DD2497 Project specification

Davis Freimanis
davisf@kth.se

Thomas Peterson
thpeter@kth.se

Emelie Eriksson
emee@kth.se

Marcus Lignercrona
mlig@kth.se

October 2018

1 Introduction

A common way for attackers to get access to remote computers is by abusing insecure network connections. In this project we intend to make a simple firewall to counter the most basic ways of abusing network traffic. The idea is to implement the firewall according to figure 1. In this figure inbound packets travel from the network towards the user process through the network server(And outbound packets travel in the opposite direction). After entering the network server, the packets have to travel through a couple of decision servers which acts like filters. The packets that survive the filters exit the network server and end up i at their corresponding destination(user process or the network driver). Packets that do not survive the filtering process are logged in a logfile together with a brief note describing why they were dropped.

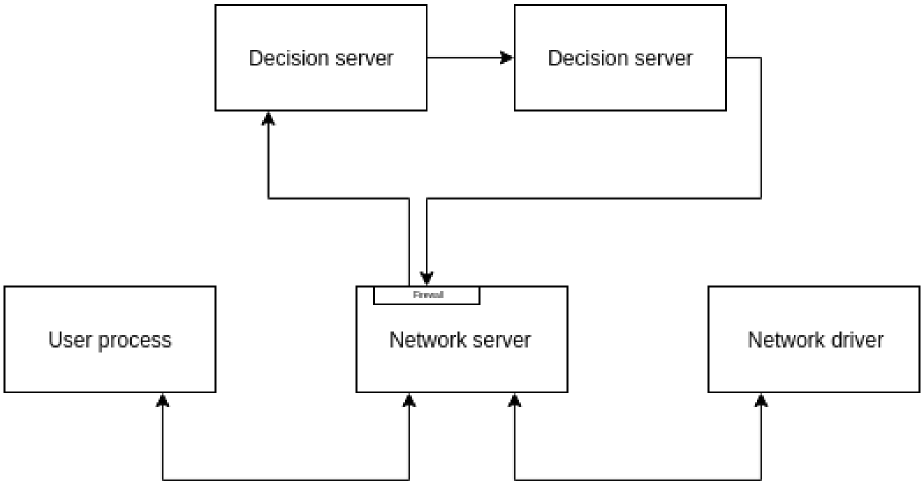

Figure 1: Firewall structure

2 Mandatory requirements

The first part of the project is to create a firewall that can monitor in and outbound network traffic as well as filter this traffic using whitelists and blacklists.

The mandatory requirements would be:

- A firewall that is able to intercept inbound and outbound network packets
- A server, dec, for filtering out unwanted network traffic
- Dec should be able to filter source/destination ports and packet type(TCP/UDP) by using whitelists and blacklists
- The firewall should be able to communicate with the dec server to decide which packets to block and subsequently drop these packets.
- The firewall should adopt the principle of fail safe defaults. For example, if a packet is not in a whitelist or blacklist it should be blocked by default.
- The firewall should be able to log dropped packets together with what rules they were breaking.

3 Optional requirements

When the most basic functions of the firewall has been implemented there are some additional features that we would like to implement. Firstly, we would like to make the packet filtering more advanced by analyzing packets more in depth rather than just filtering according to rules. Consequently, it should be able to detect basic dos attacks and tcp syn scans. Additionally, we would like the firewall to have encrypted and signed configuration files.
The optional requirements are:

- The filters should be able to detect basic dos attacks and be able to block the source IP of a dos attack. Thus, ensuring the minix server availability for other users.
- The firewall should be able to detect and block attempts to scan the system with tcp syn packages.
- The firewall should have encrypted configuration files.
- The firewall should be able to receive new configurations that are signed and verify the signatures of these new configurations before adding them to the original configurations.