Automatic DDOS Attack Rule Generation Applied to Bro SIDS

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

Abstract

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

1 Introduction

A Denial of Service (DoS) attack is an attack that aims to disable services of a target system. There are two main types of DoS attacks: *vulnerability DoS* and *flood DoS* [7]. In one hand, a vulnerability DoS aims to exploit a vulnerability of a target system to reduce its 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 flood by using multiple machines to produce traffic. When multiple machines are used in the attack, it is called a Distributed Denial of Service (DDoS) attack.

DDoS attacks have increased in power and frequency. In 2011, the peak attack was measured at 60 Gb/s [9], in 2015, 500 Gb/s and in 2016 1.1 Tb/s [3]. In the third quartile of 2016 more than 5000 attacks where observed, whereas 200 in the entire 2012 [2]. As the number of attacks increase and downtime costs are exceeding on average $300K per hour [1] a need for an efficient and effective mitigation method has become crucial. The first task before the mitigation is the detection of an attack. 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. Based on the detection methods of IDSs, two categories can be identified: *Anomaly-based* and *Signature-based* [5]. 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 key characteristic of an attack for which predefined signatures are known. An AIDS has as benefit that it can detect unknown attacks but with the weaknesses that it has a low accuracy, needs time to learn a baseline of a system and has difficulties to trigger alerts before an attack scales up. A SIDS has as benefit that it has a high accuracy but with the weaknesses that it is ineffective in detecting unknown attacks and it is hard to maintain an up to date signature list [6].

Our hypothesis is that due to the high accuracy a SIDS is a suitable system that can fulfill the requirement of successfully and efficiently detecting DDoS attacks when the major downside of keeping an up to date signature list is tackled. The solution for this problem is to generate signatures for new attacks. This can be done either manually or automatically. As a manual approach requires significant amount of manual effort [7], we propose an automatic method. For this research we generate

rules from extracted features of DDoS attacks for the Bro SIDS[1]. Bro is an open source network security monitor that offers the functionality of a SIDS. The features of DDoS attacks are extracted by a different research of DDoSDB[2].

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

- **RQ1:** What are the DDoS characteristics that could be used for generating BRO detection/mitigation rule?
- **RQ2:** What is the performance of automatic rule generation against a DDoS attack for the Bro SIDS?
- **RQ3:** What is the accuracy and efficiency for Bro automatic generated rules when applied on an ongoing DDoS attack?

The first RQ will be answered by analyzing the most common DDoS attack vectors described by Akami [4]. The second RQ will be answered by building a proof of concept that generates signatures based on a given stream of features of DDoS attacks. The third and last RQ will be answered by replaying an attack for which a signature was generated and analyze what the performance of Bro is with these signatures implemented.

2 Content

2.1 DDoS Attacks and BRO

In this section we will first define the notion of a DDoS attack by explaining how the infrastructure looks like. Then we will elaborate on various DDoS attacks used nowadays and discuss their main characteristics. After this we will discuss the syntax of the detection rules of the BRO SIDS.

2.1.1 The DDoS Attack

Figure 2.1.1 shows the infrastructure of a DDoS attack. Actors involved in a DDoS attack are denoted by a letter (A-D) whereas data streams are denoted by numbers (1-5).

[1] https://www.bro.org/
[2] http://ddosdb.org/

A DDoS attack starts with an attacker (A). The attacker sends data needed to start the attack (1) to the Command and Control (C&C) servers (B). The C&C servers control the infected machines (C). The infected machines are also known under the name of bots. The C&C servers plus the infected machines are more commonly named as a botnet. The C&C servers send a message (2) to the infected machines. In case of the Ramnit botnet, only the infected machines counted 3.2 million machines [8]. At this point two paths are used to get to the target machine (E). The first path possible is aiming the infected machines directly to the target (4). The second path possible is using public services (D) like a DNS to reach the target (5).

In the next subsection we will describe various types of DDoS attacks.

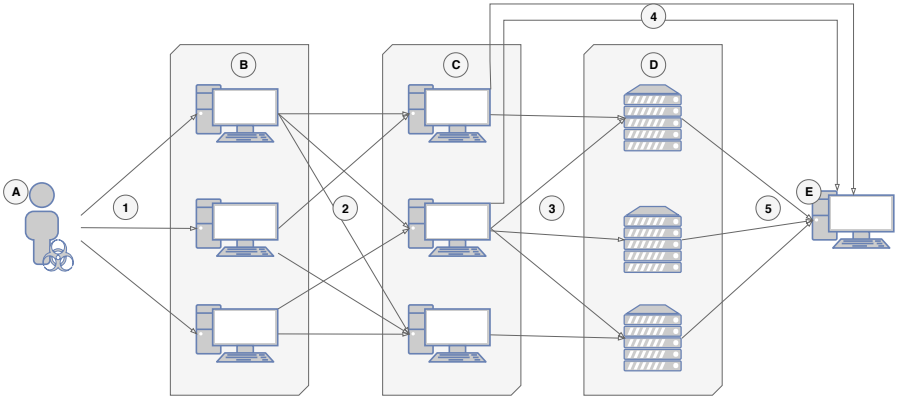

Figure 1: Overview of DDoS attack infrastructure

2.1.2 Types of Attacks

In this section we will briefly elaborate on various types of attack. The main characteristics can be found in Table . . . .

UDP Fragment The UDP Fragmantation attack exploits the fragmentation used in the IP protocol. When a packet is to big to be sent across a network link, it will be broken down into smaller packets and later on resembled again. In a UDP Fragmentation attack, fraudulent UDP packets are sent which are larger than the maximum transmission unit (MTU) of the network. The idea is that the packets can not be reassembled and thereby consuming the server's resources.

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-excee 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). 2017.

[4] Akamai. State of the Internet/Security (Q4/2017). 2017.

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

[6] Hung Jen Liao, Chun Hung Richard Lin, Ying Chih Lin, and Kuang Yuan Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, 2013.

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

[8] Europol Corporate Communications Lisanne Kosters. BOTNET TAKEN DOWN THROUGH INTERNATIONAL LAW ENFORCEMENT COOPERATION. 2015.

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