Security Challenges for Virtualization in Cloud

A. Tayab[1], Junaid[2], W. Talib[3], M. Fuzail[4]

[1,2,3,4]Computer Science & Engineering Department,University of Engineering & Technology, Lahore, Pakistan
[1]awaisriaz333@yahoo.com

***Abstract*-**Virtualization is a model that is vastly growing in IT industry. Virtualization provides more than one logical resource in one single physical machine. Infrastructure use cloud services and on behalf of virtualization, cloud computing is also a rapidly growing model of IT industry. Cloud provider and cloud user, both remain ignorant of each other's security. Since virtualization and cloud computing are rapidly expanding and becoming more and more complex in infrastructure, more security is required to protect them from potential attacks and security threats.

Virtualization provides various benefits in terms of hardware utilization, resources protection, remote access and other resources. This paper intends to discuss the common exploits of security uses in the virtualized environment and focuses on the security threats from the attacker's perspective. This paper discuss the major areas of virtualized model environment and also address the security concerns. And finally presents a solution for secure virtualization in IT infrastructure and to protect inter communication of virtual machines.

***Keywords*-**VM, Virtual Machine, Cloud, Security, Attacks, Hypervisor

I. INTRODUCTION

This research paper presents the security issue that we face in virtualized environment. Virtualization is the latest technology that we use in our private or public cloud or infrastructure to reduce the cost of physical machines and make the infrastructure more efficient. Virtualization makes it possible to run more than one operating system called virtual machines (VM)ononе physical server and each and every virtual machineact as the owner of the physical server. Based on virtualization, cloud has a pool of virtualized computers and customers pay for the running applications. The use of virtual machine provides two main benefits:

sharing of resources

isolation

In the non-virtual environment, all of the resources are operating system-specific i.e. if a system has 1GB of physical memory and running tasks using 0.5GB of physical memory then the rest will be unused and cannot be fully utilized. But in the virtual environment, all resources are assigned to virtual machine and therefore, resources are fully utilized.

Virtual environment also provide isolation that is if one machine in the virtual server fails it won't affect the performance of other running virtual machines. According to American surveys [iii], more than 60% of the organizations are involved in the cloud services and are using the Virtual environment. Even the federal agencies of United States are using some services of cloud. In other words cloud is the most rapidly growing business of IT era.

[i] The next portion will describe the technical background and research that have already been introduced in terms of security threats. Later portions will describe virtualization and cloud computing in detail. The second last portion depicts the major security threats whereas in the last section the proposed security model is described.

II. TECHNICAL BACKGROUND

Virtualization and cloud security becomes serious issue of concern now a days, many researchers has put their ideas and methodologies on the security of virtual and cloud environment.

As being most growing industry in IT world, virtualization and cloud computing becomes theserious issue of concern in terms of security.

Reference [i] has proposed the idea of migrating the virtual machines from one host server to another and also the possible attacks that can be accomplished when migrating the Virtual machines. Denial of service attack and intercommunication VM attacks are more common and frequent. Un-encrypted channel when migrating the virtual machine from one machine to another can cause the man in middle attack and also guest VM can attack on the host operating machine. Access control policies, usage of firewalls,port blockage,Pre-VM firewall, encryption/decryption methods are used for the overcome of security.

Reference [ii] has proposed the idea on the security of virtualization in cloud computing. The user doesn't know where his data is residing in the cloud and user didn't know for what he is paying against services. Privacy declared as the major security concern in the cloud. His security model which composed of virtual

machine monitor VMM for monitoring of guest virtual machine in which all the activities are monitored by the detector and stored in the log file. It can monitor guest virtual machines and middleware integrity attacks while remaining transparent to users.

According to [iii] has proposed the idea on the security of cloud. Many of the organization are moving towards the cloud computing and they even don't know about the background security issues. Cyber-crimes causes loss of millions dollars for many organization, so most of the organizations compelled to discontinue to the cloud services. His proposed idea for the overcome of security is by using Virtual machine monitor, hyper safe and cloud Visor.

Reference [iv] stated that the cloud computing depends on virtualization for the distribution of services to end users and the security issues exists between the guest-to-guest virtual machines. His proposed idea is on security of cloud and virtualization. Hypervisor is the software which is used to create the virtual environment but on the other hand it also causes the security issues in guest virtual machines. There are some security attacks that occurs in the virtual environment like jail breaking, migration, client side and virtual network service. They mainly focused on the guest-to-guest virtual machines attacks in which one of the host or guest infected machine can infect all of the other machines. To protect guest virtual machines which are compromised by the attacker efficiently detects the guest-to-guest attacks and also the hidden attacker who run the tasks without appearing in the processes list.

According to [v] presented the virtual security framework which comprises of two parts: one is system security and second is security management of virtual network. The host machine is the control point of all virtual machines where we can start, stop and pause the VM's and also host machine can modify the hard disk storage, associated memory and also their physical location in hard disks. Some attacks that occurs in the virtual environment like the VM escape in which attacker runs the code in VM and gains the access to the hypervisor, poor isolation to machine can also cause the inter-VM attacks. Hissecurity model uses the virtual firewall which protects the network and virtual machines from outside attacks and also to use the vIDS/vIPS which collect the data behavior and sign of attacks in the virtual environment.

III. Virtualization and Cloud Components

Virtualization is most important element in making cloud environment. Virtualization help the IT department to host their running application on the cloud and make it easy to access and hence for this the security issue is most important and under consideration. The phrase virtual machine refers to a software computer like a physical computer, runs an operating system and applications. An operating system on a virtual machine is called a guest operating system. [Vi]

To monitor all this virtual machines the management layer is used which is called virtual machine manager VMM. Virtual machine manager is centralized monitoring tool and it shows all the resources which are utilized by all hosted virtual machines.

Most commonly used technique in virtualization is hypervisor which allows the many virtual machines called guest operating system to run parallel without degrading or effecting the performance of other virtual machines. Hypervisor monitor the execution and resource utilization of guest operating system. Hypervisor installed on the physical host server. [vii] hypervisor duty is to just run the guest machine called virtual machines.

IV. Virtualization Methods

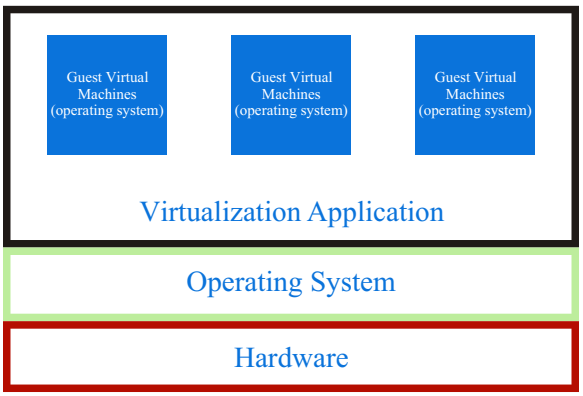
In IT departments the physical servers are directly connected to the physical switches and routers and hence the management and monitoring of traffic is not a tough task by IT professionals but in case of virtualization the virtual switch is connected to the physical server via the physical NIC so in this case the management of traffic effects the performance and lack security. [vii]

There are several methods we can used in virtualization infrastructure but every method or approach has own significant and drawbacks. [Vii] These methods are illustrated in Fig. 1. And both methods are discussed with detail.

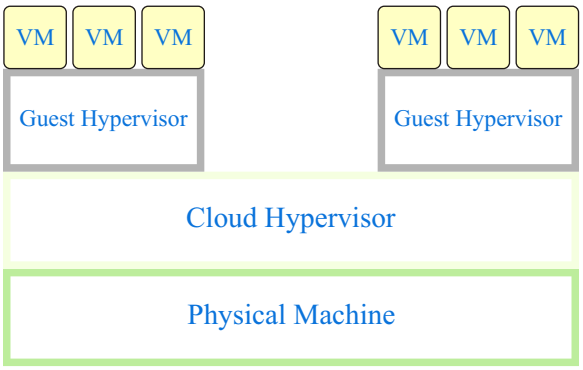
a. Operating-system based virtualization
b. Hypervisor-base virtualization

A. Operating-system based virtualization

In this method virtualization is based on the host operating system and all the virtual machines are directly influenced by the host operating system. The host operating system has all control on the virtual machines. This method is much simpler to implement but has some very serious drawbacks. Because of direct control of operating system to virtual machines, so it become more easier for attacker to inject DOS attacks or malicious attacks to kernel of operating system, so the whole virtualization infrastructure can be affected and attacker can have control all the virtual machines and can harm the virtual machines in the future. [vii]



(a) Operating-system based virtualization



Public (Cloud) Infrastructure

(b) Hypervisor based virtualization

Fig. 1 Virtualization Methods

B. Hypervisor-based virtualization

Hypervisor is available on the boot time of the machine and can be used to control the sharing of system resources across the multiple virtual machines.

As this technique is more controllable in the environment, so we can utilize additional security tools such as intrusion detection system(IDS) [vii], but problem with this approach is the single point of failure due to the reason that if the hypervisor is under attack then the attacker can take hold to all other virtual machines. But controlling or attacking from virtual machine to hypervisor is difficult. [vii]

V. Security Threats and Attacks in Virtualization Environment

The security threats found in the virtualized infrastructure are very common to the threats that we faced in the physical machines. The following are the list of some threats that are found in the virtualized environment.[v]

A. Attacks among virtual machines

Isolation is provided by the virtualized environment if deployed with carefulness. But if the structure of infrastructure is not policy based or control based then this cause the attacks between the virtual machines and the attacks among the virtual machine and virtual machine manager.[v]

One virtual machine can contaminate all other running virtual machine which exist on the same Host or physical server. The attacker just attack on the one target virtual machine and upon getting successful overtaking on one desired virtual machine the attacker can control or harm the overall virtual infrastructure and when attacker gets the full control over the hypervisor he can perform the spoofing attacks.

B. Virtual machine Outflow

Virtual machine outflow is an achievement in which the attacker/aggressor can run the scripting code and break out the limit of running operating system and can gain the access to the hypervisor on which all other virtual machines are running. Virtual machine outflow is the procedure in which attacker can negotiate the isolation among the host and virtual machines. The scripting code able to evade the VMM Layer and able to approach the other virtual machines and can also have the root privileges. In other words that the virtual machine overflow from the virtual machine boundary. [v]

C. Denial of service attack

DOS attack is passive type of attack in which the attacker over-flood the destination machine so that services offered by the destination machine will be inaccessible to the intended users. The DOS attack term is basically entertained in the computer network area but it's not limited to that but also used for CPU reserve management.

DOS attack in virtual environment can flood the destination machine with external requests so it can't able to respond the genuine traffic and purpose of this attack is to reset the machine or consuming running services and blocking the communication track between the planned user and victim virtual machine.

In virtual environment because the guest machine and host machine used the same physical resources so it is possible for guest machine attacker to inject the attack to all other guest machines and the attacker can take all conceivable resources of the schemes.

D. Data Leakage

When user move towards the cloud, they are unaware of data residing in the cloud because their data is not exist in in the local machine and secondly data is not protected by encryption or and other security algorithms. These problems cause the data over flow or data leakage. This becomes the hitches for the organization from security concern. All cloud provider's stores data on the third vendor storage. [vii]

Data leakage can be protected by a method in which user can use their encrypted keys mechanism.

All encryption based on user management key but problem with this solution is that there are many users on the cloud and to manage each user encryption management key scheme is tough task.

VI. Proposed Security Architecture

In this portion, we propose major security model which is used to secure virtual infrastructure and to protect the virtual machine from being attacked and also to secure the inter-VM communication.

A. Virtual Firewall architecture

Virtual firewall (VF) architecture shown in Fig. 2 used and positioned in virtual environment to inspect all the incoming and outing traffic and packets. The virtual firewall tends to be software based installed on the guest VM or physical machine. It can also installed and managed in Virtual machine manager. V-firewall can protects the virtual machines from spoofing or over flooding of packets.

Virtual firewall also defends the VM's from attacker or any other malware and keep the VM's secure from outside or internal threads.

On the other hand physical firewall protects the external and internal traffic but it doesn't monitor the inter-VM communication. So the attacker in your internal network can compromises the virtual machines. Virtual firewall adds the benefits by inspecting and monitoring the external traffic and also between the virtual machines.

With more and more critical applications it becomes threatening to protect the virtual infrastructure from attacks and also from misbehaving end users. Virtual firewall rules allow you to confine various type of traffic upcoming from inbound (external network) to the virtual infrastructure and from outbound (virtual machines) to the inbound and also between the virtual machines. In this way virtual infrastructure can be protected from inbound and outbound attacks.

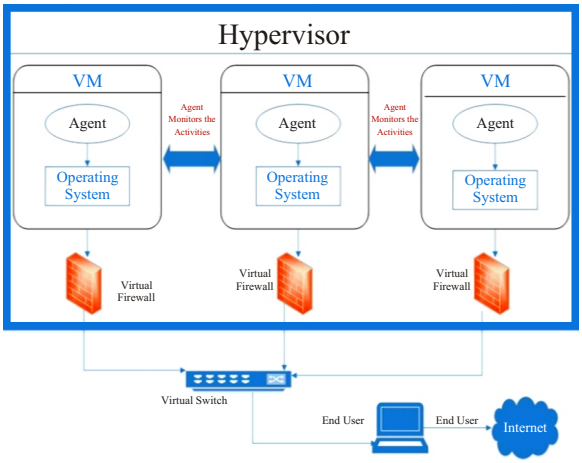


Fig. 2. virtual firewall architecture

In our proposed model, our main focus is to secure the inter-VM communication and secure traffic flow between virtual machines.

In this model, Virtual-firewall is used to install on the hypervisor machine which is either physical or virtual. Agent need to install on guest machines. Agent is service based software installed on operating system which monitors the activities on the virtual machines and send the information to V-firewall in form of logs. End users or virtual machine when tries to communicate with the virtual server the traffic flow like follows as shown in Fig. 3.

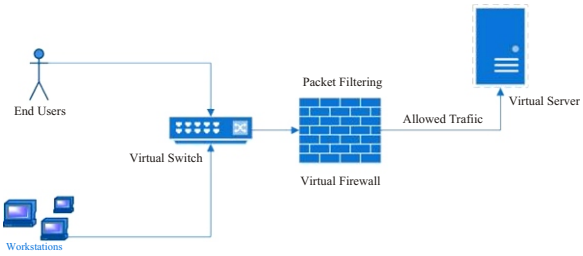


Fig. 3. virtual firewall

i. End client to virtual switch
ii. Virtual switch to virtual firewall
iii. Packet filtering
iv. Decision either to block or allow the traffic

Agent monitors the allowed inbound and outbound traffic and provide the logs.

In order to secure from the attacker prospective, only specific IP or IP ranges need to allow on the v-firewall. Expect allowed IP, all traffic will be discarded.

All virtual machines on the same hypervisor cannot communicate with each other unless they are manually explicitly allowed on the virtual firewall.

VII. Implementation

This architecture implemented on the 5nine virtual firewall and Microsoft Hyper-V as a hypervisor. 5 nine virtual firewall contains the management console and agent module. Agent module need to be installed on all guest machines. Purpose of agent is to block all incoming and outgoing traffic on the virtual machines. After installing the agent on the machine all the broadcast, TCP, UDP, ARP, ICMP etc. traffic will be blocked.

In DHCP enabled environment, machine will not able to get the IP lease from DHCP due to blockage of broadcast traffic as shown in Fig. 4.

Heartbeat service is used to check if all the security policies and rules are enforcing on the virtual machine, and virtual machine can be start and stopped in case of network filter is not communicated to prevent security exploits. Network traffic between virtual machines can be monitored and tracked to prevent from the malicious traffic. Network administrator can define the ports

based rules for incoming and outing traffic to internal and external users. Like traditional firewall rules, v-firewall rules can also base on the source and destination IP, source and destination port.

Purpose of this architecture is to secure the communication between the virtual machines and to prevent it from external and internal malicious attacks and unwanted traffic.

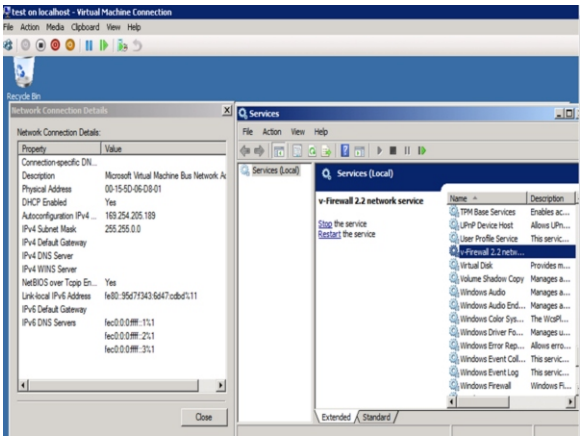


Fig. 4. DHCP Traffic Block

A . Simulation Setup and Environment

The level of access to each virtual machine is defined on the v-firewall rules. When the user access the virtual machine the traffic routes from the virtual-switch to the v-firewall before actually routing to the virtual machine and here decision has to be taken either to allow or block the traffic. All user activities are monitored and logged when user is accessing the resources of virtual machine. In this way, security layers has been added to virtual machines.

The activities of virtual machines are measured in the test environment and test environment has flowing requirement as shown in Table I.

Microsoft Hypervisor named hyper-V server 2008R2 with 4GB RAM with Intel core i5 processor used for simulation purpose. Two testing virtual machines with 4GB RAM, Intel core i5 processor and OS server 2008R2 are created on the same hypervisor. DHCP set to be enabled on both testing virtual machines in order to get the IP lease. We need to install the 5-nine virtual firewall manager on the hypervisor and agent need to be installed on the both virtual machines. By adding the virtual machines on virtual firewall manager block the incoming and outgoing traffic on the virtual machines due to agent. Agent by default blocks every traffic on the LAN card. Agent used heart beat services to communicate with the firewall manager. We need to manually add rules on virtual firewall manager to allow the required traffic on the every single virtual machine. Security between virtual machines can be enhanced by use of this agent. Only required protocol can be allowed on the virtual machine for secure communication to other virtual machine.

TABLE I
TEST ENVIRONMENT

Features	Vm1	Vm2	hypervisor
RAM	4GB	4GB	4GB
MODEL	Intel corei5	Inter corei5	Intel corei5
OS	Windows server2008 R2	Windows server2008 R2	Hyper-V server2008 R2
DHCP Enabled	YES	YES	YES

B. Results and Discussions

Test result measured by enabling the DHCP, ARP, TCP and ICMP (ping)protocol on the VM2 from the virtual firewall management console. We tried to communicate with the Virtual machine 2 using the ICMP protocol. We send the default 32 bytes packet of ICMP(ping) using the ping command on command prompt and get the reply from the virtual machine due to allowed rule on the manage console as shown in the Fig. 5. First of all when we tried to send the ICMP packet to the machine using the virtual machine IP, the traffic goes to virtual switch, virtual switch and v-firewall are bind together through the agent to inspect the incoming and outing traffic. Allowed incoming traffic should match the rule to communicate with the virtual machine.

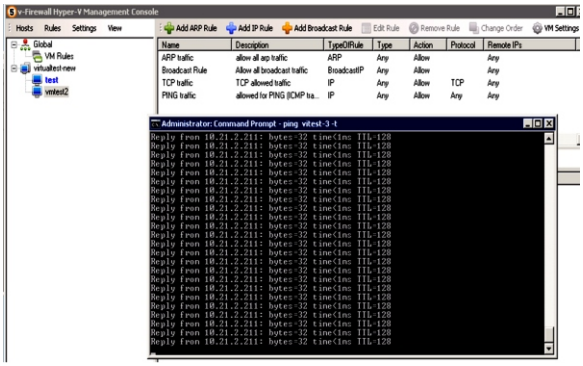


Fig. 5 Allowed Traffic

Another test result was measured by blocking ICMP (ping) protocol on virtual firewall rule so that any virtual machine on the network not able to send the ICMP or ping traffic to that machine as shown in the Fig. 6. After sending ICMP traffic to virtual machine from hypervisor, the output was "destination host unreachable". When traffic arrives at the virtual switch which is bind with virtual firewall it checks the rule and dropped the traffic due to denied protocol ICMP rule. We can also block the incoming and outgoing traffic on source and destination IP addresses and also on the basis of source and destination ports. Most of the enterprise web application are bind to the specific ports or IP address, so traffic can be allowed or denied by use of these parameter in the firewall rule.

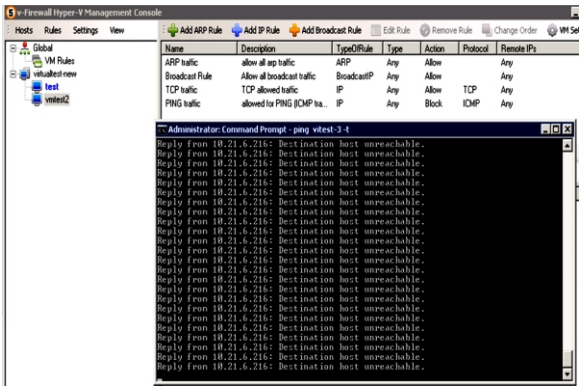


Fig. 6. Blocked Traffic

VIII. Conclusion and Future Work

In our security researched work, we present the security model for secure inter-VM communication in local and cloud environment. We tried to diminish the centralized workload from virtual machines and hypervisor. We present the security model which helps to overcome the security payload for cloud users and help them to minimize the risk of attacks in virtualized environment. We implement this model on the Microsoft Hyper-V hypervisor and calculates the results. Our future work focuses on the performance and scalability of this architecture on different platforms and hypervisors.

References

[i] M. R. Anala , J. S., G. Shobha, *A Framework for Secure Live Migration of VirtualMachines.* IEEE, 2013(978-1-4673-6217-7/13), pp. 243-248.

[ii] Artem Volokyta, I. K., Dmytro Ivanov, *Secure Virtualization in Cloud Computing.* February 2012,pp.21-22

[iii] P. K. M. Bora, *Cloud Security Tactics: Virtualization and the VMM.* 2012 IEEE, 2012(Department of Information Technology Hellenic American University).

[iv] C. D. Karthic , S. S., S. U. Muthunagai, *Efficient Access of Cloud Resources through Virtualization Techniques.* IEEE, 2012: pp. 5-7.

[v] Chen, S. L. Z. L. X., Z. Corporation, and C. Shenzhen, *Virtualization security for cloud computing service.* International Conference on Cloud and Service Computing, 2011(2011 IEEE),pp.174-179

[vi] R. Anand , S.S.a.R.R., *Security Issues in Virtualization Environment.* International Conference on Radar, Communication and Computing (ICRCC), 2012(2012),pp.254-256.

[vii] Farzad Sabahi, M., IEEE, *Secure Virtualization for Cloud Environment UsingHypervisor-based Technology.* International Journal of Machine Learning and Computing, 2012. Vol. 2(February 2012),pp.39-45.

[viii] M. R. Anala, J. S., G. Shobha, *A Framework for Secure Live Migration of VirtualMachines.* International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013,pp.243-248.

[ix] A. van Cleeff, W. P., R. Wieringa, *Security Implications of Virtualization A Literature Study.* International Conference on Computational Science and Engineering, 2009 IEEEDOI 10.1109/CSE.2009.267),pp.353-358.

[x] Chunxiao Li, S. M., IEEE, Anand Raghunathan, Fellow, IEEE, and and F. Niraj K. Jha, IEEE, *A Trusted Virtual Machine in an Untrusted Management Environment.* IEEE TRANSACTIONS ON SERVICES COMPUTING,2012.VOL.5(OCTOBER-DECEMBER 2012),pp.474-483.

[xi] A. S. Ibrahim, *Emerging Security Challenges of Cloud Virtual Infrastructure.* In Proceedings of APSEC 2010 Cloud Workshop 2010,p.66-68.

[xii] Z. Nan, *Virtualization Safety Problem Analysis.* Electrical and Information Engineering College, Shaanxi University of Science and Technology Xi' an 710021, P. R. China, 2011,pp.195-197 .

[xiii] J. Sahoo, *Virtualization: A Survey On Concepts,Taxonomy And Associated Security Issues.* Second International Conference on Computer and Network Technology, 2010 (978-0-7695-4042-9/10 IEEE),pp.90-95

[xiv] Sina Manavi, S. M., Nur Izura Udzir, Azizol Abdullah, *Hierarchical Secure Virtualization Model for Cloud,* IEEE, pp. 219-224.

[xv] Xiaorui Wang1, Q. W., Xiaolong Hu1, Jianping Lu1, *SECURITY TECHNOLOGY IN VIRTUALIZATION SYSTEM STATE OF THE ART AND FUTURE DIRECTION,* IET 2012,pp.1-7.