International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

*Review Article*

# Review of Alerts Generated for the Particular Attacks

**Sameer***

Shah Satnam Ji P.G Boys' College, Sirsa, India

Received 25 Aug 2017, Accepted 20 Oct 2017, Available online 30 Oct 2017, **Vol.7, No.5 (Sept/Oct 2017)**

***Abstract***

*Since the earlier days of human civilization, the need to keep data safe and secret is around. Several methodologies and later technologies have been devised and used for the same purpose. But the whole concept of securing data from unwanted attacks took a big turn with the widespread of Internet. Although internet provides uncountable benefits like emails, world-wide availability of information, video conferencing, e-commerce, etc; but it is also the biggest tool for hackers and crackers who may use sensitive data and information for their selfish purposes. A major methodology for protection of data is Intrusion detection which is one of the prime areas of research today. This paper surveys the existing literature on types of Intrusion, existing techniques and architectures used for their detection. This paper uses Snort tool for traffic analysis and comparison of alerts generated for the particular attack with respect to several protocols.*

***Keywords:*** *Gigabit, IDS, services, domain, intrusion, snort, prevention, Detection, techniques.*

## 1. Introduction

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 attempt 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 is primarily a network based activity with increasing global network connectivity. 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. Research in misuse detection has focused mainly on detecting network intrusions using different classification algorithms, association rules and cost sensitive modeling. Unlike signature-based intrusion detection systems, models of misuse are created automatically, and they can be more sophisticated and precise than manually created signatures. Anomaly detection algorithms build models of normal behavior and automatically detect any type of deviation from it. The major benefit of anomaly detection algorithms is their ability to potentially detect unforeseen attacks. In addition, they may also be able to detect new or unusual, but non-intrusive, network behavior that is of interest to a network manager. 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 tool is a single-threaded application that operates at the user-level, as shown in Figure 2.1. Snort uses libpcap packet capture library to access raw network packets. Figure depicts the underlying supporting building blocks traversed by an incoming packet from the NIC. The libpcap library offers a API to the socket interface of the Linux kernel networking subsystem. This subsystem is primarily comprised of the TCP/IP network protocol stack,softirq, and network device driver. Softirq is the non-urgent (or deferrable) kernel high priority event that handles incoming packets and forward it for

*Corresponding author: Sameer

processing by the network stack. In order to boost Linux performance to suit today's Gigabit traffic, current versions of Linux implement a new packet reception mechanism known as New API (NAPI) .This NAPI is integrated into the network device driver that handles packets in groups using softirqs.

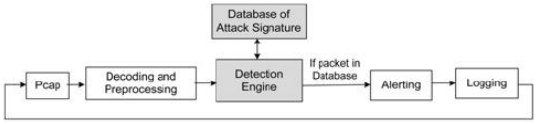



**Figure 2.1** Snort basic software components

Snort is a single threaded application which can be configured to operate in four modes: sniffer, packet logger, network intrusion detection system (NIDS) and intrusion prevention system (IPS). Packet sniffing and logging functions are the elementary parts of Snort, but Snort's beefiness and popularity come from its intrusion detection capabilities, and specifically working as NIDS. The IPS is a newly added feature and allows Snort tool to take preventive action against malicious or unwanted traffic such as dropping or re-directing packets to another destination. Snort captures raw packets with libpcab and then decodes and preprocesses them prior to forwarding them to the detection engine. The preprocessing includes layer three IP fragment reassembly, layer four transmission control protocol (TCP) session reconstruction. The detection engine checks packet payloads against several rules. If one or more rules matched, an attack is detected and the corresponding alert or loggings are performed.. The detection engine is the heart of Snort and the most complex part. It is essentially responsible for analyzing every packet based on rules that are loaded a trun time. The detection engine is the most computationally intensive part. This is mainly due to string matching within the packet payload against thousands of patterns.

## 3. Capturing network traffic

Snort is defaulted to work as a filter of network activity and therefore must be adjusted to work with collection of network packet information. The first step in this process is to log network traffic into a database system that is supported by snort such as:mysql, postgresql, odbc. mssql, or oracle. After the snort system is set to log this information the next step is to create rules that will log not only the community decided on rules but also the normal traffic from the network that the servers experience during the time that the attacks are being recorded. In order to achieve a log of the normal traffic to the servers an additional file from the community based rules is added to system to log all the rest of the traffic and therefore this normal traffic that can be used as part of the training set. This will create the desired effect of one database to hold all network traffic that is also marked as an attack on normal traffic

## 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 module for the Snort Intrusion Detection System. It provides real-time reporting from the My SQL database generated by Snort. This requires a platform with My SQL, 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.

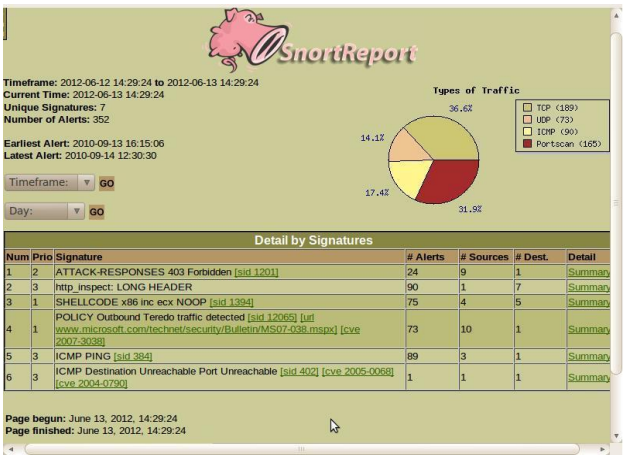



**Figure 5.1:** Snort Report-1 showing Intrusion Detection for 6-Signatures

*5.1 http_inspect: LONG HEADER Summary*

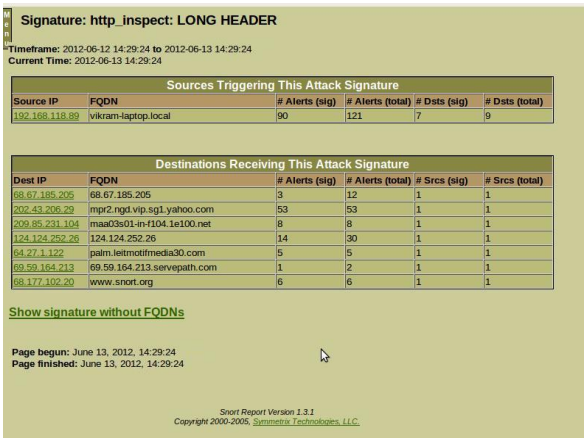
* max_header_length *

This option will take integer as an argument. This integer is the maximum length allowed for an HTTP client request header field. Requests that exceed this length will cause a Long Header alert. This particular alert is off by default. To enable, specifiying an integer argument to max_ header_ length of 1 to 65535. Specifying a value of 0 is treated as disabling the alert. A total of 90 such alerts are generated by source, as shown in figure 2.3.

*5.2 SHELLCODE x86 inc ecx NOOP Summary*

These signatures are based on shell code that is common among multiple publicly available exploits. Because these signatures check all type of traffic for shell code, these signatures are disabled by default. There is a large performance hit by enabling these signatures. The summary of this signature is shown in figure 2.4.

`



**Signature: http_inspect: LONG HEADER**

**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 | 90 | 121 | 7 | 9 |

Destinations Receiving This Attack Signature

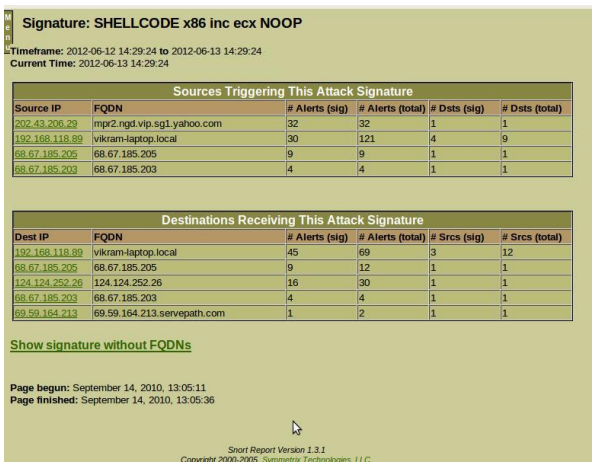
| Dest IP | FQDN | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|---|
| 68.67.185.205 | 68.67.185.205 | 3 | 12 | 1 | 1 |
| 202.43.206.29 | mpr2.ngd.vip.sg1.yahoo.com | 53 | 53 | 1 | 1 |
| 209.85.231.104 | maa03s01-in-f104.1e100.net | 8 | 8 | 1 | 1 |
| 124.124.252.26 | 124.124.252.26 | 14 | 30 | 1 | 1 |
| 64.27.1.122 | palm.leitmotifmedia30.com | 5 | 5 | 1 | 1 |
| 69.59.164.213 | 69.59.164.213.servepath.com | 1 | 2 | 1 | 1 |
| 68.177.102.20 | www.snort.org | 6 | 6 | 1 | 1 |

Show signature without FQDNs

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

*Snort Report Version 1.3.1*
*Copyright 2000-2005, Symmetrix Technologies, LLC.*

**Figure 5.3** Snort report signature summary of http_inspect: LONG HEADER.



**Signature: SHELLCODE x86 inc ecx NOOP**

**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) |
|---|---|---|---|---|---|
| 202.43.206.29 | mpr2.ngd.vip.sg1.yahoo.com | 32 | 32 | 1 | 1 |
| 192.168.118.89 | vikram-laptop.local | 30 | 121 | 4 | 9 |
| 68.67.185.205 | 68.67.185.205 | 9 | 9 | 1 | 1 |
| 68.67.185.203 | 68.67.185.203 | 4 | 4 | 1 | 1 |

Destinations Receiving This Attack Signature

| Dest IP | FQDN | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|---|
| 192.168.118.89 | vikram-laptop.local | 45 | 69 | 3 | 12 |
| 68.67.185.205 | 68.67.185.205 | 9 | 12 | 1 | 1 |
| 124.124.252.26 | 124.124.252.26 | 16 | 30 | 1 | 1 |
| 68.67.185.203 | 68.67.185.203 | 4 | 4 | 1 | 1 |
| 69.59.164.213 | 69.59.164.213.servepath.com | 1 | 2 | 1 | 1 |

Show signature without FQDNs

**Page begun:** September 14, 2010, 13:05:11
**Page finished:** September 14, 2010, 13:05:36

*Snort Report Version 1.3.1*
*Copyright 2000-2005, Symmetrix Technologies, LLC.*

**Figure** 5.4: Snort report signature summary of SHELLCODE x86 inc ecx NOOP.

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=0.73
4.SHELLCODE x86 inc ecx NOOP
Ratio of alerts generated on destination= alerts (sig)/alerts(total)=77/115=0.63
5.SNMP Broadcast Trap
Ratio of alerts generated on destination =alerts(sig)/alerts(total)=1/2=0.50
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=0.014
10.Stream5 : Data sent on stream not accepting data
Ratio of alerts generated on destination = alerts(sig)/alerts(total)=1/138=0.006

*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. UDP (31.4%).
3. ICMP (20.5%).

Portscan(20.2%)

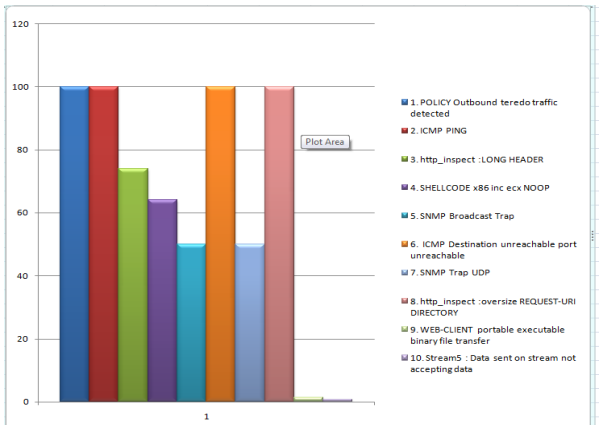



**Figure 5.5 :** Alert ratio of signatures for the particular attack

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

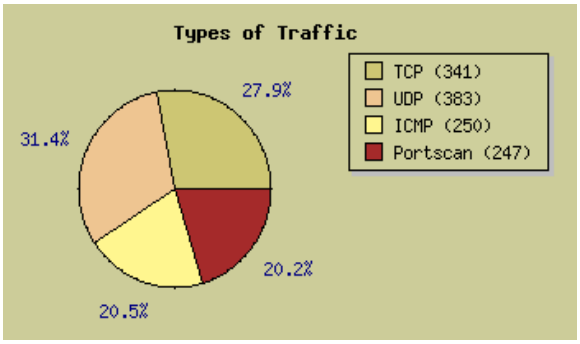



**Figure 5.6:** Traffic Analysis by Snort from the network.

## Conclusions

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 example: 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 is made to show the strength and weakness of this approach.

We hope this study will be useful for researchers to carry forward research on system security for design of a ideal Intrusion and Detection System that not only will have identified strengths but also overcome the drawbacks in this field of security.

## References

Xiangning; Zhiping JIANG;Xinli TIAN(2010) ,The detection and prevention for ARP Spoofing based on Snort proceeding International Conference on Computer Application and System Modeling (ICCASM 2010) ,v5-137

Sergei Egorov; Gene Savchuk , SNORTRAN: An Optimizing Compiler for Snort Rules.

Zhou Zhimin; Chen Zhongwen ;Zhou Ti echeng, Guan Xiaohui ,The Study on Network Intrusion Detection System of Snort ,proceeding 2010 International Conference on Networking and Digital Society .194

David Gullett; Symmetric Technologies ,014-snortinstallguide292.pdf

Kang Hong ; Zhang Jiangang ,An Improved Snort Intrusion Detection System Based on Self-similar Traffic Model by Kang Hong and Zhang Jiangang.(College of Economics and Management Shandong University of Science and Technology Qingdao, China ,97

Jiqiang Zhai; Yining Xie ;Research on Network Intrusion Prevention System Based on Snort Proceeding 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE) ,251.

Dihua Liu; Hui Li Research on Intelligent Intrusion Prevention System Based on Snort 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE),478

Shiv Kumar ;R.C.Joshi Design and Implementation of IDS Using Snort, Entropy and Alert Ranking System Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011) .264

Xingkui Liu Xinchun Liu Ninghui Sun , ,Fast and Compact Regular Expression Matching Using Character Substitution proceeding 2011 Seventh ACM/IEEE Symposium on Architectures for Networking and Communications Systems .85

Safaa O. Al-Mamory;Ali Hamid; Asala Abdul-Razak; Zainab Falah.String Matching Enhancement for Snort IDS.1020.

Yaron Weinsberg ;Shimrit Tzur-David ;Danny Dolev, One Algorithm to Match Them All:On a Generic NIPS Pattern Matching Algorithm,proceeding High Performance Switching and Routing Conference (HPSR'07).

Yu-Xin Ding; Min Xiao; Ai-Wu Liu (12-15 July 2009 ) ,Research and implementation on snort-based hybrid intrusion detection system ,Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding.

Cong Liu Ai Chen Di Wu Jie Wu, A DFA with Extended Character-set for Fast Deep Packet Inspection, proceeding 2011 International Conference on Parallel Processing.110.

Muraleedharan N; Arun Parmar ; Manish Kumar , A Flow based Anomaly Detection System using Chi-square Technique,285.

Kuo Zhao; Jianfeng Chu; Xilong Che; Lin Lin, Liang Hu ,Improvement on Rules Matching Algorithm of Snort Based on Dynamic Adjustment.