eISSN:2600-7920
INTI JOURNAL
Vol.1, 2018 (16)

Study on Security Testing-as-a-Service (TaaS) in Cloud Environment

[1]Ponkoodalingam Kannan, [1]Gai Vincent, [1]Deshinta Arrova Dewi

[1]Faculty of Information Technology and Sciences (FITS), INTI International University, Nilai Negeri Sembilan Malaysia.

Corresponding Author: pon.kannan@newinti.edu.my, Deshinta.ad@newinti.edu.my

Abstract

Cloud computing in the 21st century is nothing new in the IT field. Cloud computing is a myriad group of servers where it stores data remotely in a data center. With today's technology, cloud computing has changed on how the way of a user getting resources and managing services and solutions. This leads to the offering of Software-as-a-Service (SaaS) for clouds where it eases the user from using daily applications. However, the improvement in technology is also directly proportional towards the increase of security threats towards cloud environment. Thus, in order to provide the cloud services successfully, the cloud needs to be tested and audited before deploying to the public. This research aims to critically study on the threats that may jeopardize the cloud and provide a solution on how to improve the security of cloud computing. Two scenarios are included in the study with its virtualization. The data and network integrity attack are conducted as part of security testing.

Keywords

Cloud testing; cloud computing; security testing.

Introduction

Cloud computing is first established its meaning and definition back in 1996 when an inside information from Compaq is mentioned but then the term is only popularized in 2006 when Amazon releases its cloud computing Amazon EC2 (Regalado, 2011). Cloud computing is nothing but a group of supercomputers (or what we knew as a data center) that are connected remotely (i.e. located in different regions or even continents) in order to provide users with their usage of computers without having the needs to have a bulk computer equipment. In fact, nowadays most of the daily operation that a user would use (e.g. E-Mail, Office365 and Amazon Web Services) are all operated by cloud. The services are thus known as Software-as-a-Service (SaaS) (Malhtra and Jain, 2013).

However, with the improvements and advancements in cloud services, security threats became an issue; especially all data are kept remotely; i.e. the clients do not have the physical access to the server itself. Thus, the level of security needs to be the hot issue and at the same time,

how can the network engineers ensure that the network is secured enough? Therefore, the following chapters will be explaining on the security for the cloud computing and focusing mainly in Security Testing-as-a-Service (TaaS).

The entire aim of the research is to study how safe the current cloud computing is and how to improve the security of the cloud by conducting security testing. Cloud computing is a new way of branding for the computer; transforming the IT industry. Cloud computers have two parts, application delivered as services (Software-as-a-Service; SaaS) and the hardware and software systems in the server that provides the services (Bai, Li, Chen, Tsai & Gao, 2011).

However, there are certain issues that cloud computing is facing in order to have an effective cloud testing. There are multiple questions that are being asked despite different research papers addressing software testing are published but not many results have been tested and executed in the real world. Since security is and will always a major issue, the author will need to look into the issues in security and quality assurance for the clouds and the SaaS. Thus, in order to have a better understanding of cloud computing and cloud testing-as-a-service (TaaS), it is very crucial to have the best applicable facts finding methods for the project. Thus, the author has used the approach of primary and secondary research in order to gain more info.

Methodology

The primary research for the project is to be conducted by interviewing individuals who have the most experience working and dealing with cloud computing but dealing with testing of the cloud is very rare as per discussed earlier in Malaysia market. Thus, these individuals are highly crucial as they might provide the most important key points and function input for the system. Besides that, an observation of how the cloud is being operated and tested is a way of doing research that allows the developer to be able to have a clearer and better understanding on how cloud computing works and takes place in terms of daily operation.

The secondary research method for this research is towards the searching published article. Published journals are used to study and review in order to have a better understanding of cloud computing and proposed methods or suggestions on how can secure the cloud computing by conducting testing. Reliable sources such as IEEE and ACM provide and insight and a thorough description of the cloud. Next, the design of the proposed Testing as a Service (Taas) is outlined as depicted in figure 1 below.

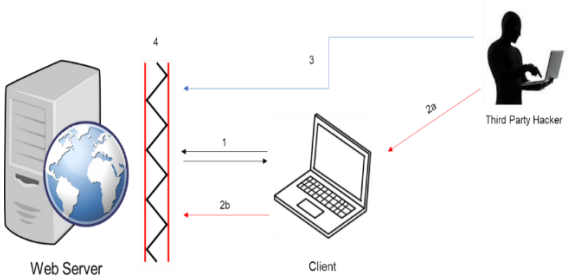

Figure 1. The concept of the TaaS in this paper

This paper focuses on two different types of situation as a comparison for with and without the services to protect the cloud. Web server is used as a representative for cloud computing as a web server and it is considered as one of the software-as-a-service (SaaS) that is offered in cloud computing.

Situation #1: Without (4), protection service

1. Client ensures that there is a communication process ongoing together with the web server.
2. Third party hacker launches an attack through the client and from the client it poses as the legitimate user to exploit the web server.
3. Third party hacker is able to access the server by intercepting the client-server transaction and make damages.
4.

Situation #2: With (4), protection service

Third party hacker will need a longer time and possibly making the hacker to have a very small percentage to be able to break the protection service that is deployed.

In response to both situations, a virtualization is considered fundamentals of the cloud competing where it delivers the shared computing resources, software or data as a service through the Internet. Then it comes to the context where there is the existence of a private and public cloud. Private allows the tenant of the cloud to utilize fully of the resources of the computer that has been divided and managed through a virtual machine while public cloud is open to everyone to use; in which the resources are limited to be used (Angeles, 2014).

In this paper, a list of testing criteria is developed that should fulfill the requirements and objectives. The action or the testing is considered as a successful testing. While the criteria are not met, the testing of the steps is considered as failed. A failed step should be rechecked and identified to see what went wrong and how can the system be improved to meet the criteria. Since this research is based on a current existing intrusion detection system but with only addition of the author's own rules on how to make the program more efficient, the passing or fail criteria for this project would be a simple one but strict criteria as if any one of the criteria did not pass, the entire project would be considered a failure. The amendments need to be made until the system or the rules satisfies the criteria. The passing criteria for the testing are as follows:

- Both IDS is able to read the rules implemented by the author.
- Both IDS is able to run after the additional addition of the rules.
- Attacks are detected by the IDS using the rules implemented when the attack begins.

Results and Discussion

Table 1 shows the result of the unit testing for network communications among the virtual machines. The purpose of this testing is to find out whether can the virtual machines communicate with each other. Thus, a simple test is done by conducting a ping of IP addresses from the virtual machines. The result of the ping indicates that all three computers can ping among each other. Thus, the testing is a success.

Test No	1	
Test Name	Network communications among virtual machines.	
Objective	To ensure that the virtual machines are able to communicate with each other.	
Step No	Test Description	Expected Result
1	Ping the IP address of the participating virtual machines.	All computers able to ping each other.

Table 1. Network connection among virtual machines

Table 2 refers to the result of unit testing for OSSEC rules configuration. The purpose of this testing is to find out whether both the server and the agent is able to include in a set of additional rules that will be used to monitor for data integrity attack. The result of the testing indicates that the rules are successfully implemented and the server-agent is able to begin to monitor, making the result a success.

Test No	2			
Test Name	OSSEC rules configuration.			
Objective	To ensure that the server and agent are having a set of rules that will be used to monitor for data integrity checksum attack.			
Step No	Test Description	Expected Result	Result Outcome	Pass?
1	Launch the OSSEC agent for Windows environment.	OSSEC agent can be launched.	Similar to the expected result.	Yes
2	Open up the configuration from the interface and update the configurations for the agent.	Configurations can be updated and saved.	Similar to the expected result.	Yes
3	Open up the rules folder in the OSSEC Server under Ubuntu environment	Rules document can be opened up using *sudo* privileges.	Similar to the expected result.	Yes
4	Update the set of rules for data integrity monitoring.	Rules can be updated and saved	Similar to the expected result.	Yes

Table 2. OSSEC rules configuration

Table 3 shows the unit testing result for OSSEC agent from the Windows environment to communicate with the server. The purpose of this testing is to figure out whether the agent is able to obtain the configuration information from the server in order to communicate and provide the information about the data integrity to the server. The result of the unit testing indicates that the communication is successful as the management console in the server side is able to detect the agent and display out the path and checksum of each directory monitored.

Test No	3			
Test Name	OSSEC agent communication with the server			
Objective	To ensure that the agent is able to get the configuration information from the server.			
Step No	Test Description	Expected Result	Result Outcome	Pass?
1	IP address of the server is identified using *ifconfig*	The IP address is found.	Similar to the expected result.	Yes
2	The pre-shared key generated by the server for the agent	A long pre-shared key is generated.	Similar to the expected result.	Yes
3	The IP address and pre-shared key are entered into the agent's interface in the Windows environment.	The pre-shared key and the IP address can be identified by the agent.	Similar to the expected result and the agent's name is generated.	Yes
4	Connection is established	Management console will be able to see the connected agent.	Similar to the expected result.	Yes

Table 3. OSSEC agent communication with the server

Table 4 shows the result of integration testing for data integrity attack detection. The purpose of the testing is to make sure that the agent and server are able to communicate with each other and the agent is feeding the information back to the server and keep updating on the data integrity of the agent's system. The result came back with everything passed the test where when there is an attack, the value of the checksum is changed.

Test No	Actions	Description	Outcome of Result	Pass?
1	Reading the new rules specified	This action will read the new rules set in order to monitor based on the rules	The system is able to read the rules when the monitoring runs.	Yes
2	Clear of database and initialization of first time reading hash value	This action will clear the pre-existed data in the database and reload the new values	The system is cleared of the old value and updated with the new one.	Yes
3	Specifying the pathway of the monitored file and reload the file integrity information	This action will determine which folder that will be monitored and the initial hash file will be redownloaded.	The pathway is displayed with checksum number in the management console page in Ubuntu environment.	Yes

4	Launch the attack from a remote computer and modify the file.	This action is will demonstrate whether the attack is successful or not	The number of checksum changed is displayed in the management console page.	Yes

Table 4. Data integrity attack detection

Table 5 shows the result of integration testing on network attack detection. The purpose of the system is to test whether the rules of the network intrusion detection system (IDS) is working based on the additional rule set by the author. The result of the testing comes back with full pass after an attack has been launched and alert is generated not only on the command prompt screen but also files generated indicating more details of the attack.

Test No	Actions	Description	Outcome of Result	Pass?
1	Reading of rules set.	This action will read the specified rules for the network rule-based IDS to follow.	Rules are detected and read when IDS is loaded	Yes
2	Launch the IDS using the command prompt.	This action will start the network rule-based IDS.	IDS is launched and ready for attack detection from the command prompt interface.	Yes
3	Launch the attack from a remote computer	This action will now check for the IDS whether is it working or not based on the rules.	Command prompt output produces multiple alerts on the attack.	Yes
4	Log file generated from the alert generated from the command prompt.	This action will then have a folder with the alert and the details of the alert generated.	The log file is generated with the file extension "*.ids"* when the alert is generated from the detection.	Yes

Table 5. Integration testing on network attack detection

Conclusions

As a conclusion, cloud computing is a technology where it serves the purpose of helping the users to be able to use the computing power of a supercomputer without the needs to purposely purchase a supercomputer. Then it comes to the era where cloud computing is used to host multiple virtual machines or as what we know; virtualization where there are multiple plans that any of the cloud hosting providers can offer to allow the users to be able to run multiple instances of operating system and still being able to maximize the performance of the computers; as if each operating system is run on a single computer. With more data being available on the net, the concern of security comes in with the following question: is my data safe online? Numerous news has been reporting on massive breach on cloud servers or servers hosting information of a user where the information is all leaked out and everyone is free to view everyone's information. Therefore, this

paper has proposed a research with the title of Study and Implementation of Security Testing-as-a-Service (TaaS) in a Cloud Environment.

The proposed of TaaS solution is rule-based intrusion detection system where the application of OSSEC and Snort comes in. The implementation own additional rules to the system where the rules will play a role in helping the currently existing rules to protect the system. OSSEC works by checking for data integrity checksum of which the agent will be installed in the system that wants to protect will provide feeds to the remote server on the data integrity from time to time. On the other hand, Snort also works as an intrusion detection system but on a network level. Similarly using the same concept of rule-based, the author has provided a set of rules for Snort to monitor the connection of the system that it wishes to protect. Should there is any attack ongoing, Snort will release multiple alerts stating that there has been a possible attack and an alert file is generated to inform the user that there has been an attack and requires immediate attention. This idea of this project is applied as a final year project for Bachelor in Computer Science at INTI International University.

References

Malhotra, R., Dr., & Jain, P. (2013). Testing Techniques and its Challenges in a Cloud Computing Environment. The SIJ Transactions on Computer Science Engineering & Its Applications (CSEA), 88-93.

Bai, X., Li, M., Chen, B., Tsai, W., & Gao, J. (2011). Cloud testing tools. Proceedings Of 2011 IEEE 6Th International Symposium On Service Oriented System (SOSE). doi: 10.1109/sose.2011.6139087

Regalado, A. (2011). Who Coined 'Cloud Computing'?. Retrieved from https://www.technologyreview.com/s/425970/who-coined-cloud-computing/

Angeles, S. (2014, January 20). Virtualization vs. Cloud Computing: What's the Difference? Retrieved from https://www.businessnewsdaily.com/5791-virtualization-vs-cloud-computing.html