Acceptance clause: by completing this project the student accepts that he/she is responsible for what he/she will do and that he/she will **not use** these tools outside the virtual one created for that purpose. The student also accepts the legal repercussions that some of these actions may be subject to if these actions are carried out on external sites.

Project 5: Denial of Service

Level: 3

Difficulty: medium-high

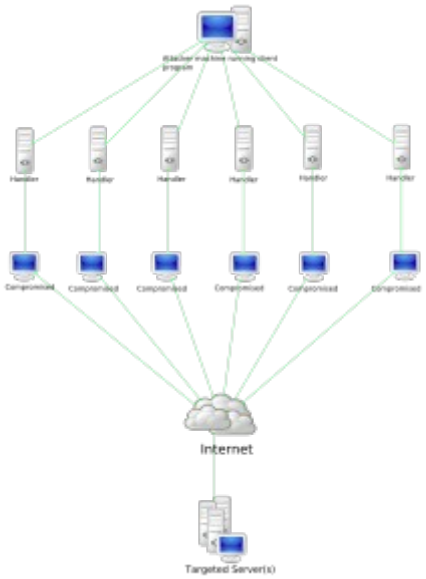
Environment: Linux Machines (VM)

Objective: Install and analyze the indicated tools obtaining to create a DoS on worker1 (DO NOT USE outside the virtual network).

Task: The student will have to collect information about DoS, and configure Router to execute a http DoS at worker1. After it, the user will protect worker1 using iptables or mitigating DoS with some specific tools for Apache2 (https://blog.shekyan.com/2011/11/how-to-protect-against-slow-http-attacks.html).

Necessary: Start with project 4 to learn about firewalls.

In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. More sophisticated strategies are required to mitigate against this type of attack, as simply attempting to block a single source is insufficient because there are multiple sources.
A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, thus disrupting trade. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Reference & more info: https://en.wikipedia.org/wiki/Denial-of-service_attack



SlowHTTPTest

SlowHTTPTest is a highly configurable tool that simulates some Application Layer Denial of Service attacks by prolonging HTTP connections in different ways. Use it to test your web server for DoS vulnerabilities, or just to figure out how many concurrent connections it can handle.

Application Layer DoS attacks, such as **slowloris**, **Slow HTTP POST**, **Slow Read attack** (based on TCP persist timer exploit) by draining concurrent connections pool, as well as **Apache Range Header attack** by causing very significant memory and CPU usage on the server.

Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service. This tool is sending partial HTTP requests, trying to get denial of service from target HTTP server.

Slow Read DoS attack aims the same resources as slowloris and slow POST, but instead of prolonging the request, it sends legitimate HTTP request and reads the response slowly.

Installation and usage examples

How I knocked down 30 servers using slowhttptest

Slow Read DoS attack explained

Test results of popular HTTP servers

How to protect against slow HTTP DoS attack

Latest official image is available at Docker Hub: docker pull shekyan/slowhttptest:latest

References: https://github.com/shekyan/slowhttptest/wiki