Using Jquery with Snort to Visualize Intrusion

Alaa El - Din Riad [1] , Ibrahim Elhenawy[2], Ahmed Hassan[3] and Nancy Awadallah[4]

[1]Vice Dean for Students Affairs, Faculty of Computer Science and Information Systems, Mansoura University, Egypt
Mansoura,,DK, 35513, Egypt

[2]Faculty of Computer Science and Information Systems, Zagazig University, Egypt
Zagazig, Egypt

[3]Faculty of Engineering , Mansoura University , Egypt
Mansoura,,DK, 35513, Egypt

[4]Faculty of Computer Science and Information Systems, Mansoura University, Egypt
Mansoura,,DK, 35513, Egypt

Abstract

The explosive growth of malicious activities on worldwide communication networks, such as the Internet, has highlighted the need for efficient intrusion detection systems. The efficiency of traditional intrusion detection systems is limited by their inability to effectively relay relevant information due to their lack of interactive / immersive technologies. Visualized information is a technique that can encode large amounts of complex interrelated data, being at the same time easily quantified, manipulated, and processed by a human user. Authors have found that the representations can be quite effective at conveying the needed information and resolving the relationships extremely rapidly. To facilitate the creation of novel visualizations this paper presents a new framework that is designed with using data visualization technique by using Jquery & Php for analysis and visualizes snort result data for user.

Keywords: *Intrusion Detection System, Snort rule Visualization techniques, , Php , Jquerry.*

1. Introduction

Data visualization is a technique that has been used for a long time to represent information. Although old, yet powerful, its main outcome is that it allows the representation of data by different formats and shapes, each one highlighting a particular group of features.

Visualization represents a powerful link between the most dominant information-processing systems, the human brain and the modern computer. It is a key technology for extracting information, and therefore it is becoming more and more necessary in the field of Network Security. The power of network visualization goes beyond the simple "illustration" of network behavior to help the analyst to discriminate between normal and abnormal activities. [1][2].

Using data visualization technique to support the result of snort (IDS) , we consider that PHP and Jquery as data visualization technique , we will deal with data of snort database to detect which data will be useful for network administrator to be visualized .

The framework introduced here is powerful because it is general, it can be applied to a wide domain of visualization problems. This research will assist users of visualization to explore, communicate, and understand their results.

The organization of this paper: next section discusses related research, section 3 discusses snort rules, and section 4 presents proposed system by using data visualization techniques for intrusion detection.

2. Related Research

J.Blustein, C.Fu and D.L.Silver presents proposed system that utilizes spatial hypertext workspace as the user interface could reduce the impact of high false alarm from IDS. This system may improvement the user's willingness to continuously monitor the system [3].

R.F.Erbacher discuss how user behavior can be exhibited within the visualization techniques, the capabilities provided by the environment, typical characteristics users should look out for (i.e., how

unusual behavior exhibits itself), and exploration paradigms effective for identifying the meaning behind the user's behavior [4] .

H.Koike and K.Ohno propose a visualization system of a NIDS log named SnortView, which supports administrators in analyzing NIDS alerts much faster and much more easily. Instead of customizing the signature DB, they propose to utilize visualization to recognize not only each alert but also false detections [5].

N.Rangaraju and M.Terk describe a framework that is designed to simplify the process of building immersive visualization of structural analysis of building structures. They describe the components of the framework and describe two applications that were created to test their functionality [6].

J.Peng, C.Feng and J.W.Rozenblit proposed a hybrid intrusion detection and visualization system that leverages the advantages of current signature-based and anomaly detection methods. The hybrid instruction detection system deploys these two methods in a two staged manner to identify both known and novel attacks.
When intrusion is detected, autonomous agents that reside on the system will automatically take actions against misuse and abuse of computer system, thus protecting the system from internal and external attacks [7].

Y.Park and J.Park presents Web Application Intrusion Detection System (WAIDS); an intrusion detection method based on an Anomaly Intrusion Detection model for detecting input validation attacks against web applications. Their approach is based on web application parameters which has identical structures and values. WAIDS derives a new intrusion detection method using generated profile from web request data in normal situation. By doing this, it is possible to reduce analysis time and false positives rate [8].

R.U. Rehman consider snort as an open source packet sniffer and logger that can be used as a lightweight Intrusion Detection System (IDS) to detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, and more. The Basic Analysis and Security Engine (BASE) displays and reports intrusions and attacks logged in the Snort database in a web browser for convenient analysis [9].

A.Komlodi, J. R. Goodall and W.G. Lutters report a framework for designing information visualization (IV) tools for monitoring and analysis activities.They studied ID analysts' daily activities in order to understand their routine work practices and the need for designing IV tools [10].

K.Abdullah presents new techniques to aid in network security using information visualization. Research contributions have been made in network data scaling and processing, port activity visualization, useful visualization showing a larger amount of information than textual methods, scaling port numbers and IP address for maximum use of screen space without occlusion, performing and using user study results to design an IDS alarm visualization tool [11].

R.Erbacher, M.Garber are attempting to improve the administrators ability to analyze the available data, make far more rapid assessments as to the nature of a given event or event stream, and identify anomalous activity not normally identified as such [12] .

K.Nyarko,T.Capers, etc., present a network intrusion visualization application with haptic integration, NIVA,which allows the analyst to interactively investigate as well as efficiently detect structured attacks across time and space using advanced interactive three-dimensional displays [13].

From previous studies we present our framework which be overcome on the problem of how to describe intrusion detection system results for network administrator.

3. Snort Rule

Snort uses a simple, lightweight rules description language that is flexible and quite powerful.
Snort rules operate on network (IP) layer and transport (TCP/UDP) layer protocols [9].

3.1 Rule Structure

Snort rules are divided into two logical sections as illustrated in Fig.1, the rule header and the rule options.

Rule Header	Rule Options

Fig. 1: Basic structure of Snort rules [9]

The rule header contains information about what action a rule takes. It also contains criteria for matching a rule against data packets. The options part usually contains an alert message and information about which part of the packet should be used to generate the alert message. The options part contains additional criteria for matching a rule

against data packets. A rule may detect one type or multiple types of intrusion activity.
Intelligent rules should be able to apply to multiple intrusion signatures [9][14] .
The general structure of a Snort rule header is shown in Fig. 2

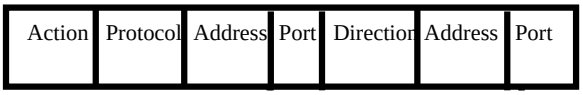

Fig. 2: Structure of Snort rule header [9]

Fig. 3 describes snort rule sample:

```
alert tcp any any -> 192.168.1.0/24 111
(content:"|00 01 86 a5|"; msg: "mountd
access";)
```

Fig. 3: Sample Snort Rule [14]

3.2 Rule classtype

Rules can be assigned classifications and priority numbers to group and distinguish them.
Using the classification keyword is useful to prioritize intrusion detection data.
The class type keyword, is found at the file (classification.config) which is included in the (snort.conf) file using the include keyword [9].
Each line in the (classification.config) file has the following syntax:

Config classification: name, description, priority.

The *name* is a name used for the classification. The name is used with the classtype keyword in Snort rules. The *description* is a short description of the class type. *Priority* is a number that shows the default priority of the classification, which can be modified using a priority keyword inside the rule options. An example of this configuration parameter is as follows:

Config classification: DoS, Denial of Service Attack, 2

In the above line the classification is DoS (Denial of Service) and the priority is 2.
Fig. 4 illustrates rule uses default priority with the classification DoS:

```
alert udp any any -> 192.168.1.0/24 6838
(msg:"DoS"; \content: "server"; classtype:
DoS;)
```

Fig. 4: Using classtype in a rule [9]

In the next section we will use of the classification keyword in displaying Snort alerts by visualizing it through PHP & Jquery as visualization techniques.

4. Proposed System

This research aims to design a system for visualize intrusion detection by using PHP & Jquery as data visualization technique .The system introduces four components as showed in Fig. 5 and illustrated in detail in our previous paper [15].

This paper interest in "IDS Database","Analysis Engine ", "Visualized System" components which are described sequencing in section 4.1, 4.2 and 4.3.

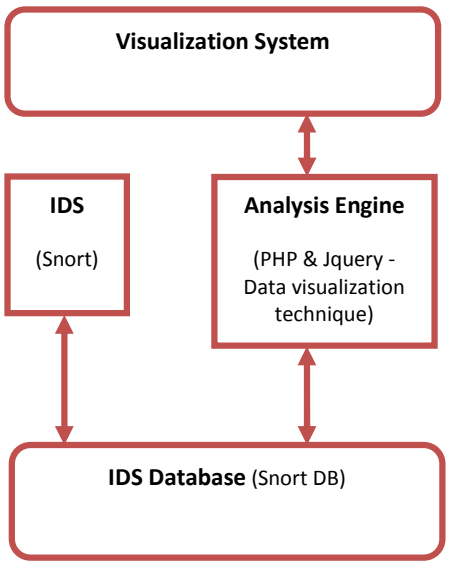

Fig. 5: Proposed System Structure

4.1 IDS (Snort) Database

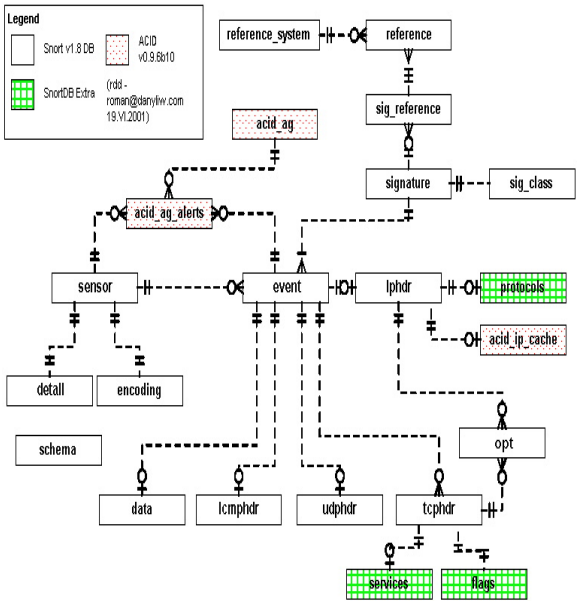

Fig. 6: Snort database schema [16]

The next table illustrates five tables of Snort database from which component related to (Snort or ACID) and its description.

Table 1: snort tables [16]

Table	Component	Description
event	Snort	Meta-data about the detected alert
signature	Snort	Normalized listing of alert/signature names, priorities, and revision IDs
sig_class	Snort	Normalized listing of alert/signature classifications
iphdr	Snort	IP protocol fields
acid_ag	ACID	Meta-data for alert groups

4.2 Analysis Engine

This component responsible for retrieving data from snort database which be detected from snort (IDS) to be analyzed and processed it by PHP & Jquery.

The next figure (Fig.7) illustrated the relationship between previous tables in Table1.

Fig.8 is a screenshot of retrieving data from tables. There is a classification column which means signature classification:
(Misc attack – Attempted user - Attempted recon- Attempted dos – Web application activity – Bad unknown)

After retrieving data from snort tables, we using Jquery & PHP to visualize signature classification as it will be showed in section 4.3.

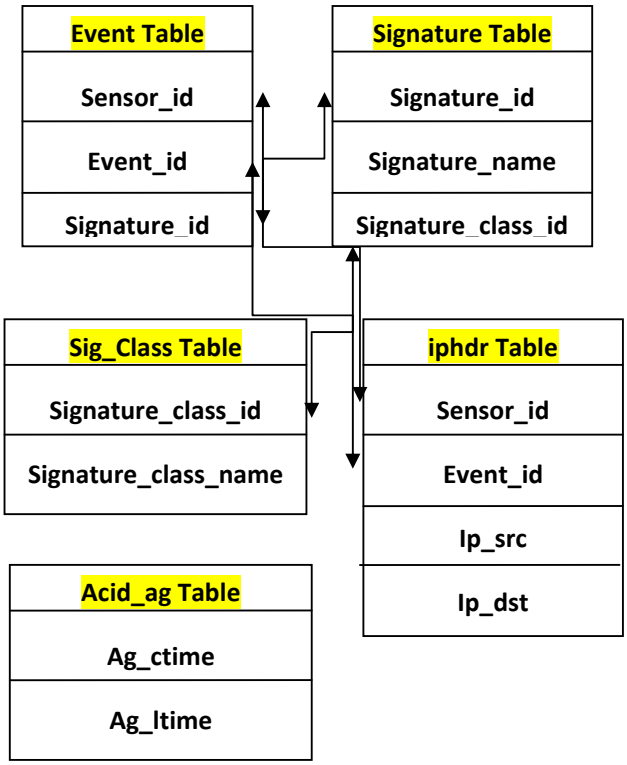

Fig.7: The relationship between used tables

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

Fig.8: Use of the classification keyword in displaying Snort alerts [9]

The previous table included retrieved data from 5 tables which are illustrated and it's relation in fig.7: (Event, Signature, Sig_Class, iphdr, Acid_ag).

Researchers will use second column (**Classification**) from table in fig.8 to extract visualization system as it will be showed in fig.9 .

4.3 Visualization System

This component will be user interface for snort intrusion detection system result implemented by Jquery & PHP (Data Visualization Technique).

The next figure is an output from using PHP & Jquery as data visualization techniques after implementing data which was retrieved from (**Classification** column in fig.8) .This classification is according to signature (Misc-attack , Bad-unknown, Attempted-recon, Web-application-activity, Attempted-user , Trojan-activity, Attempted-dos).

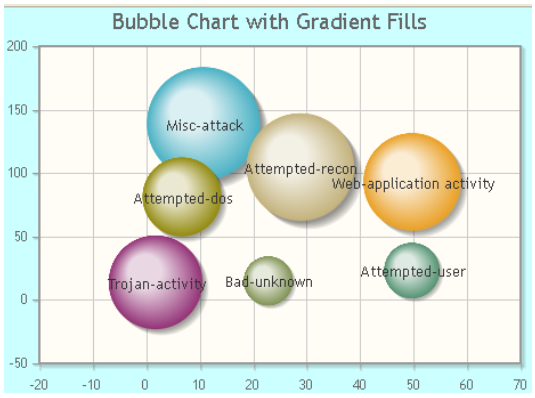

Fig. 9: Visualization System

4.4 Flowchart for proposed System

The next figure (fig.10) illustrates the flowchart of our proposed system which contains processes such as:

- Execute snort rules from (IDS component).
- Retrieving data from snort Database component.
- Using PHP & Jquery technique as analysis engine component.
- Extract new charts from analysis engine .

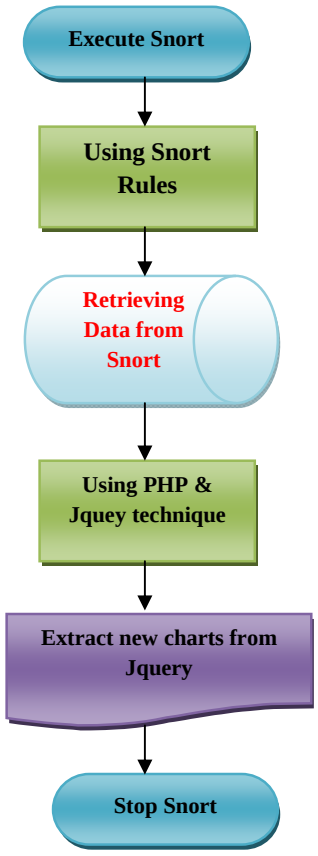

Fig.10: Flowchart for proposed System

5. Conclusion & Future Work

Intrusion detection is an information intensive and deeply analytic process that cannot be undertaken without the assistance of a computer.

Intrusion detection systems must handle masses of information (often in real-time) so as to report the abnormal use of networks and computer systems.

Our proposed system has proven to be effective for visually the intrusion which be detected by snort system.

In the future work we will compare between using visualization tools for intrusion detection
such as NetGrok and using visualization techniques such as CSS & JQUERY.

References

[1] Nurbol, H. Xu, H.Yang, F.Meng, L. Hu,"A real-time intrusion detection security visualization framework based on planner-scheduler",IEEE ,2009 .

[2] I. Onut , B.Zhu , A. Ghorbani, " A novel visualization technique for network anomaly detection" , proceedings of the 2nd Annual Conference on Privacy, Security and Trust (PST),p.167-174, 2004 .

[3] J.Blustein, C.Fu, D.L.Silver," Information Visualization for an Intrusion Detection System", ACM, 2005.

[4] R.F.Erbacher," Intrusion Behavior Detection Through Visualization", IEEE , 2003 .

[5] H.Koike and K.Ohno ,"SnortView: Visualization System of Snort Logs" IEEE , 2004 .

[6] N.Rangaraju and M.Terk ," Framework for Immersive Visualization of Building Analysis Data " , IEEE , 2001 .

[7] J.Peng, C.Feng and J.W.Rozenblit,"A Hybrid Intrusion Detection and Visualization System", IEEE , 2006 .

[8] Y.Park and J.Park ," Web Application Intrusion Detection System for Input alidation Attack" , IEEE , 2008 .

[9] R.U. Rehman " Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID" , Publishing as Prentice Hall PTR Upper Saddle River, New Jersey, 2003.

[10] A.Komlodi, J.R. Goodall, W. G. Lutters, "An Information Visualization Framework for Intrusion Detection, 2004, IEEE

[11] K.Abdullah , " Scaling and Visualizing Network Data to Facilitate in Intrusion Detection Tasks" ,Phd., School of Electrical and Computer Engineering ,Georgia Institute of Technology ,May 2006 .

[12] R.Erbacher, M.Garber,"Visualization Techniques for Intrusion Behavior Identification ", 2004, IEEE.

[13] K.Nyarko, T.Capers, C.Scott, K.Ladeji-Osias," Network Intrusion Visualization with NIVA, an Intrusion Detection Visual Analyzer with Haptic Integration", 2002, IEEE.

[14]ftp://petrinet.dvo.ru/pub/Vyatta/build-so/pkgs/vyatta-snort/debian/my/snort_rules.html , last visit on 29-11-2011

[15] A.M.Riad, I. Elhenawy, A.Hassan, N.Awadallah, "Data Visualization Technique Framework for Intrusion detection", JCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, September 2011.

[16]http://www.andrew.cmu.edu/user/rdanyliw/snort/acid_db_er_v102.html - last visit 03/10/2011

Authors

Alaa El - Din Riad, Vice Dean for Students Affairs, Faculty of Computer and Information Sciences, Mansoura University

Ibrahim Elhenawy, Faculty of Computer and Information Sciences, Zagazig University

Ahmed Hassan, Department of Electrical Engineering, Faculty of Engineering, Mansoura University

Nancy Awadallah Researcher Assistant, Master in E-commerce Security 2008, Faculty of computer science & Information System - Mansoura University - Egypt