EX.No:1	IMPLEMENT SYMMETRIC KEY ALGORITHMS

AIM:

To use Data Encryption Standard (DES) Algorithm for a practical application like User MessageEncryption.

ALGORITHM:

1. Create a DESKey.
2. Create a Cipher instance from Cipherclass, specify the following information and separated by aslash(/).
   a. Algorithmname
   b. Mode(optional)
   c. Paddingscheme(optional)
3. Convert String into ***Byte[]*** array format.
4. Make Cipher in encrypt mode, and encrypt it with ***Cipher.doFinal()*** method.
5. Make Cipher in decrypt mode, and decrypt it with ***Cipher.doFinal()*** method.

PROGRAM:

DES.java

```
Importjava.security.InvalidKeyException;
importjava.security.NoSuchAlgorithmException;
importjavax.crypto.BadPaddingException;
import javax.crypto.Cipher;
importjavax.crypto.IllegalBlockSizeException;
import javax.crypto.KeyGenerator;
importjavax.crypto.NoSuchPaddingException;
import javax.crypto.Secretey;
```

```
publicclass DES
{
    publicstaticvoid main(String[] argv){
        try{
    System.out.println("MessageEncryptionUsingDESAlgorithm\n ---------");
            KeyGeneratorkeygenerator=KeyGenerator.getInstance("DES");Se
    cretKeymyDesKey=keygenerator.generateKey();
            CipherdesCipher;
            desCipher=Cipher.getInstance("DES/ECB/
            PKCS5Padding");desCipher.init(Cipher.ENCRYPT_MODE,myD
            esKey);byte[] text = "Secret Information
            ".getBytes();System.out.println("Message [Byte Format] : " +
            text);System.out.println("Message :"+new String(text));
            byte[] textEncrypted =
            desCipher.doFinal(text);System.out.println("EncryptedMessage:"
            +textEncrypted);desCipher.init(Cipher.DECRYPT_MODE,
            myDesKey);byte[]textDecrypted=desCipher.doFinal(textEncrypte
            d);
System.out.println("Decrypted Message:"+newString(textDecrypted));
}catch(NoSuchAlgorithmException e){
    e.printStackTrace();
}catch(NoSuchPaddingException e){
    e.printStackTrace();
}catch(InvalidKeyException e){
    e.printStackTrace();
}catch(IllegalBlockSizeException e){
    e.printStackTrace();
}catch(BlockPaddingException e){
    e.printStackTrace();
}}}
```

OUTPUT:

MessageEncryptionUsingDESAlgorithm

Message[ByteFormat]:[B@4dcbadb4

Message:SecretInformation

EncryptedMessage:[B@504bae78

DecryptedMessage:SecretInformation

RESULT:

Thus the java program for DES Algorithm has been implemented and the output verified successfully.

EX.No:2a	IMPLEMENT ASYMMETRIC KEY ALGORITHMS AND KEY EXCHANGE ALGORITHMS - RSAALGORITHM

AIM:

ToimplementRSA(Rivest–Shamir–Adleman) algorithmbyusingHTMLandJavascript.

ALGORITHM:

1. Choosetwoprime numberpand q
2. Compute thevalue ofnandp
3. Findthevalue of***e*** (public key)
4. Computethevalue of***d***(privatekey)usinggcd()
5. Dotheencryptionanddecryption
   a. Encryptionisgivenas,

      $$c=t^e \bmod n$$

   b. Decryption is given as,

      $$t=c^d \bmod n$$

PROGRAM:rsa.html

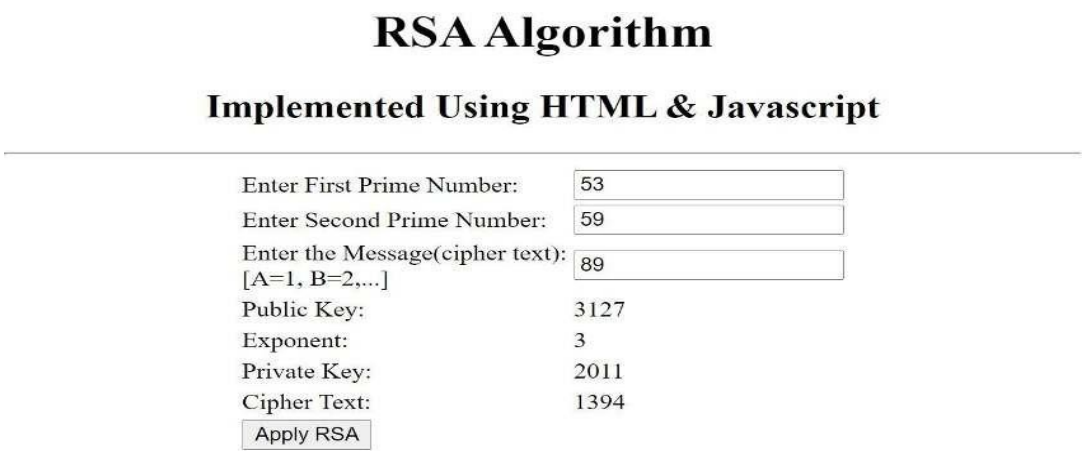
```
<html>
<head>
   <title>RSAEncryption</title>
   <metaname="viewport"content="width=device-width,initial-scale=1.0">
</head>

<body>
   <center>
      <h1>RSAAlgorithm</h1>
      <h2>ImplementedUsingHTML&Javascript</h2>
      <hr>
      <table>
```

```
<tr>
   <td>Enter FirstPrimeNumber:</td>
   <td><inputtype="number"value="53"id="p"></td>
</tr>
<tr>
   <td>EnterSecondPrimeNumber:</td>
   <td><inputtype="number"value="59"id="q"></p>
   </td>
</tr>
<tr>
   <td>EntertheMessage(ciphertext):<br>[A=1,B=2,...]</td>
   <td><inputtype="number"value="89"id="msg"></p>
   </td>
</tr>
<tr>
   <td>PublicKey:</td>
   <td>
      <pid="publickey"></p>
   </td>
</tr>
<tr>
   <td>Exponent:</td>
   <td>
      <pid="exponent"></p>
   </td>
</tr>
<tr>
   <td>PrivateKey:</td>
   <td>
      <pid="privatekey"></p>
```

```
                    </td>
                </tr>
                <tr>
                    <td>CipherText:</td>
                    <td>
                        <pid="ciphertext"></p>
                    </td>
                </tr>
                <tr>
                    <td><buttononclick="RSA();">ApplyRSA</button></td>
                    <\tr>
            <\table>
            </center>
        </body>
<scripttype="text/javascript">
functionRSA(){
vargcd,p,q, no,n, t,e,i,x;
gcd = function (a, b) { return (!b) ? a : gcd(b, a % b); };
p=                  document.getElementById('p').value;
q=document.getElementById('q').value;
no=document.getElementById('msg').value;
n = p * q;
t= (p - 1) * (q- 1);
for(e=2;e<t;e++){
if(gcd(e,t)==1){
break;
}
}
for(i=0;i<10;i++){
x = 1 +i* t
```

```
if (x % e == 0) {
d = x / e;
break;
}
}
ctt=Math.pow(no,e).toFixed(0);
ct =ctt% n;
dtt=Math.pow(ct,d).toFixed(0);
dt= dtt% n;
document.getElementById('publickey').innerHTML =
n;document.getElementById('exponent').innerHTML =
e;document.getElementById('privatekey').innerHTML=d;document.getElementById('ciph
ertext').innerHTML=ct;
}
</script>
</html>
```

OUTPUT:



RESULT:

Thus the RSA algorithm has been implemented using HTML&CSS and the output has been verified successfully.

EX.No:2b	IMPLEMENT ASYMMETRIC KEY ALGORITHMS AND KEY EXCHANGE ALGORITHMS – DIFFIE-HELLMANKEYEXCHANGEALGORITHM

AIM:

Toimplement theDiffie-Hellman KeyExchangealgorithmforagivenproblem.

ALGORITHM:

1. AliceandBobpublicly agree touseamodulus$p$=23andbase$g$=5(whichis aprimitiverootmodulo 23).
2. Alicechoosesa secretinteger $\boldsymbol{a}$=4,thensendsBob $A = g^a \bmod p$
   - $A=5^4 \bmod 23=4$
3. Bobchoosesa secretinteger$\boldsymbol{b}$=3,thensends Alice $B=g^b \bmod p$
   - $B=5^3 \bmod 23=10$
4. Alicecomputes$\boldsymbol{s}=B^a \bmod p$
   - $\boldsymbol{s}=10^4 \bmod 23=18$
5. Bob computes $\boldsymbol{s}=A^b \bmod p$
   - $\boldsymbol{s}=4^3 \bmod 23=18$
6. AliceandBobnowsharea secret(thenumber18).

PROGRAM: DiffieHellman.java

```
classDiffieHellman{
  publicstaticvoidmain(Stringargs[]){
    intp=23;/*  publiclyknown(prime  number)*/
    int g = 5; /* publicly known (primitive root) */
    intx=4;/*onlyAlice knowsthissecret*/
    int  y  =  3;  /*  only  Bob  knows  this  secret  */
    doublealiceSends  =(Math.pow(g,  x))%p;
    doublebobComputes=(Math.pow(aliceSends,y))%p;
    doublebobSends = (Math.pow(g,y)) %p;
```

```
        doublealiceComputes =(Math.pow(bobSends,x))%p;
        doublesharedSecret =(Math.pow(g,(x* y)))% p;
        System.out.println("simulationofDiffie-Hellman keyexchangealgorithm\
        n---------- ");
        System.out.println("Alice Sends : " + aliceSends);
        System.out.println("Bob Computes : " +
        bobComputes);System.out.println("Bob Sends : " + bobSends);
        System.out.println("AliceComputes:"+aliceComputes);System.out.println("S
        haredSecret :"+sharedSecret);
        /*sharedsecretsshould matchandequality istransitive*/
        if((aliceComputes==sharedSecret)&&(aliceComputes==bobCompute
           s))System.out.println("Success:SharedSecretsMatches!"+sharedSec
           ret);
        else
           System.out.println("Error:SharedSecretsdoesnotMatch");
    }}
```

OUTPUT:

Simulation of Diffie-Hellman key exchange algorithm

AliceSends:4.0

BobComputes:18.0

BobSends:10.0

AliceComputes:18.0

SharedSecret :18.0

Success:SharedSecretsMatches!18.0

RESULT:

Thus the Diffie-Hellman key exchange algorithm has been implemented using Java Program and the output has been verified successfully.

EX.No:3	IMPLEMENT DIGITAL SIGNATURE SCHEMES

AIM:

Toimplement theSIGNATURESCHEME -DigitalSignatureStandard.

ALGORITHM:

1. CreateaKeyPairGenerator object.
2. InitializetheKeyPairGenerator object.
3. GeneratetheKeyPairGenerator.
4. Getthe private keyfromthepair.
5. Createasignatureobject.
6. InitializetheSignatureobject.
7. Adddatato theSignatureobject.
8. CalculatetheSignature

PROGRAM:

```
importjava.security.KeyPair;
importjava.security.KeyPairGenerator;
importjava.security.PrivateKey;
import java.security.Signature;
importjava.util.Scanner;
publicclassCreatingDigitalSignature{
publicstaticvoidmain(Stringargs[])throwsException{
Scanner sc = new Scanner(System.in);System.out.println("Enter some
text");Stringmsg =sc.nextLine();
    KeyPairGeneratorkeyPairGen=KeyPairGenerator.getInstance("DSA");keyPair
    Gen.initialize(2048);
    KeyPairpair=keyPairGen.generateKeyPair();
```

```
        PrivateKeyprivKey=pair.getPrivate();
        Signaturesign=Signature.getInstance("SHA256withDSA");sign.initSign(privK
        ey);
      byte[]bytes="msg".getBytes();
      sign.update(bytes);
      byte[]signature=sign.sign();
     System.out.println("Digital        signatureforgiventext:"+newString(signature,
"UTF8"));
      }
      }
```

OUTPUT:

```
Entersometext
Hihoware you
Digitalsignatureforgiventext:0=@gRD???-?.????/yGL?i??a!?
```

RESULT:

Thus the Digital Signature Standard Signature Scheme has been implemented and the output has been verified successfully

EX.No:4	INSTALLATION OF WIRE SHARK, TCPDUMP AND OBSERVE DATA TRANSFERRED IN CLIENT-SERVER COMMUNICATION USING UDP/TCP AND IDENTIFY THE UDP/TCP DATAGRAM

AIM:

ToinstallationofWireshark,tcpdumpandobservedatatransferredinclient-servercommunicationusingUDP/TCP andidentifytheUDP/TCP datagram.

PROCEDURE:

The first part of the lab introduces packet sniffer, Wireshark. Wiresharkis a freeopen-source network protocol analyzer. It is used for network troubleshooting and communicationprotocol analysis. Wireshark captures network packets in real time and display them inhuman-readableformat.Itprovidesmanyadvancedfeaturesincludinglivecaptureandoffline analysis, three-pane packet browser, coloring rules for analysis. This document usesWireshark for the experiments, and it covers Wireshark installation, packet capturing, andprotocol analysis.

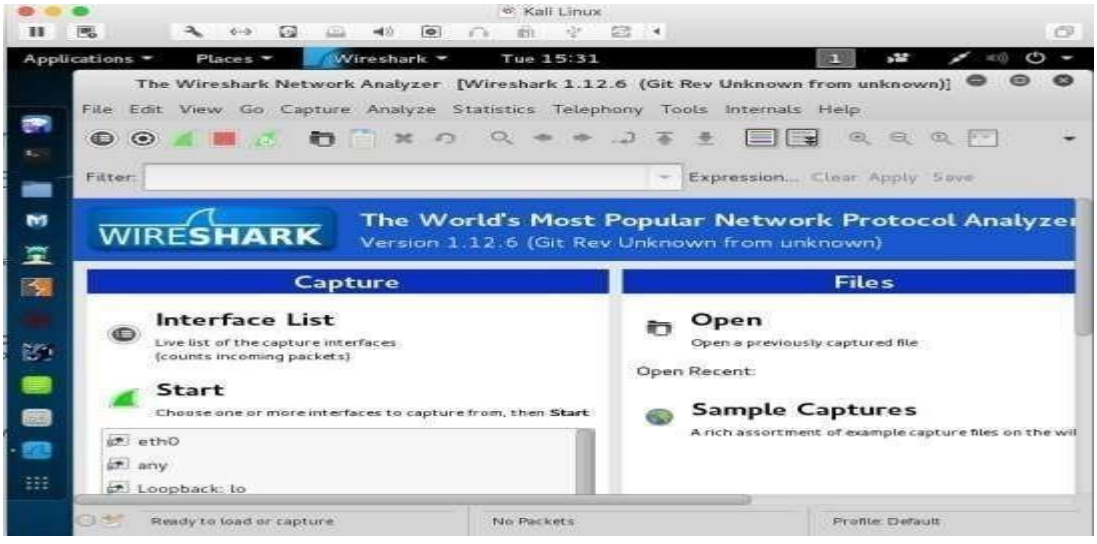


Figure1:Wireshark in KaliLinux

Background

TCP/IPNetworkStack

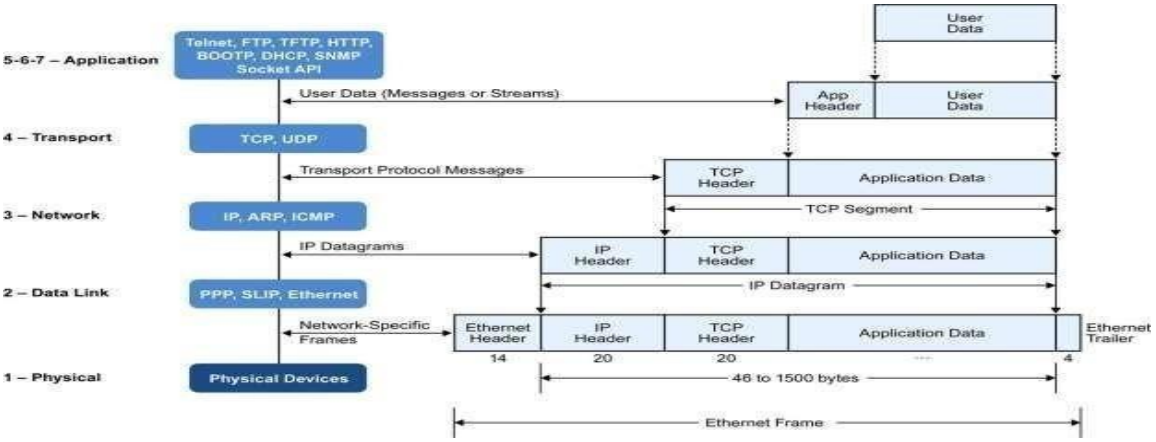
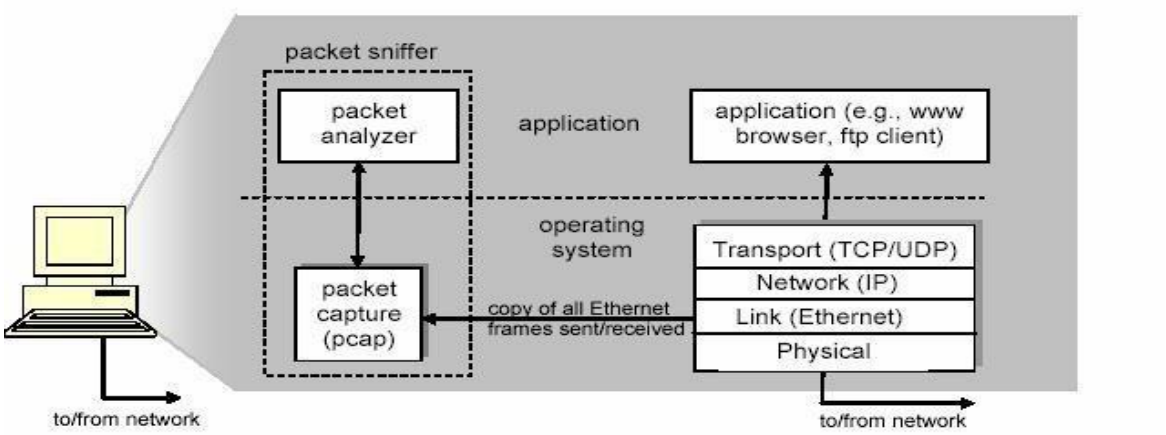


Figure2:EncapsulationofDatain theTCP/IPNetworkStack

PacketSniffer

Packet sniffer is a basic tool for observing network packet exchangesin a computer.As thename suggests, a packet sniffer captures ("sniffs") packets being sent/received from/by yourcomputer; it will also typically store and/or display the contents of the various protocol fields inthese captured packets. A packet sniffer itself is passive. It observes messages being sent andreceivedbyapplicationsandprotocolsrunning onyour computer,butneversends packetsitself.



GettingWireshark

TheKaiLinuxhasWiresharkinstalled.YoucanjustlaunchtheKaliLinuxVMandopenWiresharkt here.

WiresharkcanalsobedownloadedfromhereHttps://www.wireshark.org/download.html

StartingWireshark:

WhenyouruntheWiresharkprogram,theWiresharkgraphicuserinterface

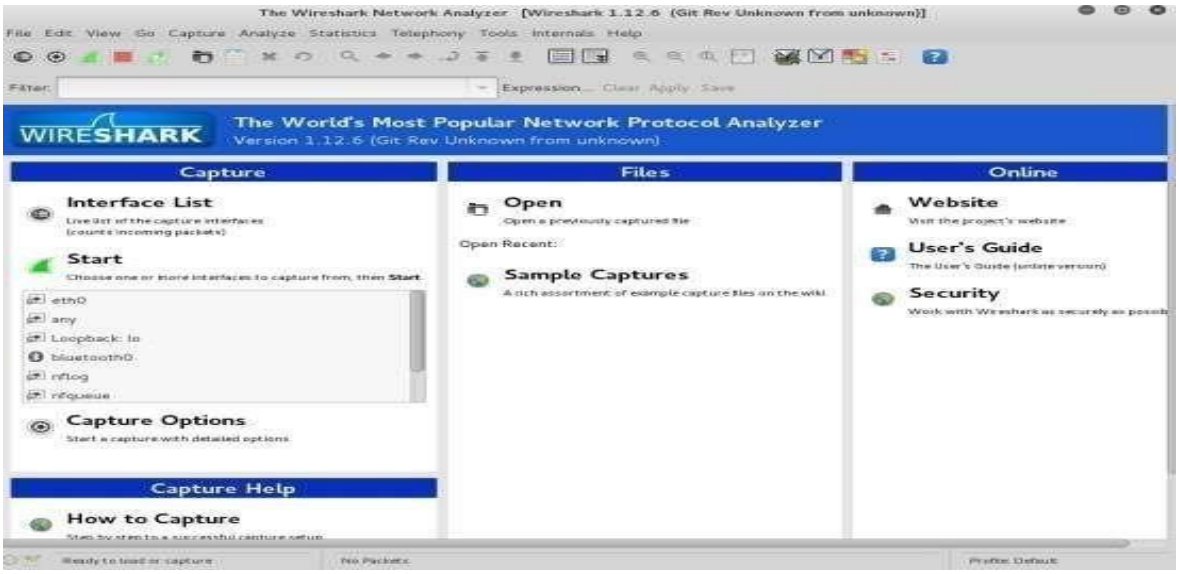
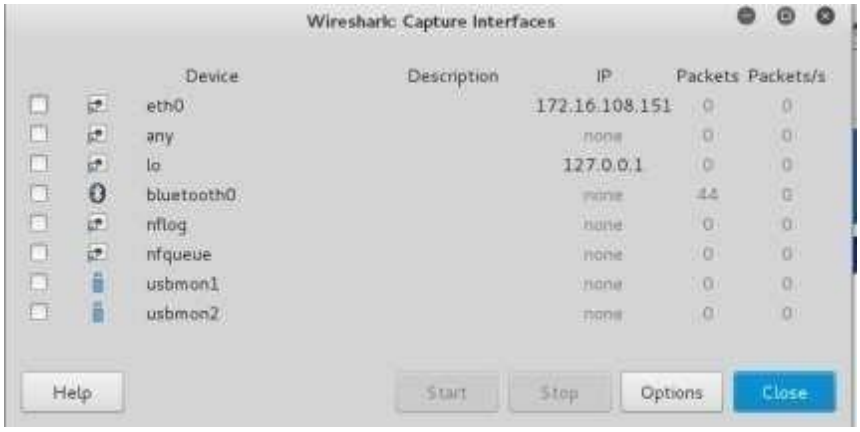


Figure: Currently,theprogramisnotcapturingthepackets

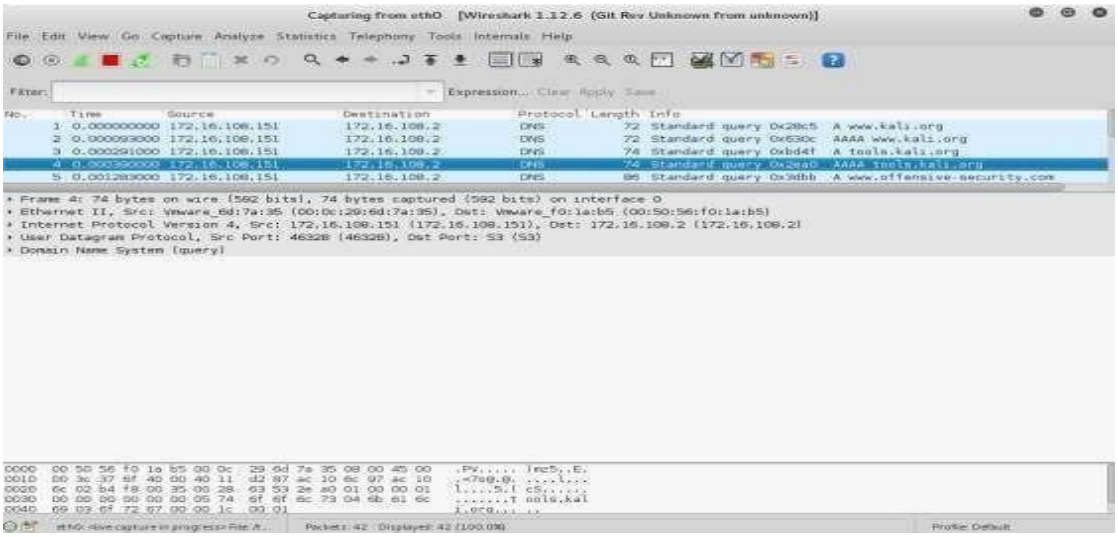
Then, youneedto choose aninterface.Ifyouarerunning the Wireshark on yourlaptop,

youneed to select WiFi interface. If you are at a desktop, you need to select the Ethernet interfacebeing used. Note that there could be multiple interfaces. In general, you can select any interfacebut that does not mean that traffic will flow through that interface. The



network interfaces (i.e.,the physical connections) that your computer has to the network are shown.

Afteryouselecttheinterface,youcanclickstartto capturethepackets asbelow.



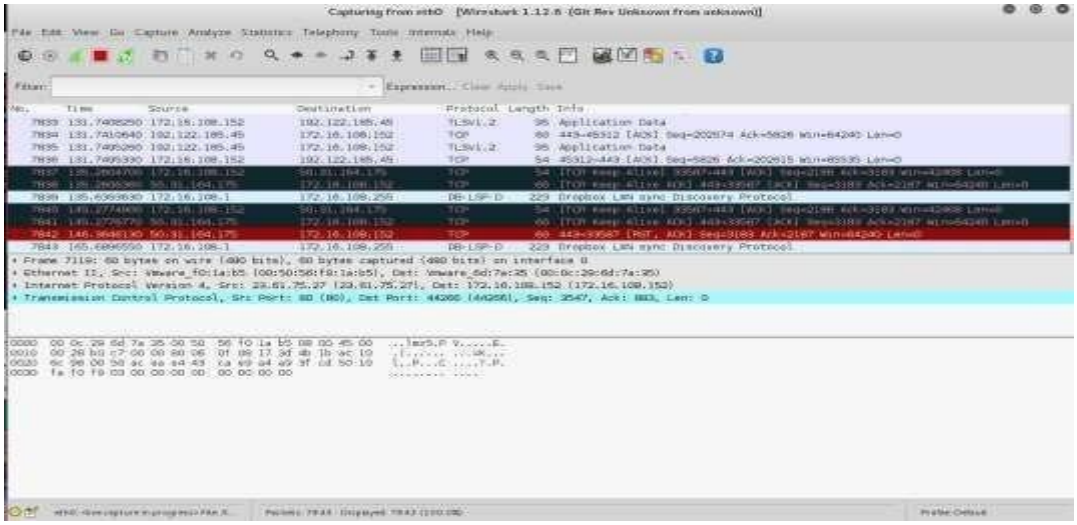
CapturingPackets

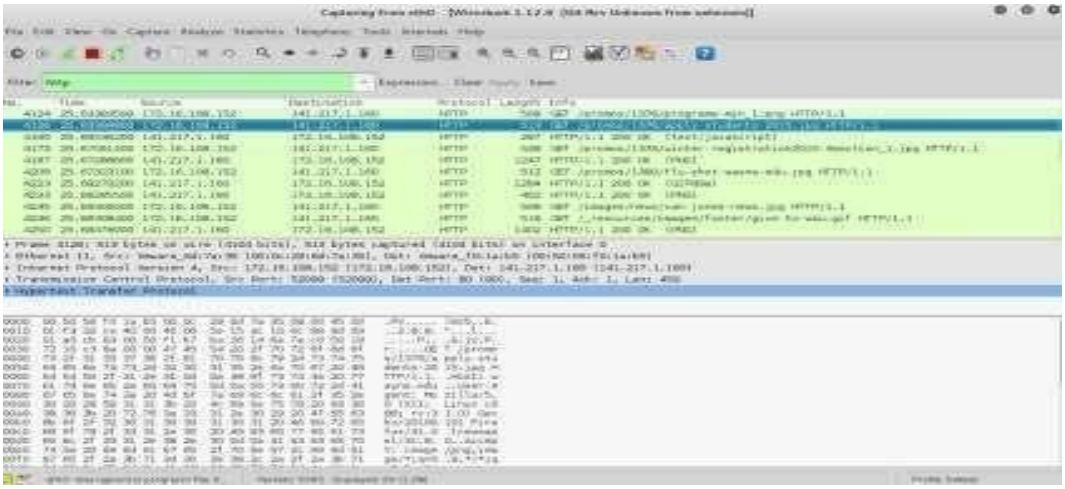
After downloading and installing Wireshark, you can launch it and click the name of an interfaceunder Interface List to start capturing packets on that interface. For example, if you want tocapture trafficonthewirelessnetwork,click yourwirelessinterface.

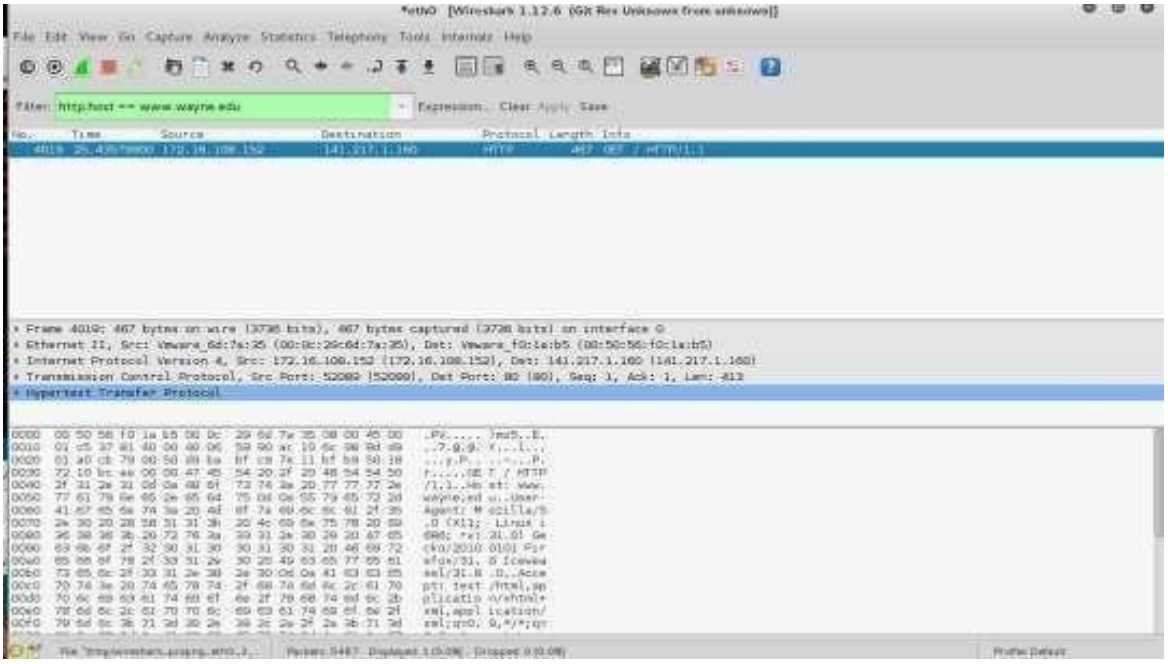
TestRun

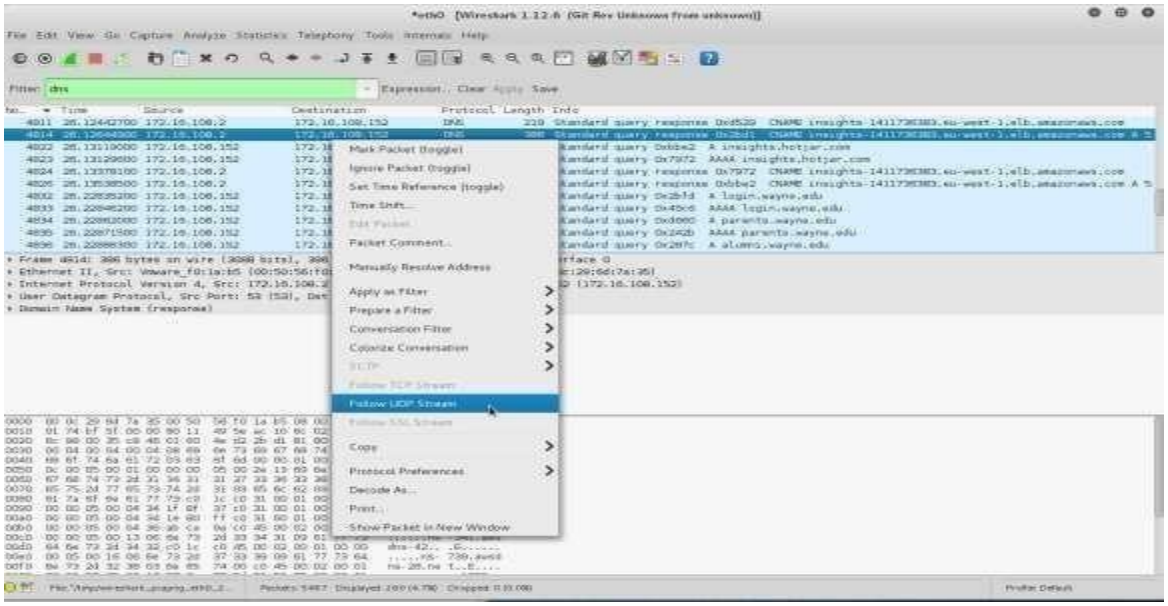
Dothefollowingsteps:

1. Startup the Wireshark program (selectaninterfaceandpressstarttocapturepackets).
2. Startup your favourite browser (ceweaselinKaliLinux).
3. In your browser, goto Wayne State home page by typing www.wayne.edu.
4. After your browser has displayed the http://www.wayne.edupage, stopWireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappearand the main Wireshark window to display all packets captured since you began packet capture see image below:









RESULT:

Installation of Wireshark, tcpdump and observe datatransfer redinclient-server communication using UDP/TCP and identify the UDP/TCP datagram.

EX.No:5	CHECK MESSAGE INTEGRITY AND CONFIDENTIALITY USING SSL

AIM:

To check the Message Integrity and Confidentiality using SSL.

PROCEDURE:

SSLSessioninDetails

Handshaking-Cipher suit Negotiation

ClientsendsaplaintextClient_Hellomessageandsuggestssomecryptographicparameters(collectivelycalledciphersuit)tobeusedfortheircommunicationsession.TheClient_Hellomessagealsocontainsa 32-byterandom numberdenoted asclient_random.Forexample,.

Client_Hello:

Protocol Version: TLSv1 if you can, else SSLv3.

KeyExchange:RSAifyoucan,elseDiffe-Hellman.

Secret Key Cipher Method: 3DES if you can, else DES.

Message Digest:SHA-1ifyoucan,elseMD5.

DataCompression Method:PKZipif youcan,elsegzip.

Client RandomNumber:32bytes

The stronger method (in terms of security) shall precede the weaker one, e.g. RSA (1024-bit)precedesDH,3DESprecedesDES,SHA-1 (160-bit)precedesMD5 (128-bit).

Server responds with a plaintext Server_Hello to state the ciphersuit of choice (server decidesontheciphersuit).Themessagealsocontainsa32-byte random number denote d as server_random.

Forexample,

Server_Hello:

ProtocolVersion:TLSv1

KeyExchange:RSA.

SecretKeyCipherMethod:DES.

Message Digest:SHA-1

DataCompressionMethod:PKZip.

ServerRandomNumber: 32bytes

Handshaking-KeyExchange

The server sends its digital certificate to the client, which is supposedly signed by a root CA. Theclient uses the root CA'spublic key to verify the server's certificate (trusted root-CAs' public keyare pre-installed inside the browser). It then retrieves the server's public key from the server'scertificate.(If the server'scertificateis signed by a sub-CA, the clienthas to build a digitalcertificate chain, leadingtoatrustedroot CA,toverifythe server'scertificate.)

Thenextstepisto establishtheSession Key:

1. The client generates a 48-byte (384-bit) random number called pre_master_secret, encryptsitusingthe verifiedserver'spublickeyandsends itto theserver.
2. Server decrypts the pre_master_secret using its own private key. Eavesdroppers cannotdecrypt thepre_master_secret,astheydonotpossesstheserver'sprivate key.
3. Client and serverthen independently and simultaneously create the session key, based onthe pre_master_secret, client_random and server_random. Notice that both the server andclient contribute to the session key,through the inclusion of the random number exchangein the hello messages. Eavesdroppers can intercept client_random and server_random astheyare sentin plaintext,butcannotdecrypt thepre_master_secret.
4. InaSSL/TLSsession,thesessionkeyconsistsof6secretkeys(tothwartcrypto-analysis).3 secret keys are used for client-to-server messages, and the other 3 secret keys are used forserver-to-client messages. Among the 3 secret keys, one is used for encryption (e.g.,

DESsecret key), one is used for message integrity (e.g., HMAC) and one is used for cipherinitialization. (Cipher initialization uses a random plaintext called Initial Vector (IV) toprime thecipherpump.)

5. Client and server use the pre_master_secret (48-byte random number created by the clientandexchangesecurely),client_random,server_random,andapseudo-randomfunction(PRF)togenerateamaster_secret.Theycanusethemaster_secret,client_random,server_random, and the pseudo-random function (PRF) to generate all the 6 shared secretkeys. Once the secret keys are generated, the pre_master_secret is no longer needed andshould bedeleted.

6. Fromthispointonwards,alltheexchanges areencryptedusingthesessionkey.

7. The client sends Finished handshake message using their newly created session key. Serverrespondswith aFinishedhandshakemessage.

MessageExchange

Clientandservercanusetheagreed-uponsessionkey(consistsof6secretkeys)forsecureexchange of messages

Sendingmessages:

1. The sender compresses the message using the agreed upon compression method(e.g.,PKZip,gzip).

2. The sender has hes the compressed data and the secret HMAC key to make an HMAC, to assur e message integrity.

3. The sender encrypts the compressed data and HMAC using encryption/ decryption secret key, to assure message confidentiality.

ASSLSessionTrace

WecoulduseOpenSSL'ss_client(with debugoption)toproduceaSSLsession trace

> **openssls_client?**

(Displaytheavailableoptions)

Thefollowingcommandturnsonthedebugoptionandforcestheprotocolto beTLSv1:

➢ **openssls_client -connectlocalhost:443-CAfile ca.crt-debug-tls1**

Loading'screen'intorandomstate–done

CONNECTED(00000760)

writeto00988EB0[009952C8](102bytes=>102 (0x66))

0000- 16 03 01 00 61 01 00 00-5d03 01 40 44 35 27 5c....a...]..@D5'\

0010-5ae8 74 26e9 49 37 e2-063b 1c6d 7737 d1aeZ.t&.I7..;.mw7..

0020- 44 07 86 47 98 fa 84 1a-8d f472 00 00 3600 39D..G .....r..6.9

0030 - 00 38 00 35 00 16 00 13-00 0a00 33 00 32 00 2f.8.5.....3.2./

0040- 00 07 00 66 0005 00 04-00 63 00 6200 61 00 15...f.....c.b.a..

0050- 00 12 00 09 00 65 00 64-00 60 00 14 00 11 00 08 .....e.d.`.....

0060 - 00 06 00 03 01 .....

0066-<SPACES/NULS>

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5))

0000 - 16 03 01 00 2a *

TraceAnalysis

The data to be transmitted is broken up into series of fragments. Each fragment is protected forintegrityusingHMAC.

EachSSLrecordbeginswith a5-byteheader:

Byte0:RecordContentType.FourContentTypes aredefined,asfollows:

Content Type	HexCode	Description
Handshake	0x16	The record carries a handshaking
messageApplication_Data	0x17	EncryptedApplicationData
Change_Cipher_Spec	0x14	Toindicateachangeinencryptionmethods.
Alert	0x15	Tosignalvarioustypes of errors

Byte 1&2: SSL version(0x0301forTLSv1,0x0300 forSSLv3).

Byte3&4:Therecord length,excluding the5-byte header.

Client_Hello

The first handshake message is always sent by the client, called client_hello message. In thismessage, the client tells the server its preferences in terms of protocol version,

ciphersuit, andcompression method. The client also includes a 32-byte random number (client_random) in themessage, which is made up of a 4-byte GMT Unix time (seconds since 1970), plus another 28randombytes.

Server_Hello

In response to the client_hello message, the server returns a server_hello message to tell theclientits

choiceofprotocolversion,ciphersuitandcompressionmethod.Theserveralsoincludes a32-byterandomnumber(server_random) inthemessage.

Certificate

The certificate message consists of a chain of X.509 certificates in the correct order. The firstcertificate belongs to the server, and the next certificate contains the key that certifies the firstcertificate (i.e., the server's certificate), and so on. The client uses the server's public key (containedinsidetheserver'scertificate)toeitherencryptthepre_master_secretorverifytheserver_key_exchange, dependingonwhichciphersuitis used.

Server_Key_Exchange

Server_Hello_Done

This is an empty message indicating that the server has sent all the handshaking messages. This isneededbecausethe servercansendsomeoptionalmessagesafter thecertificatemessage

Client_Key_Exchange

The client_key_exchange message contains the pre_master_secret when RSA key exchangeis used. The pre_master_secret is 48-byte, consists of protocol version (2 bytes) and 46 randombytes.

Certificate_Verify

Change_Cipher_Spec

UnknownHandshakingMessage(D4) -tocheck

Application_Data

Client-to-Server-theHTTPrequestmessage:GET/test.htmlHTTP/1.0

Server-to-Client -theHTTPresponsemessage

RESULT:

Thus the confidentiality and Integrity using SSL was verified.

EX.No:6	EXPERIMENT EAVESDROPPING, DICTIONARY ATTACKS, MITM ATTACKS

AIM:

Toexperimenteavesdropping,Dictionaryattacks,MITMattacks.

PROCEDURE:

Password cracking is a term used to describe the penetration of a network, system, or resourcewith or without the use of tools to unlock a resource that has been secured with a password.Password cracking tools may seem like powerful decryptors, but in reality are little more thanfast,sophisticatedguessingmachines.

Types of password breaking

Dictionaryattack

Asimple*dictionary*attackisusuallythefastestwaytobreakintoamachine.Adictionaryfile (a text file full of dictionary words) is loaded into a cracking application, which is runagainst useraccountslocatedby theapplication

Bruteforceattack

A *brute force* attack is a very powerful form of attack, though it may often take a long time towork depending on the complexity of the password. The program will begin trying any andeverycombinationofnumbers andlettersandrunning them againstthehashedpasswords.

Hybrid attack

Another well-known form of attack is the *hybrid* attack. A hybrid attack will add numbers orsymbols to the search words to successfully crack a password. Many people change theirpasswords by simply adding a number to the end of their current password. Therefore, thistype of attack is the most versatile, while it takes longer then a standard dictionary attack itdoesnottakeas long as a bruteforceattack.

Task1–MicrosoftOfficePassword Recovery

ManyapplicationsrequireyoutoestablishanIDandpasswordthatmaybesavedandautomatically substituted for future authentication. The password will usually appear on thescreen as a series of asterisks. This is fine as long as your system remembers the password foryou but what if it "forgets" or you need it for use on another system. Fortunately, many utilitieshave been written to recover such passwords. In this task, you will use OfficeKey to recover thepasswordforaMSword document.

Step1: Findthefolder“Lab1” onyourdesktop,andopenit.

YouwillfindOfficeKeyandaMSdocumentin thefolder.

Step2: Openthe OfficeKey–PasswordRecoverytool

Step3: Press the“Recover” button inthe upperleft corner, orselectFile Recover

Step4: Choosethepassword protectedMS OfficeFileyouhavesavedto theDesktop.

Step 5: After running the first password auditing session, check to see if Office key has crackedthe password. If the password has not been cracked press the Settings button on theuppertoolbar.

Step6: OnceintheSettings menuyouwillbeabletomodifythesearchparameters andcustomize amoretargetedsearch

Step7: Repeatsteps3and4until thepassword hasbeencrackedand openstheMS Office File.

Step8: WritedownthecontentsoftheMSworddocumentandthepasswordinto yourlabreportandsubmitittoyour TA

RESULT:

Thus the experiment for Eavesdropping, Dictionaryattacks, MITM attacks was done successfully.

EX.No:7	EXPERIMENT WITH SNIFF TRAFFIC USING ARP POISONING

AIM

PerformanExperimenttoSniffTrafficusingARPPoisoning

PROCEDURE:

ARP is the acronym for Address Resolution Protocol. It is used to convert IP address to physicaladdresses [MAC address] on a switch. The host sends an ARP broadcast on the network, and therecipient computer responds with its physical address [MAC Address]. The resolved IP/MACaddressis then used to communicate. **ARP poisoning is sending fake MAC addresses to the switch so thatit can associate the fake MAC addresses with the IP address of a genuine computer onanetworkandhijack the traffic**.

ARPPoisoningCountermeasures:

Static ARP entries: these can be defined in the local ARP cache and the switch configured toignoreall auto ARP reply packets. The disadvantage of this method is, it's difficult to maintain on large networks. IP/MACaddressmappinghastobedistributedtoallthecomputersonthenetwork.

ARPpoisoningdetectionsoftware:thesesystemscanbeusedtocrosscheckthe IP/MAC address resolution and certify them if they are authenticated. Uncertified IP/MAC addressresolutionscanthenbeblocked.

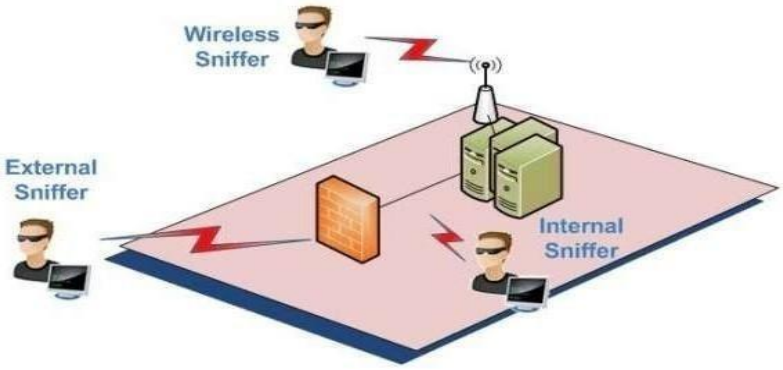
Whatisnetworksniffing?

Computerscommunicatebybroadcastingmessagesonanetworkusing IPaddresses.Onc eamessage has been sent on a network, the recipient computer with the matching IP addressrespondswithits MACaddress.

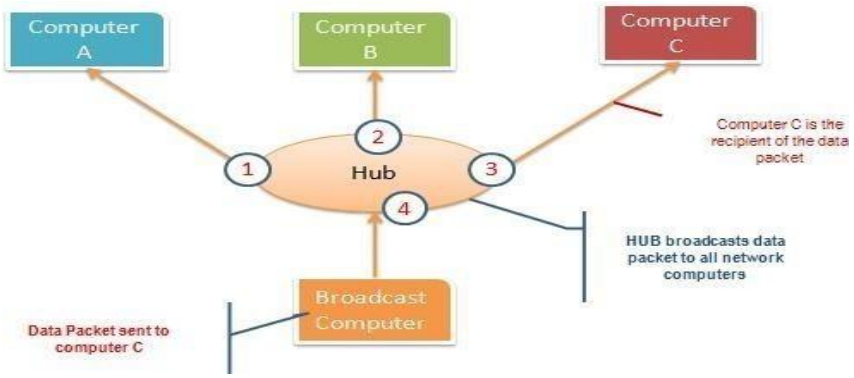
Network sniffing is the process of intercepting data packets sent over a network.

PassiveandActiveSniffing

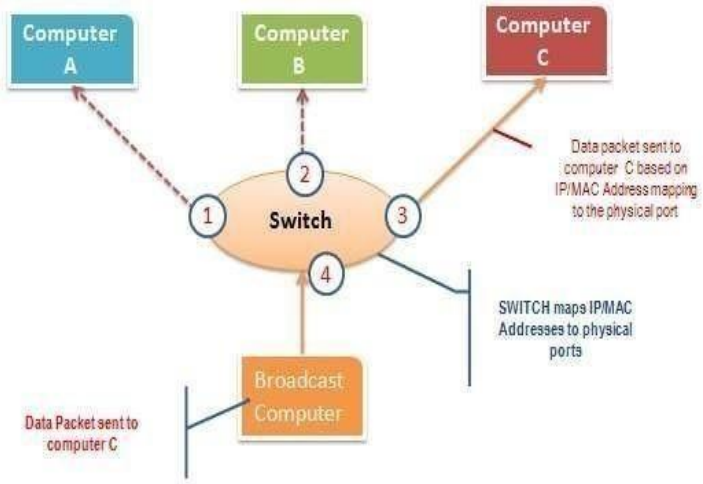
Before we look at passive and active sniffing, let's look at two major devices used to networkcomputers; hubs and switches.



Ahubworksbysendingbroadcastmessagestoalloutputportsonitexcepttheonethathassen tthebroadcast.



A switch works differently; it maps IP/MAC addresses to physical ports on it.



Passive sniffing is intercepting packages transmitted over a network that uses a hub. It iscalledpassivesniffingbecauseitisdifficulttodetect.Itisalsoeasy toperformas thehubsendsbroadcastmessagestoallthecomputers onthenetwork.

Active sniffing is intercepting packages transmitted over a network that uses a switch. Therearetwomainmethods used tosniff switchlinkednetworks,ARP Poisoning,andMACflooding.

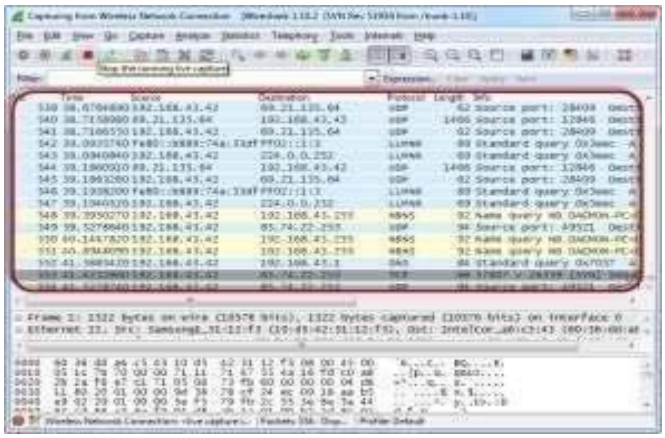
SniffingthenetworkusingWireshark

DownloadWiresharkfromthislinkhttp://www.wireshark.org/download.html

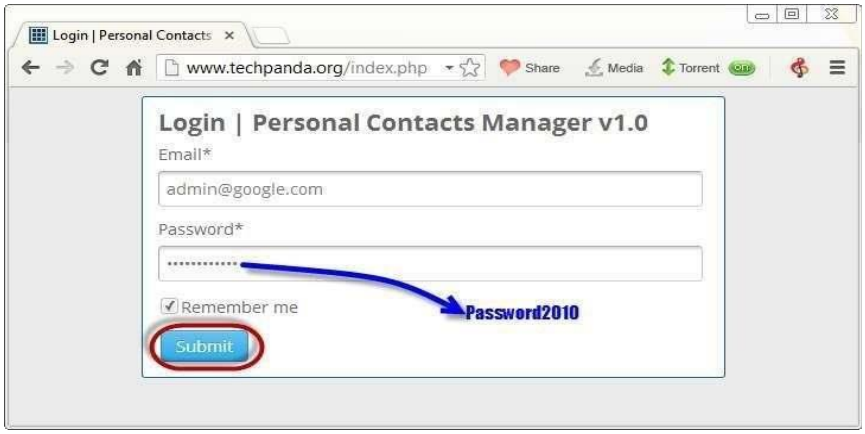
- OpenWireshark
- Youwillgetthefollowing screen

Selectthenetworkinterfaceyouwanttosniff.Noteforthisdemonstration,weareusingawirelessnetworkconnection.Ifyouareonalocalareanetwork,thenyoushouldselectthelocalareanetworkinterface.

- Click onstart buttonas shownabove



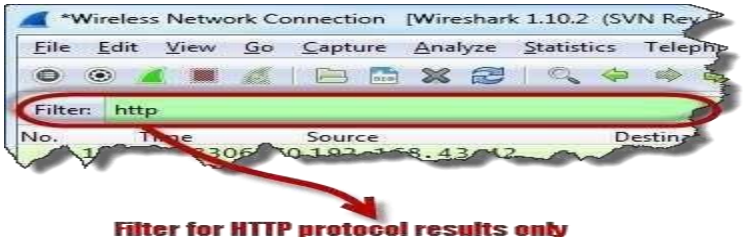
- Openyourwebbrowserandtypeinhttp://www.techpanda.org/



- Theloginemail is**admin@google.com**andthepassword is**Password2010**
- Clickonsubmitbutton
- Asuccessfullogonshould giveyouthefollowingdashboard

- GobacktoWiresharkandstopthelivecapture

- FilterforHTTPprotocolresultsonly using thefiltertextbox



- LocatetheInfocolumn andlookforentries withthe HTTPverbPOST andclickonit

- Just below the log entries, there is a panel with a summary of captured data. Look forthesummarythatsaysLine-basedtextdata: application/x-www-form-url encoded
- You should be able to view the plaintext values of all the POST variables submitted totheserver viaHTTP protocol.

Result:

Thustheexperiment to SniffTrafficusing ARPPoisoningwas performed.

EX.No:8	DEMONSTRATE INTRUSION DETECTION SYSTEM USING ANY TOOL

AIM:

TodemonstrateIntrusionDetectionSystem (IDS)usingSnortsoftwaretool.

STEPSONCONFIGURINGANDINTRUSIONDETECTION:

1. DownloadSnortfromtheSnort.orgwebsite.(http://www.snort.org/snort-downloads)
2. DownloadRules(https://www.snort.org/snort-rules).Youmustregistertogettherules. (Youshoulddownloadtheseoften)
3. Doubleclickonthe.exeto installsnort.Thiswillinstallsnortinthe"C:\ Snort"folder.Itisimportant tohaveWinPcap(https://www.winpcap.org/install/)installed
4. ExtracttheRulesfile.You willneedWinRARforthe.gzfile.
5. Copyallfiles fromthe"rules"folderoftheextractedfolder.Nowpastetherulesinto *"C:\Snort\rules"*folder.
6. Copy "snort.conf" file from the "etc" folder of the extracted folder. You must paste it into "C:\Snort\etc"folder.Overwrite anyexisting file. Remember if you modify your snort.conf fileanddownloadanewfile,youmustmodify itforSnortto work.
7. Openacommandprompt(cmd.exe)andnavigatetofolder"C:\Snort\bin"folder.
8. Tostart(execute)snortinsniffer modeusefollowingcommand:

snort -dev-i 3

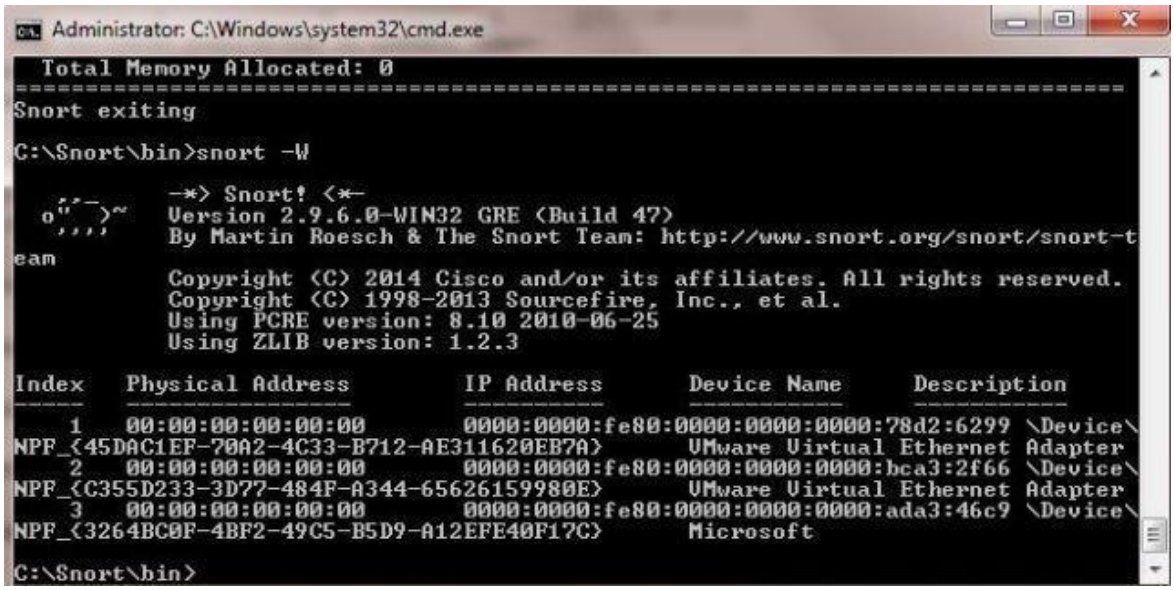
-iindicatestheinterface number.Youmustpickthecorrect interfacenumber.

Inmycase,itis3.

-devisused torunsnort tocapture packets onyournetwork.

Tocheck theinterfacelist,usefollowingcommand:

snort-W



Findinganinterface

You can tell which interface to use by looking at the Index number and finding Microsoft.As you canseein theabove example,theotherinterfacesareforVMWare.

To run snort in IDS mode, you will need to configure the file “snort.conf” according to your networkenvironment.

To specify the network address that you want to protect in snort.conf file, look for the following line.varHOME_NET192.168.1.0/24(You willnormallysee anyhere)

Youmay alsowantto settheaddressesofDNS_SERVERS, ifyouhavesomeonyournetwork.

examplesnort

Change the RULE_PATH variable to the path of rules folder.varRULE_PATHc:\

snort\rules

pathtorules

Changethepathofalllibraryfileswiththe nameandpathonyoursystem.andyoumustchangethepathofsnort_dynamicpreprocessorvariable.

C:\Snort\lib\snort_dynamiccpreprocessor

You need to do this to all library files in the "C:\Snort\lib" folder. The old path might be:"/usr/local/lib/…".youwillneedtoreplacethatpathwithyoursystempath.UsingC:\Snort\ libChangethe path of the"dynamicengine" variablevalue inthe "snort.conf"file..

dynamicengineC:\Snort\lib\snort_dynamicengine\sf_engine.dll

Addthepathsfor"include classification.config"and"include reference.config"files.include c:\ snort\etc\classification.config

includec:\snort\etc\reference.config

Removethecomment(#)ontheline to allowICMPrules, if itiscommentedwith a#.include $RULE_PATH/icmp.rules

You can also remove the comment of ICMP-info rules comment, if it iscommented.include $RULE_PATH/icmp-info.rules

To add log files to store alerts generated by snort,search for the "output log" test in snort.conf andaddthefollowing line:

outputalert_fast:snort-alerts.ids

Comment(adda#)thewhitelist $WHITE_LIST_PATH/white_list.rulesandtheblacklist

Changethenested_ipinner,\tonested_ip inner#,\Comment out(#)followinglines:

#preprocessornormalize_ip4

#preprocessornormalize_tcp:ipsecnstream

#preprocessor normalize_icmp4

#preprocessornormalize_ip6

#preprocessornormalize_icmp6

Savethe"snort.conf"file.

TostartsnortinIDS mode,runthe followingcommand:

snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3(Note: 3isusedformyinterfacecard) Ifalogiscreated,selecttheappropriateprogramto openit.YoucanuseWordPardorNotePad++toreadthefile.

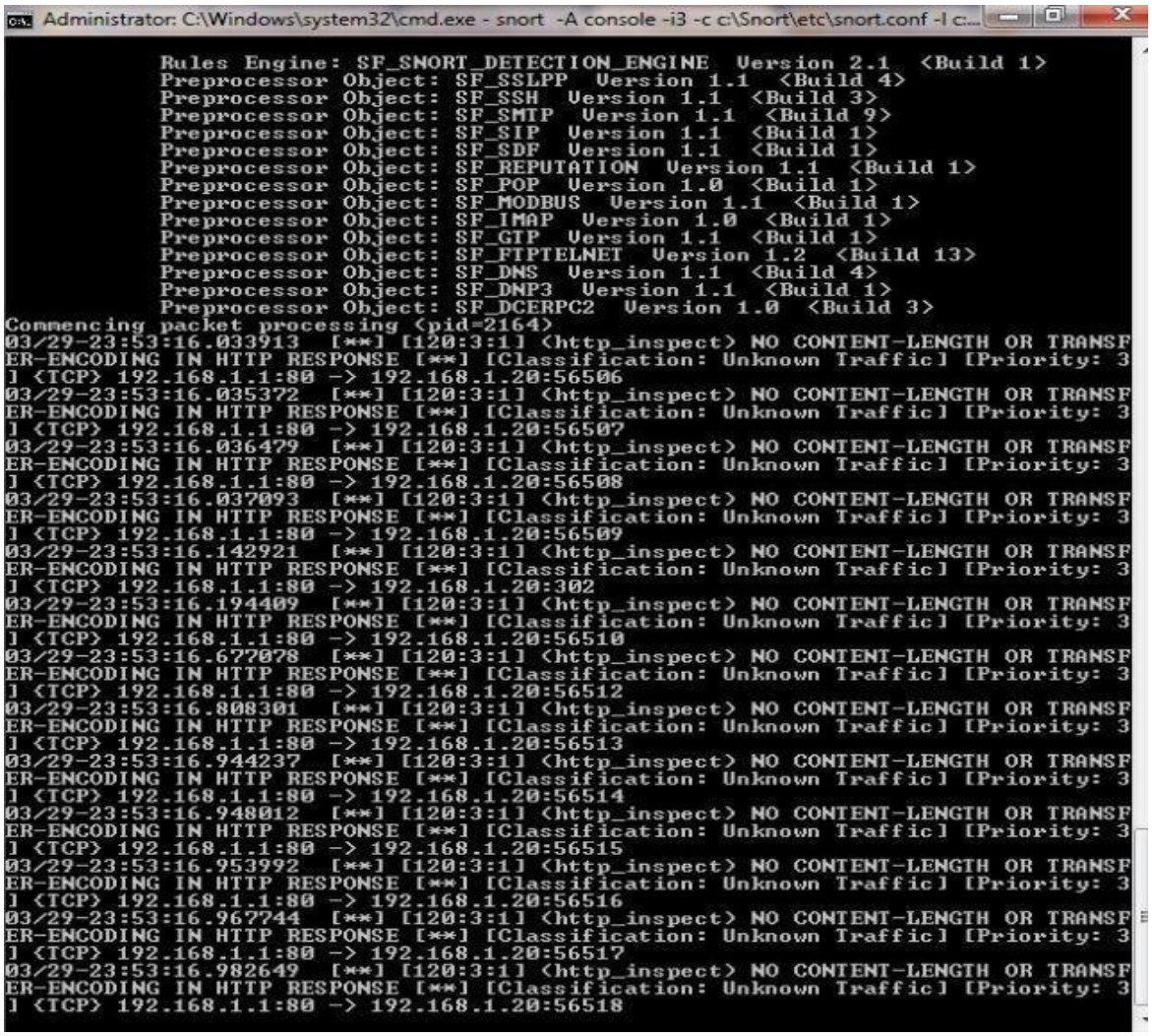
To generate Log files in ASCII mode, you can use following command while running snort in IDSmode:

snort-Aconsole-i3-cc:\Snort\etc\snort.conf-lc:\Snort\log-Kascii

Scanthecomputerthatisrunning snortfromanothercomputerbyusingPINGorNMap (ZenMap).

Afterscanningorduringthescanyoucancheckthesnort-alerts.ids filein thelogfoldertoinsureitisloggingproperly.You willseeIP address foldersappear.

Snortmonitoring traffic –



RESULT:

Thus the Intrusion Detection System(IDS) has been demonstrated by using the Open SourceSnortIntrusion DetectionTool.

EX.No:9	EXPLORE NETWORK MONITORING TOOLS

AIM:

ToexploreaboutNetwork monitoringtools

Network monitoring is an essential part of network management. It involves using various tools tomonitorasystemnetworkanddeterminesslownessandweakconnections,amongotherissues.K nowing more about these tools can help you understand them better and use the right ones that suityour requirements.

PROCEDURE:

WhatAreNetworkMonitoring Tools?

Network monitoring tools aresoftware that you can use to evaluatenetwork connections. Thesesoftwareprogramscan help you monitor a network connection and identifynetworkissues,whichmayincludefailingnetworkcomponents,slowconnectionspeed,n etworkoutageorunidentifiabl econnections. Network management and monitoring tools canalsohelyouresolvetheseissuesorestablishsolutionsthatpreventspecificissuesfromoccurrin ginthefuture.

NetworkMonitoringTools

Hereareeightmonitoringtoolsalongwiththeirdescriptions andfeatures:

1. SolarWindsNetworkPerformanceMonitor

SolarWindsNetworkPerformanceMonitorisamulti-vendormonitoringtool.Itallowsuserstomonitor multiple vendors' networks at the same time. Italsoprovidesnetworkinsightsfothoroughvisibilityintothehealthofthenetworks.Somepromin entfeaturesincludenetworkavailabilitymonitoring,intelligentnetworkmapping,criticalpathvis ualisation,performanceanalysisandadvancedalerting.SolarWindsalsoallowsuserstotrackVP Ntunnelstatus.ItpromptswhenaV PNtunnel is available to help users ensure a stable connection between sites. SolarWinds provides aseven-dayfree trial,afterwhich userscanchoose a preferredsubscriptionplan.

2. DatadogNetworkMonitoring

DatadogNetworkMonitoringoffersservicesforon-premisesdevicesandcloudnetworks.Ahighlighting feature of this tool is the visualisations. It offers various graphical representationsof allthe network connections on a system. It also allows users to track key metrics like network latency,connection churn and transmission control protocol (TCP) retransmits. Users can monitor the health ofa network connection at different endpoints at the application, IP address, port or process ID layers.Otherprominentfeaturesinclude automatedlogcollectionand user interfacemonitoring.

3. PaesslerPRTGNetworkMonitor

Paessler's network connection monitoring tool provides a clean user interface and network visibility onmultiple devices. Users can track the health of different connection types like local area networks(LAN),wideareanetwork(WAN),servers,websites,applicationsandservices.Thetool salsointegrate with various technologies, which makes it easier to use it for different types of applications. Itprovides distribute monitoring, allowing users to track network connections on devices in differentlocations. The tool also provides apps for mobile platforms that can help users to track network healthonmobilephones.

4. ManageEngineOpManager

ManageEngine OpManager is a good network monitoring and managing tool for users that prefer in-depth view of network health and issues. This tool provides over 2000 network performancemonitorsthatallowuserstotrackandmonitortheirconnectionsandperformdetaileda nalysesoniss ues.Italsoprovides over 200 dashboard widgets that can help users customise their dashboard to their ownsuitability. Other features include CPU, memory and disk utilisation monitoring on local and virtualmachines. It also allows setting network performance threshold and notifies the user in case of aviolation.

5. Domotz

Domotz is an expansive tool that provides a list of features for monitoring network

connections. Itallows users to customise their network monitoring preferences. Users can write scripts the retrieve thedata they wish to evaluate. It also allows connection to open ports on remote devices while ensuringnetwork security. Users can also scan and monitor network connections globally. Domotz also allowsto backup and restore network configuration for switches, firewalls and access points and alerts whenthere is achangein theconfiguration.

6. Checkmk

Checkmk is a tool that allows users to automate it completely. You can customise its operations andenable it to perform tasks automatically. It also identifies network and security components without theuser requiring manual set up. For example, the tool can identify a firewall even if the user has not set itup. Its Agent Bakery feature enables users to manageagents and automate agentupdating. Thisreduces manual effort to monitor network connections. The tool also includes over 2000 plug-ins forenhancing network monitoring.

7. ProgressWhatsupGold

Progress Whatsup Gold is a basic network monitoring software. It provides a minimal user interfacewith essential features like device monitoring,applicationmonitoring,analysingnetworktraffic andmanagingconfigurations.Thetoolallowsuserstomonitorclouddevices,inspectsuspiciousconnections,automateconfigurationbackupsand identify,and resolve bandwidthissues.

OtherToolsForNetworkMonitoring

Herearethreeadditionaltools fornetworkmonitoring:

- FortraIntermapper: This tool enables users to monitor network connections using networkmaps, allowing them to get a holistic view of all the connections. Italso provides variouscolour codes for different network status, along with real-time notifications through text, emailand sound.

Nagios Core: Nagios Core is a monitoring engine that works as the primary application for allNagiosprojects,includingtheNagiosNetworkAnalyser.ItintegrateswithotherNagiosapplications andprovidesuserswithfeatureslikeavisualdashboard,customapplicationmonitoring,automatedalertsystem,advancedusermanagementandnetworksecuritymonitoring

• Zabbix: Zabbix provides a thorough network monitoring solution with features like servermonitoring, cloud monitoring, application monitoring and service monitoring. The tool alsoincludesfeatureslikemetric collection,

ToChooseaNetworkMonitoringAndManagementTool:

Understandtherequirements

Understanding why you require network monitoring software is important in the process. Define whatfeature you want and for what purpose. This can help you identify the right tool for your use. It mayalsohelp youchoosethecorrectsubscription planonpaidtools.

Browsemultipletools

Once you identify the requirements, consider browsing multiple tools. Visit the websites of the toolsand look for the features you require. Spend time studying the features and understand how they can beusefulto yourrequirements. Youcanalsoidentifyafewtoolsandcomparetheirfeaturestoeachother.

Considerthebudget

Some tools may be free to use, while some may require you to purchase a subscription plan Paid tools typically offer a freetrial period of upto 30days.Once you identify which tool you may liketous ,see if it is free or requires payment.If it is a paid tool,try exploring its features and efficiency duringt hetrialperiod.Consider keeping a backup tool incase the tool that you choose does not fit your usage.

RESULT:

Thus the network monitoring tools was explored.

EX.No:10	STUDY TO CONFIGURE FIREWALL, VPN

AIM:

To study the features of firewallinprovidingnetworksecurityandtosetFirewallSecurityin windows.

PROCEDURE:

FirewallinWindows7

Windows 7 comes with two firewalls that work together. One isthe**Windows Firewall**, and the other is **Windows Firewall with Advanced Security (WFAS)**.Themaindifferencebetweenthemisthe complexityofthe rules configuration. Windows Firewall uses simple rules thatdirectlyrelate toa program or a service. The rules in WFAS can be configured based on protocols, ports, addresses andauthentication. By default, both firewalls come with predefined set of rules that allow us to utilizenetwork resources. This includes things like browsing the web, receiving e-mails, etc. Other standardfirewall exceptions are File andPrinterSharing,NetworkDiscovery, PerformanceLogsandAlerts,RemoteAdministration,WindowsRemoteManagement,Remote Assistance,Remot eDesktop,WindowsMediaPlayer,WindowsMediaPlayerNetworkSharing Service

With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outboundtraffic is allowed, and inbound responses to that traffic are also allowed. Inbound trafficinitiatedfrom externalsourcesis automaticallyblocked.

When we first connect to some network, we are prompted toselecta network location. This feature is known as Network Location Awareness(NLA). This feature enables us to assign a network profileto the connection based on the location. Different network profiles contain different collections offirewall rules. In Windows 7, different network profiles can be configured on different interfaces. Forexample, our wired interface can have different profile than our wireless interface.

There are two different network profiles available:

- Public
- Home/Work-privatenetwork

ConfiguringWindowsFirewall

ToopenWindowsFirewallwecangoto**Start>ControlPanel>Windows**

Bydefault,Windows Firewallisenabledfor bothprivate(home or work)and public networks. Itis also configured to block all connectionsto programs that are not on the list of allowed programs.To configure exceptions we can go to the menu on the left and select "Allow a program or featurethroughWindows Firewall"option.

FirewallCustomization

Note that we can modify settings for each type of network location (private or public).Interesting thing here is that we can block all incoming connections, including those in thelistofallowedprograms.

Windows Firewall is actually a Windows service. As you know, services can be stoppedand started. If the Windows Firewall service is stopped, the Windows Firewall will notwork.

FirewallService

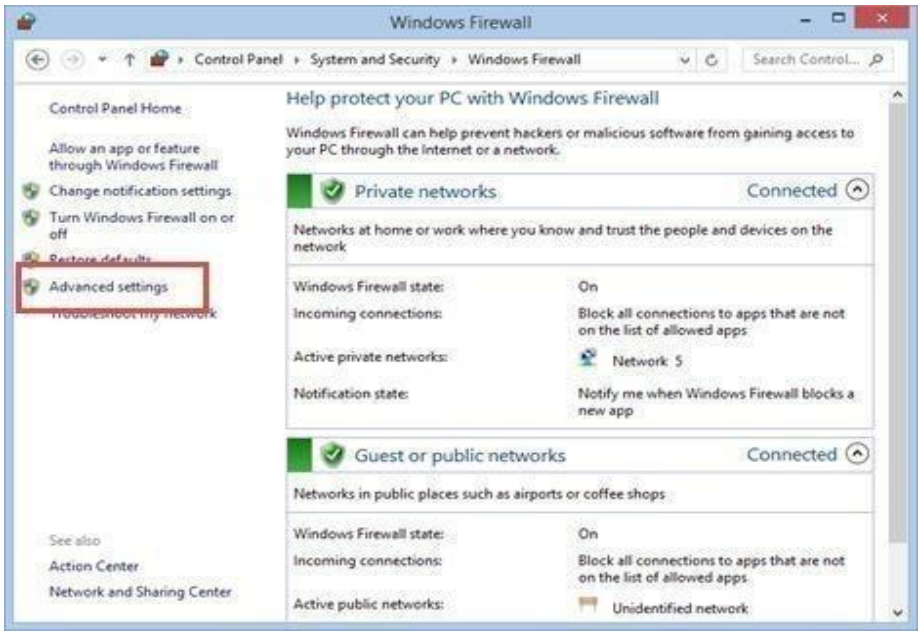
In our case the service is running.Ifwestop it, wewillgeta warningthatwe shouldturnon ourWindowsFirewall.

HowtoStart&UsetheWindowsFirewallwithAdvancedSecurity

The *Windows Firewall with Advanced Security* is a tool which gives you detailed controlovertherulesthatareappliedbythe*WindowsFirewall*.Youcanviewallthe rulesthatare used by the *Windows Firewall*, change their properties, create new rules or disableexistingones.

Youhaveseveralalternativestoopeningthe*WindowsFirewallwith AdvancedSecurity*:

OneistoopenthestandardWindowsFirewallwindow,bygoingto*"ControlPanel->SystemandSecurity->WindowsFirewall"*.Then,click ortap*Advanced settings*.



InWindows7,anothermethodistosearchfortheword*firewall*inthe*StartMenu*searchboxandclic kthe*"WindowsFirewall withAdvanced Security"*result.

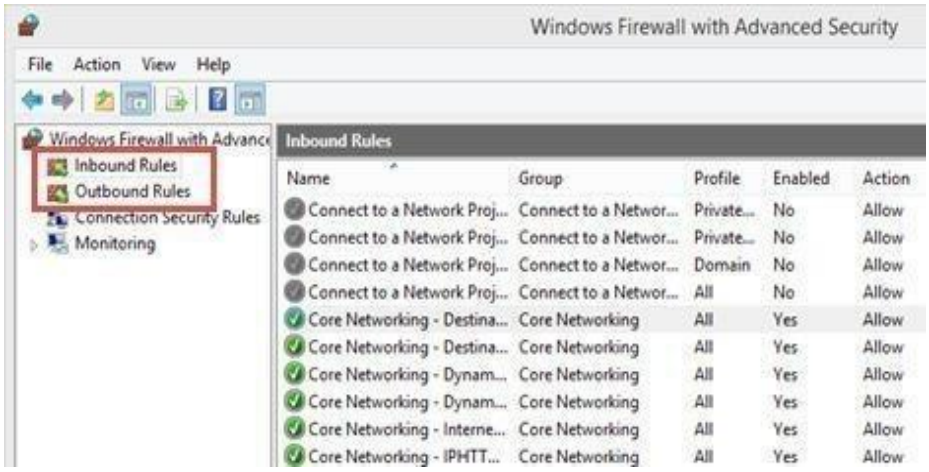
WhatAreTheInbound&OutboundRules?

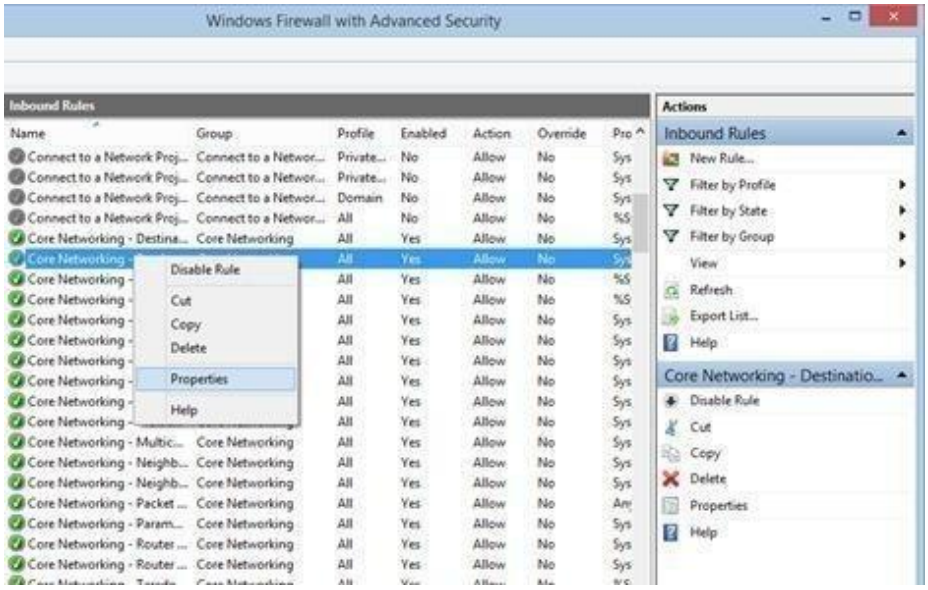
In order to provide the security you need, the *Windows Firewall* has a standard set ofinbound and outbound rules, which are enabled depending on the location of the networkyouareconnectedto.

Inbound rules are applied to the traffic that is coming from the network and the Internet toyour computer or device. Outbound rules apply to the traffic from your computer to thenetworkortheInternet.

These rules can be configured so that they are specific to: computers, users, programs,services, ports or protocols. You can also specify to which type of network adapter (e.g.wireless,cable,virtualprivatenetwork)oruserprofileitisapplied to.

In the *Windows Firewall withAdvancedSecurity*,youcanaccessallrules and edittheir properties. All you have to do is clickor tap the appropriate unit in the left-sidepanel.





WhataretheConnectionSecurityRules?

Connection security rules are used to secure traffic between two computers while itcrosses the network. One example would be a rule which defines that connectionsbetweentwospecificcomputersmustbeencrypted

Ifyouwanttoseeiftherareanysuchrulesonyourcomputer,clickortap*"Connection Security*

*Rules"*on the panel on the left.By default,there are no suchrulesdefinedonWindowscomputersanddevices.Theyaregenerallyusedinbusinessenvironmentsand suchrulesaresetbythe networkadministrator.

WhatdoestheWindowsFirewallwithAdvancedSecurityMonitor?

The *Windows Firewall with Advanced Security* includes some monitoring features aswell. Inthe *Monitoring* section you can find the following information: the firewallrulesthatareactive (both inbound and outbound), the connection security rules that are active and whetherthere areany activesecurity associations.

RESULT:

Thus study of the features of firewall in providing network security and to set Firewall Security in windows.