IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Prevention of Vulnerable Virtual Machines against DDOS Attacks in the Cloud

[1]Dr.Balaji K, [2]Tanushree M, [3]Pavan Kalyan, [4]Manik Rahul, [5]Rohit

[1]Professor, Department of MCA, Cambridge Institute of Technology CITech, Bengaluru, India, [2,3,4] Student, Department of MCA, CITech, Bengaluru, India.

ABSTRACT

One of the biggest issues that has drawn a lot of research and development attention in recent years is cloud security. Notably, assailants will investigate exploits in a cloud system and infiltrate virtual machines to release more extensive Distributed Denial-of-Service attacks (DDoS). Early-stage tactics including multi-step exploitation, low-frequency vulnerability scanning, and turning found susceptible virtual machines into zombies are sometimes used in DDoS assaults. Finally, DDoS attacks are launched using the zombies that have been infected. When it comes to cloud systems, especially Infrastructure-as-a-Service (IaaS) clouds, zombie exploration attack detection is truly problematic. This might occur from cloud customers installing susceptible software on their virtual computers.

Keywords: Attack graph model, NICE, distributed denial of service attack, cloud security, and cloud attacks

1.Introduction

Cloud computing is a system that maintains information and applications via central remote servers and the internet. Through cloud computing, users and companies may access their personal files from any computer with an internet connection and use apps without having to install them. This technology centralizes bandwidth, processes, and information storage, enabling far more efficient computing. Typically, cloud computing is used to deliver network-based services that appear to be delivered by actual server hardware but are actually delivered by simulated virtual hardware. by a piece of software that runs on one or more physical computers. Since these virtual servers aren't real, they can be moved around and scaled up or down without affecting the end user. A network-based environment with an emphasis on resource or computation sharing is called cloud computing. In reality, clouds are hosted on the Internet and attempt to hide complexity from users. Cloud computing encompasses the technology and software found in the data centers that host the applications that are provided as services over the Internet. Cloud providers leverage self-service capabilities in conjunction with virtualization technology to deliver computer resources through network infrastructure. Several types of virtual computers are housed on the same physical server as infrastructure in cloud settings. According to recent studies, security is the most crucial consideration for users moving to the cloud. According to a recent poll by the Cloud Security Alliance (CSA), of all security concerns, abuse and illicit use of cloud computing are seen as the biggest security threat. In these situations, attackers might leverage cloud vulnerabilities and leverage cloud system resources to launch attacks.

2.Cloud attacks come in several ways. Among the significant assaults that have been made are

1) A denial-of-service attack on the cloud is becoming a more common security risk. The attack usually occurs against the will of the impacted cloud users and purposefully jeopardizes the virtual machines availability.

2) A distributed denial-of-service attack against the cloud occurs when several hacked systems or compromised virtual machines attack one target (the cloud), depriving cloud users of the system's services. A compromised computer is referred to as a "zombie" or "bot." A botnet, also referred to as a zombie army, is a collection of hijacked computers.

3) XML-based Distributed Denial of Service (DDOS) attack: XML DoS assaults are highly asymmetrical; an attacker needs to use a fraction of the bandwidth or processing power required by the victim to handle the payload in order to send the attack payload. Even worse, there are numerous DoS vulnerabilities in XML-processing programs.

4) HTTP-based Distributed Denial of Service (DDOS) attack: When an HTTP client, such as a web browser, communicates with an HTTP server, such as a web server, it makes requests, of which there are two primary types: GET and POST. The term "normal links" refers to requests that are made using the GET protocol; these requests are intended to get static material, which is identified by its URL. This includes images.

NICE (Network Intrusion detection and Countermeasure Selection in Virtual Network Systems)

In order to create a defense-in-depth intrusion detection framework, NICE (Network Intrusion detection and Countermeasure Selection in Virtual Network Systems) was implemented. NICE integrates attack graph analysis techniques into the intrusion detection systems for improved attack detection.

There are two primary steps to NICE:

(1) To record and examine cloud traffic, install a thin, mirroring-based network intrusion detection agent (NICE-A) on every cloud server. A NICE-A periodically scans a cloud server's virtual system vulnerabilities to create Scenario Attack Graphs (SAGs). NICE will then determine whether or not to place a VM in network inspection state, depending on how serious the vulnerability is in relation to the collaborative attack goals.

(2) To highlight potential attack behaviours, virtual network reconfigurations or Deep Packet Inspection (DPI) can be done to a virtual machine (VM) that has entered the inspection state.

NICE's contributions are shown in the following manner:

(1) In a virtual networking context, we design and implement NICE, a novel multi-phase distributed network intrusion detection and prevention system that records.

(2) To evaluate and quarantine questionable virtual machines (VMs) for more research and security, NICE includes a software switching solution. Without interfering with currently running regular cloud services, NICE can increase the likelihood of attack detection and increase resilience against VM exploitation attacks.

(3) By comparing attack behavior, NICE uses a revolutionary attack graph approach for attack detection and prevention. It also recommends practical responses.

(4) To reduce resource consumption, NICE optimizes the deployment on cloud servers. Our research demonstrates that as compared to proxy-based network intrusion detection systems, NICE uses less computational overhead.

3.SYSTEM ARCHITECTURE:

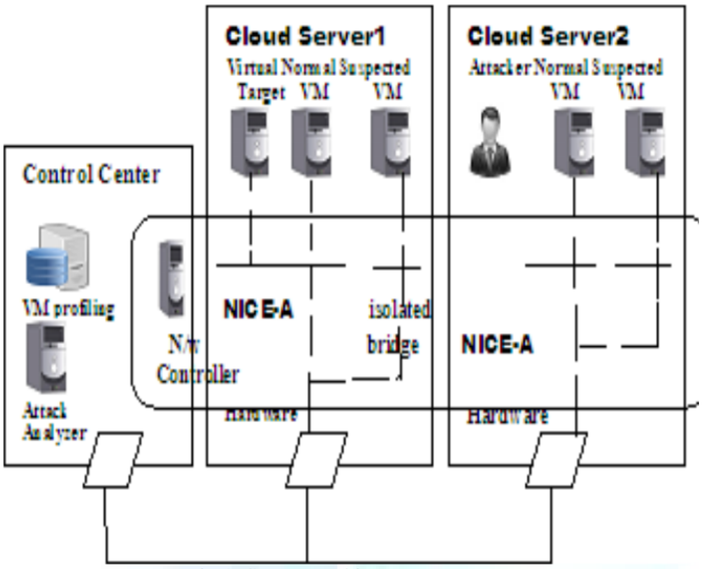

Fig 1: System architecture

Figure provides an illustration of the suggested NICE framework. It displays one cloud server cluster with the NICE framework within. The distributed and lightweight Nice-A on each physical cloud server, a network controller, a VM profiling server, and an attack analyzer are the main parts of this system.

4. SOLUTIONS TO THE PROBLEM:

4.1 GLORIOUS MODEL

This section explains how to use attack graphs to represent security risks and weaknesses in a virtual networked system. It also suggests a virtual machine protection model that uses virtual network reconfiguration techniques to stop VMs from being attacked.

Threat model:
We consider that an attacker may be found inside or outside the virtual networking system in this attack model. The main objective of the attacker is to take advantage of weak virtual machines and turn them into zombies. Our defense strategy is centered on attacks using virtual networks. detection and reconfiguration techniques to strengthen the defense against zombie incursions. Neither host-based intrusion detection systems nor how to manage encrypted traffic for attack detections are topics covered in my work. My suggested method can be implemented in a cloud networking system that offers Infrastructure-as-a-Service (IaaS), with the understanding that the Cloud Service Provider (CSP) is already up and running.

An attack graph model:
Attack graph model is a modelling tool that shows every potential multi-stage, multi-host attack path. This is important information for comprehending threats and determining the best course of action for countermeasures. Every node in an attack graph reflects an exploit's precondition or consequence. Since regular protocol interactions can potentially be utilized for attacks, the acts may not always constitute an active attack. An attack graph can be useful in locating known vulnerabilities, potential threats, and potential attacks on a cloud system. The attack graph gives us a comprehensive picture of the system's present security condition and allows us to forecast potential threats and attacks by correlating detected events or actions. It does this by providing data of all known vulnerabilities in the system as well as the connectivity infrastructure.

4.2 SYSTEM COMPONENTS:

4.2.1 Nice-A

Every cloud server has the Network-based Intrusion Detection System (NIDS) agent NICE-A installed. It examines all traffic entering and leaving the real cloud servers as well as traffic moving between virtual machines (VMs) via the bridges. It will probe every virtual bridge in the Open switch by sniffing a mirroring port. Every bridge establishes a separate subnet within the virtual network and links to all associated virtual machines. The virtual machines' traffic on the mirrored software bridge will be mirrored via the SPAN, RSPAN, or ERSPAN method to a particular port on a particular bridge.

4.2.2 VM Profiling:

Cloud virtual machines can be profiled to obtain detailed information about their current state, services that are active, open ports, etc. The connectivity of a virtual machine (VM) with other VMs is a significant feature that determines its profile. To confirm the legitimacy of alerts related to a virtual machine, it is also necessary to be aware of the services that are operating on that machine. An attacker can search for open ports on any virtual machine by using a port-scanning tool to do a thorough network analysis. Thus, details regarding any open ports on a virtual machine (VM) and their past usage are important factors in assessing the VM's vulnerability.

4.2.3 Attack Analyzer:

The attack analyzer is responsible for carrying out the primary tasks of the NICE system, which include creating and updating attack graphs, coordinating alerts, and choosing countermeasures. Information collection, creating the attack graph, and analyzing potential exploit paths are the three stages involved in creating and utilizing the Scenario Attack Graph (SAG). SAG can be used to model assault pathways with this information. The security level of each virtual machine (VM) in the virtual network of the cloud system can be determined using VSI.

Operations related to alert correlation and analysis are also managed by the Attack Analyzer. There are two main purposes for this component:

(1) Creates an Alert Correlation Graph (ACG)

(2) Gives the network controller threat intelligence and relevant countermeasures so they can reconfigure the virtual network. The NICE attack graph is built using the data listed below: Information about the topology and setup of virtual networks, cloud systems, and vulnerabilities.

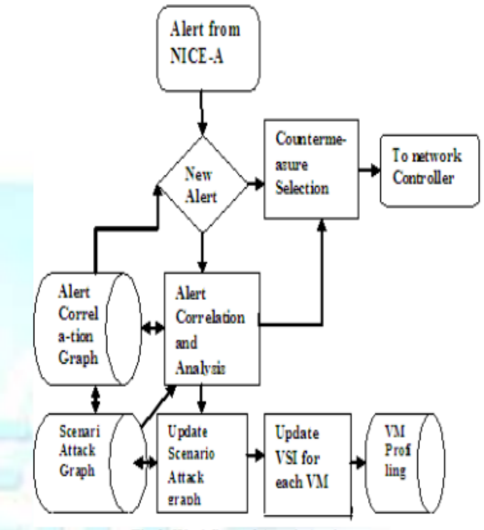
Alert from NICE-A
New Alert
Counterme-asure Selection
To network Controller
Alert Correl a-tion Graph
Alert Correlation and Analysis
Scenari Attack Graph
Update Scenario Attack graph
Update VSI for each VM
VM Prof ling

Fig 2: Workflow of Attack Analyzer

4.2.4 Network Controller:

A crucial element in enabling programmable networking and realizing virtual network reconfiguration is the network controller. The control functionalities for OVS and OFS were combined into the network controller in NICE, enabling the cloud system to define security and filtering rules in a comprehensive and integrated way. The network controller is in charge of gathering network data for the active Open Flow network and feeds attack analyzer data so that attack graphs can be created.

5. CONCLUSIONS:

As discussed NICE in this work, which is a suggested to identify and counteract cooperative attacks in the virtual networking environment of the cloud. NICE conducts attack detection and prediction using the attack graph concept. The suggested method looks into how to leverage software switch-based solutions' programmability to increase detection accuracy and thwart collaborative attacks' victim exploitation stages. Only the network IDS strategy is examined by NICE in order to thwart zombie exploratory attacks. Host-based IDS solutions must be integrated into the cloud system in order to enhance detection accuracy and cover the complete range of IDS.

7. REFERENCES:

[1] Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang, "NICE: Network Intrusion Detection and Countermeasure, Selection in Virtual Network Systems,

[2] K.Santhi, "A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013.

[3] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, "Detecting spam zombies by monitoring outgoing messages," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr. 2012.

[4] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using bayesian attack graphs," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74, Feb. 2012.

[5] E. Keller, J. Szefer, J. Rexford, and R. B. Lee, "NoHype: virtualized cloud infrastructure without the virtualization," Proc. of the 37th ACM ann. int'l symp. on Computer architecture (ISCA '10), pp. 350- 361. Jun. 2010.