Universitat Politècnica de Catalunya

Software Defined Security

Project

Authors:

Sergi Ger Roca

Arnau Gris García

Pau Cuesta Arcos

Marc Iglesias Aulinas

Course 2022-2023
May 1, 2023

Contents

1 Scenario

In our project, we would like to implement the following scenario:

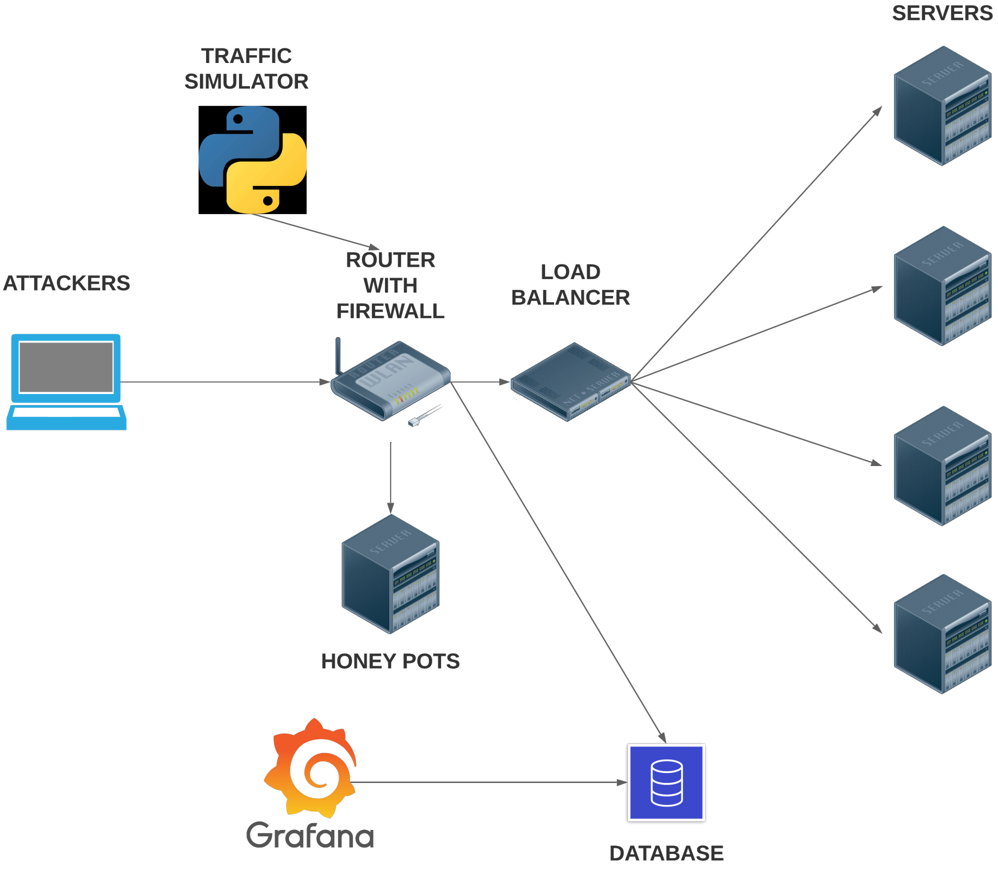

Figure 1: Project scenario

In this scenario, we have the following items:

- **ATTACKERS**; This will be some attacker's (python scripts) that will launch some network attacks to the network infrastructure.
- **TRAFFIC SIMULATOR**: This will be a python script that will emulate some "normal" traffic to the network.
- **ROUTER WITH FIREWALL**: This will be the router of the network, this will include a firewall with some default rules to redirect the traffic and also some predefined rules to avoid some network attacks.
- **LOAD BALANCER**: This load balancer will balance the traffic to the different servers.
- **HONEY POTS**: Here we will have some honey pots to handle different attacks, this honey pots will be implemented using Snort, and also using Snort

we will adapt the firewall to the different attacks on live-time.

- **SERVERS**: This will be our servers implemented using MiniNet.
- **DATABASE**: We will use InfluxDB database to store traffic from the network.
- **GRAFANA**: we will use Grafana to see on a visual way the traffic data from the db, like using charts.

1.1 Attacks to implement

We will like to implement the following attacks:

1. **DDOS**: We will implement a python script that perform DOS attack to the network, this script will be run from several attackers, reproducing a DDOS attacks. This DOS will be a scale attack: for example, we will start launching 10 requests x second, and then scale it on time, like one minute later duplicate the requests x second.
2. **Port Scanning**: To implement port scanning, we will use some regular Kali tools, like NMAP.