

**Using the software tools/commands to perform the following, generate an analysis report:**

**A. Password Cracking**

- a. Use MD5 generator in the site <https://www.md5hashgenerator.com/> to find out the MD5 hash for the following words i. Admin12345 ii. Ethical@#\$\$%Hacking

## MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

admin123

Generate →

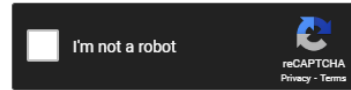
Your String	admin123
MD5 Hash	0192023a7bbd73250516f069df18b500 <button>Copy</button>
SHA1 Hash	f865b53623b121fd34ee5426c792e5c33af8c227 <button>Copy</button>

- b. Use crackstation.net to feed in the above MD5 hashes and find out its equivalent words. Display the results obtained.

## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

0192023a7bbd73250516f069df18b500



**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
0192023a7bbd73250516f069df18b500	md5	admin123

**Color Codes:** Green Exact match, Yellow Partial match, Red Not found.

## B. Dictionary attack

Steps: 1

- Go to <https://www.python.org/downloads/release/python-370/>

Version	Operating System	Description	MD5 Sum	File Size	GPG
<a href="#">Gzipped source tarball</a>	Source release		41b6595deb4147a1ed517a7d9a580271	22745726	<a href="#">SIG</a>
<a href="#">XZ compressed source tarball</a>	Source release		eb8c2a6b1447d50813c02714af4681f3	16922100	<a href="#">SIG</a>
<a href="#">macOS 64-bit/32-bit installer</a>	macOS	for Mac OS X 10.6 and later	ca3eb84092d0ff6d02e42f63a734338e	34274481	<a href="#">SIG</a>
<a href="#">macOS 64-bit installer</a>	macOS	for OS X 10.9 and later	ae0717a02efa3b0eb34aad680dc498	27651276	<a href="#">SIG</a>
<a href="#">Windows help file</a>	Windows		46562af86c2049dd0cc7680348180dca	8547689	<a href="#">SIG</a>
<a href="#">Windows x86-64 embeddable zip file</a>	Windows	for AMD64/EM64T/x64	cb8b4f0d979a36258f73ed541def10a5	6946082	<a href="#">SIG</a>
<a href="#">Windows x86-64 executable installer</a>	Windows	for AMD64/EM64T/x64	531c3fc821ce0a4107b6d2c6a129be3e	26262280	<a href="#">SIG</a>
<a href="#">Windows x86-64 web-based installer</a>	Windows	for AMD64/EM64T/x64	3cfdaf4c8d3b0475aaec12ba402d04d2	1327160	<a href="#">SIG</a>
<a href="#">Windows x86 embeddable zip file</a>	Windows		ed9a1c028c1e99f5323b9c20723d7d6f	6395982	<a href="#">SIG</a>
<a href="#">Windows x86 executable installer</a>	Windows		ebb6444c284c1447e902e87381afeff0	25506832	<a href="#">SIG</a>
<a href="#">Windows x86 web-based installer</a>	Windows		779c4085464eb3ee5b1a4fffd0eabca4	1298280	<a href="#">SIG</a>

- Run the setup python-3.7.0-amd64
  - Go to custom installation
- Create passlist.txt

```
passlist - Notepad
File Edit Format View Help
admin
abcde
12345
mypass
root|
```

- Create md5 encryption for few words. use the link <https://www.visiospark.com/password-encryption-tool/> to enter a password and fetch its MD5 encryption.

```
md5list - Notepad
File Edit Format View Help
21232f297a57a5a743894a0e4a801fc3
63a9f0ea7bb98050796b649e85481845
a029d0df84eb5549c641e04a9ef389e5|
```

### Packages, Classes and methods

<b>hashlib</b>	Module to generate message digest or secure hash from the source message
<b>Encode('utf-8')</b>	Returns an encoded version of the given string. By default, Python uses utf-8 encoding.
<b>strip()</b>	Used to strip off any blank space in the string.
<b>hexdigest()</b>	To convert hashed object into hexadecimal format.

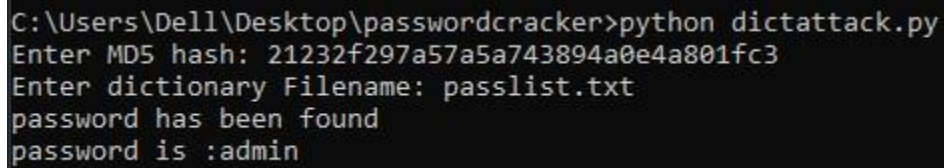
- Write the python code in notepad and save as dictattack.py import hashlib flag=0

```
p_hash=input("Enter MD5 hash")
dictionary=input("Enter dictionary
Filename:") try:
password_file=open(dictionary,"r")
except: print("No file found") quit()
for word in password_file:

    enc_word=word.encode('utf-8') digest
=hashlib.md5(enc_word.strip()).hexdigest()
if(digest==p_hash): print("password has
been found") print("password is :"+word)
```

```
        flag=1        break
if(flag==0):
print("No password
found")
```

- In the command prompt d:\passwordcracking>python dictattack.py



```
C:\Users\Dell\Desktop\passwordcracker>python dictattack.py
Enter MD5 hash: 21232f297a57a5a743894a0e4a801fc3
Enter dictionary Filename: passlist.txt
password has been found
password is :admin
```

### C. Encrypt and Decrypt Passwords

Use the link <https://www.visiospark.com/password-encryption-tool/> to enter a password and generate report that contains encrypted data generated by various algorithms

Results

Encryption Type	Encrypted Password
Original Password:	password
DES:	\$1\$8IDb3wW\$XF4qOWsWzK0ryba/Sg.w2/
MD5:	5f4dcc3b5aa765d61d8327deb882cf99
sha1:	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
sha224:	d63dc919e201d7bc4c825630d2cf25fcd93d4b2f0d46706d29038d01
sha256:	5e884898da2047151d0e56f8dc6292773603d0d6aabbdd62a1ef721d1542d8
sha384:	a8b64babd0aca91a59b0bb7761b421d4f2bb38280d3a75ba0f21f2bebc45583d446c598660c94ce680c47d19c30783a7
sha512:	b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6d103fd07c95385f1ab0cacbc86
ripemd128:	c9c6d316d6dc4d952a789fd4b8858ed7

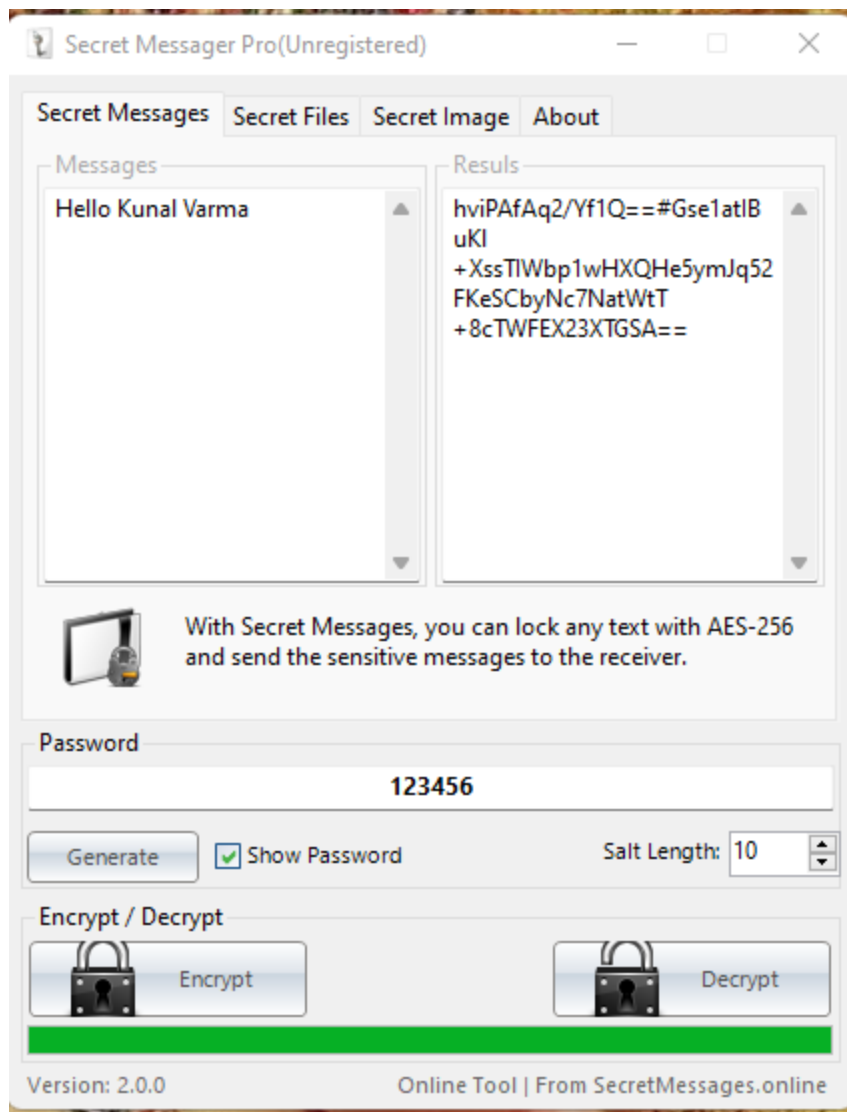
This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish. [Cookie settings](#) [ACCEPT](#)

ripemd160:	2c08e8f5884750a7b99f6f2f342fc638db25ff31
ripemd256:	f94cf96c79103c3ccad10d308c02a1db73b986e2c48962e96ecd305e0b80ef1b
ripemd320:	c571d82e535de67ff5f87e417b3d53125f2d83ed7598b89d74483e6c0dfe8d86e88b380249fc8f1b4
whirlpool:	74dfc2b27acfa364da55f93a5cae29ccad3557247eda238831b3e9bd931b01d77fe994e4f12b9d4cfa92a124461d2065197d8cf7f33f88566da2db2a4d6eae
snefru:	8ec80c31fab12b5f7930e6c9288c3076852aeef8f560a9ed91fb2e33838e6871
snefru256:	8ec80c31fab12b5f7930e6c9288c3076852aeef8f560a9ed91fb2e33838e6871
gost:	db4d9992897eda89b50f1d3208db607902da7e79c6f3bc6e6933cc5919068564
gost32:	bbeda74f
crc32:	35c246d5
fnv132:	9b693732
fnv164:	da5bcd06b53c0a92
joaat:	08d63509
haval128_3:	2221b19499669a2da53c49ca13c5e5be

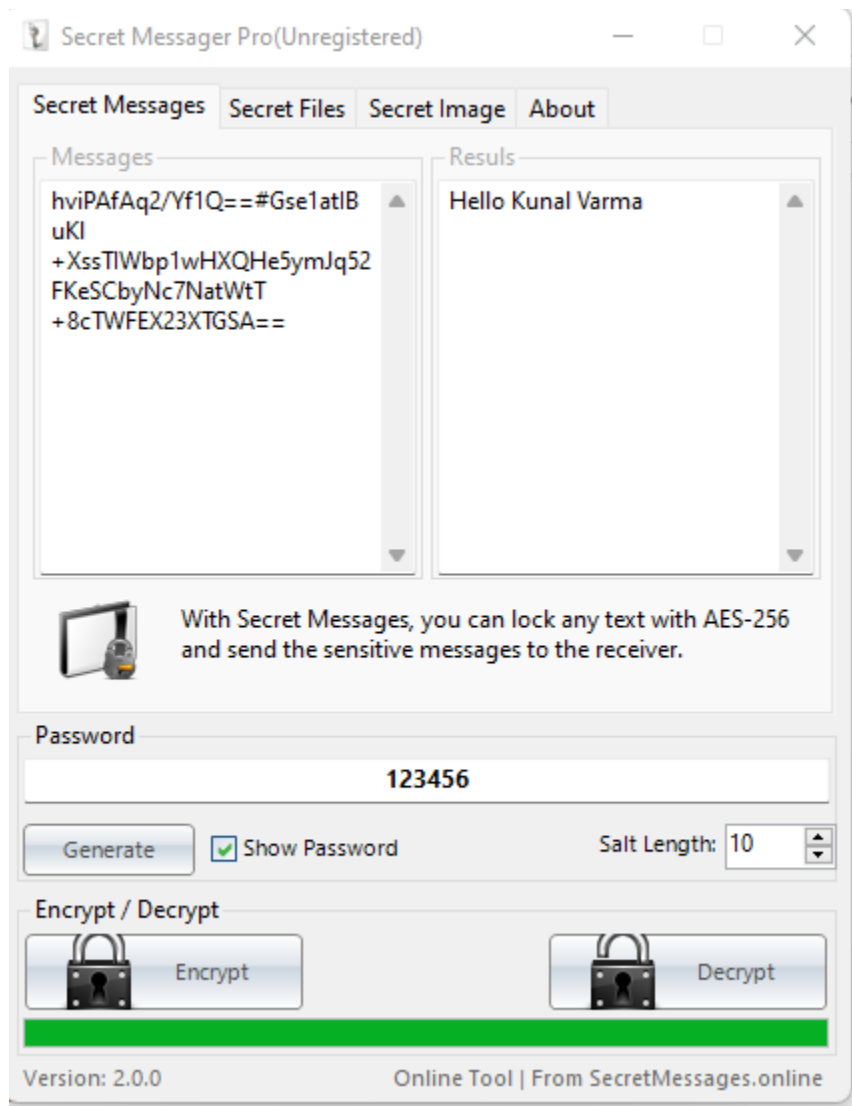
This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish. [Cookie settings](#) [ACCEPT](#)

Go to <http://secretmessages.online/Home/Software> and download SecretMessengerPro\_2.0.0. Encrypt and decrypt text and password using the secretmessengerpro software.

## Encryption:



**Decryption:**



## D. DoS Attack

### 1 Denial of Service Attacks\_ The Ping of Death-3\_D\_1

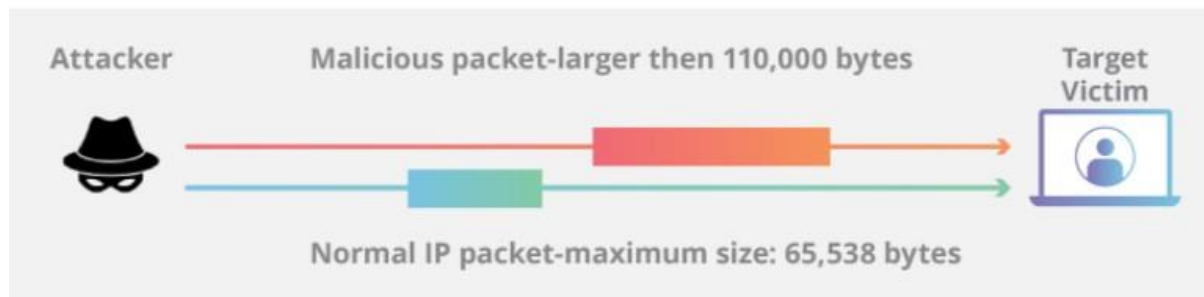
#### What is a ping of death attack?

A Ping of death (PoD) attack is a denial-of-service (DoS) attack, in which the attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash. The original ping of death attack is less common today. A related attack known as an ICMP flood attack is more prevalent.

#### How does a ping of death attack work?

An Internet Control Message Protocol (ICMP) echo-reply message or “ping”, is a network utility used to test a network connection, and it works much like sonar – a “pulse” is sent out and the “echo” from that pulse tells the operator information about the environment. If the connection is working, the source machine receives a reply from the targeted machine.

While some ping packets are very small, IP4 ping packets are much larger, and can be as large as the maximum allowable packet size of 65,535 bytes. Some TCP/IP systems were never designed to handle packets larger than the maximum, making them vulnerable to packets above that size.



When a maliciously large packet is transmitted from the attacker to the target, the packet becomes fragmented into segments, each of which is below the maximum size limit. When the target machine attempts to put the pieces back together, the total exceeds the size limit and a buffer overflow can occur, causing the target machine to freeze, crash or reboot.

While ICMP echo can be used for this attack, anything that sends an IP datagram can be used for this exploit. That includes **TCP**, **UDP** and **IPX** transmissions.

A simple tutorial on how to perform DoS attack using **ping of death** using CMD:

**Disclaimer:** This is just for educational purposes. It’s nothing great but you can use it to learn.

Here are the steps:

- Open Notepad
- Copy the following text on the notepad `:loop`

```
ping <IP Address> -l 65500 -w 1 -n 1
```

```
goto :loop
```

In the above command, replace <IP Address> with an IP address.

- Save the Notepad with any name. Let’s say *dos.txt*
- Right click on the dos.txt and click on *rename*.
- Change the extension from .txt to *.bat*
- So, now the file name should be *dos.bat*



- Double click on it and you will see a command prompt running with a lot of pings.

## 2 Denial of Service Attacks (Part 3)\_ TCP SYN Flooding-3\_D\_2

### What is a SYN flood attack

TCP SYN flood (a.k.a. SYN flood) is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

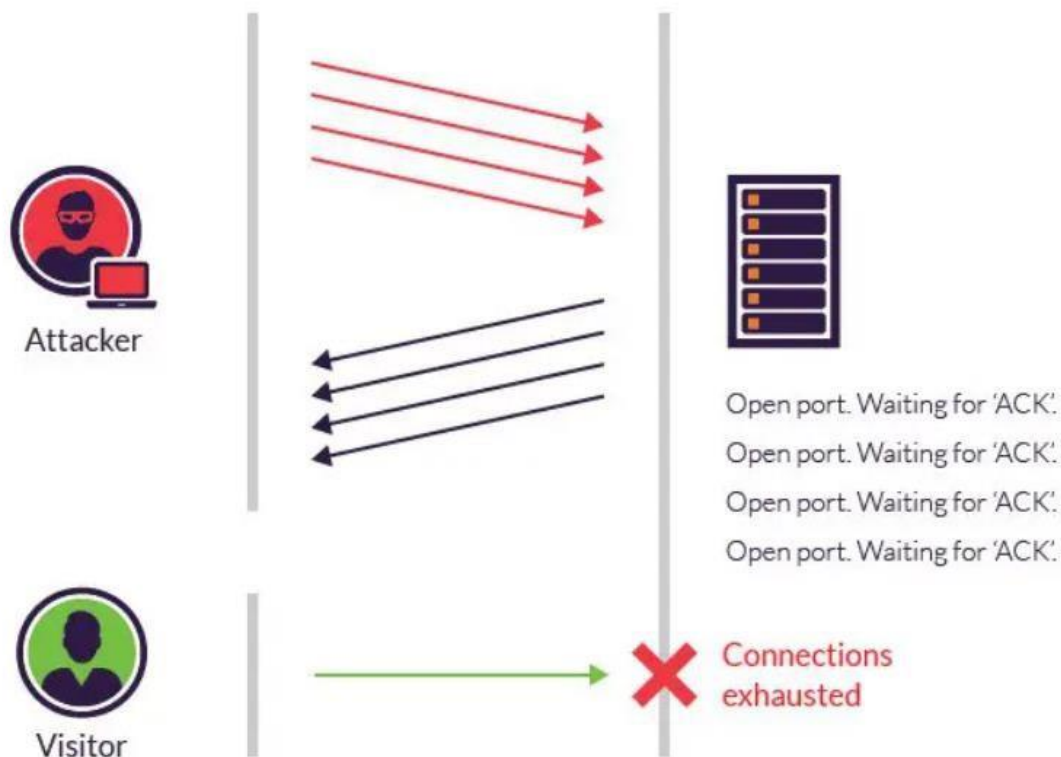
### Attack description

When a client and server establish a normal TCP “three-way handshake,” the exchange looks like this:

1. Client requests connection by sending SYN (synchronize) message to the server.
2. Server acknowledges by sending SYN-ACK (synchronize-acknowledge) message back to the client.
3. Client responds with an ACK (acknowledge) message, and the connection is established.

In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address. The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port.

The malicious client either does not send the expected ACK, or—if the IP address is spoofed—never receives the SYN-ACK in the first place. Either way, the server under attack will wait for acknowledgement of its SYN-ACK packet for some time.



### 3 Denial of Service Attacks (Part 5)\_ The Smurf Attack\_(240p)- 3\_D\_3

#### Smurf Attack

Smurf attack exploits the target by sending repeated ping request to broadcast address of the target network. The ping request packet often uses forged IP address (return address), which is the target site that is to receive the denial of service attack. The result will be lots of ping replies flooding back to the innocent, spoofed host. If number of hosts replying to the ping request is large enough, the network will no longer be able to receive real traffic.

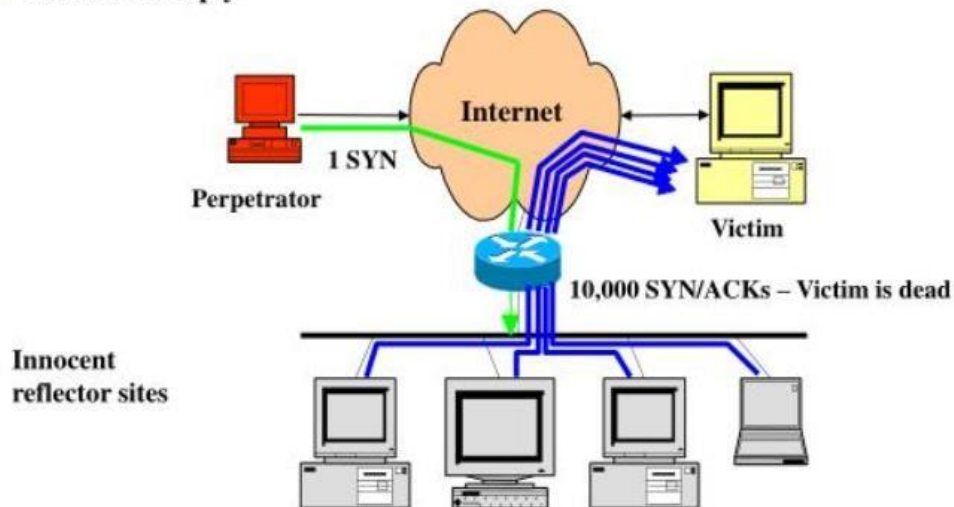
The Smurf Attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on

## Smurf Attack

— ICMP echo (spoofed source address of victim)  
Sent to IP broadcast address

— ICMP echo reply

ICMP = Internet Control  
Message Protocol



### E. ARP poisoning in Windows

ARP command to view and modify the ARP table entries on the local computer. This may display all the known connections on your local area network segment (if they have been active and in the cache). The Arp command is useful for viewing the ARP cache and resolving address resolution problems.

Syntax (Inet means Internet address)

```
arp[-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s  
InetAddrEtherAddr [IfaceAddr]]
```

```
cmd. Command Prompt
C:\>arp -a

Interface: 192.168.159.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.159.254      00-50-56-f9-b2-b9    dynamic
  192.168.159.255      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: 192.168.171.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.171.254      00-50-56-f5-d1-f5    dynamic
  192.168.171.255      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: 192.168.43.245 --- 0xb
  Internet Address      Physical Address      Type
  192.168.43.1         94-14-7a-77-a5-34    dynamic
  192.168.43.255      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
```

### On Linuxrform ARP Poisoning inWindows

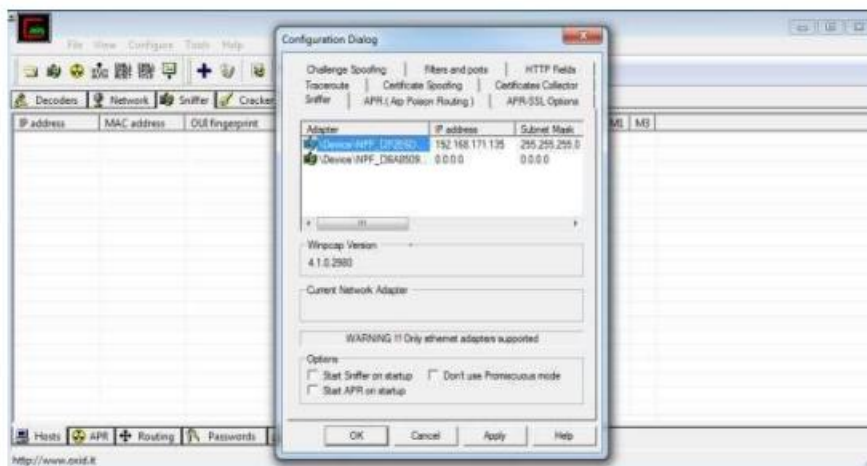
```
rootclient@google:~$ arp
Address      HWtype  HWaddress      Flags Mask    Iface
192.168.171.254 ether 00:50:56:f5:d1:f5 C             ens33
_gateway     ether 00:50:56:e8:82:1f C             ens33
rootclient@google:~$
```

Step 1: Download and install Cain & Abel software in VMware.

Step 2: GO to sniffer and then click on configuration, select the appropriate wireless adapter.



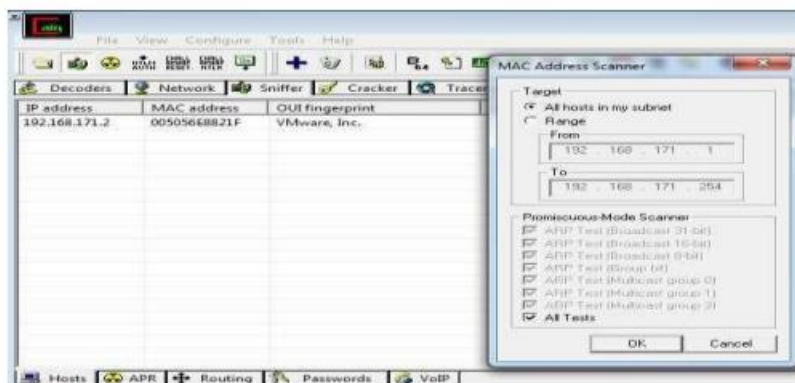
### Step 3: Activate sniffer



Step 4: click on + icon. Check all tests checkbox and then click ok



Step 5: click on APR then click on blank screen and then click on the + icon. Select any IP address (IPv4 address)

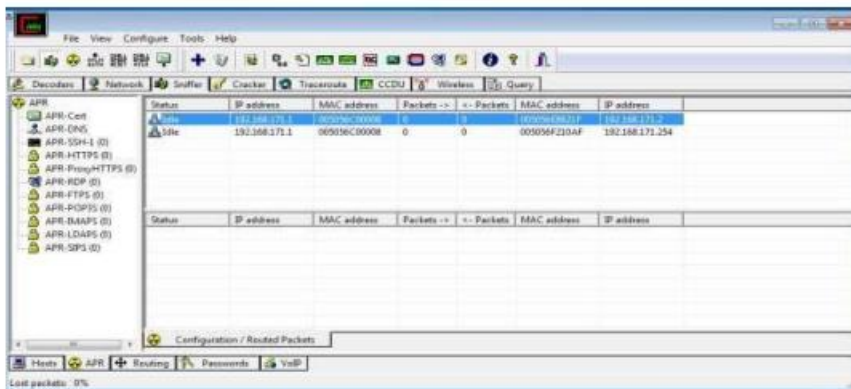
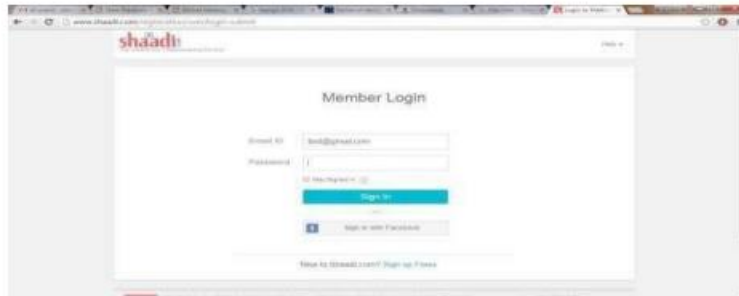
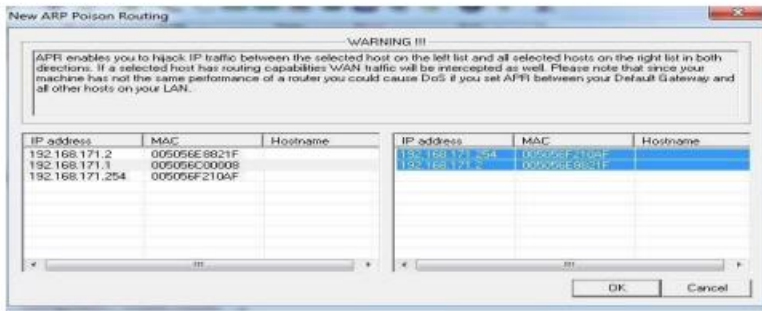


Step 6: select all the IP address and MAC address and then click on OKply ARP.

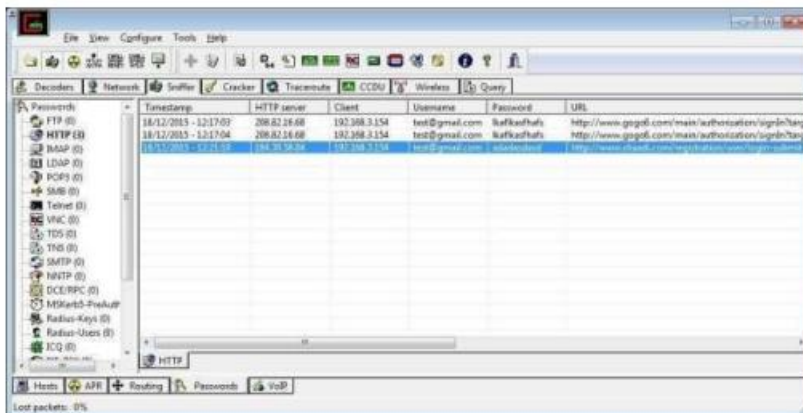


Step7: Go to any website on source ip address.





Step 8: Go to password option in the cain&abel and see the visited site password.



**F. Ifconfig, ping, netstat, traceroute.**

**G. Steganography Tools**