A COMPREHENSIVE STUDY ON CLASSIFICATION OF PASSIVE INTRUSION AND EXTRUSION DETECTION SYSTEM

[1]Mrs. J.Lekha and [2]Dr.G.Padmavathi

[1]Research Scholar, Department of Computer Science,
Avinashilingam Institute of Home Science and Higher Education for Women,
&
Assistant Professor, Department of Computer Science,
Sri Krishna Arts and Science College,
Coimbatore, Tamil Nadu, India
saran.lekha@gmail.com
[2]Professor and Head, Department of Computer Science
Avinashilingam Institute of Home Science and Higher Education for Women,
Coimbatore, Tamil Nadu, India
ganapathi.padmavathi@gmail.com

ABSTRACT

Cyber criminals compromise Integrity, Availability and Confidentiality of network resources in cyber space and cause remote class intrusions such as U2R, R2L, DoS and probe/scan system attacks .To handle these intrusions, Cyber Security uses three audit and monitoring systems namely Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS). Intrusion Detection System (IDS) monitors only inbound traffic which is insufficient to prevent botnet systems. A system to monitor outbound traffic is named as Extrusion Detection System (EDS). Therefore a hybrid system should be designed to handle both inbound and outbound traffic.

Due to the increased false alarms preventive systems do not suite to an organizational network. The goal of this paper is to devise a taxonomy for cyber security and study the existing methods of Intrusion and Extrusion Detection systems based on three primary characteristics. The metrics used to evaluate IDS and EDS are also presented.

KEYWORDS

Cyber space, Cyber Security, Remote class attacks, Intrusion Detection Systems (IDS), Extrusion Detection Systems (EDS), Inbound traffic, Outbound traffic.

1. INTRODUCTION

Today most of the security organizations such as Home Land security called Federal Protective Service (FPI) and USGAO (Government Accountability Office) poorly seek for Audit monitoring and Information Control Systems for cyber security. Intrusions are attempts to bypass security

David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA - 2013
pp. 281–292, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3529

mechanisms of a computer network. Intrusions can be caused by persons or events who are intelligent in breaking into the system and misuse network resources. According to National Vulnerability Database a minimum of 4900 [17] new software vulnerabilities have been identified from 2005 to 2011. These attacks may inject some malware (virus, worm, Trojan horse) and result in Denial of Service (DoS), Distributed Denial of Service (DDoS) and botnet systems. Cyber Security aims at preventing and identifying misuse and malfunction of digital resources by ensuring Data Security, System Integrity and Network Security. Cyber security tools and techniques are classified and shown in Fig 1.Intrusion Detection is the process of monitoring events occurring in a computer system or network and analyzes them to find signs of intrusions. Some traditional security services such as firewalls act as first line of defense to filter the incoming attacks and stop the outsider attacks. They do not find the root cause of an attack. They can be bypassed by tunneling mechanisms. However most of the security breaches arise from insiders IDS and EDS are demanded as second line of defence to monitor both outsider and insider intrusions that bypass firewalls. They are the prominent methods of protecting individual applications, single host and other hosts on the network. These systems have become essential tools in many risk based network applications such as Business networks, Military networks, Stock trading, Medicine, Weather forecasting, Health monitoring, Banks, Biology Education, Research, Chemical and Hazardous areas, Interface Control systems and Web applications.

IDS may be a hardware or software that monitors and analyses events entering a computer system or network in order to detect and alert the administrator for signs of security violations based on some existing data. The data may be historical information about intrusions (knowledge based or Misuse based), information about current working configuration of the system (behaviour based or Anomaly based). The limitation of Intrusion Detection System is that, it does not indicate the consequence of an intrusion. Since none of the intrusions are distinct (i.e each new attack is a sequence of the older ones. Eg. The prerequisite for [5] launching a DDoS attack is to install a DDoS daemon tool on the system to be attacked), detection systems are insufficient to protect a computer network. Similarly the consequence of an attack may be a compromised system within the monitored environment to outsource attacks to other systems, which demanded EDS.

In many cases, when an internal system on the network is compromised, it becomes a bot and can inject malware to other system on the network. When a malware propagates in to an infected bot system, it can be controlled by another system called C&C server. C&C server exists at attackers place and forms a network with bot systems called bot network or botnet. This problem of phishing occurs in many organizations's Internet or Intranet. Extrusion Detection Systems (EDS) is a system which monitors outgoing [12] traffic sent by infected system (botnet system) on the monitored network. The outgoing traffic may be an attack response traffic (send error message), malware (download confidential information from locally connected systems), Propagation traffic (propagate virus/worm) and Commanded traffic (send spam, scan financial information such as credit card status). Traditional Intrusion Detection Systems cannot trace the cause after an attack. EDS helps government agencies and organizations to monitor outgoing traffic leaving their organization. Not much work has been done on assuring security to track data sent out of a system or a network. An extrusion detection system can perform two tasks: i) they can monitor attacks outgoing within the network and ii) attacks that penetrate outside the network.

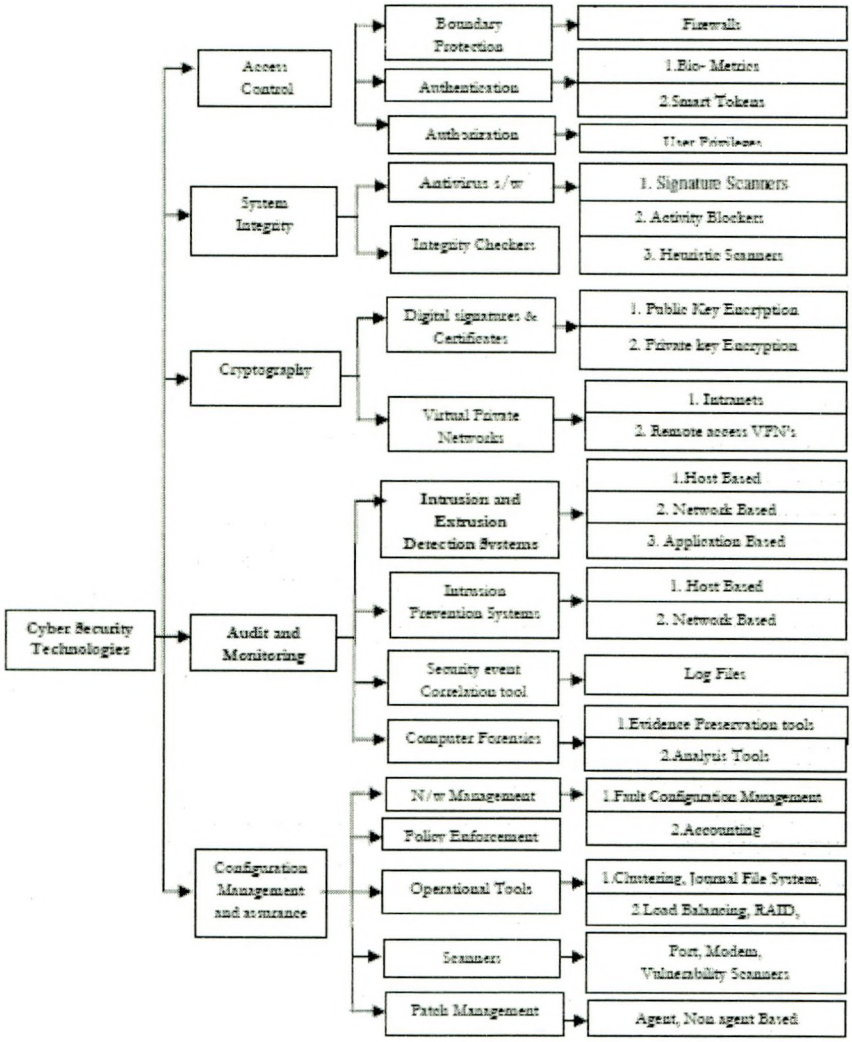

Fig. 1. Tools and Techniques for Cyber Security

EDS can be combined with anomaly and misuse detection systems. To deal with fraud detection, extrusion detection system may be combined with anomaly based systems. To prevent botnet systems on the network, extrusion detection system may be combined with misuse detection systems. Therefore IDS and EDS are required to analyze the prerequisite [16] and the consequence of attacks.The objective of this paper is i) to present a detailed insight into various methods of classifying Intrusion and Extrusion Detection Systems based on three primary characteristics ii) present a detailed study on knowledge based IDS and EDS iii) study the evaluation metrics used to measure the performance of IDS and EDS.

This paper is organized as follows: Section 2 presents a survey on existing methods of Intrusion and Extrusion detection systems for cyber security. Section 3 provides various characteristics based on which Intrusion and Extrusion Detection System can be classified and a new taxonomy

of IDS and EDS is framed. Section 4 presents various evaluation metrics and methods that can be used for measuring the performance of knowledge based intrusion detection systems. Finally in section 5 the aspiration of this review is concluded.

2. STATE OF THE ART : IDS and EDS

This section gives the evolution of Intrusion and Extrusion Detection systems from its year of inception. The first intrusion detection system was designed by James Anderson in the year 1980. In his seminal paper "Computer Security Threat Monitoring and Surveillance", he had mentioned that that system's audit trials can be used to track system misuse or users behavior. He laid the beginning for host based intrusion detection system. In 1984 SRI International's Dorothy Denning analyzed the authentication information of ARPANET users in Navy and designed a model for intrusion detection and expert systems [IDES] and published it as paper named "An Intrusion Detection Model". In 1988, Davis of Lawrence Berkely's Lab designed an IDS called "SRI Haystack" that used known patterns to trace user's audit trials in US Army. This was the first commercial product in the market. In the same year, Multics Intrusion Detection and alerting System was developed by Denning and Neumann. In 1990 Todd Heberlein developed the first Network Intrusion Detection System (NIDS) called Network Security Monitor (NSM) which analyzed network traffic in distributed environment and published it as a paper entitled "A Network Security Monitor". Air force cryptology support centre developed Automatic Security Measurement system (ASIM) to monitor traffic on their network which is still used all over the world. Haystack Labs in 1991 proposed a Network Anomaly Detection and Intrusion Reporter (NADIR) that used statistical methods using normal profiles for intrusion detection. In 1994 Mark Gosbie developed IDS based on autonomous agents in distributed environment. In 1996 Staniford Chen developed GrIDS, a graph based IDS which plotted the user activity on a computer and network of computers as an activity graph and showed reports on policy violations. In 1998, a rule based packet analysis intrusion detection system [PAIDS] was developed and named Bro by Lawrence Berkely National Laboratory. In 1998's an open source intrusion detection system called Snort was developed by Martin Roesch which performs traffic analysis, packet logging and intrusion detection using a predefined rule set. After that many commercial IDS products were released.Extrusion Detection Systems (EDS) came into focus of researchers from 2006 onwards. In 2007, Guofei Gu developed an application to correlate both inbound and outbound traffic. In 2007, Sunny Behal developed a system named N-EDPS for preventing botnet attacks. In 2011, Robert Koch in his study had stated Network based Extrusion Detection systems as one of the powerful systems for insider attacks. Ankita Tuteja and Ravi Shanker in 2012 published their research work that optimizes signature based intrusion detection system Snort to monitor outbound traffic.

3. CLASSIFICATION OF IDS AND EDS

Intrusion and Extrusion detection systems can be classified as shown in Fig 2. The following are the primary characteristics [1] discussed:

- Source of Data
- Detection Approach and
- Response Type.

3.1 Source of Data

Based on the data source, IDS and EDS may be classified as Host Based, Network Based and Application Based.

3.1.1 Host Based.

In Host Based Intrusion and Extrusion Detection Systems (HIDS), IDS and EDS need to be placed on the system they have to monitor. The system may be a server system, workstation, external network devices such as printers, routers and gateways, mainframes, firewall or an enterprise network. They investigate activities

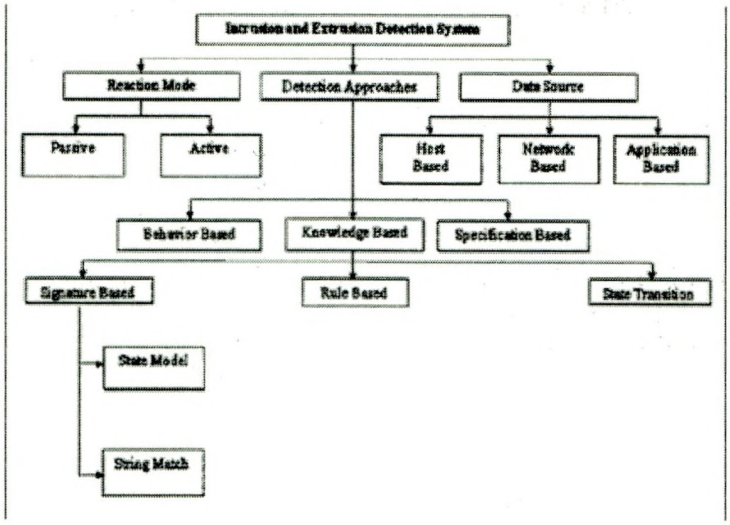

Fig. 2. Taxonomy of Intrusion nd Extrusion Detection System

recorded in audit log such as (System activities, User activities) related to operating system. The system activities may be file system [2] attributes such as accesspermissions, i-node, share links, user-id, and group-id, file size, modification time stamp, accesstime stamp. User activities may be activities such as login logout time, changes in user identity, authentication status, failed attempts to restricted information, keystroke features etc.

Advantage:. The advantage of Host based intrusion and extrusion detection is that they can record success or failure of attack that helps in forensic analysis; they are much focussed on the deployed system, not limited to bandwidth or encrypted and compressed messages. They do not require NIC to be in promicious mode because it does not monitor all the packets crossing the network, it only monitors only traffic incoming to the host. Since they monitor traffic intended to a single host they are good at monitoring interactions to application layer and can effectively handle application layer attacks such as memory modifications, malicious application request, buffer overflow and file modification.

Limitations:. The limitations are that they are operating system dependent and can crash the operating system after an intrusion. Expensive to deploy one agent per host in environment with large systems and when they sniff the network traffic incoming to it they work only in application layer and cannot monitor outgoing traffic. It is difficult to correlate results from multiple hosts.

3.1.2 Network Based.

The NIDS/NEDS collect, filter and analyze traffic passing at selected points of a single network or interconnected network. NIDS and NEDS require the following components:

- Sensors to monitor network traffic
- Management server for functionality
- Management console for result display.

The sensors can act in any one of the two modes: inline and passive. An inline sensor requires to be integrated with network hardware like firewall or switch. All the traffic passes only through the inline sensors which enable them to block the attack. A passive sensor only monitors the traffic passing through the Network Interface Card by a simple physical tap. NIC is said to be in promicious mode. They reside on Network Interface Card [3] of connected hosts in two modes:

- Non promicious mode and
- Promicious mode.

In non promicious mode, the NIC captures the packets on the network that contains a specific MAC address. However in promiscuous mode, NIC captures all the packets that interface with it and stores in libpcap library. They investigate SNMP (Simple Network Management Protocol), network packet header and payload information such as source address, destination address, packet size, protocol used, flag bits and packet content. NIDS and NEDS can be placed at many junctions: Between Internet and external firewall, external firewall and internal firewall, local server and internal firewall, workstation and internal firewall and in combination with switches and routers.

Advantages:. The advantage is that it assures real time detection, cost effective, difficult for the attacker to hide evidences does not depend on operating system, damage of intrusion is decreased and since it works at network layer they can analyze both incoming and outgoing traffic. They can work within defense in depth strategy. The network intrusion and extrusion detection system analyses traffic on network, transport and application layers to detect some remote class intrusions such as U2R, R2L, probe/scan and DoS as listed the table 1.

Limitations:. In high traffic, they can potentially miss packets leading to insertion and evasion attacks and cannot work with encrypted and compressed data. They do not record success or failure of an attack. They just indicate that an attack has happened.

3.1.3 Application Based.

This type of IDS and EDS monitor specific software or application by investigating applications transaction log file traces which gives the possible set of execution paths of an application.

Advantage: . It can record the user interface with the application and alert [11] the administrator when the user performs some unauthorized access of application's resources. It can also work in encrypted environments.

Table 1. Classification of Network Based Attacks

Attack Name	Attack Classification	Attack Name	Attack Classification
udpstorm	DoS	guess_passwd	R2L
smurf		phf	
pod		snmpguess	
land		named	
processtable		imap	
warezmaster		snmpgetattack	
apache2		xlock	
mailbomb		sendmail	
neptune		xsnoop	
icmp flood		worm	
sync flood		arp positioning	
ping flood		dns spoofing	
ping of death		dhcp spoofing	
tear drop		icmp redirection	
low rate dos		irdp spoofing	
nuke		Route mangling	
Send mail flood		Trojan Horse	
flooding		Remote OS fingerprinting	
Portsweep	Probe / Scan	Buffer_overflow	U2L
mscan		rootkit	
Saint		Perl	
satan		ps	
Ipsweep		Load_module	
Nmap		Sqlattack	
Icmp scan, udp scan tcp stealth scan		Ping of death	

Limitations: . It can be easily evaded and cannot detect tampering attacks (e.g Trojan Horse). Powerful when combined with host based or network based IDS.

3.1.4 Hybrid:.

This type of IDS and EDS combines both host and network based IDS with Application based IDS.

3.2 Detection Approach

Detection approaches process the data and analyze whether an intrusion has happened or not. They categorize the intrusions as successful attempts and failed attempts. The primary class IDS based on detection approaches are:

- Knowledge Based/Top Down/Misuse Based Approach
- Behavior Based/Bottom Up/Anomaly Based Approach
- Specification Based Approach

3.2.1 Knowledge Based/Top Down/Misuse Based Approach.

The knowledge based approach process the incoming packets and matches it with database [4] of known attack patterns. It is called as top down approach because it uses prestored pattern to detect incoming attacks. It is also called misuse based approach since the attacks are detected based on known misuses.The knowledge based [1] approach can be primarily classified as Signature Based, Rule Based, State transition based depending on the method of representing and relating attack signatures. The system is called signature based if it records the current signature and compares it with the database containing predefined attacks in the form of patterns using string matching algorithms or state models. The accuracy of the signature based IDS is measured [6] by the number of false negative alerts it generates. The rule based methods store attack as predefined rules (if then construct) to compare it with the incoming facts. The rules may be written in any rule based programming. An inference engine is used to compare the pre-programmed rules with the facts. Rule based expert systems are capable of automatically generating rules for new attack scenarios with the knowledge of artificial intelligence. The State transition based systems represent attacks in the form of states transition diagrams using an automaton (DFA/NFA). All the packets need to pass through these automata and the transition results in sequel state if there is no such attack in the packet. The advantage of knowledge based method is its accuracy to detect the attacks and its ability to name and categorize the type of attacks. The disadvantage is that it cannot detect new upcoming attacks.EDS can have the same detection approaches [8] as IDS. Ankita Tuteja et al have [14] implemented EDS in Snort and have classified new types of attacks. Behal, S et al in his work [15] developed an EDS which detects four different types of malware in the system.

3.2.2 Behaviour / Bottom up / Anomaly Based Approach.

Behaviour based approach processes the incoming data and compares it with profiles that represent normal behaviour of users, hosts, or networks, and detects attacks if there are significant deviations from this profile. It is called bottom up approach because it uses normal profiles to detect attacks. Moreover, it is called anomaly based because it alerts the administrator for an abnormal (anomalous) behavior. Anomaly based IDS can [1] be categorized as Statistical, Distance, Profile, Model and Rule Based systems. The advantage is its ability to detect new attacks. The disadvantages are: High false-alarm and limited by training data, Cannot name the

attacks, Can be fooled by attackers for normal behavior, Difficult to set boundary between normal and anomaly behavior, Can be trained to accept anomaly also. Due to this problem, it cannot be used in network or digital forensic analysis.

3.2.3 Specification Based Approach

This type of IDS and EDS store the universal specification about predetermined protocol behaviors or states. It is also called as Stateful protocol because it works by recording protocol behavior and compares each request with response thereby identifying unexpected sequence of commands and keeping track of authentication for each session. It makes the IDS to understand Network, Transport and Application layer protocol behaviors. The main advantage is that it is helpful in investigating an incident for network forensics. The drawbacks are: it is resource initiative since the IDS need to understand the protocol behavior and time initiative to update versions of universal protocols in the IDS database.

3.3 Response Type

The response or reaction of IDS and EDS can be classified as Passive and Reactive. A Passive IDS and EDS detects an attack and logs it into audit records and sends an alert to administrator's console. It does not handle any measures to stop or prevent attack sequences. Alert can be used in situations where real time notification is required. Eg: e-mail, messaging, bulgar alarm. Log may be used to store the sequence as text in windows registry, pcap lib, Oracle / SQL database unified and CSV. A Reactive IDS detects logs and stops or limits the source of attack similar to an application layer firewall. They are also called as Intrusion Prevention Systems (IPS).The different response types of IDS and EDS are listed in Table 2.

4. EVALUATING IDS AND EDS

The performance of IDS and EDS can be evaluated based on the following performance metrics

- Efficiency: It represents the percentage of runtime, resource consumption and storage consumption.
- Accuracy: It represents the percentage of true alarms by the system.
- Effectiveness: It represents the percentage of attacks identified by the system.
- Security: It represents the resilient capacity of the system in identifying attacks.
- Interoperability: It represents how the system interoperates with each other.
- Collaboration: It represents how the system collaborates with other security mechanisms.
- Using Benchmark Data set: Select a dataset which [9] contains traces of all remote class attack patterns. DARPA data set 1998/1999/2000, KDD Cup 1998 and LARIAT 2000 data sets.
- Using Synthetic traffic: Attack traces can be generated by using commercial tools such as Tcp replay which replays the traffic stored in Pcap and perform load testing in switches or routers.
- Using Evasion techniques: These are modifications [7] made to attacks to fool intrusion detection system from detecting it. Eg : Obfuscating attack payload by encoding it, fragmenting packets, overlapping signatures.

Table 2. Response Types of IDS And EDS

S.No	Response Type	Purpose
1	Alert	Generate an alert and log.
2	Log	Log the packet
3	Pass	Ignore the packet
4	Activate	Alert and activate another dynamic rule
5	Dynamic	Remain idle and get activated by an activate rule and log
6	Drop	Make IP tables drop the packet and log the packet.
7	Reject	Make IP tables drop the packet and log the packet, and send TCP reset if the protocol is TCP or ICMP unreachable message if the protocol is UDP.
8	Sdrop	Makes IP table drop the packet.

- Update Delay: The efficiency of IDS can also be measured using windows of vulnerability and windows of visibility. The former one is the time taken for a new attack to penetrate a system, where the latter is the [10] time taken for the IDS to update patches and alert the administrator.
- ROC Curve: ROC [13] stands for Receiver Operating Characteristics or Relative Operative Characteristics because it graphically plots two operating characteristics of IDS i.e True Positive and False Positive.
- Confusion Matrix: It is a two dimensional matrix representing classification of attack results. It maps the number of attacks misclassified as j instead of i. Table 3 shows the general confusion matrix for successful and failed attempts.

True Positive = No. of correct attacks classification / Total No. of attack traces

False Positive = No. of misclassified traces / Total No. Of attack traces

Table 3. Metrics for measuring IDS alerts

Standard Metrics	Prediction Connection Label	
	Failed Attempts	Successful Attempts
Actual Connection Label	False Positive (FP)	True Positive (TP)
	False Negative (FN)	
	True Negative (TN)	

True Negative IDS in idle state when there is attack

False Negative IDS failing to alarm for an actual attack.

True Positive IDS alarming for an actual attack.

False Positive IDS alarming for non suspicious events

Cost Matrix: Maps the cost of misclassifying an attack i into attack j. CPE (Cost Per Example) gives the summation of all misclassified attacks and total cost of misclassification as shown in Eq.1. Lower the CPE, better the classification

$$CPE = 1/N \sum_{i=1}^{N} \sum_{j=1}^{N} CM(i,j) * C(i,j) \quad (1)$$

N : No of observed nodes,
CM(i,j) : Confusion Matrix value of misclassified attacks,
C(i,j) : Cost of misclassification.

5. CONCLUSION

In this paper a comprehensive study on classification of Intrusion and Extrusion Detection system is presented because understanding the primary classification of IDS and EDS is necessary for the construction of new detection architecture. Types of IDS and EDS, its unit of measurement are discussed to identify the methods through which the performance of IDS and EDS can be increased. The future work aims at a study on detailed methodologies of signature based string matching methods and devising a new mechanism that overcomes the existing limitations of signature based network intrusion and extrusion detection systems.

REFERENCES

[1] Sabahi, F , Movaghar, A. " Intrusion Detection : A survey", Proceedings of Third International Conference on Systems and Networks Communications 2008 IEEE, pp:23-26.

[2] Yahui Yang; Chunfang Huang; Zhijing Qin, "A Network Misuse Detection Mechanism Based on Traffic Log", Proceedings of International Conference on Network Security, Wireless Communications Trusted Computing 2009 IEEE, pp: 526-529.

[3] Mohammed Abdul Qadeer, Mohammed Zahid, "Network Traffic Analysis and Intrusion Detection using Packet Sniffer" Proceedings of Second International Conference on Communication Software and Networks 2010 IEEE, pp:313-317.

[4] Yuebin Bai, Hidestune Kobayashi, "Intrusion Detection Systems: Technology and Development", Proceedings of the 17th International Conference on Advanced Networking and Applications (AINA ' 03) 2003 IEEE, pp: 710-715.

[5] Tillmann Werner, Christoph Fuchs, Elmar Gerhards-Padilla, Peter Martini "Nebula – Generating Syntactical Network Intrusion Signatures" Proceedings of 4th International Conference on Malicious and Unwanted Software 2009 IEEE, pp: 31-38.

[6] Moses Garuba, Chunmei Liu, and Duane Fraites, "Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems", Proceedings of Fifth International Conference on Information Technology: New Generations 2008 IEEE, pp:592-598.

[7] Tsung-Huan Cheng, Ying-Dar Lin, , Yuan-Cheng Lai, and Po-Ching Lin, "Evasion Techniques: Sneaking through Your Intrusion Detection / Prevention Systems", IEEE Communications Surveys & Tutorials 2011,pp:1-10.

[8] Yan Luo and Jeffrey J.P. Tsai, "A Framework for Extrusion Detection Using Machine Learning", Proceedings of 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC) 2008 IEEE, pp:83-88.

[9] Christian Kreibich, Jon Crowcroft "Honeycomb – Creating Intrusion Detection Signatures Using Honeypots" ACM SIGCOMM Computer Communications Review 2004, pp: 51-56.

[10] Yoon – Ho Choi, Moon-Young Jung and Seung- Woo "L+1 –MWM: A Fast Pattern Matching Algorithm for High-Speed Packet Filtering", Proceedings of 27th Conference on Computer Communications, 2008 IEEE, pp: 2288-2296.

[11] Richard Lippmann, Seth Webster, and Douglas Stetson "The Effect of Identifying Vulnerabilities and Patching Software on the Utility of Network Intrusion Detection" Proceedings of 5th International Symposium 2002 Springer, pp: 307-326.

[12] Rebecca Bace and Peter Mell, "NIST Special Publication on Intrusion Detection Systems", Publications of National Institute of Standards and Technology june 2011,pp:1-53

[13] Robert Koch, "Towards Next-Generation Intrusion Detection",Proceedings of 3rd International Conference on Cyber Conflict IEEE 2011, pp:1-18.

[14] Robert Koch, "Towards Next-Generation Intrusion Detection",Proceedings of 3rd International Conference on Cyber Conflict IEEE 2011, pp:1-18.

[15] Alicherry, M.; Muthuprasanna, M.; Kumar, V., "High Speed Pattern Matching for Network IDS/IPS", Proceedings of 14th International Conference on Network Protocols, IEEE 2006. pp: 187 - 196 .

[16] Koral Ilgun, Richard A. Kemmerer, , and Phillip A. Porras, "State Transition Analysis: A Rule-Based Intrusion Detection Approach", IEEE Transactions On Software Engineering, Vol. 21, No. 3, March 1995 , pp:1-19.

WEB REFERENCES

[17] http://nvd.nist.gov/home.cfm