International Journal of Engineering & Technology, 8 (1) (2019) 53-58

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 20985
Research paper



A comparative paper on measuring the performance of snort and suricata with variable packet sizes and speed

M. Naga Surya Lakshmi [1] *, Dr. Y. Radhika [2]

[1] Research Scholar, Dept. of CSE, GIT, GITAM University, Visakhapatnam, Andhra Pradesh, India
[2] Professor, Dept. of CSE, GIT, GITAM University, Visakhapatnam, Andhra Pradesh, India
**Corresponding author E-mail: mnslakshmi.gitam@gmail.com*

Abstract

This survey paper focuses mainly on comparing the performance of free open-source IDS tools like snort and Suricata, for identifying malignant activities on HIDS. Among the existing intrusion detection tools, Snort is one of the best free open-source tools and for over a decade it is the most widely used tool in the computing industry. The objective of Suricata is to offer signature-based intrusion detection and the latest version is released in the year 2018. Suricata is combined with the latest advancements in recent technology such as multi-threading of the process in order to get better processing rate. We evaluated the processing speed, consumption of memory, and accuracy. We observed in the process of handling a larger amount of network traffic data Suricata has shown better results when compared with Snort and both tools have registered with like accuracy.

Keywords: *Snort; Suricata; Intrusion Detection System; TCP; UDP.*

1. Introduction

Intrusion detection systems (IDSs) can also be termed as a second defending shield for defending threats, and play a vital role in giving widespread defending. In view of the fact that it is hard to build up a comprehensive way to avoid network attacks, mainly on complex machines, and intruders are constantly annoying to stumble on innovative behavior to find a way around these prevention techniques, IDS have turned into an unavoidable component of security systems. IDS come into access only occurring after an intrusion. The main objective of an intrusion detection system is to identify potential network threats to systems and to offer suitable alerts such as alerting security experts, terminating, destructive network links, and other related issues.

Numerous data security approaches are realistic today to guard data frameworks against unauthorized utilize, replication, adjustment, decimation and infection assaults. An Intrusion Detection System (IDS) is a program that examines what happens or has occurred amid an execution and attempts to discover signs that the PC has been abused. There are bounteous written works on Intrusion location framework, and a few IDS approaches have been proposed. The fundamental thought is that interruption conduct includes the strange use of the framework.

Diverse methods and methodologies have been utilized in later advancements. A portion of the methods utilized is measurable methodologies, prescient example age, master frameworks, keystroke observing, state change examination, design coordinating, and information mining procedures.

Disregarding the numerous advancements in network security over the previous decade, the Internet remains an unfriendly situation for our organized PC frameworks. As per Symantec Internet Security Threat Report for 2010, "The volume and refinement of malignant action expanded altogether in 2010" [1]. Assaults by worms, for example, Stuxnet and adventures in generally utilized projects, for example, Adobe Acrobat are ongoing cases of the bore and recurrence of vindictive movement that is seen being made with the present innovation. It is not any more sheltered to overlook the security dangers that we face, and we keep on becoming increasingly needy upon computers network and the Internet.

Intrusion detection was one of the most popular research areas in the field of security since 1987[2]. Denning proposed an intrusion detection Scheme in the year 1987. Numerous methods have been acquainted with distinguishing interruptions successfully and productively; so the security objectives of a framework - secrecy, respectability, and accessibility could be fulfilled. Analysts have been dealing with discovering answers to the accompanying inquiries: How to identify assaults successfully and proficiently, which reactions to give against recognized assaults, how to ceaselessly adjust to new assault methodologies, and such like. Significant research territories on interruption location could be outlined as takes after (Lundin and Jonsson, 2002): establishments, information gathering, identification techniques, reaction, IDS condition and design, IDS security, testing and assessment, operational angles, and social perspectives. In this investigation, we look at the developmental calculation based methodologies proposed for each examination zone on interruption identification.

Copyright © 2019 M. Naga Surya Lakshmi, Dr. Y. Radhika. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. Related data: evolution of ids

The genesis of intrusion detection commencing with James Anderson's technical report in the year 1980 at Computer Security Threat Monitoring and Surveillance for the U.S. Air Force. The paper demonstrated that review records could be utilized to recognize PC abuse and to distinguish risk characterizations, and it offered proposals to enhance inspecting of frameworks to distinguish abuse. It depends on the convictions that an interloper's conduct will be perceptibly not the same as that of an honest to goodness client, and that numerous unauthorized activities will be distinguishable.

Dr. Dorothy Denning has presented a model that would investigate review trails from government frameworks and track client movement, in the Year 1985. He named this framework as Intrusion Detection Expert System (IDES), and it was the central investigation into IDS innovation. In the year 1986, he proposed an expansion to his past interruption discovery display, which has subjects, objects, review records, profiles, oddity records, and the action runs as real segments in the proposed demonstrate. Subjects allude to the initiators of movement in a data framework; they are generally typical clients. Items are the assets overseen by the data framework, for example, records, orders, and gadgets. Review records are those created by the data framework in light of activities performed or endeavored by subjects on objects.

Sheaf presented a joined model of both oddity recognition and abuse discovery. IDS that models singular clients and additionally gatherings of clients. It allocates beginning profile to new clients and updates the profiles once an example of genuine conduct is perceived. Bundle utilized an alternate measurable peculiarity recognition calculation.

Lunt, T.F., has proposed a review of a study of computerized review trail examination strategies and interruption recognition frameworks was exhibited. Lunt utilizes the mix of two methodologies IDES to end up solid interruption location framework. The IDES is solid in factual approach.

Todd Heberlein, 1989, proposed an IDS framework called Network System Monitor (NSM) was presented by Todd. NSM was not the same as IDES and DIDS (Distributed Intrusion Detection System) in that it would break down system activity instead of framework logs. NSM, alongside the now economically accessible Stalker IDS, made new mindfulness and enthusiasm for IDS look into for the business and open segments.

Marcus J. Ranum, 1990, has created business IDS called Network Flight Recorder (NFR). Christopher Klaus and Thomas E. Noonan established Internet Security Systems (ISS) and discharged a system based interruption identification framework called Real Secure. In the Same year, Teng, Chen, And Lu have presented a period based inductive machine (TIM) model to catch a client's standard of conduct. As a broadly useful device, TIM finds fleeting consecutive examples in an arrangement of occasions. Consecutive examples speak to exceedingly redundant exercises and are relied upon to give a prediction. The transient examples, which are spoken to as guidelines, are created and altered from the information utilizing a coherent surmising, called inductive speculation. At the point when connected to interruption identification, the principles depict the standards of conduct of either a client or a gathering of clients in view of past review history.

Mukherjee, B., Heberlein, L., and Levitt, K, in 1994, have distributed a data in view of studied a few host-based and arrange based IDSs, and recognized the qualities of relating frameworks are distinguished. The host-based frameworks utilize the host working framework's review trails as the principle wellspring of contribution to distinguish meddlesome action, while a large portion of the system based IDSs assemble their discovery component by an observing system movement, and some utilize have review trails too. A diagram of a factual inconsistency discovery calculation utilized in a run of the mill IDS is additionally included [8].

Suspend, H., Dacier, M., And Wespi, 2000 This paper examined a scientific classification of interruption identification frameworks that features different parts of this region. This scientific categorization separates groups of interruption identification frameworks as indicated by their properties.

Yu Chen, Yu-Kwong Kwok, and Kai Hwang, 2005, This paper display another flag preparing way to deal with distinguishing and recognize the assaults (by inspecting the recurrence space attributes of approaching traffic flows to a server). This procedure is successful in that its identification time is not as much as a couple of moments. Besides, this procedure involves straightforward usage, making it deployable, in actuality, arrange conditions.

Jeyanthi Hall, 2007, this paper shows an abnormality based interruption identification approach, which consolidates radio recurrence fingerprinting (RFF) and Hotelling's T 2, a multivariate factual process control procedure, for distinguishing this assault. RFF is a system used to exceptionally distinguish a handset in light of the transceiver point (set of highlights) of the flag it produces. The approach is to relate a handset profile of a remote gadget with its comparing MAC address. Subsequently, in spite of the fact that the MAC address can, in any case, be ridiculed, the transceiver prints from the ill-conceived gadget would not coordinate the profile of the real gadget. In addition, the achievement rate of remote IDS can be additionally enhanced, by investigating numerous sequentially requested transceiver prints, before rendering a choice.

Naeimeh Laleh and Mohammad Abdollahi Azgomi, 2009. This paper talked about the misrepresentation that is developing amazingly with the development of current innovation and the all-inclusive superhighways of correspondence which results in the loss of billions of dollars all through the world every year. This method has a tendency to propose another scientific categorization and finish a survey for the diverse sorts of misrepresentation and information mining procedures of extortion location.

In the year 2010, Yurong Xu, James Ford, and Fillia Makedon have presented a paper on Intrusion Detection System. This paper presents a conveyed wormhole recognition calculation called Wormhole Geographic Distributed Detection (WGDD) that depends on the recognizing system issue caused by the presence of a wormhole. Since wormhole assaults are inactive, this calculation utilizes a bounce considering strategy a test system to recognize wormhole assaults, at that point recreates nearby maps in every hub. From that point onward, it utilizes an element called "measurement" to recognize irregularities caused by wormholes. The fundamental preferred standpoint of utilizing a disseminated wormhole recognition calculation is that it gives the estimated area of a wormhole, which might be helpful data for advanced protection systems.

3. Information about snort

Snort is a notable name in the data security network as it was made in 1998 by Martin Roesch who is the author of Source fire and who is as yet driving improvement of Snort. Snort is an open source organizes interruption anticipation and identification framework (IDS/IPS) that joins the advantages of mark, convention, and oddity based review. It utilizes a set of standards to check for unfriendly bundles in the system and after that create cautions to the system executive. The primary point of Snort, Suricata and some other IDS framework is to viably break down all parcels passing toss the system with no bundle drops [7]. Essentially, Snort is a multi-mode organize packet

Sniffing Tool, Snort tool can be executed in Sniffer mode, Packet Logging mode, NIDS mode. The principal goal of the Snort is to perform organize activity investigation progressively and post handling utilizing Network Forensic. Snort keeps running in NIDS mode if there is no charge line switches are gotten and it searches for the Snort design document called snort.conf.

3.1. Snort security policy

For Any Successful interruption, location relies upon strategy and administration as much as innovation. The Security Policy expresses the how quick an interruption can be identified and alarms the overseer as notices. Reaction coordination is likewise assumed an imperative part in the age of alarms.

3.2. Snort design

Snort is a lightweight and convenient device, which can be utilized in any working framework. Snort has enrolled quick and high plausible recognition over a 100Mbps system and it is effectively configurable utilizing neighborhood tenets and it likewise underpins many logging and detail choices. Snort utilized Libpcap and Tcpdump sniffing interfaces for location and Snort rules are composed and created in view of identification motor and module configuration permits clients with higher adaptability.

3.3. Location engine

Snort is fundamentally implied for an abuse identification utilizing mark database and intermittently signature storehouse refreshes and at whatever point new assaults are distinguished. Snort is having the high scope of location abilities like Fingerprinting in the working framework, cushion floods, Guess passwords and port outputs. Snort rules are straightforward and exceedingly adaptable to make new principles.

3.4. Module interfaces

The preprocessor is utilized to control or inspected before providing for the recognition motor module, and Detection interface performs basic and single tests on a solitary field of the system parcel. Yield interface reports results by taking from other application modules.

3.5. Utilizing snort in sniffer mode

In Sniffer mode, it works like much like tcpdump and in this mode Snort disentangles parcels and sends them into stdout record area, to have better understandability of system movement, Snort utilizes sifting interface like BPF to shape the system activity.

3.6. Utilizing snort in packet logger mode

This logging mode gives multi-mode bundle logging alternatives to deal with tcpdump information, XML information parcels, and ASCII Flat record, and so on. In this mode, Post-handling movement is performed to recognize abnormal exercises in the system.

3.7. NIDS mode

In Network interruption location mode, there is achievability of composing more number of Snort rules for the signature database. NIDS mode gives different discovery modes by utilizing modules and interfaces. This mode can deal with more number of Rules or marks and bizarre exercises produced because of measurable information and furthermore it performs arrange the convention check to contrast each system bundle and guidelines database.

3.8. Snort rules

Snort rules are profoundly adaptable and simple to change and adjust, where it isn't that substantially less demanding in other business NIDS instruments.

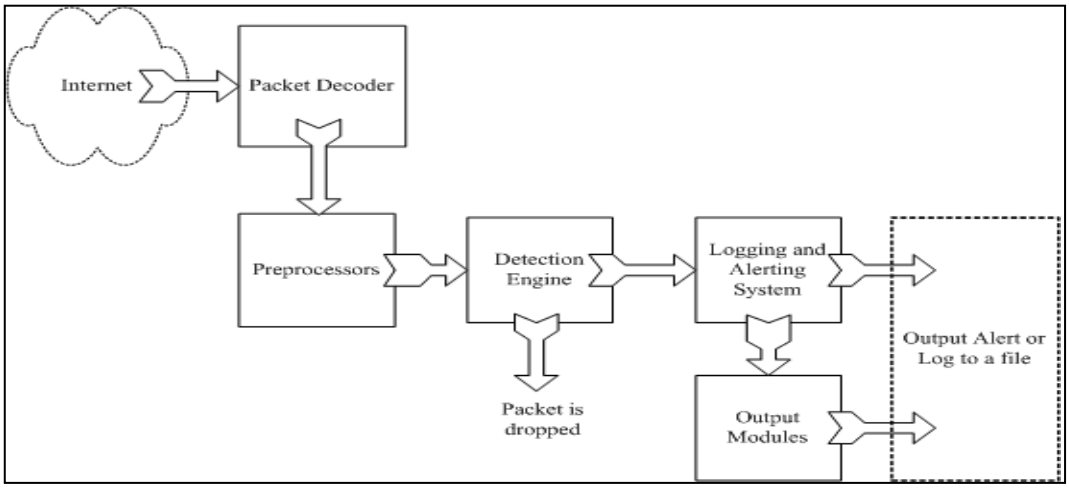


Fig. 3.1: Snort Architecture.

4. Suricata

Suricata is a one of the free open source Intrusion Detection System that exploits remotely created run sets to screen sniffed arranges activity and give alarms when suspicious occasions occur. Like most IDS it is intended to detect internal existing system security parts. The underlying arrival of Suricata keeps running on a Linux 2.6 stage and backings both inline and detached activity checking the design fit for taking care of various gigabit movement levels. Suricata fills in as a multithreaded motor. Suricata is an open source interruption identification and a counteractive action framework created by the 'Open Information Security Foundation'.
The beta adaptation was discharged in December 2009, while the main stable variant came in July 2010. Suricata was made to convey new thoughts and innovation to the interruption discovery field. [3] Open Information Security Foundation (OISF) furnishes Suricata with interruption location and counteractive actions govern set.
The way toward keeping up an ideal security level is streamlined by the Suricata motor. Suricata can utilize rules from various assets, for example, Emerging Threats and Snort VRT rules, to give the most ideal govern set.
As other system interruption discovery frameworks, Suricata screen arrange activity and make cautions/alarms logs when vindictive movement is distinguished. Suricata is intended to be good with other security parts, and it offers highlights, for example, bound together yield usefulness, and it is conceivable to acknowledge calls from different applications through its pluggable libraries.
Suricata likewise underpins a wide assortment of parcel procurement techniques, similar to Snort. The present Suricata discharge underpins the bundle obtaining utilizing the accompanying catch techniques:

- High-performance capture of network packets using AF_PACKET and PF_RING approaches
- Standard capture can be done using PCAP and Net filter integration methodologies.
- IPS mode is mainly used as Net filter approach on Linux operating System Using NFQUEUE.

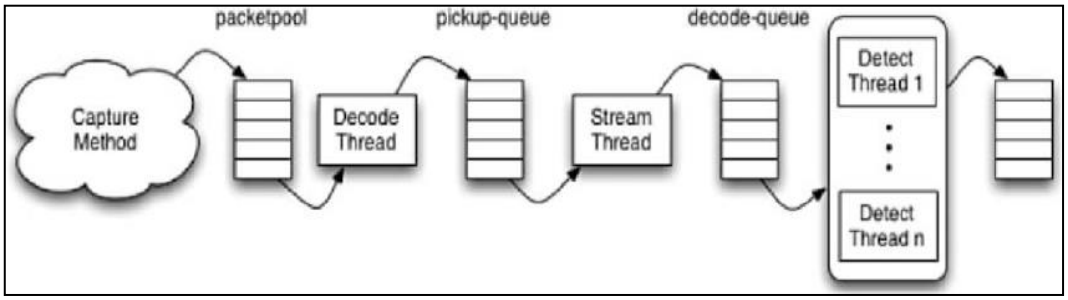


Fig. 4.1: Suricata Architecture.

5. Comparison of snort vs. suricata

5.1. Exceptionally scalable

Basically, Suricata is multi-variant detection tool. This implies one example can be run and it will adjust the heap of handling over each processor runs on a sensor Suricata is designed to utilize. This enables item equipment to accomplish 10-gigabit speeds on the genuine activity without yielding tenet set scope.

5.2. Convention identification

The most well-known conventions are consequently perceived by Suricata as the stream begins, hence permitting principle essayists to compose a control to the convention, not to the port anticipated. This makes Suricata a Malware Command and Control Channel seeker like no other. Off port HTTP CnC channels, which regularly slide appropriate by most IDS frameworks, are no problem for Suricata! Besides, because of committed catchphrases, you can coordinate on convention fields which run from HTTP URI to an SSL endorsement identifier.

5.3. Document identification, MD5 checksums, and file extraction

Suricata is able to analyze a large number of incoming networks packets of a system. The document's MD5 checksum is computed on the fly, so in the event that you have a rundown of md5 hashes you need to keep in your system, or needs to keep out; Suricata can discover it [3]. Snort is a free and open source Network Intrusion Prevention System and the Network Intrusion Detection System made by Martin Roesch in 1998 [2]. NIDS is the sort of Intrusion Detection System (IDS) that is utilized for checking information streaming on the network [11]. Snort is, by a long shot, the highest quality level among open source NIDS frameworks. Snort marks are stayed up with the latest by its devoted clients and the Snort site has sufficient documentation, including instructional exercises. It isn't, be that as it may, simple to utilize and requires an accomplished security IT expert to design it appropriately. The way that it's free makes it the dear of little and medium measured organizations that can't manage the cost of the extravagant GUIs and wizards of business arrange security items There are likewise have based interruption discovery frameworks, which are introduced on a specific host and recognize assaults focused on the host as it were. Albeit all interruption identification techniques are still new, Snort is positioned among the best quality frameworks accessible today.
Snort is coherently separated into numerous segments. These segments cooperate to identify specific assaults and to create yield in a required configuration from the recognition framework. A Snort-based IDS comprises of the accompanying significant segments: Packet Decoder, Preprocessors, Detection Engine, Logging and Alerting System and Output Modules Any information bundle originating from the Internet enters the parcel decoder. On its way towards the yield modules, it is either dropped, logged or an alarm is produced [6].

5.4. Bundle decoder

Bundles from various kinds of system interfaces are taken by parcel decoder and the bundles to be pre handled or to be sent to the location motor are readied. The interfaces might be Ethernet, SLIP, PPP et cetera.

5.5. Pre-processors

Preprocessors are segments or modules that can be utilized with Snort to mastermind or adjust information bundles before the location motor does some activity to see whether the parcel is being utilized by an intruder [7]. Some preprocessors likewise perform location by discovering oddities in parcel headers and creating cautions. Preprocessors are essential for any IDS to get ready information parcels to be broke down against the rules in the location motor. Programmers utilize distinctive methods to trick an IDS in various ways [8]. Preprocessors are additionally utilized for parcel defragmentation. At the point when a substantial information lump is exchanged to a host, the parcel is generally divided

5.6. The detection engine

The obligation of a discovery motor which is the meet imperative piece of Snort is to distinguish if any interruption action exists in a bundle. The recognition motor utilizes Snort rules for this reason. The tenets are perused into inside information structures or chains where they are coordinated against all parcels. In the event that a bundle coordinates any control, proper move is made; generally, the parcel is dropped. Suitable activities might log the bundle or creating alarms [12].

5.7. Logging and alerting system

Contingent on what the discovery motor finds inside a parcel, the bundle might be utilized to log the movement or create an alarm. Logs are kept in basic content documents, tcpdump-style records or some other form [11]. The majority of the log documents are put away under/var/log/Snort organizer as a matter of course. Many summon line alternatives examined in the following section can adjust the sort and detail of data that is logged by the logging and cautioning framework.

5.8. Yield modules

Distinctive tasks relying upon how you need to spare yield produced by the logging and alarming arrangement of Snort should be possible by yield module or modules. Fundamentally these modules control the sort of yield produced by the logging and cautioning system [9].

6. Experimental results

The Snort and Suricata have been tested on the Windows operating system and to measure the accurate performance of both IDS tools, we tested with different packet sizes for both UDP and TCP. Another parameter internet speed has taken into consideration in order to predict the performance of packet capturing. We have tested under various internet speeds.

6.1. Transmission control protocol

In this first phase, snort and Suricata have been tested on the TCP protocol. Snort has performed well with zero packet drops with a packet size 512 at internet speed of 200Mbps and higher, on the other hand, Suricata has not dropped packets at the same internet speed. Table 1 shows the percentage of packet loss at variable speeds. Whereas Suricata dropped 2% of packet loss at the speed of 400Mbps. When we increased the packet size to 1024, we have observed there is a decrement of 2% packet loss compared with packet loss recorded with a packet size of 512. The Suricata tool also registered 12% decrement in packet loss, with a packet size 1024 and speed 1Gbps.

Table 1: Packet Loss Recorded with A Packet Size of 512 and 1024, Under TCP Protocol

IDS Tool	Packet Size	Internet Speed 200 Mbps	400 Mbps	600 Mbps	800 Mbps	1Gbps
Snort	512	Zero Packet Loss	Zero Packet Loss	Zero Packet Loss	3%	4%
	1024	Zero Packet Loss	Zero Packet Loss	Zero Packet Loss	1%	2%
	2048	Zero Packet Loss	Zero Packet Loss	Zero Packet Loss	2%	3%
Suricata	512	Zero Packet Loss	2%	5%	28%	29%
	1024	Zero Packet Loss	Zero Packet Loss	Zero Packet Loss	16%	18%
	2048	Zero Packet Loss	Zero Packet Loss	Zero Packet Loss	17%	19%

6.2. User datagram protocol

Both Snort and Suricata have produced relatively same results like in TCP. When the packet size is 512 and Speed is 200Mbps and 400Mbps, Snort has produced zero packet loss. When we increased the speed to 600Mbps, Snort has dropped 30% packets. Snort has dropped 42% packets when the speed is increased to 800Mbps. The results have been shown in Table 2.

Table 2: Packet Loss Recorded with A Packet Size of 512 and 1024, Under UDP Protocol

IDS Tool	Packet Size	Internet Speed 200 Mbps	400 Mbps	600 Mbps	800 Mbps	1Gbps
Snort	512	Null	Null	30%	42%	43%
	1024	Null	Null	Null	30%	29%
	2048	Null	Null	Null	27%	28%
Suricata	512	1%	3%	21%	38%	38%
	1024	Null	Null	Null	8%	9%
	2048	Null	Null	Null	9%	10%

7. Conclusion

In the proposed survey analysis, mainly network packet loss has been identified. We have been observed the reciprocal relationship between packet size and packet loss. When there is an increment in packet size, the decrement of packet loss has been observed and vice versa. In this study, the rate of packet loss with variable internet speed is shown.

References

[1] Fossl, M. (2011). *Symantec Internet security threat ReportTrends for 2010.*Symantec Corp.
[2] DOROTHY E. DENNING, an Intrusion-Detection Model, IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. SE-13, NO. 2, FEBRUARY 1987, 222-232.
[3] Suricata Vs Snort (2012), "Suricata-vs-snort", [Online] Available: http:// www.aldeid.com /wiki/Suricata-vs-snort.
[4] K. Scarfone, P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)". Computer Security Resource Center (National Institute of Standards and Technology). February 2007.
[5] A. Chittur, "Model Generation for an Intrusion Detection System Using Genetic Algorithms".January 2005.
[6] David J.Day, Benjamin M.Burns. (2011),"A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines" The Fifth International Conference on Digital Society, 2011, pp.1-4.
[7] Qing-Xiu Wu.,"The Network Protocol Analysis Technique in Snort", International Conference on Solid State Devices and Materials Science, 2012, pp.1-4. https://doi.org/10.1016/j.phpro.2012.03.224.
[8] Adeeb Alhomoud, Rashid Munir, Jules Pagna Disso, Irfan Awan, Al-Dhelaan, 2011,"Performance Evaluation Study of Intrusion Detection Systems", The 2nd International Conference on Ambiems, Networks, and Technologies, 2011. Pp.1-4.
[9] Snort (2011). "Snort", [Online] Available: http://www.snort. org.
[10] Snort Software (2012),"Snort (software)", [Online] Available: en.wikipedia.org/wiki/Snort_ (software).
[11] Richard Bejtlich, "The Tao of Network Security Monitoring", Addison-Wesley, 2004.
[12] Packet Loss (2011), "Packet loss", [Online] Available: HTTP:// www.nessoft.com/kb/42.
[13] Suricata ids. URL: http://www.openinfosecfoundation.org, 2011.