|  |  |
| --- | --- |
| **EX.No:1** | **IMPLEMENTSYMMETRICKEYALGORITHMS** |
|  |

# AIM:

TouseDataEncryptionStandard(DES)Algorithmforapracticalapplicationlike User MessageEncryption.

# ALGORITHM:

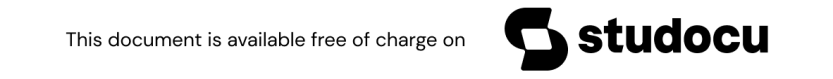
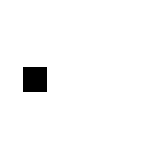
1. CreateaDESKey.
2. CreateaCipherinstancefromCipherclass,specifythefollowing information and separated by aslash(/).
   1. Algorithmname
   2. Mode(optional)
   3. Paddingscheme(optional)
3. ConvertString into***Byte[]***arrayformat.
4. MakeCipherinencrypt mode,andencryptitwith ***Cipher.doFinal()*** method.
5. MakeCipherindecrypt mode,anddecryptitwith ***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;

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



publicclassDES

{

publicstaticvoidmain(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("DecryptedMessage:"+newString(textDecrypted));

}catch(NoSuchAlgorithmExceptione){ e.printStackTrace();

}catch(NoSuchPaddingExceptione){ e.printStackTrace();

}catch(InvalidKeyExceptione){ e.printStackTrace();

}catch(IllegalBlockSizeExceptione){ e.printStackTrace();

}catch(BlockPaddingExceptione){ e.printStackTrace();

}}}

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

# OUTPUT:

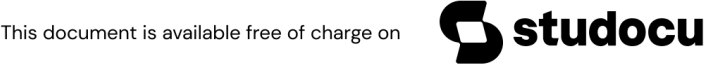
MessageEncryptionUsingDESAlgorithm

Message[ByteFormat]:[B@4dcbadb4 Message:SecretInformation EncryptedMessage:[B@504bae78 DecryptedMessage:SecretInformation

# RESULT:

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

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



|  |  |
| --- | --- |
| **EX.No:2a** | **IMPLEMENTASYMMETRICKEYALGORITHMSANDKEY**  **EXCHANGEALGORITHMS - RSAALGORITHM** |
|  |

# AIM:

ToimplementRSA(Rivest–Shamir–Adleman)algorithmbyusingHTMLandJavascript.

# ALGORITHM:

1. Choosetwoprimenumberpandq
2. Computethevalueofnandp
3. Findthevalueof***e***(publickey)
4. Computethevalueof***d***(privatekey)usinggcd()
5. Dotheencryptionanddecryption
   1. Encryptionisgivenas,

### c=temodn

* 1. Decryptionisgivenas,

***t=cdmodn***

## 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>

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

<tr>

<td>EnterFirstPrimeNumber:</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>

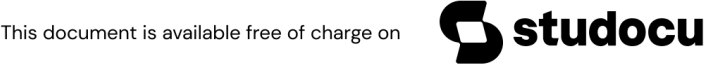
<tr>

<td>PrivateKey:</td>

<td>

<pid="privatekey"></p>

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



</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

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

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 =

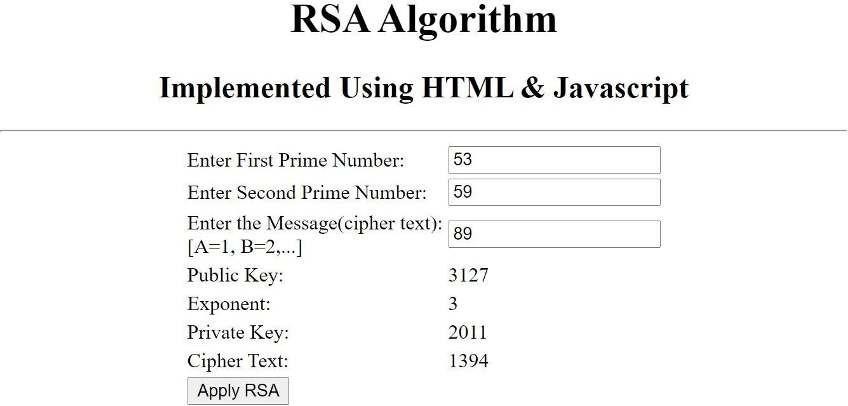
n;document.getElementById('exponent').innerHTML = e;document.getElementById('privatekey').innerHTML=d;document.getElementById('ciph ertext').innerHTML=ct;

}

</script>

</html>

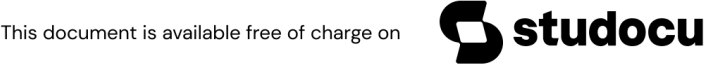
# OUTPUT:

****

**RESULT:**

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

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



|  |  |
| --- | --- |
| **EX.No:2b** | **IMPLEMENTASYMMETRICKEYALGORITHMSANDKEY EXCHANGE ALGORITHMS –**  **DIFFIE-HELLMANKEYEXCHANGEALGORITHM** |
|  |

# AIM:

ToimplementtheDiffie-HellmanKeyExchangealgorithmforagivenproblem.

# ALGORITHM:

1. AliceandBobpubliclyagreetouseamodulus*p*=23andbase*g*=5(whichis aprimitiverootmodulo 23).
2. Alicechoosesasecretinteger***a***=4,thensendsBob*A*=*g****a***mod*p* o *A*=5**4**mod 23=4
3. Bobchoosesasecretinteger***b***=3,thensendsAlice*B*=*g****b***mod*p*

o *B*=5**3**mod23=10

1. Alicecomputes***s***=*B****a***mod*p*

o ***s***=10**4**mod23=18

1. Bobcomputes***s***=*A****b***mod*p*

o ***s***=4**3**mod23=18

1. AliceandBobnowshareasecret(thenumber18).

## PROGRAM:DiffieHellman.java

classDiffieHellman{ publicstaticvoidmain(Stringargs[]){

intp=23;/\* publiclyknown(prime number)\*/intg=5;/\*publiclyknown(primitiveroot)\*/ 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;

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

doublealiceComputes =(Math.pow(bobSends,x))%p; doublesharedSecret =(Math.pow(g,(x\* y)))% p; System.out.println("simulationofDiffie-Hellmankeyexchangealgorithm\ 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:

SimulationofDiffie-Hellmankeyexchangealgorithm

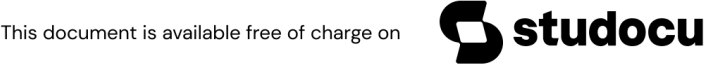
AliceSends:4.0 BobComputes:18.0 BobSends:10.0 AliceComputes:18.0 SharedSecret :18.0

Success:SharedSecretsMatches!18.0

# RESULT:

ThustheDiffie-HellmankeyexchangealgorithmhasbeenimplementedusingJava Program and the output has been verified successfully.

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



|  |  |
| --- | --- |
| **EX.No:3** | **IMPLEMENTDIGITALSIGNATURESCHEMES** |
|  |

# AIM:

ToimplementtheSIGNATURESCHEME-DigitalSignatureStandard.

# ALGORITHM:

1. CreateaKeyPairGeneratorobject.
2. InitializetheKeyPairGeneratorobject.
3. GeneratetheKeyPairGenerator.
4. Gettheprivatekeyfromthepair.
5. Createasignatureobject.
6. InitializetheSignatureobject.
7. AdddatatotheSignatureobject.
8. CalculatetheSignature

# PROGRAM:

importjava.security.KeyPair; importjava.security.KeyPairGenerator; importjava.security.PrivateKey;import java.security.Signature; importjava.util.Scanner; publicclassCreatingDigitalSignature{

publicstaticvoidmain(Stringargs[])throwsException{

Scannersc=newScanner(System.in);System.out.println("Entersome text");Stringmsg =sc.nextLine();

KeyPairGeneratorkeyPairGen=KeyPairGenerator.getInstance("DSA");keyPair Gen.initialize(2048);

KeyPairpair=keyPairGen.generateKeyPair();

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

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:

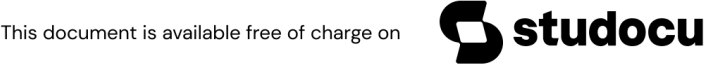
Entersometext Hihowareyou

Digitalsignatureforgiventext:0=@gRD???-?.????/yGL?i??a!?

# RESULT:

Thusthe DigitalSignature Standard Signature Scheme hasbeenimplementedandthe output has been verified successfully

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



|  |  |
| --- | --- |
| **EX.No:4** | **INSTALLATION OF WIRE SHARK, TCPDUMP AND OBSERVE DATATRANSFERREDINCLIENT-SERVERCOMMUNICATION**  **USINGUDP/TCPANDIDENTIFYTHEUDP/TCPDATAGRAM** |
|  |

# 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.



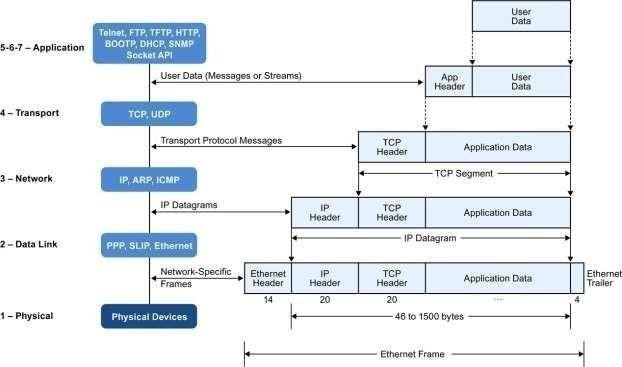
**Figure1**:WiresharkinKaliLinux

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

## Background

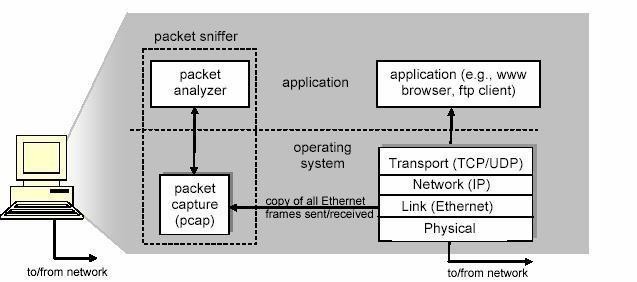
**TCP/IPNetworkStack**

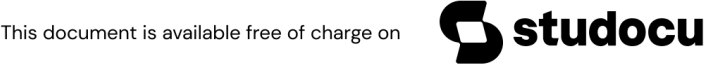
****

**Figure2**:EncapsulationofDataintheTCP/IPNetworkStack

## PacketSniffer

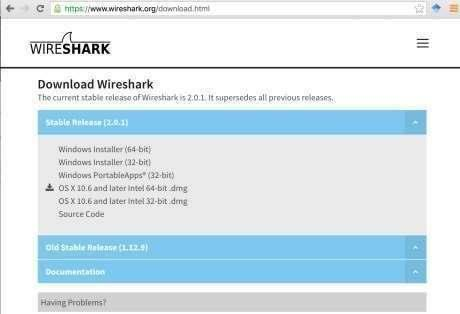
Packet sniffer is a basic tool for observing network packet exchangesin a computer.As thename suggests, a packet sniffer captures (“sniffs”) packets being sent/received from/by yourcomputer; it will also typically store and/or display the contents of the various protocol fields inthese captured packets.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





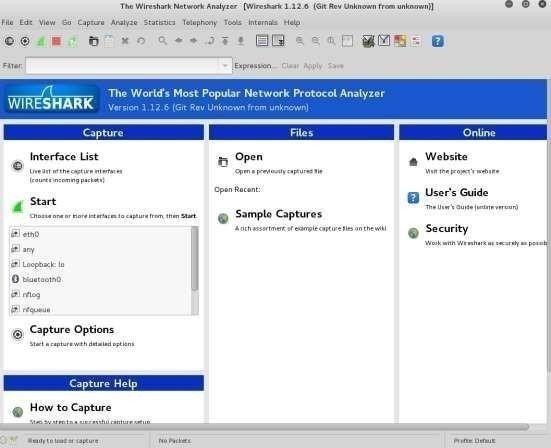
**GettingWireshark** TheKaiLinuxhasWiresharkinstalled.YoucanjustlaunchtheKaliLinuxVMandopenWiresharkt here.

Wiresharkcanalsobedownloadedfromhere:https://[www.wireshark.org/download.html](http://www.wireshark.org/download.html)



## StartingWireshark:

WhenyouruntheWiresharkprogram,theWiresharkgraphicuserinterface



**Figure:**Currently,theprogramisnotcapturingthepackets

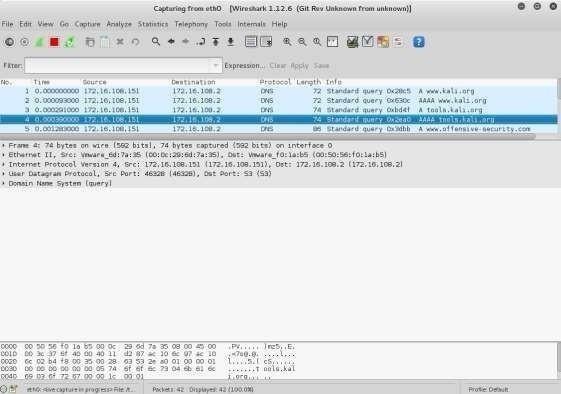
Then,youneedtochooseaninterface.IfyouarerunningtheWiresharkonyourlaptop,

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

youneed to select WiFi interface. If you are at a desktop, you need to select the Ethernet interfacebeing used. Notethat there could bemultipleinterfaces. Ingeneral, you can select anyinterfacebutthatdoesnotmeanthattrafficwillflowthroughthatinterface.The

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

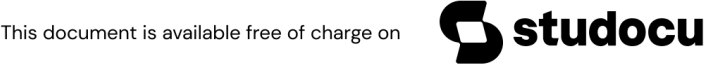
Afteryouselecttheinterface,youcanclickstarttocapturethepacketsasbelow.



## CapturingPackets

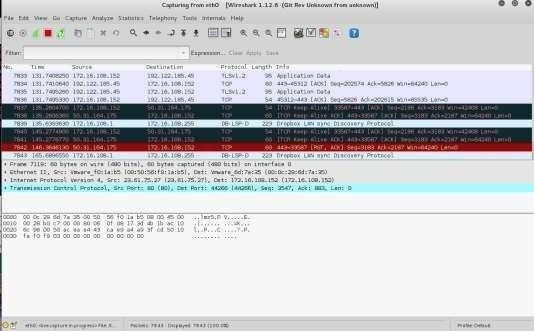
After downloading and installing Wireshark, you can launch it and click the name of an interfaceunder Interface List to start capturing packets on that interface. For example, if you want tocapture trafficonthewirelessnetwork,click yourwirelessinterface.

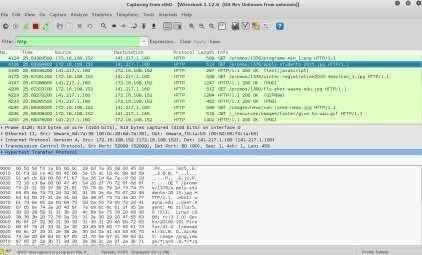
DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

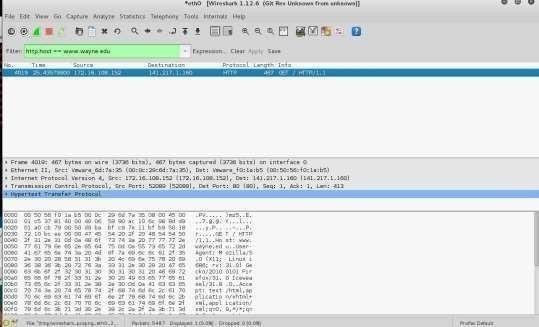


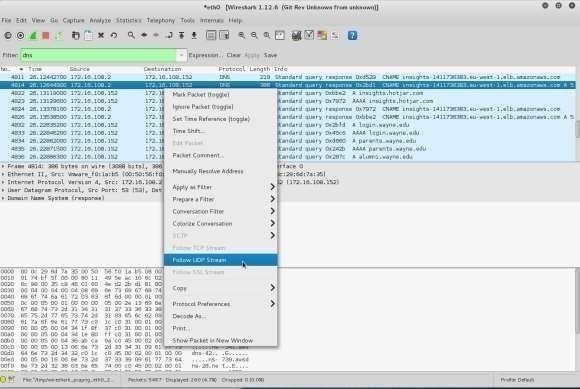
## TestRun Dothefollowingsteps:

1. StartuptheWiresharkprogram(selectaninterfaceandpressstarttocapturepackets).
2. Startupyourfavouritebrowser(ceweaselinKaliLinux).
3. Inyourbrowser,goto WayneStatehomepagebytyping[www.wayne.edu.](http://www.wayne.edu/)
4. After your browser has displayed the [http://www.wayne.edupage](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** | **CHECKMESSAGEINTEGRITYAND**  **CONFIDENTIALITYUSINGSSL** |
|  |

# AIM:

TochecktheMessageIntegrityandConfidentiality usingSSL.

# PROCEDURE:

## SSLSessioninDetails

**Handshaking-Cipher suit Negotiation** ClientsendsaplaintextClient\_Hellomessageandsuggestssomecryptographicparameters(colle ctivelycalledciphersuit)tobeusedfortheircommunicationsession.TheClient\_Hellomessageal socontainsa 32-byterandom numberdenoted asclient\_random.Forexample,.

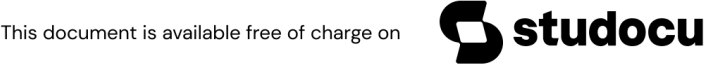
Client\_Hello:

ProtocolVersion:TLSv1ifyoucan,elseSSLv3. KeyExchange:RSAifyoucan,elseDiffe-Hellman.

SecretKeyCipherMethod:3DESifyoucan,elseDES. Message Digest:SHA-1ifyoucan,elseMD5.

DataCompressionMethod:PKZipifyoucan,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.)

ThenextstepistoestablishtheSessionKey:

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 sessionkey,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 secretkeysareusedforclient-to-servermessages,andtheother3secretkeysareused forserver-to-clientmessages.Amongthe3secretkeys,oneisusedforencryption(e.g.,

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

DESsecret key), one is used for message integrity (e.g., HMAC) and one is used for cipherinitialization.(Cipherinitializationuses arandomplaintextcalled InitialVector (IV) toprime thecipherpump.)

1. 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\_rando m,server\_random,andthepseudo-randomfunction(PRF)togenerateallthe6shared secretkeys. Once the secret keys are generated, the pre\_master\_secret is no longer needed andshould bedeleted.
2. Fromthispointonwards,alltheexchangesareencryptedusingthesessionkey.
3. The client sends Finished handshake message using their newly created session key. Serverrespondswith aFinishedhandshakemessage.

## MessageExchange

Clientandservercanusetheagreed-uponsessionkey(consistsof6secretkeys)forsecureexchange of messages

Sendingmessages:

1. Thesendercompressesthemessageusingtheagreed uponcompression method(e.g.,PKZip,gzip).
2. ThesenderhashesthecompresseddataandthesecretHMACkeytomakean 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(withdebugoption)toproduceaSSLsessiontrace

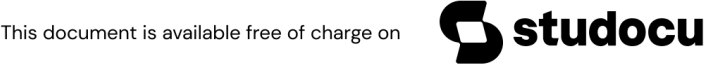
## > openssls\_client?

(Displaytheavailableoptions) ThefollowingcommandturnsonthedebugoptionandforcestheprotocoltobeTLSv1:

## openssls\_client-connectlocalhost:443-CAfileca.crt-debug-tls1

Loading'screen'intorandomstate–done

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



CONNECTED(00000760) writeto00988EB0[009952C8](102bytes=>102 (0x66))

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

0010-5ae87426e94937 e2-063b1c6d7737d1aeZ.t&.I7..;.mw7..

0020-44 07 86 4798 fa84 1a-8df472 00 00 3600 39D..G r..6.9

0030-00 38 00 35 00 1600 13-00 0a00 33 00 3200 2f.8.5.......3.2./

0040-00 07 00 66 0005 0004-00 63 00 6200 61 00 15...f.....c.b.a..

0050-00 12 00 09 00 65 00 64-0060 00 14 00 11 00 08.....e.d.`......

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

0066-<SPACES/NULS>

readfrom00988EB0[00990AB8](5bytes=>5(0x5)) 0000 - 16 03 01 00 2a \*

## TraceAnalysis

Thedatatobetransmittedisbrokenupintoseriesoffragments.Eachfragmentis protected forintegrityusingHMAC.

EachSSLrecordbeginswith a5-byteheader: Byte0:RecordContentType.FourContentTypes aredefined,asfollows:

|  |  |  |
| --- | --- | --- |
| **ContentType** | **HexCode** | **Description** |
| Handshake | 0x16 | Therecordcarriesahandshaking |
| messageApplication\_Data 0x17 EncryptedApplicationData | | |
| Change\_Cipher\_Spec0x14 | | Toindicateachangeinencryptionmethods. |
| Alert | 0x15 | Tosignalvarioustypesoferrors |

Byte1&2:SSLversion(0x0301forTLSv1,0x0300forSSLv3). Byte3&4:Therecord length,excluding the5-byte header.

## Client\_Hello

Thefirsthandshakemessageisalwayssentbytheclient,calledclient\_hellomessage.Inthismessage, the client tells the server its preferences in terms of protocol version,

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

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\_hellomessage, the server returns a server\_hellomessage to telltheclientitschoiceofprotocolversion,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 theserver's public key

(containedinsidetheserver'scertificate)toeitherencryptthepre\_master\_secretorverifytheserve r\_key\_exchange, dependingonwhichciphersuitis used.

## Server\_Key\_Exchange Server\_Hello\_Done

This is an empty message indicating thatthe 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.

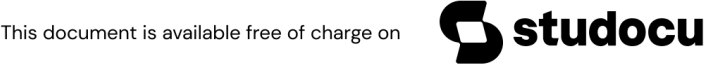
## Certificate\_Verify Change\_Cipher\_Spec

UnknownHandshakingMessage(D4)-tocheck

## Application\_Data

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

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



# RESULT:

ThustheconfidentialityandIntegrityusingSSLwasverified.

|  |  |
| --- | --- |
| **EX.No:6** | **EXPERIMENTEAVESDROPPING,DICTIONARY**  **ATTACKS,MITMATTACKS** |
|  |

# 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.

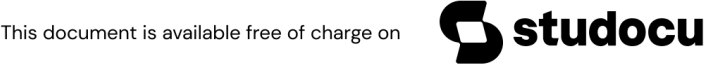
## Typesofpasswordbreaking Dictionaryattack

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

## Bruteforceattack

A*bruteforce*attackisaverypowerfulformofattack, thoughitmayoftentakealongtime towork depending on the complexity of the password. The program will begin trying any andeverycombinationofnumbers andlettersandrunning them againstthehashedpasswords.

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



## Hybridattack

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 theirpasswordsbysimplyaddinganumber tothe endoftheir currentpassword.Therefore, thistype of attack is the most versatile, while it takes longer then a standard dictionary attack itdoesnottakeas long as a bruteforceattack.

## Task1–MicrosoftOfficePasswordRecovery

ManyapplicationsrequireyoutoestablishanIDandpasswordthatmaybesavedandaut omatically 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

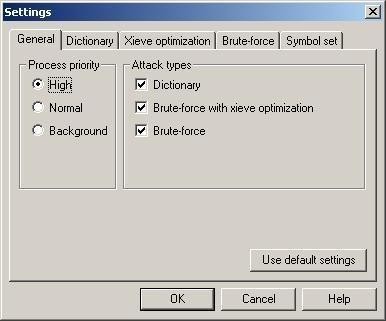
**Step3:**Pressthe“Recover”buttonintheupperleftcorner,orselectFileRecover

**Step4:**ChoosethepasswordprotectedMSOfficeFileyouhavesavedtotheDesktop.

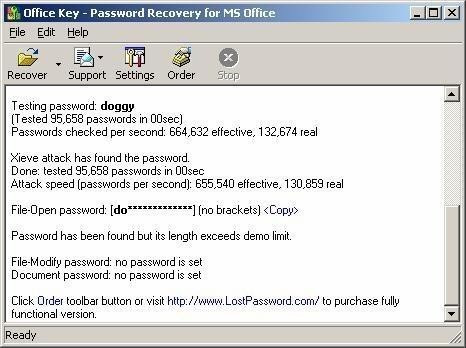


**Step 5:** After running the first password auditing session, check to see if Office key has crackedthe password. If the password has not been cracked press the Settings button on theuppertoolbar.

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



**Step6:**OnceintheSettings menuyouwillbeabletomodifythesearchparameters andcustomize amoretargetedsearch



**Step7:**Repeatsteps3and4until thepassword hasbeencrackedand openstheMS Office File. **Step8:**WritedownthecontentsoftheMSworddocumentandthepasswordinto yourlabreportandsubmitittoyour TA

# RESULT:

ThustheexperimentforEavesdropping,Dictionaryattacks,MITMattackswas done successfully.

|  |  |
| --- | --- |
| **EX.No:7** | **EXPERIMENTWITHSNIFFTRAFFICUSINGARP**  **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 anARP broadcast on the network, and therecipient computer responds with its physical address [MAC Address]. The resolved IP/MACaddressis then used to communicate. **ARP poisoningissendingfakeMACaddressestotheswitchsothatitcanassociatethefake MAC addresses with the IP address of a genuine computer onanetworkandhijack the traffic**.

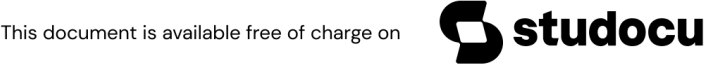
## ARPPoisoningCountermeasures:

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

## Whatisnetworksniffing?

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

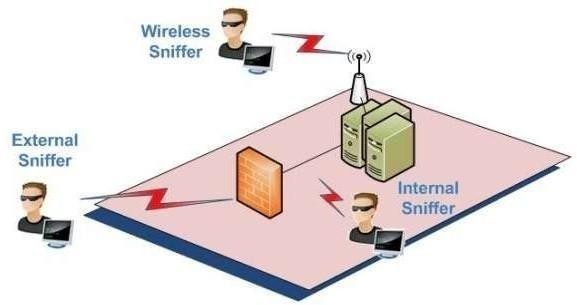


ComputerscommunicatebybroadcastingmessagesonanetworkusingIPaddresses.Onc eamessagehasbeensentonanetwork,therecipientcomputerwiththematchingIP addressrespondswithits MACaddress.

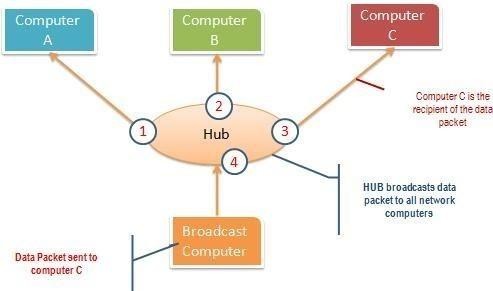
## Networksniffingistheprocessofinterceptingdatapacketssentovera network.

**PassiveandActiveSniffing**

Beforewelookatpassiveandactivesniffing,let’slookattwomajordevicesusedto networkcomputers; hubs and switches.

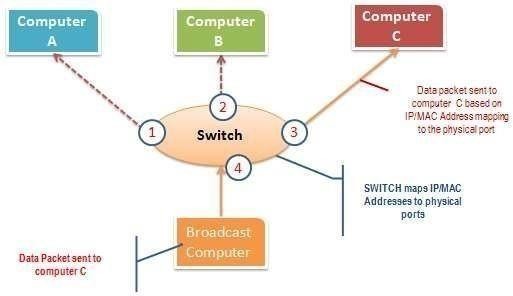


## Ahubworksbysendingbroadcastmessagestoalloutputportsonitexcepttheonethathassen tthebroadcast.



**Aswitchworksdifferently;itmapsIP/MACaddressestophysicalportson it**.

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



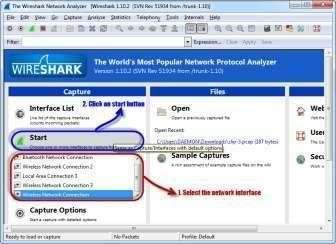
**Passive sniffing is intercepting packages transmitted over a network that uses a hub**. It iscalledpassivesniffingbecauseitisdifficulttodetect.Itisalsoeasy toperformas thehubsendsbroadcastmessagestoallthecomputers onthenetwork.

**Activesniffingisinterceptingpackagestransmittedoveranetworkthatusesaswitch**. Therearetwomainmethods used tosniff switchlinkednetworks,ARP Poisoning,andMACflooding.

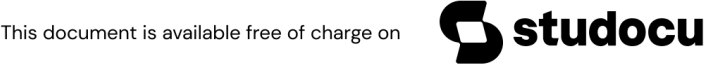
## SniffingthenetworkusingWireshark

DownloadWiresharkfromthislink<http://www.wireshark.org/download.html>

* OpenWireshark
* Youwillgetthefollowingscreen

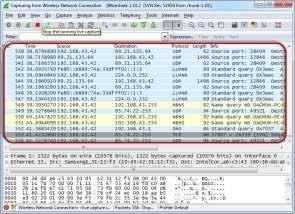


Selectthenetworkinterfaceyouwanttosniff.Noteforthisdemonstration,weareusingawirelessne tworkconnection.Ifyouareonalocalareanetwork,thenyoushouldselectthelocalareanetworkint erface.

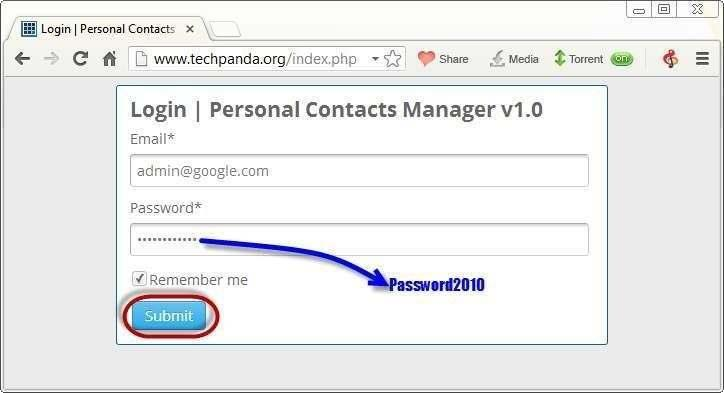


DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

* Clickonstartbuttonas shownabove



* Openyourwebbrowserandtypein<http://www.techpanda.org/>

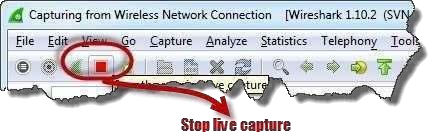


* Theloginemail[is**admin@google.com**andthepassword](mailto:isadmin@google.comandthepassword)is**Password2010**
* Clickonsubmitbutton
* Asuccessfullogonshouldgiveyouthefollowingdashboard

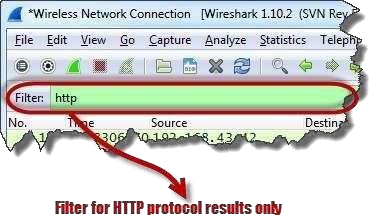


* GobacktoWiresharkandstopthelivecapture

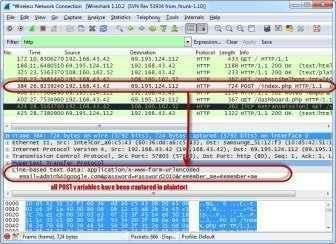
DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



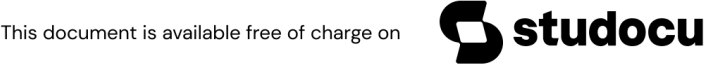
* FilterforHTTPprotocolresultsonlyusingthefiltertextbox



* LocatetheInfocolumnandlookforentrieswiththeHTTPverbPOSTandclickonit



* Justbelowthelogentries,thereisapanelwithasummaryofcaptureddata.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:

Thus the experiment toSniff Traffic using ARP Poisoning was performed.

|  |  |
| --- | --- |
| **EX.No:8** | **DEMONSTRATEINTRUSIONDETECTIONSYSTEM**  **USINGANYTOOL** |
|  |

# AIM:

TodemonstrateIntrusionDetectionSystem(IDS)usingSnortsoftwaretool.

# STEPSONCONFIGURINGANDINTRUSIONDETECTION:

1. DownloadSnortfromtheSnort.orgwebsite.(<http://www.snort.org/snort-downloads)>
2. DownloadRules(https://[www.snort.org/snort-rules).Youmustregistertogettherules.](http://www.snort.org/snort-rules).Youmustregistertogettherules) (Youshoulddownloadtheseoften)
3. Doubleclickonthe.exeto installsnort.Thiswillinstallsnortinthe“C:\Snort”folder.ItisimportanttohaveWinPcap(https://[www.winpcap.org/install/)installed](http://www.winpcap.org/install/)installed)
4. ExtracttheRulesfile.YouwillneedWinRARforthe.gzfile.
5. Copyallfilesfromthe“rules”folderoftheextractedfolder.Nowpastetherulesinto

*“C:\Snort\rules”*folder.

1. 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.
2. Openacommandprompt(cmd.exe)andnavigatetofolder“C:\Snort\bin”folder.
3. Tostart(execute)snortinsniffermodeusefollowingcommand:

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

snort-dev-i3

-iindicatestheinterfacenumber.Youmustpickthecorrectinterfacenumber. Inmycase,itis3.

-devisusedtorunsnorttocapturepacketsonyournetwork.

## Tochecktheinterfacelist,usefollowingcommand:

snort-W



## Findinganinterface

YoucantellwhichinterfacetousebylookingattheIndexnumberandfinding Microsoft.As you canseein theabove example,theotherinterfacesareforVMWare.

TorunsnortinIDSmode,youwillneedtoconfigurethefile“snort.conf”accordingto your networkenvironment.

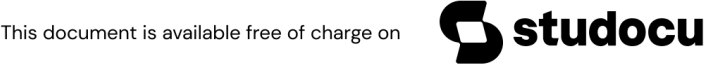
Tospecifythenetworkaddressthatyouwanttoprotectinsnort.conffile,lookforthe following line.varHOME\_NET192.168.1.0/24(You willnormallysee anyhere)

YoumayalsowanttosettheaddressesofDNS\_SERVERS,ifyouhavesomeonyournetwork.

## examplesnort

ChangetheRULE\_PATHvariabletothe path ofrules folder.varRULE\_PATHc:\

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



snort\rules

## pathtorules

Changethepathofalllibraryfileswiththe nameandpathonyoursystem.andyoumustchangethepathofsnort\_dynamicpreprocessorvariabl e.

C:\Snort\lib\snort\_dynamiccpreprocessor

Youneedtodothistoalllibraryfilesinthe“C:\Snort\lib”folder.Theoldpathmight 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“includeclassification.config”and“includereference.config”files.includec:\ snort\etc\classification.config

includec:\snort\etc\reference.config

Removethecomment(#)onthelinetoallowICMPrules,ifitiscommentedwitha#.include

$RULE\_PATH/icmp.rules

Youcanalsoremovethecommentof ICMP-inforulescomment,ifit iscommented.include

$RULE\_PATH/icmp-info.rules

Toaddlogfilestostorealertsgeneratedbysnort,searchforthe“outputlog”testin 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.

TostartsnortinIDSmode,runthefollowingcommand:

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

snort-cc:\snort\etc\snort.conf-lc:\snort\log-i3(Note:3isusedformyinterfacecard)Ifalogiscreated,selecttheappropriateprogramto openit.YoucanuseWordPardorNotePad+

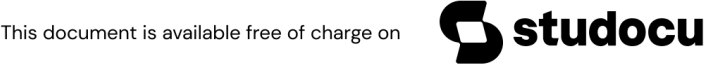
+toreadthefile.

Togenerate Log filesin ASCIImode, you can usefollowing command while runningsnort 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.

Snortmonitoringtraffic–





# RESULT:

ThustheIntrusionDetectionSystem(IDS)hasbeendemonstratedbyusingthe Open SourceSnortIntrusion DetectionTool.

|  |  |
| --- | --- |
| **EX.No:9** | **EXPLORENETWORKMONITORINGTOOLS** |
|  |

# AIM:

## ToexploreaboutNetworkmonitoringtools

Networkmonitoringisanessentialpartofnetworkmanagement.Itinvolvesusingvarious

tools tomonitorasystemnetworkanddetermineslownessandweakconnections,amongotherissues.K nowingmoreaboutthesetoolscanhelpyouunderstandthembetterandusetherightones that suityour requirements.

# PROCEDURE:

## WhatAreNetworkMonitoringTools?

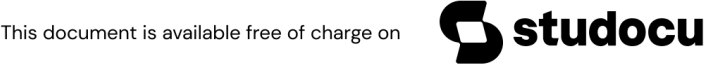
Networkmonitoringtoolsaresoftwarethatyoucanusetoevaluatenetwork connections.Thesesoftwareprogramscanhelpyoumonitoranetworkconnectionandidentifynetworkissues,whichmayincludefailingnetworkcomponents,slowconnectionspeed,n etworkoutageorunidentifiableconnections.Networkmanagementandmonitoringtools canalsohelyouresolvetheseissuesorestablishsolutionsthatpreventspecificissuesfromoccurrin ginthefuture.

## NetworkMonitoringTools

Hereareeightmonitoringtoolsalongwiththeirdescriptionsandfeatures:

## SolarWindsNetworkPerformanceMonitor

SolarWindsNetworkPerformanceMonitorisamulti- vendormonitoringtool.Itallowsuserstomonitor multiple vendors' networks at the same time. Italsoprovidesnetworkinsightsfothoroughvisibilityintothehealthofthenetworks.Somepromin entfeaturesincludenetworkavailabilitymonitoring,intelligentnetworkmapping,criticalpathvis ualisation,performanceanalysisandadvancedalerting.SolarWindsalsoallowsuserstotrackVP Ntunnelstatus.ItpromptswhenaVPNtunnelisavailabletohelpusersensureastable connection between sites. SolarWinds provides aseven-dayfree trial,afterwhich userscanchoose a preferredsubscriptionplan.



## DatadogNetworkMonitoring

DatadogNetworkMonitoringoffersservicesforon- premisesdevicesandcloudnetworks.Ahighlightingfeatureofthistoolisthevisualisations.It offers various graphical representationsof allthe network connections on a system. It alsoallows users to track key metrics like network latency,connection churn and transmissioncontrolprotocol(TCP)retransmits.Userscanmonitorthehealthofanetworkconnectionat different endpoints at the application, IP address, port or process ID layers.Otherprominentfeaturesincludeautomatedlogcollectionanduserinterfacemonitoring.

## 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.

## 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 2000networkperformancemonitorsthatallowuserstotrackandmonitortheirconnectionsandperformdetaileda nalysesoniss ues.Italsoprovides over 200 dashboard widgets that can help users customise theirdashboardtotheirownsuitability.OtherfeaturesincludeCPU,memoryanddisk utilisationmonitoringonlocalandvirtualmachines.Italsoallowssettingnetwork performance threshold and notifies the user in case of aviolation.

## Domotz

Domotzisanexpansivetoolthatprovidesalistoffeaturesformonitoringnetwork

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

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.

## 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 usersto manageagents and automate agentupdating. Thisreduces manual effort to monitor network connections. The tool also includes over 2000 plug-ins forenhancing network monitoring.

## ProgressWhatsupGold

ProgressWhatsupGoldisabasicnetworkmonitoring software.Itprovidesaminimaluserinterfacewithessentialfeatureslikedevice monitoring,applicationmonitoring,analysingnetworktraffic andmanagingconfigurations.Thetoolallowsuserstomonitorclouddevices,inspectsuspiciousco nnections,automateconfigurationbackupsand identify,and resolve bandwidthissues.

## OtherToolsForNetworkMonitoring

Herearethreeadditionaltoolsfornetworkmonitoring:

* + 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 networkstatus, along with real-time notifications through text, emailand sound.

NagiosCore:NagiosCoreisamonitoringenginethatworksastheprimaryapplicationfor allNagiosprojects,includingtheNagiosNetworkAnalyser.ItintegrateswithotherNagiosapplica tionsandprovidesuserswithfeatureslikeavisualdashboard,customapplicationmonitoring,auto matedalertsystem,advancedusermanagementandnetworksecuritymonitoring

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

* + Zabbix: Zabbix provides a thorough network monitoring solution with features like servermonitoring,cloudmonitoring,applicationmonitoringandservicemonitoring.The toolalsoincludesfeatureslikemetric 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 identifythe right tool for your use. It mayalsohelp youchoosethecorrectsubscription planonpaidtools.

## Browsemultipletools

Onceyouidentifythe requirements,considerbrowsingmultipletools.Visitthewebsitesof 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 topurchase a subscriptionplan 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** | **STUDYTOCONFIGUREFIREWALL,VPN** |
|  |

# AIM:

TostudythefeaturesoffirewallinprovidingnetworksecurityandtosetFirewallSecurityin windows.

# PROCEDURE:

## FirewallinWindows7

Windows7comeswithtwofirewallsthatworktogether.Oneisthe**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 rulesinWFAScanbeconfiguredbasedonprotocols,ports,addressesandauthentication.By default,bothfirewallscomewithpredefinedsetofrulesthatallowustoutilizenetwork resources.Thisincludesthingslikebrowsingtheweb,receivinge-mails,etc.Other standardfirewall exceptions are File andPrinterSharing,NetworkDiscovery, PerformanceLogsandAlerts,RemoteAdministration,WindowsRemoteManagement,Remote Assistance,RemoteDesktop,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.

Whenwefirstconnecttosomenetwork,wearepromptedtoselectanetworklocation. 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.

Therearetwodifferent networkprofilesavailable:

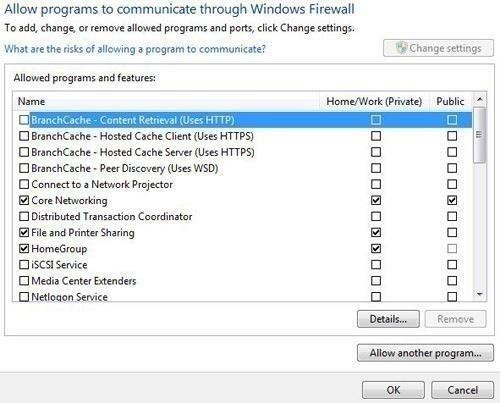
* Public
* Home/Work-privatenetwork

## 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.

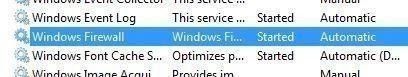


## FirewallCustomization

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

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

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



## FirewallService

Inourcasetheserviceisrunning.Ifwestopit,wewillgetawarningthatweshouldturnon ourWindowsFirewall.

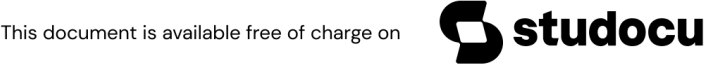


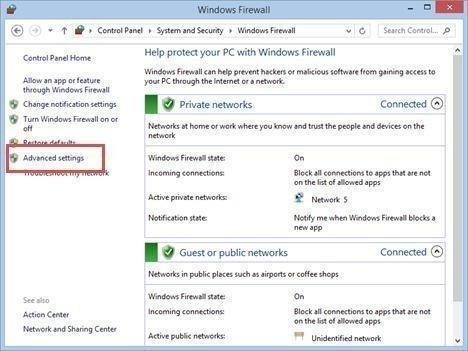
## HowtoStart&UsetheWindowsFirewallwithAdvancedSecurity

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*WindowsFirewallwithAdvancedSecurity*: OneistoopenthestandardWindowsFirewallwindow,bygoingto*"ControlPanel-*

*>SystemandSecurity->WindowsFirewall"*.Then,clickortap*Advancedsettings*.





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



## WhatAreTheInbound&OutboundRules?

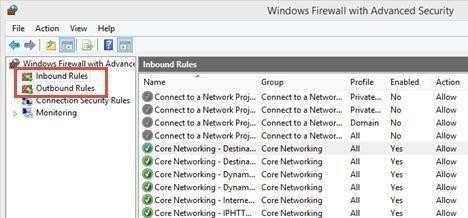
In order to provide the security you need, the *Windows Firewall* has a standard set ofinbound and outbound rules, which are enabled depending on the location of the networkyouareconnectedto.

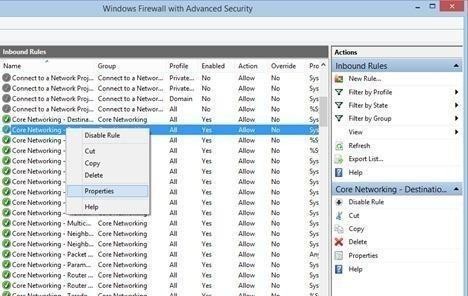
Inbound rules are applied to the traffic that is coming from the network and the Internet toyour computer or device. Outbound rules apply to the traffic from your computer to thenetworkortheInternet.

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

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.



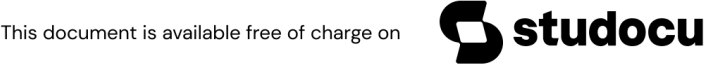


## WhataretheConnectionSecurityRules?

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

Ifyouwanttoseeifthereareanysuchrulesonyourcomputer,clickortap*"ConnectionSecurity*

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)



*Rules"*on the panel on the left.By default,there are no suchrulesdefinedonWindowscomputersanddevices.Theyaregenerallyusedinbusinessenviro nmentsand 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 linproviding network security and to set Firewall Security in windows.

DownloadedbyVaidegiM[(vaidegi.kjanagi@gmail.com)](mailto:(vaidegi.kjanagi@gmail.com)

