Ontology based intrusion detection system

Aarti Kashyap[1] , **Aarti Kashyap**[2] ,

[1]

[2]

kaarti.sr@gmail.com

Abstract

The increase in the usage of web services has also lead to an increase in web-based attacks. To detect these attacks, intrusion detection systems(IDS) were developed. One category of widely popular attacks is the denial of service (DoS) attacks. In the past few years, a new category of DoS attacks called slow DoS attacks have been growing rapidly and are becoming difficult to detect despite the availability of detection mechanisms. The need to develop detection mechanisms against such apparent threats led to the introduction of ontology-based intrusion detection systems (IDS) [Undercoffer *et al.*, 2003]. We introduce a novel method of intrusion detection for Slow DoS attacks by encoding the knowledge about the attacks using an ontology. We analyze the traffic characteristics for four categories of Slow DoS attacks based on a dataset generated by Sharafaldin et al. [Sharafaldin and Habibi, 2018]. Further, we create an ontology based on the attributes of network protocols. We use the ontology to store information about network packets. Finally, we use the completed ontology to query the existence of complex relations between the network packet features to detect slow DoS attacks [Razzaq *et al.*, 2014]. We conclude by discussing the advantages of approaching network attack detection mechanisms from an ontological perspective compared to other ad-hoc techniques.

1 Introduction

1.1 Slowloris attack tool

Slowloris is a type of slow DoS attack tool which utilizes minimal bandwidth with fewer side effects on unrelated services and ports. It works by opening multiple connections to the targeted web server and keeping them open as long as possible. The attacked servers open more connections, waiting for each of the attack requests to be completed.

1.2 Ontology

Ontology is defined as a set of concepts and categories in a subject area or domain along with their properties and relations between them. We use an ontology to represent the relationships between different attributes of a packet in networking [Silva and Rafael, 2015].

1.3 Approach

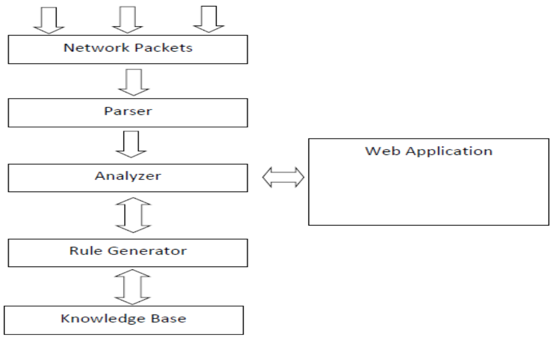

Figure 1: Intrusion detection system for slowDos attacks

1.4 Results

In case of an active slow DoS attack, we observed that the response packets from the server side are empty and do not contain any data in them. In order to make sure that the connection is active, the server keeps sending an empty response packet in fixed intervals. In order to automate the above characteristic, we calculate the difference (Z) between the two attributes obtained from the data set: total backward packets(TBP) and total forward packets(TFP). For each source-destination pair, we calculate the ratio between the number of connections for which Z is positive and the number of connections for which Z is negative. This gives us an estimation of empty packets and packets which contain data. Depending on the ratio, we can predict if there is an active Slow DoS attack.

Table 1: Query Results for a Particular Source IP

Source IP	Z is less than 0	Z is greater than 0	Z Total
172.16.0.1	5654	142	5796
192.168.10.15	5	3	8
192.168.10.25	15	1	16

References

[Razzaq *et al.*, 2014] Abdul Razzaq, Khalid Latif, H. Farooq Ahmad, Ali Hur, Zahid Anwar, and Peter Charles Bloodsworth. Semantic security against web application attacks. *Information Sciences*, 2014.

[Sharafaldin and Habibi, 2018] Imran Sharafaldin and Arash Habibi. Towards generating a new intrusion detection dataset and intrusion traffic characterization. 2018.

[Silva and Rafael, 2015] D. V. Silva and G. R. Rafael. Ontologies for network security and future challenges. 2015.

[Undercoffer *et al.*, 2003] Jeffrey Undercoffer, Anupam Joshi, and John Pinkston. Modeling computer attacks: An ontology for intrusion detection. In *Recent Advances in Intrusion Detection*. Springer Berlin Heidelberg, 2003.