Cloud Computing Ethical Hacking

Kumar Kishan Chandra[1], Dr.AnandKr.Pandey[2], Supriya Raj[3]
Corresponding Author: Kumar Kishan Chandra

Abstract: *The Ethical hacking is a form of penetration testing where the tester assumes the role of a legitimate attacker with permission of system owner. The network and security expert who will attempt to find weakness in the computer system and network in order to inform their owner about their existence. The security risks are known the process of hardening the network & system can take place. This form of penetration testing is becoming more common, as keeping a system virus free during its development. Its extensively more difficult the more complex said system .The extreme time pressure development increases the probability of error, making it easier to test for weakness at a another day. The Cloud computing is a way of computing, where most of our data is stored in the cloud through internet. The Cloud computing capability that provides an abstraction between the cloud computing and ethics. Its underlying technical architecture like servers, storage, networks enabling convenient, ad-hoc network access to a shared pool of configurable computing resources. This can be rapidly provisioned and released with minimum management effort.*

Date of Submission: 30-01-2019 Date of acceptance:16-02-2019

I. Introduction

The Cloud Computing provides us means of accessing the applications as utilities over the Internet. Its allow us to create, configure, and customize the applications online or offline. The term Cloud refers to a Network . In other words, we can say that Cloud computing is something, which is present at remote location. It canbe provide services over a public and private networks, i.e., WAN, LAN or MAN .Applications such as mail, Video conferencing, customer relationship management (CRM) are all execute on cloud.

A hardware is not shared, unauthorized access of data could be restricted easily. Due to more concrete data protection solutions in comparison to a shared a infrastructure model. However it is owning an infrastructure in occurs having to purchase hardware and operating system costs, as the result of maintenance and upgrade the software and hardware. This approach does not allow the infrastructure capacity to measure up or down depending on the current resource demands. The Cloud computing addresses such problems i.e high maintenance cost and adaptable by outsourcing the services in a pay-as-you-go manner. The Cloud computing is still new, ethical discussion is also nascent yet in comparison to that for traditional computing models, hence it needs to be mature. There are different model of services provided by a Cloud computing. A first model of this is Software-as-a-Service (SAAS), where specific online services are provided by Cloud service providers, e.g., Goggle Docs and Drop box services. The second form of this services is infrastructure as a service (IAAS), where hardware resources such as CPU, memory, storage and communication bandwidth are provided for customers. In this self-service model, users can create their own ad-hoc machines and specify its required processing power of the VMs and networking services e.g., firewalls. The example of this model is Microsoft Azure and Amazon web services. The third model is Platform-as-a-Service (PAAS), where besides the infrastructures of a platform to develop an application is provided. PAAS e.g., Apprenda makes the development, testing, and deployment of applications quick, simple, and cost-effective. Although the cloud computing is a promising innovation with various benefits in the world of computing, it comes with risk free. Some of them are discussed below:

Security and Privacy

The biggest concern about cloud computing is data management and infrastructure management in cloud is provided by third-party, it is always to risk to handover the sensitive information to cloud service providers. The cloud computing vendors ensure highly secured password protected accounts, any sign of security breach may result in loss of customers and their business too.

In a Lock In it is very difficult for the customers to switch from one Cloud Service Provider (CSP) to another cloud service Provider. It results in dependency on a particular CSP for service.

In Isolation Failurea risk involves the failure of isolation mechanism that separates storage, memory and routing between the different tenants.

In the Management Interface Compromise public cloud provider, the customer management interfaces are accessible through the Internet or Network .

In Insecure or Incomplete Data Deletionit is possible that the data requested for deletion may not get deleted. It happens because either of the following reasons

- Extra copies of data are stored but are not available at the time of deletion
- Disk that stores data of multiple tenants is destroyed.

1.2 Ethical Hacking

A Ethical Hacking sometimes called as Penetration Testing is an act of intruding or penetrating into system networks& Internet to find out threats, vulnerabilities in the systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major losses. It is a purpose of ethical hacking is to improve a security of the network or internet by fixing the virus found during testing. Aethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the admin of the system for the purpose of improving the security and defending the systems from attacks by external users.Ethical hackers are expected to report all the external users and weakness found during the process to the management. An Informationof security is a state of well-being of information and infrastructure in which the possibility of theft, tampering, and attacking of information and services is kept very low. The ethical hacking is a form of legal hacking done by the permission of an organization or admin to help itsincrease security. Here we discuss many of the business aspects of penetration (pen) testing. How should a pen test be performed, what types can be performed, what the legal requirements are made and what type of report should be delivered for all basic items that we need to know before we perform any type of security testing. Howeverfirst we need to review some security basic task. We must walk before we can run. Next, it moves on to the subject of risk analysis, and it finishes up with the history of hacking and a discussion of some of the pertinent laws. Hacking is a part of computing for almost five decades and it is a very broad discipline, inwhich it covers a wide range of topics. The firstwe know an event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated. A Ethical hacking is the act of finding the possible entry points that exist in a computer system , a computer network(LAN,WAN and MAN) or Internet and finally entering into them.The Hacking is usually done to gain a unauthorized access of a computer system or a network, either to harm the systems or to steal sensitive information available on the computer. The ethical hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for the testing purpose. This term of hacking is what we call Ethical Hacking. A computer expert who does the act of hacking is called a "Hacker".The hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems. The objective of this research the topic of ethical hacking and penetration testing, and compile a course on the subject based on this research.. The security community and professionals linked to it generally take the path of total transparency, making it iseasier for both ethical hackers and legitimate attackers to find information on security risks and threats.

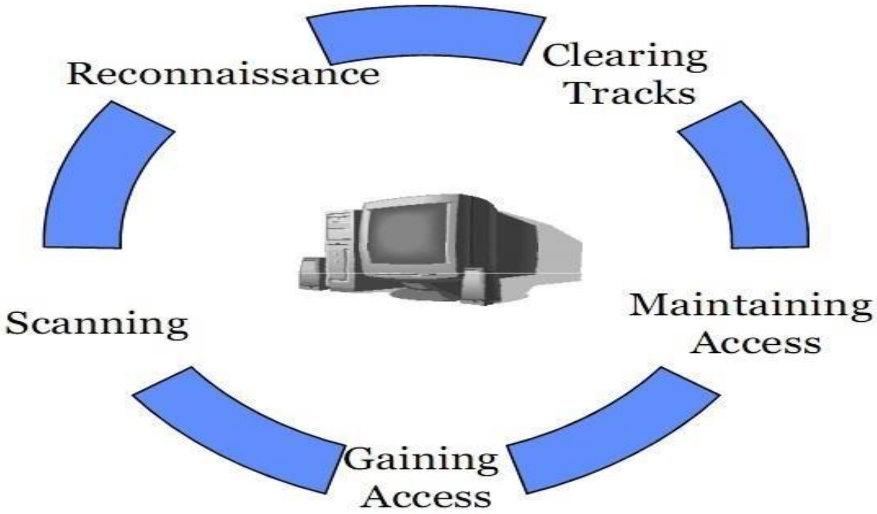
II. Hacking Process

A different approaches to hacking process can be simplified into three different categories: white box, grey box and black boxing, a white box test the penetration tester has all the important information on the network and the credentials necessary to access it.Here this test examines the development and internal workings of the system. In the grey box testing the tester has partial knowledge of the system, usually only the knowledge to complete the test. This analyses the way an insider attack would work – for example how well the security would hold up if one of the employees would attempt to extract secure information. Black box testing is process where the attacker has no prior knowledge of the system or the network and tries to behave exactly like a legitimate assailant. The goal in this test is to find the soft spots of a network in order to secure them against future attacks. The Black box testing is the most common of the all three main approaches. The reason to this is the difficulty, and proportionally the price, of the two others. A white box testing is the most extensive as deep as going through the code written for the system to find any errors and any security issues. All of three of these are important, especially with respect to one another. A best way to assure complete confidentiality and sincerity is to lock a machine in a safe room with no Internet access, but this provides absolutely no availability. There must be a balance between the three and leaning towards a single aspect should be kept to a reasonable and explicable level.The Information Security Management System, also known as ISMS, in the company policy when it comes to IT-related matter. Not at all organisations have an ISMS, but it is recommended especially for larger companies. An ISMS is a long-term plan for security situations. It includes organisational policy for preventive security and the protocol to follow in the case of an attack. Crafting an ISMS can be divided into four stages of a cycle. These stages are sometimes referred to as the "Plan-Do-Check-Act" cycle. A first stage is to plan an appropriate and inclusive security plan for aspecified needs of the organisation . Once that is completed, the next step is to follow this policy while simultaneously evaluating the policy, placing improvements as necessary. The last stage is the act stage where the improvements are implemented. This is the stage under which reaction to an attack fails.

2.1 The Hacking Phase

The five phases of Hacking are as follow:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks



Reconnaissance:-It is a primary phase that the Hacker tries to collect as much as information possible about a target. It includes the Identifying the Target, and finding out the target's IP Address Range, Network, DNS records, etc.

Scanning:- It involves taking the information during the reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase can include diallers, port scanners, network mappers, sweepers, and virus scanners. Hackers are seeking any information that can help them toperpetrate attack such as computer names, IP addresses, and user accounts.

Gaining Access:- After scanning, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2.Herethis is the phase where the real hacking is takes place. Hackers discovered the scanning phase are now exploited to gain access. The method of connection ofthe hacker uses for an exploit can be a local area network LAN, either wired or wireless, local access to a PC, the Internet, or offline. Examplesit includes stack based buffer overflows, denial of service (DoS), and session hacking ..

Maintaining Access:-The hacker have gained access, they want to keep that access for future exploitation and attacks. Sometimes the hackers harden the system from other hackers or security personnel by securing their exclusive access of backdoors, rootkits, and external users .The hacker owns the system, they can be use it as a base to launch additional attacks. In this case, this is referred to as a zombie system.

Covering Tracks:-The hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security to continue to use the owned system, to remove the evidence of hacking, or to avoid legal action. A hackers is try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of the activities during this phase of the attack include steganography, the use of tunnelling protocols, and altering log files. When an attacker gains access to the network connection between the two communicating end appliances they can see and adjust all information flowing through the connection. This isn't an issue if all the target wants to do is browse an online forum without logging in, but in case the target decides to use this unsecured connection to connect to their online bank the attacker can find out personal information or even hijack the session for personal benefit.

III. Ethical Analysis of Cloud Competing

A Cloud computing offers platform independency as the software is not required to installed l on the Computer System .The Cloud Computing is making the business applications mobile and collaborative.

It is the biggest concern about cloud computing that data management and infrastructure management in cloud is provided by the third-party it is always risk to handover the sensitive information to cloud service providers. Just as core technologies, the essential ethical principles of IT remain unchanged with the event of cloud computing. The even though the governing ethics remain largely unchanged, it is important to reexamine them, especially in light of the fact that so much of what they used to be entirely internal considerations of operations and a risk management, hve been entrusted to providers and individuals who sit well outside the direct organizational control. Service providers must beunder stood the operational risk they are assuming for their customers. Providers become straight wards of customer data, functional operation, and risk mitigation. The customers also have a responsibility as they are, most likely, providing services to customers of their own. The consumers of cloud services must have a deep understanding of the technology being utilized and its accompanying risks. The only way to meet this responsibility is to one perform due diligence when considering a third party cloud services provider and two maintain consistent communication with their chosen provider. Ultimately its comes down to some pretty ideas: to be honest, responsible, respectful of privacy, and treat both customers and vendors as we would like to treated. The Cloud computing can reach its full potential if a real, lasting trust is established between providers and customers through a well-defined system of ethics. Industry Perspectives is a content channel at Data Centre Knowledge highlighting thought leadership in the data centre arena. To View previously published Industry Perspectives in our Knowledge Library. It offers businesses online services on demand such as Gmail, iCloud and Salesforce and allows them to cut costs on hardware and IT support.. It analyses the informational duties of hosting companies that own and operate cloud computing datacentres e.g., Amazon. It considers the cloud services providers leasing 'space in the cloud' from hosting companies e.g., Dropbox, Salesforce. And it examines the business and private 'cloudier' using these services. The first part of the paper argues that hosting companies, services providers and cloudier have mutual informational epistemic obligations to provide and seek information about relevant issues such as consumer privacy, reliability of services, data mining and data ownership. The concept of intelligence is developed as an epistemic virtue governing ethically effective communication. The second part considers of potential forms of government restrictions on or proscriptions against the development and use of cloud computing technology. Referring to this concept of technology neutrality it argues that interference with hosting companies and cloud services providers is hardly justified. It is argued to however, that businesses using cloud services e.g., banks, law firms, hospitals etc. A storing client data in the cloud will have to follow the rather more stringent regulations.

History of Cloud Computing

A cloud computing, is a Client/Server computing which is basically a centralized storage in which all the software applications, all the data and all the controls are resided on the server side.A single user wants to access a specific data forrunning a program. Connect to the server and then gain appropriate access, and then it can do business. Then after, distributed computing came into picture, where all the computers are networked together and share their resources when they needed. On the basis of above computing aspects there was emerged of cloud computing concepts .

Around 1961, John MacCharty suggested in a speech at MIT that computing can be sold like a utility, just like a water or electricity. It has a brilliant idea but it like all brilliant ideas, it was ahead in its time, after next few decades, despite interest in this model, the technology simply was not ready for this model .

But timewas passed and the technology caught that idea and after few years that we mentioned it:

At 1999, Salesforce.com started delivering a applications to his users using a simple website. An application was delivered to enterprises over the Internet, and this way the dream come true for cloud computing.

In 2002, Amazon started Amazon Web Services, providing cloud computing services like storage, computation and even a human intelligence. However,they have only starting with the launch of the Elastic Compute Cloud in 2006 a truly commercial service open to everybody.

In 2009, Google Apps also provide thecloud computing enterprise applications.

In 2009, **Microsoft** *launched Windows Azure*, and companies like Oracle and HP have all joined this game. They proves that today, cloud computing has become a mainstream.

In essence cloud computing amounts to three developments that are relevant to an ethical analysis:
1) The cloud due to outsourcing and off shoring of ICT functionality to the cloud.
2) The storage of data in multiple physical locations across many servers they around the world.
3) Interconnection of multiple services across the cloud. At thedifferent levels functionality of different providers is connected to provide a specific service to an end-user.

Cloud computing entails the outsourcing or off shoring of ICT tasks to third party service providers. Any of the information that used to be stored locally is stored in the cloud. The user places his computation and data on machines he can't directly control. Thereby, to a large extend customers or users of a cloud computer service relinquish control over computation and data.In cloud computing a specific service is delivered to a user depends on another system which in turn depends on other systems. A cloud service to the end-users can be built on a framework serviced in the cloud by another company. Cloud computing typically makes use a service-oriented architecture SOA where all functionality consists of services which can be aggregated into larger applications performing functions to end-users .The complex structure of cloud services can make it difficult to determine who is responsible in case something undesirable happens.Data, especially personal data, stored in the cloud should be managed properly. Accountability provides a promising approach to empower users to ensure this is being done. Users of an accountable cloud would be able to check whether the cloud is performing as agreed .For the provision of accountability transparency -adequate information about how data handled within the cloud and it is clear allocation of responsibility are key elements,together with recorded evidence, these elements can be use to decide who is responsible whenever a problem occurs or dispute arises.Since accountability requires detailed records of actions by its users in the cloud, between privacy and accountability .It is therefore important to consider what is being recorded, and who the record is made available .Moreover, as argued earlier, in a de-perimeterised world not only the border of the organizations IT infrastructure blurs, also the border of the organization's accountability becomes less clear .

References

[1]. Lecture Notes
[2]. Tutorials Point
[3]. Springer
[4]. Research Gate
[5]. K.P. Andriole and R. Khorasani. (2010). Cloud Computing: What Is It and Could It Be Useful? Journal of the American College of Radiology. Volume 7, Issue 4, Pages 252-254 (April 2010)
[6]. M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis and A. Vakali. (2009). Cloud Computing: Distributed Internet Computing for IT and Scientific Research. IEEE Internet Computing, vol. 13, no. 5, pp. 10-13, September/October, 2009

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Kumar Kishan Chandra." Cloud Computing Ethical Hacking" IOSR Journal of Computer Engineering (IOSR-JCE) 21.1 (2019): 69-73.