ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (332-334), Month: April - June 2015, Available at: www.researchpublish.com

Threat of Cyber Attack and Network Security DoS Attack Analysis and New Preventing Method

[1]Takamasa Nakayama, [2]Tarik Eltaeib

[1, 2] Department of Computer Science, University of Bridgeport, Bridgeport, USA

***Abstract*: Lately, network security is considered to be one of the most critical issues for both companies and private persons. Sony Pictures Entertainment hack which first happened on November 24, 2014 is still fresh in our memories. The hackers stole the data of Sony Pictures employees, which included their personal information, such as family structures, e-mails, information about salaries and copies of unreleased films. Data protection is already reached status of our lifeline, and get to know about the criminal technique will reduce risk of exposing our life to danger. This paper is focusing on DoS attack, which is mainly aiming for paralyzing the function of web sites and its alteration. It is also one of the most common techniques for cyber attacking. This paper attempts to analyze the variety of DoS attacks and its countermeasures.**

***Keywords:* DoS attacks; TCP SYN flooding attack.**

I. INTRODUCTION

While refer to them all as cyber attack, there are a large variety of techniques of attacks. CSI/FBI 2010-2011 Computer Crime and Security Survey [1] categorizing data in types of attacks experienced by percent of respondents. In the table of attack types, Malware infection is placed number one and the percentage (67%) overwhelms other type of attacks. Being fraudulently represented as sender of phishing messages (39%) is placed number two, and Laptop or mobile hardware theft or loss (34%), Bots/ zombies within the organization (29%), Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.) (25%) follows after (Column of 2010). DoS attack, which is well known as one of the major cyber attacks, has 17% in the table and the percentage is slowly decreasing from 2005.

Apparently, this table expresses there is not much thread against cyber attack because the most of issues with high percentage are relating to insiders of enterprises except malware. However, consider of the amount of losses once getting damage, we cannot ignore the thread of rest of the cyber attacks. Incidentally, although the report expresses percentage of DoS attack decreasing, it is jumping up to 29% in 2009. This result also represents the thread of cyber attack is not able to predict.

There are two common types of attacks in DoS attack. One is Bandwidth attack, which refers attacks to network itself and it gives big impact on network traffic. Another common way, Connectivity attack, refers attacks to server operating systems by sending enormous unnecessary connection requests. It makes available resources in the server exhausted and legitimate users' request will be ignored.

More specifically, it is possible to categorize major DoS attack into 8 categories. F5 attack, TCP-SYN flood, UDP flood, ICMP flood, SMURF attack, Connection flood, DDoS attack, and DRDoS attack.

F5 attack is the easiest way of participating DoS attacks. Usually Web browser assigns F5 key as a reload function. So simply consecutive hit of F5 key turns into DoS attack. But some server has countermeasures against the reload access that F5 key only retrieve data from cache memory in closest access point. TCP-SYN flood is a technique sending enormous SYN packets that is connection requirements in very limited time. Usually host server has to send back SYN/ACK packet to the sender when they get SYN packet from sender and sender returns ACK packet so connection is established. TCP-SYN attack ignores the sending back process. The host eventually gets out of available resources and exhausted. UDP flood refers keep sending huge packet or enormous small packets to UDP port and place stress on targeted network bandwidth or network devices. Since UDP is a connectionless protocol, it is easy to disguise its source address for senders. ICMP flood makes targeted system resource or bandwidth saturated with enormous ICMP Echo Requests and as same as UDP flood, ICMP flood is a connectionless protocol, so easy to hide their source address for malicious senders. SMURF attack sends ICMP echo requests from disguised souse address for saturating bandwidth of host server. Connection flood attack is a technique keeping connection one after the other with TCP port in targeted host and occupy the available sockets. DDoS attack is advanced form of DoS attack using outsider's machines as a step-stone and sends massive packets to a target from those multiple machines. DDoS attack is much harder to fully defense than DoS and the users of those "step-stones" are mostly just people who are nothing relating to the attack. Finally, DRDoS attack is a transformation of DDoS attack, which does not require sneaking into outsider's hosts and just using them as a relay station. As listed above, DoS attack has many variations and some of them are still hard to fully defense.

II. RELATED WORKS

Z.Chao-yang [2] is analyzing various DoS attacks and proposing three effective ways for defending attacks. One is using a router. When packet arrives to router, router usually takes out its destination address and compares the information with its routing table. Unicast RPF is a technique applies its process. Unicast RPF checks not destination address but its source address. If the source address exists on routing table, it sends the packet to its destination. If it does not exist, it discards the packet. Technically, once router is connected to network, the network is registered as routing information in the router. So all source address suppose to be on the routing table. However, PC being infected with a virus often sends a packet which source address is disguised as different address. So Unicast RPF is one of the effective ways for preventing DoS attack. Another way of preventing DoS attack is to use TCP intercept function. TCP intercept function can reduce the thread of TCP SYN flooding attack by monitoring illicit TCP SYN packets. TCP intercept has two modes, intercept mode and watch mode. Intercept mode intercepts TCP SYN from client at router. Router sends back SYN ACK to the client and checks if it is possible to have connection with the client. If client does not reply back ACK to router, it means the TCP SYN is illicit, so router practically protects server from DoS attack. Intercept mode place a lot of stress on the router, and also it has some restrictions. For example, intercept mode disturbs negotiation between client and server. So it is impossible to negotiate about MSS, for example, if you use intercept mode. Watch mode is more moderate mode compare to intercept mode. Router basically just monitor TCP SYN from clients and it reaches to server directly. Watch mode monitors if the client sends back ACK or not more strictly and if it doesn't, router sends RST to server and close the connection. Third way for preventing DoS attack is to crease the Trusted Platform Module. TPM chip can be used to restrict user access when an abnormality is detected in network. Normally, the network data is transferred through several switches before reaching to servers. If those switches have a TPM chips inside, it can detects DoS attacks before the attacks reaches to server. Same time TPM authentication allows only clients with permission to visit the server under the abnormal circumstance. It is very effective way for preventing DoS attacks, however, it restricts clients who can access to the site. So it is hard to utilize the method for a popular site that receives a lot of access.

III. DETECTION

W.Liu [3] summarizes the signs of DoS attack very well. If an enormous number of data packets suddenly appear and network traffic grows rapidly, plus server run with overload and the performance decreased, it can be sign of the attack. Also if the length of data is much more than the usual average, there is a possibility of attack. Lastly, if the packets being sent are not the part of network service connections and the destination port is not normal port, there is a thread of attack. These are just logic and does not indicate its countermeasure, so the author experimented with WinPcap, a tool to capture and send the network packet flexibly, to see actual SYN flood attack and its detection. From the paper, it is possible to see the program successfully detecting DoS attacks.

M.Agarwal et al.[4] focused on proposing de-authentication DoS attack detection methodology. Their experiment proofed increase threshold actually makes the accuracy of detection increases but the detection rate falls. Conversely, if the value of threshold is low, it easily detects de-authentication DoS attack, but it contains some small amounts of false positives.

IV. CONCLUSION

In this paper, the variety of DoS attack methods are analyzed and some popular techniques for preventing DoS attacks are also presented. From viewing experiments result from other papers, it is possible to say that DoS attack is detectable by regulating the level of filter, but the rate of detection never able to be 100% in our technology yet. It is important to constantly regulate the level of attack detection and simultaneously combine multiple programs and protect server.

REFERENCES

[1] Computer Security Institute, 15th Annual 2010/2011 COMPUTER CRIME AND SECURITY SURVEY<http:// gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2010.pdf>

[2] Z.Chao-yang, DOS attack analysis and study of new measures to prevent, Intelligence Science and Information Engineering (ISIE), 2011 International Conference on 20-21 Aug. 2011

[3] W.Liu, Research on DoS Attack and Detection Programming, Intelligent Information Technology Application, 2009. IITA 2009. Third International Symposium on 21-22 Nov. 2009

[4] M.Agarwal, S.Biswas, and S.Nandi, Detection of De-authentication Denial of Service attack in 802.11 networks, India Conference (INDICON), 2013 Annual IEEE, 13-15 Dec. 2013