

<b>Branch: CSE (IVYear / VII SEM)</b>	<b>L</b>	<b>T</b>	<b>P</b>	<b>MARKS</b>
<b>7CS4-22: Cyber Security Lab</b>	<b>0</b>	<b>0</b>	<b>4</b>	<b>100(IA:60, ETE:40)</b>
<b>Total Hours – 30</b>				
<b>Credit-2</b>				
<b>COURSE ASSESSMENT METHOD: Two midterm and one end term examination</b>				
<b>PRE-REQUISITES: Basics Computer and Network knowledge.</b>				

### **EXPERIMENT 1**

#### **AIM:**

Introduction of cyber security

#### **Objective:**

Student should be able to understand the concept of cyber security, Cyber threats and Cyber security related tools

**Outcomes:** Students are able to identify the cyber attacks and they got an idea what is the need of cyber security lab in their curriculum.

#### **THEORY:**

- What is cyber security?

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

- Why is cyber security important?

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

- Cyber attacks can be extremely expensive for businesses to endure.
  - In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
  - Cyber-attacks these days are becoming progressively destructive.
- Cybercriminals are using more sophisticated ways to initiate cyber attacks.

- Types of Cyber Attacks

- A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft. Cyber-attacks can be classified into the following categories:

1. Web-based attacks and
2. System based attack

- Web-based attacks

- ✓ These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information. Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following:

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

- System-based attacks

System-based attacks These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

### **Vulnerability, threat**

- Vulnerability, threat, Harmful acts as the recent epidemic of data breaches illustrates, no system is immune to attacks.

- Any company that manages, transmits, stores, or otherwise handles data has to institute and enforce mechanisms to monitor their cyber environment, identify vulnerabilities, and close up security holes as quickly as possible. Before identifying specific dangers to modern data systems, it is crucial to understand the distinction between cyber threats and vulnerabilities.
- Cyber threats are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.
- Examples of common types of security threats include phishing attacks that result in the installation of malware that infects your data, failure of a staff member to follow data protection protocols that cause a data breach, or even a tornado that takes down your company's data headquarters, disrupting access.
- Vulnerabilities are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them.
- Types of vulnerabilities in network security include but are not limited to SQL injections, server misconfigurations, cross-site scripting, and transmitting sensitive data in a nonencrypted plain text format.
- When threat probability is multiplied by the potential loss that may result, cyber security experts, refer to this as a risk.

### CIA Triad

- The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.
- CIA triad broken down:
  - Confidentiality
    - It's crucial in today's world for people to protect their sensitive, private information from unauthorized access. Protecting confidentiality is dependent on being able to define and enforce certain access levels for information. In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached. Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and Unix file permissions.
    - Integrity
 

Data integrity is what the "I" in CIA Triad stands for. This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

- Availability

This is the final component of the CIA Triad and refers to the actual availability of your data. Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it's available when it is needed.

Understanding the CIA triad The CIA Triad is all about information. While this is considered the core factor of the majority of IT security, it promotes a limited view of the security that ignores other important factors. For example, even though availability may serve to make sure you don't lose access to resources needed to provide information when it is needed, thinking about information security in itself doesn't guarantee that someone else hasn't used your hardware resources without authorization. It's important to understand what the CIA Triad is, how it is used to plan and also to implement a quality security policy while understanding the various principles behind it. It's also important to understand the limitations it presents. When you are informed, you can utilize the CIA Triad for what it has to offer and avoid the consequences that may come along by not understanding it.

### Assets and Threat

- An asset is any data, device or other component of an organization's systems that is valuable – often because it contains sensitive data or can be used to access such information.
- For example: An employee's desktop computer, laptop or company phone would be considered an asset, as would applications on those devices.
- Likewise, critical infrastructure, such as servers and support systems, are assets.
- An organization's most common assets are information assets. These are things such as databases and physical files – i.e. the sensitive data that you store
- A threat is any incident that could negatively affect an asset – for example, if it's lost, knocked offline or accessed by an unauthorized party.
- Threats can be categorized as circumstances that compromise the confidentiality, integrity or availability of an asset, and can either be intentional or accidental.
- Intentional threats include things such as criminal hacking or a malicious insider stealing information, whereas accidental threats generally involve employee error, a technical malfunction or an event that causes physical damage, such as a fire or natural disaster.

## EXPERIMENT 2

### AIM:

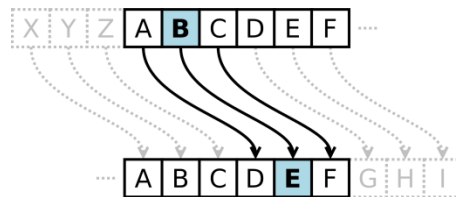
Implement the following Substitution & Transposition Techniques concepts:

- a) Caesar Cipher
- b) Rail fence row & Column Transformation

### THEORY:

#### Caesar Cipher

- The Caesar Cipher, named after Julius Caesar of Ancient Rome, is a type of substitution cipher where each letter of the original (plaintext) message is substituted with another letter.
- **Encrypting with the Caesar Cipher**
  - But how do we decide what letter is replaced by what? That's where the **key** comes into play. Found in almost every encryption algorithm, the key determines **how the data is encrypted**.
  - In the Caesar cipher, the key is a number from 0 to 25, because there are 26 letters in the alphabet. This means that for any given message, there are 26 different ways we can encrypt the message.
  - For each letter, the key determines **which letter is replacing the current letter, by counting down the alphabet**. In the following example, let's say we wanted to encrypt the letter B with a key of 3, we would find the 3rd letter that appears after B - which is C, D, then finally E.



- This can easily be shown by lining up two alphabets, one on top of each other, with the second alphabet starting at the letter shifted 3 letters down. This means that the bottom row should be shifted to the *left*.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

- You might notice that the second row starts has the letters ABC right after Z. This is because when you are shifting down the alphabet, if you reach the end (Z), it will loop around to the beginning (A).
- This type of visual makes it much more clear what letter should become what. If we wanted to encrypt the word BILLY, we would simply take each **unique** plaintext letter (top row) and find its matching ciphertext letter (bottom row), or:

A [B] CDEFGH [I] JK [L] MNOPQRSTUVWXYZ [Y] Z

D [E] FGHIJK [L] MN [O] PQRSTUVWXYZA [B] C

So we clearly see that:

- B becomes E
- I becomes L
- L becomes O
- Y becomes B

(Note that we only have to find unique letters, like the L because each L will always turn into the same letter)

So the final ciphertext is ELOOB. Note that when we reach the end of the alphabet, we keep counting starting with A, B, etc...

## Decrypting with the Caesar Cipher

Decrypting works in a very similar way - except this time, instead of counting “down” the alphabet, you count “up”! As an example, let’s try to decrypt ELOOB using a key of 3 - because we know the result should be our original plaintext, BILLY. Let’s start by aligning our alphabets:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

XYZABCDEFGHIJKLMNOPQRSTUVWXYZ

Notice how this time, instead of shifting the bottom row to the left, now we are shifting it to the *right*. We can then find our ciphertext letters (top row) E,L,O,B and find their corresponding plaintext letters (bottom row).

A [B] CD [E] FGHIJK [L] MN [O] PQRSTUVWXYZ



X [Y] ZA [B] CDEFGH [I] JK [L] MNOPQRSTUVWXYZ

We can now see that:

- E becomes B
- L becomes I
- O becomes L
- B becomes Y

Which gives us our original plaintext, BILLY.

Next, we're going to learn about a python implementation of the Caesar cipher.

### **PROGRAM: (Caesar Cipher)**

```
#include<stdio.h>

#include<string.h>

#include<conio.h>

#include<ctype.h>

void main()
{
    char plain[10], cipher[10];
    int key,i,length;
    int result;
    clrscr();
    printf("\n Enter the plain text:");
    scanf("%s", plain);
    printf("\n Enter the key value:");
    scanf("%d", &key);
    printf("\n \n \t PLAIN TEXT: %s",plain);
    printf("\n \n \t ENCRYPTED TEXT: ");
    for(i = 0, length = strlen(plain); i < length; i++)
```

```

{
    cipher[i]=plain[i] + key;
    if (isupper(plain[i]) && (cipher[i] > 'Z')) cipher[i] = cipher[i] - 26;
    if (islower(plain[i]) && (cipher[i] > 'z')) cipher[i] = cipher[i] - 26;
    printf("%c", cipher[i]);
}
printf("\n \n \t AFTER DECRYPTION : ");
for(i=0;i<'A') plain[i]=plain[i]+26;
if(islower(cipher[i])&&(plain[i]<'a')) plain[i]=plain[i]+26;
printf("%c",plain[i]);
}
getch();
}

```

### **OUTPUT:**

Enter the plain text: Hi

Enter the key value: 3

Plain text: hello

Encrypted text: Koor

After Decryption: Hello

## EXPERIMENT 2 (b)

### AIM:

To write a C program to implement the rail fence transposition technique.

### THEORY:

In the rail fence cipher, the plain text is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we reach the bottom rail. When we reach the top rail, the message is written downwards again until the whole plaintext is written out. The message is then read off in rows.

### **PROGRAM: (Rail Fence)**

```
#include <stdio.h>

#include<conio.h>

#include<string.h>

void main()
{
    int i,j,k,l;
    char a[20],c[20],d[20];
    clrscr();
    printf("\n\t\t RAIL FENCE TECHNIQUE");
    printf("\n\nEnter the input string : ");
    gets(a); l=strlen(a);
    /*Ciphering*/
    for(i=0,j=0;i<l;i++)
    {
        if(i%2==0)
            c[j++]=a[i];
```

```

}
for(i=0;i <1;i++)
{
if(i%2==1)
c[j++]=a[i];
}
c[j]='\0';
printf("\nCipher text after applying rail fence :");
printf("\n%s",c);
/*Deciphering*/
if(l%2==0) k=l/2;
else k=(l/2)+1;
for(i=0,j=0;i<k;i++)
{
d[j]=c[i];
j=j+2;
}
for(i=k,j=1;i<1;i++)
{
d[j]=c[i];
j=j+2;
}
d[1]='\0';
printf("\n Text after decryption\n");
printf("%s",d);
getch();
}

```

### **OUTPUT**

Enter the input string: COMPUTER SCIENCE

Cipher text after applying rail fence: CMUE CECOPTRSINE

Text after decryption: computer science

**RESULT:** Thus the rail fence algorithm had been executed successfully.

### EXPERIMENT 3

#### AIM:

Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).

#### THEORY:

Diffie-Hellman key exchange(DH) is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.

#### **ALGORITHM:**

1. select prime number i.e.  $q$
2. find the primitive root of  $q$  i.e.  $x$
3. Assume private key for user 'A' is  $x$ . Calculating public key for user A is  $Y_A = x^X \text{ mod } q$
4. Assuming private key is  $X_B$ . Calculating public key is  $Y_B$ ,  $Y_B = x^{X_B} \text{ mod } q$
5. Generating secret key  $K$ ,  $K = (Y_A)^{X_B} \text{ mod } q$ ,  $K = (Y_B)^{X_A} \text{ mod } q$
6. Stop

#### **PROGRAM:**

```
<script>
```

```
// This program calculates the Key for two persons
```

```
// using the Diffie-Hellman Key exchange algorithm
```

```
// Power function to return value of  $a^b \text{ mod } P$ 
```

```
function power(a, b, p)
```

```
{
```

```
    if (b == 1)
```

```

        return a;
    else
        return((Math.pow(a, b)) % p);
}

// Driver code
var P, G, x, a, y, b, ka, kb;

// Both the persons will be agreed upon the
// public keys G and P

// A prime number P is taken
P = 23;
document.write("The value of P:" + P + "<br>");

// A primitive root for P, G is taken
G = 9;
document.write("The value of G:" + G + "<br>");

// Alice will choose the private key a
// a is the chosen private key
a = 4;
document.write("The private key a for Alice:" +
               a + "<br>");

// Gets the generated key
x = power(G, a, P);

```

```
// Bob will choose the private key b
// b is the chosen private key
b = 3;

document.write("The private key b for Bob:" +
               b + "<br>");

// Gets the generated key
y = power(G, b, P);

// Generating the secret key after the exchange
// of keys
ka = power(y, a, P); // Secret key for Alice
kb = power(x, b, P); // Secret key for Bob

document.write("Secret key for the Alice is:" +
               ka + "<br>");
document.write("Secret key for the Bob is:" +
               kb + "<br>");

// This code is contributed by Ankita saini

</script>
```



**OUTPUT:**

The value of P : 23

The value of G : 9

The private key a for Alice : 4

The private key b for Bob : 3

Secret key for the Alice is : 9

Secret Key for the Bob is : 9

## EXPERIMENT 4

### AIM:

Installation of virtual machine on system. Familiarisation of Kali Linux

### THEORY:

#### **Virtual machine**

- A virtual machine is a simulated computer system which runs on a physical computer
- In other words, a virtual machine is a computer inside a computer.
- The entire idea of a virtual machine revolves around having a system that distributes resources from our physical host to our Virtual environment.
- The resource distribution is set up via a user's needs so specific limits can be set in terms of CPU that can be used, or space allocated to our virtual machine.
- Settings are created and applied during the installation/ setup of virtual machine, with the hypervisor controlling the actual resource allocation.

#### **What is Virtual Box?**

- Virtual Box is open source software that works for virtualization on computers with X86 architecture.
- This software acts as a hypervisor and you can have several operating systems together on one computer.
- When configuring the virtual machine, the user can specify the number of resources he gives to the virtual machine.
- Resources can include things like CPU number, RAM, and hard drive space.
- Link for starting the Oracle VM virtualbox
  - <https://www.virtualbox.org/manual/ch01.html>

#### **What is Kali Linux?**

- Kali Linux is an operating system designed and developed based on Debian and used for penetration testing.
- The good thing about this operating system is that it has more than 600 different tools for penetration testing.
- And is known as the most famous operating system with security applications.

- Kali Linux has a rolling release in which they try to keep all packages up to date and at the same time be stable. There is also a community version that releases all updates quickly.
- Link for installing kali inside virtualbox
  - <https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/>
  - <https://www.youtube.com/watch?v=e6l-sJRhLP4>

## EXPERIMENT 5

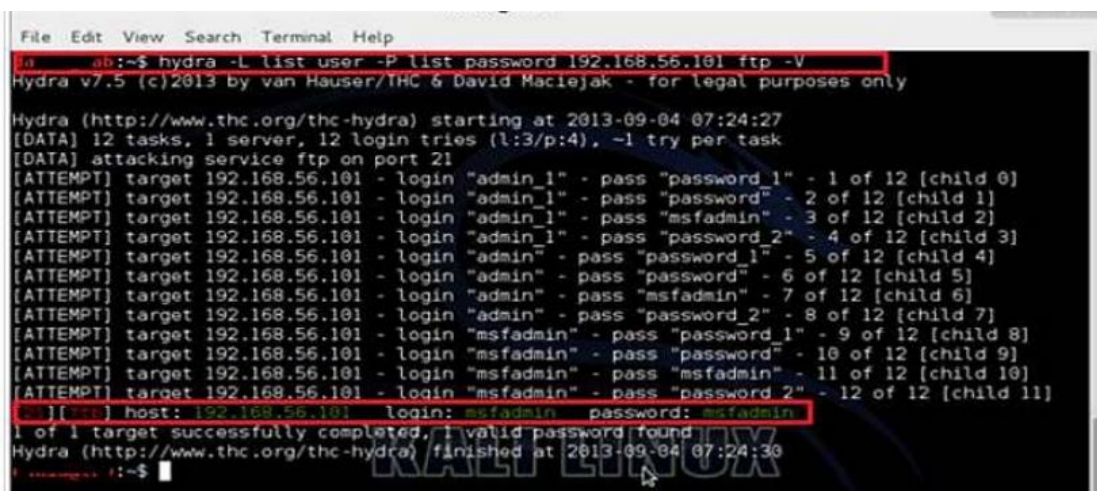
### AIM:

Implement the following Attack:

- a) Dictionary Attack
- b) Brute Force Attack

### THEORY:

- In a dictionary attack, the hacker uses a predefined list of words from a dictionary to try and guess the password.
- If the set password is weak, then a dictionary attack can decode it quite fast.  
**Hydra** is a popular tool that is widely used for dictionary attacks.
- Take a look at the following screenshot and observe how we have used Hydra to find out the password of an FTP service
  - Link for Hydra demonstration-  
<https://www.youtube.com/watch?v=ptYiPqrCU3E>
  - <https://www.youtube.com/watch?v=D2-Eq12hZ1o&t=583s>



```
File Edit View Search Terminal Help
root@kali:~# hydra -L list user -P list password 192.168.56.101 ftp -V
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-09-04 07:24:27
[DATA] 12 tasks, 1 server, 12 login tries (l:3/p:4), -1 try per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password_1" - 1 of 12 [child 0]
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password" - 2 of 12 [child 1]
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "msfadmin" - 3 of 12 [child 2]
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password_2" - 4 of 12 [child 3]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password_1" - 5 of 12 [child 4]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password" - 6 of 12 [child 5]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "msfadmin" - 7 of 12 [child 6]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password_2" - 8 of 12 [child 7]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password_1" - 9 of 12 [child 8]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password" - 10 of 12 [child 9]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "msfadmin" - 11 of 12 [child 10]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password_2" - 12 of 12 [child 11]
[+] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-09-04 07:24:30
root@kali:~#
```

### THEORY: BRUTE FORCE ATTACK

- In a brute-force attack, the hacker uses all possible combinations of letters, numbers, special characters, and small and capital letters to break the password.

- This type of attack has a high probability of success, but it requires an enormous amount of time to process all the combinations.
- A brute-force attack is slow and the hacker might require a system with high processing power to perform all those permutations and combinations faster.
- **John the Ripper** or Johnny is one of the powerful tools to set a brute-force attack and it comes bundled with the Kali distribution of Linux.



- Link for demo - <https://www.youtube.com/watch?v=XjVYl1Ts6XI>

## EXPERIMENT 6

### AIM:

Installation of Wire shark, tcpdump, etc and observe data transferred in client server communication using UDP/TCP and identify the UDP/TC datagram.

### THEORY:

#### **Brief History of Wireshark**

- Wireshark has a very rich history. Gerald Combs, a computer science graduate of the University of Missouri at Kansas City, originally developed it out of necessity.
- The first version of Combs's application, called Ethereal, was released in 1998 under the GNU Public License (GPL).
- Eight years after releasing Ethereal, Combs left his job to pursue other career opportunities.
- Unfortunately, his employer at that time had full rights to the Ethereal trademarks, and Combs was unable to reach an agreement that would allow him to control the Ethereal "brand."
- Instead, Combs and the rest of the development team rebranded the project as Wireshark in mid-2006 thereafter it continuing.

#### **The Benefits of Wireshark**

- Wireshark offers several benefits that make it appealing for everyday use.
- It is aimed at both the journeyman and the expert packet analyst, and offers a variety of features to entice each.

Let's examine Wireshark according to the criteria defined for selecting a packet-sniffing tool.

#### **Supported protocols:**

- Wireshark excels in the number of protocols that it supports more than 850 as of this writing.
- These range from common ones like IP and DHCP to more advanced proprietary protocols like AppleTalk and Bit Torrent.
- And because Wireshark is developed under an open source model, new protocol support is added with each update.

**User-friendliness:**

- The Wireshark interface is one of the easiest to understand of any packetsniffing application.
- It is GUI-based, with very clearly written context menus and a straightforward layout.
- It also provides several features designed to enhance usability, such as protocol-based color coding and detailed graphical representations of raw data.
- Unlike some of the more complicated command-line-driven alternatives, like tcpdump, the Wireshark GUI is great for those who are just entering the world of packet analysis.

**Cost:**

- Since it is open source, Wireshark's pricing can't be beat: Wire-shark is released as free software under the GPL.
- You can download and use Wireshark for any purpose, whether personal or commercial.

**Program support:**

- A software package's level of support can make or break it.
- When dealing with freely distributed software such as Wireshark, there may not be any formal support, which is why the open source community often relies on its user base to provide support.
- Luckily for us, the Wireshark community is one of the most active of any open source project.

**Operating system support:**

- Wireshark supports all major modern operating systems, including Windows, Mac OS X, and Linux-based platforms.
- You can view a complete list of supported operating systems on the Wire-shark home page.

**Installing Wireshark**

- The Wireshark installation process is surprisingly simple. However, before you install Wireshark, make sure that your system meets the following requirements:
  - More than 400 MHz processor or faster
  - More than 512 MB RAM
  - At least 75 MB of available storage space
  - NIC that supports promiscuous mode

## WinPcap capture driver

- The WinPcap capture driver is the Windows implementation of the pcap packet-capturing application programming interface (API). Simply put, this driver interacts with your operating system to capture raw packet data, apply filters, and switch the NIC in and out of promiscuous mode. Although you can download WinPcap separately (from <http://www.winpcap.org/>), it is typically better to install WinPcap from the Wireshark installation package, because the included version of WinPcap has been tested to work with Wireshark.

## Installing on Microsoft Windows Systems

The first step when installing Wireshark under Windows is to obtain the latest installation build from the official Wireshark

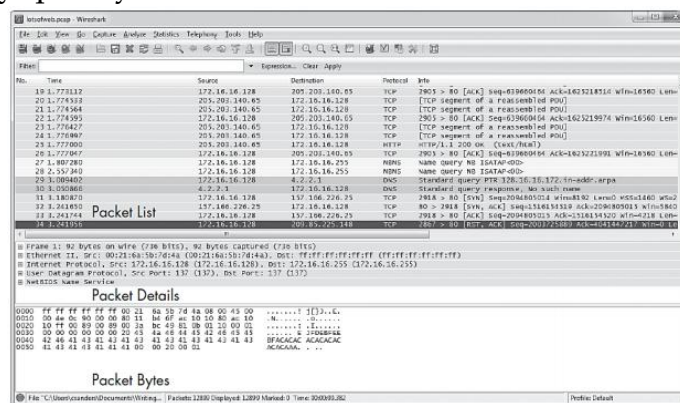
- web page, <http://www.wireshark.org/>.
- Navigate to the Downloads section on the website and choose a mirror. Once you've downloaded the package, follow these steps:
  1. Double-click the .exe file to begin installation, and then click Next in the introductory window.
  2. Read the licensing agreement, and then click I Agree if you agree. Select the components of Wireshark you wish to install.
  3. For our purposes, you can accept the defaults by clicking Next.
  4. Click Next in the Additional Tasks window.
  5. Select the location where you wish to install Wireshark, and then click Next.
  6. When the dialog asks whether you want to install WinPcap, make sure the Install WinPcap box is checked, as shown in Figure-2, and then click Install. The installation process should begin.
  7. About halfway through the Wireshark installation, the WinPcap installation should start. When it does, click Next in the introductory window, read the licensing agreement, and then click I Agree.
  8. WinPcap should install on your computer. After this installation is complete, click Finish.
  9. Wireshark should complete its installation. When it's finished, click Next.
  10. In the installation confirmation window, click Finish.

**Wireshark Fundamentals** Once you've successfully installed Wireshark on your system, you can begin to familiarize yourself with it. Now you finally get to open your fully functioning packet sniffer



**First Packet Capture** To get packet data into Wireshark, perform first packet capture. So, To capture some packets,

1. Open Wireshark.
2. From the main drop-down menu, select Capture and then Interfaces. You should see a dialog listing the various interfaces that can be used to capture packets, along with their IP addresses.
3. Choose the interface you wish to use and click Start, or simply click the interface under the Interface List section of the welcome page. Data should begin filling the window.
4. Wait about a minute or so, and when you are ready to stop the capture and view your data, click the Stop button from the Capture drop-down menu. Once you have completed these steps and finished the capture process, the Wireshark main window should be alive with data. As a matter of fact, you might be overwhelmed by the amount of data that appears, but it will all start to make sense very quickly as we break down the main window of Wireshark one piece



at a time.

5. The three panes in the main window depend on one another. In order to view the details of an individual packet in the Packet Details pane, you must first select that packet by clicking it in the Packet List pane. Once you've selected your packet, you can see the bytes that correspond with a certain portion of the packet in the Packet Bytes pane when you click that portion of the packet in the Packet Details pane. Here's what each pane contains:

**Packet List:** The top pane displays a table containing all packets in the current capture file. It has columns containing the packet number, the relative time the packet was captured, the source and destination of the packet, the packet's protocol, and some general information found in the packet. **Packet Details:** The middle pane contains a hierarchical display of information about a single packet. This display can be collapsed and expanded to show all of the information collected about an individual packet. **Packet Bytes:** The lower pane perhaps the most confusing displays a packet in its raw, unprocessed form; that is, it shows what the packet looks like as it travels across the wire. This is raw information

with nothing warm or fuzzy to make it easier to follow. 2.8 Wireshark Preferences Wireshark has several preferences that can be customized to meet your needs. To access Wireshark's preferences, select Edit from the main drop-down menu and click Preferences.

**THE CONVERSATIONS WINDOW BELOW CONFIRMS THAT THE TWO USERS ARE COMMUNICATING**

The image shows the 'Conversations' window in Wireshark for the file 'lotsfweb.pcap'. The window has tabs for various network protocols, with 'IPv4: 103' selected. Below the tabs is a table titled 'IPv4 Conversations' showing communication between various IP addresses. The table columns are: Address A, Address B, Packets, Bytes, Packets A->B, Bytes A->B, Packets A<-B, Bytes A<-B, and Rel Start. The data shows multiple bidirectional communication sessions between different IP addresses.

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start
74.125.103.163	172.16.16.128	3 927	4 232 435	2 882	4 173 482	1 045	58 953	39.2470910
66.35.45.201	172.16.16.136	1 106	807 006	596	702 314	510	104 692	10.3063300
74.125.103.147	172.16.16.128	608	633 494	435	620 562	173	12 932	9.9661320
74.125.166.28	172.16.16.128	553	532 821	382	519 254	171	13 567	3.2428500
64.208.21.43	172.16.16.128	551	357 373	309	280 314	242	77 059	6.0854720
65.173.218.96	172.16.16.136	473	331 336	263	305 759	210	25 577	59.4323280
4.23.40.126	172.16.16.197	451	318 740	234	291 841	217	26 899	73.0858700
172.16.16.197	204.160.126.126	449	185 482	243	66 891	206	118 591	16.4978080
74.125.95.149	172.16.16.128	415	323 881	271	289 966	144	33 915	3.2435920
72.32.92.4	172.16.16.136	387	130 428	190	97 845	197	32 583	14.2455230
172.16.16.128	205.203.140.65	363	251 133	128	72 072	235	179 061	1.7092310
172.16.16.128	204.160.104.126	327	149 268	161	64 263	166	85 005	3.3174460

At the bottom of the window, there are checkboxes for 'Name resolution' (checked) and 'Limit to display filter' (unchecked), along with 'Help', 'Copy', and 'Close' buttons.

## RESULT

Installation of Wire shark, tcpdump, etc has been done and observed data transferred in client server communication using UDP/TCP and identify the UDP/TC datagram.

## EXPERIMENT 7

### AIM:

Install all rootkits and study variety of options

### THEORY:

The term **Rootkit** originally referred to a collection of tools used to gain administrative access on UNIX operating systems. The collection of tools often included well-known system monitoring tools that were modified to hide the actions of an unauthorized user. An unauthorized user would replace the existing tools on the system with the modified versions preventing authorized users from discovering the security breach. **Rootkits** in Windows refers to programs that use system hooking or modification to hide files, processes, registry keys, and other objects in order to hide programs and behaviors.

In particular, Windows **rootkits** do not necessarily include any functionality to gain administrative privileges. In fact, many Windows rootkits require administrative privileges to even function.

Two basic classes of Windows rootkits : kernel mode rootkits & user mode rootkits.

**Rootkit** - "A tool used to protect backdoors and other tools from detection by administrators". Rootkit is a malicious software program, used to gain elevated access to a computer while it remains hidden from the owner of the computer and installed security software. Rootkits typically run at a low level and load before the computer's operating system to remain hidden. The rootkit can then divert any OS functions that would reveal its presence and display manipulated results to the user. Malicious users or software often install a rootkit once they have gained access to a computer, through vulnerabilities in the computer's software or through gaining the password by social engineering, for example. The rootkit allows them continued access to the computer, but it leaves no trace of their activity, as

it would if they were logged in through a normal user account. Once installed, the rootkit owner can access the computer at any time to run software, or to control the computer remotely.

## **WHY ROOT KITS ARE USED**

Root kits are used by criminals for a variety of purposes, usually to turn a computer into part of a botnet, which can then, in turn, go on to infect other computers or send spam email messages. The rootkit owner can install keyloggers to capture user-entered passwords for online banking and similar activities, or steal the user's personal details to use for identity fraud.

If the rootkit owner uses the computer for criminal acts, such as breaking into other computers, it will appear as if the computer owner is responsible if authorities trace the connection.

## **HOW ROOT KITS STAY UNDETECTED**

Many root kits infect the boot sectors of the computer's hard disk, allowing them to load before the computer's operating system. The rootkit then patches the operating system and changes common functions to hide its existence.

For example, the root kit could intercept calls for a list of files in a directory, removing its own file names before showing the results to the user, so it would appear as if the directory is clean. Both anti-virus and security software programs are vulnerable to the effects of a root kit, which runs at a lower level, ensuring the anti-virus software cannot detect or remove it. This leads the anti-virus software into believing the system is clean, when it is actually infected and running malicious software.

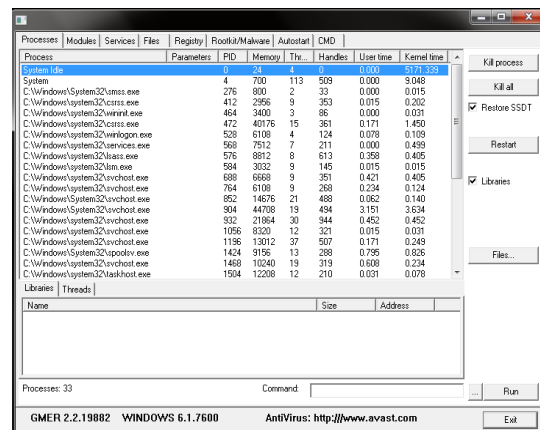
## **CURRENT ROOTKIT CAPABILITIES:**

Root kits Hide processes, Hide files, Hide registry entries, Hide services, Completely bypass personal firewalls, Undetectable by antivirus, Remotely undetectable, Covert

channels - undetectable on the network, Defeat cryptographic hash checking, Install silently, All capabilities ever used by viruses or worms.

## STEPS:

- Download Rootkit Tool from GMER website. [www.gmer.net](http://www.gmer.net)
- This displays the Processes, Modules, Services, Files, Registry, RootKit/Malwares, Autostart, CMD of local host.
- Select Processes menu and kill any unwanted process if any.



- Modules menu displays the various system files like .sys, .dll
- Services menu displays the complete services running with Autostart, Enable, Disable, System, Boot.
- Files menu displays full files on Hard-Disk volumes.
- Registry displays Hkey\_Current\_user and Hkey\_Local\_Machine.
- Rootkits/Malwares scans the local drives selected.
- Autostart displays the registry base Autostart applications.
- CMD allows the user to interact with command line utilities or Registry.

- Modules:
- Services:

Name	File	Address	Size
ntkrnlpa.exe	\SystemRoot\system32\ntkrnlpa.exe	82E44000	4259840
halmacpi.dll	\SystemRoot\system32\halmacpi.dll	82E0D000	225280
kdcom.dll	\SystemRoot\system32\kdcom.dll	80B8E000	32768
mcupdate_GenuineInt...	\SystemRoot\system32\mcupdate_GenuineIntel.dll	8B618000	491520
PSHED.dll	\SystemRoot\system32\PSHED.dll	8B690000	69632
BOOTVID.dll	\SystemRoot\system32\BOOTVID.dll	8B6A1000	32768
CLFS.SYS	\SystemRoot\system32\CLFS.SYS	8B6A9000	270336
CI.dll	\SystemRoot\system32\CI.dll	8B6EB000	700416
\Wd01000.sys	\SystemRoot\system32\drivers\Wd01000.sys	8B823000	462848
WDFLDR.SYS	\SystemRoot\system32\drivers\WDFLDR.SYS	8B894000	57344
ACPI.sys	\SystemRoot\system32\DRIVERS\ACPI.sys	8B8A2000	294912
WMILIB.SYS	\SystemRoot\system32\DRIVERS\WMILIB.SYS	8B8EA000	36864
msisadv.sys	\SystemRoot\system32\DRIVERS\msisadv.sys	8B8F3000	32768
pci.sys	\SystemRoot\system32\DRIVERS\pci.sys	8B8FB000	172032
vdrvroot.sys	\SystemRoot\system32\DRIVERS\vdrvroot.sys	8B925000	45056
iusb3hcs.sys	\SystemRoot\system32\DRIVERS\iusb3hcs.sys	8B930000	28672
partmgr.sys	\SystemRoot\system32\drivers\partmgr.sys	8B937000	69632
volmgr.sys	\SystemRoot\system32\DRIVERS\volmgr.sys	8B948000	65536
volmgrx.sys	\SystemRoot\system32\drivers\volmgrx.sys	8B958000	307200
intelide.sys	\SystemRoot\system32\DRIVERS\intelide.sys	8B9A3000	28672
PCIIDE.SYS	\SystemRoot\system32\DRIVERS\PCIIDE.SYS	8B9A4000	57344
pciide.sys	\SystemRoot\system32\DRIVERS\pciide.sys	8B9B8000	28672
mountmgr.sys	\SystemRoot\system32\drivers\mountmgr.sys	8B9BF000	90112
atapi.sys	\SystemRoot\system32\DRIVERS\atapi.sys	8B9D5000	36864
ataport.SYS	\SystemRoot\system32\DRIVERS\ataport.SYS	8B800000	143360
amdaxata.sys	\SystemRoot\system32\DRIVERS\amdaxata.sys	8B9DE000	36864
fltmgr.sys	\SystemRoot\system32\drivers\fltmgr.sys	8B796000	212992
fileinfo.sys	\SystemRoot\system32\drivers\fileinfo.sys	8B9E7000	69632
Ntfs.sys	\SystemRoot\system32\drivers\Ntfs.sys	8B425000	1241088
msrpc.sys	\SystemRoot\system32\Drivers\msrpc.sys	8B854000	176128

GMER 2.2.19882    WINDOWS 6.1.7600    AntiVirus: <http://www.avast.com>    Exit

## RESULT

Study and installation of Rootkits has been completed successfully.

## EXPERIMENT 8

### AIM:

Perform an Experiment to Sniff Traffic using ARP Poisoning.

### THEORY:

Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines' MAC addresses. ARP Poisoning is also known as **ARP Spoofing**.

Here is how ARP works –

- When one machine needs to communicate with another, it looks up its ARP table.
- If the MAC address is not found in the table, the **ARP\_request** is broadcasted over the network.
- All machines on the network will compare this IP address to MAC address.
- If one of the machines in the network identifies this address, then it will respond to the **ARP\_request** with its IP and MAC address.
- The requesting computer will store the address pair in its ARP table and communication will take place.

What is ARP Spoofing?

ARP packets can be forged to send data to the attacker's machine.

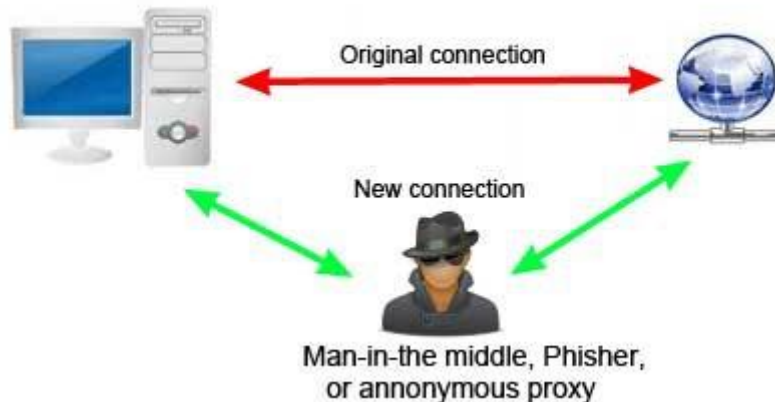
- ARP spoofing constructs a large number of forged ARP request and reply packets to overload the switch.
- The switch is set in **forwarding mode** and after the **ARP table** is flooded with spoofed ARP responses, the attackers can sniff all network packets.

Attackers flood a target computer ARP cache with forged entries, which is also known as **poisoning**. ARP poisoning uses Man-in-the-Middle access to poison the network.

What is MITM?

The Man-in-the-Middle attack (abbreviated MITM, MitM, MIM, MiM, MITMA) implies an active attack where the adversary impersonates the user by creating a connection between the victims and sends messages between them. In this case, the victims think that they are communicating with each other, but in reality, the malicious actor controls the communication.

## Man-in-the-middle attack



A third person exists to control and monitor the traffic of communication between two parties. Some protocols such as **SSL** serve to prevent this type of attack.

### ARP Poisoning – Exercise

In this exercise, we have used **BetterCAP** to perform ARP poisoning in LAN environment using VMware workstation in which we have installed **Kali Linux** and **Etercap** tool to sniff the local traffic in LAN.

For this exercise, you would need the following tools –

- VMware workstation
- Kali Linux or Linux Operating system
- Ettercap Tool
- LAN connection

**Note** – This attack is possible in wired and wireless networks. You can perform this attack in local LAN.

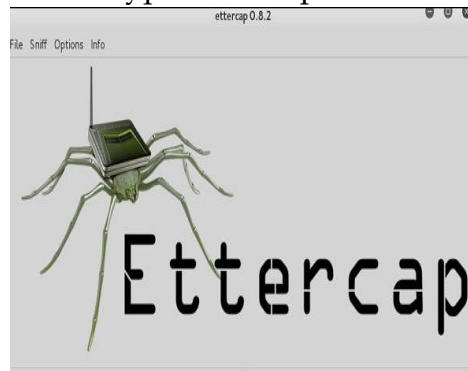
**Step 1** – Install the VMware workstation and install the Kali Linux operating system.

**Step 2** – Login into the Kali Linux using username pass “root, toor”.

**Step 3** – Make sure you are connected to local LAN and check the IP address by typing the command **ifconfig** in the terminal.



**Step 4** – Open up the terminal and type “Ettercap -G” to start the graphical version of



Ettercap

**Step 5** – Now click the tab “sniff” in the menu bar and select “unified sniffing” and click OK to select the interface. We are going to use “eth0” which means Ethernet connection.

**Step 6** – Now click the “hosts” tab in the menu bar and click “scan for hosts”. It will start scanning the whole network for the alive hosts.

**Step 7** – Next, click the “hosts” tab and select “hosts list” to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.

**Step 8** – Now we have to choose the targets. In MITM, our target is the host machine, and the route will be the router address to forward the traffic. In an MITM attack, the attacker intercepts the network and sniffs the packets. So, we will add the victim as “target 1” and the router address as “target 2.”

In VMware environment, the default gateway will always end with “2” because “1” is assigned to the physical machine.

**Step 9** – In this scenario, our target is “192.168.121.129” and the router is “192.168.121.2”. So we will add target 1 as **victim IP** and target 2 as **router IP**.

**Step 10** – Now click on “MITM” and click “ARP poisoning”. Thereafter, check the option “Sniff remote connections” and click OK.

**Step 11** – Click “start” and select “start sniffing”. This will start ARP poisoning in the network which means we have enabled our network card in “promiscuous mode” and now the local traffic can be sniffed.

**Note** – We have allowed only HTTP sniffing with Ettercap, so don’t expect HTTPS packets to be sniffed with this process.

**Step 12** – Now it’s time to see the results; if our victim logged into some websites. You can see the results in the toolbar of Ettercap.

This is how sniffing works. You must have understood how easy it is to get the HTTP credentials just by enabling ARP poisoning.

ARP Poisoning has the potential to cause huge losses in company environments. This is the place where ethical hackers are appointed to secure the networks.

Like ARP poisoning, there are other attacks such as MAC flooding, MAC spoofing, DNS poisoning, ICMP poisoning, etc. that can cause significant loss to a network.

In the next chapter, we will discuss another type of attack known as **DNS poisoning**.

## **RESULT**

Sniff Traffic using ARP Poisoning has been done successfully

## EXPERIMENT 7

### AIM:

Demonstrate intrusion detection system using any tool (snort or any other s/w)

### THEORY:

With the development of network technologies and applications, network attacks are greatly increasing both in number and severity. As a key technique in network security domain, Intrusion Detection System (IDS) plays vital role of detecting various kinds of attacks and secures the networks. Main purpose of IDS is to find out intrusions among normal audit data and this can be considered as classification problem. Intrusion detection systems (IDS) are an effective security technology, which can detect, prevent and possibly react to the attack. It performs monitoring of target sources of activities, such as audit and network traffic data in computer or network systems, requiring security measures, and employs various techniques for providing security services.

With the tremendous growth of network-based services and sensitive information on networks, network security is becoming more and more important than ever before.

**Intrusion:** Attempting to break into or misuse your system. Intruders may be from outside the network or legitimate users of the network. Intrusion can be a physical, system or remote intrusion.

Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent.

### **About Snort:**

Snort is an open source network intrusion prevention system, capable of performing realtime traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and

probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

**Snort has three primary uses:** It can be used as a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc), or as a full blown network intrusion prevention system.

The privacy of the Snort community is very important to Sourcefire. If you choose to optout, the information collected at the time of registration will not be used for any Sourcefire marketing efforts. In addition, Sourcefire will not sell or distribute any personal information to 3rd party companies.

**SNORT can be configured to run in three modes:**

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

**Sniffer Mode:** `snort -v` Print out the TCP/IP packets header on the screen

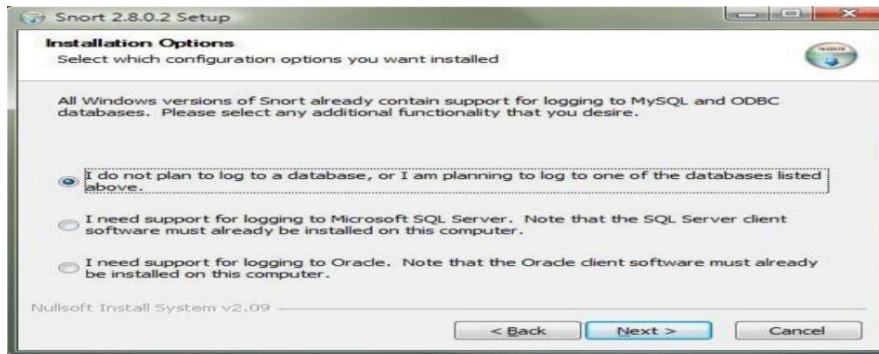
**Packet Logger Mode:** `snort -dev -l c:\log` [create this directory in the C drive] and snort will automatically know to go into packet logger mode, it collects every packet it sees and places it in log directory.

**Network Intrusion Detection System Mode:** `snort -d c:\log -h ipaddress/24 -c nort.conf`

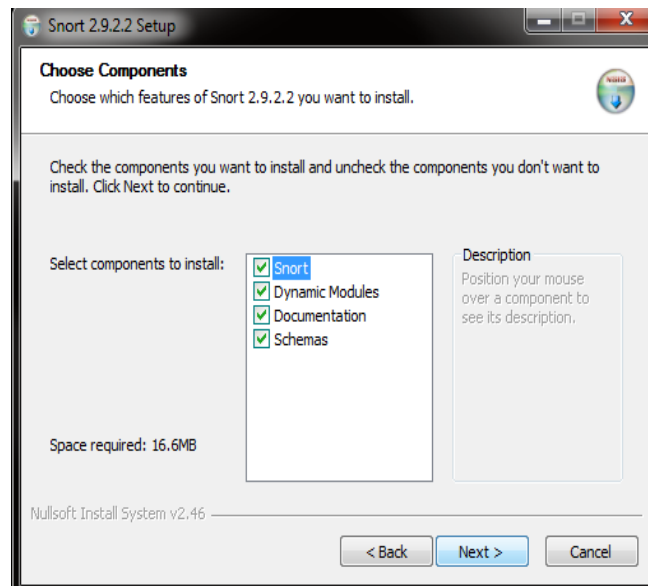
This is a configuration file applies rule to each packet to decide it an action based upon the rule type in the file.

**Working with Snort:**

1. Go to the web site [www.snort.org/start/download](http://www.snort.org/start/download)
2. Click on download option and support path to save the setup file.

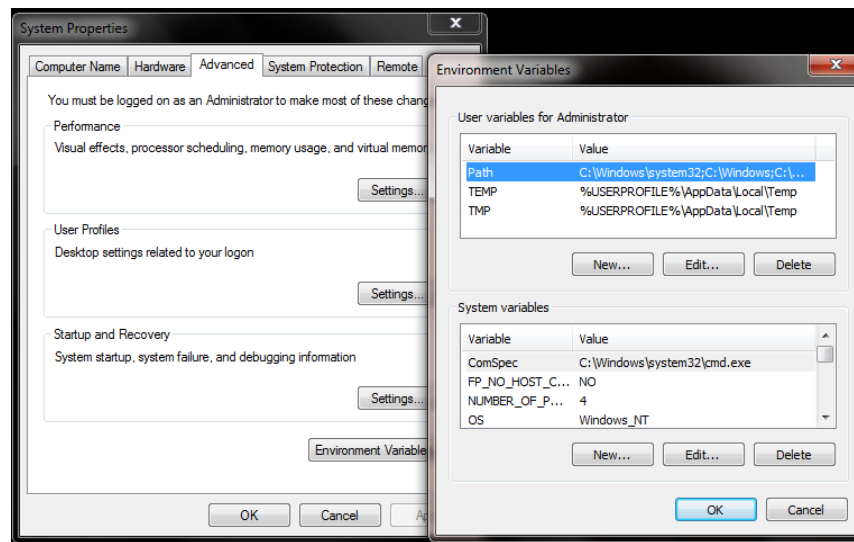


3. Double click on Snort Installation icon to run setup.
4. Accept License agreement and Specify path for installation, and then Click on Next.
5. Install snort with or without database support.
6. Skip the WinPcap driver installation
7. Select all the **components** and Click Next.



8. Install and Close.
9. Add the path variable in windows environment variable by selecting new classpath.
10. Create a path variable and point it at snort.exe variable name: **path** and variable value as **c:\snort\bin**.

Click OK button and then close all dialog boxes.



12. Type the following commands:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Admin>cd\

C:\>cd snort

C:\snort>cd bin

C:\snort\bin>snort_
```

13. Go to command prompt and get into **Snort/bin** directory and run **Snort.exe** file.

14. An editor window displays the complete details of packets flowing across the system, the IP Address of packet generator, date & Time, length of Packet, Time to live(TTL) Etc at Realtime.

15. By analyzing these details Intruders can be traced at real time.

```
C:\WINDOWS\system32\cmd.exe - snort
Len: 50
=====
03/26-14:49:59.901369 192.168.1.18:137 -> 192.168.1.255:137
UDP TTL:128 TOS:0x0 ID:42600 IpLen:20 DgmLen:78
Len: 50
=====
03/26-14:50:00.651323 192.168.1.18:137 -> 192.168.1.255:137
UDP TTL:128 TOS:0x0 ID:42601 IpLen:20 DgmLen:78
Len: 50
=====
03/26-14:50:00.838813 192.168.1.18:3698 -> 91.220.62.30:443
TCP TTL:128 TOS:0x0 ID:42602 IpLen:20 DgmLen:48 DF
***** Seq: 0xDF46AE79 Ack: 0x0 Win: 0xFFFF TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=====
03/26-14:50:02.787661 192.168.1.92:1094 -> 255.255.255.255:1211
UDP TTL:128 TOS:0x0 ID:34172 IpLen:20 DgmLen:103
Len: 75
=====
```

16. These details can be documents by using a print screen option.

## **RESULT:**

Intrusion detection system using any snort was developed successfully.

## EXPERIMENT 9

### **AIM:**

Demonstrate how to provide secure data storage, secure data transmission and digital signatures (GnuPG).

### **THEORY:**

GnuPG allows you to encrypt and sign your data and communications; it features a versatile key management system, along with access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications.

### **INSTALLING THE SOFTWARE:**

1. Visit [www.gpg4win.org](http://www.gpg4win.org) Click on the "Gpg4win 2.3.0" button
2. On the following screen, click the "Download Gpg4win" button.
3. When the "Welcome" screen is displayed, click the "Next" button
4. When the "License Agreement" page is displayed, click the "Next" button
5. Set the check box values as specified below, then click the "Next" button
6. Set the location where you want the software to be installed. The default location is fine. Then, click the "Next" button.
7. Specify where you want shortcuts to the software placed, then click the "Next" button.
8. If you selected to have a GPG shortcut in your Start Menu, specify the folder in which it will be placed. The default "Gpg4win" is OK. Click the "Install" button to continue
9. A warning will be displayed if you have Outlook or Explorer opened. If this occurs, click the "OK" button.
10. The installation process will tell you when it is complete. Click the "Next" button
11. Once the Gpg4win setup wizard is complete, the following screen will be displayed. Click the "Finish" button
12. If you do not uncheck the "Show the README file" check box, the README file will be displayed. The window can be closed after you've reviewed it



Link for demonstration - <https://www.youtube.com/watch?v=H5jXg0Wx2cM>

**RESULT:**

Thus the secure data storage, secure data transmission and for creating digital signatures (GnuPG) was developed successfully.