Denial of Service Attack and Defense Experiment

Jin Minhao
Department of Computer Science and Software Engineering
Xi’an Jiaotong-Liverpool University
Suzhou China
Minhao.Jin17@student.xjtlu.edu.cn

I. INTRODUCTION

In recent years, the network security has continuously been a concerned topic with the rapid development of network technology and application. However, with the help of some DDoS (Distributed Denial of Service) tools, the DoS attack becomes one of the most popular intrusion methods which breaches the network security and often makes great economic losses and impact [1]. In this paper, one DoS attack method, UDP (User Datagram Protocol) flood will be introduced and a DoS attack experiment with using UDP flood will be designed and discussed.

II. MECHANISM OF UDP FLOOD ATTACK

UDP stands for User Datagram Protocol which is a connectionless protocol to process packets. In the model of OSI (Open System Interconnection), the UDP protocol is located at the transport layer. UDP flood comes under category of DDoS flood attacks [2]. A common method for attacking is to use a large number of UDP packets to impact DNS servers or Radius authentication servers, streaming media video servers. UDP flood of 100k bps often collapses the devices on the line, such as the firewall, causing the entire network segment to collapse. Since UDP is a connectionless protocol, an attacker can send a large number of small UDP packets with spoofed source IP addresses. Victim on receiving these packets, sends the acknowledgement to the source IP address. The victim device keeps waiting for the response if it does not get any feedback in turn. At last when victim gives up communication, almost all its resources will have been consumed and finally resulting in crash of the system. Also, as long as a UDP port is opened to provide related services, then attacks can be made against these related services.

III. EXPERIMENT STEPS

Two computers are needed in this experiment. One PC stands for the attacker and another one represents as the victim device.

Step 1: the victim looks up for its own IP address and tells the attacker. To check whether the connection between attacker and victim is available.

Step2: the victim enables a monitoring of UPD packets in the system service. CPU utility and memory utility of the victim start to be recorded.

Step3: the attacker runs UDP Flood program in Kali Linux. Choose the victim’ s IP address as the target. Set the maximum attacking time to 60 seconds, sending speed of UDP packets to maximum and the sending content to empty. Then the attacker starts the attacking experiment.

Step4: during the UDP flood attack, CPU utility and memory utility of the victim device should be recorded for future analysis.

Step5: Redo this experiment for more accurate measurements.

IV. WHY CHOOSING THIS TOPIC

Internet of things (IoT) are applied in various domains, however, they are vulnerable to DoS attack [3]. Thus, precautions should be applied on these nodes. Our group aims to record the effect of three DoS attack methods: SYN flood, TCP connect flood, and UDP flood. Moreover, after the data have been collected, defense methods will be designed and applied on the victim device in future study.

V. CONCLUSION

In conclusion, this paper mainly discussed the mechanism of UDP flood attack, a rough experimental process and the aim of choosing this topic. After the experiment is done, a more detailed analysis will be delivered in the assignment 2.

VI. REFERENCES

[1] W. Liu, "Research on DoS Attack and Detection Programming," *2009 Third International Symposium on Intelligent Information Technology Application*, Shanghai, 2009, pp. 207-210.

[2] A. Singh, D Junefa, "Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks", *IJEST*, vol. 2, no. 8, pp. 3405-3411, 2010.

[3] L. Liang, K. Zheng, Q. Sheng and X. Huang, "A Denial of Service Attack Method for an IoT System," *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*, Fuzhou, 2016, pp. 360-364.