ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

A Literature Survey on Empirical Study of Network Security System through Dos Attack

Amar Kumar Yadav[1], V Uma Rani[2]

M.Tech Student, Dept. of Computer Network & Information Security, SIT, JNTU, Hyderabad, India[1]

Assoc. Professor, Dept. Computer Network & Information Security, SIT, JNTU, Hyderabad, India [2]

ABSTRACT:Computer network have become increasingly ubiquitous. The world has come to rely on these networks to provide transport for many different mission critical services. However , with the increase in networkedapplication ,there has also been an increase in difficult for network administrator to control what traffic traverses their network,manage and secure these networks from different attacks. Incomputernetworks, an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an Asset..when purpose of attack is only to learn and get some information from your system but the system resources are not altered or disabled in any way, we are dealing with a passive attack. Active attack occurs where the perpetrator accesses and either alters, disables or destroys your resources or data. There are different types of attacks among which a denial of service attack (Dos) is most common dangerous attacks on network. It is an active attack on networking structure to disable a server from servicing its clients. Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Failure of network security leads to major threat to various organization such as reputation loss,business loss,service interruption etc. In this paper, we discuss different types of Dos attack on computer network and the literature survey which we had done.

KEYWORDS:Computer Network ,Network Security,Dos Attack,Virtualization,GNS3,Firewall

I. INTRODUCTION

With rapid increase in the usage of computer networks for storing and sharing data, security breaches and attacks on computer networks has also increased at an alarming rate.Even attacks from outside has increased in the past few years.It also has been revealed by UK government,annual survey on cyber security not only the large organization but even the smal business has been badly targeted . Network security is the protection of network systems from the theft or damage to their hardware,software or information, as well as from disruption or misdirection of the services they provide It consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

Computer Network Security is becoming one of the most important issues in today's IT security world. The rapid growth of the commercialized Internet has opened up many securityvulnerabilities especially due to the fact that most of the major corporations now provide web services, which often create a large part of the companies' revenue. If these services are compromised or inaccessible, it could result major threat to various organization such as reputation,loss,business loss,service interruption etc . Nowadays, one of the most significant threat for computer network is Denial of Service attacks.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

A. DoS Attack

Denial of Service attacks (DoS) are aimed at exhausting resources of a target, in order to make the service inaccessible for legitimate users . These attacks could have many forms,but usually they send overwhelming amounts of invalid requests to the target. If there are multiple sources of attack, this is called Distributed Denial of Service attack (DDoS) . The strength of Dos and DDoS attacks is that these attacks are very easy to perform and could have significantly negative impacts upon the target. Recent growth of hacktivism, from groups such as Anonymous are commonly known to use Denial of Service attacks as a form of protest . Therefore motivations for executing DDoS attacks can vary. Nevertheless these attacks are becoming a very large problem, especially with the lack of simple and effective mitigation processes. The following are the common ways of DoS attacks .

- The denial of service by saturation is to submerge a terminal request, and to make sure that it's not able to meet the particular demands;
- The denial of service by vulnerability exploitation that is exploiting a flaw of the remote system to render it unusable.

B. Types Of DoS Attacks

The first DOS attack occurred on November 2, 1988.This attack was self propagating & self replicating and as a result 15% of systems connected to network was stopped running and were infected. There are several kinds of DOS attacks which is generally divided into 3 categories.

- **Volume Based Attacks:** Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attacks goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).
- **Protocol Attacks:** Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps).
- **Application Layer Attacks:** This This includes attacks that concentrate on operating system vulnerability. It Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Comprised of request that seem right ,the target of those attacks is to breakdown the online server. The magnitude of this attack is measured in Requests per second (Rps).

C. Symptom Of DoS Attacks

Not Not all disruptions to service are the result of a denial-of-service attack. There may be technical problems with a particular network, or system administrators may be performing maintenance. However, the following symptoms *could* indicate a DoS or DDoS attack:

- Unusually slow network performance (Opening files or Accessing websites)
- Unavailability of a particular services.
- Inability to access any websites.
- Dramatic increase in the amount of Spam you receive in your account.

D. Protection

Unfortunately ,there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

- Install and maintain anti-virus software

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

- Install a firewalls, and configure it to restrict traffic coming into and leaving your Network.
- Follow good security practices for distributing your email address. Applying email filters may help you manage unwanted traffic.

II. LITERATURE REVIEW

Arianit Maraj , Genc Jakupll, Ermir Rogova, Xheladin Grajqevci [2017] have describe about the potential damage from DOS attacks and analyze the ramifications of the damage [1]. Author has use same penetration testing approach that are used by malicious attacker in order to test network security. The only difference is authorization. They have analyze different firewalls and other protective systems and they role in overall security during these attacks. For testing network systems, They have simulate DoS (Denial of Service) attacks on network with different topology
Dos attack can be avoided by implementing appropriate systems for protection against these attacks. One of the alternatives is using next generation firewalls, which are capable in neutralizing such attacks, but not in the case when attacker has more bandwidth than the bandwidth that the victim utilize. In order to avoid such an attack, there is a need to continuously monitor the network and identify such attacks (lP address of the attacker). In addition, since it is very easy to interrupt services from the internal network, there is a paramount need to protect the servers with the next generation firewalls.

Tomar Kuldeep and Tyagi S.S [2014] have introduced the computer network and importance of computer network. Different type of network attacks like passive attack,insider attacks, distributed attacks ,active attacks ,close in attacks are explained briefly [2]. It have also highlighted some popular dos attack like ICMP flood attacks,teardrop attacks,SYN-flood attacks,Land attacks,Surf attacks ,Distributed Dos attacks. writer have discussed few protective mechanism against these Dos attacks. According to writer by proper configuration of Firewall,IDS/IPS ,ISP edge Router we can control the effect of Dos attacks.
This paper also simulate the dos attack using GNS3 .ICMP-flood attacks was simulated and the result was observed.The simulation results show that policy inspection success rate becomes very high and packets were dropped and even reached to maximum level.According to writer there are many mechanisms available to counter these types of attacks but for small organization or small networks it is very hard to implement ,configure or purchase mechanisms.

Shamma Al Kaabi,Nouf Al Kindi,Shaikha Fazari and Zouheir Trabelsi [2016] have proposed an ethical educational platform, called DoS_VLab, that aims at allowing students experience common denial of service (DoS) atacks, in secure academic environment [3]. DoS_VLab platform is based on virtualization technologies and GNS3 network simulator for building virtual networks. Compared to traditional physical laboratories, practices show that the DoS_Vlab platform helped produce more lab practices within the students,reduced taining hours required for implementing hands-on lab exercises, and resulted in higher completion rate of the hands-on lab exercises.
This paper give brief introduction about virtualizatiion environment and GNS3 simulator.They have also mention the benefits of using virtual technologies for information security education.The entire process of using virtual lab is described in paper.The writer have created virtual lab and hac simulated dos attack like ARP Cache Poisoining Attacks,TCP SYN flood attacks,Land Attack etc.Virtual lab platform provides students with a secure virtual laboratory environment, and experimental experiences on common DoS attacks. In addition, DoS_VLab platform reflects the real network environment, and meets the requirements of information security courses.

Majed Tabash and Tawfiq Barhoom [2014] have Proposed an approach merging methods from data mining to detect and prevent DoS attacks, by using multi classification techniques to achieve a sufficient level of accuracy and reduce false alert alarm.They have also evaluate their approach in comparison with other existing approaches [4].The work was based on European Gaxa Hospital (EGH) Datased to detect Dos attacks.
The proposed system involved the following steps for detecting and preventing Dos attacks: data acquisition,Dos identification labeling,preprocessing,processing stage and finally evaluation of the approach ,in addition to a defene mechanism by PfSense firewall and snort tool.Ther writer claims that their approach achieved the best classification accuracy for detecting Dos attacks and preventing Dos attacks by defense mechanism(snort tool on PfSense firewall).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

Awatef Balobaid , Wedad Alawad and Hanan Aljasim [2016] have describe the impacts of several types of Dos/Ddos attacks in the cloud and the procedures that they use to affect the services availability has been studied [5].Several mitigation techniques are also discussed in this paper.To study the impacts of Dos/Ddos attack simulation work has been done.During simulation the writer has observed the effectiveness of software based firewall and hardware based firewall.
Open source tools has been used to simulate dos attack and openstack as platform for cloud environment.Kali linux is used as attacker system.Different network monitoring tools (bmon,IPTraf,Wireshark) are used to monitor the network traffic.Iptables and firewall are used as mitigation tools.
According to writer single security device is not capable of mitigation Dos or Ddos attacks,which means other defense techniques are required to protect the full cloud structure including servers,network devices ,application etc.

Kemal Hajdarevic,Adna Kozic and Zerina Masetic [2017]have describes a simulation-based training scenario using simulator and by using hacking tools in which student trainees experiences the symptoms and effects of a Ddos attack,practice their response in a simulated environment with goal to prepare them for the real attacks [6].
GNS3 is a network software emulator first released in 2008. It allows the combination of virtual and real devices, used to simulate complex networks. Author have used GNS3 to create differnt topology and simulate the attack using automated scripts or tools such as Net Tools5 or specially designed operating systems such as Kali Linux which are used for ethical hacking purpose.Routers like cisco 3725 and 7200 series are used to simulate the attacks.Efficiency of firewall is checked during the attack.
This implementation and findings indicates the need to develop scenario similar to those presented here with goal to educate large number of future newtwork administrator who may not have enough experience,tools such as intrusion detection and prevention systems but whor are still expected to proactively monitor and defend computer networks for which they are responsible.

III.CONCLUSION

The different aspects and the theortical study on the different way of Denial of Service attack,Its impacts on network performance and mitigation techniques have been studied, analyzed and presented in this paper. We have also presented the differnet technique and advantage of using virtual labarotary for security testing.

IV.ACKNOWLEDGEMENT

I would like to express my gratitude to Ms. V. Uma Rani for her Encouragement and guidance. We are also thankful to the faculty member of School Of Informatiion Technology for their valuable suggestion .

REFERENCES

1. Arianit Maraj,Genc Jakupi,Ermir Rogova and Xheladin Grajqevic ,"Testing of network Security Through Dos Attacks", Mediterranean Conference on Embedded Computing (MECO),Bar, Montenegro , pp. 1-6, June 11-15 , 2017
2. Tomar Kuldeep and Tyagi S.S , "Enhancing Netwok Security by Impleting Preventive Mechanism using GNS3", International Conference on Reliability,Optimization and Information Technology, Faridabad, India ,pp. 300-305, February 6-8 , 2014
3. shamma Al Kaabi,Nouf Al KINdi,Shaikha Al Fazari and Zouheir Trabelsi,"Virtualization based Ethical Educational Platform for Hands-on Lab Activities on Dos Attacks", IEEE Global EngineeringEducation Conference(EDUCON), Abu Dhabi, United Arab Emirates, pp.273-280, April 10-13, 2016
4. Majed Tabash and Tawfiq Barhoom,"An Approach for Detecting and Preventing DoS Attacks in LAN,"International Journal of Computer Trends and Technology(IJCTT)-Vol. 18 ,pp. 265-271, 2014
5. Awatef Balobaid,Wedad Alawad and Hanan Aljasim,"A Study on the Impacts of DoS and DdoS Attacks on Cloud and Mitigation Techniques,2016 International Conferenceon Computing, Analytics and Security Trends (CAST), Pune, India , pp. 416-421,Dec. 19-21, 2016
6. Kemal Hajdarevic,Adna Kozic and Indira Avdgic,"Training Network Managers in Ethical Hacking Techniques to Manage Resource Starvation Attacks using GNS3 Simulator", International Conference on Information, Communication and Automation Technologies (ICAT) , Sarajevo, Bosnia-Herzegovina , pp. 1-6 , Oct 26-28,2017
7. Gaurav Kumar,Eman Adelfattah,Johnathon holbrooks and Alexander Perez,"Analyzing the effect of Dos attacks on network Performance" , International Conference on Communication, Computing and Digital Systems (C-CODE), pp.372-376, Oct.19-21, 2017
8. N. Muraleedharan and B. Janet ,"Behaviour Analysis of HTTP Based Slow Denial of Service Attack",IEEE WiSPNET conference, Chennai, India pp. 1852-1856, March 22-24, 2017