Bro, Do You Even Generate?

Automatic Signature Generation against DDoS Attacks applied to Bro SIDS

René Boschma
University of Twente
r.boschma@student.utwente.nl

1. INTRODUCTION

A Denial of Service (DoS) attack is an attack that aims to disable the service a target supplies. There are two main types of DoS attacks: *vulnerability DoS* and *flood DoS* [11]. In one hand, a vulnerability DoS aims to exploit a vulnerability of the target system to reduce performance or render it useless. An example of such an attack is to send a malformed message to the target machine which can not deal with this message and as a result stops working. On the other hand, a flood DoS attack tries to exhaust the resources of the target. An example of such an attack is to fill the entire bandwidth of the target with messages of the attacker. The attacker can accomplish such bandwidth by using multiple machines to produce traffic. When multiple machines are used in the attack, the attack is called a Distributed Denial of Service (DDoS) attack.

DDoS attacks are increasing in power. In 2011 the peak attack was measured at 60 Gb/s [12], in 2015 500 Gb/s and in 2016 1.1 Tb/s [3]. Also, the frequency of the attacks are increasing: in the third quartile of 2016 more than 5000 attacks where observed, whereas 200 in the entire 2012 [2]. An explanation for this increase in frequency could be the rise of *booters*[4]. A booter, also called stressers, are websites that offer DoS attacks via a website. Booters eliminate the need for any technical knowledge to launch an attack. Clients of booters only need to pay a couple of dollars to launch an attack.

As the number of attacks is increasing and downtime costs are exceeding on average $300K per hour [1] a need for an efficient and effective mitigation method becomes bigger. Before mitigation can be done, first proper detection must be done. Intrusion Detection Systems (IDS) are such systems that can fulfill this task. An IDS is a system that monitors a system or network for malicious and/or suspicious activities within a network or system. Two main categories of IDSs are present: *host-based* and *network-based* [6]. A Host-based IDS (HIDS) is only for a single machine. A Network-based IDS (NIDS) is for an entire network. A NIDS usually scans the incoming and outgoing traffic of a network endpoint. Based on the detection methods of IDSs, again two categories can be identified: *Anomaly-based* and *Signature-based* [8]. An Anomaly-based IDS (AIDS) bases its detection on a constructed baseline and detects deviations from this baseline. A Signature-based IDS (SIDS) bases its detection on signatures. An AIDS has as benefit that it can detect unknown attacks but with the weakness that it has a low accuracy and difficulty to trigger alerts at the right time. A SIDS has as benefit that it has a high accuracy but with the weakness that it is ineffective in detecting unknown attacks and it is hard to maintain an up to date signature list [10].

Due to the high accuracy we believe that SIDSs are promising systems that can fulfill the requirement of successfully and efficiently detecting DoS attacks when the major downside of keeping an up to date signature list is tackled. That is why we propose an automatic method to generate signatures and apply this to specific SIDS. We have chosen Bro[1] as SIDS. Bro is an open source network security monitor that offers the functionality of a SIDS.

To pursue our goal we have the defined the following research questions (RQ) as the basis of the proposed research:

- **RQ1:** What are the current developments in automatic rule generation for Signature-based Intrusion Detection Systems (SIDS)?
- **RQ2:** How well do automatic generated signatures perform when applied to a real DoS attack?
- **RQ3:** How can automatically generated signatures be implemented in the SIDS Bro?

The remainder of this proposal is organized as follows. Section 2 will discuss the related work identified. Section 3 will discuss the intended approaches on how to answer each research question. In Section 4 we will conclude with a planning for the introduced research.

2. RELATED WORK

[1] `https://www.bro.org/`

Fallahi et. al. [6] implemented automatic rule generation for the SIDS Snort. They used two data mining algorithms called Ripper and C5.0. They investigated five types of attacks and tested it on the ISCX 2012 dataset. Rather than looking to individual packets, they looked at the flow of data. From the flow 17 features were selected to generate rules. Fallahi et. al. applied this approach to a single dataset which contained various attacks, rather than focusing on DoS attacks.

Fouda [7] proposes a payload based signature generation specific for DDoS attacks. Various pattern matching algorithms are tested to find the amount of similarity between incoming traffic and traffic that is associated with a DDoS attack. It was found that Smith-Waterman and Longest Common Substring algorithms yielded the highest accuracy. A problem apparent in this approach is that it tends to become slow. In 2003 IDSs could only cope with up to 200 Mbps of traffic [9].

Chimetseren et. al [5] proposes signature based generation method using Discrete Fourier Transform. In this method the payload between client and server are regarded as discrete waveform. They create a spectrum for normal, known attack and unknown attack sessions. This approach is tested on the Kyoto2006+ dataset[2]. By also generating a spectrum for normal sessions, they are able to detect unknown attacks. However, this does yield a 5% false positive in the selected dataset.

3. PROPOSAL

[TODO]

4. PLANNING TASKS

In this section, we will briefly discuss the planning of the research. Figure 1 pictures the intended planning. The first 7 weeks are planned for writing the proposal. This period knows two deadlines at the end of week 14 and 16. The first deadline is the deadline for the draft proposal and the second the deadline for the final proposal. During this period not that much time can be spent on the actual research due to other obligations.

The remainder of the time the actual research will be carried out. During this period, more time can be spent per week in comparison to the proposal period. The research period is defined in time per RQ. The first and last RQs are more theory based and therefore probably cost less time than RQ 2 which is more practical. During RQ 2 there is also a holiday planned where no time will be spent on this research.

Finally, a week to finalize the entire research is planned. This period is intended as a buffer in case some parts of the research are going less prosperous than intended.

[2] http://www.takakura.com/Kyoto_data/

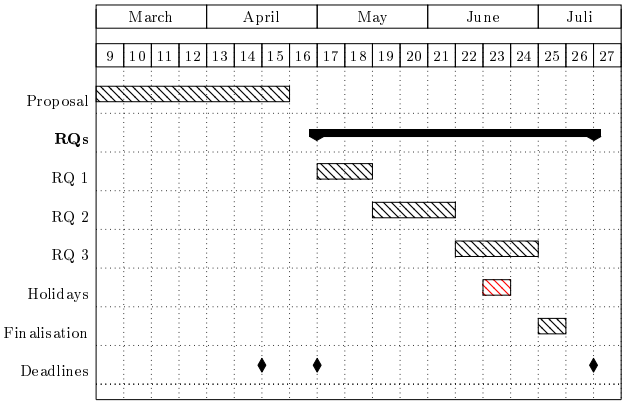

Figure 1: Planning of this research.

5. REFERENCES

[1] Cost of hourly downtime soars: 81% of enterprises say it exceeds $300k on average. http://itic-corp.com/blog/2016/08/cost-of-hourly-downtime-soars-81-of-enterprises-say-it-exceeds-300k-on-average/. Accessed: 2018-03-21.

[2] Akamai. State of the Internet/Security (Q3/2017). page 40, 2016.

[3] Akamai. State of the Internet/Security (Q1/2017). 4:26, 2017.

[4] J. Cardoso de Santanna. Ddos-as-a-service: Investigating booter websites, 11 2017. CTIT Ph.D. thesis Series No. 17-448, ISSN 1381-3617.

[5] E. Chimetseren, K. Iwai, H. Tanaka, and T. Kurokawa. A Study of IDS using Discrete Fourier Transform. pages 463–466, 2014.

[6] N. Fallahi and A. Sami. Automated Flow-based Rule Generation for Network Intrusion Detection Systems. pages 1948–1953, 2016.

[7] K. M. I. A. Fouda. Mathematics & Computer Science Payload Based Signature Generation for DDoS Attacks. 2017.

[8] A. G. Fragkiadakis, V. A. Siris, N. E. Petroulakis, and A. P. Traganitis. Anomaly-based intrusion detection of jamming attacks, local versus collaborative detection. *Wireless Communications and Mobile Computing*, 15(2):276–294, 2013.

[9] H. Lai, S. Cai, H. Huang, J. Xie, and H. Li. A parallel intrusion detection system for high-speed networks. *Applied Cryptography and Network Security*, pages 439–451, 2004.

[10] H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, 2013.

[11] D. Lin. Network Intrusion Detection and Mitigation against Denial of Service Attack. *WPE-II Written Report*, (January):1–28, 2013.

[12] A. Networks and A. Networks. Arbor Networks 9th Annual Worldwide Infrastructure Security Report. 2014.