFE
* MEDIUM
* EXPOSED
* SUGGESTION
* FOUND
* NOT FOUND
* HARDENED
* PARTIALLY HARDENED
* PROTECTED
* ACTIVE

1. UNSAFE: Indicates that a particular entity, system, or condition poses a risk or danger. It implies that there are vulnerabilities or hazards that need to be addressed or mitigated.
2. MEDIUM: Suggests a moderate level of risk or concern. It implies that there may be some vulnerabilities or potential issues that should be addressed, but they may not pose an immediate threat.
3. EXPOSED: Indicates that sensitive or confidential information, systems, or resources are accessible or visible to unauthorized parties. It implies a security vulnerability that needs attention to prevent unauthorized access or data breaches.
4. SUGGESTION: Refers to a recommendation or advice provided regarding a specific situation or context. It suggests a course of action or solution that may improve a particular condition or achieve a desired outcome.
5. FOUND: Signifies the identification or discovery of a particular item, object, or information. It indicates that something has been located or detected.
6. NOT FOUND: Indicates the absence or inability to locate a particular item, object, or information. It suggests that the searched entity is missing or does not exist.
7. HARDENED: Refers to the strengthening or fortification of a system or security measures. It implies that security controls, protocols, or configurations have been enhanced to protect against potential threats or vulnerabilities.
8. PARTIALLY HARDENED: Suggests that only some aspects or components of a system or security measures have been strengthened or fortified. It implies that there are still areas that need further improvement or protection.
9. PROTECTED: Signifies that appropriate security measures or controls are in place to safeguard a particular entity, system, or resource. It implies that necessary precautions have been taken to prevent unauthorized access or potential harm.
10. ACTIVE: Indicates that a particular entity, system, or process is operational, functioning, or engaged in a specific activity. It implies that it is currently in use or in an active state.



**Q3. How many suggestions are given by lynis?**

20

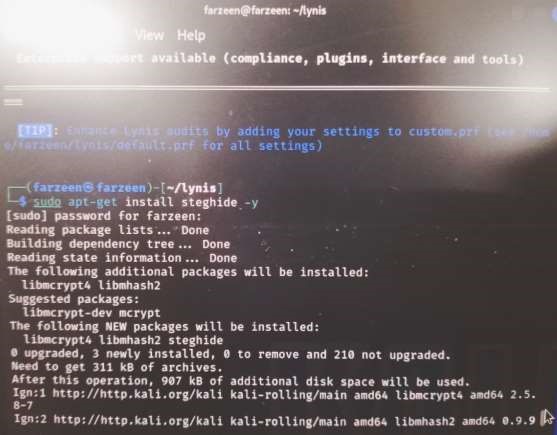
**Q4. Find any three suggestion and give your solution?**

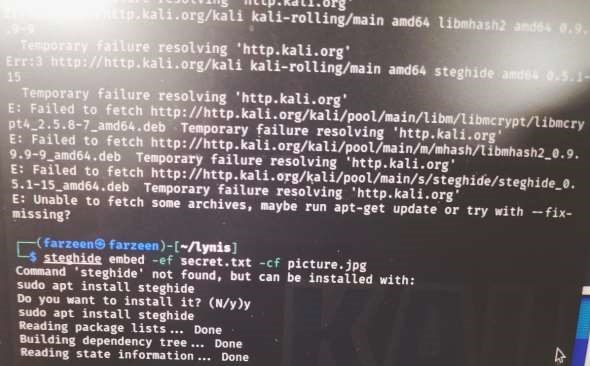
To change password

### Task 2 Steghide tool

Steghide is a steganography program that is able to hide data in various kinds of image- and audio-files. Take screenshots of the steps mentioned(including the commands and their outputs too). Also explain the flags used in each command (use steghide --help).

1.Install steghide tool in linux.





1. Choose a cover image “picture.jpg” and a large message in a file “secret.txt”.

(Keep a copy of these two files as backup for further steps)

1. Embed the secret message secret.txt inside the image picture.jpg, using a passcode.
2. Display the image file with the embedded text file. Is there any noticeable distortion in the new image?
3. Get information about the embedded file before extracting it(use the info command). Also, try to get information about the embedded data.
4. Now, retrieve the hidden message from the image file using the passcode. Could you open the file? Is the secret message the same as before?

### Task 3 Authentication and Authorization

**Part 1:** Adding Groups, Users, and Passwords on a Linux System

**Step 1:** Open a terminal window in Ubuntu. Escalate privileges to the root level by entering the sudo su command. Enter the password when prompted.

**Step 2:** Create a new group named ISAA by entering the command groupadd ISAA

**Part 2:** Verify Users, Groups, and Passwords

**Step 1:** Verify the new group has been added to the group file list by entering cat /etc/group

The new group ISAA will be added to the bottom of the /etc/group file with a group ID. What is the group ID of ISAA in your list?

**Step 2:** Add a new user with the first letter of your first name followed by the second name. e.g., for bill gates, the new username should be bgates, all in small letters.

**Step 3:** Place the new user in the ISAA group.

**Step 4:** Add another new user named with the first letter of your second name followed by the first name. e.g., for bill gates, the new username should be gbill, all in small letters.

**Step 5:** Verify the newly created users in the passwd file and the shadow file .

What can you find in the passwd file and the shadow file? What is the difference between these two files?

**Part 3:** Using Symbolic Permissions

**Step 1:** At the prompt, enter su –l and enter the password.

**Step 2:** View your present directory: pwd

**Step 3:** Go back one directory level to the /home directory using cd ..

**Step 4:** List all directories and their permissions using

**Step 5:** Enter the second user’s folder by using the cd command

Are you able to enter the second user's home directory from the first user?

**Step 6:** Open a terminal as root, and cd to the /home directory.

**Step 7:** Change the permission on second user’s folder by using each of the following commands.

After running each of these commands,

i) check if you can enter the second user's account using cd ii) List the directories with their respective permissions.

How is the output different from the result obtained in Step 4?

What is done by each of these commands?

Write the chmod commands to enable and disable [read and write] permission to group.

**Part 4:** Absolute Permissions The other way of assigning permissions besides using symbolic permissions is the use of absolute permissions. Absolute permissions use a three digit octal number to represent the permissions for owner, group and other.

**Step 1:** In a terminal, login as the second user

**Step 2:** Modify the “others” field for the second user’s folder so that others will be able to read and execute but not write while still maintaining the “user” field to read, write, and execute. (use chmod)

**Step 3:** cd to the second user’s directory

Are you able to enter the second user’s folder and read the files within the directory?

Are you able to see the test.txt file?

**Step 4:** Attempt to create a file.

Are you able to create a file? Why?

What is the minimum permission needed for the first user to create a file in the second user's directory?

