Journal of Advances in Science and Technology

Vol. VI, Issue No. XII, February-2014, ISSN 2230-9659

REVIEW ARTICLE

DETECTION AND MITIGATION OF DENIAL OF SERVICE (DOS) ATTACKS IN COMPUTER NETWORKS

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

Journal of Advances in Science and Technology
Vol. VI, Issue No. XII, February-2014, ISSN 2230-9659

Detection and Mitigation of Denial of Service (DoS) Attacks in Computer Networks

Bhawna Sharma[1] S. K. Sharma[2]

[1]Asst. Professor, Dept. of Computer Science, DAV College, Yamunanagar - 135 001,

E-Mail: bhawnasharma@live.com

[2]Associate Professor, Dept. of Statistics, GNK College, Yamunanagar

----------♦----------

INTRODUCTION

The basic idea behind DoS attacks is to force a large number of individual systems connected to the Internet, to send bulk traffic to the same destination at the same time. The aggregated traffic that those systems produce can easily cripple the available network or system resources of the recipient. Thus the recipient, the victim, of this attack will no longer be able to have reliable network access or serve legitimate clients, if the victim is a network server. Mostly two methods are used for lunching DoS attacks. One of these methods is known as flooding, other is implementing a malware that can change system configuration causing DoS attacks. Next subsections describe both of these in detail.

FLOODING

The most straightforward method is sending a stream of packets to the victim to use all of the systems resources . Victim can be a single PC, Web server or proxy connected to the Internet. The strength of an attack lies in the volume rather than the contents of the attack traffic.

The attack traffic can be similar to the legitimate traffic that causes difficulty in defense.

MALWARE

Malware is software used by a hacker designed to gain access, not purposefully permitted by a user, to a computer and instruct the computer to perform a task for the hacker. Various types of Malware are Trojans, spyware, adware, key loggers, dialers, root kits, botnets, crimeware, badware, viruses and worms. The purposes for writing malware include financial gain, espionage, revenge, anger, and recognition or just to see how fast it might spread. These attacks exploits security hole of the software such as operating system and web server bugs, then causes system crash or degrade in the performance.

RELATED WORK

Arguably, a researcher can mark the beginnings of Denial of Service Attacks by carefully choosing their history. The more modern, technology-oriented, among us could argue that it occurred after the First World War when Germany tried jamming Russian wireless transmitters. The real difficulty in reducing DoS effect is multiple techniques involve in such attacks. Attacker takes advantage of the holes in the application. After the failure they have plenty of optional techniques to carry on. Researchers introduce a framework for classifying DoS attack based on header contents, ramp-up behaviors and novel techniques based on spectral analysis. With this they agree on when large attacks occurs like root server attack additional-detection sites would provide more insight when projecting the prevalence of DoS activity on the internet.

Sailesh Kumar evaluates a no. of current NIDS system and algorithms they employ to detect and combat security threats, both technical and economical perspectives. Finally giving the idea that more distributed version of NIDS mechanisms need to be standardized.

Review analysis of DoS/DDoS attacks & list of basic network attack prevention techniques & their comparison are elucidated these types of high performance platforms will become as common place as firewall and routers to provide much needed counter-DoS techniques and will be of major benefits overall within the security parameters.

After realizing the power of DoS attacks Bryan gatenby suggested action in the encouragement of overall internet Security, implementation of a detection mechanism & firewall, rate limiting and

resource multiplication policy and agreement with IPS concerning malicious traffic. Hacker can use different ways for executing attacks successfully. Author explores the effectiveness of machine learning techniques in developing automatic defense against DDOS attacks based on artificial neural networks. But concludes that this technique can be extended to use multiple algorithms.

A look at the above literature spark the fact the there is a still some unfolded challenges that still needs to be addressed. Following sections discuss the existing challenges & their counter measures in details.

CHALLENGES

Internet development provides a golden way to share information & resources but unfortunately its security becomes the biggest challenge for secure working. According to ("Denial-of-service attack", 2007) Dos Attack can result in:

1. Consumption of computational resources, such as bandwidth, disk space, or CPU time;
2. Disruption of configuration information, such as routing information;
3. Disruption of physical network components.
4. Damages physical network components.

Malware intended to:

1. Trigger error in the micro code of the machine.
2. Trigger error in the sequencing of instruction.
3. Exploit error in the operating system to cause resource starvation and thrashing.
4. Crash the Operating System itself.

There is no particular answer to the question that why these kinds of attacks are initiated? What is the real motive behind these attacks?

It is the mind stance of hacker for

1. Just having fun
2. Extortion
3. Online gaming
4. Hacktivism.

A botnet owner was hacked by a businessman to take down the website of his competitors causing them to loss more than $1million [leyden.2005]. Due to IP Spoofing, Nil Security between Victim & hacker, No distributed defense System, hiding details of attack by the company owners for their Goodwill are some reasons why these attacks are so powerful. It is difficult to eliminate the effect of attack completely but it is very crucial to mitigate the risk by applying multi-pronged approach. Design your business for survivability, Design your network for survivability, be a good netizen (net citizen). Security of your system also depends on the security measures applied by other computers in your network.

There is No universal solution to this problem but something can be done to minimize the possibility of launching DoS attacks, some of them are describe in net few sub sections:

COUNTER MEASURE

As the frequency of the Dos attack is concern it is very difficult to eradicate the effect of attack completely. However mitigation is possible by executing Avoid-Detect-Prevent cycle, which is described in subsequent subsection below:

AVOID

Avoidance is a crucial phase of any defense system. Yet it is not taken seriously by some sites in the beginning and prompted after experience. Attack can be handled only after knowing its technical aspects such as network design, agreements with your ISP, putting detection mechanism and response plan in place and perhaps taking out an insurance policy.

General Principal that apply to the DoS defense system are-Differentiate critical services with non-critical once, Identify and understand the inter-dependences of various service providers on your network. System and network must go for absorbing the attack, degrade services or shut down all service till the attack last.

It is important to have discussion phase during and after the attack within organization (Technical staff, service management) and outside organization (ISP, law enforcement, media & other). The important concepts related to Avoidance of these attacks are:-

Design network or system for survivability*: It* means separate critical services if possible, over provision as much as possible & minimizes your target-cross-section.

Monitoring*:* system and network performance matrices, network protocol mix, n/w traffic flows are some characteristics that form the definition for a normal system

behavior. Before planning monitoring aspects one should pay attention to the mostly targeted resources during the attack. Monitoring can be performed at two levels 1 network level (throughput monitoring, device performance metrics) 2. Host level monitoring

(gathering performance static, network behavior). To avoid bottleneck pay attention while implementing remote monitoring capabilities. Some non-technical steps to reduce DOS risk are: cultivate analysis capabilities, create an incident response plane, and develop an ongoing relationship with your service providers. Placing firewalls prevents unauthorized access to private networks by analyzing packet entering the network and blocking those, which do not satisfy security criteria.

DETECT

Today networks are extremely heterogeneous. An effective detection system is needed to prevent or respond any DOS attacks in real time. Why we need detection system? First, after detecting an attack before the actual damage occurs, the target has more time to implement attack reaction techniques to protect legitimate users. Second, it helps to identify the attackers so that legal actions can be taken. Third, if attacks can be detected close to attack sources, attack traffic can be filtered before it wastes any network bandwidth .Requirements of good Detection system are:

1. Multiple detection Mechanism
2. Attack coverage
3. Granularity of attack detection
4. Consolidation of alarms
5. Response action. .

A good detection technique should have a short detection time and low false positive rate. There are various types of detection mechanism

1. Anomaly detection.
2. Signature/Pattern based detection.
3. DOS-attack-specific Detection.

Signature Based Detection is simply looking for the signatures of known attacks in order to detect the attack. A database of signatures is built by hand a priori . *This* technique is used by Snort . Snort has one main disadvantage; new attacks that do not have well-defined signatures may go undetected until the signature is defined.

Anomaly Based detection cope the current traffic with the base line, set of preprogrammed threshold . This includes statistical approaches like a Chi-Square-Test on the entropy values of the packet headers , covariance analysis , clustering and feature space modeling . Different techniques taken from pattern analysis and machine learning such as Wavelets, Markov Models, Genetic Algorithms, Artificial Neural Networks (ANN) and Bayesian Learning have also been applied. Because of the irregular traffic in the network cause static threshold to fail. That's why threshold are to change timely.

DOS-ATTACK-SPECIFIC DETECTION.

It is based on the special features of DoS attack. Generally, DoS attack traffic is created at an attacker's will. First, attackers want to send as much traffic as possible to make an attack powerful. Hence, attack traffic does not observe any traffic control protocols, such as TCP flow control. In addition, there will be a flow rate imbalance between the source and the victim if the victim is unable to reply to all packets. Second, attack traffic is created in a random pattern to make an attack anonymous. Third, for each known attack, attack traffic at the target is highly correlated with abnormal traffic behavior at the attack sources.

Many techniques have been proposed to detect an ongoing DoS attack. Cisco routers provide support for attack detection via RMON and Netflow data that can be processed offline to detect an attack. Multops exploits the correlation of incoming and outgoing packet rates at different level of subnet prefix aggregation to identify attacks. Wang provides a rigorous statistical model to detect abrupt changes in the number of TCP SYN packets as compared to the TCP SYN ACK packets.

Bro, an intrusion detection system uses change in (statistical) normal behavior of applications and protocols to detect attacks while Cheng use spectral analysis to detect high volume DoS attack due to change in periodicities in the aggregate traffic. All the above techniques are based on anomaly-detection which is faster than static Signature-scan technique on the basis of ramp-up & spectral analysis to build upon existing approach of header analysis that's track no. of source connection to a single destination

CONCLUSION

The most fundamental lesson to be learned from distributed denial of service is the fact that all sites on the Internet are interdependent, whether they know it or not. The impact upon your site and its operations is dictated by the security of other sites and the ability of a remote attacker to implant the tools and, subsequently, to control and direct multiple systems worldwide to launch an attack.

Attackers typically exploit well-known vulnerabilities, many of which have readily available fixes. Complicating matters are the intrusion tools that are widely available. Intruders have automated the

processes for discovering vulnerable sites, compromising them, installing daemons, and concealing the intrusion. Even security-conscious sites can suffer a denial of service because attackers can control other, more vulnerable computer systems and use them against the more secure site. Thus, although you may be able to "harden" your own systems to help prevent having them used as part of a distributed attack, currently available technology does not enable you to avoid becoming a victim. There is some hope for the future in technological and other approaches. Handling denial of service is essentially an exercise in risk management. There are sometimes technical solutions to management problems. There are always management solutions to technical problems. We encourage readers to look at denial of service from both points of view.

REFERENCE

[1.] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communications Review*, Volume 34, Number 2, April 2004, pp. 39-53

[2] G. Koutepas, F. Stamatelopoulos, and B. Maglaris, "Efficiency and Performance Issues in Distributed Intrusion Detection Systems", Applied Telecommunication Symposium 2002 (ATS 02), San Diego, CA, USA, April 2002

[3]" DoS attack Techniques" june22, 2005

[4] *Y. Xie and S.-Z. Yu, "A novel model for detecting application layer ddos attacks," in Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums on. IEEE Press, 2006, pp. 56–63.*

[5] "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems" *ACM Transactions on Computational Logic, Vol. 2, No. 3, 09 2006, Pages 1{0??.*

[6] M. V. Mahoney and P. K. Chan, "Learning no stationary models of normal network traffic for detecting novel attacks," in *KDD '02 Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*. New York, NY, USA: ACM Press, 2002, pp. 376–385.

[7] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to ddos attack detection and response," in *DARPA Information Survivability Conference and Exposition, 2003. Proceedings*, vol. 1. IEEE Press, 2003, pp. 303–314.

[8] S. Jin and D. Yeung, "A covariance analysis model for ddos attack detection," in *Communications, 2004 IEEE International Conference on*, vol. 4. IEEE Press, 2004, pp. 1882–1886.

[9] S.-Y. Jin and D. Yeung, "Ddos detection based on feature space modeling," in *Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on*, vol. 7. IEEE Press, 2004, pp. 4210–4215.

[10] T. Shon, Y. Kim, C. Lee, and J. Moon, "A machine learning framework for network anomaly detection using svm and ga," in Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. Proceedings from the Sixth Annual IEEE. IEEE Press, 2005, pp. 176–183.

[11] D. Gavrilis and E. Dermatas, "Real-time detection of distributed denialof- service attacks using rbf networks and statistical features," Comput. Netw. ISDN Syst., vol. 48, no. 2, pp. 235–245, 205.