Performance Analysis of Real Time Intrusion Detection and Prevention System using Snort.

, [1]Mukesh Sharma,[2]Akhil Kaushik, [3]Amit Sangwan
[1]Associate.Professor, [2]Assistant.Professor, [3]Mtech Scholor ,
Department of Computer Science and Engineering
The Technological Institute of Textile and Science,Bhiwani-127021, Haryana – India

Abstract:

Nowadays Intrusion Detection and Prevention System represents an essential line of defense against variety of web attacks that can compromise with the security and proper functioning of the entire security system. With the evolution of internet, possibilities and opportunities are limitless, unfortunately, so too are the risks and chances of malicious intrusions. Network is interconnection or links, for example network of road, network of computer. Security is the freedom from danger or anxiety so Network Security is about securing and protecting the network (externally and internally) from Distributed Denial of Service attacks, rapidly propagating viruses, self-replicating worms and other attacks. Network security begins with authorization and authentication. In this paper capturing of network traffic, performance and reports analysis generated by snort and corresponding alert ratio of signatures for the particular attack are to be evaluated. This intrusion detection system is one of the security defense tools for computer networks. In recent years this research has lacked in direction and focus today SNORT stands out as the most widely deployed IDS, We survey the existing techniques, types and architectures of Intrusion Detection Systems in the literature. Performance analysis of real time Intrusion Detection and prevention system and traffic analysis by Snort from the network are to carried out in this paper.

Keywords and Phrases: staeful , IDS ,services, domain ,intrusion , snort, analysis, prevention, Detection, techniques.

1. Introduction:

The idea of a network intrusion detection system is to have a device of some sort that can 'see' all the traffic on its part of the network available. It continuously looks at this traffic, and based on a set of defined rules, it will activate an action of some kind on packets that match one of the defined rules from the set of rules.One could think of its functionality as very similar to that of antivirus software - scan content for stuff considered spiteful, and take action. Intrusion is the act or attempt of using a particular computer system or computer resources without the requisite privileges, causing willful or incidental damage whereas Detection involves identifying individuals or machines that perform or attempts intrusion. Intrusion Detection Systems (IDS) are computer programs that tries to perform intrusion detection by comparing observable behavior against suspicious patterns, preferably in real-time Intrusion detection techniques based upon data mining are generally fall into one of two categories: anomaly detection and misuse detection. In the misuse detection, each instance in a data set is labeled as 'normal' or 'intrusive' and a learning algorithm is trained over the labeled data. Unlike signature-based intrusion detection systems, models of misuse are created automatically, and they can be more sophisticated and precise than manually created signatures.The major benefit of anomaly detection algorithms is their ability to potentially detect unforeseen attacks.A major limitation of anomaly detection systems is a possible high false alarm rate. There are two main categories of anomaly detection techniques, namely supervised and unsupervised. In supervised anomaly detection technique, given a set of normal data to train on, and given a new set of test data, goal is to determine whether the test data is 'normal' or anomalous. Unlike supervised anomaly detection where the models are built only according to the normal behavior of the network, unsupervised anomaly detection attempts to detect anomalous behavior without using any knowledge about the training data. In unsupervised anomaly detection approaches are based on statistical approaches, clustering , outlier detection schemes, state machines, etc.

2.Methods for IDS:

Snort Architecture:

Snort was created by Martin Roesch in 1998. As most open-source projects, it started out as a small-scale application made just for fun, as an alternative to the full-blown commercial intrusion detection systems. The Snort tool is a small, lightweight open source IDS which has become the most widely used IDS. It is capable of performing real-time traffic analysis. Snort is a free and open source Network Intrusion prevention system (NIPS) and network intrusion detection (NIDS) capable of performing packet logging and real-time traffic analysis on IP networks. Snort performs protocol analysis, and content searching/matching, it is commonly used to actively block or passively detect a variety of attacks and probes, such as buffer overflows, stealth port scans, web application attacks, SMB probes, and OS fingerprinting attempts, amongst other features.. Snort employs both signature based techniques and anomaly based techniques to detect an intrusion. Signatures are used for detecting intrusions. Snort has a rich rule set which depend upon the signatures present in either the header part of the packet or payload of the packet so as to detect intrusions.

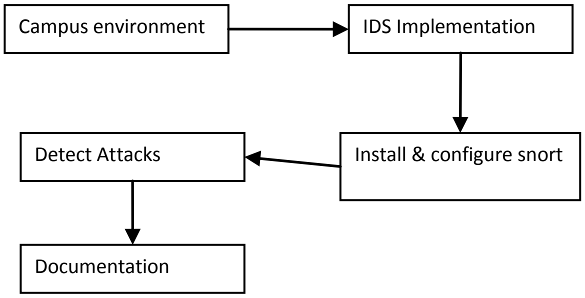


Figure 2.1.shows Process of Implementation of SNORT.

Snort captures raw packets with libpcap and then it decodes and preprocesses them prior to forwarding them to the detection engine. The preprocessing includes early packet droppings, classification, layer three IP fragment reassembly, layer four TCP session reconstructions and so forth. The detection engine checks packet headers as well as payloads against several thousands of rules stored in a database of pre-defined attack signatures, as shown in Figure 2.2

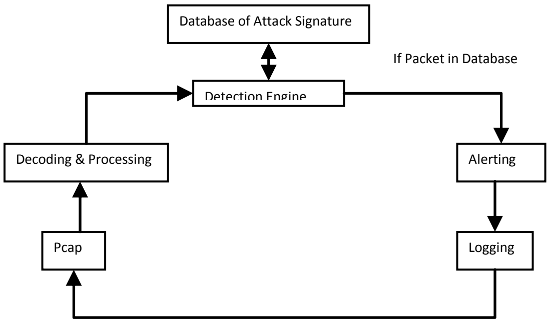


Figure 2.2: Snort basic software components

3.Classification of Intrusion Detection System:

Intrusion detection systems can be classified on the basis of a multitude of factors. With respect to the place where the intrusion detection system takes place we have two kinds of IDSs Such as:-

a) **Host Based IDSs**: IDS that operate on a host to detect malicious activity on that host are called Host based IDS.
b) **Network Based IDS**: IDS which operate on network data flows are called network based IDS.

3.1 Intrusion Detection Techniques

Host Based IDSs and Network Based IDS may use any of the following methods for detecting the unauthorized intrusion .

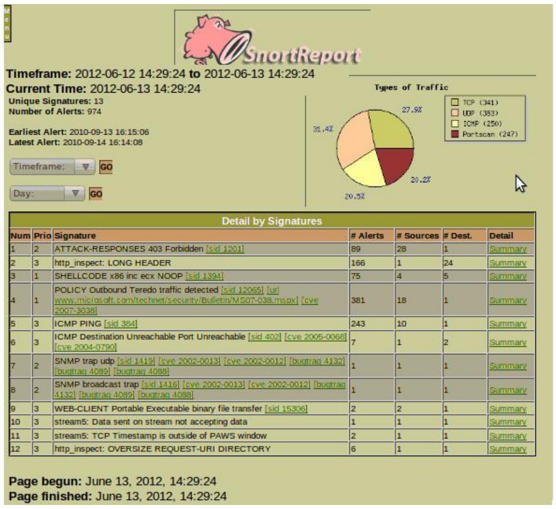
a) **Application-based IDS**: An application-based IDS concentrates on events occurring within some specific application.
b) **Signature-based IDS**: A signature-based IDS examines ongoing traffic, activity, transactions, or behavior for matches with known patterns of events specific to known attacks.
c) **Anomaly-based IDS**: An anomaly-based IDS examines ongoing traffic, activity, transactions, or behavior for anomalies on networks or systems that may indicate attack.

4.Stateful protocol analysis:

This method compares predetermined profiles of generally accepted definitions of benign protocol activity for each of the protocol state against observed events to identify any deviation. This analysis is an intrusion detection technique which looks for the misuse of a particular protocol. Intrusion detection system employ protocol analysis in order to understand the traffic and supervision of the execution of some selected protocols ie Tcp ,Udp Icmp etc. Protocol analysis is generally designed to analyze specifically one protocol and also require model of that protocol's normal usage. Ordinary usage of a protocol can be defined as the practical usage area of that protocol. Any change in the defined usage of practical area of a protocol can be considered as abnormal usage. In this analysis, each packet on network can be viewed in terms of its underlying protocol. All fields of a protocol are compared against its normal behavior an also puts an effort to locate any malicious event. Some of the benefits of protocol analysis are for preventing evasion, false positives reduction, space search reduction,, extra detection capability and it also verifies protocol to detect implement flaws, if any. Protocol analysis is suitable for detecting anomalies.

5.Reports Generated by SNORT.

Snort's report is an add-on facility for the Snort Intrusion Detection System. It provides real-time reporting from the MySQL database generated by Snort tool. This requires a platform with MySQL, PHP,and Snort. Figure 5.1shows intrusions detected by SNORT tool with the number of alerts generated corresponding to the particular attack signature. This provides information about the name of the signature. And also gives the information about the number of sources which are generating the attacks for a predefined attack signature and the number of destinations for which alerts are generated in the Intrusion and detection System.



Timeframe: 2012-06-12 14:29:24 **to** 2012-06-13 14:29:24
Current Time: 2012-06-13 14:29:24
Unique Signatures: 13
Number of Alerts: 974

Earliest Alert: 2010-09-13 16:15:06
Latest Alert: 2010-09-14 16:14:08

Detail by Signatures

Num	Prio	Signature	# Alerts	# Sources	# Dest.	Detail
1	2	ATTACK-RESPONSES 403 Forbidden [sid 1201]	89	28	1	Summary
2	3	http_inspect: LONG HEADER	166	1	24	Summary
3	1	SHELLCODE x86 inc ecx NOOP [sid 1394]	75	4	5	Summary
4	1	POLICY Outbound Teredo traffic detected [sid 12065] [url www.microsoft.com/technet/security/Bulletin/MS07-038.mspx] [cve 2007-3038]	381	18	1	Summary
5	3	ICMP PING [sid 384]	243	10	1	Summary
6	3	ICMP Destination Unreachable Port Unreachable [sid 402] [cve 2005-0068] [cve 2004-0790]	7	1	2	Summary
7	2	SNMP trap udp [sid 1419] [cve 2002-0013] [cve 2002-0012] [bugtraq 4132] [bugtraq 4089] [bugtraq 4088]	1	1	1	Summary
8	2	SNMP broadcast trap [sid 1416] [cve 2002-0013] [cve 2002-0012] [bugtraq 4132] [bugtraq 4089] [bugtraq 4088]	1	1	1	Summary
9	3	WEB-CLIENT Portable Executable binary file transfer [sid 15306]	2	2	1	Summary
10	3	stream5: Data sent on stream not accepting data	1	1	1	Summary
11	3	stream5: TCP Timestamp is outside of PAWS window	2	1	1	Summary
12	3	http_inspect: OVERSIZE REQUEST-URI DIRECTORY	6	1	1	Summary

Page begun: June 13, 2012, 14:29:24
Page finished: June 13, 2012, 14:29:24

Figure 5.1: Snort Report-1 showing Intrusion Detection for 11-Signatures.

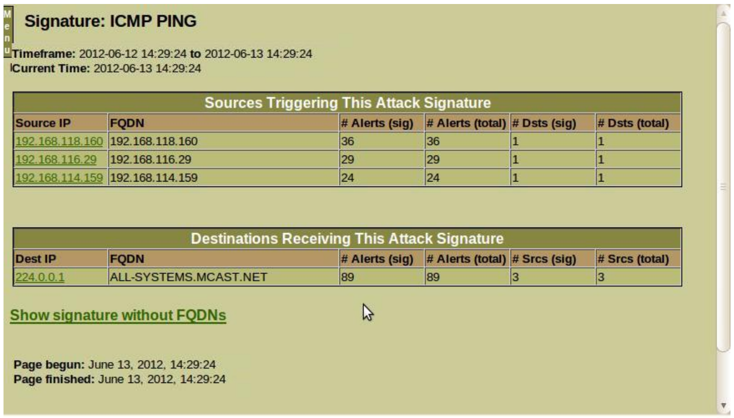
5.1 2 ICMP PING

It sends a small packet of information containing an ICMP ECHO_REQUEST to a specified computer, which then sends an ECHO_REPLY packet in return. The IP address 127.0.0.1 is set by convention to always indicate your own computer. Therefore, a ping to that address will always ping yourself and the delay should be very short. The Summary of this signature is shown in figure 5.3

ping -c count	ping -c 10	Specify the number of echo re to send.

5.2 ICMP Destination Unreachable Port Unreachable.

The Destination Unreachable message is an ICMP message which is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason. A Destination Unreachable message may be generated as a result of a TCP, UDP or another ICMP transmission. The Summary of this signature is shown in figure 5.4



Signature: ICMP PING

Timeframe: 2012-06-12 14:29:24 **to** 2012-06-13 14:29:24
Current Time: 2012-06-13 14:29:24

Sources Triggering This Attack Signature

Source IP	FQDN	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
192.168.118.160	192.168.118.160	36	36	1	1
192.168.116.29	192.168.116.29	29	29	1	1
192.168.114.159	192.168.114.159	24	24	1	1

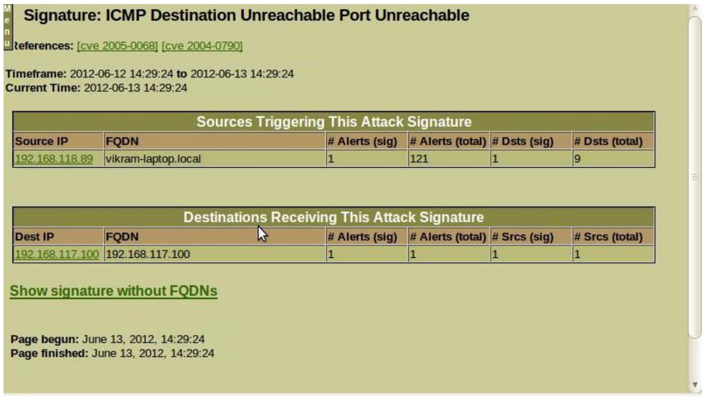
Destinations Receiving This Attack Signature

Dest IP	FQDN	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
224.0.0.1	ALL-SYSTEMS.MCAST.NET	89	89	3	3

Show signature without FQDNs

Page begun: June 13, 2012, 14:29:24
Page finished: June 13, 2012, 14:29:24

Figure 5.3 **:** Snort report signature summary of "ICMP PING"



Signature: ICMP Destination Unreachable Port Unreachable

References: [cve 2005-0068] [cve 2004-0790]

Timeframe: 2012-06-12 14:29:24 **to** 2012-06-13 14:29:24
Current Time: 2012-06-13 14:29:24

Sources Triggering This Attack Signature

Source IP	FQDN	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
192.168.118.89	vikram-laptop.local	1	121	1	9

Destinations Receiving This Attack Signature

Dest IP	FQDN	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
192.168.117.100	192.168.117.100	1	1	1	1

Show signature without FQDNs

Page begun: June 13, 2012, 14:29:24
Page finished: June 13, 2012, 14:29:24

Figure 5.4: Snort report signature summary of "ICMP Destination Unreachable Port Unreachable"

This has been observed from the implementation of Snort as Intrusion Detection System that:-

Total number of signatures detected by snort is=10 .

1. POLICY Outbound teredo traffic detected
Ratio of alerts generated on destination
=alerts(sig)/alerts(total)=73/73=1

2 ICMP PING
Ratio of alerts generated on destination
=alerts(sig)/alerts(total)=89/89=1
3. http_inspect :LONG HEADER
Ratio of alerts generated on destination =alerts (sig)/alerts(total)=88/120=0.74
4.SHELLCODE x86 inc ecx NOOP
Ratio of alerts generated on destination= alerts (sig)/alerts(total)=77/115=0.64
5.SNMP Broadcast Trap
Ratio of alerts generated on destination
=alerts(sig)/alerts(total)=1/2=0.5
6. ICMP Destination unreachable port unreachable
Ratio of alerts generated on destination
=alerts(sig)/alerts(total)=1/1=1
7.SNMP Trap UDP
Ratio of alerts generated on destination
=alerts(sig)/alerts(total)=1/2=0.50
8.http_inspect :oversize REQUEST-URI DIRECTORY
Ratio of alerts generated on destination
=alerts(sig)/alerts(total)=6/6=1
9.WEB-CLIENT portable executable binary file transfer
Ratio of alerts generated on destination
=alerts(sig)/alerts(total)=2/140=0.015
10.Stream5 : Data sent on stream not accepting data
Ratio of alerts generated on destination =
alerts(sig)/alerts(total)=1/138=0.007

5.3 Traffic Analysis by Snort.

It has been observed from the figure 6.1 that snort has captured the following traffic :-

1. TCP (27.9%).
2. ICMP (20.5%).
3. UDP (31.4%).
4. PORT SCAN(20.2%)

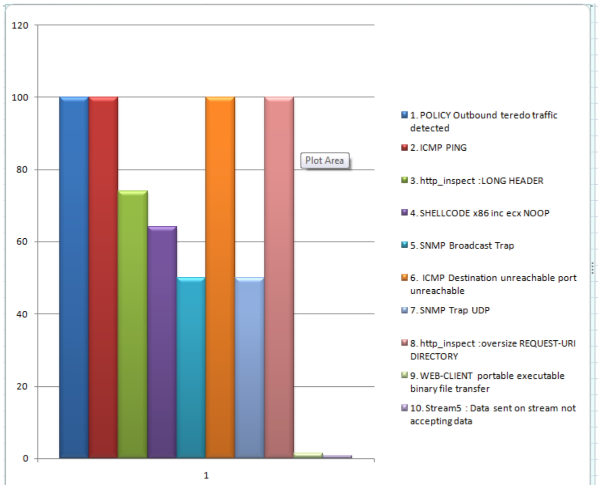


Figure 5.5 : Alert ratio of signatures for the particular attack.

This has been observed from the analysis of alerts that, **POLICY Outbound,ICMP Destination unreachable port unreachable and ICMP PING** has the highest alert ratio size.

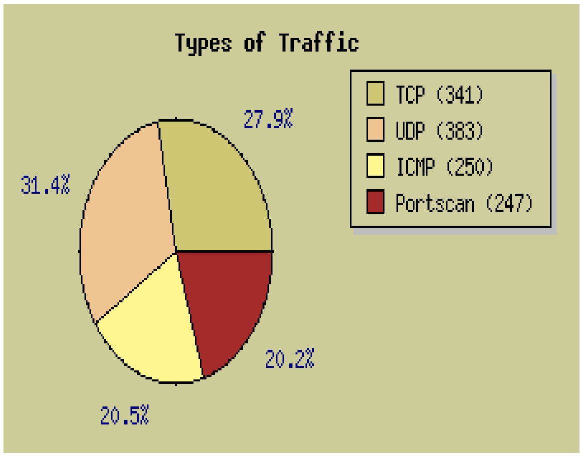


Figure 5.6: Traffic Analysis by Snort from the network.

6.Conlcusions and Future Scopes.

Snort is a powerful tool as an Intrusion Detection system. As far as the future of the snort is concerned, it can have IP-TABLES. Snort reports can also be included with false positive and false negative alerts.

If packets drop facility is added then the same SNORT can also be used as Intrusion Detection & Prevention System.When deploying Snort as Intrusion and Detection System , it is important to make sure the used rules are relevant and up to date, otherwise the system will be much less efficient due to low signal-to-noise ratio in the case of a bad choice of rules and due to Snort missing attacks completely in the case of a Snort system with rules not being updated properly. Apart from the challenge of selecting or writing good rules for Snort, there is a related disadvantage of this, since Snort only looks for things defined in its rule set, it doesn't have the ability to tell what traffic is considered to be normal from each host on the network, and what traffic seems to be out of place. This way, 'normal' behavior but from the 'wrong' computer on the network isn't noticed unless rules are to be setup on that host-by-host basis. There are few systems who have started to deal with this problem, called 'anomaly based intrusion detection systems', for e.g. ASDIC2 which is developed in Uppsala. However there are obvious advantages of using the Intrusion and Detection system , such as Snort in a network. Properly configured, it gives a good overview of what is going on in the particular network, and provides a way of automatically logging packets from potential attacks for future references. With some careful thinking, it can even be used for reacting directly to attacks as they occur .Comparison and analysis of alerts generated for the particular attack with respect to several protocols and signatures is made to show the strength and weakness of this approach

7. References:

#[1] Muraleedharan N, Arun Parmar , Manish Kumar ," A Flow based Anomaly Detection System using Chi-square Technique,285.

#[2] Kuo Zhao, Jianfeng Chu, Xilong Che, Lin Lin, Liang Hu ,"Improvement on Rules Matching Algorithm of Snort Based on Dynamic Adjustment"

#[3] Sebastian Schmerl1, Hartmut Koenig2, Ulrich Flegel3,i, Michael Meier4, René Rietz5," Systematic Signature Engineering by Re-use of Snort Signatures", proceeding 2008 Annual Computer Security Applications Conference ,23

[4] Daxin T. and Yang X., "A Multi-core Supported Intrusion Detection System", Proceedings of IFIP International Conference on "*Network and Parallel Computing*" (NPC 2008), pp: 50 -55, 2008

[5] Jain, P.and Goyal, S.; "An Adaptive Intrusion Prevention System Based on Immunity", Proceedings of IEEE International Conference on "*Advances in Computing, Control, & Telecommunication Technologies*", pp: 759 – 763, 2009.

[6]Cansian, A.M., da Silva, A.R.A. and de Souza, M.; "An attack signature model to computer security intrusion detection", Proceedings of IEEE Conference Proceedings *MILCOM* 2002, vol. 2, pp: 1368 – 1373, 2002.

[7] Marhusin, M.F., Cornforth, D. and Larkin, H.; "An overview of recent advances in intrusion detection", Proceedings of 8th IEEE International Conference on "*Computer and Information Technology*", pp: 432 – 437, 2008.

[8]Chandradeep, K.B.; "A Scheme for the Design and Implementation of a Distributed IDS", Proceedings of 1st IEEE International Conference on "*Networks and Communications*", pp: 265 – 270, 2009.

[9]Salah, K. and Qahtan, A.; "Boosting throughput of Snort NIDS under Linux", Proceedings of IEEE International Conference on "*Innovations in Information Technolog*", pp: 643 – 647, 2008.

[10] Ortiz, J., Tomelden, J., Beheshti, M., Kowalski, K. and Han, J.; "Component Based Information Network for Computer Security", Proceedings of 6th IEEE International Conference on "*Information Technology: New Generations*", pp: 467 – 469, 2009.

[11] Zhang Hu; "Design of Intrusion Detection System Based on a New Pattern Matching Algorithm", Proceedings of IEEE International Conference on "*Computer Engineering and Technology*", vol. 1, pp: 545 – 548, 2009

[12] Ahmed, M.; Pal, R.; Hossain, M.; Hasan, K. and Bikas, A.N.; "A Comparative Study on the Currently Existing Intrusion Detection Systems", Proceedings of IEEE International Conference on "Computer Science and Technology", pp: 151 – 154, 2009.

[13] Brian Caswell and Jeremy Hewlett. Snort Users Manual (available from http://www.snort.org/docs/)

[14] Dan S. and YanLing S.; "Detection of Network Intrusion Based on a HMM Model", Proceedings of 2nd IEEE International Conference on "*Multimedia and Information Technology (MMIT)*", vol.1, pp: 286 – 289, 2010.

[15] Migliardi, M. and Resaz, V.; “Distributed Intrusion Detection: Simulation and Evaluation of Two Methodologies”, Proceedings of 3rd IEEE International Conference on “*Emerging Security Information, Systems and Technologies*”, pp: 42 – 48, 2009.

[16] Muthuregunathan, R., Siddharth, S., Srivathsan, R. and Rajesh, S.R.; “Efficient Snort Rule Generation Using Evolutionary Computing for Network Intrusion Detection”, Proceedings of First IEEE International Conference on “*Computational Intelligence, Communication Systems and Networks*”, pp: 336 – 341, 2009