iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VI **Month of publication:** June 2014

DOI:

www.ijraset.com

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

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

An Advanced Hybrid Intrusion Detection System in Cloud Computing Environment

Vikas Singh[#1], Amit Kumar[#2], Astt. Prof. Devender Kumar[*3]

[#*]*Department of Computer Science & Engineering*
MERI – College Of Engineering & Technology
Asanda (Near Sampla) Bahadurgarh, Haryana

Abstract: ***Today, Cloud Computing Security (also known as Cloud Security) is the major concern. Cyber-attacks have not only grown to an unimaginable volume but also a sophistication and variety that would have been hard to believe a few years back. Cloud Computing holds the potential to eliminate the requirements for setting up high cost computing infrastructure for the I.T based solution and services that the industry uses. In computer networking, cloud computing is computing that involves a large number of computers connected through a communication network such as the Internet. Cloud computing and Intrusion detection and prevention system are one such measure to reduce these attacks. Different researches have proposed different IDS's time to time. Most of the researchers combine the features of Anomaly based detection methodologies and Signature based methodologies. Intrusion Detection System which is more efficient than the traditional Intrusion Detection System. In this paper, we present a modified Hybrid Intrusion Detection System that combines the advantages of two different detection methodologies- Anomaly based intrusion detection methodology and Honeypot methodology. We use both the IDS individually and then together and maintain the data record time to time. From the data record we find conclusion that the resulting Intrusion Detection System is much better in detection intrusions from the existing Intrusion Detection Systems.***

Keywords: IDPS (Intrusion Detection and Prevention System), Hybrid IDS, Cisco Packet Tracer, Flow Matrix, KFSensor, SNORT.

1. INTRODUCTION

Cloud computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Reaching the point where computing functions as a utility has great potential, promising innovations we cannot yet imagine. Cloud computing is a recent computing model; provides consistent access to wide are distributed resources. It promises to provide a flexible IT architecture, accessible through Internet for light weight portable device.[1][2]. It revolutionized the IT word with its service availability assurance, rapid accessibility and scalability. Cloud computing denotes the infrastructure as a "Cloud" from which businesses and customers are competent and capable to access applications from anywhere in the world using on demand techniques. There are various issues that need to be dealt with respect to security and privacy in a cloud computing scenario.

2. RELATED WORK

There are many researcher have gone through the various security issues related to cloud computing environment. Dimitrios Zissis and Dimitrios Lekkas[2] discussed security issues in cloud computing but they have no method to validate his work. After that Meiko Jensen, Nils Gruschka and Luigi Lo Lacon[3] gives various technical security issues in cloud computing environment. Milan Yo, Lucian Popa, Y.Steven Ko, Sylvia Ratnasmy and Ion Stoica design a hypervisor based cloud police[4] and Seongwook Jin[5] Architectural Support for Secure Virtualization under a Vulnerable Hypervisor.

ISSN: 2321-9653

Other researcher works on developing on Intrusion Detection and Prevention system to stop intruders form attacking. They used hybrid intrusion detection and prevention. Zhi-Hong Tian gives An architecture for intrusion detection using honeypot[6]. After their Andy Bechtolsheim developed a hybrid real time agent based intrusion detection and prevention system for wireless network.

There after a lot of research is being done to combine an anomaly based IDS and Signature based IDS. Kai Hwang, Ying Chen, Hua Liu[7] propose Cooperative anomaly and intrusion detection system (CAIDS). Similarly J.Gomes[8] and his colleague have done research and implement on Snort based hybrid IDS. Emmanuel Hooper[9], An Intelligent Intrusion Detection and Response System Using Hybrid Ward Hierarchical Clustering Analysis.

Some researchers try to integrate honeypot technology to IDS. Honeypot attract an attacker towards it and works in cooperation with firewall. The firewall will stop the intruder visit whose IP address is set in the firewall as blacklist by honeypot technology. Prof. Smita Jawale[10] design architecture for Intrusion Detection System using Virtual Honeypots. This overcomes the problem information overload, false positive, false negative and unknown attacks.

Here we have to propose a new Intrusion detection and prevention system design which is more efficient than traditional IDS. The Intrusion Detection System (IDS) is based on Anomaly Detection Methodology and Honeypot Technology. To implement this system we have design architecture in the computer network lab and collect data to validate the proposed Hybrid Intrusion Detection System.

3. ARCHITECTURE FOR HIDS

First of all we consider a network, simulated and configured on Cisco packet tracer and then implemented it in real time to analyze network properly. Figure 1 shows the network architecture

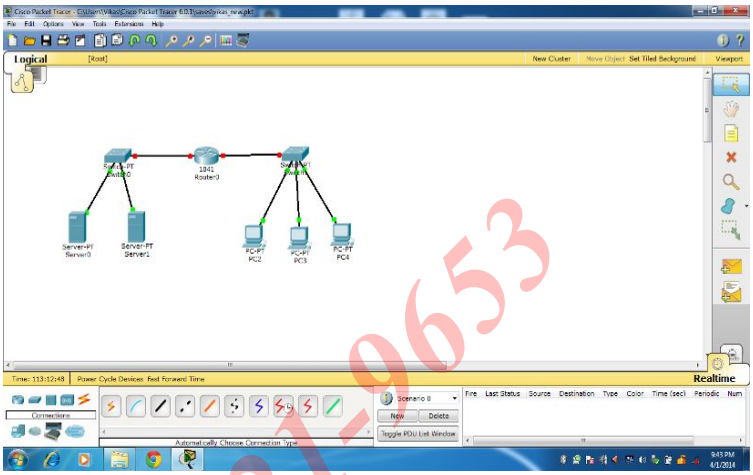


Figure1: Network Architecture

configured in Cisco packet tracer[11][12]. The network architecture consists of three nodes and a server. Server is connected to router to route data packets to various networking device and to connect LAN to WAN. Behind the router we are using four nodes, one is server and other three are connected to router through a switch. The server communicated with the nodes using router via switch. We have installed two types of Intrusion Detection System. One is based on Honeypot technology and other is based on anomaly IDS. Honeypot can attract the attacker whenever it tries to perform malicious activities over the computer network and later with this system we can make and update their signature in database whereas anomaly based IDS can analyze the network and record the normal traffic and whenever it finds any anomalous activity is warns. Both these system strongly restrict an attacker to attack on computer network. We use KFSensor[13][14] that is Honeypot technology based and FlowMatrix[15] that is anomaly based IDS.

4. RESULT AND STUDY:

To validate our algorithm we have implement the system into three phases:

Phase I. In this phase first of all we studied KFSensor and study the system with KFSensor for 10 days and record some results. In this phase we find that KFSensor is capable to detect those attacks for which different systems directly contact or interact with it but KFSensor cannot detect those attacks which are done by the systems that are not directly connected or interact by it.

ISSN: 2321-9653

Phase II. In this phase we studied FlowMatrix and study the system again for 10 days and record some results. We find that the anomaly detection based FlowMatrix is capable of detecting various attacks either known or unknown attacks in the computer network but it may give various false positives.

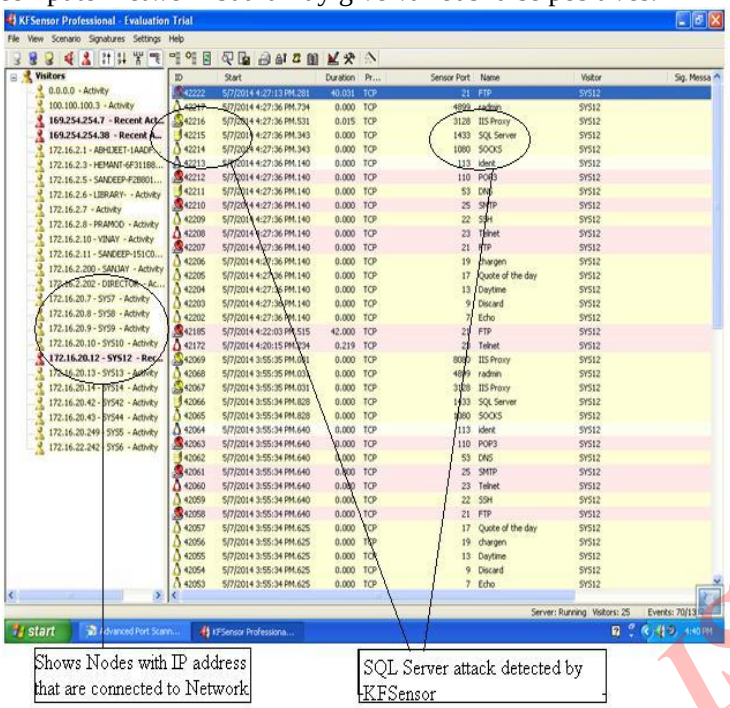


Figure2: Network activities of all the nodes and attacks by the three nodes 172.16.20.10, 172.16.20.11, 172.16.20.12

Phase III: in this phase we installed both KFSensor and FlowMatrix and study a system again for 10 days. Here we find the different results that attacks which cannot be detected by KFsensor and detected by FlowMatrix. The combine logs is generated which capture the attacks and than administrator can take corrective actions over the attacks.
Description of all three phases and its result given as

4.1 Analysis of Phase I
There are three nodes for attack with IP address as 172.16.20.10, 172.16.20.11 and 72.16.20.12 and the node with IP address 172.16.20.13 is server FlowMatrix and the node with IP address 172.16.20.14 is server as KFSensor. We create network traffic by the help of different tools like attack ping, port scanner, free SNMP etc. when we attack using these tools some logs are generated. Through log we found that KFSensor generate the records of only those nodes that are directly connected or communicated with the server and ignore rest nodes. This is the main disadvantage of IDS which include only honeypot technology. Hense, we have also use flowmatrix which is anomaly based IDS. We found some differences in the anomaly graph of FlowMatrix if the attacks takes place at some other point in the network which are not captured by KFSensor. Figure 2 shows the network activity of all the nodes and the attacks made by three nodes.
Both Intrusion Detection System FlowMatrix and KFSensor has their own way of detecting attacks. KFSensor based on honeypot technology can attract the attacker towards itself. Figure 3 given below shows that the FlowMatrix is based on anomaly based methodology and it is capable of detecting all types of attacks in network.

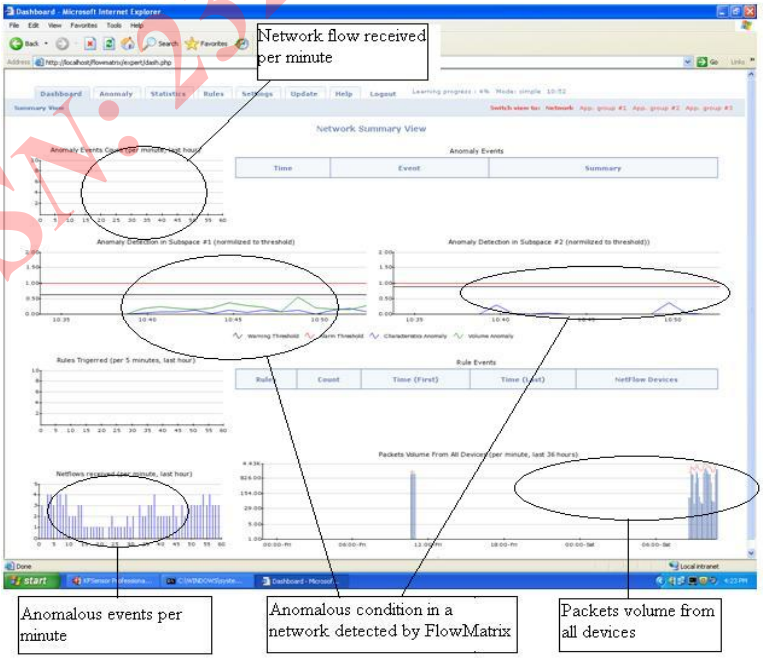


Figure 3: FlowMatrx (Anomaly Based IDS)

4.1.1 Analysis of KFSensor at Personal networks

We have not only analyzed KFSensor only to the network which we have created at the network lab but also to other different network such as to Personal network. We have analyzed it on 3rd May in between 03-04 p.m. and get some valid results, some attacks were also noticed

ISSN: 2321-9653

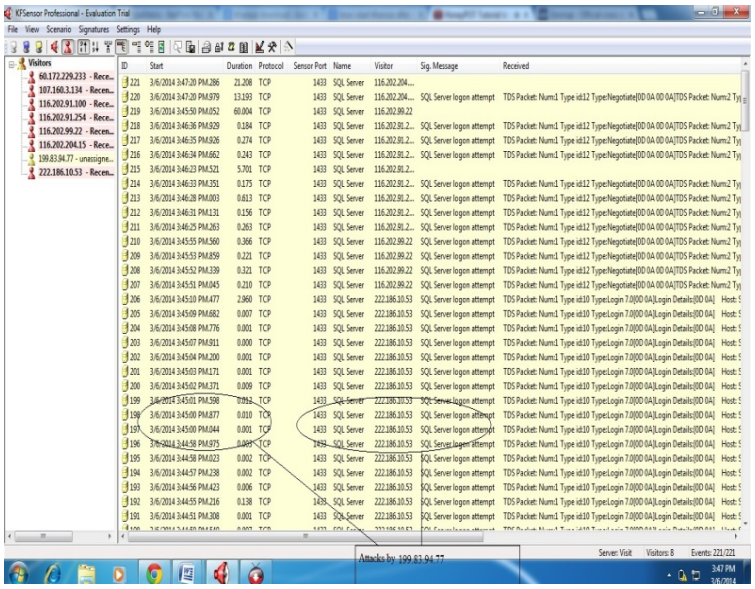


Figure 4: KFSensor at Personal networks

In the table 4 below we have analyze the following characteristics of KFSensor and conclude that KFSensor is a Host based Honeypot intrusion detection system which can attract the attacker towards itself to protect the organization from attack and block that user in future to enter the organization's premises by updating that user's signature into its database. It gives lesser false alarm but is highly vulnerable to taken over by bad guys and also they are not capable to detect attack from those user who do not directly communicate with it.

Properties	KFSensor
Detect novel attacks	Yes
Sends Alert by Email	Yes
Easy Administration	Yes
User Friendly	Yes
System Requirements	Low
Detect attacks from other nodes which Don't Communicate to it	NO
Risk (Taken over by the bad guys)	Very High
False Alarm	Lesser
Host Based/Network Based	Host Based

Table 1: Characteristics observed through overall experiment of KFSensor

4.2 ANALYSIS OF PHASE 2

The detailed analysis of Phase 2 is given as-

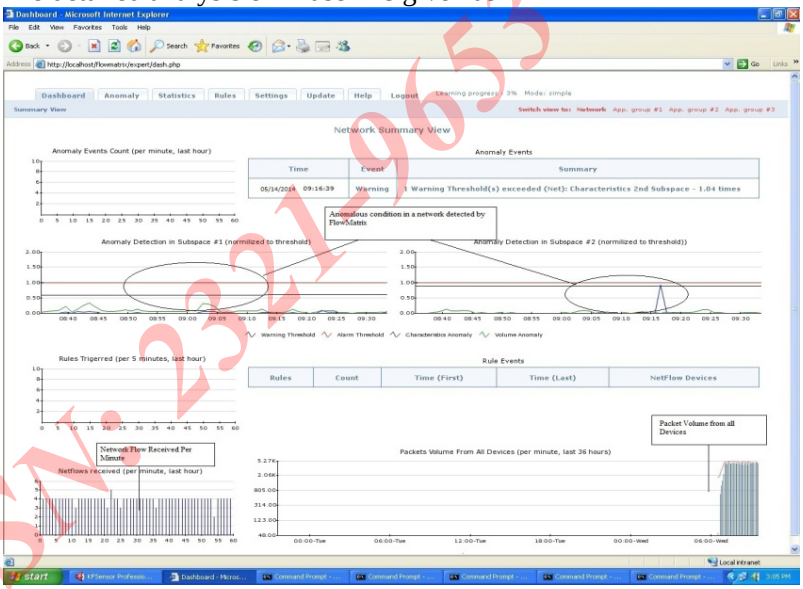


Figure 5: FlowMatrix showing the alert which is not capture by KFSensor

In phase 2 we have studied Flowmatrix and we find that it not only detect an attack where the systems are directly communicating with the server "where Flowmatrix is installed" but also, it can detect those attacks where the nodes are not directly communicating with server. This is the major advantage and main motive of hybridizing KFSensor with Flowmatrix.

Figure 6 shows the IDS KFSensor and the network activities on 14th May between 09 a.m. to 11:00 a.m

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

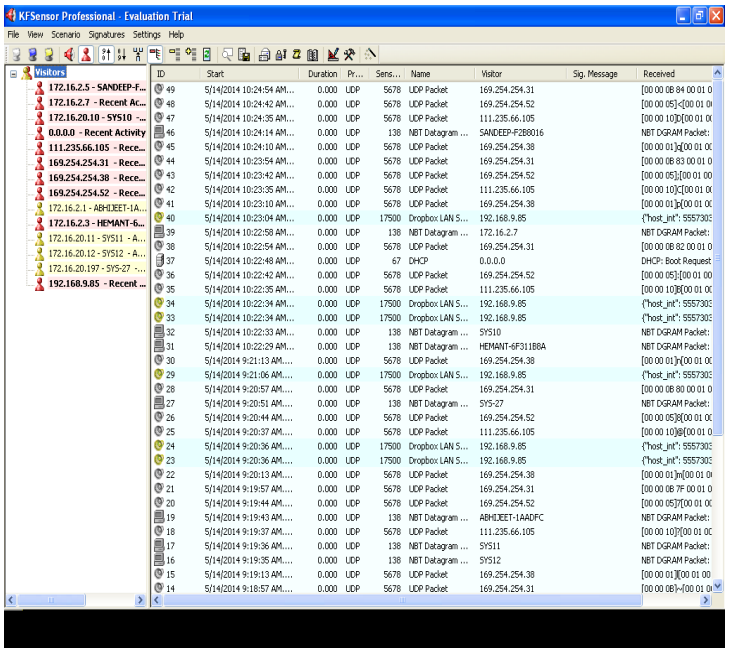
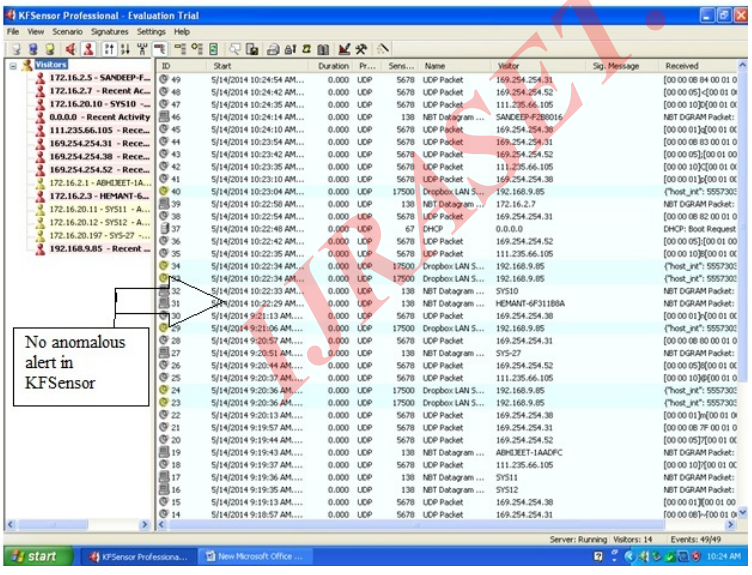


Figure 6: KFSensor detecting activities by only those node which directly communicate with it

We had run both Flowmatrix and KFSensor together but we can see that the results are entirely different in Flowmatrix and KFSensor. The alert in Flowmatrix is different from KFSensor. In figure 33 we can see both KFSensor and Flowmatrix together and find that it is Flowmatrix which is showing an alert however in the KFSensor there are no such warnings or alert.



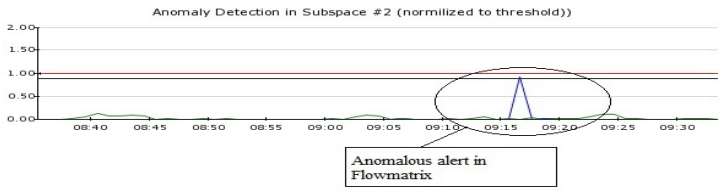


Figure 7: Comparison between KFSensor and Flowmatrix

Through the table below we can go through the characteristics we had gone through the complete experiment. Thus, we come to know that though Flowmatrix is more prone to unknown attack, they can detect more attacks than KFSensor

Properties	Flowmatrix
Detect novel attacks	Yes
Sends Alert by Email	No(Some Anomaly Based IDS do send Alerts by Email)
Easy Administration	Lesser than KFSensor
User Friendly	Yes
System Requirements	High
Detect attacks from other nodes which do not communicate to it	Yes
Risk (Taken over by the bad guys)	Very Low
False Alarm	Higher
Host Based/Network Based	Network Based

Table 2: Characteristics observed while doing experiments with Flowmatrix

4.3 ANALYSIS OF PHASE 3

In phase 3 we have studied both KFSensor and Flowmatrix together and find that if we used both KFSensor and Flowmatrix together it can became a much effective IDS. As through honeypot we can find out all those new attacks where an attacker directly communicates with KFSensor and through Flowmatrix we can detect attacks where nodes are directly or not directly communicate with flowmatrix. As in phase 1 we

ISSN: 2321-9653

have shown that KFSensor only recognize those attacks where a node communicate with it thus all other attacks goes undetected which are detected by Flowmatrix. Figure 32 shows that as the node with ip address 192.165.9.85 do attack to node with IP address 172.16.20.11 it gives an alert. However if the node try to do attack to some other network devices other than server then KFSensor will not give an alert to an administrator.

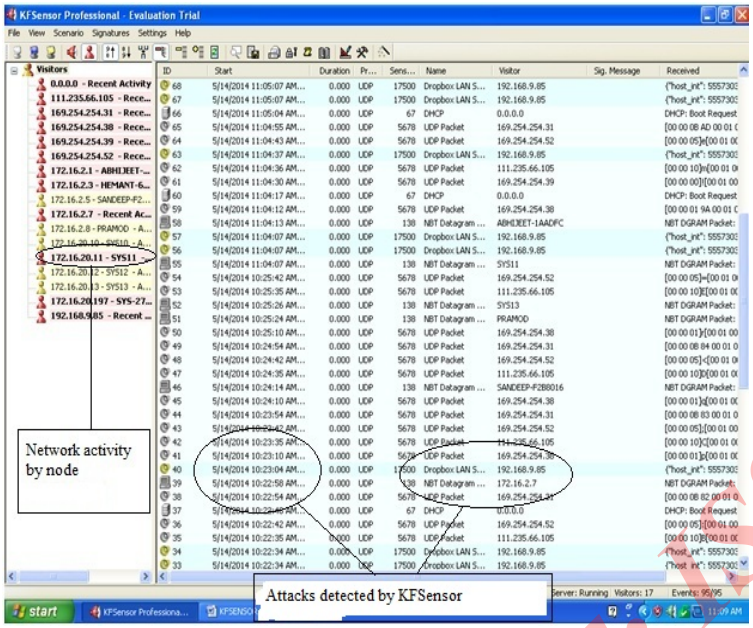


Figure 8: Network activity by Nodes and attacks detected by KFsensor

Thus we have deployed yet another IDS with KFSensor i.e. Flowmatrix which is capable of detecting those attacks in the network which goes undetected by KFSensor. Figure 33 will shows that an attack which goes undetected by KFSensor is detected by Flowmatrix.

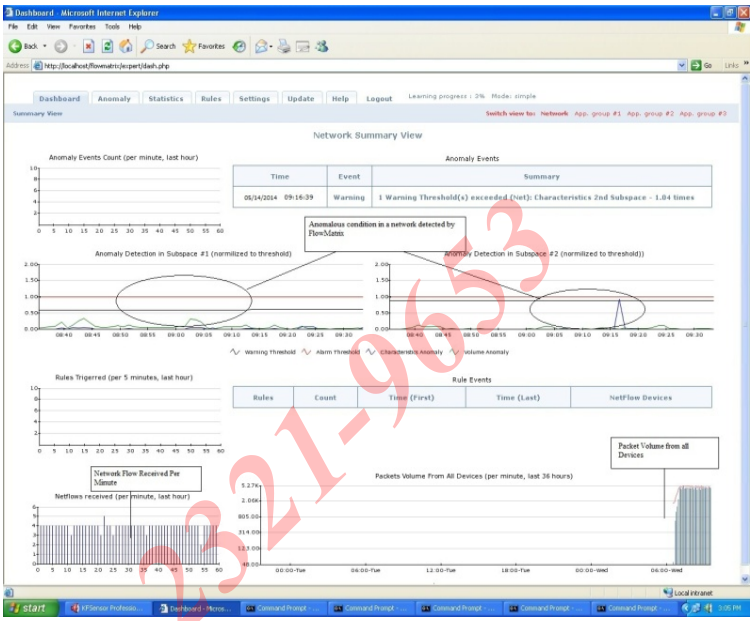


Figure 8: Attack which goes undetected by KFSensor is detected by Flowmatrix.

In Figure 9 we can find the combine log from KFSensor and Flowmatrix

ISSN: 2321-9653

Figure 9: Combine log from KFSensor and Flowmatrix

Properties	KFSensor	Flowmatrix
Detect novel attacks	Yes	Yes
Sends Alert by Email	Yes	No(Some Anomaly Based IDS do send Alerts by Email)
Easy Administration	Yes	Lesser than KFSensor
User Friendly	Yes	Yes
System Requirements	Low	High
Detect attacks from other nodes which do not communicate to it	NO	Yes
Risk (Taken over by the bad guys)	Very High	Very Low
False Alarm	Lesser	Higher
Host Based/Network Based	Host Based	Network Based

Table 3: Characteristics observed while doing experiments with KFSensor and FlowMatrix

Through the table above we can determine the characteristics of both KFSensor and Flowmatrix which we have analyzed throughout the experiments. We can see that the characteristics which are not good for KFSensor are good for Flowmatrix and the characteristics which are not good for Flowmatrix are good for KFSensor.

CONCLUSION:

We have developed an improved framework for hybrid intrusion detection system in cloud computing to ensure the confidentiality in organization. We have used two technologies for this framework- honeypot technology and anomaly based IDS. For the honey pot technology we have used KFSensor and for anomaly based IDS we have used Flowmatrix. We have given an algorithm and on that basis we designed an architecture and implement it as real time. We have studied the behavior of the implemented system and introduced various attacks which were detected by the system and alert was generated against it. The combined log generated can help the network administrator to take the corrective actions. The work can be further extended by developing a framework to incorporate the anomaly based attacks.

ISSN: 2321-9653

LIST OF REFERENCES:

[1]. Cloud Security Alliance: Top Threats to Cloud Computing V1.0. Available: http://www.cloudsecurityalliance.org/topthreats, 2010.

[2]. Dimitrios Zissis, Dimitrios Lekkas: Addressing Cloud Computing Security Issues, Future Generation Computer Systems Dec 2010, pp 583-592.

[3]. Meiko Jensen et. al. : On Technical Security Issues in Cloud Computing, IEEE International conference on Cloud Computing, 2009.

[4]. Lucian Popa, Minlan Yu et. al. : Cloud Police: Access Control out of the Network, Hotnets, Monterey, CA, USA, Oct 2010.

[5]. Seongwook Jin et. at. : Architectural Support for Secure Virtualization under a Vulnerable Hypervisor, Appears in the 44th Annual IEEE/ACM International Symposium on Microarchitecture, Porto Alegre, Brazil, Dec 2011.

[6]. Zhi-Hong Tian et. at. : An architecture for intrusion detection using honeypot, International Conference on Machine Learning and Cybernetics, IEEE, Nov 2003, pp. 2096-2100.

[7]. Kai Hwang et. at. : Defending Distributed Systems Against Malicious Intrusions and Network Anomalies, Parallel and Distributed Processing Symposium, Proceedings. 19th IEEE International, 2005.

[8]. J. Gomez et. at. : Design of a Snort based Hybrid Intrusion Detection System, International Work-Conference on Artificial Neural Networks, Part- II, 2009. pp 515-522.

[9]. Emmanuel Hooper, An Intelligent Intrusion Detection and Response System Using Hybrid Ward Hierarchical Clustering Analysis, International Conference on Multimedia and Ubiquitous Engineering, IEEE, 2007, pp 1187-1192.

[10]. Prof. Smita Jawale et. at. : Intrusion Detection System using Virtual Honeypots, International Journal of Engineering Research and Applications, Mar 2012, pp 275-279.

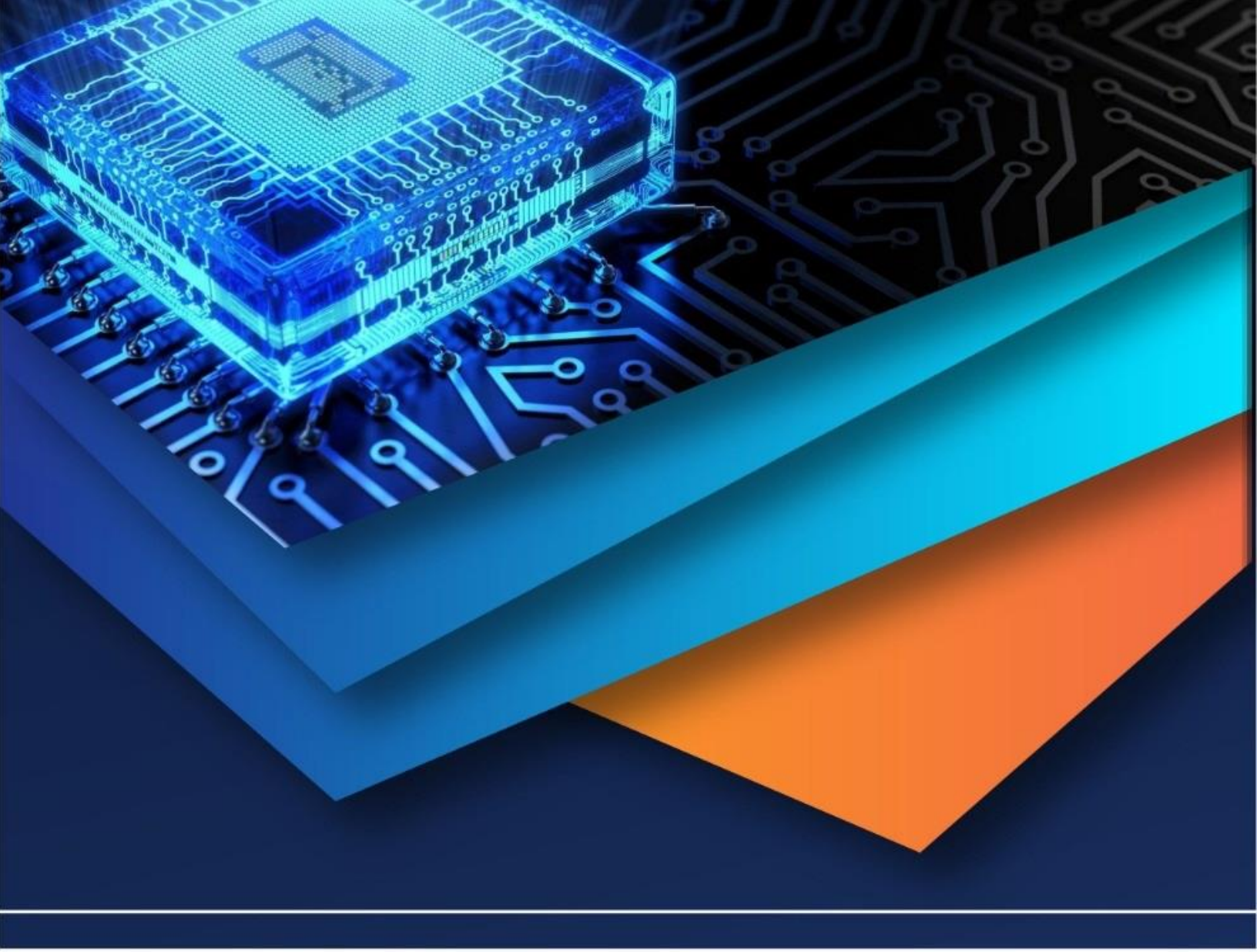
[11]. CISCO: Packet Tracer 6.0 Brochure, Available:http://www.cisco.com/web/learning/netacad/downloads/pdf/PacketTracer6_0_Brochure_0707.pdf, 2013.

[12]. CISCO: Cisco Packet Tracer Data Sheet, Available:http://www.cisco.com/web/learning/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf

[13]. Introduction to KFSensor- A windows based honeypot IDS, Available: http://blogs.microsoft.co.il/, Oct 2012.

[14]. KFSensor- A windows based honeypot IDS download, Available: http://www.keyfocus.net.

[15]. AKMA Lab: FlowMatrix download, Available:http://www.akmalabs.com/downloads_flowmatrix.php, 2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY