An Improved Hybrid Intrusion Detection System in Cloud Computing

Ajeet Kumar Gautam
School of Information and Communication Technology, Gautam Budha University, Greater Noida, UP, INDIA

Vidushi Sharma, Ph.D
School of Information and Communication Technology, Gautam Budha University, Greater Noida, UP, INDIA,

Shiva Prakash
Department of Computer Science & Engineering, Madan Mohan Malaviya Engineering College, Gorakhpur, INDIA,

ABSTRACT
Today, ssecurity is a major concern. Cloud computing and Intrusion Detection and Prevention Systems are one such measure to mitigate these attacks. Different researchers have proposed different IDSs time to time some of these IDS's combine features of two or more IDSs which are called as Hybrid Intrusion Detection Systems. Most of the researchers combine the features of Signature based detection methodology and Anomaly based detection methodology. For a signature based IDS if an attacker attacks slowly and organized, the attack may go undetected through the IDS, as signatures include factors which are based on duration of the events and the actions of attacker do not match. Sometimes, for an unknown attack there is no signature updated or an attacker attack in the mean time when the database is updating. Thus, signature-based IDS fail to detect unknown attacks. Anomaly based IDS suffer from many false-positive readings. Thus there is a need to hybridize those IDS which can overcome the shortcomings of each other. In this paper we proposed a new approach to IDS (Intrusion Detection System) which is more efficient than the traditional IDS (Intrusion Detection System). The IDS is based on Honeypot Technology and Anomaly based Detection Methodology. We have designed Architecture for the IDS in a packet tracer and then implemented it in real time. We have discussed experimental results performed both the Honeypot and Anomaly based IDS have some shortcomings but if we hybridized these two technologies, the newly proposed HIDS is capable enough to overcome these shortcomings with much enhanced performance. In this paper, we present a modified Hybrid Intrusion Detection System (HIDS) that combines the positive features of two different detection methodologies - Honeypot methodology and anomaly based intrusion detection methodology. In the experiment we run both the Intrusion Detection System individually first and then together and record the data from time to time. From the data we can conclude that the resulting IDS is much better in detecting intrusions from the existing IDSs.

Keywords - Intrusion Detection and Prevention System (IDPS), Hybrid Intrusion Detection System, KFSensor, FlowMatrix, Paket Tracer

1. INTRODUCTION
Cloud computing is a recent research topic in the area of computing environment[1][2][3]. Several researchers have made contribution. Almost all the organizations whether small scale organizations or large scale organizations, they are making use of cloud technology but due to security factors[4][5] The technology is still not working. Many researchers have gone through the security issues in cloud computing. Wang Jun-Jie and Mu Sen [6] discussed various security issues in cloud computing and its countermeasures. However, the paper is very theoretical and there are no methods that can validate his work. Thereafter Meiko Jensen, J¨org Schwenk, Nils Gruschka and Luigi Lo Iacono [7] discussed the technical security issues in cloud computing. To provide security in cloud computing there are different areas in it such as ensuring confidentiality of virtual machines, compromised hypervisor, malicious insider and other network attacks discussed in the next chapter. Different researchers propose different ideas to mitigate risks such as Jinzhu Kong [8] discussed how to protect the confidentiality of virtual machines against distrusted host. The researcher acquaints the concept of virtualization and deals with the security of the virtualized system. Many researchers propose models to mitigate network attacks in cloud computing like Lucian Popa, Minlan Yu, Y. Steven Ko, Sylvia Ratnasamy and Ion Stoica [9] design a hypervisor based CloudPolice and Saketh Bharadwaja, Weiqing Sun, Mohammed Niamat and Fangyang Shen [10] design Collabra, which is a Xen hypervisor based collaborative intrusion detection system. Later on Jakub Szefer and B. Ruby Lee [11] works in the area which is entirely different from all other researches they put forward the case of hardware protection of guest Virtual Machines from compromised hypervisors.

Other researcher's work in developing an Intrusion detection and prevention system to stop intruders from attacking the organization's network. They used a hybrid detection methodology in intrusion detection and prevention system. Dwen Ren Tsai, Wen Pin Tai, and Chi-Fang Chang [12] proposes a hybrid intelligent intrusion detection system to recognize novel attacks through data mining of the behaviors of attacks. However, this hybrid system has partly solved the problem to recognition novel attacks of intrusion later Vaidehi Kasarekar and Byrav Ramamurthy in [13] developed a Hybrid Real Time Agent Based Intrusion Detection and Response System to increase security in wireless networks.

Thereafter, a lot of research is being done to combine a signature based IDS and an anomaly based IDS like Kai Hwang, Ying Chen, Hua Liu [14] proposes CAIDS (Cooperative anomaly and intrusion detection system). CAIDS integrates two different detection engines NIDS (Network Intrusion Detection System) and ADS (Anomaly Detection System). Similarly Yu-Xin Ding, Min Xiao and AI-Wu Liu [15] have done research and implementation on snort-

based hybrid intrusion detection system. The researchers combine misuse detection system and anomaly detection system. They make use of SNORT for misuse based detection system. Thus, we can see that different researchers incorporate different methodology in hybrid detection system. Working in same direction Xuanwu Zhou, Xiaoyuan Yang, Ping Wei and Yupuhu [16] developed a hybrid IDS scheme based on biological immunology and mobile agent that can be a solution to the security threats and system flaws from the transfer of immune pathological mechanisms into IDS but due to rapid development of intrusion and attack techniques the proposed IDS is vulnerable to new threats due to negligence to immune pathology. Later, Emmanuel Hooper [17] proposes an intelligent intrusion detection and response system using hybrid ward hierarchical clustering analysis and R Rangadurai Karthick, Vipul P. Hattiwale and Balaraman Ravindran[18] describe an adaptive network intrusion detection system, that uses a two stage architecture. In the first stage a probabilistic classifier is used to detect potential anomalies in the traffic. In the second stage a HMM based traffic model is used to narrow down the potential attack IP addresses.

approach solves the problems information overload, unknown attacks, false positives and false negatives later Guan Xin and Li Yun-Jie in 2010 [20] study the feasibility of honey pot technology and intrusion prevention system together and thus proposed a new intrusion prevention system model that is based on immune principle of intrusion prevention system and honeypot technology.

In the journal we have proposed a new architectural design to IDS (Intrusion Detection System) which is more efficient than the traditional IDS (Intrusion Detection System). The IDS is based on Honeypot technology [33][34] and Anomaly based Detection Methodology[35]. To implement such a system we have designed an architecture in the network lab and collect data to validate the proposed Hybrid intrusion Detection System.

2. ARCHITECTURAL DESIGN

We have considered a network, simulated and configured first on packet tracer[36][37] and then implemented it in real time to analyze the network properly, so that while developing it in real time it became easy to configure all the network devices. Figure 1 shows the network

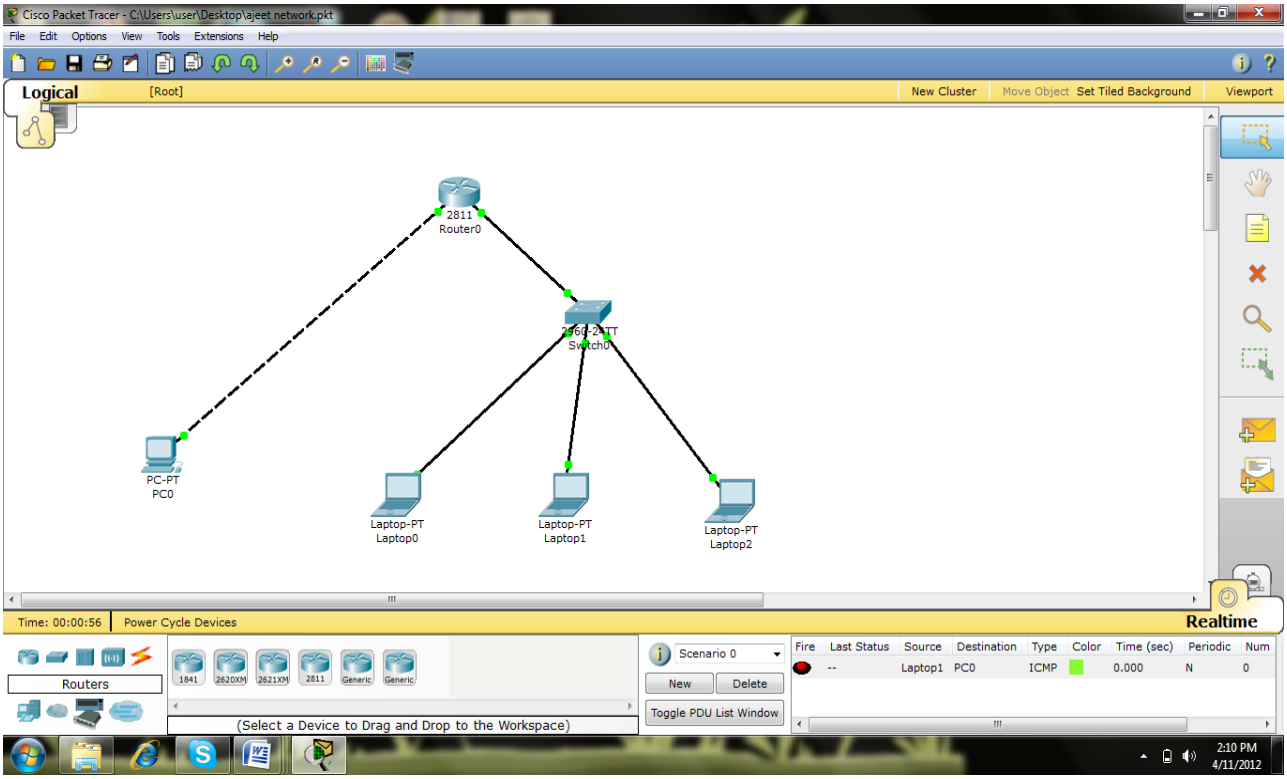


Figure 1: Network configured in packet tracer

Many researchers integrate honeypot technology to intrusion detection system. They attract an attacker towards it and work in cooperation with Fire Wall. The system will refuse the visit of the intruder whose IP address is set in the Fire Wall as blacklist by the honeypot. In this direction Zhi-Hong Tian, Bin-Xing Fang and Xiao-Chun Yun [19] design AAIDHP (An Architecture for Intrusion Detection using Honey Pot). The

configured in packet tracer. The network consists of three nodes and a server. Server is connected to the router to route packets to different networking device and to connect LAN to WAN. Behind the routers we are using 4 nodes, one is made into a server and the other three are connected to a router through a switch. The server communicates with the nodes

with the help of the router via switch. In a server we have installed two types of Intrusion Detection Systems (IDSs). One of the systems is based on honeypot technology and the other is anomaly based IDS. Honeypot can attract the attacker whenever it tries to perform a malicious activity across the network and later with this system we can make their signatures and update these signatures in the database whereas anomaly based detection system can analyse the network and record the normal network traffic and whenever it finds any anomalous behavior it throws an alert. Both these systems can strongly restrict an attacker while coming to your private network. For a honeypot technology we are using KFSensor and for anomaly based IDS we are using FlowMatrix.

3. RESULT AND ANALYSIS

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

Phase 1: In phase 1 we have studied KFSensor and analyzed a system for 10 days and record some results. Here we find that though KFSensor is capable to detect those attacks for which the different systems directly interact with it but, it cannot identify those attacks which are done by the systems that are not directly linked by it.

Phase 2: In phase 2 we have studied FlowMatrix and analyze a system again for 10 days and record some results. We found that FlowMatrix is capable of detecting various attacks either know attacks or unknown attacks in the network, however it does not attract a attacker like KFSensor do, more over it may give various false positives.

All the three phases are described below in details and there results are displayed.

3.1 Analysis of phase 1

There are three nodes for attack or to create network traffic. Which have an IP address as 20.1.1.20, 20.1.1.30 and 20.1.1.40 and the node with IP address 10.1.1.25 is server with FlowMatrix and the node with IP address 10.1.1.30 is server with KFSensor. We have created network traffic through different tools such as Attack Ping, Free Port Scanner, Free SNMP etc. Here we have used many more attacking tools to attack at different networking devices such as router, switch, server and other nodes. While attacking from these tools some logs are generated. Through the log we found that KFSensor generate records of only those nodes which are directly communicating with the server and ignore the rest of the nodes. This is the major drawback in IDS which incorporate only honeypot technology. Since, we have also installed FlowMatrix which is anomaly based IDS we found some deviations in the anomaly graph in FlowMatrix if the attacks takes place at some other point in the network which are not recorded by KFSensor.

In the Figure 2 below shows the network activity of all the nodes and the attacks by the three nodes 20.1.1.20, 20.1.1.30 and 20.1.1.40.

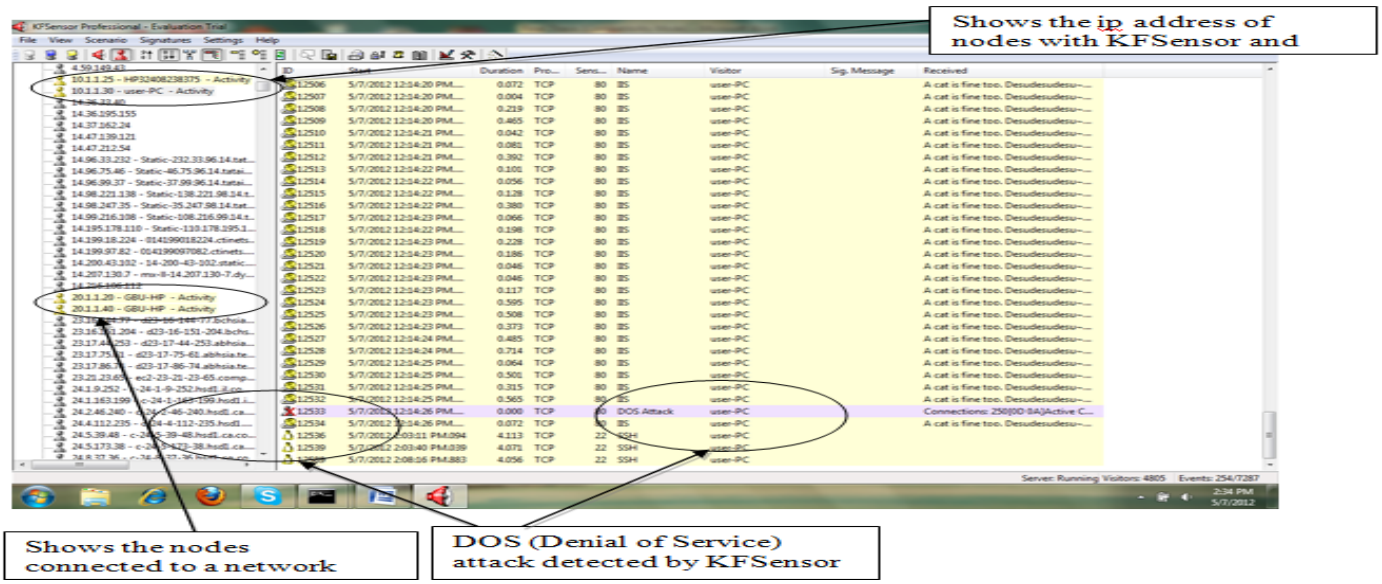


Figure 2: Network activity of all the nodes and the attacks by the three nodes 20.1.1.20, 20.1.1.30 and 20.1.1.40.

Phase 3: In phase 3 we have installed both KFSensor and FlowMatrix and analyse a system again for 12 days. Here we find different results that attacks which go undetected by KFSensor are detected by FlowMatrix and with KFSensor we can get some new definitions of attack in database. A combined log is generated which captures the attacks and the administrator can take corrective actions.

Both the ids KFSensor and FlowMatrix has their own way of detecting attacks In KFSensor we can see that the honeypot can attract an attacker towards itself thus with KFSensor we not only detect an attack whose definitions are already exists in its database but also detect new attacks through honeypot technology and later make signatures of these attack and update to database.

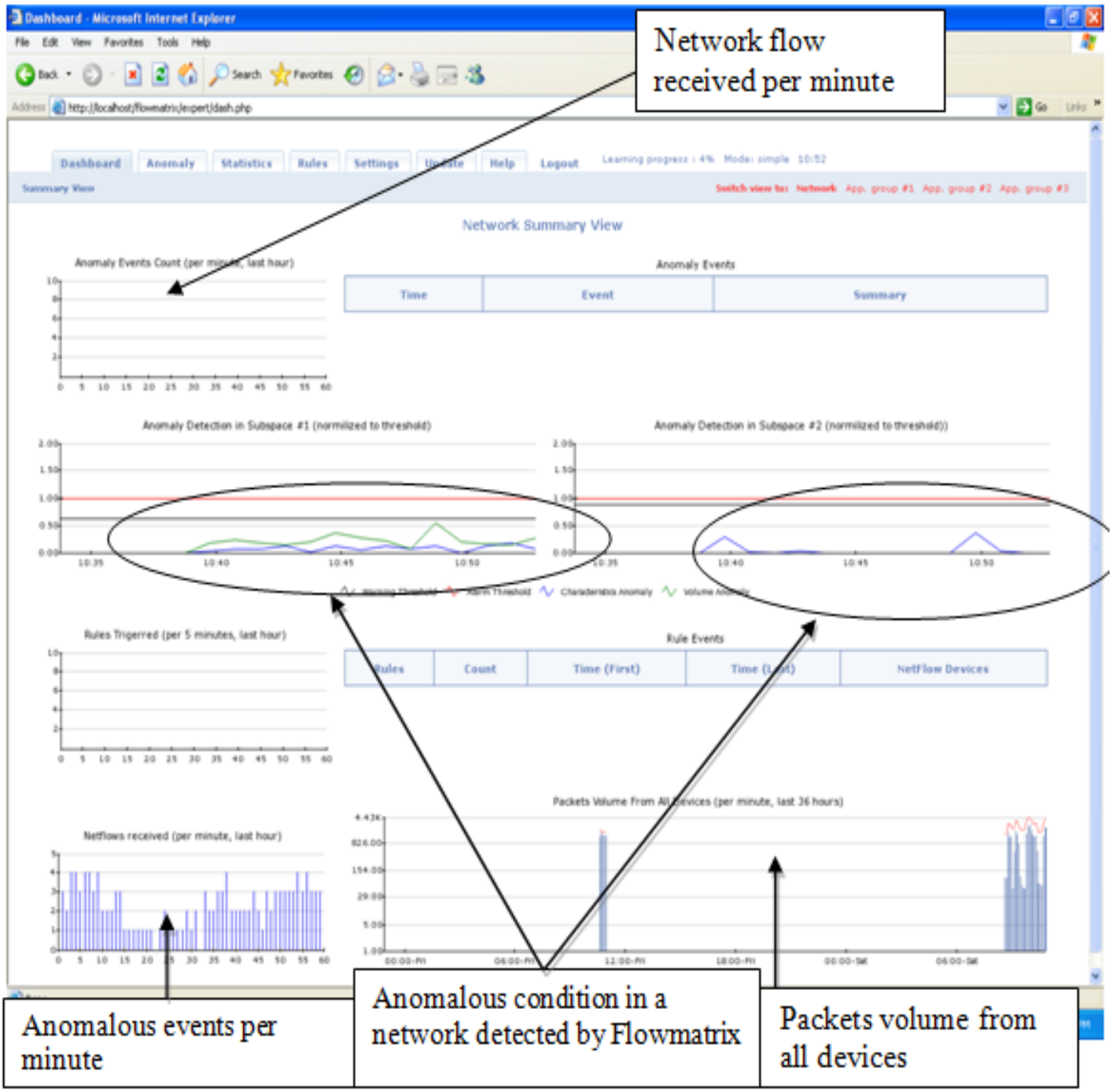


Figure 3: Anomaly based IDS- FlowMatrix

Drawback of honeypot is that they can only track and capture activity that directly interacts with them. They cannot detect attacks against other systems in the network. In Figure 3 below we can see the ids which is on anomaly based methodology "FlowMatrix" . FlowMatrix is capable of detecting all types of attack in the network.

3.1.1. Analysis of KFSensor at GBU networks

We have not only analyzed KFSensor only to the network which we have created at the network lab but also to other network. We have analyzed it on 4rth may in between 10-11 p.m. and get some valid results, some attacks were also noticed.

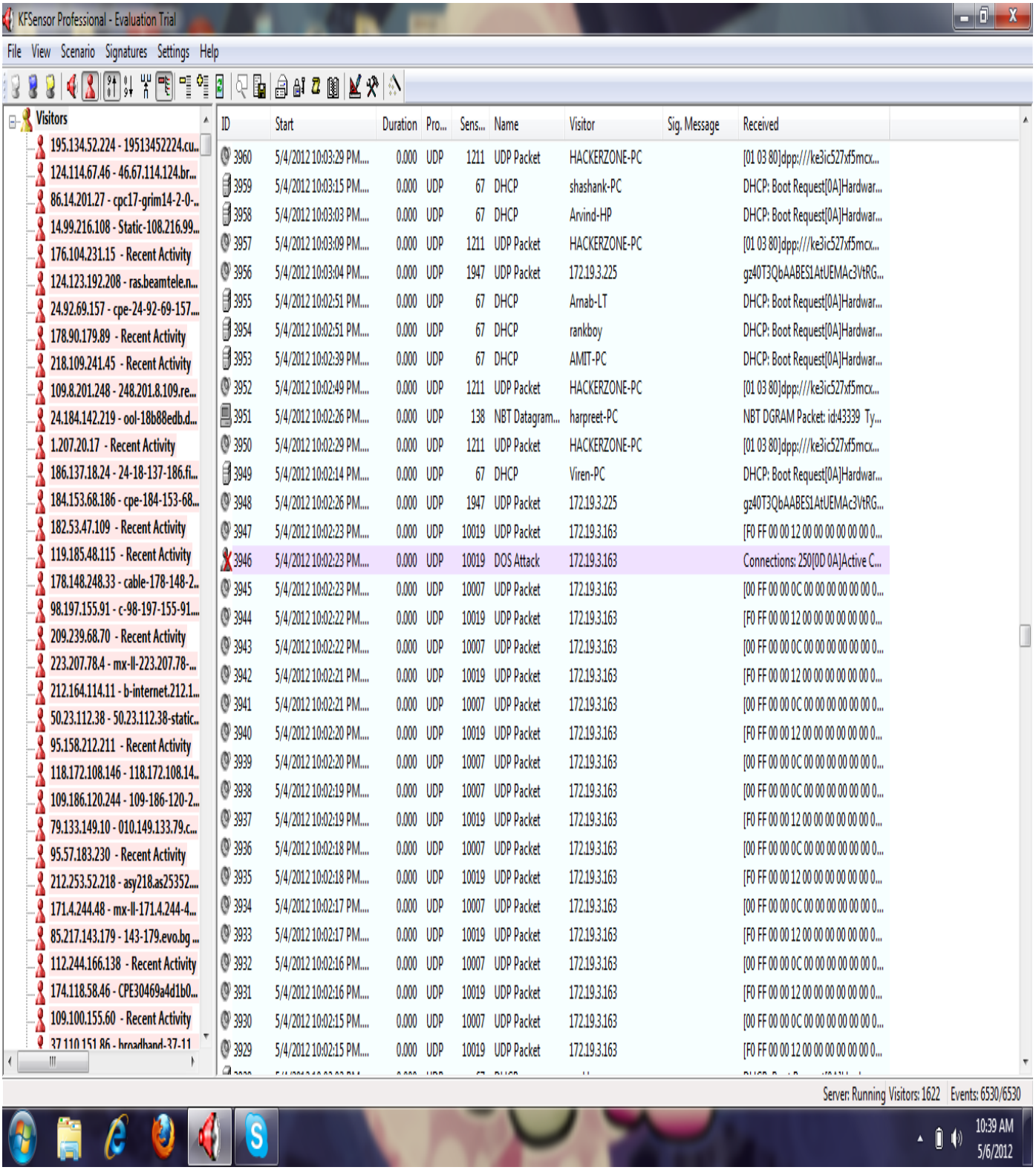


Figure 4: Logs generated by KFSensor when connected to Gautam Buddha University, Greater Noida, INDIA network

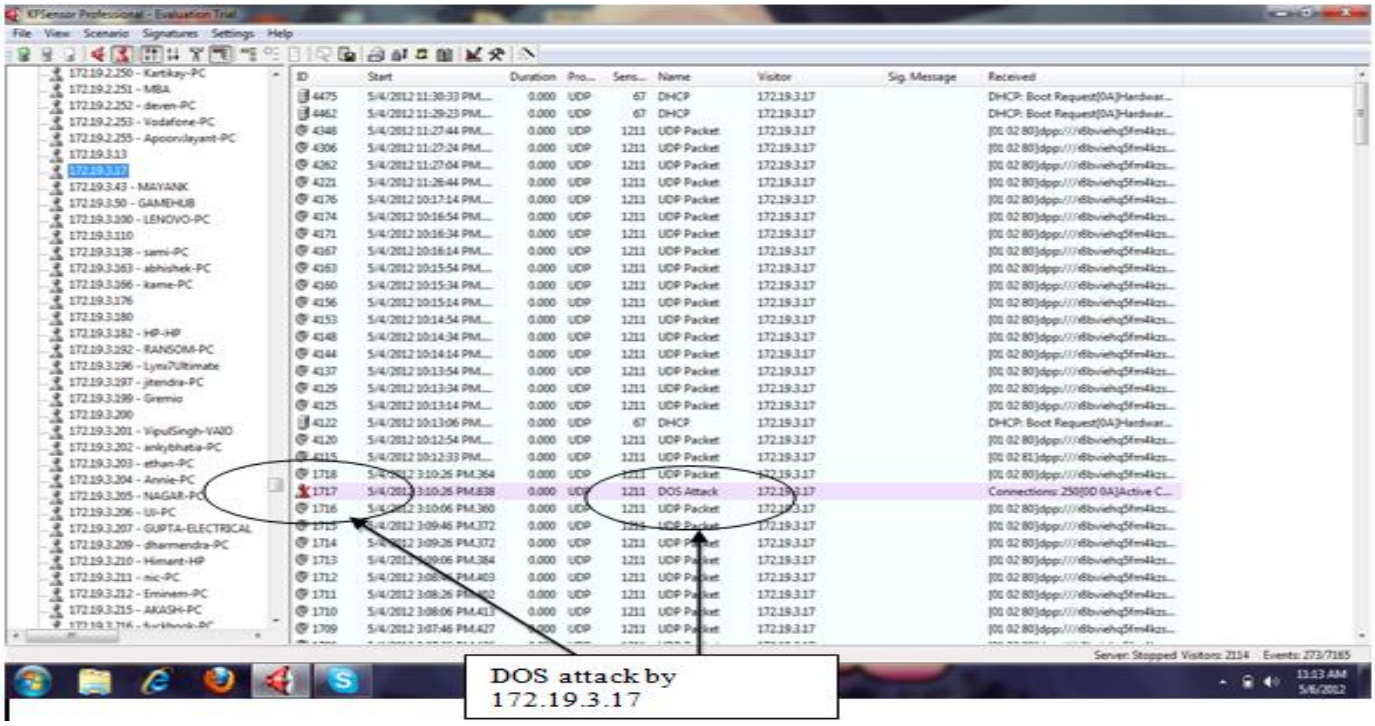


Figure 5: Attack noticed when connected to GBU main

In the table 1 below we have analysed 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 be taken over by bad guys and also they are not capable to detect attack from those users who do not directly

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 do not communicate to it	NO
Risk (Taken over by the bad guys)	Very High
False Alarm	Lesser
Host Based/Network Based	Host Based

3.2 Analysis of phase 2

The detailed analysis of Phase 2 is given as-

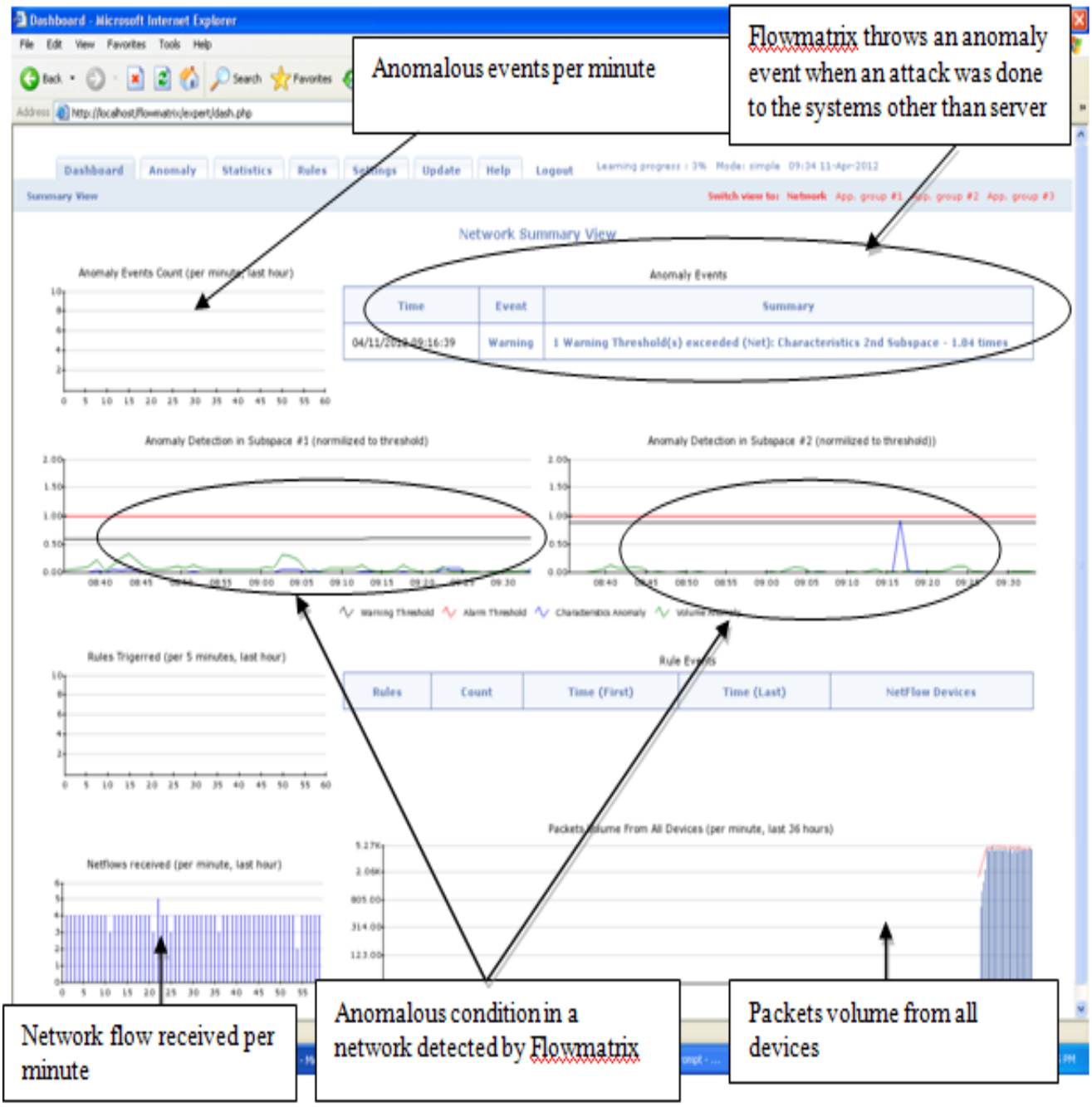


Figure 6: FlowMatrix showing the alert which is not capture by KFSensor

In phase 2 we have studied FlowMatrix and we find that it not only detects 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 7 shows the ids KFSensor and the network activities on 11th April between 11 a.m. to 1:05 p.m.

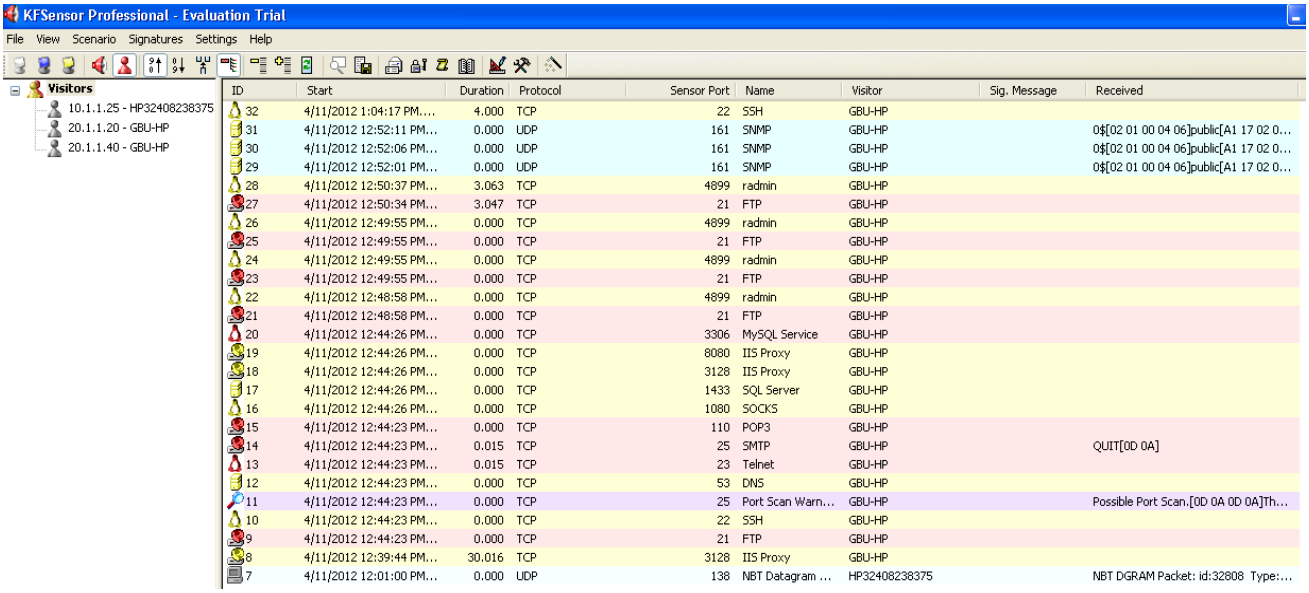


Figure 7: KFSensor detecting activities by only those node which directly communicate with it

KFSensor detecting activities by only those node which directly communicate with it We ran 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 8 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.

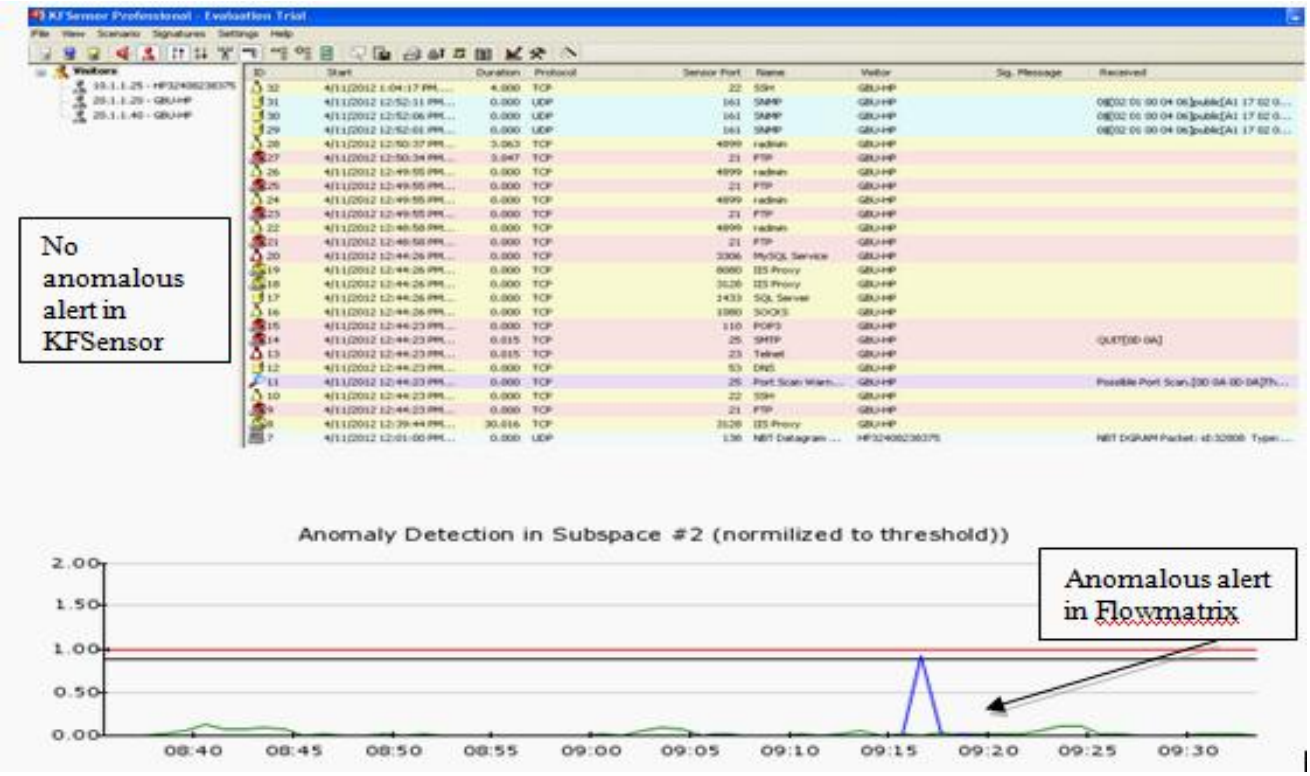


Figure 8: Comparison between KFSensor and FlowMatrix

Through the table 2 below we can go through the characteristics we had gone through the complete experiment.

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

Thus, we come to know that though FlowMatrix is more prone to unknown attack, yet they can detect more attacks than KFSensor

3.3 Analysis of phase 3

In phase 3 we have studied both KFSensor and FlowMatrix together and found that if we use both KFSensor and FlowMatrix together, it can become 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 indirectly communicating with FlowMatrix. In phase 1 we 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 9 shows that as the node with ip address 20.1.1.20 do DoS attack to node with IP address 10.1.1.25 it gives an alert. However if the node try to do DoS attack to some other network devices other than server then KFSensor will not give an alert to an administrator.

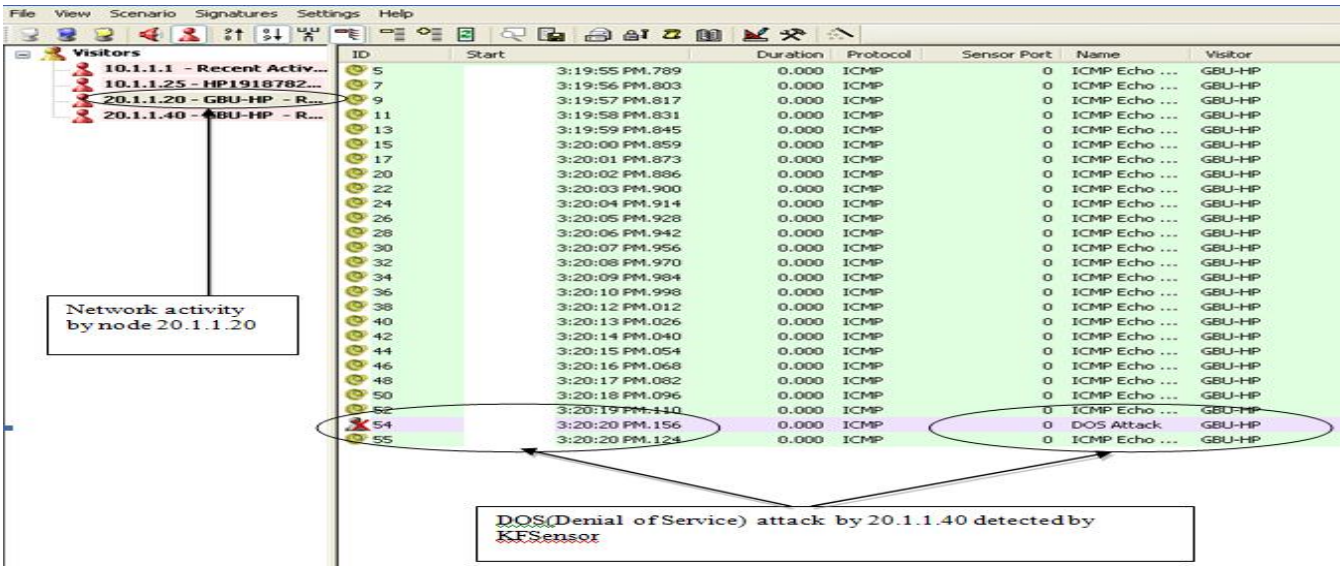


Figure 9: Node with IP address 20.1.1.20 does DoS attack to node with IP address 10.1.1.25

Thus we deploy yet another ids with KFSensor i.e. FlowMatrix which is capable of detecting those attacks in the network which goes undetected by KFSensor. Figure 10 will shows that an attack which goes undetected by KFSensor is detected by FlowMatrix.

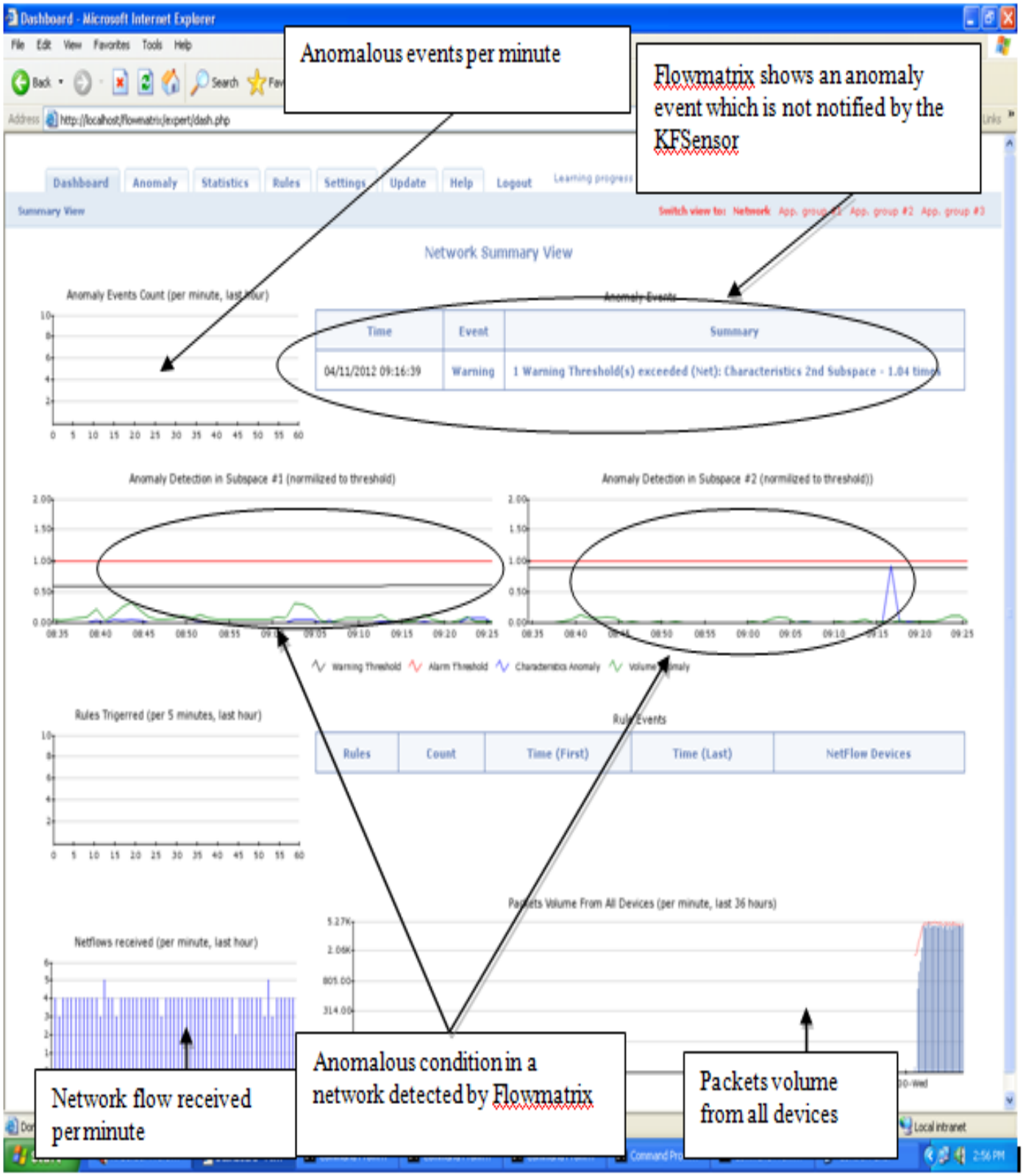


Figure 10: Attack which goes undetected by KFSensor is detected by FlowMatrix.

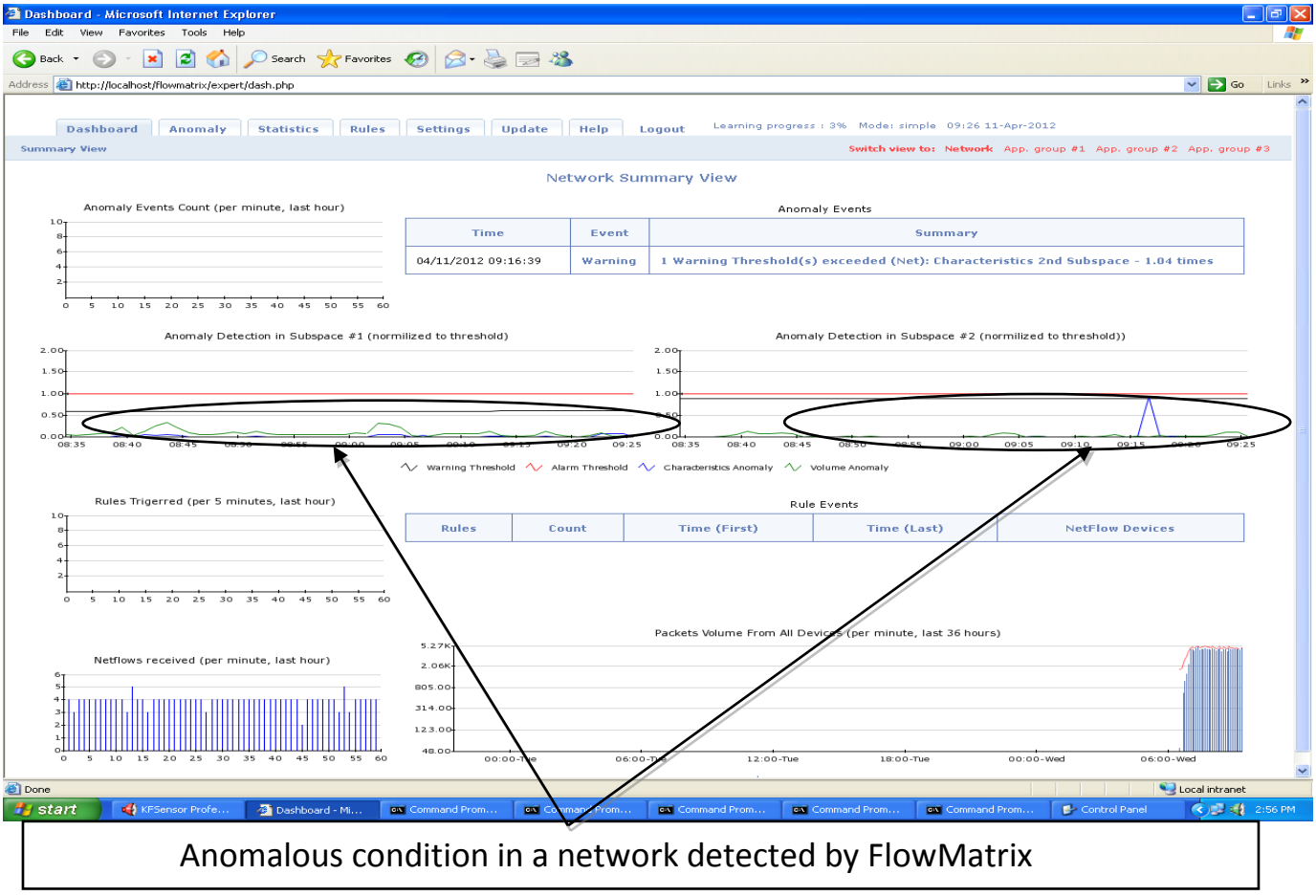
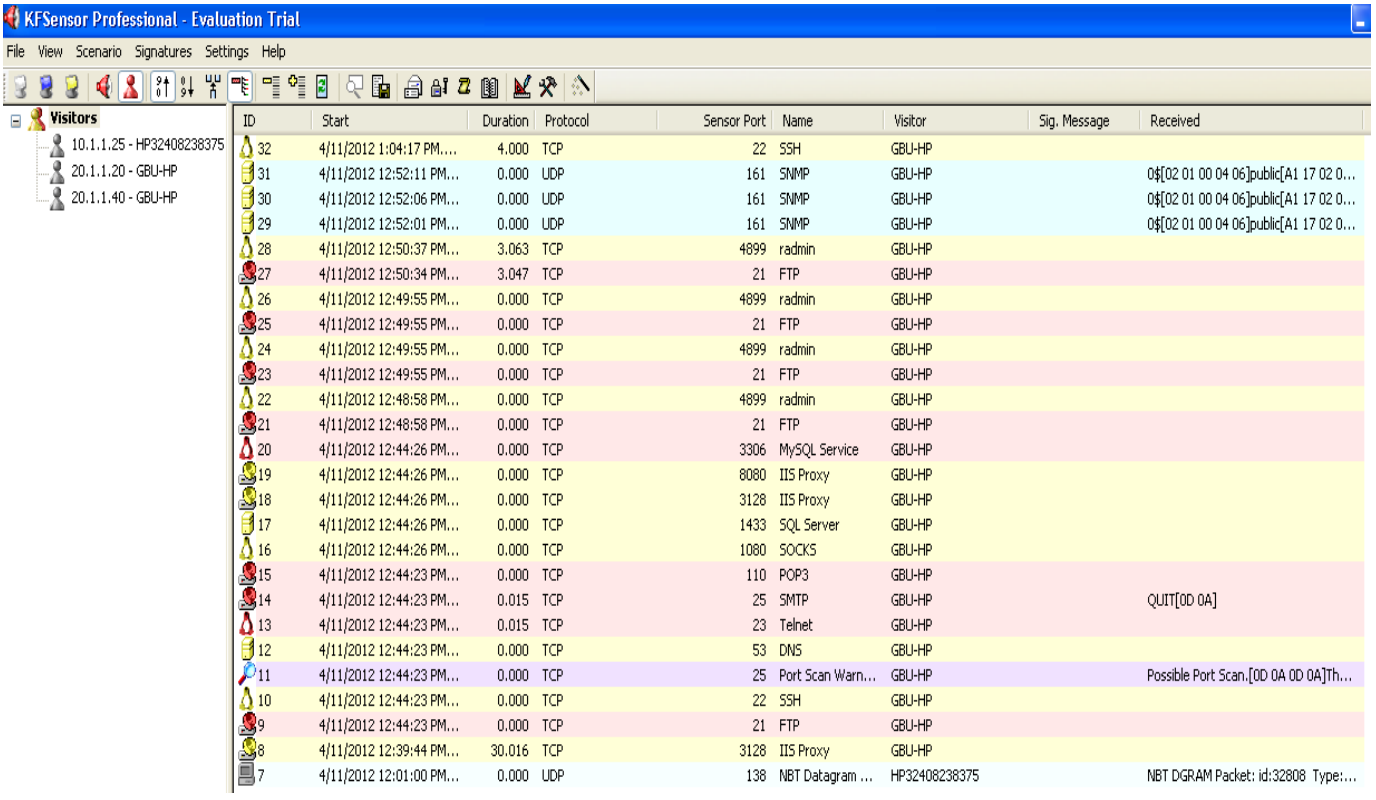


Figure 11: Combine log from KFSensor and FlowMatrix



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

Through the table 3 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. Thus, if we merge both the systems together we can get the better detection system also KFSensor is Host based detection system and FlowMatrix is Network based detection system thus if we deploy both these system together we can get fully secured intrusion detection system.

4. 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.

REFERENCES

[1] Cloud Security Alliance (2010). "Top Threats to Cloud Computing V1.0" Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[2] Wang Jun-Jie and Mu Sen, "Security Issues and Countermeasures In Cloud Computing", International Conference On Grey Systems And Intelligent Services (Gsis), in *Proc*. in *IEEE*, 2011, Pp. 843-846.

[3] Meiko Jensen, J¨Org Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", International Conference On Cloud Computing, in *Proc*. in *IEEE* 2009, Pp. 109-116.

[4] Jinzhu Kong, "Protecting the Confidentiality of Virtual Machines Against Untrusted Host", International Symposium on Intelligence Information Processing And Trusted Computing, in *Proc.* in *IEEE*, 2010, Pp. 364-368.

[5] Lucian Popa, Minlan Yu, Steven Y. Ko, Sylvia Ratnasamy, and Ion Stoica, "Cloudpolice: Taking Access Control Out of The Network", Proceedings of The Ninth ACM Sigcomm Workshop On Hot Topics In Networks, ACM. 2010.

[6] Saketh Bharadwaja, Weiqing Sun, Mohammed Niamat and Fangyang Shen, "Collabra: A Xen Hypervisor Based Collaborative Intrusion Detection System", in International Conference on Information Technology: New Generations in *Proc.* in *IEEE*, 2011, Pp. 695-700.

[7] Jakub Szefer, Ruby B. And Lee, "a case for hardware protection of guest virtual machines from compromised hypervisors in cloud computing", International Conference On Distributed Computing Systems Workshops in *Proc.* in *IEEE*, 2011, Pp. 248-252

[8] Kai Hwang, Ying Chen and Hua Liu, "Defending Distributed Systems Against Malicious Intrusions and Network Anomalies", International Workshop on Security in Systems and networks in *Proc.* in *IEEE*, 2005.

[9] Yu-Xin Ding, Min Xiao and Ai-Wu Liu, "Research and Implementation On Snort-Based Hybrid Intrusion Detection System" in International Conference On Machine Learning And Cybernetics, in *Proc.* in *IEEE*, 2009, Pp. 1414-1418.

[10] Zhi-Hong Tian, Bin-Xing Fang and Xiao-Chun Yun, "An architecture for intrusion detection using honey pot", International Conference on Machine Learning and Cybernetics, in *IEEE*, (4) , Pp. 2096-2100.

[11] Guan Xin and Li Yun-jie, "An new Intrusion Prevention Attack System Model based on Immune Principle", International Conference on e-Business and Information System Security (EBISS), in IEEE, 2010, Pp. 1-4.

[12] Roderick Douglas, "Lecture Notes on Cloud Technologies, Sheffield Hallam University, Sheffield, U.K. 2011.

[13] Andy Bechtolsheim (2008). "Cloud computing", Available: http://netseminar.stanford.edu/seminars/Cloud.pdf

[14] F5 Networks (2009). "Cloud Computing Solutions" Available: http://www.f5.com/solutions/cloud-computing/

[15] Cisco (2004) "Cloud", Available: Http://Www.Cisco.Com/Web/Solutions/Trends/Cloud /Index.Html

[16] Craig Baldinng (2008). "Itg2008 World Cloud Computing Summit", Available: Http://Cloudsecurity.Org/

[17] Roderick Douglas, "Lecture Notes on Cloud Technologies, Sheffield Hallam University, Sheffield, U.K. 2011.

[18] Reese, George (2009) "Cloud Application Architectures", O'reilly Media Available: http://shop.oreilly.com/product/9780596156374.do

[19] Rittinghouse, John (2009) "Cloud Computing: Implementation, Management, And Security" Available: http://lawlist.law.suffolk.edu/highlights/stuorgs/jhtl/book_reviews/2009_2010/Josh%20Matloff%20Book%20Review.pdf

[20] Andrew J. Younge, Robert Henschel, James T. Brown, Gregor Laszewski, Judy Qiu and Geoffrey C. Fox, "Analysis Of Virtualization Technologies For High Performance Computing Environments", Fourth International Conference On Cloud Computing, in *Proc.* in *IEEE*, 2011, Pp. 9-16.

[21] Key Focus (2003) "KFSensor overview" Available: http://www.keyfocus.net/kfsensor/

[22] Key Focus (2003) "KFSensor overview" Available: http://www.keyfocus.net/kfsensor/download/

[23] AKMA Lab (2010). "FlowMatrix download" Available: http://www.akmalabs.com/downloads_flowmatrix.php

[24] CISCO (2008). "Packet Tracer 5.0 Brochure" Available: http://www.cisco.com/web/learning/netacad/downloads/pdf/PacketTracer5_0_Brochure_0707.pdf

[25] CISCO (2010). ""Cisco Packet Tracer Data Sheet" Available : http://www.cisco.com/web/learning/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf