Analysis of Blended-mode DoS Attack

Xin-Yang Ou, Hua Zhang

State Key Laboratory of networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

Keywords: DoS attack, Blended-mode

Abstract. Most techniques of DoS attack are single-model, which have the disadvantages of low attack efficiency and weak adaptability. This paper presents a blended-mode DoS attack mode and we focus on the analysis of the efficiency of this mode. In this mode, we combine different DoS attack modes to attack the target at the same time for increasing theefficiency. In this paper, through some experiments we verify the high efficiency of this mode.

Introduction

DoS attack technology has been developing rapidly in recent years and it has been recognized as one of the most serious security threats to the network. DoS attack is in which an attacker trying to make the target server stop providing services. It exists in many areas and has many attacking modes such as Anti_DoS[1], 802.11 Network DoS[2], Mobile ad-hoc DoS[3] and VANET DoS[4]. The attacker can make two effects to the server by launching DoS attack. One is to force the server run out of its resources. Another is to use IP spoofing technology to force the server reset the connection to the legitimate users. The DDoS comes into being based on DoS, but its essence remains the DoS attack. So in this paper we regard it as DoS too.

DoS attack tools widespread on the Internet such as Slowloris[5], HPing[6], etc. By analyzing these attack tools, we find that most of them are single-mode DoS attack. HPing launch the DoS attack by constantly sending “ping” command and Slowloris by attacking the ARP and DNS protocols. So most of the DoS attack tools have their own limitations.

Every year, the information publishing platform CVE(Common Vulnerabilities and Exposures)[7] will release a lot of information about the DoS vulnerability. However, the information is mostly related to single-mode DoS attacks and it is not complicated to prevent or mitigate it.

This paper focuses on the blended-mode DoS attack. We analyze the characteristics of various modes, and ultimately select three most common and representative DoS attack modes. They are SYN-DoS mode attack, TCP-DoS mode attack and HTTP-DoS mode attack. The former two launch DoS attack by exhausting the server’s system resources, and the last one by exhausting the server’s application resource. Through analysis, we find that we can enhance the attack efficiency by combining these three attack modes. We simulate our idea by setting up a virtual network environment and analyze the result. The experiment shows that for the three attack modes we selected, none of them can get high attack efficiency because there are already many measures[8] to prevent of mitigate it. But when we combine them together to launch blended-mode DoS attack, it can greatly increase the efficiency.

In the second part of this paper, we will introduce the basic principles of these three attack modes, and then propose a blended-mode DoS attack by combing them together. In the third part, we design and implement a DoS attack system based on the blended-mode DoS attack. In the fourth part, we make some experiments to test the system, and verify the high efficiency of blended-mode DoS attack through the results got from the experiments. In the end of this paper, we make a summary about our work and list some following work we need to do.

Theory

The fundamentals of SYN-DoS[9] mode、TCP-DoS[10] mode and HTTP-DoS[11] mode are shown as follows：

- SYN-DoS mode

SYN-DoS mode attack is one of the most common attacks. It utilizes the TCP protocol. During TCP connection establishment process, it need to connect the two sides by completing the three-way handshake. Only when the three-way handshake is successfully completed before it establishes a TCP connection. In the process of the three-way handshake, the server needs to keep all the unfinished handshake information and stay at a status(called half-open link) where the server receives the TCP-SYN and transmits the SYN-ACK, but the third handshake ACK is not received, until the three-way handshake is completed or timeout. If an attacker constantly sends a connection request to the target server but do not complete the three-way handshake, the server may have to keep so much half-open links so that it can no longer accept any connection request.

- TCP-DoS mode

In the TCP connection, the operating system's kernel need to maintenance messages of each TCP connection. But if the connections are too many, it will take up a lot of memory and CPU time. Through numerous TCP connections to make the target server resource exhaust, this kind of attack is called TCP-DoS mode attack. In general, just utilize a program like Telnet can exhaust a low-security server’s TCP connection resources. Differ from the SYN-DoS mode, TCP-DoS mode does not need to keep sending connection request to the victim server. It only needs to send enough connection requests and when the number of requests reach to a certain amount, the attack can stop. But the victim server system is still not available. While in SYN-DoS mode, as long as the attack once stopped, the victim server system can be soon restored to normal.

- HTTP-DoS mode

HTTP-DoS mode is somewhat similar to TCP-DoS mode, it is the semantics of HTTP protocol for Web pages on legitimate request. What it differs from the ordinary TCP-DoS mode is that the latter occupy the connection resources only and it has only a few data transmission while HTTP-DoS mode constantly request data from the target server and it occupy both bandwidth resources and connection resources. In HTTP-DoS mode, the attackers keep requesting many different pages so that the server is busy in sending webs to attackers, which makes the server unable to provide services to other legitimate users.

By analyzing the characteristics of the three attack modes we find they can assist each other to consume server system resources from different aspects, and the server itself also takes a lot of CPU resources to be switched in response to different requests. So we can combine these three modes to form a blended-mode DoS attack.

Blended-mode DoS Attack System

The entire system contains many modules. It needs a global module to control the system running state and ensure that the system can launch the blended-mode DoS attack. Thus, we design a DoS attack system after the analysis above. The system frame is shown on Figure 1.

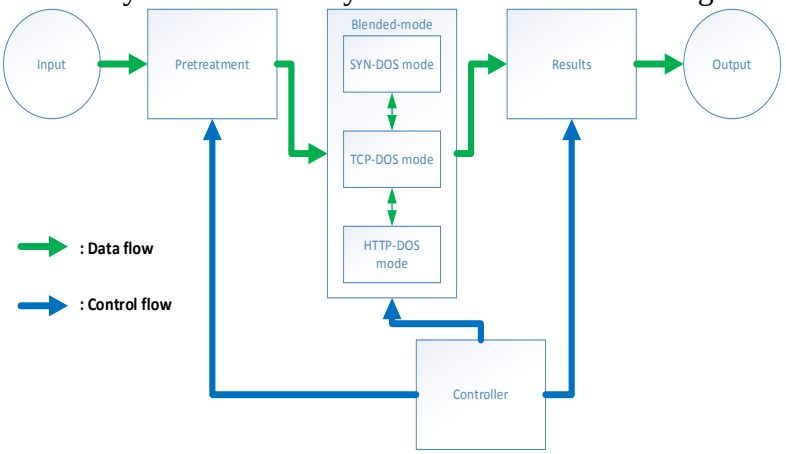

Figure1. System Frame

Next, we will introduce how the system works and how to implement it by Python language.

- Input and Pretreatment

The input data is IP address for the target server and some other auxiliary parameters. It is passed to the pre-processing program to check its validity at first. We make a regular match through Python's re module for the input IP. If IP match the format, we can continue to test if IP host is reachable by Python's urllib2 module. IP is valid if it can be reached. There is also a validity check for the auxiliary parameters. They are legal when they are among the parameters we defined.

- Blended-mode DoS Attack

Under the condition that the input data is legal, our system launch each single-mode DoS attack through opening multi-thread to fork a blended-mode DoS attack. We can utilize Python's thread module and threading module to implement this.

- Results and Output

The system generates and outputs the results when the attack finishes. The results involve whether the attack is successful of fail and the number of attacks each single-mode DoS attack has launched if the attack succeed.

- Controller

This is an independent module. It controls the operating procedures of the system. It also contains exception handling and overtime processing.

The most feature of the system is its attacking parallelism. In addition, the system is controlled by a independent controller.

Experiment and Analysis

In this section, we will do some experiments to test our system and analysis the results.

Attack Evaluation

Next, we will make a experiment for the blended-mode DoS attack system mentioned above and analyze the results. First, we set up a virtual network test environment as shown in Figure 2. We choose Apache as the Web server, and set it up in a Windows7 operating system. And for the client, we launch the blended-mode DoS attack by Python language under Windows7 operating system. The server and the client connect to the LAN via a router.

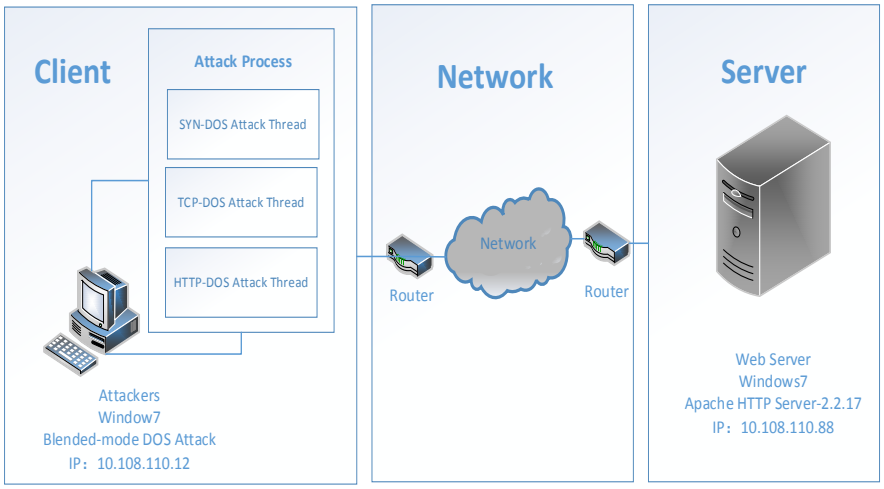

Figure2. Virtual Network Test Environment

We divide our test into the following two groups: single-mode DoS attack and blended-mode DoS attack. In order to compare the efficiency of the blended-mode DoS attack, we also have launched a slow-read mode DoS[12] attack and a reflective mode DoS[13] attack. We define success or failure of the attack as follows:

- Success(S):The server can't respond to the legitimate connection requests any more;
- Failure(F):The server can still respond to the legitimate connection requests;

We use the number of attacks to indicate the efficiency of an attack. Note that the number of attacks in blended-mode DoS attack is the sum of the number of attacks of all single-mode. The larger the number of attacks, the lower efficiency of the attack. The test results are shown in Table 1.

Table1. Test Results

Attack Mode				Attack Result	Attack Efficiency
	SYN-DoS	TCP-DoS	HTTP-DoS		
Single Mode	✓			F	—
		✓		S	800~900
			✓	S	900~1000
Blended Mode	✓	✓		S	200~300
		✓	✓	S	100~200
	✓		✓	S	200~300
	✓	✓	✓	S	100~150
Other Mode	Slow-read Mode DoS			S	600~800
	Reflective Mode DoS			S	300~400

By analyzing the test results, we find that among single-mode DoS attacks, SYN-DoS mode attack failed. The possible reason for this failure is, in an unmodified client TCP stack case, the attacking client system will automatically respond to the SYN-ACK sent by the server. It will release the corresponding half-open links on the server, which will reduce the attack efficiency. For other single-mode DoS attacks, although every of them can succeed but it has to launch a large number of attacks. While in a blended-mode DoS attack, every test is successful, and the number of attacks is far less than the number by a single-mode. When compared to the slow-read mode DoS attack and reflective mode DoS attack, blended-mode DoS attack also gets better results. The possible reason may be blended-mode DoS attack consumes server system resources from different aspects, and each single-mode it combines can assist each other. When the SYN-DoS mode attack is blocked, it contributes to launching TCP-DoS mode attack. When both the SYN-DoS mode and the TCP-DoS mode attacks are blocked, it's beneficial to the HTTP-DoS mode attack. These assistants are determined by the individual single-mode characteristics.

Detection and Mitigation Mechanisms

For the defense or mitigation of the DoS attack, we should think highly about the blended-mode. Considering the characteristics of the blended-mode, we put forward some measures. We can improve the ability of resistance of the server by using SYN cookie/cache or set a TCP agency to hide the server. We should close any module or service or port of the server that we don't need. We can also use the flow control and the filtering mechanism to protect the server.

Summary

After analyzing the existing DoS attacks we found most of them are single-mode, In order to increase the efficiency of DoS attack, we propose a blended-mode DoS attack, and verify the efficiency of our method through a experiment. The main principle of our method is to select three single-mode DoS attacks which can assist each other, put them together to form a blended-mode DoS attack. We proved that the blended-mode DoS attack is more efficient by doing some experiments in this paper.As security workers or technical people, we should think more about it when we consider the security of a system.

Acknowledgments

This work is supported by NSFC (Grant Nos. 61300181, 61202434), the Fundamental Research Funds for the Central Universities (Grant No. 2015RC23).

References

[1] Yan Feng. Capability analysis and improvement of JFKi anti-DoS. Information and Network Security (ICINS 2013), 2013 International Conference. 2013, pp. 1-5.

[2] Nagarjun P.M.D., Kumar V.A., Kumar C.A., Ravi A.. Simulation and analysis of RTS/CTS DoS attack variants in 802.11 networks. Pattern Recognition, Information and Mobile Engineering (PRIME), 2013 International Conference. 2013, pp. 258-263.

[3] Kanthe A.M., Simunic D., Djurek M.. Denial of service (DoS) attacks in green mobile ad-hoc networks. MIPRO, 2012 Proceedings of the 35th International Convention. 2012, pp. 675-680.

[4] Yeongkwun Kim, Injoo Kim, Shim C.Y.. A taxonomy for DoS attacks in VANET. Communications and Information Technologies (ISCIT), 2014 14th International Symposium. 2014, pp. 26-27.

[5] Duravkin, I., Loktionova, A., Carlsson, A.. Method of Slow-Attack Detection. Infocommunications Science and Technology, 2014 First International Scientific-Practical Conference. 2014, pp. 171-172.

[6] Padmashani, R., Sathyadevan, S., Dath, D.. BSnort IPS Better Snort Intrusion Detection/Prevention System. Intelligent Systems Design and Applications (ISDA), 2012 12th International Conference. 2012, pp. 46-51.

[7] http://cve.mitre.org/about/index.html

[8] Shichao Liu, Liu X.P., El Saddik A.. Denial-of-Service (dos) attacks on load frequency control in smart grids. Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES. 2013, pp. 1-6.

[9] Virgilio, M., Marchetto, G., Sisto, R.. Interest Flooding Attack Countermeasures Assessment on Content Centric Networking. Information Technology - New Generations (ITNG), 2015 12th International Conference. 2015, pp. 721-724.

[10] Wazid, M., Katal, A., Sachan, R.S., Goudar, R.H.. E-TCP for Efficient Performance of MANET under JF Delay Variance Attack. Information & Communication Technologies (ICT), 2013 IEEE Conference. 2013, pp. 145-150.

[11] Van der Toorn, O., Hofstede, R., Jonker, M., Sperotto, A.. A First Look at HTTP(S) Intrusion using NetFlow/IPFIX. Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium. 2015, pp. 862-865.

[12] Junhan Park, Iwai K., Tanaka H., Kurokawa T.. Analysis of Slow Read DoS attack. Information Theory and its Applications (ISITA), 2014 International Symposium. 2014, pp. 60-64.

[13] Zhang Chao-yang. DoS Attack Analysis and Study of New Measures to Prevent. Intelligence Science and Information Engineering (ISIE), 2011 International Conference. 2011, pp. 426-429.