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

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

IJRASET: ISSN: 2321-9653

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.

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

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

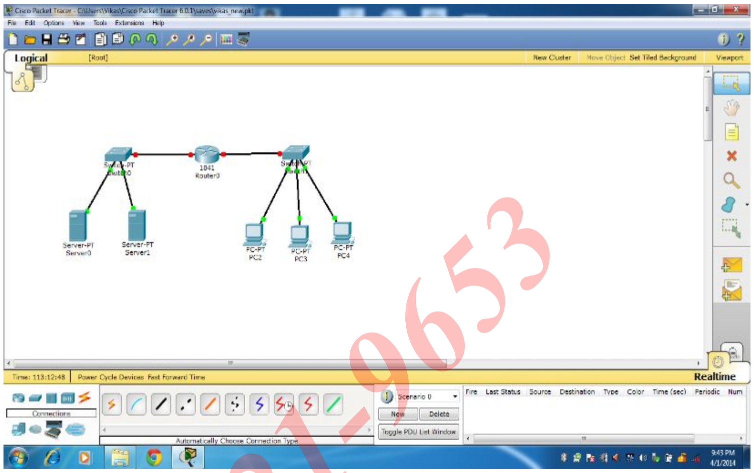


Figure1: Network Architecture

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:

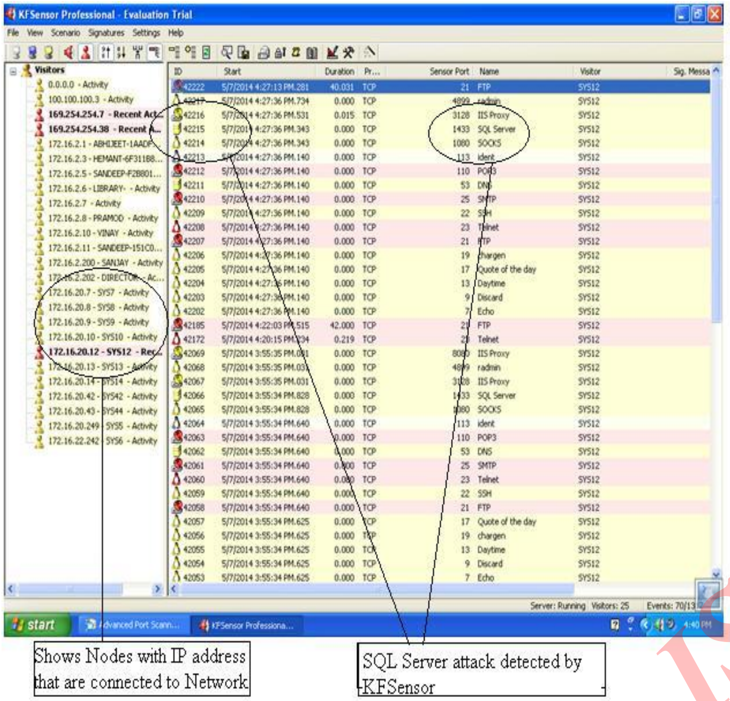
To validate our algorithm we have implement the system into three phases:

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.

IJRASET: ISSN: 2321-9653

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

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.


KFSensor Professional - Evaluation Trial

Visitors
- 0.0.0.0 - Activity
- 100.100.100.3 - Activity
- 169.254.254.7 - Recent Act...
- 169.254.254.38 - Recent A...
- 172.16.2.1 - ABHIJEET-1AADF...
- 172.16.2.3 - HEMANT-6F311B8...
- 172.16.2.5 - SANDEEP-F2B801...
- 172.16.2.6 - LIBRARY- - Activity
- 172.16.2.7 - Activity
- 172.16.2.8 - PRAMOD - Activity
- 172.16.2.10 - VINAY - Activity
- 172.16.2.11 - SANDEEP-151C0...
- 172.16.2.200 - SANJAY - Activity
- 172.16.2.202 - DIRECTOR - Ac...
- 172.16.20.7 - SYS7 - Activity
- 172.16.20.8 - SYS8 - Activity
- 172.16.20.9 - SYS9 - Activity
- 172.16.20.10 - SYS10 - Activity
- 172.16.20.12 - SYS12 - Rec...
- 172.16.20.13 - SYS13 - Activity
- 172.16.20.14 - SYS14 - Activity
- 172.16.20.42 - SYS42 - Activity
- 172.16.20.43 - SYS44 - Activity
- 172.16.20.249 - SYS5 - Activity
- 172.16.22.242 - SYS6 - Activity

ID	Start	Duration	Pr...	Sensor Port	Name	Visitor	Sig. Messa
42222	5/7/2014 4:27:13 PM.281	40.031	TCP	21	FTP	SYS12	
42217	5/7/2014 4:27:36 PM.734	0.000	TCP	4899	radmin	SYS12	
42216	5/7/2014 4:27:36 PM.531	0.015	TCP	3128	IIS Proxy	SYS12	
42215	5/7/2014 4:27:36 PM.343	0.000	TCP	1433	SQL Server	SYS12	
42214	5/7/2014 4:27:36 PM.343	0.000	TCP	1080	SOCKS	SYS12	
42213	5/7/2014 4:27:36 PM.140	0.000	TCP	113	ident	SYS12	
42212	5/7/2014 4:27:36 PM.140	0.000	TCP	110	POP3	SYS12	
42211	5/7/2014 4:27:36 PM.140	0.000	TCP	53	DNS	SYS12	
42210	5/7/2014 4:27:36 PM.140	0.000	TCP	25	SMTP	SYS12	
42209	5/7/2014 4:27:36 PM.140	0.000	TCP	22	SSH	SYS12	
42208	5/7/2014 4:27:36 PM.140	0.000	TCP	23	Telnet	SYS12	
42207	5/7/2014 4:27:36 PM.140	0.000	TCP	21	FTP	SYS12	
42206	5/7/2014 4:27:36 PM.140	0.000	TCP	19	chargen	SYS12	
42205	5/7/2014 4:27:36 PM.140	0.000	TCP	17	Quote of the day	SYS12	
42204	5/7/2014 4:27:36 PM.140	0.000	TCP	13	Daytime	SYS12	
42203	5/7/2014 4:27:36 PM.140	0.000	TCP	9	Discard	SYS12	
42202	5/7/2014 4:27:36 PM.140	0.000	TCP	7	Echo	SYS12	
42185	5/7/2014 4:22:03 PM.515	42.000	TCP	21	FTP	SYS12	
42172	5/7/2014 4:20:15 PM.234	0.219	TCP	23	Telnet	SYS12	
42069	5/7/2014 3:55:35 PM.031	0.000	TCP	8080	IIS Proxy	SYS12	
42068	5/7/2014 3:55:35 PM.031	0.000	TCP	4899	radmin	SYS12	
42067	5/7/2014 3:55:35 PM.031	0.000	TCP	3128	IIS Proxy	SYS12	
42066	5/7/2014 3:55:34 PM.828	0.000	TCP	1433	SQL Server	SYS12	
42065	5/7/2014 3:55:34 PM.828	0.000	TCP	1080	SOCKS	SYS12	
42064	5/7/2014 3:55:34 PM.640	0.000	TCP	113	ident	SYS12	
42063	5/7/2014 3:55:34 PM.640	0.000	TCP	110	POP3	SYS12	
42062	5/7/2014 3:55:34 PM.640	0.000	TCP	53	DNS	SYS12	
42061	5/7/2014 3:55:34 PM.640	0.000	TCP	25	SMTP	SYS12	
42060	5/7/2014 3:55:34 PM.640	0.000	TCP	23	Telnet	SYS12	
42059	5/7/2014 3:55:34 PM.640	0.000	TCP	22	SSH	SYS12	
42058	5/7/2014 3:55:34 PM.640	0.000	TCP	21	FTP	SYS12	
42057	5/7/2014 3:55:34 PM.625	0.000	TCP	17	Quote of the day	SYS12	
42056	5/7/2014 3:55:34 PM.625	0.000	TCP	19	chargen	SYS12	
42055	5/7/2014 3:55:34 PM.625	0.000	TCP	13	Daytime	SYS12	
42054	5/7/2014 3:55:34 PM.625	0.000	TCP	9	Discard	SYS12	
42053	5/7/2014 3:55:34 PM.625	0.000	TCP	7	Echo	SYS12	

Server: Running Visitors: 25 Events: 70/13

Shows Nodes with IP address that are connected to Network

SQL Server attack detected by KFSensor

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

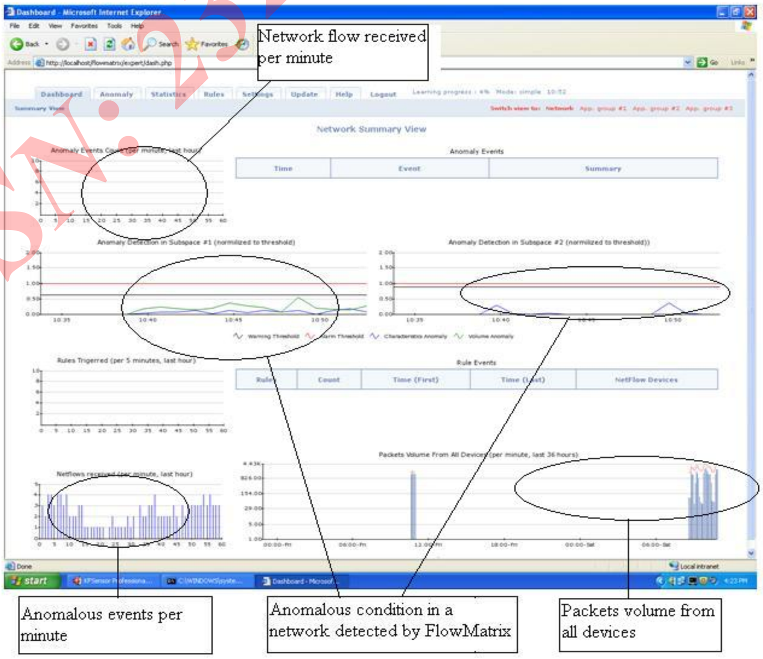
Phase III: in this phase we installed both KFSensor and FlowMatrix and study a system again for 10 days. Here we find the different results that attacks which cannot be detected by KFsensor and detected by FlowMatrix. The combine logs is generated which capture the attacks and than administrator can 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.


Dashboard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/flowmatrix/expert/dash.php
Dashboard Anomaly Statistics Rules Settings Update Help Logout
Summary View
Network Summary View
Anomaly Events Count (per minute, last hour)
Anomaly Events
Time Event Summary
Anomaly Detection in Subspace #1 (normilized to threshold)
Anomaly Detection in Subspace #2 (normilized to threshold))
Warning Threshold Alarm Threshold Characteristics Anomaly Volume Anomaly
Rules Trigerred (per 5 minutes, last hour)
Rule Events
Rule Count Time (First) Time (Last) NetFlow Devices
Netflows received (per minute, last hour)
Packets Volume From All Devices (per minute, last 36 hours)
Done
Local intranet

Network flow received per minute

Anomalous events per minute

Anomalous condition in a network detected by FlowMatrix

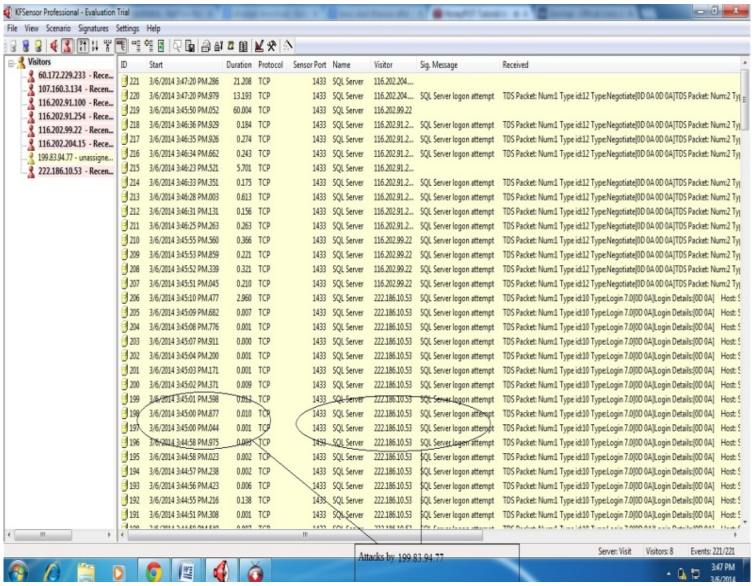
Packets volume from all devices

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

IJRASET: ISSN: 2321-9653



ID	Start	Duration	Protocol	Sensor Port	Name	Visitor	Sig. Message	Received
221	3/6/2014 3:47:20 PM.286	21.208	TCP	1433	SQL Server	116.202.204....		
220	3/6/2014 3:47:20 PM.979	13.193	TCP	1433	SQL Server	116.202.204....	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
219	3/6/2014 3:45:50 PM.052	60.004	TCP	1433	SQL Server	116.202.99.22		
218	3/6/2014 3:46:36 PM.929	0.184	TCP	1433	SQL Server	116.202.91.2...	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
217	3/6/2014 3:46:35 PM.926	0.274	TCP	1433	SQL Server	116.202.91.2...	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
216	3/6/2014 3:46:34 PM.662	0.243	TCP	1433	SQL Server	116.202.91.2...	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
215	3/6/2014 3:46:23 PM.521	5.701	TCP	1433	SQL Server	116.202.91.2...		
214	3/6/2014 3:46:33 PM.351	0.175	TCP	1433	SQL Server	116.202.91.2...	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
213	3/6/2014 3:46:28 PM.003	0.613	TCP	1433	SQL Server	116.202.91.2...	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
212	3/6/2014 3:46:31 PM.131	0.156	TCP	1433	SQL Server	116.202.91.2...	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
211	3/6/2014 3:46:25 PM.263	0.263	TCP	1433	SQL Server	116.202.91.2...	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
210	3/6/2014 3:45:55 PM.560	0.366	TCP	1433	SQL Server	116.202.99.22	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
209	3/6/2014 3:45:53 PM.859	0.221	TCP	1433	SQL Server	116.202.99.22	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
208	3/6/2014 3:45:52 PM.339	0.321	TCP	1433	SQL Server	116.202.99.22	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
207	3/6/2014 3:45:51 PM.045	0.210	TCP	1433	SQL Server	116.202.99.22	SQL Server logon attempt	TDS Packet: Num:1 Type id:12 Type:Negotiate[0D 0A 0D 0A]TDS Packet: Num:2 Ty
206	3/6/2014 3:45:10 PM.477	2.960	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
205	3/6/2014 3:45:09 PM.682	0.007	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
204	3/6/2014 3:45:08 PM.776	0.001	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
203	3/6/2014 3:45:07 PM.911	0.000	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
202	3/6/2014 3:45:04 PM.200	0.001	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
201	3/6/2014 3:45:03 PM.171	0.001	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
200	3/6/2014 3:45:02 PM.371	0.009	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
199	3/6/2014 3:45:01 PM.598	0.012	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
198	3/6/2014 3:45:00 PM.877	0.010	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
197	3/6/2014 3:45:00 PM.044	0.001	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
196	3/6/2014 3:44:58 PM.975	0.003	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
195	3/6/2014 3:44:58 PM.023	0.002	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
194	3/6/2014 3:44:57 PM.238	0.002	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
193	3/6/2014 3:44:56 PM.423	0.006	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
192	3/6/2014 3:44:55 PM.216	0.138	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S
191	3/6/2014 3:44:51 PM.308	0.001	TCP	1433	SQL Server	222.186.10.53	SQL Server logon attempt	TDS Packet: Num:1 Type id:10 Type:Login 7.0[0D 0A]Login Details:[0D 0A] Host: S

Attacks by 199.83.94.77

Server: Visit Visitors: 8 Events: 221/221

Figure 4: KFSensor at Personal networks

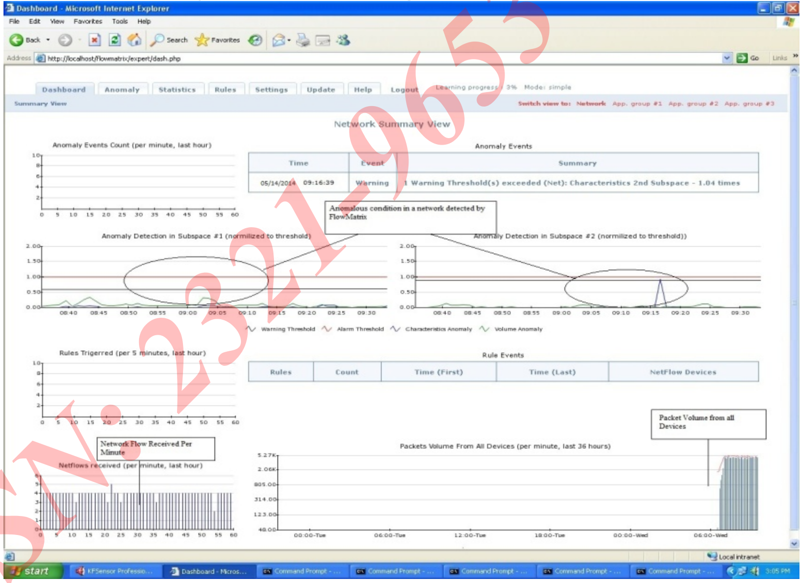
In the table 4 below we have analyze the following characteristics of KFSensor and conclude that KFSensor is a Host based Honeypot intrusion detection system which can attract the attacker towards itself to protect the organization from attack and block that user in future to enter the organization's 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-


Dashboard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/flowmatrix/expert/dash.php
Go Links
Dashboard Anomaly Statistics Rules Settings Update Help Logout
Learning progress : 3% Mode: simple
Summary View
Switch view to: Network App. group #1 App. group #2 App. group #3
Network Summary View
Anomaly Events Count (per minute, last hour)
Anomaly Events
Anomaly Detection in Subspace #1 (normilized to threshold)
Anomaly Detection in Subspace #2 (normilized to threshold))
2.00 1.50 1.00 0.50 0.00
08:40 08:45 08:50 08:55 09:00 09:05 09:10 09:15 09:20 09:25 09:30
Warning Threshold Alarm Threshold Characteristics Anomaly Volume Anomaly
Rules Trigerred (per 5 minutes, last hour)
Rule Events
Netflows received (per minute, last hour)
Packets Volume From All Devices (per minute, last 36 hours)
5.27K 2.06K 805.00 314.00 123.00 48.00
00:00-Tue 06:00-Tue 12:00-Tue 18:00-Tue 00:00-Wed 06:00-Wed
0 5 10 15 20 25 30 35 40 45 50 55 60
Local intranet
start KFSensor Professio... Dashboard - Micros... Command Prompt - ... Command Prompt - ... Command Prompt - ... Command Prompt - ... Command Prompt - ...
3:05 PM

Time	Event	Summary
05/14/2014 09:16:39	Warning	1 Warning Threshold(s) exceeded (Net): Characteristics 2nd Subspace - 1.04 times

Anomalous condition in a network detected by FlowMatrix

Rules	Count	Time (First)	Time (Last)	NetFlow Devices

Packet Volume from all Devices

Network Flow Received Per Minute

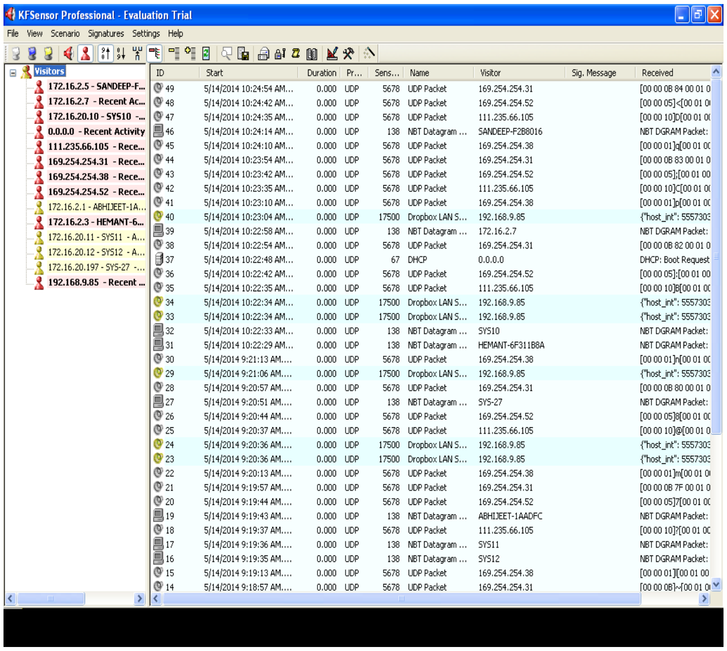
Figure 5: FlowMatrix showing the alert which is not capture by KFSensor

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

IJRASET: ISSN: 2321-9653

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

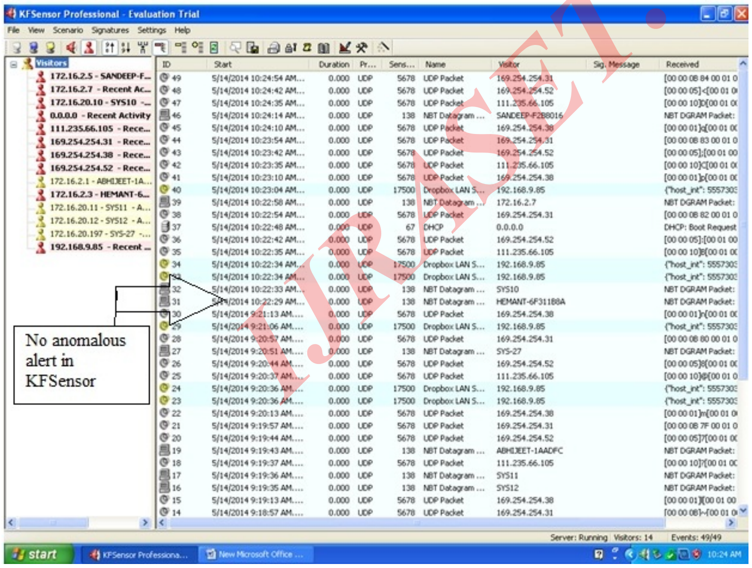

KFSensor Professional - Evaluation Trial
File View Scenario Signatures Settings Help

Visitors
- 172.16.2.5 - SANDEEP-F...
- 172.16.2.7 - Recent Ac...
- 172.16.20.10 - SYS10 -...
- 0.0.0.0 - Recent Activity
- 111.235.66.105 - Rece...
- 169.254.254.31 - Rece...
- 169.254.254.38 - Rece...
- 169.254.254.52 - Rece...
- 172.16.2.1 - ABHIJEET-1A...
- 172.16.2.3 - HEMANT-6...
- 172.16.20.11 - SYS11 - A...
- 172.16.20.12 - SYS12 - A...
- 172.16.20.197 - SYS-27 -...
- 192.168.9.85 - Recent ...

ID	Start	Duration	Pr...	Sens...	Name	Visitor	Sig. Message	Received
49	5/14/2014 10:24:54 AM...	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 84 00 01 0
48	5/14/2014 10:24:42 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]<[00 01 0
47	5/14/2014 10:24:35 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]D[00 01 0
46	5/14/2014 10:24:14 AM...	0.000	UDP	138	NBT Datagram ...	SANDEEP-F2B8016		NBT DGRAM Packet:
45	5/14/2014 10:24:10 AM...	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]q[00 01 0
44	5/14/2014 10:23:54 AM...	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 83 00 01 0
43	5/14/2014 10:23:42 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05];[00 01 00
42	5/14/2014 10:23:35 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]C[00 01 0
41	5/14/2014 10:23:10 AM...	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]p[00 01 0
40	5/14/2014 10:23:04 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
39	5/14/2014 10:22:58 AM...	0.000	UDP	138	NBT Datagram ...	172.16.2.7		NBT DGRAM Packet:
38	5/14/2014 10:22:54 AM...	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 82 00 01 0
37	5/14/2014 10:22:48 AM...	0.000	UDP	67	DHCP	0.0.0.0		DHCP: Boot Request
36	5/14/2014 10:22:42 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]:[00 01 00
35	5/14/2014 10:22:35 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]B[00 01 0
34	5/14/2014 10:22:34 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
33	5/14/2014 10:22:34 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
32	5/14/2014 10:22:33 AM...	0.000	UDP	138	NBT Datagram ...	SYS10		NBT DGRAM Packet:
31	5/14/2014 10:22:29 AM...	0.000	UDP	138	NBT Datagram ...	HEMANT-6F311B8A		NBT DGRAM Packet:
30	5/14/2014 9:21:13 AM....	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]n[00 01 0
29	5/14/2014 9:21:06 AM....	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
28	5/14/2014 9:20:57 AM....	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 80 00 01 0
27	5/14/2014 9:20:51 AM....	0.000	UDP	138	NBT Datagram ...	SYS-27		NBT DGRAM Packet:
26	5/14/2014 9:20:44 AM....	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]8[00 01 0
25	5/14/2014 9:20:37 AM....	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]@[00 01 0
24	5/14/2014 9:20:36 AM....	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
23	5/14/2014 9:20:36 AM....	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
22	5/14/2014 9:20:13 AM....	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]m[00 01 0
21	5/14/2014 9:19:57 AM....	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 7F 00 01 0
20	5/14/2014 9:19:44 AM....	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]7[00 01 0
19	5/14/2014 9:19:43 AM....	0.000	UDP	138	NBT Datagram ...	ABHIJEET-1AADFC		NBT DGRAM Packet:
18	5/14/2014 9:19:37 AM....	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]?[00 01 0
17	5/14/2014 9:19:36 AM....	0.000	UDP	138	NBT Datagram ...	SYS11		NBT DGRAM Packet:
16	5/14/2014 9:19:35 AM....	0.000	UDP	138	NBT Datagram ...	SYS12		NBT DGRAM Packet:
15	5/14/2014 9:19:13 AM....	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]l[00 01 00
14	5/14/2014 9:18:57 AM....	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B]~[00 01 0

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.


KFSensor Professional - Evaluation Trial
File View Scenario Signatures Settings Help
No anomalous alert in KFSensor
start
KFSensor Professiona...
New Microsoft Office ...
10:24 AM

Visitors
- 172.16.2.5 - SANDEEP-F...
- 172.16.2.7 - Recent Ac...
- 172.16.20.10 - SYS10 -...
- 0.0.0.0 - Recent Activity
- 111.235.66.105 - Rece...
- 169.254.254.31 - Rece...
- 169.254.254.38 - Rece...
- 169.254.254.52 - Rece...
- 172.16.2.1 - ABHIJEET-1A...
- 172.16.2.3 - HEMANT-6...
- 172.16.20.11 - SYS11 - A...
- 172.16.20.12 - SYS12 - A...
- 172.16.20.197 - SYS-27 -...
- 192.168.9.85 - Recent ...

ID	Start	Duration	Pr...	Sens...	Name	Visitor	Sig. Message	Received
49	5/14/2014 10:24:54 AM...	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 84 00 01 0
48	5/14/2014 10:24:42 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]<[00 01 0
47	5/14/2014 10:24:35 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]D[00 01 0
46	5/14/2014 10:24:14 AM...	0.000	UDP	138	NBT Datagram ...	SANDEEP-F2B8016		NBT DGRAM Packet:
45	5/14/2014 10:24:10 AM...	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]q[00 01 0
44	5/14/2014 10:23:54 AM...	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 83 00 01 0
43	5/14/2014 10:23:42 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05];[00 01 00
42	5/14/2014 10:23:35 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]C[00 01 0
41	5/14/2014 10:23:10 AM...	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]p[00 01 0
40	5/14/2014 10:23:04 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
39	5/14/2014 10:22:58 AM...	0.000	UDP	138	NBT Datagram ...	172.16.2.7		NBT DGRAM Packet:
38	5/14/2014 10:22:54 AM...	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 82 00 01 0
37	5/14/2014 10:22:48 AM...	0.000	UDP	67	DHCP	0.0.0.0		DHCP: Boot Request
36	5/14/2014 10:22:42 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]:[00 01 00
35	5/14/2014 10:22:35 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]B[00 01 0
34	5/14/2014 10:22:34 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
33	5/14/2014 10:22:34 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
32	5/14/2014 10:22:33 AM...	0.000	UDP	138	NBT Datagram ...	SYS10		NBT DGRAM Packet:
31	5/14/2014 10:22:29 AM...	0.000	UDP	138	NBT Datagram ...	HEMANT-6F311B8A		NBT DGRAM Packet:
30	5/14/2014 9:21:13 AM....	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]n[00 01 0
29	5/14/2014 9:21:06 AM....	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
28	5/14/2014 9:20:57 AM....	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 80 00 01 0
27	5/14/2014 9:20:51 AM....	0.000	UDP	138	NBT Datagram ...	SYS-27		NBT DGRAM Packet:
26	5/14/2014 9:20:44 AM....	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]8[00 01 0
25	5/14/2014 9:20:37 AM....	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]@[00 01 0
24	5/14/2014 9:20:36 AM....	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
23	5/14/2014 9:20:36 AM....	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
22	5/14/2014 9:20:13 AM....	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]m[00 01 0
21	5/14/2014 9:19:57 AM....	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B 7F 00 01 0
20	5/14/2014 9:19:44 AM....	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]7[00 01 0
19	5/14/2014 9:19:43 AM....	0.000	UDP	138	NBT Datagram ...	ABHIJEET-1AADFC		NBT DGRAM Packet:
18	5/14/2014 9:19:37 AM....	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]?[00 01 0
17	5/14/2014 9:19:36 AM....	0.000	UDP	138	NBT Datagram ...	SYS11		NBT DGRAM Packet:
16	5/14/2014 9:19:35 AM....	0.000	UDP	138	NBT Datagram ...	SYS12		NBT DGRAM Packet:
15	5/14/2014 9:19:13 AM....	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]l[00 01 00
14	5/14/2014 9:18:57 AM....	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 0B]~[00 01 0

Server: Running Visitors: 14 Events: 49/49

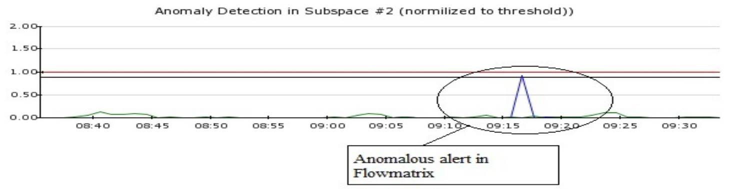


Figure 7: Comparison between KFSensor and Flowmatrix

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

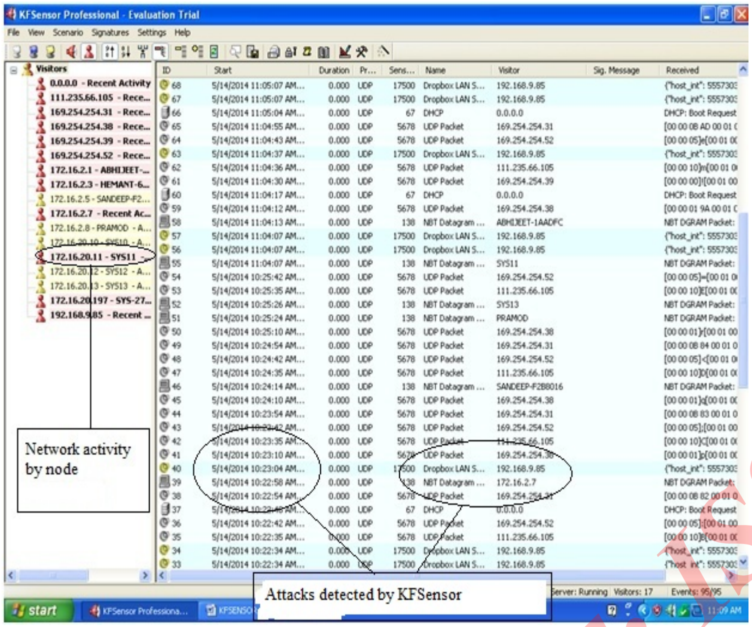
Table 2: Characteristics observed while doing experiments with Flowmatrix

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

IJRASET: 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.

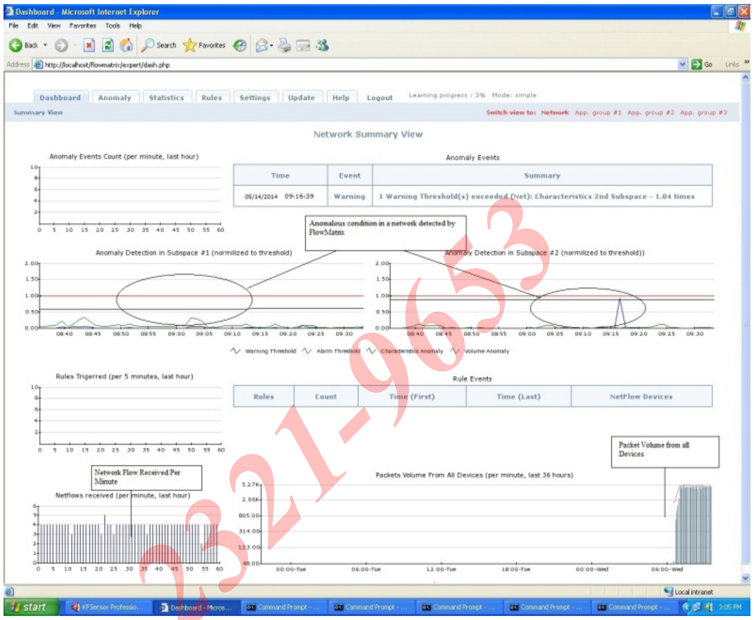

KFSensor Professional - Evaluation Trial
File View Scenario Signatures Settings Help
Network activity by node
Attacks detected by KFSensor
Server: Running Visitors: 17 Events: 95/95
start
KFSensor Professiona...
KFSENSOR
11:09 AM

Visitors
0.0.0.0 - Recent Activity
111.235.66.105 - Rece...
169.254.254.31 - Rece...
169.254.254.38 - Rece...
169.254.254.39 - Rece...
169.254.254.52 - Rece...
172.16.2.1 - ABHIJEET-...
172.16.2.3 - HEMANT-6...
172.16.2.5 - SANDEEP-F2...
172.16.2.7 - Recent Ac...
172.16.2.8 - PRAMOD - A...
172.16.20.10 - SYS10 - A...
172.16.20.11 - SYS11 -...
172.16.20.12 - SYS12 - A...
172.16.20.13 - SYS13 - A...
172.16.20.197 - SYS-27...
192.168.9.85 - Recent ...

ID	Start	Duration	Pr...	Sens...	Name	Visitor	Sig. Message	Received
68	5/14/2014 11:05:07 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
67	5/14/2014 11:05:07 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
66	5/14/2014 11:05:04 AM...	0.000	UDP	67	DHCP	0.0.0.0		DHCP: Boot Request
65	5/14/2014 11:04:55 AM...	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 AD 00 01 0
64	5/14/2014 11:04:43 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]e[00 01 00
63	5/14/2014 11:04:37 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
62	5/14/2014 11:04:36 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]m[00 01 0
61	5/14/2014 11:04:30 AM...	0.000	UDP	5678	UDP Packet	169.254.254.39		[00 00 00]![00 01 00
60	5/14/2014 11:04:17 AM...	0.000	UDP	67	DHCP	0.0.0.0		DHCP: Boot Request
59	5/14/2014 11:04:12 AM...	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01 9A 00 01 0
58	5/14/2014 11:04:13 AM...	0.000	UDP	138	NBT Datagram ...	ABHIJEET-1AADFC		NBT DGRAM Packet:
57	5/14/2014 11:04:07 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
56	5/14/2014 11:04:07 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
55	5/14/2014 11:04:07 AM...	0.000	UDP	138	NBT Datagram ...	SYS11		NBT DGRAM Packet:
54	5/14/2014 10:25:42 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]=[00 01 0
53	5/14/2014 10:25:35 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]E[00 01 00
52	5/14/2014 10:25:26 AM...	0.000	UDP	138	NBT Datagram ...	SYS13		NBT DGRAM Packet:
51	5/14/2014 10:25:24 AM...	0.000	UDP	138	NBT Datagram ...	PRAMOD		NBT DGRAM Packet:
50	5/14/2014 10:25:10 AM...	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]r[00 01 00
49	5/14/2014 10:24:54 AM...	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 84 00 01 0
48	5/14/2014 10:24:42 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]<[00 01 0
47	5/14/2014 10:24:35 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]D[00 01 00
46	5/14/2014 10:24:14 AM...	0.000	UDP	138	NBT Datagram ...	SANDEEP-F2B8016		NBT DGRAM Packet:
45	5/14/2014 10:24:10 AM...	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]q[00 01 00
44	5/14/2014 10:23:54 AM...	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 83 00 01 0
43	5/14/2014 10:23:42 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05];[00 01 00
42	5/14/2014 10:23:35 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]C[00 01 00
41	5/14/2014 10:23:10 AM...	0.000	UDP	5678	UDP Packet	169.254.254.38		[00 00 01]p[00 01 00
40	5/14/2014 10:23:04 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
39	5/14/2014 10:22:58 AM...	0.000	UDP	138	NBT Datagram ...	172.16.2.7		NBT DGRAM Packet:
38	5/14/2014 10:22:54 AM...	0.000	UDP	5678	UDP Packet	169.254.254.31		[00 00 08 82 00 01 0
37	5/14/2014 10:22:48 AM...	0.000	UDP	67	DHCP	0.0.0.0		DHCP: Boot Request
36	5/14/2014 10:22:42 AM...	0.000	UDP	5678	UDP Packet	169.254.254.52		[00 00 05]:[00 01 00
35	5/14/2014 10:22:35 AM...	0.000	UDP	5678	UDP Packet	111.235.66.105		[00 00 10]B[00 01 00
34	5/14/2014 10:22:34 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303
33	5/14/2014 10:22:34 AM...	0.000	UDP	17500	Dropbox LAN S...	192.168.9.85		{"host_int": 5557303

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.


Dashboard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/flowmatrix/expert/dash.php
Go Links
Dashboard
Anomaly
Statistics
Rules
Settings
Update
Help
Logout
Learning progress : 3% Mode: simple
Summary View
Switch view to: Network App. group #1 App. group #2 App. group #3
Network Summary View
Anomaly Events Count (per minute, last hour)
10
8
6
4
2
0 5 10 15 20 25 30 35 40 45 50 55 60
Anomalous condition in a network detected by FlowMatrix
Anomaly Detection in Subspace #1 (normilized to threshold)
Anomaly Detection in Subspace #2 (normilized to threshold))
2.00
1.50
1.00
0.50
0.00
08:40 08:45 08:50 08:55 09:00 09:05 09:10 09:15 09:20 09:25 09:30
Warning Threshold
Alarm Threshold
Characteristics Anomaly
Volume Anomaly
Rules Trigerred (per 5 minutes, last hour)
Network Flow Received Per Minute
Netflows received (per minute, last hour)
6 5 4 3 2 1 0
Packet Volume from all Devices
Packets Volume From All Devices (per minute, last 36 hours)
5.27K
2.06K
805.00
314.00
123.00
48.00
00:00-Tue 06:00-Tue 12:00-Tue 18:00-Tue 00:00-Wed 06:00-Wed
Local intranet
start
KFSensor Professio...
Dashboard - Micros...
Command Prompt - ...
3:05 PM

Anomaly Events

Time	Event	Summary
05/14/2014 09:16:39	Warning	1 Warning Threshold(s) exceeded (Net): Characteristics 2nd Subspace - 1.04 times

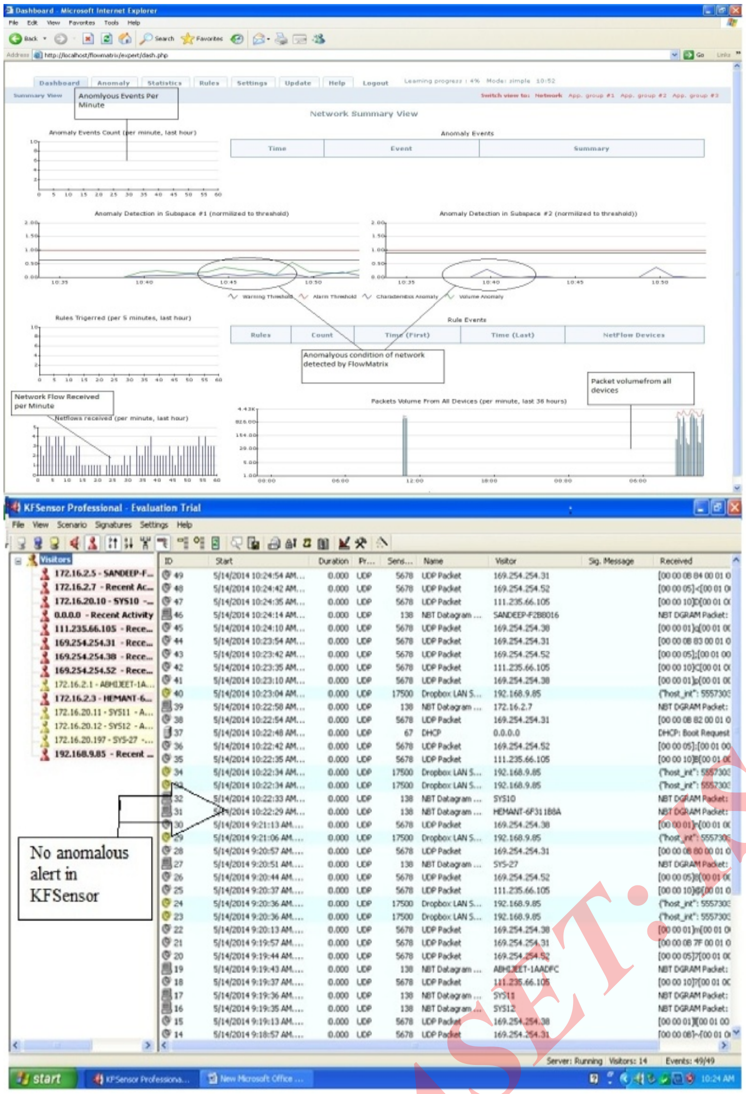
Rule Events

Rules	Count	Time (First)	Time (Last)	NetFlow Devices

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

IJRASET: ISSN: 2321-9653


Dashboard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
http://localhost/flowmatrix/expert/dash.php
Dashboard
Anomaly
Statistics
Rules
Settings
Update
Help
Logout
Anomlyous Events Per Minute
Network Summary View
Anomaly Events Count (per minute, last hour)
Anomaly Events
Time
Event
Summary
Anomaly Detection in Subspace #1 (normalized to threshold)
Anomaly Detection in Subspace #2 (normalized to threshold)
Warning Threshold
Alarm Threshold
Characteristics Anomaly
Volume Anomaly
Rules Trigerred (per 5 minutes, last hour)
Rule Events
Rules
Count
Time (First)
Time (Last)
NetFlow Devices
Anomalyous condition of network detected by FlowMatrix
Packet volumefrom all devices
Network Flow Received per Minute
Netflows received (per minute, last hour)
Packets Volume From All Devices (per minute, last 36 hours)
KFSensor Professional - Evaluation Trial
File View Scenario Signatures Settings Help
Visitors
172.16.2.5 - SANDEEP-F...
172.16.2.7 - Recent Ac...
172.16.20.10 - SYS10 -...
0.0.0.0 - Recent Activity
111.235.66.105 - Rece...
169.254.254.31 - Rece...
169.254.254.38 - Rece...
169.254.254.52 - Rece...
172.16.2.1 - ABHIJEET-1A...
172.16.2.3 - HEMANT-6...
172.16.20.11 - SYS11 - A...
172.16.20.12 - SYS12 - A...
172.16.20.197 - SYS-27 -...
192.168.9.85 - Recent ...
No anomalous alert in KFSensor
start
KFSensor Professiona...
New Microsoft Office ...
10:24 AM

```
ID  Start                     Duration  Pr...  Sens...  Name               Visitor           Sig. Message  Received
49  5/14/2014 10:24:54 AM...  0.000     UDP    5678     UDP Packet         169.254.254.31                  [00 00 08 84 00 01 0
48  5/14/2014 10:24:42 AM...  0.000     UDP    5678     UDP Packet         169.254.254.52                  [00 00 05]<[00 01 0
47  5/14/2014 10:24:35 AM...  0.000     UDP    5678     UDP Packet         111.235.66.105                  [00 00 10]D[00 01 0
46  5/14/2014 10:24:14 AM...  0.000     UDP    138      NBT Datagram ...   SANDEEP-F2B8016                 NBT DGRAM Packet:
45  5/14/2014 10:24:10 AM...  0.000     UDP    5678     UDP Packet         169.254.254.38                  [00 00 01]q[00 01 0
44  5/14/2014 10:23:54 AM...  0.000     UDP    5678     UDP Packet         169.254.254.31                  [00 00 08 83 00 01 0
43  5/14/2014 10:23:42 AM...  0.000     UDP    5678     UDP Packet         169.254.254.52                  [00 00 05];[00 01 0
42  5/14/2014 10:23:35 AM...  0.000     UDP    5678     UDP Packet         111.235.66.105                  [00 00 10]C[00 01 0
41  5/14/2014 10:23:10 AM...  0.000     UDP    5678     UDP Packet         169.254.254.38                  [00 00 01]p[00 01 0
40  5/14/2014 10:23:04 AM...  0.000     UDP    17500    Dropbox LAN S...   192.168.9.85                    {"host_int": 555730
39  5/14/2014 10:22:58 AM...  0.000     UDP    138      NBT Datagram ...   172.16.2.7                      NBT DGRAM Packet:
38  5/14/2014 10:22:54 AM...  0.000     UDP    5678     UDP Packet         169.254.254.31                  [00 00 08 82 00 01 0
37  5/14/2014 10:22:48 AM...  0.000     UDP    67       DHCP               0.0.0.0                         DHCP: Boot Request
36  5/14/2014 10:22:42 AM...  0.000     UDP    5678     UDP Packet         169.254.254.52                  [00 00 05]:[00 01 0
35  5/14/2014 10:22:35 AM...  0.000     UDP    5678     UDP Packet         111.235.66.105                  [00 00 10]B[00 01 0
34  5/14/2014 10:22:34 AM...  0.000     UDP    17500    Dropbox LAN S...   192.168.9.85                    {"host_int": 555730
33  5/14/2014 10:22:34 AM...  0.000     UDP    17500    Dropbox LAN S...   192.168.9.85                    {"host_int": 555730
32  5/14/2014 10:22:33 AM...  0.000     UDP    138      NBT Datagram ...   SYS10                           NBT DGRAM Packet:
31  5/14/2014 10:22:29 AM...  0.000     UDP    138      NBT Datagram ...   HEMANT-6F31188A                 NBT DGRAM Packet:
30  5/14/2014 9:21:13 AM....  0.000     UDP    5678     UDP Packet         169.254.254.38                  [00 00 01]n[00 01 0
29  5/14/2014 9:21:06 AM....  0.000     UDP    17500    Dropbox LAN S...   192.168.9.85                    {"host_int": 555730
28  5/14/2014 9:20:57 AM....  0.000     UDP    5678     UDP Packet         169.254.254.31                  [00 00 08 80 00 01 0
27  5/14/2014 9:20:51 AM....  0.000     UDP    138      NBT Datagram ...   SYS-27                          NBT DGRAM Packet:
26  5/14/2014 9:20:44 AM....  0.000     UDP    5678     UDP Packet         169.254.254.52                  [00 00 05]8[00 01 0
25  5/14/2014 9:20:37 AM....  0.000     UDP    5678     UDP Packet         111.235.66.105                  [00 00 10]@[00 01 0
24  5/14/2014 9:20:36 AM....  0.000     UDP    17500    Dropbox LAN S...   192.168.9.85                    {"host_int": 555730
23  5/14/2014 9:20:36 AM....  0.000     UDP    17500    Dropbox LAN S...   192.168.9.85                    {"host_int": 555730
22  5/14/2014 9:20:13 AM....  0.000     UDP    5678     UDP Packet         169.254.254.38                  [00 00 01]m[00 01 0
21  5/14/2014 9:19:57 AM....  0.000     UDP    5678     UDP Packet         169.254.254.31                  [00 00 08 7F 00 01 0
20  5/14/2014 9:19:44 AM....  0.000     UDP    5678     UDP Packet         169.254.254.52                  [00 00 05]7[00 01 0
19  5/14/2014 9:19:43 AM....  0.000     UDP    138      NBT Datagram ...   ABHIJEET-1AADFC                 NBT DGRAM Packet:
18  5/14/2014 9:19:37 AM....  0.000     UDP    5678     UDP Packet         111.235.66.105                  [00 00 10]?[00 01 0
17  5/14/2014 9:19:36 AM....  0.000     UDP    138      NBT Datagram ...   SYS11                           NBT DGRAM Packet:
16  5/14/2014 9:19:35 AM....  0.000     UDP    138      NBT Datagram ...   SYS12                           NBT DGRAM Packet:
15  5/14/2014 9:19:13 AM....  0.000     UDP    5678     UDP Packet         169.254.254.38                  [00 00 01]][00 01 00
14  5/14/2014 9:18:57 AM....  0.000     UDP    5678     UDP Packet         169.254.254.31                  [00 00 08]~[00 01 0
Server: Running   Visitors: 14   Events: 49/49
```

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.

IJRASET: 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.

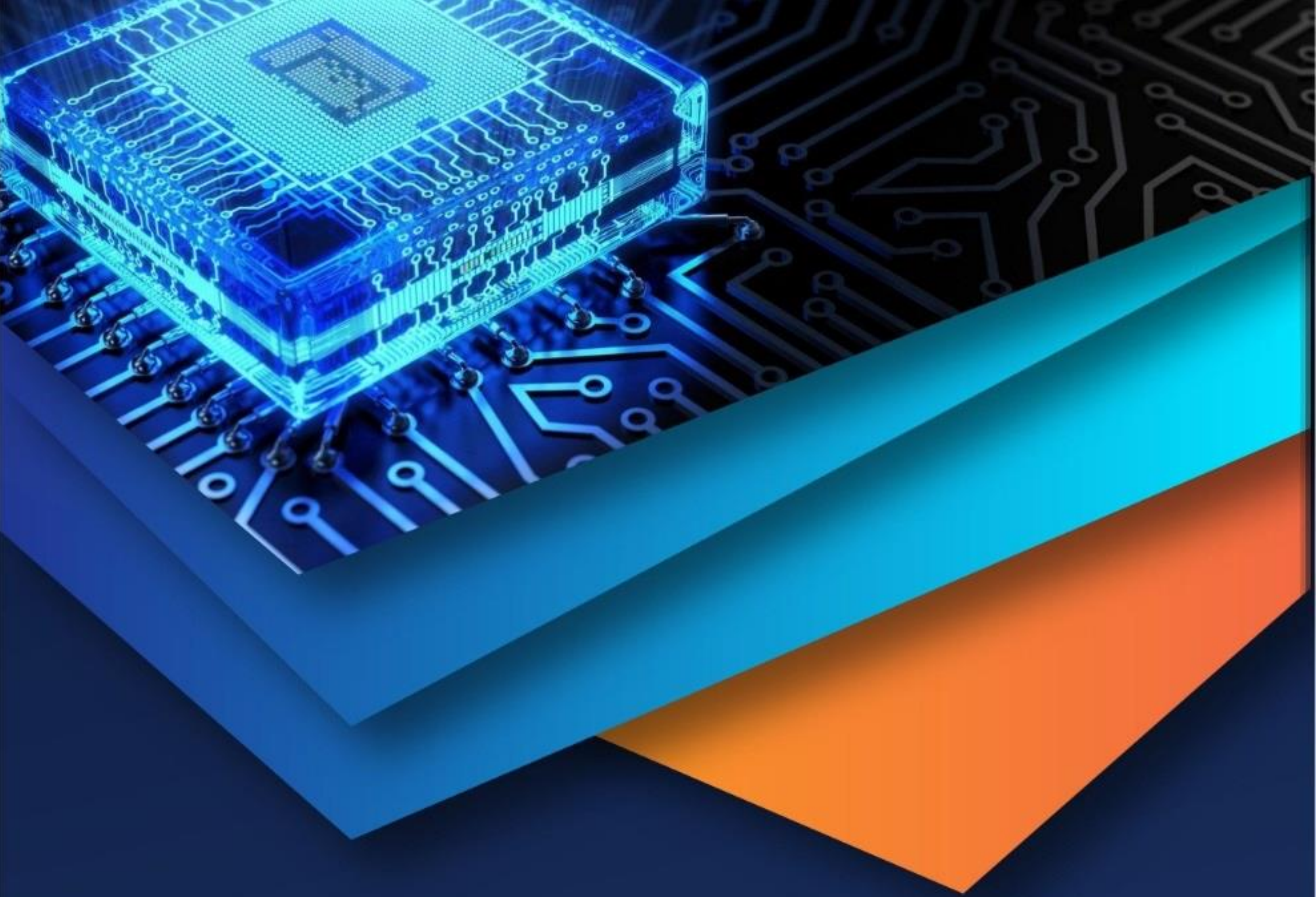
[12]. CISCO: Cisco Packet Tracer Data Sheet, Available:http://www.cisco.com/web/learning/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf

[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.

IJRASET: ISSN: 2321-9653



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL
FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)