IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Applying Appropriate Security Policies Against Threats On Virtual Machines Using Multi-Step Approach: A Strategy

E.S. Phalguna Krishna [1], G. Mani Kumar [2], B. Madhu Priya[3]

[1]Dept of CSE, Sree Vidyanikethan Engineering College, India
[2]Student, Sree Vidyanikethan Engineering College, India
[3]Student, Sree Vidyanikethan Engineering College, India

Available online at: www.ijcseonline.org

Accepted: 14/Jul/2018, Published: 31/Jul/2018

Abstract: Security plays the most crucial role in cloud computing. Since the past years, there is a lot of research is going on security. On the other side of the coin, attackers are exploring, developing themselves drastically and exploiting the vulnerabilities in the cloud. Virtualization technology can be defined as backbone of the Cloud computing. Exploiters are taking the advantage of vulnerabilities in Virtual Machines. Thereby launching DDOS attacks, they can able to compromise virtual machines. Services like Saas, IaaS which helps for support end users may get affected and attackers may launch attacks either directly or by using zombies. Generally, Every Data Centre has their own security policies to deal with the security issues. However, in data centers, all the security policies are commonly been applied to the applications irrespective of their category or security threats that it face. The existing approach may take lots of time and wastage of resources. In this paper, we have developed an approach to segregate the applications as per the type of threats (by adapting detection mechanisms) being faced. Based on the zone in which applications are falling, only the relevant security policies will only be applied. This approach is optimized where we can effectively reduce the latency associated with applying security policies.

Keywords: Virtual Machine, Security, Threats.

I. INTRODUCTION

Virtualization can be considered as the backbone for cloud computing with which users can access multiple instances of apps, resources etc. Virtualization technology will allow one computer to do the job of multiple computers. This environment lets one computer host multiple operating systems at the same time. It transforms hardware into software. It is an emulation of a fully functional virtual computer that can run its own applications and operating system and also Creates virtual elements of the CPU, RAM, and hard disk. Hence, By using virtualization it is possible to run operating systems and multiple applications on the same server at the same time, thereby it raises the utilization and flexibility of hardware.

Some of the virtualization technologies include VMware, Hyper V, Virtual Iron etc.,

1.1Virtual Machines

These are the things that can manage OS and application as a Single unit by encapsulating them into Virtual Machines. A Virtual machine (VM) is an efficient, isolated duplicate of a real machine.

Virtual machines can be provisioned to any system

Duplicate: The behavior of the VM should be identical to the real machine. There is no difference with respect to the execution of the program at the low level.

Isolate: Multiple Virtual Instances corresponding to different Virtual Machines execute without interfering with each other

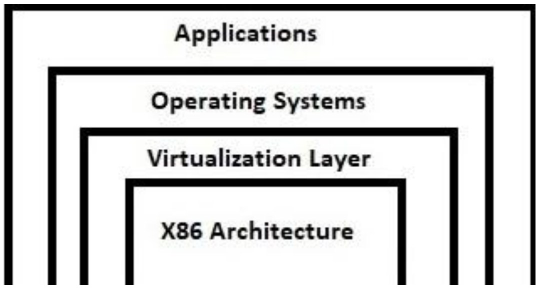

Fig 1: Layers of Virtualization

Efficient VM should operate at the speed of the underlying hardware.

While creating virtual machines, all the hardware resources of the computer are shared. By virtualization, it creates an emulation in which user can use actual owned resources. But at the implementation, these resources are shared between the multiple numbers of users at any given point in time. Further, Disks are partitioned into virtual disks and a normal user time-sharing terminal serves as Virtual machine operators console.

1.2 Types of Virtual Machines: Type 1 / Type 2

1)Type 1

They also called Hypervisors or virtual machine monitor or VMM. Hypervisors of this type are dependent on bare metal (bare machine) and always interacts with the machine. They Sit just above the Hardware and virtualizes the complete hardware. It runs on the physical hardware and is the real operating system. Normal unmodified operating systems like Linux, Windows runs at the top of the hypervisor. The server[5] which is hosting Type 1 Hypervisor requires some form of persistent storage[6] for storing the files of concern. In ESX server, the kernel uses device drives to actually get interfaced with bare metal.

• Example: Xen, VMware ESX server

2)Type 2 hypervisor

It is considered the most common type of hypervisor and depends on the underlying OS. These hypervisors require being directly installed on bare metal. It runs on an OS. It relies on OS services to manage Hardware. A normal unmodified host operating system like Linux or Windows runs on the physical hardware.

A type 2 hypervisor like VMware Workstation runs on the host operating system. Once after installing the host operating system, we can now deploy hypervisor and it doesn't modify it. Examples include QEMU, VMware Workstation etc.

II. THREATS ON VMS:

Like any other technology, Virtual Machines are prone to different categories of threats. Some attacks against virtual machine environments are variations of common threats such as denial of service etc. Others are still largely theoretical but likely approaching as buzz and means increase, these are the critical weaknesses.

1) VM Sprawl:

VMs are easy to deploy, and many organizations view them as hardware-like tools that don't merit formal policies. This has led to VM sprawl, which is the unplanned proliferation of VMs.

Attackers can take advantage of poorly monitored resources. More deployments also mean more failure points, so sprawl can cause problems even if no malice is involved.

2) Hyperjacking :

By using Hyperjacking, Attacker may take control of the hypervisor to gain access to the VMs and their data. It is typically launched against type2 hypervisors that run over a host OS although type 1 attacks are theoretically possible but practically difficult.

In reality, hyper jacking is rare due to the difficulty of directly accessing hypervisors. However, Hyperjacking is considered a real-world threat, and administrators should take the offensive and plan for it.

3) VM escape :

A guest OS escapes from its VM encapsulation to interact directly with the hypervisor. By doing so, the attacker can gain access to all VMs and, if guest privileges are high enough, the host machine can also be targeted as well. Although few, if any instances are known, experts consider VM escape to be the most serious threat to VM security.

4) Denial of Service:

Considered as the most common threat, These attacks exploit many hypervisor platforms and range from flooding a network with traffic to sophisticated leveraging of a host's own resources. The availability of botnets continues to make it easier for attackers to carry out campaigns against specific servers and applications with the goal of derailing the target's online services[3].

5) Incorrect VM Isolation:

To remain secure and correctly share resources, VMs must be isolated from each other. Improper control over VM deployments can lead to isolation breaches in which VMs communicate. Attackers can exploit this virtual drawbridge to gain access to multiple guests and possibly the host. The attacker can take the loopholes in the interfaces and can attack.

6) Unsecured VM migration:

This occurs when a VM is migrated to a new host, and security policies and configuration are not updated to reflect the change. Potentially, the host and other guests could become more vulnerable. Attackers have an advantage in that administrators are likely unaware of having introduced weaknesses and will not be on alert.

7) Host and guest vulnerabilities:

Host and guest interactions can magnify system vulnerabilities at several points. Their operating systems, particularly Windows, are likely to have multiple weaknesses. Like other systems, they are subject to vulnerabilities in email, Web browsing, and network protocols. However, virtual linkages and the co-hosting of different data sets make a serious attack on a virtual environment particularly damaging.

8) Dynamic environment:

Tracking and updating what you have can be a challenge as people create, suspend and move virtual machines. If you don't update your golden image from which virtual machines are deployed, you can end up needing to find and patch many virtual machines.

Mitigating Risk:

In order to overcome the existing problem with respect to the security, one can take several steps to minimize risk.

- **Characterization:** Here we characterize all deployed virtualization and any active security measures beyond built-in hypervisor controls on VMs.

- **Standards:** Security controls should be compared against industry standards to determine gaps.

  This Coverage includes anti-virus, intrusion detection, and active vulnerability scanning.

In addition to the above, consider these action steps:

VM traffic monitoring: Monitoring of VM backbone network traffic efficiently is critical. Conventional methods failed to detect VM traffic because it is controlled by internal soft switches. However, hypervisors have effective monitoring tools that should be enabled and tested. Also, by maintaining traffic logs we can have vigilance over the network traffic.

Administrative control: Procedures such as authentication, authorization, Identity management etc must be done as a regular process by the concerned admins. Sometimes, Due to VM sprawl and other issues, secure access can become compromised.

Customer security: Outside of the VM, make sure protection is in place for Customer interactive interfaces such as websites.

VM segregation: In addition to normal isolation, strengthen VM security through functional segregation. For example, consider creating separate security zones for desktops and servers. The goal is to minimize intersection points to the extent feasible.

III. VIRTUALIZATION VULNERABILITIES

Virtualization has improved many aspects of IT management but it increases the task of cyber security difficulty. The nature of virtualization introduces a new threat matrix.

Single Server :

- VMs run on a single server which poses serious security problems.
- A Virtual monitor should be root secure meaning that no privilege within the virtualized guest environment permits interference with the host system been found in all virtualization software which can be exploited by malicious, local users to bypass certain security restrictions or gain privileges.
- For example, the vulnerability of Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest OS.
- Vulnerability in Virtual PC and Virtual Server could allow elevation of privilege.

Ease of reconfiguration:

Ability to flexibly reconfigure restart and also the movement of VM‘s to other servers. Because of this easiness, an optimal environment to propagate vulnerabilities and unknown configuration errors have been created.

Dormant machines:

In public cloud environments, VM is available for any application even though it is offline.

- For example, a Web server that can access the physical server on which it resides.
- So a remote user on one VM can access another dormant VM if both reside on the same physical server.
- As Dormant machines can‘t perform malware scans, they are highly susceptible to malware attacks.
- Exploitation of this vulnerability is not only restricted to the VMs on a particular hypervisor but also affect other physical devices in the cloud.

For example, A Dormant machine might have been backed up or archived to another server or storage device.

Patch management:

Generally, users do the patch management in cloud computing and attackers could easily misuse this opportunity to attack VMs.

Cross-VM information leakage:

It is the ability of a malicious instance to utilize side channels to learn information about co-resident instances.

IV. MODULES

1) Packet Feeder:

The packet comes from different streams and they are fed into the packet feeder module which acts as the entry point to this approach. The responsibility of the packet the feeder is to collect packets from multiple incoming streams and store them in the module “FLOW DISCRIMINATOR”.

2) Flow Differentiator:

It manipulates as per the type of packets based on its properties (multimedia, text, voice, images etc).

3)Decision Maker:

This Module shows “Outlier Analysis” technique to distinguish different types of flows or vulnerabilities. For example Normal traffic, Flash Crowd traffic, DDOS traffic, dos traffic etc. Our approach using Outliers requires a lesser amount of computations and considered to be effective in distinguishing the attacks.

4) Zone Manager :

Based upon the nature of attacks on VMs, it is prescribed to adopt only the policies which are relevant.

ADVANTAGES:

- Rearranges the application of rule sets on different classifications of applications.
- This approach simultaneously minimizes the time taken by the data center admin by concerned with the consequential set of security strategies.

BLOCK DIAGRAM

The Packet Feeder which present in Network layer receives and reads all the packet and collects its properties. Based on the properties, it delineates Normal packets from attack packets and sends the traffic pattern to the Flow Differentiator which resides in Datalink Layer and Flow differentiator has a wide base of preloaded attack templates and patterns and based on this database, it performs identification of outliers will be achieved and attack traffic is differentiated from the normal traffic. Further, it also validates the existing attack.

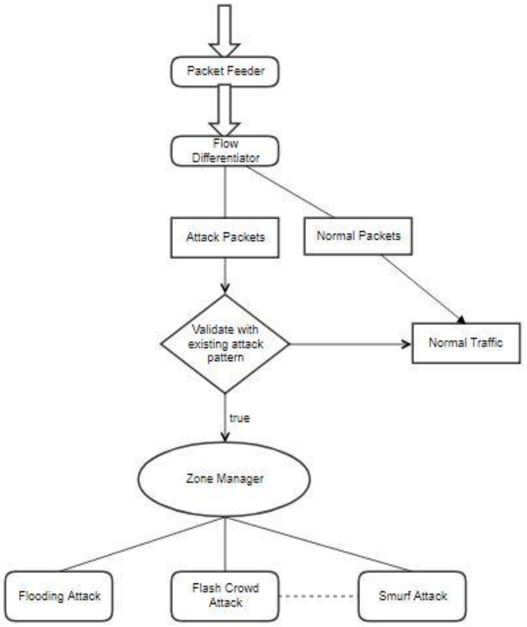

Fig 2:Block Diagram of our approach

In the following step, the decision maker collects traffic pattern from Flow Differentiator and compasses a case with an existing attack pattern and identifies a particular attack. Finally, the Zone manager segregates the attack traffic based on a particular attack and applies appropriate security policies. The main function is to categorize the traffic based on the attack that has performed and applies only a subset of security policies will be applicable instead of applying all the security policies.

V. METHODOLOGY

Users from varied locations post the Service Requests in the stream of packets to the Virtual servers/Virtual machines, which internally make use of virtualization technology. The packets approached are fed into the “Packet Feeder” module which behaves as a starting point for this approach. The responsibility of the packet feeder is to accumulate packets from succeeding streams and feed them to the module “Flow Discriminator”. The flow discriminator which takes various streams of packets as input distinguishes what type of packet stream it is based on its properties like file extension, contents of the packet functions of the packets etc and categorize them accordingly such as multimedia, voice, text, images etc. The variations are done mainly to adopt the admissible decision strategies and proper security policies. All categorized packet streams are given as input next module named “Decision Maker”. Decision Maker is the most important module which applies the Outlier Analysis technique to discriminate and differentiate between various types of vulnerabilities in the flow. For example Normal traffic, Flash Crowd traffic[2][3], Dos traffic, DDOS traffic. An advantage of using the Outliers in this approach just not only minimize the number of computations but also considered to be powerful in terms of discriminating the attacks. Finally, the various malicious traffic from normal traffic is sent to the “Zone Manager” which in turn distinguishes the DDOS traffic from FLASH CROWD traffic. Based on the type of VMs it is suggested to adopt necessarily untypical policies to safeguard users trust. This paper incorporates three cases: Normal Traffic, DDoS, Flash Crowd.

Based on the case, we apply the related significant security policies.This is in converse with the previous approach, wherein which the admins of the data center used to adopt common security policies for the discrete set of applications. The previous approach not only utilizes time but also leads to consuming more number of processor cycles.

Typically data center own distinct categories of applications. In order to provide the security, each and every data center maintains a set of security policies. It enumerates what it means to be secure for a system, organization or other entity. But the circumstances are like data center admins or tools apply the complete set of security policies in spite of the concept thereby consuming many processor cycles and advances the latency. In this paper, we have used an approach to segregate the applications as per the type of threats (by adapting detection mechanisms) being faced and we segregate them into zones. Based on the zone in which it is sited, only the relevant security policy terms will only be applied. This approach is optimized where we can efficiently decrease the latency combined with applying security policies. Consider a scenario in which a data center hosts the different set of software applications on their infrastructure. Let S be the main ruleset, there exists Subsets Si, Sj, Sk. For example, A, B, C, D applications belong to a particular type of application (multimedia) or facing particular threat (DDoS)[1].Let P,Q,R & X,Y be various categories. Then suppose A, B, C, D, are the applications that are facing DDoS attack[5] as a threat at this instance, Then it may be relevant to apply for example Si set of rules on those machines which are fabricated by it, In place of applying S. Where Si, Sj, Sk $\subseteq$ S. We accepted applications A, B, C, D as web apps and they are prone to DDoS attacks and Si as the subset of a rule set that consists of the security policies and mitigation strategies to be applied for DDoS. Similarly Sj ε (P,Q,R,S) and Sk ε (X,Y).

VI. CONCLUSION:

The flow differentiator is responsible to identify and differentiate the attacks. The VM's which were attacked will be taken care by Zone managers. They to segregate VM's & its corresponding applications to concerned zones. Zone maintains subset of rules which are specifically devoted to certain attacks and hence only the relevant security policies will be applied to the VM's which are running those applications that are affected with security threats. The proposed approach effectively minimizes the security policies and uses only fewer resources.

REFERENCES

[1]. Arbor Application Brief**: "**The Growing Threat of Application-Layer DDoS Attacks".2011.

[2]. Zhang Fu, Marina Papatriantafilou, and Philippas Tsigas "Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts" IEEE Transactions On Dependable And Secure Computing, Vol.9, No.3, May/June 2012.

[3]. Shui Yu, Weijia Jia, Song Guo, Yong Xiang, and Feilong Tang ,"Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient" IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 6, June 2012.

[4]. Ke Li, Wanlei Zhou, Ping Li, Jing Hai and Jianwen Liu, "Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics" Third International Conference on Network and System Security pno: 9-17 .2009.

[5]. Ari, B. Hong, E. L. Miller, S. A. Brandt, and D. D. E. Long, " Modeling , Analysis and Simulation of Flash Crowds on the Internet," Storage Systems Research Centre Jack Baskin School of Engineering University of California, Santa Cruz Santa Cruz, CA, ech. Rep. UCSC-CRL -03-15, Feb. 28, 2004 .