DDoS Network Flow Forensics Analyser

Cristian Turetta, *VR421196* and Andrea Perazzoli, *VR421197*

Abstract—Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. This report introduces ...

1 Introduction

Denial of Service (DoS) attack is launched to make an internet resource unavailable often by overwhelming the victim with a large number of requests. DoS attacks can be categorized on the basis of single source and multi source. Multi source attacks are called distributed Dos or DDoS attacks [1].

There are various type of tool in order to detect and deal with DDoS attacks, these tools can be applied in real time, such as intrusion detection systems (IDS) or by analysing network flow records offline doing a forensics analysis, which is our focus. Computing forensics analysis over a recorded network flow can be useful, we may understand if someone is trying to flood a network to get a denial of service and eventually recognise it. Evidence of such intrusions is required in case the affected wants to pursue the court and legal action is to be taken against the adversary.

Forensics investigations are not trivial to accomplish and often done manually, this because the attacker can mask its attempts by mixing legitimate requests with malicious ones.

DDoS attacks aim to compromise the availability of a system or a network, the attack is launched by the adversary which has take control over bots, compromised machines connected to internet, that sends several requests to the victim and overwhelm it with large amount of traffic. This creates a bottleneck and the victim can no further deal with this traffic denying service to them.

During DDoS attacks, the log files swell up to huge sizes, these log files if analysed properly and effectively can help detect and recover from a DDoS attack [1]. Log files can take a long time if processed through conventional means thus we decide to use big data's tool and framework in order to get a faster processing and investigation.

In this report we present our tool which uses *Pig-latin* script embedded into a *Python* program that can be used to analyse network log file, `pcap` format [2], and returns statistical information about the recorded traffic. In Section 2 we present the statistical tool used in our analysis. In Section 3 we present the project structure and implementation. In Section 4 we focus on analysis results. In Section 5 we discuss the performance of our tool in terms of computational time and resources. Section 6 concludes the report with our considerations.

References

[1] Rana Khattak, Shehar Bano, Shujaat Hussain, Zahid Anwar. *DOFUR: DDoS Forensics Using mapReduce*. Frontiers of Information Technology, 2011.

[2] Wireshark Wiki, Development. Last access *May 15 2019*. https://wiki.wireshark.org/Development/LibpcapFileFormat