Ankita Tuteja, Ravi Shanker / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.1768-1774

Optimization of Snort for Extrusion and Intrusion Detection and Prevention

Ankita Tuteja* Ravi Shanker**
*(Department of Computer Science LPU, Phagwara, Punjab)
** (Department of Computer Science LPU, Phagwara, Punjab)

ABSTRACT
Intrusion is an attempt or threat resulting to unauthorized attempt to access information, manipulate information or render a system unreliable or unusable. Firewall can prevent unauthorized access but it cannot monitor the network attacks. In order to monitor network activities we need an Intrusion detection system which is the first line of defense against network activity. Over the last decades, malicious software or malware in the form of viruses, worms, Trojan horses, Botnets have risen to become a primary source of most of the threats used for scanning, distributed denial of service activities and direct attacks taking place across the internet. Most of the work has been done to monitor the inbound traffic i.e. Intrusion traffic but goal here is to monitor outbound traffic i.e. extrusion traffic as well. For the purpose of detection of Intrusion and Extrusion traffic Snort is optimized which is primarily made for Intrusion detection and prevention. It is famous Intrusion detection system in the field of open source software. Further the optimization of the Snort database is done to make it more network specific on the two designed parameters. The experimental results shows that working according to the designed system architecture a more secure network can be obtained through which specific network attacks can be easily targeted.

Keywords-Extrusion, Intrusion, Malware, Signature, Signature-Based, Snort

I. INTRODUCTION
Every network is potentially vulnerable to network intrusions despite of all security measures. It is practically impossible to build a completely secure network. Many business and government organizations use the internet as a means of providing public access to public records and information. Here arises the concept of Intruders which may be a hacker or a cracker. The three types of intruders are, Masquerader who is an unauthorized user who penetrates a computer system's access control and gains acccess to user accounts. Misfeasor, who is legitimate user who accesses resources he is not authorized to access or who is authorized such access but misuses his privileges. Clandestine user, a user who seizes the supervisory control of the system and uses it to evade auditing and access control.

Initially firewall was used but it could only prevent unauthorized access and cannot monitor network attacks. Intrusion Detection is the possibility of finding the incorrect or inappropriate action. It is considered as one of the consistent security measures against an incident. The incident may be a threat, attack or occurrence of damage to information. Security measures include detection, prevention, correction, reduction, reaction and evaluation.

Every system includes a software or hardware which is responsible for monitoring all the activities within the system or network in order to detect malicious activity and report to administrator. To protect a network from vast number of threats a Network based intrusion detection system is needed. The data of the single host might be insufficient to properly identify such malware. An ideal network-based intrusion detection system would correlate data from as many hosts as possible and could provide better detection. There are many problems of false alarms and false negatives as the amount of data to be analyzed is huge so in order to overcome the issues we need the analysis of the outbound traffic as well which we say as the extrusion traffic which would be more useful to the detect attacks because it is always assumed that a host always react to an infection of penetration in some way. So this can be acknowledged by monitoring both the outbound and intra network [11].

Another reason why extrusion is included with the intrusion is that intrusion is only the half solution to secure a network from different types of malware. There may be a possibility that an attack will make past the network boundary or even originate from the inside the network boundary so it is beneficial that the entire network is monitored.

The signature-based detection methodology is used as it is very effective at detecting known threats by comparing signature against observed events to identify possible attacks.

Snort is a lightweight network intrusion detection system capable of performing real time traffic analysis and packet logging on IP networks. Snort uses signature based detection. When we include extrusion with intrusion the problem of false negative decreases this is because

extrusion confirms that an intrusion has taken place as the infected host always moves outward for attack propagation thus confirming the intrusion.

Our Contributions: Our primary contribution to this paper is (1) to analyze the entire traffic both inbound, outbound, intra network. (2) To work for the reduction of false alarms. (3) To analyze offline traffic as well. (4) To carry out network specific optimization using Snort. (5) To make network more secure.

II. RELATED WORK

The proposed work utilizes the concept from the paper [11] about the study of extrusion detection that how important extrusion detection is in combination with intrusion. The factors for the optimization of snort database are taken from C. Lussi paper [4] as the optimization is very important after the traffic is being analyzed on the basis of signature and frequency. Different factors from the different sources are studied and combined to build an efficient system that could be developed such that the attacks which are compromising our network security and too harmful for the network could be prevented and security could be enhanced.

III. SYSTEM DESIGN AND IMPLEMENTATION

Snort itself cannot do the entire work there are number of software's which need to compiled together to carry out the desired task.

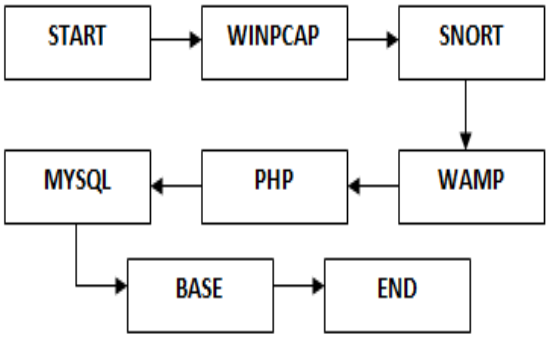

Fig1: Software applications for Snort installation

Winpcap is a packet capture library, Wamp is Windows Apache MySql Php server and BASE which is Basic Analysis and Security Engine is used for traffic analysis.

We have two modes in which Snort works one is the Intrusion detection mode, Snort does not log each captured packet as it does in the network sniffer mode. Instead it applies rules on all catured packets. If a packet matches a rule only then it is logged or an alert is generated. If packet doensot match any rule, the packet is dropped silently and no log entry is created. We used Snort in intrusion detection mode where we provided a configuration file on the command line which further contains information about input and output plugins. The name of the snort configuration file is snort.conf.

Signatures and rules for signature-based detection are downloaded from the various sources as from the official site of snort itself and from www.emergingthreats.com

Fig2 shows the proposed NIEDPS to detect and prevent any extrusion and intrusion activity. Both online and offline traffic will be analyzed. The main aim is to provide a software solution such that false alarms could be reduced and more secure network could be made. The extrsuion has two parts (1) Detection of attacks within the network (2) Detecting the movement of data out from the network

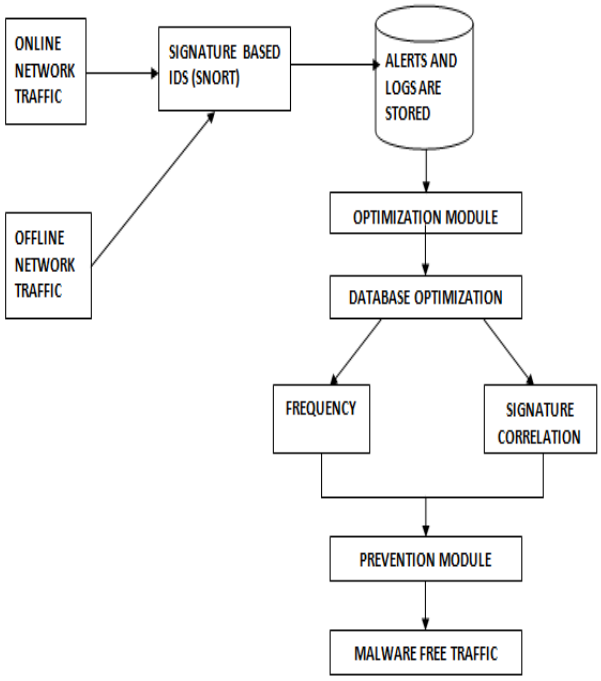

Fig2: System Design

We ran snort in the Intrusion detection mode where it matches the packets of data and logs and generates alerts correspondingly. The analysis of traffic is done on the basis of IP addresses i.e. the source and destination IP addresses as well as source and destination Ports.

Afte the packet of data are matched alerts generated and stored in the database the next step would be to filter it on two designed factors:

- **Frequency**: Will check whether a particular signature exceeds a fixed limit.
- **Signature-correlation**: This will combine signature with that of frequency.

A table will be separately created inside Snort database which will have two entries for the frequency search; it will import two fields from already existing database:

- **Signature-name**
- **Frequency**

Fig3: Shows table for signature-name and frequency

We will decide a certain threshold value for frequency by making analysis from BASE, this decision of setting the threshold value for the frequency will highly depend upon how large the network is and how frequently a particluar signature is triggered in the network. In the results and discussion column of the paper we will be representing the signatures with their frequency when we implemented the proposed work on our test enviornment. Say we set our threshold value of frequency to 265. Now, we need to fire the query saying if the frequency is greater than 265 the database should show the remaining filtered signatures. Same is the case with if a particular signature is found in combination with a certain value of frequency a query will be fired and the filetered signatures will be left. The resulting traffic would thus be dropped thus preventing it.

Simple alerting is insufficient; we want to actively respond to an attempt that compromise security.

If we change rule type from alert to drop, Snort will start dropping whole of the traffic that matches with the rules in the database. So, in this way snort NIDS could be converted into a reactive NIDS.

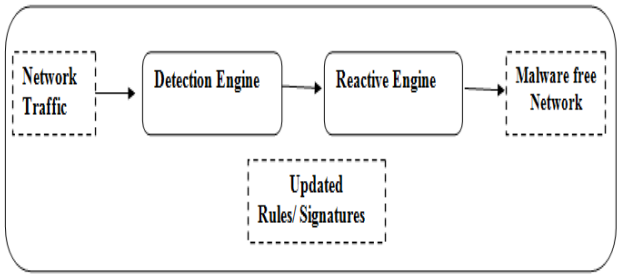

Fig4: Block Diagram of NIEDS

Depending on the alerts generated, we analyze those alerts and observed which kind of attack is more harmful to the network under observation and need to be dropped. Also filtering is done on the basis of the two designed factors signature and frequency as discussed above. We convert those rules/ signatures from alert type to drop type.

The other way of creating reactive NIDS is:

- If you want to reset any illegitimate connection attempts, use the ttresp/tt keyword.
- If you want to use Snort to modify the rules of a firewall to block unwanted traffic, use SnortSAM.
- If you want to use Snort as a filter to remove unwanted traffic, you need to run Snort inline. This removes the problem of attacker using an intrusion prevention system to create a denial of service. As it drops only packets that are suspect, it doesn't exclude an entire IP address.

We have used the first method that converts the types of rules from alert to drop. So we have made a Reactive and Preventive system for malware detection in a network.

Using snort the rules can be applied to following parts of packets:

- The IP header of the packet
- The transport layer header. This includes TCP, UDP and ICMP header.

Initially we had 5775 Snort rules/signatures. We ran the snort IDS for four weeks on a network, Analyze the traffic and make one table comprises of Signatures verses frequency with which they occur. From this, we got the top triggered signatures in a network under analysis. We repeat the exercise with Intrusion rules and extrusion rules separately and compare the two. There were number of malware types like botnets which can't be detected with Intrusion rules only. So it indicates that Extrusion traffic is equally important to analyze along with Intrusion traffic. After optimization only 1785 rules remains in Snort rules database.

BASE provides a web front-end to query and analyze the alerts coming from a SNORT IDS system. Multiply the values obtained from BASE by 1, 00 000 to show the escalation of results for at least 1 month as the results are for 1 hour of Network activity only. The optimization of rules is done in the following way:

- Unique alerts
- Categories of traffic in our network along with frequency of signatures triggered.
- Unique Source and Destination IP addresses observed
- Unique Source and Destination IP ports observed
- Top most frequent alerts in a network
- Show the traffic profile by protocol.

All these points are related to optimization of rules. As we have removed those rules from the rules database that never triggered during the course of analysis of network over a span of 4 weeks.

Snort will read all the contents from the specified tcpdump or log file and store the results in database which can be then analyzed using BASE. Our tool can read any log file which is in .pcap or .tcpdump format. The data of the file will be stored to MySQL database and output will be shown in BASE accordingly.

We had used our tool to read 2000 DARPA LLS_DDOS_1.0-inside.dump file. The majority of the traffic analyzed is ICMP-93%, TCP 6% and UDP-1%.

So, the tool is generalized one and can be used for both offline and online signature based detection of malware.

IV. RESULTS AND DISCUSSION

Below given are the screenshots from BASE after the test environment was analyzed.

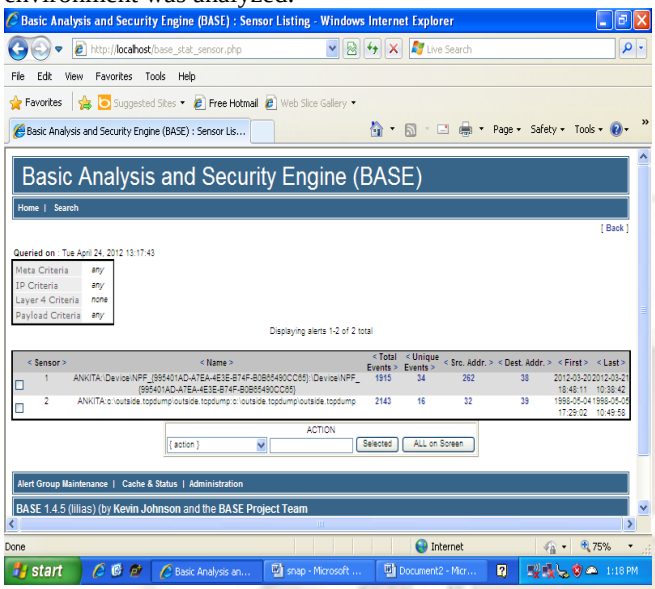

Fig5: Both offline and online analysis of traffic

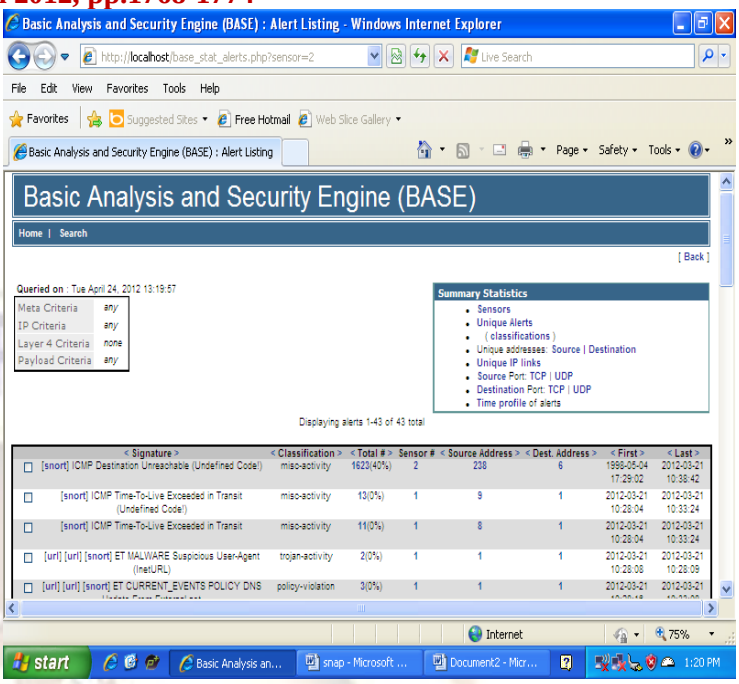

Fig7: Alert Listing

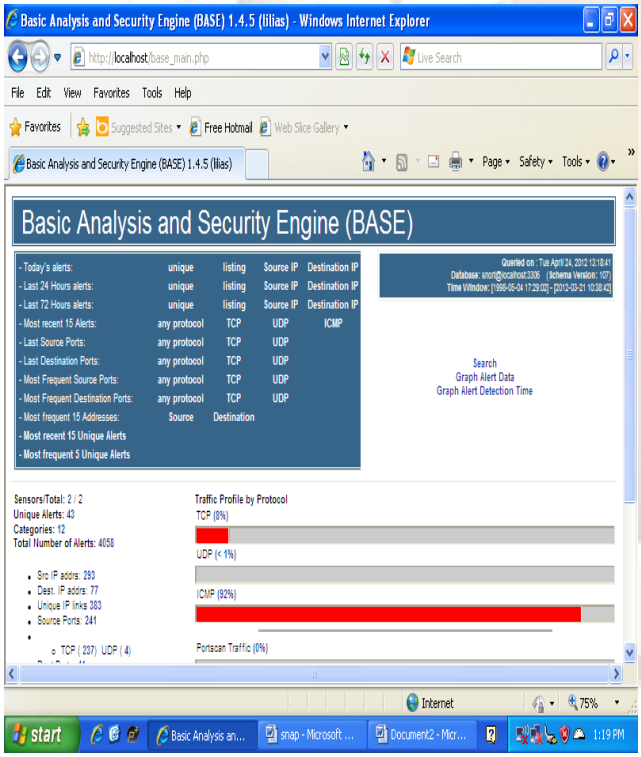

Fig6: Main screen of the traffic analyzed

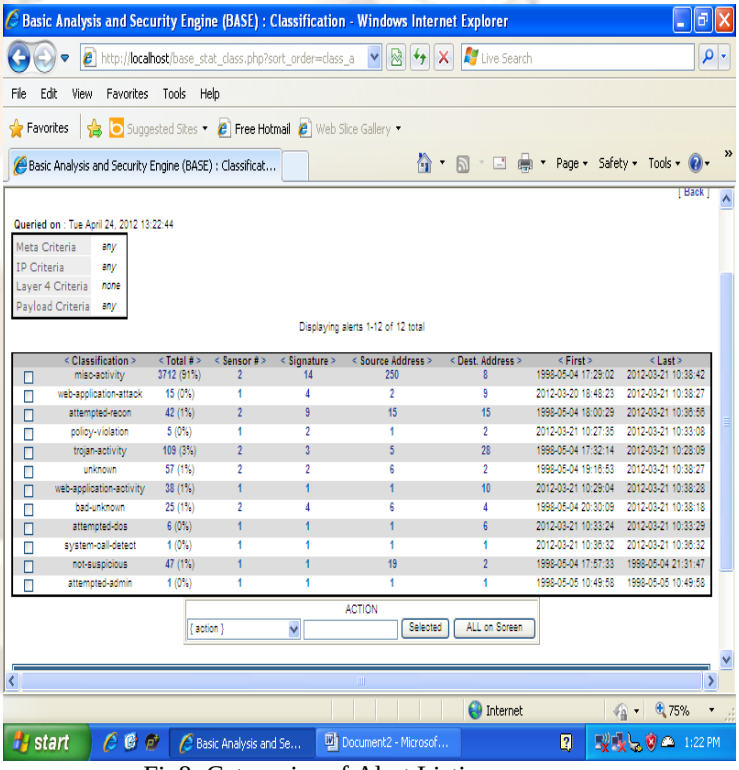

Fig8: Categories of Alert Listing

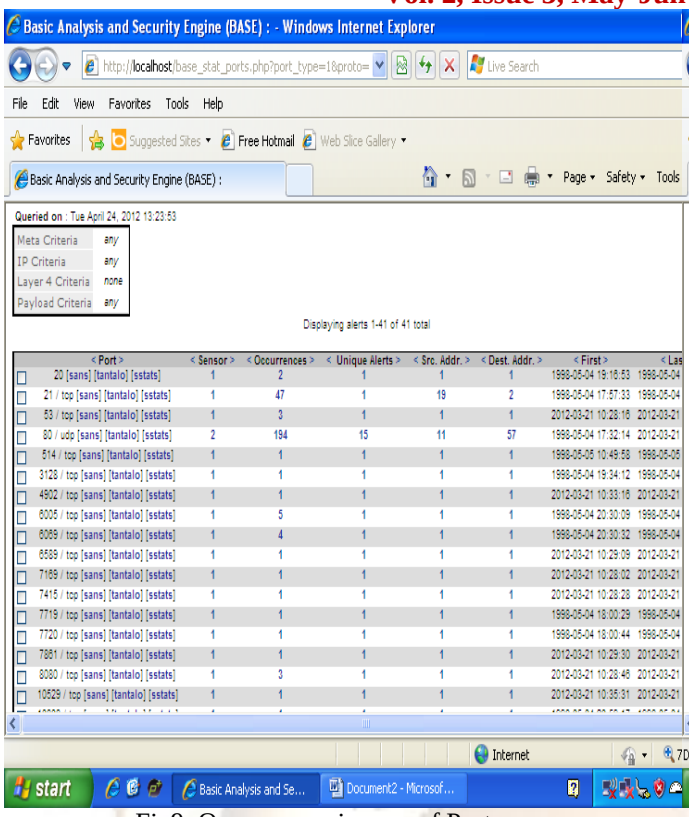

Fig9: Occurrences in case of Ports

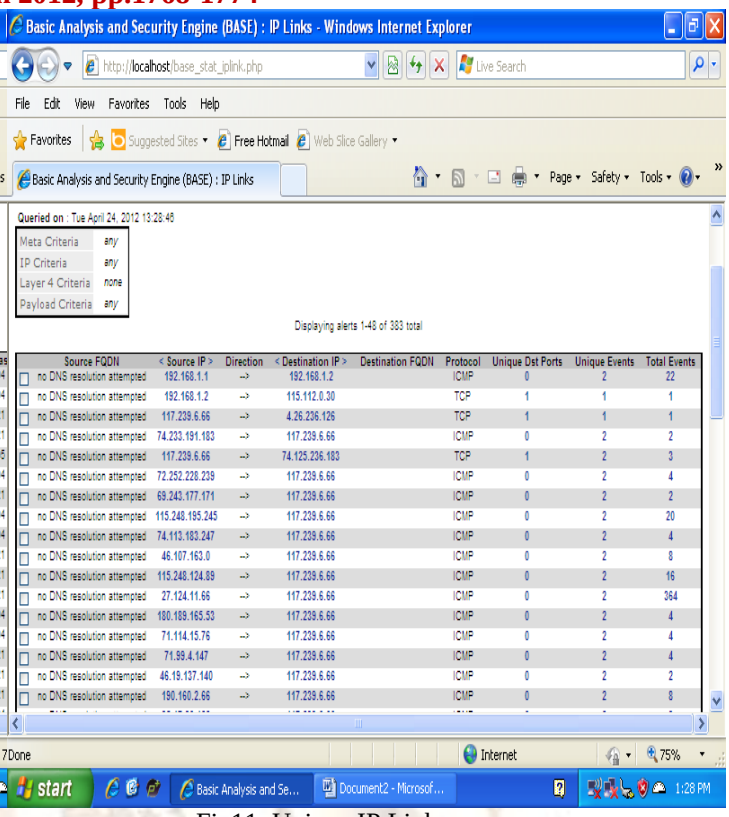

Fig11: Unique IP Links

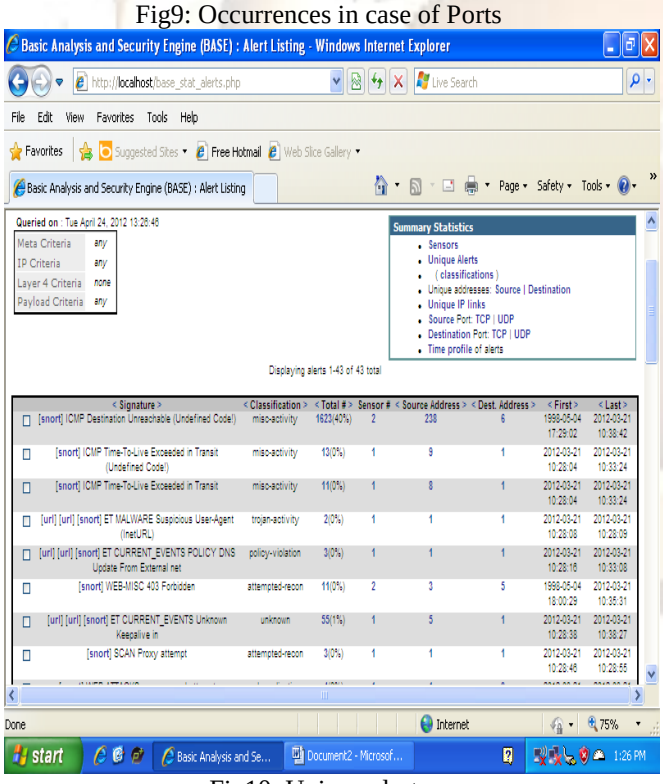

Fig10: Unique alerts

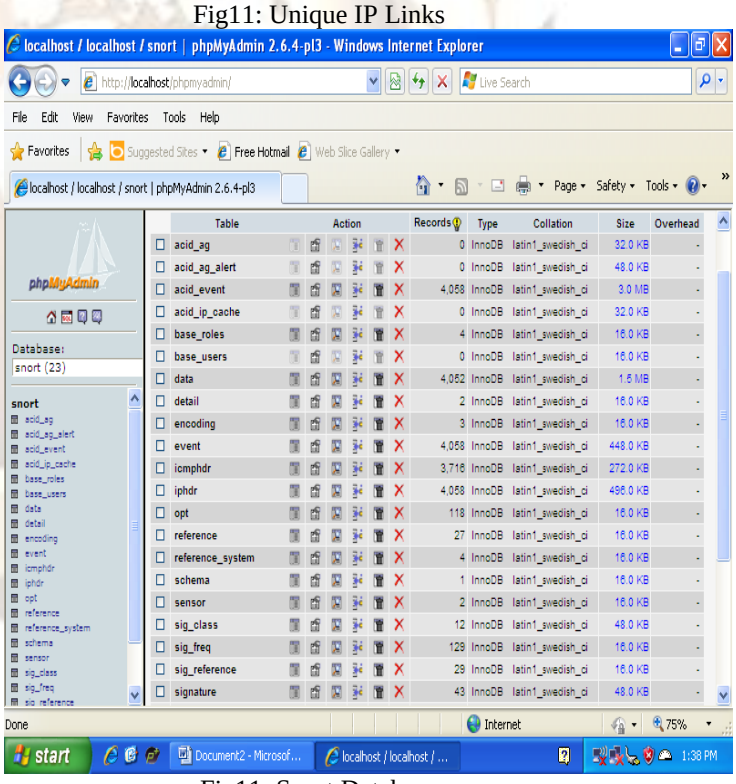

Fig11: Snort Database

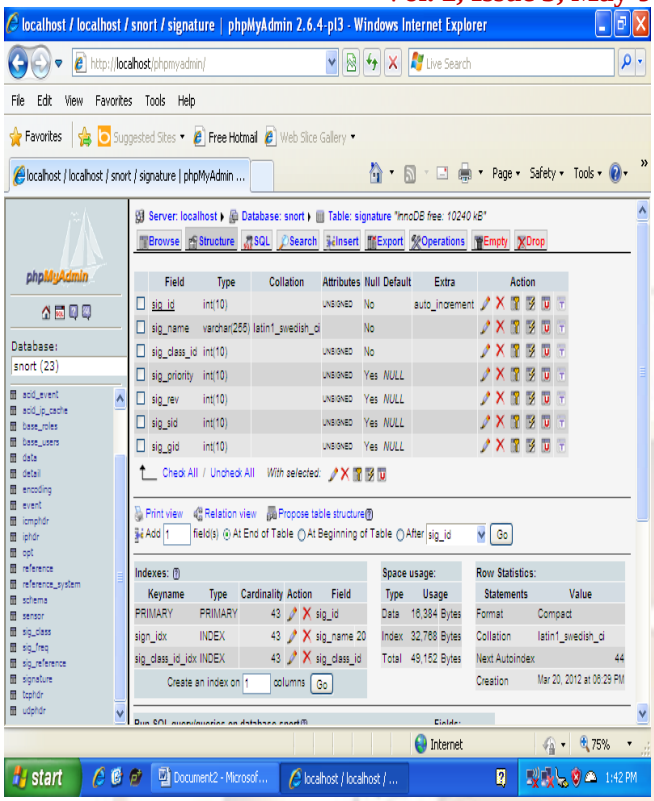

Fig13: Contains all the information about signatures

SIGNATURE
DNS SPOOF query response with ttl: 1 min. and no authority
ET CURRENT_EVENTS POLICY DNS Update From External net
ET CURRENT_EVENTS Unknown Keepalive in
ET DROP Spamhaus DROP Listed Traffic Inbound
ET MALWARE Fun Web Products Agent Traffic
ET MALWARE Fun Web Products Spyware User Agent
ET MALWARE Possible Windows executable sent when remote host claims to send a Text File
ET MALWARE Possible Windows executable sent when remote host claims to send a Text File
ET MALWARE SOCKSv5 UDP Proxy Inbound Connect Request (Windows Source)
ET RBN Known Russian Business Network IP TCP
ET RBN Known Russian Business Network IP UDP
FTP Bad login
ICMP Destination Unreachable (Fragmentation Needed and DF bit was set)
ICMP Destination Unreachable (Network Unreachable)
ICMP Destination Unreachable (Undefined Code!)
ICMP Fragment Reassembly Time Exceeded
ICMP L3retriever Ping
ICMP PING (Undefined Code!)
ICMP PING
ICMP PING CyberKit 2.2 Windows
ICMP PING NMAP
ICMP PING Sun Solaris
ICMP PING Windows
ICMP superscan echo
ICMP Time-To-Live Exceeded in Transit (Undefined Code!)
ICMP traceroute
MISC Large ICMP Packet
SHELLCODE x86 NOOP
WEB-ATTACKS cc command attempt
WEB-ATTACKS mail command attempt
WEB-ATTACKS netcat command attempt
WEB-ATTACKS rm command attempt
WEB-CGI archie access
WEB-CGI calendar access
WEB-CGI redirect access
WEB-CGI rsh access
WEB-CGI wrap access
WEB-IIS scripts access
WEB-IIS Unauthorized IP Access Attempt
WEB-IIS view source via translate header
WEB-MISC 403 Forbidden
WEB-MISC backup access
WEB-MISC count.cgi access
WEB-MISC handler access
WEB-MISC http directory traversal
WEB-MISC Invalid URL
WEB-MISC musicat access
WEB-MISC whisker head

Table1: Top Triggered Signature

Generic Protocol Command Decode
Executable code was detected
Access to a potentially vulnerable web application
Unknown Traffic
Network Trojan was detected
Potential Corporate Privacy Violation
Potentially Bad Traffic
Web Application Attack
Potentially Bad Traffic
Attempted Information Leak
Misc Attack

Table2: Summary of Attacks

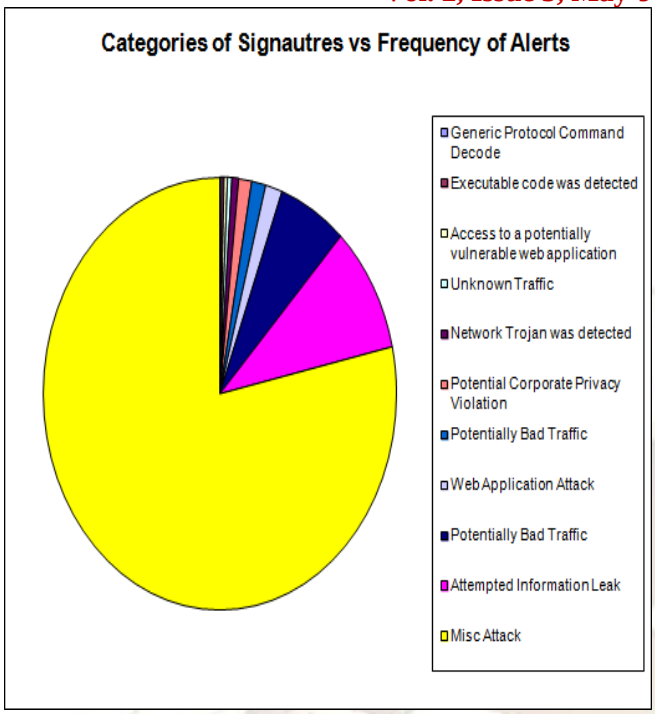

Fig14: Categories of signature verses Frequency of alerts

V. CONCLUSION

Snort is a common Intrusion detection system which for our task was modified to analyze extrusion traffic as well. The proposed work was carried out on Windows XP because of its friendly interface. We have tried our best to optimize Snort so that our network could be made more secure. Different factors from various sources are studied and combined together to come up with efficient system so that our network could be made more secure. With the advantages there are also some drawbacks of Intrusion detection system which will prevail among them are that Intrusion detection system are not a solution to all security concerns, an IDS is not a subsitute for a good security policy and human intervention is required. In the proposed work also human intervention is required once an attack is detected and reported it is our responsibility of the to determine how it occurred, correct the problem and take necessary action to prevent the occurrence of the same attack in future.

REFERENCES

[1] Charlie Scott, Paul Wolfe, Bert Hayes, *Snort For Dummies* (Wiley Publishing, Inc., Indianapolis, 2004)

[2] Karen Scarfone, Peter Mell, *Guide to Intrusion Detection and Prevention Systems* (National Institute of Standards and Technology Special Publication 800-94, 2007)

[3] Rafeeq Ur Rehman *Intrusion Detection Systems with Snort* (Pearson Education, Inc., 2003)

[4] Cecile Lussie, *Signature Based Extrusion Detection*, Institute for Technische Informatik und kommunikationsnetze, MA, 2008

[5] Farzaneh Izak Shiri, Bharanidharan Shanmugam, Norbik Bashah Idris, A Parallel Technique for improving the performance of Signature-Based Network Intrusion Detection System, *IEEE*,2011

[6] Mohd Nazri Ismail, Mohd Taha Ismail, Framework of Intrusion Detection System via Snort Application on Campus Network Environment, *International Conference on Future Computer and Communication*, 2009.

[7] Muhammad Naveed, Shams Un Nihar, Mohammad Inayatullah Babar, Network Intrusion Prevention by Configuring ACLs on the Routers, *International Conference Emerging Technologies (ICET)*,2010

[8] Rebecca Bacel and Peter Mell2, *NIST Special Publication on Intrusion Detection Systems*, Special Publication 800-94, February 2007.

[9] SANS Institute-Understanding Intrusion Detection Systems, 2001

[10] Sunny Behal, Amanpreet Singh Brar, Krishan Kumar, Signature-Based Botnet Detection and Prevention, *Springer*, 2009.

[11] Sunny Behal, Krishan Kumar, An Experimental Analysis for Malware Detection Using Extrusions, *International Conference on Computer and Communication Technology*, 2011

[12] Zhou Zhimin, Chen Zhongwen, Zhou Ti echeng, Guan Xiaohui, The Study of Network Intrusion Detection System of Snort, International *Conference on Networking and Digital Society*,2010

[13] http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html

[15] http://www.streetdirectory.com/travel_guide/154241/security/importance_of_network_security_system.html

[16] http://www.brighthub.com/computing/enterprise - security /articles/69275.aspx

[17] http://qualitative.wikidot.com/dimensions-of-research

[18] www.snort.org

[19] www.emergingthreats.com