iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VII **Month of publication:** July 2018

DOI: http://doi.org/10.22214/ijraset.2018.7116

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VII, July 2018- Available at www.ijraset.com

Proposed Model for Automatic Evidence Collection in IDS

Dr.B.Mukunthan[1], T.Saravanan[2], Nivetha[3]
[1]*Research Advisor, PG & Research Department of Computer Science, Jairams Arts & Science College, Karur-03, (TN) India*
[2] *PG & Research Department of Computer Science, Jairams Arts & Science College, Karur-03, (TN) India*
[3]*Research Scholar, PG & Research Department of Computer Science, Jairams Arts & Science College, Karur-03, (TN) India*

Abstract: ***Web has changed and enhanced the method for working in associations and organizations, in the meantime this vast system additionally opened entryways for assailants as new assaults are developing step by step. To shield the associations and frameworks from these assaults, arrange security comes without hesitation. System security is the strategy made by the executive by running security programming or introducing apparatuses in the system with a specific end goal to shield the system and its assets from security dangers. In arrange security, Intrusion Detection System (IDS) is one of the well-known and effective component to secure the system. The point of IDS is to offer a layer of insurance against unapproved (or malevolent) employments of frameworks by detecting the defencelessness in the framework or abuse of a security strategy, and cautions framework director to a continuous (or later) assault. IDSs work is constrained to distinguish the interruption and react to executive about the interruption by observing the framework persistently. IDS can't protect confirm about the interruption, which makes it difficult to see the harm in the framework and assemble data about the assault and henceforth make it difficult to get the interloper. Despite the fact that proof can be gathered from IDS's and framework log records, however uprightness, unwavering quality, and culmination of such confirmation are suspicious as log documents can likewise be changed by an interloper.***

Keywords: IDS,

I. INTRODUCTION

A. Introduction to Intrusion Detection System (IDS)

When a hacker or system user exploits or breaks into the system by taking illegal action, is called intrusion. The intruder may be an insider or an outsider, who does malicious activities or actions in an unauthorized manner. Intrusion detection is a process of finding unauthorized activities (intrusion) by inspecting the inbound traffic. Intrusion detection involves observation and analysis of user and system activities, auditing of vulnerabilities and configurations of the system, evaluating the integrity of data files and critical system, statistical analysis of activity patterns, analysis of abnormal activities, and audit of operating system [1].

First concepts about Intrusion Detection System (IDS) was given in the early 80s by James P. Anderson. Intrusion detection system can be a physical appliance or security software to monitor the network traffic in order to detect suspicious activity. Many IDS keep information about the detected intrusions in a log file for further analysis or to combine these logs with other data to make policy and decisions. Most of the intrusion detection system detects suspected intrusion and then informs to the system administrator by sending an alert. Originally IDS was thought as a single, stand-alone system based on audit records processing based detection. Today IDS is a distributed system which contains multiple systems combined together [2].

Brian Cusack and Muteb Alqahtani [3] have proposed “Acquisition of evidence from Network Intrusion detection systems”. This work evaluates the performance of NIDS in wired networks under different workloads to find the evidential value of the NIDS. Jorge Herrerias and Roberto Gomez [4] have proposed “A log correlation model to support the evidence search process in a forensic investigation” to correlate the logs coming from diverse log files of various applications. Fahmid Imtiaz has studied the “Intrusion Detection System Logs as Evidence and Legal Aspects”. This study focuses on the potential of using an intrusion detection system generated logs in legal as evidence in legal proceedings. Leonard Kwan, Pradeep Ray and Greg Stephens [5] have proposed “Towards a Methodology for Profiling Cyber Criminals”. This work proposed an approach using honeynets to collect legally valid evidences from cybercrime. Due to lack of effective methodologies of collecting evidence and prosecute the attacker, many cybercrimes go unpunished. Proposed approach addresses this problem by using generation-III honeynet. Collie and Byron [6] have studied “Intrusion Investigation and Post-Intrusion Computer Forensic Analysis”.

This paper gives an overview of the investigation and handling of security incidents, from the perspective of a legal administrative investigator. This work proposes a prologue to the investigation of intrusions and likewise portrays various post-intrusion computer forensics methodology and tools. This includes incident response, intrusion investigation, real-time intrusion investigation, post-intrusion forensics, and intrusion reconstruction. Stephenson and Peter [7] have studied "The application of intrusion detection systems in a forensic environment". This paper describes the framework to explore the applicability of IDS in process of collection and management of digital.

II. PROPOSED MODEL FOR AUTOMATIC EVIDENCE COLLECTION

Proposed model named "Application of IDS in automatic evidence collection using digital forensics" can be used to automatically collect the information about the attack detected by anomaly based intrusion detection system whenever an attack occurs and then analyze the collected information to get evidence. The fundamental work of an IDS is to detect the attack and respond to the system administrator. This limits IDS to preserve the detailed information about the attack and hence about the attacker. IDS alone is unable to give any information about the techniques and tools use in the attack by the attacker and also not able to trace the attacker. The intrusion detection system is also not able to give any information about what and how much amount of damage to the system is done by particular attack. To overcome this problem we have proposed a model in which digital forensic tool is used along with intrusion detection system. This digital forensic tool will capture the memory image of the system in order to preserve the information about the intrusion. Proposed model gives the way to automatically trigger the digital forensic tool whenever the intrusion detection system alerts an intrusion. Two models are given below first by using signature based intrusion detection system and other is by using anomaly based intrusion detection system. In the following section we have discussed system model, flowchart, tools used, and type of attack used for both the models.

A. Model with Signature Based IDS

1) *System Model and Assumptions:* System model with signature based IDS is shown in Figure 3.1 [8]. The function of each component is described below. Target host is a system that is to be protected from the attacker or intruder. This system consist of valuable assets such as data files, credential information, databases, system files, logs and many more important things that have to be protected from the attackers.

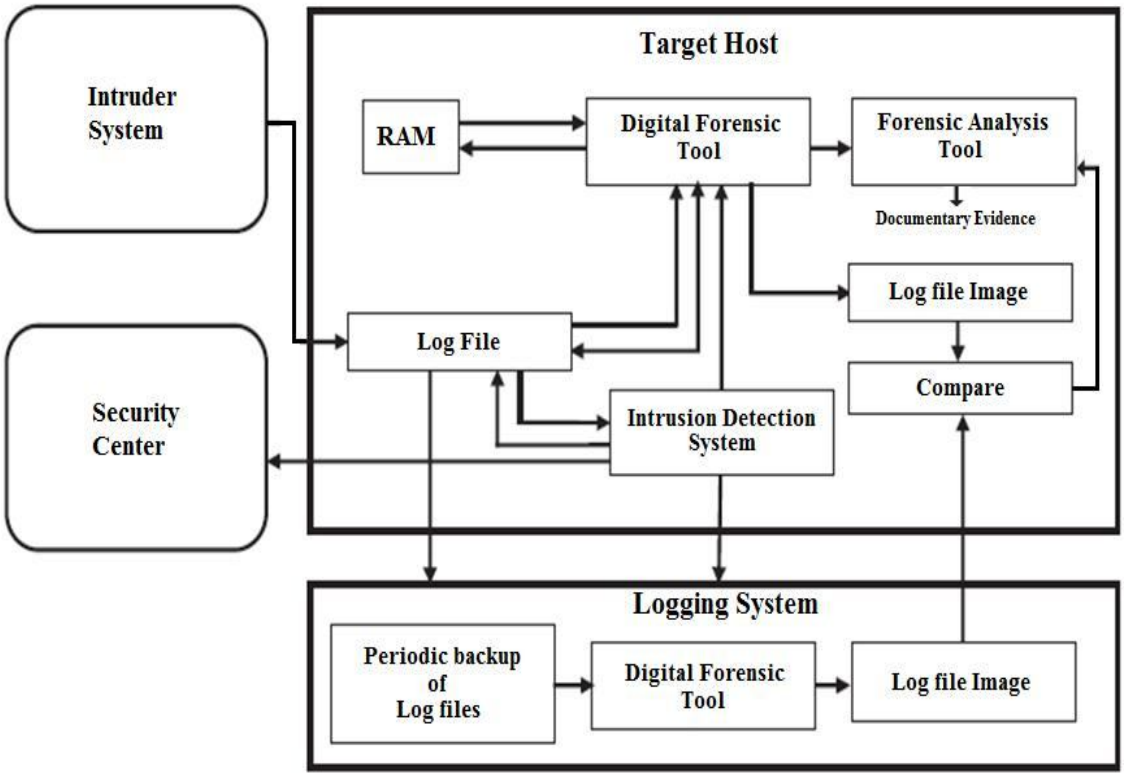


Figure 1: System model with Signature Based Intrusion Detection System.

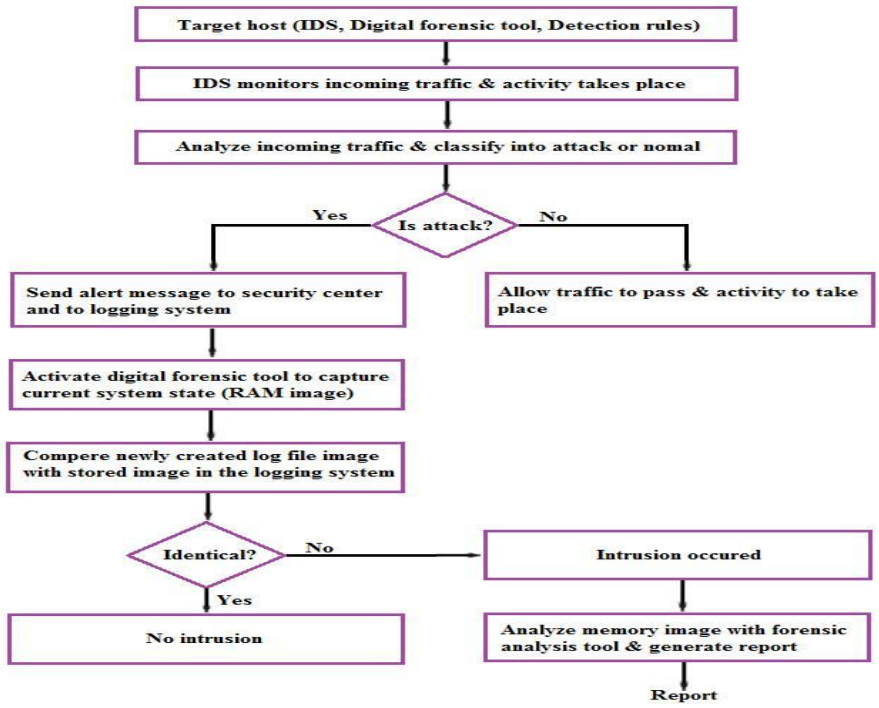
2) *Target Host:* This is the system that has to be protected from the attacks as it has many valuable assets. Target host consists intrusion detection system, digital forensic tool (memory acquisition tool), and forensic analysis tool (memory analysis tool). This system runs under the supervision of the system administrator.
3) *Intruder System:* This is the system from where the intruder launches the attack on the target host by sending the malicious packets. The intruder system consists techniques and tools required to launch the attack.
4) *Security Center:* This is the system from where the security administrator monitors the target host. On intrusion occurrence an alert is sent to the security center to notify administrator about the intrusion. An alert can be sent in various ways, such as audio message, email, and message on console. Intrusion detection system: To protect the target host some security mechanism is needed that monitor the system continuously and detect the intrusion whenever occurs. In this work IDS is used to secure the system, which inform the security administrator about the attack and automatically activate the digital forensic tool to capture the memory image of the system.Signature based intrusion detection system is used in this model. Signature based intrusion detection system is based on signature matching. Signature (or rules) of known attacks written in the configuration file of the intrusion detection system are matched with the new incidents to classify new event as an attack or normal traffic. Signature based intrusion detection system has three main component, packet capture unit, preprocessor unit, detection engine. The detection engine reads the rules for known attack from rule file (or configuration file) using appropriate plugins.
5) *Logging System:* Logging system the system used to store a copy of the log files of the target host. Back up of target hosts log files is taken periodically (i.e. 12 hours, 3 days, 2 weeks), and stored on this system to protect them from intrusion.
6) *Digital Forensic Tool:* Digital forensic tool is a framework to collect efficient and forensically sound data from the attacked system. Digital forensic tools may be of many types such as memory acquisition tool, disk capture tool. In our proposed model we have used memory acquisition tool to capture the physical memory image of the target host whenever an attack is detected on the system.
7) *Forensic Analysis Tool:* Forensic analysis tool is a set of utilities used to analyze the information collected from the digital forensic tool, in order to find the digital evidence. Forensic analysis tool generate the evidence from the collected information which gives much information about the attack in an understandable format, and such information is acceptable by the court in legal proceedings. There are numerous types of forensic analysis tools such as, memory analysis tool, disk analysis tool, email analysis tool, file and data analysis tool, registry analysis tool, application analysis tool, etc. In our proposed model we have used a memory analysis tool which will analyze the previously captured image.

III.METHODOLOGY

The methodology of the system model with signature based intrusion detection system is given in following steps and pictorial representation of the same in the form of flowchart is shown in Figure .2.

A. Steps

1) Signature based intrusion detection system is deployed on the target host which has to be protected from intrusions or malicious activities. Target host contains intrusion detection system, digital forensic tool, and forensic analysis tool.
2) IDS is deployed in such a way that all the traffic coming to the host must pass through IDS. IDS monitors the incoming traffic continuously to detect unwanted traffic or malicious activity.
3) For every incoming packet, IDS generates and matches its signature (some specific pattern that is defined as an attack in the rule file by the system administrator) to the previously stored attack signatures to classify incoming traffic as attack or normal. If the signature of incident traffic matches with any of the stored signature, then that incoming traffic is classified as an attack.



If incoming traffic is classified as normal traffic then IDS simply allow it to pass and corresponding activity to take place.

But if incoming traffic is classified as an attack that means an intrusion is detected by IDS. Hence an alert message is sent to the security center to inform the security administrator about the intrusion and notification also send to the logging system to create an image of stored log files.

Simultaneously, digital forensic tool is activated to capture the current system state in order to preserve the information about the attack for future analysis. RAM (and log file) image is captured to get current system state which contains all running processes, connections established, files altered or created and much more information about the system when an attack is taking place.

To verify the attack newly captured log file image is compared with the image created from the stored log file image. If both are identical, then there is no intrusion means false alarm was given by IDS.

But if both images are not same then definitely an intrusion has occurred.

As intrusion has occurred, captured RAM image is now analyzed by using forensic analysis (Memory analysis) tool to get useful information from RAM image.

The information found from analysis can be used to create a report about the intrusion. This report can be used as documentary evidence in court in legal proceeding. By default an HTML report is generated by the tool used here for analysis.

B. Model with Anomaly based IDS

1) Sytem Model and Assumptions: System model with anomaly based IDS for proposed approach is shown in Figure Most of the components like intruder system, target host, security center, digital forensic tool, forensic analysis are already discussed under section system model with signature based IDS. Intrusion detection system used in this model is different from previous one.

Intrusion detection system: In this model anomaly based intrusion detection system is used in which definitions of normal data behavior are stored and compared with incident to categorize the incident as an intrusion or normal.

Anomaly based Intrusion detection system has three main components, packet capture unit, Event engine, and policy layer mechanism. Intrusion detection system is deployed on the target host so that all the traffic coming to that host will first go to intrusion detection system. Intrusion detection system then decides whether the traffic is normal or suspicious. If traffic is normal then the intrusion detection system notifies the system administrator and activate digital forensic tool, otherwise allow the traffic to simply pass and corresponding activity to take place.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VII, July 2018- Available at www.ijraset.com

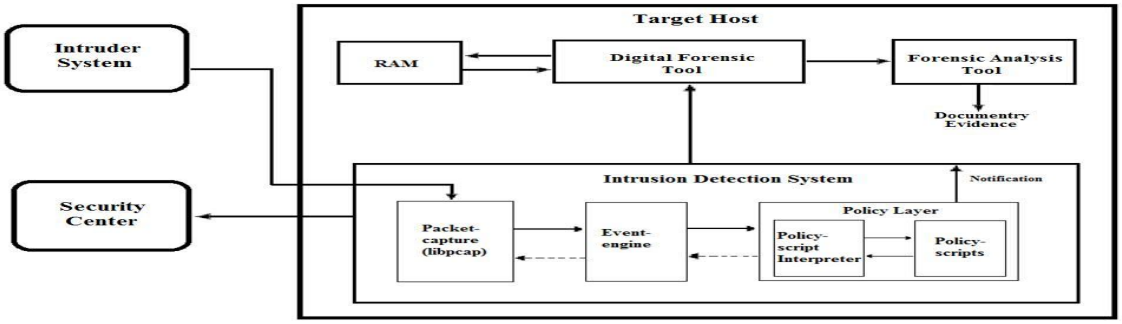


Figure 3: System model with Anomaly Based Intrusion Detection System.

C. Methodology

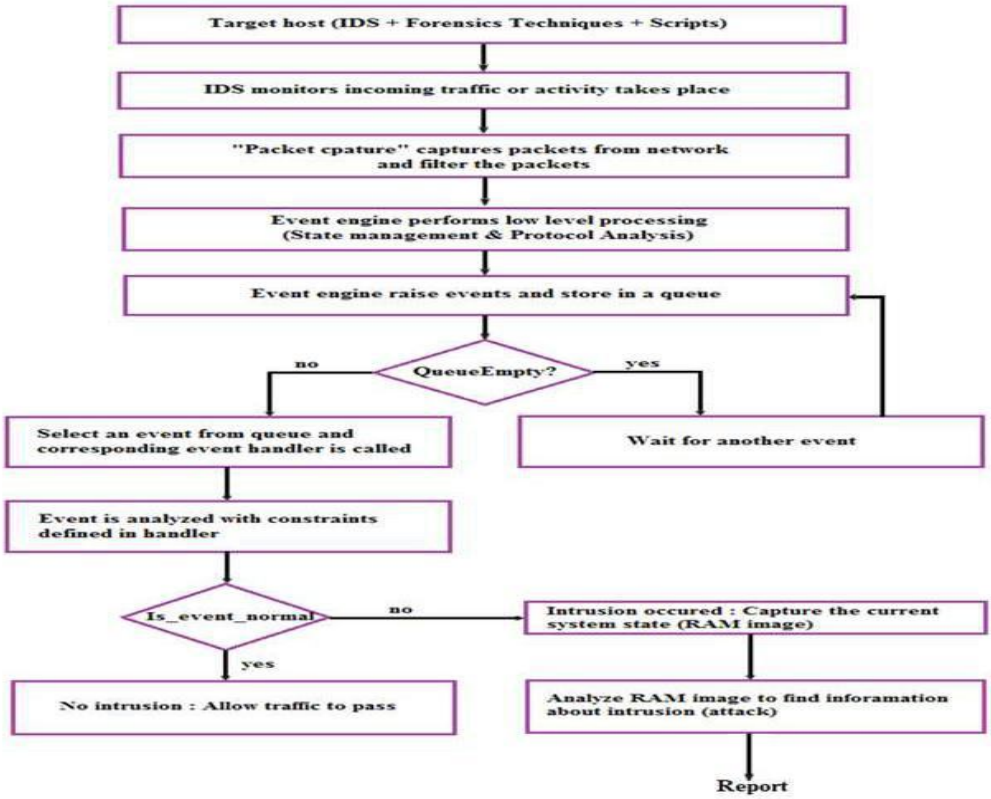
The following steps shows the working of the model with anomaly based IDS and pictorial representation of the same is shown in the flowchart in Figure 3.4.

Steps

1) Intrusion detection system is deployed on the target host monitors the network traffic continuously to protect the system from intrusions.

2) Packet capture unit catches data packets flowing through the channel and filter them based on the filter written such as a filter to allow only tcp packets, filter to allow only udp packets, filter to allow packets on or from any specific port such as port 79 for finger, 21 for ftp, and 23 for telnet.

3) Packet captured by the packet capture unit are filtered and then sent to the event engine to generate relevant events from the data streams. The packet capture unit performs low level processing of the data coming from lower layer. Low level processing involves management of connection states, various application analysis, management of timers, data structure, scripts etc.



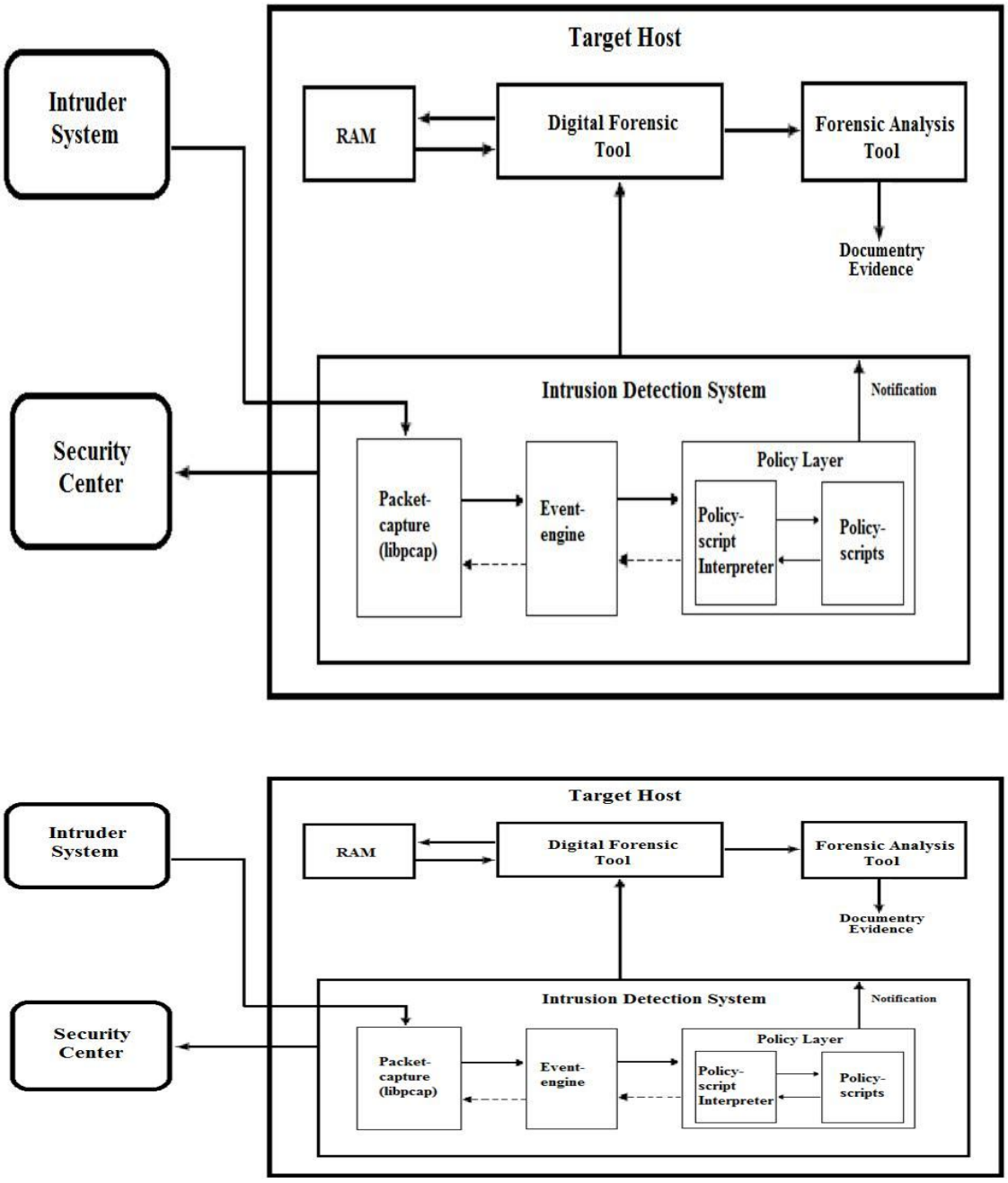


Figure.4: Flowchart for model with Anomaly based IDS.

4) After analyzing the data packets Event engine raise an event and place it in a queue. Events are some relevant activities in the system or network such as connection established is an event.

5) At the policy layer event handlers are written for almost every type of events. Every time one event from the queue is taken and the corresponding event handler from policy layer is called. This process continues until the queue becomes empty, when the queue becomes empty interpreter waits for new events to be placed in the queue.

6) Every time an event is analyzed with corresponding event handler and if it violats the normal data behavior policies, then classified as an intrusion otherwise simply allows to pass

7) If an event is classified as an intrusion means intrusion has taken place in the system and hence alert is sent to security center and digital forensic tool is activated to dump the physical memory (RAM) of the system which will contain useful information about the attack.

8) Once the physical memory image is captured, it can be analyzed with forensic analysis tool to get the useful information such as number and name of the processes running at the time of the intrusion, connections established, files open or modified, system tables altered, etc

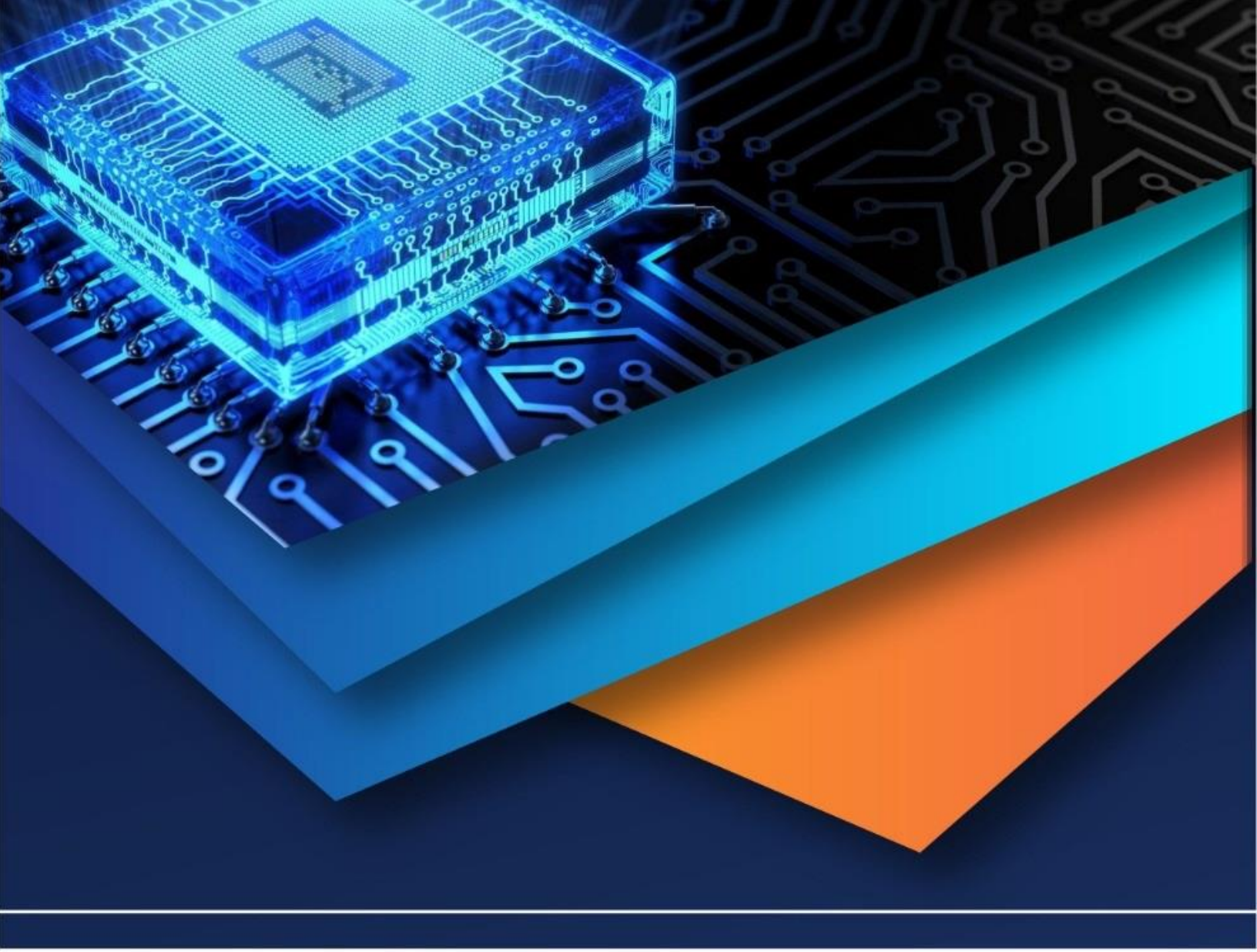
9) A report can be generated from the information found in memory image analysis. This report can be used as evidence (documentary type) in a legal proceeding in order to punish the attacker.

IV. CONCLUSION

In this work "Application of Intrusion Detection System in Automatic Evidence Collection using Digital Forensics" is proposed by using both signature and anomaly based intrusion detection system. In this work intrusion detection system is used to detect intrusion and then current system image is captured by digital forensic tool. Further, this captured memory image is analyzed by using forensic analysis tool. In this work two models have been given, first model used signature based intrusion detection and other is using anomaly based intrusion detection. To save prove in its unique shape, we have proposed Application of Intrusion Detection System in programmed Evidence Collection utilizing Digital Forensics. In our model at whatever point an interruption is distinguished, IDS advises the head by sending an alarm and additionally actuate the computerized measurable device to catch the present condition of the framework. This caught framework picture contains all the data about the arrangement of the time when the assault was occurring. Consequently such picture can be utilized as confirmation in lawful procedures. We utilized both mark based IDS and abnormality based IDS in the work and watch that mark based IDS can't recognize novel dangers while peculiarity based IDS can distinguish such dangers.

REFERENCES

[1] Clive Grace. Understanding intrusion detection systems. PC Network Advisor, 122:11–15, 2000.
[2] Debra Anderson, Teresa F Lunt, Harold Javitz, Ann Tamaru, Alfonso Valdes, et al. Detecting unusual program behavior using the statistical component of the Next-generation Intrusion Detection Expert System (NIDES). SRI
[3] Brian Cusack and Muteb Alqahtani. Acquisition of evidence from network intrusion detection systems. 2013.
[4] Jorge Herrerias and Roberto Gomez. A log correlation model to support the evidence search process in a forensic investigation. In Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on, pages 31–42. IEEE, 2007.
[5] Leonard Kwan, Pradeep Ray, and Greg Stephens. Towards a methodology for profiling cyber criminals. In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, pages 264–264. IEEE, 2008
[6] Federal Agent Byron S Collie, Headquarters Air Command, and Royal Australian Air Force. Intrusion investigation and post-intrusion computer forensic analysis. Headquarter Air Command, Royal Australian Air Force, year=2006
[7] Peter Stephenson. The application of intrusion detection systems in a forensic environment. In The Third International Workshop on Recent Advances in Intrusion Detection (RAID), 2000. Komal Barhate and CD Jaidhar. Automated digital forensic technique with intrusion detection systems. In Advance Computing Conference (IACC), 2013 IEEE 3rd International, pages 185–189. IEEE, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY