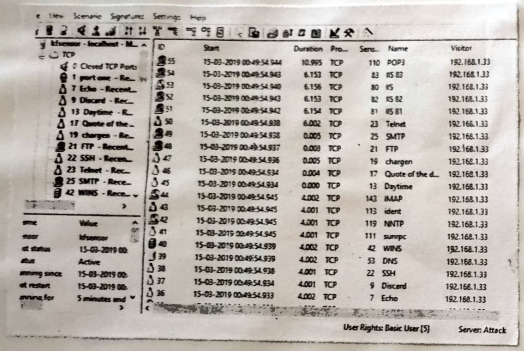
Output:



Ex. No. 1 | Date | Page No.

Setup a honeypot and monitor the honeypot on network.

• Honey Pot:

Honeypot impersonates a real servers to deceive hackers and deflect their attacks. The intruder believes they have obtained exposure to the actual piece because the honeypot gives the appearance of being authentic.

The masked system is in the DMZ. that mean the intruder does not have access to the internal infrastructure honeypot periodically monitor and manage the intruders whether and manage the attack comes from outside. The infrastructure or inside it honeypot widely.

• kF Sensor:

kF sensor is a windows honeypot. It is to identify all networks hackers.

Attacker VM → kalilinux

Victim VM → Window 10.

Severity:

Red → More dangerous (High)

Yellow → Average (Medium)

Grey → Low

Ex. No.	Date	Page No.

Ports:

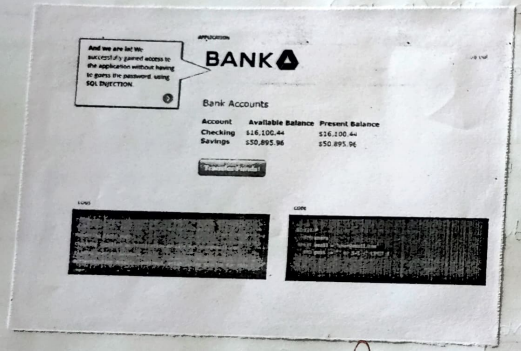
Services Ports.

- FTP (20,21)
- SSH (22)
- Telnet (23)
- SMTP (25)
- DNS (53)
- NetBIOS over TCP (137,139)
- SMB (445)
- HTTP and HTTPS (80,443,8080,8443)
- Ports (1433, 1434 and 3306)
- Remote desktop (3389)
- Services Ports
- DHCP (67)

The dynamic host Configuration Protocol

- CMD (4444)
- MySQL (3306)
- NBT Name Service (137)
- NBT Datagram Service (138)
- NBT Session Service (139)
- NBT SMB (445)
- POP 3 (110)
- Socks (1080)
- NNTP (119)
- MS RPC (135)

Output:



Ex. No. 2	Date	Page No.

Write a script or code to demonstrate SQL injection attacks.

SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via webpage input.

Requirements

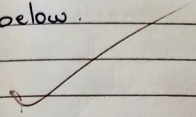
1. APC

Procedure:

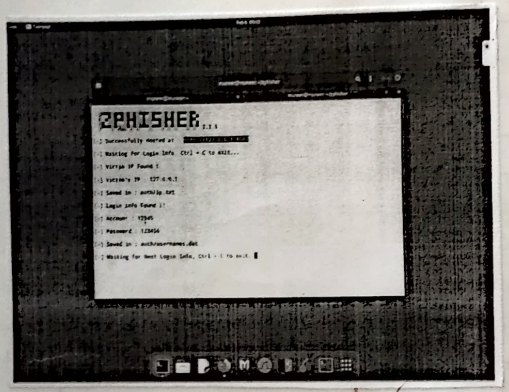
1. Go to "Hacks Planning" website.
2. Click on SQL Injection.
3. You will see a bank login page.
4. You can also see the application log window which show all the details entered in web page.
5. Try entering USERNAME as username@gmail.com and password as password.
6. Since the password is incorrect you can see that log window shows that there is an SQL Syntax error.
7. Below image shows a new section called Code which shows that the user name and password you enter directly goes into the SQL query.

Ex. No.	Date	Page No.

8. This behaviour shows that application might be vulnerable to SQL injection.
9. Now try entering username and password as below.



Output:



Ex. No. 3	Date	Page No.

Create a social networking website login page using phishing techniques.

The practise of sending fraudulent communications that appear to come from a reputable source. Usually done through email. An art of psychological to deceive people into reveling sensitive information

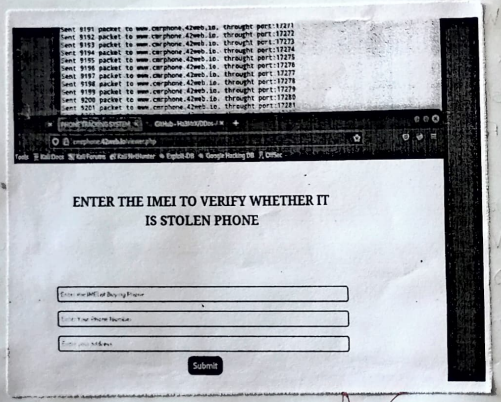
Requirements:

1. V.M. Ware
2. Linux
3. Zphisher
4. cloud Fare

Procedure:

1. Open VMWare and Create kali linux and setup it
2. Open root terminal and clone github zphisher respositories.
3. Open zphisher tool and install all requirements
4. Follow the Process.
   git clone: https://github.com/htr-tech/zphisher
5. cd zphisher
6. bash zphisher.sh
7. Selection of desired page from displayed pages.
8. Selection the hosting tunnel such a ngrock, cloudfoare and etc.
9. Link will be displayed and forward it to a victim.

Output:



Ex. No. 4	Date	Page No.

Write a code to demonstrate Dos attacks.

The practise of sending fraudulent communications that appear to come from a reputable source. Usually done through email. An art of psychological manipulation to deceive people into reveling sensitive information.

Requirements:
1. VM Ware / Virtual Box
2. Linux
3. https://github.com/Ha3Mrx/DDOS-Attack.

Procedure:
1. Install VMWare / Virtual Box and open it.
2. Install kali linux in the VM Ware / Virtual Box and log in.
3. Open terminal and type this command.
4. git clone https://github.com/Ha3Mrx/DDOS-Attack
5. cd DDOS-Attack
6. Python2 ddos-attack.py
7. Seled website for target
8. Example: www.cmrphone42web.io
9. Select the ports number for traffic
10. Example: 8080
11. ctrl+c for stop the attack

Aim: Demonstrate Web-based Password Capturing technique using Wireshark.

Requirements:

Wireshark

Procedure:

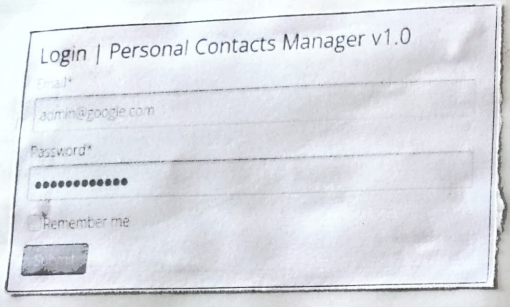
step 1: Download Wireshark from this link
http://www.wireshark.org/download.html

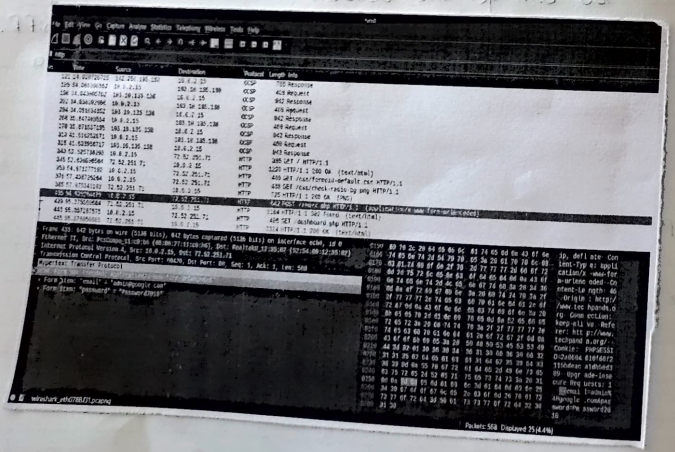
step 2: Open Wireshark
You will get the screen
Select the network interface you want to sniff.
Note for this demonstration, we are using a wireless network connection. If you are on a local area network interface.

step 3: click on start button.

step 4: Open your web browser and type in

http://www.techpanda.org/





Ex. No.	Date	Page No.

step 5: The login email as admin@google.com and Password is Password2010

step 6: Click on submit button.

step 7: A successful logon should give you the dashboard.

step 8: Go back to Wireshark and stop the Live Capture.

step 9: Filter for HTTP protocol results only using the filter text box.

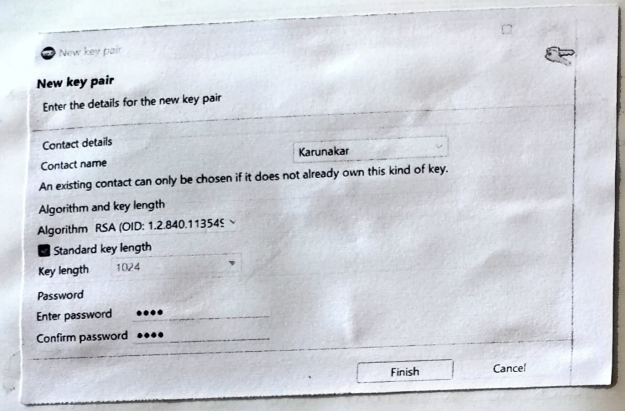
step 10: Locate the info column and look for entries with the HTTP verb Post and Click on it.

- Just below the log entries, there is a Panel with a summary of Captured data. Look for summary that says

Line-based text data: application/x-www-form-urlencoded

Ex. No.	Date	Page No.

- You should be able to view the Plaintext values of all the Post variables submitted to Servers via HTTP Protocol.



Ex. No. 06	Date	Page No.

Install jcryptool (or any other Equivalent) and demonstrate Asymmetric Crypto algorithm, Hash and Digital/PKI signatures studied in theory Cryptography & Network Security.

Aim: Jcryptool and Demonstrate of Asymetric key Crypto Algorithm, Hash and Digital Signature/PKI

Requirements:

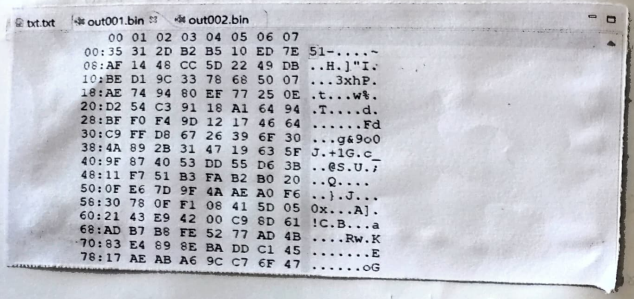
Jcryptool

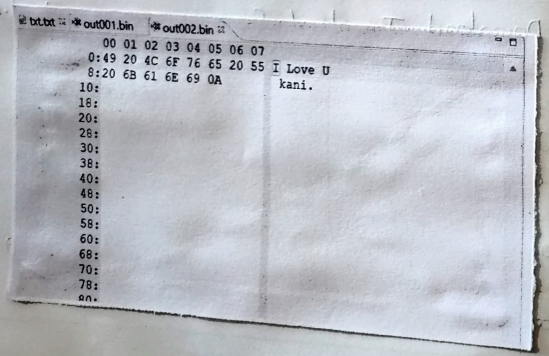
Procedure:

step 1: Download Jcryptool from www.cryptool.org and extract it.

step 2: Open a new text and save it after writing a message on it.

step 3: Now open the Algorithms option from the upper left corner and select the RSA algorithm from Assymmetric algorithms.





Ex. No.	Date	Page No.

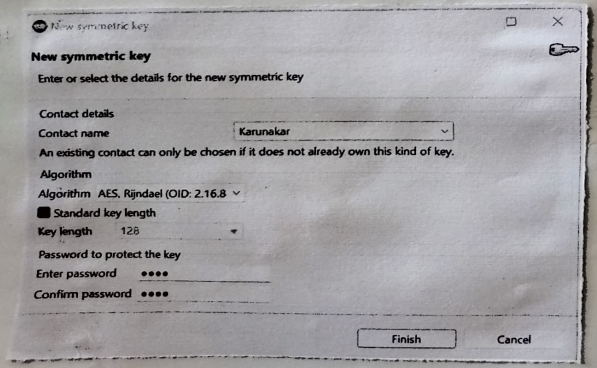
Step 4: Now Create a New key pair using the users name as contact name and user password.

Step 5: Encrypt the Plain text/message using the new key pair.

Step 6: To decrypt the encrypted message again open the RSA algorithm and select the decrypt option.

Step 7: User must choose the same key pair and give the user password when asked.

Step 8: For hashing of a message just select the Prefered hashing algorithm which requires no further input.



Ex. No. 07 | Date | Page No.

Install Jcryptool and demonstrate Symmetric crypto algorithm, Hash and Digital/PKI signatures studied in the theory Cryptography & Network Security

Aim: Jcryptool and Demonstration of Symmetric key Crypto Algorithm and Digital signature/PKI

Requirements:

Jcryptool

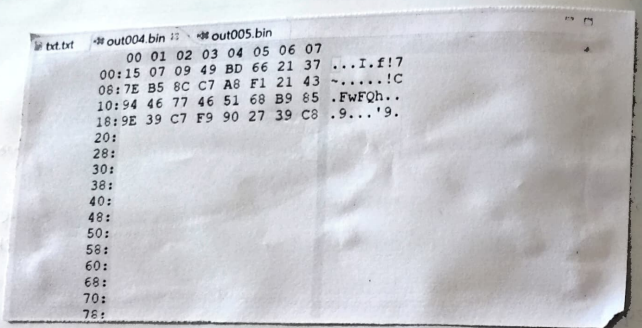
Procedure:

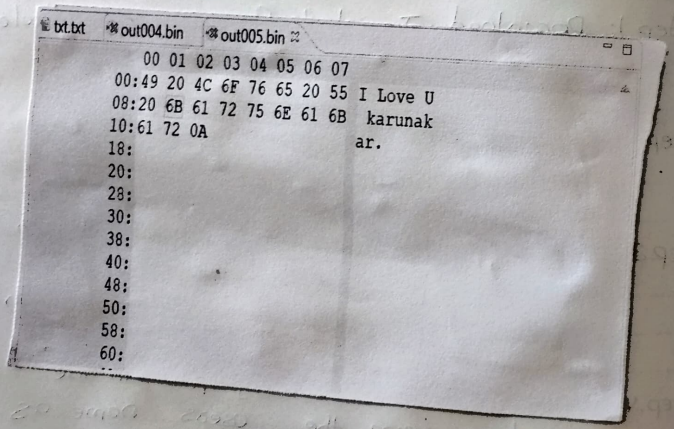
step 1: Download Jcryptool from www.cryptool.org and extract it.

step 2: Open a new text and save it after writing a message on it.

step 3: Now open the Algorithms option from the upper left corner and select the AES algorithm from Symmetric algorithm.

step 4: Now Create a New key pair in the key store using the users name as Contact name and user password





Ex. No.	Date	Page No.

step 5: Encrypt the plain text/message using the new key pair and the Password.

step 6: To decrypt the encrypted message again open the AES algorithm and Select the decrypt option.

step 7: Users must choose the same key Pair and give the user password when asked.

step 8: For Signaturing a file select DSA from Digital Signature and Create a new key pair also store it.

step 9: Now the file is digital signed and to verify it Select the DSA again from digital signature and Select the stored key and give the Password.

step 10: And it show a message that it is valid.