Multi-nodes Traffic Replay Method based on IP-mapping

Zhixian Huang[1,a] ,Kaikun Dong[1,b], Hongri Liu[1,c] ,Bailing Wang[1,2,d], Guodong Xin[1,2,d] and Shujiang Xu[3,e]

[1]Harbin Institute of Technology, Haerbin 150000, China;

[2]Harbin University of Technology (Weihai) Innovation Pioneer Park Co., Ltd. Weihai, 264209, China;

[3]Qilu University of Technology (Shandong Academy of Science), Jinan, 250000, China.

[a]15036769597@163.com, [b]kaikun.dong@gmail.com, [c]lhr_5687@163.com, [d] wbl@hit.edu.cn, [e] xushj@sdas.org

Abstract. Traffic replay is a common method in traffic generation applied to the construction of network cyber ranges. At present, the implementation of replaying traffic within cyber ranges is one client one server or multi-nodes one-way communication, the effect is inferior. Therefore, this paper proposes a multi-nodes traffic replay method to solve high replay delay error during interactive replay in small scale. Based on this method, an IP-mapping method is designed to solve the problem of large file allocation in multiple machines. Experiments showed this method can support multi-nodes traffic replay, and replay delay error is significantly lower than Tcpreplay.

Keywords: cyber ranges, IP-mapping, traffic replay, traffic generation.

1. Introduction

The current network environment is faced with various threats. In order to study and deal with various security threats, an experimental platform capable of simulating a real network environment is needed, and the network cyber ranges is proposed. It is a relatively isolated, self-controllable network security experimental platform [1]. An indispensable element in a real network environment is the traffic. Therefore, nodes in this platform need to generate meaningful network traffic. Common methods for generating traffic include network protocol simulation, traffic generation based on traffic models [2], and traffic replay. Usually, the common network protocol is simulated on the application layer to implement the task of generating traffic. This method is applied to provide background traffic in a simple scenario; Existing traffic generation tools such as D-ITG [3], swing [4], Harpoon [5], which uses traffic models to generate traffic. Although it is not authentic enough, it`s suitable for stress testing of network devices. Traffic replay is a method of preprocessing the original traffic file into replay streams and replay the stream at specific time. Since replaying with real network traffic, which can meet the requirements of the network cyber range and is regarded as the proper method to generate traffic.

Cheng [6] and Google designed and implemented a traffic replay system called Monkey, which consists of Monkey see and Monkey do. Hong [7] and Wu first proposed an interactive flow replay method, and developed the replay system TCPOpera. Li [8] proposed a replay method based on IP address mapping. The topology similarity is calculated by characteristic of traffic. At the same time, multiple virtual topology similarities are calculated. Comparing the similarities, the virtual topology with the closest similarity is selected.

Among them, in Li's method, when calculating the topology similarity, need to acquire the physical topology of the original traffic file. For some complex network topologies, the implementation is difficult and the scalability is inferior. Besides, all of these replay method base on two machine interactive communication or multi-nodes one-way communication, which is not applicable to cyber ranges. Therefore, this paper proposes a multi-nodes interactive replay method. And an IP-mapping method is also designed to allocate multiply replay streams into replay nodes, where the number of replay nodes is far smaller than replay streams.

The rest of this paper is organized as follow. Section 2 introduces the algorithm and implementation of multi-nodes replay method. We verify the replay method and compare the replay method to Tcpreplay in replay delay error at Section 3. Section 4 summarize the paper.

2. Methodology

2.1 Traffic File Pre-processing.

The raw traffic being replay needs to remove "noise" traffic. This paper will use the BPF filtering mechanism to filter the packets. In order to ensure the integrity of the session during replay, the replay traffic is shunted according to the <source IP address, destination IP address, source port, destination port, transport layer protocol> five tuples, and each stream is filtered as a replay unit. These streams are grouped by stream characteristics, such as the number of packets, the size of the stream, and the average interval of the packets.

2.2 IP-mapping.

For IP-mapping method, contains the client IP-mapping and the server IP-mapping. Because the number of clients and servers in the traffic file is often not equal, and the traffic characteristics of the two are differentiated, which means the traffic of the client access server is less than the traffic responded by the server to the client. Therefore, for the client, the one-to-one mapping method is applied to increase the byte size of replay stream as a selection criterion. For server IP-mapping, reducing the packet delay of each stream as a mapping target. Client IP-mapping process is as follows: first, according to the statistical feature of flow size select the top K streams as the traffic replayed by the client. The virtual client IP address and the reality client IP address in the top K streams are mapped by using a hash function.

After selecting top K streams for client IP address mapping, the server-side IP address mapping process begins, get the server IP addresses interacting with K clients from the top K streams. Regard these IP addresses as index, a set of flows that the server communicates with the client is counted. The mapping standard for each server is obtained as t by weighting average time interval and the number of packets.

2.3 Multi-nodes Traffic Replay.

There are two issues during replay. First, since the traffic replay involves packet reconstruction and transmission functions, the time cost is high. In addition, for the traffic replay part, since the replay node needs to replay multiple streams, it needs to be managed by some strategy. For the time inaccuracy problem, this method takes actions to ensure time accuracy. Before the replay starts, clock synchronization is needed, and all nodes starts the replay program at the same time. Besides, the timestamp of the first packet in the original traffic file is regard as the replay start absolute timestamp to ensure the start of replay packet is same. During the replay, in order to reduce the packet transmission time error, we adopt the following strategy: compare the program execution time T1 and the packet relative timestamp T2. When T1>=T2, it means that the last packet is executed too long, At this occasion, the packet needs to be directly sent. When T1<T2, it indicates that it is not the correct time to send packet, so the program needs to sleep, and the sleep time is (T2-T1). Refer to sleep function, the select function has higher precision for s level, while the nanosleep has higher precision for ms level. Therefore, it is necessary to assemble two functions according to the sleep time. For the replay of each stream, we use thread pool to manage multiply replay stream. It also involves the reconstruction and transmission of the data packet. In order to focus on the design of the replay method and simplify packet transmission process, the libnet [11] library is used to read the transport layer workloads in the original data packet and then reconstruct the UDP packet header. Network layer and link layer header information are also auto completed by construction function of libnet, finally use the specific function to send the packet.

3. Experiment and Analysis

The experiment needs to verify the mapping effect and replay effect. For the mapping effect, we pay attention to server IP-mapping. The server side aims to reduce packet delay error. Therefore, using Tcpdump on all replay servers to capture packets during replay and calculate the replay delay error. Finally, in order to verify the replay effect, the replay delay error is also used as the replay effect evaluation standard, and the experimental object is the current usage rate replay tool Tcpreplay and replay method proposed in this paper.

The current experiment selects a traffic file with 10 minutes and performs replay it on 2 clients and 3 servers. According to statistic result, there are 863 TCP connections. Before IP address mapping, the size of stream file bytes in each client is as follows:

Table 1. Statistic Information of Original Traffic File

IP	Flow number	Size of flow
10.245.142.16	126	4364625
10.245.142.13	142	3714632
10.245.142.6	291	2000815
10.245.142.12	53	710872
10.245.142.10	139	462082
10.245.142.5	34	357651
10.245.142.40	35	183669
10.245.142.33	19	62936
10.245.142.27	24	15653

The current mapping method selects top two sets of stream files in terms of flow sizes for replay. For the server IP- mapping effect, capturing the replay process packets and calculating the replay delay error, the three replay delay errors shown in the figure below are obtained.

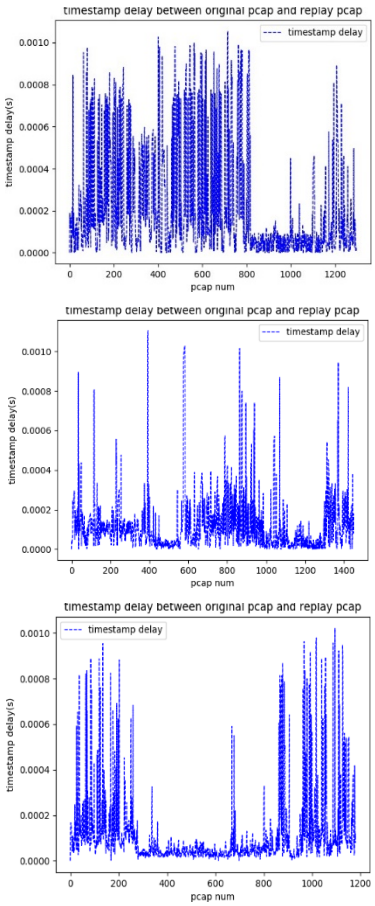

Fig. 1 three servers replay delay error

From this observation, it can be found that the replay delay errors of the three nodes are all around 0.2ms and the target of minimizing the delay error by each node is satisfied, and the IP-mapping method is relatively stable. Finally, for the replay effect verification method, the replay method of this paper and Tcpreplay using the same data stream files. One experimental result is shown in the following figure.

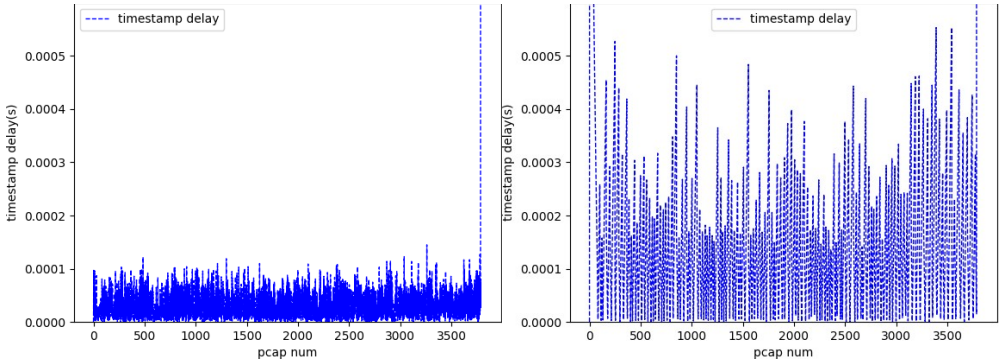

Fig. 2 multi-nodes replay(left) and Tcpreplay(right) in replay delay error

It can be seen that Tcpreplay replay delay error increases with the number of replay packets, showing a tendency to drop first and then rise, which is not stable enough. The experimental results of the replay method proposed in this paper are shown in the left figure. The replay delay error does not increase with the increase of the data packet, stable range is below 0.1ms.

4. Conclusion

The network cyber range is proposed as a platform for conducting network attack behavior and defense experiments. It needs to simulate the network environment by generating traffic between the virtual nodes, and the traffic replay is applied to the cyber range as the method due to the highest traffic authenticity. However, the current traffic replay method has the problems of simple replay structure and relatively low feasibility of mapping method. In view of the above problems, this paper proposes a relatively simple and feasible mapping method based on the characteristics of client and server traffic, and implement a multi-node replay method. For the replay method, a strategy for reducing the replay delay error is proposed. It has been verified by experiments that it can meet the demand of the cyber range.

Acknowledgments

The work of this paper is funded by the project of National Key Re- search and Development Program of China (No. 2016YFB0800802, No. 2017YFB0801804), Frontier Science and Technology Innovation of China(No. 2016QY05X1002-2), National Regional Innovation Center Science and Technology Special Project of China (No. 2017QYCX14), Key Research and Development Program of Shandong Province (No. 2017CXGC0706), and University Co-construction Project in Weihai City.

References

[1]. FANG Binxing, JIA Yan, Cyber Ranges: state-of-the-art and research challenges, Journal of Cyber Security, vol.1 No.3, pp.1-8, July 2016.

[2]. Kokkonen T., Hmlinen T., Silokunnas M., Siltanen J., Zolotukhin M., Neijonen M. (2015) Analysis of Approaches to Internet Traffic Generation for Cyber Security Research and Exercise. In: Balandin S., Andreev S., Koucheryavy Y. (eds) Internet of Things, Smart Spaces, and Next

Generation Networks and Systems. ruSMART 2015, NEW2AN 2015. Lecture Notes in Computer Science, vol 9247. Springer, Cham.

[3]. A. Botta, A. Dainotti, A. Pescap," A tool for the generation of real- istic network workload for emerging networking scenarios", Computer Networks (Elsevier), 2012, Volume 56, Issue 15, pp 3531-3547.

[4]. Kashi Venkatesh Vishwanath and Amin Vahdat. 2009. Swing: realistic and responsive network traffic generation. IEEE/ACM Trans. Netw. 17, 3 (June 2009), 712-725.

[5]. Joel Sommers, Hyungsuk Kim, and Paul Barford, Paul Barford. 2004. Harpoon: a flow-level traffic generator for router and network tests. SIGMETRICS Perform. Eval. Rev. 32, 1 (June 2004), 392-392.

[6]. Cheng, Yu Chung, et al. "Monkey See, Monkey Do: A Tool for TCP Tracing and Replaying." General Track: Usenix Technical Conference DBLP, 2004.

[7]. Hong SS, Wong F, Wu S F, et al. TCPtransform: Property-Oriented TCP Traffic Transformation[J]. Lecture Notes in Computer Science, 2005, 35(4): 222-240.

[8]. Li, Lun, et al. Traffic Replay in Virtual Network Based on IP-Mapping. Algorithms and Architectures for Parallel Processing. Springer Interna- tional Publishing, 2015.

[9]. McCanne S, Jacobson V. The BSD Packet Filter: A New Architecture for User-level Packet Capture[C]//USENIX winter. 1993, 46.