ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

Demonstrating the Weaknesses of IDS and Firewall on Policy Violation in the Cloud

Ruth Oginga[1], Felix Musau[2], Christopher Maghanga[3]

P.G. Student, Department of Computer Science and IT, Kabarak University, Nakuru, Kenya[1]

Professor, Department of Computer Science, Riara University, Nairobi, Kenya[2]

Doctor, Department of Computer Science and IT, Kabarak University, Nakuru, Kenya[3]

ABSTRACT: Organizations are increasingly becoming aware of the business value that cloud computing brings and are taking steps towards transition to the cloud. With the diverseness of technologies, there are different security attacks and challenges. There are several important challenges that exist with regard to efficient provisioning and delivery of services through cloud. Threats on the cloud environment can be due to policy violation. Despite the use of protection systems to detect any malicious activities, policy violation is one factor that hinders widespread usage of cloud. The focus of this paper is on demonstrating the weaknesses of IDS and firewall on policy violation in the cloud. In particular, the research design used was based on mixed research and the prototype was tested by a group of experts. The results were demonstrated using algorithm, flow charts and experiments. It was recommended that security and applicable policies needs to be implemented to safe guard the customers' data.

KEYWORDS: Policy violation, cloud, security, Weaknesses

I. INTRODUCTION

Cloud computing is defined as both the applications dispersed as services over the Internet and the systems software and hardware in the data centers that offer those services (Zhang et.al., 2010). The need for cloud computing was possibly necessitated by increased corporate information volumes beyond the convectional computer storage growing into thousands of Gigabytes over time. The distributive nature of businesses and systems and the reliance of data for performing most business operations mean data has to be available anywhere and anytime. Cloud computing is a platform that provides such flexibility of making data available on demand and is becoming a popular method of data storage as well as a service platform. Most importantly, cloud computing provides a storage facility that is hosted and accessible over the internet, making data readily available when and as required (Hashem et al., 2015. Security is viewed as one of the main adoption stoppers to cloud computing and the complexity of infrastructure involved leaves the door open to various threats coming from outside and within. Intrusions, malware or security policy violations of curious or malicious users are just but a few. Control assets and information policy are required in order to protect organization assets of the cloud-computing environment. Acceptable use policy is needed to make sure controls and monitoring of services is provided. Acceptable use policy is a set of rules applied by organizational network administrators to restrict the ways in which the network is used and set guidelines as to how it should be used. Different network administrators use different types of network-based and host-based security software to detect malicious activities in the cloud. The main target of the assailants is to make an attack to the presented resources in the Cloud computing settings (Hameed et al., 2016).

Various methods can be used to detect intrusions but each one is specific to a specific method. The main goal of an intrusion detection system is to detect the attacks efficiently. Furthermore, it is equally important to detect attacks at the beginning stage in order to reduce their impacts (Jabez, & Muthukumar, 2015). Major problem with the cloud IDS is that it lacks the proactive capability to prevent attacks at its initial stage. Firewalls are configured to protect against unauthenticated interactive logins from the outside world. However, Firewalls cannot prevent attacks coming from Intranet (He et al., 2014). Detection and prevention tools have weaknesses that need to be demonstrated in order to be

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

come up with a more robust system. Therefore there is need to demonstrate the weaknesses of IDS and firewall on policy violation in cloud. The main objective is to identify the weaknesses of IDS and firewall and demonstrate those weaknesses using a prototype.
As for the remaining part of this paper, Section I is introductions which contain problem statement and objectives. This is followed by a detailed description of related work in section II, Section III is Methodology. Section IV is Results and Discussion which is demonstrated using Algorithm, flowcharts experiments, and finally, conclusions and future work are provided in section V.

II. RELATED WORK

Vieira et al. (2010) have tested the deployment of IDS at different positions in the cloud to detect DoS attacks. The authors have considered two scenarios to calculate the IDS performance based on its position in the cloud. Calculation results have shown that detection of DoS attacks using a single IDS instance located close to the Cloud Controller which will significantly increase the load on Cloud Controller. On the other hand, deployment of split instances of IDS at each virtual machine affects only the CPU load of the attacked VM and there is no significant impact on other VMs.
The proposed technique is signature based so unable to detect unknown attacks. Another model to counter the attack is called 'CloudAV' is provided by Zhang et al., (2014). They gave two main features that make it more efficient, accurate and fast as a malware detection system. One of the features is antivirus as a network service it is a detection capability by host-based antivirus. It is more efficient and effective as cloud-network-service. Each host runs a lightweight Process to detect new files and then sends them to network service for quarantine and for further analysis rather than running complex analysis software on each end-host.

The second feature is the N-version protection. It is malicious software identification determined by multiple heterogonous detection engines similar to the idea of N-version programming. The notion of N-version protection has been provided in this solution so that the malware detection system should leverage the detection capabilities of multiple heterogeneous detection engines to determine malicious and unwanted files more effectively (Xu et al., 2016).
However, the number of false positives encountered during normal operations increase compared to 1-version engines.
Modi et al. (2012) proposed and implemented a Network intrusion detection system (NIDS) which uses Snort to detect known attacks and Bayesian classifier to detect unknown attacks. NIDS deployed in all servers work in a collaborative approach by generating alerts into the knowledge base and thus making detection of unknown attacks easier. In the given technique, signature-based detection is followed by anomaly-based detection, since it detects just unknown attacks. However, the detection rate is increased by sending alert to other NIDS deployed in the cloud.

According to Riaz et al. (2017) grid and Cloud Computing Intrusion Detection System (GCCIDS), this is designed to cover the attacks that network and host-based systems cannot detect. Their proposed method uses the integration of knowledge and behavior analysis to detect specific intrusions. However, the proposed prototype cannot discover new types of attacks or create an attack database, which must be considered during implementing IDS.

According to Hu et al. (2014) enforcing a conflict-free security policy in cloud environments based on SDN has been studied in Flowguard. These works deal effectively with direct conflicts by rejecting the policy and implementing role-based and signature-based enforcement to ensure applications do not circumvent existing security policy. However, a flow can be defined in multiple layers, where traditional policy checking approaches do not consider; for examples, indirect security violations, partial violations or cross-layer conflicts cannot be handled them. Moreover, they appear not to fully leverage the SDN paradigm that lets flow rules do traffic shaping in addition to implementing accept/deny security policy.
According to Bulajoul et al. (2015) designed, a real network to present experiments that use a Snort NIDPS. Their experiments demonstrate the weaknesses of NIDPSes, such as inability to process multiple packets and propensity to drop packets in heavy traffic and high-speed networks without analysing them. They tested Snort's analysis performance, gauging the number of packets sent, analysed, dropped, filtered, injected, and outstanding.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

III. METHODOLOGY

The research design for this study was based on the mixed methods research design. Mixed method research design has the advantages of using multiple ways to explore a research problem. Here the researcher used experimental design and survey of literature for gathering requirement and simple random sampling method was adapted.

IV. RESULTS AND DISCUSSION

Results demonstrated existing Weaknesses of the Firewall and IDS.
In the firewall demonstration, the weaknesses that were tested are external and internal attacks. The external attacker can hack on the computer on the network that has a firewall and internal computer can scan the network within and without the firewall detection.

Algorithm for demonstrating weaknesses of Firewall

Step 1: Start
Step 2 User: User request to be signed up in the firewall server
Step 3 Actors: Verifies and add the user to the server
Step 4: Firewall server prompt user to enter username and password

a. The user enters username and password
b. Server checks username

If username does not exist in the file system it sends invalid username to go to step 2
Step 5 Short descriptions: Login verifies user access to firewall server based on username and password pair that is entered by the user on the end user device (personal computers or iPad or smartphone)
Step 6 User initializes the devices used in the server at the same time
Step 7 Pre-condition: User is connected to the network (tested through IP address ping with VM1, external attacker, internal attacker, and the firewall server)
Step 8 Invariant: If time out occurs, restarts the procedures go to step 4 above
Step 9: External attacker exploits VM1 by sending a download file
Step 10: VM1 downloads the file that contains exploit without knowing
If the external attacker can access and get a screenshot of what VM1 is accessing, then go to step 12 else go to step 13
Step 11: Internal attacker to scan and access the entire network without exploit (scan target 192.168.3.0/24). If the internal attacker can scan and access the network then go to step 12 else go to step 13
Step 12 Weakness has been demonstrated
Step 13 Stop, connection established in cloud

Exploited Virtual Machine

Fig 2 shows a machine that has been captured by an attacker and screenshot has been taken on what the virtual machine is accessing. Meterpreter shows that a session has been created between the virtual machine and an attacker. Ls command shows the partitions and the files that an attacker can access the user's machine. The results were as expected, as shown in fig 1.

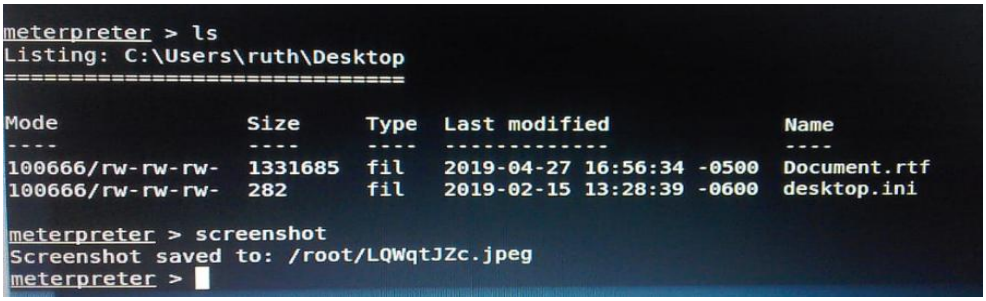

Fig 1 Exploited Virtual Machine

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

The screenshot file

The screenshot shows the external attacker has gained access to the user's machine and has a screenshot of what he or she is accessing on the machine. The results were as expected, as shown in Fig 2. This shows that the firewall could not detect unknown attacks. The operation was mostly based on signatures for known-bad software, so systems are not ready for day-zero exploits for which signatures are not yet available.

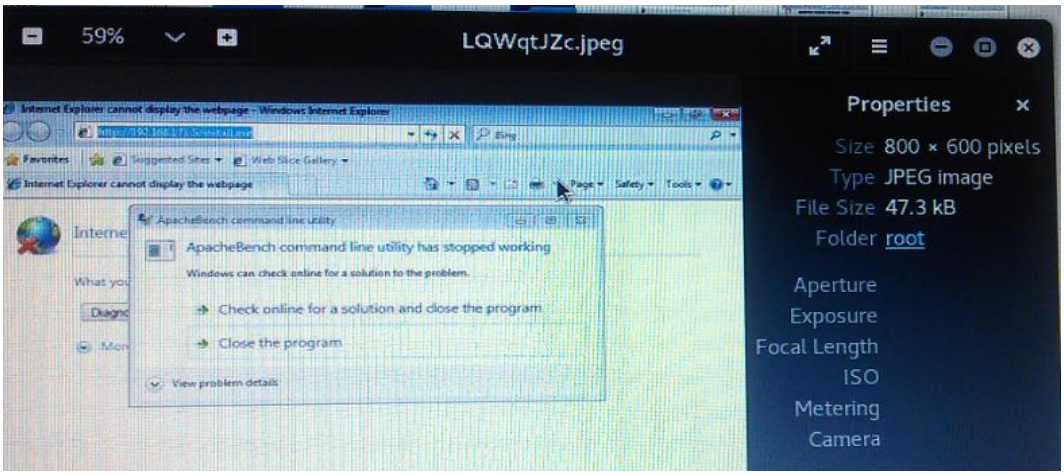

Fig 2: Screenshot file

Scanning by the Internal Attacker

Attacker net1 is a virtual machine on the network. Here the internal attacker can scan the network as shown in fig 3. The exploiting tool used for scanning was Zenmap. Intense scanning is a compressive scanning of the network. It scans all TCP ports. While a scan is running and after it completes, the output of the nmap command is shown on the screen. The nmap-T4-A-V 192.168.3.0/24command was used to scan the entire network server for any opened ports by the internal attacker. Then the nmap command was used to scan and report the IP addresses. The results were as expected. Next, NMAP output was used to view the metadata and display the information. There were four hosts' machines with opened ports such 445, 22, and 135 which was on the network server. Nmap scans do not use the pivots you have set up. This means that the firewall could not detect threats from the internal attacker.

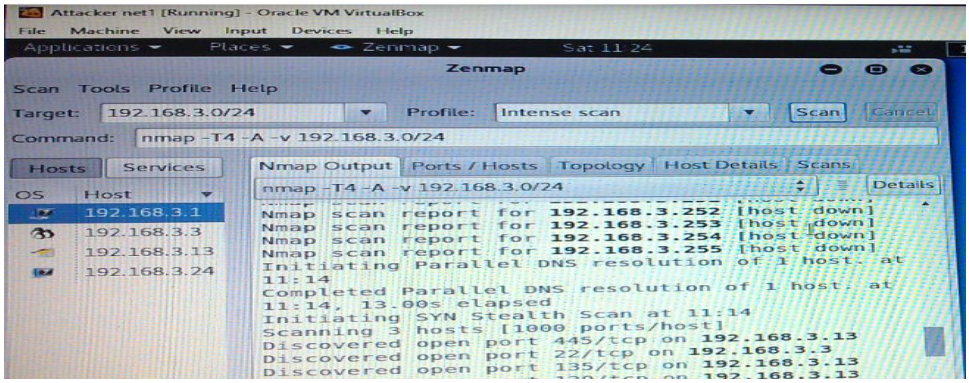

Fig 3: Scanning by Internal Network

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

Algorithm for demonstrating weaknesses of IDS

Step 1: Start
Step 2 User: User request to be signed up in the IDS server
Step 3 Actors: Verifies and add the user to the server
Step 4: IDS server prompt user to enter username and password

a. The user enters username and password
b. Server checks username

If username does not exist in the file system it sends invalid username to go to step 2
Step 5 Short descriptions: Login verifies user access to firewall server based on username and password pair that is entered by the user on the end user device (personal computers or iPad or smartphone)
Step 6 User initializes the devices used in the server at the same time
Step 7 Pre-condition: User is connected to the network (tested through IP address ping with VM1, external attacker and the IDS server)
Step 8 Invariant: If time out occurs, restarts the procedures go to step 3 above
Step 9:VM1 accesses the website on the internet
Step 10: IDS server views the site and sends a report as a threat alert then go to step 12 else go step 13 (false positive)
Step 11: External attacker manages to send an exploit file to VM1. If VM1 downloads the file and IDS server fails to detect it go to step 12 else go to step 13 (false negative)
Step 12 Weakness has been demonstrated
Step 13 Stop, connection established in cloud

Demonstration of the existing Weaknesses of the Intrusion Detection system

In the IDS demonstration, the weaknesses that were tested are a false positive and false negative. False positive is when snort used in IDS is sending an alert of attack while the user is accessing a website. A false negative is when an external attacker is able to hack on the user's pc without being detected by the snort used in IDS.

False Positive

A false positive is an instance where an IDS incorrectly identifies a normal activity to be malicious. During normal operation, an IDS can generate thousands of false alarms per day. Network intrusion detection systems no matter if they are anomaly-based or signature-based - share a common problem: the high number of false alerts or false positives. These problems usually cause the user, the network administrator to lose confidence in the alerts, lower the defence levels in order to reduce the number of false positives or to have an overload of work to recognize true attacks due to IDS mistakes.

False alert

This is the example of the false alert, while site accessed is actually a website. The results as shown in fig 4 curlhttp://www.testmyids.com/ this a website the user's pc is accessing. The website was found to contain data such uid=0(root) gid=0(root) groups=0(root). cat/var/log/snort/snort.log.1556536332 commands read the alert log from snort and gather the list of critical ports to give a report of the file. It was found out that snort gave a report of the live attack. The report also shows the content type, length of the file, date and time accessed. It further gives the server the file is received from and the last time the file was modified. The result was as expected, as shown in fig 4. This weakness of false positive can be curbed by developing a strong technique that would only detect an alert when it happened.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

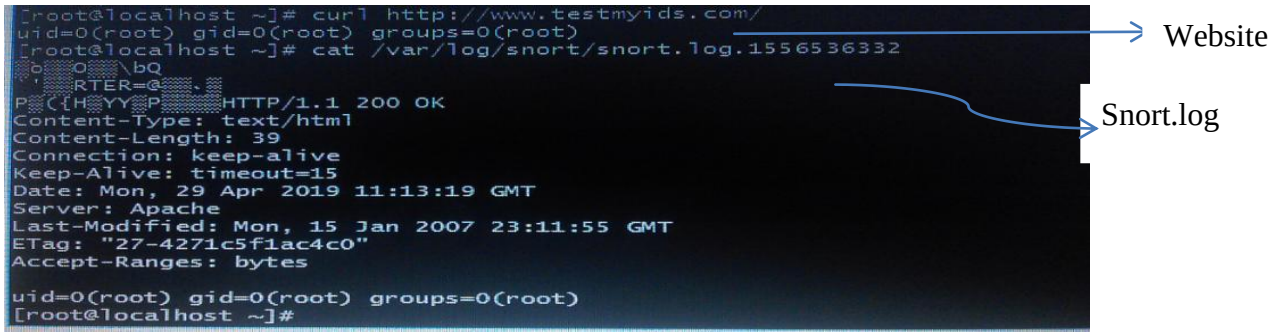

Fig 4 False Alert

Launching an Exploit

Metasploit was used to launching an attack on the virtual machine. The external attacker to the virtual machine to gain access to the machine launches Metasploit. This is done through the network in our case it through the IDS to demonstrate its weakness on the false negative. Metasploit V5.0.10.dev was used as a hacking tool and file system was used to store the file. The exploit commands were used to launch the hacking tools. It was then found out that, the attacker gained access to the user's machine through the interpreter as mention in fig 5.

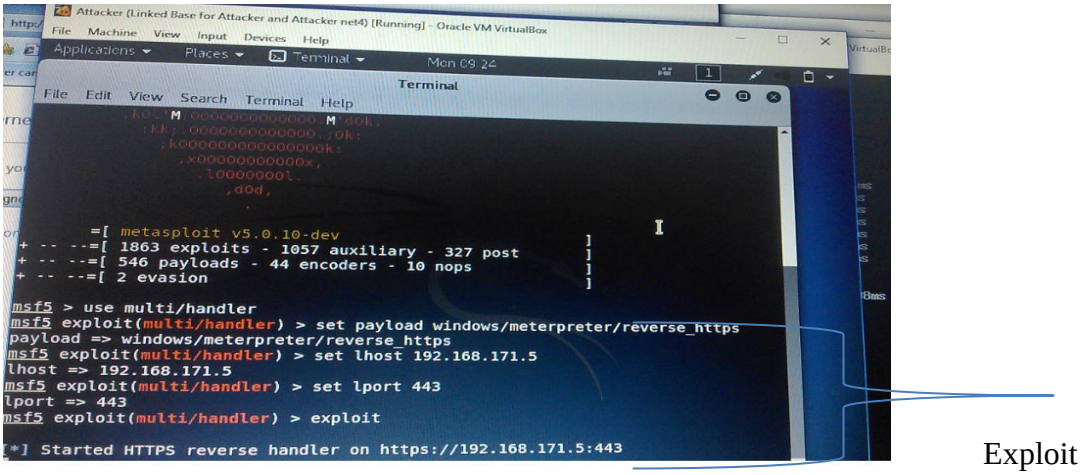

Fig 5 Launching an exploit

Downloaded File

This is to show that the exploit has been sent and the virtual machine is requested to download the file. Fig 6 shows a virtual machine trying to run a file that contains an exploit. This is an example of a file that can be downloaded while it has been sent by an attacker. When the virtual machine goes ahead to download the file then the attacker gains access to the machine. The information of the file is also indicated. That means the file is from the IP address of 192.168.171.5 and the URL is http://192/168.171.5/install.exe. Once the file is downloaded and saved the machine is automatically in the hands of the hacker who has an IP address of 192.168.171.5 as shown the fig 6.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

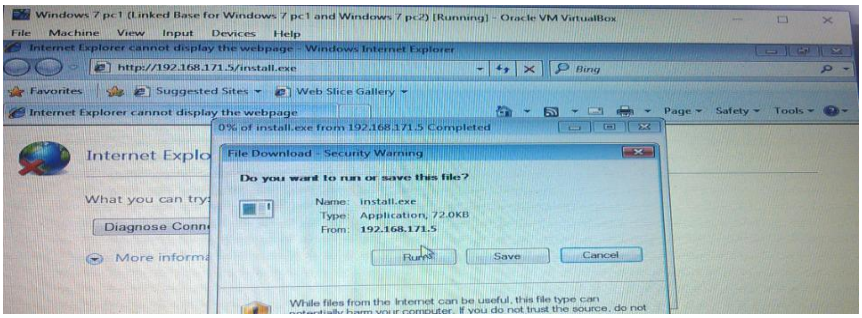

Fig 6 Downloaded File

Virtual machine versus the Attacker's machine

This shows proof that the attacker is accessing the virtual machine and can screenshot what the user in the virtual machine is doing in the machine. It also shows how the attacker saves the file and where it is saved. Fig 7 shows an attacked machine on the left and the right side shows that an attacker can see everything the being done in the virtual machine. The attacker has gained access and can do anything with the virtual machine. Fig 7 shows files downloaded by an attacker from the virtual machines where they are stored. All the information acquired the virtual machine are stored in the home directory and can be accessed by the attacker.

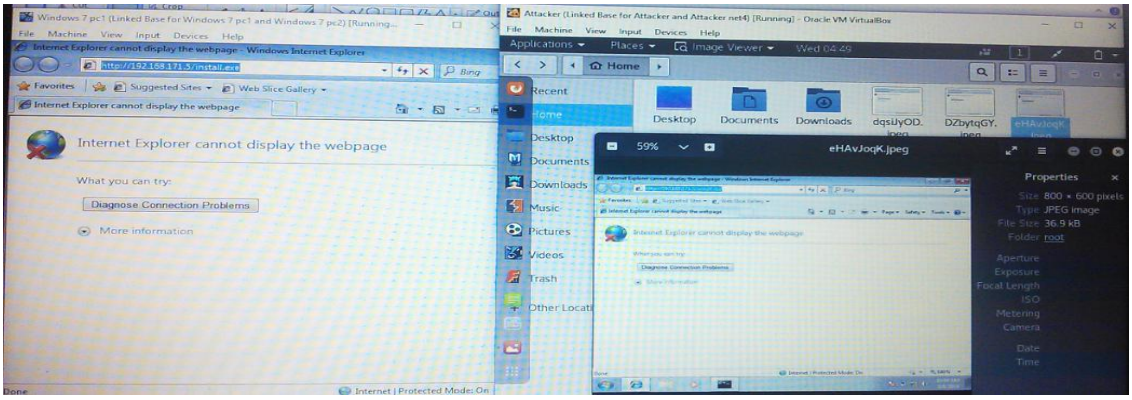

Fig 7 Virtual Machine versus the attacker's machine

False negative

False negative occurs when the IDS fails to detect malicious activity. Although the issue of the IDS not being able to detect malicious data is still a problem and is something that still needs further investigation, reducing the false alarms should be the main priority.

IDS router connection

The IDS could not detect the attack on the virtual machine, which is on the network. The IDS connection is established with the virtual machine and the attacker but could not detect an attack thus demonstrating the false negative. The IDS in this research used the snort. In the IDS server, it shows that there is a communication between the snort with the external attacker and users' machine but it could not detect the attack used to attack the user's machine. It was found out that it could not report on the Metasploit file downloaded by the user as a hacking tool thus demonstrating the false negative. The IDS could connect to the virtual machine with an IP address of 192.168.10.28 that is presumed to be under attack by the external attacker. It can also connect to the external attacker through the IP address of

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

192.168.171.5 without detecting an exploit. The results as shown in the figure above show communication between the server and the machine, and could not detect the attacks.

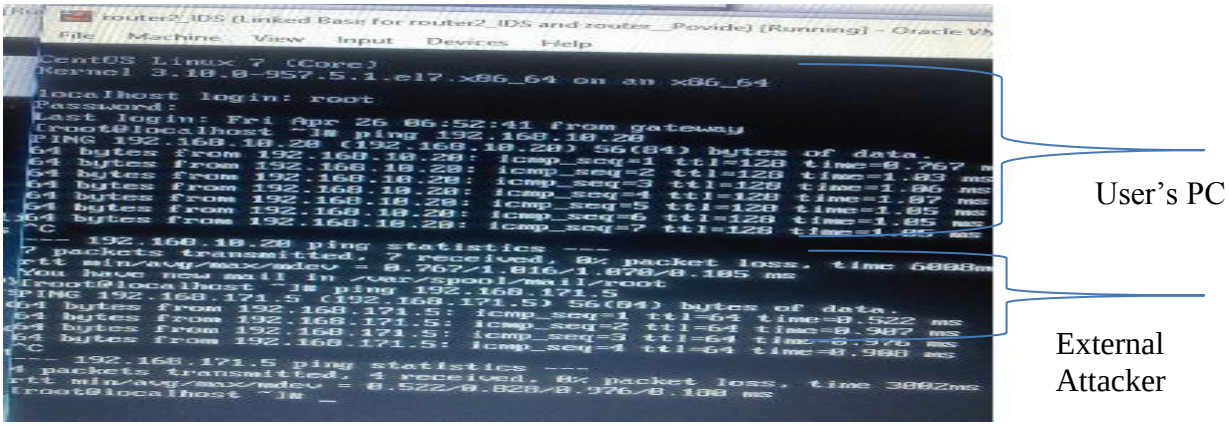

Fig 8: IDS Router connection

V. CONCLUSION AND RECOMMENDATIONS

The emphasis of the research was Cloud computing environment, which offers users access to computing resources that can be hosted at the premises of the Cloud Service Provider (CSP) or in remote locations. It offers benefits like cost saving, convenience, and scalability but it is not without challenges, especially in terms of security, as it can be influenced by criminal activities, as indicated by the Cloud Security Alliance (CSA). Increasing cost of cybercrime and the growing adoption of Cloud by organizations has demonstrated that there is need for policy violation detection model in the cloud environment. However, the architecture of the Cloud, where computing resources are shared together, along with its multi-tenancy and the ease with which resources are released and reallocated, all contribute to making policy violations. This refers to a procedure such weakness identification, demonstration, experimentation, and evaluation. More positively, the resources offered by the Cloud can be influenced not only for illegal purposes but also for weak policies. Therefore, the first weakness of firewall was demonstrated through an experiment. The test was done on the firewall to demonstrate if an internal user on the network can scan the network. The weakness was achieved. The second test was on the penetration of external user using a Metasploit exploit tool to gain access to the user's machine by sending a download file. The second weaknesses of IDS/IPS were demonstrated through the false positive and false negative. False positive was demonstrated by a user's virtual machine accessing a website while the IDS report it as an attack. The other demonstration was on false negative where the external user managed to gain access to the user's machine without being detected by IDs.

The experiments demonstrated and verified the weaknesses of firewall and IDS, but went further than this to determine it in relation to the cloud environment. It was found that there are two stages of testing that is penetration and scanning stage. There is a required tool to curb the weaknesses through scanning and detecting true attacks. The researcher encouraged a futuristic evaluation of the proposed model, as it would provide an assessment that would help enforce operational tests that may end up providing confidence, based on the performance of the model. Further improvements will allow the model to adapt easily to various scenarios. It is the researcher's opinion that if extensive research on the suggested future work is conducted, then POVIDE model adaptation in the cloud environment will be more accepted.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 9, September 2019

REFERENCES

[1]Bulajoul, W., James, A., & Pannu, M. "Improving network Intrusion Detection System performance through quality of service configuration and parallel technology" *Journal of Computer and System Sciences*, *81*(6), pp. 981-999, 2015.
[2]Hameed, A., Khoshkbarforoushha, A., Ranjan, R., Jayaraman, P. P., Kolodziej, J., Balaji, P., & Khan, S. U. A survey and taxonomy on energy-efficient resource allocation techniques for cloud computing systems. *Computing*, *98*(7), pp. 751-774, 2016
[3]Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U., "The rise of big data on cloud computing": Review and open research issues. *Information systems*,Vol *47*, pp.98-115, 2015
[4]He, X., Chomsiri, T., Nanda, P., & Tan, Z. (2014). Improving cloud network security using the Tree-Rule firewall. *Future Generation Computer Systems*, vol *30*, pp. 116-126, 2014
[5]Hu, H., Han, W., Ahn, G. J., & Zhao, Z. "FLOWGUARD: Building robust firewalls for software-defined networks" In *Proceedings of the Third Workshop on Hot Topics in Software-defined Networking ACM*, pp. 97-102, 2014
[6]Jabez, J., & Muthukumar, B. "An Intrusion Detection System (IDS): Anomaly detection using outlier detection approach" *Procedia Computer Science*, vol *48*, pp. 338-346, 2015
[7]Modi, C. N., Patel, D.R., Patel, A., & Muttukrishnan, R. "Bayesian Classifier and Snort based network intrusion detection system in cloud computing" *Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*, pp. 1-7, 2012
[8]Riaz, A., Ahmad, H. F., Kiani, A. K., Qadir, J., Ur Rasool, R. A. I. H. A. N., & Younis, U. "Intrusion Detection Systems in Cloud Computing: A contemporary review of techniques and solutions" *Journal of Information Science & Engineering*, Vol 3, pp. *33*, 2017.
[9]Vieira, K., Schulter, A., Carlos, B., Westphall, C., & Westphall, M. "Intrusion detection for grid and cloud computing", *IEEE Computer Society*, pp. 38-43, 2010
[10]Xu, H., Zhou, Y., & Lyu, M. "N-version obfuscation" In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security* pp. 22-33, (2016)
[11]Zhang, Q., Cheng, L., & Boutaba, R., "Cloud computing: state-of-the-art and research challenges" *Journal of internet services and applications*, Vol1, pp. 7-18, 2010
[12]Zhang, Z., Zhang, W., Wang, J., & Chen, X. "An Effective Cloud-Based Active Defense System against Malicious Codes" In *Information and Communication Technology-EurAsia Conference* pp. 690-695, 2014