Cloud Intrusion Detection System

Muhammad Hanis Bin Norli
Universiti Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail,
Kuala Lumpur, Malaysia
muhdhanisnorli@yahoo.com

Mardiana Binti Mahari
Universiti Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail,
Kuala Lumpur, Malaysia
mardianam@unikl.edu.my

***Abstract*—Issue of security is very paramount in any organization, especially organization that has confidential data. Therefore, this project intends to aid in security of the company by introducing intrusion detection system to the cloud service. This project is not just the normal intrusion detection system that only detect malicious packet in the network, it is a project that has notification alert to users. By this, the users will receive notification in the router interface which is installed in the router. With the help of IDS, notification will be prompt to the users of any malicious attacks that are happening to their system.**

Keywords—Snort IDS, Cloud, Router, OpenWrt.

I. INTRODUCTION

Malicious packet and intrusion of network are problems that cannot be regarded as trivial. The problem of network intrusion especially in cloud service is an issue that will not go away by itself. The problems are particularly complicated by the advance of new technology that will lead to more intrusion. Installing intrusion detection system will help the cloud service to detect any intrusion that might happen. The IDS represent as a protection to the cloud network making it able to recognize malicious packets or intrusion events. This is especially needed to cloud service since security is the most important key for a cloud to gain customers trust.

Over the past decade, the security of confidentiality data and security of information have become major global issues. Face with problems such as the increasing number of intrusion tools over the years. This project therefore offers great opportunities for Information Technology sectors. With IDS installed over the cloud, it is important to focus on intrusion areas that are usually seen by hackers. These are the key security that should be monitored at all times without hesitation. With the added benefits of alerting the users, a safe and secure system can be created where network administrator can monitor their cloud service all the times. This system can detect any intrusion on the system and has the ability to prompt notifications that will notify administrator of the system. The intrusion detection system is to be installed on cloud service to provide protection and detection from malicious packets. Current intrusion can be detected and alert the user through router interface.

II. RELATED WORKS

A. Faster and effective IDS

With the advent of anomaly-based intrusion detection systems, many approaches and techniques have been developed to track novel attacks on the systems. The most significant open issues regarding Anomaly based Network Intrusion Detection systems are identified, among which assessment is given particular emphasis. The presented information constitutes an important point to start for addressing Research & Development in the field of IDS. Countermeasures which are faster and more effective are needed to cope up with the attacks ever-growing. We find that the majority of surveyed works do not meet these requirements. On the whole, the findings confirm a common trend in the experimental computer science [1]. It is clear that IDS alone are not enough to protect our network whether we are using anomaly or signature-based IDS. With the help of slack application, user can be alert to the incoming intrusion and do immediate action.

B. Limit of IDS

The normal and abnormal behaviors in networked computers are hard to forecast, as the limits cannot be explained clearly. This prediction method usually generates fake alarms in many anomaly-based intrusion detection systems. The concept of fuzzy logic is to reduce the fake alarm rate in determining intrusive behavior. The set of fuzzy rules is applied to identify the normal and abnormal behavior in a computer network. The authors proposed a technique to generate fuzzy rules that are able to detect malicious activities and some specific intrusions. This system presented a novel approach for the presentation of generated fuzzy rules in classifying different types of intrusions. The advantage of their proposed mechanism is that the fuzzy rules are able to detect the malicious activities. But they failed to implement the real time network traffic, more attributes for the classification rules [2]. This shows that the systems are not able to capture information about the attacks. With this project, the IDS will have the information of the incoming attacks as the attacks will be notified to the router interface. Since users are connected to the network of the router, they can take immediate action of incoming intrusion to the system.

C. Network attack on cloud

The common network attacks affect the cloud security at the network layer which includes Address Resolution Protocol (ARP) spoofing, IP spoofing, port scanning, man-in-middle attack, Routing Information Protocol (RIP) attack, Denial of Service (DoS) and Distributed Denial of Service (DDoS) [3]. Therefore, providers must protect the systems against both insiders and outsider attacks. The traditional network security channels like firewall can be used to stop many outsider attacks but attacks from within the network as well as complicated outsider attacks such as DoS and DDoS attacks can't be control easily by using such mechanism. To overcome such problems, an intrusion detection system (IDS) comes into play. The IDS play very important role in the security of cloud and instead of detecting only known attacks, it can detect many known and unknown attacks.

D. Virtual cloud IDS

Many efforts have been taken in the area of Cloud computing and intrusion detection system but still there are more attacks that have not been detected. In, the researchers worked in this field to overcome the current security threats in the Cloud computing through implementing IDS in Cloud environment which is responsible of monitoring the utilization of resources for the virtual machine using data acquired from virtual machine monitors [4]. The project has chosen three types of attacks in the cloud for IDS to detect and prevent. The types of attacks are port scanning, denial of service and backdoor.

E. Cloud Protection

IDS is the first technique to be chose as the most important technique. It is because IDS play an important role to detect malicious packets. Before able to prevent, detection must come first before able to know the type of attack to be blocked. The Intrusion Detection System (IDS) is used to detect many kinds of attacks behavior that can compromise the security of the web application system. These kinds of attacks that can be detected by the IDS include Worms, Viruses, unauthorized logins, access to sensitive files and folders, increase access privileges [5].

III. PROTOTYPE SYSTEM

Prototype of cloud storage is run from a private network. Administrator and users can login from a laptop, desktop, or Android device and have access to the same workspace regardless what type of device they are using within the same network. This prototype provides the users to access share drives, browse the internet and functions just as other router would. Moreover, the prototype includes IDS protection, user privilege access and data storage to be shared among the users. The development process consists of several stages starting with hardware and software installed to the router. There are steps need to be done in order for the router to work with the IDS. The Router need to be installed and configured correctly in order to success in developing IDS with cloud service.

The system that is to be implemented consists of the following goals and objectives:

- To study how intrusion detection system can protect Cloud service.
- To develop intrusion detection system that can notify user of intrusions.
- To test the intrusion detection system on cloud service.

Figure 1 shows the logical diagram which includes cloud IDS and end devices.

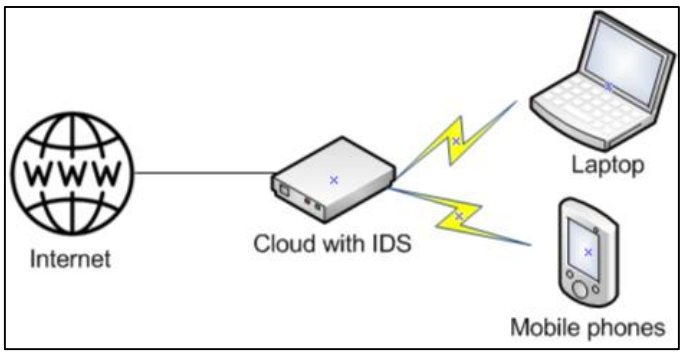
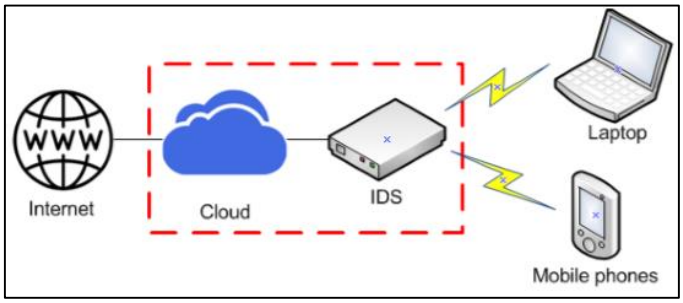


Figure 2 shows the physical diagram which includes cloud IDS with detail and end devices.



IV. TESTING AND RESULT

To ensure the prototype meet the objectives of project, several testings have been used in order to test the prototype. It is very important to meet the objectives since security is the key for Cloud and the Snort IDS.

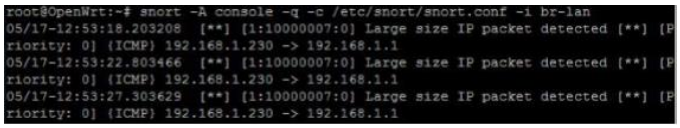
The attack testing has been done to show the different type of attacks aiming the router. Detection of attacks have been recorded during the duration of attacks. All data and result has been shown with the installation of Snort IDS to the cloud storage network.

A. Denial of Service Attack

Denial of service attack is well known among hackers to target a network. The aim of denial of service attack is to shut down a machine or network, making it inaccessible to its intended users. Users will not have access to the network, therefore accessibility is being compromised. DoS attacks accomplish the attack by flooding the target with traffic or sending it information that triggers a crash. Usually large

packets size will be used to make the attacker accomplished their target.

Figure 3 shows Cloud IDS able to detect DoS.



B. Host Discovery Attack

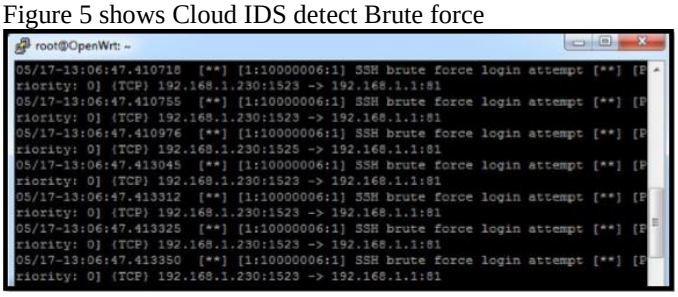
Host discovery attack is also well known among network attackers. Aim of a host discovery attack is to know the status of an IP address whether it is up or down. If the IP address found to be up, this means that host is currently using the network and is on uptime. However, if the IP address found is down, this mean that the host is not using the network and is on downtime. Network attack can only be done when the host is connected to the network. That is why this attack is very crucial to be detected and stopped at the same time.

Figure 4 shows Cloud IDS able to detect host discovery.

C. Bruteforce Attack

In cryptography, a brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. Aim of a brute force attack is to try any possible password to match with the victim's password. Usually, the dictionary of brute force attack will contain millions of words and usually in very large size. Some hackers will share their dictionary with others as well to keep the dictionary update as possible. Brute force attack can be done in many operating system as attacker only need the login page of the network. Windows operating system will be used for brute force attack the Cloud IDS login page.

Figure 5 shows Cloud IDS detect Brute force



Results

DENIAL OF SERVICE ATTACK ATTEMPT	CLOUD IDS DETECTION
1	SUCCESSFULLY DETECT
2	SUCCESSFULLY DETECT
3	SUCCESSFULLY DETECT
4	SUCCESSFULLY DETECT
5	SUCCESSFULLY DETECT

From DoS attack's result, all attempt of the attacks are successfully detected by Cloud IDS. This shows that Snort IDS protect and alert all the DoS attacks from being harmed. DoS protection and alert is needed now more than ever, as attacks continue to increase very rapidly. Accessibility is very important in a network security to maintain services.

HOST DISCOVERY ATTACK ATTEMPT	CLOUD IDS DETECTION
1	SUCCESSFULLY DETECT
2	SUCCESSFULLY DETECT
3	SUCCESSFULLY DETECT
4	SUCCESSFULLY DETECT
5	SUCCESSFULLY DETECT

From host discovery attack's result, all attempt of the attacks are successfully detected by Cloud IDS. Cloud IDS is able to alert users of host discovery attacks which are using network mapper. It is very important to know a system being discovered by other attacker in order to stop the attack. This is because attacker will run host discovery attack before continuing with next attack.

BRUTE FORCE ATTACK ATTEMPT	CLOUD IDS DETECTION
1	SUCCESSFULLY DETECT
2	SUCCESSFULLY DETECT
3	SUCCESSFULLY DETECT
4	SUCCESSFULLY DETECT
5	SUCCESSFULLY DETECT

From this brute force result's analysis, all attempt of the attacks are successfully detected by Cloud IDS. Brute-force attacks work by calculating every possible combination that could make up a password and testing it to see if it is the correct password. It is very crucial to have more attempt with brute force attack since the attacker will try to brute force as many times as possible to get the correct password.

V. CONCLUSION

The rationale for installing IDS is almost always to protect a private network against intrusion. In most cases, the purpose of the IDS is to detect malicious packets that are entering the network, and often to prevent unnoticed and unauthorized packets which are tagged as malicious or abnormal. IDS implementation is so important because maximum security is much needed nowadays. We must not forget about the important of having notification as well. Malicious packets can be detected before entering our network. This will give extra protection to our network.

The notification of Snort IDS provides an additional layer of defense, sending notification of any intrusion alert in the network. This follows the classic military doctrine of "defense in depth," which is just as applicable to IT security. Along with intrusion detection system, the cloud can be protected. With this project, users can acknowledge the incoming intrusion faster through their mobile phone and computer with ease. Cloud service will be protected even more than other cloud service without IDS and notification alerts.

REFERENCES

[1] Akash G Mohod, S. J. (2013). Analysis of IDS for Cloud Computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM).

[2] Hassan, M. M. (March 2013). Current Studies On Intrusion Detection System, Genetic Algorithm And Fuzzy Logic. International Journal of Distributed and Parallel Systems (IJDPS).

[3] Hassen Mohammed Alsafi, W. M. (2012). IDPS: An Integrated Intrusion Handling Model for Cloud. Faculty of Information and Communication Technology.

[4] Snehal G. Kene, D. P. (2015). A Review on Intrusion Detection Techniques for Cloud Computing and Security Challenges. International Conference on Electronics and Communication System.

[5] V.Jyothsna, V. P. (August 2011). A Review of Anomaly based Intrusion. International Journal of Computer Applications (0975 – 8887).