Intrusion Detection Systems with Snort

Rana M Pir
Lecturer
Leading University, Sylhet Bangladesh

***Abstract*— Network based technology and Cloud Computing is becoming popular day by day as many enterprise applications and data are moving into cloud or Network based platforms. Because of the distributed and easy accessible nature, these services are provided over the Internet using known networking protocols, Protocol standards and Protocol formats under the supervision of different management's tools and programming language. Existing bugs and vulnerabilities in underlying technologies and legacy protocols tend to open doors for intrusion so many Attacks like Denial of Service (DDOS), Buffer overflows, Sniffer attacks and Application-Layer attacks have become a common issue today. Recent security incidents and analysis Have manual response to such attacks and resolve that attacks are no longer feasible. In Internet and Network system application or platform facing various types of attacks in every day. Intrusion Prevention and the IDS tools that are employed to detect these attacks and discuss some open source tools to prevent and detection of intrusion and how can we use Open Source tools in our system. Snort is an open source Network Intrusion Detection System (NIDS) which is available free of cost. NIDS is the type of Intrusion Detection System (IDS) that is used for scanning data flowing on the network. There is also host-based intrusion detection systems, which are installed on a particular host and detect attacks targeted to that host only. Although all intrusion detection methods are still new, Snort is ranked among the top quality systems available today.**

***Index Terms*— Intrusion detection system, Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID**

I. Introduction to Intrusion Detection and Snort

Intrusion detection is the process of monitoring the attacks and events occurring in a computer or network system and analyzing them for signs of possible incidents of attacks, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware, Denial of Service (DDOS), Buffer overflows, Sniffer attacks and Application-Layer attacks), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems and misuse their privileges or attempt to gain additional privileges for which they are not authorized. As network attacks have increased in number and severity over the past few years, intrusion detection systems have become a necessary addition to the security infrastructure of most organizations.

This Paper is intended as a primer in intrusion detection, developed for those who need to understand what security goals intrusion detection mechanisms serve, how to select and configure intrusion detection systems for their specific system and network environments, how to manage the output of intrusion detection systems, and how to integrate intrusion detection functions with the rest of the organizational security infrastructure.

Security is a big issue for all networks in today's enterprise environment. Hackers and intruders have made many successful attempts to bring down high-profile company networks and web services. Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of firewalls, encryption, and virtual private networks. Intrusion detection is a relatively new addition to such techniques. Intrusion detection methods started appearing in the last few years. Using intrusion detection methods, you can collect and use information from known types of attacks and find out if someone is trying to attack your network or particular hosts. The information collected this way can be used to harden your network security, as well as for legal purposes. Both commercial and open source products are now available for this purpose. Many vulnerability assessment tools are also available in the market that can be used to assess different types of security holes present in your network. A comprehensive security system consists of multiple tools, including:

II. Type Types of Attacks

Denial-of-Service (DOS) attacks, It is an attempt to forbid the authorized users from utilizing the requested service/ resource. A more advanced Distributed Denial of Service occurs when in a distributed environment the attacker sends or rather floods the server or a target system with numerous connection requests knocking the target system to the knees, leaving them no other option to restart their system. Some well known DOS attacks are:
SYN Attack where the attacker exploits the inability of the server to handle unfinished connection requests. Server is flooded with connection requests. The server crashes waiting for the acknowledgments of the requests.
Ping of Death where the attacker sends a ping request which is larger than 65,536 bytes which is the maximum allowed size for the IP, causing the system to crash or restart

Logon Abuse attacks, a successful logon abuse attack would bypass the authentication and access control mechanisms and grant a user with more privileges that authorized.

Application-Level Attacks, The attacker exploits the weakness in the application layer – for example, security weakness in the web server, or in faulty controls in the filtering of an input on the server side. Examples include malicious software attack (viruses, Trojans, etc), web server attacks, and SQL injection.

Spoofing attack, the attacker impersonates an legitimate user. IP spoofing is a common example where the system is convinced that it is communicating with a trusted user and provides access to the attacker. The attacker sends a packet with an IP address of a known host by alerting the packet at the transport layer.

Sniffer Attack, A sniffer is an application that can capture network packets. Sniffers are also known as network protocol analyzers. While protocol analyzers are really network troubleshooting tools, they are also used by hackers for hacking network. If the network packets are not encrypted, the data within the network packet can be read using a sniffer. Sniffing refers to the process used by attackers to capture network traffic using a sniffer. Once the packet is captured using a sniffer, the contents of packets can be analyzed. Sniffers are used by hackers to capture sensitive network information, such as passwords, account information etc.

III. Components of Snort

Snort is logically divided into multiple components. These components work together to detect particular attacks and to generate output in a required format from the detection system. A Snort-based IDS consists of the following major components: •

- Packet Decoder
- Preprocessors
- Detection Engine
- Logging and Alerting System
- Output Modules

Figure shows how these components are arranged. Any data packet coming from the Internet enters the packet decoder. On its way towards the output modules, it is either dropped, logged or an alert is generated.

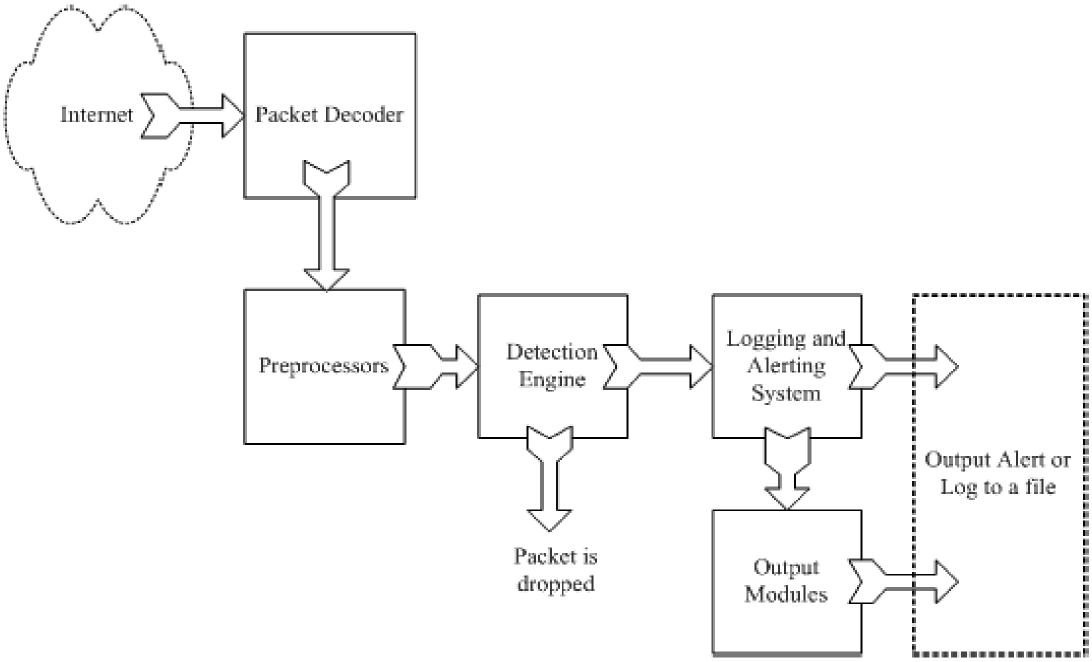


Fig 1 Components of Snort

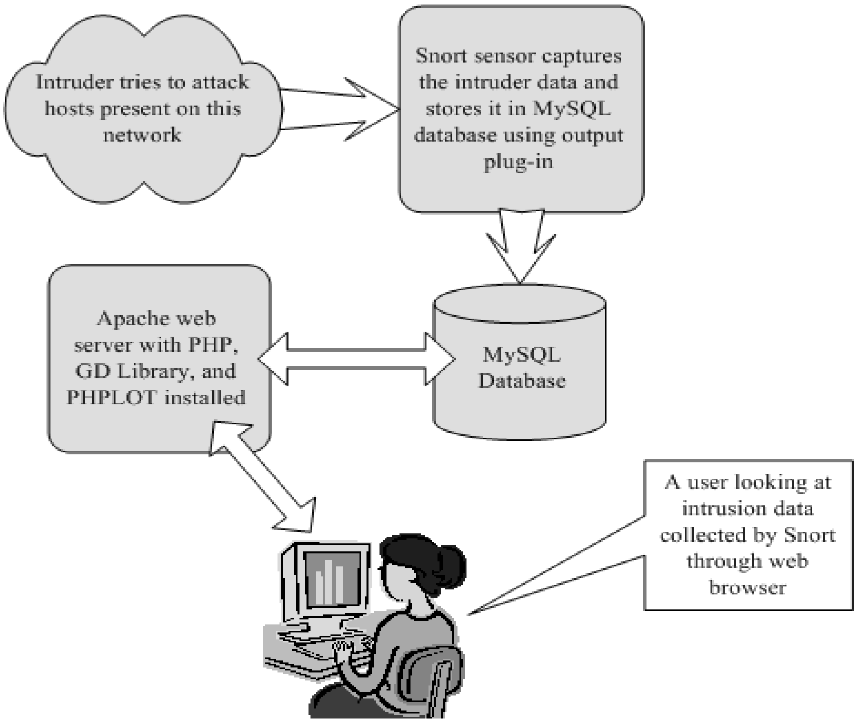

Intruder tries to attack hosts present on this network
Snort sensor captures the intruder data and stores it in MySQL database using output plug-in
Apache web server with PHP, GD Library, and PHPLOT installed
MySQL Database
A user looking at intrusion data collected by Snort through web browser

Fig 2 Block diagram of a complete network intrusion detection system consisting of Snort, MySQL, Apache, ACID, PHP

Snort Installation Scenarios

- Test Installation
- Single Sensor Production IDS
- Single Sensor with Network Management System Integration
- Single Sensor with Database and Web Interface
- Multiple Snort Sensors with Centralized Database

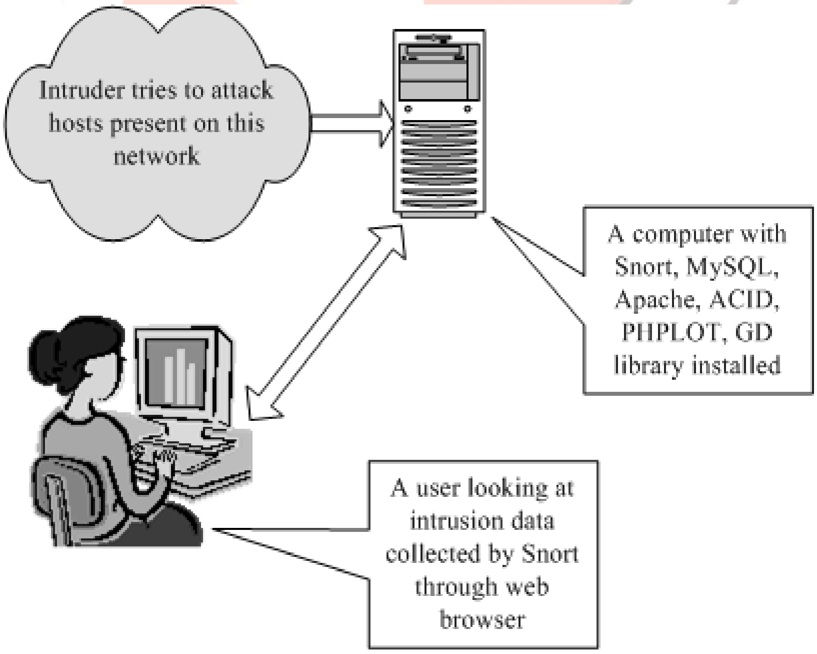

Intruder tries to attack hosts present on this network
A computer with Snort, MySQL, Apache, ACID, PHPLOT, GD library installed
A user looking at intrusion data collected by Snort through web browser

Fig 3 A network intrusion detection system with web interface

IV. Installing Snort and Getting Started

Installing Snort

In this section you will learn how to install precompiled version of Snort as well as how to compile and install it by yourself. Installation of the pre-compiled RPM package is very easy and requires only a few steps. However if you get Snort in source code format, the installation process may take some time and understanding.

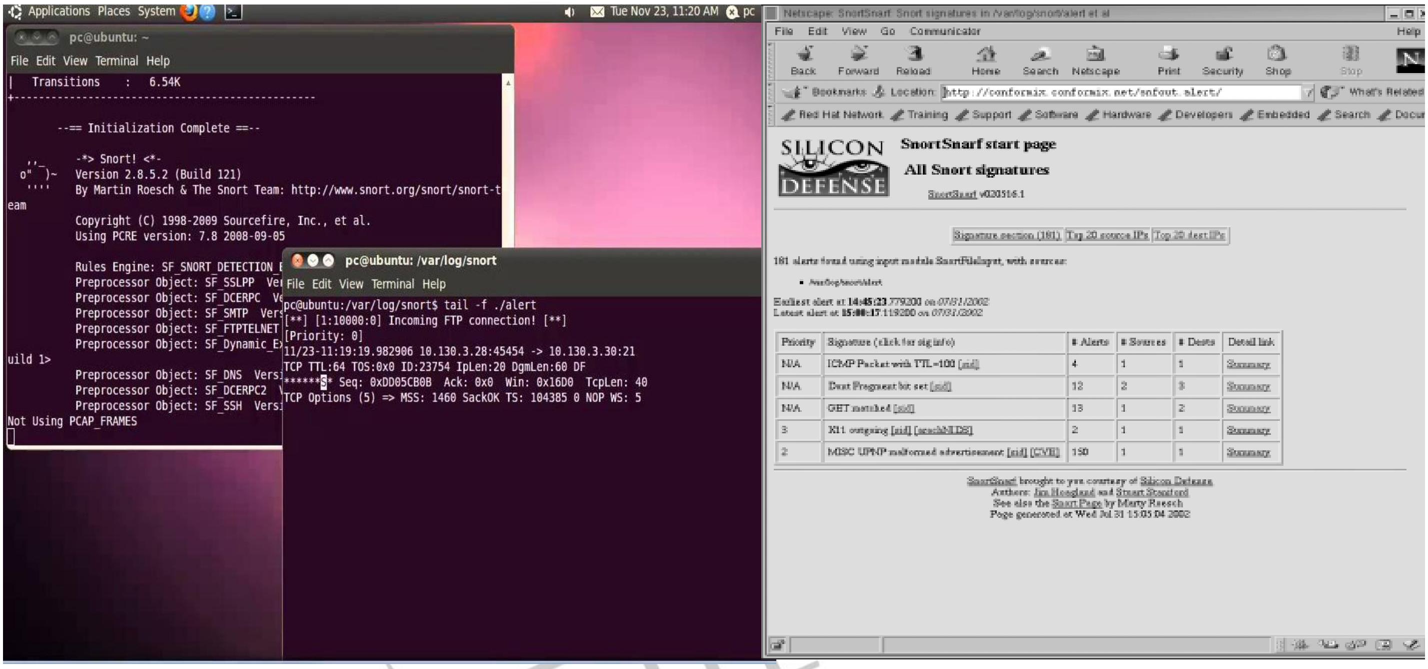
Download

Download the latest version from Snort web site (http://www.snort.org). At the time of writing this book, the latest binary file is snort-1.9.0-1snort.i386.rpm.

Install
Run the following command to install Snort binaries: rpm --install snort-1.9.0-1snort.i386.rpm.

Starting, Stopping and Restarting Snort
To run Snort manually, use the following command:
/etc/init.d/snortd start
This command will start Snort and you can run the Snort daemon using the "ps –ef" command. You should see a line like the following in the output of this command:
root 15999 1 0 18:31 ? 00:00:01 /usr/sbin/
snort -A fast -b -l /var/log/snort -d -D -i eth0 -c /etc/
snort/snort.conf

To stop Snort, use the following command:
/etc/init.d/snortd stop
To restart Snort, use this command:
/etc/init.d/snortd restart


Applications Places System
Tue Nov 23, 11:20 AM pc
pc@ubuntu: ~
File Edit View Terminal Help
pc@ubuntu: /var/log/snort
File Edit View Terminal Help
Netscape: SnortSnarf: Snort signatures in /var/log/snort/alert et al
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: What's Related
Red Hat Network Training Support Software Hardware Developers Embedded Search Docu
SILICON DEFENSE

```
|   Transitions    :   6.54K
+-----------------------------------------------


        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.8.5.2 (Build 121)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 1998-2009 Sourcefire, Inc., et al.
           Using PCRE version: 7.8 2008-09-05

           Rules Engine: SF_SNORT_DETECTION_E
           Preprocessor Object: SF_SSLPP  Ve
           Preprocessor Object: SF_DCERPC  V
           Preprocessor Object: SF_SMTP  Vers
           Preprocessor Object: SF_FTPTELNET
           Preprocessor Object: SF_Dynamic_E
uild 1>
           Preprocessor Object: SF_DNS  Versi
           Preprocessor Object: SF_DCERPC2  V
           Preprocessor Object: SF_SSH  Versi
Not Using PCAP_FRAMES
```

```
pc@ubuntu:/var/log/snort$ tail -f ./alert
[**] [1:10000:0] Incoming FTP connection! [**]
[Priority: 0]
11/23-11:19:19.982906 10.130.3.28:45454 -> 10.130.3.30:21
TCP TTL:64 TOS:0x0 ID:23754 IpLen:20 DgmLen:60 DF
******S* Seq: 0xDD05CB0B  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 104385 0 NOP WS: 5
```

Location: http://conformix.conformix.net/snfout.alert/

SnortSnarf start page

All Snort signatures

SnortSnarf v020516.1

Signature section (181) | Top 20 source IPs | Top 20 dest IPs

181 alerts found using input module SnortFileInput, with sources:

- /var/log/snort/alert

Earliest alert at **14:45:23**.779200 on *07/31/2002*
Latest alert at **15:00:17**.119200 on *07/31/2002*

Priority	Signature (click for sig info)	# Alerts	# Sources	# Dests	Detail link
N/A	ICMP Packet with TTL=100 [sid]	4	1	1	Summary
N/A	Dont Fragment bit set [sid]	12	2	3	Summary
N/A	GET matched [sid]	13	1	2	Summary
3	X11 outgoing [sid] [arachNIDS]	2	1	1	Summary
2	MISC UPNP malformed advertisement [sid] [CVE]	150	1	1	Summary

SnortSnarf brought to you courtesy of Silicon Defense
Authors: Jim Hoagland and Stuart Staniford
See also the Snort Page by Marty Roesch
Page generated at Wed Jul 31 15:03:04 2002

Fig 4 Snort Installation and Starting Page for MySQL and PHP

Snort Modes

- Network Sniffer Mode
- Logging Snort Data in Text Format
- Logging Snort in Binary Format
- Network Intrusion Detection Mode

Snort Alert Modes

Fast Mode
The fast alert mode logs the alert with following information:

- Timestamp
- Alert message (configurable through rules)
- Source and destination IP addresses
- Source and destination ports

To configure fast alert mode, you have to use "-A fast" command line option. This alert mode causes less overhead for the system. The following command starts Snort in fast alert mode:
/opt/snort/bin/snort -c /opt/snort/etc/snort.conf -q -A fast

Full Mode

This is the default alert mode. It prints the alert message in addition to the packet header. Let us start Snort with full alerting enabled with the following command:

```
/opt/snort/bin/snort -c /opt/snort/etc/snort.conf -q -A full
```

UNIX Socket Mode

If you use "-a unsock" command line option with Snort, you can send alerts to another program through UNIX sockets. This is useful when you want to process alerts using a custom application with Snort. For more information on socket, use the "man socket" command.

No Alert Mode

You can also completely disable Snort alerts using "-A none" command line option. This option is very useful for high speed intrusion detection using unified logging. You can disable normal logging using this option while using the unified option.

Sending Alerts to Syslog

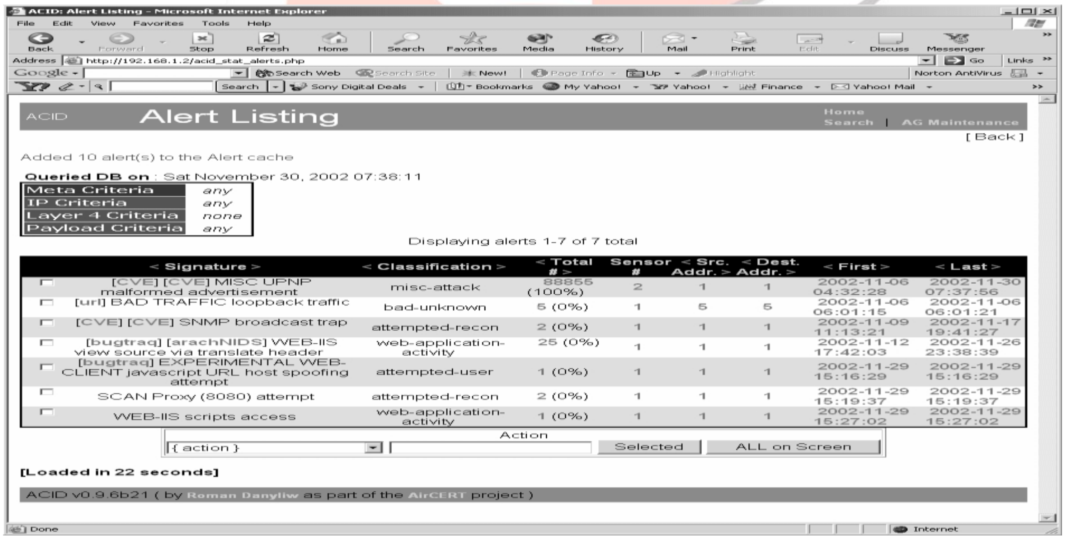
This command allows Snort to send alerts to Syslog daemon. Syslog is a system logger daemon and it generates log files for system events. It reads its configuration file /etc/syslog.conf where the location of these log files is configured. The usual location of syslog files is /var/log directory. On Linux systems, usually /var/ log/messages is the main logging file. For more information, use the "man syslog" command. The "man syslog.conf" command shows the format of the syslog. conf file. Depending on the configuration of the Syslog using /etc/syslog.conf file, the alerts can be saved into a particular file. The following command enables Snort to log to the Syslog daemon: /opt/snort/bin/snort -c /opt/snort/etc/snort.conf –s

Sending Alerts to SNMP

One very useful feature of Snort is SNMP traps. You can configure an output plug-in to send messages in the form of SNMP traps to a network management system. Using this feature you can integrate your intrusion detection sensors into any centralized NMS like HP OpenView, OpenNMS, MRTG and so on. Snort can generate SNMP version 2 and version 3 traps

Sending Alerts to Windows

Snort can send alerts to Microsoft Windows machines in the form of pop-up windows. These pop-up windows are controlled by Windows Messenger Service. Windows Messenger Service must be running on your Windows machine for pop-up windows to work. You can go to Control Panel and start the *Services* applet to find out if Windows Messenger Service is running. The *Services* applet is found in the Administrative Tools menu on your Windows system. Depending on your version of Microsoft Windows, it may be found in Control Panel or some other place


ACID: Alert Listing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss Messenger
Address
Go Links
Google
Search Web Search Site New! Page Info Up Highlight
Norton AntiVirus
Search Sony Digital Deals Bookmarks My Yahoo! Yahoo! Finance Yahoo! Mail
Home
Search | AG Maintenance
[Back]
Selected
ALL on Screen
Done
Internet

http://192.168.1.2/acid_stat_alerts.php

ACID Alert Listing

Added 10 alert(s) to the Alert cache

Queried DB on : Sat November 30, 2002 07:38:11

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

Displaying alerts 1-7 of 7 total

	< Signature >	< Classification >	< Total # >	Sensor #	< Src. Addr. >	< Dest. Addr. >	< First >	< Last >
□	[CVE] [CVE] MISC UPNP malformed advertisement	misc-attack	88855 (100%)	2	1	1	2002-11-06 04:32:28	2002-11-30 07:37:56
□	[url] BAD TRAFFIC loopback traffic	bad-unknown	5 (0%)	1	5	5	2002-11-06 06:01:15	2002-11-06 06:01:21
□	[CVE] [CVE] SNMP broadcast trap	attempted-recon	2 (0%)	1	1	1	2002-11-09 11:13:21	2002-11-17 19:41:27
□	[bugtraq] [arachNIDS] WEB-IIS view source via translate header	web-application-activity	25 (0%)	1	1	1	2002-11-12 17:42:03	2002-11-26 23:38:39
□	[bugtraq] EXPERIMENTAL WEB-CLIENT javascript URL host spoofing attempt	attempted-user	1 (0%)	1	1	1	2002-11-29 15:16:29	2002-11-29 15:16:29
□	SCAN Proxy (8080) attempt	attempted-recon	2 (0%)	1	1	1	2002-11-29 15:19:37	2002-11-29 15:19:37
□	WEB-IIS scripts access	web-application-activity	1 (0%)	1	1	1	2002-11-29 15:27:02	2002-11-29 15:27:02

Action: { action }

[Loaded in 22 seconds]

ACID v0.9.6b21 (by Roman Danyliw as part of the AirCERT project)

Fig 5

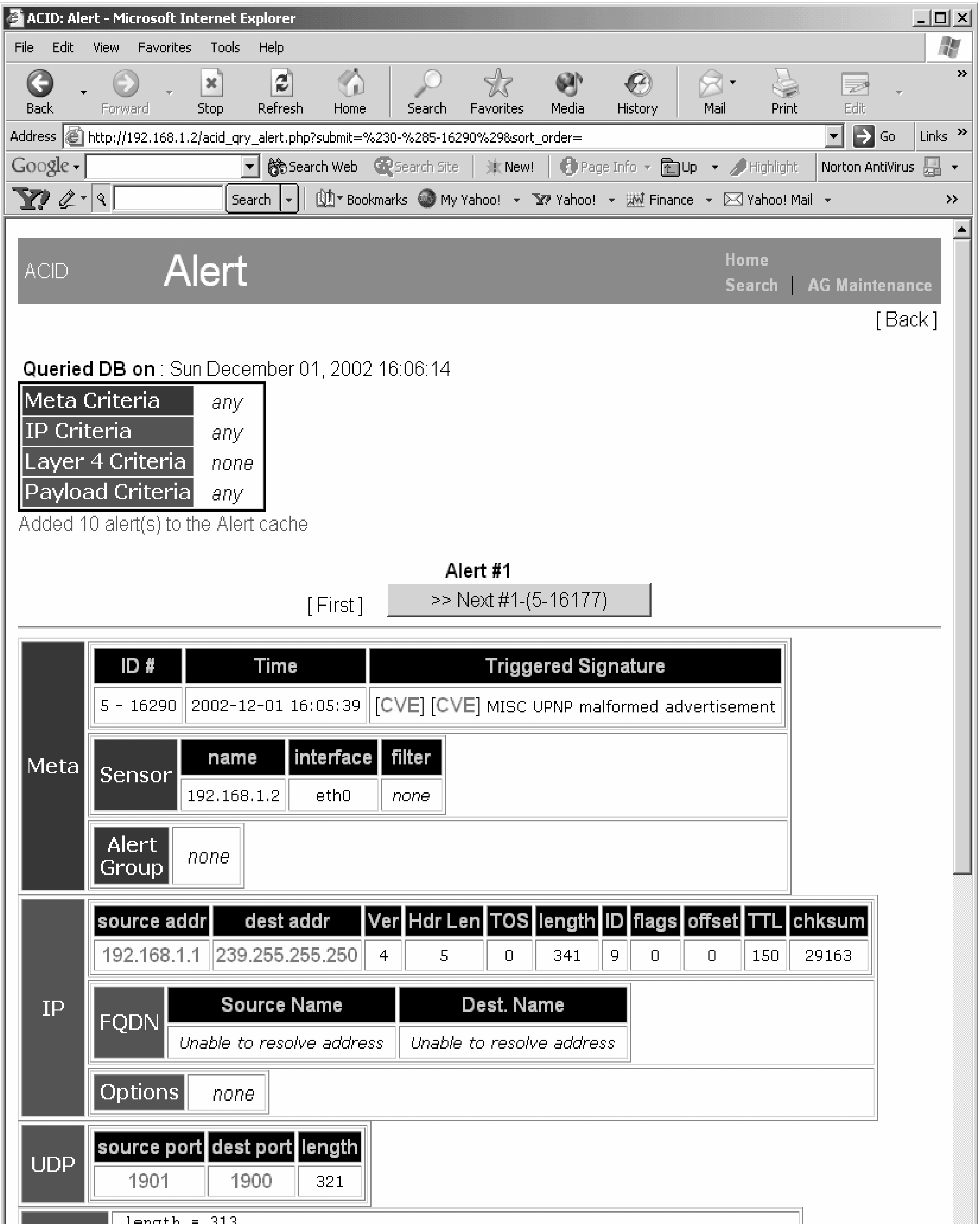
Sample snort.conf File

The following is a sample configuration file for Snort. All lines starting with the # character are comment lines. Whenever you modify the configuration file, you have to restart Snort for the changes to take effect.

```
# Variable Definitions
var HOME_NET 192.168.1.0/24
var EXTERNAL_NET any
var HTTP_SERVERS $HOME_NET
var DNS_SERVERS $HOME_NET
var RULE_PATH ./
# preprocessors
preprocessor frag2
preprocessor stream4: detect_scans
preprocessor stream4_reassemble
preprocessor http_decode: 80 -unicode -cginull
preprocessor unidecode: 80 -unicode -cginull
preprocessor bo: -nobrute
preprocessor telnet_decode
preprocessor portscan: $HOME_NET 4 3 portscan.log
preprocessor arpspoof
# output modules
output alert_syslog: LOG_AUTH LOG_ALERT
output log_tcpdump: snort.log
output database: log, mysql, user=rr password=boota \
dbname=snort host=localhost
output xml: log, file=/var/log/snortxml
# Rules and include files
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/smtp.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/tftp.rules
include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/sql.rules
include $RULE_PATH/x11.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/myrules.rules
```

If you define your own rule types, they are checked last in the sequence. For example, if you have defined a rule type snmp_alerts, the order of rule application will be:

Alert -> Pass -> Log ->snmp_alerts


ACID: Alert - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit
Address http://192.168.1.2/acid_qry_alert.php?submit=%230-%285-16290%29&sort_order=
Go Links
Google Search Web Search Site New! Page Info Up Highlight Norton AntiVirus
Search Bookmarks My Yahoo! Yahoo! Finance Yahoo! Mail
ACID Alert
Home
Search | AG Maintenance
[Back]

Queried DB on : Sun December 01, 2002 16:06:14

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

Added 10 alert(s) to the Alert cache

Alert #1

[First] >> Next #1-(5-16177)

Meta

ID #	Time	Triggered Signature
5 - 16290	2002-12-01 16:05:39	[CVE] [CVE] MISC UPNP malformed advertisement

Sensor	name	interface	filter
	192.168.1.2	eth0	*none*

Alert Group	*none*

IP

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
192.168.1.1	239.255.255.250	4	5	0	341	9	0	0	150	29163

FQDN	Source Name	Dest. Name
	Unable to resolve address	*Unable to resolve address*

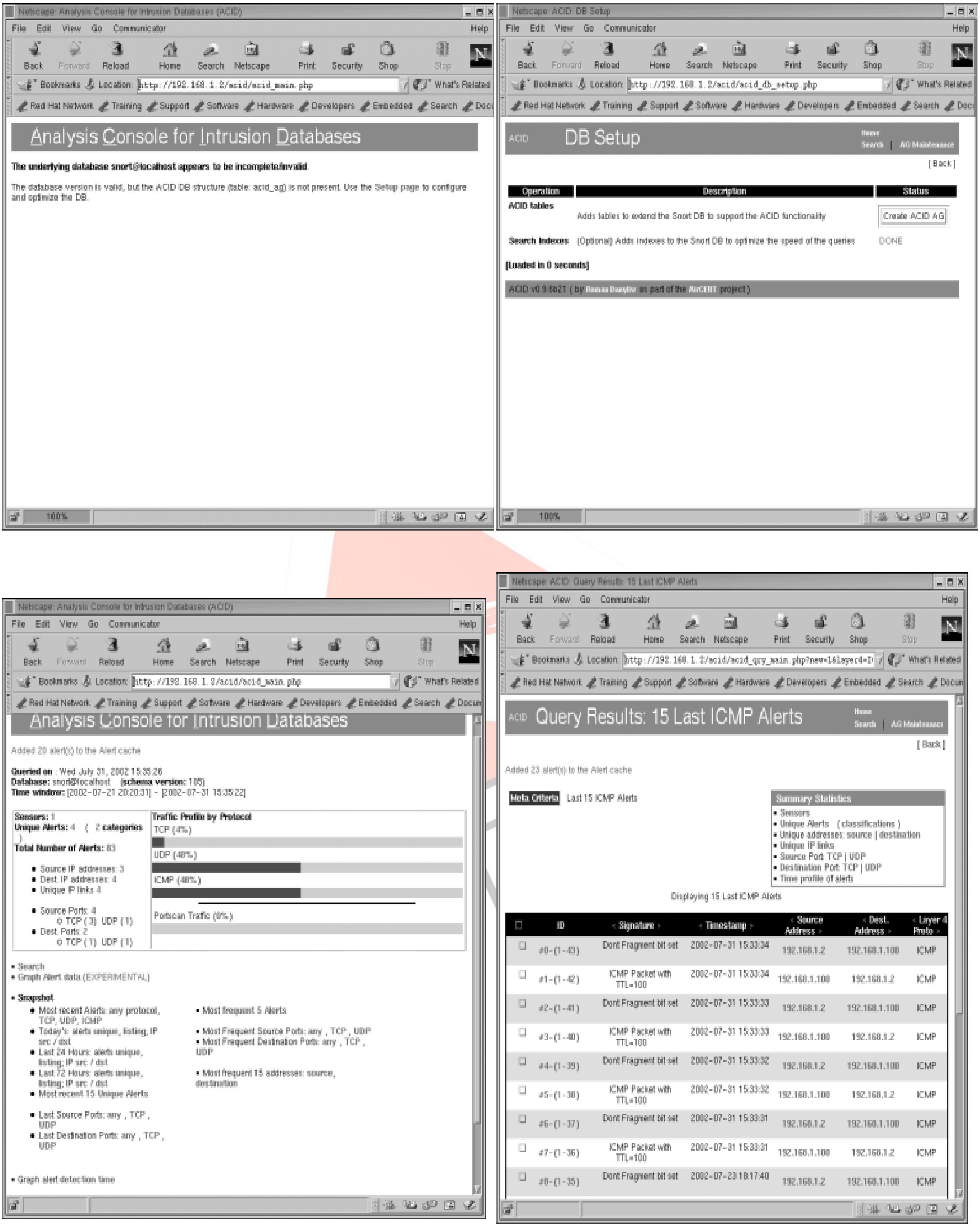
Options	*none*

UDP

source port	dest port	length
1901	1900	321

length = 313

Fig 6 Snort Rules based Alert Screen


File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: What's Related
Red Hat Network Training Support Software Hardware Developers Embedded Search Docu
100%

Netscape: Analysis Console for Intrusion Databases (ACID)

http://192.168.1.2/acid/acid_main.php

Analysis Console for Intrusion Databases

The underlying database snort@localhost appears to be incomplete/invalid.

The database version is valid, but the ACID DB structure (table: acid_ag) is not present. Use the Setup page to configure and optimize the DB.

Netscape: ACID: DB Setup

http://192.168.1.2/acid/acid_db_setup.php

ACID DB Setup

Home
Search | AG Maintenance

[Back]

Operation	Description	Status
ACID tables	Adds tables to extend the Snort DB to support the ACID functionality	Create ACID AG
Search Indexes	(Optional) Adds indexes to the Snort DB to optimize the speed of the queries	DONE

[Loaded in 0 seconds]

ACID v0.9.6b21 (by Roman Danyliw as part of the AirCERT project)

Netscape: Analysis Console for Intrusion Databases (ACID)

http://192.168.1.2/acid/acid_main.php

Analysis Console for Intrusion Databases

Added 20 alert(s) to the Alert cache

Queried on : Wed July 31, 2002 15:35:26
Database: snort@localhost **(schema version:** 105)
Time window: [2002-07-21 20:20:31] - [2002-07-31 15:35:22]

Sensors: 1
Unique Alerts: 4 (2 **categories**)
Total Number of Alerts: 83

- Source IP addresses: 3
- Dest. IP addresses: 4
- Unique IP links 4
- Source Ports: 4
  - TCP (3) UDP (1)
- Dest. Ports: 2
  - TCP (1) UDP (1)

Traffic Profile by Protocol
TCP (4%)
UDP (48%)
ICMP (48%)
Portscan Traffic (0%)

- Search
- Graph Alert data (EXPERIMENTAL)

- **Snapshot**
  - Most recent Alerts: any protocol, TCP, UDP, ICMP
  - Today's: alerts unique, listing; IP src / dst
  - Last 24 Hours: alerts unique, listing; IP src / dst
  - Last 72 Hours: alerts unique, listing; IP src / dst
  - Most recent 15 Unique Alerts
  - Last Source Ports: any , TCP , UDP
  - Last Destination Ports: any , TCP , UDP
  - Most frequent 5 Alerts
  - Most Frequent Source Ports: any , TCP , UDP
  - Most Frequent Destination Ports: any , TCP , UDP
  - Most frequent 15 addresses: source, destination

- Graph alert detection time

Netscape: ACID: Query Results: 15 Last ICMP Alerts

http://192.168.1.2/acid/acid_qry_main.php?new=1&layer4=I

ACID Query Results: 15 Last ICMP Alerts

Home
Search | AG Maintenance

[Back]

Added 23 alert(s) to the Alert cache

Meta Criteria Last 15 ICMP Alerts

Summary Statistics
- Sensors
- Unique Alerts (classifications)
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

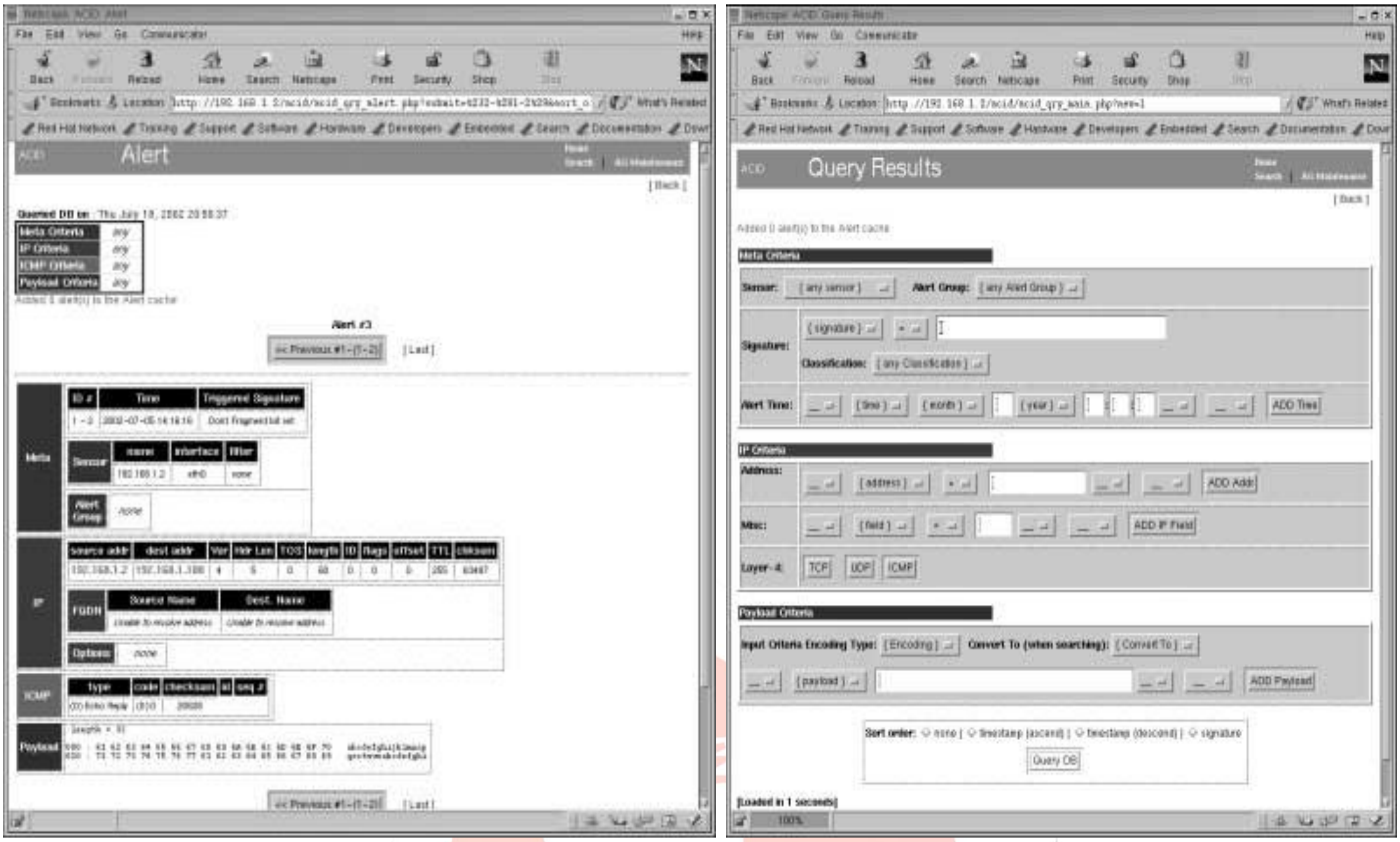
Displaying 15 Last ICMP Alerts

□	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
□	#0-(1-43)	Dont Fragment bit set	2002-07-31 15:33:34	192.168.1.2	192.168.1.100	ICMP
□	#1-(1-42)	ICMP Packet with TTL=100	2002-07-31 15:33:34	192.168.1.100	192.168.1.2	ICMP
□	#2-(1-41)	Dont Fragment bit set	2002-07-31 15:33:33	192.168.1.2	192.168.1.100	ICMP
□	#3-(1-40)	ICMP Packet with TTL=100	2002-07-31 15:33:33	192.168.1.100	192.168.1.2	ICMP
□	#4-(1-39)	Dont Fragment bit set	2002-07-31 15:33:32	192.168.1.2	192.168.1.100	ICMP
□	#5-(1-38)	ICMP Packet with TTL=100	2002-07-31 15:33:32	192.168.1.100	192.168.1.2	ICMP
□	#6-(1-37)	Dont Fragment bit set	2002-07-31 15:33:31	192.168.1.2	192.168.1.100	ICMP
□	#7-(1-36)	ICMP Packet with TTL=100	2002-07-31 15:33:31	192.168.1.100	192.168.1.2	ICMP
□	#8-(1-35)	Dont Fragment bit set	2002-07-23 18:17:40	192.168.1.2	192.168.1.100	ICMP

Fig 7 Mysql Database Create and Query Result using snort tools

Alert Details

Figure shows details about a particular ICMP packet that you would see when you click on an alert as shown in Figure 6-5. As you can see, there are different sections on the page. Each section displays a particular layer of the data packet. The topmost section provides general information about the alert. The IP section displays all parts of the IP header. The ICMP header displays ICMP data, followed by the payload. Payload is displayed both in hexadecimal and ASCII text. Refer to Appendix C for information about different protocol headers.



http://192.168.1.2/acid/acid_qry_alert.php?submit=%232-%281-2%29&sort_o

ACID Alert

[Back]

Queried DB on : Thu July 18, 2002 20:58:37

Meta Criteria	any
IP Criteria	any
ICMP Criteria	any
Payload Criteria	any

Added 1 alert(s) to the Alert cache

Alert #3

<< Previous #1-(1-2) [Last]

Meta

ID #	Time	Triggered Signature
1 - 3	2002-07-05 14:18:16	Dont Fragment bit set

Sensor	name	interface	filter
	192.168.1.2	eth0	none

Alert Group: none

IP

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
192.168.1.2	192.168.1.100	4	5	0	60	0	0	0	255	63467

FQDN	Source Name	Dest. Name
	Unable to resolve address	Unable to resolve address

Options: none

ICMP

type	code	checksum	id	seq #
(0) Echo Reply	(0) 0	20020		

Payload

```
length = 32
000 : 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70   abcdefghijklmnop
010 : 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
```

<< Previous #1-(1-2) [Last]

http://192.168.1.2/acid/acid_qry_main.php?new=1

ACID Query Results

[Back]

Added 0 alert(s) to the Alert cache

Meta Criteria

Sensor: { any sensor } Alert Group: { any Alert Group }

Signature: { signature } =

Classification: { any Classification }

Alert Time: { time } { month } { year } ADD Time

IP Criteria

Address: { address } = ADD Addr

Misc: { field } = ADD IP Field

Layer-4: TCP UDP ICMP

Payload Criteria

Input Criteria Encoding Type: { Encoding } Convert To (when searching): { Convert To }

{ payload } ADD Payload

Sort order: ○ none | ○ timestamp (ascend) | ○ timestamp (descend) | ○ signature

Query DB

[Loaded in 1 seconds]

100%

Fig 8

V. CONCLUSION

Network security is primary and important of any organization. Using Snort we detect intrusion atomically by defining Intrusion detection rules and policy. We protect their home or organization from several types of attacks. Snort Intrusion Detection tools allows the users customize installation as per their security requirement. Snort Tools have their own advantages and disadvantages, using that we detect the instruction we make alert for that and prevent that instruction using Snort tools.

REFERENCES

[1] NIST, Guide to Intrusion Detection and Prevention Systems (IDPS)
[2] SnortSam at http://www.snortsam.net/
[3] Activeworx web site at http://activeworx.com/idspm/
[4] Rusty's Unreliable Guides at http://www.netfilter.org/unreliable-guides/
[5] Easy IDS at http://www.argusnetsec.com
[6] Snort at http://www.snort.org
[7] MySQL database at http://www.mysql.org
[8] ACID at http://www.cert.org/kb/acid
[9] SAMBA at http://www.samba.org
[10] The Internet Protocol RFC 791 at http://www.rfc-editor.org/rfc/rfc791.txt
[11] The nmap at it web site http://www.nmap.org
[12] Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID Rafeeq Ur Rehman Prentice Hall PTR Upper Saddle River, New Jersey 07458 www.phptr.com
[13] DOUGLAS J. BROWN, BILL SUCKOW, and TIANQIU WANG, "A Survey of Intrusion Detection Systems"
[14] A Survey of Intrusion Detection systemsy. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[15] SURYA BHAGAVAN AMBATI, DEEPTI VIDYARTHI, "A BRIEF STUDY AND COMPARISON OF, OPEN SOURCE INTRUSION DETECTION SYSTEM TOOLS" International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-1, Issue-10, Dec-2013
[16] OSSEC website, http://www.ossec.net/, 30 Oct 2013

[17] SNORT website , http://www.snort.org , 30 Oct 2013

[18] Tripwire website http://www.tripwire.com,30 Oct 2013

[19] Martin Roesch, “SNORT – Light weight Intrustion detection for networks”,Proceedings of LISA '99: 13th Systems Administration Conference Seattle, Washington, USA, November 7–12, 1999