IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Detection of Distributed Denial of Service and Counter Measure Selection Mechanism in Cloud System

Mrs. Sweta Kamat[1], Mrs. Poonam Sinai Kenkre[2], Mr. Shreedhar Niradi[3]

Assistant Professor, Computer Engineering Department, S.R.I.E.I.T, Goa, India[1, 2, 3]

Abstract: Cloud security is one of most significant problems that have attracted plenty of analysis and development effort in past few years. Significantly, attackers will explore vulnerabilities of a cloud system and compromise virtual machines to deploy additional large-scale Distributed Denial-of-Service (DDoS). DDoS attacks typically involve early stage actions like multi-step exploitation, low frequency vulnerability scanning, and compromising known vulnerable virtual machines as zombies, and eventually DDoS attacks through the compromised zombies. Inside the cloud system, particularly the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is very troublesome. This is often as a result of cloud users could install vulnerable applications on their virtual machines. to forestall vulnerable virtual machines from being compromised within the cloud, we have a tendency to propose a multi-phase distributed vulnerability detection, activity, and measure choice mechanism referred to as NICE, that is constructed on attack graph primarily based analytical models and reconfigurable virtual network-based countermeasures. The planned framework leverages Open Flow schedule genus Apis to create a monitor and management plane over distributed programmable virtual switches so as to considerably improve attack detection and mitigate attack consequences. The system and security evaluations demonstrate the potency and effectiveness of the planned resolution.

Keywords: Network security, cloud computing, intrusion detection, attack graph, zombie detection.

I. INTROUDUCTION

In recent studies have shown that users migrating to the cloud consider security because the most significant issue. A recent Cloud Security Alliance (CSA) survey shows that among all security problems, abuse and wicked use of cloud computing is taken into account because the high security threat, during which attackers will exploit vulnerabilities in clouds and utilize cloud system resources to deploy attacks. In ancient knowledge centers, wherever system directors have full management over the host machines, vulnerabilities may be detected and patched by the supervisor during a centralized manner.

However, reparation known security holes in cloud knowledge centers, wherever cloud users typically have the privilege to manage software package put in on their managed VMs, might not work effectively and might violate the Service Level Agreement (SLA). Moreover, cloud users will install vulnerable computer code on their VMs that primarily contributes to loopholes in cloud security. The challenge is to ascertain a good vulnerability/attack detection and response system for accurately characteristic attacks and minimizing the impact of security breach to cloud users.

During a cloud system wherever the infra-structure is shared by doubtless numerous users, abuse and wicked use of the shared infrastructure advantages attackers to take advantage of vulnerabilities of the cloud and use its resource to deploy attacks in additional economical ways in which. Such attacks square measure more practical within the cloud surroundings since cloud users typically share computing resources, e.g., being connected through constant switch, sharing with constant knowledge storage and file systems, even with potential attackers [1].

II. EXISTING SYSTEM

Cloud users can install vulnerable software on their VMs, which essentially contributes to loopholes in cloud security. The challenge is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users.

In a cloud system where the infrastructure is shared by potentially millions of users, abuse and nefarious use of the shared infrastructure benefits attackers to exploit vulnerabilities of the cloud and use its resource to deploy attacks in more efficient ways. Such attacks are more effective in the cloud environment since cloud users usually share computing resources, e.g., being connected through the same switch, sharing with the same data storage and file systems, even with potential attackers. The similar setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software, networking, etc., attracts attackers to compromise multiple VMs [3].

LIMITATIONES OF EXISTING SYSTEM:

1. No detection and prevention framework in a virtual networking environment.
2. Not accuracy in the attack detection from attackers.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

III. PROPOSED SYSTEM

In this article, we tend to propose NICE (Network Intrusion detection and measure choice in virtual network systems) to ascertain a defense-in-depth intrusion detection framework. For higher attack detection, NICE incorporates attack graph analytical procedures into the intrusion detection processes. we tend to should note that the planning of NICE doesn't shall improve any of the present intrusion detection algorithms; so, NICE employs a reconfigurable virtual networking approach to notice and counter the makes an attempt to compromise VMs, so preventing zombie VMs.

BENFITS OF PLANNED SYSTEM:
The contributions of NICE are presented as follows:

- We devise NICE, a brand new multi-phase distributed network intrusion detection and interference framework during a virtual networking surroundings that captures and inspects suspicious cloud traffic while not interrupting users' applications and cloud services.
- NICE incorporates a package switch resolution to quarantine and examine suspicious VMs for any investigation and protection. Through programmable network approaches, NICE will improve the attack detection likelihood and improve the resiliency to VM exploitation attack while not interrupting existing traditional cloud services.
- NICE employs a unique attack graph approach for attack detection and interference by correlating attack behavior and conjointly suggests effective countermeasures.
  NICE optimizes the implementation on cloud servers to reduce resource consumption. Our study shows that NICE consumes less process overhead compared to proxy-based network intrusion detection solutions.

III. OVERVIEW OF NICE SYSTEM DESIGN

In this section, we first present the system design overview of NICE and then detailed descriptions of its components.

System Design Overview
The planned NICE framework is illustrated in Figure. It shows the great framework among one cloud server cluster. Major parts during this framework square measure distributed and light-weighted NICE-A on every physical cloud server, a network controller, a VM identification server, and an attack analyzer. The latter 3 parts square measure situated in an exceedingly centralized center connected to software package switches on every cloud server (i.e., virtual switches engineered on one or multiple UNIX software package bridges).

NICE-A could be a software package agent enforced in every cloud server connected to the center through an obsessive and isolated secure channel, that is separated from the traditional information packets exploitation Open Flow tunneling or VLAN approaches. The network controller is accountable for deploying attack countermeasures supported selections created by the attack analyzer [5].

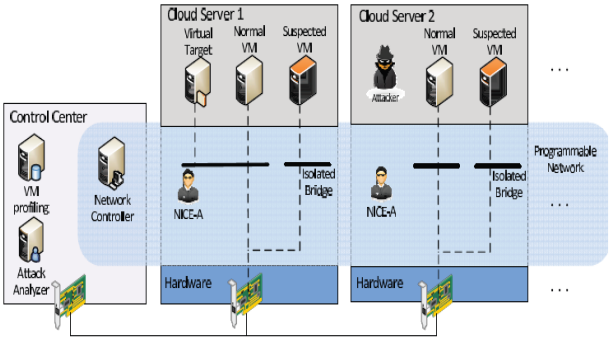

Figure 1.NICE Architecture within one Cloud Server.

Analyzer based on the evaluation results from the cost benefit analysis of the effectiveness of countermeasures. Then, the network controller initiates countermeasure actions by reconfiguring virtual or physical OFSs.

V. CONCLUSION AND FUTURE WORK

In this paper, we've presented NICE, that is planned to detect and mitigate cooperative attacks within the cloud virtual networking setting. NICE utilizes the attack graph model to conduct attack detection and prediction. The planned resolution investigates a way to use the program ability of computer code switches-based solutions to enhance detection accuracy and defeat victim exploitation phases of cooperative attacks. The system performance analysis demonstrates the feasibility of NICE and shows that the planned resolution will considerably scale back the danger of the cloud system from being exploited and abused by internal and external attackers. NICE solely investigates the network IDS approach to counter zombie consumptive attacks. To enhance the detection accuracy, host-based IDS solutions area unit required to be incorporated and to hide the total spectrum of IDS within the cloud system. This could be investigated within the future work. To boot, as indicated within the paper, we are going to investigate the measurability of the planned NICE resolution by work the suburbanized network management and attack analysis model supported current study.

REFERENCES

[1] Could Security Alliance, "Top Threats to Cloud Computing v1.0," https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Mar. 2010.
[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," ACM Comm., vol. 53, no. 4, pp. 50-58, Apr. 2010.
[3] B. Joshi, A. Vijay an, and B. Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," Proc. IEEE Int'l Conf. Computer Comm. and Informatics (ICCCI '12), Jan. 2012.
[4] H. Takabi, J.B. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Dec. 2010.
[5] "Open switch Project," http://openvswitch.org, May 2012.
[6] 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.
[7] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "Bot Hunter: Detecting Malware Infection through IDS-driven Dialog Correlation," Proc. 16th USENIX Security Symp. (SS '07), pp. 12:1-12:16, Aug. 2007.
[8] G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," Proc. 15th Ann. Network and Distributed System Security Symp. (NDSS '08), Feb.