A Relevance Technical Approach for Screening the Significance of IDS in Cloud Forensics

Shaik Khaja Mohiddin, Yalavarthi Suresh Babu

Abstract**: *Due to an exponential growth of technology with huge and huge amount of data which is generated and has to be processed and this data is not related to a single area which is related to multiple areas and also this raises the need for the storage of data, which emphasizes the importance of cloud, now every small industry or small organizations has moved maximum towards cloud. Storage of data in cloud has many advantages including which has accessing the data with respect to any place, with respect to any device with a minimal internet connection beside this there is a downfall with respect to the intruders who are considered as the major threat for the data stored in the cloud. The importance which is given for storage of data in the cloud the same has to be implemented for protection of data inside the cloud, well which sometimes failed to be achieved this stresses for the need of Intrusion Detection System. An Intrusion Detection System (IDS) also plays an important role during the process of Cloud Forensics. In This paper we have traced out the importance of IDS in Cloud Forensics by using a snort IDS which is an open source we have gone with the process of using snort by tuning the rules in snort according to our requirements. Where the intrusion activities are being sniffed by the IDS which are then detected by the Forensic Analysis tools and then they are being analysed during the forensic process.***

Index Choice: IDS: Intrusion Detection System, IPS: Intrusion protection system, CF: Cloud Forensics, SLA: Service Level Agreement, CSP: Cloud Service Provider.

I. INTRODUCTION

The entire paper is divide into 12 sections where each section is having its own significance where I section deals with Introductions with the basic concepts which are being involved with IDS and also describes basic types in IDS, II section deals with the various capabilities which are being exhibited by IDS due to which it is considered as the tool for sniffing, III section deals with snort architecture, IV section deals with basic concepts of Forensic in cloud,V section deals with the three dimensional view of cloud forensics, VI section describes about the basic steps which has to be followed from collection to the presentation of forensic evidences, VII section deals with the implementation which clearly shows the steps which are being involved from the installation of snort IDS in cloud environment to the successfully running of snort, VIII discussed about the results, XI section describes Comparison of various cloud forensic existing tools their usage along with importance, X deals with conclusion and how to extend the concept in future XI section deals with references.

In general we can classify the intrusion detection/ Prevention systems into either active or passive IDS or IPS. In Active Intrusion Detection systems or Intrusion prevention systems they are being configured automatically to block any suspected attacks without the intervention of an operator, here the advantage is that according to the attack the system carries out the corrective action. Where as in Passive IDS/IPS is just designed to just detect and alert the attack and informs that to the operator but it does not take any preventive or corrective measures to carry out the task.

In a general scenario we can classify various IDS in the following different categories which are discussed below

A. Network Intrusion detection systems (NIDS)

Here by monitoring the network traffic with respect to a network hubs, network switches, network taps an IDS is used to analyze the behaviour of intruder during the unauthorized attacks and to carry out the necessary tasks. e.g. snort.

B. Host-Based Intrusion Detection System (HIDS)

Here the presence of an agent on the host carries out the required application logs, analyzing system calls, modified file systems; here software agents are present who carry out the task of IDS.

C. Perimeter Intrusion Detection System (PIDS)

For certain infrastructure having perimeter fences when an intrusion attack happens on those fences then they are being traced with exact position by the IDS.

D. VM Based Intrusion Detection Systems (VMIDS)

Here the intruder activities on a particular cloud are going to be monitored by the VM by installing IDS on the VM itself.

II. CAPABILITIES OF IDS

When unauthorized activities are being carried out over a given network then they are being traced out and intimated to the operators with the help of IDS and when if necessary depending on the IDS it may carry out the overcoming activities with or without operator's intervention. IDS have the following general capabilities.

Revised Manuscript Received on December 22, 2018.

Shaik Khaja Mohiddin, Research Scholar , Dept. of CSE, Acharya Nagarjuna Univeristy,Guntur, Asso.Prof.,Dept. of CSE, VVIT , Nambur Guntur, Andhra Pradesh, India

Dr. Yalavarthi Suresh Babu, Prof. Dept. of CSE, JKC College, Guntur, Andhra Pradesh, India

- Whenever IDS detects any unauthorized event then they are immediately intimates the operator with relevant alarm and notification.
- Even a non IT expert staff can also carry out the operations using these IDS with the help of user friendly environment created by them.
- It prevents the data after the attack simply by blocking the server or the intruders in order to avoid further loss of data
- Provides an easy way to understand, detect and tune the operating system in order to carry out audit trails.
- User policy violation tracking.

III. SNORT ARCHITECTURE

Snort architecture is accomplished with five components which work to analyze traffic as well as monitoring the network it is helpful for generating alerts when it encounters signs for intrusions.

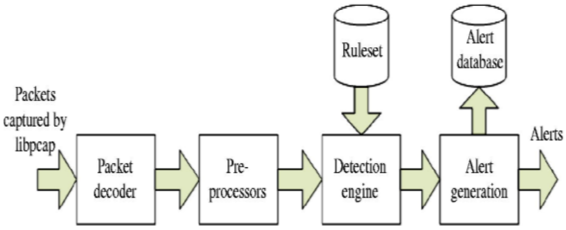


Fig 1: Snort architecture (source snort manual)

It has the following components

Packet decoder: captures the packets from network traffic and initiates the detection engine.

Preprocessors: with respect to different plugins the packets which are captures are then processed.

Detection engine: the preprocessor data is sent to the detection engine where the data packets are being matched with the rules and depending on the packets with respect to different time the malicious packets are traced out.

Logging and alerting system: here the logging and alerts are managed by the systems.

Output module: here the different logs generated by different alerting systems are being saved.

IV. FORENSICS IN CLOUD

Cloud forensics is the combination of digital forensic and cloud computing, when certain mischief happens with the data stored in the cloud then cloud forensic is the scenario where one can get relevant information regarding what has been carried out with respect to the clients data which is stored in the cloud.

Steps involved in the cloud forensic process: cloud forensic is carried out by the following steps:

- **Identification:** before starting the forensic investigation one has to exactly find out whether really some mischief has happened or not after conformation and identification then investigator can start his investigation.
- **Preservation:** the collected clues during the investigation play an important role during the investigation process so they should be preserved carefully for future references.
- **Collection:** whatever were the clues which are collected during the investigation should be preserved properly.

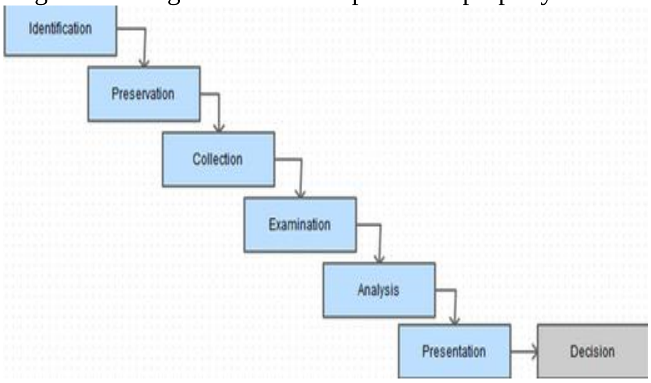


Fig2. Steps to be carried out during the forensic process in the cloud.

- **Examination :** all the collected clues during the forensic investigation in the cloud should be examined properly to get a conclusion
- **Analysis:** the collected, examined data should be analyzed properly so that a conclusion is derived by the investigator on what might happen with the data by the intruder.
- **Presentation**: as the collected information is in the form of technical information which has to present in the cyber court where some judge may not be aware of the technical terminology completely so the presentation plays a vital role.
- **Decision:** depending on the analyzed and presented data before the court decision is taken by the court which has to be followed strictly and the accused should be convicted.

V. APPLYING THREE DIMENSIONAL CONCEPTS FOR CLOUD FORENSICS

When major cloud service providers such as Google, Amazon, and Salesforce.com are compared among themselves common aspects is noticed that these cloud tycoons have extended their cloud data centers throughout the world and they provide the services on the basis of cost effectiveness, service availability, data in the cloud centers are being replicated among other data centers which are located in various jurisdictions so that during an unexpected failure they can have the backup of their relevant data. The way, in which these service providers' deals with The customers during the forensics concepts differ from each other, the emergence of multi-tenancy, multi –jurisdiction strengthens to have them as a default setting for cloud forensic. When a problem is being encountered these cloud service providers have their different approaches to overcome the same problem. When certain mischief is happened with respect to the data using cloud forensic one can trace out the cause for the mischief and related information regarding the status of data.

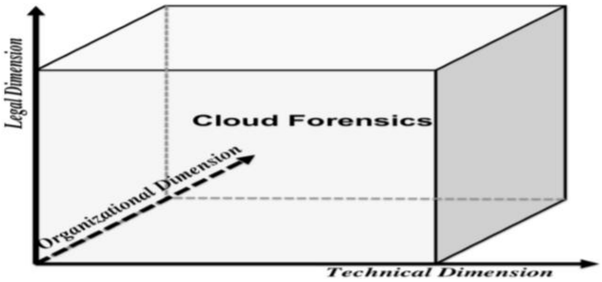


Fig3: showing three dimensions of cloud forensic.

During the early developments of cloud forensics was assumed to be associated with three dimensions such as legal, technical and organizational.

Cloud Forensic Dimensions	Associated with Parameters
Technical	They compromise the tools and the techniques which are being carried out during forensic process in the cloud.
Organizational	Investigators: they carry out the examination when certain misconduct is carried out with the cloud data they should be an expertise person.
	IT professionals: they provide technical support to the investigators during the investigation by the cloud forensic expert.
	• Incident Handlers: when certain incidents are happening with respect to data leakage in the cloud, breach of data, when cloud data effected by malicious codes they play a vital role in the above said situations.
	• Legal Advisors: they deal with legal issued pertaining to the cloud such as multi-tenancy and jurisdictional issues so that forensic activities should not be disturb the integrity of others data stored in the cloud.
	• External Assistance: External parities and CSP should be taken help during the forensic investigation process.
Legal	• Here development with respect to the SLA agreements between the CSP and clients along with certain regulations which assures that there is no breach carried out when the investigation on the data stored in the cloud is carried out. [1][2]

Table 1: Shows the three dimensional view of cloud forensics

VI. STEPS TO BE CARRIED OUT DURING CLOUD FORENSICS

Following are the steps which are involved during the cloud forensic process and are stated as identification, collection, organization and presentation. Which are explained as follows.

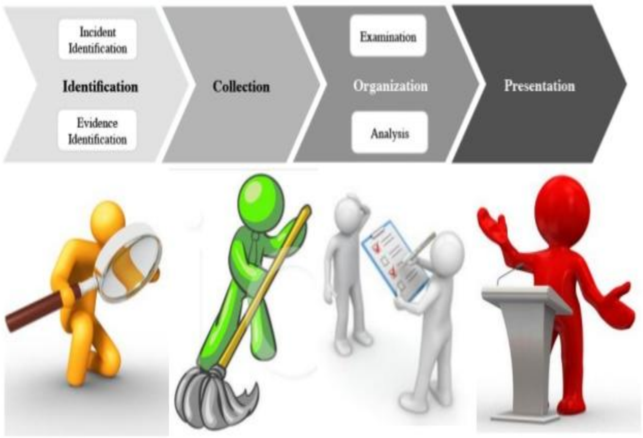


Fig4: Steps involved in cloud forensic process

Identification: Identification is the first and initial step which is carried out during the forensic analysis here we have to identify whether really mischief has been happened with the data in the cloud.

Collection: The clues which come across during the forensic analysis should be collected properly and preserved so that they can be presented in a proper way.

Organization: Clues which are collected should be organized in a proper way for presentation if the collected clues are not presented in a proper way then it may be lead for the offender to escape.

Presentation: The clues which have been collected during the forensic investigation should be presented in a proper way where non technical legal persons has to get satisfied who are not much familiar with the technical process and terms.

Forensic phase	List of challenges
identification	Decentralization information Reliance chain Reliance on CSP
collection	Unavailability Trust Time synchronization Multi-Tenancy
organization	Cross-jurisdiction Erased information Lack of investigation tools
presentation	Make familiarize of technical concepts to non technical persons Lack of Experienced persons

Table 2: Shows Challenges in cloud forensics

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

VII. IMPLEMENTATION

On VMWare workstation we have installed ubuntu on one virtual machine and in ubuntu we have installed snort , which is an open source IDS which is helpful for sniffing unauthorized attacks which are being carried out on the cloud for that purpose we have installed a windows server. We have tuned snort IDS with the required

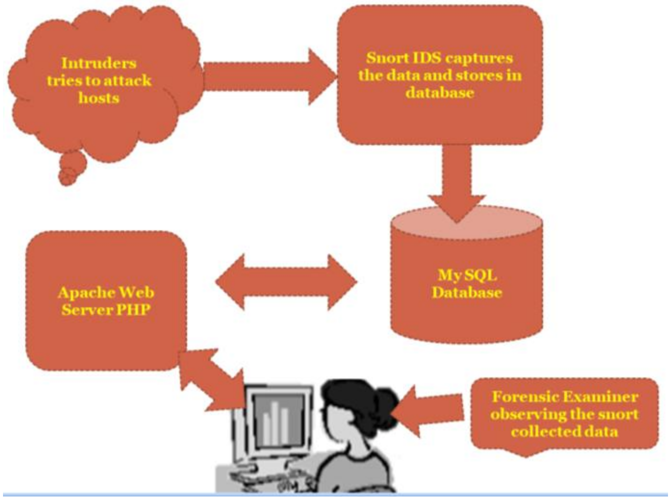

Intruders tries to attack hosts
Snort IDS captures the data and stores in database
My SQL Database
Apache Web Server PHP
Forensic Examiner observing the snort collected data

Fig 5: Snort used in NIDS

E. Installation code

```
sudo apt-get update && sudo apt-get dist-upgrade –y
mkdir ~/snort_src
cd ~/snort_src
sudo apt-get install -y build-essential autotools-dev
libdumbnet-dev libluajit-5.1-dev libpcap-dev \ libpcre3-dev
zlib1g-dev pkg-config libhwloc-dev
sudo apt-get remove -y cmake
cd ~/snort_src
wget https://cmake.org/files/v3.10/cmake-3.10. 3. tar.gz
tar -xzvf cmake-3.10.3.tar.gz
cd cmake-3.10.3 ./bootstrap
make
sudo make install
sudo apt-get install -y liblzma-dev openssl libssl-dev cpputest
libsqlite3-dev \ uuid-dev
sudo apt-get install -y
asciidoc dblatex source-highlight w3m.......
```

VIII. OBTAINED RESULTS AND DISCUSSION

After successful installation of snort IDS which is a free open source, whenever a particular unauthorised access is being carried out that is by default sniffed by snort IDS and then it sends an alarm to the forensic examiner who has been analyzing the data sent and collected by snort in the database. Where the incident is first examined if its unauthorised then the clues are being collected and examined thoroughly and then they are presented in a proper way. The required attacks are being performed which are being monitored and recorded in the snort database and during the investigation it is used. Inside the snort database the information during the attack by the intruder is noted in the form of packets which are should in the following diagrams

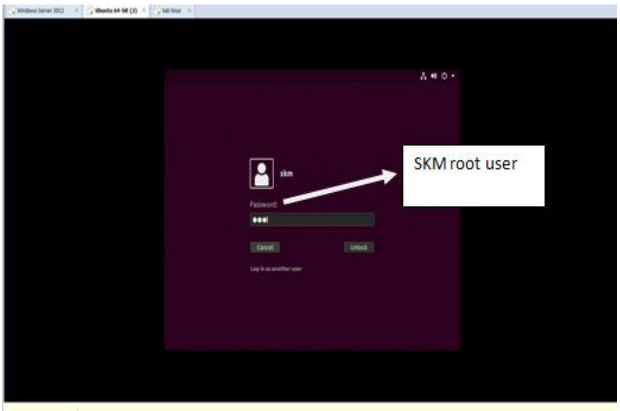
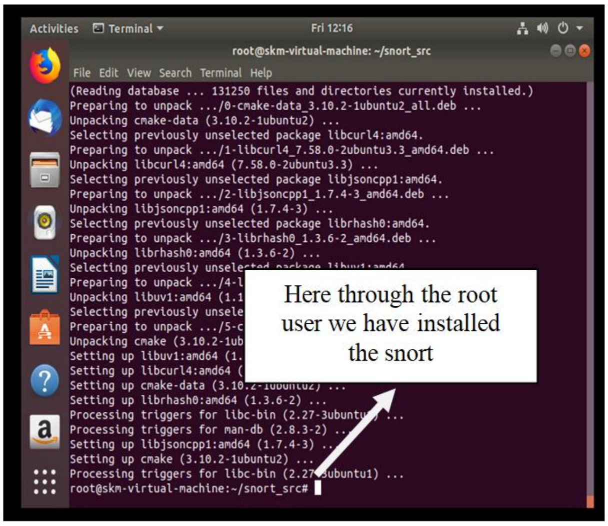
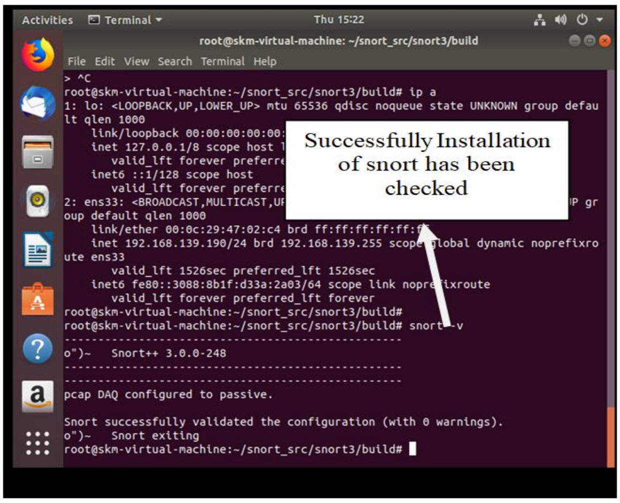


Fig 6: Creation of Root user


Activities
Terminal
Fri 12:16
File Edit View Search Terminal Help
Here through the root user we have installed the snort

```
root@skm-virtual-machine: ~/snort_src
(Reading database ... 131250 files and directories currently installed.)
Preparing to unpack .../0-cmake-data_3.10.2-1ubuntu2_all.deb ...
Unpacking cmake-data (3.10.2-1ubuntu2) ...
Selecting previously unselected package libcurl4:amd64.
Preparing to unpack .../1-libcurl4_7.58.0-2ubuntu3.3_amd64.deb ...
Unpacking libcurl4:amd64 (7.58.0-2ubuntu3.3) ...
Selecting previously unselected package libjsoncpp1:amd64.
Preparing to unpack .../2-libjsoncpp1_1.7.4-3_amd64.deb ...
Unpacking libjsoncpp1:amd64 (1.7.4-3) ...
Selecting previously unselected package librhash0:amd64.
Preparing to unpack .../3-librhash0_1.3.6-2_amd64.deb ...
Unpacking librhash0:amd64 (1.3.6-2) ...
Selecting previously unsele
Preparing to unpack .../4-l
Unpacking libuv1:amd64 (1.1
Selecting previously unsele
Preparing to unpack .../5-c
Unpacking cmake (3.10.2-1ub
Setting up libuv1:amd64 (1.
Setting up libcurl4:amd64 (
Setting up cmake-data (3.10
Setting up librhash0:amd64 (1.3.6-2) ...
Processing triggers for libc-bin (2.27-3ubuntu ...
Processing triggers for man-db (2.8.3-2) ...
Setting up libjsoncpp1:amd64 (1.7.4-3) ...
Setting up cmake (3.10.2-1ubuntu2) ...
Processing triggers for libc-bin (2.27 3ubuntu1) ...
root@skm-virtual-machine:~/snort_src#
```

Fig 7: installation of required packages for snort.

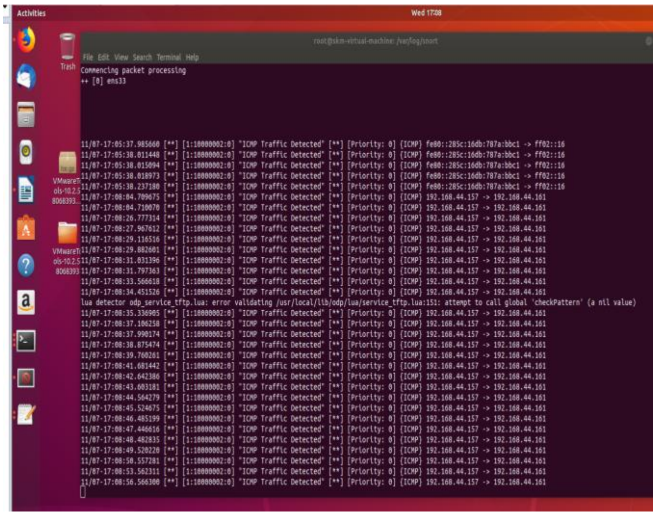

Activities
Terminal
Thu 15:22
File Edit View Search Terminal Help
Successfully Installation of snort has been checked

```
root@skm-virtual-machine: ~/snort_src/snort3/build
> ^C
root@skm-virtual-machine:~/snort_src/snort3/build# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:
    inet 127.0.0.1/8 scope host l
       valid_lft forever preferre
    inet6 ::1/128 scope host
       valid_lft forever preferre
2: ens33: <BROADCAST,MULTICAST,UP                                          UP gr
oup default qlen 1000
    link/ether 00:0c:29:47:02:c4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.139.190/24 brd 192.168.139.255 scope global dynamic noprefixro
ute ens33
       valid_lft 1526sec preferred_lft 1526sec
    inet6 fe80::3088:8b1f:d33a:2a03/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@skm-virtual-machine:~/snort_src/snort3/build#
root@skm-virtual-machine:~/snort_src/snort3/build# snort -v
--------------------------------------------------
o")~   Snort++ 3.0.0-248
--------------------------------------------------
--------------------------------------------------
pcap DAQ configured to passive.

Snort successfully validated the configuration (with 0 warnings).
o")~   Snort exiting
root@skm-virtual-machine:~/snort_src/snort3/build#
```

Fig 8: Checking the succesfull installation of snort in

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



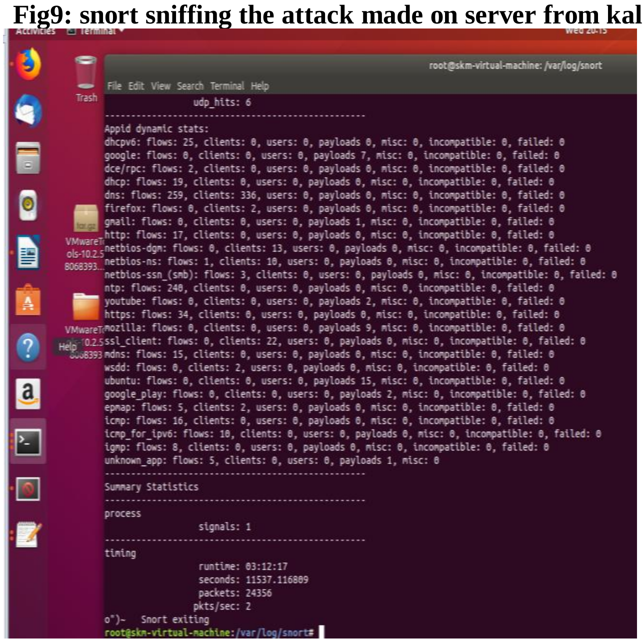
```
Commencing packet processing
++ [0] ens33



11/07-17:05:37.985660 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} fe80::285c:16db:787a:bbc1 -> ff02::16
11/07-17:05:38.011448 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} fe80::285c:16db:787a:bbc1 -> ff02::16
11/07-17:05:38.015094 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} fe80::285c:16db:787a:bbc1 -> ff02::16
11/07-17:05:38.018973 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} fe80::285c:16db:787a:bbc1 -> ff02::16
11/07-17:05:38.237180 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} fe80::285c:16db:787a:bbc1 -> ff02::16
11/07-17:08:04.709675 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:04.710070 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:26.777314 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:27.967612 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:29.116516 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:29.882601 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:31.031396 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:31.797363 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:33.566618 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:34.451526 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
lua detector odp_service_tftp.lua: error validating /usr/local/lib/odp/lua/service_tftp.lua:151: attempt to call global 'checkPattern' (a nil value)
11/07-17:08:35.336905 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:37.106258 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:37.990174 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:38.875474 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:39.760261 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:41.681442 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:42.642386 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:43.603181 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:44.564279 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:45.524675 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:46.485199 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:47.446616 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:48.482835 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:49.520220 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:50.557281 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:53.562311 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
11/07-17:08:56.566300 [**] [1:10000002:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.44.157 -> 192.168.44.161
```

Activities
Wed 17:08
root@skm-virtual-machine: /var/log/snort
File Edit View Search Terminal Help
Trash

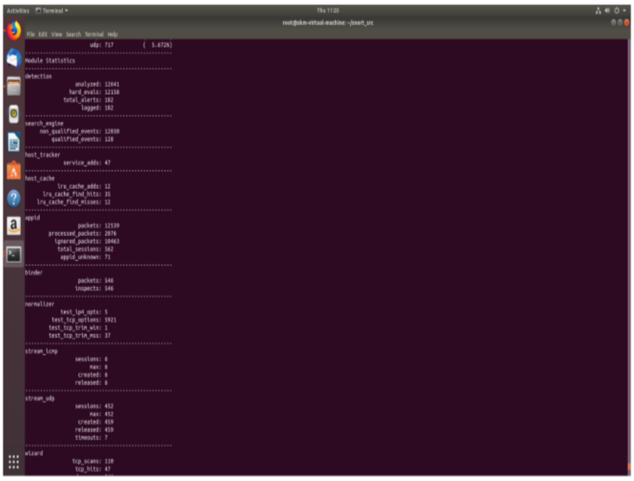
Fig9: snort sniffing the attack made on server from kali



```
                   udp_hits: 6
--------------------------------------------------
Appid dynamic stats:
dhcpv6: flows: 25, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
google: flows: 0, clients: 0, users: 0, payloads 7, misc: 0, incompatible: 0, failed: 0
dce/rpc: flows: 2, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
dhcp: flows: 19, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
dns: flows: 259, clients: 336, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
firefox: flows: 0, clients: 2, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
gmail: flows: 0, clients: 0, users: 0, payloads 1, misc: 0, incompatible: 0, failed: 0
http: flows: 17, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
netbios-dgm: flows: 0, clients: 13, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
netbios-ns: flows: 1, clients: 10, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
netbios-ssn_(smb): flows: 3, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
ntp: flows: 240, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
youtube: flows: 0, clients: 0, users: 0, payloads 2, misc: 0, incompatible: 0, failed: 0
https: flows: 34, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
mozilla: flows: 0, clients: 0, users: 0, payloads 9, misc: 0, incompatible: 0, failed: 0
ssl_client: flows: 0, clients: 22, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
mdns: flows: 15, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
wsdd: flows: 0, clients: 2, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
ubuntu: flows: 0, clients: 0, users: 0, payloads 15, misc: 0, incompatible: 0, failed: 0
google_play: flows: 0, clients: 0, users: 0, payloads 2, misc: 0, incompatible: 0, failed: 0
epmap: flows: 5, clients: 2, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
icmp: flows: 16, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
icmp_for_ipv6: flows: 10, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
igmp: flows: 8, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, failed: 0
unknown_app: flows: 5, clients: 0, users: 0, payloads 1, misc: 0
--------------------------------------------------
Summary Statistics
--------------------------------------------------
process
                  signals: 1
--------------------------------------------------
timing
                  runtime: 03:12:17
                  seconds: 11537.116809
                  packets: 24356
                 pkts/sec: 2
o")~   Snort exiting
root@skm-virtual-machine:/var/log/snort# 
```

Activities
Terminal
Wed 20:15
root@skm-virtual-machine: /var/log/snort
File Edit View Search Terminal Help
Trash
Help

Fig 10: Total results which are being sniffed by snort IDS



```
                   udp: 717          (  5.672%)
--------------------------------------------------
Module Statistics
--------------------------------------------------
detection
                 analyzed: 12641
               hard_evals: 12150
             total_alerts: 182
                   logged: 182
--------------------------------------------------
search_engine
     non_qualified_events: 12030
         qualified_events: 128
--------------------------------------------------
host_tracker
             service_adds: 47
--------------------------------------------------
host_cache
            lru_cache_adds: 12
       lru_cache_find_hits: 35
     lru_cache_find_misses: 12
--------------------------------------------------
appid
                  packets: 12539
        processed_packets: 2076
          ignored_packets: 10463
           total_sessions: 562
            appid_unknown: 71
--------------------------------------------------
binder
                  packets: 546
                 inspects: 546
--------------------------------------------------
normalizer
            test_ip4_opts: 5
         test_tcp_options: 5921
        test_tcp_trim_win: 1
        test_tcp_trim_mss: 37
--------------------------------------------------
stream_icmp
                 sessions: 6
                      max: 6
                  created: 6
                 released: 6
--------------------------------------------------
stream_udp
                 sessions: 452
                      max: 452
                  created: 459
                 released: 459
                 timeouts: 7
--------------------------------------------------
wizard
                tcp_scans: 110
                 tcp_hits: 47
```

Activities
Terminal
Thu 11:20
root@skm-virtual-machine: ~/snort_src
File Edit View Search Terminal Help

Fig: 11 Total results categorised in group packest

IX.AN OVERVIEW OF THE EXISTING CLOUD FORENSIC TOOLS:

There exists certain limitations for digital forensics which can be defined by [3][4], which exists in the areas of Legal Aspect, volume of data, Capacity of Tools, Forensic Analysis Automation and visualization, these existing limitations make further need for the new cloud forensic tool which has to carry out the necessary things.

S. no.	Tool name	Purpose
1	Digital Forensics Frame works	It is an open source; it can be easily handled by non-experts as well as experts also.
2	Open computer Forensics Architecture	It is an open source forensic framework, it is used for storing data and it uses Postgre SQL, it works on Linux platform.
3	CAINE	Computer Aided Investigative Environment, it is an open source, it is helpful in integrating software modules from existing software tools.
4	X-Ways Forensics	It runs on almost all available windows versions, digital examiners consider it as an advanced stand.
5	SANS Investigative Forensics Toolkit (SIFT)	It is a operating system forensic used for multipurpose which has all required tools to be used in digital forensic process which has an inbuilt platform on Ubuntu .
6	EnCase	This tools has a forensic platform which is utilized for multipurpose it gathers information from different devices very fast and also this tool also produces report based evidence. it is a paid tool.
7	Registry Recon	This is a paid tool it is well known for registry analysis, it gathers the registry info., from evidence and again rebuilds the registry.
8	Sleuth Kit (+Autopsy)	It is used in the forensic analysis of computers, it is a windows and unix based tool.
9	Libforensics	It is available with various demo tools in order to extract information from different types of evidences.
10	Volatility	It is used for analysis in malware, it is a memory based forensic framework.
11	WindowsSCO PE	It is used for volatile memory analysis it also works as reverse engineering tool.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

12	**Corner's Toolkit**	This tool is used to recover the data from the devices which are working based on Unix operating systems.
13	**Oxygen Forensic Suite**	Using this tool one can gather the information from mobile; one can also recover calendar information, call logs, contacts.
14	**Bulk Extractor**	This tool is very fast as it does not follow file system structure during the extraction of data from files.
15	**Xplico**	The data from the applications which uses network and internet protocols can be extracted using this tool.
16	**Mandiant Redline**	It is used for file and memory analysis, when a process is running on the host it collects the information, it is also helpful to gather meta data, registry data, and internet history for building up a report.
17	**Computer Online Forensic Evidence Extractor (COFEE)**	Forensic experts in computers use this tool kit, as it was developed by Microsoft, it collects evidences within the windows systems.
18	**P2eXplorer**	It is an image mounting tool, on the hard disk these images are mounted and they are then analyzed by file explorer.
19	**PlainSight**	With Linux distribution, It is a CD based Knoppix , it is useful in gathering information related to internet history.
20	**XRY**	Developed by Micro Systems, it is helpful for recovery of crucial and analyzed data from the mobile.
21	**HELIX3**	It is an incident responsive CD based digital forensic suite, it also includes hex editors, tools for password cracking.
22	**Cellebrite UFED**	It is very helpful to collect information with high accuracy on mobile data.
24	**FTK Imager**	This tool is used for the examination of folders and files which are being stored in network drives, DVDs,/CDs, hard .
25	**DEFT**	It is a linux based CD which consists of number of open source and freely available forensic tools.
26	**Bulk Extractor**	This tool is helpful for scanning of directory of files, disk images, e mail address.

Table 3: Shows various tools which are being used in the cloud during any kind of cyber attack

X. CONCLUSION AND FUTURE WORK

We are planning to use this kind of snort IDS in a cloud environment which is an experimental set on a VMware workstation where we are using three virtual machines which are having three different IP addresses and all the three VMs are being communicated among themselves easily where we are installing our requirements with respect to forensics analysis using forensic analysis tools such as Slueth Kit, CAINE, Xplico.. .. we collect the results which are being obtained with respect to snort IDS . So rather than storing and accessing the data through the cloud from anywhere when certain mischief has happened to the data than it has to be immediately brought to the notice of forensic experts , and it is also stressed that FaaS (Forensics as a Service) should be considered as the basic requirements along with the necessary services which are being included as IaaS,PaaS,SaaS...

XI. REFERENCES

1. Broadhurst R. Developments in the global law enforcement of cyber- crime. Policing: An International Journal of Police Strategies & Management. 2006 Jul 1;29(3):408-33..
2. Liles S, Rogers M, Hoebich M. A survey of the legal issues facing digital forensic experts. InIFIP International Conference on Digital Forensics 2009 Jan 26 (pp. 267-276) . Springer , Berlin, Heidelberg.
3. Henry P, Williams J, Wright B. The sans survey of digital forensics and incident response. SANS Institute InfoSec Reading Room. 2013 Jul.
4. Miranda Lopez E, Moon SY, Park JH. Scenario-Based Digital Forensics Challenges in Cloud Computing. Symmetry. 2016 Oct 20;8(10):107.
5. Mohiddin S.K., Yalavarthi. An analytical comparative approach of cloud forensic tools during cyber attack in cloud". Proceedings in Advanced in intelligent and system computing. 2018.