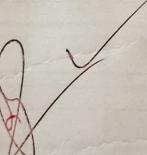


## Output:



Scenarios	Signatures	Settings	Logs
<b>Monitored - Localhost - M</b>			
1 port scan - Rec.	55	15-03-2019 00:49:54.944	10.993 TCP 110 POP3 192.168.1.33
1 port scan - Rec.	54	15-03-2019 00:49:54.943	6.153 TCP 82 85 83 192.168.1.33
7 Echo - Rec.	53	15-03-2019 00:49:54.943	6.158 TCP 80 15 192.168.1.33
9 Discard - Rec.	52	15-03-2019 00:49:54.943	6.153 TCP 82 85 92 192.168.1.33
13 Daytime - Rec.	51	15-03-2019 00:49:54.942	6.005 TCP 81 15 88 192.168.1.33
17 HTTP - Rec.	50	15-03-2019 00:49:54.939	6.005 TCP 22 Telnet 192.168.1.33
19 chargen - Rec.	49	15-03-2019 00:49:54.938	0.005 TCP 25 SMTP 192.168.1.33
21 FTP - Rec.	48	15-03-2019 00:49:54.937	0.005 TCP 21 FTP 192.168.1.33
22 SSH - Rec.	47	15-03-2019 00:49:54.936	0.005 TCP 19 chargen 192.168.1.33
23 Telnet - Rec.	46	15-03-2019 00:49:54.934	0.004 TCP 17 Quote of the d... 192.168.1.33
25 SMTP - Rec.	45	15-03-2019 00:49:54.934	0.000 TCP 13 Daytime 192.168.1.33
26 WHOIS - Rec.	44	15-03-2019 00:49:54.934	4.002 TCP 143 IMAP 192.168.1.33
41 Value	43	15-03-2019 00:49:54.934	4.002 TCP 113 ident 192.168.1.33
42 Identifier	42	15-03-2019 00:49:54.934	4.001 TCP 119 NNTP 192.168.1.33
43 User	41	15-03-2019 00:49:54.934	4.001 TCP 111 Kerberos 192.168.1.33
44 Action	40	15-03-2019 00:49:54.939	4.002 TCP 42 WHOIS 192.168.1.33
45 among since	39	15-03-2019 00:49:54.939	4.002 TCP 53 DNS 192.168.1.33
46 at restart	38	15-03-2019 00:49:54.938	4.001 TCP 22 SSH 192.168.1.33
47 at start	37	15-03-2019 00:49:54.938	4.001 TCP 9 Discard 192.168.1.33
48 generic For	36	15-03-2019 00:49:54.933	4.001 TCP 7 Echo 192.168.1.33

User Rights: Basic User [5] Server Attack

Setup a honeypot and monitor the honeypot on network.

### Honeypot

Honeypot impersonates a real server 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 marked system is in the DMZ that means the intruder does not have access to the internal infrastructure honeypot periodically monitors and manages the intruder whether and manage the attack comes from outside. The infrastructure or inside it honeypot widely.

### KF Sensors

KF Sensors is a windows honeypot. It is to identify all networks hackers.

Attacker VM → KaliLinux

Victim VM → Windows 10.

### Severity

Red → More dangerous (High)

Yellow → Average (Medium)

Grey → Low

Ports:

Services

- 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)

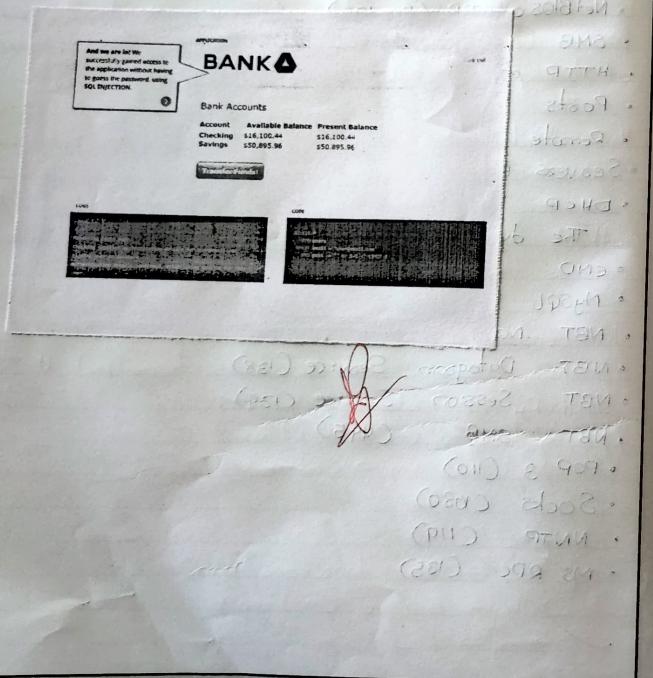
Services Ports

- 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 Planet" website.
2. Click on SQL injection.
3. You will see a bank login page.
4. You can also see the application log window which shows all the details entered in web page.
5. Try entering `username` as `username@gmail.com` and `password` as `password`. EXPLORE TO INVENT
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.

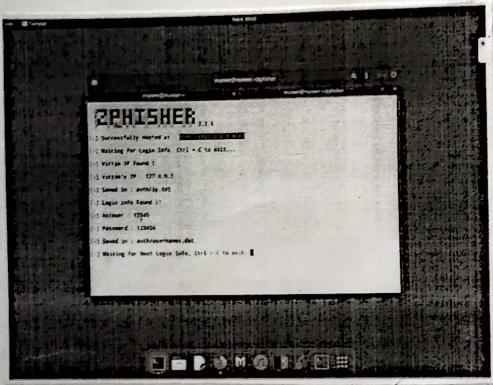
8. This behaviour shows that application might be vulnerable to SQL injection.
  9. Now try entering username and password as below.



## GROUP OF INSTITUTIONS

## EXPLORE TO INVENT

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 revealing sensitive information.

Requirements:

1. V.M. Ware
2. Linux
3. Zphisher
4. cloudflare

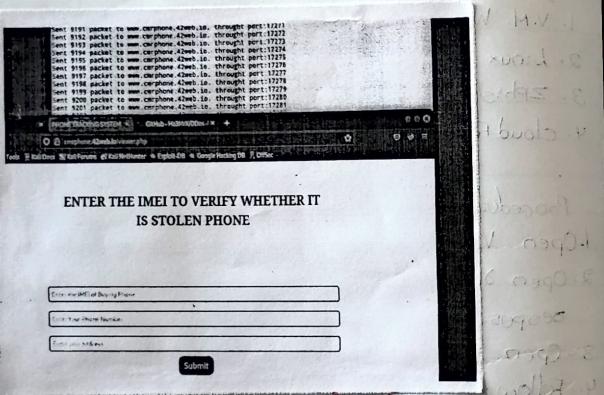
Procedure:

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

Write a code to demonstrate Dos attacks.

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

Output:



ENTER THE IMEI TO VERIFY WHETHER IT IS STOLEN PHONE

Enter your IMEI Number
Enter your phone number
Enter your address

Submit

Requirements:

1. VM Ware / Virtual Box
2. Linux
3. <https://github.com/Ha3MrX/Dos-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/Dos-Attack`
5. `cd Dos-Attack`
6. `python2 ddos-attack.py`
7. Select website for target
8. Example: `www.carnphone.42web.io`
9. Select the port 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

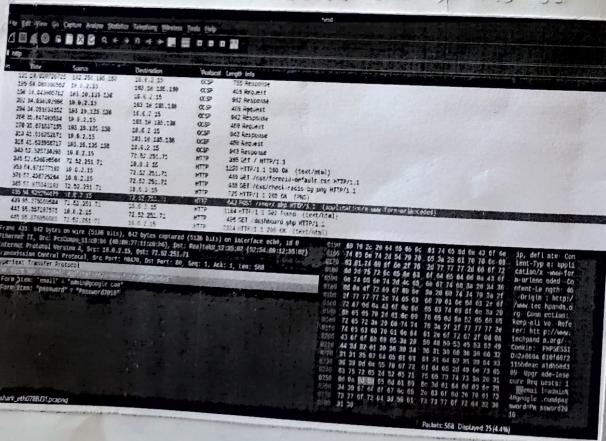
<http://www.techpanda.org/>

Login | Personal Contacts Manager v1.0

Username\*  
admin@google.com

Password\*  
\*\*\*\*\*

Remember me



Step 5: The login email is admin@google.com and password is Password2010

Step 6: Click on submit button.

Step 7: A successful login should give you the dashboard.

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

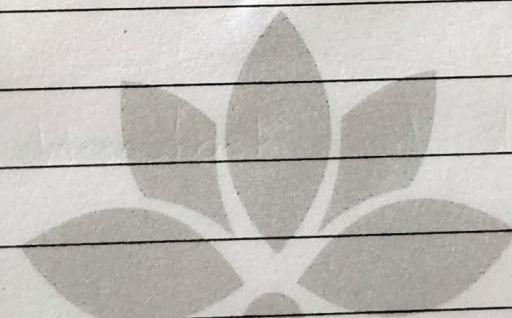
Step 9: Filter for HTTP protocol results only using the filter text box.

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

- Just below the big 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

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



CMR

GROUP OF INSTITUTIONS

EXPLORE TO INVENT

New key pair

Enter the details for the new key pair

Contact details

Contact name

An existing contact can only be chosen if it does not already own this kind of key.

Algorithm and key length

Algorithm RSA (OID: 1.2.840.113545)

Key length 1024

Password

Enter password

Confirm password

Finish Cancel

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 Asymmetric key Crypto Algorithm, Hash and Digital Signature /PKI

Requirements:

Jcryptool

Procedure:

step 1: Download Jcryptool from [www.cryptool.org](http://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 Asymmetric algorithms.

txt.txt \* out01.bin \* out02.bin

```
00 01 02 03 04 05 06 07
00:35 31 2D B2 B5 10 ED 7E 51-...
06:AF 14 48 CC 5D 22 49 DB ..H.]!`I.
10:BE D1 9C 33 78 68 50 07 ...3xhP.
18:AE 74 94 80 EF 77 25 0E .t...w%.
20:D2 54 C3 93 18 A1 64 94 .T...d.
28:0C F0 F4 9D 12 17 46 64 .....Fd
30:CD 5A DB 67 26 39 EF 30 ...g&90
38:4B 69 2B 31 47 19 63 5F J.+1G.c_
40:9E 67 40 53 DD 55 D6 3B .8S.U;
48:11 F7 51 B2 FA B2 B0 20 .Q...
50:0F E6 1D 9F 4A AE A0 F6 ..J...
56:30 78 0B FF 08 41 5D 05 0x...A].
60:21 43 E9 42 00 C9 6D 61 !C.B...a
68:AD B7 B8 FE 52 77 AD 4B ....RW.K
70:83 E4 69 8E BA DD C1 45 .....E
78:17 AE AB A6 9C C7 6F 47 .....oG
```

Text output

txt.txt \* out01.bin \* out02.bin

```
00 01 02 03 04 05 06 07
04:49 20 4C 6F 76 E5 20 55 I Love U
8:20 6B 61 6E 69 0A kani.
10:
18:
20:
28:
30:
38:
40:
48:
50:
58:
60:
68:
70:
78:
en.
```

Ex. No.

Date

Page No.

Step 4: Now Create a New key pair using the user's name as contact name and user's 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 preferred hashing algorithm which requires no further input.

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

Aim: Jcryption and Demonstration of Symmetric key Crypto Algorithm and Digital Signature /PKI

Requirements:

Jcryption

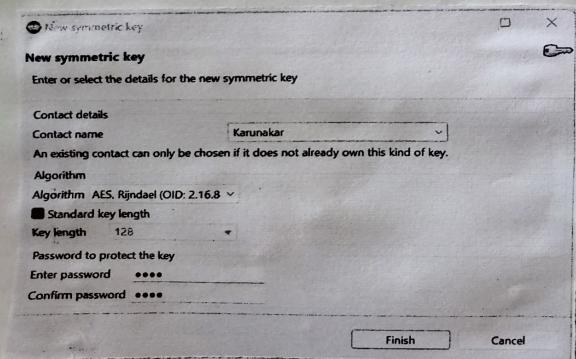
Procedure:

Step 1: Download Jcryption from [www.cryptologic.com](http://www.cryptologic.com) 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 user's name as Contact name and user password.



txt.txt \* out004.bin \* out005.bin  
00 01 02 03 04 05 06 07  
00:15 07 09 49 BD 66 21 37 ...I.f!7  
06:7E B5 8C C7 A8 F1 21 43 .....!C  
10:94 46 77 46 51 68 B9 85 .FwFQh..  
18:9E 39 C7 F9 90 27 39 C8 .9...!9.  
20:  
28:  
30:  
38:  
40:  
48:  
50:  
58:  
60:  
68:  
70:  
78:

but4pass

subiect

txt.txt \* out004.bin \* out005.bin  
00 01 02 03 04 05 06 07  
00:49 20 4C 6F 76 65 20 55 I Love U  
08:20 6B 61 72 75 6E 61 6B karunak  
10:61 72 0A ar.  
18:  
20:  
28:  
30:  
38:  
40:  
48:  
50:  
58:  
60:  
68:

20130303 2020 0111 1000 20130303  
karunakar 20130303 2020 0111 1000 20130303

Ex. No.

Date

Page No.

Step 8: 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 signing a file select RSA 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 RSA again from digital signature and Select the stored key and give the Password.

Step 10: And it shows a message that it is valid.