Intrusion Detection System: A Review

Vikrant H. Modi
Department of Electronics
And Communication
L.J Institute of Engineering
And Technology,

Ami A. Patel
Department of Electronics
And Communication
L.J Institute of Engineering
And Engineering,

***Abstract*-In 21st century, because of easily available internet, virtually anybody can access it and access any network. To avoid any unauthorized access network security is one of the most important requirements in a system. Over the last years, many software solutions have been developed to enhance Network Security and this paper provides one such solution which has become prominent in the last decade: Intrusion Detection System (IDS). In this paper we have provide an overview of different types of Intrusion Detection Systems, the advantages and disadvantages of the same. Finally, the details of examples of Intrusion Detection System proposed by other authors have been elaborated. The examples are as follows. (1) Usefulness of DARPA Dataset for Intrusion Detection System Evaluation. (2) Performance Enhancement of Intrusion Detection System using Advance Sensor Fusion. (3) Analysis And Evaluation of Network Intrusion Detection Methods to Uncover Data Theft.**

***Index* Terms- Anomaly IDS, DARPA Dataset, Misuse IDS, False Positive, False Negative, SNORT**

I.INTRODUCTION

INTERNET is a global public network [1]. Internet has changed the face of communication and computation. The connectivity it provides allows corporations to extend their activity and increase productivity [2]. Because of ease of accessibility of internet introduced a new kind of criminality: cyber-crime [4]. This type of crime developed exponentially during the past decade, mainly due to the democratization of the Internet [5]. It is reported in [6] that, during the period of 1991-1996, information theft rose by 250 % and 99 % of all major companies reported one incident of major security breach and 10 billion dollars were lost in the US due to telecom and computer related frauds. Data is the most important asset in an organization [7]. This highlights the crucial need for network security in order to keep data secure. Hackers and intruders have made many successful attempts to bring down high-profile company networks and web services. Computer network security is often deployed in two ways. The first security application tries to establish a strong outside barrier in order to prevent unauthorized users gaining access to a network. Since internal users still need to access resources outside the local network, this barrier has to let some communications go through. Intruders usually take advantage of these characteristics to carry out exploits. In order to address this security issue, the second type of exploits. Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of firewalls, encryption, and virtual private networks. Firewall can be found in most of all corporate networks and form the first barrier against intrusion. Without good configuration, firewalls are useless. Unfortunately, as well as being very popular they are also often miss-configured, allowing any traffic by default rather than denying all of it [3]. That is the main disadvantages of firewall. In compare to firewall Intrusion Detection System (IDS0 is renowned and widely-deployed security tool to detect attacks and malicious activities in information system. It is generally deployed as a second line of defense along vulnerability monitor, access control and authentication that protects information system [8]. It searches for security violation incidents, recognizes unauthorized accesses, identifies information leakages and intervention of malicious programs Intrusion Detection provides a way to identify, and thus allow responses to, attacks against these systems. As a result, certain preventive mechanisms (e.g., firewalls, access control, and authentication) may not be as effective as expected. IDS play a role as a reactive agent rather than a proactive agent [6] in the security landscape of the system, whose primary job is to inform the system administrator in the event of an intrusion.

TAXONOMY

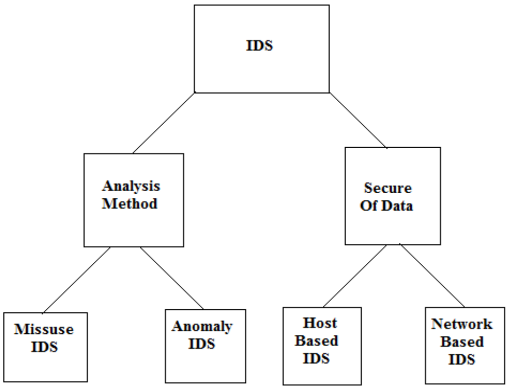

Figure1. Taxonomy of IDS

Intrusion detection system can be broadly classified based on two parameters as shown in figure1:

(a) Analysis method used to identify intrusion, which is classified into Misuse IDS and Anomaly IDS.

(b) Source of data that is used in the analysis method, which is classified into Host based IDS Network based IDS.

A. MISUSE (SIGNATURE-BASED) IDS

The misuse (signature-based) detection is normally used for detecting known attacks. It requires that all known threats will be defined first, and the information regarding these threats to be submitted to the IDS. Thus, the IDS is able to then compare all incoming or outgoing activity against all known threats in its knowledge base and raise an alarm if any activity matches information in the knowledge base. The information stored in this knowledge base is usually known as signatures [9].The process for actually comparing a signature with an attack include simple string matching – which involves looking for unique key words in network traffic to identify attacks – to more complex approaches such as rule-based matching which defines the behavior of an attack as a signature [9]. Following are the advantages-disadvantages of misuse detection technique [10, 11]:

Advantages: (1) Misuse detectors are very efficient in detecting attacks without signaling false alarms (FA). (2) Misuse detectors can quickly detect specially designed intrusion tools and techniques. (3) Misuse detectors provide system administrators an easy to use tool to monitor their systems even if they are not security experts.

Disadvantages: (1) Misuse detectors can only detect attacks known beforehand. For this reason the systems must be updated with newly discovered attack signatures. (2) Misuse detectors are designed to detect attacks that have signatures introduced to the system only. When a well – known attack is changed slightly and a variant of that attack is obtained, the detector is unable to detect this variant of the same attack.

B. ANOMALY (BEHAVIOUR-BASED) IDS

Anomaly detectors detect behaviors on a computer or computer network that are not normal. According to this approach, behaviors deviating from behaviors assumed as “normal” are thought to be attacks and anomaly detectors compute the deviation in order to detect these attacks. Anomaly detectors construct profiles of users, servers and network connections using their normal behaviors. These profiles are produced using the data that is accepted as normal. After the profile construction, detectors monitor new event data, compare the new data with obtained profile and try to detect deviations [10, 11].

Anomaly detection technique learning what is considered normal behavior by the two main approaches: self-learning or programmed anomaly detection. In the self-learning approach, the anomaly detection system will begin to automatically monitor events, such as live network traffic, on the environment it has been implemented on and attempt to build information on what is considered normal behavior [9]. This is otherwise known as offline learning, and may involve feeding the system a network traffic data set which contains normal network traffic [12]. Following are the advantages-disadvantages of anomaly detection technique:

Advantages: (1) Anomaly-based IDSs, superior to signature-based ones, are able to detect attacks even when detailed information of the attack does not exist. (2) Anomaly-based detectors can be used to obtain signature information used by misuse-based IDS.

Disadvantages: (1) There is a higher rate of false alarms, which means a lower precision [13]. (2) It also needs periodic online retraining behavior profile. (3) Anomaly-base approach requires a large set of learning data that consist of system event log in order to construct normal behavior profile.

C. HOST-BASED Vs. NETWORK-BASED IDS

Intrusion Detection can be implemented either on the hosts that need to be protected or on a network device that can sniff the traffic for all the hosts on the network. Based on the implementation locations, there are two common types of IDS, viz., I) host-based IDS, and II) network-based IDS.

Host-based IDS (HIDS) examines information at the local host or operating system on which it is installed. It examines actual system calls and system log files.

Network-based IDS (NIDS) examines the actual network packets that are traveling across the network. It examines this traffic for known signs of instructive activity. Because NIDS is watching network traffic, any attack signatures detected may succeed or fail, It is usually difficult if not impossible for NIDS to access the success or failure or the actual attacks. It only indicates the presence of intrusive activity.

D. CLASSIFICATION OF ATTACKS

The classification of the various attacks found in the network traffic is explained in detail in the thesis work of Kendall [27] respect to DARPA intrusion detection evaluation dataset and is explained here in brief.

The attacks fall into five main classes namely, Probe, Denial of Service (DOS), Remote to Local (R2L), User to Remote (U2R) and the Data Attacks.

The Probe or san attacks automatically san a network of computers or a DNS server to find valid IP address (ipsweep, Isdomain, mscan), active ports (portsweep, mscan), host operating system types (queso, mscan) and known vulnerabilities (Satan).

The DoS attacks are designed to disrupt a host or network service. These include the Solaris operating system crash (Selfping), active termination of all TCP connections to a specific host (Tcpreset), corruption of ARP cache entries for a victim not in others' caches (Arppoison), crash the Microsoft Windows NT web server (Crashiis) and crash Windows NT (Dosnuke).

In R2l attacks, an attacker who does not have an account on a victim machine gains local access to the machine (guestdict), extracts files from the machine (ppmacro), modifies data in transit to the machine (framespoof).

In U2R attacks, a local user on machine is able to obtain privileges normally reserved for the UNIX super or Windows NT administrator. The data attack is to extra filter special files which the security policy specifies should remind on the victim hosts. These include secret attacks, where a user who is allowed to access the files extra filters the data (ntfsdos, sqlattack).

E. LATEST INTRUSION DETECTION SOFTWARES

Anomaly detection based intrusion detection systems are separated into many sub-categories in the literature including statistical methodologies [14-17], data mining [18, 19], artificial neural networks

[20], genetic algorithms [21] and immune systems [22]. Among these sub-categories, statistical methods are the most commonly used ones in order to detect intrusions by analyzing abnormal activities occurring in the network. Various Anomaly based ids software's are PHAD [23], NETAD [24], ALAD [25] etc. Various Misuse based IDS software's are BRO, Suricata, Cisco IDS, Snort [26] etc.

II. TESTING of INTRUSION DETECTION SYSTEM

The main challenge in IDSs deployment is assessing and comparing performances of their systems with other IDSs [30]. These evaluations are needed and driven by the fact that security systems have to prove what they are capable of detecting, and how well they operate compared to the each other, [3] mention detection rate and false alarm rate as the best suited Evaluation matrices of IDSs. The detection rate is total intrusions injected in the traffic. The false alarm rate is equivalent to the false-positive rate of the IDS. There are mainly four Alarm types.

TABLE1
ALARMS TYPES

Alarm Type	Definition
True-Positive	IDS rightfully flags an attack as such
False-Positive	IDS triggers an alarm although no attack is actually happening
False-Negative	Real attack that the IDS does not flag as intrusion
True-Negative	IDS does not flag legitimate events as attacks(most common situation)

Performance evaluation of IDS done by using either offline evaluation or online evaluation.

Offline evaluation consists of recreating datasets of network traffic including attacks without recreating the whole network topology.

The use of tcpdumps and replay tools allow such type of evaluation [31]. The most commonly used datasets were created by **D**efense **A**dvanced **R**esearch **P**rojects **A**gency (**DARPA**) / **M**assachusetts **I**nstitute of **T**echnology (**MIT**) **L**incoln Labs in 1998 and 1999, called 1998 DARPA set and 1999 DARPA set, and also sometimes called **I**ntrusion **D**etection **E**valuation (**IDEVAL**) datasets [28, 32].The DARPA sets are simulations of network traffic based on observation of real network traffic including common attacks, which aim at providing blind evaluation material for researchers [32]. These datasets were captured at the edge of a network, at the border routers.

The 1998 **DARPA** set includes 7 weeks of training data with labeled test data and 2 weeks of unlabelled test data [32]. During the first test competition, 8 IDSs were tested. The data set includes also over 300 instances of 38 attacks. The 1999 **DARPA** set presents over 5 billion connections over 5 weeks: 2 were attack-free and 3 weeks included attacks. Another data set was created in 1999, based on the 1998 **DARPA** set: the 1999 **K**nowledge **D**iscovery and **D**ata (**KDD**) Cup, created for a machine learning evaluation competition. The **DARPA** 1999 test data consisted of 190 instances of 57 attacks which included 37 Probes, 63 DoS attacks, 53 R2L attacks, 37 U2R/Data attacks.

The main advantages of the DARPA sets are that they allow fast identical trial runs for IDSs evaluation. The fact that the sets are free to use allows many researchers to carry out the same experiments and thus compare and thus compare IDSs between each other [31]. Many critical papers showed that these sets are flawed [3], the main shortcomings begin:

(1) Simple, limited network topology
(2) Low background traffic and linear attacks distribution
(3) Limited number of victim target systems
(4) Simulated traffic includes unlikely IP header attribute values.

After seeing the shortcomings of correct offline evaluation, there is a critical need for realistic traffic and attack generators, as well as data sets mixing both type of traffic in a realistic manner [34].

Current researchers focus their work on simulation test-beds and attacks generators [3]. Lincoln Labs' work aiming at creating an online test-bed resulted in the **L**incoln **A**daptable **R**eal-time **I**nformation **A**ssurance **T**est-bed (**LARIAT**) tool [35]. **LARIAT** is capable of generating realistic background user traffic and real network attacks.

It was created to overcome the issue inherent to the DARPA sets, in order to create a next generation of test-bed. The main two goals of **LARIAT** are supporting real-time evaluation and creating easily deployable and configurable test-bed [35]. It simulates an internal and external network: it is thus possible to evaluate IDSs 'plugged' in between both simulated networks. The main issue with **LARIAT** is that its use is limited to the US military and to "some academic organizations under special circumstances".

Two main advantages of a real-time, on-line evaluation are that intrusion detection systems are able to perform active rather than passive monitoring during the evaluation and they can take action in response to a particular attack or a possible detection. Theoretically, these systems could query hosts to determine status and use data sources not provided in corpora used for the off-line evaluations. Another advantages is that an intrusion detection system such as CPU and memory usage, and ease of installation and configuration.

The main disadvantage of the real-time evaluation is that in many cases only one intrusion detection system can be evaluated at a time and attacks and background traffic must be regenerated for each system evaluated. Therefore it is a very time-consuming process and is not well suited to training 9as opposed to testing) intrusion detection systems.

In contrast, the off-line evaluations are produced once and can be used by any number of systems at any time for evaluation or training. In the off-line evaluation, systems and tested using network traffic, audit logs, system logs, files system information, and other host information collected on test-bed network and distributed to evaluation participant. Systems process this data in batch mode and attempts identify attack action in the midst of normal activities.

The off-line approach was well suited for those research systems that participated in the 1999 evaluation, as support of active monitoring was not required for those systems. Eventually it will be necessary to support future research systems and existing commercial systems that perform dynamic querying of the network or host.

Although parts of these systems might be evaluated in the exiting offline style, real-time evaluation components will be required.

III.SNORT-BASED INTRUSION-DETECTION SYSTEM

Snort is free, extremely powerful and widely used by researchers. Snort is a free and open source network intrusion prevention system (NIPS) and network Intrusion Detection System (NIDS) created by Martin Roesch in 1998. Snort is now developed by Source fire, of which Roesch is the founder and CTO. In 2009, Snort entered Info World Open Source Hall of Fame as one of the "greatest [pieces of] open source software of all time" [35].

Snort is a Network Intrusion Detection System, which is used to detect malicious activity in the network traffic. It is a widely used NIDS and this motivated us to study its architecture and analyze the different components of an IDS. Snort can be configured to run in four different modes i.e., as packet sniffer, packet logger, Network-based Intrusion Detection System and Inline Mode (IPS).

Sniffer mode- In this mode Snort uses a packet capturing tool to sniff packets from the network traffic and display it on console. No logging is done in Sniffer mode.

Logger Mode- In this mode Snort will analyze the contents of a packet, compare them with set of pre-defined rules and generate alerts if a match is found (i.e., if a packet is found to be malicious).

Inline mode- This mode is known as Intrusion Prevention mode. In this mode Snort will take raw data from **IPTABLES** and check it against its rule set. If any alerts are generated then **IPTABLE** rules are updated accordingly to prevent that malicious activity from occurring.

A paper presented by Ciza Thomas [36] has analyzed the DARPA 1998 data set using Snort and has concluded that any sufficiently advanced IDS should be able to achieve good false positive detection performance on the DARPAIDS evaluation data set.

The major benefit of SNORT is that it can detect a large number of different attacks such as viruses, Denial of Services, malware etc.

The major drawback of Snort is that it uses only signature based technique to detect the intrusion but if anomaly behavior occur then it will not be possible for SNRT to detect that anomaly attack.

A. EXPERIMENTAL EVALUATION

The IDS Snort was evaluated with the DARPA 1999 data set [36] and the results are shown in table II. It can be noted in table II that some of the attacks for a certain attack type may get detected whereas some other attacks from the same attack type may not get detected. Hence some of the attack types appear in both rows of Table II.

TABLE II
ATTACKS DETECTED BY SNORT
FROM THE DARPA 1999 DATA SET

Attacks detected by Snort	Teardrop,Dosnuke,portseep,sshtroja,sechole,ftpwrite,ynga,phf,netcat,Iand.satan,no-setup,imap,nc-breakin,ncftp.guessftp,Tcpreset,sqlattack,ntinfoscan.neptune,httptunntl,udpstorm,ls,xclock,xsnoop,named,loadmodule,ppmacro
Attacks not detected by Snort	Ps,portsweep,crashils,sendmail,netcat,nfsdos,sshtrojan,ftpwrite,back,guesspop,xsnoop,pod,snmpget,eject,dict,guesstelnet,syslogd,guestftp,netbus,Crashiis,secret,smurf,httptunnel,loadmod,secret,ps,xtrem1,casesen,named,ffbconfig,arpposion,warez,apache2,fdformat,sqlattack

The Snort is designed as network IDS; extremely good at detecting distributed port scans and also fragmented attacks which hide malicious packets by fragmentation. The preprocessor of Snort is highly capable of defragmenting the packets. Matching the alert produced by Snort with the packets in the data set by means of timestamp might those signatures.

In a study made by Sommers et al. [37], after comparing the two IDSs Snort and Bro, they comment that Snort's drop rates seem to degrade less intensely with volume for the DARPA data set. They have also concluded in paper that Snort's signature set has been tuned to detect DARPA attacks. Even then, if we cannot detect all the attacks of this nine year old data set, it clearly shows the inability of reproducing the signatures of all available attacks in the data set of signature-based Ids. This shows the inability of the IDSs rather than the deficiency of the data set.

B. ATTACK CLASSIFICATION IN SNORT

In the most widely used open source network intrusion prevention and detection system, namely the Snort, attack classification is based on its impact on the computer system. The attacks whose effect is the most critical have the highest priority. The priority levels are divided into high, medium and low ones. High level priority attacks are such as the attempted administrator privilege gain, the network "Trojan", or the web application attack. Medium priority attacks are the Denial of Service (DoS) attacks, a nonstandard protocol or event, potentially band traffic, attempted log-in using a suspicious user etc. Low-level priority attacks are the ICMP event, the network scan, the generic protocol command etc. [38].

IV. CONCLUSION

For Misuse Detection techniques (Signature Detection) mostly use SNORT IDS, will more accurately detect and generate correct alarm for the signature based attacks.

At the same time for Anomaly Detection technique Anomaly detection based IDS will detect accurately and generate correct alarms for novel attacks.

V. REFERENCES

[1]. "Intrusion Detection Systems, Definition, Need and Challenges", SANS Institute, 2008.

[2]. Sriram Sundar Rajan, "An overview of Intrusion Detection Systems", Ph.D. Dissertation.

[3]. Julien Corsini, "Analysis and Evaluation of Network Intrusion Detection Methods to Uncover Data Theft." Ph. D. Dissertation, 2009.

[4]. N. I. of Standards & Technology," An Introduction to Computer Security": The NIST Handbook, NIST, Ed. U.S. Department of Commerce,2006

[5]. J. Grossklags, N. Christin, and J. Chuang. "Security and insurance management in networks with heterogeneous agents", in 9th

ACM conference on Electronic Commerce, New York, NY, USA: ACM, 2008, pp 169-169.

[6]. Aurobindo Sundaram, "An Introduction to Intrusion Detection", Crossroads, Volume 2, Issue 4 Pages: 3-7, 1996.

[7]. K. Labib, "Computer Security and Intrusion Detection", Crossroads, volume 11, Issue 1, pp. 2-2, 2004.

[8]. Kanubhai K. Patel, "An Architecture of Hybrid Intrusion Detection System", Volume 2, No. 2, pp. 197-202

[9]. Axelsson, S. (2000). "Intrusion-detection systems: A taxonomy and survey". Tech. Rep. 99-15, Department Of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 2000.

[10]. Base R. "Intrusion Detection Technology", Indianapolis, USA, Macmillan Technical Publishing, 2000.

[11]. Mukherjee B, Heberlin LT, Levitt KN. "Network Intrusion Detection" IEEE Network 1994, 8(3):26-41.

[12]. Gong F. (2003). "Deciphering Detection Techniques", Part II Anomaly Based Intrusion Detection [White Paper], McAfee Security, McAfee Security White Paper, 2003, Retrieved October 10, 2012, from https://securemacafee.com/japan/products/pdf/Deciphering_Detection_Techniques-Anomaly-Based_Detection_WP_en.pdf

[13]. Stillerman M. Morceau, and Stillman M. (1999) "Intrusion Detection for Distributed Applications", Communications of the ACM, 42(7), July, 1999, 62-69.

[14]. Denning DE. "An Intrusion-Detection Model". IEEE Trans Software Eng. 1997;13(2):222-32

[15]. Javitz HS, Vanldes A. "The SRI IDSE statistical Anomaly Detector", In IEEE symposium on security and privacy, Oakland, CA, May 1991, pp. 361-26

[16]. Neuman PG, Porras Pa. "Experience with EMERALD to date". In first USENIX workshop on intrusion detection and network monitoring, Santa Clara. CA; 11-15 April 1999.pp. 73-80

[17]. Lankewicz L., Bernard M."Real time Anomaly Detection Using A Nonparametric Pattern Recognition Approach". In proceeding of the seventh annual computer security applications conference, San Antonio TX; 8-6 December 1991,pp.80-9

[18]. Noel S, Wijesekera D, Youman C. "Modern Intrusion Detection, Data Mining and Degrees of Attack Guilt" In Applications of data mining in computer security. Kluwer Academic Publisher, 2002.

[19]. Lee W. Stolfo S. "Data Mining Approaches for Intrusion Detection". In proceeding of the

seventh USENIX security symposium (Security 1998), San Antonio, TX; 26-29 January 1998.

[20]. Debar H., Becker M., Siboni D. "A Neural Network Component For An Intrusion Detection System". In proceedings of the 1992 IEEE symposium on security and privacy, Oakland, CA; 4-6 May 1992, pp.240-50

[21]. Ludovic M. GASSATA; "A Genetic Algorithm as an Alternative Tool for Security Audit Trails Analysis". In First International Workshop on the recent advanced in intrusion detection, Louvain-la-Neuve, Belgium; 14-16 September 1998.

[22]. Kim J, Bentley P."The Artificial Immune Model for Network Intrusion Detection". In Seventh European Congress On Intelligent Techniques and Soft Computing (EUFIT'99), Aachen, Germany, 13-19 September 1999

[23]. Machoney MV, Chan PK, "PHAD: Packet Header Anomaly Detection For Identifying Hostile Network Traffic" Florida Institute of Technology, Technical report, CS-20001-04

[24]. Machoney MV, "Network Traffic Anomaly Detection Based On Packet Bytes". In Proceeding of ACM-SAC, 2003.

[25]. Machoney MV, Chan PK, "Learning Non stationary Models of Normal Network Traffic for Detecting Novel Attacks". Proceedings of eighth International Conference on Knowledge discovery and data mining, 2000, pp. 376-85.

[26]. Rosech M. "Snort-Lightweight Intrusion Detection For Networks". In Proceeding Of The 13th LISA Conference of USENIX association; 1990.

[27]. K. Kendall."A Database of Computer Attacks For The Evaluation Of Intrusion Detection System", Thesis, MIT, 1999.

[28]. M.L Laboratory, " DARPA Intrusion Detection Datasets", 1999 [Online], Available: http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/1999data.html

[29]. Snort Manual, www.snort.org/does/snortmannual. 260

[30]. H. Bidgoli, Handbook of Information Security, Ed. Wiely, 2005.

[31]. D. J. Fried, I. Graf, W. Haines, K. R Kenall, D Mcclung, D. Weber, S. E. Webwe, D Wyschogrod, R. K. Cunningham and M. A Zissman, " Evaluation Of Intrusion Detection System: The 1998 DARPA Offline Intrusion Detection Evaluation", In proceedings of the 2000 DARPA Information Survivability Conference and Exposition, 2000, pp. 12-26

[32]. M. V. Machoney and P. K. Chan, " An analysis of the 1999

DARPA data for Network Anomaly Detection", In proceedings of Sixth International Symposium On Recent Advances in Intrusion Detection. Springer-Verlag, 2003.pp 220-237.

[33]. A. Patecha and J.M Park, "An overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends", Computer Networks, volume. 51, pp. 3448-3470

[34]. R. Braden, "Requirements of Internet Hosts-Communication Layers", United States, 1989.

[35]. P. Fogla and W. Lee, "Evading Network Anomaly Detection System Formal Reasoning and Practical Techniques", in CC'06. In proceeding of the 13th ACM conference on Computer and Communication Security, New York, USA: ACM, 2006.

[36]. Ciza Thomas, Vishwas Sharma, N. Balakrishnan, "Usefulness DARPA Dataset for Intrusion Detection Evaluation", International symposium and security, proceeding of SPIE, 6973, 15, 2008.

[37]. J. Sommers, V. Yegneswaram, P. Barford, "Toward Comprehensive transfer generation for Online IDS Evaluation", Technical Report, University of Wisconsin.

[38]. A. Baker. J. B. Beale, " Snort 2.1 Intrusion Detection (Second Edition)", pp.751, 2004.