SECURITY LAB MODEL PRATICAL

BATCH : 4

NAME : T . YOKESH

REG NO : 211517205123

ROLL NO : 2017PITIT223

SUB-CODE : IT8761

DEGREE/BRANCH : B.Tech /IT

DATE : 10/11/2020[AN]

Security Lab model pratical

T. YOKESH
2017PITIT223
10/11/2020

1. Hill cipher :-

Aim :-
to implement a program to encrypt and decrypt using hill cipher substitution technique

Algorithm :-
1. In the hill cipher each letter is represented by a number modulo 26.
2. to encrypt a message, each block of n letters is multiplied by an invertible n x n matrix again modulus 26.
3. to decrypt the message, each block is multiplied by inverse of matrix.
4. the matrix used for encryption is the cipher key and it should be choosen randomly
5. the cipher can be adapted to an alphabet with any number of letters.
6. All arithmetic just needs to be done modulo the number of letters instead of modulo 26.

Program :-

Hillcipher.java

```
class hillcipher
{
Public static int [][] keymat = new int [][]
        {{1,2,1},{2,3,2},{2,2,3}};
Public static int [][] invkeymat = new int [][]
        {{-1,0,1},{2,-1,0},
        {-2,2,-1}};
Public static String key = "ABCDEFGHIJKLMNOPQRS
        UUWXYZ";
private static string encode (char a, char b, char c)
{
  string ret = " ";
  int x, y, z;
  int posa = (int) a - 65;
  int posb = (int) b - 65;
  int posc = (int) c - 65;
x = posa * keymat[0][0] + posb * keymat[1][0]
        + posc * keymat[2][0];
y = posa * keymat[0][1] + posb * keymat[1][1] +
        posc * keymat[2][1];

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

```
private static string decode (char a, char b, char c)
{
  string ret = "";
    int x, y, z;
  int posa = (int) a - 65;
  int posb = (int) b - 65;
  int posc = (int) c - 65;
  x = posa * inykeymat[0][0] + posb * inykeymat[1][0]
                + posc * inykeymat[2][0];
  y = posa * inykeymat[0][1] + posb * inykeymat[1][1]
                + posc * inykeymat[2][1];
  z = posa * inykeymat[0][2] + posb * inykeymat[1][2]
                + posc * inykeymat[2][2];
  a = key.charAt((x%.26<0)?(26+x%.26):
                (x%.26));
  b = key.charAt((y%.26<0)?(26+y%.26):
                (y%.26));
  ret = "" + a + b + c;
  return ret;
}
public static void main (String[] args) throws
                java.lang.Exception
{
  string msg;
  string inc = "";
  string dec = "";
  int n;
```

```
msg = "security laboratory";
System.out.println("simulation of hill cipher");
System.out.println("input message : "+msg);

msg = msg.toUpperCase();
msg = msg.replaceAll("JS", "");

if(n)=0){
for(int i=1; i<=(3-n); i++){
    msg+='x';
}
}
System.out.println("padded message :"+msg);
char[] pdchars = msg.toCharArray();
for(int i=0; i<msg.length(); i+=3)
{ enc+= encode(pdchars[i], pdchars[i+1],
                pdchars[i+2]);
}
System.out.println("encoded msg : "+msg)
char[] dechars = enc.toCharArray();
for(int i=0; i<enc.length(); i+=3)
{ dec+= decode(dechars[i], dechars[i+1],
                dechars[i+2]);
}
System.out.println("decode msg:"+msg);

}
}
```

output :-

simulating hill cipher

- - - - - - -

input message : security laboratory

padded message : security laboratory

encrypted message : EABESDILLCAEFBDUKSXO

decrypted message : security laboratory

Result :-

thus the program for hill cipher encr
and decryption algorithm has been implemented
and output verified successfully.

```
C:\Users\Yokesh\Desktop>java hillCipher
simulation of Hill Cipher
-------------------------
Input message : SecurityLaboratory
padded message :SECURITYLABORATORY
encoded message :EACSDKLCAEFQDUKSXU
decoded message :SECURITYLABORATORY

C:\Users\Yokesh\Desktop>
```

2- Exploring N-Stalker, a Vulnerability assessment tool.

Aim:-
To download the N-Stalker Vulnerability assessment tool and exploring the features.

Exploring N-Stalker:

* N-Stalker web application security scanner is a web security assessment tool
* It incorporates with a well known stealth HTTP security scanner and 35,000 web attack signature database.
* This tool is available in both free and paid version.
* once update you will note the status as upto the date.
* you need to download from www.nstalker.com

1. Start N-Stalker from a windows compu
start -> programs -> N-Stalker -> N-Stalker fre
edition.

2. Enter a host or range of address to scan
3. click start scan.
4. After scan the N-Stalker report manag
will prompt.
5. select a format for generating repo
6. Review the html report for vulner

Now goto "scan session", enter the target url

In scan policy, you can from the bar options.

* manual test which will crawl the websites and waiting bar manual attacks.
* full xss assessment
* owasp policy.
* webservices infrastructure analysis

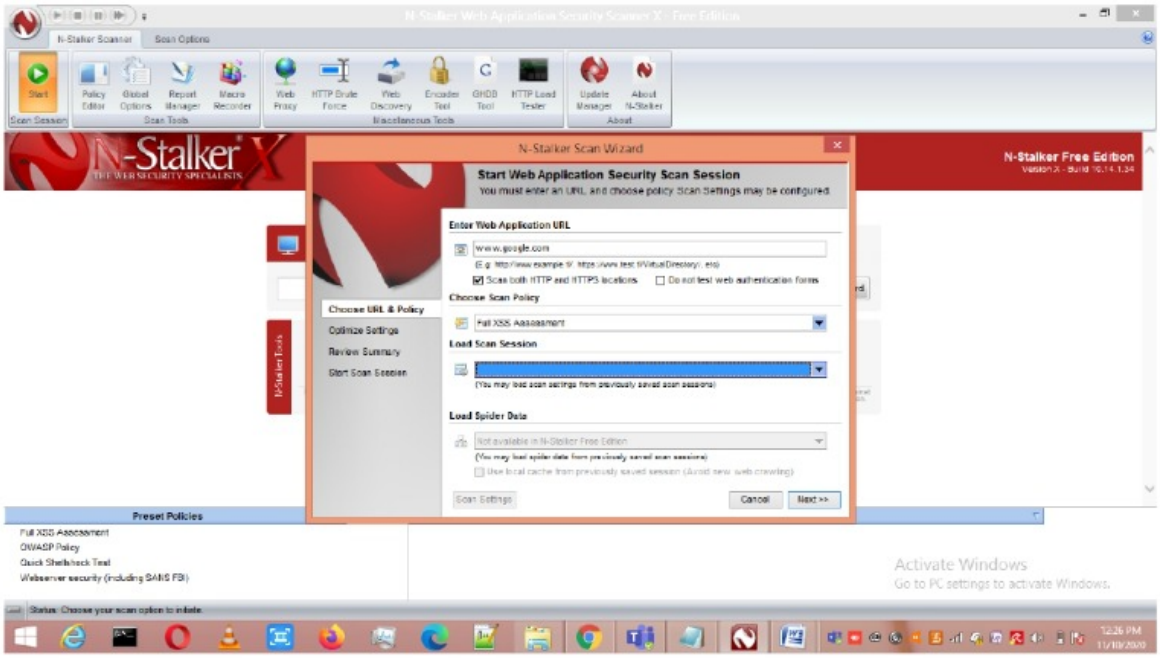
Once done, start the session and start scan

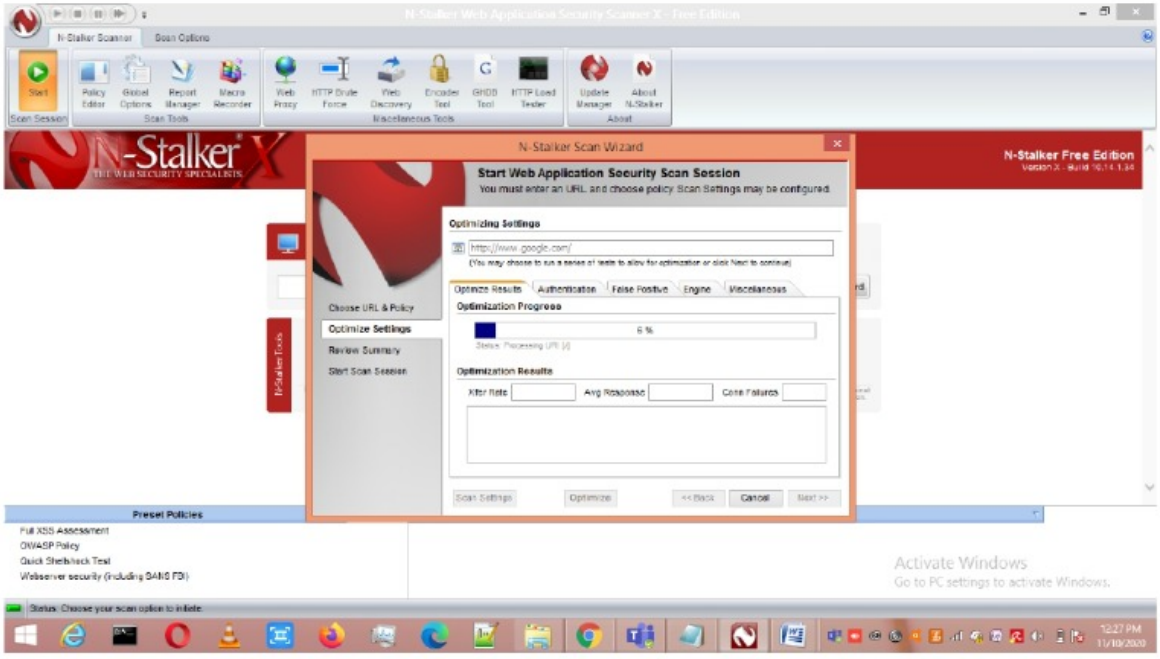
the scanner will crawl the whole website and will show the scripts, broken pages, hidden fields, information leakage, vulnerability related information which help to analyze

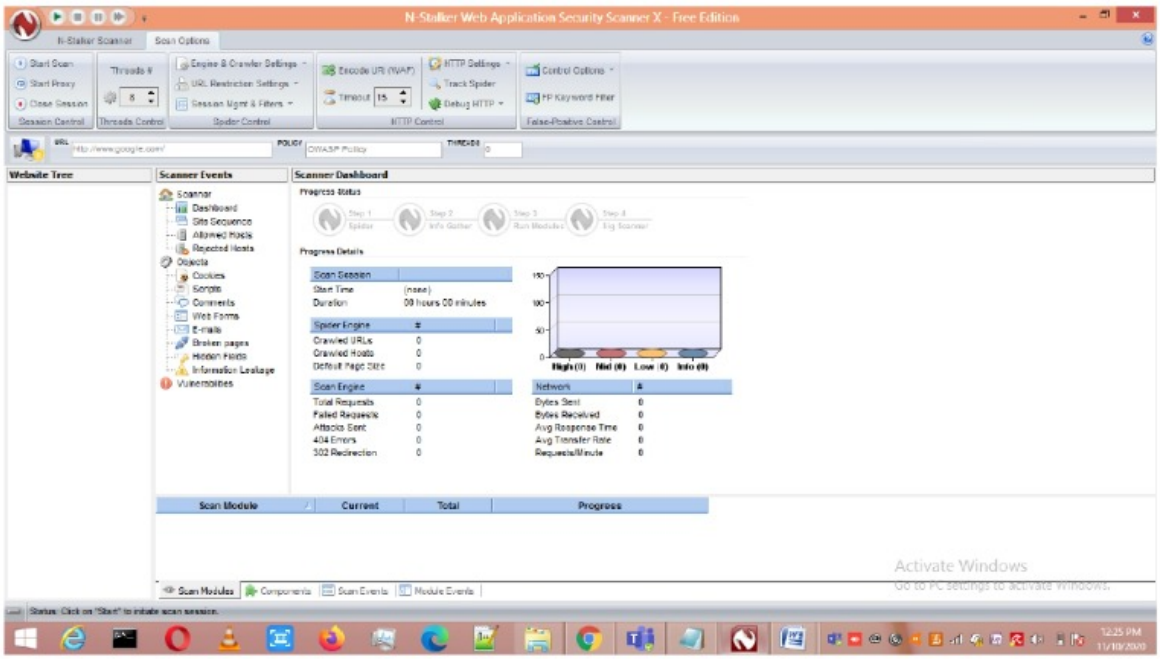
Result :-

Thus the N-Stalker vulnerability assessment tool has been downloaded, installed and the features has been explored by using a vulnerable website.

OUTPUT:


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.google.com
Choose Scan Policy
Full XSS Assessment
Load Scan Session
Load Spider Data
Choose URL & Policy
Optimize Settings
Review Summary
Start Scan Session
Scan Settings
Cancel
Next >>
N-Stalker Free Edition
Preset Policies
Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)
Activate Windows
Go to PC settings to activate Windows.


N-Stalker Scan Wizard
Start Web Application Security Scan Session
You must enter an URL and choose policy. Scan Settings may be configured.
Optimizing Settings
http://www.google.com/
Optimize Results
Authentication
False Positive
Engine
Miscellaneous
Optimization Progress
6 %
Optimization Results
Choose URL & Policy
Optimize Settings
Review Summary
Start Scan Session
Scan Settings
Optimize
<< Back
Cancel
Next >>
N-Stalker Free Edition
Preset Policies
Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)
Activate Windows
Go to PC settings to activate Windows.


N-Stalker Web Application Security Scanner X - Free Edition
N-Stalker Scanner
Scan Options
Website Tree
Scanner Events
Scanner Dashboard
Progress Status
Progress Details
Scan Session
Start Time
(none)
Duration
00 hours 00 minutes
Spider Engine
Crawled URLs
Crawled Hosts
Default Page Dirs
Scan Engine
Total Requests
Failed Requests
Attacks Sent
404 Errors
302 Redirection
Network
Bytes Sent
Bytes Received
Avg Response Time
Avg Transfer Rate
Requests/Minute
Scan Module
Current
Total
Progress
Activate Windows