International Journal of Scientific Research in Computer Science and Engineering
Vol.11, Issue.4, pp.86-90, August 2023
E-ISSN: 2320-7639
Available online at: www.isroset.org

Review Paper

Public and Private Cloud Security through Vulnerabilities Assessment of VirtualMachine

Prabhat Bisht[1]

[1]Scientist C, NIC, Chandigarh, Haryana, India

Author's Mail Id: prabhatbisht@gmail.com

Received: 28/Jun/2023; **Accepted**: 31/Jul/2023; **Published**: 31/Aug/2023

***Abstract*—**Virtualization in cloud computing is one of the biggest milestones leading us to next generation web technology. Use of virtualization technology through virtual machines in cloud computing is rapidly growing and offering best opportunities for availability, reliability, elastically, throughput, scalability, efficiency, and flexibility. Research shows that over 70 percent of organizations are planning to adopt cloud oriented services through virtualization by the end of 2017.
Most of the companies delayed adopting cloud virtualization services because of the security concerns or many adopted this technology before adopting advanced security measures. Virtualization is achieved through Virtual Machine (VM) in cloud, so security of virtual machines is a matter of great concern for cloud service provider or cloud service user. Vulnerable Virtual Machine (VM) is a biggest reason for threats, due to which organization valuable information canbe compromised.
This research paper focus on security of Virtual Machines through vulnerabilities assessment of Virtual Machines inCloud.

Keywords—Virtual Machine Environment (VME), Virtual Machine (VM), Transport Layer Security (TLS),Secure Shell(SSH), Data Encryption Standard (DES), File Transport Protocol (FTP),Secure Socket Layer (SSL), RemoteProcedure Call (RPC).

1. Introduction

Whether it is Public [1] or Private [2] Cloud, Virtualization Technology [3] [4] presents enterprises with many opportunities in terms of application hosting or data management or accessibility, as well as many new challenges. Every organization must aware that security should be properly implemented and followed as per organizational guidelines without implementing server side security , server resources are not safeguard from cyber threats. Data confidentiality, Integrity and Availability is a major concern for all the organizations, attackers always tries to find vulnerabilities in web application and In addition to this, attackers are always ready to introduce new attack vectors to damage VM and the services hosted over them. Unfortunately, based on our interaction with cloud service providers , it is found that not every organization is well aware about the security principles to virtual machines, despite the fact that most VM in cloud are open to the same risks as physical servers or client server are. VM need to be periodically analyzed for vulnerabilities and vulnerabilities must be patched and protected just like traditional client server type physical servers. Organization need to make sure that their virtual machines are included in their security strategy. This paper highlights security concerns with VME, focusing on Vulnerabilities assessment of VM in cloud computing environment. Most of this security concern applies both to hosted hypervisors as well as bare-metal hypervisors which do not have a host operating system. Our study revealed that VM security is not properly safeguarded by many organizations and loopholes overlooked by many organizations which sometimes lead to attack on economic and technical end of the organization. The reason behind this is VM are not properly assessed for vulnerabilities and vulnerabilities are not properly patched which left virtualmachines vulnerable to intruders.

This research paper revealed vulnerabilities [5] by severity any classified them in different categories. This paper aims to present deep analysis on detecting and defending various vulnerabilities any virtual machine can have and make a safe place for hosting.

2. Statement of Problem

Security challenges with virtualization in cloud
Depending upon the project requirements, virtual machines are configured for scalability, n numbers of VM's are configured horizontally or vertically to scale the application. This mean that any traditional network security system, such as an intrusion detection system (IDS) [6] or data loss prevention (DLP) detection system will not work in VM network. To overcomethis layer of complexity, cloud service providers like Amazon[7], Microsoft [8] and Google [9] etc.

must deploy virtual firewalls and similar devices to detect intruders over public or private network. Organization or cloud service users should make it sure that there is proper firewall implementation policy.

How to safeguard VM's from getting infected with worms, viruses, Trojan horse or malware? And how to safeguard it from spreading are few questions among cloud service administrators, what will happen if malware spread from virtual machines and infect host server ?. Guest-to-host infection could lead to widespread malware infections across many computers in network system. Research have been carried out in past on guest-to-host infections and it is recommended that Cloud administrators should keep host servers up to-date with latest patch updates and should patch known vulnerabilities as identified and recommended by security team . Hardening of virtual machines can limit potential damage to server resources. There are certain circumstances where malware might be able to spread from the VM to the host computer e.g. Shared folders between VM and host servers and because of shared folders worms can spread from one system to another. This requires administrative interaction and which disable any network sharing permission to resources line pend drive and any external devices that could lead to malware spreading. Worms could also spread by exploiting vulnerabilities of exposed operating system services. Here, the host server and VM act like two separate systems on the network. Just keep in mind that, depending on the setup, the network traffic might occur only on virtual private network through digital certificate.
This paper focuses on Vulnerabilities assessment of Virtual machines in cloud computing.

3. Detection of Vulnerabilities in Virtual Machine (VM).

Performed vulnerabilities assessment [10] on RHEL, UBUNTU and CENTOS based operating system VM(s). Our research revealed different types of vulnerabilities, which are classified in following categories.

a) Vulnerabilities by risk
1) High risk
2) Medium risk
3) Low risk
4) Informational risk

b) Exposure – Internal
1) Number of Trojans or backdoor applications
2) Number of wireless devices attached
3) Number of rogue applications means potentially unwanted application and malware

a) Vulnerabilities by risk

1. High Risk – High risk vulnerability if detected on VM can directly lead an attacker gaining privileged root access (e.g. administrator) to the machine over a remote connection.

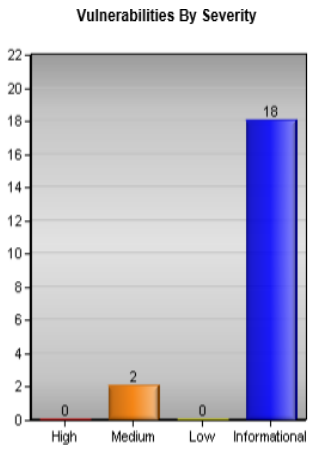
2. Medium Risk – Medium risk vulnerability if detected on VM can directly lead an attacker gaining non-privileged access (e.g. other than administrator root user) to the machine over a remote connection.

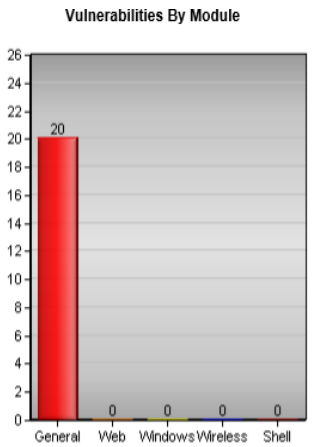
3. Low Risk – Low risk vulnerability if detected on the VM can provides enticement i.e. Valuable & critical data to the attacker that may be used by attacker to launch a more informed attack against the VME. In addition, this type of vulnerability may indirectly lead to an attacker gaining some form of access to the VM over a remote connection.

4. Informational Risk – This type of finding on the VME provides informative data to an attacker that isof lesser value to an attacker than the enticement data.

Table 1: Classification of Vulnerabilities Detected

Risk Level	Vulnerabilities
Medium	TLS Diffie-Hellman Key Exchange Logjam Vulnerability.
Medium	Medium SSL/TLS Protocol Triple-DES Information Disclosure Vulnerability.
Informational	RPC statd.
Informational	RPC portmap.
Informational	Secure Socket Layer (SSL) CertificateExpired Or Expiring.
Informational	Web Server Self-Signed TLS/SSL X.509 Certificate.
Informational	FTP Server Found.
Informational	SSL Server Information Detected.
Informational	SSH server found.
Informational	Hidden WWW Server Name Detected.
Informational	Web Server Redirection Detected.
Informational	FTP Server With Clear Text Authentication Detected.
Informational	Apache JServ Protocol Connector Detected.
Informational	Web Server HTTP Protocol Version Detected.
Informational	SSL/TLS Server Preferred CipherSuite Detection.
Informational	TLS/SSL Server X.509 Certificate SHA1 Signature Detected.
Informational	Insecure TLS/SSL Protocol Detection.
Informational	TLS 1.0 Supported Cipher Suites Detected.
Informational	TLS 1.1 Supported Cipher Suites Detected.
Informational	TLS 1.2 Supported Cipher Suites Detected.





Total Vulnerabilities (20)

Virtual Machine	High	Medium	Low	Informational	critical
IP (127.0.0.1)	-	2	-	18	-

b) Exposure –Internal

1. Number of Trojans /backdoor application

Our research shows that few services running over VM are commonly associated with trojan and backdoor applications [11] that can compromise security aspects of VM host network's over cloud. Sometime Trojan or backdoor services may be mistakenly downloaded from the internet through the web or e-mail attachment, or it may be sometime uploaded on a host for later use by the attacker. This type of services allows an attacker to establish a remote connection to the VM, or may provide valuable information relative to the VM host over network. Retrieval of usernames and passwords, retrieval of host data, or launching an attack against other networks are all possible if a machine is compromised with a Trojan or backdoor program.

2. Number of wireless devices

Our research reveals that wireless access points potentially allow attackers to view all traffic passing in and out of the network that the wireless access point serves or it may even allow the attacker to participate as a node on the network itself. This scenario represents an important security exposure as seemingly private, internal resources of VM over cloud have mistakenly become available via poorly controlled wireless access devices over network. It is strongly recommended that wireless access points should be properly configured such that they only allow authorized resources to connect to the network.

3. Number of rogue application (unwanted software and malware)

Most of the time rogue applications are generally entertainment and leisure programs that allow users to share data over network, such as music files or real-time chat with friends. Many of these applications open up additional, unsecured ports on the host machine and allow for remote connections .Additional unsecured ports are the great threats to VM over cloud. In some cases these applications allow for plaintext communication of potentially sensitive organization information. In general, these applications are installed by the user on machines, with little if any knowledge of their existence by network management and security personnel. As such, there is little possibility of monitoring the communications of these applications, or ensuring that they are secure. File and resource sharing programs, such as Team viewer etc.

4. Description of Vulnerabilities

Risk Level Medium

1) TLS Diffie-hellman Key exchange logjam vulnerability

TLS protocol is used to encrypt communication overnetwork. Most of the time it is found that information disclosure vulnerability over VM is present in few versions of TLS protocol. The flaw lies in Diffie- Hellman Key Exchange. If this vulnerability is successfully exploited it could allow an attacker to read and modify data passed over the encrypted connection.

2) SSL/TLS Protocol Triple DES Information disclosure.

It is recommended that VM service provider or users should properly configure their TLS/SSL implementation in order to disable 3DES cipher suites. For compatible consideration, OpenSSL move 3DES cipher suites from HIGH to MEDIUM. But this stillleave a door for attackers to exploit this vulnerability. Soit strongly recommended updating TLS to 1.1.0 or later version in order to completely disable 3DES cipher suites.

Information Risk

1) RPC statd

In VM it is found that RPC services are mostly enabled in the UNIX or LINUX server through /etc/inetd.conf or /etc/rc configure file(s). It is strongly recommended that this service and any additional unnecessary RPC servicesbe immediately disabled in the service configuration files of VM. It is noted that RPC services are regularly found to be vulnerable to buffer overflow and format string attacks that lead to complete compromise of the target system. Exploitation of RPC services affects all major UNIX operating systems including Solaris, HP/UX, AIX, Irix, Linux, FreeBSD

2. RPC portmap

It is strongly recommended that RPC service and any additional unnecessary RPC services be strictly disabled in the service configuration files of VM. It was possible to connect to the portmap service on the target system through TCP port 111.Attackers can exploit this type of vulnerability for gaining access to VM.

3. Secure Socket Layer (SSL) Certificate Expired Or Expiring

Research shows that in many VM, one or morecertificates in the certificate chain returned from an SSL server has expired or are set to expire in less than 30/60/90 days. Immediately replace the certificate with a new, valid certificate for providing additional security to VM over cloud. These certificates are created by a authorized Certificate Authority (CA) [12] and installed on web servers by system administrators. Every certificates generated by CAs include an expiration date. When the expiration date has passed, SSL clients and servers no longer consider the certificate valid. In SSL- enabled web server, this results in users visiting the web site receiving a warning indicating that the SSL certificate is no longer valid, this is one of vulnerability which is mostly exploited by attackers any information transmitted during this time declared unsafe and vulnerable.

4. Web Server Self-Signed TLS/SSL X.509 Certificate

In UNIX based VM, one or more self-signed TLS/SSL

X.509 certificates were obtained from the remote web server. Transport Layer Security i.e TLS is a protocol used for establishing secure connection between client and server over network. X.509 is an ITU-T standard for Public Key Infrastructure (PKI). X.509 defines the specific format for public key certificates.
It is strongly recommended that do not use self-signed certificates as it did not provide secure client/server communications.

5. FTP /SFTP Server Found
For best VM security our research strongly recommends that verify FTP server's configuration in port 22 and it complies with corporate policy. Best recommendation is use of digital certificate over Virtual Private Network for uploading and downloading files from VM over cloud

6. SSL Server Information Detected
Ensure that SSL server complies with the organization policy. Configure the server to support the latest version of the protocol, strong encryption ciphers and appropriate digitally signed certificate. One can verify SSL certificate from SSL Labs.

7. SSH Server Information Detected
For best VM security our research strongly recommends that verify SSH service configuration in port 22 and it complies with organization policy. Best recommendation is use of digital certificate over Virtual Private Network for accessing UNIX shell over network

8. Hidden WWW Server Name Detected
Ensure that web server complies with organization policy. WWW is a apache web server directory for hosting web based contents using HTTP. Web server name can be hidden as a security measure.

9. Web Server Redirection Detected
In our research most of the time it is noted that web server redirection status was detected on the host.
Ensure that Web server complies with organizational policies.

10. FTP Server With Clear Text Authentication Detected
One of vulnerability in VM, FTP server with clear text authentication was detected on the host. Ensure that the FTP server complies with organizational policy. A FTP server is used for transferring files to and from remote systems connected in a network. FTP server with clear text authentication was detected on the host.

11. Apache JServ Protocol Connector Detected
One of a vulnerability which is commonly detected in VM is Apache JServ Protocol (AJP) connector on the host. Ensure that Apache JServ Protocol (AJP) connector complies with organizational policy.
Apache JServ Protocol (AJP) is a binary protocol used to conduct inbound requests from web server using an application server.

12. Web Server HTTP Protocol Version detected.
HTTP protocol version was obtained from the host through web server. Ensure that web server complies with organizational policy. Web servers are widely used to serve static and dynamic content and render it in the client's browser.

13. SSL/TLS Server Preferred Cipher Suit Detection
The cipher suite the SSL/TLS server preferred to use has been detected in VM which makes VM vulnerable to cyber-attacks. Always consider using the TLS 1.2 or later protocol and always prioritize secure cipher suites. Presently AEAD cipher suites were considered as secure for VM over cloud. But for TLS 1.1 and prior, it should be safe to use CBC or RC4 cipher suites our research shows that successful exploitation could allow an attacker to decrypt the sensitive data.

14. TLS/SSL Server X.509 Certificate SHA1 Signature Detected
Our study revealed that in most of the VM, TLS/SSL server X.509 certificate's signature computed with SHA1 hash algorithm was detected on the host, which makes VM vulnerable to threats.
Ensure that TLS/SSL server complies with organizational policies. SHA1 is a hashing algorithm used in the process of computing X.509 certificate signature.

15. Insecure TLS/SSL Protocol Detection
It is strongly recommended to use TLS v1.1 or later to ensure environment is configured to use only secure versions of cryptography and security protocols.
TLS 1.0, SSL v2.0 and SSH v1.0 have known vulnerabilities that an attacker can use to gain control on VM.

16. TLS 1.1 Supported Cipher Suites Detected
SSL/TLS supported vulnerable cipher suite was detected on the host. Ensure that SSL/TLS configuration complies as per organizational policies.

5. Conclusion

Virtual Machines (VM) in cloud computing environment need security solutions that go beyond earlier traditional protections in order to achieve VM security in cloud. That holds true for standalone virtualized servers as well as those hosted in VME. Understanding what vulnerabilities exist in Cloud Computing will help organizations to patch the vulnerabilities and making the VM safe for hosting. This paper presented security issues which virtual machines can have in cloud and the best possible methods of avoiding them. As described in this paper, virtualization and networks security are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major security concerns for cloud users. Virtual networks in cloud are also target for some attacks especially when communicating with remote virtual machines. This research focus towards the necessity of vulnerabilities assessment of virtual machines in cloud.

Data Availability
Literature review of Research publication and VM vulnerabilities assessment reports

Conflict of Interest
Author declare that author do not have any conflict of interest with anyone for publication of this work.

Funding Source
None

Authors' Contributions
This work is carried out by author independently.

Acknowledgement
Author acknowledges ISROSET for providing a platform for publishing research/survey/review papers.

References

[1]. Peter M. Mell, Timothy Grance, "*The NIST definition of cloud computing*," National Institute of Standards and Technology, Vol.**1**, Issue.**1**, pp.**1-7, 2011.**
[2]. Talwana Jonathan Charity, Gu Chun Hua ,"*Resource Reliability using Fault Tolerance in Cloud Computing*," In the proceedings of the 2016 International Conference on Next Generation Computing Technologies-IEEE, India, **2016.**
[3]. Fatima Shakeel, Seema Sharma, "*Green Cloud Computing: A review on Efficiency of Data Centres and Virtualization of Servers*," In the proceeding of the 2017 International Conference on Computing, Communication and Automation-IEEE, India **2017.**
[4] Shruti Sharma, Sharanjit Singh, Amardeep Singh, Ramanpreet Kaur, "*Virtualization in Cloud Computing*," International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET) ,Vol.**2**, Issue.**4**, pp.**2394-4099, 2016**
[5] B. Grobauer, T. Walloschek, E. Stocker, "*Understanding cloud computing vulnerabilities*," IEEE Security & Privacy, Vol.**9**, Issue.**2**, pp.**50-57, 2011.**
[6] Zakira Inayat , Abdullah Gani , Nor Badrul Anuar , Shahid Anwar , Muhammad Khurram Khan ,"*Cloud-Based Intrusion Detection and Response System Open Research Issues and Solution"*, Arabian Journal of Science and Engineering, Vol.**42**, pp.**399–423, 2017.**
[7] Prabhat Bisht, Manmohan Singh Rauthan, "Machine Learning and Natural Language Processing Based Web Application Firewall for Mitigating Cyber Attacks in Cloud," *International Journal of Scientific Research in Computer Science and Engineering*, Vol.**11**, Issue.**3**, pp.**1-15, 2023.**
[8] Prabhat Bisht , Manmohan Singh Rauthan , Raj Kishore Bisht , "Component based web application firewall for analyzing and defending SQL injection attack vectors" , *International Journal of Recent Technology and Engineering*, Vol.8, Issue.3, pp.**4183–4190, 2019.**
[9] Prabhat Bisht, Devesh Pant, Manmohan Singh Rauthan, "*Analyzing and defending web application vulnerabilities through proposed security model in cloud computing*", International journal of science and technology graphic era university, Vol.**6**, Issue.**2**, pp.**183-196, 2018.**
[10] Shahil, U M and Deekshitha, Ms. and Anam M, Nuzha and Basthikodi, Mustafa, "*DDOS Attacks in Cloud Computing and its Preventions*", JETIR- International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN: 2349-5162, May, Vol.**6**, Issue.**5**, pp.**405-408, 2019.**
[11] Christof Paar , "*Hardware Trojans and Other Threats against Embedded Systems*," In the Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, **2017.**

AUTHORS PROFILE

Prabhat Bisht earned his MCA from Govind Ballabh Pant Institute of Engineering and Technology, ***Pauri Garhwal*** (GBPIET), and having 17 years of working experiences in IT sector. Author is currently enrolled as a Research Scholar in CSE Branch from Uttarakhand Technical University, Dehradun. Author researches focus on Cloud Computing Technology, Cyber Security Assurance, Web Application Security and Machine Learning Algorithms and have published research papers in international journals of science and technologies and in many international conferences.

Call for Papers:
Authors are cordially invited to submit their original research papers, based on theoretical or experimental works for publication in the journal.

Make a Submission

All submissions:
- must be **original**
- must be **previously unpublished research results**
- must be **experimental or theoretical**
- must be in **the journal's prescribed Word template**
- and will be **peer-reviewed**
- may not be **considered for publication elsewhere at any time during the review period**