Investigation of Vulnerabilities in Cloud Environment: A Research Analysis

[1]Arti Sharma, [2]Pawanesh Abrol
[1]CMJ University, Shillong, India
[2]Dept. of CS and IT, University of Jammu, Jammu (J&K), India

Abstract

Cloud computing is gaining remarkable popularity currently because of its enormous advantages. However, there are several security challenges associated with cloud environment that inhibit the proper adoption of this technology. The problem of vulnerability is one of such challenges. Vulnerabilities make the system prone to external attacks and problems. Further, these keep on increasing exponentially every year. There is a need to efficiently classify and manage the vulnerabilities and to analyze them for identifying the measures to reduce them effectively. This will improve the security of the system. One way to deal with vulnerabilities is finding them and patch them. Several standards and efficient methods and tools are required to deal with this problem. The present study has been conducted to assess the vulnerabilities in a cloud environment. There are two major objectives. The first objective is to identify and understand different types of vulnerabilities in cloud environment. The second objective is to analyze and propose ways and means for effective handling of different vulnerabilities. On the basis of results obtained, the recommendations have been presented.

Keywords

Cloud Computing, Vulnerability, Security, Risk, Vulnerability Assessment and Management

I. Introduction

Cloud computing is a technology which is used to support maximum number of users, provides elastic services with minimum resources. Cloud computing has become one of the latest technical terminologies because it can be used in many types of applications. Also many companies use cloud computing for their business promotions. In fact, with the advent of cloud computing, various different technologies are being developed which are making the normal PCs to work elastically. Its advantages include characteristics like cost saving, ubiquitous, flexible, elastic, green savings, virtualization, instant scalability, reliability etc. These distinguish it from other technologies [1]. The character of cloud computing is in virtualization. A number of factors can be virtualized such as IT resources, software, hardware, operating system, storage and manage them in cloud computing platform. There are many applications of cloud computing. However, in spite of all this, complete migration to the cloud is not possible. There are various issues which make this technology difficult to implement [2]. One of the significant issues in cloud platform is vulnerability. A vulnerable system cannot be secure. So, to make the security of the system strong, problems of vulnerability need to be removed or minimized [3]. In fact, one of the first steps in securing a computer system is to understand the vulnerabilities in the system that can be exploited to compromise its security. In order to reduce an attacker's chance, it is necessary to keep the system up to date either by using a security scanner or by hiring a team of experts. Threats, risks and vulnerabilities are the three challenges which must be considered while designing any system. These design issues are important and an assessment of these is again important. Vulnerability assessment is also known as vulnerability analysis. It is the process that defines, identifies and classifies the security holes (vulnerabilities) in a computer, network or communication infrastructure. Vulnerability analysis of the cloud computing infrastructure can forecast the effectiveness of proposed counter measures and evaluate their actual effectiveness after they are put into use. Different vulnerability assessment tools are available for detecting different vulnerabilities. Vulnerability scanners are one of them. There are different types of vulnerability scanners such as port scanners, network scanners, web application security scanners, computer malware scanners. Based on the availability of tools there are different categories of tools like freeware, shareware, open source and commercial tools. There are various tools which are used in the term vulnerability management. In present study, Nessus vulnerability scanner version 5.0.3 has been used along with feed type HomeFeed. It is also called as remote scanner because it does not need to be installed on a computer to test that computer. In typical operation, each port on a computer is tested, services that are running are determined. Tests are performed to identify vulnerabilities in it which could be used by a hacker to carry out a malicious attack.

In this case study research analysis has been done to analyze the security and the possible ways to minimize the respective vulnerabilities. The objectives of this paper are twofold. The first objective is to identify and understand different types of vulnerabilities in cloud environment. The second objective is to analyze and propose recommendations for effective handling of different vulnerabilities. Assessment of vulnerabilities is very essential to increase the security of various processes in the cloud environment.

II. Literature Review

Lot of research has been going on in the field of cloud computing in general. Issue of vulnerabilities is one of them. Substantial research work needs to be done in the domain of vulnerability analysis in different cloud environments. A survey of the literature review conducted for the said study is presented below.

The lack of security and standards in cloud represents an obstacle for most enterprises for moving into the cloud. A. Sharma et al. have addressed various challenging implementation issues and obstacles for the cloud environment [2]. The core technologies in cloud computing like web application, virtualization and cryptography have vulnerabilities that are either intrinsic to the technology or prevalent in the implementation of technology. Vulnerability is a prominent factor of risk. So security relates to saving data and programs from danger and vulnerabilities [3][5]. However, Sharma et al. [3] have proposed a broader classification of vulnerability issues based on an extensive research survey in cloud computing environment and also have analyzed various vulnerabilities on different environments and platforms using different tools. As vulnerabilities keep increasing every year, so there is a severe need to classify, manage and analyze them efficiently. The problem of vulnerability management is still relatively new. S. Kotikela et al. [6] have presented a solution for vulnerability management.

They have proposed and successfully implemented an ontological framework for vulnerability management in cloud. The framework is capable of assessing and scanning the vulnerabilities in popular software as well as software created by users thus, making the tedious task of vulnerability management easy and effective. There are often, multiple sources of potential vulnerabilities in any multi- tier cloud environment. S. bleikertz et al. [7] have presented a novel approach in the security assessment of the end user configuration of multi-tier architectures deployed on infrastructure clouds like Amazon EC2. In their assessment they have focused on the reach ability and vulnerability of services in the virtual infrastructure and presented a way for the visualization and automated analysis based on reach ability and attack groups. Under a cloud computing environment, the impact range of vulnerability needs to be described. Vulnerability caused by misconfiguration will also increase. T. Takahashi et al. [8] have discussed that composition of multiple resources is a major factor that affect cyber security information in cloud computing. It is a technique wherein multiple resources comprise one service and users may indirectly use various resources. Resource dependency information is required to identify who is affected by certain cyber security risks and to whom certain cyber security information such as warnings and vulnerability needs to be delivered. They have proposed an ontological approach toward cyber security in cloud computing. The data security in cloud computing is one of the challenges to be addressed before this technique is accepted and applied widely. J. Feng et al. [9] have analyzed the integrity vulnerability existing in the current cloud storage platforms and have shown the problem of repudiation. They have specifically designed a novel non- repudiation (NR) protocol and have also discussed the robustness of the NR protocol against typical attacks in the network environments. In another study, J.Feng et al. [10] have studied the vulnerability in the Amazon's AWS cloud in data integrity due to the missing of connection between the uploading and downloading phases and have suggested different solutions to make up the missing link. Risk management framework is one of the security assessment tool to reduction of threats and vulnerabilities and mitigate security risks. X.hang et al.[11] have presented information risk management for better understanding the critical areas of focus in cloud computing environments, to identifying threats and vulnerabilities. This framework covers all cloud service models and cloud deployment models. Cloud providers can apply this framework to organizations to do risk mitigation.

On the basis of the survey of various research aspects related to security and vulnerability of cloud computing environments, the current research study has been undertaken to identify the different vulnerability issues at specific platforms selecting appropriate tools. Details have been given in the next section.

III. Methodology

As explained above that the present study has been conducted with the following objectives.

- To understand the different types of vulnerabilities in the cloud environment.
- To analyze and propose recommendations for effective handling of different vulnerabilities.

In order to achieve these above objectives and to effectively analyze the vulnerabilities, specific tools and environments have been selected on the basis of research survey presented above, availability, relevance and significance. The operating systems, tools and environments used are as follows.

A. Operating Systems Used

Sedulity operating system corporate edition 3.0 version (Linux based) and Windows XP Service Pack2

B. Tools Used

Nessus, AngryIP Scanner, Zenmap

C. Environment

Vulnerability tool Nessus deployed on base machine with Sedulity operating system and virtual cloud machine on target machine with windows XP Service Pack2 operating system.

The tests have been conducted using the base machine having Sedulity operating system and the target machine in virtualized cloud environment having Windows XP operating system. The specific host information included for generating the test results includes Netbios Name: JMD-258634709AB, IP: 192.168.1.18, MAC Address: 08:00:27:d4:16:a5. The test methodology involves the following. Initially, a total no of systems live in the network are detected. The total number of system live at that particular network (e.g. LAN) with their IP addresses and names are identified and listed. Subsequently, a number of ports both open and closed are scanned. After this, vulnerabilities of the selected system are identified and analyzed. The details of different vuln erabilities are given in the next section.

IV. Results and Recommendations

The results of different vulnerabilities obtained by running above mentioned tools on the given environment have been given below.

A. Results Summary

After conducting the vulnerability analysis as explained above, a detailed report has been generated. The results obtained are categorized and further analyzed for severity, impact or risk factor. The categorization is as shown in Table 1.

Table 1: Different Categories of Cloud Vulnerabilities

Critical	High	Medium	Low
4	1	2	1

The details of different vulnerabilities have been presented in Table 2. These results are discussed in detail below.

Table 2: Result of Different Vulnerabilities in the Given Environment

SR.No	Vulnerabilities	Details
1	Critical Vulnerabilities	35362-MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution(958687)
		22194-MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution(921883
		18502-MS05-027: Vulnerability in SMB could allow Remote Code Execution(896422)
		34477-MS08-067: Microsoft Windows
2	High Vulnerabilities	22034-MS06-035: Vulnerability in Server Service could allow Remote Code Execution (917159)
3	Medium Vulnerabilities	26290- Microsoft Windows SMB Null Session Authentication
		57608- SMB Signing Disabled
4	Low Vulnerabilities	11197-Multiple Ethernet Driver Frame Padding information Disclosure (Etherleak)

1. Critical Vulnerabilities

(i). 35362-MS09-001 Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687)

(a). Description

It is possible to crash the remote host due to a flaw in SMB (Server Message Block). The flaw contains two privately reported vulnerabilities and one publically disclosed vulnerability in Microsoft's Server Message Block(SMB) protocol. It is a Microsoft network file sharing protocol used in Microsoft Windows. The vulnerabilities could allow RCE (Remote Code Execution) on affected systems which means that if an attacker gets successful to exploit these vulnerabilities, then he can take complete control of that system. For example, could install programs, view, change or delete data or even can create new accounts with full user rights. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. Most attempts to exploit this vulnerability would result in a system denial of service condition. This vulnerability is caused by the Microsoft SMB protocol software insufficiently validating the buffer size before writing to it which makes the system to stop responding and restart. All systems with SMB server service are affected by this vulnerability.

(b). Solution

This vulnerability is rated critical for all supported editions of Microsoft Windows. So handling of critical vulnerabilities is very important. Some of the ways to reduce the severity of exploitation of this vulnerability may include like firewall best practices and standard default firewall configurations can help networks from attacks that originate outside the enterprise perimeter. Systems which are connected to the internet must have a minimal number of ports exposed. The SMB ports should be blocked from the internet. Microsoft provides various detection and deployment tools and guidance for the security updates. This really helps the IT professionals to understand how to use various tools to deploy the security updates like Windows update, Microsoft update, Microsoft Base Security Analyzer(MBSA) etc. Also Microsoft has released a set of security patches for Windows XP.

(ii). 22194-MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883)

(a). Description

The remote host is vulnerable to buffer overrun in the server service that may allow an attacker to execute arbitrary code on the remote host with system privileges because the attacker takes the complete control of the system after successfully exploiting this vulnerability. The server service allows the sharing of local resources like disks and printers so that other users on the network can access them. Buffer overrun occurs when writing data to a buffer overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety. It alters the way the program operates which ultimately results in the crash or a breach of system security.

(b). Solution

All workstations and servers are at a great risk from this vulnerability and an attacker could try to exploit this vulnerability over the internet also. Firewall best practices and standard default firewall configurations can help networks from attacks that originate outside the enterprise perimeter. Systems which are connected to the internet must have a minimal number of ports exposed. Apart from this, different security updates and patches are available which help to protect from different vulnerabilities. The updates remove the vulnerabilities by modifying the way the server service validates in RPC(Remote Procedure Call) communications before it passes the message to the allocated buffer.

(iii). 18502-MS05-027: Vulnerability in SMB could allow Remote Code Execution (896422)

(a). Description

This is Remote Code Execution (REC) vulnerability. An attacker who successfully exploit this vulnerability could remotely take control of an affected system and then he can install programs, view, change , delete data or create new accounts with full user rights. The vulnerability results because of the process that the affected operating systems use to validate certain incoming SMB packets. Because of the nature of this issue, attempts to exploit this vulnerability would most likely result in a denial of service condition.

(b). Solution

Firewall best practices and standard default firewall configurations can help networks from attacks that originate outside the enterprise perimeter. Systems which are connected to the internet must have a minimal number of ports exposed. Use a personal firewall like Internet Connection Firewall to protect from network based attempts to exploit this vulnerability, enable advanced TCP/IP filtering on systems, and block the affected ports by using IPSec on the affected systems. Other than this, use certain patches and security updates.

(iv). 34477-MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution(958644)

(a). Description

This is again a Remote Code Execution vulnerability. An attacker who successfully exploit this vulnerability could take complete control of an affected system remotely. On Microsoft Windows XP, an attacker could exploit this vulnerability over RPC(Remote Procedure Call) without authentication to run arbitrary code. This vulnerability is caused by the Windows Server Service not properly handling specially crafted RPC requests. RPC is a protocol that a program can use to request a service from a program located on another computer in a network. RPC helps with interoperability because the program using RPC does not have to understand the network protocol that are supporting communication. In RPC, the requesting program is the client and the service providing program is the server. All workstations and servers are at a great risk from this issue.

(b). Solution

Firewall best practices and standard default firewall configurations can help networks from attacks that originate outside the enterprise perimeter. Systems which are connected to the internet must have a minimal number of ports exposed. Use a personal firewall like Internet Connection Firewall to protect the internet connection by blocking unsolicited incoming traffic. Certain vulnerability detection and deployment tools and guidance are available which the administrators and IT professionals must use to protect their systems from these attacks. Apart from this, certain security patches and updates are available which surely are very helpful.

2. High Vulnerabilities

(i). 22034-MS06-035: Vulnerability in Server Service could allow Remote Code Execution (917159)

(a). Description

The remote host is vulnerable to heap overflow in the server service that may allow an attacker to execute an arbitrary code on the remote host with system privileges. This is a Remote Code Execution vulnerability. An attacker can take full control of system and can install new programs, view, change, delete data or even can create new accounts with full user rights. This vulnerability is mainly caused by an unchecked buffer in the server service. Any anonymous user who could deliver a special crafted network packet to the affected system could try to exploit this vulnerability. Attempts to exploit this vulnerability will most probably result in denial of service condition caused by an unexpected restart of the affected system. In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host to store SMB traffic during transport.

(b). Solution

Microsoft Windows operating systems implement protections against heap overflows since Windows XP Service Pack2 such as safe unlinking and cookies. It can also mitigate these threats through the use of Data execution Prevention. Firewall best practices and standard default firewall configurations can help networks from attacks that originate outside the enterprise perimeter. Systems which are connected to the internet must have a minimal number of ports exposed. Both workstations and servers are at a great risk but the servers could be at more risk especially if they support a large amount of SMB traffic. So the implementation of right and proper security resources like updates, patches etc are very necessary.

3. Medium Vulnerabilities

(i). 26290 - Microsoft Windows SMB Null Session Authentication

(a). Description

The remote host is running Microsoft Windows. When a program or service is started by using the system user account, the service logs on with null credentials. This can be a potential security risk because it allows for an unauthenticated log on to the system. A hacker or worm can exploit this vulnerability and potentially access sensitive data on the system. Apart from unauthorized access, it also allows partial confidentiality, integrity and availability violation, allows unauthorized disclosure of information and disruption of service.

(b). Solution

The simplest way to reduce null session vulnerability is to disable Netbios and verify that ports 139 and 445 having unnecessary services are closed. Also modify the registry key.

(ii). 57608- SMB Signing Disabled

(a). Description

Signing is disabled on the remote server. This can allow man-in-the-middle attacks against the SMB server. SMB signing is a feature through which communications using SMB can be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their print of origination and their authenticity. This security mechanism in the SMB protocol helps to avoid issues like tampering of packets and man-in-the-middle attacks.

(b). Solution

Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'.

4. Low Vulnerabilities

(i). 11197-Multiple Ethernet Driver Frame Padding information Disclosure (Etherleak)

(a). Description

The remote host is vulnerable to an 'Etherleak'. The remote Ethernet driver seems to leak bits of the content of the memory of the remote operating system. An attacker may take advantage of this flaw only when its target is on the same physical subnet.

(b). Solution

It is recommended to contact the network device driver's vendor for a fix.

Different vulnerabilities have different levels of threat perceptions. Certain vulnerabilities require immediate attention as these can result in loss of confidentiality and integrity of the system. In contrast, there can be some threat perceptions which may not require immediate attention. However, these may be rectified in order to minimize any external attempt of exploitation.

V. Conclusion and Future Work

This study has been conducted with two major objectives. The first objective is to understand different types of vulnerabilities in cloud environment. An extensive study has been conducted wherein the works of different researchers in the field of assessment and detection of cloud computing vulnerabilities. Another objective has been the analysis and proposing of the recommendations for effective handling of different vulnerabilities. Using select tools on the cloud environment the report generated were analysed for different vulnerabilities like critical, high, medium and low. It was observed that different vulnerabilities have different levels of threat perceptions and their rectification is necessary in every level. For example, in our report we found some critical and high vulnerabilities in Windows Remote Code Execution, medium vulnerabilities in Windows SMB (Server Message Block) and low vulnerability in Ethernet driver. The report generated was further analyzed for assessment of the severity and impact of different vulnerabilities in the given cloud environment. Some recommendations for respective vulnerabilities have also been proposed.

Further, we have been working to extend the vulnerability assessment and analysis on different environments. A comparative analysis shall be done on different cloud environments for identifying and analyzing some other vulnerabilities under different platforms.

References

[1] Sharma, A.,Abrol, P.,"Implementation issues of cloud computing", proc. 8th JK Science Congress JKSC-12, Sep. 2012.

[2] Sharma, A., Abrol, P.,"Cloud Computing Environment: Problems in Implementation", Int. J. Computers & Distributed system", Vol. 01, No. 03, pp. 64-68, Oct. 2012.

[3] Sharma, A., Abrol, P., "Vulnerabilities in Cloud Computing: A Research Perspective", Int. J. Comput., Communication & Emerging Technology, Vol. 01, No. 02, 2012.

[4] "Vulnerability management", Wikipedia, April, 2013. [Online] Available: http://www.en.wikipedia.org/wiki/ Vulnerability management May 11, 2013.

[5] Sharma, A., Abrol, P., "Vulnerability Issues in cloud computing", proc. 7th JK Science Congress JKSC-11, pp 191, Oct. 2011.

[6] Kotikela, S., Kavi, K., Gomathisankaran, M., "Vulnerability Assessment in Cloud Computing", Int. Conf. Security Management (SAM'12), pp. 67–73, July 16-19, 2012.

[7] Bleikertz,S., Schunter, M., Probst, C.W.,"Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds", In ACM Cloud Comput. Security Workshop (CCSW'10), Chicago, Illinois, USA, Oct.8, 2010

[8] Takahashi, T., Kadobayashi, Y., Fujiwara, H.,"Ontological Approach toward Cyber security in Cloud Computing", 3rd International Conference of Security of Information and Networks(SIN'10), Taganrog, Rostov-on-Don, Russian Federation, ACM Press, pp. 100-109, Sep. 07 - 11, 2010.

[9] Feng, J., Chen, Y., Ku, W.S., Liu, P., "Analysis of Integrity Vulnerabilities and a Non-repudiation Protocol for Cloud Data Storage Platforms", 2nd Int. Workshop Security Cloud Comput. (SCC 2010), Held Conjunction With 39th International Conf. Parallel Processing (ICPP 2010), San Diego, California, USA,IEEE Press, pp. 231–258, Sept. 13, 2010.

[10] Feng, J., Chen, Y., Liu, P.,"Bridging the Missing Link of Cloud Data Storage Security in AWS", 7th IEEE Consumer Comm. Networking Conf. (CCNC 2010), Las Vegas, NV ,pp. 390-391, Jan. 09-12, 2010.

[11] Zhang, X., Wuyong, N., Li, H., "Information Security Risk Management Framework for the Cloud Computing Environments", 10th IEEE Int. Conf. Comput. Inform. Technology (CIT 2010), Bradford, pp. 1328–1334, June 29 2010, July 1 2010.

Arti Sharma is presently pursuing her PhD in Computer Science from CMJ University Shillong, under the guidance of Dr. Pawanesh Abrol. Her area of research work includes vulnerabilities in cloud computing environment.

Pawanesh Abrol has done Ph.D. in Computer Science. Presently, he has been working as Associate Professor in the Department of Compute Science and IT, University of Jammu, Jammu, J&K, India. His research interests include cloud computing, image authentication and computer visualization techniques. He has published more than forty research papers in different national and international journals and conferences. Dr. Abrol is a member of ACM and also the State Coordinator of Computer Society of India, J&K State. Besides, he also holds the degree of MBA (HR).