1.	Write a program to a. Accept a message “________________”. b. Create a matrix of 5x5 for the message. c. Transpose the matrix. d. Display the encrypted message.
2.	Write a program to a. Set the Encrypted message as “________________” . b. Create a matrix of 5x5 for the cipher. c. Transpose the matrix. d. Display the decrypted message.
3.	Write a program to a. Accept a message. b. Generate a Random Key. c. Perform $C_i = (M_i + K) mod\ 26$ d. Display the content of matrix in the message format.
4.	Write a program to a. Set the Encrypted message as “________________” . b. Accept the Key ____________ . c. Perform $M_i = (C_i + 26 - K) mod\ 26$ d. Display the decrypted message.
5.	Write a program to a. Randomly Generate prime numbers b. Compute N c. Compute ϕ(N) d. Generate e and check e, ϕ(N) are relatively prime or not.
6.	Write a program to a. Accept Two Prime Numbers _________&_________. b. Compute N c. Compute ϕ(N) d. Accept e that is relatively prime with ϕ(N). e. Compute $d = e^{-1} mod\ \phi(\mathrm{N})$ f. Display Public and Private Keys.
7.	Write a Program to implement Diffie Hellman Algorithm.
8.	Write and Execute any five network reconnaissance commands. 1. Ping Command The ping command is one of the most often used networking utilities for detecting devices on a network and for troubleshooting network problems. When you ping a device you send that device a short message, which it then sends back (the echo). The general format is ping hostname or ping IPaddress. Example

ping www.google.com or ping 216.58.208.68

This article covers the ping command in more detail

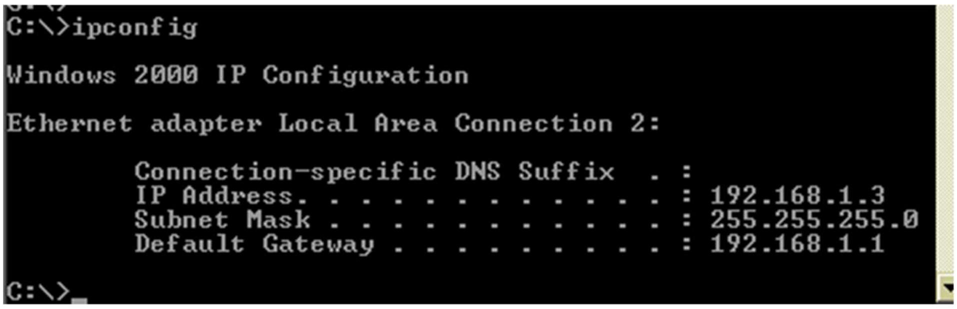
2. ipconfig Command

Another indispensable and frequently used utility that is used for finding network information about your local machine like IP addresses, DNS addresses etc

Basic Use: Finding Your IP Address and Default Gateway

Type the command ipconfig at the prompt.

The following is displayed



```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\>_
```

Ip config has a number of switches the most common are:

ipconfig /all – displays more information about the network setup on your systems including the MAC address.

ipconfig /release – release the current IP address

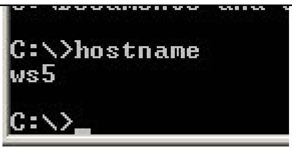
ipconfig /renew – renew IP address

ipconfig /? -shows help

ipconfig/flushdns – flush the dns cache

3. Hostname Command

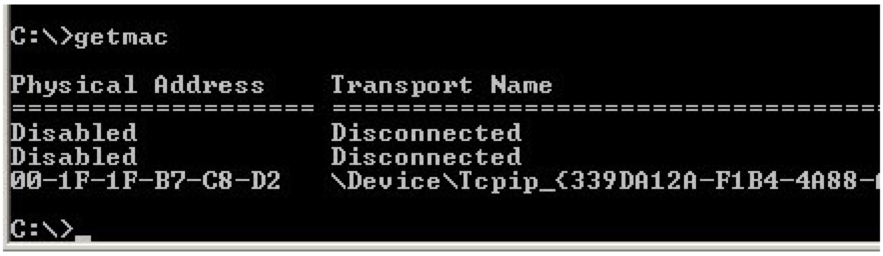
A very simple command that displays the host name of your machine. This is much quicker than going to the control panel>system route.



```
C:\>hostname
ws5

C:\>_
```

4. getmac Command

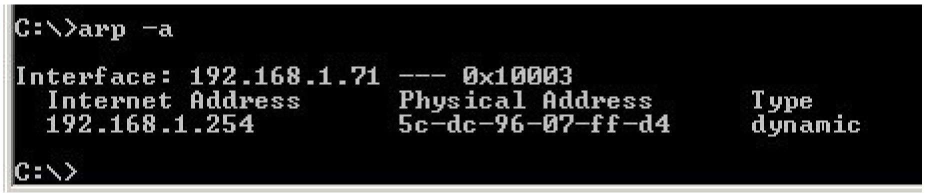
Another very simple command that shows the MAC address of your network interfaces



```
C:\>getmac

Physical Address    Transport Name
=================== ==================================
Disabled            Disconnected
Disabled            Disconnected
00-1F-1F-B7-C8-D2   \Device\Tcpip_{339DA12A-F1B4-4A88-

C:\>_
```

5. arp Command

This is used for showing the address resolution cache. This command must be used with a command line switch arp -a is the most common.



```
C:\>arp -a

Interface: 192.168.1.71 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.1.254         5c-dc-96-07-ff-d4     dynamic

C:\>
```

Type arp at the command line to see all available options.

9. Write and Execute any five Nmap commands.

1.Scan list of Hosts from a File

If you have more hosts to scan and all host details are written in a file , you can directly ask nmap to read that file and perform scans. Let’s see how to do that.

Create a text file called “nmaptest.txt” and define all the IP addresses or hostname of the server that you want to do a scan.

```
[root@server1 ~]# cat > nmaptest.txt

localhost
server2.tecmint.com
192.168.0.101
```

Next, run the following command with “iL” option with nmap command to scan all listed IP address in the file.

```
[root@server1 ~]# nmap -iL nmaptest.txt
```

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-18 10:58 EST
Interesting ports on localhost.localdomain (127.0.0.1):
Not shown: 1675 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
111/tcp open  rpcbind
631/tcp open  ipp
857/tcp open  unknown

Interesting ports on server2.tecmint.com (192.168.0.101):
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
958/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerbook
MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Interesting ports on server2.tecmint.com (192.168.0.101):
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
958/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerbook
MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 3 IP addresses (3 hosts up) scanned in 2.047 seconds
```

2. Scan an IP Address Range

You can specify an IP range while performing scan with Nmap.

```
[root@server1 ~]# nmap 192.168.0.101-110

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:09 EST
Interesting ports on server2.tecmint.com (192.168.0.101):
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
```

```
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerbook
MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 10 IP addresses (1 host up) scanned in 0.542 seconds
```

3. Scan Network Excluding Remote Hosts

You can exclude some hosts while performing a full network scan or when you are scanning with wildcards with "–exclude" option.

```
[root@server1 ~]# nmap 192.168.0.* --exclude 192.168.0.100

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:16 EST
Interesting ports on server2.tecmint.com (192.168.0.101):
Not shown: 1674 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
957/tcp  open  unknown
3306/tcp open  mysql
8888/tcp open  sun-answerbook
MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 255 IP addresses (1 host up) scanned in 5.313 seconds
You have new mail in /var/spool/mail/root
```

4. Scan OS information and Traceroute

With Nmap, you can detect which OS and version is running on the remote host. To enable OS & version detection, script scanning and traceroute, we can use "-A" option with NMAP.

```
[root@server1 ~]# nmap -A 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:25 EST
Interesting ports on server2.tecmint.com (192.168.0.101):
Not shown: 1674 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 4.3 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.2.3 ((CentOS))
111/tcp  open  rpcbind  2 (rpc #100000)
957/tcp  open  status   1 (rpc #100024)
3306/tcp open  mysql   MySQL (unauthorized)
8888/tcp open  http    lighttpd 1.4.32
```

```
MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=4.11%P=i686-redhat-linux-gnu%D=11/11%Tm=52814B66%O=22%C=1%M=080027)
TSeq(Class=TR%IPID=Z%TS=1000HZ)
T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=
134%DAT=E)

Uptime 0.169 days (since Mon Nov 11 12:22:15 2013)

Nmap finished: 1 IP address (1 host up) scanned in 22.271 seconds
You have new mail in /var/spool/mail/root
```

In above Output, you can see that nmap is came up with TCP/IP fingerprint of the OS running on remote hosts and being more specific about the port and services running on the remote hosts.

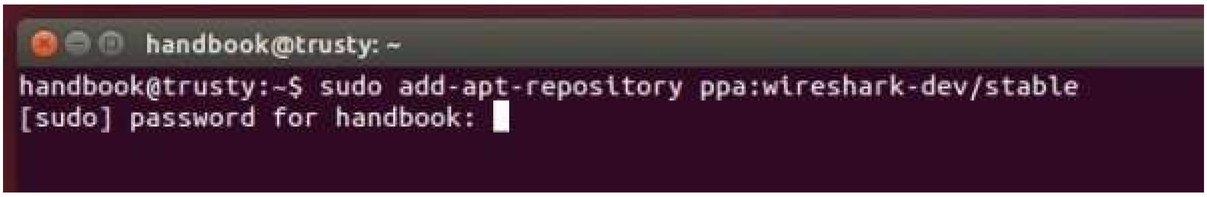
5. Perform a Fast Scan

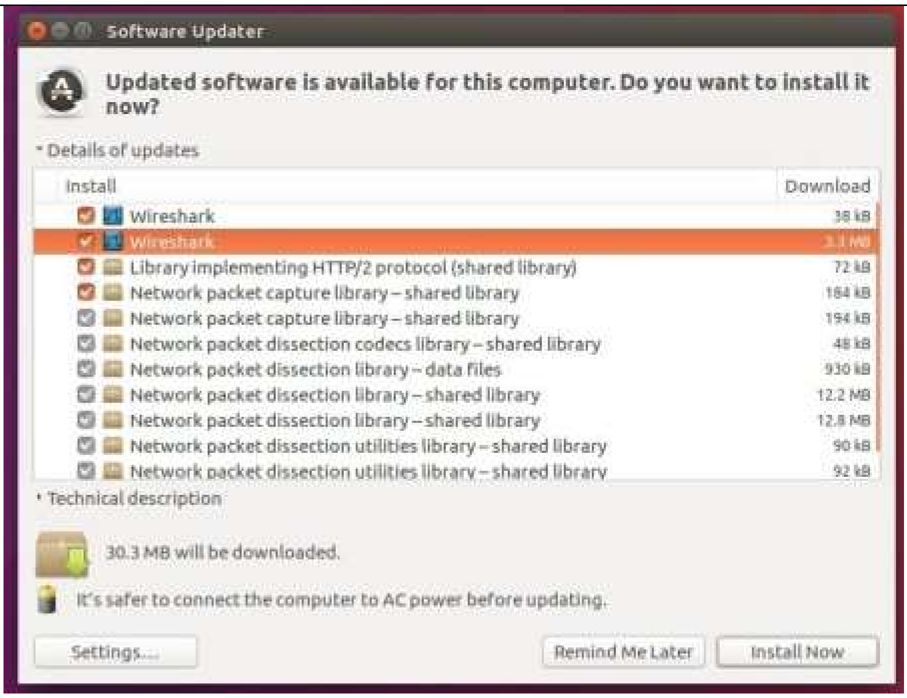
You can perform a fast scan with “-F” option to scans for the ports listed in the nmap-services files and leaves all other ports.

```
[root@server1 ~]# nmap -F 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:47 EST
Interesting ports on server2.tecmint.com (192.168.0.101):
Not shown: 1234 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
3306/tcp open  mysql
8888/tcp open  sun-answerbook
MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.322 seconds
```

10.	Write a Program to implement MD-5 Algorithm.
11.	Write a Program to implement SHA Algorithm.

12.	Write a program to a. Accept a message b. Compute $C = M^{e} mod\ N$ c. Display the encrypted message. Note use packages.
13.	Write a program to a. Set a Cipher. b. Compute $M = C^{d} mod\ N$ c. Display the decrypted message. Note use packages.

14.	Download and install wireshark and capture icmp, tcp, and http packets in promiscuous mode.
	Type the commands on the terminal to install wireshark:
	sudo apt-get update
	sudo apt-get install wireshark
	or
	1. To add the PPA, open terminal from Unity Dash / App Launcher, or via Ctrl+Alt+T shortcut keys, and then run command:
	sudo add-apt-repository ppa:wireshark-dev/stable
	Type in your password (no visual feedback due to security reason) when it asks and hit Enter.
	
	
	`handbook@trusty:~$ sudo add-apt-repository ppa:wireshark-dev/stable`
	`[sudo] password for handbook:`
	2. For those who have a previous release installed, launch Software Updater (or Update Manager) to upgrade it to the latest:



Updated software is available for this computer. Do you want to install it now?

▾ Details of updates

Install	Download
☑ Wireshark	38 kB
☑ Wireshark	3.3 MB
☑ Library implementing HTTP/2 protocol (shared library)	72 kB
☑ Network packet capture library – shared library	184 kB
☑ Network packet capture library – shared library	194 kB
☑ Network packet dissection codecs library – shared library	48 kB
☑ Network packet dissection library – data files	930 kB
☑ Network packet dissection library – shared library	12.2 MB
☑ Network packet dissection library – shared library	12.8 MB
☑ Network packet dissection utilities library – shared library	90 kB
☑ Network packet dissection utilities library – shared library	92 kB

▸ Technical description

30.3 MB will be downloaded.

It's safer to connect the computer to AC power before updating.

To capture ICMP tracert traffic:

a. Start a Wireshark capture.
b. Open a command prompt.
c. Type tracert -d 8.8.8.8 and press Enter to trace the route to one of Google's public DNS servers. The -d option prevents DNS name resolution, which in this case will improve performance and reduce the amount of captured traffic.
d. When the trace is complete, close the command prompt.
e. Stop the Wireshark capture.

To analyze tracert traffic:

a. Observe the traffic captured in the top Wireshark packet list pane. Look for traffic with ICMP listed as the protocol. To view only ICMP traffic, type icmp (lower case) in the Filter box and press Enter.
b. Select the first ICMP packet, labeled Echo (ping) request.
c. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Internet Control Message Protocol frame.
d. Expand Internet Protocol Version 4 to view IPv4 details.
e. Observe the Time to live. Notice that the time to live is set to 1.
f. Expand Internet Control Message Protocol to view ICMP details.
g. Observe the Type. Notice that the type is 8 (Echo (ping) request). Tracert is performed through a series of ICMP Echo requests, varying the Time-To-Live (TTL) until the destination is found.
h. In the top Wireshark packet list pane, select the second ICMP packet, labeled Time-to-live exceeded.
i. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Internet Control Message Protocol frame.
j. Expand Internet Protocol Version 4 to view IPv4 details.
k. Observe the Source. This is the IP address of the router where the time was exceeded.

l. Expand Internet Control Message Protocol to view ICMP details.
m. Observe the Type. Notice that the type is 11 (Time-to-live exceeded).
n. Observe the Code. Notice that the code is 0 (Time to live exceeded in transit).
o. Observe the fields that follow. Notice that the contents of the request packet are returned with the time exceeded error.
p. Continue selecting alternate ICMP Echo Request and ICMP Time-To-Live Exceeded packets. Notice that the request is repeated three times for each time-to-live count, and each reply indicates the IP address of the router where the time to live was exceeded.
q. Close Wireshark to complete this activity. Quit without Saving to discard the captured traffic.

Capture HTTP Packets

a. Open your Internet browser.
b. Clear your browser cache.
c. Open Wireshark
d. Click on "Capture > Interfaces".
e. A pop up window will show up.
f. You probably want to capture traffic that goes through your ethernet driver. Click on the Start button to start capturing traffic via this interface.
g. Visit the URL that you wanted to capture the traffic from.
h. Go back to your Wireshark screen and stop capturing.
i. After the traffic capture is stopped, please save the captured traffic into a *.pcap format file.

Capture HTTP traffic:

a. Open a new web browser window or tab.
b. Search the Internet for an http (rather than https) website.
c. Start a Wireshark capture.
d. Navigate to the website found in your search.
e. Stop the Wireshark capture.

Select Destination Traffic

a. Observe the traffic captured in the top Wireshark packet list pane. To view only HTTP traffic, type http (lower case) in the Filter box and press Enter.
b. Select the first HTTP packet labeled GET /.
c. Observe the destination IP address.
d. To view all related traffic for this connection, change the filter to ip.addr == <destination>, where <destination> is the destination address of the HTTP packet.

Analyze TCP Connection Traffic

a. Observe the traffic captured in the top Wireshark packet list pane. The first three packets (TCP SYN, TCP SYN/ACK, TCP ACK) are the TCP three way handshake. Select the first packet.
b. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.
c. Expand Ethernet II to view Ethernet details.
d. Observe the Destination and Source fields. The destination should be your default gateway's MAC address and the source should be your MAC address. You can use ipconfig /all and arp -a to confirm.
e. Expand Internet Protocol Version 4 to view IP details.
f. Observe the Source address. Notice that the source address is your IP address.
g. Observe the Destination address. Notice that the destination address is the IP address of the

HTTP server.

h. Expand Transmission Control Protocol to view TCP details.

i. Observe the Source port. Notice that it is a dynamic port selected for this HTTP connection.

j. Observe the Destination port. Notice that it is http (80). Note that all of the packets for this connection will have matching MAC addresses, IP addresses, and port numbers.

Analyze HTTP Request Traffic

a. Observe the traffic captured in the top Wireshark packet list pane.

b. Select the fourth packet, which is the first HTTP packet and labeled GET /.

c. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol / Hypertext Transfer Protocol frame. Also notice that the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol values are consistent with the TCP connection analyzed in Activity 3.

d. Expand Hypertext Transfer Protocol to view HTTP details.

e. Observe the GET request, Host, Connection, User-Agent, Referrer, Accept, and Cookie fields. This is the information passed to the HTTP server with the GET request.

f. Observe the traffic captured in the top Wireshark packet list pane.

g. Select the fifth packet, labeled TCP ACK. This is the server TCP acknowledgement of receiving the GET request.

Analyze HTTP Response Traffic

a. Observe the traffic captured in the top Wireshark packet list pane.

b. Select the second HTTP packet, labeled 301 Moved Permanently.

c. Observe the packet details in the middle Wireshark packet details pane.

d. Expand Hypertext Transfer Protocol to view HTTP details.

e. Observe the HTTP response, Server, Expires, Location, and other available information. This response indicates that the requested page has permanently moved to the location provided.

f. Observe the traffic captured in the top Wireshark packet list pane.

g. Select the next packet, labeled TCP ACK. This is the client TCP acknowledgement of receiving the HTTP response.

Analyze HTTP Request Traffic

a. Observe the traffic captured in the top Wireshark packet list pane.

b. Select the third HTTP packet, labeled GET /wiki/Wikiversity:Main_Page.

c. Observe the packet details in the middle Wireshark packet details pane.

d. Expand Hypertext Transfer Protocol to view HTTP details.

e. Observe the HTTP request fields. Notice that the request is similar to the request in Activity 4 above, except that the new page location is requested.

f. Observe the traffic captured in the top Wireshark packet list pane.

g. Select the next packet, labeled TCP ACK. This is the server TCP acknowledgement of receiving the GET request.

Analyze HTTP Response Traffic

a. Observe the traffic captured in the top Wireshark packet list pane.

b. Select the next packet, labeled TCP segment of a reassembled PDU. Notice that because the server response is longer than the maximum segment PDU size, the response has been split into several TCP segments.

c. Observe the packet details in the middle Wireshark packet details pane.

d. Observe the packet contents in the bottom Wireshark packet bytes pane.

e. Observe the traffic captured in the top Wireshark packet list pane. Notice that for every two TCP segments of data, there is a TCP ACK acknowledgement of receiving the HTTP response.

f. Select the last HTTP packet, labeled HTTP 200 OK.

g. Observe the packet details in the middle Wireshark packet details pane. Notice the Reassembled TCP Segments listed.

h. Expand Hypertext Transfer Protocol to view HTTP details.

i. Observe the full HTTP response to be passed to the web browser.

j. Expand Line-based text data to observe web page content.

k. In the web browser, right-click on the web page and view the page source. Notice that it is identical to the line-based text captured in Wireshark.

l. Close the web browser.

m. Close Wireshark to complete this activity. Quit without Saving to discard the captured traffic.

15.

a. Download and install Ettercap.

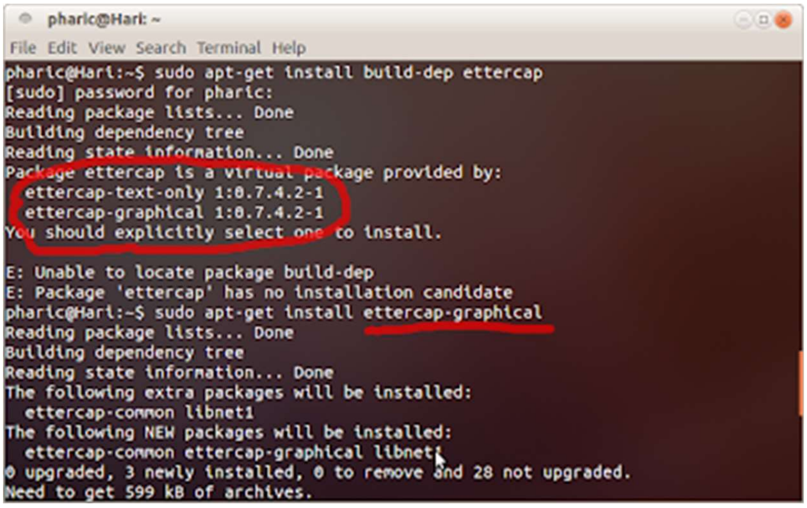
b. Perform ARP Poisoning.

Installing ettercap on Linux
Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

For installing ettercap, use the following commands :

```
sudo apt-get install zlib1g zlib1g-dev
sudo apt-get install build-essential
sudo apt-get install ettercap
```

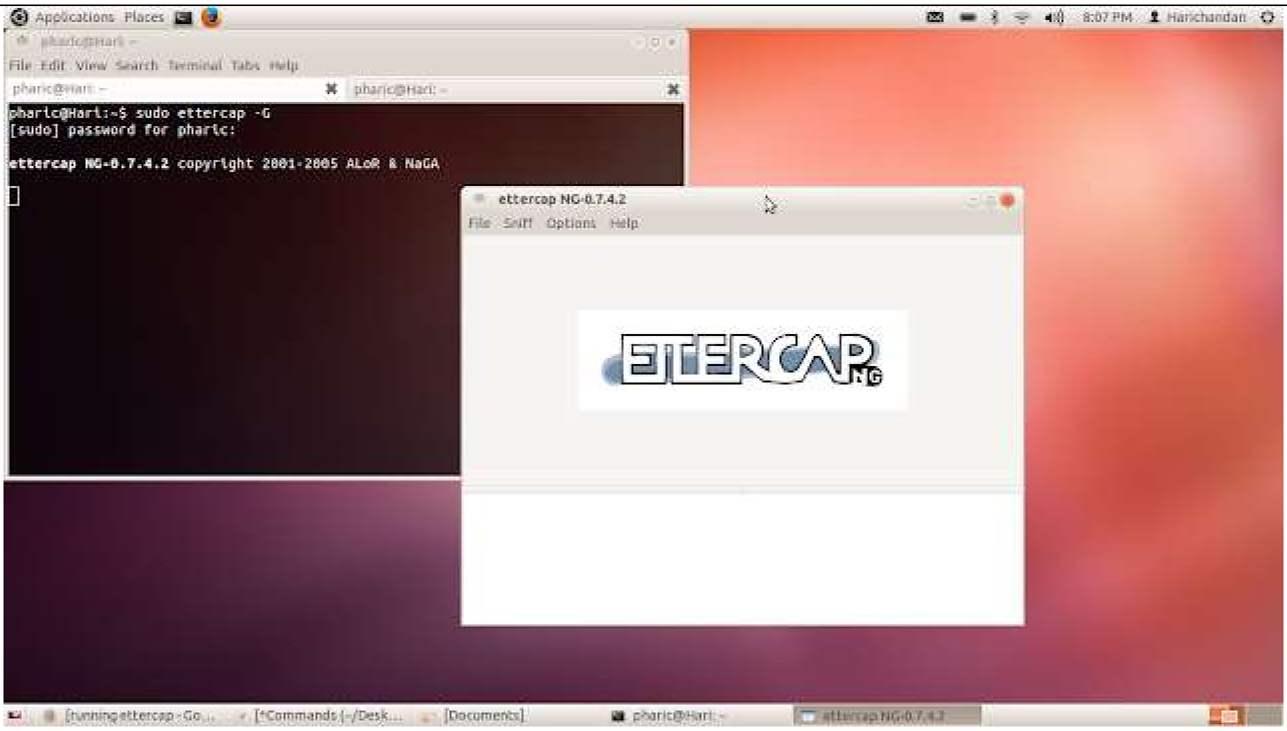
You will be prompted to choose between ettercap text-only and ettercap-graphical packages. Choose accordingly



```
pharic@Hari:~$ sudo apt-get install build-dep ettercap
[sudo] password for pharic:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package ettercap is a virtual package provided by:
  ettercap-text-only 1:0.7.4.2-1
  ettercap-graphical 1:0.7.4.2-1
You should explicitly select one to install.

E: Unable to locate package build-dep
E: Package 'ettercap' has no installation candidate
pharic@Hari:~$ sudo apt-get install ettercap-graphical
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  ettercap-common libnet1
The following NEW packages will be installed:
  ettercap-common ettercap-graphical libnet1
0 upgraded, 3 newly installed, 0 to remove and 28 not upgraded.
Need to get 599 kB of archives.
```

For installing ettercap-graphical, use the command :
sudo apt-get install ettercap-graphical

After the installation is done, you can open ettercap in different modes. For opening ettercap in graphic mode, use :
sudo ettercap –G

	 Applications Places 8:07 PM Harichandan pharic@Hari: ~ File Edit View Search Terminal Tabs Help ettercap NG-0.7.4.2 File Sniff Options Help ETTERCAP NG [running ettercap - Go... [*Commands (~/Desk... [Documents] pharic@Hari: ~ ettercap NG-0.7.4.2 pharic@Hari:~$ sudo ettercap -G [sudo] password for pharic: ettercap NG-0.7.4.2 copyright 2001-2005 ALoR & NaGA Note: For ARP Poisoning follow the steps given in the practical.