60-564 : Security and Privacy on the Internet

Snort Testing System
by using
Activeworx Security Center (ASC), MySQL and CommView on Windows XP

UNIVERSITY OF WINDSOR

Instructor: Dr. A. K. Aggarwal

Prepared by:

1. Md. Shamsul Wazed	SID: 100 791 020
2. Quazi Rahman	SID: 102 447 301

School of Computer Science

March 12, 2006

Table of Contents

1. Introduction

Security for network is one of the most important issues facing nearly all computer users. Intrusion Detection System (IDS) have been developed to collect data about network traffic coming into a system and tries to match it against known pattern of attack signatures. Traffic that fits a pattern can be blocked, detail of attack can be logged and administrators can be informed of the attempt. Snort[1] is a very popular, freeware IDS, developed by Marty Roesch. A Window version of Snort is recently released with its success and popularity. The Snort architecture currently has over 1200 rules available for download from the Snort website, and a default set of rules comes with the package. There are a number of Graphical User Interfaces (GUI) available for monitoring Snort, analyzing result and writing Snort rules.

The purpose of this project is to installation and configuration of a completer Snort implementation. This report contains all the necessary information for installation and understanding the architectural layout of the implementation. In this project we have used Activeworx Security Center (ASC)[2] as the add-on of Snort and implemented on Windows XP operating system. With the help of ASC we can view and analyze the logs. Its IDS event can allow monitoring alerts easily and generates statistics. The most commonly used Database MySQL[3] is used here as the Database server. CommView[4] is used in this project for packet generating, packet monitoring and analyzing purpose. .Net Framework is installed as an addition software requirement of ASC Desktop.

To implement the project, we have used two computers connected via a switch at our university network lab. The packet sniffer and packet generator CommView is installed on one computer to generate the attack packets with snort signature and send them out to the second computer. The snort GUI interface ASC along with CommView is mounted on the second computer to monitor the alerts and generate the statistics. The goal of this project is also to verify that the packets generated with some specific snort signature is properly captured by the tool ASC desktop.

2. Software Requirement

There are four primary software packages are used to implement this project. The MySQL database server, CommView, Snort and ASC. Below is a brief description of each of the packages and their purpose in our project.

i) MySQL Server :

MySQL is a SQL based database server for a variety of platforms and is the most supported platform for storing Snort alerts. All of the IDS alerts that are triggered from our sensors are stored in the MySQL database.

ii) CommView

CommView is a powerful network monitor and analyzer designed for LAN administrators, security professionals, network programmers and home users - virtually anyone who wants a full picture of the traffic flowing through a PC or LAN segment. This tool also allows to edit and send packets via the network card. Any kind of packets, like IP, TCP, UDP, or ICMP packets, can be generated and have full control over the packet contents.

iii) Snort

Snort is a very popular network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It is very lightweight and flexible, and designed originally to run on UNIX based systems. It has recently been made for Windows based system. This is the software package that is used to gather information from the network. A Snort rule is a set of packet characteristics that is compared to incoming traffic, a match between a rule and a packet will be triggering an alert.

iv) Activeworx Security Center (ASC)

Activeworx Security Center was designed by and for security administrators to bring a common view of all security events in the network environment. It allows a user to view, search, graph, diagram, report and correlate between logs from IDS, TCPDump, Firewall, Syslog, keystrokes and vulnerabilities in a simple to use yet powerful Interface. It support for both MySQL and Microsoft SQL Database. This is a product of BrightTools Inc (ww.brighttools.com) and offering a free download of 15 days trial version.

3. Installation of MySQL

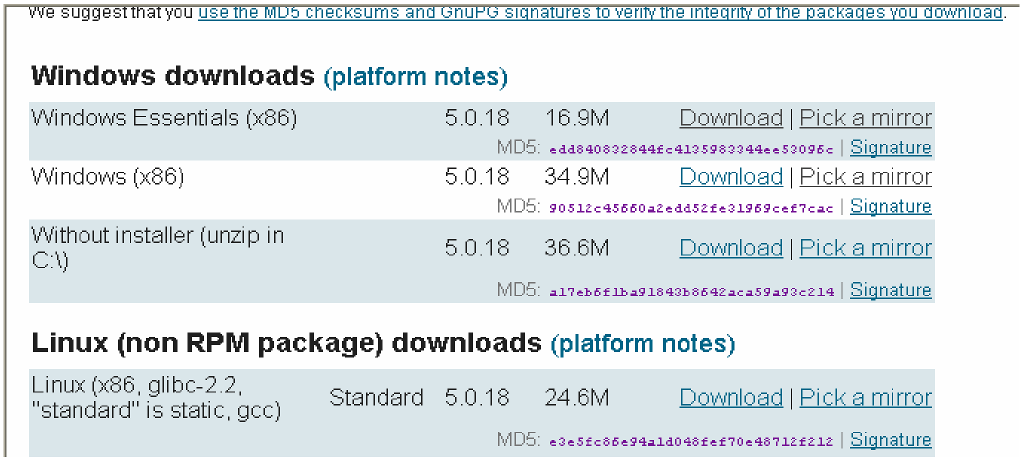
MySQL is a database that becomes the world's most popular open source database because of its consistent fast performance, high reliability and ease of use. It is used in more than 6 million installations ranging from large corporations to specialized embedded applications on every continent in the world. MySQL is also become the database of choice for a new generation of applications built on the LAMP stack (Linux, Apache, MySQL, PHP / Perl / Python.). MySQL runs on more than 20 platforms including Linux, Windows, OS/X, HP-UX, AIX, Netware, giving the kind of flexibility that puts you in control. MySQL is a freeware and MySQL AB is the company of the MySQL founders and main developers of official web-site http://www.mysql.com.

i) Requirements of MySQL:

To run MySQL on Windows a 32-bit Windows operating system, such as 9x, Me, NT, 2000, XP, or Windows Server 2003, is needed. A Windows NT based operating system (NT, 2000, XP, 2003) permits to run the MySQL server as a service. It should support TCP/IP protocol. Copy of the “MySQL 5.0” (installed in this project) binary distribution for Windows can be downloaded from http://dev.mysql.com/downloads/. It needs enough space on the hard drive to unpack, install, and create the databases in accordance with your requirements (generally a minimum of 200 megabytes is recommended).

ii) Installation of MySQL:

Download MySQL Database Server 5.0 from http://dev.mysql.com/downloads/.



We suggest that you use the MD5 checksums and GnuPG signatures to verify the integrity of the packages you download.

Windows downloads (platform notes)

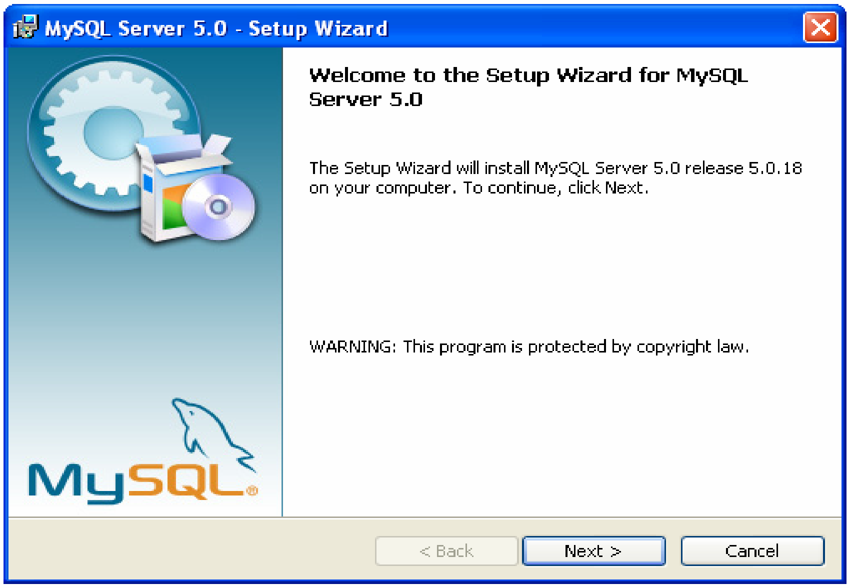
Windows Essentials (x86)	5.0.18	16.9M	Download | Pick a mirror	
		MD5: edd840832844fc41359833 44ee53096c	Signature	
Windows (x86)	5.0.18	34.9M	Download | Pick a mirror	
		MD5: 90512c45660a2edd52fe31969cef7cac	Signature	
Without installer (unzip in C:\)	5.0.18	36.6M	Download | Pick a mirror	
		MD5: a17eb6f1ba91843b8642aca59a93c214	Signature	

Linux (non RPM package) downloads (platform notes)

Linux (x86, glibc-2.2, "standard" is static, gcc)	Standard	5.0.18	24.6M	Download | Pick a mirror	
			MD5: e3e5fc86e94a1d048fef70e48712f212	Signature	

Fig 1 : Windows download for MySql

Install MySQL Server:



MySQL Server 5.0 - Setup Wizard

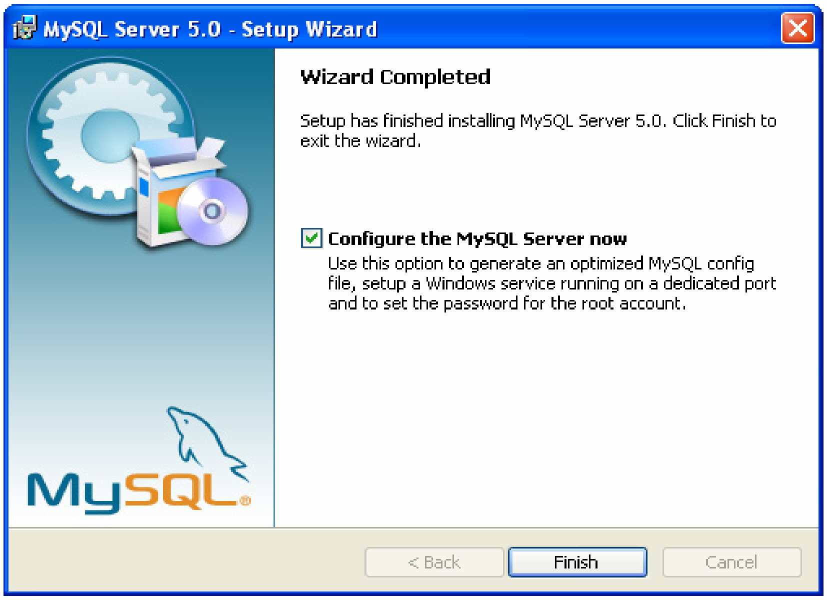
Welcome to the Setup Wizard for MySQL Server 5.0

The Setup Wizard will install MySQL Server 5.0 release 5.0.18 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law.

Fig 2 : MySQL Setup Welcome menu

Now the server should be configured:



MySQL Server 5.0 - Setup Wizard

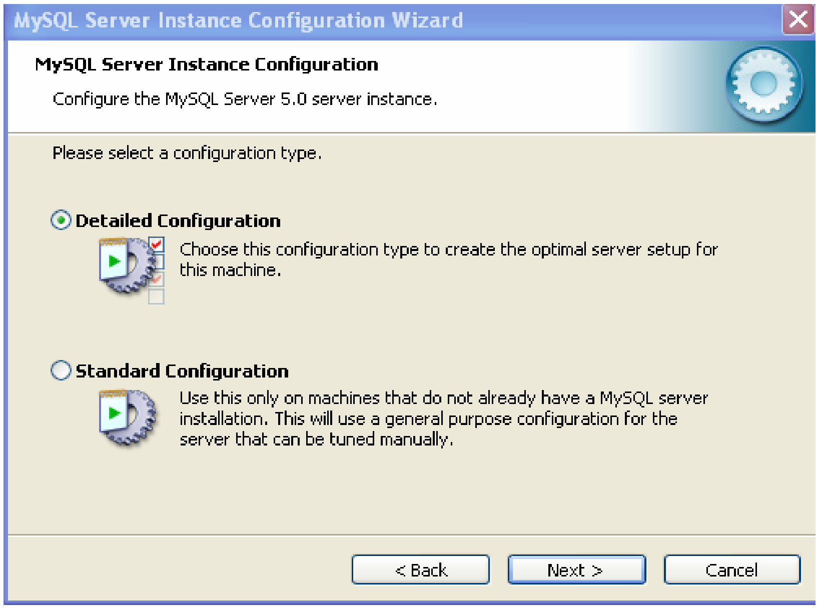
Wizard Completed

Setup has finished installing MySQL Server 5.0. Click Finish to exit the wizard.

☑ **Configure the MySQL Server now**
Use this option to generate an optimized MySQL config file, setup a Windows service running on a dedicated port and to set the password for the root account.

Fig 3 : MySQL Setup Wizard

Perform a detailed configuration:



MySQL Server Instance Configuration Wizard

MySQL Server Instance Configuration

Configure the MySQL Server 5.0 server instance.

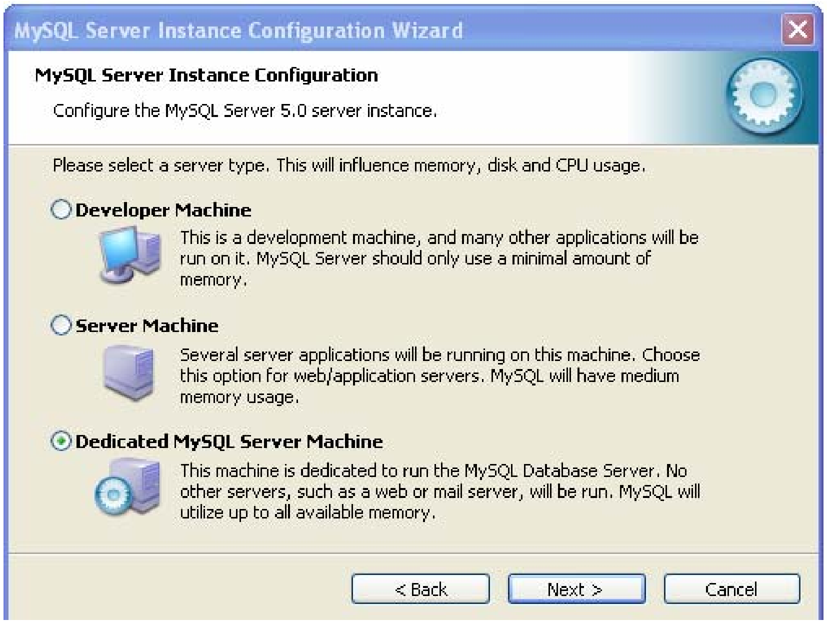
Please select a configuration type.

● **Detailed Configuration**
Choose this configuration type to create the optimal server setup for this machine.

○ **Standard Configuration**
Use this only on machines that do not already have a MySQL server installation. This will use a general purpose configuration for the server that can be tuned manually.

Fig 4 : MySQL Configuration type

The server should be a dedicated MySQL server:



MySQL Server Instance Configuration Wizard

MySQL Server Instance Configuration

Configure the MySQL Server 5.0 server instance.

Please select a server type. This will influence memory, disk and CPU usage.

○ **Developer Machine**

This is a development machine, and many other applications will be run on it. MySQL Server should only use a minimal amount of memory.

○ **Server Machine**

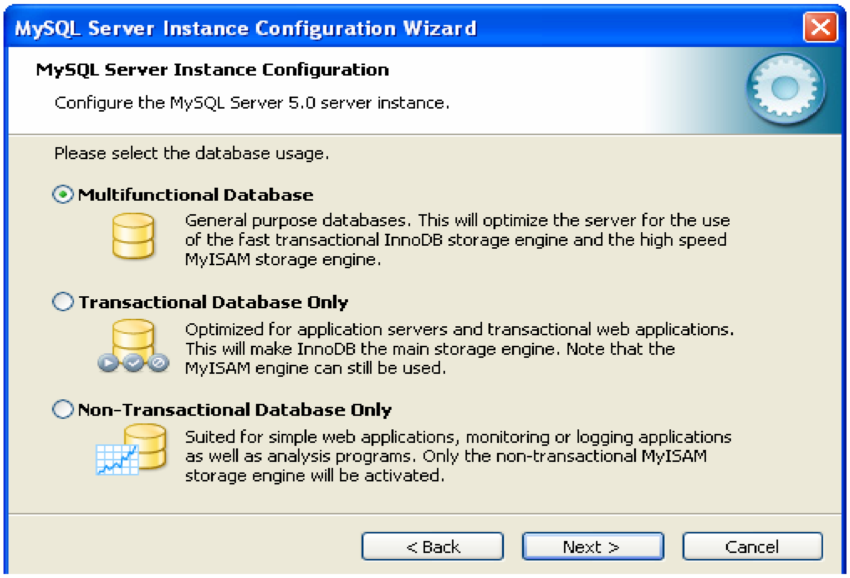
Several server applications will be running on this machine. Choose this option for web/application servers. MySQL will have medium memory usage.

● **Dedicated MySQL Server Machine**

This machine is dedicated to run the MySQL Database Server. No other servers, such as a web or mail server, will be run. MySQL will utilize up to all available memory.

Fig 5 : MySQL Server selection

Select the default option, Multifunctional Database:



MySQL Server Instance Configuration Wizard

MySQL Server Instance Configuration

Configure the MySQL Server 5.0 server instance.

Please select the database usage.

● **Multifunctional Database**

General purpose databases. This will optimize the server for the use of the fast transactional InnoDB storage engine and the high speed MyISAM storage engine.

○ **Transactional Database Only**

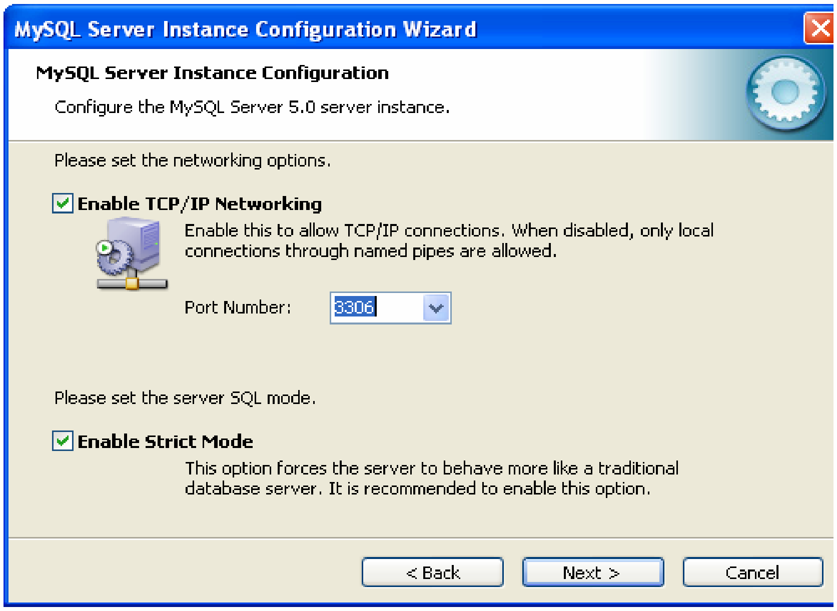
Optimized for application servers and transactional web applications. This will make InnoDB the main storage engine. Note that the MyISAM engine can still be used.

○ **Non-Transactional Database Only**

Suited for simple web applications, monitoring or logging applications as well as analysis programs. Only the non-transactional MyISAM storage engine will be activated.

Fig 6 : MySQL Database usages

Configure Network support:



MySQL Server Instance Configuration Wizard

MySQL Server Instance Configuration

Configure the MySQL Server 5.0 server instance.

Please set the networking options.

☑ Enable TCP/IP Networking

Enable this to allow TCP/IP connections. When disabled, only local connections through named pipes are allowed.

Port Number: 3306

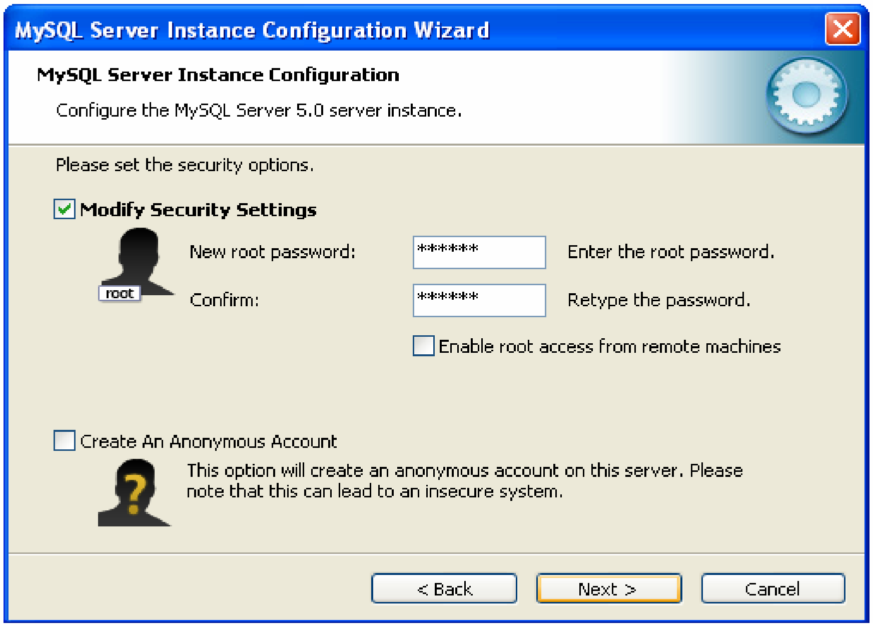
Please set the server SQL mode.

☑ Enable Strict Mode

This option forces the server to behave more like a traditional database server. It is recommended to enable this option.

Fig 7 : MySQL Network option

Change root password:



MySQL Server Instance Configuration Wizard

MySQL Server Instance Configuration

Configure the MySQL Server 5.0 server instance.

Please set the security options.

☑ Modify Security Settings

New root password: ******* Enter the root password.

Confirm: ******* Retype the password.

□ Enable root access from remote machines

□ Create An Anonymous Account

This option will create an anonymous account on this server. Please note that this can lead to an insecure system.

Fig 8 : MySQL Password setup

MySQL server configuration is complete.

iv) MySQL Connector/ODBC:

ODBC (Open Database Connectivity) provides a way for client programs to access a wide range of databases or data sources. It is an optional requirement to connect with the MySQL server. ODBC is a standardized API that allows connections to SQL database servers. ODBC usually is used when database independence or simultaneous access to different data sources is required. "MyODBC 3.51" (installed in this project) is a 32-bit ODBC driver, also known as the MySQL ODBC 3.51 driver and it is available for download from http://dev.mysql.com/downloads/connector/odbc/3.51.html.

v) Using MySQL:

Followings are some of the examples how to use the different databases and tables using commands from the DOS prompt:

```
C:\mysql\MySQL Server 5.0\bin>mysql -u root -p
Enter password: *****

Welcome to the MySQL monitor.  Commands end with; or \g.
Your MySQL connection id is 18 to server version: 5.0.18-nt
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| aef                |
| aw_aef             |
| aw_asc             |
| aw_fw              |
| ids                |
| mysql              |
| sebek              |
| syslog             |
| tcpdump            |
| test               |
| vuln               |
+--------------------+
12 rows in set (0.19 sec)

mysql> use ids;
Database changed
```

```
mysql> show tables;
+------------------+
| Tables_in_ids    |
+------------------+
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
| opt              |
| reference        |
| reference_system |
| schema           |
| sensor           |
| sig_class        |
| sig_reference    |
| signature        |
| tcphdr           |
| udphdr           |
+------------------+
16 rows in set (0.00 sec)

mysql> describe event;
+-----------+------------------+------+-----+---------+------+
| Field     | Type             | Null | Key | Default | Extra|
+-----------+------------------+------+-----+---------+------+
| sid       | int(10) unsigned | NO   | PRI |         |      |
| cid       | int(10) unsigned | NO   | PRI |         |      |
| signature | int(10) unsigned | NO   | MUL |         |      |
| timestamp | datetime         | NO   | MUL |         |      |
+-----------+------------------+------+-----+---------+------+
4 rows in set (0.19 sec)

mysql> select* from event;
Empty set (0.00 sec)

mysql> show tables;
+------------------+
| Tables_in_ids    |
+------------------+
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
| opt              |
| reference        |
| reference_system |
| schema           |
| sensor           |
| sig_class        |
| sig_reference    |
| signature        |
| tcphdr           |
| udphdr           |
+------------------+
16 rows in set (0.00 sec)

mysql> describe event;
+-----------+-------------+------+-----+---------+-------+
| Field     | Type        | Null | Key | Default | Extra |
+-----------+-------------+------+-----+---------+-------+
| sid       | int(11)     | NO   |     |         |       |
| cid       | int(11)     | NO   | PRI |         |       |
| signature | int(11)     | NO   |     |         |       |
| timestamp | varchar(30) | YES  |     | NULL    |       |
+-----------+-------------+------+-----+---------+-------+
4 rows in set (0.02 sec)


mysql> describe event;
+-----------+-------------+------+-----+---------+-------+
| Field     | Type        | Null | Key | Default | Extra |
+-----------+-------------+------+-----+---------+-------+
| sid       | int(11)     | NO   |     |         |       |
| cid       | int(11)     | NO   | PRI |         |       |
| signature | int(11)     | NO   |     |         |       |
| timestamp | varchar(30) | NO   |     |         |       |
+-----------+-------------+------+-----+---------+-------+
4 rows in set (0.03 sec)


mysql> describe signature;
+----------+-------------+------+-----+-------+-------------+
|Field     |Type         | Null | Key | Default | Extra      |
+----------+-------------+------+-----+---------+------------+
|sig_id   |int(10)unsigned|NO  |PRI  |NULL   |auto_increment |
|sig_name  | varchar(255)|NO | MUL |        |               |
|sig_class_id|int(10) unsigned| NO |   MUL |     |          |
|sig_priority|int(10) unsigned | YES  |    | NULL   |        |
|sig_rev  |int(10) unsigned | YES  |      | NULL   |         |
|sig_sid |int(10) unsigned | YES  |     | NULL  |           |
+---------+-------------+------+-----+-------+-------------+
6 rows in set (0.00 sec)
```

```
mysql> select* from event;
+-----+-----+-----------+-----------------------------+
| sid | cid | signature | timestamp                   |
+-----+-----+-----------+-----------------------------+
|   2 |   1 |         0 | 2006-03-03 14:59:24.520+005 |
|   2 |   2 |         0 | 2006-03-03 14:59:27.836+005 |
|   2 |   3 |        13 | 2006-03-03 15:07:59.143+005 |
|   2 |   4 |        13 | 2006-03-03 15:08:01.389+005 |
|   2 |   5 |        13 | 2006-03-03 15:08:19.497+005 |
|   2 |   6 |        13 | 2006-03-03 15:08:19.558+005 |
|   2 |   7 |        13 | 2006-03-03 15:08:40.738+005 |
|   2 |   8 |        13 | 2006-03-03 15:08:43.001+005 |
|   2 |   9 |        14 | 2006-03-03 15:08:45.478+005 |
|   2 |  10 |        15 | 2006-03-03 15:08:45.538+005 |
|   2 |  11 |        16 | 2006-03-03 15:08:45.542+005 |
|   2 |  12 |        14 | 2006-03-03 15:08:52.295+005 |
|   2 |  13 |        17 | 2006-03-03 15:09:45.520+005 |
|   2 |  14 |        14 | 2006-03-03 15:09:45.533+005 |
|   2 |  15 |        18 | 2006-03-03 15:09:45.537+005 |
|   2 |  16 |        13 | 2006-03-03 15:09:45.550+005 |
+-----+-----+-----------+-----------------------------+
16 rows in set (0.00 sec)

mysql> select* from signatures;
ERROR 1146 (42S02): Table 'ids.signatures' doesn't exist


mysql> select* from signature;
-------+-------------+--------------+---------+---------+
| sig_id | sig_name
       | sig_class_id | sig_priority | sig_rev | sig_sid |
-------+-------------+--------------+---------+---------+
|  13 | NETBIOS SMB IPC$ unicode share access |  13 |  3 |
15 |     538 |
| 14 | ICMP L3retriever Ping  |  14 |   2 |   4 |     466 |
|  15  |  NETBIOS  SMB-DS  Session  Setup  AndX  request  unicode
username overflow attempt |   15 |  1 |       5 |    2404 |
| 16 | NETBIOS SMB-DS IPC$ unicode share access|13| 3 | 7 |
2466 |
| 17 | NETBIOS SMB Session Setup AndX request unicode username
overflow attempt    |    15 |       1 |       4 |    2403 |
| 18 | NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow
attempt     |       13 |            3 |       4 |    3000 |
+--------+-----------------------------------------------
6 rows in set (0.00 sec)
```

4. Installation of CommView

CommView is a program for monitoring Internet and Local Area Network (LAN) activity capable of capturing and analyzing network packets. It gathers information about data passing through your dial-up connection or Ethernet card and decodes the analyzed data.

With CommView you can see the list of network connections and vital IP statistics and examine individual packets. Packets are decoded down to the lowest layer with full analysis of the most widespread protocols. Full access to raw data is also provided. Captured packets can be saved to log files for future analysis. A flexible system of filters makes it possible to drop packets you don't need or capture only those packets that you wish to capture.

CommView is a helpful tool for LAN administrators, security professionals, network programmers, or anyone who wants to have a full picture of the traffic going through one's PC or LAN segment.

i) System Requirements :

- An Ethernet or Wireless Ethernet network card supporting the NDIS 3.0 driver standard, or a standard dial-up adapter.
- Pentium II of higher.
- Windows 98/Me/2000/XP/2003 or Windows XP 64-bit Edition on AMD Opteron or Athlon64.
- Windows 2000/XP/2003 users: you MUST have administrative privileges to install and run CommView.
- 32 MB RAM (128 MB recommended).
- 6 MB of free disk space.

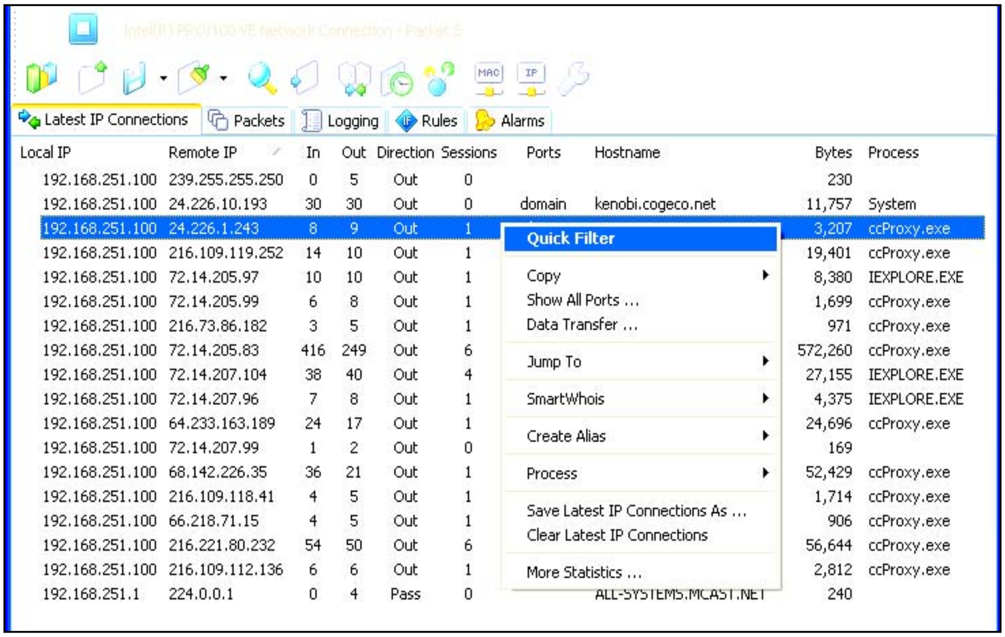
ii) Installing CommView :

- If you already have an older CommView version installed, uninstall it and reboot.
- Go to the Internet site http://www.tamos.com/download/main/. Click on the download button for CommView 5.0 and save the file to the folder of your choice.
- Unzip the ZIP archive to a temporary folder.
- Double-click setup.exe to execute it.
- Setup will guide you through the rest of the installation process.

iv) Using CommView :

(a) LATEST IP CONNECTION

This tab is used for displaying detailed information about your computer's network connections (IP protocol only). To start capturing packets, select File = > Start Capture in the menu, or click on the corresponding button on the toolbar.



Local IP	Remote IP	In	Out	Direction	Sessions	Ports	Hostname	Bytes	Process
192.168.251.100	239.255.255.250	0	5	Out	0			230	
192.168.251.100	24.226.10.193	30	30	Out	0	domain	kenobi.cogeco.net	11,757	System
192.168.251.100	24.226.1.243	8	9	Out	1			3,207	ccProxy.exe
192.168.251.100	216.109.119.252	14	10	Out	1			19,401	ccProxy.exe
192.168.251.100	72.14.205.97	10	10	Out	1			8,380	IEXPLORE.EXE
192.168.251.100	72.14.205.99	6	8	Out	1			1,699	ccProxy.exe
192.168.251.100	216.73.86.182	3	5	Out	1			971	ccProxy.exe
192.168.251.100	72.14.205.83	416	249	Out	6			572,260	ccProxy.exe
192.168.251.100	72.14.207.104	38	40	Out	4			27,155	IEXPLORE.EXE
192.168.251.100	72.14.207.96	7	8	Out	1			4,375	IEXPLORE.EXE
192.168.251.100	64.233.163.189	24	17	Out	1			24,696	ccProxy.exe
192.168.251.100	72.14.207.99	1	2	Out	0			169	
192.168.251.100	68.142.226.35	36	21	Out	1			52,429	ccProxy.exe
192.168.251.100	216.109.118.41	4	5	Out	1			1,714	ccProxy.exe
192.168.251.100	66.218.71.15	4	5	Out	1			906	ccProxy.exe
192.168.251.100	216.221.80.232	54	50	Out	6			56,644	ccProxy.exe
192.168.251.100	216.109.112.136	6	6	Out	1			2,812	ccProxy.exe
192.168.251.1	224.0.0.1	0	4	Pass	0		ALL-SYSTEMS.MCAST.NET	240	

Fig 9 : Log view for all IP connections

The meaning of some of the columns and menu commands are explained below:

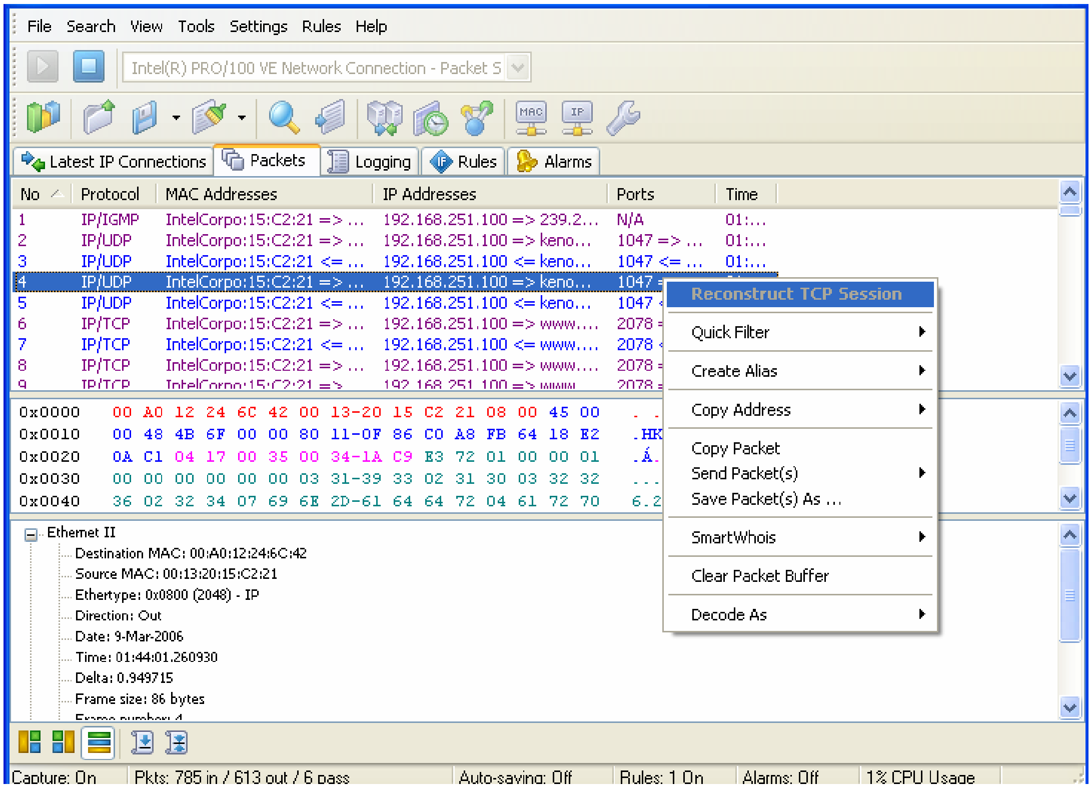
Process – shows the process on your computer that sends or receives packets in the session. This column is only available in Windows 2000/XP/2003. Mapping packets to processes only works for incoming and outgoing packets, as CommView cannot be aware of processes running on other computers that send or receive packets. Naturally, there may be several applications on the local computer exchanging data with a remote computer, so the Latest IP Connections tab only shows the latest process that sent or received data for this particular pair of IP addresses. If you would like to map a process to a particular packet, you can see this information in the decoded packet tree in the Packets tab. CommView can display the full path to the process that sent or received packets, check the Display full process path checkbox in Settings => Options, General tab to enable this feature.

(b) Menu Commands

SmartWhois – sends the selected source or destination IP address to SmartWhois, if it is installed on your system. SmartWhois is a stand-alone application developed by our company capable of obtaining information about any IP address or hostname in the world. It automatically provides information associated with an IP address, such as domain, network name, country, state or province, city. The program can be downloaded from web-site.

(c) Packet

This tab is used for listing all captured network packets and displaying detailed information about a selected packet.



No	Protocol	MAC Addresses	IP Addresses	Ports	Time
1	IP/IGMP	IntelCorpo:15:C2:21 => ...	192.168.251.100 => 239.2...	N/A	01:...
2	IP/UDP	IntelCorpo:15:C2:21 => ...	192.168.251.100 => keno...	1047 => ...	01:...
3	IP/UDP	IntelCorpo:15:C2:21 <= ...	192.168.251.100 <= keno...	1047 <= ...	01:...
4	IP/UDP	IntelCorpo:15:C2:21 => ...	192.168.251.100 => keno...	1047 =	
5	IP/UDP	IntelCorpo:15:C2:21 <= ...	192.168.251.100 <= keno...	1047 <	
6	IP/TCP	IntelCorpo:15:C2:21 => ...	192.168.251.100 => www....	2078 =	
7	IP/TCP	IntelCorpo:15:C2:21 <= ...	192.168.251.100 <= www....	2078 <	
8	IP/TCP	IntelCorpo:15:C2:21 => ...	192.168.251.100 => www....	2078 =	
9	IP/TCP	IntelCorpo:15:C2:21 =>	192.168.251.100 => www	2078 =	

```
0x0000   00 A0 12 24 6C 42 00 13-20 15 C2 21 08 00 45 00   . .
0x0010   00 48 4B 6F 00 00 80 11-0F 86 C0 A8 FB 64 18 E2   .HK
0x0020   0A C1 04 17 00 35 00 34-1A C9 E3 72 01 00 00 01   .Á.
0x0030   00 00 00 00 00 00 03 31-39 33 02 31 30 03 32 32   ...
0x0040   36 02 32 34 07 69 6E 2D-61 64 64 72 04 61 72 70   6.2
```

```
⊟ Ethernet II
    Destination MAC: 00:A0:12:24:6C:42
    Source MAC: 00:13:20:15:C2:21
    Ethertype: 0x0800 (2048) - IP
    Direction: Out
    Date: 9-Mar-2006
    Time: 01:44:01.260930
    Delta: 0.949715
    Frame size: 86 bytes
    Frame number: 4
```

Capture: On | Pkts: 785 in / 613 out / 6 pass | Auto-saving: Off | Rules: 1 On | Alarms: Off | 1% CPU Usage

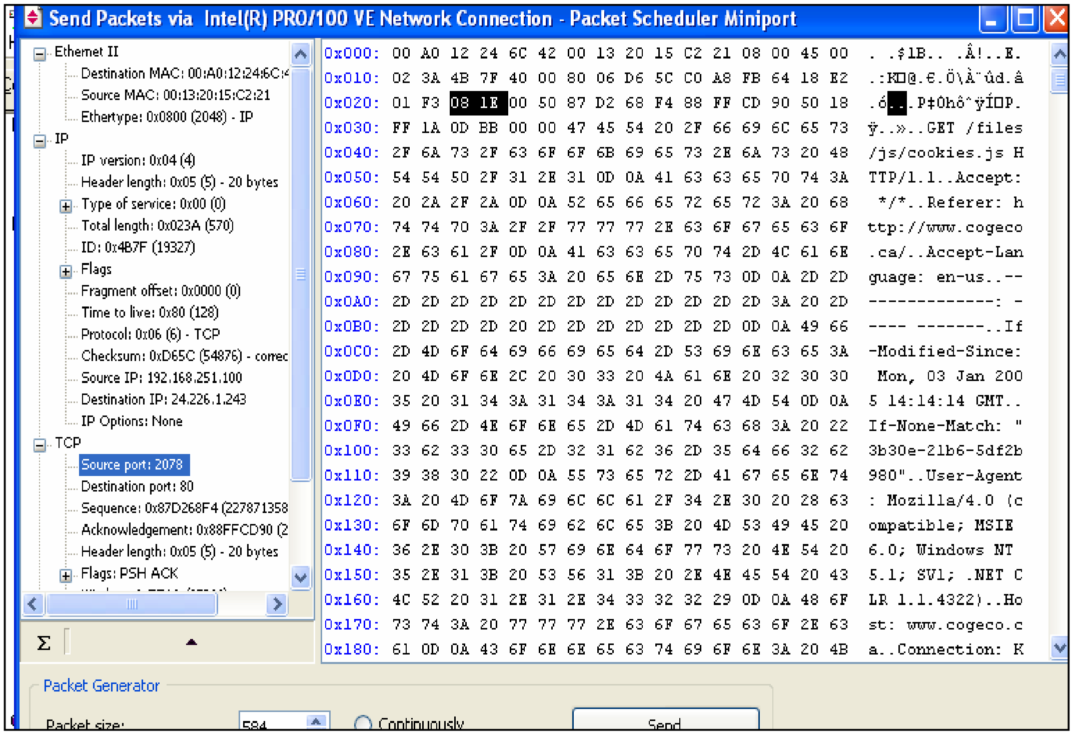
Fig 10 : Log view for all packets

The top table displays the list of captured packets. Using this list we can select a packet that we want to have displayed and analyzed. When we select a packet by clicking on it, other panes show information about the selected packet.

(d) Packet Generator

This tool allows editing and sending packets via network card. It is available only under Windows NT/2000/XP/2003. To open the Packet Generator, click Tools => Packet Generator, or select a packet from the Packets tab, right-click on it, and select the Send Packet command.

The Packet Generator is a tool for replaying pre-captured data, testing firewalls and intrusion detection systems, as well as for performing other specific tasks that require manual packet crafting.


Send Packets via Intel(R) PRO/100 VE Network Connection - Packet Scheduler Miniport
Σ
Packet Generator
○ Continuously
Send

```
⊟ Ethernet II
    Destination MAC: 00:A0:12:24:6C:4
    Source MAC: 00:13:20:15:C2:21
    Ethertype: 0x0800 (2048) - IP
⊟ IP
    IP version: 0x04 (4)
    Header length: 0x05 (5) - 20 bytes
  ⊞ Type of service: 0x00 (0)
    Total length: 0x023A (570)
    ID: 0x4B7F (19327)
  ⊞ Flags
    Fragment offset: 0x0000 (0)
    Time to live: 0x80 (128)
    Protocol: 0x06 (6) - TCP
    Checksum: 0xD65C (54876) - correc
    Source IP: 192.168.251.100
    Destination IP: 24.226.1.243
    IP Options: None
⊟ TCP
    Source port: 2078
    Destination port: 80
    Sequence: 0x87D268F4 (227871358
    Acknowledgement: 0x88FFCD90 (2
    Header length: 0x05 (5) - 20 bytes
  ⊞ Flags: PSH ACK
```

```
0x000: 00 A0 12 24 6C 42 00 13 20 15 C2 21 08 00 45 00  . .$lB.. .Â!..E.
0x010: 02 3A 4B 7F 40 00 80 06 D6 5C C0 A8 FB 64 18 E2  .:K□@.€.Ö\À¨ûd.â
0x020: 01 F3 08 1E 00 50 87 D2 68 F4 88 FF CD 90 50 18  .ó...P‡Òhô^ÿÍ□P.
0x030: FF 1A 0D BB 00 00 47 45 54 20 2F 66 69 6C 65 73  ÿ..»..GET /files
0x040: 2F 6A 73 2F 63 6F 6F 6B 69 65 73 2E 6A 73 20 48  /js/cookies.js H
0x050: 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A  TTP/1.1..Accept:
0x060: 20 2A 2F 2A 0D 0A 52 65 66 65 72 65 72 3A 20 68   */*..Referer: h
0x070: 74 74 70 3A 2F 2F 77 77 77 2E 63 6F 67 65 63 6F  ttp://www.cogeco
0x080: 2E 63 61 2F 0D 0A 41 63 63 65 70 74 2D 4C 61 6E  .ca/..Accept-Lan
0x090: 67 75 61 67 65 3A 20 65 6E 2D 75 73 0D 0A 2D 2D  guage: en-us..--
0x0A0: 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 3A 20 2D  -------------: -
0x0B0: 2D 2D 2D 2D 20 2D 2D 2D 2D 2D 2D 2D 0D 0A 49 66  ---- -------..If
0x0C0: 2D 4D 6F 64 69 66 69 65 64 2D 53 69 6E 63 65 3A  -Modified-Since:
0x0D0: 20 4D 6F 6E 2C 20 30 33 20 4A 61 6E 20 32 30 30   Mon, 03 Jan 200
0x0E0: 35 20 31 34 3A 31 34 3A 31 34 20 47 4D 54 0D 0A  5 14:14:14 GMT..
0x0F0: 49 66 2D 4E 6F 6E 65 2D 4D 61 74 63 68 3A 20 22  If-None-Match: "
0x100: 33 62 33 30 65 2D 32 31 62 36 2D 35 64 66 32 62  3b30e-21b6-5df2b
0x110: 39 38 30 22 0D 0A 55 73 65 72 2D 41 67 65 6E 74  980"..User-Agent
0x120: 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63  : Mozilla/4.0 (c
0x130: 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53 49 45 20  ompatible; MSIE
0x140: 36 2E 30 3B 20 57 69 6E 64 6F 77 73 20 4E 54 20  6.0; Windows NT
0x150: 35 2E 31 3B 20 53 56 31 3B 20 2E 4E 45 54 20 43  5.1; SV1; .NET C
0x160: 4C 52 20 31 2E 31 2E 34 33 32 32 29 0D 0A 48 6F  LR 1.1.4322)..Ho
0x170: 73 74 3A 20 77 77 77 2E 63 6F 67 65 63 6F 2E 63  st: www.cogeco.c
0x180: 61 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B  a..Connection: K
```

Packet size: 584

Fig 11 : Generating a TCP packet

The Packet Generator allows us to change the packet contents and have the packet decode displayed in the left window as you edit it. We can create packets of any kind; we have full control over the packet contents. For IP, TCP, UDP, and ICMP packets, we can automatically correct the checksum(s) by clicking on the *Sigma* button.

We can also click on the button with an arrow on it to display the list of available packet templates. The program comes with TCP, UDP, and ICMP packet templates; using them is often faster than typing hex codes in the editor window. These templates contain typical TCP, UDP, and ICMP packets, but if we need to edit many packet fields and use meaningful values that suit our needs, such as real MAC and IP addresses, port numbers, SEQ and ACK numbers, etc, we can use our own templates rather than the built-in ones. We can drag-and-drop a packet from the CommView Packets tab to the Templates section in the Packet Generator window.

5. Installation of Snort

Snort is the most widely used Intrusion Detection System. It is supported on multiple platforms including UNIX, LINUX, Solaris, FreeBSD and Windows. Snort works with ASC Desktop through the database output plug-in. WinPcap[5] is required to be installed to access Snort.

i) WinPcap

WinPcap is the industry-standard tool for link-layer network access in Windows environments. It allows applications to capture and transmit network packets bypassing the protocol stack. Winpcap.org is also the home of WinDump, the Windows version of the popular tcpdump tool as a command line network analyzer. WinDump can be used to watch, diagnose and save to disk network traffic according to various complex rules. The latest stable WinPcap version for Windows 95/98/ME/NT4/2000/XP/2003/Vista is 3.1 and it can be freely downloaded from http://www.winpcap.org/install/default.htm#Developer.

Download the executable file "winPcap_3_1.exe" file of size 456 KB and run. Follow the instructions on the screen and the installation applet will automatically detect the operating system to install the correct drivers for winPcap.

ii) Snort

As of March 2006, Snort version 2.4.3 is available at http://www.snort.org/dl/binaries/win32/ in the form of Windows binary packages. Visit the Snort web-site, download and execute the file "Snort-243-Installer.exe" of size 1.43 MB. Select "typical" installation and install the Snort in C:\Snort directory.

- Snort configuration file is located at C:\Snort\etc\snort.conf
- Snort executable file located at C:\Snort\bin\snort.exe
- Snort log files are stored at C:\Snort\bin\log\alert.ids and C:\Snort\bin\log \snort.log.<time>, and
- C:\Snort\rules directory contains the snort rules.

Snort rules can be downloaded from http://www.snort.org/pub-bin/downloads.cgi. Unzipped the file "snortrules-pr-2.4.tar.gz" of 770 KB and copied the rules files from its \rules directory into C:\Snort\rules directory. There are 59 nos of *.rules files contains more than thousands of Snort rules.

iii) Snort Configuration :

Snort.conf file is located at C:\Snort\etc directory. Edit the configuration file before Snort running. The following steps can be taken to create a custom configuration:

1) Set the variables for your network
2) Configure preprocessors
3) Configure output plugins
4) Add any runtime config directives
5) Customize your rule set

Edit the configuration file as follows :

1) Set the HOME_NET variable as `var HOME_NET 192.168.1.100/24`
2) Set the RULE_PATH variable as `var RULE_PATH c:\Snort\rules`
3) Uncomment the format `output alert_syslog: LOG_AUTH LOG_ALERT`
4) Uncomment the format `output log_tcpdump: snort.log`
5) Uncomment the format `include c:\Snort\rules\classification.config`
6) Uncomment the format `include c:\Snort\rules\reference.config`
7) Use database format as `output database: alert, mysql, user=root password=wazed dbname=ids host=localhost`
8) Use database format as `output database: log, mysql, user=root password=wazed dbname=tcpdump host=localhost`
9) Copies all 10 Snort rules to be tested into c:\Snort\rules\local.rules file, and keep the include file as `include $RULE_PATH/local.rules`. All other include rules file should be commented unless is required.
10) Keep the preprocessors configuration as it is
11) Save the configuration file and exit.

iv) Testing of Snort :

To test, execute the command within the c:\Snort\bin directory:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>cd\
C:\>cd snort\bin
C:\Snort\bin>snort -A console -v -i2
Running in packet dump mode
Initializing Network Interface \Device\NPF_{1B5F3736-6D03-4434-BFC4-BEACCC5B6594}
        --== Initializing Snort ==--
Initializing Output Plugins!
Decoding Ethernet on interface \Device\NPF_{1B5F3736-6D03-4434-BFC4-BEACCC5B6594}
        --== Initialization Complete ==--
   ,,_     -*> Snort! <*-
  o"  )~   Version 2.4.3-ODBC-MySQL-FlexRESP-WIN32 (Build 26)
   ''''    By Martin Roesch & The Snort Team:
http://www.snort.org/team.html
           (C) Copyright 1998-2005 Sourcefire Inc., et al.
 NOTE: Snort's default output has changed in version 2.4.1!
       The default logging mode is now PCAP, use "-K ascii" to activate
       the old default logging mode.

03/09-10:24:08.907866 192.168.1.100:1281 -> 192.168.1.1:5678
TCP TTL:128 TOS:0x0 ID:4154 IpLen:20 DgmLen:48 DF
******S* Seq: 0xC10E62D1  Ack: 0x0  Win: 0xFFFF  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

..........................................................................................................................
..........................................................................................................................

03/09-10:24:30.089210 192.168.1.100:1282 -> 192.168.1.1:5678
TCP TTL:128 TOS:0x0 ID:4161 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0xAFC874AA  Ack: 0x18770C  Win: 0x0  TcpLen: 20
===========================================================================
Snort received 46 packets
    Analyzed: 46(100.000%)
    Dropped: 0(0.000%)
===========================================================================
Breakdown by protocol:
    TCP: 20         (43.478%)
    UDP: 15         (32.609%)
   ICMP: 1          (2.174%)
    ARP: 10         (21.739%)
  EAPOL: 0          (0.000%)
   IPv6: 0          (0.000%)
ETHLOOP: 0          (0.000%)
    IPX: 0          (0.000%)
   FRAG: 0          (0.000%)
  OTHER: 0          (0.000%)
DISCARD: 0          (0.000%)
==========================================================================

Action Stats:
ALERTS: 1
LOGGED: 1
PASSED: 0
===========================================================================
Snort exiting
```

From a separate machine, use nmap to generate events for Snort to detect:

```
nmap –sP 192.168.1.100
```

An alert would be seen like this:

```
03/09-10:38:06.911226 [**] [1:469:1] ICMP PING NMAP [**][Classification:
Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.101 ->
192.168.1.100
```

Some other necessary Snort commands are as follows :

To run the snort using rule files and be verbose for interface i2, use the command

-
  ```
  snort -c C:\snort\etc\snort.conf –v -i2
  ```

This will apply the rules configured in the snort.conf file to each packet to decide if an action based upon the rule type in the file should be taken.

To save the log files into snort\log directory, use the command

-
  ```
  snort -dv -l c:\snort\log -h 192.168.1.100/24 -c
    C:\snort\etc\snort.conf
  ```

If no output directory is specified, it will default to .\snort\bin\log directory.

To save the payload into a text file, use the command

-
  ```
  snort -dv -v -i2 > c:\snort\log\saveLog.txt
  ```

where the payloads will be saves into "saveLog.txt" file

Use the following command line to log to the default facility in /var/log/snort and send alerts to a fast alert file:

-
  ```
  snort -c c:\snort\etc\snort.conf  -b -A fast -v -i2
  ```

Two files, alert.ids and snort.log.***, will be generate under C:\Snort\bin\log\ directory

The content of *alert.ids* file is look like as :

```
03/05-10:22:43.093983  [**] [1:1384:8] MISC UPnP malformed advertisement
[**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.1.1:1900 ->
239.255.255.250:1900
03/05-10:23:20.626936  [**] [1:540:11] CHAT MSN message [**]
[Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP}
192.168.1.100:1237 -> 65.54.228.46:1863
03/08-05:02:16.732529  [**] [1:999999:1] Wazed TCP traffic [**] [Priority:
0] {TCP} 64.124.109.223:80 -> 192.168.1.100:2392
03/08-05:02:19.070266  [**] [1:1384:8] MISC UPnP malformed advertisement
[**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.1.1:1900 ->
239.255.255.250:1900
```

(*where, rule# 999999, rev 1, is user defined rule for TCP traffic*)

6. Installation of ASC Desktop

ASC Desktop will allow us to view IDS data in many different ways, some of them include:

- Unique Views
- List Views
- Interactive Graphs and charts
- Event Relationship Diagrams
- Payload decoders

ASC for IDS has 3 parts

- ASC Desktop
- Database Servers
- Sensors

Two Different types of Databases, Primary Database and Event Databases, are used. It Support for unlimited sensors/devices per database and can be installed on any operating system. We will use the default Snort IDS database schema.

Sensors are computers running Snort IDS with the Database output plug-in. It works with Snort 1.8 or newer.

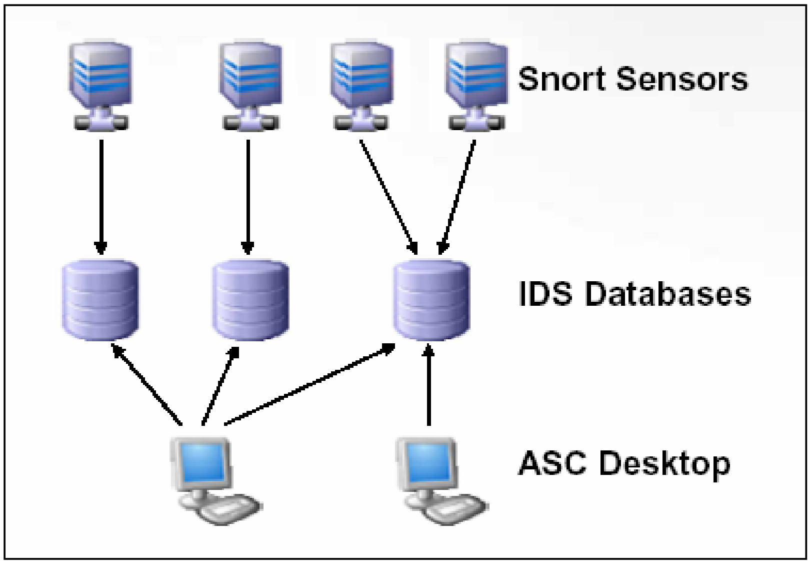


Fig 12 : 3 parts of ASC for IDS

Minimum system requirements for the ASC Desktop

- CPU : Pentium 4 or later
- Memory : 512 MB of greater
- Available Disk Space : 250MB
- Operating System : Any OS that runs MySQL, Windows for MS SQL

i) Download the Activeworx Installer files

Download the BrightTools product of ASC components for 15 days evaluation from the site http://www.brighttools.com/support/download.html#. There are 5 Microsoft Installer files for download.

ASC Desktop – asc.desktop.msi of size 55.7 MB

ASC Manager – asc.manager.msi of size 51.1 MB

ASC Network Collector – asc.network.collector.msi of size 4 MB

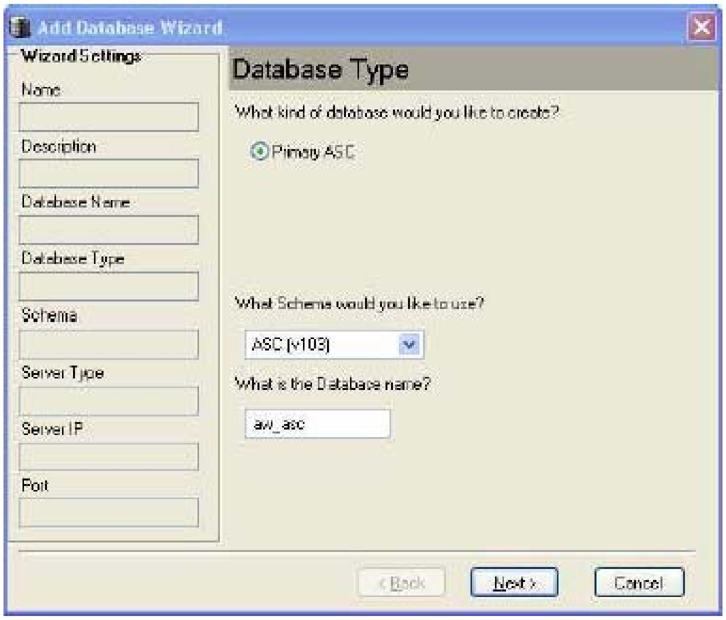
ASC Windows Evemtlog Collector – asc.winlog.collector.msi of size 5 MB and

ASC Check Point Collector – asc.checkpoint.collector.msi of size 4.2 MB

Run all the above files to install ASC Desktop application.

ii) Primary Database

We need to configure the primary database when running ASC Desktop for the first time.



What kind of database would you like to create?

● Primary ASC

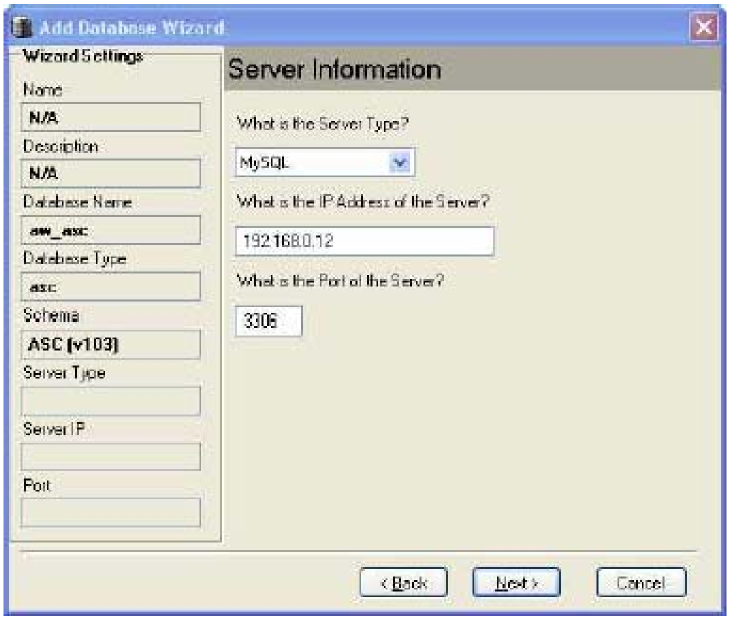
What Schema would you like to use?

ASC (v103)

What is the Database name?

aw_asc

Fig 13 : Creating the primary database *aw_asc* by using *ASC(v103)* schema



Add Database Wizard

Wizard Settings

Name: N/A

Description: N/A

Database Name: aw_asc

Database Type: asc

Schema: ASC (v103)

Server Type:

Server IP:

Port:

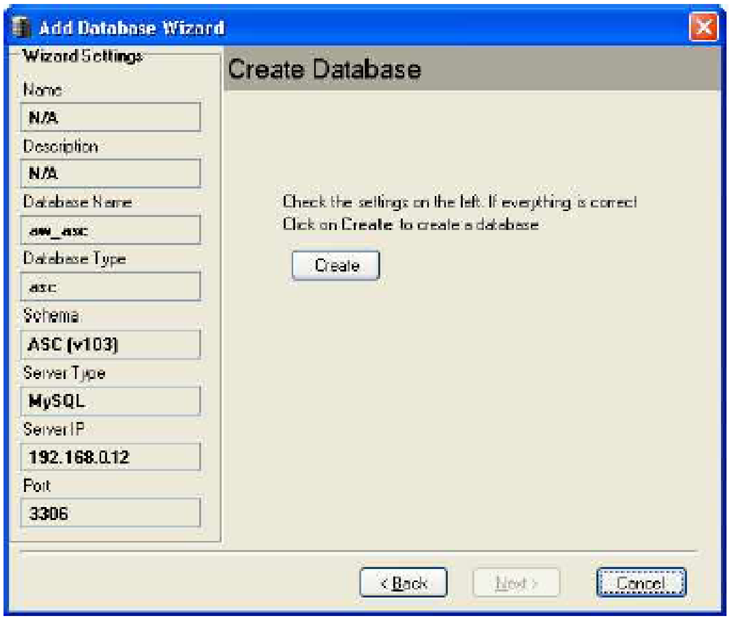
Server Information

What is the Server Type? MySQL

What is the IP Address of the Server? 192.168.0.12

What is the Port of the Server? 3306

Fig 14 : Configure the MySQL server information



Add Database Wizard

Wizard Settings

Name: N/A

Description: N/A

Database Name: aw_asc

Database Type: asc

Schema: ASC (v103)

Server Type: MySQL

Server IP: 192.168.0.12

Port: 3306

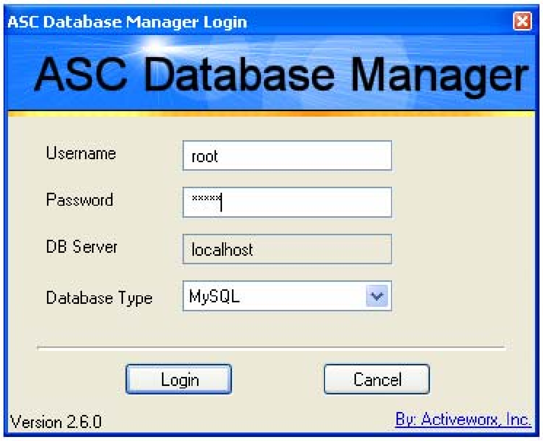
Create Database

Check the settings on the left. If everything is correct
Click on Create to create a database

Fig 15 : Create the database from entered setting

iii) Event Database :

To create Event Database, log into database server with user name and password.



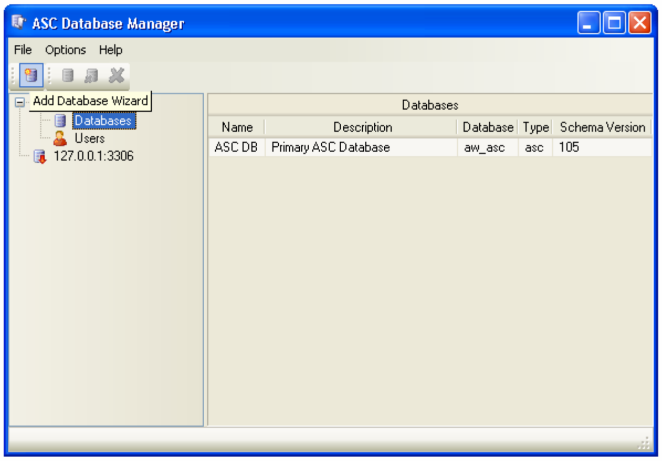
Username: root

Password: *****

DB Server: localhost

Database Type: MySQL

Fig 16 : Log-in into ASC Database Manager

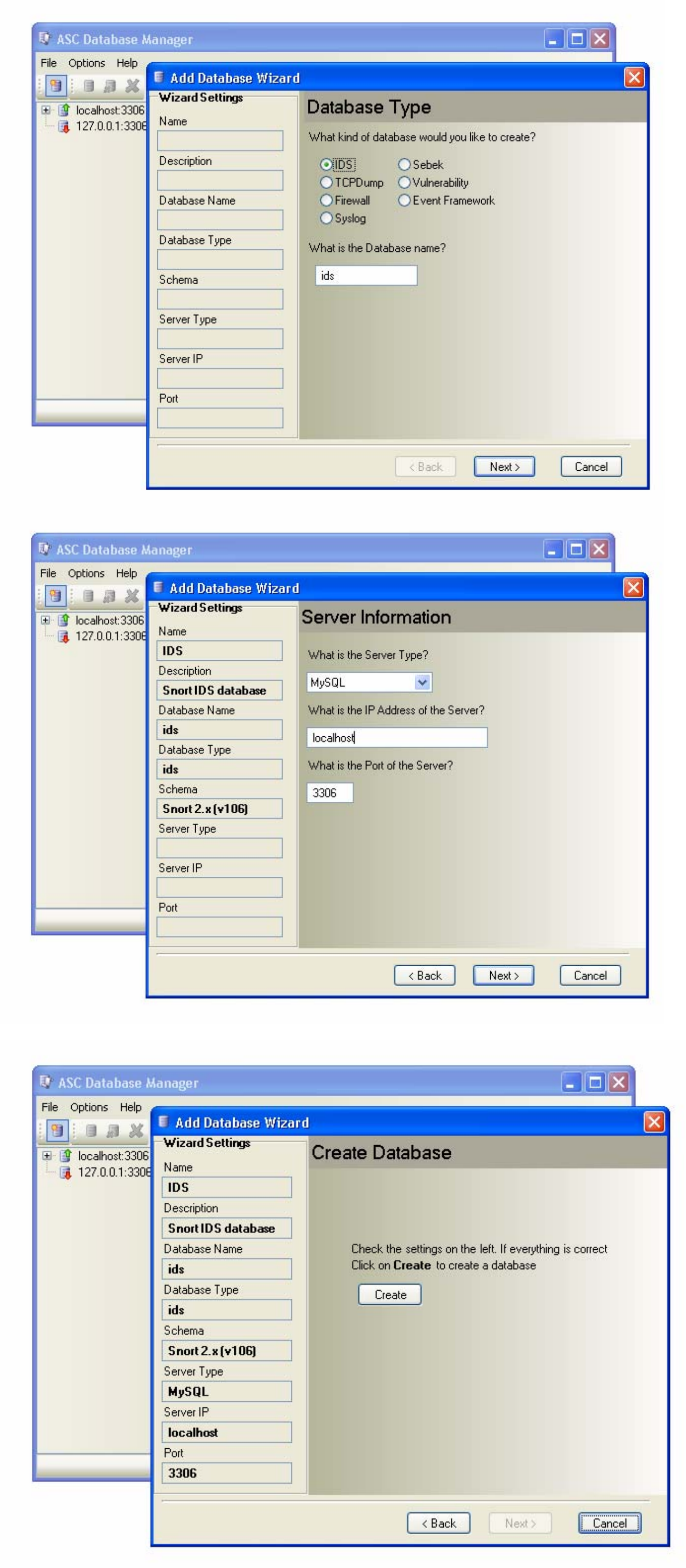


Name	Description	Database	Type	Schema Version
ASC DB	Primary ASC Database	aw_asc	asc	105

Fig 17 : ASC Database Manger displaying its Primary Database as aw_asc

Click on *Add Database Wizard* icon, configure the database setting and enter database server information to create an event database. There are 6 kind of event database in ASC to create, these are –

1. IDS
2. TCPDump
3. Firewall
4. Syslog
5. Sebek
6. Vulnerability



Database Type

What kind of database would you like to create?

● IDS ○ Sebek
○ TCPDump ○ Vulnerability
○ Firewall ○ Event Framework
○ Syslog

What is the Database name?

ids

Server Information

Name	IDS
Description	Snort IDS database
Database Name	ids
Database Type	ids
Schema	Snort 2.x (v106)

What is the Server Type?

MySQL

What is the IP Address of the Server?

localhost

What is the Port of the Server?

3306

Create Database

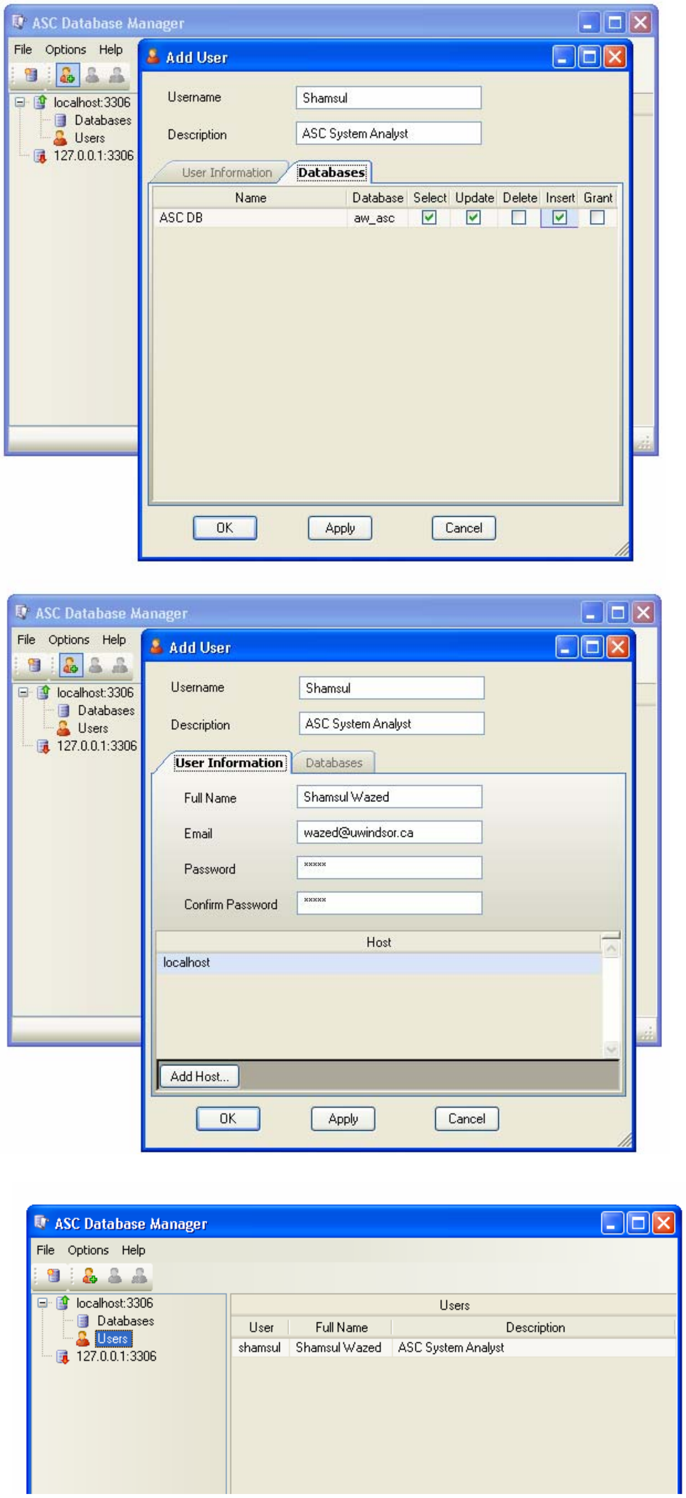
Name	IDS
Description	Snort IDS database
Database Name	ids
Database Type	ids
Schema	Snort 2.x (v106)
Server Type	MySQL
Server IP	localhost
Port	3306

Check the settings on the left. If everything is correct
Click on **Create** to create a database

Create

Fig 18 : Steps to create an Event Database (IDS) using ASC Database Manger

To create a new user to work with ASC Desktop, click on *Add User* icon. Fill the user information and set the new users permissions as follows –



Username: Shamsul

Description: ASC System Analyst

Name	Database	Select	Update	Delete	Insert	Grant
ASC DB	aw_asc	☑	☑	☐	☑	☐

Full Name: Shamsul Wazed

Email: wazed@uwindsor.ca

Password: *****

Confirm Password: *****

Host
localhost

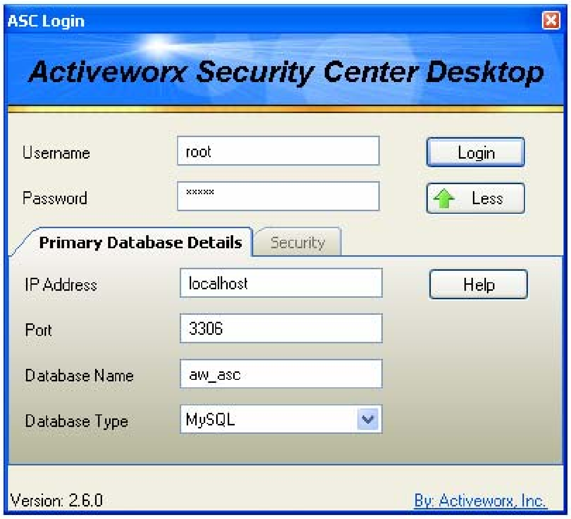
Users

User	Full Name	Description
shamsul	Shamsul Wazed	ASC System Analyst

Fig 19 : Steps to create a new user using ASC Database Manger

iv) ASC Desktop :

ASC Desktop is now installed and ready to use. Before the ASC Desktop, Snort should be run in background. Click on *ASC Desktop* icon to logon by using username and password.

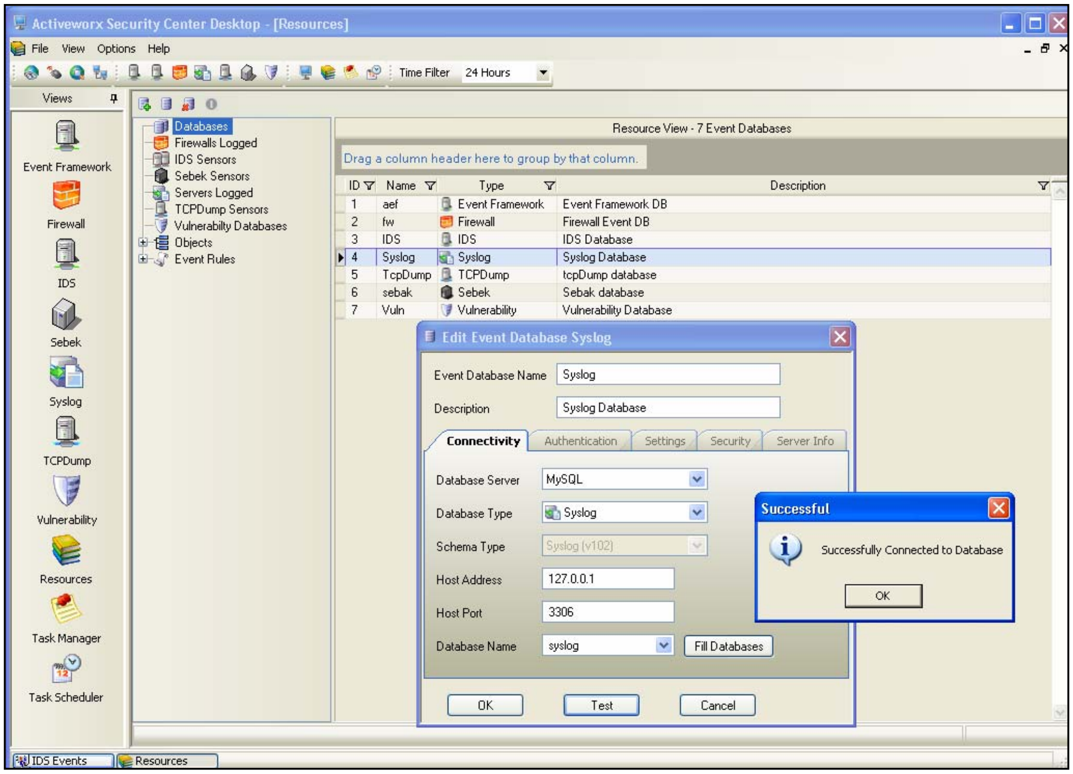


Username	root
Password	*****
IP Address	localhost
Port	3306
Database Name	aw_asc
Database Type	MySQL

Version: 2.6.0

Fig 20 : ASC Desktop login window

The resources form is used to add existing snort databases, delete/edit databases that are viewable within ASC Desktop, and view the sensors that are in each of the databases. This form can be view by clicking on the *Resource* menu item that is located on the side menu.



Resource View - 7 Event Databases

ID	Name	Type	Description
1	aef	Event Framework	Event Framework DB
2	fw	Firewall	Firewall Event DB
3	IDS	IDS	IDS Database
4	Syslog	Syslog	Syslog Database
5	TcpDump	TCPDump	tcpDump database
6	sebak	Sebek	Sebak database
7	Vuln	Vulnerability	Vulnerability Database

Edit Event Database Syslog

Event Database Name	Syslog
Description	Syslog Database
Database Server	MySQL
Database Type	Syslog
Schema Type	Syslog (v102)
Host Address	127.0.0.1
Host Port	3306
Database Name	syslog

Successful

Successfully Connected to Database

OK

Fig 21 : Adding/editing snort database from Resource form

When adding snort databases from this form, the database must already exist, otherwise the database must be created by using the Database Manager. The database setting can be edited by double clicking on the database icon.

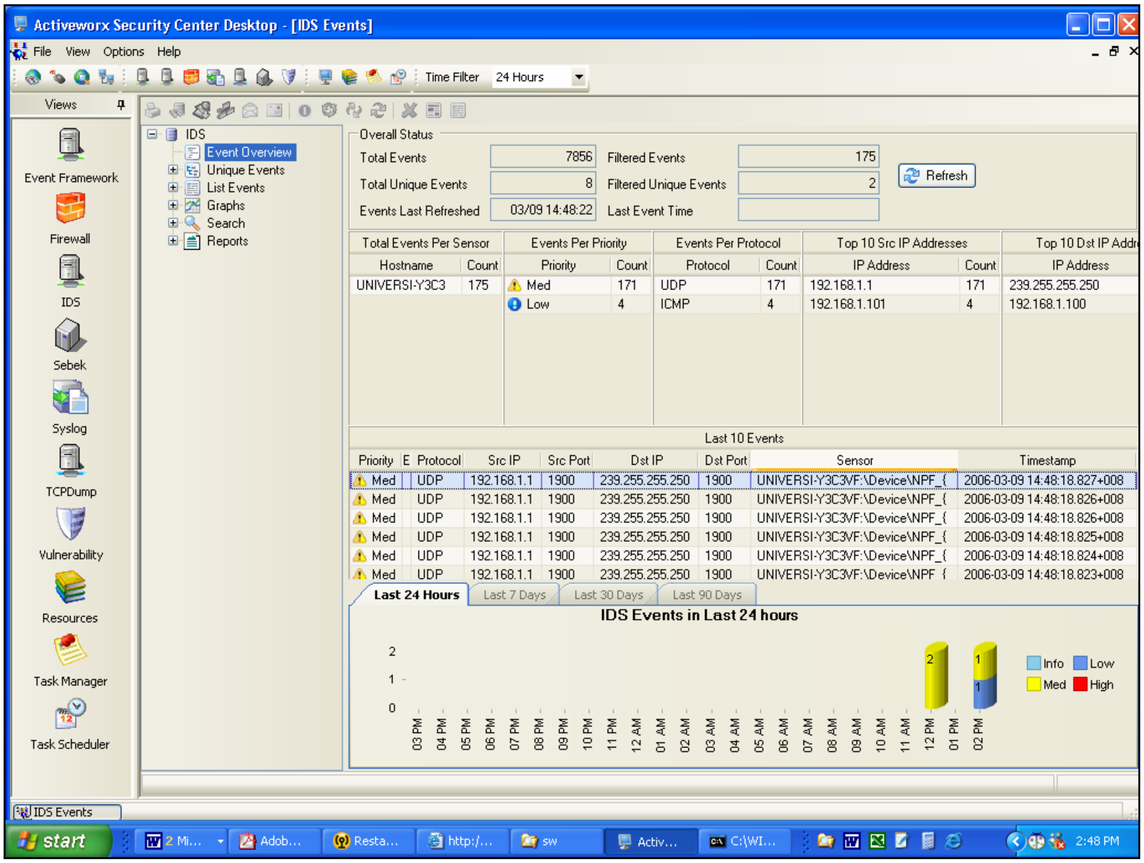
7. How to work with the Project

PC 1 (IP : 192.168.1.100) - Run *Snort* from console by using the command from c:\snort\bin, `snort -c c:\snort\etc\snort.conf -h 192.168.1.100/24 -v -i2.` Logon into *ASC Desktop* and open IDS form. Run CommView for packet analyzing and monitoring purpose.

PC 2 (IP : 192.168.1.101) - Run CommView for packet analyzing and monitoring purpose. Generate packet (ICMP/TCP/UDP) with Snort signature and send to PC2 via switch.

i) Event Overview

Click on *IDS* form and select *Event Overview*



Time Filter 24 Hours

Overall Status

Total Events	7856	Filtered Events	175
Total Unique Events	8	Filtered Unique Events	2
Events Last Refreshed	03/09 14:48:22	Last Event Time	

Total Events Per Sensor		Events Per Priority		Events Per Protocol		Top 10 Src IP Addresses		Top 10 Dst IP Addr
Hostname	Count	Priority	Count	Protocol	Count	IP Address	Count	IP Address
UNIVERSI-Y3C3	175	⚠ Med	171	UDP	171	192.168.1.1	171	239.255.255.250
		● Low	4	ICMP	4	192.168.1.101	4	192.168.1.100

Last 10 Events

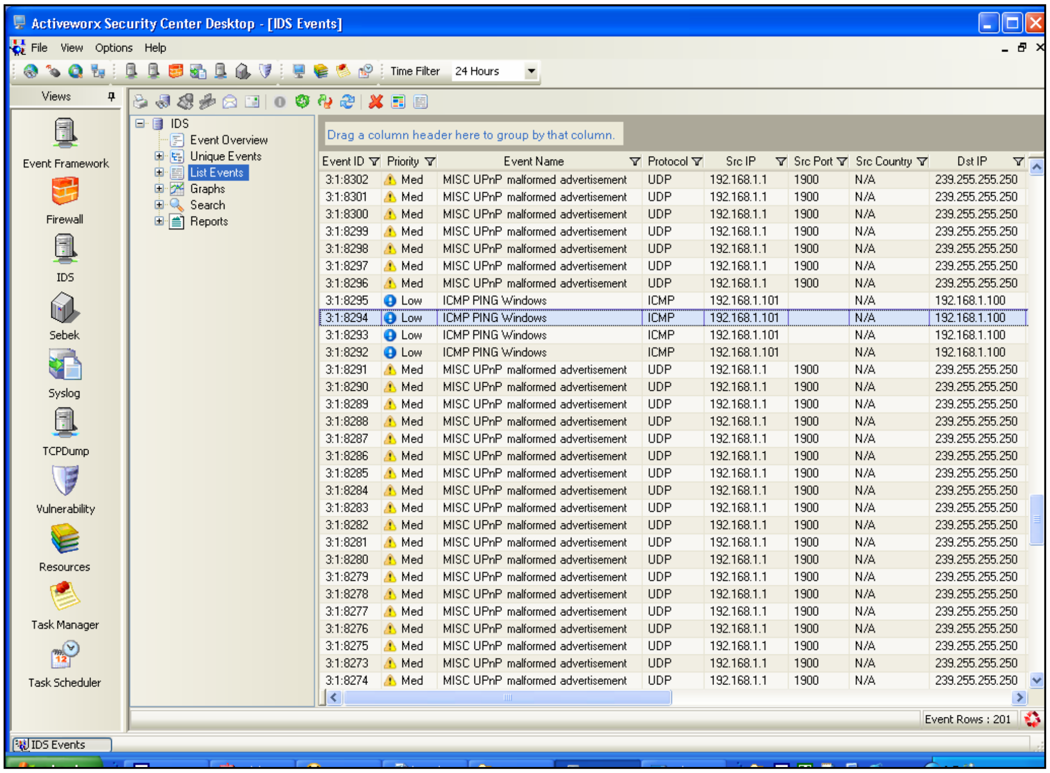
Priority	E	Protocol	Src IP	Src Port	Dst IP	Dst Port	Sensor	Timestamp
⚠ Med		UDP	192.168.1.1	1900	239.255.255.250	1900	UNIVERSI-Y3C3VF:\Device\NPF_{	2006-03-09 14:48:18.827+008
⚠ Med		UDP	192.168.1.1	1900	239.255.255.250	1900	UNIVERSI-Y3C3VF:\Device\NPF_{	2006-03-09 14:48:18.826+008
⚠ Med		UDP	192.168.1.1	1900	239.255.255.250	1900	UNIVERSI-Y3C3VF:\Device\NPF_{	2006-03-09 14:48:18.826+008
⚠ Med		UDP	192.168.1.1	1900	239.255.255.250	1900	UNIVERSI-Y3C3VF:\Device\NPF_{	2006-03-09 14:48:18.825+008
⚠ Med		UDP	192.168.1.1	1900	239.255.255.250	1900	UNIVERSI-Y3C3VF:\Device\NPF_{	2006-03-09 14:48:18.824+008
⚠ Med		UDP	192.168.1.1	1900	239.255.255.250	1900	UNIVERSI-Y3C3VF:\Device\NPF_{	2006-03-09 14:48:18.823+008

Fig 22 : Event Overview from IDS database

An Event Overview shows the Host name, Top 10 source and destination addresses. It also shows the total number of event with their corresponding timestamp. It shows last 10 events with detail. At the end of the window a 3-D graph is plotted taking for last 24 hours events.

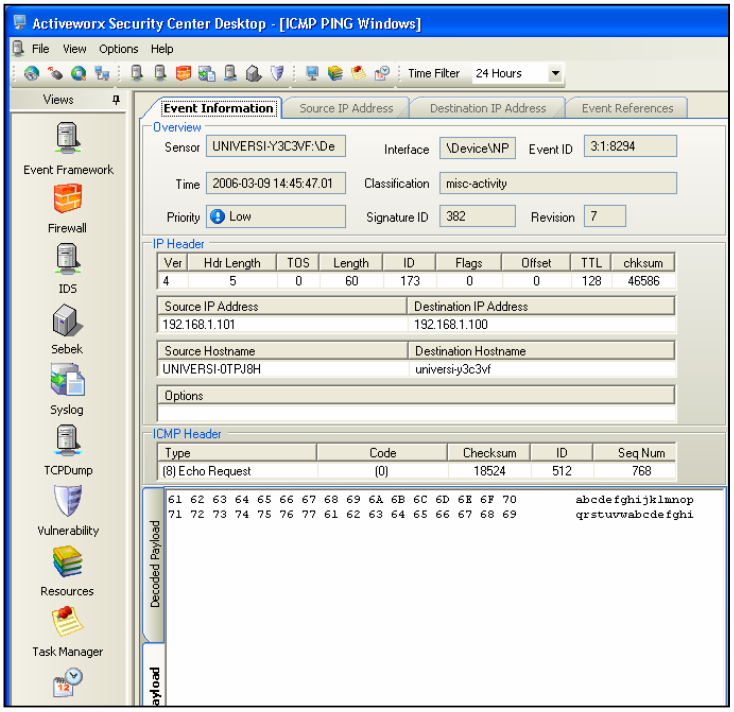
ii) List Events

To view the alert files click on *List Events*.



Event ID	Priority	Event Name	Protocol	Src IP	Src Port	Src Country	Dst IP
3:1:8302	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8301	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8300	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8299	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8298	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8297	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8296	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8295	Low	ICMP PING Windows	ICMP	192.168.1.101		N/A	192.168.1.100
3:1:8294	Low	ICMP PING Windows	ICMP	192.168.1.101		N/A	192.168.1.100
3:1:8293	Low	ICMP PING Windows	ICMP	192.168.1.101		N/A	192.168.1.100
3:1:8292	Low	ICMP PING Windows	ICMP	192.168.1.101		N/A	192.168.1.100
3:1:8291	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8290	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8289	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8288	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8287	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8286	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8285	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8284	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8283	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8282	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8281	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8280	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8279	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8278	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8277	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8276	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8275	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8273	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250
3:1:8274	Med	MISC UPnP malformed advertisement	UDP	192.168.1.1	1900	N/A	239.255.255.250

Fig 23 : View alert files from IDS database



Overview

Sensor	UNIVERSI-Y3C3VF:\De	Interface	\Device\NP	Event ID	3:1:8294
Time	2006-03-09 14:45:47.01	Classification	misc-activity		
Priority	Low	Signature ID	382	Revision	7

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	60	173	0	0	128	46586

Source IP Address	Destination IP Address
192.168.1.101	192.168.1.100

Source Hostname	Destination Hostname
UNIVERSI-0TPJ8H	universi-y3c3vf

Options

ICMP Header

Type	Code	Checksum	ID	Seq Num
(8) Echo Request	(0)	18524	512	768

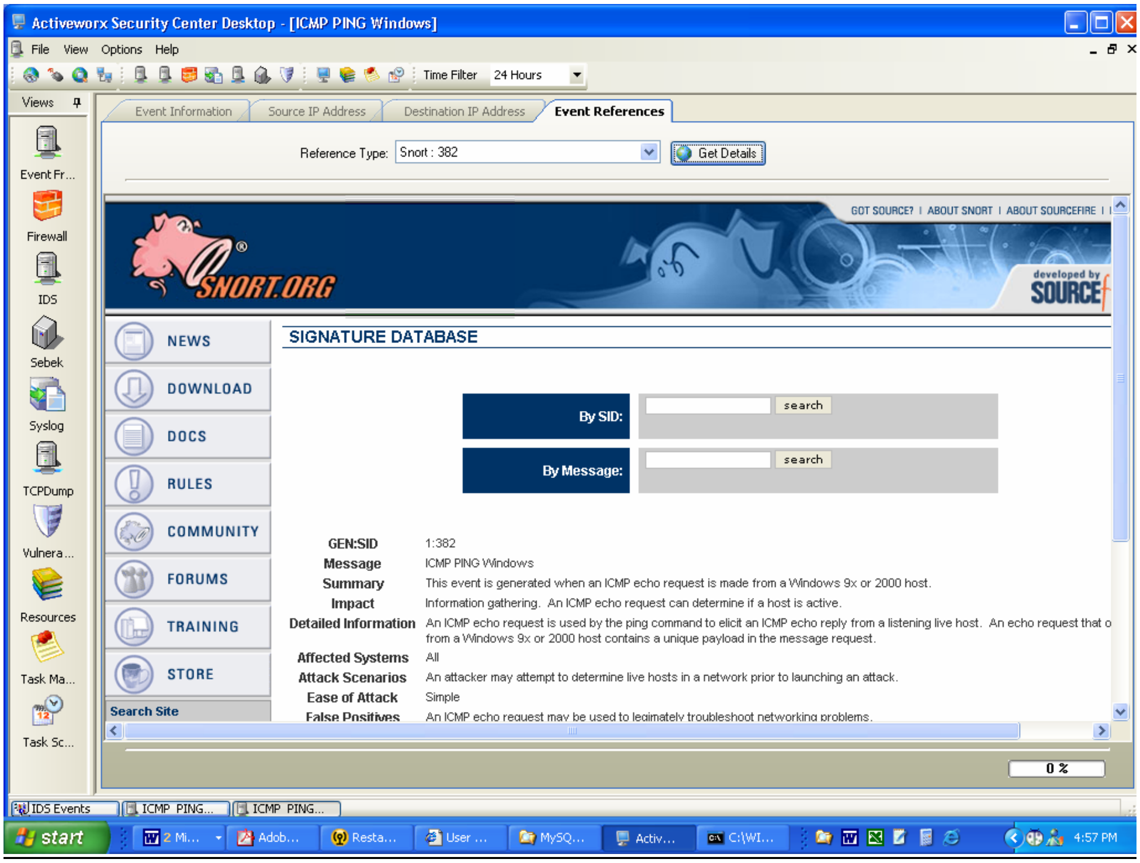
```
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70        abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69        qrstuvwabcdefghi
```

Fig 24 : Event Information when a ICMP Ping is sent from

192.168.1.101 to 192.168.1.100 which is with Snort signature of rule 382

IDS Event Details form displays (Fig 13) the details of an individual event. This includes an overview of the event, IP, TCP, UDP and ICMP Header information and a payload decoder. This form also allows us to get more information about the Source IP Address, Destination IP Address and Event References from the Internet.

To view the event reference, double click the selected event from the table shown in *List Event* form (Fig 12). Select the tab *Event Reference* and then click on button *Get Detail*. The figure below (Fig 14) shows such an event of Signature ID 382 of Message ICMP PING Windows. The event references use the references that are included with each IDS signature to go out to the Internet and find more details about the event and why it could have triggered.



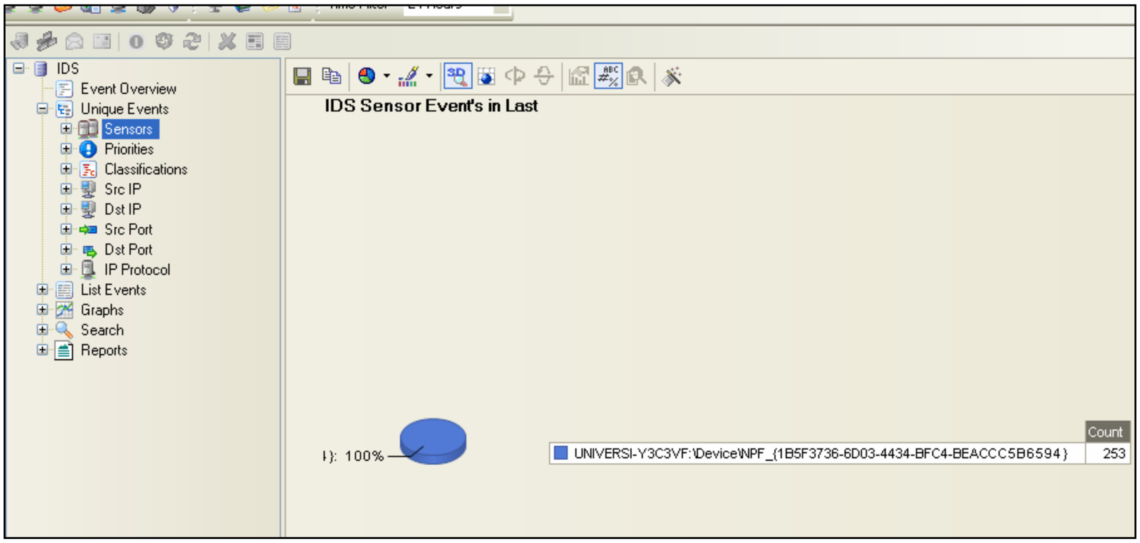
Reference Type: Snort : 382

GEN:SID	1:382
Message	ICMP PING Windows
Summary	This event is generated when an ICMP echo request is made from a Windows 9x or 2000 host.
Impact	Information gathering. An ICMP echo request can determine if a host is active.
Detailed Information	An ICMP echo request is used by the ping command to elicit an ICMP echo reply from a listening live host. An echo request that o from a Windows 9x or 2000 host contains a unique payload in the message request.
Affected Systems	All
Attack Scenarios	An attacker may attempt to determine live hosts in a network prior to launching an attack.
Ease of Attack	Simple
False Positives	An ICMP echo request may be used to legimately troubleshoot networking problems.

Fig 25 : *Event Reference* for a selected event from *List Event* IDS form

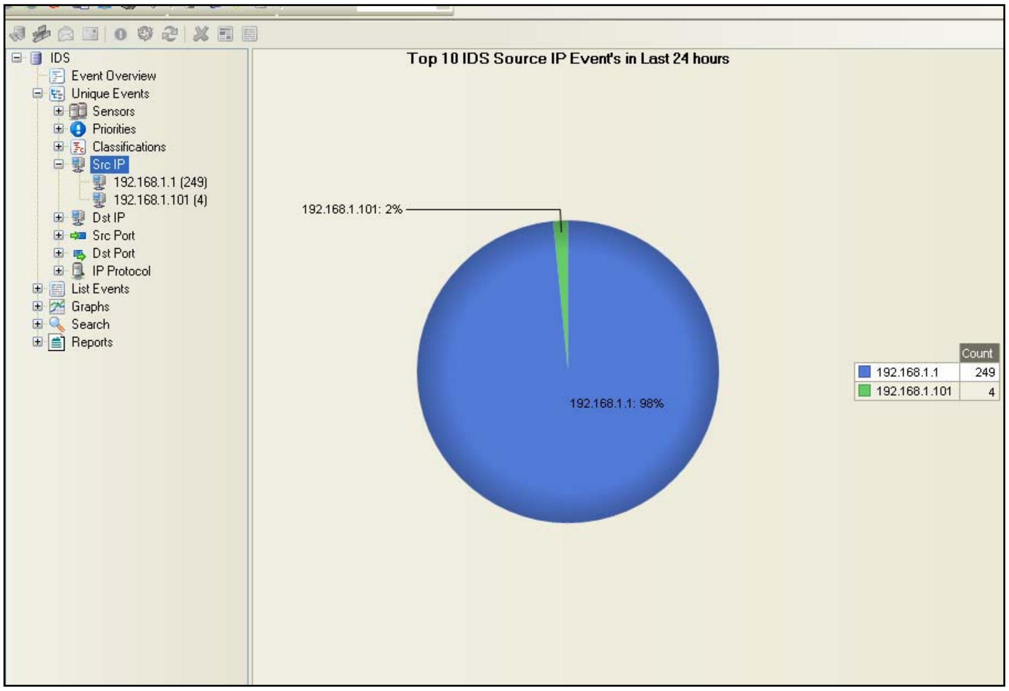
iii) Unique Events

By right clicking on a unique event we now have a context menu that will dropdown and give us a list of items that can be performed on the selected unique event.



	Count
🟦 UNIVERSI-Y3C3VF:\Device\NPF_{1B5F3736-6D03-4434-BFC4-BEACCC5B6594}	253

Fig 26 : *Sensors* showing IDS Sensor Events

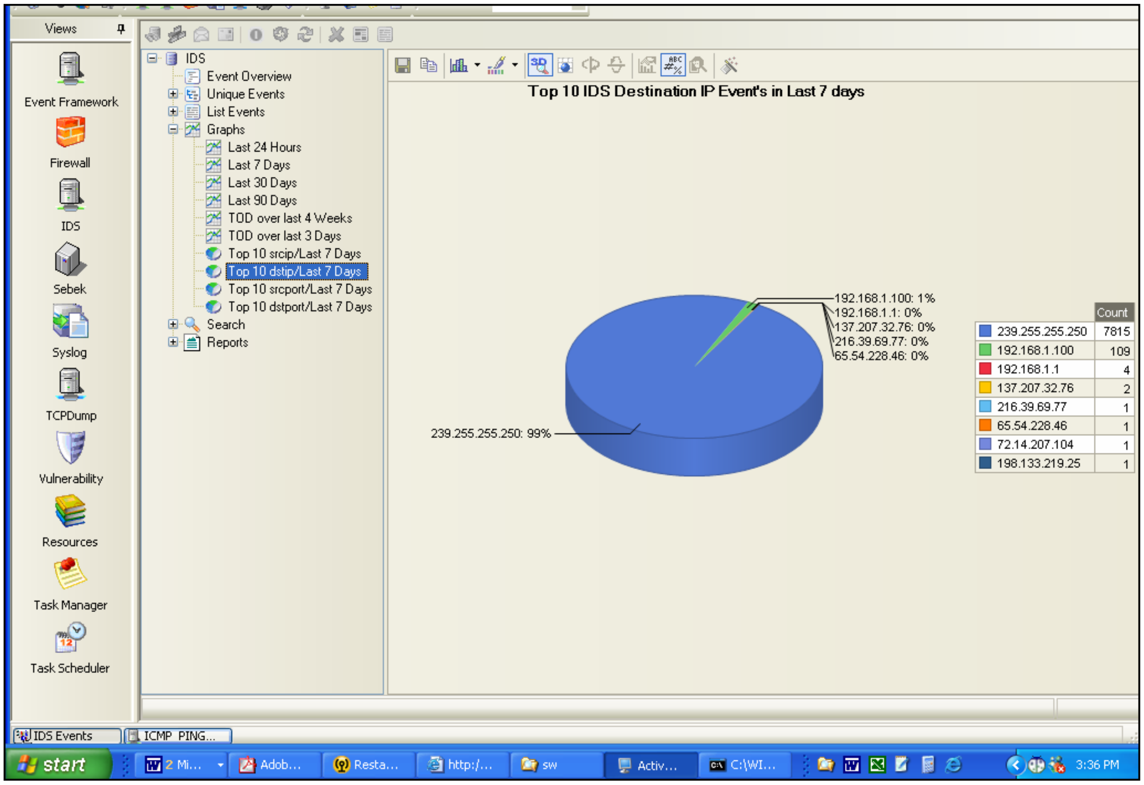


	Count
🟦 192.168.1.1	249
🟩 192.168.1.101	4

Fig 27 : *Src IP* showing Top IDS Source IP Events in Last 24 hours

iv) Graphs

All Graphs within ASC are fully interactive. There are currently 3 types of graphs: Time, Top 10, and Time of Day over a period of time. This graph shows events that have occurred over the last 7 days and highlights them based on Priority. From this graph we can have the ability to drill down into each day to view a daily graph, or view events for each day and priority level.



	Count
🟦 239.255.255.250	7815
🟩 192.168.1.100	109
🟥 192.168.1.1	4
🟨 137.207.32.76	2
🟦 216.39.69.77	1
🟧 65.54.228.46	1
🟪 72.14.207.104	1
🟦 198.133.219.25	1

Fig 28 : *Top 10 distip/Last 7 Days* showing destination IP's in Last 7 days

v) Reports

Reports are displayed using the Crystal Reports reporting engine. This report maps the source IP's and displays them in a nice report based on country. There are currently 8 reports, but each report is more of a template. Each report can be customized within ASC to display the information that is of interest to you. These custom reports can be saved and later retrieved with a couple of mouse clicks.

Reports can be fully customizable to display any information that you would like in them. Reports can also be exported to common formats such as word, Excel and Adobe Acrobat, as well as printed from within ASC Desktop.

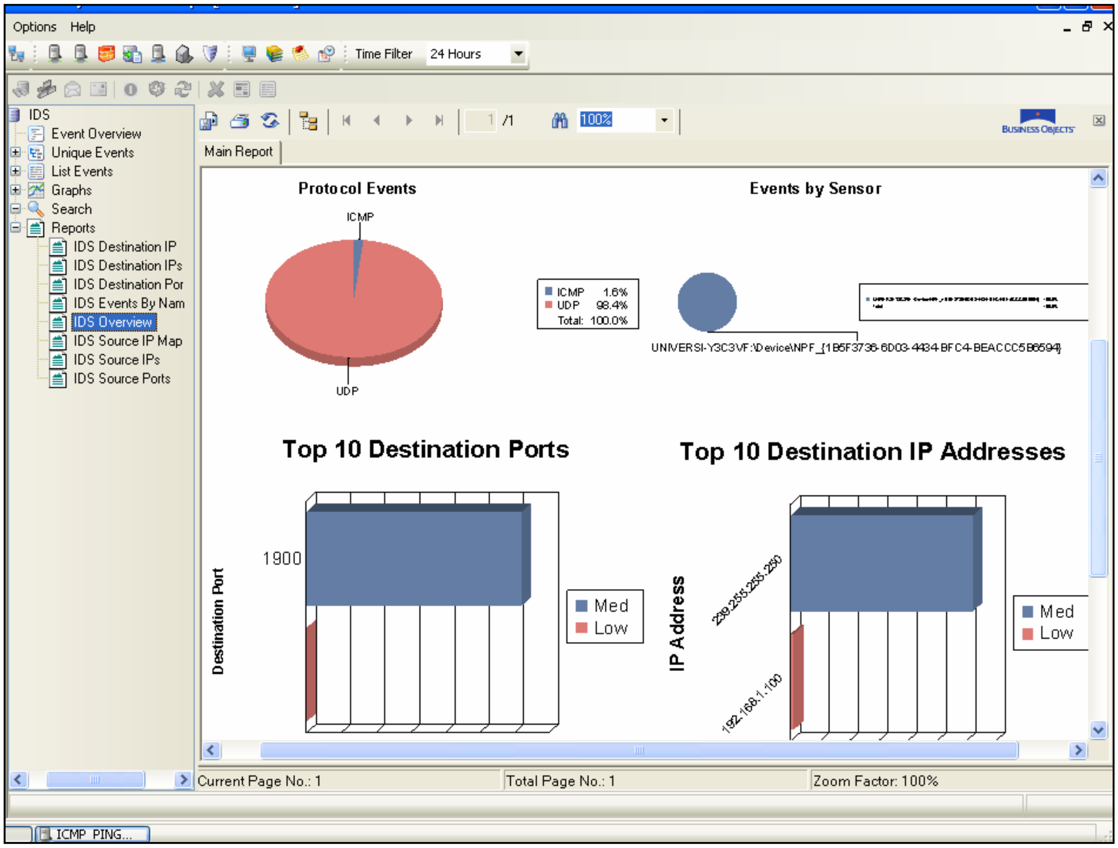
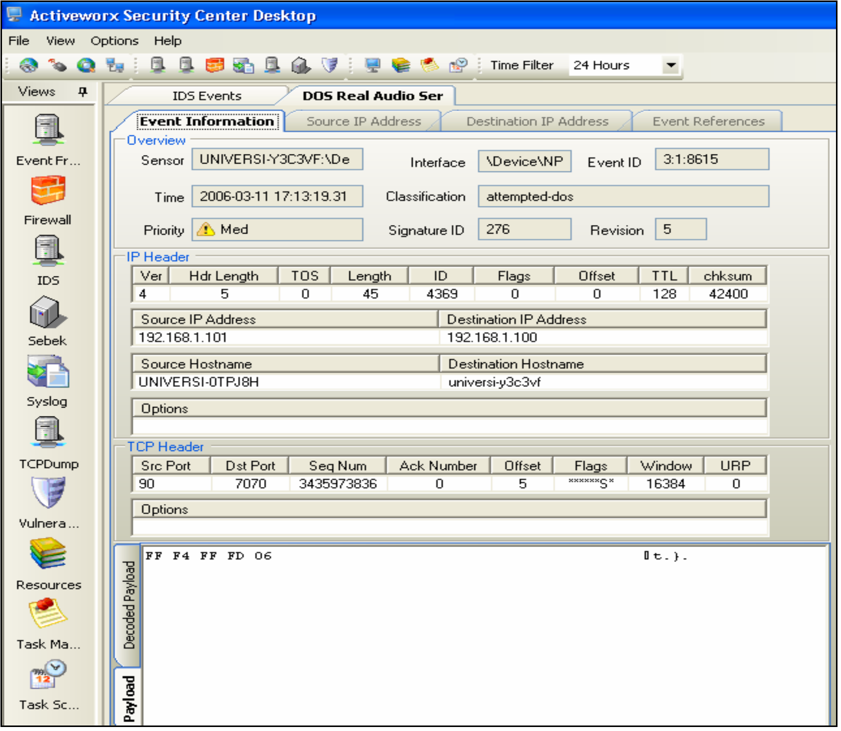


Fig 29 : Generating report of IDS overview by selecting *IDS Overview* from report submenu

8. Capturing the Packets with 10 Snort Signatures :

The following are some Snapshots of ASC Desktop IDS form when it captures files with Snort specific 10 signatures. The screenshots of capture is given below :

Signature ID: 276
Message: DOS Real Audio Server



Overview

Sensor: UNIVERSI-Y3C3VF:\De
Interface: \Device\NP
Event ID: 3:1:8615
Time: 2006-03-11 17:13:19.31
Classification: attempted-dos
Priority: Med
Signature ID: 276
Revision: 5

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	45	4369	0	0	128	42400

Source IP Address	Destination IP Address
192.168.1.101	192.168.1.100

Source Hostname	Destination Hostname
UNIVERSI-0TPJ8H	universi-y3c3vf

Options

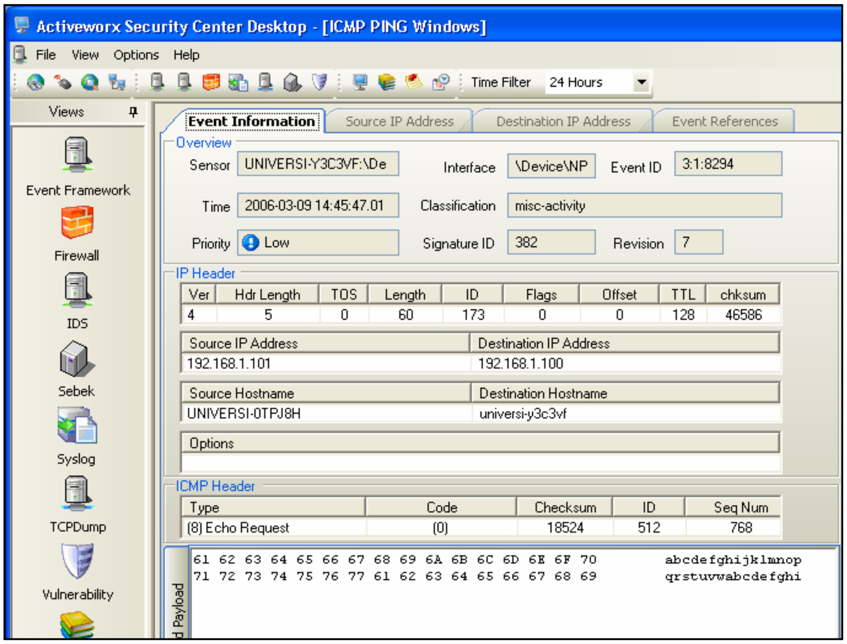
TCP Header

Src Port	Dst Port	Seq Num	Ack Number	Offset	Flags	Window	URP
90	7070	3435973836	0	5	******S*	16384	0

Options

```
FF F4 FF FD 06                                          Ӏt.}.
```

Signature ID: 382
Message: ICMP PING Windows



Overview

Sensor: UNIVERSI-Y3C3VF:\De
Interface: \Device\NP
Event ID: 3:1:8294
Time: 2006-03-09 14:45:47.01
Classification: misc-activity
Priority: Low
Signature ID: 382
Revision: 7

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	60	173	0	0	128	46586

Source IP Address	Destination IP Address
192.168.1.101	192.168.1.100

Source Hostname	Destination Hostname
UNIVERSI-0TPJ8H	universi-y3c3vf

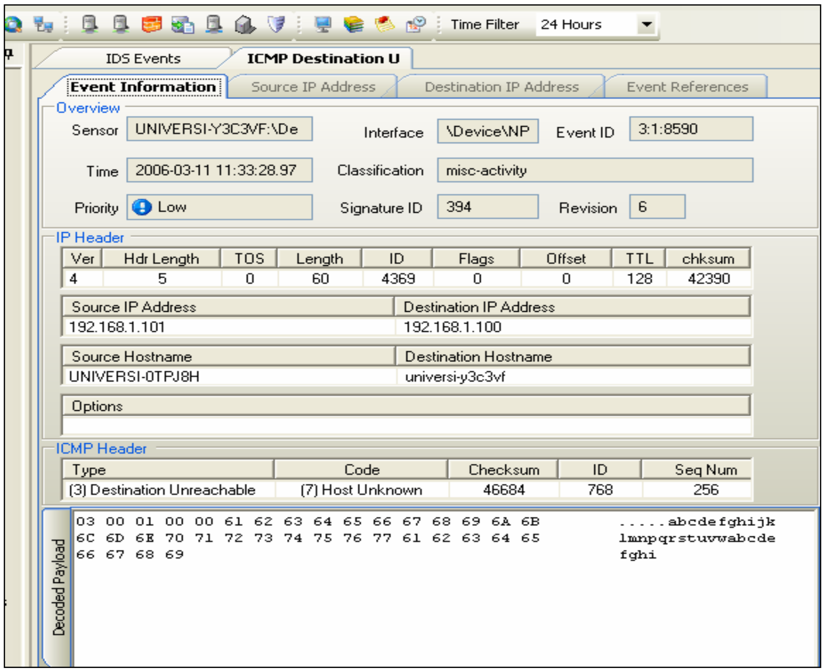
Options

ICMP Header

Type	Code	Checksum	ID	Seq Num
(8) Echo Request	(0)	18524	512	768

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

Signature ID: 394
Message: ICMP Destination Unreachable Destination Host Unknown



Overview

Sensor	UNIVERSI-Y3C3VF:\De	Interface	\Device\NP	Event ID	3:1:8590
Time	2006-03-11 11:33:28.97	Classification	misc-activity		
Priority	Low	Signature ID	394	Revision	6

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	60	4369	0	0	128	42390

Source IP Address	Destination IP Address
192.168.1.101	192.168.1.100

Source Hostname	Destination Hostname
UNIVERSI-0TPJ8H	universi-y3c3vf

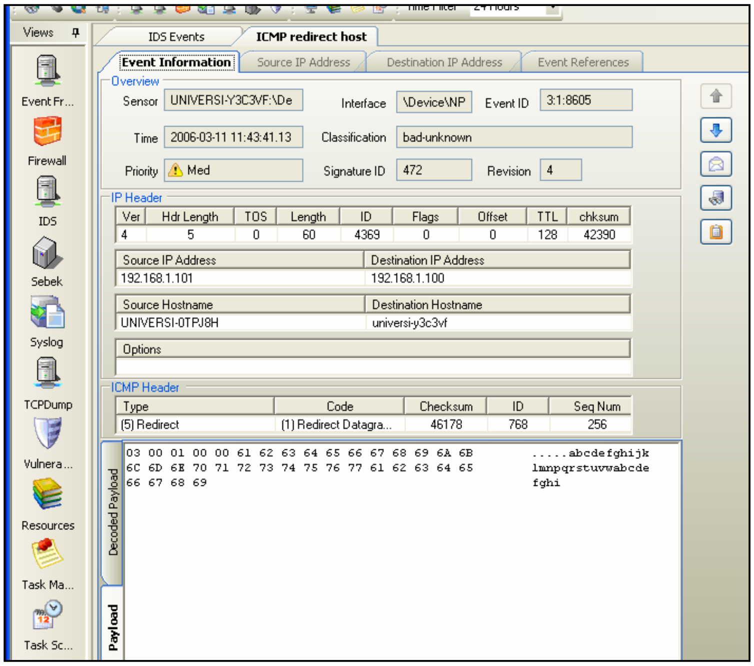
Options

ICMP Header

Type	Code	Checksum	ID	Seq Num
(3) Destination Unreachable	(7) Host Unknown	46684	768	256

```
03 00 01 00 00 61 62 63 64 65 66 67 68 69 6A 6B        .....abcdefghijk
6C 6D 6E 70 71 72 73 74 75 76 77 61 62 63 64 65        lmnpqrstuvwabcde
66 67 68 69                                            fghi
```

Signature ID: 472
Message: ICMP Redirect Host



Overview

Sensor	UNIVERSI-Y3C3VF:\De	Interface	\Device\NP	Event ID	3:1:8605
Time	2006-03-11 11:43:41.13	Classification	bad-unknown		
Priority	Med	Signature ID	472	Revision	4

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	60	4369	0	0	128	42390

Source IP Address	Destination IP Address
192.168.1.101	192.168.1.100

Source Hostname	Destination Hostname
UNIVERSI-0TPJ8H	universi-y3c3vf

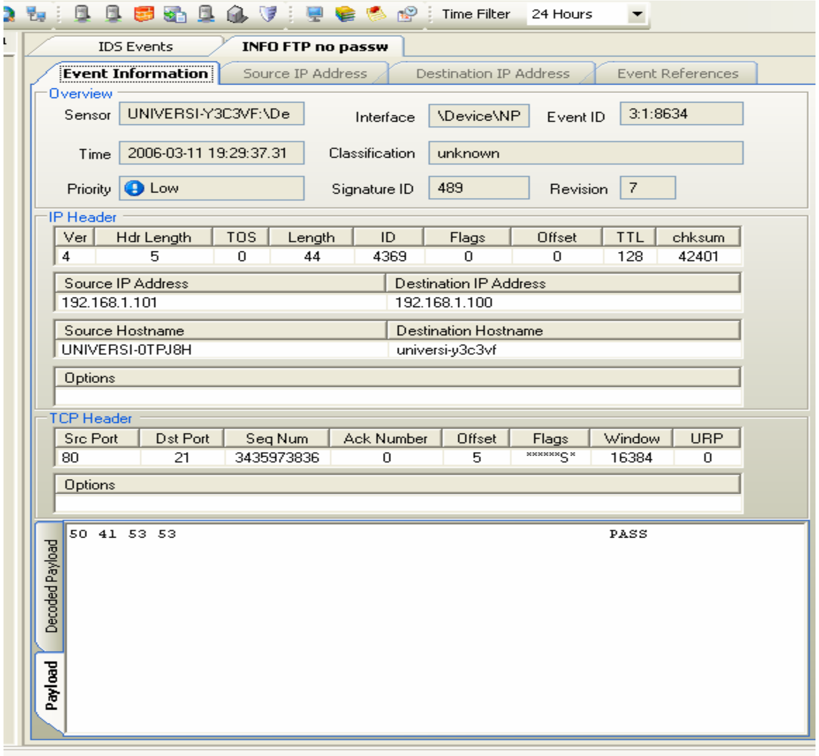
Options

ICMP Header

Type	Code	Checksum	ID	Seq Num
(5) Redirect	(1) Redirect Datagra...	46178	768	256

```
03 00 01 00 00 61 62 63 64 65 66 67 68 69 6A 6B        .....abcdefghijk
6C 6D 6E 70 71 72 73 74 75 76 77 61 62 63 64 65        lmnpqrstuvwabcde
66 67 68 69                                            fghi
```

Signature ID: 489
Message: INFO FTP no password



Overview

Sensor	UNIVERSI-Y3C3VF:\De	Interface	\Device\NP	Event ID	3:1:8634
Time	2006-03-11 19:29:37.31	Classification	unknown		
Priority	Low	Signature ID	489	Revision	7

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	44	4369	0	0	128	42401

Source IP Address	Destination IP Address
192.168.1.101	192.168.1.100

Source Hostname	Destination Hostname
UNIVERSI-0TPJ8H	universi-y3c3vf

Options

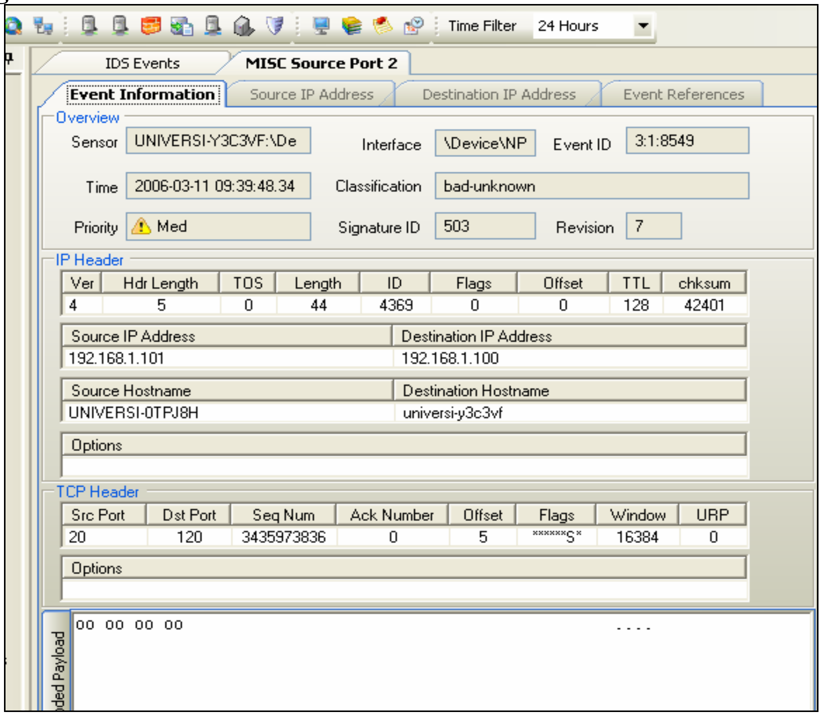
TCP Header

Src Port	Dst Port	Seq Num	Ack Number	Offset	Flags	Window	URP
80	21	3435973836	0	5	******S*	16384	0

Options

```
50 41 53 53                                                PASS
```

Signature ID: 503
Message: MISC Source Port 20 to <1024



Overview

Sensor	UNIVERSI-Y3C3VF:\De	Interface	\Device\NP	Event ID	3:1:8549
Time	2006-03-11 09:39:48.34	Classification	bad-unknown		
Priority	Med	Signature ID	503	Revision	7

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	44	4369	0	0	128	42401

Source IP Address	Destination IP Address
192.168.1.101	192.168.1.100

Source Hostname	Destination Hostname
UNIVERSI-0TPJ8H	universi-y3c3vf

Options

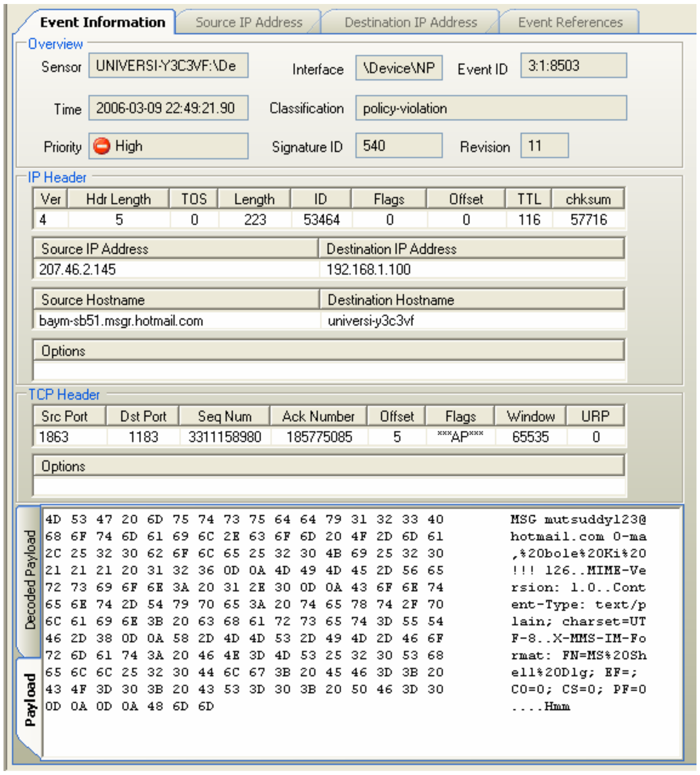
TCP Header

Src Port	Dst Port	Seq Num	Ack Number	Offset	Flags	Window	URP
20	120	3435973836	0	5	******S*	16384	0

Options

```
00 00 00 00                                                ....
```

Signature ID: 540
Message: CHAT MSN message



Overview

Sensor	UNIVERSI-Y3C3VF:\De	Interface	\Device\NP	Event ID	3:1:8503
Time	2006-03-09 22:49:21.90	Classification	policy-violation		
Priority	● High	Signature ID	540	Revision	11

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	223	53464	0	0	116	57716

Source IP Address	Destination IP Address
207.46.2.145	192.168.1.100

Source Hostname	Destination Hostname
baym-sb51.msgr.hotmail.com	universi-y3c3vf

Options

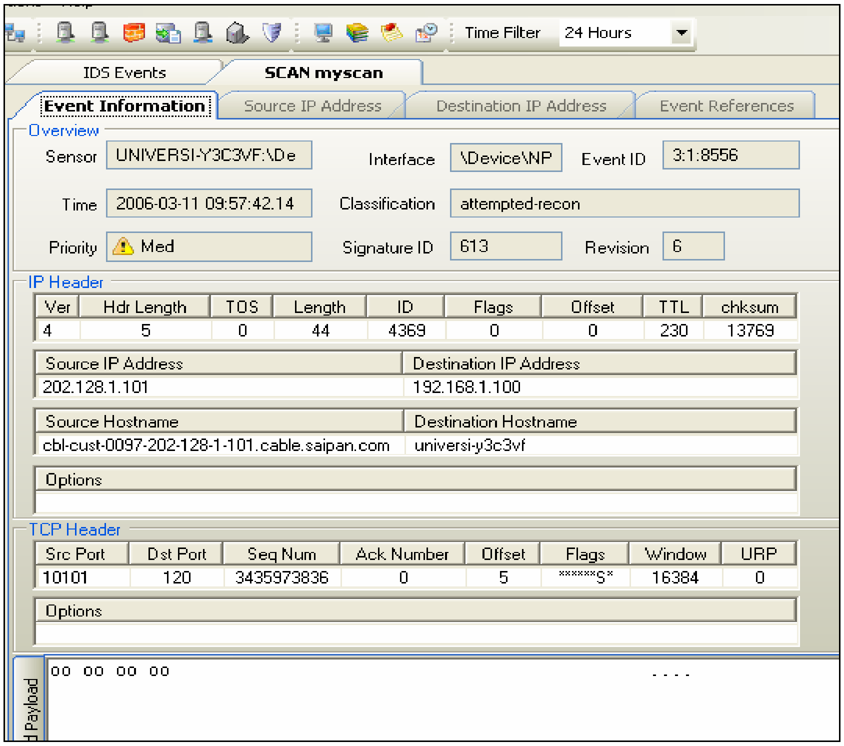
TCP Header

Src Port	Dst Port	Seq Num	Ack Number	Offset	Flags	Window	URP
1863	1183	3311158980	185775085	5	***AP***	65535	0

Options

```
4D 53 47 20 6D 75 74 73 75 64 64 79 31 32 33 40        MSG mutsuddy123@
68 6F 74 6D 61 69 6C 2E 63 6F 6D 20 4F 2D 6D 61        hotmail.com O-ma
2C 25 32 30 62 6F 6C 65 25 32 30 4B 69 25 32 30        ,%20bole%20Ki%20
21 21 21 20 31 32 36 0D 0A 4D 49 4D 45 2D 56 65        !!! 126..MIME-Ve
72 73 69 6F 6E 3A 20 31 2E 30 0D 0A 43 6F 6E 74        rsion: 1.0..Cont
65 6E 74 2D 54 79 70 65 3A 20 74 65 78 74 2F 70        ent-Type: text/p
6C 61 69 6E 3B 20 63 68 61 72 73 65 74 3D 55 54        lain; charset=UT
46 2D 38 0D 0A 58 2D 4D 4D 53 2D 49 4D 2D 46 6F        F-8..X-MMS-IM-Fo
72 6D 61 74 3A 20 46 4E 3D 4D 53 25 32 30 53 68        rmat: FN=MS%20Sh
65 6C 6C 25 32 30 44 6C 67 3B 20 45 46 3D 3B 20        ell%20Dlg; EF=;
43 4F 3D 30 3B 20 43 53 3D 30 3B 20 50 46 3D 30        CO=0; CS=0; PF=0
0D 0A 0D 0A 48 6D 6D                                   ....Hmm
```

Signature ID: 613
Message: SCAN myscan



Overview

Sensor	UNIVERSI-Y3C3VF:\De	Interface	\Device\NP	Event ID	3:1:8556
Time	2006-03-11 09:57:42.14	Classification	attempted-recon		
Priority	⚠ Med	Signature ID	613	Revision	6

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	44	4369	0	0	230	13769

Source IP Address	Destination IP Address
202.128.1.101	192.168.1.100

Source Hostname	Destination Hostname
cbl-cust-0097-202-128-1-101.cable.saipan.com	universi-y3c3vf

Options

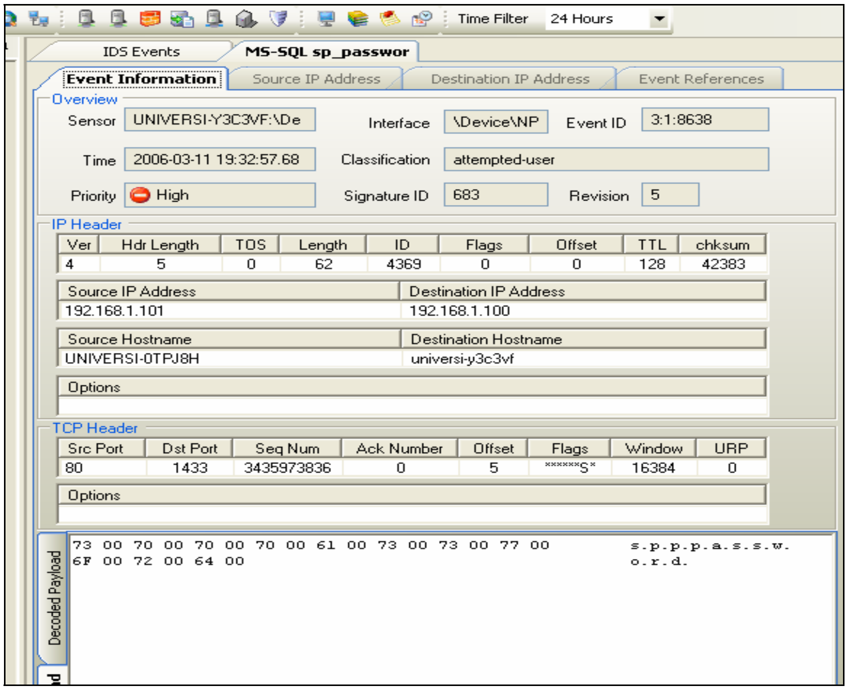
TCP Header

Src Port	Dst Port	Seq Num	Ack Number	Offset	Flags	Window	URP
10101	120	3435973836	0	5	******S*	16384	0

Options

```
00 00 00 00                                            ....
```

Signature ID: 683
Message: **MS-SQL sp_password - password change**



Overview

Sensor: UNIVERSI-Y3C3VF:\De
Interface: \Device\NP
Event ID: 3:1:8638
Time: 2006-03-11 19:32:57.68
Classification: attempted-user
Priority: High
Signature ID: 683
Revision: 5

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	62	4369	0	0	128	42383

Source IP Address	Destination IP Address
192.168.1.101	192.168.1.100

Source Hostname	Destination Hostname
UNIVERSI-0TPJ8H	universi-y3c3vf

Options

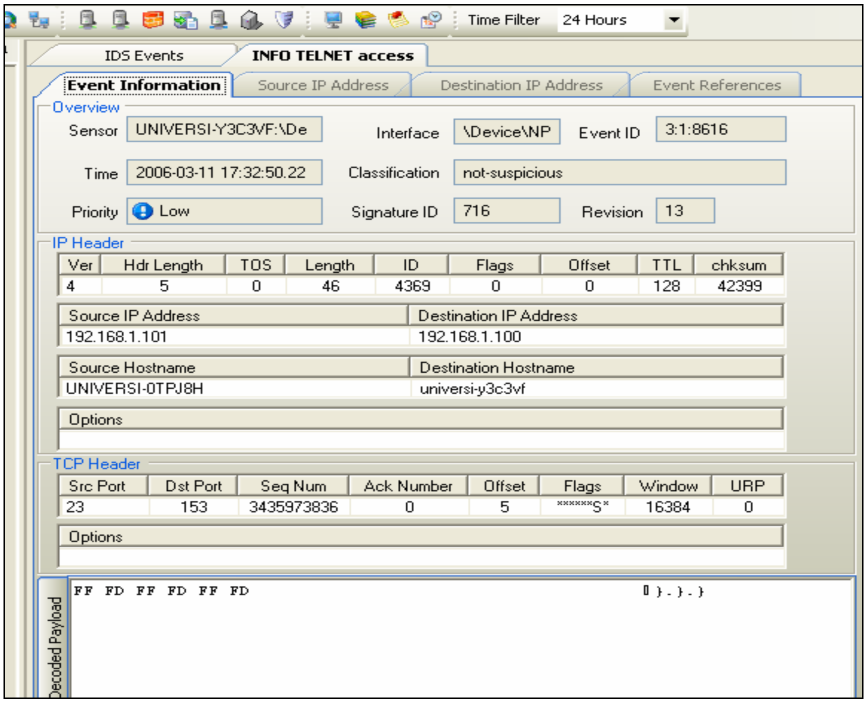
TCP Header

Src Port	Dst Port	Seq Num	Ack Number	Offset	Flags	Window	URP
80	1433	3435973836	0	5	******S*	16384	0

Options

```
73 00 70 00 70 00 70 00 61 00 73 00 73 00 77 00         s.p.p.p.a.s.s.w.
6F 00 72 00 64 00                                       o.r.d.
```

Signature ID: 716
Message: INFO TELNET access



Overview

Sensor: UNIVERSI-Y3C3VF:\De
Interface: \Device\NP
Event ID: 3:1:8616
Time: 2006-03-11 17:32:50.22
Classification: not-suspicious
Priority: Low
Signature ID: 716
Revision: 13

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	46	4369	0	0	128	42399

Source IP Address	Destination IP Address
192.168.1.101	192.168.1.100

Source Hostname	Destination Hostname
UNIVERSI-0TPJ8H	universi-y3c3vf

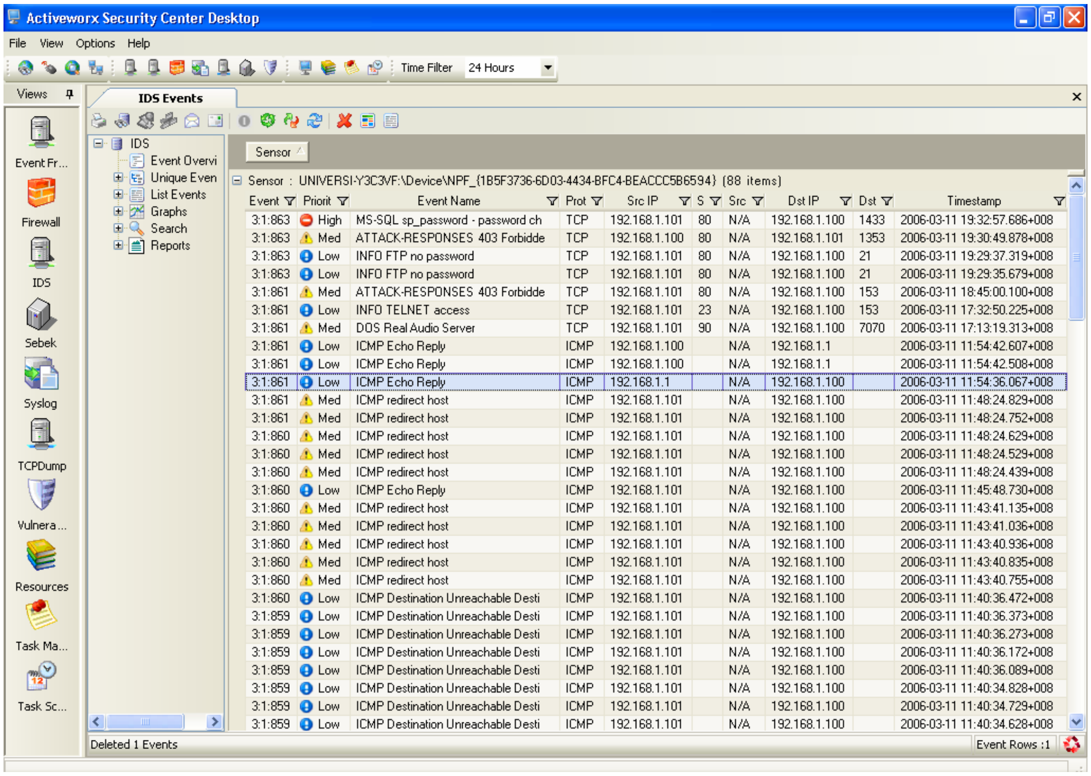
Options

TCP Header

Src Port	Dst Port	Seq Num	Ack Number	Offset	Flags	Window	URP
23	153	3435973836	0	5	******S*	16384	0

Options

```
FF FD FF FD FF FD                                       ▯}.}.}
```



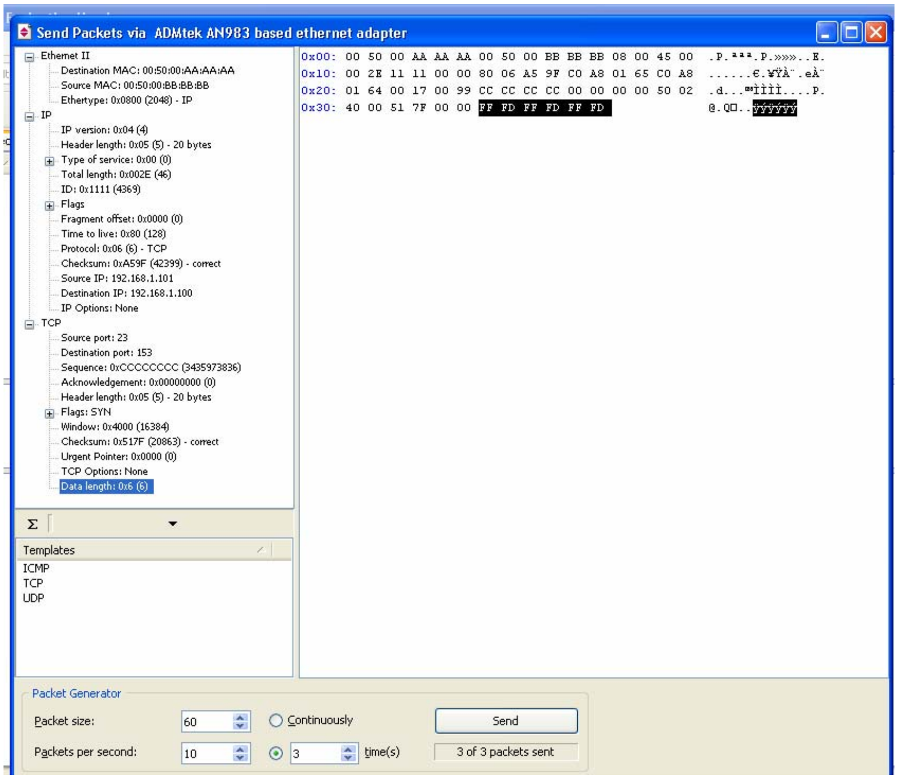
Sensor : UNIVERSI-Y3C3VF:\Device\NPF_{1B5F3736-6D03-4434-BFC4-BEACCC5B6594} (88 items)

Event	Priorit	Event Name	Prot	Src IP	S	Src	Dst IP	Dst	Timestamp
3:1:863	High	MS-SQL sp_password - password ch	TCP	192.168.1.101	80	N/A	192.168.1.100	1433	2006-03-11 19:32:57.686+008
3:1:863	Med	ATTACK-RESPONSES 403 Forbidde	TCP	192.168.1.100	80	N/A	192.168.1.101	1353	2006-03-11 19:30:49.878+008
3:1:863	Low	INFO FTP no password	TCP	192.168.1.101	80	N/A	192.168.1.100	21	2006-03-11 19:29:37.319+008
3:1:863	Low	INFO FTP no password	TCP	192.168.1.101	80	N/A	192.168.1.100	21	2006-03-11 19:29:35.679+008
3:1:861	Med	ATTACK-RESPONSES 403 Forbidde	TCP	192.168.1.101	80	N/A	192.168.1.100	153	2006-03-11 18:45:00.100+008
3:1:861	Low	INFO TELNET access	TCP	192.168.1.101	23	N/A	192.168.1.100	153	2006-03-11 17:32:50.225+008
3:1:861	Med	DOS Real Audio Server	TCP	192.168.1.101	90	N/A	192.168.1.100	7070	2006-03-11 17:13:19.313+008
3:1:861	Low	ICMP Echo Reply	ICMP	192.168.1.100		N/A	192.168.1.1		2006-03-11 11:54:42.607+008
3:1:861	Low	ICMP Echo Reply	ICMP	192.168.1.100		N/A	192.168.1.1		2006-03-11 11:54:42.508+008
3:1:861	Low	ICMP Echo Reply	ICMP	192.168.1.1		N/A	192.168.1.100		2006-03-11 11:54:36.067+008
3:1:861	Med	ICMP redirect host	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:48:24.829+008
3:1:861	Med	ICMP redirect host	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:48:24.752+008
3:1:860	Med	ICMP redirect host	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:48:24.629+008
3:1:860	Med	ICMP redirect host	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:48:24.529+008
3:1:860	Med	ICMP redirect host	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:48:24.439+008
3:1:860	Low	ICMP Echo Reply	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:45:48.730+008
3:1:860	Med	ICMP redirect host	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:43:41.135+008
3:1:860	Med	ICMP redirect host	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:43:41.036+008
3:1:860	Med	ICMP redirect host	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:43:40.936+008
3:1:860	Med	ICMP redirect host	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:43:40.835+008
3:1:860	Med	ICMP redirect host	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:43:40.755+008
3:1:860	Low	ICMP Destination Unreachable Desti	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:40:36.472+008
3:1:859	Low	ICMP Destination Unreachable Desti	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:40:36.373+008
3:1:859	Low	ICMP Destination Unreachable Desti	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:40:36.273+008
3:1:859	Low	ICMP Destination Unreachable Desti	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:40:36.172+008
3:1:859	Low	ICMP Destination Unreachable Desti	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:40:36.089+008
3:1:859	Low	ICMP Destination Unreachable Desti	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:40:34.828+008
3:1:859	Low	ICMP Destination Unreachable Desti	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:40:34.729+008
3:1:859	Low	ICMP Destination Unreachable Desti	ICMP	192.168.1.101		N/A	192.168.1.100		2006-03-11 11:40:34.628+008

Deleted 1 Events

Event Rows :1

Fig 30 : Log view produced by ASC IDS form



```
Ethernet II
    Destination MAC: 00:50:00:AA:AA:AA
    Source MAC: 00:50:00:BB:BB:BB
    Ethertype: 0x0800 (2048) - IP
IP
    IP version: 0x04 (4)
    Header length: 0x05 (5) - 20 bytes
    Type of service: 0x00 (0)
    Total length: 0x002E (46)
    ID: 0x1111 (4369)
    Flags
    Fragment offset: 0x0000 (0)
    Time to live: 0x80 (128)
    Protocol: 0x06 (6) - TCP
    Checksum: 0xA59F (42399) - correct
    Source IP: 192.168.1.101
    Destination IP: 192.168.1.100
    IP Options: None
TCP
    Source port: 23
    Destination port: 153
    Sequence: 0xCCCCCCCC (3435973836)
    Acknowledgement: 0x00000000 (0)
    Header length: 0x05 (5) - 20 bytes
    Flags: SYN
    Window: 0x4000 (16384)
    Checksum: 0x517F (20863) - correct
    Urgent Pointer: 0x0000 (0)
    TCP Options: None
    Data length: 0x6 (6)
```

```
0x00:  00 50 00 AA AA AA 00 50 00 BB BB BB 08 00 45 00   .P.ªªª.P.»»»..E.
0x10:  00 2E 11 11 00 00 80 06 A5 9F C0 A8 01 65 C0 A8   ......€.¥ŸÀ¨.eÀ¨
0x20:  01 64 00 17 00 99 CC CC CC CC 00 00 00 00 50 02   .d...™ÌÌÌÌ....P.
0x30:  40 00 51 7F 00 00 FF FD FF FD FF FD               @.Q□..ÿýÿýÿý
```

Packet size: 60

Packets per second: 10

○ Continuously

● 3 time(s)

3 of 3 packets sent

Fig 31 : Generating TCP packet with SID 716 using CommView

9. Implementation Difficulties

The followings are the difficulties we faced to implement the Snort Add-on project.

a) The schema *snort.v106* provided by the Brighttools Inc[2]. has created the table *event* by taking timestamp field of *datetime* type. But this type wasn't acceptable when the add-on was running. Hence, we drop the table and create a new *event* table with timestamp field of *varcahar* type.

```
mysql> use ids;
Database changed
mysql> drop table event;
Query OK, 0 rows affected (0.06 sec)
mysql> create table event (sid integer not null , cid integer not null
primary key, signature integer not null, timestamp varchar(30) not null);
mysql> describe event;
+-----------+-------------+------+-----+---------+-------+
| Field     | Type        | Null | Key | Default | Extra |
+-----------+-------------+------+-----+---------+-------+
| sid       | int(11)     | NO   |     |         |       |
| cid       | int(11)     | NO   | PRI |         |       |
| signature | int(11)     | NO   |     |         |       |
| timestamp | varchar(30) | NO   |     |         |       |
+-----------+-------------+------+-----+---------+-------+
4 rows in set (0.03 sec)
```

b) Generating the packets when using classtype, flow:to_server, icode, itype, rawbytes, reference, etc are really difficult to implement. CommView failed to generate such packets with those constraints. CommView can only generate ICMP/TCP/UDP packets of sort of simple contents, some specific length, offset, depth etc.

c) The format of generated packet can be saved in CommView. There generating any previous packet we need to configure the packet again before send to the network.

10. Conclusion

Implementing the project was a time-consuming, trial and error approach. Installing different tools and set them to work together was a real challenge.

We have observed the following points:

1. When Snort has peaked up some signature, it tries to insert in the signature database, but there may be times when database schema does not mach with how Snort is expecting it to be.
2. There were some occurrence when Snort can peak up the signature when there is no payload in the packet, but it cannot peak up the same signature when send with some payloads.
3. There have been situations when Snort is updating the database with events and signatures, but Add-on cant find any data to show in its interface. The reason was the difference between database names and schemas that both the tools were expecting.
4. Creating IP packets with desired signature was a real challenge. We have given lots of efforts to achieve this goal with ultimately some success. The tool we were using for the purpose, CommView, was not letting us to create totally handcrafted IP packet, though we could modify the packets.

As we have mentioned earlier, Snort is a very popular network intrusion detection system. It has three primary uses: as a straight packet sniffer, a packet logger, or as a full-blown network intrusion detection system. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes. Snort uses a flexible rules language to describe traffic that it should collect or pass, a detection engine that utilizes a modular plug-in architecture, and a real-time alerting capability.

11. References

[1] http://www.snort.org

[2] http://www.brighttools.com

[3] http://www.mysql.com

[4] http://www.tamos.com

[5] http://www.winpcap.org

[6] http://www.lookuptables.com