lOMoARcPSD|31761673

## LIST OF EXPERIMENTS

|  |  |  |  |
| --- | --- | --- | --- |
| **Ex.**  **No.** | **Date** | **Name of the Experiment** | **Sign** |
| **1** |  | Implement Symmetric Key Algorithms |  |
| **2(a)** |  | Implementingasymmetrickeyalgorithms |  |
| **2(b)** |  | ImplementingKeyexchangealgorithms |  |
| **3.** |  | Calculate themessagedigestofatextusing theSHA-1 algorithm. |  |
| **4.** |  | Implement theSIGNATURESCHEME-DigitalSignatureStandard. |  |
| **5.** |  | Installation ofWireshark,tcpdumpandobservedatatransferredinclient-servercommunication using UDP/TCP and identify theUDP/TCPdatagram. |  |
| **6.** |  | CheckmessageintegrityandconfidentialityusingSSL |  |
| **7** |  | ExperimentEavesdropping,Dictionaryattacks,MITMattacks |  |
| **8** |  | Experiment withSniffTrafficusingARPPoisoning |  |
| **9** |  | Demonstrateintrusiondetection systemusinganytool. |  |
| **10** |  | Explorenetworkmonitoringtools |  |
| **11** |  | Studyto configureFirewall, VPN |  |

**EX.NO.:1**

**DATE**

**IMPLEMENT SYMMETRIC KEY ALGORITHMS**

**Aim:**

To implement symmetric key algorithms for secure data encryption and decryption.

**ALGORITHM:**

**Encryption Steps:**

1. Initialize the round keys using the main symmetric key.

2. Break the plaintext into blocks, padding the last block if necessary.

3. For each block: a. Perform the initial round key addition. b. Perform multiple rounds (10, 12,

or 14 rounds based on key length):

* Byte substitution using a substitution box (S-box).
* Row shifting within the block.
* Column mixing within the block.
* Round key addition using the current round key. c. Perform the final round without the

column mixing step.

4. Combine the encrypted blocks to create the ciphertext.

**Decryption Steps:**

1. Initialize the round keys using the main symmetric key.

2. Break the ciphertext into blocks.

3. For each block: a. Perform the initial round key addition. b. Perform the reverse of the

encryption rounds in the reverse order:

* Inverse byte substitution using an inverse S-box.
* Inverse row shifting within the block.
* Inverse round key addition using the current round key.
* Inverse column mixing within the block (if not in the final round). c. Perform the final round

without the inverse column mixing step.

4. Combine the decrypted blocks to recover the original plaintext.

5. Remove any padding added during encryption to obtain the actual original plaintext.

**Program:**

import javax.crypto.Cipher;

import javax.crypto.KeyGenerator;

import javax.crypto.SecretKey;

import java.util.Base64;

public class SymmetricEncryptionExample {

public static void main(String[] args) throws Exception {

String plaintext = "Hello, symmetric encryption!";

System.out.println("Original Text: " + plaintext);

// Generate a secret key

KeyGeneratorkeyGen = KeyGenerator.getInstance("AES");

keyGen.init(128); // You can choose 128, 192, or 256 bits

SecretKeysecretKey = keyGen.generateKey();

// Encryption

Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");

cipher.init(Cipher.ENCRYPT\_MODE, secretKey);

byte[] encryptedBytes = cipher.doFinal(plaintext.getBytes("UTF-8"));

System.out.println("Encrypted Text: " +

Base64.getEncoder().encodeToString(encryptedBytes));

// Decryption

cipher.init(Cipher.DECRYPT\_MODE, secretKey);

byte[] decryptedBytes = cipher.doFinal(encryptedBytes);

String decryptedText = new String(decryptedBytes, "UTF-8");

System.out.println("Decrypted Text: " + decryptedText);

}

}

**Output:**

Original Text: Hello, symmetric encryption!

Encrypted Text: XnO8JLmjRhKwx/mLPJ8zXyz6kfONJ6LYH8C75KxVvwk=

Decrypted Text: Hello, symmetric encryption!

## Ex.No:2(a)

## Date:

**RSAAlgorithm**

## AIM:

ToimplementRSA(Rivest–Shamir–Adleman) algorithmbyusingHTMLandJavascript.

## ALGORITHM:

1. Choosetwoprime numberpand q
2. Compute thevalue ofnand**p**
3. Findthevalue of***e*** (public key)
4. Computethevalue of***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>

<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;

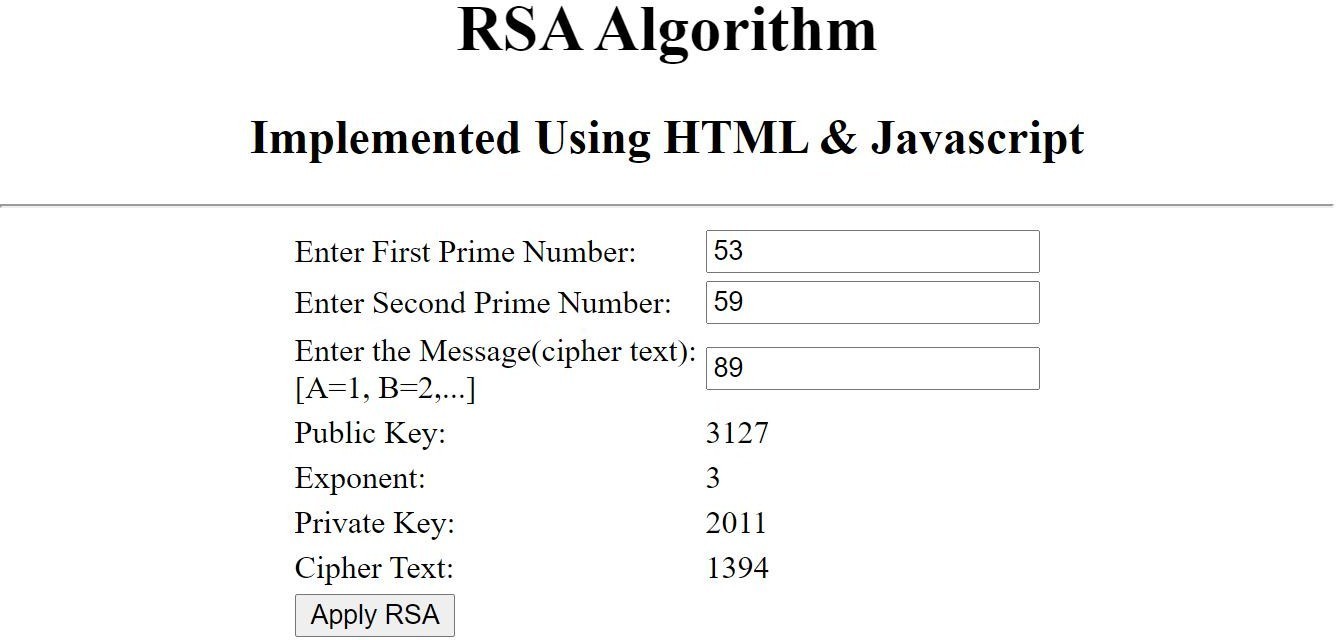
document.getElementById('publickey').innerHTML = n;document.getElementById('exponent').innerHTML = e;document.getElementById('privatekey').innerHTML=d;document.getElementById('ciphertext').innerHTML=ct;

}

</script>

</html>

## OUTPUT:



**RESULT:**

ThustheRSAalgorithmhasbeenimplementedusingHTML&CSSandtheoutputhasbeenverifiedsuccessfully.

## Ex.No: 2(b)

## Date: Diffie-Hellmankeyexchangealgorithm

**AIM:**

Toimplement theDiffie-Hellman KeyExchangealgorithmforagivenproblem.

## ALGORITHM:

* + 1. AliceandBobpublicly agree touseamodulus*p*=23andbase*g*=5(whichis aprimitiverootmodulo 23).
    2. Alicechoosesa secretinteger ***a***=4,thensendsBob *A* =*g****a***mod*p*

o *A*=5**4**mod 23=4

* + 1. Bobchoosesa secretinteger***b***=3,thensends Alice *B*=*g****b***mod*p*

o *B*=5**3**mod 23=10

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

o ***s***=10**4**mod 23=18

* + 1. Bob computes ***s***=*A****b***mod*p*

o ***s***=4**3**mod 23=18

* + 1. 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:"+aliceCo

mputes);System.out.prin[tln("SharedSecret :"+sharedSecret);](https://www.studocu.com/in?utm_campaign=shared-document&utm_source=studocu-document&utm_medium=social_sharing&utm_content=ccs354-network-ecurity)

/\*sharedsecretsshould matchandequality istransitive\*/

if((aliceComputes==sharedSecret)&&(aliceComputes==bobComputes))System.out.println("Success:SharedSecretsMatches!"+sharedSecret);

else

System.out.println("Error:SharedSecretsdoesnotMatch");

}

}

## OUTPUT:

simulationofDiffie-Hellman keyexchangealgorithm

AliceSends:4.0BobComputes:18.0BobSends:10.0

AliceComputes:18.0SharedSecret :18.0

Success:SharedSecretsMatches!18.0

## RESULT:

Thusthe*Diffie-Hellmankeyexchangealgorithm* hasbeenimplementedusingJavaProgramandtheoutputhas beenverifiedsuccessfully.

## Ex.No:3

**Date:**

## SHA-1Algorithm

**AIM:**

ToCalculatethemessagedigestofatextusing theSHA-1algorithm.

## ALGORITHM:

1. AppendPaddingBits
2. AppendLength-64bitsare appended totheend
3. PrepareProcessingFunctions
4. PrepareProcessingConstants
5. InitializeBuffers
6. ProcessingMessagein512-bitblocks (Lblocksin totalmessage)

## PROGRAM:

### sha1.java

importjava.security.\*;

publicclasssha1 {

publicstaticvoidmain(String[]a){try{

MessageDigest md = MessageDigest.getInstance("SHA1");System.out.println("Messagedigestobjectinfo:\n ");

System.out.println("Algorithm="+md.getAlgorithm());System.out.println("Provider=" + md.getProvider());System.out.println("ToString="+md.toString());

Stringinput= "";md.update(input.getBytes());byte[] output = md.digest();System.out.println();

System.out.println("SHA1(\""+input+"\")="+bytesToHex(output));input= "abc";

md.update(input.getBytes());output = md.digest();System.out.println();

System.out.println("SHA1(\""+input+"\")="+bytesToHex(output));input= "abc[defghijklmnopqrstuvwxyz";](https://www.studocu.com/in?utm_campaign=shared-document&utm_source=studocu-document&utm_medium=social_sharing&utm_content=ccs354-network-ecurity)

md.update(input.getBytes());

output=md.digest();System.out.println();

System.out.println("SHA1(\""+input+"\")="+bytesToHex(output));System.out.println();

}catch(Exceptione){System.out.println("Exception:"+e);

}

}

privatestaticStringbytesToHex(byte[]b){

charhexDigit[] ={'0','1','2','3','4','5','6','7','8','9', 'A','B','C','D','E','F'};

StringBufferbuf=newStringBuffer();

for(byteaB:b){

buf.append(hexDigit[(aB>> 4) & 0x0f]);buf.append(hexDigit[aB&0x0f]);

}

returnbuf.toString();

}

}

## OUTPUT:

Messagedigestobjectinfo:

Algorithm=SHA1Provider=SUNversion12

ToString=SHA1 Message Digest from SUN, <initialized>SHA1("")=DA39A3EE5E6B4B0D3255BFEF95601890AFD80709SHA1("abc")=A9993E364706816ABA3E25717850C26C9CD0D89D

SHA1("abcdefghijklmnopqrstuvwxyz")=32D10C7B8CF96570CA04CE37F2A19D84240D3A89

## RESULT:

Thusthe*SecureHashAlgorithm(SHA-1)*hasbeenimplementedandtheoutputhas beenverifiedsuccessfully.

## Ex.No:4

**Date:**

## DigitalSignatureStandard

**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");keyPairGen.initialize(2048);

KeyPairpair=keyPairGen.generateKeyPair();PrivateKeyprivKey=pair.getPrivate();

Signaturesign=Signature.getInstance("SHA256withDSA");sign.initSign(privKey);

byte[]bytes="msg".getBytes();sign.update(bytes);

byte[]signature=sign.sign();

System.out.println("Digital signatureforgiventext:"+newString(signature, "UTF8"));

}

## OUTPUT:

EntersometextHihoware you

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

## RESULT:

ThustheDigitalSignatureStandardSignatureSchemehasbeenimplemented andtheoutputhasbeen verifiedsuccessfully.

## InstallationofWireshark,tcpdumpandobservedatatransferredinclient-servercomm

**Ex.No:5**

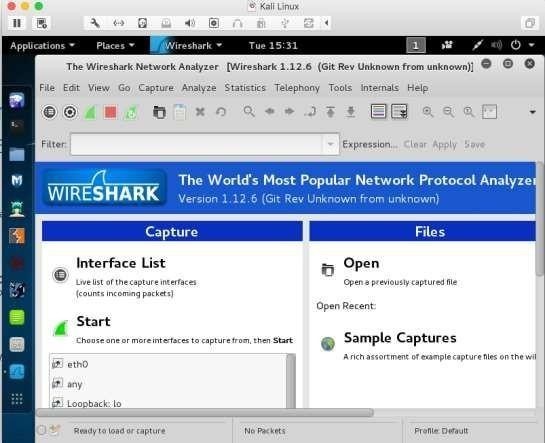
## Date:

**Aim:**

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

## Introduction:

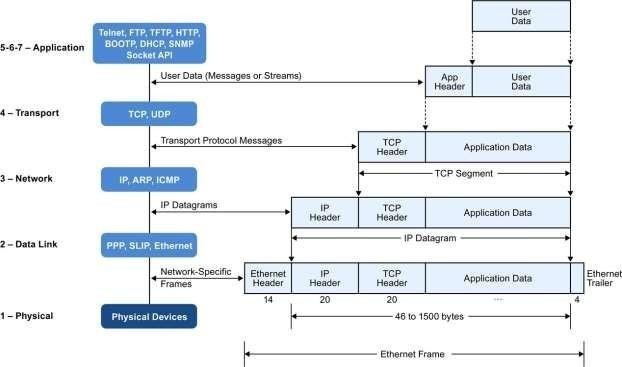
The first part of the lab introduces packet sniffer, Wireshark. Wiresharkis a freeopen-source network protocol analyzer. It is used for network troubleshooting and communicationprotocol analysis. Wireshark captures network packets in real time and display them inhuman-readableformat.Itprovidesmanyadvancedfeaturesincludinglivecaptureandoffline 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

In the CSC 4190 Introduction to Computer Networking (one of the perquisite courses), TCP/IPnetwork stack is introduced and studied. This background section briefly explains the concept ofTCP/IPnetworkstacktohelpyoubetterunderstandtheexperiments.TCP/IPisthemostcommonly used network model for Internet services. Because its most important protocols, theTransmission Control Protocol (TCP) and the Internet Protocol (IP) were the first networkingprotocols defined in this standard, it is named as TCP/IP. However, it contains multiple layersincluding applicationlayer, transportlayer,networklayer,and data link layer.

* *Application Layer*: The application layer includes the protocols used by most applicationsforprovidinguserservices.ExamplesofapplicationlayerprotocolsareHypertext

Transfer Protocol (HTTP), Secure Shell (SSH), File Transfer Protocol (FTP), and SimpleMailTransferProtocol(SMTP).

* *Transport Layer*: The transport layer establishes process-to-process connectivity, and itprovides end-to-end services that are independent of underlying user data. To implementthe process-to-process communication, the protocol introduces a concept of port. Theexamples of transport layer protocols are Transport Control Protocol (TCP) and UserDatagram Protocol (UDP). The TCP provides flow- control, connection establishment,andreliabletransmissionofdata,whiletheUDPisaconnectionlesstransmissionmodel.
* *Internet Layer*: The Internet layer is responsible for sending packets to across networks. Ithas two functions: 1) Host identification by using IP addressing system (IPv4 and IPv6);and2)packetsroutingfromsourcetodestination.TheexamplesofInternetlayerprotocolsareInternetProtocol(IP),InternetControl MessageProtocol (ICMP),andAddressResolutionProtocol(ARP).
* *Link Layer*: The link layer defines the networking methods within the scope of the localnetwork link. It is used to move the packets between two hosts on the same link. Ancommon exampleof linklayerprotocolsisEthernet.

## PacketSniffer

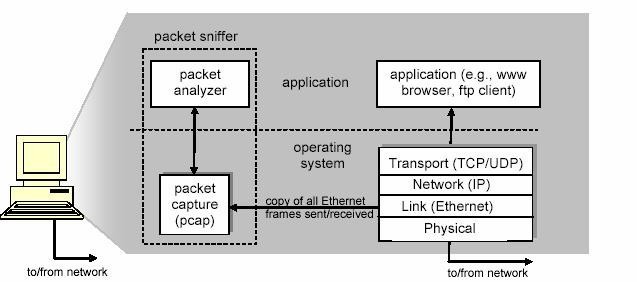
Packet sniffer is a basic tool for observing network packet exchangesin a computer.As thename suggests, a packet sniffer captures (“sniffs”) packets being sent/received from/by yourcomputer; it will also typically store and/or display the contents of the various protocol fields inthese captured packets.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

**Figure** 3 shows the structure of a packetsniffer. At the right of **Figure** 3 are the protocols(inthis case, Internet protocols) and applications (such as a web browser or ftp client) that normallyrun on your computer. The packet sniffer, shown within the dashed rectangle in **Figure** 3 is anaddition to the usual software in your computer, and consists of two parts. The packet capturelibrary receives a copy of every link-layer frame that is sent from or received by your computer.Messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP allare eventually encapsulated in link-layer framesthat are transmitted over physical media such asan Ethernet cable. In Figure 1, the assumed physical media is an Ethernet, and so all upper-layerprotocolsareeventually encapsulatedwithin anEthernet frame.Capturingalllink-layerframes

thusgivesyouaccesstoallmessagessent/received from/byallprotocols andapplications

executingin your computer.

The second component of a packet sniffer is the packet analyzer, which displays the contents ofall fieldswithina protocol message.Inorderto doso,thepacketanalyzer



PacketSnifferStructure

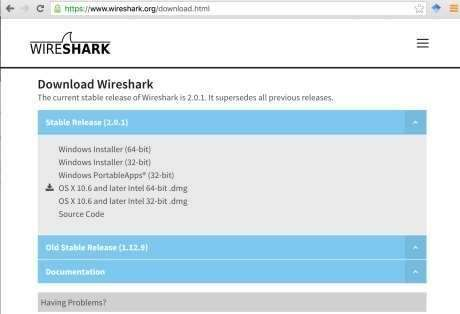
must “understand” the structure of all messages exchanged by protocols. For example, supposewe are interested in displaying the various fields in messages exchanged by the HTTP protocol in**Figure** 3. The packet analyzer understands the format of Ethernet frames, and so can identify theIP datagram within an Ethernet frame. It also understands the IP datagram format, so that it canextracttheTCPsegmentwithintheIPdatagram.Finally,itunderstands theTCPsegmentstructure,soitcanextracttheHTTPmessagecontainedintheTCPsegment.Finally,itunderstands the HTTP protocol and so, for example, knows that the first bytes of an HTTPmessage willcontainthestring“GET,”“POST,”or“HEAD”.

WewillbeusingtheWiresharkpacketsniffer[[ht](http://www.wireshark.org/)t[p://www.wireshark.org/](http://www.wireshark.org/)]fortheselabs,allowingustodisplaythecontentsofmessagesbeingsent/receivedfrom/byprotocolsatdifferent levels of the protocol stack. (Technically speaking, Wireshark is a packet analyzer thatuses a packet capture library in your computer). Wireshark is a free network protocol analyzerthat runs on Windows, Linux/Unix, and Maccomputers.

GettingWireshark

TheKaiLinuxhasWiresharkinstalled.YoucanjustlaunchtheKaliLinuxVMandopenWiresharkthere.Wiresharkcanalsobedownloadedfromhere:

https://www.wire[shark.org/download.html](https://www.studocu.com/in?utm_campaign=shared-document&utm_source=studocu-document&utm_medium=social_sharing&utm_content=ccs354-network-ecurity)

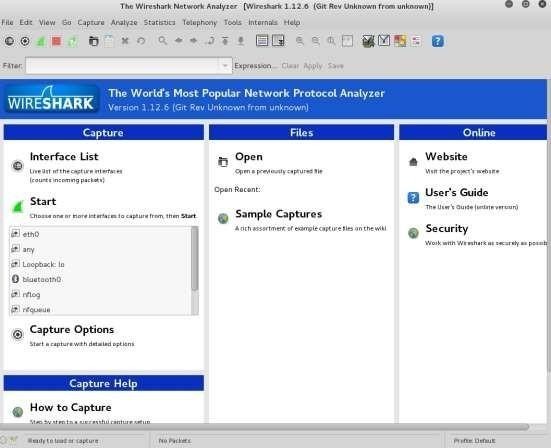


(DownloadPageofWireshark)

## StartingWireshark:

WhenyouruntheWiresharkprogram,theWiresharkgraphicuserinterfacewillbeshownas

**Figure**5.Currently,theprogramisnotcapturingthepackets.



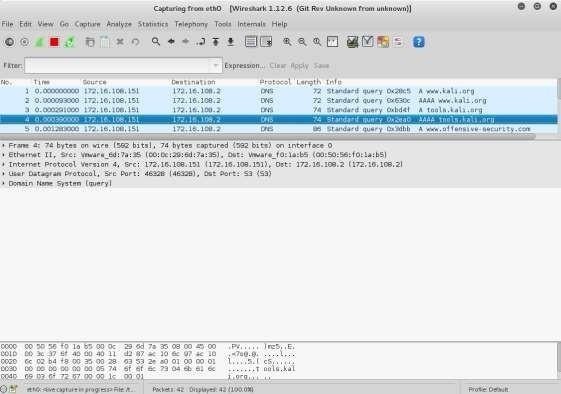
## InitialGraphicUserInterfaceofWireshark

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. The attached **Figure**6was takenfrom mycomputer.

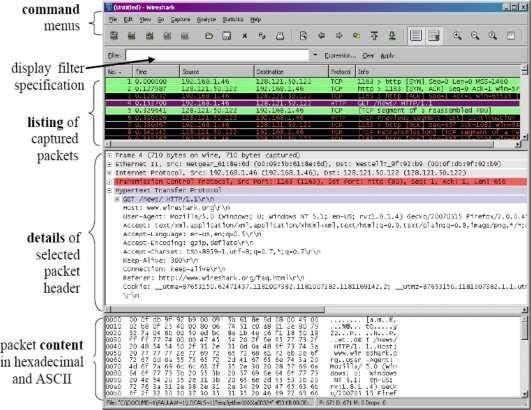
Afteryouselecttheinterface,youcanclickstartto capturethepackets asshownin**Figure**7.



CaptureInterfacesinWireshark



CapturingPacketsinWireshark



## (WiresharkGraphicalUserInterfaceonMicrosoftWindows)

TheWiresharkinterfacehasfivemajorcomponents:

The **command menus** are standard pulldown menus located at the top of the window. Of interestto us now is the File and Capture menus. The File menu allows you to save captured packet dataor open a file containing previously captured packet data, and exit the Wiresharkapplication.TheCapturemenu allowsyoutobeginpacketcapture.

The **packet-listing window** displays a one-line summary for each packet captured, including thepacket number (assigned by Wireshark; this is not a packet number contained in any protocol’sheader), the time at which the packet was captured, the packet’s source and destination addresses,the protocol type, and protocol-specific informationcontained inthe packet. The packet listingcan be sorted according to any of these categories by clicking on a column name. The protocoltype field lists the highest- level protocol that sent or received this packet, i.e., the protocol that isthesourceor ultimatesink forthis packet.

The **packet-header details window** provides details about the packet selected (highlighted) inthe packet-listing window. (To select a packet in the packet-listing window, place the cursor overthe packet’s one- line summary in the packet-listing window and click with the left mousebutton.).These detailsincludeinformationabouttheEthernetframeand IP datagram that

contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded orminimized by clicking on the right- pointing or down- pointing arrowhead to the left of theEthernet frame or IP datagram line in the packet details window. If the packet has been carriedover TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expandedor minimized. Finally,details about the highest-level protocol that sent or received this packetarealsoprovided.

The **packet-contents window** displays the entire contents of the captured frame, in both ASCIIand hexadecimalformat.

Towards the top of the Wireshark graphical user interface, is the **packet display filter field**, intowhich a protocol name or other information can be entered in order to filter the informationdisplayedinthepacket-listingwindow(andhencethepacket-headerandpacket-contentswindows). In the examplebelow, we’ll use the packet-display filter field to have Wireshark hide(notdisplay)packetsexceptthosethatcorrespond toHTTPmessages.

## 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.

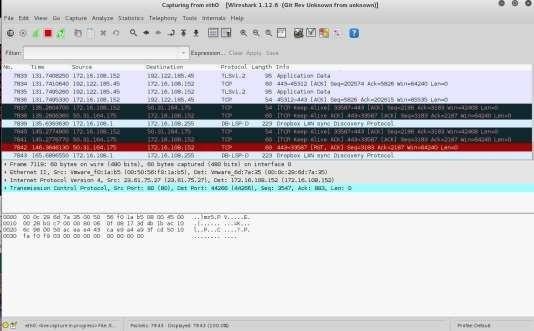
TestRun

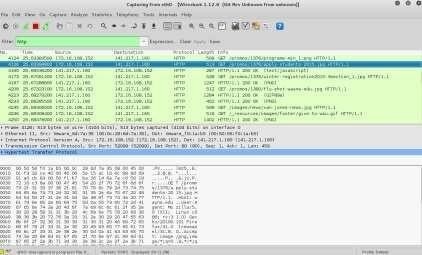
Dothefollowingsteps:

* 1. StartuptheWiresharkprogram(selectaninterfaceandpressstarttocapturepackets).
  2. Startupyourfavoritebrowser (ceweaselinKaliLinux).
  3. Inyourbrowser,goto WayneStatehomepagebytyping [www.wayne.edu.](http://www.wayne.edu/)
  4. Afteryourbrowserhasdisplayedthe[http://www.wayne.edu](http://www.wayne.edu/)page,stopWiresharkpacket

capture by selecting stop in the Wireshark capture window. This will cause the WiresharkcapturewindowtodisappearandthemainWiresharkwindowtodisplayall

packetscapturedsinceyoubeganpacketcaptureseeimagebelow:





* 1. ColorCoding:You’llprobablyseepacketshighlightedingreen,blue,andblack.

Wireshark uses colors to help you identify the types of traffic at a glance. By default,green is TCP traffic,dark blue is DNStraffic, light blue is UDP traffic,and blackidentifies TCP packets with problems — for example, they could have been deliveredout-of-order.

* 1. Younowhavelivepacketdatathatcontainsallprotocolmessagesexchangedbetween

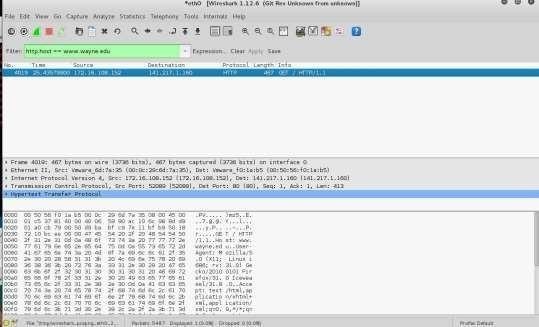
yourcomputerandothernetworkentities!However,asyouwillnoticetheHTTPmessages are not clearly shown because there are many other packets included in thepacket capture. Even though the only action you took was to open your browser, there aremanyother programsinyourcomputerthat communicateviathe networkinthe

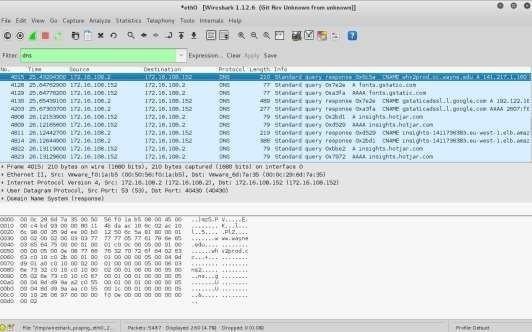
background. To filter the connections to the ones we want to focus on, we have to use thefilteringfunctionality ofWiresharkbytyping“http”inthefilteringfieldasshownbelow:

Notice that we now view only the packets that are of protocol HTTP. However, we also still donot have the exact communication we want to focus on because using HTTP as a filter is notdescriptive enough to allow us to find our connection to [http://www.wayne.edu.](http://www.wayne.edu/) We need to bemorepreciseifwewanttocapturethe correctsetof packets.

* 1. TofurtherfilterpacketsinWireshark,weneedtouseamoreprecisefilter.Bysettingthe

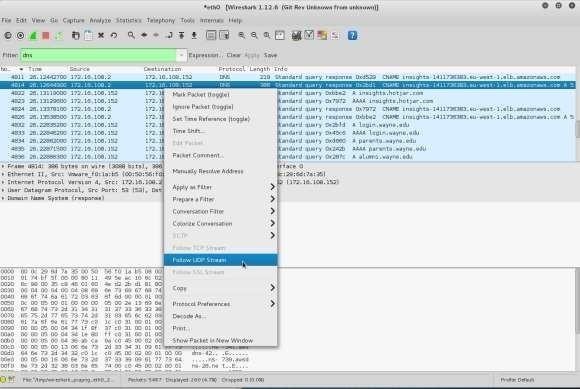
http.host[www.wayne.edu,](http://www.wayne.edu/) we are restricting the view to packets that have as an http host the[www.wayne.edu](http://www.wayne.edu/) website. Notice that we need two equal signs to perform the match not justone.Seethescreenshotbelow:



* 1. Now,wecantryanotherprotocol.Let’s useDomainNameSystem(DNS)protocolasanexample here.
  2. ofthe

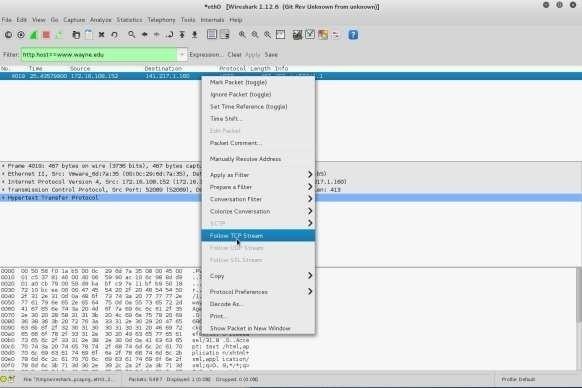
Let’strynowtofindoutwhatarethosepacketscontainbyfollowing

conversations (also called network flows), select one of the packets and press the rightmouse button (if you are on a Mac use the command button and click), you should seesomethingsimilartothescreenbelow:



Click on**FollowUDPStream,**andthenyouwillseefollowingscreen.





* 1. If we close this window and change the filter back to “http.hos ww.wayne.edu” and then follow apacketfromthelistofpackets thatmatchthatfilter,weshouldgetthesomethingsimilar tothefollowingscreens.Notethatweclickon**FollowTCPStream**this time.



## Result:

InstallationofWireshark,tcpdumpandobservedatatransferredinclient-servercommunication usingUDP/TCPandidentifytheUDP/TCPdatagram.

## Ex.No:6

**Date:**

**Aim**

# CheckmessageintegrityandconfidentialityusingSSL

## SSLSessioninDetails

**Handshaking-CiphersuitNegotiation**

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\_Helllo to state the ciphersuit of choice (server decides ontheciphersuit).Themessagealsocontainsa32-byterandomnumberdenotedasserver\_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.)

Theservercanoptionallyrequestfortheclient'scertificatetoauthenticatetheclient.Inpractice,serverusuallydoesnot authenticatetheclient.Thisis because:

* Serverauthenticatesclient bycheckingthecreditcardinane-commercetransaction.
* Mostclients donothaveadigitalcertificate.
* Authentication viadigitalcertificate takestimeandtheservermayloseanimpatient client.

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 compressesthemessageusingtheagreed-uponcompressionmethod(e.g.,PKZip,gzip).
2. ThesenderhashesthecompresseddataandthesecretHMACkeytomakeanHMAC,toassure messageintegrity.
3. ThesenderencryptsthecompresseddataandHMACusingencryption/decryptionsecretkey, to assuremessageconfidentiality.

Retrievemessages:

1. Thereceiverdecryptstheciphertextusingtheencryption/decryptionsecretkeytoretrievethecompressed dataandHMAC.
2. The receiver hashes the compressed data to independently produce the HMAC. It thenverifies the generated HMAC with the HMAC contained in the message to assure messageintegrity.
3. The receiver un-compresses the data using the agreed-upon compression method to recovertheplaintext.

Thefollowing diagramshowsthesequenceoftheSSLmessagesforatypical client/serversession.

## 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-doneCONNECTED(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 \*

readfrom 00988EB0[00990ABD](42bytes =>42(0x2A))

0000- 0200 0026 03 0140 44-3527 ccef 2b 51e1b0...&..@D5'..+Q..

0010- 44 1fef c483 72df 37-4f 9b 2bdd 11 50 1387 D....r.7O.+..P..

0020- 91 0aa2d2 28b9 00 00-16 ....(....

002a-<SPACES/NULS>

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5))0000 - 16 03 01 02 05 .....

read from00988EB0[00990ABD](517bytes=>517(0x205))0000- 0b 00 02 01 00 01 fe00-01 fb30 82 01 f730 82..........0 0.

0010- 01 60 02 01 01 30 0d 06-092a86 48 86 f7 0d 01.`...0...\*.H....

0020- 01 04 05 00 304d 31 0b-30 09 06 0355 04 06 13....0M1.0...U...

0030 - 02 55 53 31 10 30 0e06-0355 04 0b 13 07 74 65 .US1.0...U...te

0040- 73 74 31 30 3131 0c30-0a06 03 5504 03 13 03 st1011.0...U....

0050- 63 68 63 31 1e30 1c06-092a86 48 86 f7 0d 01 chc1.0...\*.H....

0060 - 09 01 16 0f 63 68 63 40-7465 73 74 31 30 31 2e chc@test101.

0070- 63 6f 6d 30 1e17 0d 30-34 3032 32 36 30 36 35com0 040226065

0080 - 36 35 34 5a17 0d 30 35-3032 32 35 30 36 35 36654Z0502250656

0090- 35 34 5a30 3b31 0b 30-0906 03 5504 06 13 02 54Z0;1.0...U....

00a0- 55 53 31 0c30 0a 06 03-5504 03 13 03 6368 63US1.0...U chc

00b0- 31 1e30 1c0609 2a86-4886 f7 0d01 09 01 16 1.0...\*.H.......

00c0- 0f63 68 6340 74 6573-74 31 3031 2e 63 6f 6d[.chc@test101.com](mailto:.chc@test101.com)

00d0- 30 81 9f 30 0d06 09 2a-8648 86 f70d 01 01 010..0...\*.H......

00e0- 05 00 03 81 8d00 30 81-8902 81 8100 cd e49e......0.........

00f0-7cb6d2 344ed353 46-25c75388 2560 e646|..4N.SF%.S.%`.F

0100- db64 3a7361 92 ac 23-92cd2c94 a9 8f c6 7f.d:sa..#..,.....

0110- 4773 c0d98d 34b7 2c-ddc986bd82 6f ceacGs...4.,.....o..0120- d8 e2ba 0f e5f5 3a 67-2c89 1a1b03 eb21 85......:g,. !.

0130- 28 e3 2998 84 ed4675-82 fa0f30 a3 a9a571(.)...Fu...0..q

0140- 464cd60d 17c419 fd-44fbe2 18 46a69dabFL......D...F...

0150- 91 de6b a17ffe30 06-28 5d d8 d329 00 c3 1d..k...0.(]..)...

0160- 4c13 00 61 8ff3 85 51-f568 d8 6925 02 03 01 L..a...Q.h.i%...

0170- 00 01 30 0d 06 09 2a86-4886 f7 0d 01 01 04 05..0...\*.H.......

0180- 00 0381 81 00 29fdbf-5aed708f 53 a4e9 14 .....)..Z.p.S...

0190- 4c5eba84c654 1bf2-c03cc4300f7f 12 80L^...T...<.0....

01a0- 4e01b7fd 39 50 f1 41-0dd8 aa77 d9 8725 1a N...9P.A...w..%.

01b0- 1ee297 88 4f53 75 c8-7022 6a0161 0f 51 3e OSu.p"j.a.Q>

01c0- 13 19 9c 64 f2 76 14 e8-8525 23 a211c48cf8 ...d.v...%#.....

01d0- 23 2cd1 c3d3 713ae6-7154 1007 dc72 ffee#,...q:.qT...r..

01e0-e83ecf 8e 77 73e9 9f-f59a9060 4da0aa03.>..ws.....`M...

01f0- 32 1f 11 6f 2e9a5f 3c-770522 0c81bf 29 962..o..\_ 5 (0x5))

0000 - 16 03 01 01 8d .....

read from 00988EB0 [00990ABD] (397 bytes => 397 (0x18D))0000- 0c00 01 89 0080 e696-9d 3d 49 5be32c7cf1 =I[.,|.

0010- 80 c3bdd4 79 8e91b7-8182 51bb 05 5e 2a20....y.....Q..^\*

0020- 6490 4a79 a770 fa 15-a2 59cbd523 a6a6efd.Jy.p...Y..#...

0030- 09c4 3048d5 a22f 97-1f 3c 20 129b 48 000e..0H../..<..H..

0040 - 6edd 06 1cbc05 3e37-1d 79 4e53 27 df61 1en >7.yNS'.a.

0050 - bb be 1b ac 9b 5c 60 44-cf 02 3d 76 e0 5e ea 9b .....\`D..=v.^..0060- ad 991b 13 a63c97 4e-9e f183 9eb5 db 1251.....<.N Q

0070- 36 f726 2e56 a88715-38 dfd823 c6 505085 6.&.V...8..#.PP.

0080- e2 1f0d d5 c8 6b00 01-02 00 8011 3f5f fae4.....k......?\_..

0090- 79 9a0bd9 e067 37 c4-2a 88 22b0 95 b7a7bey....g7.\*.".....

00a0- 9379 9d 51ae31 4799-df47 dd80 5e3d 2a4a.y.Q.1G..G..^=\*J

00b0- 298b fdc163 5e 48 e8-e3fd ac 95 1b 3a 5f 75)...c^H .:\_u

00c0- 98 2d3c9cba 68 18 7b-be38 2c693d 41b7 c3.-<..h.{.8,i=A..

00d0- 08 a1dab0 a8 a4 fe9a-d61e56ff4c8c 6e6b V.L.nk

00e0- 18f1ec9d22a99027-c1c62c0ebd 0e13d4 ...."..'..,.....

00f0- fdb2 c9 8f 6fbb8e06-e0b5 1f f7 87 035f a8 ....o \_.

0100- 12 4fbb cebaf176 fb-8008 3700 80 30 99ad.O....v...7..0..

0110- 9bfc3a14 6b a82cc5-fe 7b bd 1c 92 ec 19 a6..:.k.,..{......

0120- 75 2d 69 4ef49f 74 60-5dd4 3e06 97 38bcb5u-iN..t`].>..8..

0130- 0e3c1ff2 99e655 4a-36 42 a8f2b732 2a1e.<....UJ6B..2\*.

0140- a387b3 f379 4328 d1-7a0d db7c11 26 f368....yC(.z..|.&.h

0150-b173b6 784b f322 20-e4f727 08ab74 9292.s.xK."..'..t..

0160- 79 2661 40 1ee9 90 11-e8b1cf99 d9 9fc768y&a@ h

0170- 48 e8f2a5d5 d70ee1-88 9abd 0f 40 85 af2dH @..-

0180- da76 3a10 6eb9 38 4d-379c41 c89f .v:.n.8M7.A..

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5))0000 - 16 03 01 00 04 .....

readfrom00988EB0[00990ABD](4bytes =>4(0x4))0000 - 0e .

0004-<SPACES/NULS>

writeto00988EB0[00999BE0](139bytes=>139(0x8B))

0000- 16 03 01 00 86 10 00 00-8200 80 63 c23c69 26...........c...dU.....]n..

0030- 05 f1 db44 f313 a824-3a76 0e3e 1a6e55 0c...D..$:v.>.nU.

0040- 31 9b 04 99 30 ff8f d2-8d 8e0db1 67 ac43 ee1...0 g.C.

0050-b2 3fd3 c7c53381 e1-3fd2 47 6f5d 8afb4c .?...3..?.Go]..L

0060- 62 c723b3 f7ad 3ca9-0c87 4a08 07 55ba 06b.#...<...J..U..

0070- 3418 0c5fd9 35f0 2b-90 9a9d 6b 8762 410f4..\_.5.+..k.bA.

0080-b3 47 745f 5b b8 595a-b221 dd .Gt\_[.YZ.!.

writeto00988EB0[00999BE0](6bytes =>6(0x6))0000 - 14 03 01 00 01 01 ......

writeto 00988EB0[00999BE0](45bytes=> 45(0x2D))

0000- 16 03 01 00 28 0f 31 83-e0f8 91 fa33 98 68 46....(.1 3.hF

0010- c060 83 66 28 fed3 a5-00f098 d5 df 22 72 2d.`.f( "r-

0020- e4 409b 96 3b 4c f9 02-13 a7e77774 .@..;L wt

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5))0000 - 14 03 01 00 01 .....

readfrom00988EB0[00990ABD](1bytes =>1(0x1))0000 - 01 .

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5))0000 - 16 03 01 00 28 (

readfrom 00988EB0[00990ABD](40bytes =>40(0x28))

0000- d40b a6b7 e8 91 091e-e41e fc445f 80 cca1...........D\_...

0010- 5d 51 55 3e62 e80f 78-07 f62f cdf9bc498d ]QU>b..x../..I.

0020- 56 5b e8b209 2c18 52- V[.,.R

---

Certificatechain

0[s:/C=US/CN=chc/emailAddress=chc@test101.com](mailto:/C%3DUS/CN%3Dchc/emailAddress%3Dchc@test101.com)

[i:/C=US/OU=test101/CN=chc/emailAddress=chc@test101.com](mailto:/C%3DUS/OU%3Dtest101/CN%3Dchc/emailAddress%3Dchc@test101.com)

---

Servercertificate

-----BEGINCERTIFICATE-----

MIIB9zCCAWACAQEwDQYJKoZIhvcNAQEEBQAwTTELMAkGA1UEBhMCVVMxEDAOB

gNVBAsTB3Rlc3QxMDExDDAKBgNVBAMTA2NoYzEeMBwGCSqGSIb3DQEJARYPY2hjQHRlc3QxMDEuY29tMB4XDTA0MDIyNjA2NTY1NFoXDTA1MDIyNTA2NTY1NFowOzELMAkGA1UEBhMCVVMxDDAKBgNVBAMTA2NoYzEeMBwGCSqGSIb3DQEJARYPY2hjQHRlc3Q

xMDEuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDN5J58ttI0TtNTRiXH

U4glYOZG22Q6c2GSrCOSzSyUqY/Gf0dzwNmNNLcs3cmGvYJvzqzY4roP5fU6ZyyJGhsD6yGFKOMpmITtRnWC+g8wo6mlcUZM1g0XxBn9RPviGEamnauR3muhf/4wBihd2NMpAMMdTBMAYY/zhVH1aNhpJQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBACn9v1rt

cI9TpOkUTF66hMZUG/LAPMQwD38SgE4Bt/05UPFBDdiqd9mHJRoe4peIT1N1yHAiagFhD1E+ExmcZPJ2FOiFJSOiEcSM+CMs0cPTcTrmcVQQB9xy/+7oPs+Od3Ppn/WakGBNoKoDMh8Rby6aXzx3BSIMgb8plq3LOxiu

-----ENDCERTIFICATE-----

[subject=/C=US/CN=chc/emailAddress=chc@test101.com](mailto:subject%3D/C%3DUS/CN%3Dchc/emailAddress%3Dchc@test101.com)[issuer=/C=US/OU=test101/CN=chc/emailAddress=chc@test101.com](mailto:issuer%3D/C%3DUS/OU%3Dtest101/CN%3Dchc/emailAddress%3Dchc@test101.com)

---

Noclient certificateCAnamessent

---

SSLhandshakehasread1031bytesandwritten292bytes

---

New,TLSv1/SSLv3,CipherisEDH-RSA-DES-CBC3-SHA

Serverpublickeyis1024bitSSL-Session:

Protocol:TLSv1

Cipher :EDH-RSA-DES-CBC3-SHA

Session-ID:

Session-ID-ctx:

Master-Key:57FDDAF85C7D287F9F9A070E8784A29C75E788DA2757699B20F3CA50E7EE01A66182A71753B78DA218916136D50861AE

Key-Arg: None

Start Time: 1078211879Timeout:7200 (sec)Verifyreturncode:0(ok)

---

## GET/test.htmlHTTP/1.0

writeto00988EB0[009952C8](82bytes=>82 (0x52))

0000- 17 03 0100 18 74 fa45-352db1 24 59 cfad 96.....t.E5-.$Y...

0010- 34 30 01 7dbe8e70 f9-41 62 11 f136 17 03 0140.}..p.Ab..6...

0020- 0030 56 61ba2d d358-5de6 6a 83 7807 87 7a.0Va.-.X].j.x..z

0030-db b2a7 40c76d c14a-203b827d aa15 e865...@.m.J;.}...e

0040- 3b92bd c820 e9 9d 41-f1 7751 d9ae31 c4 2c;.....A.wQ..1.,

0050 - 32 5a 2Z

writeto 00988EB0[009952C8](58bytes=>58 (0x3A))

0000- 17 03 01 00 1839 2f df-4375 91 1334 1b 12 04 .....9/.Cu..4...

0010- 7def8de18654 4f 67-c81d cd07a417 0301 }....TOg........

0020- 00 1853 d9 229d eb 6e-8b79 f8 e4 82 2fbaea..S."..n.y.../..

0030- 03 a5 3f 12 85 2e9f 64-ffdc ..?....d..

read from 00988EB0 [00990AB8] (5 bytes => 5 (0x5))0000 - 17 03 01 01 48 H

readfrom 00988EB0[00990ABD](328bytes =>328(0x148))

0000 - bdeb 8b 9c 01 ac 73 30-8f ca a4 8b 2a 6f bd 02 ......s0....\*o..0010-d7fc71186147f21d-708b 107d9828a4 50..q.aG..p..}.(.P

0020-f3 0f42 e8c5e1 3e53-34bd c7 62 341b 5e 8c..B...>S4..b4.^.

0030- 99 2d 89 c6b3f019 96-22 97 43b8 8f9d 76 42.-......".C..vB

0040- 95a5 7cdb3b 22dd57-29 8de8d4 283e89 d8..|.;".W)...(>..

0050- 46e5 dc355156 f844-d1 82 44a065b0 93 22F..5QV.D..D.e.."

0060- 4b0aeb07 26 c92ae2-454cde 07 0cbb3ec6K...&.\*.EL >.

0070-bc37 94 cdec94 2f35-76 37 13 4d0f 88 9cb1.7..../5v7.M....

0080- d71c58 8a 35 5b 32bc-122b9ce65bd4 86 bd..X.5[2..+..[...

0090- 39 fc99 18 79ecf7 53-db59 74 49da07 69549...y..S.YtI..iT

00a0- f466 aa3634 39 f9 0b-8750 9e76 db 9fd0 44.f.649...P.v..D

00b0 - 0c 0d e7 65 80 9b b8 51-56 3d d0 db aa 55 ff ca...e...QV=...U..00c0- 74 38 24c18cd7 32cf-ab03b3 5929 0f 80 18t8$...2....Y)...

00d0- 6ad4 e07efd418cf7-1d 81 12 a700b371 39j..~.A q9

00e0- 78 1e3c17 42d4 99 22-697b 2d 09efd8 6ef4x.<.B.."i{ n.

00f0- 64 f661 34 728c89 f5-a8ea1cb10d 08 ff17 d.a4r...........

0100- 51 3e46 2b 38 7561 6a-1e34f4 14 14 380d 5eQ>F+8uaj.4 8.^

0110- 6ebadbef8388 eea5-2c18 5a0c27 e3d9 19n.......,.Z.'...

0120- 6ca312 c0a13d e114-96 d3 1a f9 c9f2aad6l....=..........

0130- 12 d5 36 ae 36 f2 18 f5-df c6 ef34 d7 7d 2b70..6.6 4.}+p

0140 - 99 88 47 93 91 09 56b1- ..G V.

HTTP/1.1**200OK**

Date:Tue,02Mar200407:18:08GMT

Server:Apache/1.3.29(Win32)mod\_ssl/2.8.16OpenSSL/0.9.7cLast-Modified: Sat, 07Feb2004 10:53:25GMT

ETag:"0-23-4024c3a5"

Accept-Ranges: bytesContent-Length: 35Connection: closeContent-Type:text/html

<h1>Homepageonmainserver</h1>

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

0000 - 15 03 01 00 18 .....

readfrom 00988EB0[00990ABD](24bytes =>24(0x18))

0000- a54751bd aa0f9be4-acd428 f2d0 a0c8 fa.GQ.......(.....

0010- 2cd4e5e4bec501 85- ,.......

closed

writeto 00988EB0[009952C8](29bytes=>29 (0x1D))

0000- 15 03 0100 18 d4 19b9-59 88 88 c0 c9 38 ab5c........Y 8.\

0010 - 98 8c 43 fd b8 9e14 3d-77 5e 4c 68 03 ..C =w^Lh.

## TraceAnalysis

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

EachSSLrecordbeginswith a5-byteheader:

* Byte0:RecordContentType.FourContentTypes aredefined,asfollows:

## Content Type HexCode Description

Handshake 0x16 The record carries a handshaking messageApplication\_Data 0x17 EncryptedApplicationDataChange\_Cipher\_Spec0x14 Toindicateachangeinencryptionmethods.Alert 0x15 Tosignalvarioustypes of errors

* Byte 1&2: SSL version(0x0301forTLSv1,0x0300 forSSLv3).
* Byte3&4:Therecord length,excluding the5-byte header.

Letusbeginlookinginto thehandshakemessagecontainedwithinaSSLrecord (ofContentType

0x16).Thehandshakemessagehasa4-byteheader:

* Byte0:HandshakeType,asfollows:

|  |  |
| --- | --- |
| **HandshakeType** | **HexCode** |
| hello\_request | 0x00 |
| client\_hello | 0x01 |
| server\_hello | 0x02 |
| certificate | 0x0b |
| server\_key\_exchange | 0x0c |
| certificate\_request | 0x0d |
| server\_hello\_done | 0x0e |
| certificate\_verify | 0x0f |
| client\_key\_exchange | 0x10 |
| finished | 0x14 |

* Byte1 -3:Themessagelength,excludingthe3-byteheader.

Hence,aclient\_hellorecord willbeginwitha5-byterecordheader,followedbya4-bytehandshakemessageheader.Forexample,

**Client\_Hello**

The first handshake message is always sent by the client, called client\_hellomessage. 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.

YoumustrefertoRFC2246forthestructureoftheClient\_Hellomessage.

|  |  |  |  |
| --- | --- | --- | --- |
| **Bytes** | **Len** | **Value** | **Description** |
| 00 | 1 | 16 | RecordContentType-HandshakeMessage |
| 01-02 | 2 | 03 01 | SSLversion-TLSv1 |
| 03-04 | 2 | 00 61 | RecordLength |
| 05 | 1 | 01 | HandshakeType-Client\_Hello |
| 06-08 | 3 | 00 00 5d | MessageLength(0x61-4=0x5d) |
| 09-0A | 2 | 03 01 | Clientpreferredversion(client\_version)-TLSv1 |

0B-0E4 4044 3527GMT Time

0C-2A28 5c... 72 28randombytes

Client\_Random

|  |  |  |  |
| --- | --- | --- | --- |
| 2B | 1 | 00 | SessionIDLength0 (forresumingthesession) |
| 2C-2D | 2 | 00 36 | CiphersuitLength -27choices (2-byteeach) |
| 2E-63 | 54 | .... | The27Ciphersuits (SeeTable) |
| 64 | 1 | 01 | CompressionMethod Length -1 |
| 65 | 1 | 00 | CompressionMethod:NULL. |

CiphersuitCodeusedinClient\_HelloandServer\_Hellomessagesistabulated asfollows:

## CipherSuite Aut

**h**

## Key Exchange Encryption Has

**h**

## Code

RSA\_WITH\_NULL\_MD5 RSARSA NULL MD

5 0001

RSA\_WITH\_NULL\_SHA RSARSA NULL SHA0002RSA\_EXPORT\_WITH\_RC4\_40\_MD5 RSARSA\_EXPORTRC4\_40 MD

5

RSA\_WITH\_RC4\_128\_MD5 RSARSA RC4\_128 MD

5

0003

0004

RSA\_WITH\_RC4\_128\_SHA RSARSA RC4\_128 SHA0005RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 RSARSA\_EXPORTRC2\_40\_CBC MD

5 0006

|  |  |  |  |
| --- | --- | --- | --- |
| RSA\_WITH\_IDEA\_CBC\_SHA | RSARSA | IDEA\_CBC | SHA0007 |
| RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | RSARSA\_EXPORT | DES40\_CBC | SHA0008 |
| RSA\_WITH\_DES\_CBC\_SHA | RSARSA | DES\_CBC | SHA0009 |

RSA\_WITH\_3DES\_EDE\_CBC\_SHA RSARSA 3DES\_EDE\_CB

000

DH\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SH

DH\_DSS\_EXP

C SHAA

DES\_40\_CBC SHA000

A RSAT B

DH\_DSS\_WITH\_DES\_CBC\_SHA DSSDH DES\_CBC SHA000

C

DH\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA DSSDH 3DES\_EDE\_CB

000

C SHAD

DH\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHRSADH\_EXPORTDES\_40\_CBC SHA000

A E

DH\_RSA\_WITH\_DES\_CBC\_SHA RSADH DES\_CBC SHA000FDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA DSSDH 3DES\_EDE\_CB

C SHA0010

DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_S

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HA | DSS | DH\_EXPORTRC4\_40 | | SHA0011 |
| DHE\_DSS\_WITH\_DES\_CBC\_SHA | DSS | DHE | RC4\_128 | SHA0012 |
| DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | DSS | DHE | DES\_40\_CBC | SHA0013 |

DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

RSADHE\_EXPOR

DES\_CBC SHA0014

DHE\_RSA\_WITH\_DES\_CBC\_SHA RSADH DES\_CBC SHA0015DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA RSADHE 3DES\_EDE\_CB

T

C SHA0016

DH\_anon\_EXPORT\_WITH\_RC4\_40\_MD5 - DH\_EXPORT RC4\_40 MD

5

DH\_anon\_WITH\_RC4\_128\_MD5 - DH RC4\_128 MD

5

0017

0018

DH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SH- DH\_EXPORT DES\_40\_CBC SHA 0019DH\_anon\_WITH\_DES\_CBC\_SHA - DH DES\_CBC SHA001

A

A

DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA - DH 3DES\_EDE\_CB

001

C SHAB

**Server\_Hello**

In response to the client\_hellomessage, the server returns a server\_hellomessage to tell theclientits choiceofprotocolversion,ciphersuitandcompressionmethod.Theserveralsoincludes a32-byterandomnumber(server\_random) inthemessage.

|  |  |  |  |
| --- | --- | --- | --- |
| **Bytes** | **Len** | **Value** | **Description** |
| 00 | 1 | 16 | RecordContentType-HandshakeMessage |
| 01-02 | 2 | 03 01 | SSLversion-TLSv1 |
| 03-04 | 2 | 00 2a | RecordLength |
| 05 | 1 | 02 | HandshakeType-Server\_Hello |
| 06-08 | 3 | 00 00 26 | MessageLength |
| 09-0A | 2 | 03 01 | ProtocolVersionChosen -TLSv1 |

0B-0E4 40 44 35 27 GMT Time (sec since 1970)0C-2A28 cc ...b9 28 randombytes

Server\_Random

2B 1 00 SessionIDLength0(forresumingthesession)

Ciphersuit Chosen:DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

2C-2D2 0016

2E 1 00 CompressionMethodChosen: NULL.

## 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.

## BytesLenValue Description

|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 1 | 16 | RecordContent Type-HandshakeMessage |
| 01-02 | 2 | 03 01 | SSLversion-TLSv1 |
| 03-04 | 2 | 02 05 | RecordLength |
| 05 | 1 | 0b | HandshakeType-certificate |
| 06-08 | 3 | 00 02 01 | MessageLength |
| 09-0B | 3 | 00 01 fe | CertificateLength |

Certificates(tobetraced)

TheX.509certificatestructurecanbefoundfromtheITUrecommendationX.509"Thedirectory-AuthenticationFramework".

**Server\_Key\_ExchangeServer\_Hello\_Done**

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

|  |  |  |
| --- | --- | --- |
| **BytesLen** | **Value** | **Description** |
| 00 1 | 16 | RecordContentType-HandshakeMessage |
| 01-02 2 | 03 01 | SSLversion-TLSv1 |
| 03-04 2 | 00 04 | RecordLength |
| 05 1 | 0e | HandshakeType-Server\_Hello\_Done  (checkthelast3bytes) |

**Client\_Key\_Exchange**

The client\_key\_exchangemessage contains the pre\_master\_secretwhen RSA key exchangeis used. The pre\_master\_secretis 48-byte, consists of protocol version (2 bytes) and 46 randombytes.

|  |  |  |
| --- | --- | --- |
| **BytesLen** | **Value** | **Description** |
| 00 1 | 16 | RecordContentType-HandshakeMessage |
| 01-02 2 | 03 01 | SSLversion-TLSv1 |
| 03-04 2 | 00 86 | RecordLength |
| 05 1 | 10 | HandshakeType-Client\_Key\_Exchange |
| 06-08 3 | 00 00 82 | MessageLength |

pre\_master\_secret (130 bytes): encrypted using server's public keyextractedfromtheserver'scertificate

**Change\_Cipher\_Spec**

|  |  |  |
| --- | --- | --- |
| **BytesLen** | **Value** | **Description** |
| 00 1 | 14 | RecordContentType-Change\_Cipher\_Spec |
| 01-02 2 | 03 01 | SSLversion-TLSv1 |
| 03-04 2 | 00 01 | RecordLength |
| 05 1 | 01 | ?? |

**Certificate\_Verify**

**Change\_Cipher\_Spec**

UnknownHandshakingMessage(D4) -tocheck

**Application\_Data**

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

Server-to-Client -theHTTPresponsemessage

**Alert**

**ComparisonofTLSv1,SSL v3andSSLv2**

The TLS v1 specification stated, "TLS v1 and SSL v3 are very similar". Some of minor differencesinclude minor changes in HMAC calculation, ciphersuit support, and pseudo-random numbergeneration. TLSv1 canberegarded asSSLv3.1.

SSL v2 has a big security hole in the negotiation of the ciphersuit (and should not be used). Theattackercanconvincetheclientandservertouseaweakerencryptionthanwhattheyarecapableof.Thisis called"ciphersuitrollback"attack.

## Result:

ThustheconfidentialityandIntegrityusing SSLwasverified.

## Ex.No:7

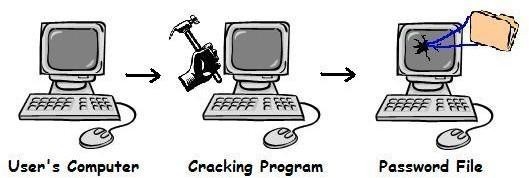
**Date:**

# ExperimentEavesdropping,Dictionaryattacks,MITMattacks

## Aim:

Toexperimenteavesdropping,Dictionaryattacks,MIMTattacks

## VisualObjective:



**Introduction**

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 breakingDictionaryattack

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.

Passwords that are composed of random letters numbers and characters are most vulnerableto thistypeof attack.

## 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 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.

## CrackingProcess

Since a brute force attack is the most time consuming and is not likely to break any passwordsthatarenotcomposedofrandomcharacters,thebestplanistousetechniquesthatarecomputationally efficient compared to untargeted and unspecific techniques. By applying whatis known about how users select passwords, an intruder can tremendously increase the odds intheir favor of finding passwords. With the right techniques, some poorpasswordscanbecracked in underasecond.

The real power of dictionary attacks come from understanding the ways in which most peoplevary names and dictionary words when attempting to create a password. By applying all thecommon transformations to every word in the electronic list and encrypting each result thenumber tested passwords multiplies rapidly. Cracking tools can often detect “clever” ways ofmanipulating words to hide their origin. For example, such cracking programs often subject eachword to a list of rules. A *rule* could be anything, any manner in which a word might appear.Typical rulesmight include

Alternateupper-andlowercaselettering.

Spellthewordforwardandthenbackward,andthenfusethetworesults(forexample:cannac).

Addthe number1to thebeginningand/orendofeachword.

Naturally,themorerulesoneappliestothewords,thelongerthecrackingprocesstakes.However,morerulesalso guaranteeahigherlikelihoodof success.

## 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.

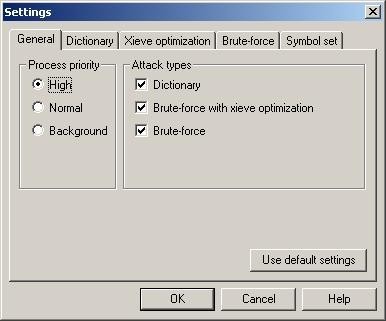
**Step2:**Openthe OfficeKey–PasswordRecoverytool

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

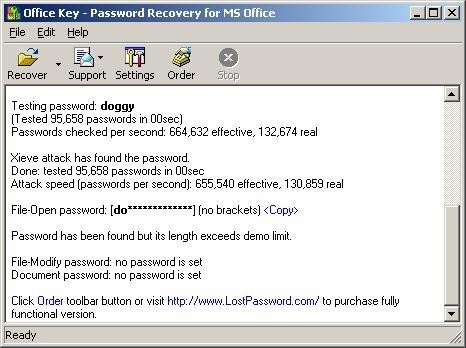


**Step4:**Choosethepassword protectedMS OfficeFileyouhavesavedto theDesktop.

**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.

## Task2–Password Auditing(Windowsplatform):

The purpose of this task is to familiarize you with act of password cracking/recovery. Passwordcracking software uses a variety of approaches, including intelligent guessing, dictionary attacksand automationthattries every possiblecombinationof characters. Given enoughtimetheautomated method can crack any password, but more effective passwords will last months beforebreaking.

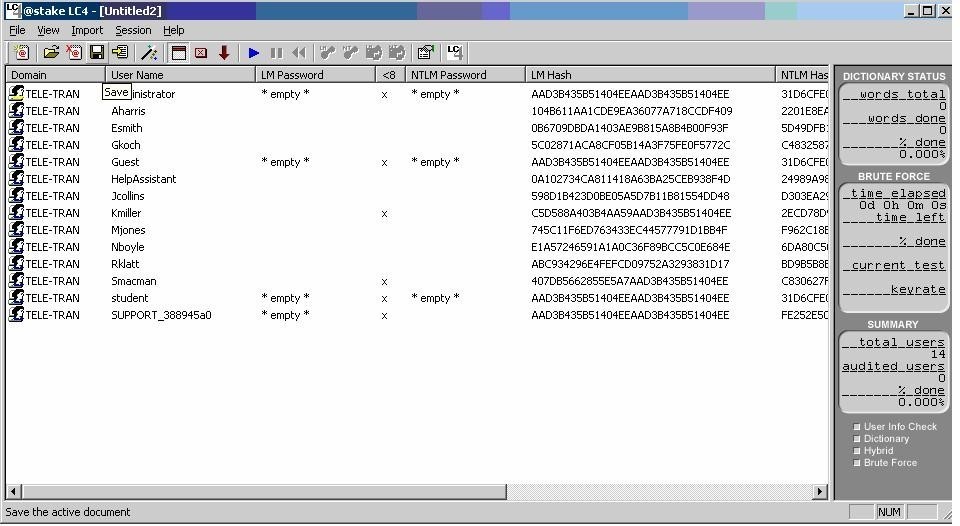
When a password is entered and saved on a computer it is encrypted, the encrypted passwordbecomes a string of characters called a “hash” and is saved to a password file.A passwordcannot be reverse-decrypted. So a cracking program encrypts words and characters given to it(wordlist or randomly generated strings of characters) and compares the results with hashedpasswords. If the hashes match then the password has successfully been guessed or “cracked”.This process is usually performed offline against a captured password file so that being lockedout of the account is not an issue, and guessing can go on continuously. Thus, revealing thepasswords is simplyamaterofCPUtimeand dictionarysize

1. Youobtaina*dictionaryfile*,whichisnomorethanaflatfile(plaintext)listofwords(commonlyreferredto as*wordlists*).
2. These words are fedthrough any number of programs thatencrypteach word.Suchencryption conforms to theDES standard.
3. Eachresultingencryptedwordiscomparedwiththetargetpassword. If amatchoccurs,there isbetter thana 90percentchance that thepasswordwascracked.

**Step1:**Goto Lab1folder, andopenLC4toaudit thepasswords onyourWindowssystem.

SelectFile NewSession

SelectImport ImportfromPWDUMPFile(in thesamefolder)Select the “Passwords”file that hasbeenprovidedtoyou.



## Objectives

This password file has been retrieved from a system that we must gain access to. To do this youmust crack as many passwords as possible as quickly as possible. We have captured the usernames and encrypted passwords for ten users. The user names follow a standard pattern of firstinitial and last name, but the passwords have no set standards. We do know that users of thissystemareencouragedtoaddnumbersandothercharacterstothewordstheychoseforpasswords.

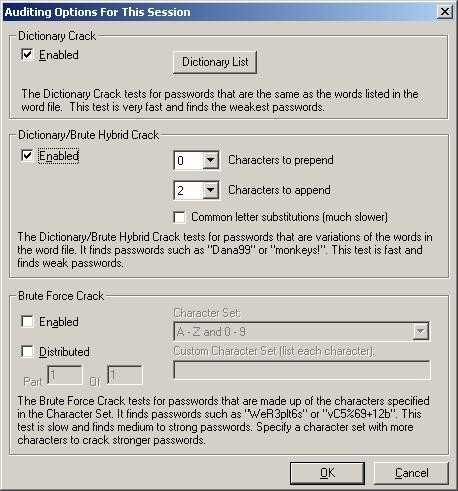
To aid you in cracking these passwordswe have managed to collect some basic informationabout the users.This personal information may help you target your searches as to what theuser’spassword maybe.

|  |  |
| --- | --- |
| **Kmiller** | KenMillerisanavidflyfisherandhisrecordnumberofcatchesis  justunder30 |
| **Smacman** | StevenMacManhasafiancéwho’snameis4letterslongandstarts  witha“K” |
| **Gkoch** | GinaKochgrewupwithherGermangrandmother,whousedtocall |

|  |  |
| --- | --- |
|  | her‘LittlePrecious’ \* |
| **Mjones** | Matt Jones was born in 1979. Hecompareshimselfto a  ShakespeareancharacterwhowasbornviaCsection |
| **Tgriffin** | TimGriffinlovesfunky‘70’sand‘80smusic. Andsongsabout  ‘Love’ |
| **Rklatt** | RyanKlattisabigStarTrekfanandhasmostlikelychosenan  obscurereferenceforhispassword \* |
| **Nboyle** | NancyBoyleisanafanofthe booksofBritish writer Douglas Adams |
| **Esmith** | EdwardSmithwasveryclosetohisgrandfatherwhodiedin1968.  Weknowhisgrandfather’snamewasalesscommonnamestartingwith‘L’ |
| **Jcollins** | JimCollinskeepsacopyofthebook“The Prince”\* |
| **Hharris** | AlanHarrishasa wifenamedSueandadaughter namedMegan  AlanwasmarriedonMay3rd.HisdaughterwasbornonAugust6th |

**Step2:**Select Session SessionOptions

Use this menu to customize your password search. Here you can add different word listfor Dictionary attacks, change Hybrid attack features. Keep in mind you are workingwith a short dead line and more in depth searches will take longer then you have. Youmust use the information given to you to target your search most specifically at morelikely passwords.



**Step 3:**Select Session Begin “Audit” or Press the blue play button on the upper toolbar to startthepassword search.

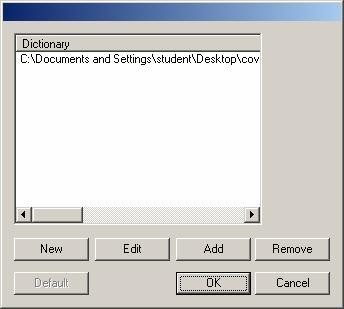
**Step 4:** After the first search has run check your progress. Have some of the passwords been crackedall the way though or have some only been partially cracked. Use what you’ve learned fromthis first search to target your next few searches. You will need to search the internet andusetheinformationyouhavebeengivenabouteachusertofindwordstheymayhaveusedastheirpassword.

**Note:** The question marksin the partially cracked passwords do not necessarily representthenumberof remainingundiscoveredcharacters.

**Step5:**AddwordstoyourwordlistSessionSessionOptions

Press the ‘Dictionary List’ button in the Dictionary crack section. Here you can edit yourcurrentwordlistandaddwordsbyselectingthe‘EDIT’buttonandenteringeachwordonanew line.Youcanalsoadd multipledictionariesand wordlist.

**Step6:** Youmaychosetoconductdictionaryattackswithotherwordlists. You canfindadditionalwordlisttousehere: ftp://ftp.cerias.purdue.edu/pub/dict



**Step7:**Continuesearchingforpossiblepasswordsduringtheremainderofthelab.Repeatingsteps3and4 eachtimeyoumodify yoursearch.

**Step8:**Onceyouhavecrackedall thepasswordsinthefile,write themdowninyourlabreportoroncethe lab timehasended, submitthepasswordsyouwereable to crack.

## Result:

Thustheexperiment forEavesdropping,Dictionaryattacks,MITMattackswasdonesuccefully.

## Ex.No:8

**Date:**

## PerformanExperimenttoSniffTrafficusing ARPPoisoning.Experiment toS

**AIM**

## PerformanExperimenttoSniffTrafficusingARPPoisoning.

Description:

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

**Operating System Security**: this measure is dependent on the operating system been used. Thefollowingarethebasictechniquesusedbyvarious operatingsystems.

* **Linuxbased**:theseworkbyignoringunsolicitedARPreplypackets.
* **MicrosoftWindows**:theARPcachebehaviorcanbeconfiguredviatheregistry.Thefollowinglistincludes someofthesoftware thatcanbeused toprotectnetworksagainst

sniffing;

* **AntiARP**–providesprotection againstbothpassiveandactivesniffing
* **AgnitumOutpostFirewall**–providesprotectionagainstpassivesniffing
* **XArp**–providesprotection againstbothpassiveandactivesniffing
* **MacOS**:ArpGuardcanbeusedtoprovideprotection.Itprotectsagainstbothactiveandpassivesniffing.
  + Computerscommunicateusingnetworks.Thesenetworkscouldbeonalocalareanetwork LAN or exposed to the internet. **Network Sniffers are programs that capturelow-level package data that is transmitted over a network.** An attacker can analyze thisinformationtodiscovervaluable information suchasuseridsandpasswords.
  + In this article, we will introduce you to common network sniffing techniques and toolsusedto sniffnetworks.

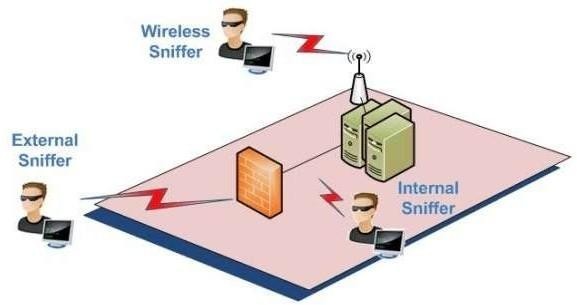
Whatisnetworksniffing?

ComputerscommunicatebybroadcastingmessagesonanetworkusingIPaddresses.Onceamessage 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.** This can bedonebythe specializedsoftware programorhardwareequipment.Sniffingcanbeusedto;

* + Capturesensitive datasuchaslogincredentials
  + Eavesdroponchatmessages
  + Capture files have been transmitted over a networkThe following are protocols thatarevulnerabletosniffing
  + Telnet
  + Rlogin
  + HTTP
  + SMTP
  + NNTP
  + POP
  + FTP
  + IMAP

Theaboveprotocolsarevulnerableif login details aresentinplaintext



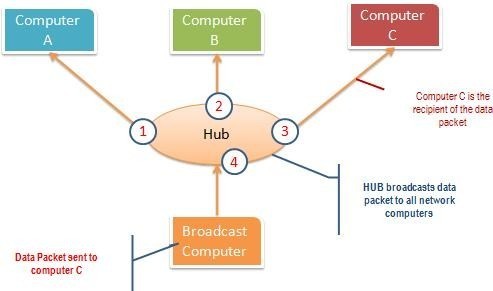
PassiveandActiveSniffing

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

**Ahubworksbysendingbroadcastmessagestoalloutputportsonitexcepttheonethathassentthebroadcast**.TherecipientcomputerrespondstothebroadcastmessageiftheIPaddress

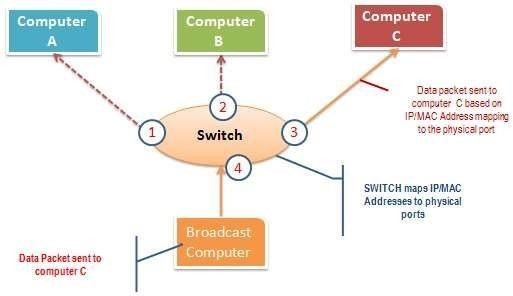
matches.Thismeanswhenusingahub,allthecomputersonanetworkcanseethebroadcastmessage.Itoperatesatthe physicallayer(layer1)of the OSI Model.

Thediagrambelow illustrateshow thehubworks.



**A switch works differently; it maps IP/MAC addresses to physical ports on it**. Broadcastmessages are sent to the physical ports that match the IP/MAC address configurations for therecipient computer. This means broadcast messages are only seen by the recipient computer.Switchesoperate atthedatalinklayer (layer2)andnetworklayer (layer3).

Thediagrambelowillustrateshow theswitchworks.



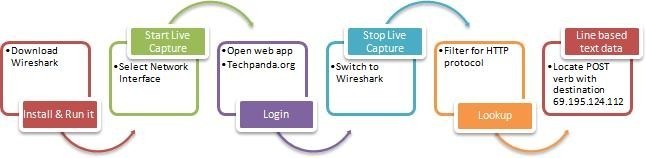
**Passive sniffing is intercepting packages transmitted over a network that uses a hub**. It iscalledpassivesniffingbecauseitisdifficulttodetect.Itisalsoeasy toperformas thehubsends

broadcastmessagestoallthecomputers onthenetwork.

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

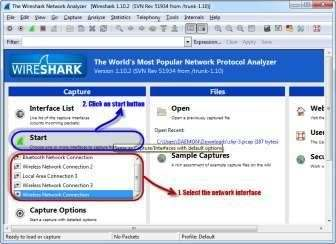
SniffingthenetworkusingWireshark

The illustration below shows you the steps that you will carry out to complete thisexercise withoutconfusion



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

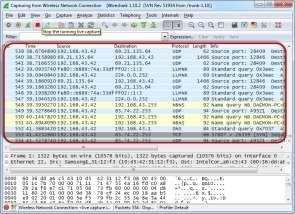
* + OpenWireshark
  + Youwillgetthefollowing screen



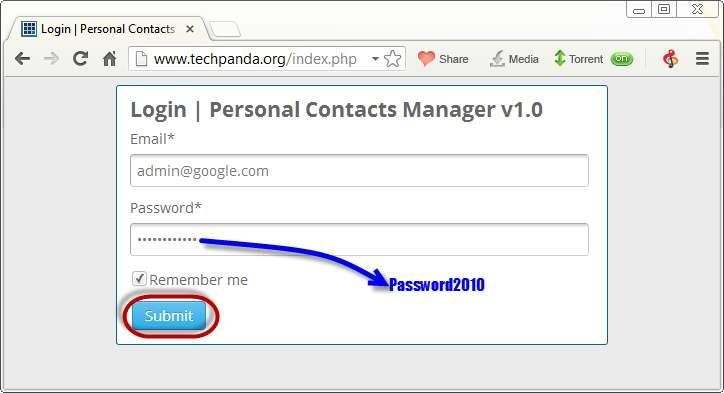
* + Selectthenetworkinterfaceyouwanttosniff.Noteforthisdemonstration,weareusingawirelessnetworkconnection.Ifyouareonalocalareanetwork,thenyoushouldselectthe

localareanetworkinterface.

* + Click onstart buttonas shownabove



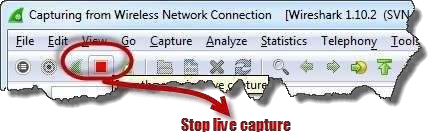
* + Openyourwebbrowserandtypein<http://www.techpanda.org/>



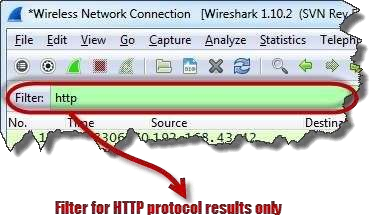
* Theloginemail is[**admin@google.com**](mailto:admin@google.com)andthepassword is**Password2010**
* Clickonsubmitbutton
* Asuccessfullogonshould giveyouthefollowingdashboard

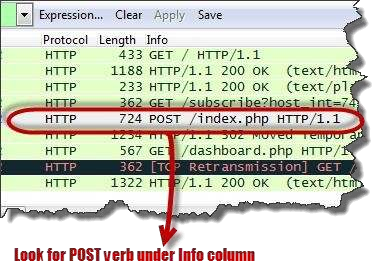


* GobacktoWiresharkandstopthelivecapture

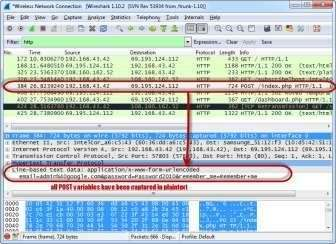


* FilterforHTTPprotocolresultsonly using thefiltertextbox





* 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:9

**Date:**

## DemonstrationofIntrusionDetectionSystem(IDS)

**AIM:**

TodemonstrateIntrusionDetectionSystem (IDS)usingSnortsoftwaretool.

## STEPSONCONFIGURINGANDINTRUSIONDETECTION:

1. DownloadSnortfromtheSnort.orgwebsite.(<http://www.snort.org/snort-downloads)>
2. DownloadRules(https://[www.snort.org/snort-rules).](http://www.snort.org/snort-rules))Youmustregistertogettherules.(Youshoulddownloadtheseoften)
3. Doubleclickonthe.exeto installsnort.Thiswillinstallsnortinthe“C:\Snort”folder.Itisimportant tohaveWinPcap(https://[www.winpcap.org/install/)](http://www.winpcap.org/install/))installed
4. ExtracttheRulesfile.You willneedWinRARforthe.gzfile.
5. Copyallfiles fromthe“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 any existing file. Remember if you modify your snort.conf fileanddownloadanewfile,youmustmodify itforSnortto work.
2. Openacommandprompt(cmd.exe)andnavigatetofolder“C:\Snort\bin”folder.(atthePrompt,typecd\snort\bin)
3. 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.

## Example:

examplesnort

Change the RULE\_PATH variable to the path of rules folder.varRULE\_PATHc:\snort\rules

pathtorules

Changethe pathofalllibrary files withthe nameandpathonyoursystem.andyoumustchangethepath ofsnort\_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/…”.youwillneedto replacethatpathwithyoursystempath.UsingC:\Snort\libChangethe path of the“dynamicengine” variablevalue inthe “snort.conf”file..

## Example:

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.

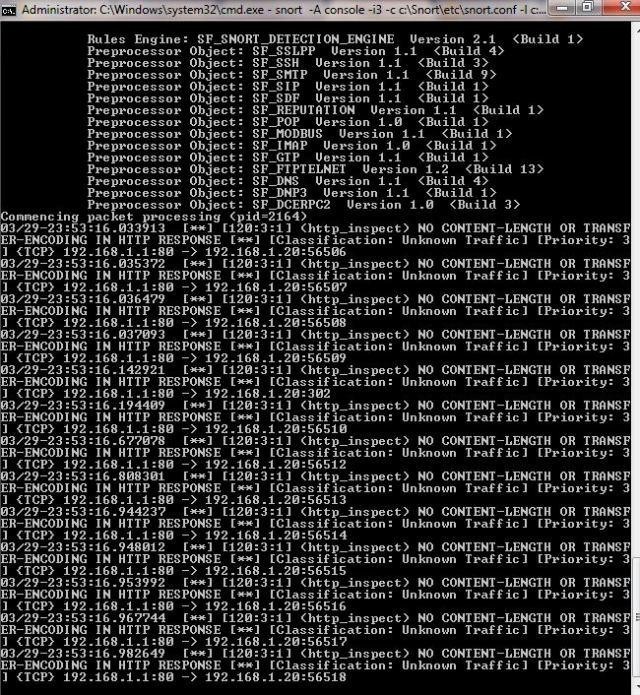
To generate Log files in ASCII mode, you can use following command while running snort in IDSmode:

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:10

**Date:**

## NetworkMonitoringTools

**Aim:**

## ToexploreaboutNetwork monitoringtools

Network monitoring is an essential part of network management. It involves using various tools tomonitorasystemnetworkanddetermineslownessandweakconnections,amongotherissues.Knowing more about these tools can help you understand them better and use the right ones that suityour requirements. In this article, we define what network monitoring tools are, provide details aboutvarioustools anddiscussaboutsometipsthat canhelpyouchoosetherighttoolforyourrequirements.

## WhatAreNetworkMonitoring Tools?

Network monitoring tools aresoftware that you can use to evaluatenetwork connections. Thesesoftware programs can help you monitor a network connection and identify network issues, which mayincludefailingnetworkcomponents,slowconnectionspeed,networkoutageorunidentifiableconnections. Network management and monitoring tools can also help you resolve these issues orestablishsolutionsthatpreventspecificissuesfromoccurringinthefuture.

## NetworkMonitoringTools

Hereareeightmonitoringtoolsalongwiththeirdescriptions andfeatures:

## SolarWindsNetworkPerformanceMonitor

SolarWindsNetworkPerformanceMonitorisamulti-vendormonitoringtool.Itallowsuserstomonitor multiple vendors' networks at the same time. It also provides network insights for thoroughvisibilityintothehealthofthenetworks.Someprominentfeaturesincludenetworkavailabilitymonitoring,intelligentnetworkmapping,criticalpathvisualisation,performanceanalysisandadvancedalerting.SolarWindsalsoallowsuserstotrackVPNtunnelstatus.ItpromptswhenaVPN

tunnel is available to help users ensure a stable connection between sites. SolarWinds provides aseven-dayfree trial,afterwhich userscanchoose apreferredsubscriptionplan.

## Auvik

Auvik is a network monitoring and management tool. It offers a quick implementation process thathelps users to set up the tool easily. It also has a clean user interface that makes it easy to navigate anduse. The tool provides in-depth network visibility that enables faster troubleshooting for networkissues. Users can automate network visibility using Auvik. It provides real-time updates on networkissuesandconfigurationchanges.

## 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.

## 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.Thetoolsalsointegrate 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

ManageEngineOpManager 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 performance monitorsthatallowuserstotrackandmonitortheirconnectionsandperformdetailedanalysesonissues.Italso

provides 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.

## 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.

## 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.

## ProgressWhatsupGold

Progress Whatsup Gold is a basic network monitoring software. It provides a minimal user interfacewith essential features like device monitoring, application monitoring, analysing network traffic 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.ItintegrateswithotherNagiosapplicationsandprovidesuserswithfeatureslikeavisualdashboard,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, businessmonitoring androotcauseanalysesofnetworkissues,and allows users toestablishathresholdfor connectionanomalies.

## TipsToChooseANetworkMonitoringAndManagementTool

Herearesomeusefultipsthatyoucanconsiderwhileselectingatoolfornetwork monitoring:

## 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 toolstypicallyofferafreetrialperiodofupto30days.Onceyouidentifywhichtoolyoumayliketouse,

seeifitisfreeorrequirespayment.Ifitisapaidtool,tryexploringitsfeaturesandefficiencyduringthetrialperiod.Considerkeeping a backuptoolincasethetoolthatyou choosedoesnotfit yourusage.

## Result:

Thusthenetworkmonitoring tools wasexplored

## Ex.No:11

**Date:**

## Studytoconfigure Firewall,VPN

**AIM:**

TostudythefeaturesoffirewallinprovidingnetworksecurityandtosetFirewallSecurityinwindows.

## FirewallinWindows7

Windows 7 comes with two firewalls that work together. One isthe**Windows Firewall**, andtheother 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, PerformanceLogs andAlerts,RemoteAdministration,WindowsRemoteManagement,RemoteAssistance,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.

When we first connect to some network, we are prompted toselecta network location. This featureis 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 threedifferentnetworkprofilesavailable:

* + Public
  + Home/Work-privatenetwork
  + Domain-usedwithinadomain

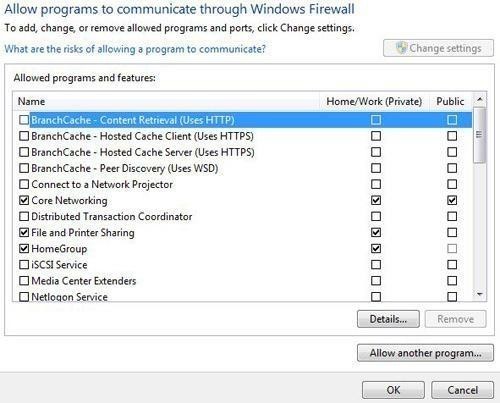
## ConfiguringWindowsFirewall

ToopenWindowsFirewallwecangoto**Start>ControlPanel>Windows**



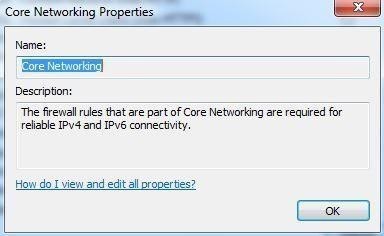
## Firewall.

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 featuretroughWindows Firewall"option.



Exceptions

To change settings in this window we have to click the "Change settings" button. As you cansee,here we have a list of predefined programs and features that can be allowed to communicate onprivate or public networks. For example, notice that the Core Networking feature is allowed on bothprivate and public networks, while the File and Printer Sharing is only allowed on private networks.Wecanalso seethedetails oftheitems in thelistbyselectingitandthenclickingtheDetailsbutton.





## Details

Ifwehaveaprogramonourcomputerthatisnotinthislist,wecanmanuallyadditbyclickingonthe "Allowanotherprogram"button.

## AddaProgram

Here we have to browse to the executable of our program and then click the Add button. Notice thatwe can also choose location types on which this program will be allowedto communicate byclickingonthe"Networklocationtypes"button.

## NetworkLocations

Many applications will automatically configure properexceptionsin Windows Firewall when werun them. For example, if we enable streaming from Media Player, it will automatically configurefirewall settings to allow streaming. The same thing is if we enable Remote Desktop feature from thesystem properties window. By enabling Remote Desktop feature we actually create an exception inWindowsFirewall.

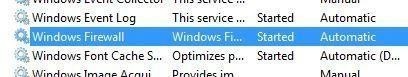
Windows Firewall can be turned off completely. To do that we can select the "Turn WindowsFirewallonoroff"optionfromthemenuontheleft.

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 the list of allowedprograms.

Windows Firewall is actually a Windows service.Asyou know, services can be stopped and started.Ifthe Windows Firewall serviceisstopped,the Windows Firewallwillnotwork.

## FirewallService



Inourcasetheserviceisrunning.Ifwestopit,wewillgetawarningthatweshouldturnon our WindowsFirewall.



## Warning

Remember that with Windows Firewall we can only configure basic firewall settings, and this isenoughformostday-to-dayusers.However,wecan'tconfigureexceptionsbasedonportsinWindowsFirewall anymore.ForthatwehavetouseWindows FirewallwithAdvancedSecurity.

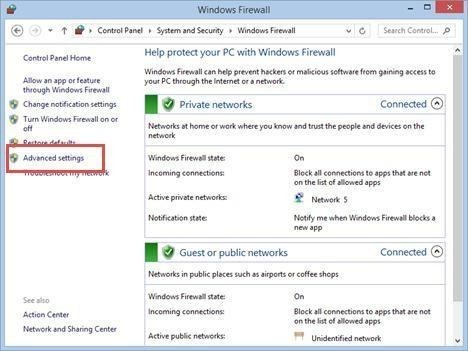
## HowtoStart&UsetheWindowsFirewallwithAdvancedSecurity

The *Windows Firewall with Advanced Security* is a tool which gives you detailed control over therules that are applied by the *Windows Firewall*. You can view all the rules that are used by the*Windows Firewall*, change their properties, create new rules or disable existing ones. In this tutorialwe will share how to open the *Windows Firewall with Advanced Security*, how to find your wayaround itand talk about thetypes ofrulesthat are availableand whatkindoftrafficthey filter.

## HowtoAccesstheWindowsFirewallwithAdvancedSecurity

Youhaveseveralalternativestoopeningthe*WindowsFirewallwith AdvancedSecurity*:

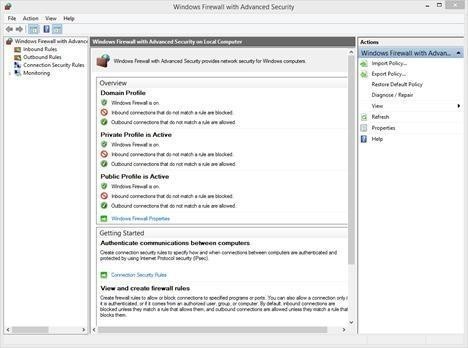
One is to open the standard Windows Firewall window, by going to *"Control Panel -> System andSecurity ->WindowsFirewall"*.Then,clickor tap*Advancedsettings*.



In Windows 7, another method is to search for the word *firewall* in the *Start Menu* search box andclick the*"WindowsFirewallwithAdvancedSecurity"*result.

In Windows 8.1, *Windows Firewall withAdvanced Security*is not returned in searchresultsand youneedto use thefirstmethodsharedaboveforopeningit.

The*WindowsFirewallwithAdvancedSecurity*looksandworksthesamebothinWindows 7 and Windows 8.1. To continue our tutorial, we will use screenshots that weremadeinWindows8.1.

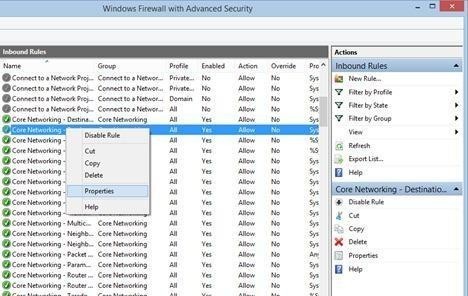


## WhatAreTheInbound&OutboundRules?

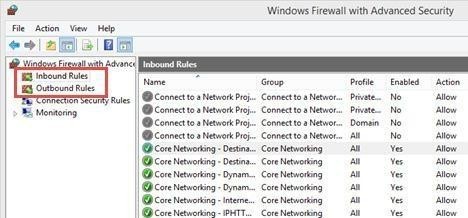
In order to provide the security you need, the *Windows Firewall* has a standard set ofinbound and outbound rules, which are enabled depending on the location of the networkyouareconnectedto.

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.

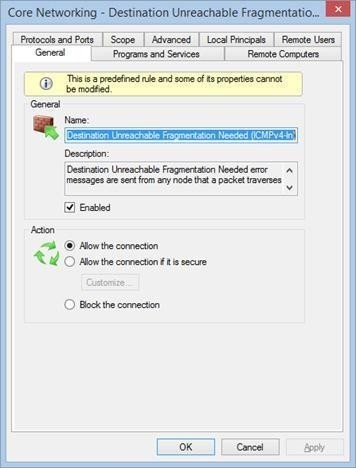


In the *Windows Firewall with Advanced Security*, you can access all rulesand edit theirproperties.Allyouhavetodoisclickortap theappropriateunit in theleft-sidepanel.



The rules used by the *Windows Firewall* can be enabled or disabled. The ones which areenabled or active are marked with a green check-box in the *Name* column. The onesthataredisabledaremarkedwithagraycheck-box.

If you want to know more about a specific rule and learn its properties, right click on it andselect *Properties* or select it and press *Properties* in thecolumn on right, which lists theactionsthatareavailableforyourselection.

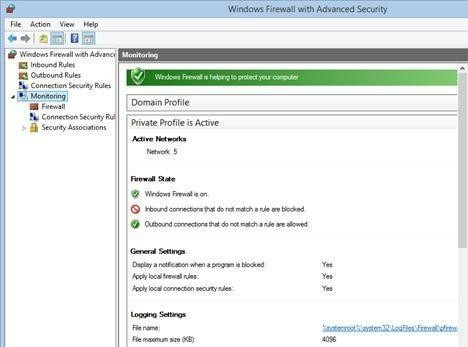


## WhatAreTheConnectionSecurityRules?

Connection security rules are used to secure traffic between two computers whileitcrossesthenetwork.Oneexamplewouldbearulewhichdefinesthatconnectionsbetweentwospecificcomputersmustbe encrypted.

Unliketheinboundoroutboundrules,whichareappliedonlytoonecomputer,connection security rules require that both computers have the same rules defined andenabled.

If you want to see if there are any such rules on your computer, click or tap *"ConnectionSecurity Rules"* on the panel on the left. By default, there are no such rules defined onWindows computers and devices. They are generally used in business environments andsuchrulesaresetbythenetworkadministrator.





## WhatDoestheWindowsFirewallwithAdvancedSecurityMonitor?

The *Windows Firewall with Advanced Security* includes some monitoringfeatures as well.In the *Monitoring* section you can find the following information: the firewall rulesthatare active (both inbound and outbound),the connection security rules that are active andwhether thereareanyactivesecurityassociations.

You should note that the *Monitoring* section shows only the active rules for the currentnetworklocation.

used to determine the operating system running on the host machine. Another feature is"boot-time filtering". This feature ensures that the firewall is working at the same timewhen the network interface becomes active, which was not the case in previous versions ofWindows.

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 toassignanetworkprofiletotheconnectionbasedonthelocation.Differentnetworkprofiles contain different collections of firewall rules. In Windows 7, different networkprofiles can be configured on different interfaces. For example,our wired interface canhave different profile than our wireless interface. There are three different network profilesavailable:

* + Public
  + Home/Work-privatenetwork
  + Domain-usedwithinadomain

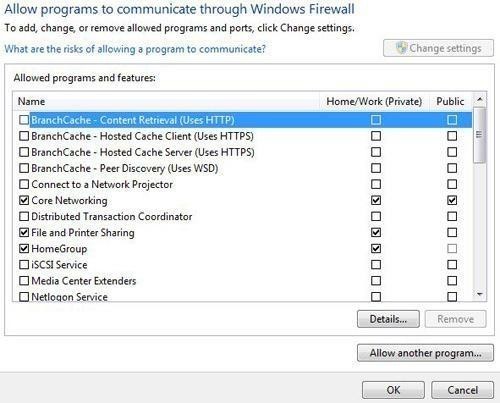
We choose those locations when we connect to a network. We can always changethelocation intheNetworkandSharing Center,inControl Panel. The Domain profile canbe automatically assigned by the NLA service when we log on to an Active Directorydomain. Note that we must have administrative rights in order to configure firewall inWindows7.

## 2.1.1ConfiguringWindowsFirewall

To open WindowsFirewall wecangoto**Start>ControlPanel>**

## WindowsFirewall.

By default, Windows Firewall is enabled for both private (home or work) and publicnetworks. It is also configured to block all connections to programs that are not on the listof allowed programs. Toconfigureexceptions we can goto the menu on the left andselect "Allowaprogram or featuretroughWindowsFirewall"option.

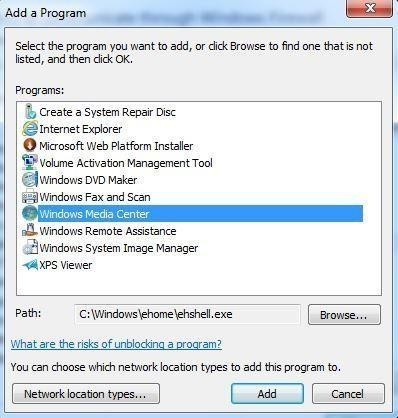


## Exceptions

To change settings in this window we have to click the "Change settings" button. As youcan see, here we have a list of predefined programs and features that can be allowed tocommunicateonprivateorpublicnetworks.Forexample,noticethattheCoreNetworking feature is allowed on both private and public networks, while the File andPrinter Sharing is only allowed on private networks. We can also see the details of theitemsinthelistbyselectingitandthenclicking theDetailsbutton.

## Details

Ifwehaveaprogramonourcomputerthatisnotinthislist,wecan



manuallyadditbyclickingonthe"Allowanotherprogram"button.

## AddaProgram

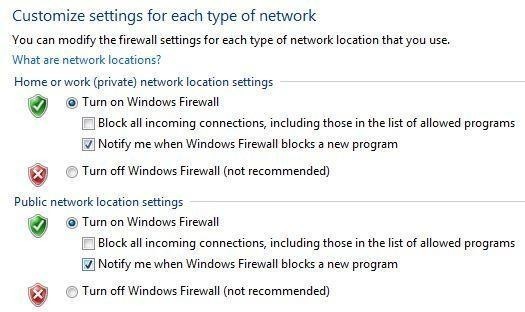
Here we have to browse to the executable of our program and then click the Add button.Notice that we can also choose location types on which this program will be allowed tocommunicate byclickingonthe"Networklocationtypes"button.



## NetworkLocations

Many applications will automatically configure proper exceptions in Windows Firewallwhen we run them. For example, if we enable streaming from Media Player, it willautomatically configure firewall settings to allow streaming. The same thing is if weenable Remote Desktop feature from the system properties window. By enabling RemoteDesktopfeatureweactuallycreateanexceptioninWindowsFirewall.

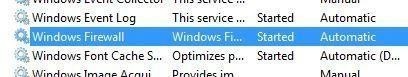
Windows Firewall can be turnedoff completely.Todo that we can select the "TurnWindowsFirewallonoroff"optionfromthemenuontheleft.



## 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.



## Warning

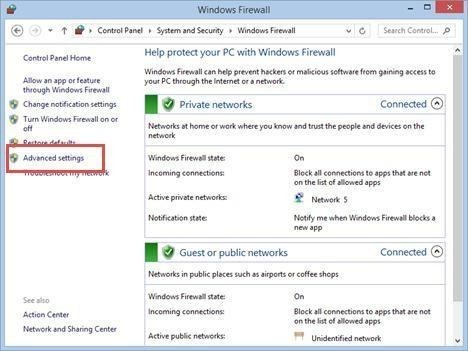
Remember that with Windows Firewall we can only configure basic firewall settings, andthis is enough for most day-to-day users. However, we can't configure exceptions based onports in Windows Firewall any more. For that we have to use Windows Firewall withAdvancedSecurity.

## 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.In thistutorialwe willsharehowtoopenthe*WindowsFirewallwithAdvanced Security*, howto find your way around it and talk about the types of rules that areavailable and what kind of traffic they filter. How to Access the Windows Firewall withAdvancedSecurity

Youhaveseveralalternativestoopeningthe*WindowsFirewallwith AdvancedSecurity*:

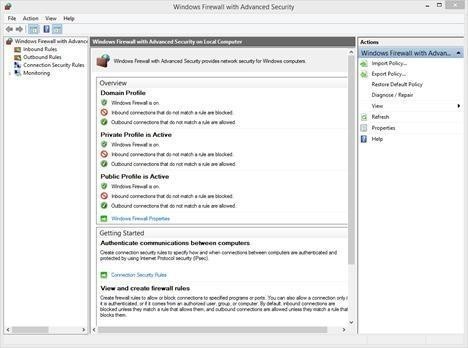
OneistoopenthestandardWindowsFirewallwindow,bygoingto*"ControlPanel->SystemandSecurity->WindowsFirewall"*.Then,click ortap*Advanced settings*.



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



In Windows 8.1, *Windows Firewall with Advanced Security* is not returned in searchresultsand youneedto use thefirstmethod sharedaboveforopeningit.

The*WindowsFirewallwithAdvancedSecurity*looksandworksthesamebothinWindows 7 and Windows 8.1. To continue our tutorial, we will use screenshots that weremadeinWindows8.1.

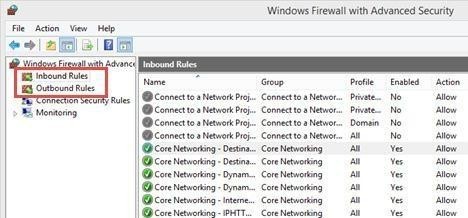
## WhatAreTheInbound&OutboundRules?

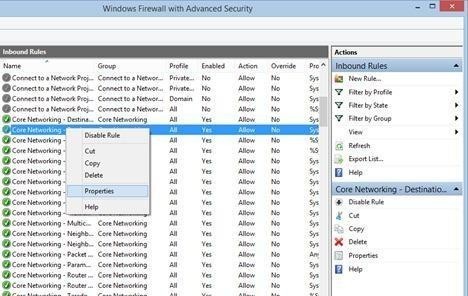
In order to provide the security you need, the *Windows Firewall* has a standard set ofinbound and outbound rules, which are enabled depending on the location of the networkyouareconnectedto.

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.

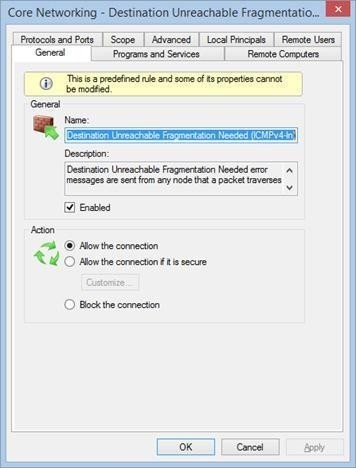
In the *Windows Firewall withAdvancedSecurity*,youcanaccessallrules and edittheir properties. All you have to do is clickor tap the appropriate unit in the left-sidepanel.





Therulesusedbythe*WindowsFirewall*canbeenabledordisabled.Theoneswhichareenabledoractivearemarkedwithagreencheck-boxinthe*Name*column.Theonesthataredisabledaremarkedwithagraycheck-box.Ifyouwanttoknowmoreaboutaspecificruleandlearnitsproperties,rightclickonitandselect*Properties*orselectitandpress*Properties*inthecolumnonright,whichliststheactionsthatareavailableforyourselection.

lOMoARcPSD|31761673



## 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.

Unliketheinboundoroutboundrules,whichareappliedonlytoonecomputer,connection security rules require that both computers have thesame rules defined andenabled.

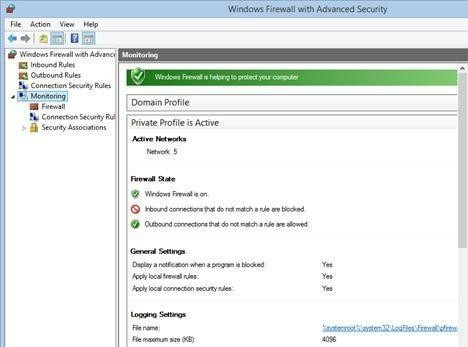
Ifyouwanttoseeifthereareanysuchrulesonyourcomputer,clickortap*"Connection Security Rules"*on the panel on the left.By default,there are no suchrulesdefinedonWindowscomputersanddevices.Theyaregenerallyusedinbusinessenvironmentsand suchrulesaresetbythe networkadministrator.

lOMoARcPSD|31761673



## 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.



You should note that the *Monitoring* section shows only the activerules for the currentnetworklocation.

## Result:

studyofthefeaturesoffirewall inprovidingnetwork securityandtosetFirewallSecurityinwindows.