IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Protecting Web Servers from Distributed Denial of Service Attacks

Prof. Dr. A.N. Banubakode[1], Badal Mehta[2], Tanmay Modak[3], Vrushal Chaudhary[4]

Professor, Information Technology, JSPM's Rajarshi Shahu College of Engineering, Pune, India[1]

Student, Information Technology, JSPM's Rajarshi Shahu College of Engineering, Pune, India[2,3,4]

Abstract: Recently many prominent websites faced the Distributed Denial of Service (DDOS) attacks. While former security threats could be faced by tight security policy and measures like using firewalls, vendor patches etc. These DDOS are new in such a way that there is no completely satisfying protection as yet. There are certain solutions based on class based routing mechanisms in the LINUX kernel which prevent most severe impacts of DDOS. However, these do not provide complete security to the web server and hence there is a need to focus on other defence mechanisms. That is why we propose to introduce a concept called Honeypot in which we create a proxy server so as to lure attackers. In this system we can identify the attacker and can be notified immediately.

Keywords: LINUX kernel, Distributed Denial of Service (DDOS) attacks, Web Servers.

I. INTRODUCTION

The extremely widely used World Wide Web environment provides a rich set of targets for motivated attackers. The main goal of the attack is the disruption of service. To prevent these attacks and prevent these servers from DDOS attacks we are implementing a system which is going to use 'Honeypot' system and 'AES 128-bit Algorithm'

In this we are using Banking application which can do online transactions and can detect attacks like SQL injection , Brute Force Attacks , URL injection, Cross site scripting attack, Personal information of the user get stored in database in encrypted format, dynamic password and PIN is generated and sent to the user on his email. After every transaction user gets notification by message. User can see his account details and mini statements. The internet was originally designed to facilitate the research and educational communities with an open and scalable network. Due to the increased number of cyber-attacks over the past years, solving the security issues has gained more importance. DOS and DDOS attacks being the most popular ones. After detailed study of DOS and DDOS attacks on the internet their victims and possible form of attacks, we realize that there are a lot of challenges in defending against these attacks. Since most of the DDOS attacks are due to the vulnerability in the Protocols at different layers of TCP/IP model of the internet, our study is mainly focused on exploration of different types of DDOS attacks and their effects on the server.

II.LITERATURE SURVEY [1]

PROPOSED WAY FOR DEFENDING AGAINST DDOS ATTACKS:-

Honeypot:-

System uses some techniques which are as follows-

Honeypot System:

A honeypotis a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

Based on design criteria, honeypots can be classified as:

1. Pure honeypots :

Are full-fledged production systems. The activities of the attacker are monitored by using a casual tap that has been installed on the honeypots link to the network.

2. High-interaction honeypots :

Imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time.

3.Low-interaction honeypots :

Simulate only the services frequently requested by attackers. When we say we are using a honeypot, we are creating a proxy server which acts exactly as the actual server. Only the admin knows that it is not the real server. The attacker tries to steal data from the proxy server and we can then identify the attacker using their IP address.

III. LITERATURE SURVEY [2]

A FEASIBLE METHOD TO COMBAT AGAINST DDOS ATTACK IN SDN NETWORK:-

In Software Defined Network, flooding attack affects the controller on a large scale. By injecting spoofed request packets continuously, attackers make a burdensome process to thecontroller, cause bandwidth occupation in the controller-switchchannel, and overload the flow table in switch. The motive of attackers is to downgrading or even shutting down the stability and quality of service of the network. In this paper, we introduce a method which protects the network against Distributed Denial of Service attacks more feasibly and effectively.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

The proposed method :
We define a temple table (T table) in the controller. The T table is used to store source IP addresses of forwarded packetsfrom the switch. Each unique IP address has a counter ci totrack the number of arrived packets.
During attack time, whenever a new packet forwarded bythe switch arrives at the controller, the controller assumesthat it might be from the DDoS attacking address firstly. Thecontroller creates a new specific entry with hard timeout and idle timeout, of which values are smaller than those of normal entries, to limit its lifetime. Then, the table is updated with the source IP address for tracking, and its counter ci is increased by 1.
When ci reaches k, by requesting the average number of packet counter s helps us in analyzing the traffic characteristics. If s is greater than n, then the source address established and transmitted real data connections. In other words, it is a frequent user. Hence, the controller issues a modification message to reset all hard timeout and idle timeout of its existing entries to normal value [6]. In vice versa, if s is smaller than n, this is malicious traffic. The controller dispatches a dropped rule for the address to the switch.
SDN is expected to replace the existing traditional network with a lot of advanced features. However, many security challenges need to be countered. In this paper, we propose a feasible method to combat againstDDoS flooding attack. Although the method can decrease the impact of DDoS attack, but not enough when the amount of attack traffic is very huge.

IV.LITERATURE SURVEY [3]

DISTRIBUTED CAPABILITIES-BASED DDOS DEFENSE:
Existing strategies against DDoS are implemented at different network locations as single point solutions. Our understanding is that, no single network location can cater to the needs of a full-proof defense solution, considering the DDoS nature and activities for its mitigation. In this paper, we get collective information about some important defense mechanisms discussing their advantages and limitations. Based on our understanding, distribution of DDoS defence can be proposed by us where we use improved techniques for capabilities-based traffic differentiation and scheduling-based rate-limiting. Additionally, so as to predict an attack, wepropose a novel approach fordetermining the prospective attackers as well as the time-to-saturation of victim. We present two algorithms for this distribution of defense. With the implementation of these incremental improvements proposed distributed approach in the defense activities is expected to provide better solution against the DDoS problem.

Algorithm 1: WPF algorithm for defense node selection.

Input: Victim node v, Path matrix P, required number of defence node d
Output: Set of d defence nodes
1 Compute a set Pk of all k-hop paths to node v;
2 Compute the set of ND of all nodes on paths in Pk: ∪p∈PkNodes(p);
3 **foreach**path p ∈ Pk **do**
4 Compute the number of paths that intersect with p as follows:
5 Identify the set of paths Q, where ∀q∈QNodes(Q) ∩ Nodes(p) > 0;
6 Intersection(p) = |Q|;
7 **end**
8 uncovered_paths = Pk;
9 **foreach**path p ∈Pk in increasing order of Intersection(p) **do**
10 **foreach**node n ∈Nodes(p) **do**
11 Compute coverage of the node n, Cnas follows:
12 Cn = paths_covered(n) ∩ uncovered paths;
13 **end**
14 **end**
15 Select the node n that provides maximum coverageCoveragen;
16 Remove paths covered(n) from the set uncovered paths;
17 Remove the selected node n from the set ND;
18 Repeat steps 9 to 17 until d nodes are not selected oruncovered_pathsis NULL;

Algorithm 2: MCNF algorithm for defense node Selection
Input: Victim node v, Path matrix P, required number of defense node d
Output: Set of d defense nodes
1 Compute a set Pk of all k-hop paths to node v;
2 Compute the set ND of all nodes on paths in Pk: ND = ∪p∈Pk Nodes(p);
3 uncovered_paths = Pk;
4 **foreach**node n ∈ ND **do**
5 Compute coverage of the node n, Cn as follows:
6 Cn = paths_covered(n) \ uncovered_paths;
7 **end**
8 Select the node n that provides maximum coverageCn;
9 Remove paths_covered(n) from the set Uncovered_paths;
10 Remove the selected node n from the set ND;
11 Repeat steps 4 to 10 until d nodes are not selected oruncovered paths is NULL;

In this survey, we discussed various DDoS defense mechanisms implemented at different network locations. A robust DDoS defense involves different activities. Any solution at a single network location cannot perform all of them efficiently. Based on this understanding, we presented a distributed defense solution. We proposed two algorithms for the defense nodes placement. Further, we proposed some initial ideas to improve traffic differentiation activity. We have also suggested adding a predictive analytical approach in identifying occurrence of an attack and identifying prospective attackers. Our

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

proposed rate-limiting scheme is based on pre-emptive scheduling. It is aimed at avoiding bandwidth crunch caused by genuine traffic and flooding attack. With rate-limiting deployed for attack traffic, this defense would ensure consistent service to the legitimate clients.
With these insights, we try to foresee the requirements and challenges in implementing these ideas. We plan to explore and investigate more on the suggested solutions. Our immediate next step would target the development of prediction algorithm for preventive defense described in Section V and traffic differentiation suggested in Section IV. We also aim at performing more detailed evaluation of the defense node placement algorithms.

V.LITERATURE SURVEY [4]

DDOS MITIGATION CLOUD –BASED SERVICE:
Software as a service (SaaS), Platforms as a service (PaaS) and most recently Security as a service (SECaaS) has been offered due to the evolution of cloud computing over the past decade from a simple storage device to more complex devices. The work presented in this paper is a response to: (1) Devices such as firewalls or IPS/IDS, that cannot counter advance DDOS attacks are the main resource constraints in physical security; (2) The expensive cost, management complexity and the traffic is verified by the requirement of high amount of resources on existing DDOS mitigation tools. A new architecture of a cloud is proposed based on firewallingservice using resources offered by the Cloud and characterized by: dropped financial costing, increased availability, reliability, self-scaling and easy managing. In order to improve the efficiency of our proposal to face DDOS attacks, Network Function Virtualization technology (NFV) and other virtualization capabilities are used to deploy, configure and test our mitigation service . We alsodetail some result and point out future work.

Cloud-based solution:
In order to find the best architecture that guarantees the stability and efficiency of cloud based services, several research works dealt with that part by proposing algorithms and architectures in order to obtain the best results in terms of network performances and security levels. Yu et al. proposed an architecture that was developed essentially to counter DDOS attacks, it is based on a dynamic resource allocation mechanism that allocates extra resources from available cloud resources pool and new virtual machines will be cloned based in the image file of the original IPS. Using this exciting technology, when the volume of DDOS attacks packets decreases, the same mitigation system will reduce the number of cloned machines and release the extra resources back to the available cloud resources pool. Moreover, this paper demonstrates the utility of SECaaS for critical information infrastructure protection. Cloud-based technologies for security are being widely used in several areas, for example, Yassin et al. proposed a cloud-based framework based on Software as a Service (SaaS) model, that is able to locate malicious activities in the network and overcome the deficiency of classical intrusion detection. Another cloud-based solution was proposed in [15] to provide intrusion detection and forensics in mobile phones, and more specifically android smart phones.
Our work suggests an efficient Cloud-Based architecture that makes use of the flexibility and availability of the Cloud to come as reinforcements of traditional security infrastructures which enable to cope with massive unanticipated volumes of traffic. Thus, the subscriber faces DDOS attacks by an innovative DDOS mitigation service characterized by self scalability, high availability and dynamic resource provisioning using a novel firewalling Cloud-based approach.

In this work, we started from the idea of using large amounts of computing resources offered by Cloud Computing associated to parallel firewall techniques to design a cloud based security service model. This Cloud-Based Security service uses security virtual machines characterized by significant resources to deal with DDoS attacks. To achieve our goals, we proposed a complete architecture which consists of three main elements: Front-Gateway, Virtual firewall instances and Back-Gateway. The results obtained demonstrate service skills to deal with Flooding attacks and increase the analysis capacity by distributing traffic across multiple virtual firewalls. The results include the latency (RTT) and the packet loss rate in the network. However and as future work, we will treat the automation of network operations such as monitoring firewall instances, Load balancing and forwarding. We are also interested in the dynamic resource allocation focus on instantiate and delete virtual firewall instances "on demand" or "on need".

V. CONCLUSION

In this paper, we present a brief survey of the origin of DDoS attacks, and some methods which are developed for the detection and prevention of these DDOS attacks. The necessary factor in inhibiting a DoS attack is to enhance the reliability of global network infrastructure. We observed that most of the approaches deal with attack traffic detection and filtering near the target. DDoS attack is one of the major threats to both network service providers and legitimate customers.

New vulnerabilities to intrude systems are being continuously explored by the attackers. We noticed that most of the protocols are vulnerable and prone to DoS attacks. Therefore, we need to devise an effective and integrated solution in prevention of DDoS attacks by upgrading the hardware together with patching software vulnerabilities. We conclude that in spite of significant development in the area of detection, identification and prevention of DDoS attacks, yet the area is worth researching.

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

V. FUTURE SCOPE

Using such technology, we can detect Hackers.
System provides Honeypot system using this we can analyse Hackers. when this is on we will able to get Hackers' information. Proposed System checks attacks related with Bank transaction, which is very helpful.

REFERENCES

[1] 1,2Khan Zeb, 2Owais Baig, 2Muhammad Kamran Asif "DDoS Attacks and Countermeasures in Cyberspace"
[2] Nhu-Ngoc Dao1, Junho Park1, Minho Park2, and Sungrae Cho1 "A Feasible Method to combat against DDoS Attack in SDN Network"
[3] Manjiri Jog, MaitreyaNatu , SushamaShelke "Distributed Capabilities-based DDoS Defense"
[4] FouadGuenane∗, Michele Nogueira†, Ahmed Serhrouchni∗ "DDOS Mitigation Cloud-Based Service"
[5] S. C. . X. Wang, "Signing Me onto Your Accounts throughFacebook and Google: A Traffic-Guided Security Study ofCommercially Deployed Single-Sign-On Web Services," in Security and Privacy (SP), 2012 IEEE Symposium, 2012.
[6] "2013 State of Social Media Spam,"Nexgate, Tech. Rep., 2013. [Online]. Available: http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.Pdf
[7] S. Sezer, S. Scott-Hayward, P. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementation challenges for software-defined networks," IEEE Communications Magazine, vol. 51, no. 7, 2013.
[8] S. Shin and G. Gu, "Attacking Software-defined networks: a first feasibility study," in Proc. the second ACM SIGCOMM workshop on Hottopics in software defined networking, 2013.

DOI10.17148/IJARCCE.2017.63154