Cyber Times International Journal of Technology & Management

Vol. 11 Issue 1, October 2017 – March 2018

TABLE OF CONTENTS

OVERVIEW OF SECURITY ISSUES IN VIRTUALIZATION

Prafulla Kumbhar
Assistant Professor,
Tilak Maharashtra Vidyyapeeth, Pune
prafullakumbhar@gmail.com

ABSTRACT

Security of virtualization is discussed mostly now days. As technology changes along with it more options are opened and more challenges occur. Many research papers are already published focussing on security issues occurs in virtualization. In this paper tried to take look on virtualization technology with its security.

KEYWORDS: *Virtual machine, Virtualization, Virtualization Security, Virtual Machine Based Rootkit (VMBR).*

I. INTRODUCTION

Virtualization is widely used technology in many companies now days. Using this technology of virtualization physical computer gets divided into parts. [6] On which machine we applying this technique are known as virtual machine. Virtual machine shares the processes of host computer. Multiple virtual machines can run on a computer. [5] The software used by host machine allows using multiple operating systems. By running multiple operating systems or applications on single machine we reduce cost and gives benefits of virtualization. Cost we needed for storage, space, power, cooling all get reduced. Then also security and strength is key point for it. [3] Security in virtualization means we trust on environment. In virtualization it is difficult to trace interactions. In market there are some security applications available. These security solutions given on hypervisor, hypervisor are a layer between physical machine's operating system and virtual environment. [1] [6] Hypervisor is software program, it contains all bugs and security issues as other software's have.

II. VIRTUALIZATION

In 1960's virtualization get developed by IBM Company. Originally it was used to make a partition between mainframe computers which shares its hardware as well as software components without harming it. [2][4]

Maintenance of mainframe computer is very difficult task. By making partition in applications it's easy to use.

After that virtualization technology becomes more popular. It reduces the cost of physical machine also reduces cost of maintenance.
Main benefit of virtualization is isolation and resource sharing. [5]

Resource sharing - When any application runs that time all resources like disk, memory, network get used. After applying virtualization all recourses mentioned above are get shared.

Isolation – Virtualization provides isolation between virtual machine and running some physical hardware. [6].

III. TYPES OF VIRTUALIZATION

Following are types of virtualization.

1. Application virtualization
2. Sever virtualization
3. Network virtualization
4. Storage virtualization

APPLICATION VIRTUALIZATION

User runs application on local machine using local resources like, by installing some application on computer. But in application virtualization every user uses isolated application environment virtually. The local machine provides CPU and RAM and running application without installing it on local machine. This isolated virtual environment act as a layer between local machine and application. [2]

SERVER VIRTUALIZATION

In this one server act as multiple server. The hypervisor layer allows multiple applications and operating systems to host locally or remotely. It reduces cost of machines and maintenance by reducing number of servers and increases efficiency of system. By using this virtualization we make smokescreen between servers and user. [1]

NETWORK VIRTUALIZATION

Using network virtualization we can create custom-made networks. It gives ability to manage traffic of network. Also we can set priorities in networks. Using this we can give more flexibility, trusted and scalable network speed.

STORAGE VIRTUALIZATION

In virtualization when logical storage get created by abstracting physical storage, which get spread over the network. Storage virtualization merges multiple storage devices in single.

Because of this it's easy to take back-up of resources. If data gets lost then easily we can recover data. Using storage virtualization we resolve the difficulty of managing storage devices. Logical storage is an aggregation of spreader physical resource by appearing single huge storage device to the user. [1]

IV. SECURITY ISSUES IN VIRTUALIZATION

Security issues in virtualization are differed as infrastructure of virtualization, network virtualization, hypervisor. When we process status of virtual machine, do software updates, conflicts occurred in resource, patching done in virtual machines. Hypervisor issues rivets to Virtual-Machine-Based-Rootkit(VMBR) attack.

In this hypervisor plays very important role of virtualization. If physical machines are get attacked threats then it affects to virtual machine also. To prevent it we have to switch it to another network. [5] Following are some issues.

VIRTUAL MACHINE BASED ROOTKIT (VMBR)

Use of rootkit is to run on operating system kernel (ring 0). Rootkit is useful for hackers because they covers themselves it's very hard to find and recognize them. Virtualization adds one more ring (ring 1). Rootkit runs in these rings. If they achieve to control all system then it's difficult to detect it.

REMOTE MANAGEMENT VULNERABILIES

Host machine manages virtual system and guest machines. Virtual machine gives facilities to control the machines. Hosts having management console to control other guests which may attacks. The attacker may control all guests by compromising with administrative console.

VIRTUAL MACHINE JUMPING

Virtualization gives isolated, encapsulated environment. Virtual operating system is not able to break out of virtual machine and interaction of guest machine and host machine. If any security issue or bug occurs in host machine then guest switches to another virtual machine and tries to maintain security.

GUEST ISOLATION

Isolation means process or application in which virtual machine can not affect or see other, kind of security in virtual machine. When secure environment denies access to the other machines. Then secured abstract guard manages and maintains completely. These kinds of isolations prevent guest from internal attacks as injections, and decreases outer attacks.

SIDE CHANNEL ATTACKS

Attacker tries to access the physical properties of hardware. Threat vector to virtualization is side channel attack. They try to use the method of cryptographic keys to access the resources.

VIRTUAL MACHINE ESCAPE ATTACKS

Host machine controls virtual machine and other guests. By breaking out guest, attacker tries to access hypervisor or guests this known as escape. Using escape guest attacker tries to access continuously all guest or hypervisor. Thus it's important to have special attention.

PACKET SNIFFING

Virtual environment shares some resources of each guest, which may be the suitable points of attacks. Physical links which are not secure provides sniffing platforms. Using virtual hubs or switches interaction takes place between guests. With the help of hub attacker compromises the packets of network communication. When virtual switches are used an Address Resolution protocol is spoofed.

DENIAL OF SERVICE

Denial of Service attack act like barrier between resources provided by the virtual machine. Virtualization shares resources of host machine and guest. VMware is a common denial of service vulnerability. Guest may cause denial of service attack while sharing resources.

THE REVERT TO SNAPSHOTS PROBLEM

Taking image of guest machine is known as Snapshot. Administrator recovers the disasters by allowing these images. It is critical but still need to focus on this issue. By inserting snapshot in an un-secured resource like un-patched application. Reusing old password or sensitive data more dangerous because it contains data of RAM

V. CONCLUSION

Virtualization having lots of benefits. In this paper we focused on more security aspects, issues. Security in virtualization is still challenge. This paper contains types of virtualization, techniques used. How it reduces the cost.

REFERENCES

[1] Durairaj. M, Kannan. P, Nov 2014, *"A Study On Virtualization Techniques And Challenges In Cloud Computing"*, International Journal of Scientific & Technology Research, Vol 3, Issue 11, ISSN 2277-8616.

[2] Gabriel Cephas Obasuyi, Arif Sari, 2015, "*Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment"*, The Management Centre of the Mediterranean, Nicosia, Cyprus, International Journal of communications, Network and system Science, 8, 260-273.

[3] Jenni Susan Reuben, 2007, "*A Survey on Virtual Machine Security*", Helsinki University of Technology, TKK T-110.5210, Seminar on Network Security <http://www.tml.tkk.fi/Publications/C/25/papers /Reuben_final.pdf> [Accessed 16 Feb 2018].

[4] Martine Wimmer, "*Virtual Security: About the Security Pros and Cons of Server Virtualization*", Siemens AG, Corporate Technology, CT IC CERT D-80200 Munich, Germany, martin.r.wimmer@siemens.com, <https://www.first.org/conference/2008/papers/ wimmer-martin-papers.pdf> [Accessed 12 Feb 2018].

[5] Somayeh Sobati Moghadam, Sept 2013, "*A survey of virtualization security*", International Journal of Science & Engineering Research, Volume 4, Issue 9, ISSN 2229-5518.

[6] "*Virtualization Overview*", White Paper, VMware, https://vmware.com/pdf/virtualization.pdf> [Accessed 13 Feb 2018].