ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 13, No. 2, 2018, *pp*.151-154

An Improved Network-based Intrusion Detection System for Virtual Private Networks

S V Athawale [1], M A Pund[2]

[1] Department of Computer Engg， AISSMS COE Pune, India

[2] Professor Computer Science & Engineering PRMIT & R ,Badnera Amravati, India

(Received March 06 2017, accepted February 11 2018)

Abstract Use of internet increases day by day so securing network and data is big issue. So, it is very important to maintain security to ensure safe and trusted communication of information between different organizations. Because of these IDS is very useful component of computer and network security. IDS system is used by many organizations or industries to detect the weakness in their security, documenting previous attacks and threats and preventing all of this from violating security policies .Because of these advantages this system is important in system security.

In this paper we find the solution for different approaches (attacks) based on intrusion detection system. In this paper we identify different attacks and find solution for different type of attacks such as DDOS, SQL injection and brute force attack. In this case we use client server architecture.

To implement this we maintain profile of user and base on this we find normal user or attacker ,when system find that attack is present then it directly block the attack.

Keywords: DDos, SQL injection, Brute force, CFG, Scenario Attack Graph, Nice Agent

1. Introduction

Nowadays, Cloud computing is one of the top security threats in which attackers can make the use of vulnerabilities and system resources to make attacks. In cloud environment millions of users shares computing resources so such attacks are very effective.

In one system we are giving solution to multiple attacks, at different stages. This is client-server based system. Multiple clients will be connected to server and our aim is to secure server.

To protect system from Brute Force attack, if client enters wrong password more than three times we will block that client. So, this will protect the attacker from entering into the system. In DDos attack, attacker will try to flood the targeted resource using multiple computers and multiple Internet connections. In this system we are using K-means algorithm for finding malicious behavior. After finding such behavior attacker will be blocked.

In SQL injection, attacker will execute malicious SQL statements to breach the database security. Attacker can access credential data such as passwords stored in database using this attack. In our system we are providing solution to such SQL injection attack.

2. Related Work

Debajyoti Mukhopadhyay, Byung-Jun Oh, Sang-Heon Shim, Young-Chon Kim have presented a study on the recent approaches like rate limit, active filtering, defence by offence, and ip traceback for handling DDos attacks[1].Anushree, Priyanka Baviskar, Pooja Dalimbe, Sneha Dhaswadikar, S V Athawale presented a paper[2] which proposes a bundle marking plan which checks the data into packets IP header field and beats the issue of IP spoofing. The marked data is utilized to remake the IP location of the entrance router joined with the attack source at the distinguishing end. The work is given to the programmable router progressively and completion of attack source recognition systems will be done. It will improve the performance of the legitimate traffic. DDOS attack is difficult to identify at the source since the attackers to spoofed IP address. Chirag D Patel, Chirag A. Patel discusses various IP Trackback schemes to find out attacker or source of attack in their paper[3]. Olof Enqvist, Fangyuan Jiang, Fredrik Kahl derive a simple brute-force algorithm which is both robust to outliers and has no algorithmic degene racies[4]. Their method is based on parameter search in a four dimensional space using a new epipolar parametrization. Jim Owens and Jeanna Matthews report on a study of brute-force SSH attacks observed on three very different networks: a residential system with a DSL Internet connection, an Internet-connected small business network ,and a

university campus network[5].In the paper S. Vaithyasubramanian, A. Christy report on a study of brute force attack on CFG passwords. CFG passwords are created using the model of the Context Free Grammar[6]. Research in field of database intrusion detection and prevention has been going on for more than two decades. The approaches used in detecting database intrusions mainly includes data mining and traditional security measures .In this section we represent literatures of several highly related research areas to IDS including: zombie detection and prevention, maintaining profile and security analysis . SQL Injection Attack Detection and Prevention Methods[7]: A Review (Dr. Manju Kaushik et al. 2014) he suggested that by using SQLIA, an attacker can get these lines gain or adjust private information. They suggest a methods to prepare for the assaults centered at set away philosophy. This system joins static application code examination with runtime acknowledgment to take out the occasion of such assaults.SQL Injection Attack (J.makesh et al. 2015) [8],In this paper many methods are given and future work to execute the firewall to the SQL server to maintain a strategic distance from the combine assaults. A main goal to detect the entire idea of SQL injection and to stay away .

SQL Injection(SQLI)(Sejal Farde,Sailee Chaudhari.2016) In this paper[9], they presented all SQL injection attack types & also tools which are used to detect or prevent all types of SQL injection attacks. SQL injection attacks allow attackers to spoof identity, cause security issues, allow complete access of all data on the users system, and destroy data.

3. Nice Model

Threat Model : In our attack model, we assume that an attacker can be located either outside or inside of the virtual networking system. The attacker's primary goal is to exploit vulnerable VMs and compromise them as zombies. Our protection model focuses on virtual-network-based attack detection and reconfiguration solutions to improve the resiliency to zombie explorations. Our work does not involve host-based IDS and does not address how to handle encrypted traffic for attack detections.

Our proposed solution can be deployed in an Infrastructure-as-a-Service (IaaS) cloud networking system, and we assume that the Service Provider is benign. We also assume that cloud service users are free to install whatever operating systems or applications they want, even if such action may introduce vulnerabilities to their controlled VMs. Physical security of cloud server is out of scope of this paper. We assume that the hypervisor is secure and free of any vulnerability.

Attack Graph Model : An attack graph is a modeling tool to illustrate all possible multi-stage, multi-host attack paths that are crucial to understand threats and then to decide appropriate countermeasures. In an attack graph, each node represents either precondition or consequence of an exploit. The actions are not necessarily an active attack since normal protocol interactions can also be used for attacks. Attack graph is helpful in identifying potential threats, possible attacks and known vulnerabilities in a cloud system. Since the attack graph provides details of all known vulnerabilities in the system and the connectivity information, we get a whole picture of current security situation of the system where we can predict the possible threats and attacks by correlating detected events or activities. If an event is recognized as a potential attack, we can apply specific countermeasures to mitigate its impact or take actions to prevent it from contaminating the cloud system. To represent the attack and the result of such actions, we extend the notation of MulVAL logic attack graph as presented by X. Ou et al. and define as Scenario Attack Graph (SAG).

VM Protection Model : The VM protection model of NICE consists of a VM profiler, a security indexer and a state monitor. We specify security index for all the VMs in the network depending upon various factors like connectivity, the number of vulnerabilities present and their impact scores. The impact score of vulnerability helps to judge the confidentiality, integrity, and availability impact of the vulnerability being exploited. Connectivity metric of a VM is decided by evaluating incoming and outgoing connections. Based on the information gathered from the network controller.

VM states can be defined as following:

1. Stable: does not exist any known vulnerability on the VM.
2. Vulnerable: presence of one or more vulnerabilities on a VM, which remains unexploited.
3. Exploited: at least one vulnerability has been exploited and the VM is compromised.
4. Zombie: VM is under control of attacker.

System Design: Nice Agent : The NICE-A is a Network-based Intrusion Detection System (NIDS) agent installed in each cloud server. It inspects the traffic going through the bridges that control all the traffic among VMs and in/out from the physical cloud servers. It will sniff a mirroring port on each virtual bridge in the Open v Switch. Each bridge creates an isolated subnet in the virtual network and connects to all related VMs. The traffic generated from the Virtual Machines on the mirrored Software Bridge will be mirrored to a specific port on a specific bridge using SPAN ERSPAN or RSPAN methods. It's more efficient to scan the traffic in cloud server since all traffic in the cloud server needs go through it; however our design is independent to the installed VM. The false alarm rate could be decreased through our architecture design.

DDOS Attack Detection Model: DDoS attacks are quick to start killing performance on the server. The first clue that you're under an attack is a server crash. With IIS, the server often returns a 503 "Service Unavailable" error. It usually starts intermittently displaying this error, but heavy attacks lead to permanent 503 server responses for all of your users.When using a DDoS protection service, all or most of the traffic going to and from a target network is routed through the protection services networking equipment. This service "scrubs" all of the potential threat DDoS traffic and forwards all valid traffic to the target's network. The problem is that when a target routes all of its traffic through a separate entity (like a protection service provider) it can add some complexity to the implementation of specific features used by many enterprises.

SQL Injection Detection Model: SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

Brute Force attack Detection Model: In cryptography, a brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search. A brute-force attack is a cryptanalytic attack that can, in theory, be used to attempt to decrypt any encrypted data [7], (except for data encrypted in an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. When password guessing, this method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used because a brute-force search takes too long. Longer passwords, passphrases and keys have more possible values, making them exponentially more difficult to crack than shorter ones.

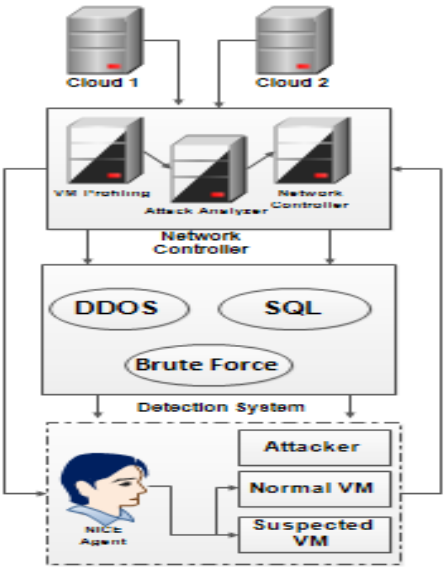

Figure 1: System Design

Table 1 Performance Table

Attack Type	Attack 1	Attack 2	Attack 3
DDOS	75%	80%	90%
SQL injection	60%	75%	85%
Brute Force	65%	75%	80%

4. Conclusion

In this paper, we presented network intrusion detection and prevention, which is proposed to detect and mitigate collaborative attacks in the virtual networking environment. The proposed solution investigates how to use the programmability of software switches based solutions to improve the detection accuracy and defeat victim exploitation phases of collaborative attacks. The system performance evaluation demonstrates the feasibility of the system and shows that the proposed solution can significantly reduce the risk of the cloud system from being exploited and abused by internal and external attackers. In order to improve the detection accuracy, host-based IDS solutions are needed to be incorporated and to cover the whole spectrum of IDS in the virtual private network systems system. This should be investigated in the future work.

5. Acknowledgements

I would like to thank the all wireless security specialists for their participation in the survey who supported my work in this way and helped me get results of better quality. I am also grateful to the M A Pund for his patience and support in overcoming numerous obstacles I have been facing through my research.

6. Reference

[1] Chirag D Patel, Chirag A. Patel, IP Traceback Techniques Review for DOS/DDOS Attacks, IJEDR Volume 3, Issue 4 , ISSN: 2321-9939, pp.761-765, 2015.

[2] Anushree , Priyanka Baviskar, Pooja Dalimbe, Sneha Dhaswadikar, S V Athawale, Defence Mechanism to Mitigate DDoS Attack For Wireless LAN, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume – 5 Issue -02 February, (2016) pp. 15714-15718.

[3] Debajyoti Mukhopadhyay, Byung-Jun Oh, Sang-Heon Shim, Young-Chon Kim, A Study on Recent Approaches in Handling DDoS Attacks CoRR abs/1012.2979 (2010).

[4] Olof Enqvist, Fangyuan Jiang, Fredrik Kahl, A Brute-Force Algorithm for Reconstructing a Scene from Two Projections, Centre for Mathematical Sciences, Lund University, Sweden fangyuan,fredrikg@maths.lth.se ,2015.

[5] Jim Owens and Jeanna Matthews, A Study of Passwords and Methods Used in Brute-Force SSH Attacks, 2015.Available at: {owensjp, jnm}@clarkson.edu.

[6] S. Vaithyasubramanian, A. Christy, An Analysis of CFG Password Against Brute Force Attack for Web Applications, Contemporary Engineering Sciences, Vol. 8, 2015, no. 9, 367 - 374 HIKARI Ltd, www.m-hikari.com http://dx.doi.org/10.12988/ces.2015.5252 .

[7] Dr.Manju Kaushik,Gazal Ojha (2014) ,SQL Injection Attack Detection and prevention Methods: A Critical Review , International Journal of Innovative Research in Science, Engineering and Technology(An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 4, April 2014.

[8] J.makesh, S.Thirunavukarasu (2015) ,SQL Injection Attack, Special Issue of Engineering and Scientific International Journal (ESIJ) ISSN 2394-187(Online) Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College ISSN 2394-7179 (Print) (TSRW-MCA-SAEC) – May 2015 16.

[9] Sejal Farde, Sailee Chaudhari ,SQL Injection(SQLI) International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5, Issue 6, (2016), June.