DHANALAKSHMI SRINIVASAN ENGINEERING COLLEGE
(AUTONOMOUS)
(Approved by AICTE & Affiliated to Anna University, Chennai)
Accredited with 'A' Grade by NAAC, Accredited by TCS
Accredited by NBA with BME, ECE & EEE
PERAMBALUR - 621 212. Tamil Nadu.
website : www.dsengg.ac.in

DEPARTMENT OF INFORMATION TECHNOLOGY

LAB MANUAL

U20IT704/NETWORK SECURITY LABORATORY

IV YEAR / VII SEMESTER

REGUALTION: 2023

Prepared by: **Approved by:**

LIST OF EXPERIMENTS

1. Perform encryption, decryption using the following substitution techniques
(i) Ceaser cipher, (ii) Play Fair cipher (iii) Hill Cipher(iv) Vigenere cipher
2. Perform encryption and decryption using following transposition techniques i) Rail fence ii) row & Column Transformation
3. Implement RSA Algorithm using HTML and JavaScript
4. Implement the Diffie-Hellman Key Exchange algorithm for a given problem.
5. Calculate the message digest of a text using the SHA-1 algorithm.
6. Demonstrate intrusion detection system (ids) using any tool eg. Snort or any other s/w.
7. Automated Attack and Penetration Tools Exploring N-Stalker, a Vulnerability Assessment Tool
8. Defeating Malware
i) Building Trojans ii) Root kit Hunter

TOTAL: 60 PERIODS

LISTOF EXERCISES

Exercise:

1. i)WriteaJava/C/C++programtoimplementsubstitutiontechniqueusingCaesarcipher algorithm with shift key = 19.

ii) Create a program to display contents of Play fair matrix and encrypt the given plaintext.

iii) Implement decryption using Hill Cipher technique with 2*2 matrix in a given plaintext

2. Write a Java/C/C++ program to implement Vigenere cipher which encrypts the plaintext “ATTACK AT DAWN” using the keyword “LEMON”.

3. Apply AES algorithm for practical applications. Apply AES algorithm for practical applications.

4. ImplementtheDiffie-HellmanKeyExchange mechanism tosharesecretkeybetweentwoend users (Alice & Bob).

5. Calculate the message digest of a text using the SHA-256 Algorithm

6. Demonstrate intrusion detection system to detect and alert on potential security breach

7. To download the N-stalker Vulnerability tool and exploring the features

8.i)Perform wireless audit on an access point or a router and decrypt WEP andWPA. (NetStumbler)

ii) Demonstrate the Installation of Root kit Hunter and find the malwares in a computer

SoftwareDownloadLinks:

- **VisualStudioCode:https://code.visualstudio.com/download**
- **Snort-https://www.snort.org/downloads**
- **N-Stalker-https://www.nstalker.com/products/editions/free/download/**
- **GMER-http://www.gmer.net/**
- **JAVA-https://www.java.com/en/download/**

Ex.No:1(a)Date :	EncryptionandDecryptionUsingCeaserCipher

AIM:

Toencryptanddecryptthegivenmessagebyusing CeaserCipher encryptionalgorithm.

ALGORITHMS:

1. InCeaserCiphereachletter intheplaintext isreplacedbyalettersomefixednumberofpositionsdownthealphabet.
2. For example, with a **leftshiftof3**, **D** would be replaced by **A**; **E** would become **B** and so on.
3. The encryption can also be represented using modular arithmetic by firsttransforming the letters into numbers, according to the scheme, **A = 0, B = 1, Z=25.**
4. Encryptionofaletterxbyashiftncanbedescribedmathematicallyas,

$$En(x)=(x+n)mod26$$

5. Decryptionisperformedsimilarly,

$$Dn(x)=(x-n)mod26$$

PROGRAM:

CaesarCipher.java

```
classcaesarCipher{
   publicstaticStringencode(Stringenc,intoffset){offs
      et =offset % 26 +26;
      StringBuilderencoded=newStringBuilder();fo
      r(chari :enc.toCharArray()){
         if(Character.isLetter(i)){
            if(Character.isUpperCase(i)){
               encoded.append((char)('A'+(i-'A'+offset)%26));
            }else{
               encoded.append((char)('a'+(i-'a'+offset)%26));
            }
         }else{
            encoded.append(i);
         }
      }
```

```
        returnencoded.toString();
    }

    publicstaticStringdecode(Stringenc,intoffset){retu
        rnencode(enc,26-offset);
    }

    publicstaticvoidmain(String[]args)throwsjava.lang.Exception{String
        msg="AnnaUniversity";
        System.out.println("SimulatingCaesarCipher\n ---------------------- ");
        System.out.println("Input:"+msg);System.out.printf("Encryp
        ted Message :
        ");System.out.println(caesarCipher.encode(msg,3));System.o
        ut.printf("DecryptedMessage :");
        System.out.println(caesarCipher.decode(caesarCipher.encode(msg,3),3));
    }
}
```

OUTPUT:

```
SimulatingCaesarCipher
-----------------------
Input:AnnaUniversity
EncryptedMessage:DqqdXqlyhuvlwbD
ecryptedMessage:AnnaUniversity
```

Exercise:

WriteaJava/C/C++programtoimplementsubstitutiontechniqueusingCaesarcipher algorithm with shift key = 19.

RESULT:

Thustheprogramforceasercipherencryptionanddecryptionalgorithmhasbeen implementedand theoutputverifiedsuccessfully.

Ex.No:1(b) Date :	PlayfairCipher

AIM:

Toimplementaprogramtoencryptaplaintextanddecryptaciphertext usingplayfairCiphersubstitutiontechnique.

ALGORITHM:

1. To encrypt a message, one would break the message into digrams (groups of2 letters)
2. Forexample,"HelloWorld"becomes"HELLOWORLD".
3. Thesedigramswillbesubstitutedusingthekeytable.
4. Since encryption requires pairs of letters, messages with an odd number ofcharactersusuallyappendanuncommonletter,suchas"X",tocompletethefinal digram.
5. Thetwolettersofthedigramareconsideredoppositecornersofarectanglein the key table. To perform the substitution, apply the following 4 rules, inorder,toeachpair of lettersintheplaintext:

PROGRAM:

playfairCipher.java

```
importjava.awt.Point;

classplayfairCipher{
   privatestaticchar[][]charTable;p
   rivatestaticPoint[]positions;

   privatestaticStringprepareText(Strings,booleanchgJtoI){s=s.t
      oUpperCase().replaceAll("[^A-Z]","");
      returnchgJtoI?s.replace("J","I"):s.replace("Q","");
   }

   privatestaticvoidcreateTbl(Stringkey,booleanchgJtoI){charTabl
      e=newchar[5][5];
      positions=newPoint[26];
      Strings=prepareText(key+"ABCDEFGHIJKLMNOPQRSTUVWXYZ",chgJtoI)
;
      intlen=s.length();
      for(inti=0,
         k=0;i<len;i++){charc=s.charAt
         (i);
```

```
        if (positions[c - 'A'] == null)
            {charTable[k/5][k%5]=c;
            positions[c- 'A']=newPoint(k%5,k/5);k++;
        }
    }
}

privatestaticStringcodec(StringBuildertxt,intdir){intlen
    =txt.length();
    for(inti= 0;i< len;i+=2){chara
        = txt.charAt(i);
        charb=txt.charAt(i+1);
        int row1 = positions[a -
        'A'].y;introw2=positions[b-
        'A'].y;int col1 = positions[a -
        'A'].x;int col2 = positions[b -
        'A'].x;if(row1==row2){
            col1=(col1+dir)%5;col
            2=(col2+dir)%5;
        }else if(col1== col2){

            row1=(row1+dir)%5;ro
            w2=(row2+dir)%5;
        }else{
            inttmp=col1;c
            ol1 =
            col2;col2=
            tmp;
        }
        txt.setCharAt(i,
        charTable[row1][col1]);txt.setCharAt(i+1,ch
        arTable[row2][col2]);
    }
    returntxt.toString();
}

private static String encode(String s)
    {StringBuildersb=newStringBuilder(s);f
    or(inti=0;i<sb.length();i+=2){
        if(i== sb.length()- 1){
```

```
            sb.append(sb.length()%2==1?'X':"");
        }elseif(sb.charAt(i)==sb.charAt(i+1)){sb.ins
            ert(i+1,'X');
        }
    }
    returncodec(sb,1);
}

private static String decode(String s)
    {returncodec(newStringBuilder(s),4);
}

publicstaticvoidmain(String[]args)throwsjava.lang.Exception{Stringkey
    ="CSE";
    Stringtxt="SecurityLab";/*makesurestringlengthiseven*//*changeJto I*/
    boolean chgJtoI =
    true;createTbl(key,chgJ
    toI);
    String enc = encode(prepareText(txt,
    chgJtoI));System.out.println("SimulatingPlayfairCipher\n ----------");
    System.out.println("Input Message : " +
    txt);System.out.println("Encrypted Message : " +
    enc);System.out.println("DecryptedMessage:"+decode(enc));
}
}
```

OUTPUT:

```
SimulatingPlayfairCipher
----------------------
InputMessage:SecurityLab
EncryptedMessage:EABPUGYANSEZD
ecryptedMessage:SECURITYLABX
```

Exercise: ii) Create a program to display contents of Playfair matrix and encrypt the given plaintext.

RESULT:

Thustheprogramforplayfaircipherencryptionanddecryptionalgorithmhasbeen implementedand the outputverifiedsuccessfully.

Ex.No:1(c)Date :	HillCipher

AIM:

Toimplementaprogramtoencryptanddecryptusingthe Hillcipher substitutiontechnique

ALGORITHM:

1. IntheHillcipherEachletterisrepresentedbyanumbermodulo26.
2. To encrypt a message, each block of n letters is multiplied by an invertible ***nxn***matrix,again***modulus26***.
3. Todecryptthemessage,eachblock ismultipliedbytheinverseof thematrixusedfor encryption.
4. Thematrixused forencryptionisthecipherkey,anditshouldbechosenrandomlyfromthe***setofinvertiblen×nmatrices(modulo 26).***
5. Theciphercan, beadaptedtoanalphabetwithanynumberofletters.
6. Allarithmeticjust needstobedonemodulo thenumberoflettersinsteadofmodulo 26.

PROGRAM:

HillCipher.java

```
classhillCipher{
   /*3x3keymatrixfor3charactersatonce*/
   publicstaticint[][]keymat=newint[][]{{1,2, 1}, {2, 3, 2},
         {2,2,1} };/*keyinversematrix*/
   publicstaticint[][]invkeymat=newint[][]{{-1, 0, 1}, {2,-1, 0}, {-2, 2,-1
}};
   publicstaticStringkey="ABCDEFGHIJKLMNOPQRSTUVWXYZ";

   privatestaticStringencode(chara,charb,charc){Strin
      gret="";
      intx,y,z;
      int posa = (int) a -
      65;intposb=(int)b-
      65;intposc=(int)c -65;
      x=posa
      *keymat[0][0]+posb*keymat[1][0]+posc*keymat[2][0];y=posa*keym
      at[0][1]+posb*keymat[1][1]+ posc*keymat[2][1];z = posa *
      keymat[0][2] + posb * keymat[1][2] + posc *
      keymat[2][2];a=key.charAt(x%26);
      b=key.charAt(y%26);
```

```
        c=key.charAt(z
        %26);ret = "" + a + b +
        c;returnret;
    }

    privatestaticStringdecode(chara,charb,charc){Strin
        gret="";
        intx,y,z;
        int posa = (int) a -
        65;intposb=(int)b-
        65;intposc=(int)c -65;
        x=posa*invkeymat[0][0]+posb*invkeymat[1][0]+posc*invkeymat[2]
[0];
        y=posa*invkeymat[0][1]+posb*invkeymat[1][1]+posc*invkeymat[2]
[1];
        z=posa*invkeymat[0][2]+posb*invkeymat[1][2]+posc*invkey
mat[2][2];
        a= key.charAt((x%26< 0)?(26+x%26):(x%26));

        b=key.charAt((y%26<  0)?(26+  y%26):(y%26));c  =
        key.charAt((z % 26 < 0) ? (26 + z % 26) : (z % 26));ret
        =""+a+b+c;
        returnret;
    }

    publicstaticvoidmain(String[]args)throwsjava.lang.Exception{Stri
        ng msg;
        Stringenc="";S
        tringdec="";int
        n;
        msg=("SecurityLaboratory");
        System.out.println("simulationofHillCipher\n ------------------------");
        System.out.println("Inputmessage:"+msg);ms
        g=msg.toUpperCase();
        msg=msg.replaceAll("\\s","");
        /*removespaces*/n=msg.length() %3;
        /*appendpaddingtextX*/if(n!=0){for(in
            ti= 1;i<= (3-n);i++){
                msg+='X';
            }
```

```
        }
        System.out.println("paddedmessage:"+msg);ch
        ar[]pdchars=msg.toCharArray();
        for(inti=0;i<msg.length();i+=3){
            enc+=encode(pdchars[i],pdchars[i+1],pdchars[i+2]);
        }
        System.out.println("encodedmessage:"+enc);char[]d
        echars=enc.toCharArray();
        for(inti= 0;i<enc.length();i+= 3){
            dec+=decode(dechars[i],dechars[i+1],dechars[i+2]);
        }
        System.out.println("decodedmessage:"+dec);
    }
}
```

OUTPUT:

```
SimulatingHillCipher
------------------------------
InputMessage :SecurityLaboratory
Padded Message :
SECURITYLABORATORYEncryptedMessage:EA
CSDKLCAEFQDUKSXUDecryptedMessage:SECU
RITYLABORATORY
```

Exercise: Implement decryption using Hill Cipher technique with 2*2 matrix in a given plaintext

RESULT:

Thustheprogramforhillcipherencryptionanddecryptionalgorithmhasbeenimplementedand theoutputverifiedsuccessfully.

Ex.No:1(d)Date :	VigenereCipher

AIM:

Toimplementaprogramforencryptionanddecryptionusingvigenere ciphersubstitutiontechnique

ALGORITHM:

1. TheVigenerecipher isamethodofencryptingalphabetictextbyusingaseries ofdifferentCaesarciphers basedonthelettersofa keyword.
2. Itisasimpleformofpolyalphabeticsubstitution.
3. To encrypt, a table of alphabets can be used, termed a Vigenere square, orVigeneretable.
4. It consists of the alphabet written out 26 times in different rows, eachalphabetshiftedcyclicallytothe leftcomparedtothepreviousalphabet,correspondingtothe26 possibleCaesarciphers.
5. Atdifferentpointsintheencryptionprocess,thecipherusesadifferentalphab etfromoneoftherowsused.
6. Thealphabetateachpointdependsonarepeatingkeyword.

PROGRAM:

vigenereCipher.java

```
publicclassvigenereCipher{
   staticStringencode(Stringtext,finalStringkey){Stri
      ngres="";
      text=text.toUpperCase();
      for(inti=0,
         j=0;i<text.length();i++){charc=text.cha
         rAt(i);
         if(c<'A'||c>'Z'){cont
            inue;
         }
         res+=(char)((c+key.charAt(j) -2*'A')%26+'A');j
         =++j%key.length();
      }
      returnres;
   }

   staticStringdecode(Stringtext,finalStringkey){Stri
      ngres="";
      text=text.toUpperCase();
```

```
        for(inti=0,
            j=0;i<text.length();i++){charc=text.cha
            rAt(i);
            if(c<'A'||c>'Z'){cont
                inue;
            }
            res+=(char)((c-key.charAt(j)+26)%26+'A');j
            =++j%key.length();
        }
        returnres;
    }

    publicstaticvoidmain(String[]args)throwsjava.lang.Exception{Stringkey
        ="VIGENERECIPHER";
        Stringmsg="SecurityLaboratory";
        System.out.println("SimulatingVigenereCipher\n ---------------------- ");
        System.out.println("Input Message : " +
        msg);Stringenc=encode(msg,key);System.out.printl
        n("EncryptedMessage:"+enc);
        System.out.println("DecryptedMessage:"+decode(enc,key));
    }
}
```

OUTPUT:

```
SimulatingVigenereCipher
------------------------
InputMessage :SecurityLaboratory
EncryptedMessage:NMIYEMKCNIQVVROWXCD
ecryptedMessage:SECURITYLABORATORY
```

Exercise: Write a Java/C/C++ program to implement Vigenere cipher which encrypts the plaintext "ATTACK AT DAWN" using the keyword "LEMON".

RESULT:

Thustheprogramforvigenerecipherencryptionanddecryptionalgorithmhasbeen implementedand the outputverified successfully.

Ex.No:2(a)Date :	RailFenceCipherTranspositionTechnique

AIM:

Toimplementaprogramforencryptionanddecryptionusingrailfence transpositiontechnique.

ALGORITHM:

1. Intherailfencecipher, theplaintextiswrittendownwardsanddiagonallyonsuccessive "rails" of an imaginary fence, then moving up when we reach thebottomrail.
2. When we reach the top rail, the message is written downwards again untilthewholeplaintextiswrittenout.
3. Themessageisthenreadoffinrows.

PROGRAM:

railFenceCipher.java

```
classrailfenceCipherHelper{i
   nt depth;

   Stringencode(Stringmsg,intdepth)throwsException{int r
      =depth;
      intl=msg.length();i
      ntc = l/depth;
      intk=0;
      charmat[][]=newchar[r][c];St
      ringenc="";
      for (int i = 0; i < c; i++)
         {for(intj=0;j<r;j++){
            if(k!=l){
               mat[j][i]=msg.charAt(k++);
            }else{
               mat[j][i]='X';
            }
         }
      }
      for (int i = 0; i < r; i++)
         {for(intj=0;j<c;j++){
            enc+=mat[i][j];
         }
```

```
        }
        returnenc;
    }

    Stringdecode(Stringencmsg,intdepth)throwsException{int r
        =depth;
        intl=encmsg.length();i
        ntc=l/depth;
        intk=0;
        charmat[][]=newchar[r][c];St
        ringdec="";
        for (int i = 0; i < r; i++)
            {for(intj=0;j<c;j++){
                mat[i][j]=encmsg.charAt(k++);
            }
        }
        for (int i = 0; i < c; i++)
            {for(intj=0;j<r;j++){
                dec+=mat[j][i];
            }
        }
        returndec;
    }
}

classrailFenceCipher{
    publicstaticvoidmain(String[]args)throwsjava.lang.Exception{railfenceCipherHelp
        errf=newrailfenceCipherHelper();
        Stringmsg,enc,dec;
        msg="AnnaUniversity,Chennai";in
        t depth=2;
        enc=rf.encode(msg,depth);d
        ec=rf.decode(enc,depth);
        System.out.println("SimulatingRailfenceCipher\n-------------------------");
        System.out.println("Input Message : " +
        msg);System.out.println("EncryptedMessage:"+enc);System.
        out.printf("DecryptedMessage:"+dec);
    }
}
```

OUTPUT:

SimulatingRailfenceCipher

Input Message : Anna University,
ChennaiEncrypted Message : An nvriy
hnanaUiest,CeniDecryptedMessage:AnnaUniv
ersity,Chennai

Exercise: Write a program in Java to implement Rail Fence cipher encryption algorithm without a key

RESULT:

Thus the java program for Rail Fence Transposition Technique has beenimplemented and theoutputverifiedsuccessfully.

Ex.No:2(b)Date :	RowandColumnTransformationTechnique

AIM:

Toimplementaprogramforencryptionanddecryptionbyusingrowand columntransformationtechnique.

ALGORITHM:

1. Considertheplaintexthelloworld,andletusapplythesimplecolumnartranspositiontechniqueasshownbelow

h	e	l	l
o	w	o	r
l	d		

2. Theplaintextcharactersareplacedhorizontallyandtheciphertextiscreatedwith verticalformat as:**holewdlolr**.
3. Now,thereceiverhastousethesametabletodecryptthecipher texttoplaintext.

PROGRAM:

TransCipher.java

```
import
java.util.*;classTra
nsCipher{
   public static void main(String args[])
      {Scanner sc = new
      Scanner(System.in);System.out.println("
      Entertheplaintext");Stringpl=sc.nextLine(
      );
      sc.close();St
      rings="";ints
      tart=0;
      for(inti=0;i<pl.length();i++){if(pl.
         charAt(i)==''){
            s=s+pl.substring(start,i);sta
            rt =i+1;
         }
      }
      s=s+pl.substring(start);
```

```
        System.out.print(s);
        System.out.println();
        //endofspacedeletion

        intk=s.length();i
        ntl=0;
        intcol=4;
        introw=s.length()/col;
        charch[][]=newchar[row][col];fo
        r(inti= 0; i< row;i++){
            for(intj=0;j<col;j++){if(l<
                k) {
                    ch[i][j]=s.charAt(l);l
                    ++;
                }else{
                    ch[i][j]='#';
                }
            }
        }
        //arrangedinmatrix

        chartrans[][]=newchar[col][row];fo
        r(inti=0;i< row;i++){
            for(intj=0;j<col;j++){trans
                [j][i]= ch[i][j];
            }
        }

        for(inti=0;i<col;i++){for(intj=
            0;j<row;j++){
                System.out.print(trans[i][j]);
            }
        }
        //
        displaySystem.out.p
        rintln();
    }
}
```

OUTPUT:

EntertheplaintextS
ecurity
LabSecurityLabSr
eictuy

Exercise: WriteaJava/C/C++programtoimplement rowtransposition technique.

RESULT:

ThusthejavaprogramforRowandColumnTranspositionTechniquehasbeenimp
lementedand theoutputverifiedsuccessfully.

Ex.No:3 Date :	RSAAlgorithm

AIM:

ToimplementRSA(Rivest–Shamir–Adleman)algorithmbyusingHTML andJavascript.

ALGORITHM:

1. Choosetwoprimenumberpandq
2. Computethe value ofnand**p**
3. Findthevalueof***e***(publickey)
4. Computethevalueof***d***(privatekey)usinggcd()
5. Dotheencryptionanddecryption
   a. Encryptionis givenas,
      $c = t^e mod n$
   b. Decryptionisgivenas,
      $t = c^d mod n$

PROGRAM:

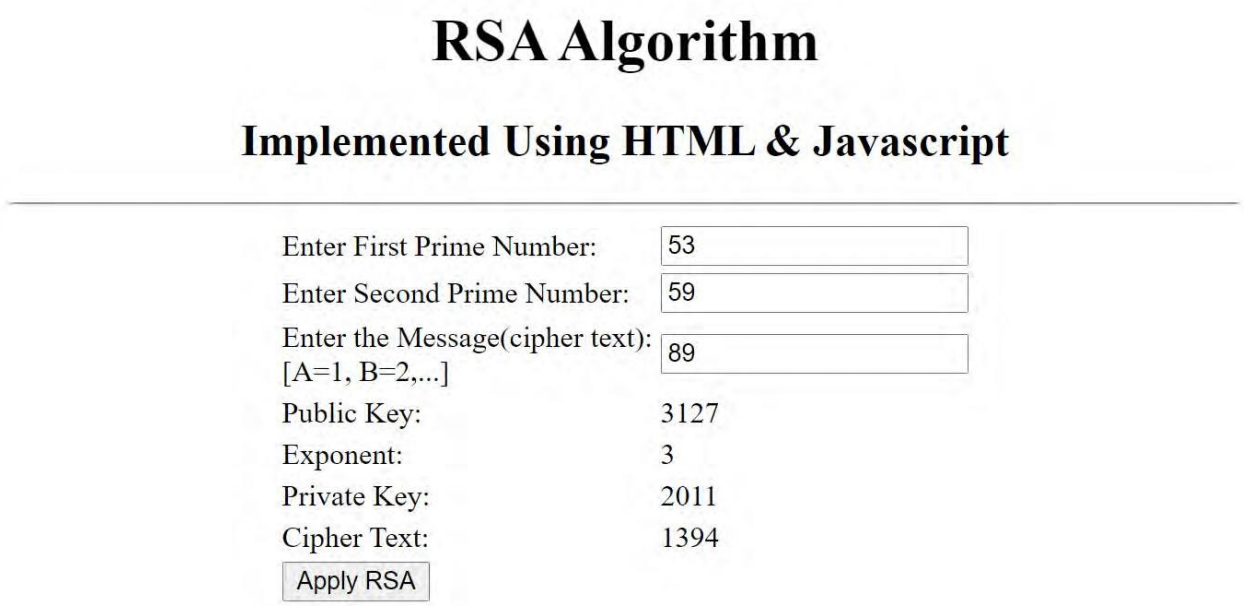
rsa.html

```
<html>

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

<body>
  <center>
    <h1>RSAAlgorithm</h1>
    <h2>ImplementedUsingHTML&Javascript</h2>
    <hr>
    <table>
      <tr>
        <td>EnterFirstPrimeNumber:</td>
        <td><inputtype="number"value="53"id="p"></td>
      </tr>
      <tr>
        <td>EnterSecondPrimeNumber:</td>
        <td><inputtype="number"value="59"id="q"></p>
```

```
            </td>
          </tr>
          <tr>
            <td>EntertheMessage(ciphertext):<br>[A=1,B=2,...]</td>
            <td><inputtype="number"value="89"id="msg"></p>
            </td>
          </tr>
          <tr>
            <td>PublicKey:</td>
            <td>
              <pid="publickey"></p>
            </td>
          </tr>
          <tr>
            <td>Exponent:</td>
            <td>
              <pid="exponent"></p>
            </td>
          </tr>
          <tr>
            <td>PrivateKey:</td>
            <td>
              <pid="privatekey"></p>
            </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.getElementBy
        Id('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);d
        t=dtt %n;

        document.getElementById('publickey').innerHTML =
        n;document.getElementById('exponent').innerHTML =
        e;document.getElementById('privatekey').innerHTML=d;docu
        ment.getElementById('ciphertext').innerHTML=ct;
    }
</script>
</html>
```

OUTPUT:



Exercise: Apply AES algorithm for practical applications. Apply AES algorithm for practical applications.

RESULT:

ThustheRSAalgorithmhasbeenimplementedusingHTML&CSSandtheoutputhas beenverifiedsuccessfully.

Ex.No:4 Date :	Diffie-Hellmankeyexchangealgorithm

AIM:

ToimplementtheDiffie-HellmanKeyExchangealgorithmforagiven problem.

ALGORITHM:

1. AliceandBobpubliclyagreetouseamodulus$p$=23andbase g=5(whichisaprimitiverootmodulo 23).
2. Alicechoosesasecretinteger$a$=4, thensendsBob$A$= g^amod$p$
   - A=5^4mod23 =4
3. Bobchoosesasecretinteger$b$=3, thensendsAlice$B$= g^bmod$p$
   - B=5^3mod 23=10
4. Alicecomputes$s$=B^amod$p$
   - s=10^4mod 23 =18
5. Bobcomputes$s$ =A^bmod$p$
   - s=4^3mod 23=18
6. Aliceand Bob nowshareasecret(thenumber18).

PROGRAM:

DiffieHellman.java

```
classDiffieHellman{
   publicstaticvoidmain(Stringargs[]){
      intp=23;/*publiclyknown(primenumber) */int g
      = 5; /* publicly known (primitive root)
      */intx=4;/*onlyAlice knowsthis secret*/
      int y = 3; /* only Bob knows this secret
      */doublealiceSends=(Math.pow(g, x))%p;
      doublebobComputes=(Math.pow(aliceSends,y))%p;do
      uble bobSends= (Math.pow(g,y))%p;
      doublealiceComputes=(Math.pow(bobSends,x))%p;do
      ublesharedSecret= (Math.pow(g,(x*y)))%p;
      System.out.println("simulationofDiffie-Hellmankeyexchangealgorithm\n--
_____");
      System.out.println("Alice Sends : " +
      aliceSends);System.out.println("BobComputes:"+bobC
      omputes);System.out.println("BobSends:"+ bobSends);
```

```
        System.out.println("AliceComputes:"+aliceComputes);Syste
        m.out.println("SharedSecret:"+sharedSecret);
        /*sharedsecretsshould matchandequalityistransitive*/
        if((aliceComputes==sharedSecret)&&(aliceComputes==bobComputes))System.
           out.println("Success:SharedSecretsMatches!"+sharedSecret);
        else
           System.out.println("Error:SharedSecretsdoesnotMatch");
    }
}
```

OUTPUT:

```
simulationofDiffie-Hellmankeyexchangealgorithm
---------------------------------------------------------------------
Alice Sends :
4.0BobComputes:18
.0BobSends:10.0
AliceComputes:18.0S
haredSecret:18.0
Success:SharedSecretsMatches!18.0
```

Exercise: ImplementtheDiffie-HellmanKeyExchange mechanism tosharesecretkeybetweentwoend users (Alice & Bob).

RESULT:

Thusthe*Diffie-Hellmankeyexchangealgorithm*hasbeenimplementedusingJava Programandthe outputhasbeen verified successfully.

Ex.No:5 Date :	SHA-1Algorithm

AIM:

ToCalculatethemessagedigestofatextusingtheSHA-1algorithm.

ALGORITHM:

1. AppendPaddingBits
2. AppendLength-64bitsareappendedtotheend
3. PrepareProcessingFunctions
4. PrepareProcessingConstants
5. InitializeBuffers
6. ProcessingMessagein512-bitblocks (Lblocksintotalmessage)

PROGRAM:

sha1.java

```
importjava.security.*;

publicclasssha1{
   publicstaticvoidmain(String[]a){try
      {
         MessageDigest md =
         MessageDigest.getInstance("SHA1");System.out.println("Messag
         edigest objectinfo:\n---------------------------------------------- ");
         System.out.println("Algorithm="+md.getAlgorithm());Sys
         tem.out.println("Provider=" +
         md.getProvider());System.out.println("ToString="+md.toS
         tring());
         String input
         ="";md.update(input.getByte
         s());byte[] output =
         md.digest();System.out.print
         ln();
         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
         ="abcdefghijklmnopqrstuvwxyz";
         md.update(input.getBytes());
```

```
            output=md.digest();
            System.out.println();
            System.out.println("SHA1(\""+
            input+"\")="+bytesToHex(output));System.out.println();
        } catch (Exception e)
            {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]);b
            uf.append(hexDigit[aB&0x0f]);
        }

        returnbuf.toString();
    }
}
```

OUTPUT:

Messagedigestobjectinfo:

Algorithm=SHA1

Provider=SUNversion12

ToString=SHA1MessageDigestfromSUN,<initialized>SHA1("")=DA39A3EE5E6B4B0D3255BFEF95601890AFD80709SHA1("abc")=A9993E364706816ABA3E25717850C26C9CD0D89D

SHA1("abcdefghijklmnopqrstuvwxyz")=32D10C7B8CF96570CA04CE37F2A19D84240D3A89

Exercise: Calculate the message digest of a text using the SHA-256 Algorithm

RESULT:

Thusthe*SecureHashAlgorithm(SHA-1)*hasbeenimplementedandtheoutputhasbeenverifiedsuccessfully.

Ex.No:6 Date :	DemonstrationofIntrusionDetectionSystem(IDS)

AIM:

TodemonstrateIntrusionDetectionSystem(IDS)usingSnortsoftwaretool.

STEPSONCONFIGURINGANDINTRUSIONDETECTION:

1. DownloadSnort fromtheSnort.orgwebsite.(http://www.snort.org/snort-downloads)
2. DownloadRules(https://www.snort.org/snort-rules).Youmustregistertogettherules.(Youshould downloadtheseoften)
3. Double click on the .exe to install snort.This will install snort in the "C:\Snort"folder.ItisimportanttohaveWinPcap(https://www.winpcap.org/install/)installed
4. ExtracttheRulesfile.YouwillneedWinRARforthe.gz file.
5. Copyallfilesfromthe"rules"folderoftheextractedfolder.Nowpastetherulesinto*"C:\Snort\rules"*folder.
6. Copy"snort.conf"filefromthe"etc"folderoftheextractedfolder.Youmustpasteitinto"C:\Snort\etc"folder.Overwriteany existing file.Remember ifyou modify your snort.conf file and download a new file, you must modify it forSnort towork.
7. Openacommandprompt(cmd.exe)andnavigateto folder"C:\Snort\bin"folder.(at thePrompt,typecd\snort\bin)
8. Tostart(execute)snortinsniffer modeusefollowingcommand:snort-dev-i3
-
iindicatestheinterfacenumber.Youmustpickthecorrectinterfacenumber.Inmycase,itis3.
-devisusedtorunsnorttocapturepacketsonyournetwork.

Tochecktheinterfacelist,usefollowingcommand:snort
-W

Findinganinterface

YoucantellwhichinterfacetousebylookingattheIndexnumberandfindingMicrosoft.As you can see in the above example, the other interfaces are forVMWare.Myinterfaceis3.

9. TorunsnortinIDS mode,youwillneed toconfigurethefile“snort.conf”accordingtoyournetwork environment.
10. Tospecifythenetworkaddressthatyouwanttoprotectinsnort.conffile,lookforthefollowingline.
varHOME_NET192.168.1.0/24(Youwillnormally seeanyhere)
11. YoumayalsowanttosettheaddressesofDNS_SERVERS,ifyouhavesomeonyournetwork.

Example:

examplesnort
12. ChangetheRULE_PATHvariabletothepathofrulesfolder.varR ULE_PATHc:\snort\rules

pathto rules

13. Changethepathofalllibraryfileswiththenameandpathonyoursystem. andyoumustchangethepath of snort_dynamicpreprocessorvariable.C:\Snort\lib\snort_dynamiccpreprocessor You need to do this to all library files in the "C:\Snort\lib" folder. The old pathmightbe:"/usr/local/lib/…". youwillneedto replacethatpathwithyoursystempath.UsingC:\Snort\lib

14. Changethepathofthe"dynamicengine"variablevalue inthe"snort.conf"file.. Example:
dynamicengineC:\Snort\lib\snort_dynamicengine\sf_engine.dll

15Addthepathsfor"includeclassification.config"and"includereference.config"files.
includec:\snort\etc\classification.configinclu
dec:\snort\etc\reference.config

16. Removethecomment(#)onthelinetoallowICMPrules, ifitiscommentedwitha#.
include$RULE_PATH/icmp.rules

17. YoucanalsoremovethecommentofICMP-inforulescomment,ifitiscommented.
include$RULE_PATH/icmp-info.rules

18. Toaddlogfilestostorealertsgeneratedbysnort,searchforthe"outputlog"test insnort.confandaddthefollowingline:
outputalert_fast:snort-alerts.ids

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

Changethenested_ipinner,\tonested_ipinner#,\

20. Comment out (#) following lines:#preprocessornormalize_ip4
#preprocessornormalize_tcp:ipsecnstream#
preprocessornormalize_icmp4#preprocessor
normalize_ip6
#preprocessornormalize_icmp6

21. Savethe“snort.conf”file.
22. TostartsnortinIDSmode,runthefollowingcommand:

snort-c c:\snort\etc\snort.conf-lc:\snort\log-
i3(Note:3isusedformyinterfacecard)

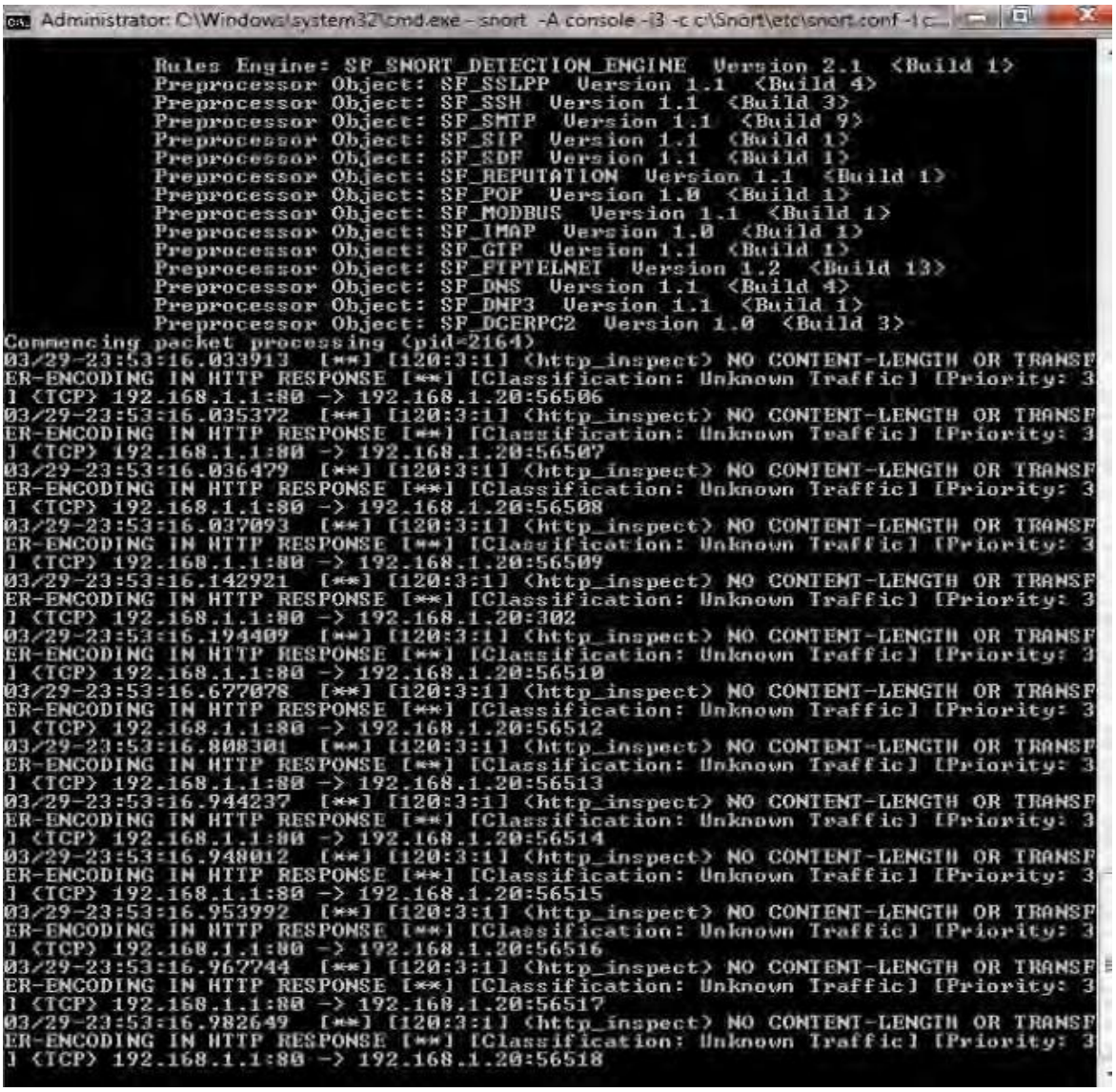
Ifalogiscreated,selecttheappropriateprogramtoopenit.YoucanuseWordPard orNotePad++toread thefile.

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

23. Scanthecomputerthatisrunningsnortfromanothercomputerbyusing PINGorNMap(ZenMap).

After scanning or during the scan you can check the snort-alerts.ids file in the logfoldertoinsureitisloggingproperly.YouwillseeIPaddressfoldersappear.

Snortmonitoringtraffic



Exercise: Demonstrate intrusion detection system to detect and alert on potential security breach

RESULT:

Thus the Intrusion Detection System(IDS) has been demonstrated by usingtheOpenSourceSnortIntrusionDetectionTool.

Ex.No:7 Date :	ExploringN-Stalker,aVulnerabilityAssessmentTool

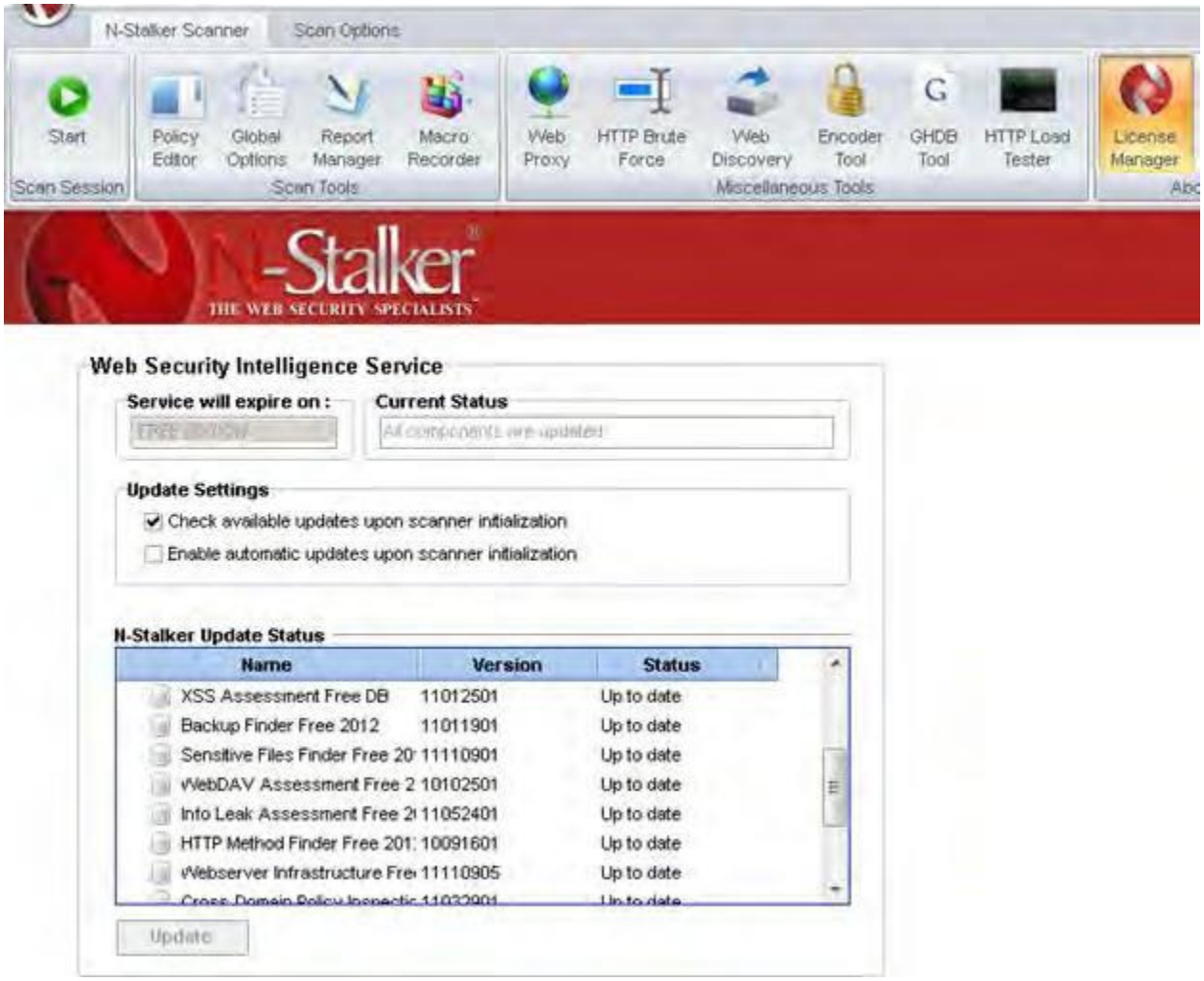
AIM:

TodownloadtheN-StalkerVulnerabilityAssessment Toolandexploringthe features.

EXPLORINGN-STALKER:

- N-StalkerWebApplicationSecurityScannerisaWebsecurityassessmenttool.
- Itincorporates withawell-knownN-StealthHTTPSecurityScannerand35,000Web attacksignaturedatabase.
- Thistoolalsocomesinbothfreeandpaid version.
- Beforescanningthetarget,goto“LicenseManager”tab, performtheupdate.
- Onceupdate, youwillnotethestatusasuptodate.
- YouneedtodownloadandinstallN-Stalkerfromwww.nstalker.com.

1. StartN-StalkerfromaWindowscomputer.TheprogramisinstalledunderStart➪Programs➪N-Stalker➪N-StalkerFreeEdition.
2. Enterahostaddressorarangeofaddressestoscan.
3. ClickStartScan.
4. Afterthescancompletes, theN-StalkerReportManagerwillprompt
5. youtoselectaformatfortheresultingreportaschooseGenerateHTML.
6. ReviewtheHTMLreportforvulnerabilities.



Nowgoto“ScanSession”,enterthetargetURL.

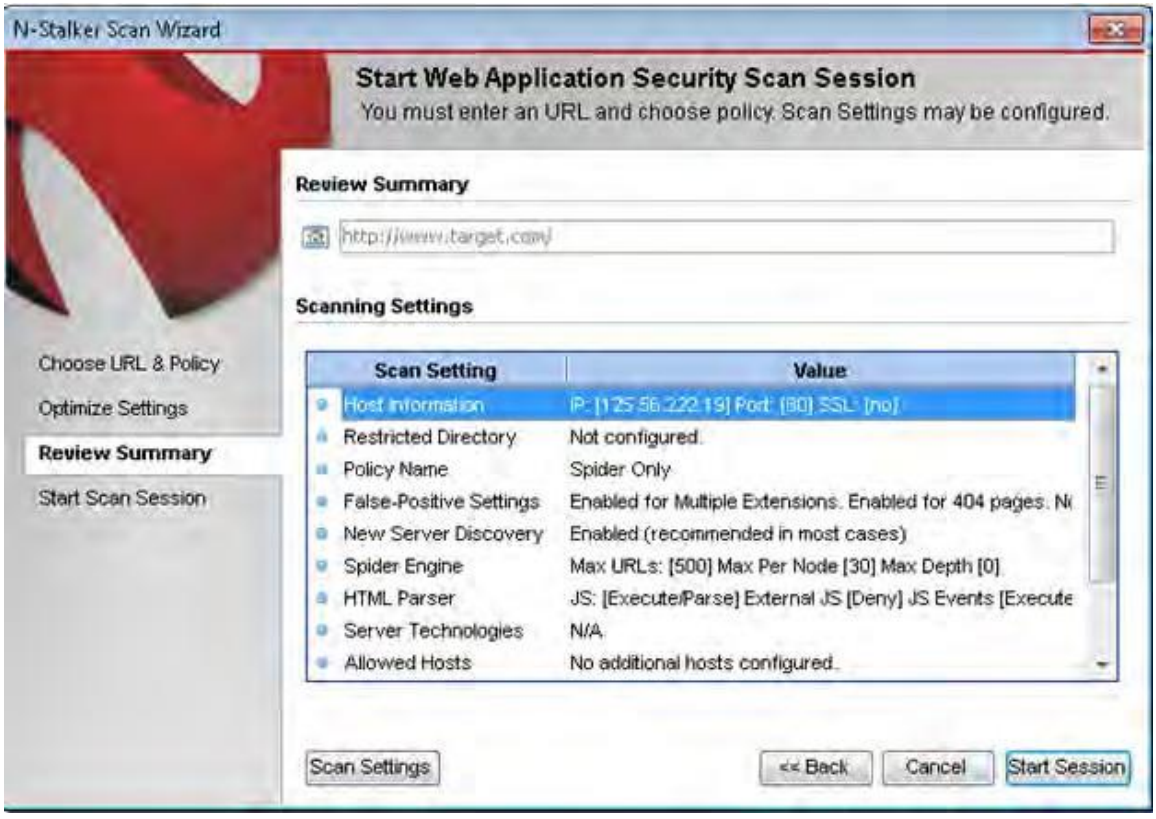
Inscanpolicy, youcanselectfromthefouroptions,

- Manualtestwhichwillcrawlthewebsiteandwillbewaitingformanualattacks .
- fullxssassessment
- owasppolicy
- Webserverinfrastructureanalysis.

Once,theoptionhasbeenselected,nextstepis“Optimizesettings”whichwillcrawlthewholewebsiteforfurtheranalysis.

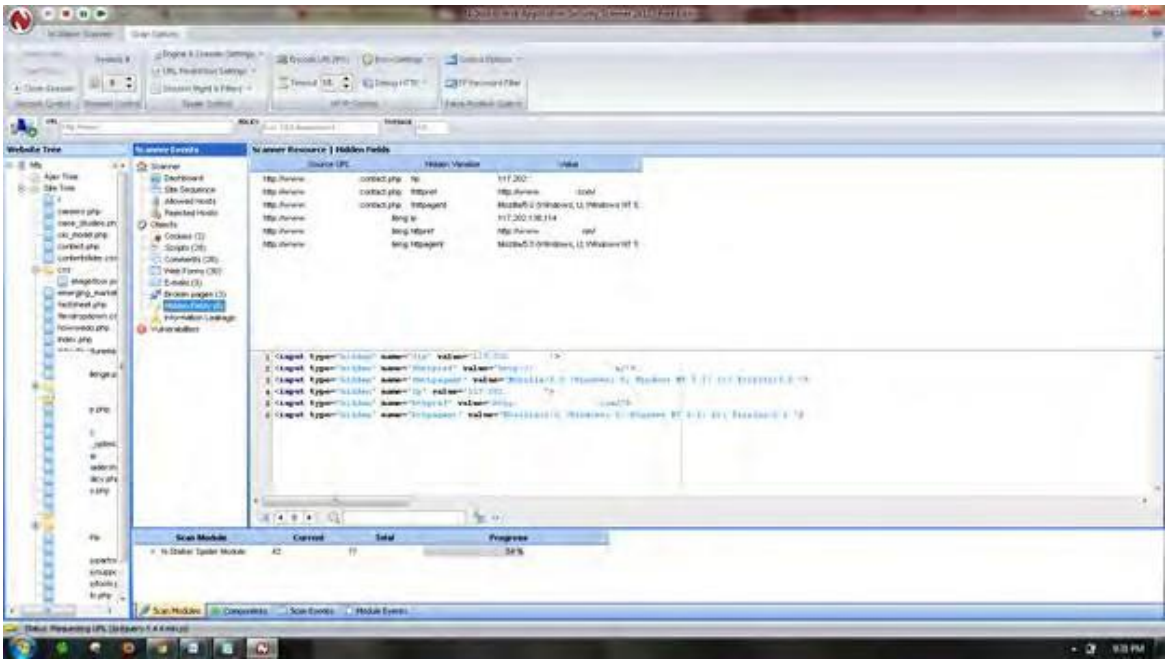
Inreviewoption,youcangetalltheinformationlikehostinformation,technologiesused,policyname,etc.


N-Stalker Scan Wizard
Start Web Application Security Scan Session
You must enter an URL and choose policy. Scan Settings may be configured.
Enter Web Application URL
www.target.com
(E.g: http://www.example.tl/, https://www.test.tl/VirtualDirectory/, etc)
Choose Scan Policy
(choose one)
Load Scan Session
(choose one)
(You may load scan settings from previously saved scan sessions)
Load Spider Data
(You may load spider data from previously saved scan sessions)
Choose URL & Policy
Optimize Settings
Review Summary
Start Scan Session
Scan Settings
Cancel
Next >>

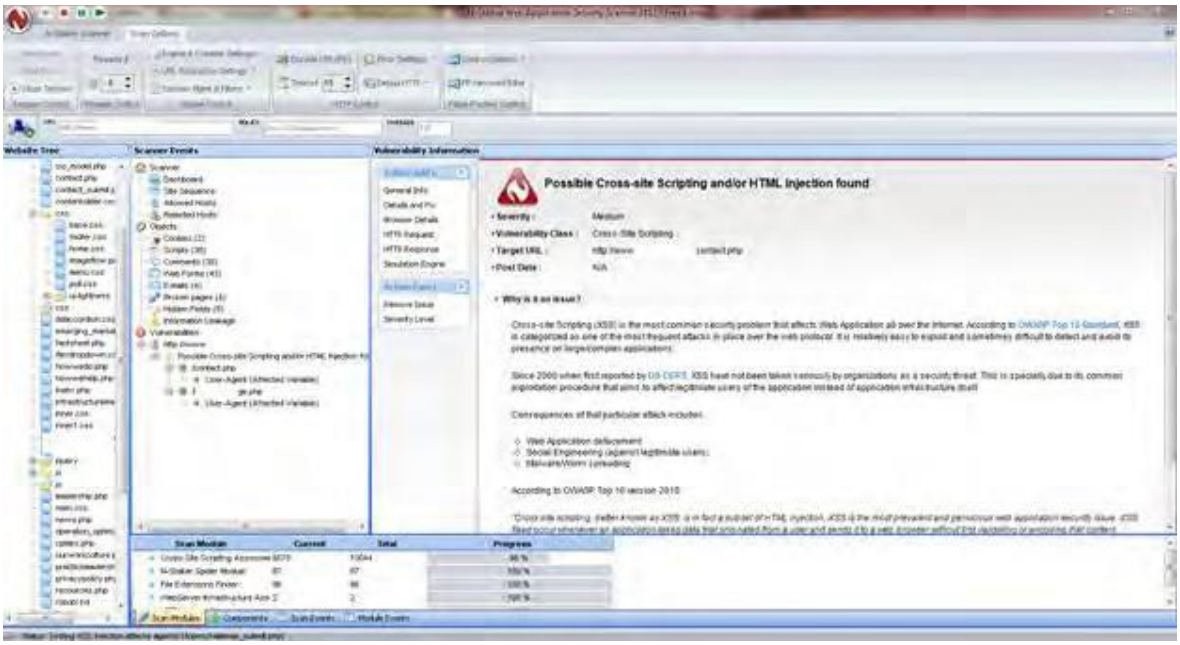

N-Stalker Scan Wizard
Start Web Application Security Scan Session
You must enter an URL and choose policy. Scan Settings may be configured.
Review Summary
http://www.target.com/
Scanning Settings
Scan Setting
Value
Host Information
IP: [125.56.222.19] Port: [80] SSL: [no]
Restricted Directory
Not configured.
Policy Name
Spider Only
False-Positive Settings
Enabled for Multiple Extensions. Enabled for 404 pages. N
New Server Discovery
Enabled (recommended in most cases)
Spider Engine
Max URLs: [500] Max Per Node [30] Max Depth [0]
HTML Parser
JS: [Execute/Parse] External JS [Deny] JS Events [Execute
Server Technologies
N/A
Allowed Hosts
No additional hosts configured.
Choose URL & Policy
Optimize Settings
Review Summary
Start Scan Session
Scan Settings
<< Back
Cancel
Start Session

Oncedone,startthesessionandstartthescan.

Thescannerwillcrawlthewholewebsiteandwillshowthescripts, brokenpages,hidden fields, information leakage, web forms related information which helps toanalyzefurther.



Oncethescaniscompleted,theNStalkerscannerwillshowdetailslikeseveritylevel, vulnerability class, why is it an issue, the fix for the issue and the URLwhich isvulnerableto theparticularvulnerability?



Exercise: To download the N-stalker Vulnerability tool and exploring the features

RESULT:

ThustheN-StalkerVulnerabilityAssessmenttoolhasbeendownloaded,installedandthefeatureshasbeenexploredbyusingavulnerablewebsite.

Ex.No:8(a) Date :	DefeatingMalware -BuildingTrojans

AIM:

TobuildaTrojanandknowtheharmness ofthetrojanmalwaresinacomputer system.

PROCEDURE:

1. CreateasimpletrojanbyusingWindowsBatchFile(***.bat***)
2. Typethesebelowcodeinnotepadandsaveitas**Trojan.bat**
3. Doubleclickon***Trojan.bat***file.
4. Whenthetrojancodeexecutes, itwillopenMS-Paint,Notepad, CommandPrompt,Explorer,etc.,infinitely.
5. Restartthecomputertostoptheexecutionofthistrojan.

TROJAN:

- Incomputing, aTrojanhorse,ortrojan,isanymalwarewhichmisleadsusersofitstrueintent.

- Trojans are generally spread by some form of social engineering, forexamplewhereauser isdupedintoexecutinganemailattachmentdisguisedto appear not suspicious, (e.g., a routine form to be filled in), or by clickingonsomefakeadvertisementon social media oranywhereelse.

- Although their payload can be anything, many modern forms act as abackdoor, contacting a controller which can then have unauthorized accessto theaffectedcomputer.
- Trojansmayallowanattackertoaccessusers'personalinformationsuchasbanki ng information,passwords,orpersonal identity.

- ***Example:****Ransomware*attacksareoftencarriedoutusinga*trojan*.

CODE:

Trojan.bat

```
@echooff
:x
start
mspaintstart
notepadstart
cmdstart
explorerstart
controlstart
calcgoto x
```

OUTPUT

(MS-Paint,Notepad,CommandPrompt,Explorerwillopeninfinitely)

Exercise: i)Perform wireless audit on an access point or a router and decrypt WEP andWPA.(NetStumbler)

RESULT:

Thusatrojanhasbeenbuiltandtheharmnessofthetrojanviruseshasbeenexplored.

Ex.No:8(b) Date :	DefeatingMalware-Rootkithunter

AIM:

Toinstallarootkithunterandfindthemalwaresinacomputer.

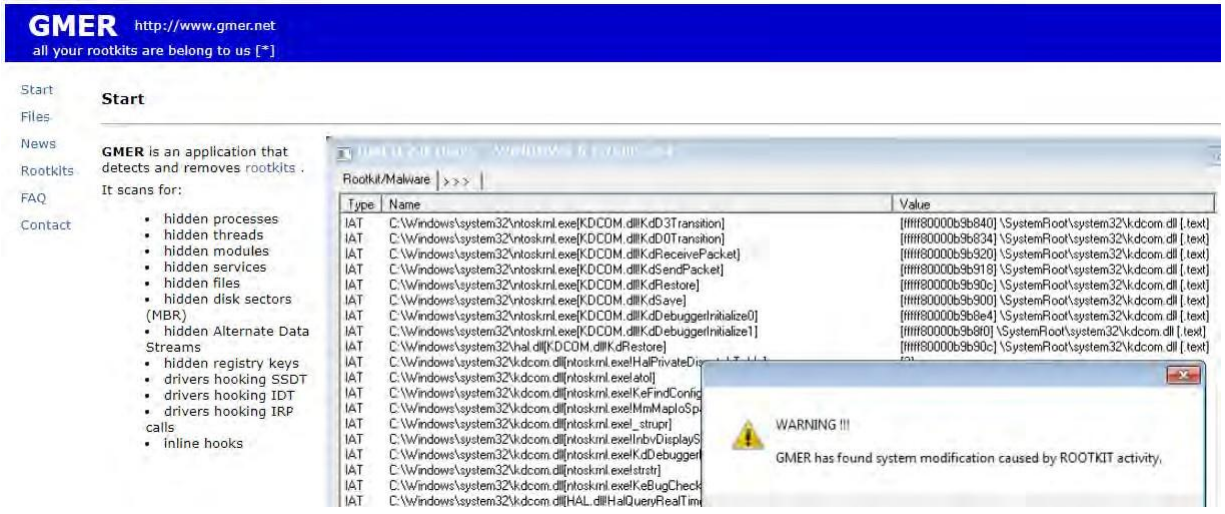
ROOTKITHUNTER:

- rkhunter(RootkitHunter)isaUnix-basedtoolthatscansforrootkits,backdoorsand possiblelocalexploits.
- ItdoesthisbycomparingSHA-1hashesofimportantfileswithknowngoodones in online databases, searching for default directories (of rootkits),wrong permissions, hidden files, suspicious strings in kernel modules, andspecialtestsforLinuxandFreeBSD.
- rkhunterisnotableduetoitsinclusioninpopularoperatingsystems(Fedora,Debian,etc.)
- ThetoolhasbeenwritteninBourneshell, toallowforportability. ItcanrunonalmostallUNIX-derived systems.

GMERROOTKITTOOL:

- GMERisasoftwaretoolwrittenbyaPolishresearcherPrzemysławGmerek,fordetectingand removingrootkits.
- ItrunsonMicrosoftWindowsand hassupport forWindowsNT,2000,XP,Vista, 7, 8 and 10. With version 2.0.18327 full support for Windows x64 isadded.

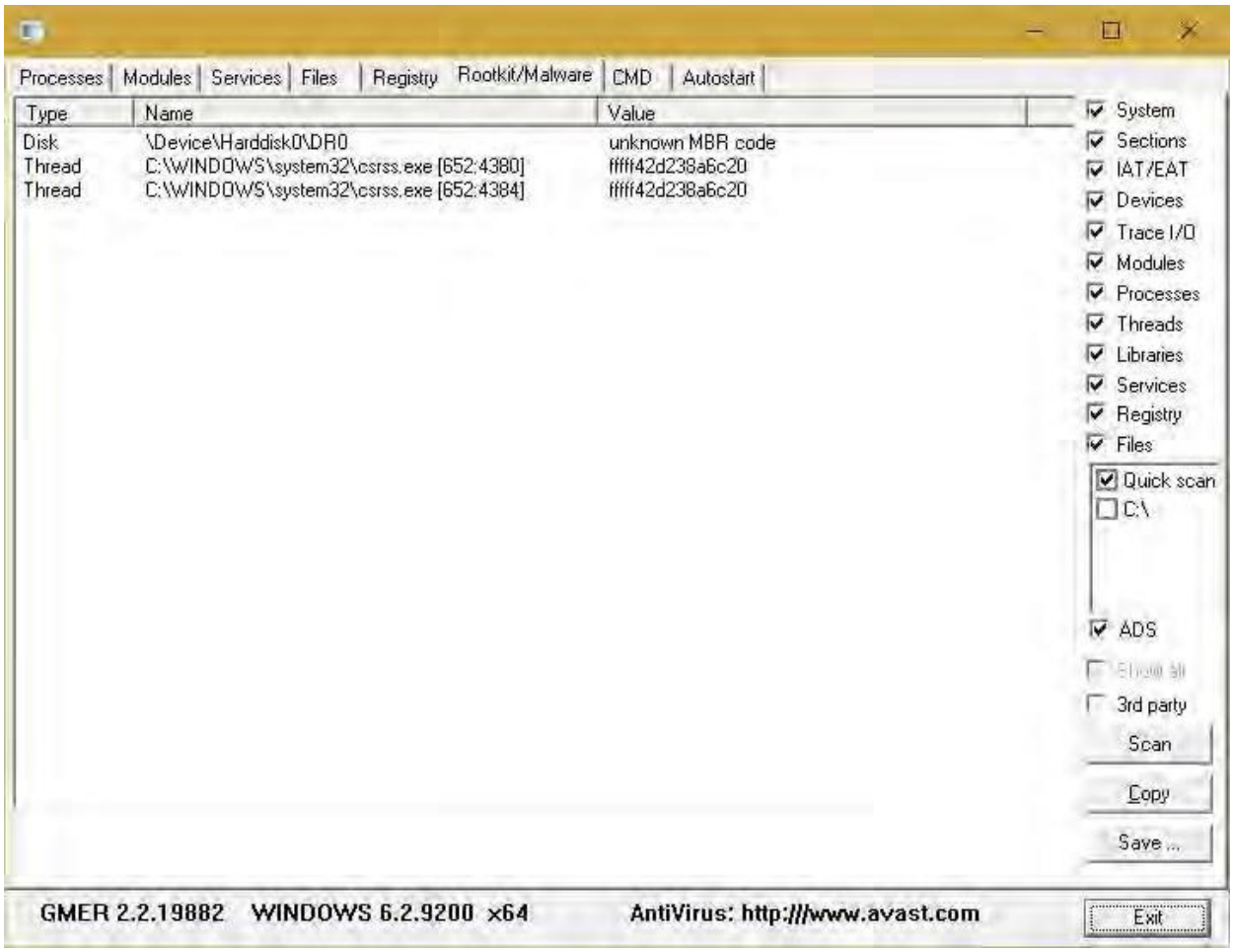
Step1



VisitGMER'swebsite(seeResources)and downloadtheGMERexecutable.

Clickthe"DownloadEXE"buttontodownloadtheprogramwitharandomfilename,asso me rootkitswillclose “gmer.exe”beforeyoucanopenit.

Step2

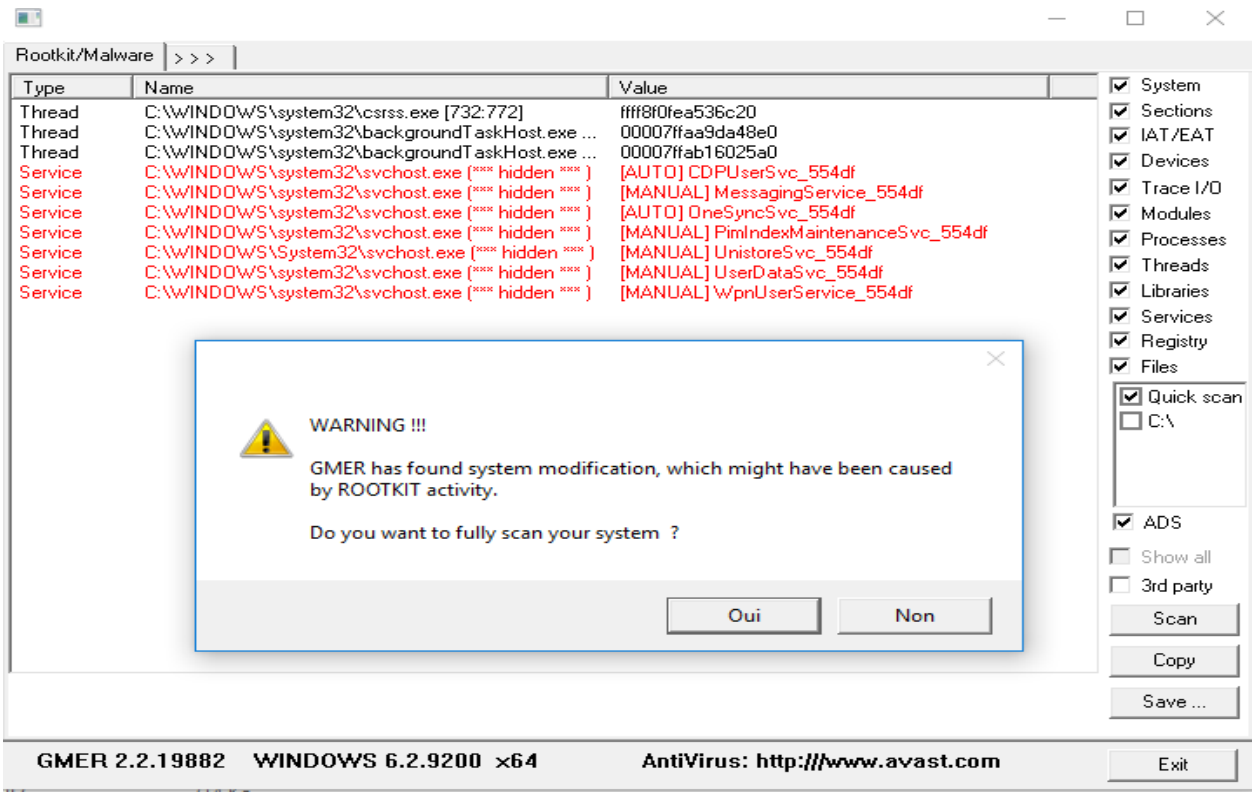


Double-clicktheiconfortheprogram.

Clickthe"Scan"buttoninthelower-rightcornerofthedialogbox.Allowtheprogramtoscanyourentireharddrive.

Step3

Whentheprogramcompletes itsscan, selectanyprogramorfilelistedinred.Right-clickitand select"Delete."



Ifthereditemisaservice,itmaybeprotected.Right-clicktheserviceandselect"Disable." Reboot your computer and run the scan again, this time selecting"Delete"whenthat serviceisdetected.

WhenyourcomputerisfreeofRootkits,closetheprogramandrestartyourPC.

Exercise: Demonstrate the Installation of Root kit Hunter and find the malwares in a computer

RESULT:

Inthisexperimentarootkit huntersoftwaretoolhasbeeninstalledandtherootkitshavebeendetected.

REFERENCES

- **WikiPedia**
  - https://en.wikipedia.org/wiki/GMER
  - https://en.wikipedia.org/wiki/Snort_(software)
  - https://en.wikipedia.org/wiki/Trojan_horse_(computing)

- **GeeksForGeeks**
  - https://www.geeksforgeeks.org/rsa-algorithm-cryptography/
  - https://www.geeksforgeeks.org/sha-1-hash-in-java/
  - https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/
  - https://www.geeksforgeeks.org/how-to-solve-rsa-algorithm-problems/
  - https://www.geeksforgeeks.org/playfair-cipher-with-examples/

- **BuildYourOwnSecurityLab,MichaelGregg,WileyIndia**
  - https://doc.lagout.org/security/Build%20Your%20Own%20Security%20Lab%20for%20Network%20Testing.pdf

- **SomeotherWebsites**
  - https://forums.malwarebytes.com/topic/200301-sneaky-rootkit-help-needed/
  - https://itstillworks.com/use-gmer-remove-rootkit-6102694.html

---