NETWORK SECURITY
LAB MANUAL
COURSE CODE: 15CS65P

FOR 6th Sem CS & E
(2017-18)

BY
Mrs. UMADEVI.M
LECTURER
COMPUTER SCIENCE &
ENGINEERING RJS POLYTECHNIC
BANGALORE-34.

For Any Feedback Contact
Email: Velumani2296@gmail.com

List of Graded Practical Exercises

Sl.No	Practical/Exercise
1	Learn to install Wine/Virtual Box/ or any other equivalent s/w on the host OS
2	Perform an experiment to grab a banner with telnet and perform the task using Netcat
3	Perform an experiment for Port Scanning with nmap, superscan or any other equivalent software
4	Using nmap 1)Find Open ports on a system 2) Find machines which are active 3)Find the version of remote OS on other systems 4)Find the version of s/w installed on other system (using nmap or any other software)
5	Perform an experiment on Active and Passive finger printing using XProbe2 and nmap
6	Perform an experiment to demonstrate how to sniff for router traffic by using the tool Cain and Abel / wireshark / tcpdump
7	Perform an Experiment how to use DumpSec.
8	Perform an wireless audit of an access point / router and decrypt WEP and WPA (softwares netstumbler or airsniff)
9	Perform an experiment to sniff traffic using ARP poisoning
10	Install IPCop on a linux system and learn all the function available on the software.
11	Install JCrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures studied in theory Network Security and Management
12	Demonstrate Intrusion Detection System (IDS) using any tool eg. Snort or any other s/w
13	Install RootKits and study variety of opt
14	Generate minimum 10 passwords of length 12 characters using open ssl command
15	Setup a honey pot and monitor the honey pot on network

EXPT NO 1: LEARN TO INSTALL VIRTUAL BOX/ OR ANY OTHER EQUIVALENT S/W ON THE HOST OS.

Oracle VM VirtualBox is an x86 virtualization software package, created by software company Innotek GmbH, purchased by Sun Microsystems, and now developed by Oracle Corporation as part of its family of virtualization products. Oracle VM VirtualBox is installed on an existing host operating system as an application; this host application allows additional guest operating systems, each known as a *Guest OS*, to be loaded and run, each with its own virtual environment.

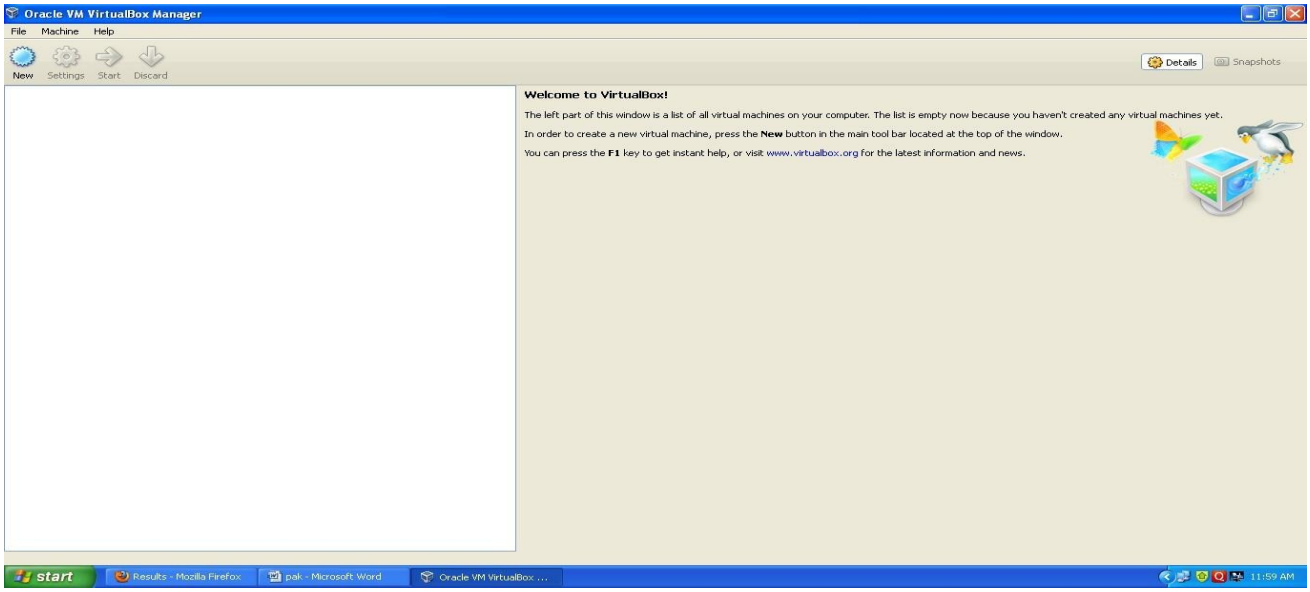
Virtualization is the creation of a virtual version of something, such as an operating system, a server, a storage device or network resources.

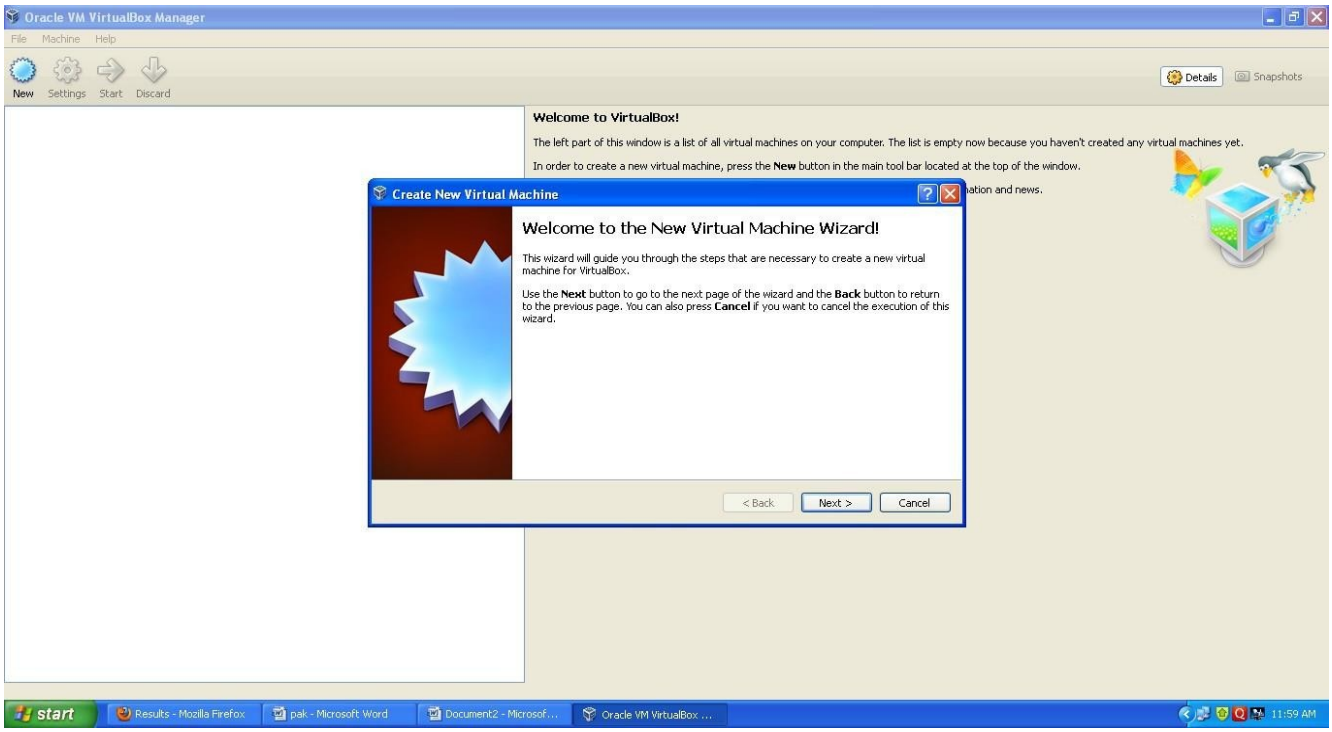
A host operating system (OS) is the original OS installed on a computer. Other operating systems are sometimes installed on a computer.

A guest OS is an operating system that is installed in a virtual machine or disk partition in addition to the host or main OS. In virtualization, a single computer can run more than one OS at the same time. In a virtualization solution, a guest OS can be different from the host OS.

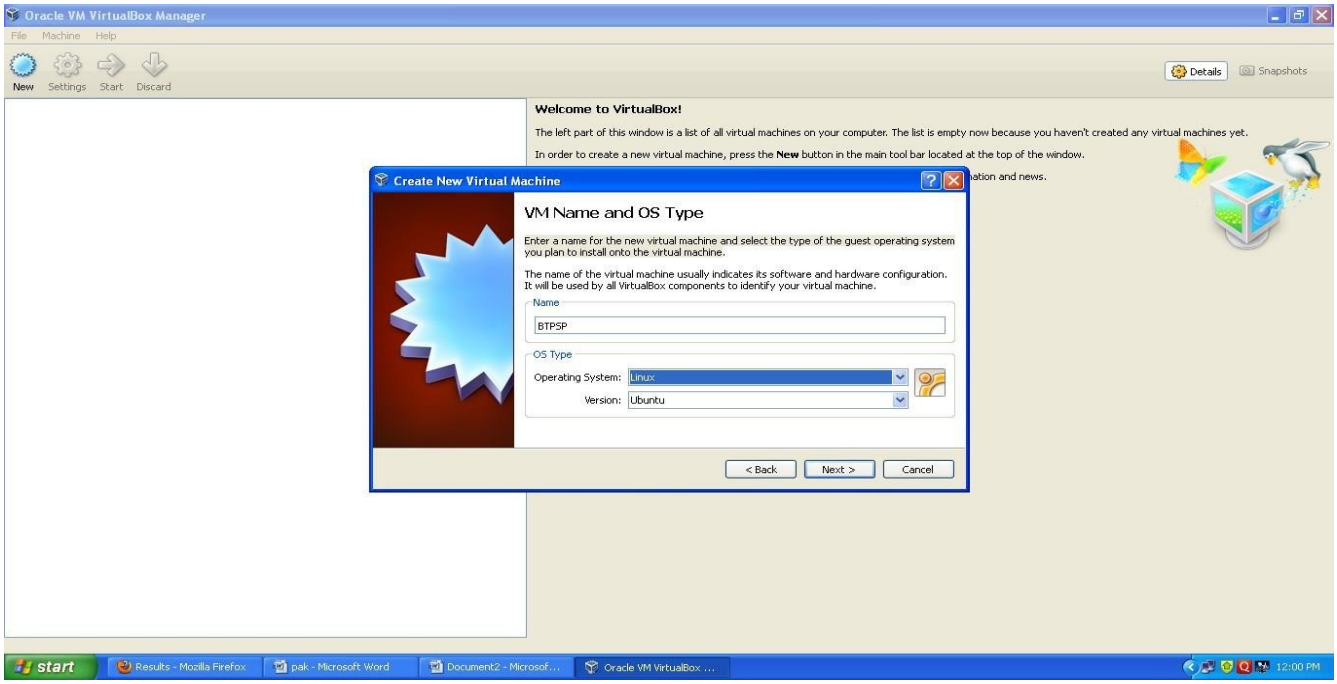
Steps:

1. Download & install virtual box.

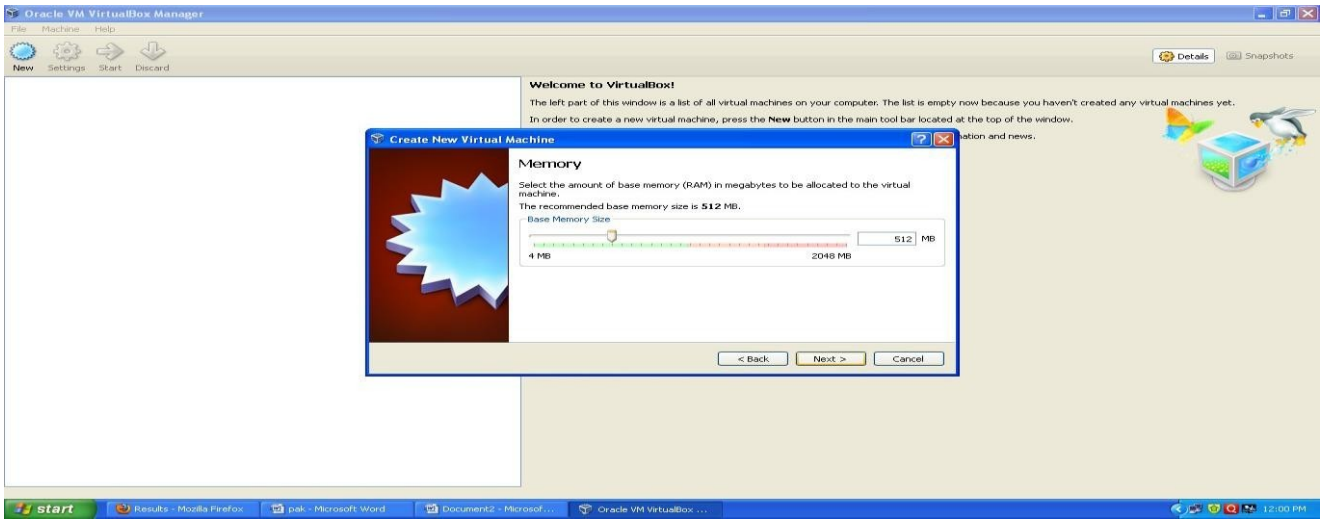




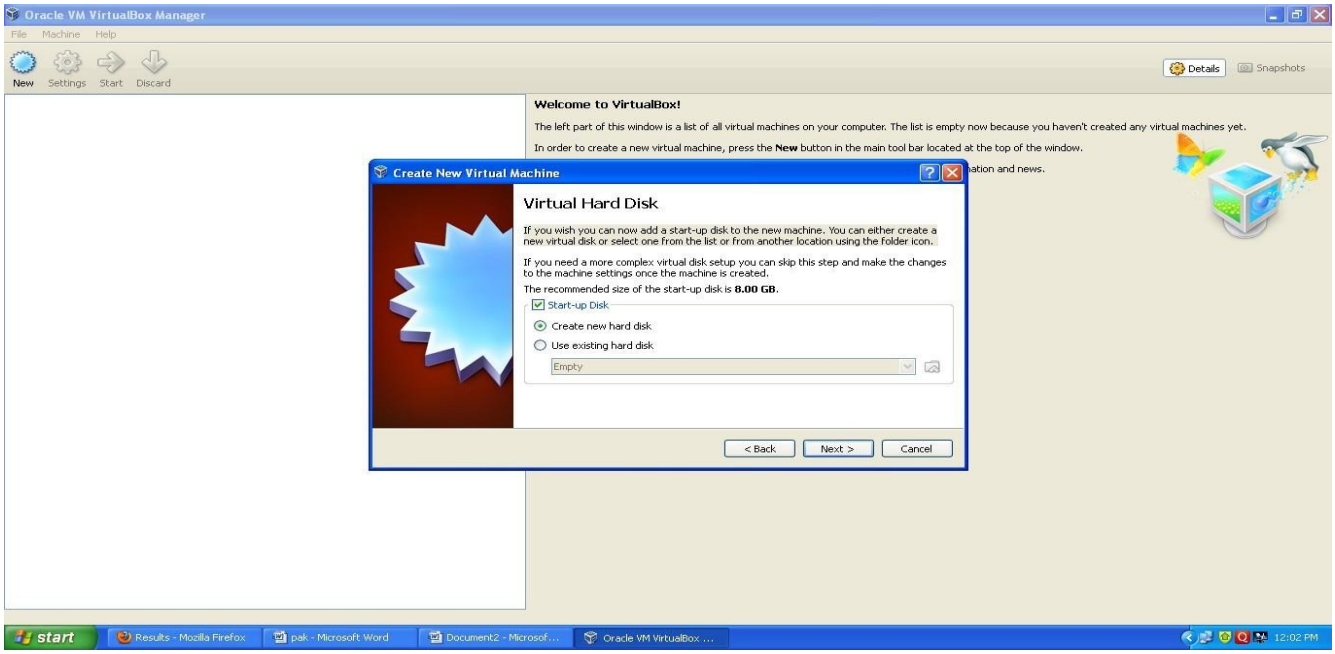
2. Enter a name for the new virtual machine and select the type of the guest operating system you plan to install onto the virtual machine.

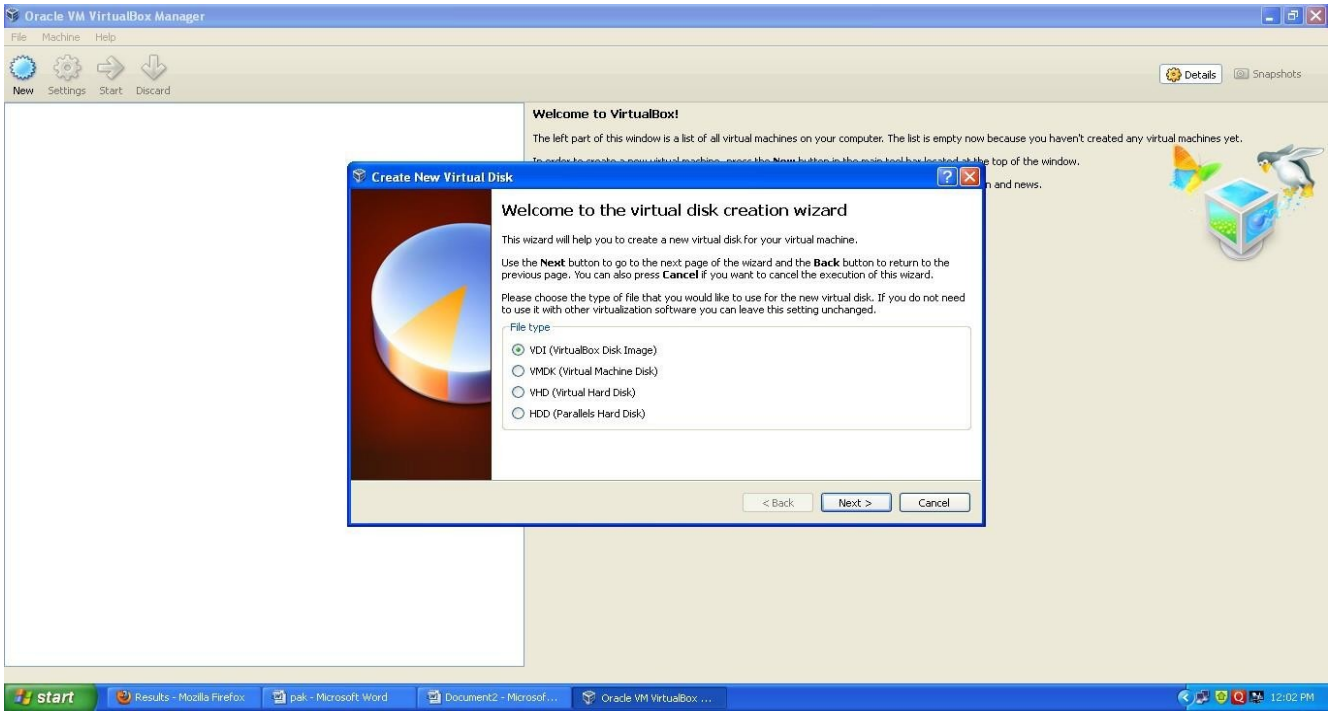


3. Select the amount of base memory (RAM) in megabytes to be allocated to the virtual machine

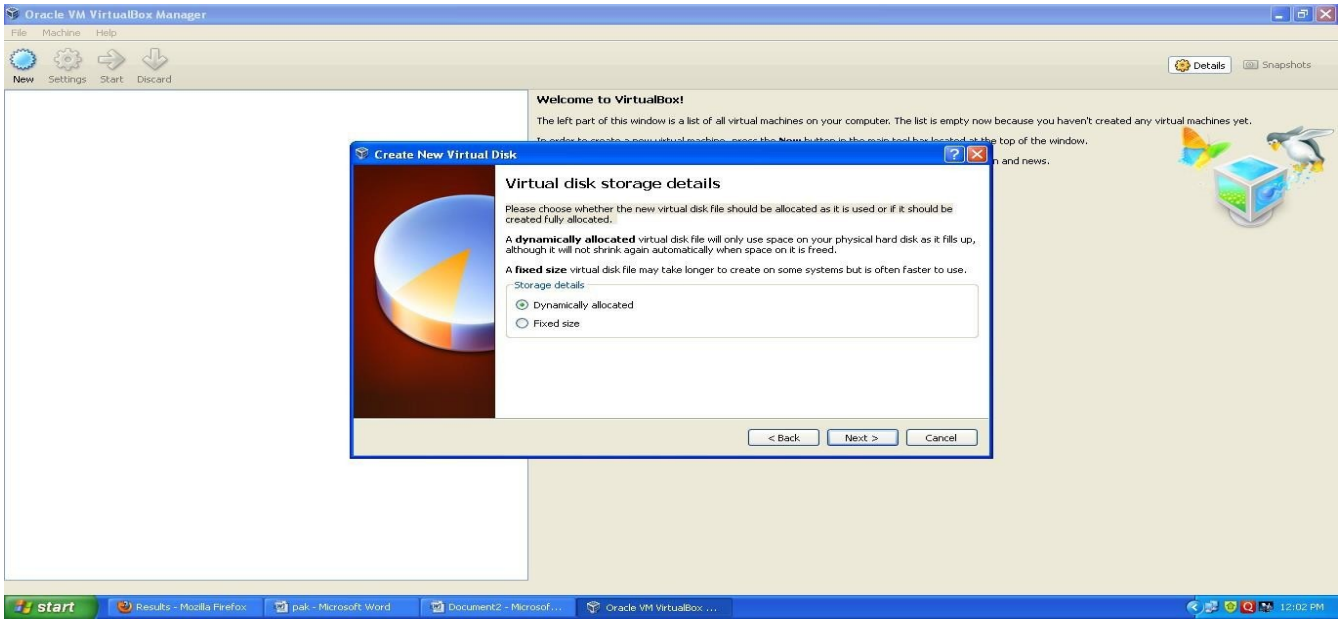


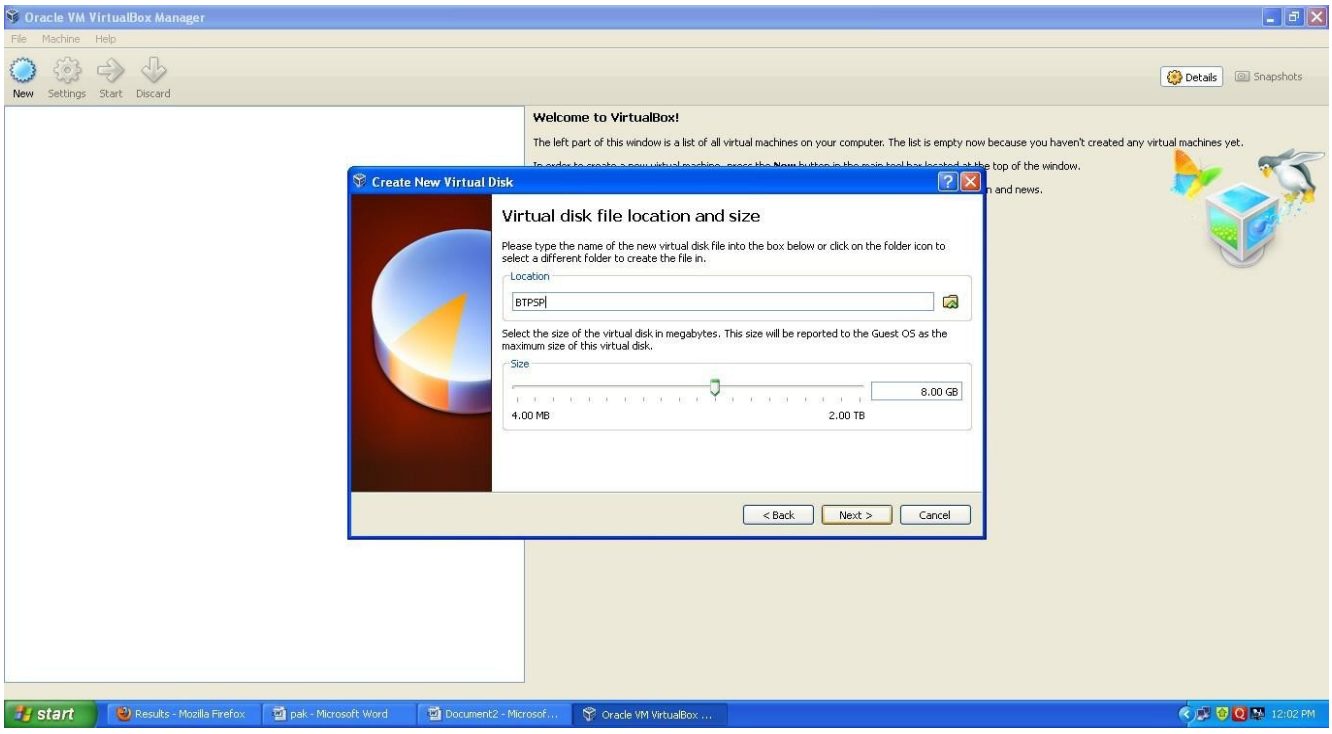
4. If you wish you can now add a start-up disk to the new machine. You can either create a new virtual disk or select one from the list or from another location using the folder icon.





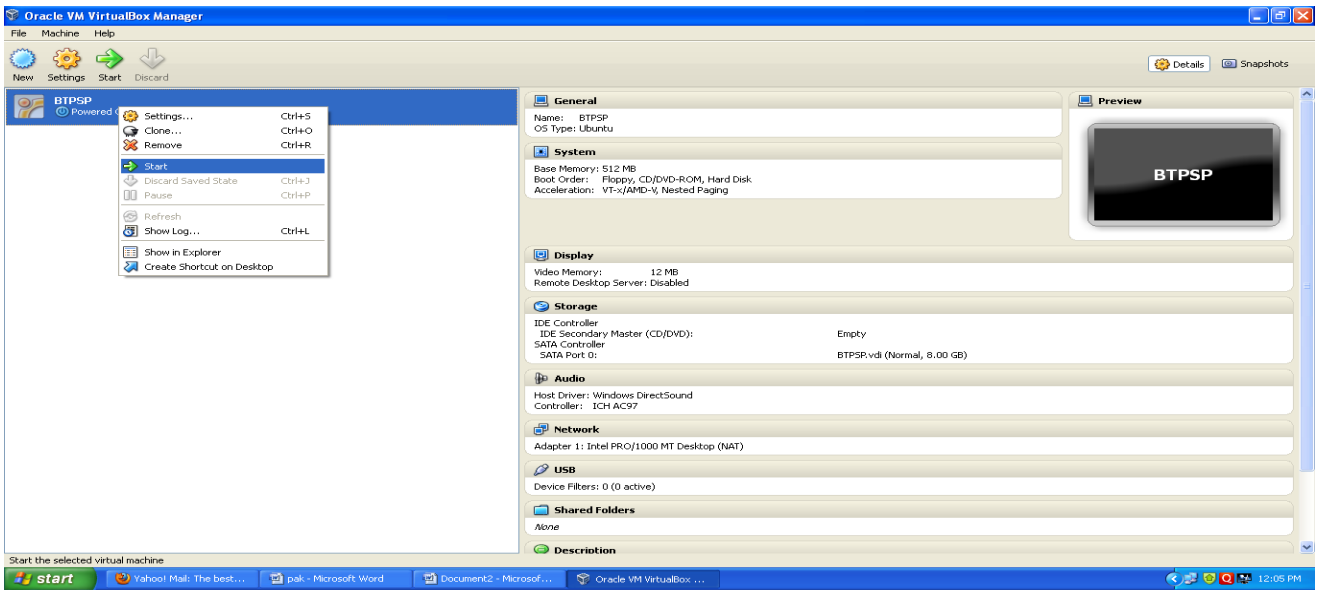
5. Please choose whether the new virtual disk file should be allocated as it is used or if it should be created fully allocated.



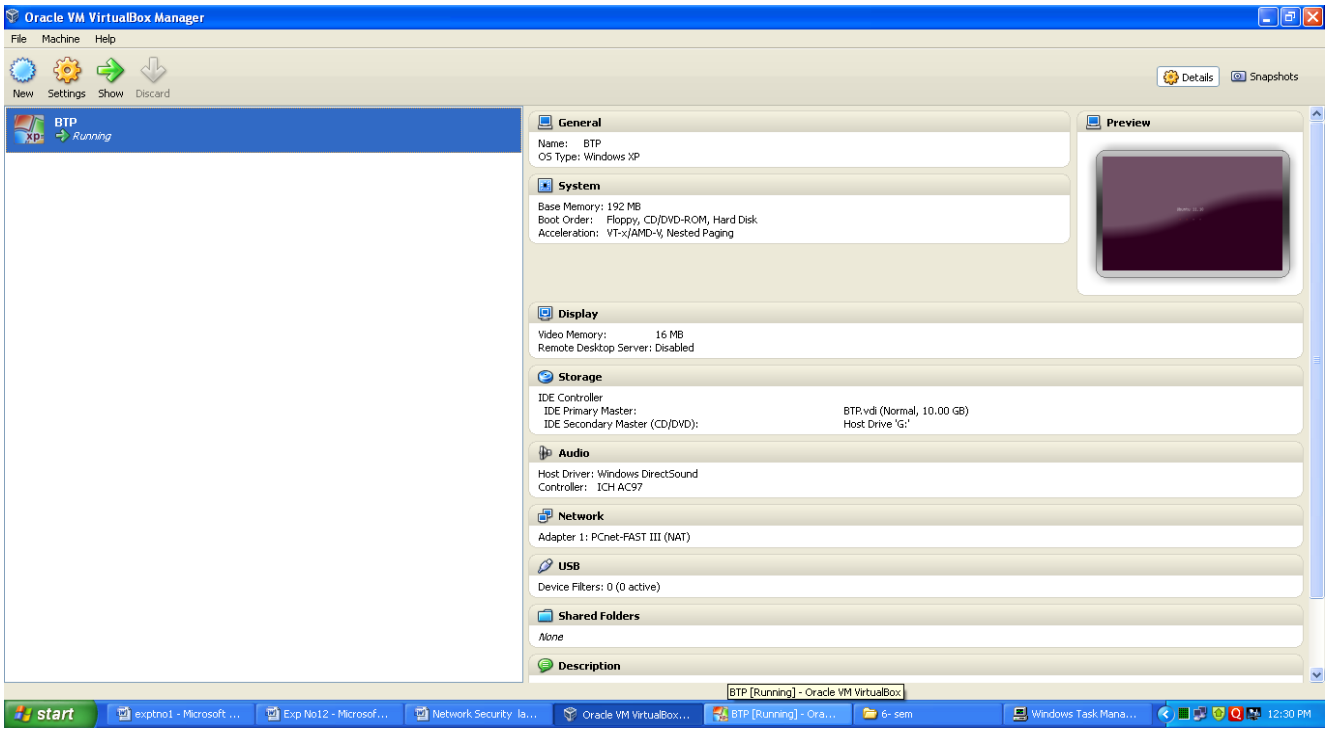


6. After creating virtual machine start the machine and install another OS

7. Right click on the v machine and click start



8. Insert bootable CD into drive. Automatically installation will start as follows.



EXPT NO 2: PERFORM AN EXPERIMENT TO GRAB A BANNER WITH TELNET AND PERFORM THE TASK USING NETCAT UTILITY.

Banner Grabbing

Banner grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Administrators can use this to take inventory of the systems and services on their network. Tools commonly used to perform banner grabbing are Telnet, which is included with most operating systems, and Netcat.

What is Telnet?

Telnet is a user command and an underlying CP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

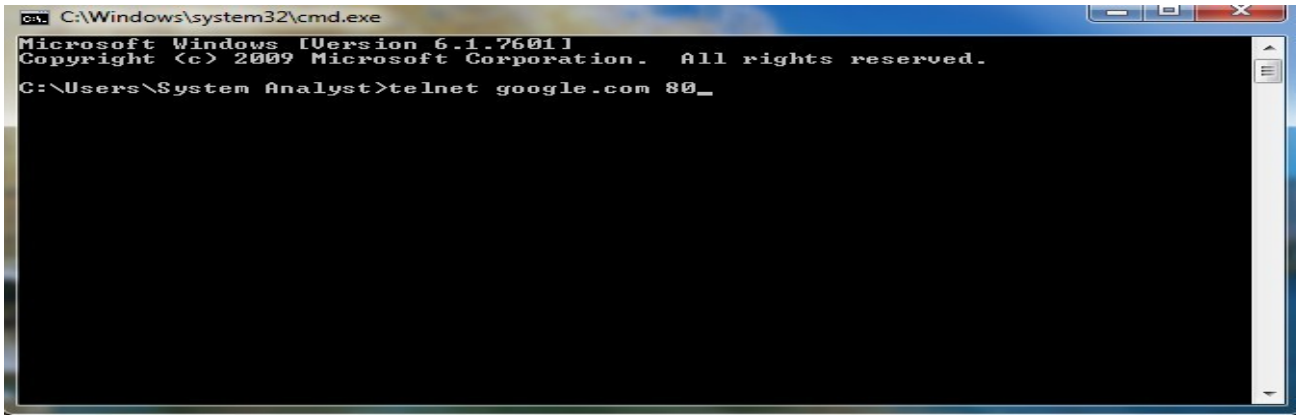
Steps for Banner Grabbing using Telnet:

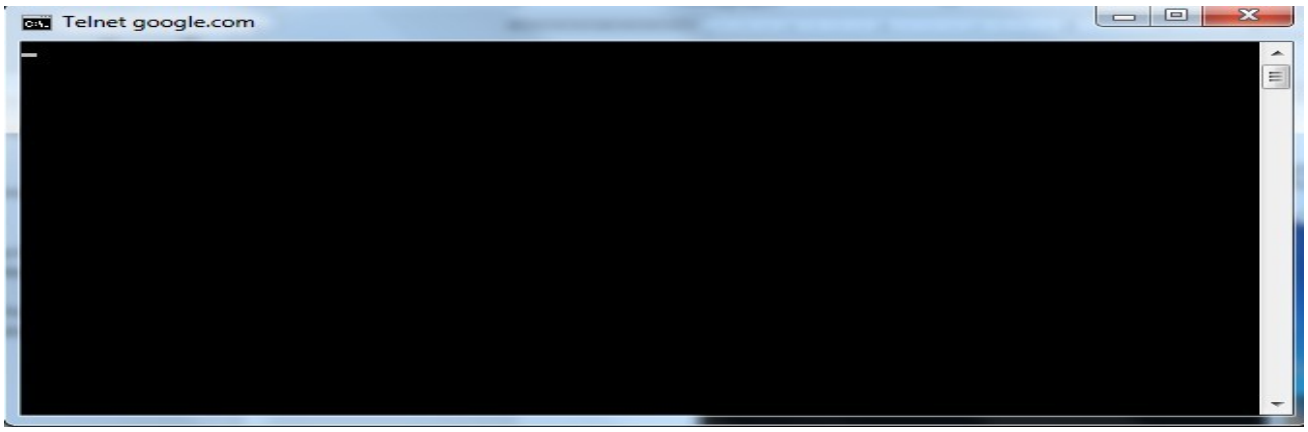
Steps:

1. Go to Command prompt
2. Type telnet followed by IP Address

Example:

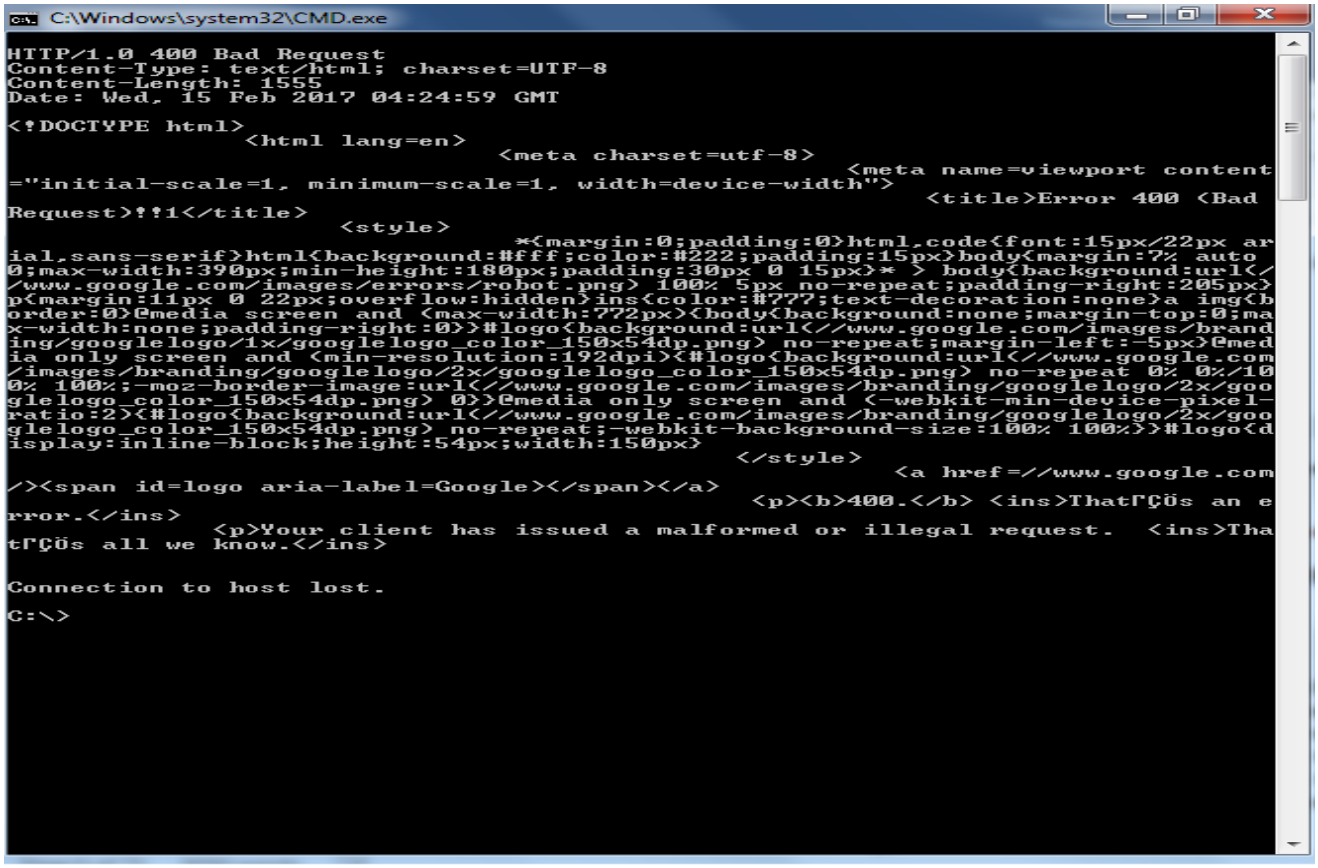
As an example lets see if Google.com has port 80(HTTP) open…



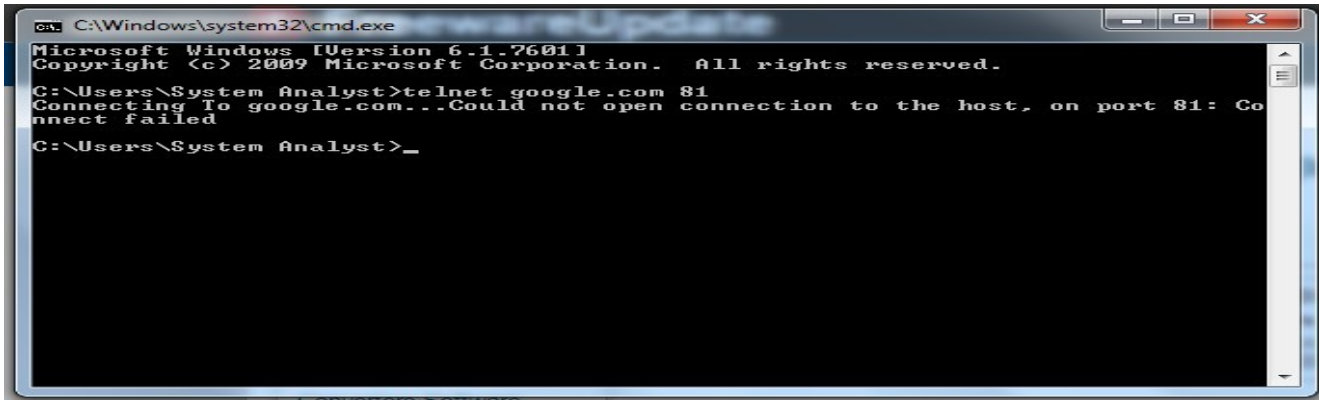


3. If you get a blank screen with a blinking cursor you have successfully connected to that TCP port.

4. Now type following GET HTTP and press enter and you will see Google's homepage being sent to you.



On the other hand if the TCP port is not open or not reachable you will see this: 0



Steps for Banner Grabbing using Netcat:

Netcat: Netcat is a featured networking utility which reads and writes data across n/w connections, using the TCP/IP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts.

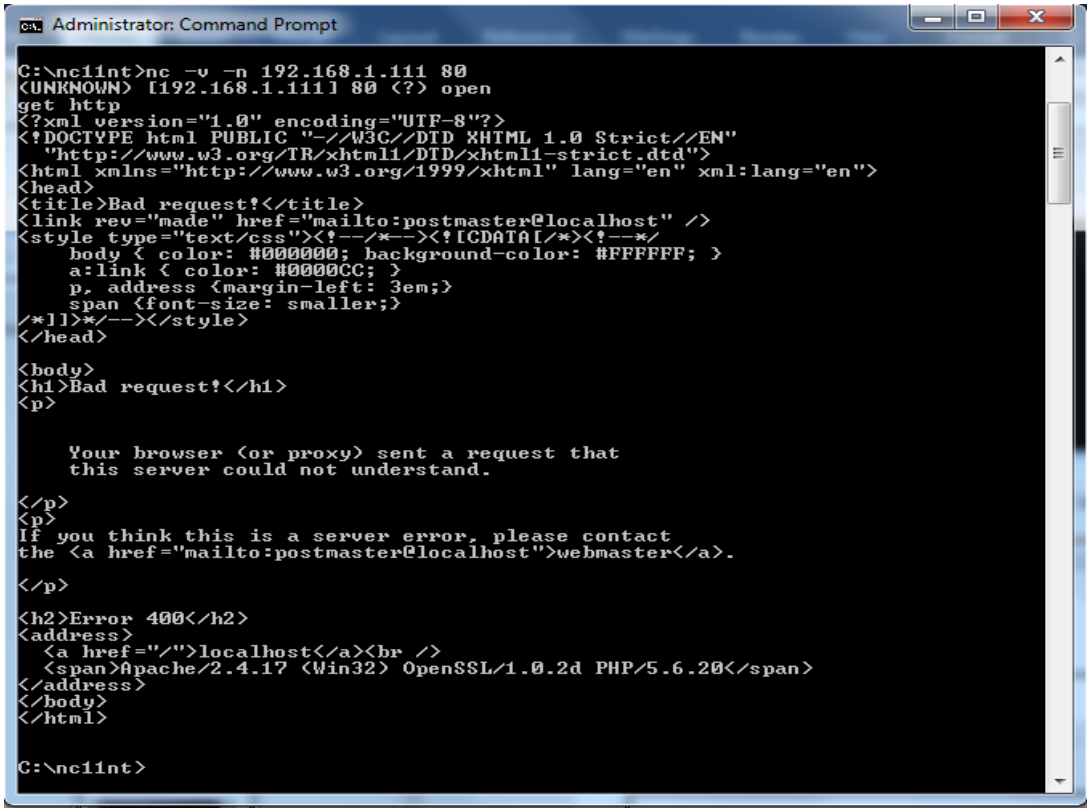
Netcat command options:

1. -e prog inbound program to exec [dangerous!!]
2. -i secs delay interval for lines sent, ports scanned
3. -n numeric only IP address,no DNS
4. -o file hex dump of traffic
5. -p port local port number
6. -r randomize local and remote ports
7. -s addr local source address
8. -t answer TELNET negotiation
9. -u UDP mode
10. -v verbose [use twice to be more verbose]

Steps:
How to work with Netcat:

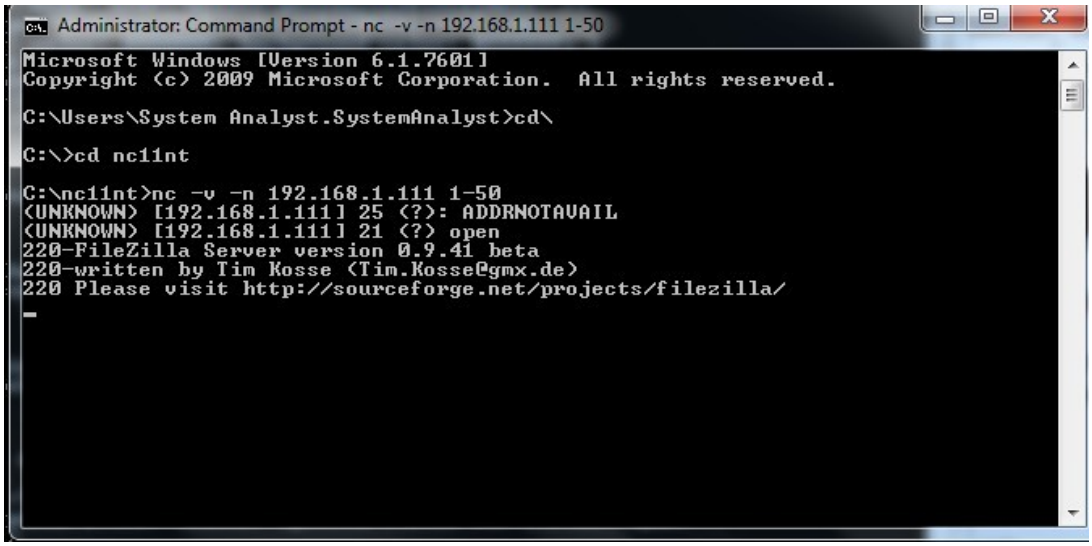
1.Go the command prompt
2.Copy the folder nc11nt to c:/from the netcat
s/w 3.In (c:\nc11nt\)
4.Type nc -v -n 192.168.1.111 80
5.You will get a blinking cursor that you have successfully connected to that TCP port.
6.Type **GET HTTP.**

We can see the details of our target web server.



Example 2:

C:\nc11nt\nc -v -n 192.168.1.111 1-50



EXPT NO 3: PERFORM AN EXPERIMENT FOR PORT SCANNING WITH NMAP, SUPERSCAN OR ANY OTHER EQUIVALENT SOFTWARE

Port Scanning

Port scanning is the process of connecting to TCP and UDP ports for the purpose of finding which services and applications are open on the target device.

Port Scanning is one of the most popular techniques attackers use to discover services they can break into. All machines connected to a LAN or connected to Internet via a modem run many services that listen at well-known and not so well-known ports. By port scanning the attacker finds which ports are available (i.e., being listened to by a service). Essentially, a port scan consists of sending a message to each port, one at a time.

Port Numbers

The port numbers are unique only within a computer system. Port numbers are 16-bit unsigned numbers. The port numbers are divided into three ranges: the Well Known Ports (0..1023), the Registered Ports (1024..49151), and the Dynamic and/or Private Ports (49152..65535).

Well-Known Ports

All the operating systems now honor the tradition of permitting only the super- user open the ports numbered 0 to 1023. These well-known ports (also called standard ports) are assigned to services by the IANA (Internet Assigned Numbers Authority, www.iana.org).

Here are a few lines extracted from this file:

echo	7/tcp	Echo
ftp-data	20/udp	File Transfer [Default Data]
ftp	21/tcp	File Transfer [Control]
ssh	22/tcp	SSH Remote Login Protocol
telnet	23/tcp	Telnet
domain	53/udp	Domain Name Server
www-http	80/tcp	World Wide Web HTTP

NMAP

Nmap is one of the most well-known port scanning tools. Nmap is available for windows and Linux as a GUI and command-line program and has ready availability of documentation, and because of the way in which the tool has been developed and maintained. You can download Nmap from http://insecure.org/nmap/download.html

Scan option	Name	Description
-sS	TCP SYN	Stealth scan

-sT	TCP Full	Full connect
-sF	FIN	Typically no reply from open ports
-sN	NULL	No flags are set
-sX	Xmas	URG,PUSH, and FIN flags are set
-sP	Ping	Performs a ping sweep
-sU	UDP Scan	Performs a Null scan
-SA	ACK	Performs an ACK scan

Port scanning with Nmap

Step 1: Install Nmap into a windows directory that is in the command path so that you can run it easily from the command line regardless of the folder in which you are located.

From the command line, enter the following:

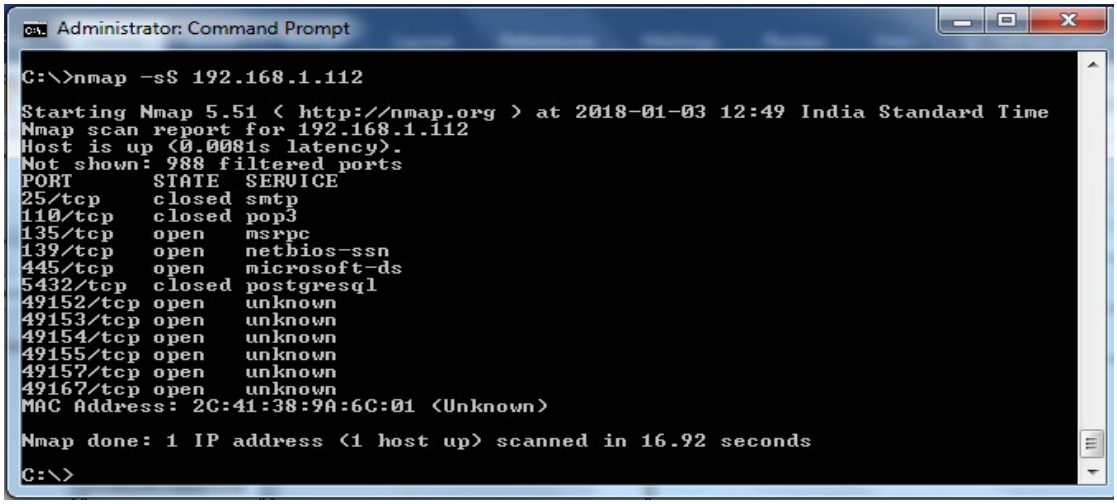
a.)C:\nmap -h

This will provide you with a listing of the command syntax of Nmap and some of the types of scans it can perform.

b.)Syntax:Nmap -sP <IP address>

EX:Nmap -sP 192.168.1.112

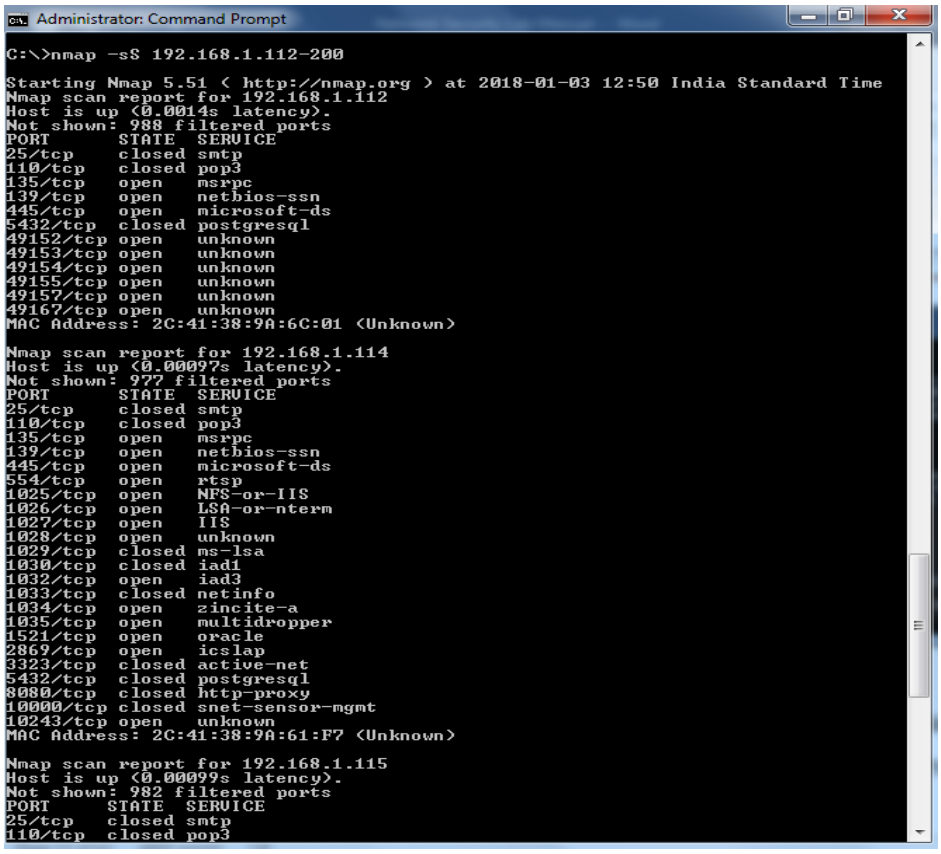
Enter an IP address that is within your network and that you have permission to scan. If you are not sure what the -sP switch (option) does,you may want to look back over the results of



Step 2:

Scanning range of IP address

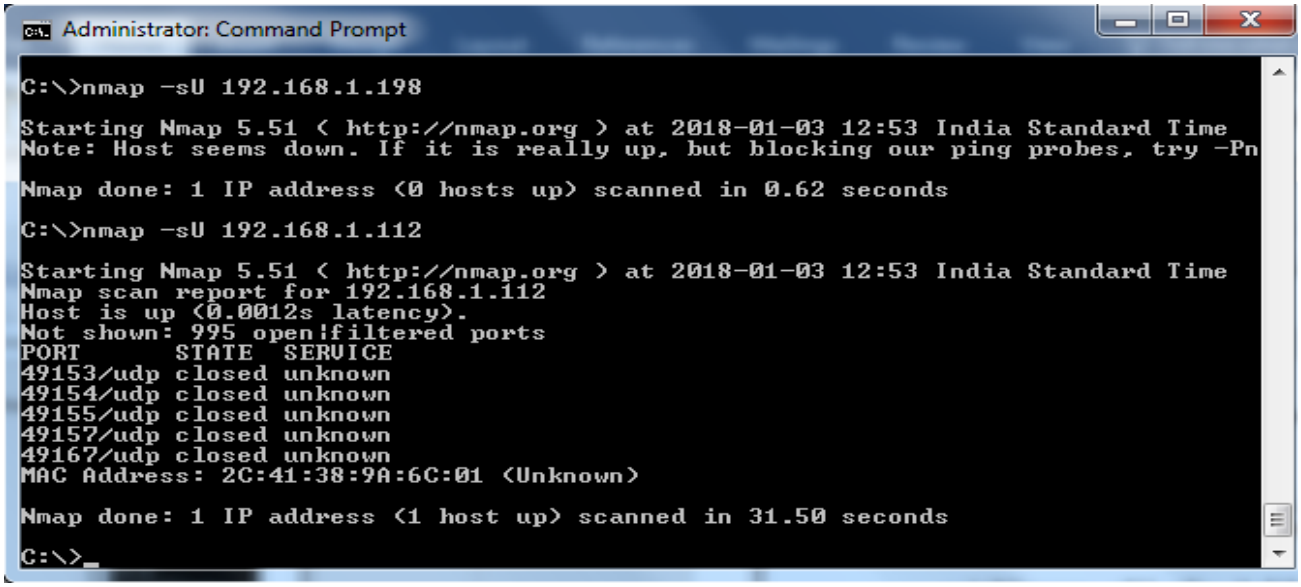
C:\Nmap -sS 192.168.1.112-200



c.) Nmap -sU <Ip Address>

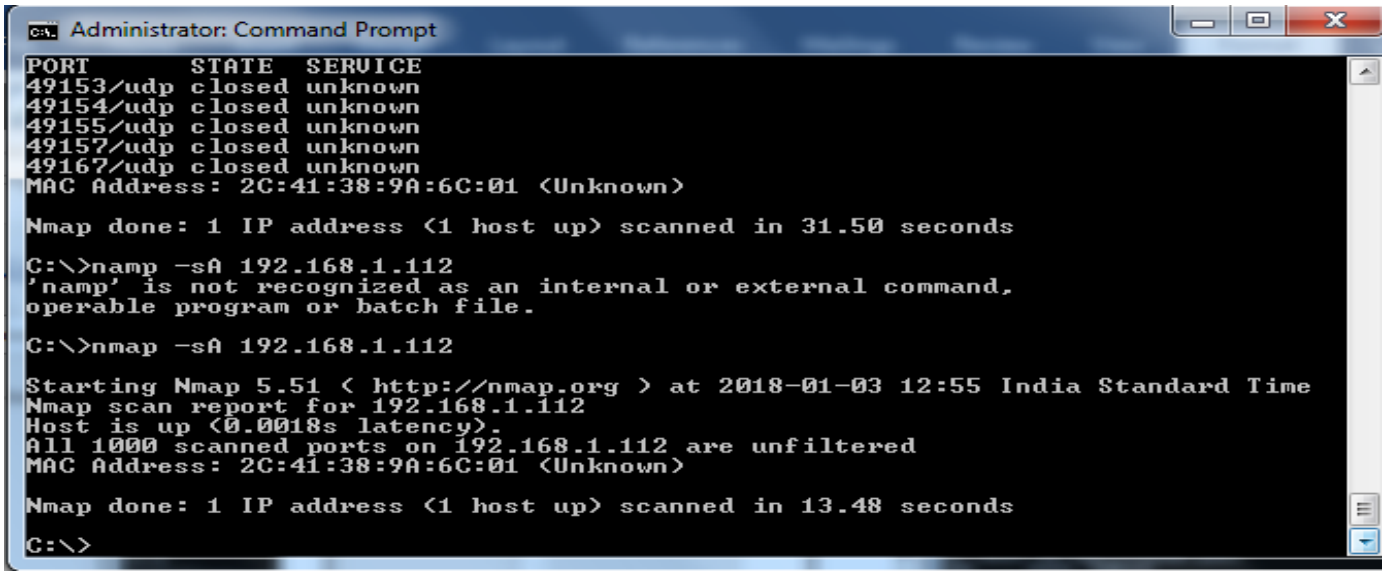
Ex:nmap -sU 192.168.1.112

Remember that the -sU is a UDP scan,so the results may be as detailed as what was returned from TCP scans



d.) Syntax: Nmap -sA <IP Address>

Ex: Nmap -Sa 192.168.1.112



This type of scan is sometimes used to deal with routers that have ACL's applied.

Superscan

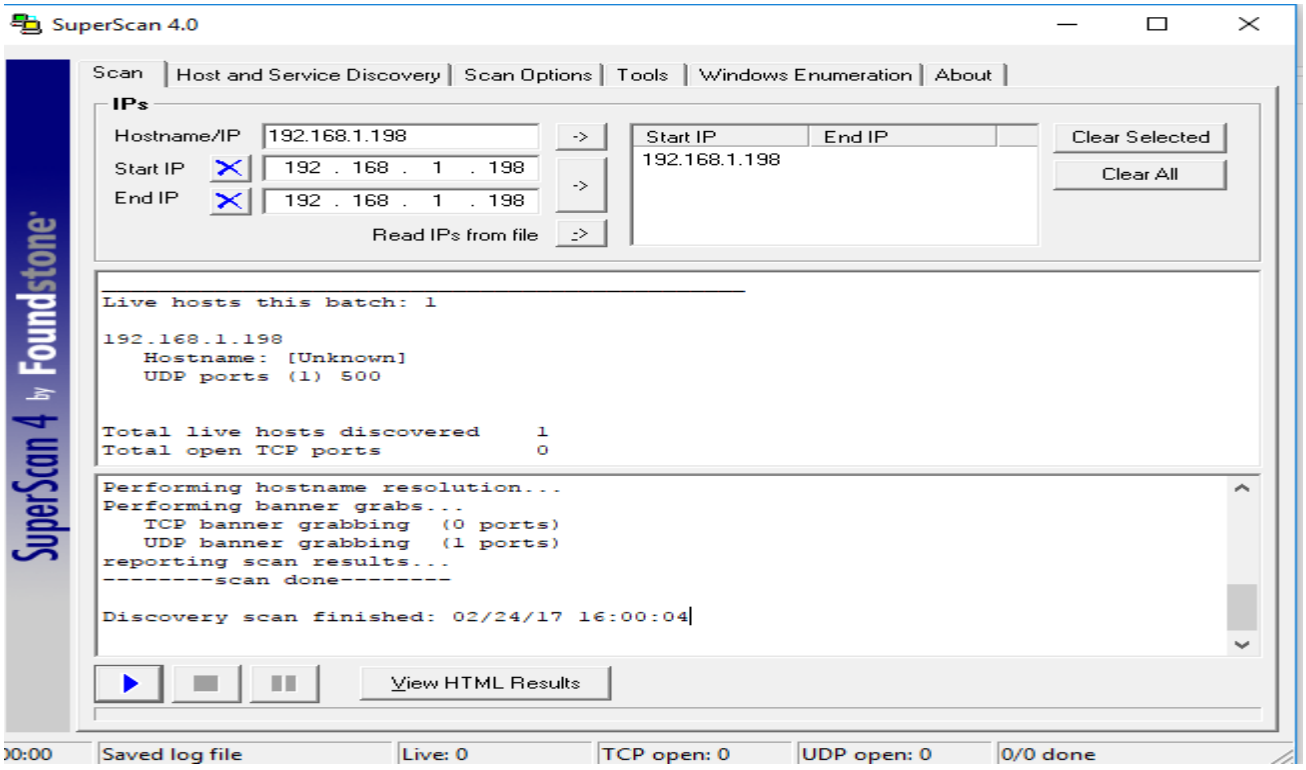
Superscan is a windows GUI-based scanner developed by Foundstone.It will scan TCP and UDP ports and perform ping scans.It will allow you to scan all ports, use a built-in list of defined ports, or specify the port range. For the price (its free), it offers great features if you are looking for a windows GUI scanner.

Port scanning with Superscan

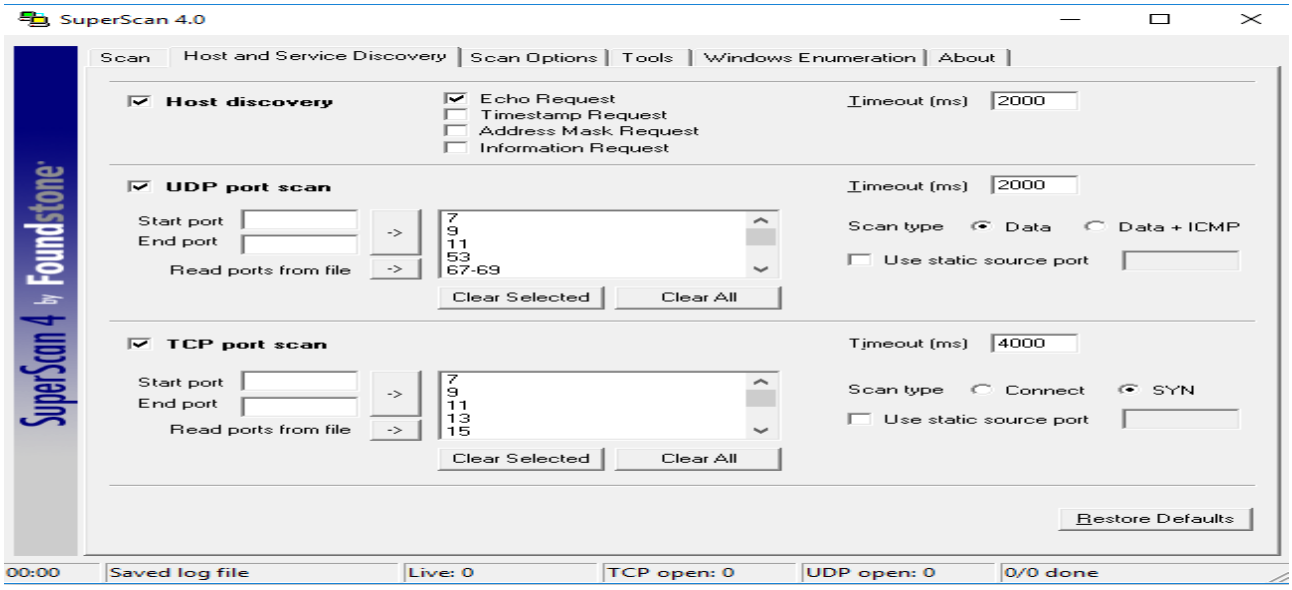
The exercise steps you through a port scanning with a GUI tool. The scanning tool that is used is Superscan. You can download Superscan from www.snapfiles.com/get/superscan.html

Step 1: After downloading , go to start → programs → system tools → superscan to start the program. The program interface will appear and look similar to Figure 4.10

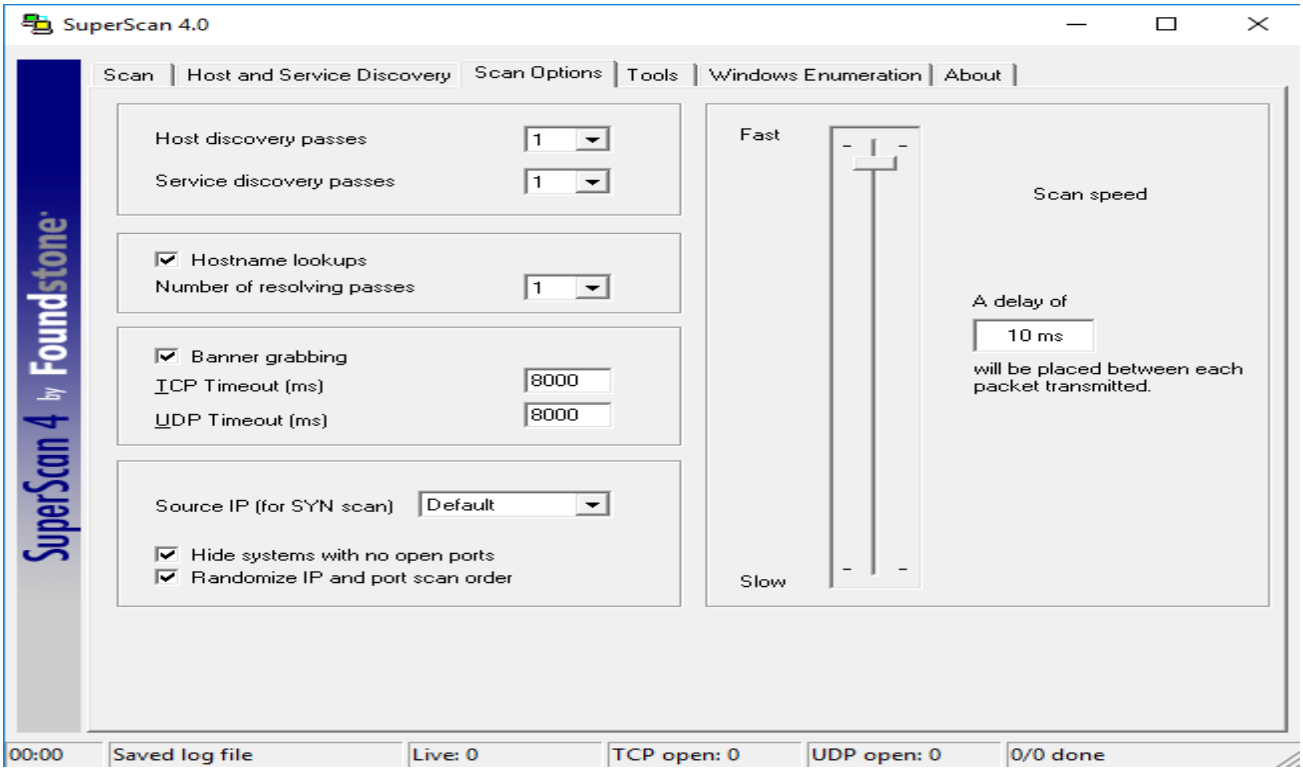
Step 2: Enter a starting and ending IP address range to scan and press the > button.



Step 3: Click the Host and Service Discovery tab. Details will appear as shown in Figure below.=



Step 4: Leave the default settings as shown in Figure above. Now, examine the scan options tab.

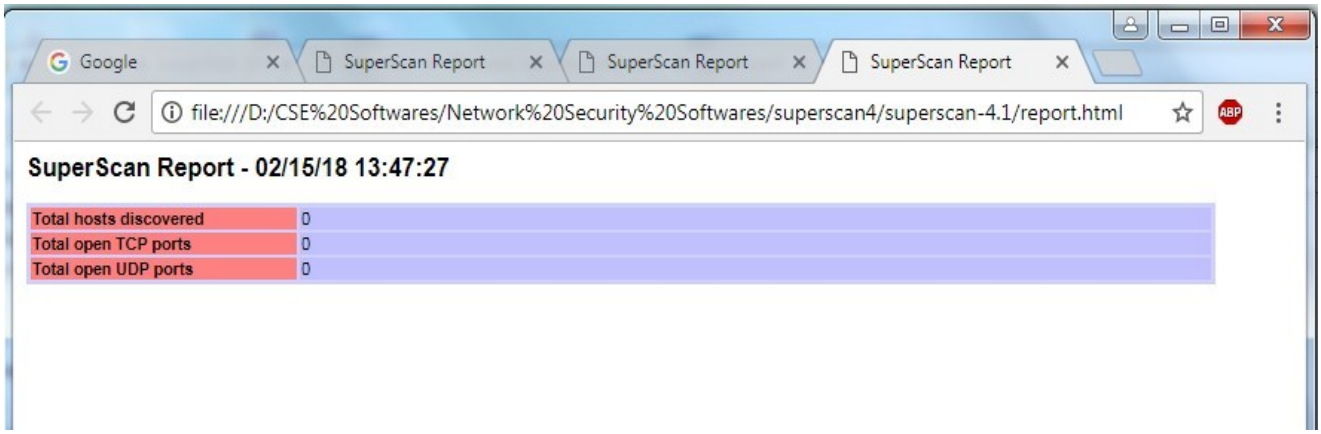


Step 5: Notice the scan options shown in Figure above. Leave the scan options set as 1ms to perform a fast scan.

Step 6: Click the start button, shown in the bottom of Figure 1. Allow the scan sometime complete.

Step 7: When the scan is complete, click Generate HTML report. A report will be generated, as shown in Figure 4-13.

Step 8. This report can be used to examine open services and determine which ports and services can be further locked down and secured. It can also help identify that only approved applications and services are running on the network.



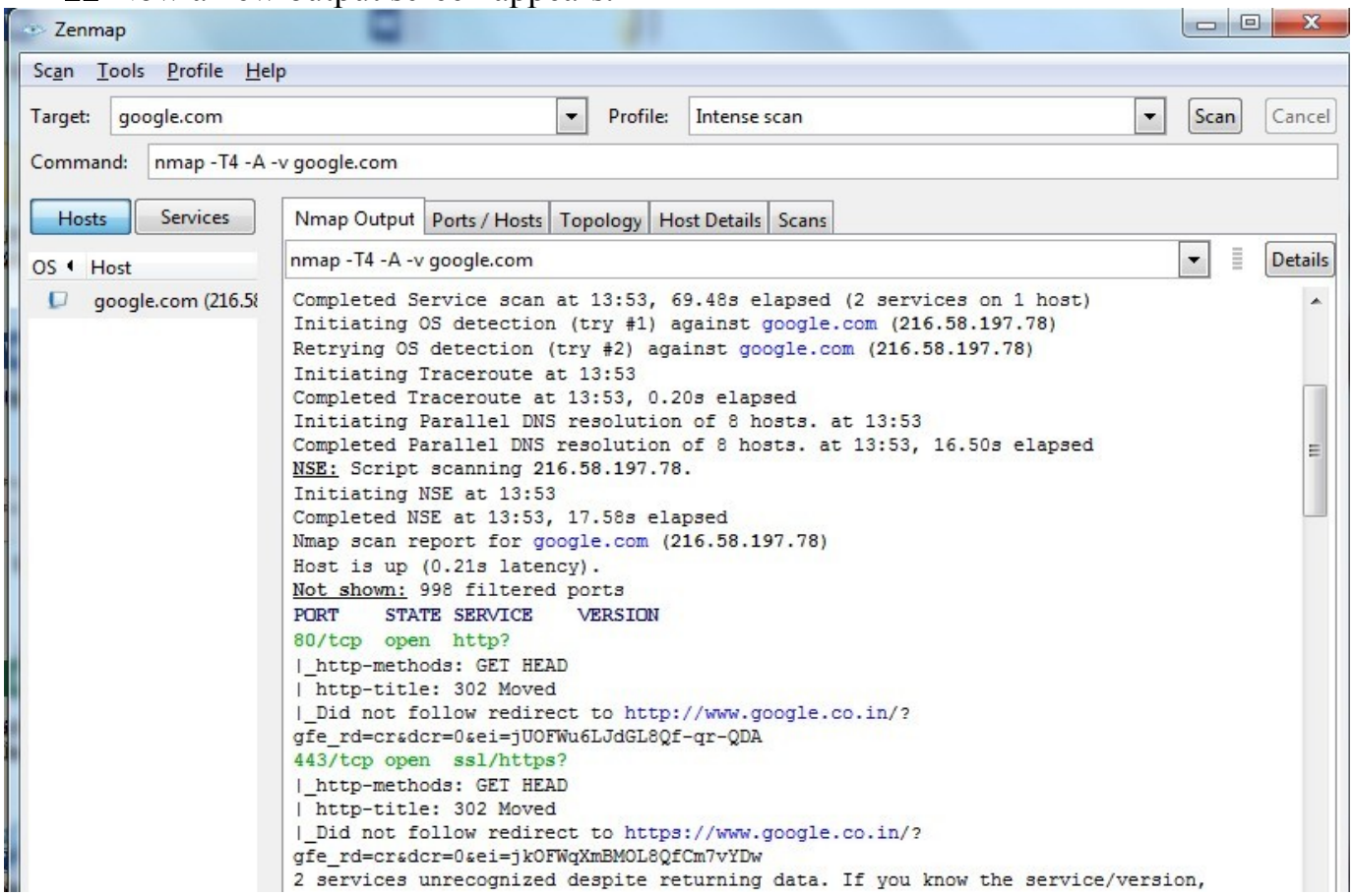
EXPT NO 4: USING NMAP
1) FIND OPEN PORTS ON A SYSTEM
2) FIND MACHINES WHICH ARE ACTIVE
3) FIND THE VERSION OF REMOTE OS ON OTHER SYSTEMS
4) FIND THE VERSION OF S/W INSTALLED ON OTHER SYSTEM

Steps:

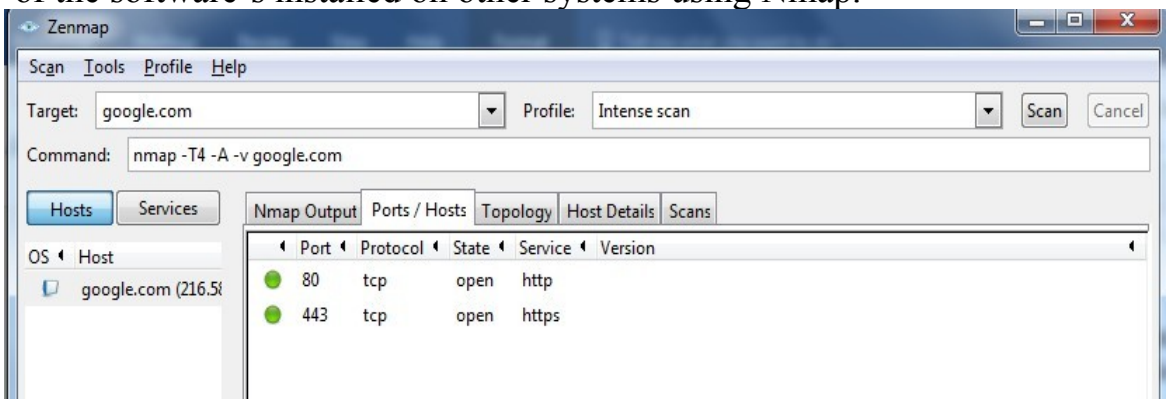
- First download Nmap and install the nmap software.

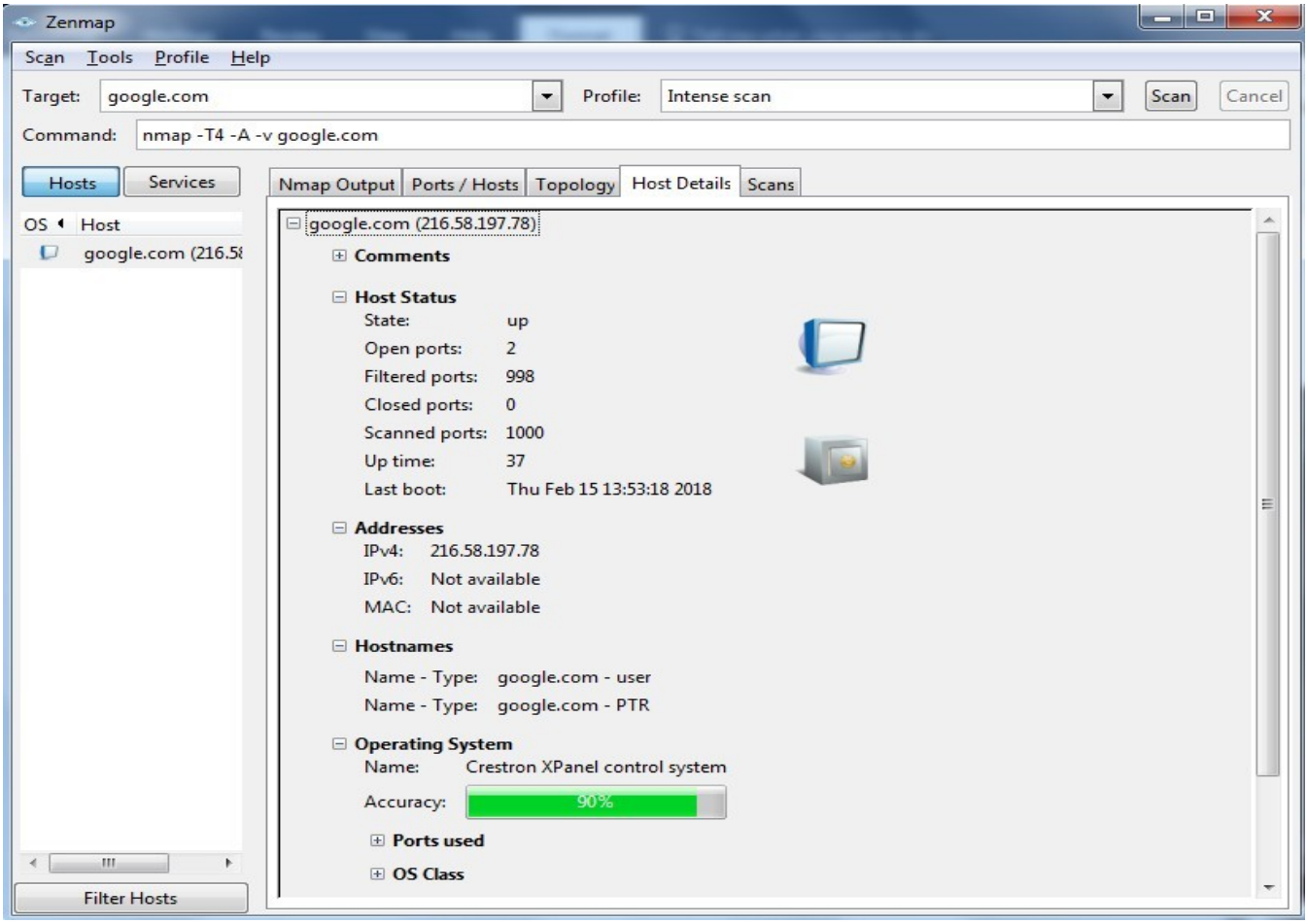
<u>These steps shown on GUI mode</u>

- Now open the Nmap software by clicking the start → All programs → Nmap → Nmap – Zenmap GUI
- Now the Zenmap screen opens.
- Now type the target IP Address: 216.58.197.78 or google.com & In Profile: use the Intense scan & start scan process by clicking the scan tab.
- Now a new output screen appears.



- Now click on Host details and we can find the open ports of the system, machines which are active, the version of the remote OS on the other systems and the version of the software's installed on other systems using Nmap.

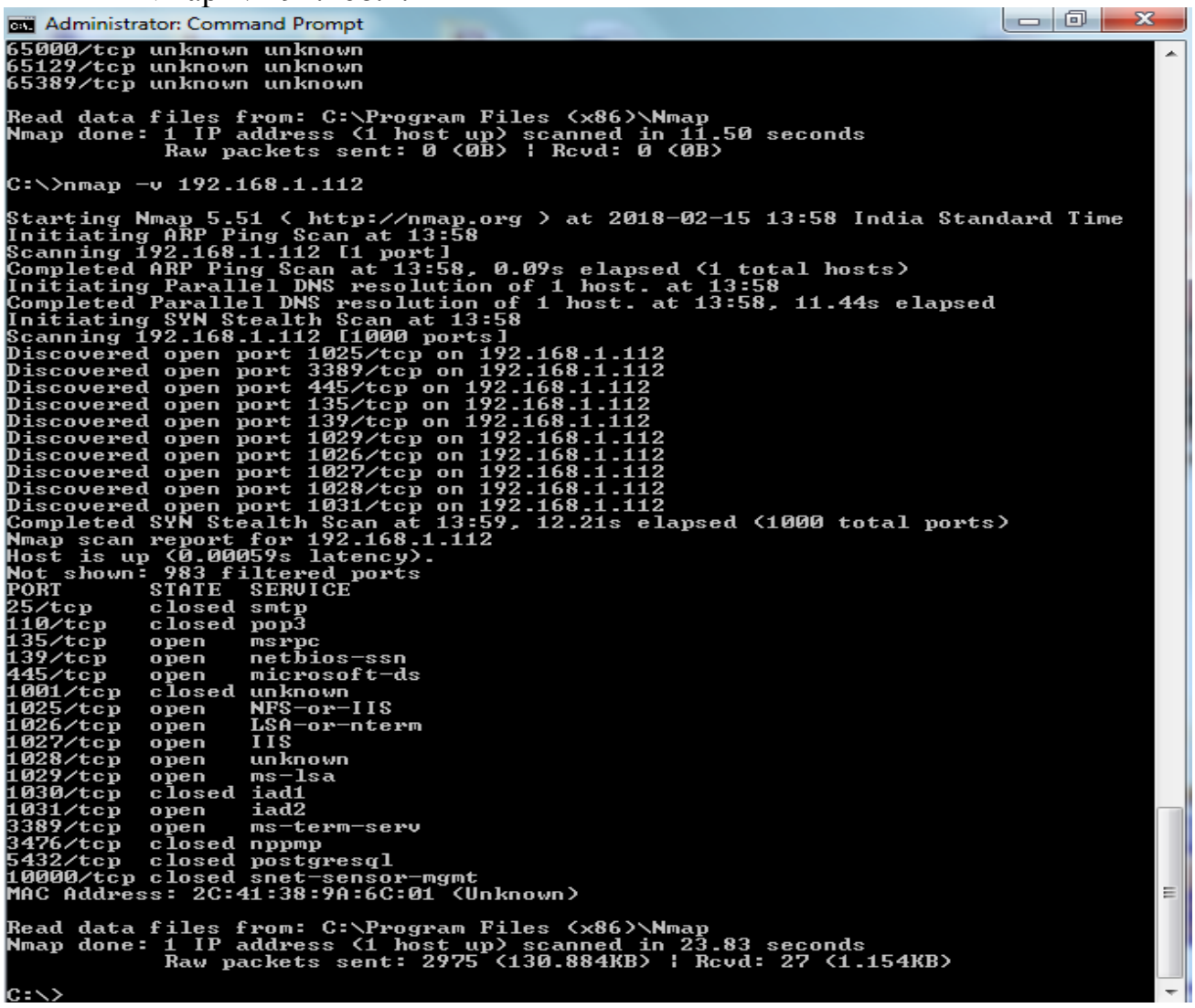




These steps shown on DOS mode

Steps:

1. After the installation of the Nmap, open the terminal and enter the following command.
2. Find open ports on a system
   Nmap -v 192.168.1.112



3. Find machine which are active in the network.
   Nmap -sP 192.168.1.198-253

```
C:\>nmap -sP 192.168.1.198-253

Starting Nmap 5.51 ( http://nmap.org ) at 2018-02-15 14:01 India Standard Time
Nmap scan report for 192.168.1.201
Host is up (0.0010s latency).
MAC Address: 2C:41:38:9A:6D:A4 (Unknown)
Nmap scan report for 192.168.1.215
Host is up (0.0010s latency).
MAC Address: 60:02:92:24:01:14 (Unknown)
Nmap scan report for 192.168.1.216
Host is up (0.0010s latency).
MAC Address: 60:02:92:24:01:56 (Unknown)
Nmap scan report for 192.168.1.225
Host is up (0.00s latency).
MAC Address: 60:02:92:24:01:51 (Unknown)
Nmap scan report for 192.168.1.226
Host is up (0.0010s latency).
MAC Address: 60:02:92:24:00:32 (Unknown)
Nmap scan report for 192.168.1.227
Host is up (0.00s latency).
MAC Address: A0:8C:FD:F3:C3:2F (Unknown)
Nmap scan report for 192.168.1.248
Host is up (0.0020s latency).
MAC Address: 2C:41:38:9A:73:0E (Unknown)
Nmap scan report for 192.168.1.251
Host is up (0.0040s latency).
MAC Address: 90:8D:78:04:C2:E3 (Unknown)
Nmap done: 56 IP addresses (8 hosts up) scanned in 17.25 seconds

C:\>nmap -sP 192.168.1.198-253
```

4. Service and version detected by Nmap
   Nmap -sV 192.168.1.112

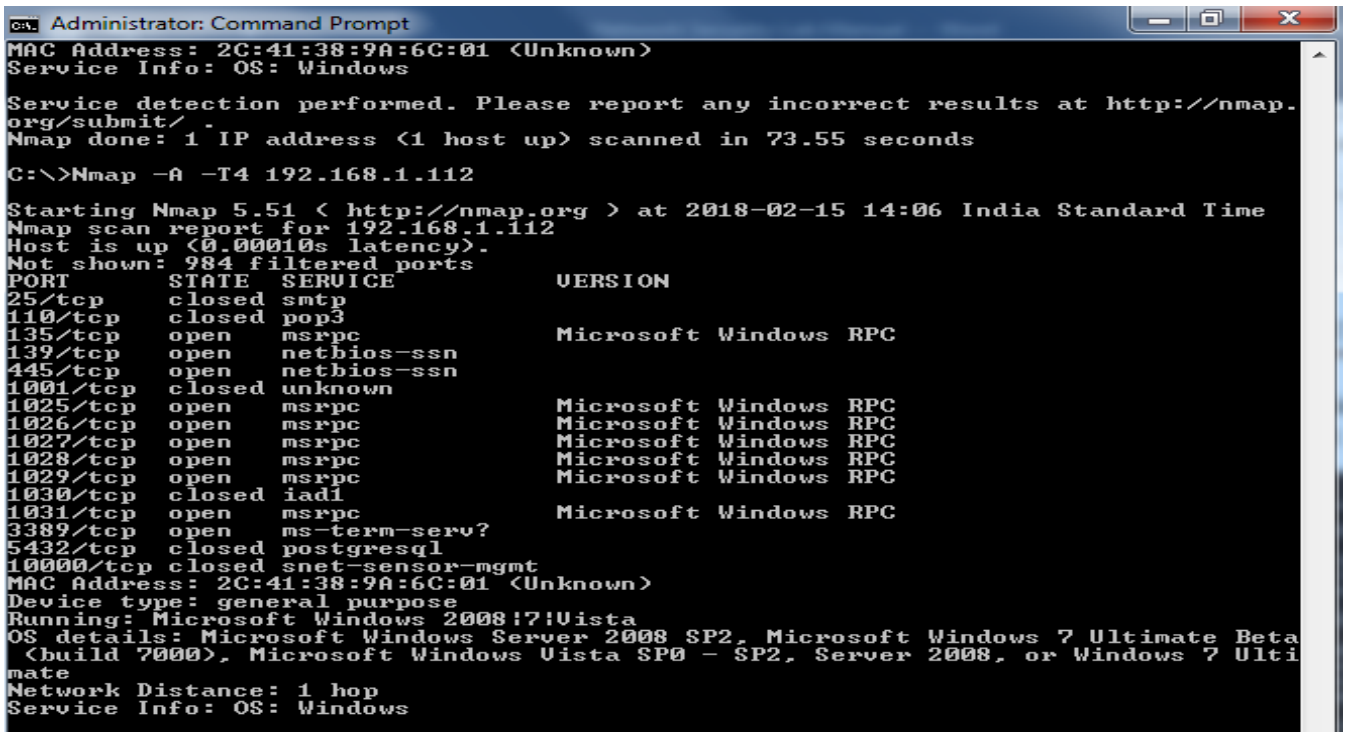
```
C:\>Nmap -sV 192.168.1.112

Starting Nmap 5.51 ( http://nmap.org ) at 2018-02-15 14:03 India Standard Time
Nmap scan report for 192.168.1.112
Host is up (0.00080s latency).
Not shown: 984 filtered ports
PORT      STATE  SERVICE          VERSION
25/tcp    closed smtp
110/tcp   closed pop3
135/tcp   open   msrpc            Microsoft Windows RPC
139/tcp   open   netbios-ssn
445/tcp   open   netbios-ssn
1001/tcp  closed unknown
1025/tcp  open   msrpc            Microsoft Windows RPC
1026/tcp  open   msrpc            Microsoft Windows RPC
1027/tcp  open   msrpc            Microsoft Windows RPC
1028/tcp  open   msrpc            Microsoft Windows RPC
1029/tcp  open   msrpc            Microsoft Windows RPC
1030/tcp  closed iad1
1031/tcp  open   msrpc            Microsoft Windows RPC
3389/tcp  open   ms-term-serv?
5432/tcp  closed postgresql
10000/tcp closed snet-sensor-mgmt
MAC Address: 2C:41:38:9A:6C:01 (Unknown)
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.55 seconds

C:\>
```

5. Find the version of software installed on the other system.
   Nmap -A -T4 192.168.1.112



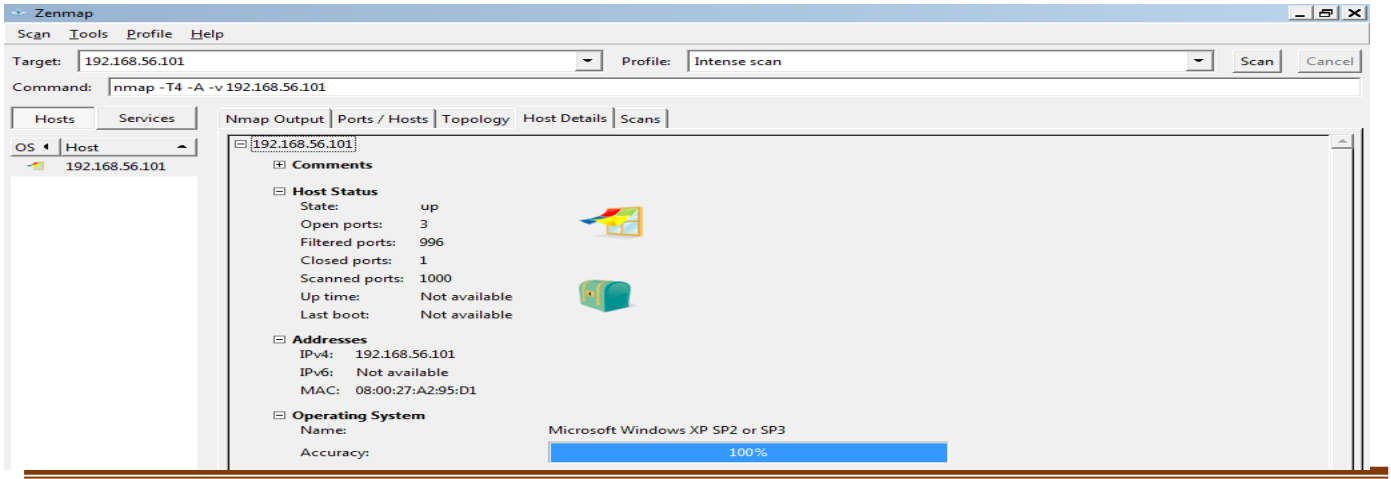
EXPT NO 5: PERFORM AN EXPERIMENT ON ACTIVE AND PASSIVE FINGER PRINTING USING XPROBE2 AND NMAP.

Fingerprinting is a process in scanning phase in which an attacker tries to identify Operating System of target Machine.

Fingerprinting can be classified into two types
Active and Passive Fingerprinting
Active Stack Fingerprinting

It involves sending data to the target system and then see how it responds. Based on the fact that teach system will respond differently, the response is compared with database and the OS is identified. It is commonly used method though there are high chances of getting detected. It can be performed by following ways.

Using Nmap : Nmap is a port scanning tool that can be used for active stack OS fingerprinting.
Syntax: nmap -O IP_address
Example: nmap –O 192.168.56.101
Using Xprobe2: This UNIX tool for active fingerprinting.
Syntax: xprobe2 -v IP_address
Example: xprobe -v 192.168.56.101
Passive Fingerprinting involves examining traffic on network to determine the operating system. There is no guarantee that the fingerprint will be accurate but usually they are accurate. It generally means sniffing traffic rather than making actual contact and thus this method is stealthier and usually goes undetected.



EXPT NO: 6 Perform an experiment to demonstrate how to sniff for router traffic by using the tool Cain and Abel / wireshark / tcpdump

PACKET SNIFFER

A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission.

In its simple form a packet sniffer simply captures all of the packets of data that pass through a given network interface. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic.

What is Wireshark?

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed.

Wireshark is perhaps one of the best open source packet analyzers available today.

Some intended purposes

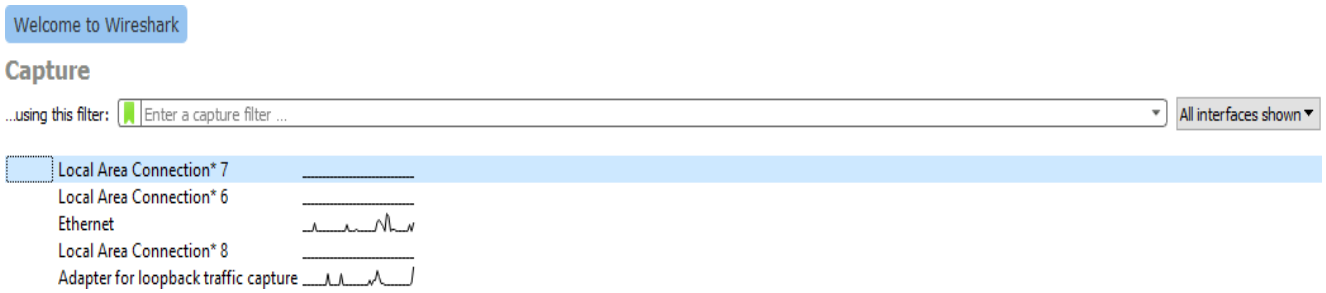
- Network administrators use it to **troubleshoot network problems**
- Network security engineers use it to **examine security problems**
- Developers use it to **debug protocol implementations**
- People use it to **learn network protocol** internals

OUTPUT

Download and install Wireshark network analyzer.

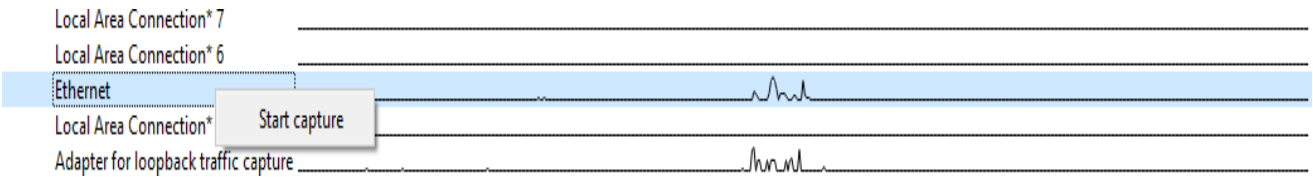
Steps to capture traffic:

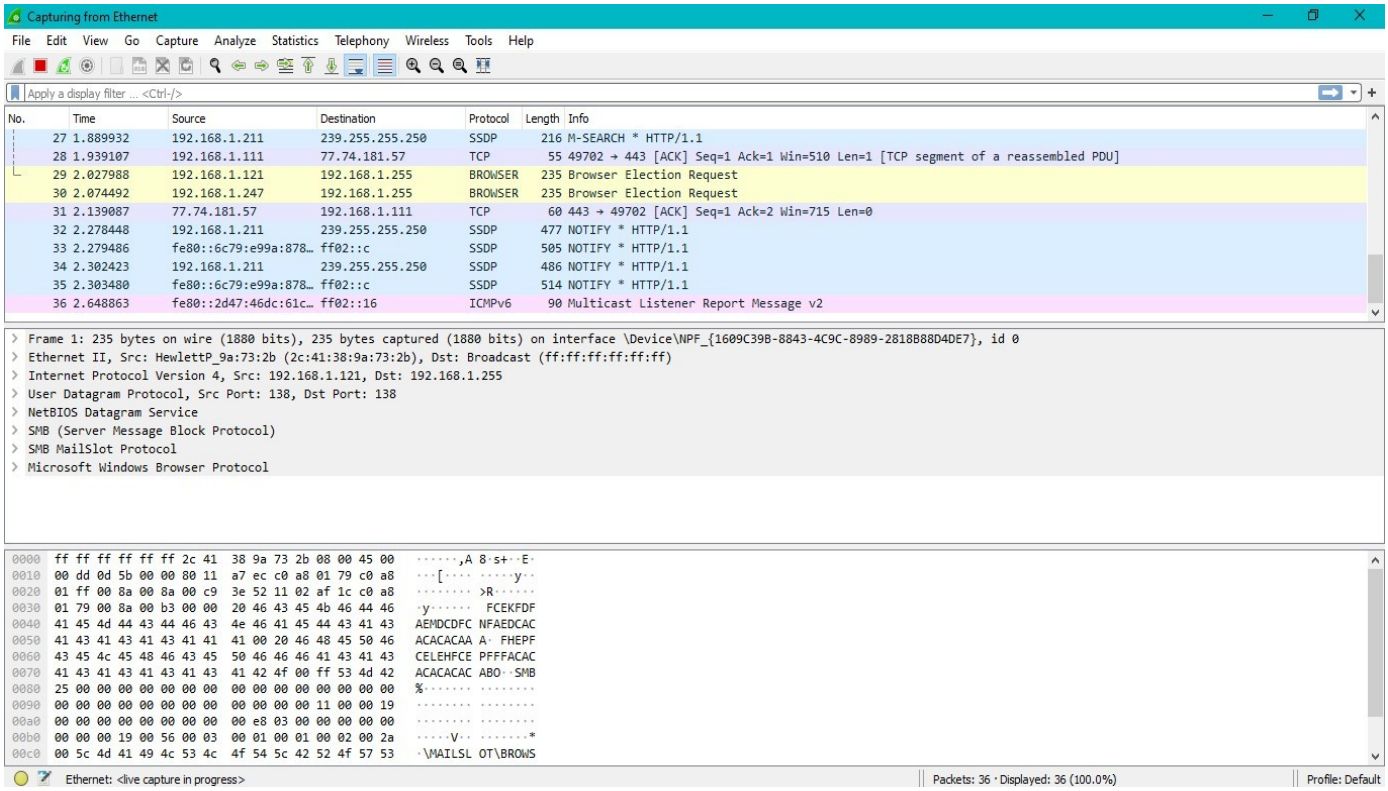
1. Open Wireshark (Network Packet Analyser).



2. Select the Local Area Connection / Ethernet depends upon the Windows used.

3. Start the capture.




Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
27 1.889932 192.168.1.211 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
28 1.939107 192.168.1.111 77.74.181.57 TCP 55 49702 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
29 2.027988 192.168.1.121 192.168.1.255 BROWSER 235 Browser Election Request
30 2.074492 192.168.1.247 192.168.1.255 BROWSER 235 Browser Election Request
31 2.139087 77.74.181.57 192.168.1.111 TCP 60 443 → 49702 [ACK] Seq=1 Ack=2 Win=715 Len=0
32 2.278448 192.168.1.211 239.255.255.250 SSDP 477 NOTIFY * HTTP/1.1
33 2.279486 fe80::6c79:e99a:878… ff02::c SSDP 505 NOTIFY * HTTP/1.1
34 2.302423 192.168.1.211 239.255.255.250 SSDP 486 NOTIFY * HTTP/1.1
35 2.303480 fe80::6c79:e99a:878… ff02::c SSDP 514 NOTIFY * HTTP/1.1
36 2.648863 fe80::2d47:46dc:61c… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
Frame 1: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits) on interface \Device\NPF_{1609C39B-8843-4C9C-8989-2818B88D4DE7}, id 0
Ethernet II, Src: HewlettP_9a:73:2b (2c:41:38:9a:73:2b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.1.121, Dst: 192.168.1.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 2c 41 38 9a 73 2b 08 00 45 00 ,A 8 s+ E
0010 00 dd 0d 5b 00 00 80 11 a7 ec c0 a8 01 79 c0 a8 [y
0020 01 ff 00 8a 00 8a 00 c9 3e 52 11 02 af 1c c0 a8 >R
0030 01 79 00 8a 00 b3 00 00 20 46 43 45 4b 46 44 46 y FCEKFDF
0040 41 45 4d 44 43 44 46 43 4e 46 41 45 44 43 41 43 AEMDCDFC NFAEDCAC
0050 41 43 41 43 41 43 41 41 41 00 20 46 48 45 50 46 ACACACAA A FHEPF
0060 43 45 4c 45 48 46 43 45 50 46 46 46 41 43 41 43 CELEHFCE PFFFACAC
0070 41 43 41 43 41 43 41 43 41 42 4f 00 ff 53 4d 42 ACACACAC ABO SMB
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 %
0090 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 19
00a0 00 00 00 00 00 00 00 00 00 e8 03 00 00 00 00 00
00b0 00 00 00 19 00 56 00 03 00 01 00 01 00 02 00 2a V *
00c0 00 5c 4d 41 49 4c 53 4c 4f 54 5c 42 52 4f 57 53 \MAILSL OT\BROWS
Ethernet: <live capture in progress>
Packets: 36 · Displayed: 36 (100.0%)
Profile: Default

EXPT NO: 7 PERFORM AN EXPERIMENT HOW TO USE DUMPSEC.

Dumpsec:

Dumpsec is a windows-based GUI enumeration tool from SomarSoft and is available from www.somarsoft.com. It enables you to remotely connect to windows machines and dump account details, share permissions, and user information.

Dumpsec's GUI-based format makes it easy to take the results and port them into a spreadsheet so that holes in system security are readily apparent and easily tracked. It can provide you with usernames, SID's, RID's, account comments, account policies, and dial-in information.

Enumeration with Dumpsec

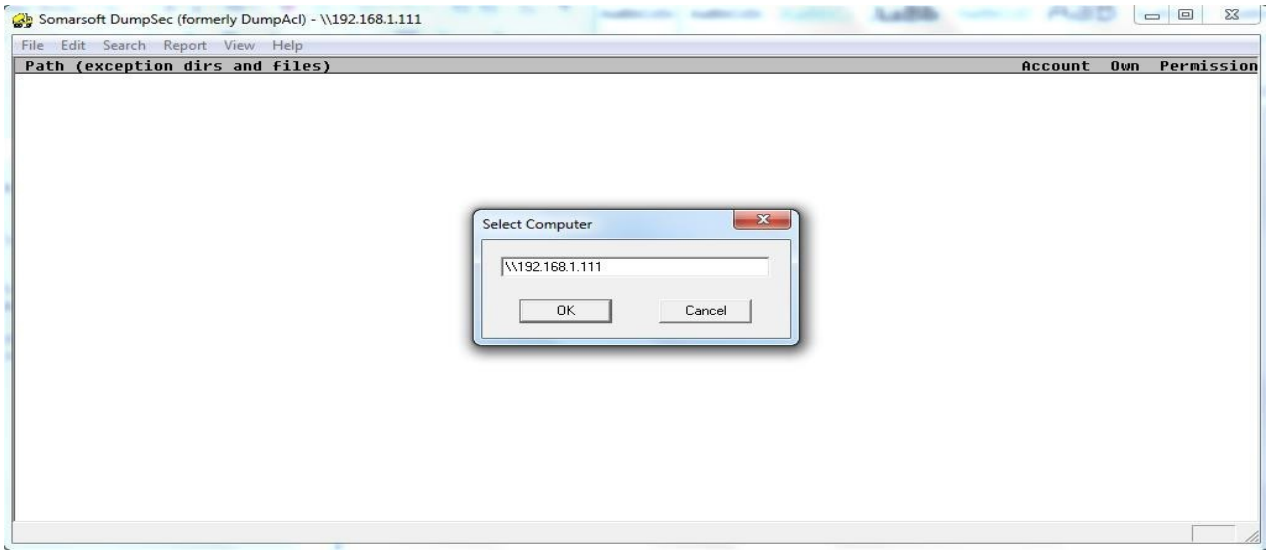
This exercise demonstrates how to use Dumpsec to enumerate a windows computer:

Step 1: Download and install Dumpsec from www.somarsoft.com.

Step 2: Once it's installed, open command prompt and establish a null session to a localhost. The command syntax for doing so is as follows:

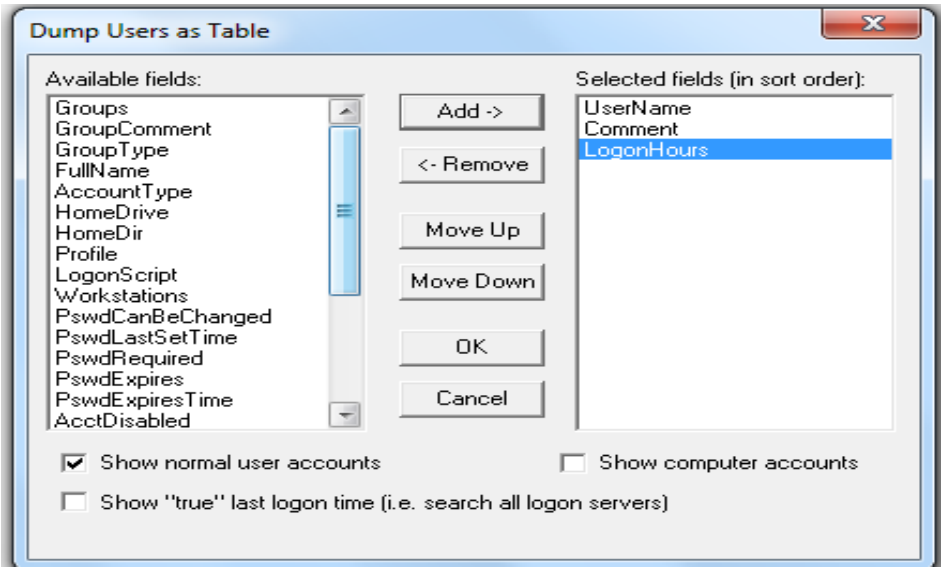
Net use //IP Address/IPC$ "" \u: ""

Step 3: Now open Dumpsec and select Report → select Computer, as shown in Figure.

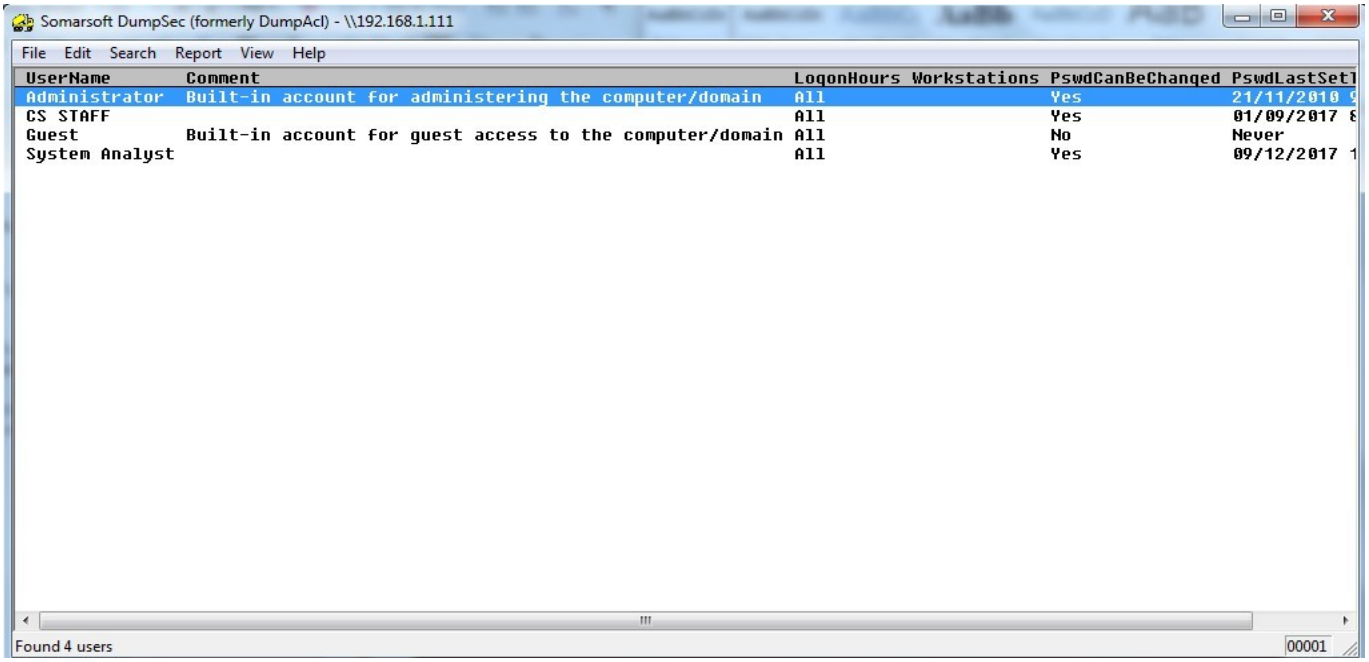


Step 4: Now select Report → Dump Users as Table, and click OK.

Step 5: You need to select all items to the left of the screen and move them to the right screen so that all fields will be selected, as shown in Figure.

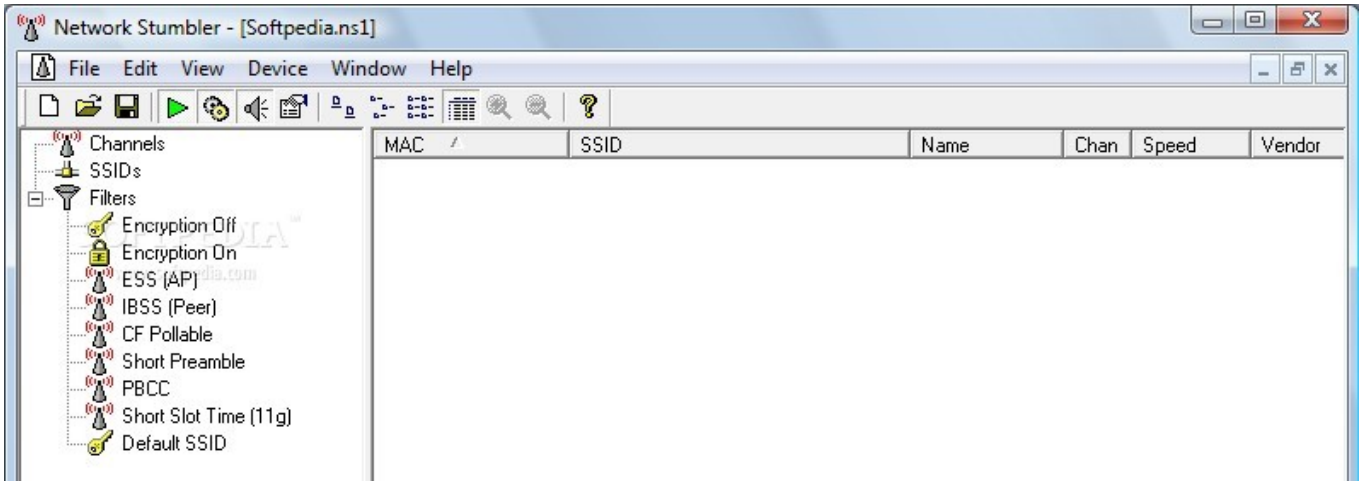


Step 6: Click the OK button, and all the open fields will be populated. Notice that you now have a complete list of users and related information, as shown in Figure

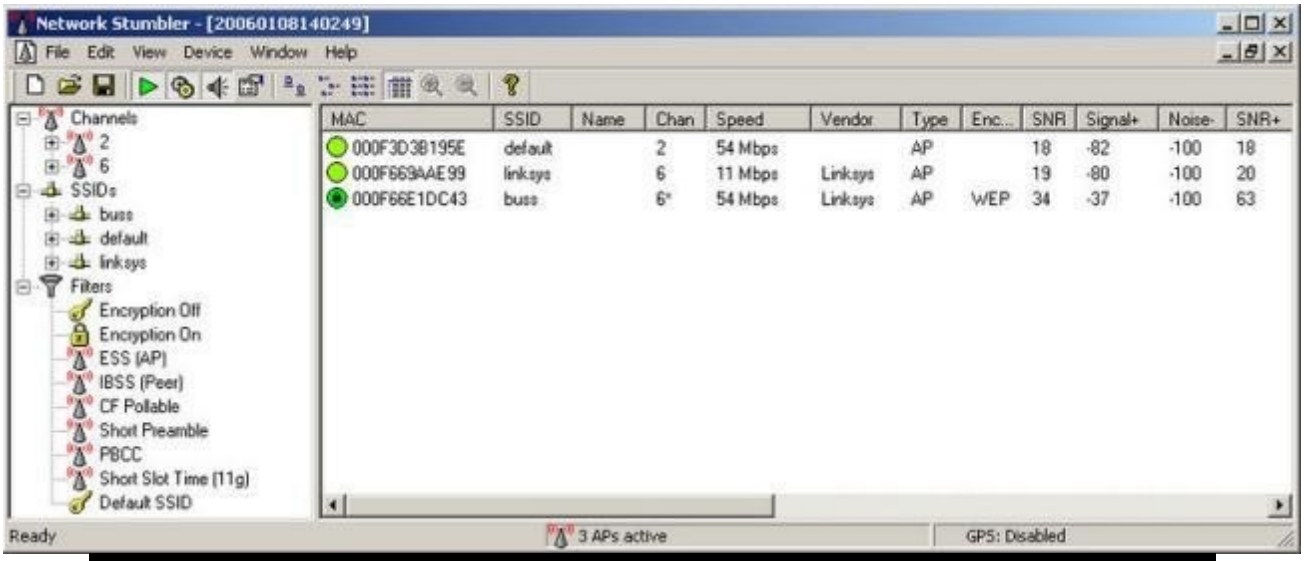


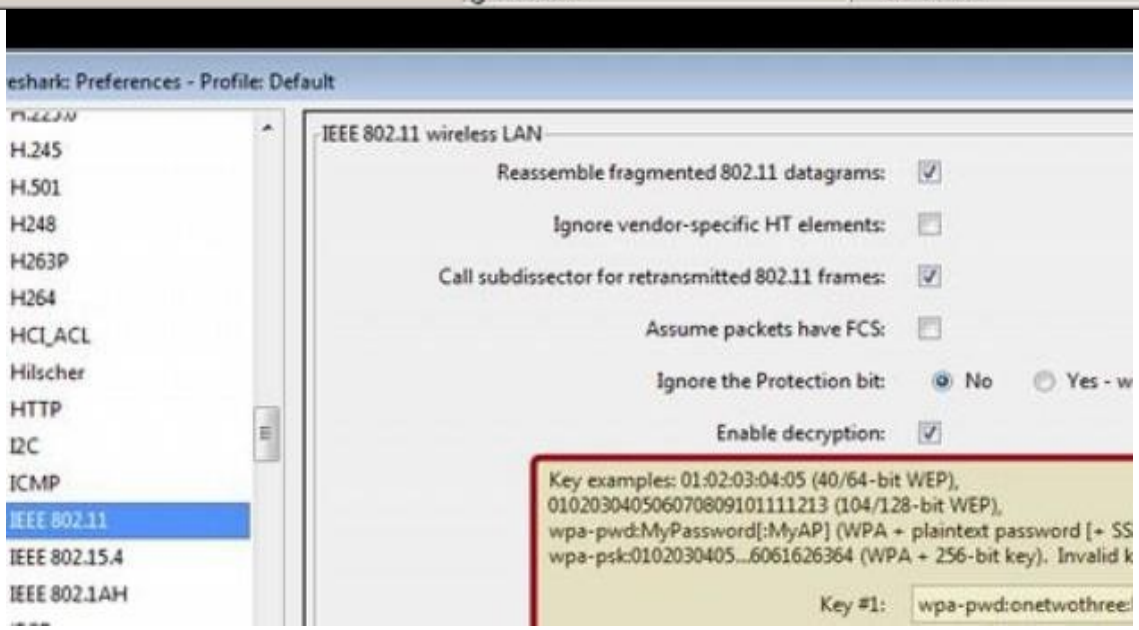
EXPT NO: 8 PERFORM AN WIRELESS AUDIT OF AN ACCESS POINT / ROUTER AND DECRYPT WEP AND WPA.

NetStumbler (Network Stumbler) is one of the Wi-Fi hacking tool which only compatible with windows, this tool also a freeware. With this program, we can search for wireless network which open and infiltrate the network. Its having some compatibility and network adapter issues.



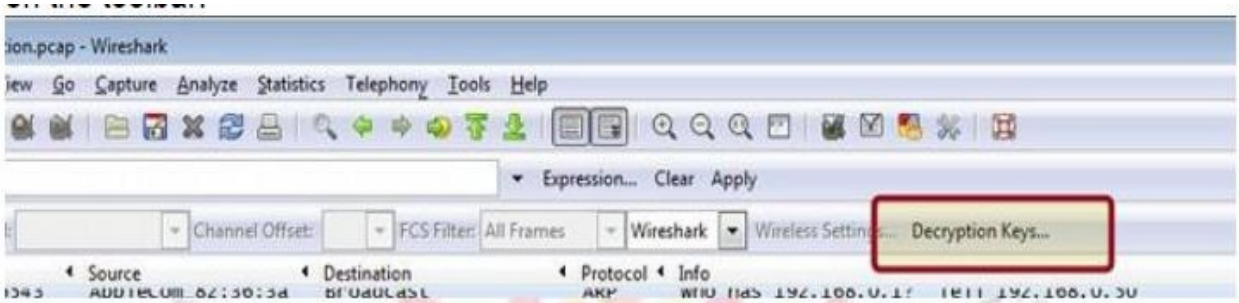
 Download and install Netstumbler
 It is highly recommended that your PC should have wireless network card in order to access wireless router.
 Now Run Netstumbler in record mode and configure wireless card.
 There are several indicators regarding the strength of the signal, such as GREEN indicates Strong, YELLOW and other color indicates a weaker signal, RED indicates a very weak and GREY indicates a signal loss.
 Lock symbol with GREEN bubble indicates the Access point has encryption enabled.
 MAC assigned to Wireless Access Point is displayed on right hand pane.
 The next coloumn displays the Access points Service Set Identifier[SSID] which is useful to crack the password.
 To decrypt use WireShark tool by selecting Edit preferences IEEE 802.11
 Enter the WEP keys as a string of hexadecimal numbers as A1B2C3D4E5





Adding Keys: Wireless Toolbar

If you are using the Windows version of Wireshark and you have an AirPcap adapter you can add decryption keys using the wireless toolbar. If the toolbar isn't visible, you can show it by selecting View->Wireless Toolbar. Click on the Decryption Keys... button on the toolbar:



This will open the decryption key managment window. As shown in the window you can select between three decryption modes: None, Wireshark, and Driver:

EXPT NO: 9 PERFORM AN EXPERIMENT TO SNIFF TRAFFIC USING ARP POISONING.

Enumeration

Enumeration can best be defined as the process of counting. From a security standpoint, it's the process the attacker follows before an attack. The attacker is attempting to count or identify systems and understand their role or purpose. This may mean the identification of open ports, applications, vulnerable services , DNS or NetBIOS names, and IP address before an attack.

Sniffing

Sniffing the network is one of the primary ways to determine which routing protocols are running. If the network is still using hubs, all an attacker has to do is to plug into an open RJ-45 wall jack to sniff the traffic. If no hubs are being used in the network, the attacker must perform active sniffing.

Cain & Abel

A multipurpose tool that can perform a variety of tasks, including windows enumeration, sniffing and password cracking. The password cracking part of the program can perform dictionary and brute-force analysis and use precomputed hash tables.

Packet sniffing

A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic.

Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission.

In its simple form a packet sniffer simple captures all of the packets of data that pass through a given network interface. Typically, the packet sniffer would only capture packets that were intended for the machine in question. However, if placed into

promiscuous

mode, the packet sniffer is also capable of capturing all packets traversing the network regardless of destination.

ARP Spoofing/ARP Poisoning

ARP stands for Address Resolution Protocol and it allows the network to translate IP addresses into **MAC** addresses. It is a type of attack where the media access control **(MAC)** address is changed by the attacker.

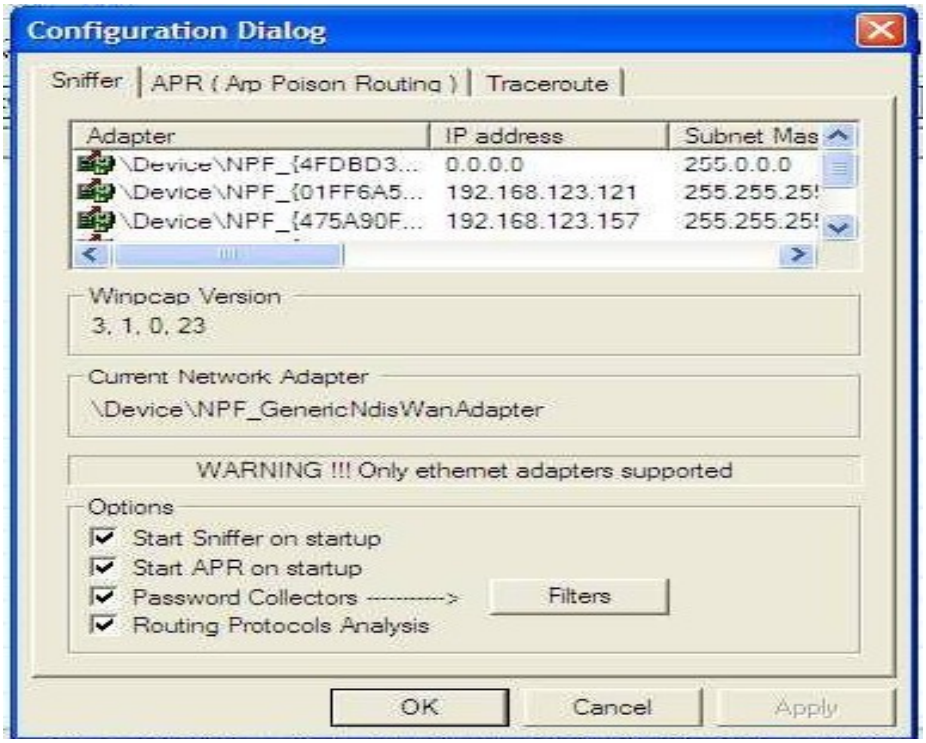
Also, called as **ARP** spoofing attacks, it is effective against both wired and wireless local networks.

ARP poisoning is when an attacker is able to compromise the **ARP** table and changes the **MAC** address so that the IP address points to another machine.

Steps:

1. Download and install cain & Abel from www.oxid.it
2. Once downloaded, cain & Abel may ask you to install Winpcap if it has not already been installed on your local windows computer.

   Once cain & Abel and select the configuration Dialog box you should get a screen like this:
   If you have more than 1 network card choose 1 of the several!

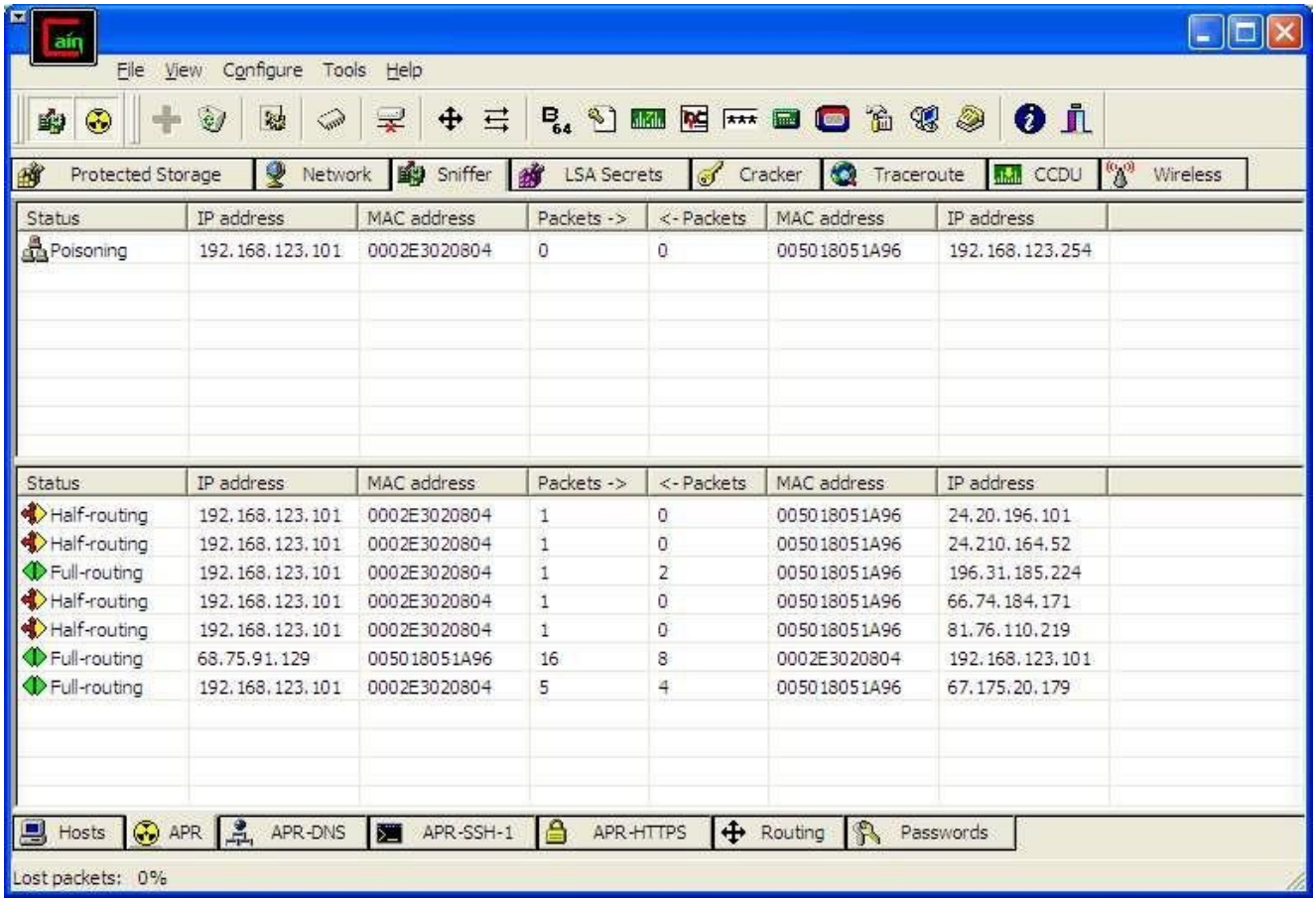


If you have more than 1 network card choose 1 of the several!

3. Click the start/stop sniffer button:

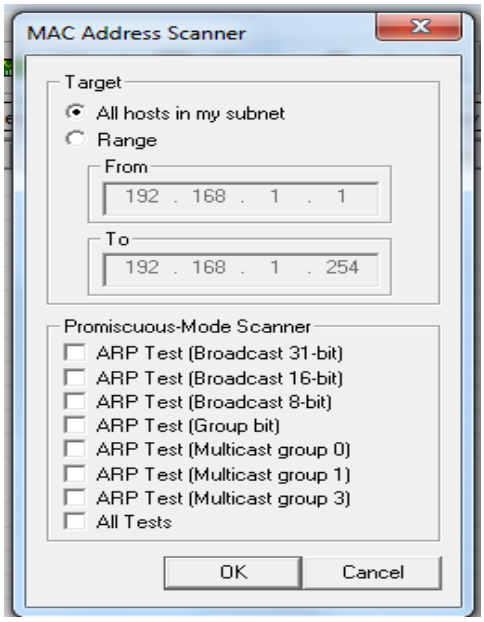
4. Click on sniffer

5. Now an IP address, MAC address screen appears on the screen.

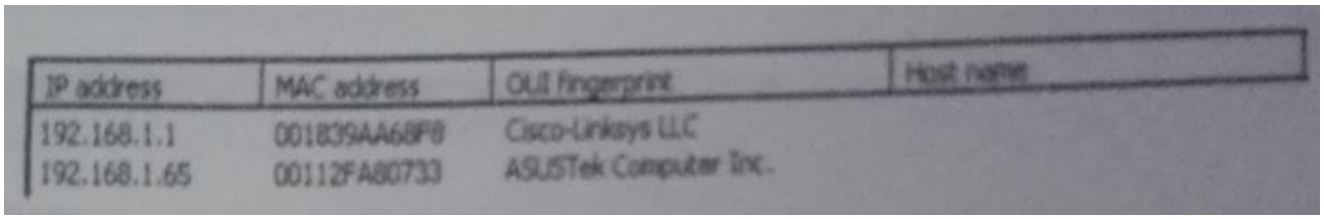


6. Next click the Add To List Button (+):

Either leave it on the subnet scan or choose your own range to scan!



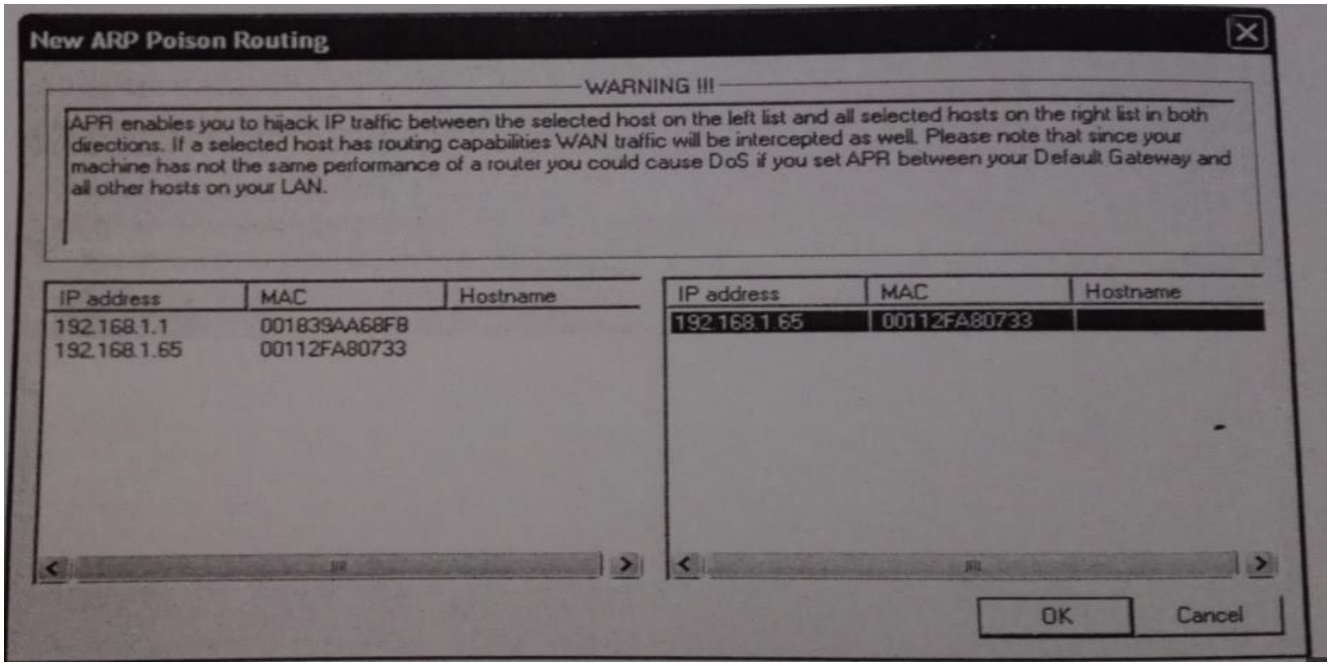
You should then see something like this:



7. Click on the ARP tab:

8. Next click the Add To List Button (+):

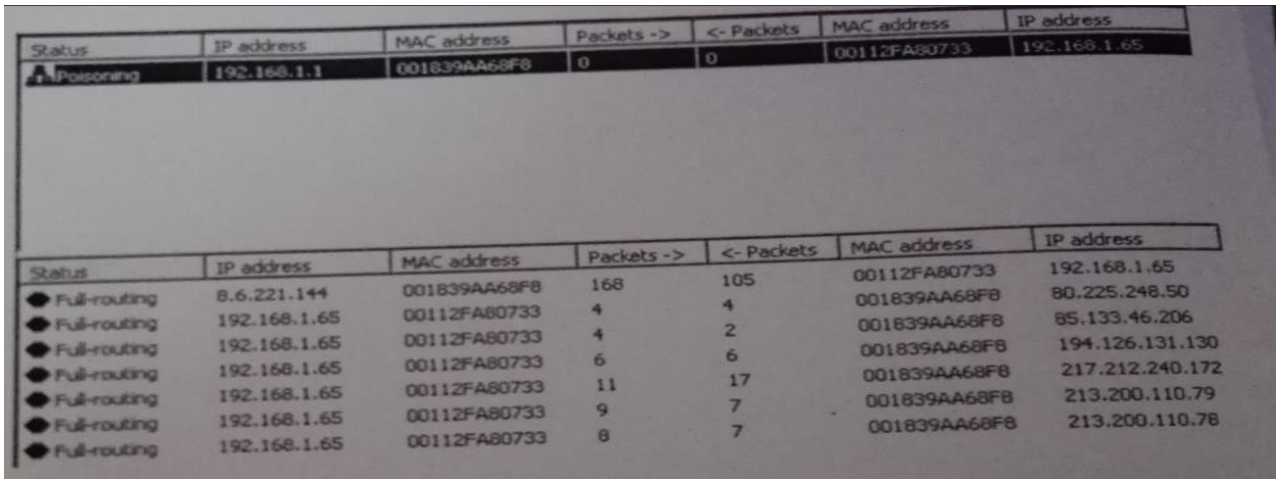
9. You will get a screen like this:



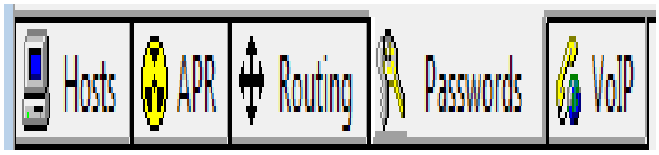
In the first section choose the Router/Server you want to log. In the second choose the client computer (the persons computer you are monitoring)

10. Click the Start/Stop ARP Button:

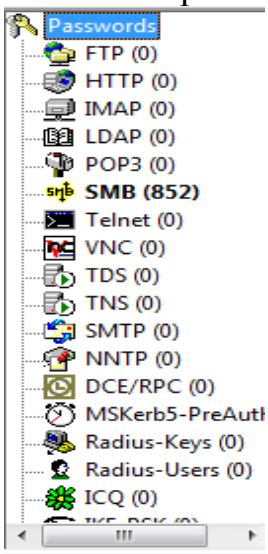
Cain should now look something like this:



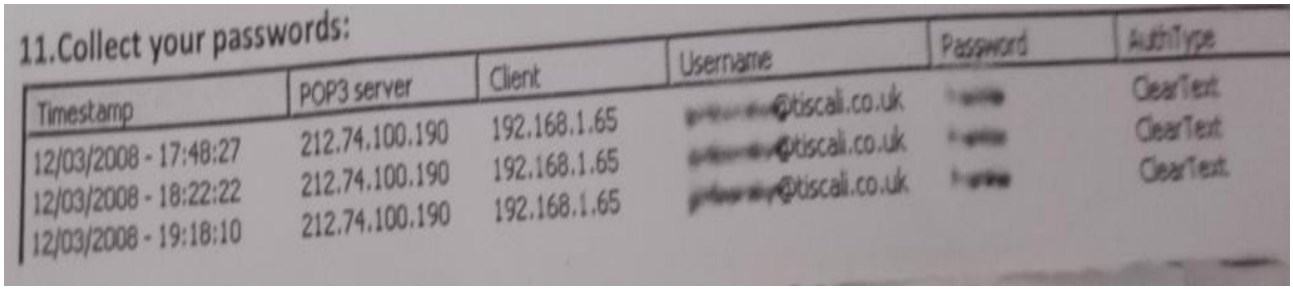
11. Go onto the Passwords Tab:



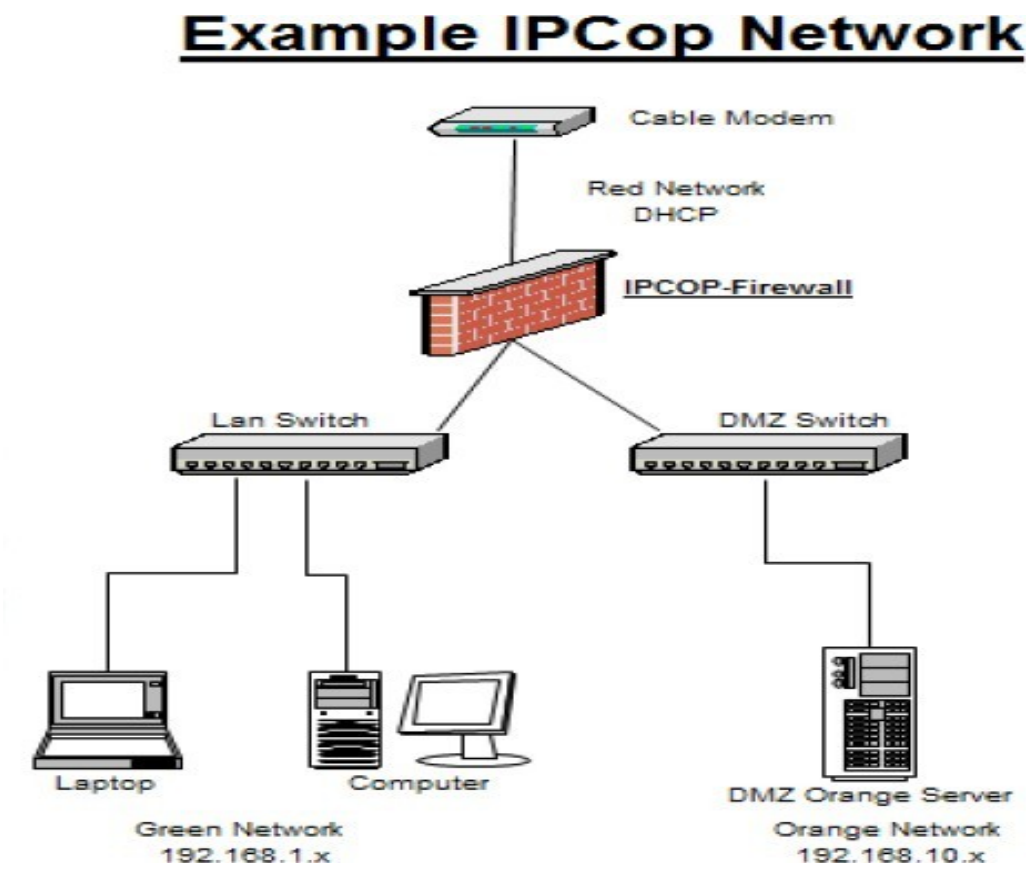
12. Choose the password type (the number shows how many you may have sniffed):



13. Collect your passwords:



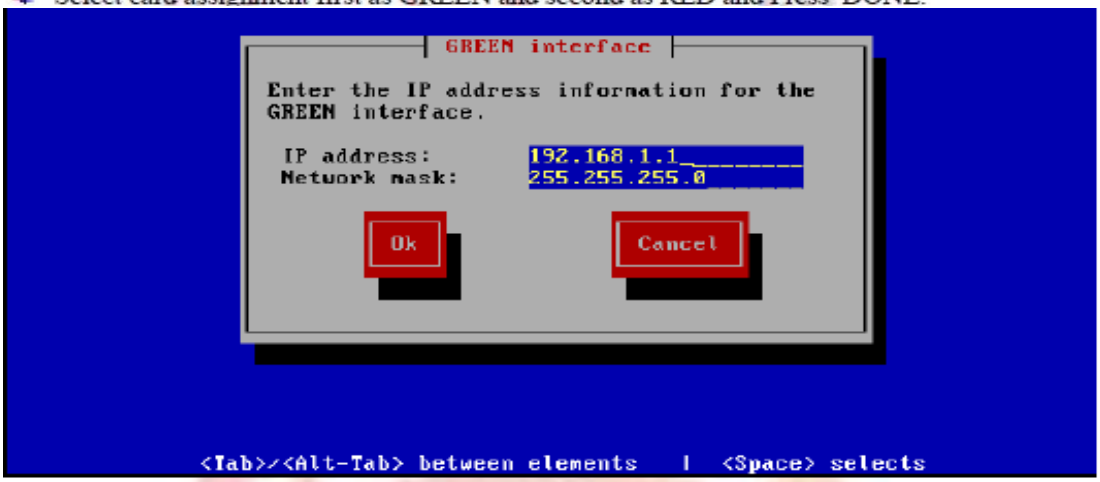
EXPT NO: 10 Install IPCop on a Linux system and learn all the function available on the software.



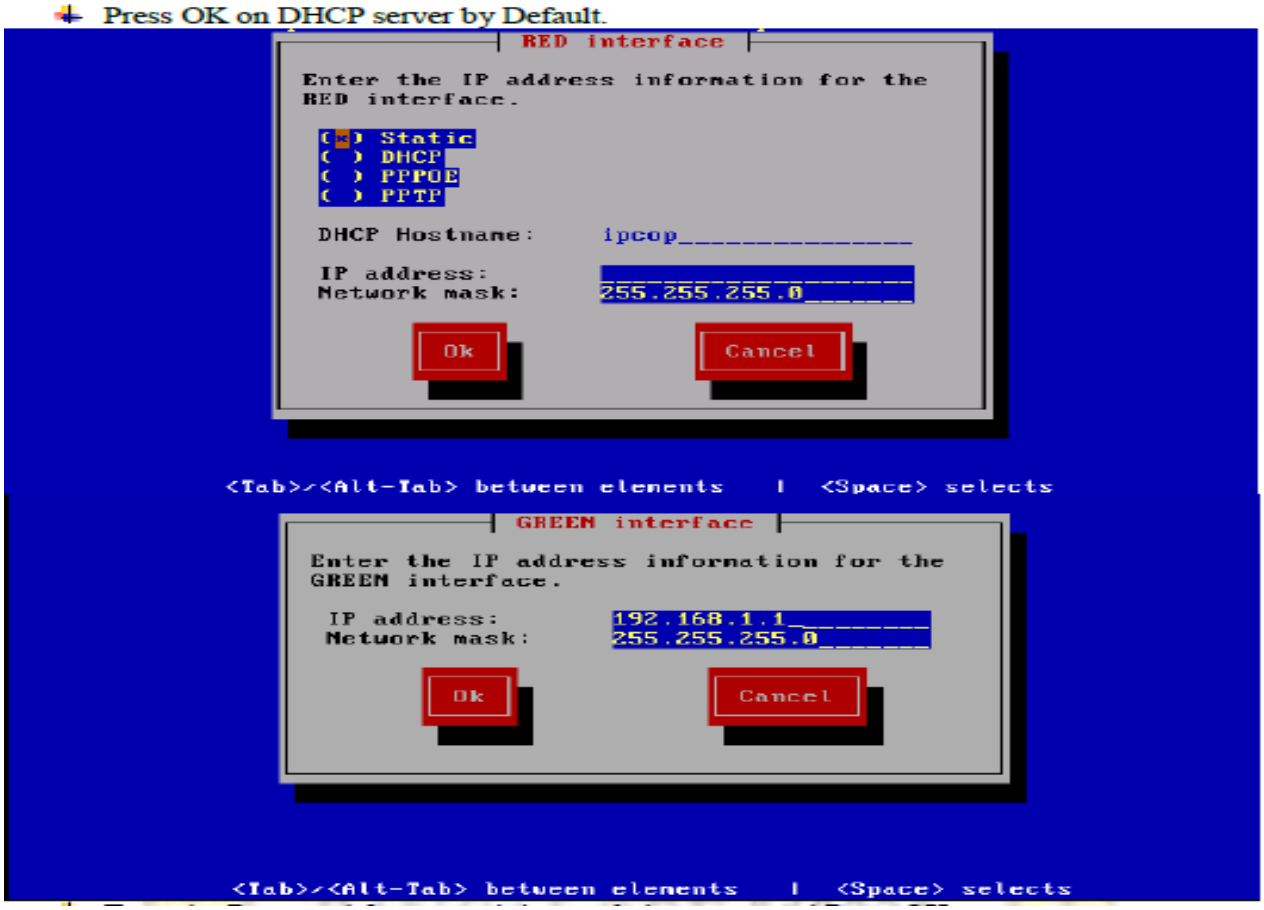
IPCOP Linux is a complete Linux distribution. Its sole purpose is to protect the network. Its main features are: IP table network filter, All types of Drive Support and Quad Network support such as GREEN(Internal Trusted Network), BLUE(Wireless Semi-Trusted Network, ORANGE(Demilitarized Zone for internet Access Servers, RED(The Internet)
Installation Procedure as follows:

- Download IPCOP 2.0.2.iso from www.ipcop.org.
- Run Virtual Box on Host PC and add IPCOP.ISO file and Start the Installation.
- The Bootup Screen appears hit enter key.

- Select Default English Language and Press Enter-Key
- Select default US layout Keyboard and Press Enter-Key.
- Select Asia/Calcutta and Press OK to proceed.
- Change the Date and Time if required and Press OK.
- Select the disk installation default HDD and Press OK.
- Skip the restore windows by pressing skip option button.
- Now Disk installation is complete press on congratulation button.
- Enter HOST name ipcop and Press OK.
- Domain Name local domain and Press OK.
- Select DHCP by pressing space bar key and Press OK.
- Select card assignment first as GREEN and second as RED and Press DONE.



- Press OK on DHCP server by Default.



- Type the Password for root minimum 6 characters and Press OK
- Type the Password for admin minimum 6 characters and Press OK.
- Type the Password for backup minimum 6 characters and Press OK.
- Your IPCOP Virtual Box Reboots.
- Type the username as root and enter the password , Press Enter-Key.
- Now open your Internet Explorer Web Browser and type the following in the address bar: https://192.168.1.1:8443/ and Press Enter-Key.
- Certificate error is obtained Click on continue which displays as not recommended anyway.
- IPCOP begins and enter the username as admin and type the password, click OK.
- The Full Fledge IPCOP firewall is now ready.

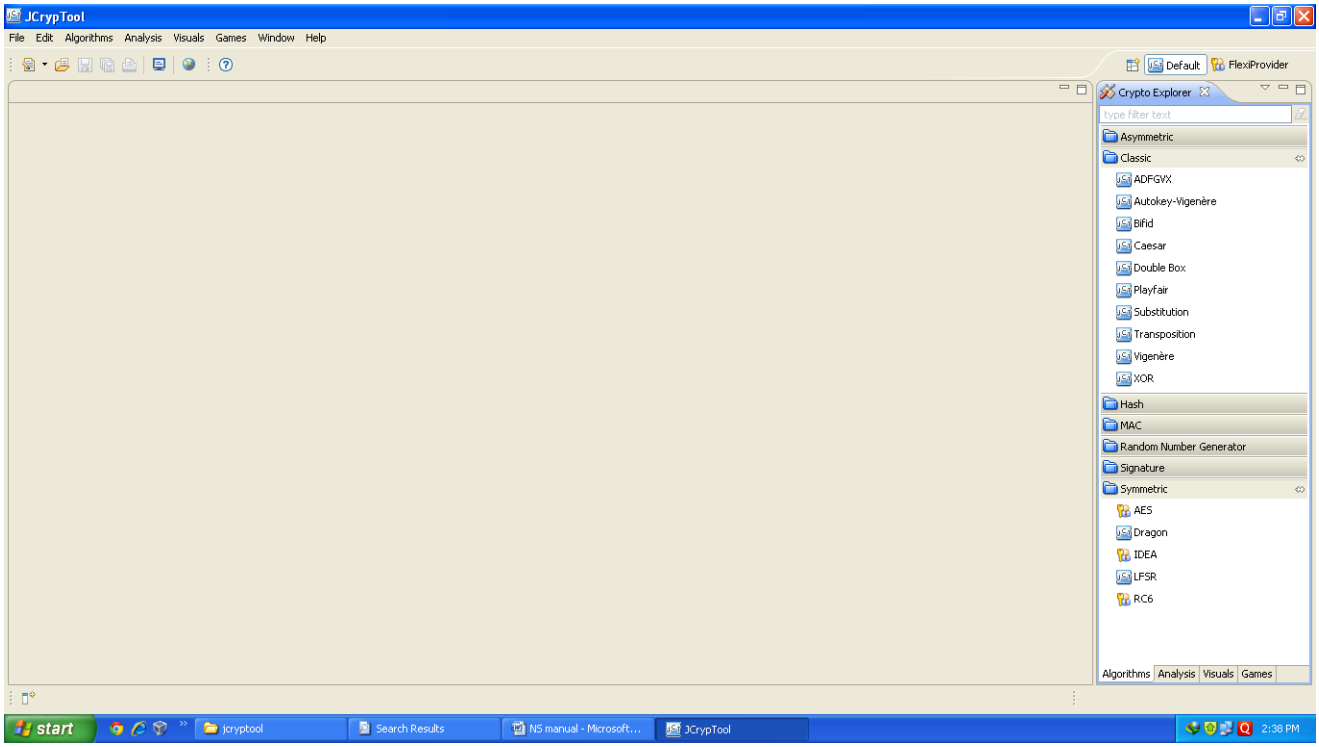
- Practice the absic options of IPCOP firewall.

EXPT NO: 11 INSTALL JCRYPT TOOL (OR ANY OTHER EQUIVALENT) AND DEMONSTRATE ASYMMETRIC, SYMMETRIC CRYPTO ALGORITHM, HASH AND DIGITAL/PKI SIGNATURES

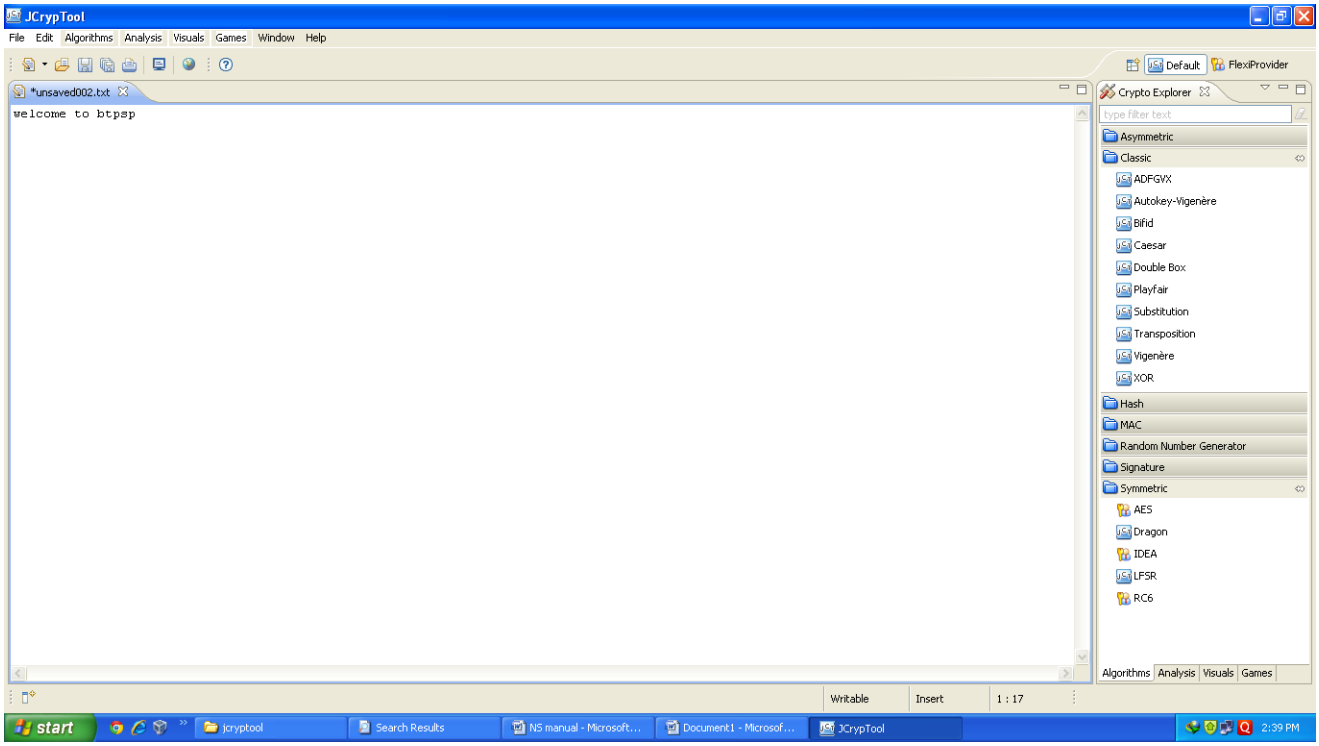
STEPS:

1. Download and install jcryptool.

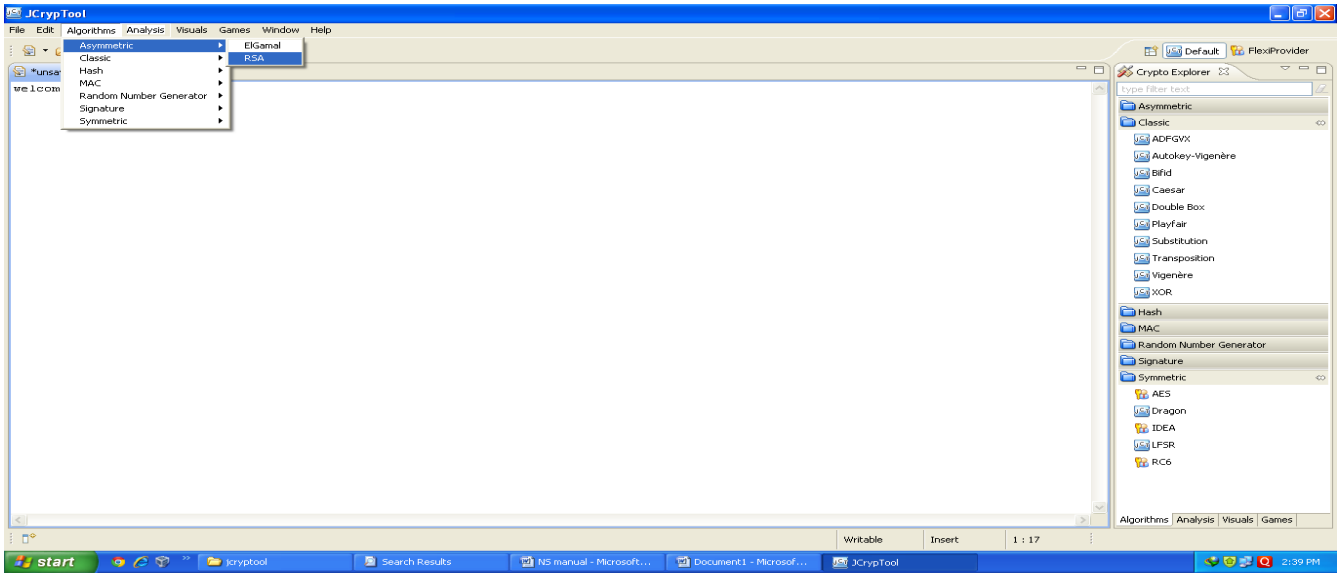
2. Open jcryptool.



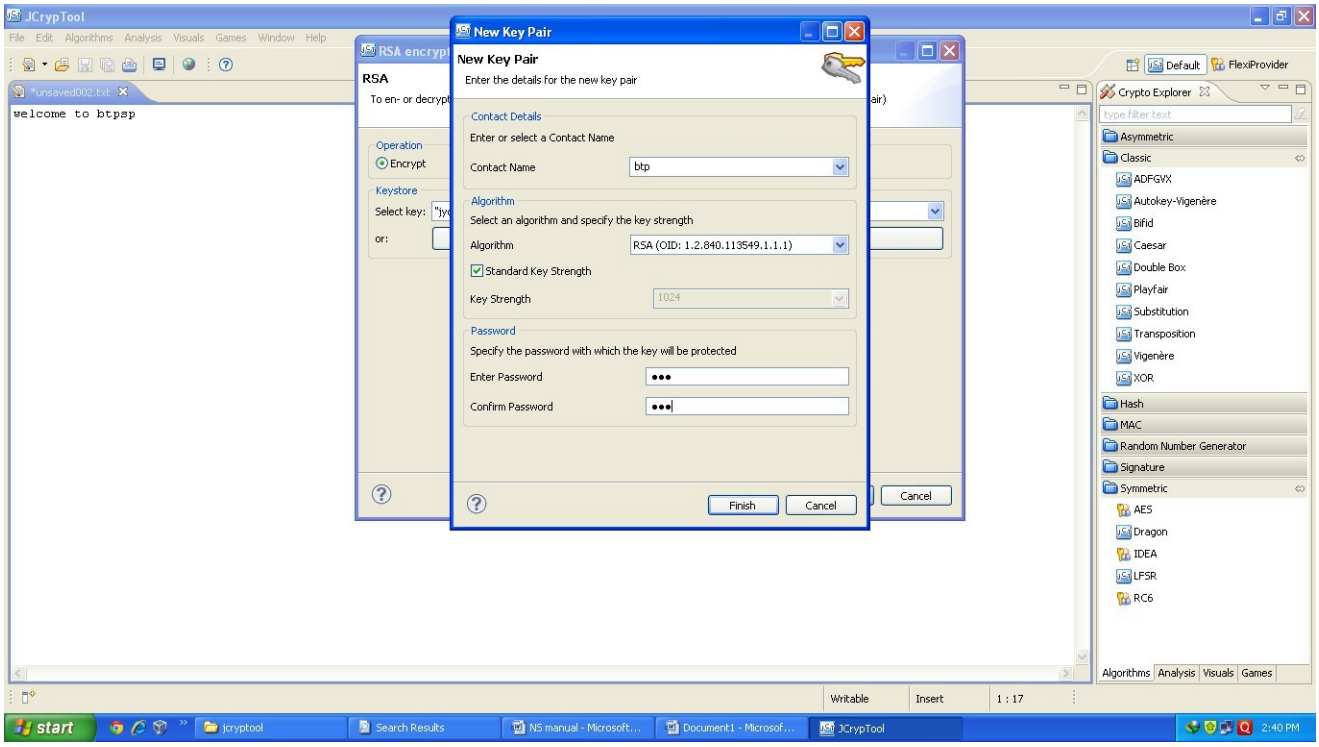
1. Open the text editor in jcryptool & write the msg which you want to encrypt.



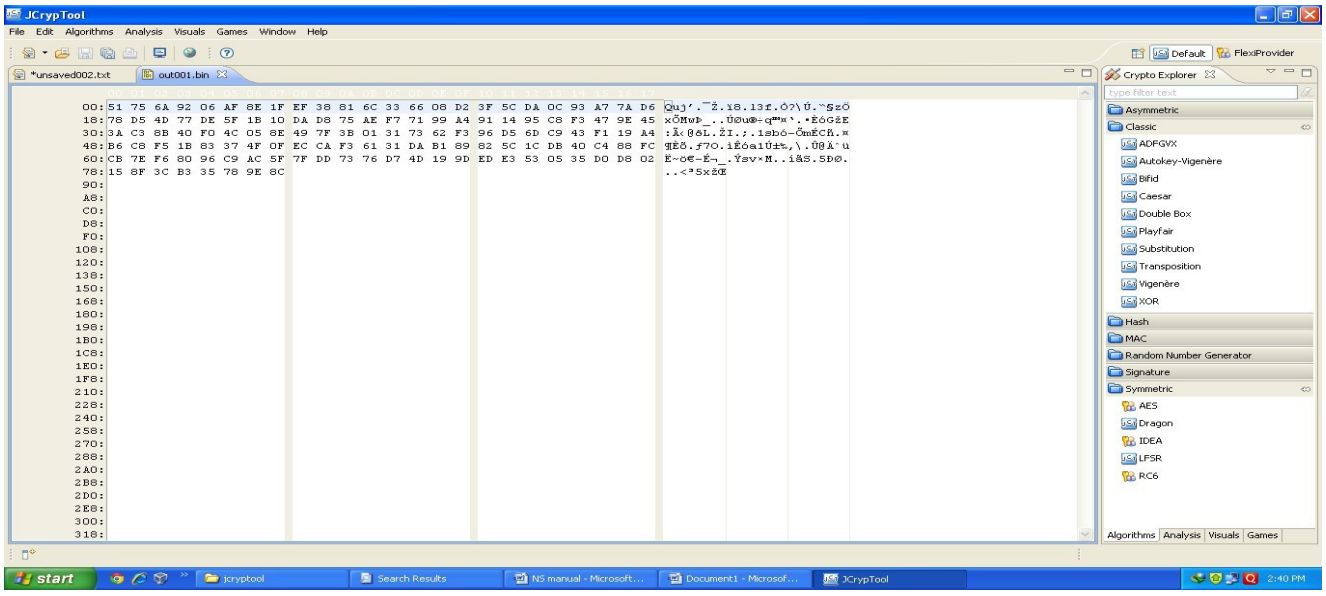
4. Select asymetric algoritham RSA.



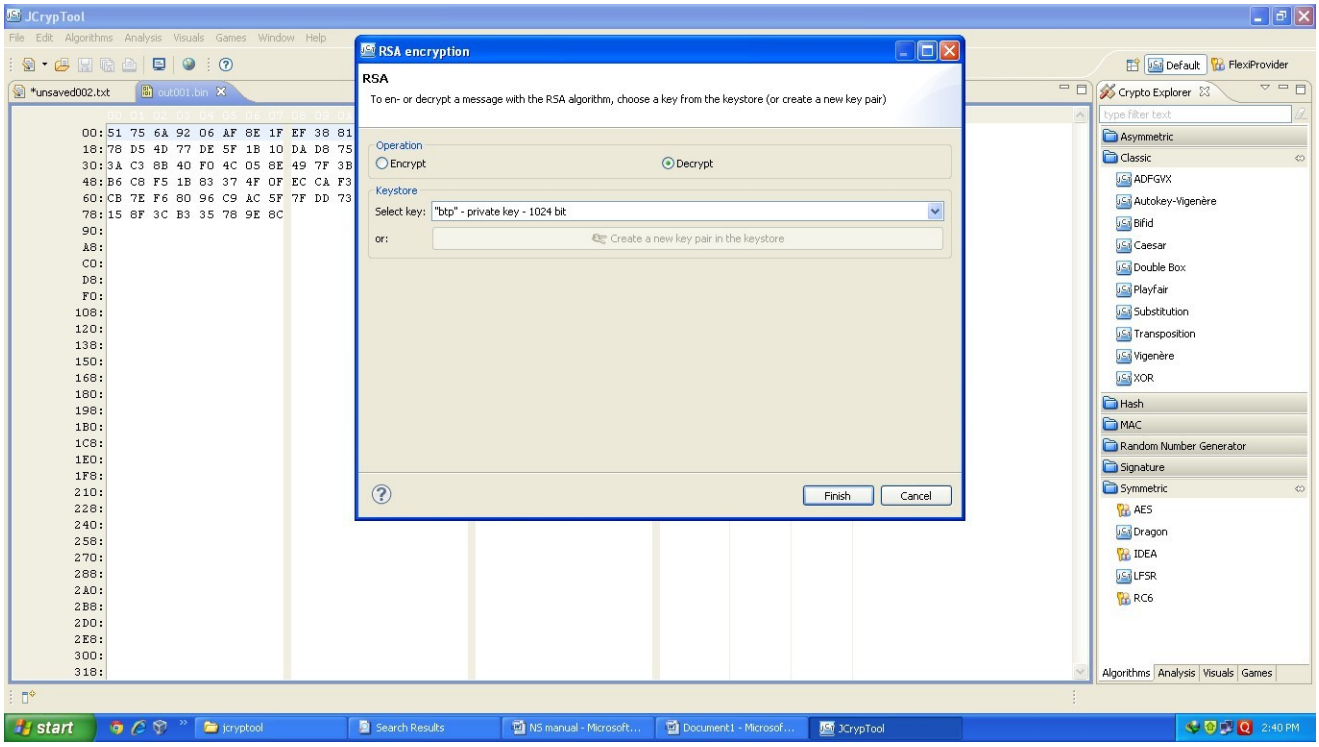
5. Provide password for encryption.



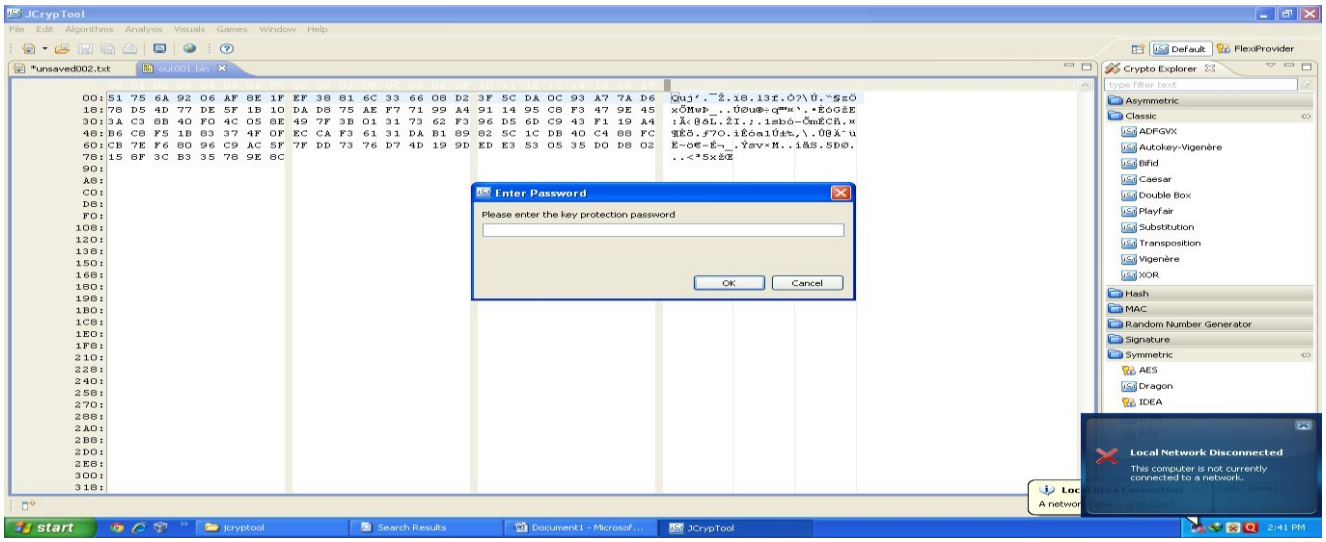
6. Following encrypted O/P will appear on screen.



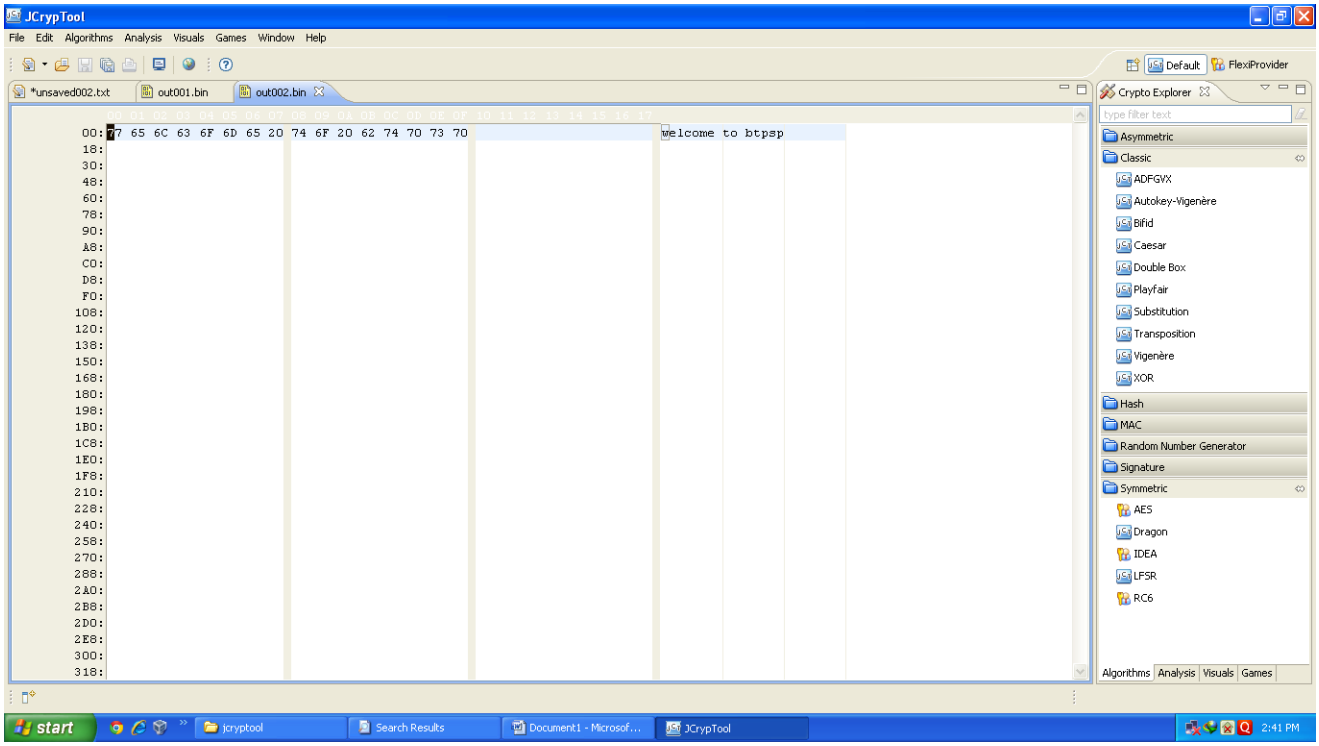
7. Decrpt the same text by selecting decrypt.



Provide the same password which provided during encryption.

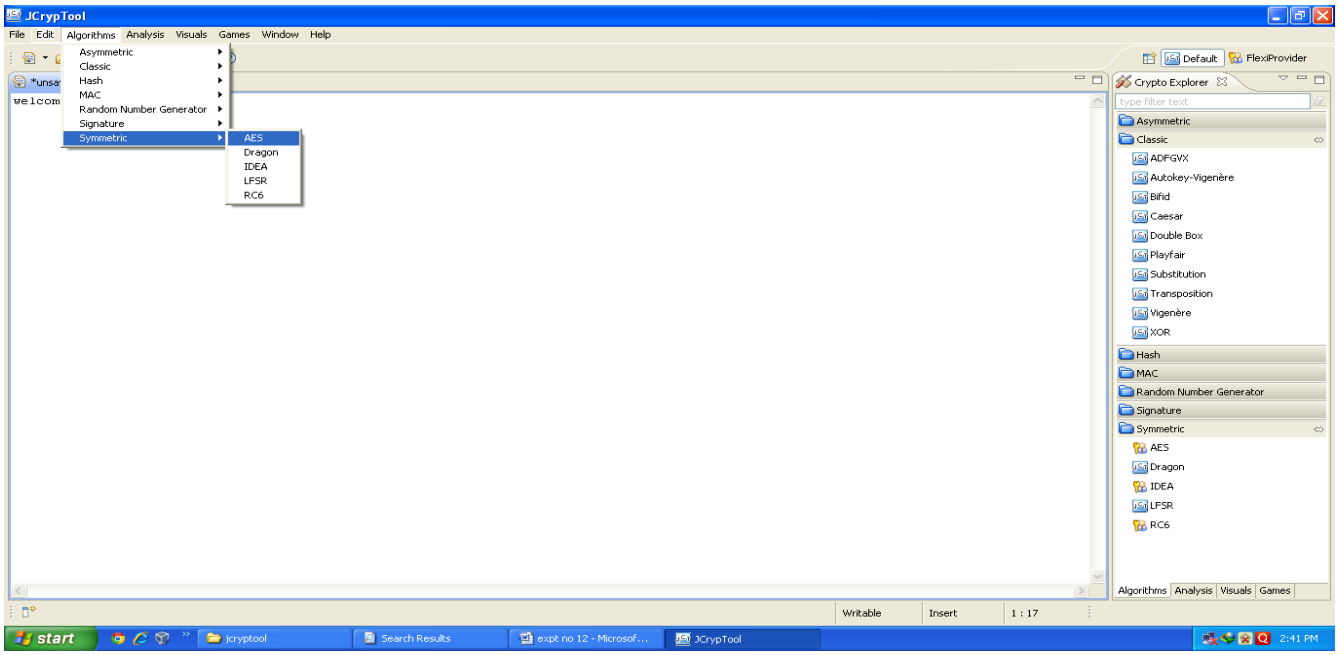


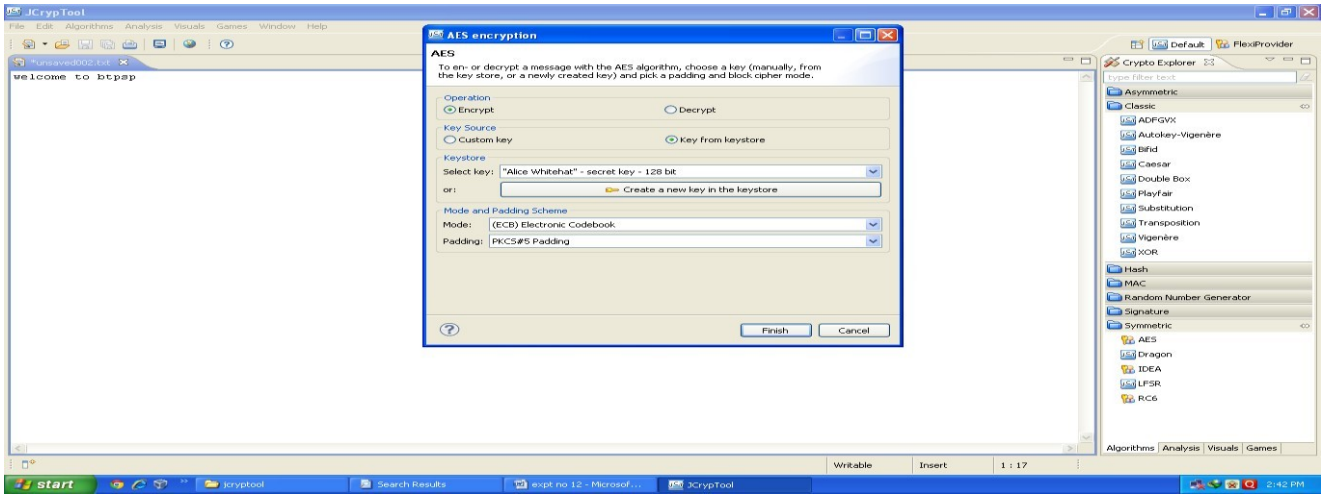
8.O/P will look like this.

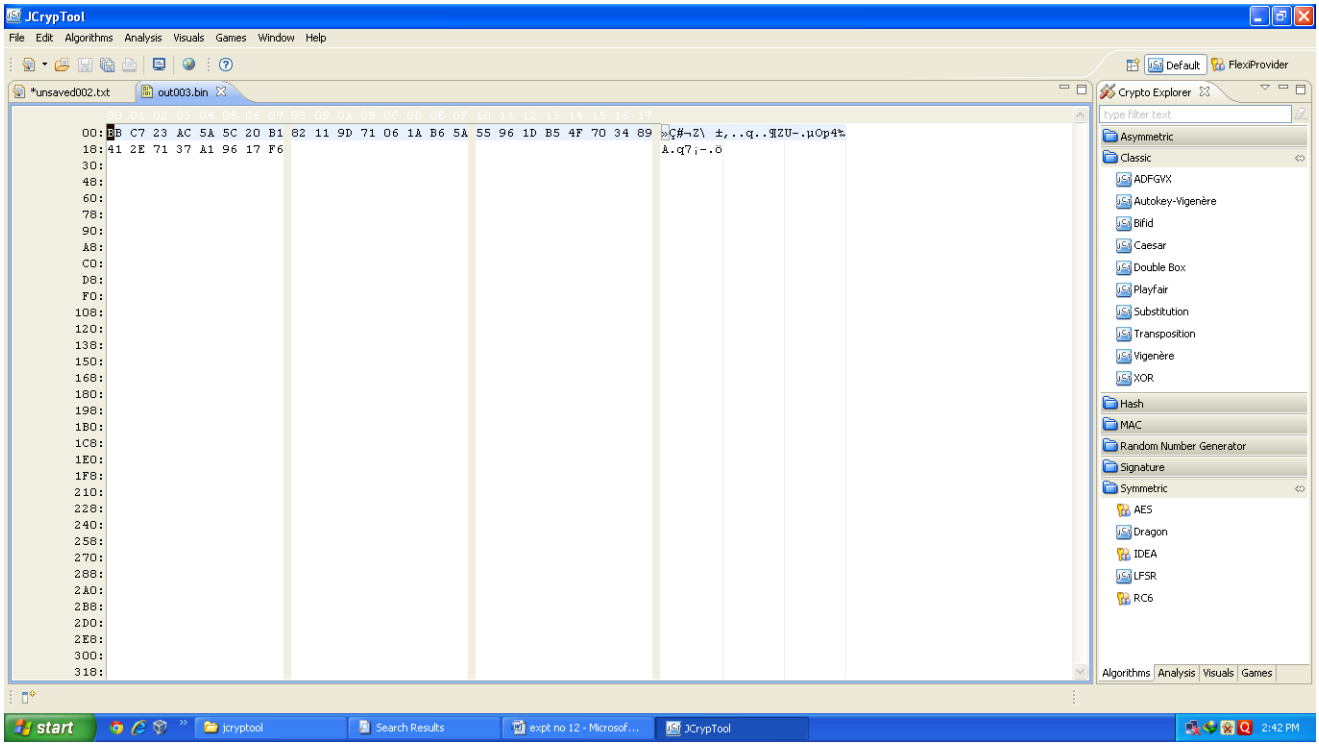


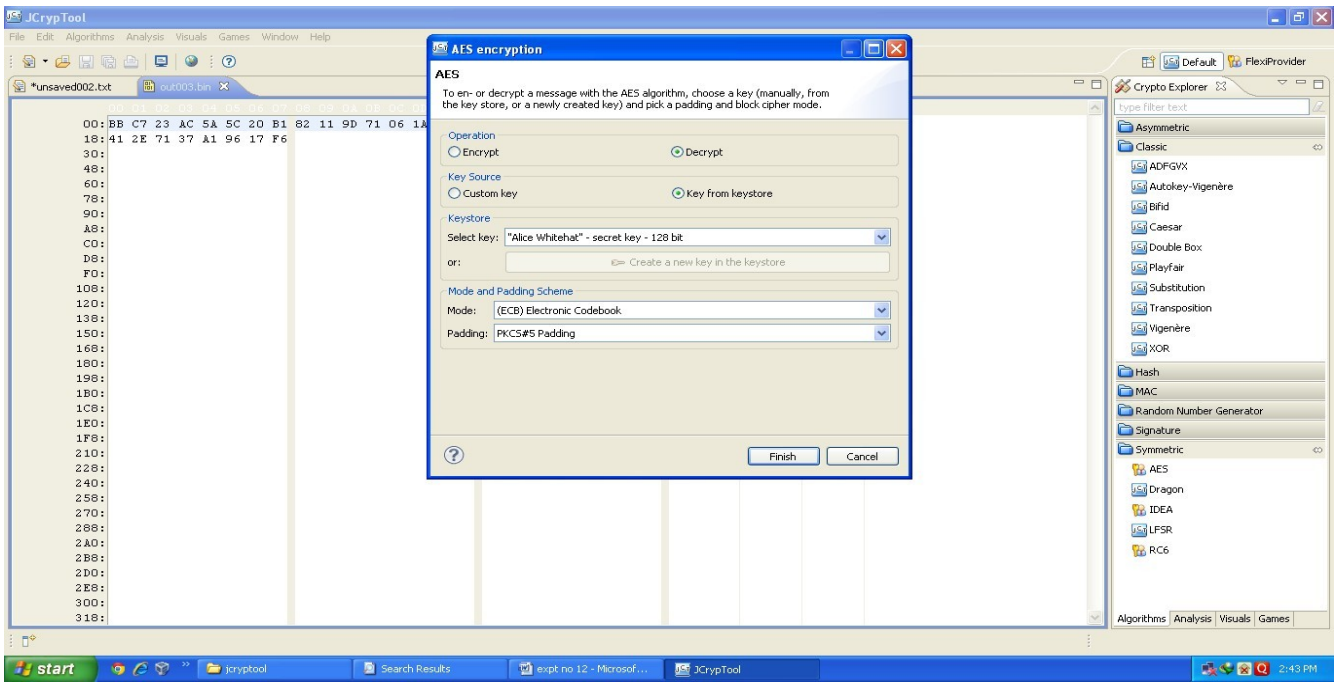
Encryption using symetric algorithms

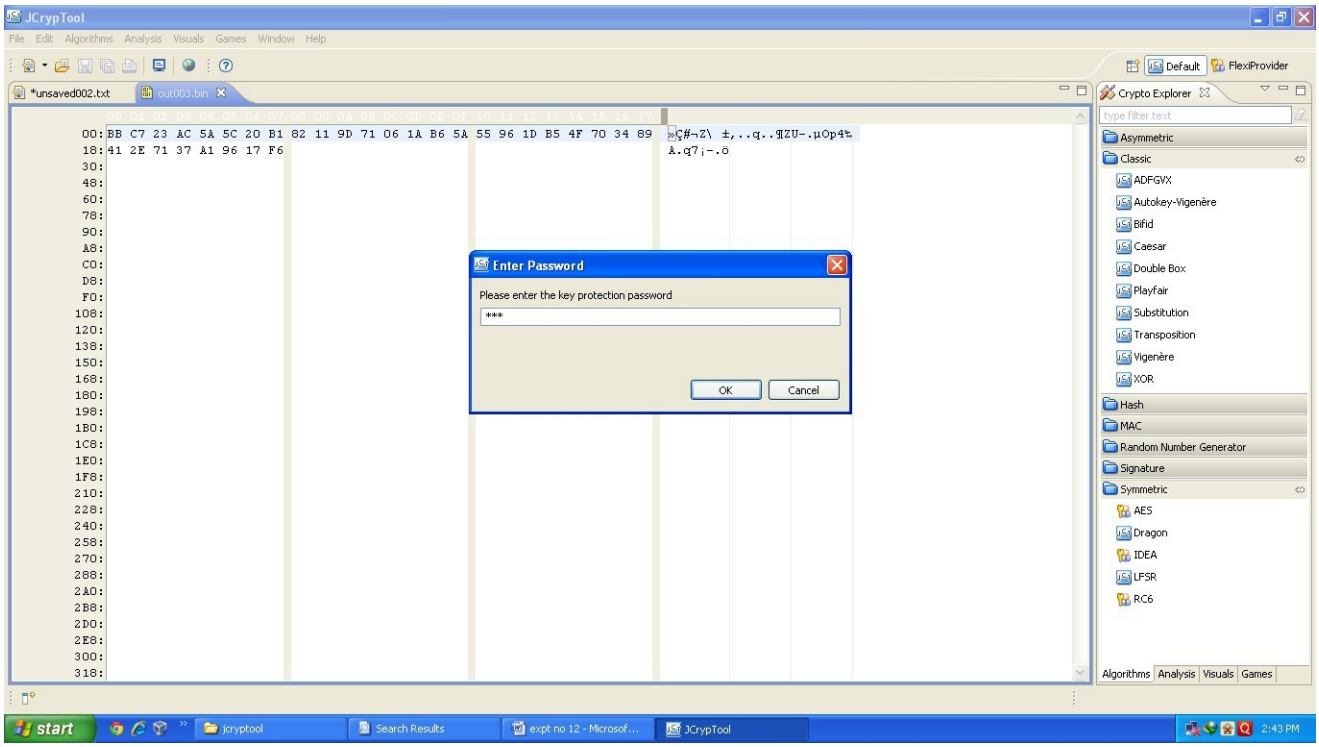
1.Select AES algorithm.

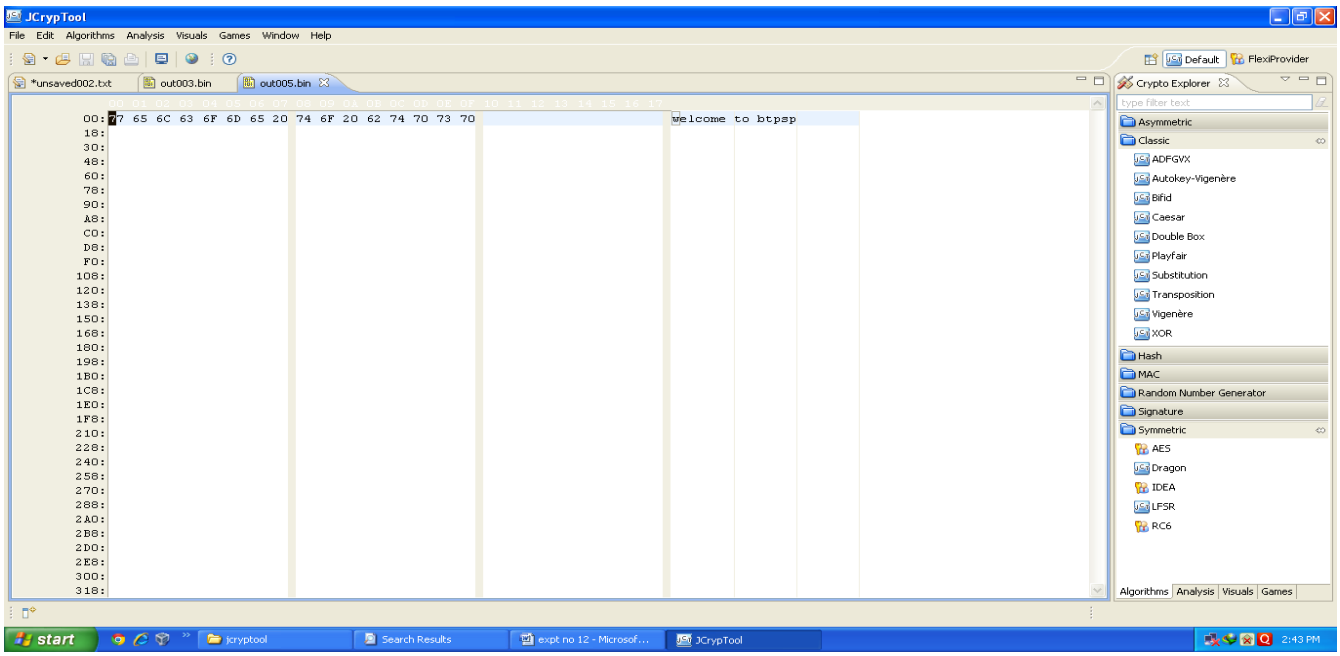



JCrypTool
File Edit Algorithms Analysis Visuals Games Window Help
AES encryption
AES
To en- or decrypt a message with the AES algorithm, choose a key (manually, from the key store, or a newly created key) and pick a padding and block cipher mode.
Operation
Encrypt
Decrypt
Key Source
Custom key
Key from keystore
Keystore
Select key: "Alice Whitehat" - secret key - 128 bit
or:
Create a new key in the keystore
Mode and Padding Scheme
Mode: (ECB) Electronic Codebook
Padding: PKCS#5 Padding
Finish
Cancel
*unsaved002.txt
welcome to btpsp
Default
FlexiProvider
Crypto Explorer
type filter text
Asymmetric
Classic
ADFGVX
Autokey-Vigenère
Bifid
Caesar
Double Box
Playfair
Substitution
Transposition
Vigenère
XOR
Hash
MAC
Random Number Generator
Signature
Symmetric
AES
Dragon
IDEA
LFSR
RC6
Algorithms Analysis Visuals Games
Writable
Insert
1 : 17
start
jcryptool
Search Results
expt no 12 - Microsof...
JCrypTool
2:42 PM

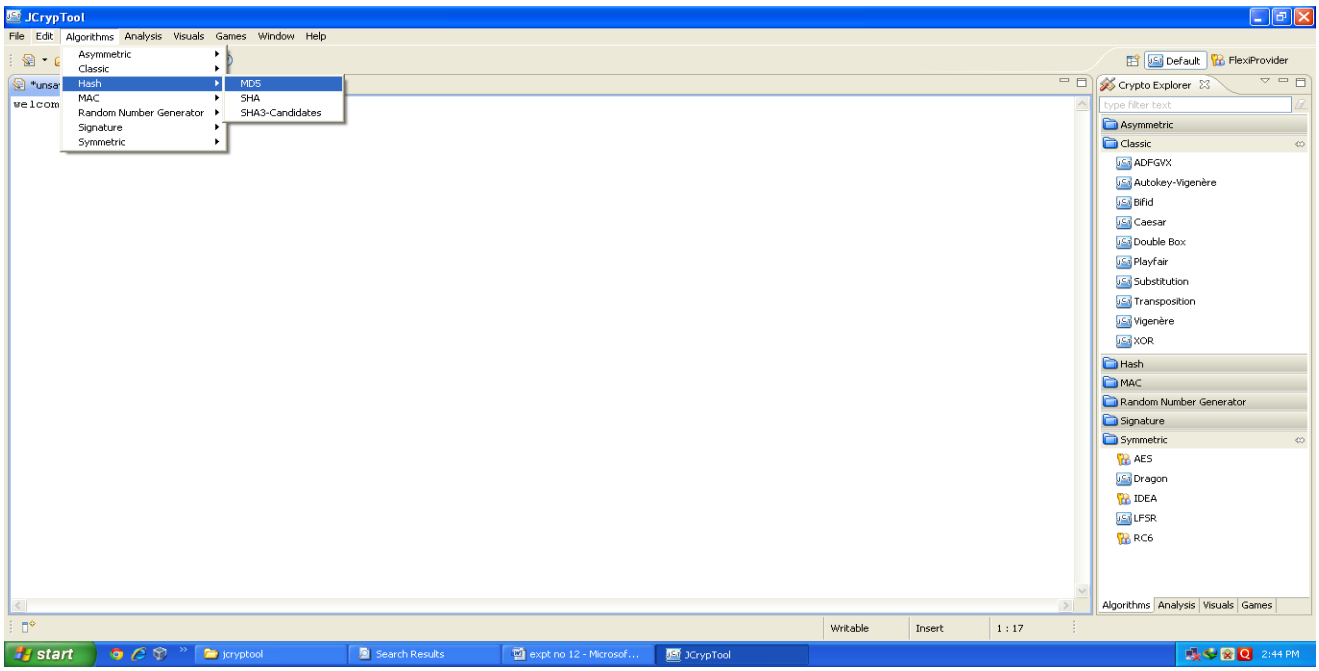

JCrypTool
File Edit Algorithms Analysis Visuals Games Window Help
Default
FlexiProvider
*unsaved002.txt
out003.bin
Crypto Explorer
type filter text
00: BB C7 23 AC 5A 5C 20 B1 82 11 9D 71 06 1A B6 5A 55 96 1D B5 4F 70 34 89
18: 41 2E 71 37 A1 96 17 F6
30:
48:
60:
78:
90:
A8:
C0:
D8:
F0:
108:
120:
138:
150:
168:
180:
198:
1B0:
1C8:
1E0:
1F8:
210:
228:
240:
258:
270:
288:
2A0:
2B8:
2D0:
2E8:
300:
318:
Asymmetric
Classic
ADFGVX
Autokey-Vigenère
Bifid
Caesar
Double Box
Playfair
Substitution
Transposition
Vigenère
XOR
Hash
MAC
Random Number Generator
Signature
Symmetric
AES
Dragon
IDEA
LFSR
RC6
Algorithms Analysis Visuals Games
start
jcryptool
Search Results
expt no 12 - Microsof...
JCrypTool
2:42 PM

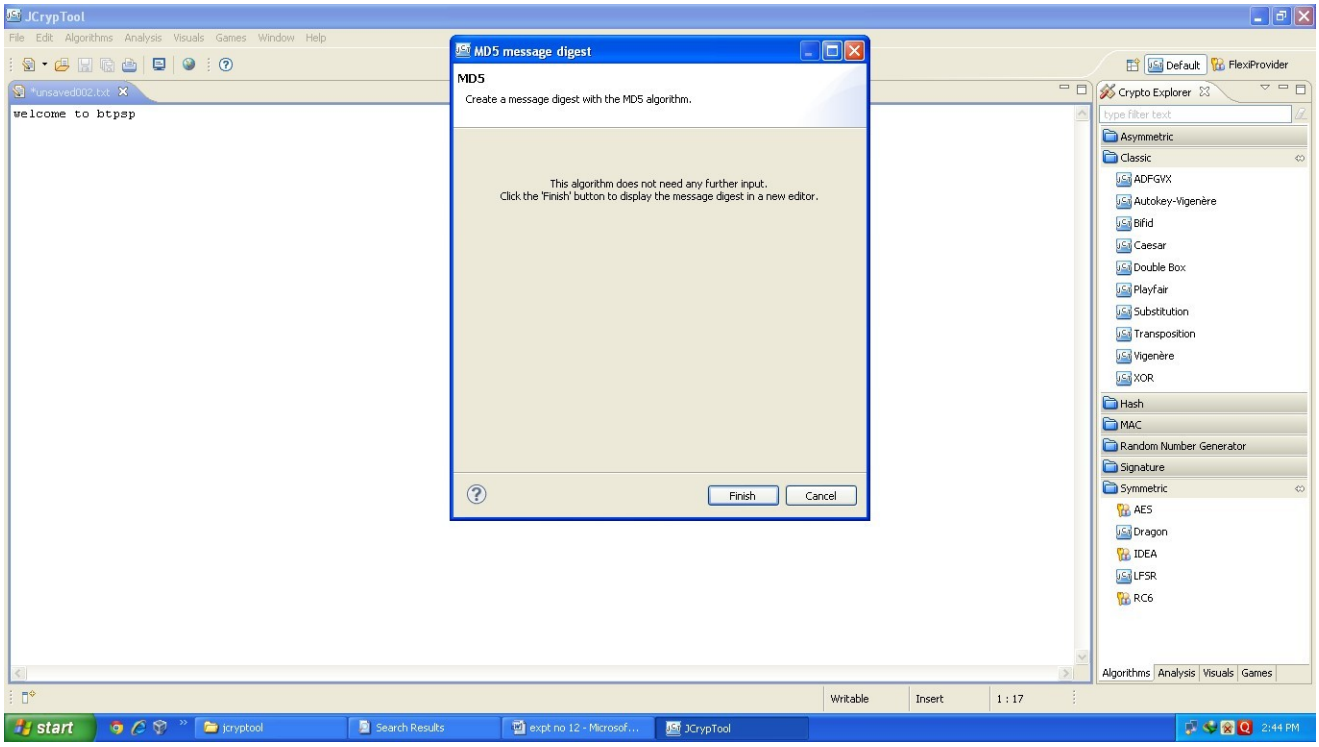

JCrypTool
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved002.txt
out003.bin
00: BB C7 23 AC 5A 5C 20 B1 82 11 9D 71 06 1A
18: 41 2E 71 37 A1 96 17 F6
AES encryption
AES
To en- or decrypt a message with the AES algorithm, choose a key (manually, from the key store, or a newly created key) and pick a padding and block cipher mode.
Operation
Encrypt
Decrypt
Key Source
Custom key
Key from keystore
Keystore
Select key: "Alice Whitehat" - secret key - 128 bit
or:
Create a new key in the keystore
Mode and Padding Scheme
Mode: (ECB) Electronic Codebook
Padding: PKCS#5 Padding
Finish
Cancel
Default
FlexiProvider
Crypto Explorer
type filter text
Asymmetric
Classic
ADFGVX
Autokey-Vigenère
Bifid
Caesar
Double Box
Playfair
Substitution
Transposition
Vigenère
XOR
Hash
MAC
Random Number Generator
Signature
Symmetric
AES
Dragon
IDEA
LFSR
RC6
Algorithms Analysis Visuals Games
start
jcryptool
Search Results
expt no 12 - Microsof...
JCrypTool
2:43 PM

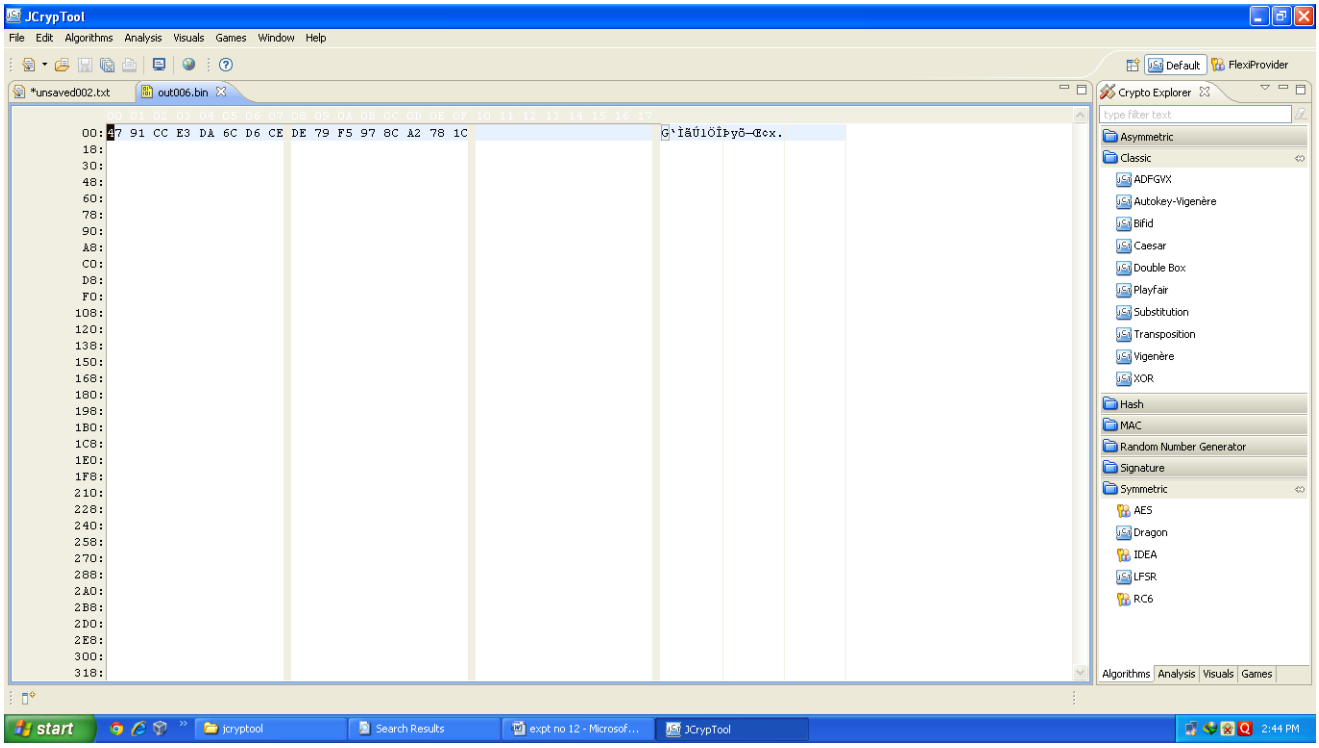

JCrypTool
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved002.txt
out003.bin
00: BB C7 23 AC 5A 5C 20 B1 82 11 9D 71 06 1A B6 5A 55 96 1D B5 4F 70 34 89
18: 41 2E 71 37 A1 96 17 F6
Enter Password
Please enter the key protection password
***
OK
Cancel
Default
FlexiProvider
Crypto Explorer
type filter text
Asymmetric
Classic
ADFGVX
Autokey-Vigenère
Bifid
Caesar
Double Box
Playfair
Substitution
Transposition
Vigenère
XOR
Hash
MAC
Random Number Generator
Signature
Symmetric
AES
Dragon
IDEA
LFSR
RC6
Algorithms Analysis Visuals Games
start
jcryptool
Search Results
expt no 12 - Microsof...
JCrypTool
2:43 PM



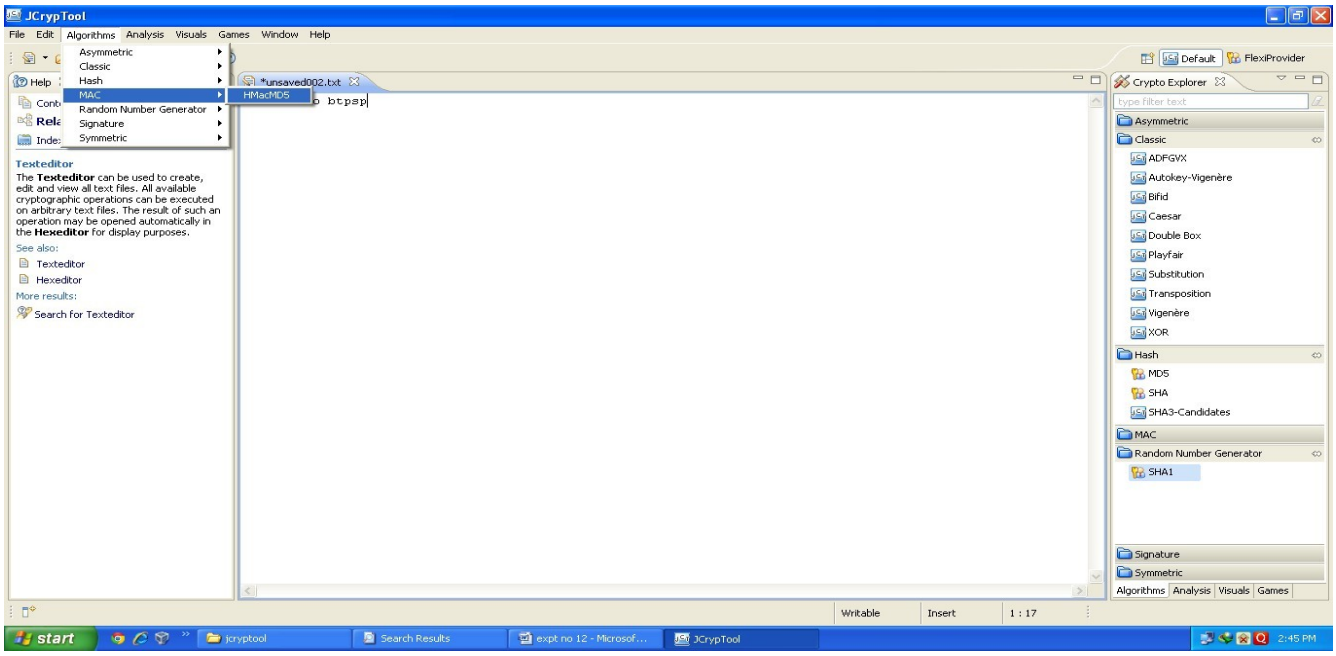
Steps for MD5

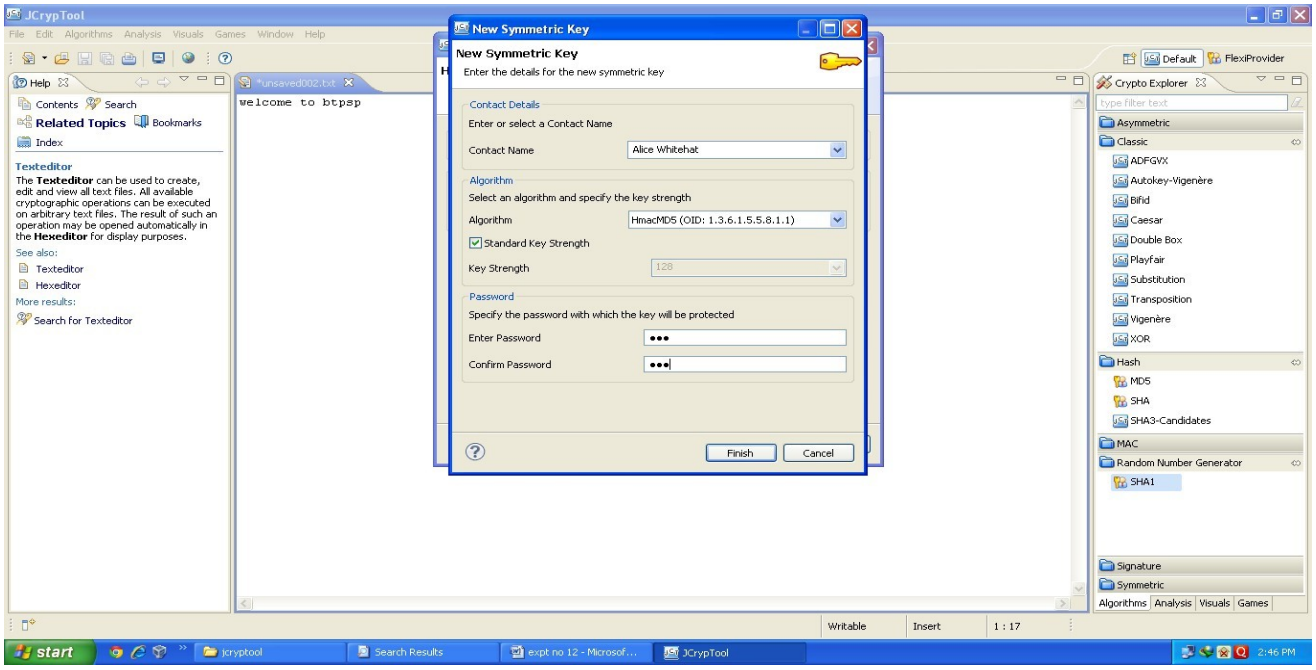


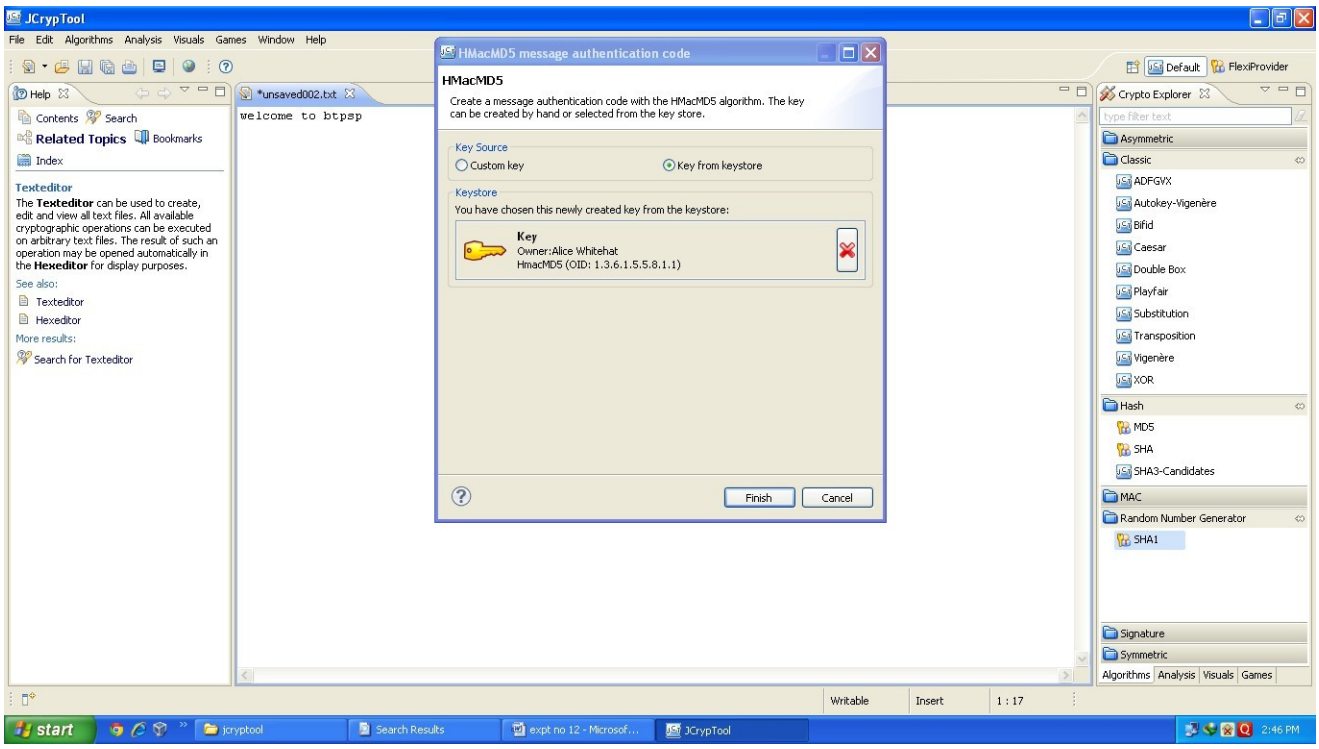

JCrypTool
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved002.txt
welcome to btpsp
MD5 message digest
MD5
Create a message digest with the MD5 algorithm.
This algorithm does not need any further input.
Click the 'Finish' button to display the message digest in a new editor.
Finish
Cancel
Default
FlexiProvider
Crypto Explorer
type filter text
Asymmetric
Classic
ADFGVX
Autokey-Vigenère
Bifid
Caesar
Double Box
Playfair
Substitution
Transposition
Vigenère
XOR
Hash
MAC
Random Number Generator
Signature
Symmetric
AES
Dragon
IDEA
LFSR
RC6
Algorithms Analysis Visuals Games
Writable
Insert
1 : 17
start
jcryptool
Search Results
expt no 12 - Microsof...
JCrypTool
2:44 PM

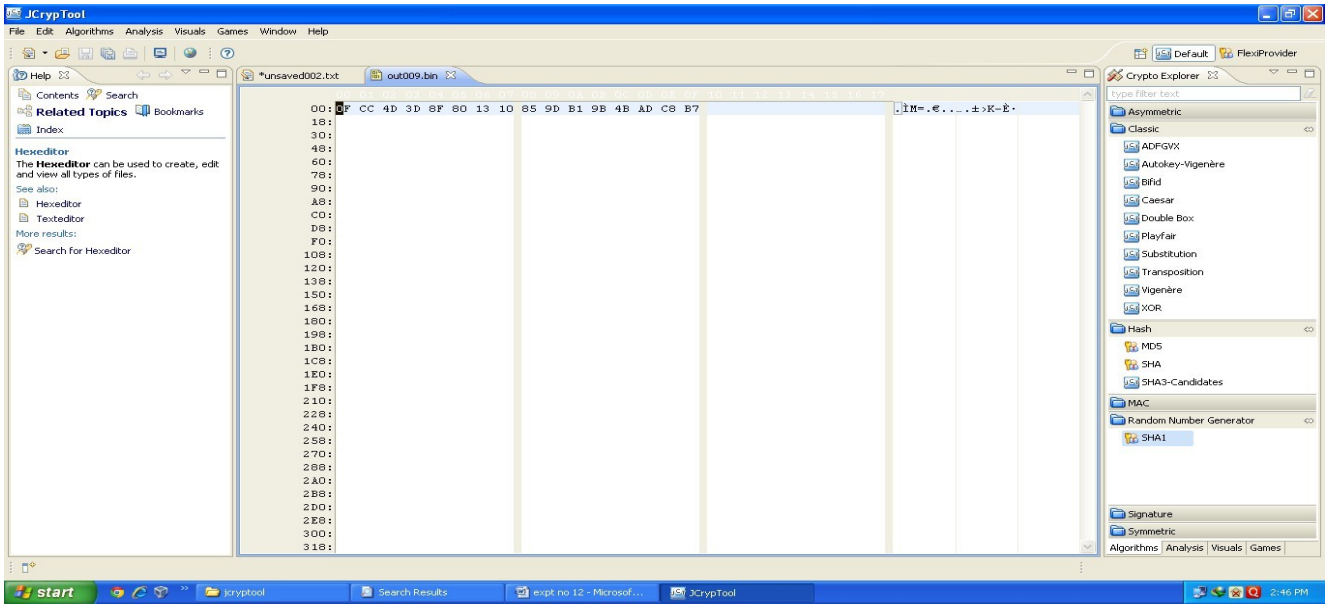

JCrypTool
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved002.txt
out006.bin
00: 97 91 CC E3 DA 6C D6 CE DE 79 F5 97 8C A2 78 1C
18:
30:
48:
60:
78:
90:
A8:
C0:
D8:
F0:
108:
120:
138:
150:
168:
180:
198:
1B0:
1C8:
1E0:
1F8:
210:
228:
240:
258:
270:
288:
2A0:
2B8:
2D0:
2E8:
300:
318:
Default
FlexiProvider
Crypto Explorer
type filter text
Asymmetric
Classic
ADFGVX
Autokey-Vigenère
Bifid
Caesar
Double Box
Playfair
Substitution
Transposition
Vigenère
XOR
Hash
MAC
Random Number Generator
Signature
Symmetric
AES
Dragon
IDEA
LFSR
RC6
Algorithms Analysis Visuals Games
start
jcryptool
Search Results
expt no 12 - Microsof...
JCrypTool
2:44 PM

Steps for MAC






JCrypTool
File Edit Algorithms Analysis Visuals Games Window Help
HMacMD5 message authentication code
HMacMD5
Create a message authentication code with the HMacMD5 algorithm. The key can be created by hand or selected from the key store.
Key Source
Custom key
Key from keystore
Keystore
You have chosen this newly created key from the keystore:
Key
Owner:Alice Whitehat
HmacMD5 (OID: 1.3.6.1.5.5.8.1.1)
Finish
Cancel
*unsaved002.txt
welcome to btpsp
Crypto Explorer
Asymmetric
Classic
ADFGVX
Autokey-Vigenère
Bifid
Caesar
Double Box
Playfair
Substitution
Transposition
Vigenère
XOR
Hash
MD5
SHA
SHA3-Candidates
MAC
Random Number Generator
SHA1
Signature
Symmetric
Writable
Insert
1 : 17
start
jcryptool
Search Results
expt no 12 - Microsof...
JCrypTool
2:46 PM


JCrypTool
File Edit Algorithms Analysis Visuals Games Window Help
*unsaved002.txt
out009.bin
00: 0F CC 4D 3D 8F 80 13 10 85 9D B1 9B 4B AD C8 B7
18:
30:
48:
60:
78:
90:
A8:
C0:
D8:
F0:
108:
120:
138:
150:
168:
180:
198:
1B0:
1C8:
1E0:
1F8:
210:
228:
240:
258:
270:
288:
2A0:
2B8:
2D0:
2E8:
300:
318:
Crypto Explorer
Asymmetric
Classic
ADFGVX
Autokey-Vigenère
Bifid
Caesar
Double Box
Playfair
Substitution
Transposition
Vigenère
XOR
Hash
MD5
SHA
SHA3-Candidates
MAC
Random Number Generator
SHA1
Signature
Symmetric
start
jcryptool
Search Results
expt no 12 - Microsof...
JCrypTool
2:46 PM

EXP NO 12: DEMONSTRATE INTRUSION DETECTION SYSTEM (IDS) USING ANY TOOL EG. SNORT OR ANY OTHER S/W

Snort can be configured to run in three modes:

1. Sniffer mode.
2. Packet Logger mode.
3. Network Intrusion Detection System mode.

1. **Sniffer mode:** Snort –v Print out the TCP/IP packets header on the screen.
   Snort –vd show the TCP/IP ICMP header with application data in transit.

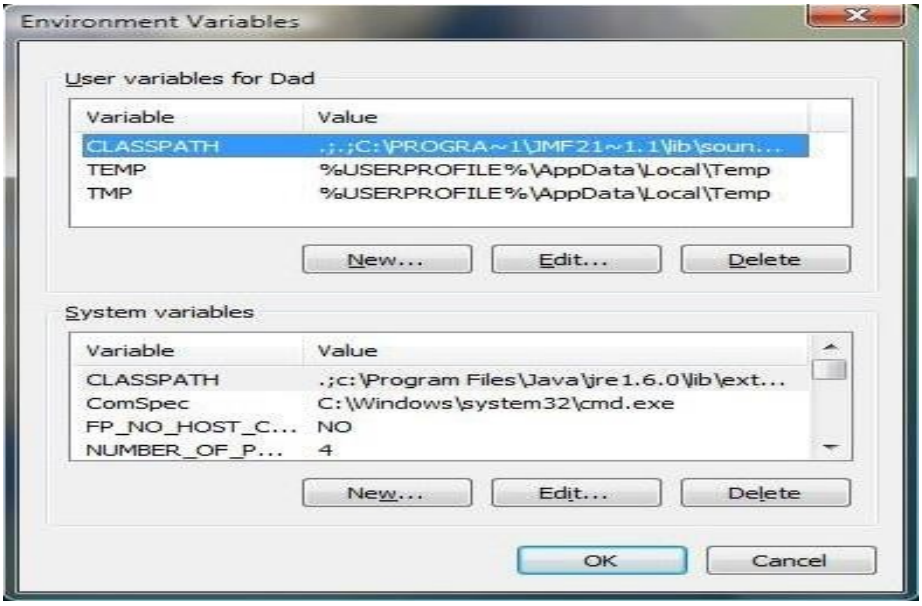
2. **Packet Logger mode:** Snort –dev -1 C:\log [Create this directory in the C drive] and snort will automatically know to go into packet logger mode, it collects every packet it sees and places it in log directory.
   Snort –dev -1 C:\log –h IP address\24. This rule tells snort that you want to print out the data link and TCP/IP headers as well as application data into the log directory.
   Snort -1 C:\log –b This is binary mode logs everything into a single file.

3. **Network Intrusion Detection System mode:**snort –d C:\log –h IP address\24 –c snort.conf
   This is a configuration file applies rule to each packet to decide it an action based upon the rule type in the file.
   Snort –d –h IP address\24 -1 C:\log –c snort.conf
   This will configure snort to run in its most basic NIDS form, logging packets that trigger rules specifies in the snort.conf

Steps:

1. Download Snort from snort.org
2. Install snort with or without database support.

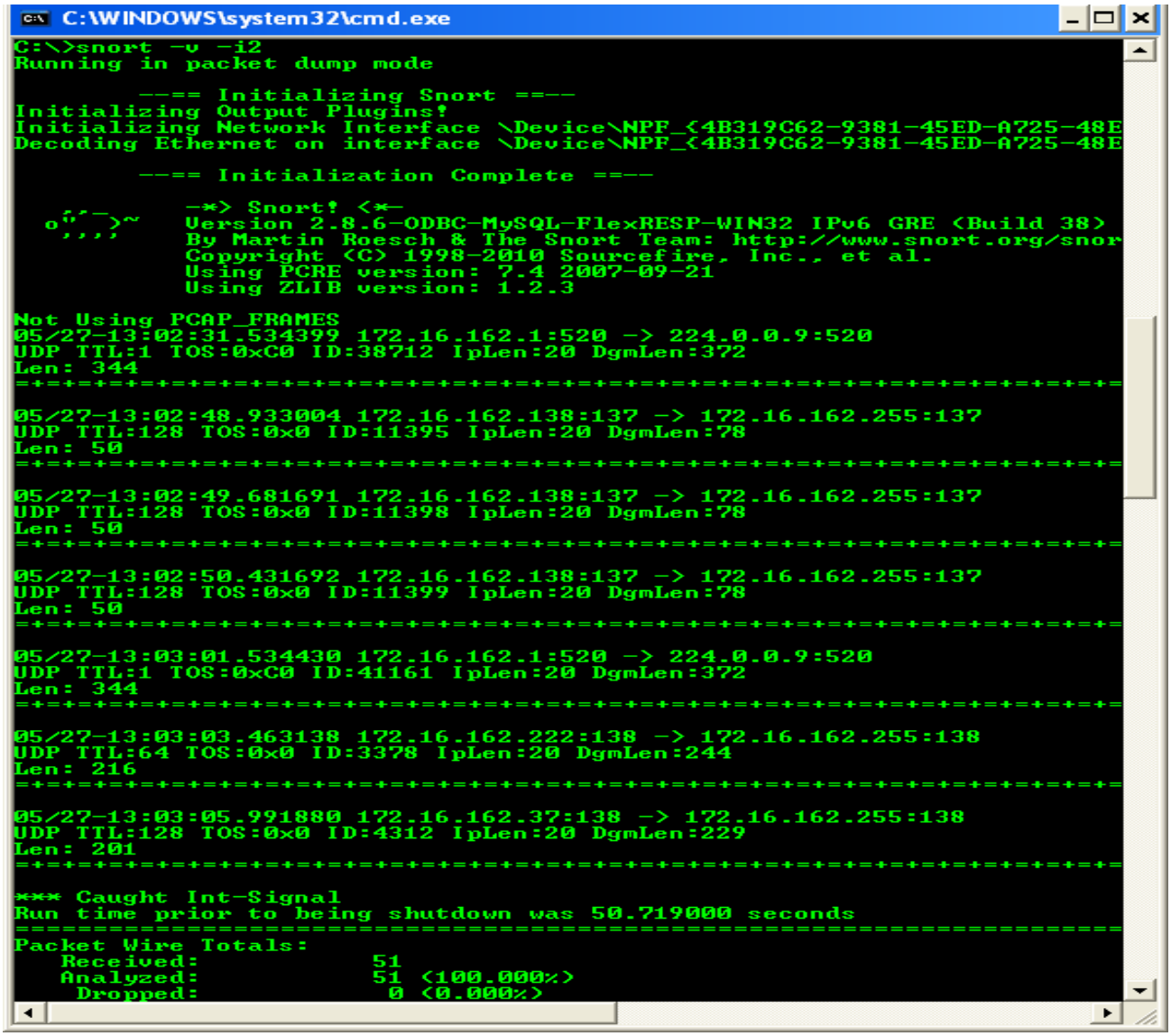
3. Select all the components and Click Next.
4. Install and Close.
5. Skip the Winpcap driver installation.
6. Add the path variable in windows environment variable by selecting new classpath.
7. Create a path variable and point it at snort.exe variable name→path and variable value→C:\snort\bin.



8. Click OK button and then close all the dialog boxes.
9. Open command prompt and type the following commands.

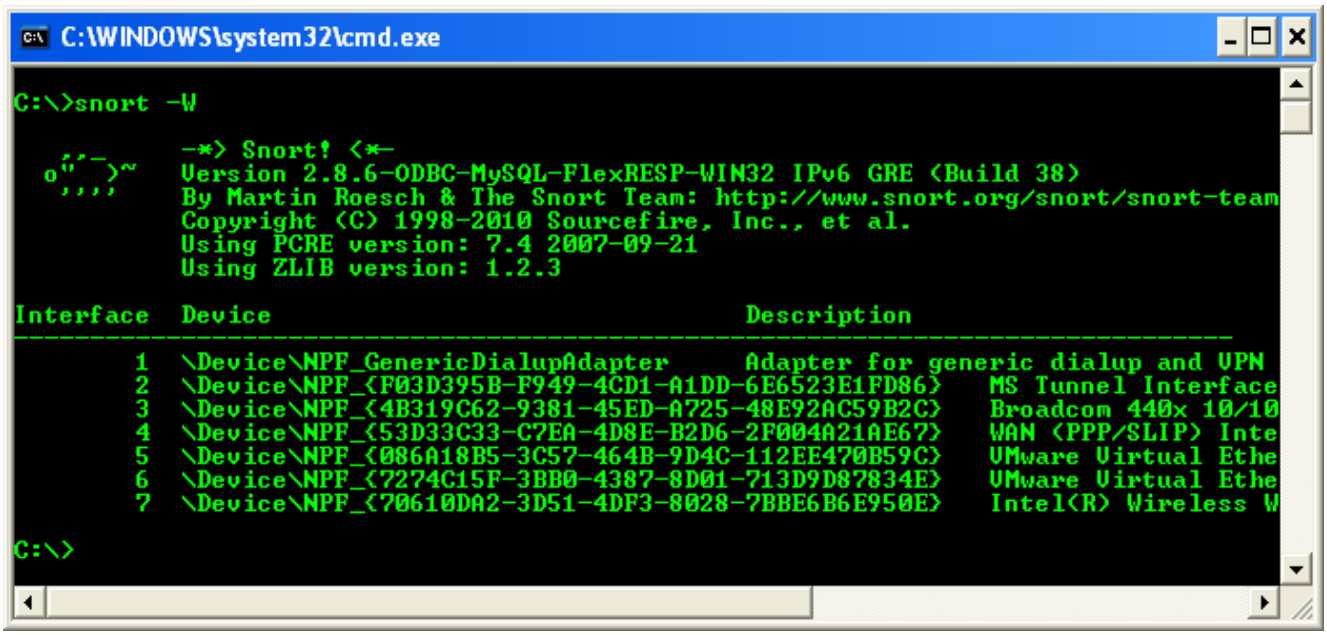
To receive a more detailed capture of packets on the wire, type:

C:\>snort -vd -i2



This command provides the TCP/IP headers and packet information (descriptive). Type snort at the command line for a full list of all the switches. If you're getting TCP headers, you know that so far, you're right on track. If you have more than one network card in your Snort IDS system, type:

C:\>snort -W



EXPT NO: 13 INSTALL ROOTKITS AND STUDY VARIETY OF OPTIONS.

A Rootkit is a stealthy type of malicious software (malware) designed to hide the existence of certain processes or programs from normal methods of detection and enables continued privileged access to a computer.

The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implements the tool). The term "rootkit" has negative connotations through its association with malware.

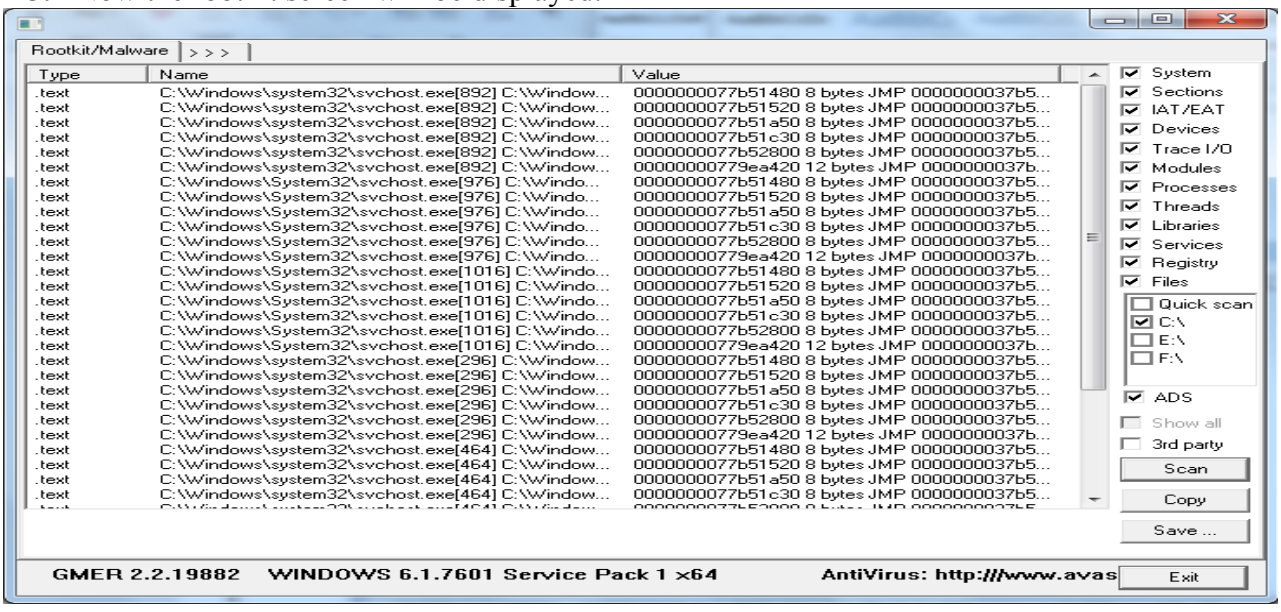
A rootkit is a collection of tools (programs) that enables administrator-level access to a computer or computer network.

A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files;

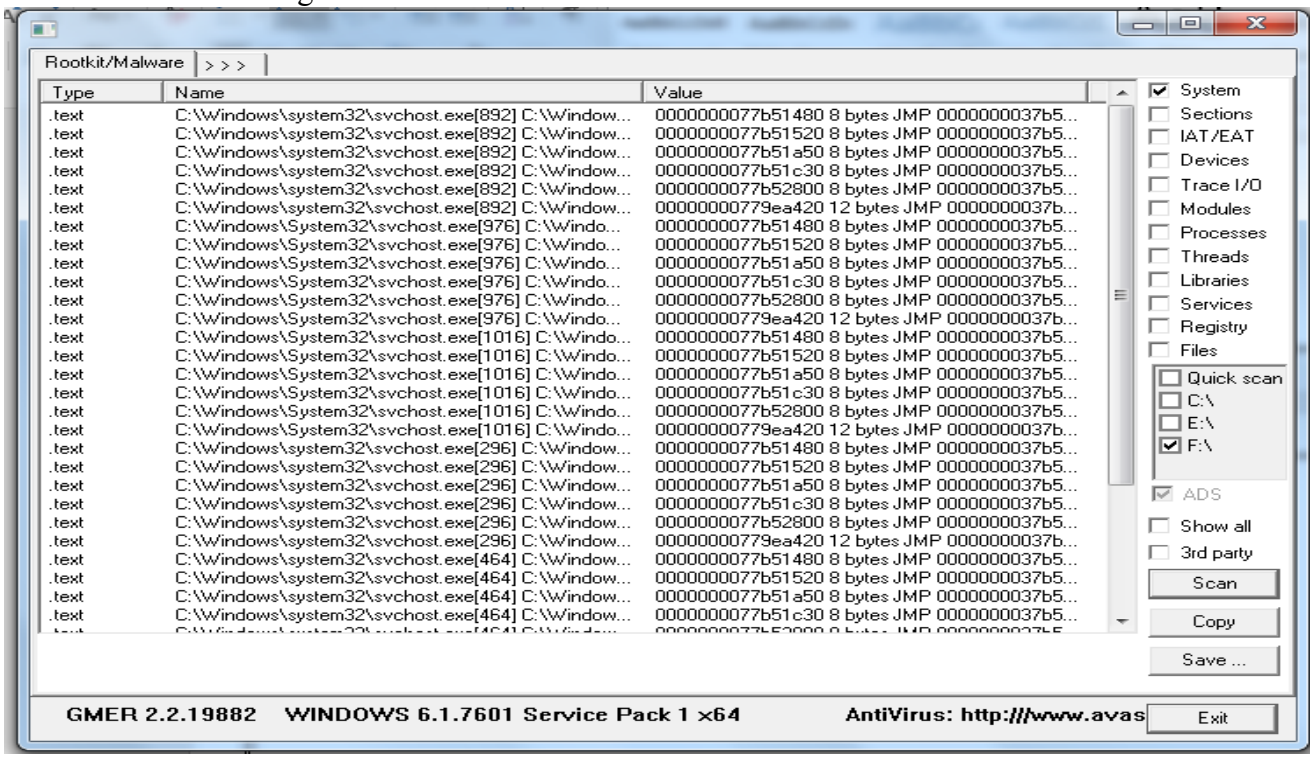
Attack other machines on the network; and alter existing system tools to escape detection.

Steps:

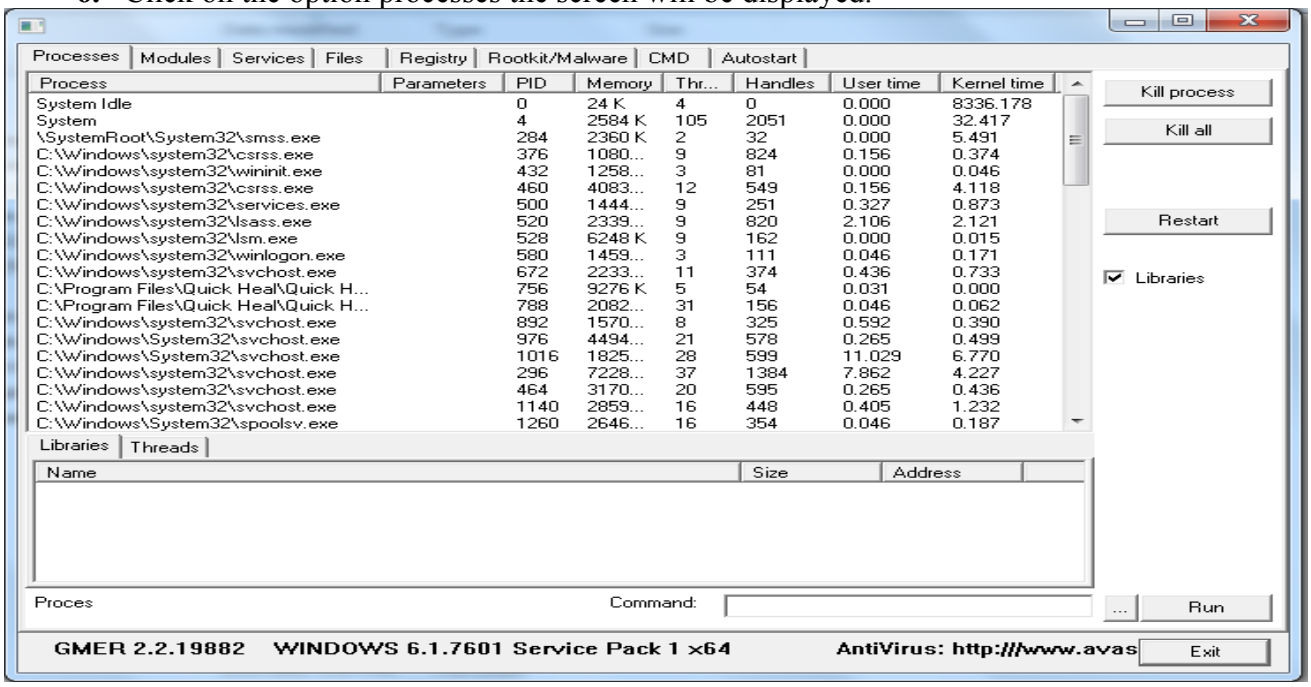
1. Double click on rootkit folder
2. Double click on the GMER rootkit application.
3. Now the rootkit screen will be displayed.



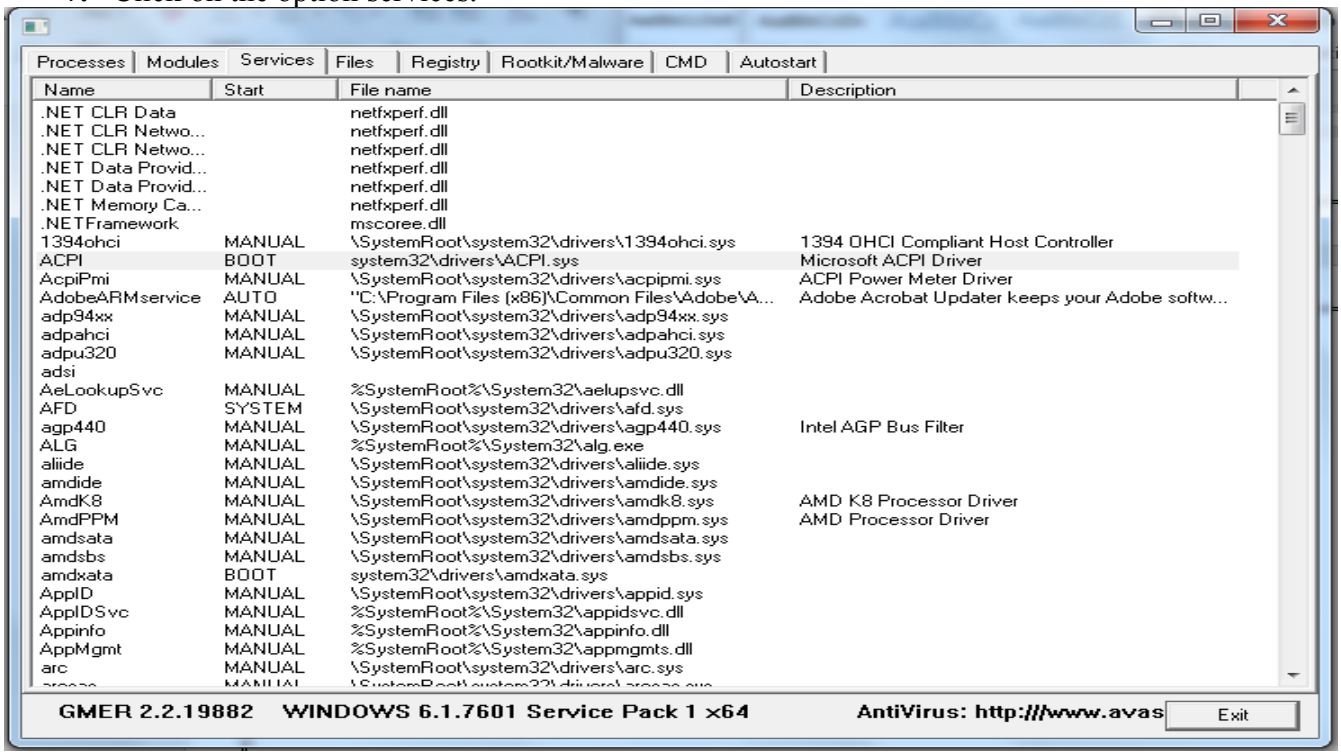
4. Select anyone of the drive which is shown at right side of the screen.
5. After selecting the drive click on scan button.



6. Click on the option processes the screen will be displayed.



7. Click on the option services.



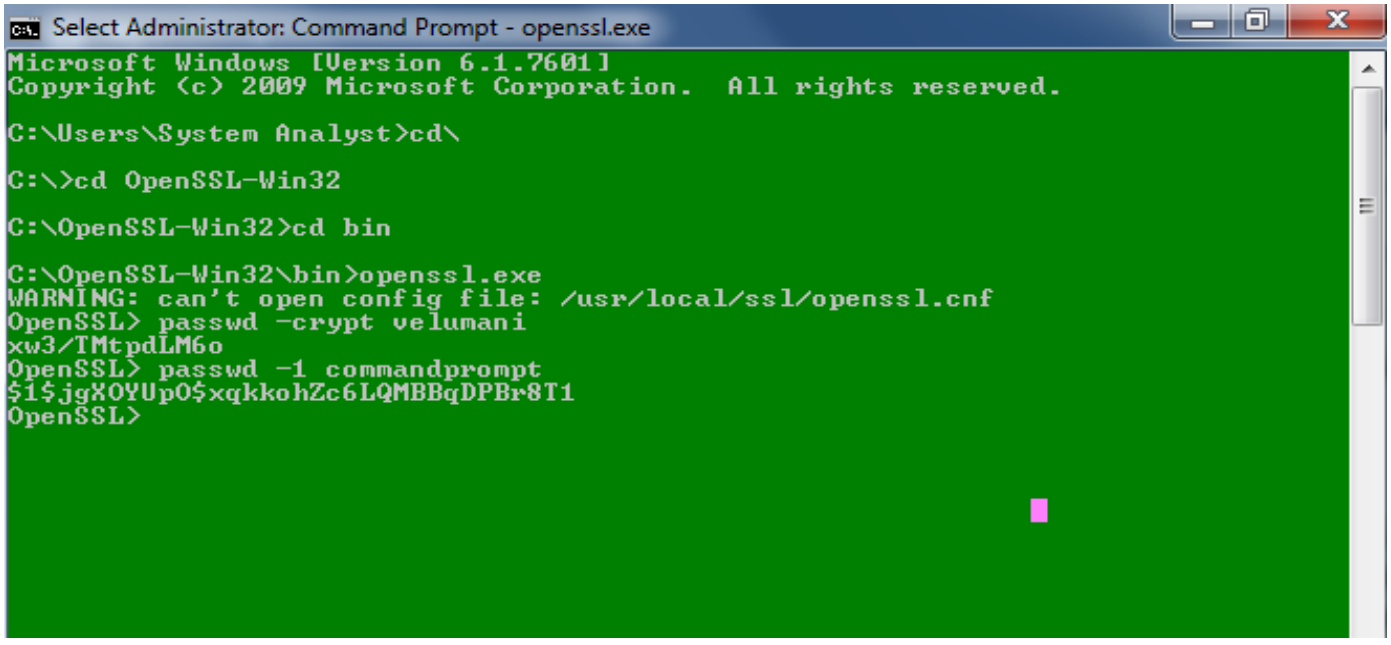
8. Now click on different options to perform different actions.

EXPT NO :14 GENERATING PASSWORD HASHES WITH OPENSSL

The OpenSSL is a command line binary can perform a wide range of cryptographic operation.

Steps:

1. Install OpenSSL setup file on to the default location.
2. Perform Full installation and click Next.
3. Create Document shortcuts in start menu and Click Next. Complete the installation.
4. Execute the OpenSSL from command prompt available at C:\ProgramFiles\OpenSSL-Win32\bin\openssl.exe OpenSSL>(This is the OpenSSL prompt)
5. Now execute the command as follows for password generation.
6. Passwd -crypt [Type your password] This is limited to 8 characters password generator.
7. Passwd -1 [Type your password] This allows you to insert password length beyond 8 characters.
8. Type this command to generate 10-12 characters passwords of 10 numbers.



EXPT NO: 15 SETUP A HONEY POT AND MONITOR THE HONEY POT ON NETWORK

WHAT IS A HONEYPOT?

A honeypot is a device placed on a computer network specifically designed to capture malicious network traffic.

Honeypots are becoming one of the leading security tools used to monitor the latest tricks and exploits of hackers by recording their every move so that the security community can more quickly respond to new exploits.

Types of honey pots

1. Production honey pots
2. Research honey pots

Honey pots

Two or more honey pots on a network from a honey-net. Honey pots and honey-net are usually implemented as a part of larger network IDS

Steps:

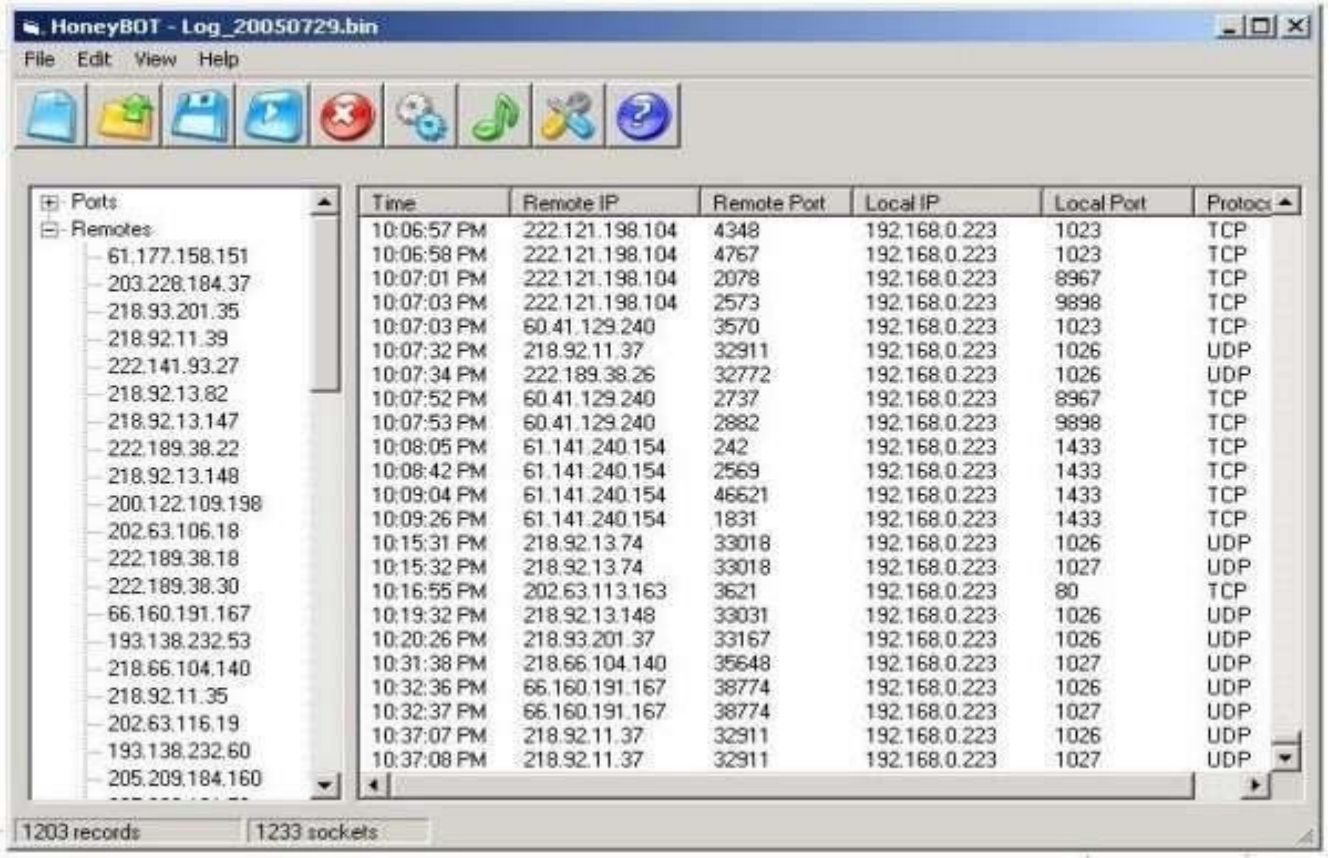
1. Click on setup file to start setup.
2. Click on next.
3. Click on agree and click next.
4. Installation process starts.
5. Open the KF sensor and view all the ports available in the network as shown below.
6. Then click on the visitors button and view all the recent visitors who have accessed the particular data from a particular host present in the network. You can also view the services which are running on the host system.

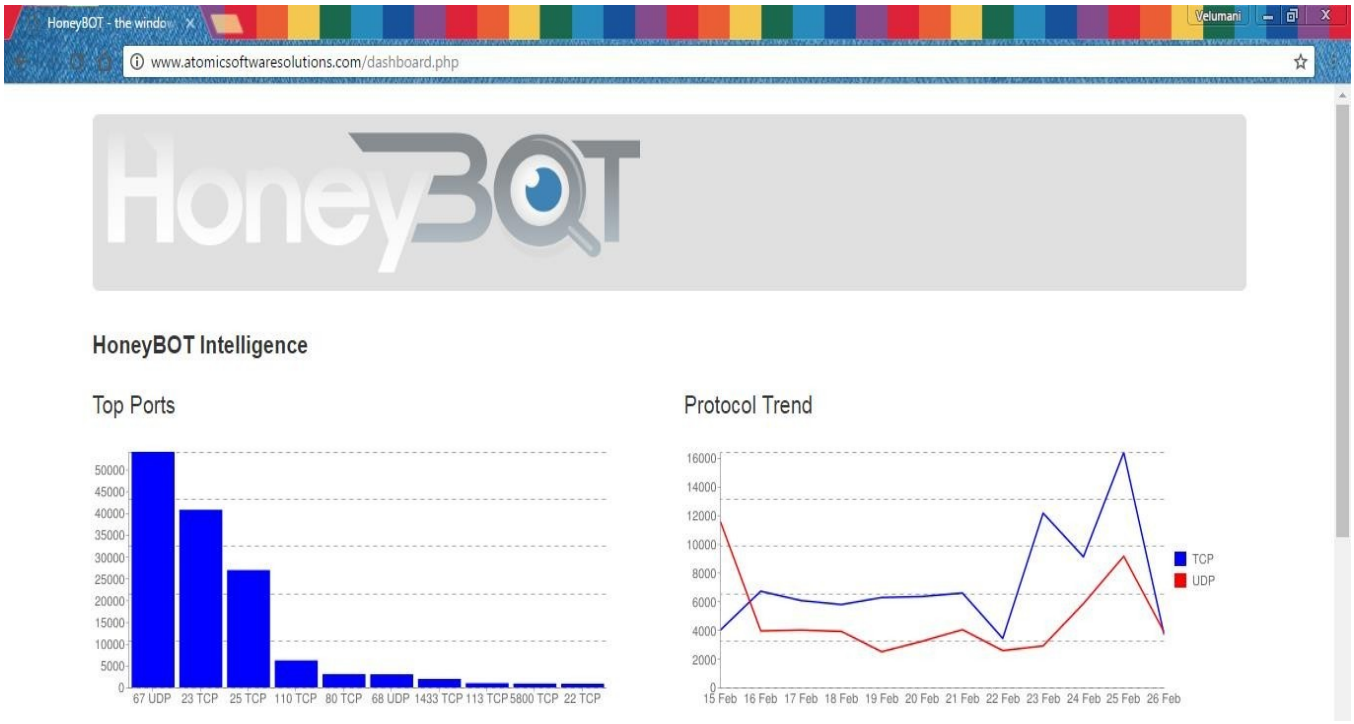
Installing Honeypot:

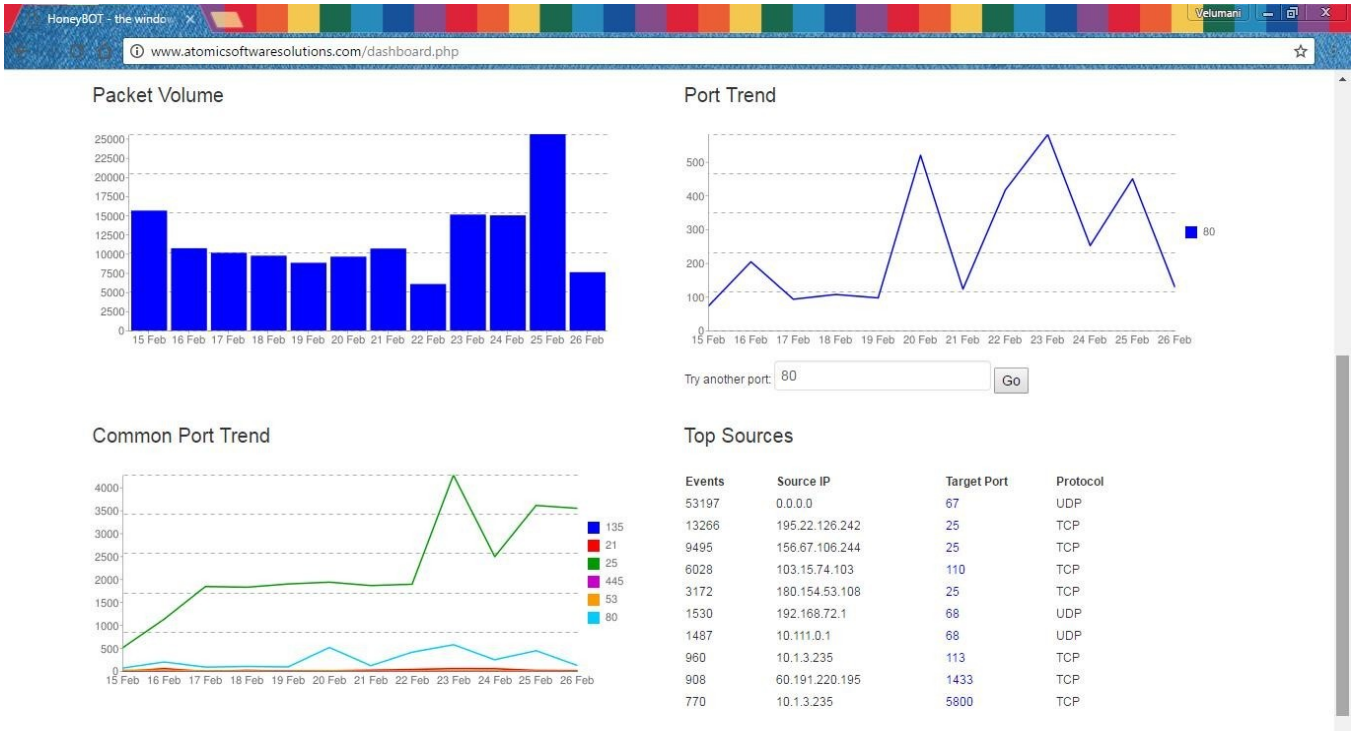
Honeypot is compatible with and has tested to work on windows 2000 and windows XP computers. At least 128MB of ram is recommended.

Steps:

1. Honeypot can be downloaded from the website at: http://www.atomicsoftwaresolutions.com/honeybot.php
2. After clicking the download link save HoneyBot_010.exe to a location on your hard drive.
3. Double click the honeybot_010.exe installation file to begin the setup process.
4. Follow the prompts in the setup process. The default installation folder for the setup is C:\honeybot\
5. Setup will create a shortcut in the Start Menu folder and an option is available to create a desktop icon.
6. Now you can launch Honeybot using the programs shortcut icon.




HoneyBOT - the windo
Velumani
www.atomicsoftwaresolutions.com/dashboard.php
HoneyBOT
HoneyBOT Intelligence
Top Ports
50000
45000
40000
35000
30000
25000
20000
15000
10000
5000
0
67 UDP
23 TCP
25 TCP
110 TCP
80 TCP
68 UDP
1433 TCP
113 TCP
5800 TCP
22 TCP
Protocol Trend
16000
14000
12000
10000
8000
6000
4000
2000
0
15 Feb
16 Feb
17 Feb
18 Feb
19 Feb
20 Feb
21 Feb
22 Feb
23 Feb
24 Feb
25 Feb
26 Feb
TCP
UDP


HoneyBOT - the windo
Velumani
www.atomicsoftwaresolutions.com/dashboard.php
Packet Volume
25000
22500
20000
17500
15000
12500
10000
7500
5000
2500
0
15 Feb
16 Feb
17 Feb
18 Feb
19 Feb
20 Feb
21 Feb
22 Feb
23 Feb
24 Feb
25 Feb
26 Feb
Port Trend
500
400
300
200
100
0
80
Try another port:
80
Go
Common Port Trend
4000
3500
3000
2500
2000
1500
1000
500
0
135
21
25
445
53
80
Top Sources
Events
Source IP
Target Port
Protocol
53197
0.0.0.0
67
UDP
13266
195.22.126.242
25
TCP
9495
156.67.106.244
25
TCP
6028
103.15.74.103
110
TCP
3172
180.154.53.108
25
TCP
1530
192.168.72.1
68
UDP
1487
10.111.0.1
68
UDP
960
10.1.3.235
113
TCP
908
60.191.220.195
1433
TCP
770
10.1.3.235
5800
TCP