Intrusion Detection Systems - Analysis and Containment of False Positives Alerts

G. Jacob Victor
Joint Director
IT &C Department, Govt. of AP, AP Secretariat, Hyderabad - 22,

Dr. M Sreenivasa Rao
School of Information Technology, JNTU, Hyderabad - 85, India.

Dr. V. CH. Venkaiah
CRRao AIMS & CS, UoH Campus, Hyderabad - 46,

ABSTRACT
The dependence on information technology became critical and IT infrastructure, critical data, intangible intellectual property are vulnerable to threats and attacks. Organizations install Intrusion Detection Systems (IDS) to alert suspicious traffic or activity. IDS generate a large number of alerts and most of them are false positive as the behavior construe for partial attack pattern or lack of environment knowledge. Monitoring and identifying risky alerts is a major concern to security administrator. The present work is to design an operational model for minimization of false positive alarms, including recurring alarms by security administrator. The architecture, design and performance of model in minimization of false positives in IDS are explored and the experimental results are presented with reference to lab environment.

Index Terms: **Vulnerability, Anomaly, Audit trail, True positives, False Positives**

1. INTRODUCTION
Computers & Communication became part of human life. The availability of low cost broadband, internet connectivity, mobile technologies increased the number of computers connected to the internet. The dependence on information technology became critical and important IT infrastructure, critical data and intangible intellectual property are vulnerable to threats and attacks.

To address Information security challenges, attain statutory compliance and to minimize the threats, security tools like Anti-viruses, Firewalls, Intrusion Detection / Prevention Systems etc are deployed. Andre Yee [15] states that "IDS have become a part of multilayered security architecture", as they detect a network or system is under attack. They don't fully guarantee security, but when used with security policy, vulnerability assessments, data encryption, user authentication, access control, and firewalls they can greatly enhance network safety.

Intrusion detection systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity. Intrusion detection systems use policies to define certain events, if detected will issue an alert or respond automatically to the event. Such a response might include logging off a user, disabling a user account and launching of scripts.

1.1 Classification of Intrusion Detection Systems (IDS)
Intrusion detection is the process of monitoring computers or networks for unauthorized access, activity, or data modification, so that action may be taken to prevent or repair the damage later.

Anderson [1] defined an intrusion attempt or a threat to be the potential possibility of a deliberate unauthorized attempt to (i) Access information (ii) Manipulate information, or (iii) Render a system unreliable or unusable.

There are two basic types of intrusion detection system: host-based and network-based. Each has a distinct approach for monitoring, securing data and systems. Host-based IDS's examine data on individual computers that serve as hosts, while network-based IDSs examine data exchanged between computers.

William Stallings [8] classified IDSs based on various parameters, Rule-based Detections and Statistical Anomaly Detection. Statistical anomaly detection systems are grouped into Profile based detections and threshold detection. Stefano Zanero [13] classified IDS based on concept of processing misuse detection or anomaly detection. IDS based on Anomaly detection create behavior model for the monitored infrastructure including its users. Any deviation from 'normal' behavior, beyond defined threshold, marks the action as suspicious. Alternately, a set of signatures stored in a knowledgebase will be used by misuse detection IDS to identify intrusion attempts.

Table 1: Comparison of IDSs

Misuse Based	Anomaly Based
require Continuous updates	No updates required
No initial training	training is required
Needs tuning as per environment	Tuning is a part of training itself
Cannot detect Novel attacks	Detect any novel attacks
Accurate alerts	Vague alerts
Very few false positives	Huge numbers of false positives
Raise a Number of non contextual alerts	Nil
Easy to design	difficult to design

Summary of differences between strengths and weaknesses of the two approaches is shown in Table 1.

1.1.1 Host, Network and stegano IDS
The classification is based on source of data to be analyzed by IDS, in Network Intrusion Detection System (NIDS) the audited data is collected from the network. In Host Intrusion Detection System (HIDS) the audited data is collected from the host itself. The NIDS are further grouped into two types first type is built-in signatures or Static, and the second type is state-full Dynamic signatures. The HIDS are two categories OS-specific and

application specific. Michael Sieffert [9] et. al. states that programs to hide steganographic content in common file types. Steganographic Intrusion Detection System shall be deployed to address stegano attacks. Daejoon Joo[10] et. al. states that neural networks can capture the relation-ships better to statistical models. In an environment, construction of rules is difficult; a neural network is best suit.

Joshua Shaul[11] says that NIDS will not assure complete protection as intrusions are also from internal source, targeted on DBMS. To address internal Intrusions on database servers, Database IDS system shall be attached to monitor relevant traffic only on that server. Database IDS will be built on specific knowledge of respective DBMS to sense potential attacks and flag.

IDS systems are expert systems based on rules, anomalies or specific signatures of an attack or it's variant. Signature will be prepared for every attack or its variants based on the behavior identified and analyzed. The malicious code will be recognized in IDS by Common Vulnerabilities and Exposures List (CVE ID) [3] or Nessus or BugTraq, ArachNIDS victim system IP address or by any other proprietary parameter or ID.

Denning (1986) presented "first IDS with six components such as Subjects, Objects, Audit records, Profiles, Anomaly records and Activity rules and published paper 'An Intrusion Detection Model' in 1986 IEEE Symposium on Security and Privacy". Steven J. Scott [4] proposed IDS/IPS based Threat Management System blend of Devices, aggregation, correlation, analysis and alarms. The security issues generally depend on traffic load, the size of network, security procedures implemented, etc. Neelakantan[20] stated that network intrusion detection systems must process lot of network data in a short time, these systems require a good deal of processing power, high random access memory (RAM) and large space to log information for any signature based intrusion detection systems. Simon Edwards [5] states that many deployments result in missed intrusions and network vulnerabilities. The environments which may be susceptible to missed intrusions are due to (i) Heavy traffic networks. (ii) Switched networks. (iii) Asymmetrical networks.

1.2 IDS Architecture

Based on the roles performed by IDS and its components, the relationship among machines, devices, applications, processes, conventions used for communication between them will define IDS architecture and categorized into three types (i) single-tiered (ii) multi-tiered, and (iii) peer-to-peer architectures (distributed IDS). Single-Tiered Architecture IDS is a single component, collects and processes data on its own. Multi-Tiered Architecture consists of three primary components 1.Sensors 2. Analyzers (Agents) and 3. Manager. Peer-to-Peer Architecture - there exists more than one pair of IDS components that exchange IDS and IDP information. The peer components perform the IDS functions.

The concept of IDS design is based on the viewpoint that attackers pattern of actions are unusual compared to a genuine client. This different behavior can be detectable. Peng Ning [2] (2005) stated Intrusion detection systems (IDSs) are a subset of preventive security mechanisms and deployed along with authentication, access control systems as a subsequent level of protection to IT Assets.

Most of IT systems and user applications were developed in their respective context without security awareness, there by susceptible to attacks. In the rest of cases, applications and systems were developed to operate in one set of parameters, deployed in the different setup resulting in vulnerability.

2. FALSE POSITIVES IN IDS

2.1 False positive

Intrusion is an activity that violates security policy. False positive is a classification of a legitimate action as anomalous action by IDS. The act of flagging a given behavior as illegal even when it is legitimate is defined as false positive. Stephen Northcutt [12] explains that most of the current IDS have very high rate of false positives as they cannot yet make wise decisions on whether the traffic coming across a given network is harmful or innocuous. A false positive is another way of saying 'mistake'. A false positive occurs when the IDS program mistakenly flags an innocent behavior.

2.2 False Negative

The act of not detecting an intrusion when the observed event is illegal is defined as false negatives. False negative can also be defined as an action of IDS system that does not detect actual anomaly/ misuse action and allows passing. Subject's normal behavior is the basis for the Anomaly detection, "any action that significantly deviates from the normal behavior is considered as intrusive". Therefore the normal behavior in IDS shall be defined explicitly. Stefano Zanero[13] proposed models for the evaluation of the IDS. More false positives are reported in anomaly detection systems while signature based systems report very low, but produce false negatives. J Snyder [14] states that "the target-based architectures will reduce false positives". False negatives also create a nuisance and issue of importance. Large number of new attacks will generate false negatives in misuse based systems, since there may not be any similar signature.

3. STUDY ON FALSE POSITIVES

A secure system is also vulnerable to abuse by insiders who abuse their privileges. It is not possible to build a completely secure system. All systems may have vulnerabilities, if any attack it shall be detected as soon as possible, preferably in real-time and take appropriate action. This is essentially what an Intrusion Detection System (IDS) does.

Anderson (1980) proposed first concepts of IDS, Denning (1986) presented first IDS and Steven J. Scott (2002) proposed IDS/IPS based Threat Management System [4] consists of Devices, aggregation, correlation, analysis and alarm.

The survey conducted by University of California concludes that "completely eliminate the false positives is similar to ensure complete security, as it is not possible to list all vulnerabilities". Therefore (i) in practice, it is not possible to build a completely secure system. (ii) Technology change is continuous, hence false positives or false negatives will continue. (iii) It is only possible to minimize the false positives or false negatives.

Subramanian Neelakantan [21] et. al**.** presented a Content Split Approach (CSA), tailored specifically for signature-based network intrusion detection to minimize the false positives.

Benjamin Morin [18] et. al. proposed correlation of Information related to the characteristics of the monitored information system, information about the vulnerabilities, information about the security tools used for the monitoring the events.

The model to reduce false positives using adaptive responses of firewall rule sets on "net work quarantine channels (NQC)" was proposed by Emmanuel Hooper [16], using firewall architectures. The model is a combination of firewall architecture associated with response rules, to deny access to critical segments to suspicious hosts in the network.

Chuyi Wei et. al. [6] proposed decision-tree-based classification method in IDS to solve the high packet-loss problem in IP6 environment. Hassen Sallay [7] et. al**.** discussed on a scalable distributed IDS Architecture for High speed Networks to improve the efficiency.

Kai Hwang [17] et. al. proposed a hybrid model of signature-based IDS and Anomaly Detection System (ADS), to get low false-positive and to sense unfamiliar attacks. The ADS was trained by exposing to abnormal traffic incidents from Internet connection, which detected anomalies more than the original two independent models. The "weighted signature generation scheme [17]**,** to integrate ADS with SNORT by extracting signatures from anomalies detected. HIDS extracts signatures from the output of ADS and adds them into the SNORT signature database for fast and accurate intrusion detection". The detection accuracy automatically reduced the false positives.

IDS is developed and marketed by security solutions providers as a product with standard parameters like: Throughput, No False positives in idle conditions, No of attacks prevented, UTM functionality etc. To ensure competitiveness of the product, the developers keep major thrust on design to ensure the optimal specifications. Efficiency of a product depends upon its design and implementation. However, effectiveness of security product depends not only on the design but also on installation configuration to fit into target environment. False positives problem can be addressed at design level or at implementation (operational) level. The Possible instances to address the problem of false positives in IDS are shown in Figure 1.

The relationship between the level of access control and user efficiency is an inverse one, which means that the stricter the mechanisms, lower the access efficiency. Similarly, setting of high threshold for security parameters will lead to low access and high false positives.

NIDS [12] often errs on the side of caution alarms when there is no problem. The basic reason is that most of the times signatures or rules set used by the NIDS to determine suspicious traffic are too generic. The main reason for the wrong interpretation was the rules were so configured.

In general, software and hardware products are deployed with default settings, and are so with IDS implementations. First reason for occurrence of false positives is non harmonized implementation with environment [12]. The second reason is non-updating patches of the OS, other products or updates to IDS products, as released. The third reason, when an attack or worm or a virus spread across the network, a large number of false positives occur, as IDS repeatedly notify reported attack from different systems in the network. Jacob et. al. [19] says that the fourth reason is the rules in the IDS may not fit to environment and recommended for transformation of rules.

It is evident that we cannot prevent subversion on our networks and systems. We should at least try to detect it and prevent similar attacks in future. The vigilant security administrators introduce more stringent rules by increasing the security thresholds, to reduce false negatives resulting in high False Positives.

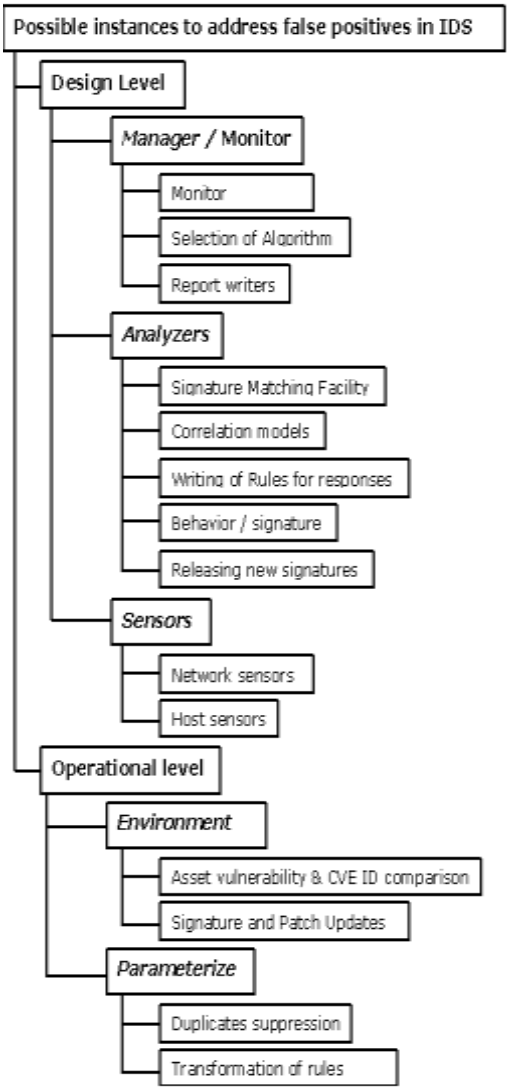

Figure 1 Instances that can be examined for minimization of false positives

False positives may seem harmless enough, but they can be costly nuisance leading to non-availability services or dropping a connection leading to lose productivity due to downtime. The false positives are the pain points for the security administrators. The security administrators cannot modify IDS design.

Most of the researchers proposed models in the first half of the Figure 1 that is at design level. The present work is on second half of the Figure 1, to study IDS alerts, configuration, rules, process and environment to examine the possibility of

minimizing false positives in an operational point of view by the security administrator.

4. PROPOSED MODEL FOR FALSE POSITIVE ALARM MINIMIZATION

The best way to secure the infrastructure and to get rid of the false positives is to review the configurations and update the security patches, update the behavior signatures [12]. Complete elimination of false positives can be achieved only when all possible threats to be listed and signature/ behavior prepared and deployed in IDS. However, it is not practically possible to list all feasible threats; therefore alternate methods are necessary to address false negatives or false positives. The present work is done using a campus network spread in multiple buildings. Snort IDS is used for the evaluation. Definitions proposed in the model are:

Definition 1: ***Global signatures*** G_s: represents global signatures being used by Snort system with combined behavioral patterns / signatures of diverse entities such as hosts, users and services in a network using Snort to capture the threats. Let G_a be the total set of alarms that can be generated using G_s.

Definition 2: ***Snort generated alarms*** A_s: are the signatures matched or partially matched within G_s based on the IDS environment. A_s is deduced based on the threats to produce generic alarms within the fixed threshold limit of IDS. Let A_a **be** the set of alarms generated with signatures by Snort, therefore

$$A_a \subset G_a \text{ ……..…..... } (1)$$

Definition 3: ***Snort matched signatures*** M_s: are the signatures exactly matched with G_s. Since M_s is deduced based on the threats of given environment alarms, M_a be the set of alarms that are exactly matched with signatures in snort (G_s), which are true positives and *may cause potential damage*, therefore

$$M_a \subset A_a \text{……..…..... } (2)$$

Definition 4: ***Repeated alarms*** R_a**:** are the set of alarms that are repeated because of the same type of activity (alarm) reported from different nodes/process/services/protocols within the network, within specified time period T_i, where the alarms are already reported and may be acted upon. Let R_a be the set of alarms repeated / generated within the time period T_i. The generated alarms R_a may be exact or partially matching signatures in snort (G_s), hence

$$R_aT_i \subset A_a \text{ ……..... } (3)$$

Therefore the partially matched alarms P_a is defined as

$$P_a = A_a - M_a \text{ ……..... } (4)$$

Analysis of the Model

1. Let G_a be the set of total alarms generated by snort.
2. Let A_a be the set of total alarms by partially or exactly matching the signatures in the current environment.

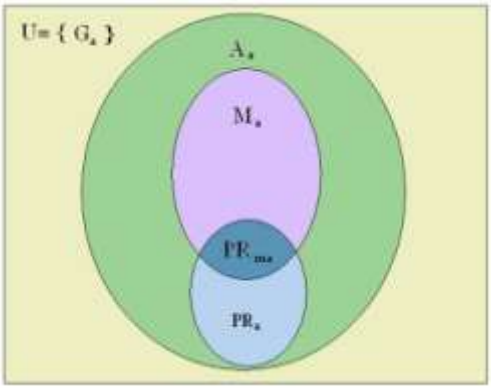

Figure 2: Alarms in IDS

3. Let M_a be the set of alarms that are exactly matched signatures. Based on the signature definitions in snort IDS, they are critical intrusions that may exploit the existing network vulnerability, hence
   $$M_a \subset G_a$$
4. Let R_a be the repeated alarms that are generated within given time period in current environment.
5. The partially matched alarms are $P_a = A_a - M_a$ as per *(4)*
6. Let F_p be the set of probable false positives in current environment.
7. The possible false positives shall be in partially matched signature alarms only. The exactly matched alarms M_a are true positives.
8. The set of possible false positives are $F_p \leq P_a$ as per (4)
9. Minimization of false positives can be achieved if the partially matched alarms are reduced to zero, i.e. $F_p = P_a = 0$
10. In general, partially matched set P_a can be eliminated by fine tuning the IDS process or by minimizing the repeated alarms, within a given period can be suppressed.

Let PR_a be the suppressed set of repeated alarms generated from G_a using suppression algorithm which implies $PR_a \subset G_a$. Probability of Repeated Alarms (Partially Matched) PR_{Pa} is defined as

$$PR_{pa} = PR_{a-(}PR_a \cap M_a) \text{ ……..... } (5)$$

PR_{ma} **Probability** ***of*** : PR_{ma} is the set of probably repeated Alarms.

$$PR_{ma=} (PR_a \cap M_a) \text{ ……..... } (6)$$

Best Case: Assuming that the model is able to suppress all repeated false positive alarms, the best case would be Ra = 0; and so $A_{a=} M_{a,}$ only the matched alarms.

Worst Case*:* Worst case situation shall arise when system do not generate repeated alarms, only non-repetitive false positives.

Analysis*:* The model is proposed to suppress only repeated alarms with in a time frame T_i, the repetitions beyond T_i will, persist. The false positives, which are not repeated are not addressed is a gap in elimination process hence few false positive will persist. Therefore choosing the time period is a critical for a specific environment.

5. MINIMIZATION EXPERIMENTS

Stephen Northcutt [12] reported that the behavior is not analyzed in IDS for the stimulus, responses, SYN floods etc. The source of attack patterns is the main reason for the wrong interpretation of the rules configured. The normal behavior is the basis for Anomaly detection, "any action that significantly deviates from the normal behavior is considered as intrusive". Therefore it is essential to define the normal behavior in IDS explicitly.

The present work is evaluated on a gigabit network spread across a campus covering multiple buildings with online real-time data on a V-LAN segment of one department traffic. The IDS is connected and configured on a V-LAN segment to observe traffic in promiscuous mode. The evaluation is carried out in the following environment. Snort [16] (Version 2.6) a signature based intrusion detection system for obtaining network specific alarms, a software sensor Winpcap [17] (Version 4.0) to collect the packets in promiscuous mode and MySql [18] (Version 4.0.25) to store data.

5.1 Keep informed of signatures

The first case of experiment was done simultaneously on two systems connected on same network stream. One system without updating snort signatures and second system with latest (with updated) signatures. The results are observed a period of time and tabulated and shown in Table 2. The observed results indicate reduction in the number of alerts. The difference in number of alerts in the two systems is the number of false positives reduced. For the stand point of reduction in alerts, updates for week duration, improved the performance in terms of significant reduction of 11.59% in alerts.

Table 2: Alerts generated before and after updating of signatures

S no	Protocol	Alerts before Signature	Alerts after Signature Updating
1	IP	938	862
2	TCP	11	08
3	UDP	873	735
4	ICMP	119	111
5	**Total**	**1941**	**1716**

5.2 Suppression of repeated alarms

The windows version of snort IDS is ported on a windows 2003 server. MySql database is also loaded on same server to store data captured by the sensor. Winpcap sensor software was ported and installed on a PC. NIC card on the PC was set into promiscuous mode to collect the traffic. The packets collected are stored on database created on the server. The designed software is used to process traffic collected by sensor, further to analyze and suppress redundant (false positives) alarms. In Figure 3, the model in brief with process flow diagram is presented.

Alarms deduced from Snort are input for the application process. With a pre-set time period parameter, the data is analyzed. The first instance of the alert is flagged and retained, while remaining alerts are stored for analysis. The Derek Woolverton [19] adaptive algorithm is used to label duplicates.

Suppression of repeated alarms is one of the proposed model and results are presented at Figures: 4 & 5. The proposed parameters viz., total alerts, matched alerts, suppressed alerts in an extended period of 3 weeks is evaluated, with one week duration in as repetitive nature.

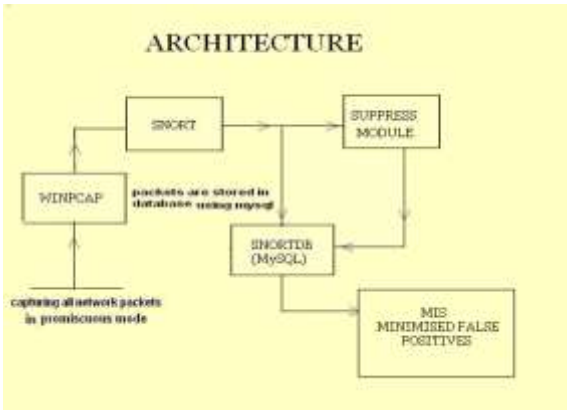

Figure 3 Architecture of the proposed System

The trend, reflecting above parameters is presented after evaluation. The observed results are indicative of the suppressed alerts based on the environment. The system effectively suppressed repeated alarms at the rate of 61.42%, 35.12% and 21.02% in the first, second and third weeks respectively.

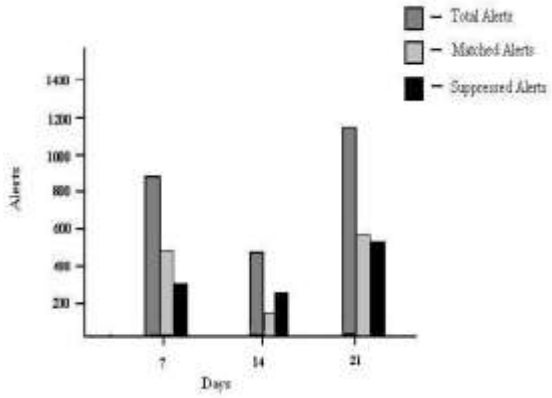

Figure 4: Graphs showing alarms & suppressed alarms

The graph drawn on two parameters is an indicative of matched alerts and alerts after suppression is shown at Figure 4. The matched and suppressed alerts are observed to be dependent on environment, reflecting the consistency in reduction of alerts. The protocol wise alerts observed on weekly basis, classified as IP, TCP, UDP and ICMP is presented in Table 3. The protocol based alerts are observed to be different with traffic. As we observe the suppressed alerts, duplicates are found to be reduced.

Table 3: **Protocol wise alarms and suppressed**

Protocol	First week (Dec' 2008)		Second week (Dec' 2008)		Third week Dec' 2008	
	Gen*.	Sup**	Gen.	Sup	Gen	Sup
IP	862	333	446	288	1247	1109
TCP	08	05	04	03	09	06
UDP	735	219	165	153	1039	750
ICMP	111	105	276	134	197	103
Total	1716	662	891	578	2492	1968

Gen.* = Generated; Sup**. = Suppressed

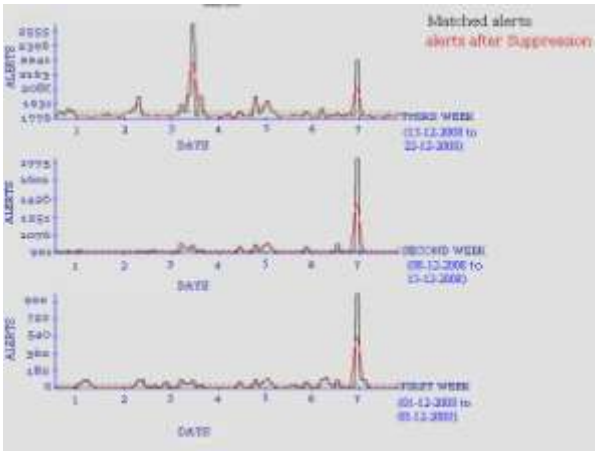

Figure 5 Traffic and suppressed alarms

5.3 Customization on Risk based model

The model based on environment and security policy. The level of security defined in the security policy is vital to reduce false positive alarms. IDS identify attackers while they are trying to expose vulnerability in the environment. Risk reduction is the objective of the IDS and responds attack to an alert. The approach in reduction of false alarm is to analyze alarm cases and quantify risk associated with alerts.

Based on the risk aversion model adopted in security policy, IDS to be customized to reduce risk by reducing factor of exposure or reduce threat level. To quantify, a parameter called Attack Accuracy Level (AAL) which is a score or number of attempts required to expose existing vulnerabilities. The AAL is computed:

AAL = high risk x √ (low risk attempts x Medium risk)

A design with high AAL is preferred for lower the successful attacks. If the accuracy level of the IDS is low the false positives will be less.

Based on observations of the environment, few signatures (1) 'MISC UPnP malformed advertisement' (2) 'NETBIOS SMB IPC$ unicode share access' (3) 'ICMP PING NMAP' (4) 'ICMP L3 retriever Ping' (5) 'SCAN UPnP service discover attempt' are selected for study and analysis.

The model is also experimented [19] simultaneously on two systems connected on same Network.

Table 4: Signature wise alarms Aug -Sept 09

SNo	Signature name	IDS without tuning	IDS after tuning
1	'MISC UPnP malformed advertisement'	649	0
2	'NETBIOS SMB IPC$ unicode share access'	23	23
3	'ICMP PING NMAP'	22	22
4	'ICMP L3retriever Ping'	68	0
5	'SCAN UPnP service discover attempt'	44	44

Based on the risk model, two rules are selected and transformed. The differences in number of alerts in the two systems are the number of false positives eliminated. The results are tabulated and shown in table 4. For the stand point of reduction in alerts, for week duration, improved the performance in terms of significant reduction of 88.95% for the selected rules.

6. CONCLUSION

Security tools installation, monitoring to ensure security is the responsibility of the Security Administrator in an organization. IDS generate a large number of alerts (false positives). Most of these alerts demand manual intervention from Administrator. Continuous monitoring of alerts and there by evolving a judgment for improving security is the major concern.

The research presents approaches for minimizing the false positives. To facilitate security administrator to address false positives, alternate models are examined and experimented. The models are (i) updating signatures (ii) suppression of repeated or partially matched alerts and (iii) configuration of environment variables by transforming rules.

The experiments were carried out on real time data. To evaluate results number of alerts generated before and after updating of signatures are compared. Similarly suppressed alarms with customization of environment parameters and with out customization are evaluated. The results showed an improvement in efficiency, while reducing false positive alerts

The examined models are having an advantage of utilizing itself into any kind of environment with a modest customization of pre-defined functionality for addressing false positives in IDS. The selection of technologies, tools and proper use of security policy makes it significant in minimization of security attacks and so false positives.

7. REFERENCES

[1] Anderson, J P (1980), Computer Security threat Monitoring and surveillance (Technical Report). Fort Washington, PA: James P Anderson Company.

[2] Peng Ning(2005), "Intrusion Detection Systems Basics", published in "Hand Book of Computer", Volume 3, edited by Hossien Bidgoli, Published by John Wiley& Sons, Inc (PP 685 to 700)

[3] Web pages hosted by "The Mitre Corporation", (2005), CVE is funded by US department of Home land, "Use of the Common Vulnerabilities and Exposures List", Web site http://cve.mitre.org/about

[4] Steven J. Scott, August 9, 2002, sjscott007@yahoo.com , "Threat Management Systems, The State of Intrusion Detection" hosted on web page: http://www.snort.org/docs/threatmanagement.pdf

[5] Simon Edwards, (September 2002), "Network Intrusion Detection Systems: Important IDS Network Security Vulnerabilities", white paper Top Layer Networks, Inc. Web page: http://www.toplayer.com/pdf/WhitePapers/wp_network_intrusion_system.pdf/

[6] Chuyi Wei et. al. [2008], "The IDS Model Adapt to Load Characteristic under IPv6/4 Environment", ISBN: 978-1-4244-2107-7, INSPEC Accession Number: 10357013,http://ieeexplore.ieee.org/Xplore/defdeny.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D4679079%26userType%3Dmem&denyReason=-134&arnumber=4679079&productsMatched=null&userType=mem

[7] Hassen Sallay, Khalid A. AlShalfan, Ouissem Ben Fred, (2009)**,** "A scalable distributed IDS Architecture for High speed Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[8] William Stallings, (2003, 3rd Edition), "Cryptography & Network Security Principles & Practices", Intrusion Detection(pp. 571).

[9] Michael Sieffert, Rodney Forbes, Charles Green, Leonard Popyack, Thomas Blake (2004) , "Stego Intrusion Detection System" http://www.dfrws.org/2004/day3/D3-Sieffert-SIDS.pdf, Assured Information Security, Inc. PO Box 1182, Rome NY 13442, USA, accessed on 20.02.08.

[10] Daejoon Joo , Taeho Hong , Ingoo Han , "The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors -, Expert Systems with Applications 25 (2003) 69–75, accessed at http://afis.kaist.ac.kr/download/inter_jnl029.pdf, Expert Systems with Applications 25 (2003) 69–75,) Published by Elsevier Science Ltd.,

[11] Joshua Shaul, ("Database IDS versus traditional Network IDS"), White Paper by Systems Engineering, Application Security Inc, http://www.appsecinc.com/presentations/Database_IDS_vs_Network_IDS.pdf

[12] "Stephen Northcutt & Judy Novak", (2003) Network Intrusion Detection (3rd .ed), Indianapolis: New Riders Publishing. P79, P401-404

[13] Stefano Zanero(2007), "Flaws and Frauds in the Evaluation of IDS.IPS Technologies", first accessed on 21.09.07, http://www.first.org/conference/2007/papers/zanero-stefano-paper.pdf

[14] J Snyder (2004). Taking Aim: "Target–Based IDS Squelch Network Noise to pinpoint the alert you really care about". Information security Magazine, January 2004.

[15] Andre Yee(January 22, 2004), NFR Security "Making false positives go away", http://www.computerworld.com/securitytopics/security/story/0,10801,89122,00.html?f=x15", accessed on 21.08.07

[16] Emmanuel Hooper (2006), "An Intelligent Intrusion Detection and Response System Using Network Quarantine Channels: Adaptive Policies and Alert Filters" , Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT 2006 Workshops)(WI-IATW'06), pp. 16-21, 0-7695-2749-3/06 $20.00 © 2006.

[17] Kai Hwang, MinCai, Ying Chen and Min Qin "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes"(2007), IEEE Transactions On Dependable And Secure Computing, Vol.4, No.1, January-March 2007, accessed on 22.02.08, at http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=4099191.

[18] Benjamin Morin 1, Ludovic M, Herv Debar, and Mireille Ducass (2007) "M2D2: A Formal Data Model for IDS Alert Correlation", Volume 2516/2002, pages 115-137 online http://www.springerlink.com/content/cwp428tlhf35rwba/

[19] Jacob et. al., "False positives in intrusion detection systems", RSPS2010conference Proceedings, 2010, PP 534 -540, ISBN 978-81-908240-0-2

[20] Neelakantan,S. & Rao, **"**A Threat-Aware Signature Based Intrusion Detection Approach for Obtaining Network-Specific Useful Alarms, in the proceedings of "Internet Monitoring and Protection, 2008. ICIMP '08" Publication Date: June 29 2008-July 5 2008, ISBN: 978-0-7695-3189-2, (pp 80-85)

[21] Subramanian Neelakantan et. al. (2009) "Content-Split Based Effective String-Matching for Multi-Core Based Intrusion Detection Systems , First International Conference on Computational Intelligence, Communication Systems and Networks Pages: 296-301 ISBN:978-0-7695-3743-6

Authors:

1. G Jacob Victor: BE(CS), from Andhra University, M.Tech (CS), from BIT, Ranchi, India; Certified Software Quality Professional (CSQP), Certified Information System Auditor (CISA), Currently, Joint Director, IT&C Department. 23 years of IT Experience in Industry & Government.

2. Dr. M Sreenivasa Rao, Professor, School of Information Technology, JNT University, Hyderabad, obtained his Graduation and Post graduation in Engineering from JNT University, Hyderabad and Ph D from University of Hyderabad. Over 23 Years of IT Experience in the Academia and Industry.

3. Dr. V. Ch. Venkaiah, Professor, CRRao AIMS & CS, UoH Campus, Gachibowli, Hyderabad, obtained PhD. from IISc, 21 years of research experience & academic Recipient of CSIR's both Junior and Senior Research Fellowship. Selected for both CSIR Research Associateship and Indo-USSR Post doctoral fellowships.