IV-CSE

EX.NO:7 PERFORM WIRELESS AUDIT ON AN ACCESS POINT
DATE: OR A ROUTER AND DECRYPT WEP AND WPA
USING NETSTUMBLER

AIM:

To perform wireless audit on an access point or a router and decrypt WEP and WPA using NetStumbler.

INTRODUCTION:

NetStumbler is one of the best known and most widely used Wireless Hacking Tools which operates on Windows. This tool is able to list Wireless Access Points and display their basic details such as: SSID, channel, speed, MAC address, vendor, and level of encryption. Unlike other tools in this category, this tool also lists the signal, noise, and signal-to-noise ratio (SNR) levels. Additionally, it has GPS support to record access point locations when wardriving.

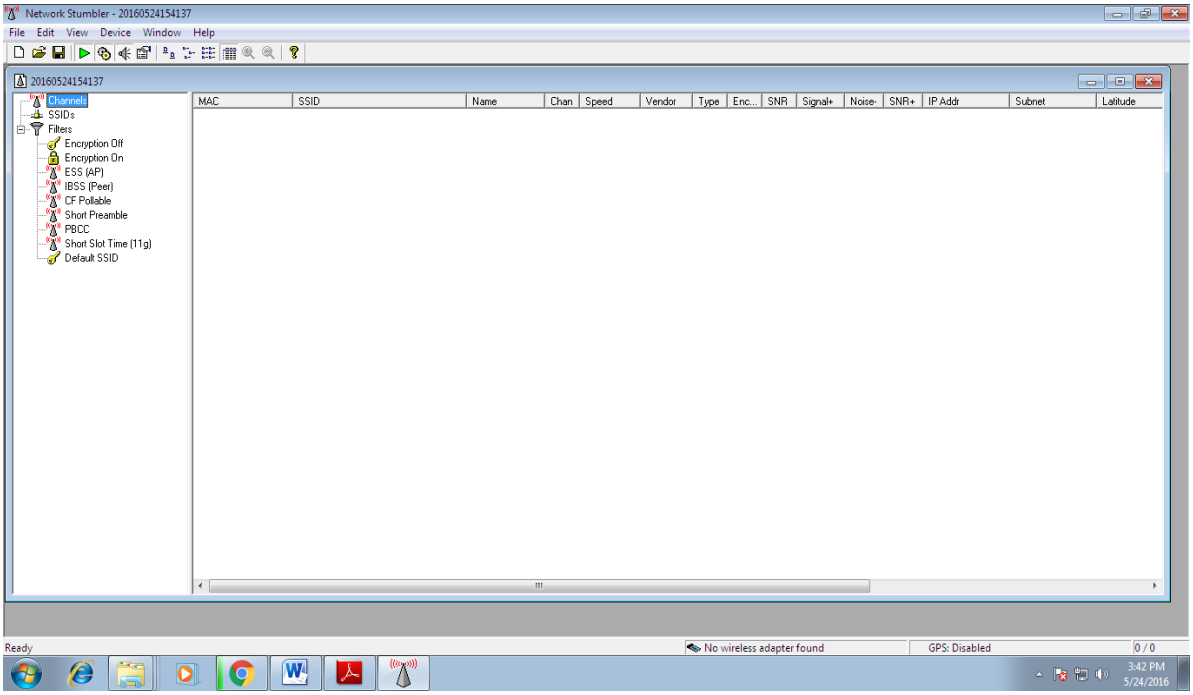
PROCEDURE:

- Download and install Netstumbler
- It is highly recommended that your PC should have wireless network card in order to access wireless router.
- Now Run Netstumbler in record mode and configure wireless card.
- There are several indicators regarding the strength of the signal, such as GREEN indicates Strong, YELLOW and other color indicates a weaker signal, RED indicates a very weak and GREY indicates a signal loss.
- Lock symbol with GREEN bubble indicates the Access point has encryption enabled.
- MAC assigned to Wireless Access Point is displayed on right hand pane.
- The next column displays the Access points Service Set Identifier[SSID] which is useful to crack the password.
- To decrypt use WireShark tool by selecting Edit→preferences→IEEE 802.11
- Enter the WEP keys as a string of hexadecimal numbers as A1B2C3D4E5

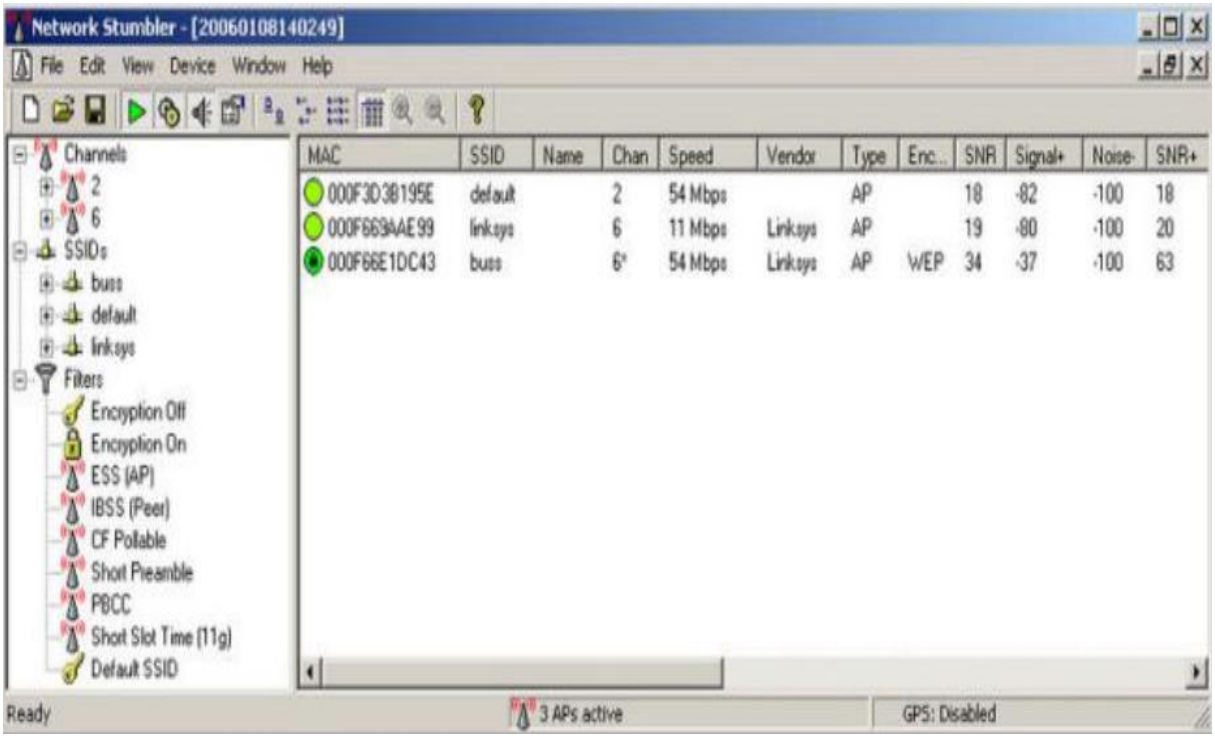
IV-CSE

OUTPUT:

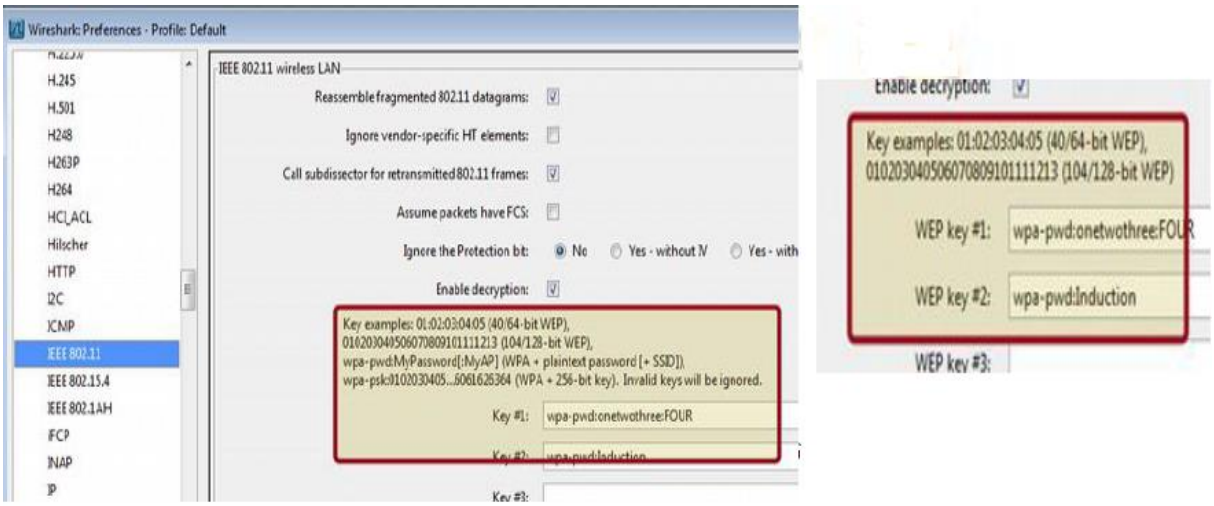
Home page:



Click on the channels icon. It will display the below window showing the MAC, SSID and other details.



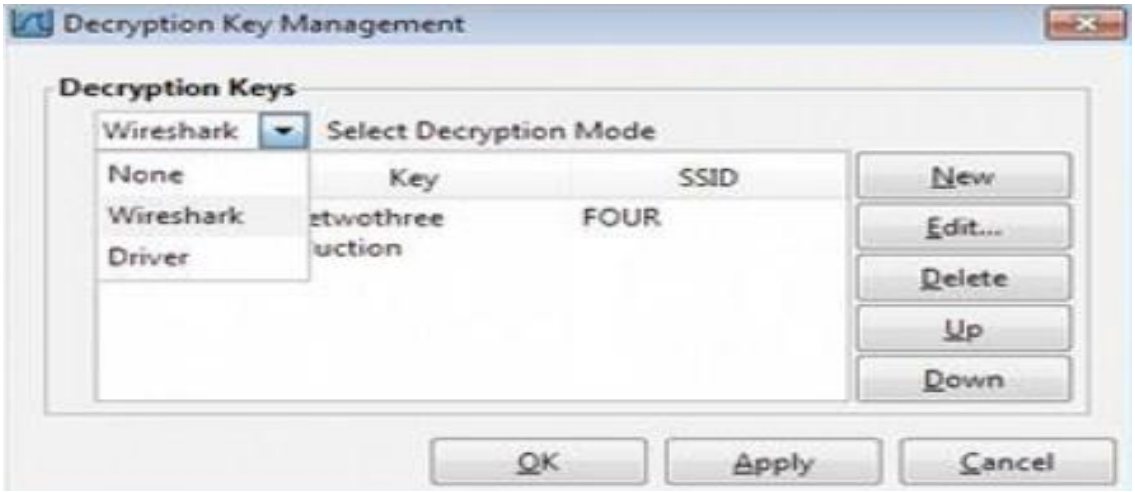
Open the wireshark tool and choose the profile:



Adding Keys: Wireless Toolbar

If you are using the Windows version of Wireshark and you have an AirPcap adapter you can add decryption keys using the wireless toolbar. If the toolbar isn't visible, you can show it by selecting View->Wireless Toolbar. Click on the Decryption Keys... button on the toolbar:

This will open the decryption key management window. As shown in the window you can select between three decryption modes: None, Wireshark, and Driver:



RESULT:

Thus, the implementation of wireless audit on an access point or a router and decrypt WEP and WPA using NetStumbler was executed and verified successfully.

IV-CSE

EX.NO:8 DEMONSTRATE INTRUSION DETECTION SYSTEM (IDs)
DATE: USING SNORT TOOL

AIM:

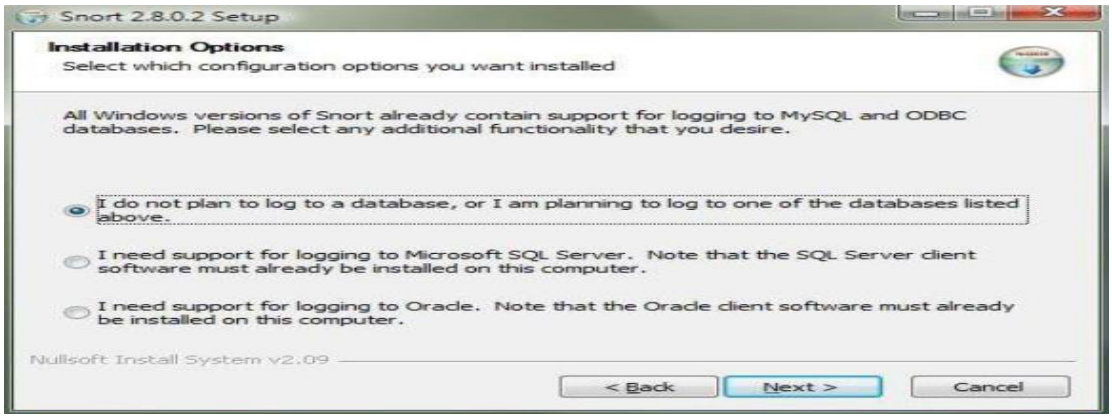
To demonstrate intrusion detection system (ids) using Snort tool.

INTRODUCTION:

Snort is an open source network intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on internet protocol (IP) networks. Snort performs protocol analysis, content searching and matching. Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection.

INSTALLATION PROCEDURE:

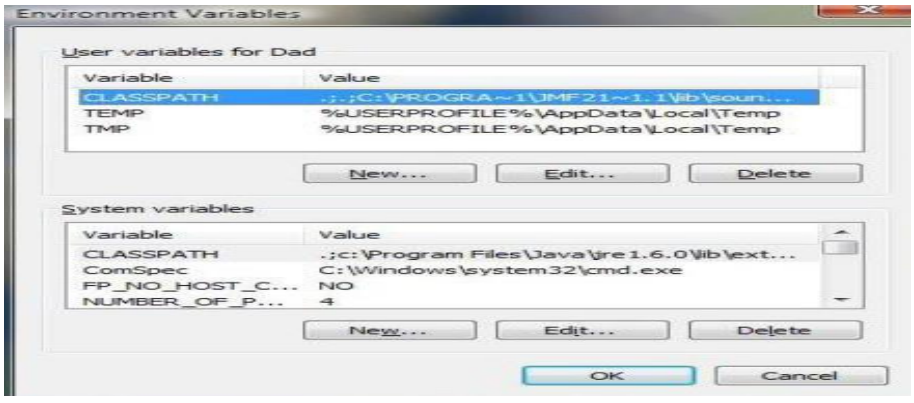
Download and install snort with or without database support.



Select all the components and Click Next.
Install and Close.
Skip the WinPcap driver installation

Add the path variable in windows environment variable by selecting new classpath. Create a path variable and point it at snort.exe

variable name→path and variable value→c:\snort\bin.



Click OK button and then close all dialog boxes.

SNORT CONFIGURATION:

Open command prompt and type the following commands under three modes:
SNORT can be configured to run in three modes:

1. Sniffer mode
2. Packet Logger mode
3. Network Intrusion Detection System mode

To work with these modes,
Choose the snort application from the path C:\Snort\bin and work on the following commands.

SNIFFER MODE:

snort –v : Print out the TCP/IP packets header on the screen
snort –vd : show the TCP/IP ICMP header with application data in transit.

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.

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.

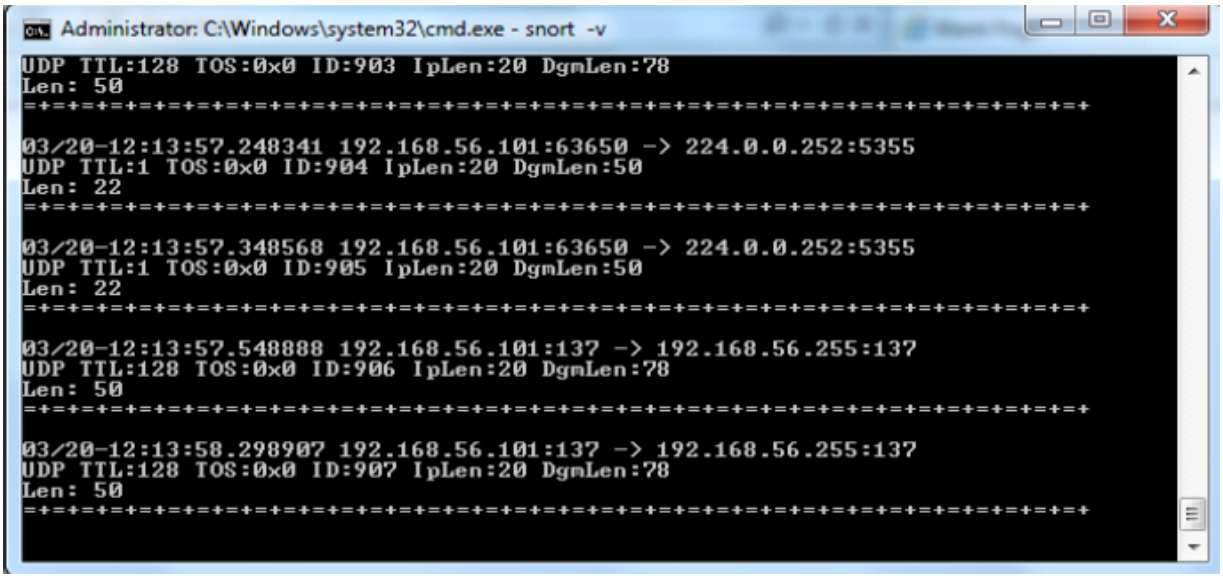
snort –l c:\log –b : This is binary mode logs everything into a single file.

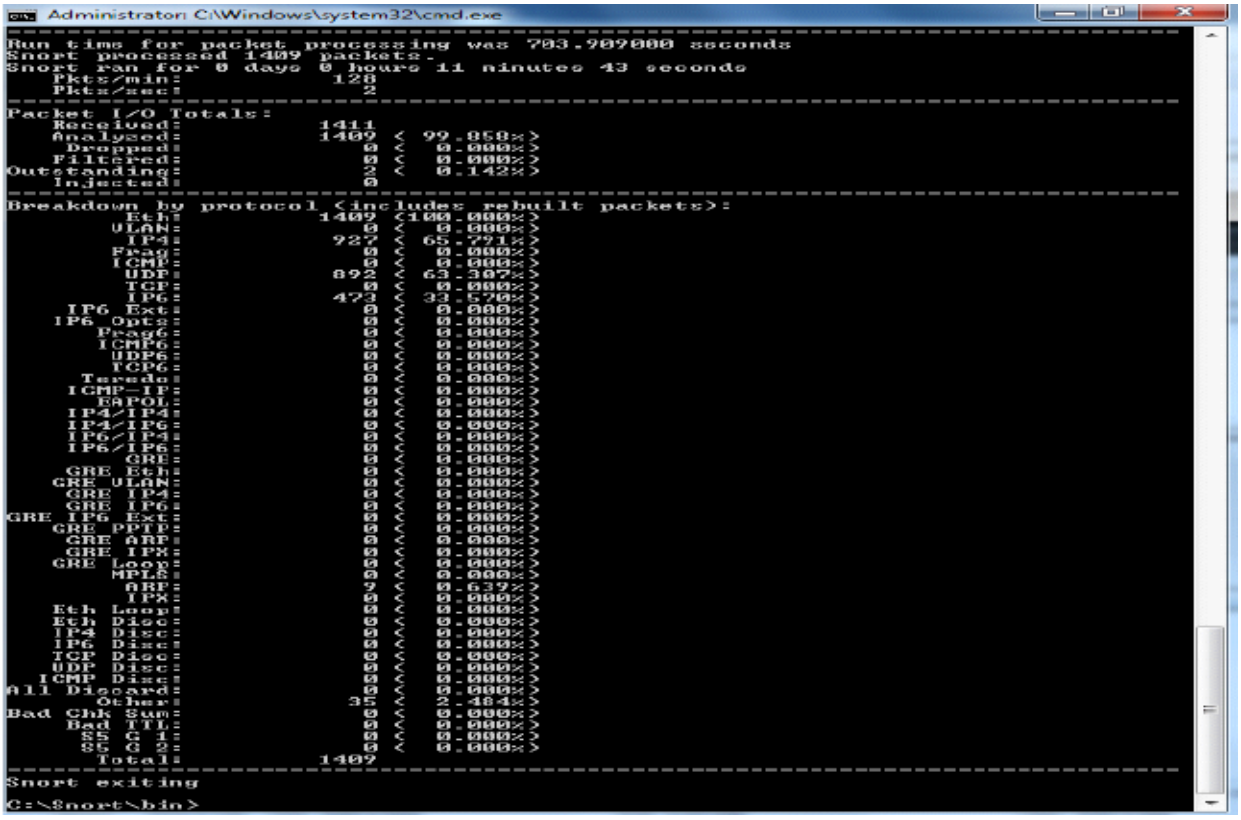
NETWORK INTRUSION DETECTION SYSTEM MODE:

snort –d c:\log –h ipaddress/24 –c snort.conf
This is a configuration file applies rule to each packet to decide it an action based upon the rule type in the file.

snort –d –h ipaddress/24 –l c:\log –c snort.conf
This will configure snort to run in its most basic NIDS form, logging packets that trigger rules specified in the snort.conf

OUTPUT:


Administrator: C:\Windows\system32\cmd.exe - snort -v
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


Administrator: C:\Windows\system32\cmd.exe
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 Intrusion Detection System (ids) using Snort tool was executed and verified successfully.