# Software Requirements Specification

# for

# DOS Attack Implementation and Mitigation

Version 1.0 approved

Prepared by Shubham Arora (14BCE0905), Shary Khanna (14BCE0887)

Softear

<date created>

Table of Contents

Table of Contents [ii](#__RefHeading___Toc441230970)

Revision History [ii](#__RefHeading___Toc441230971)

1. Introduction [1](#__RefHeading___Toc441230972)

1.1 Purpose [1](#__RefHeading___Toc441230973)

1.2 Document Conventions [1](#__RefHeading___Toc441230974)

1.3 Intended Audience and Reading Suggestions [1](#__RefHeading___Toc441230975)

1.4 Product Scope [1](#__RefHeading___Toc441230976)

1.5 References [1](#__RefHeading___Toc441230977)

2. Overall Description [2](#__RefHeading___Toc441230978)

2.1 Product Perspective [2](#__RefHeading___Toc441230979)

2.2 Product Functions [2](#__RefHeading___Toc441230980)

2.3 User Classes and Characteristics [2](#__RefHeading___Toc441230981)

2.4 Operating Environment [2](#__RefHeading___Toc441230982)

2.5 Design and Implementation Constraints [2](#__RefHeading___Toc441230983)

2.6 User Documentation [2](#__RefHeading___Toc441230984)

2.7 Assumptions and Dependencies [3](#__RefHeading___Toc441230985)

3. External Interface Requirements [3](#__RefHeading___Toc441230986)

3.1 User Interfaces [3](#__RefHeading___Toc441230987)

3.2 Hardware Interfaces [3](#__RefHeading___Toc441230988)

3.3 Software Interfaces [3](#__RefHeading___Toc441230989)

3.4 Communications Interfaces [3](#__RefHeading___Toc441230990)

4. System Features [4](#__RefHeading___Toc441230991)

4.1 System Feature 1 [4](#__RefHeading___Toc441230992)

4.2 System Feature 2 [4](#__RefHeading___Toc441230993)

5. Other Nonfunctional Requirements [4](#__RefHeading___Toc441230994)

5.1 Performance Requirements [4](#__RefHeading___Toc441230995)

5.2 Safety Requirements [5](#__RefHeading___Toc441230996)

5.3 Security Requirements [5](#__RefHeading___Toc441230997)

5.4 Software Quality Attributes [5](#__RefHeading___Toc441230998)

5.5 Business Rules [5](#__RefHeading___Toc441230999)

6. Other Requirements [5](#__RefHeading___Toc441231000)

Appendix A: Glossary [5](#__RefHeading___Toc441231001)

Appendix B: Analysis Models [5](#__RefHeading___Toc441231002)

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Date** | **Reason For Changes** | **Version** |
|  |  |  |  |
|  |  |  |  |

# Introduction

## Purpose

The purpose of this document is to give detailed description about the DOS attacks which happens on the server and providing a way to prevent them. It will explain the purpose and features of the system, the interfaces of the system, what the system will do, the constraints under which it must operate and how the system will react to external stimuli. This document is intended ethical hackers and service providers who maintains and keep a regular check on the server.

## Document Conventions

The use cases includes the priorities of tasks and functions. The priority of tasks is assumed as per the dependencies of functions provided in the models.

## Intended Audience and Reading Suggestions

The audience includes DNS providers, analysts and ethical hackers. The main aim is to show how the Denial to a user is given or how the server breaks down. This can be intended to anyone who uses web services.

## Product Scope

The scope of this product will be extended by providing a prevention system against any type of attacks on the server. The server is halted or broken down by giving a lot of continuous requests on the desired IP address. The requests are given as per the capacity of server. DOS attacks description makes a user understands the risks involved as well as the security of a server.

We extend the implementation by providing a method to prevent these attacks according to various attributes of servers.

## References

https://www.defcon.org/images/defcon-19/dc-19-presentations/Bowne/DEFCON-19-Bowne-Three-Generations-of-DoS-Attacks.pdf

N. Tripathi, N. Hubballi and Y. Singh, "How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection," 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, 2016, pp. 454-463.

doi: 10.1109/ARES.2016.20

# Overall Description

## Product Perspective

The actors for DOS attack are user and administrator. The user uses the web services and administrator has control over the server. The software does the DOS attack on a dummy server to show case how an actual DOS attack happens. The implementation of the prevention will be taken up to high scale server with various dependencies so as to secure the server with various attributes taken into consideration. The prevention of the attack on dummy server will also be showcased to give detailed view of the working of product.

## Product Functions

The functions included for the user is for loading the IP address and taking one of the methodology of attack on server, and sending requests by starting the process of software. The design will be interactive for the user. For the administrator the function will be taking the details and loading into the system so as to take prevention by running the software for authentication, time and load on server. The administrator can use functions to select various aspects and handles an attack on server effectively.

## User Classes and Characteristics

The system will have only to actors in which at least one will be on scene every time. The user has access to server load, the user can attack a server or block request using firewall. The administrator will do server setup maintenance, has access over the server and can control accordingly or access usage logs to ensure the effectiveness of server.

## Operating Environment

The environment for running the software will be windows. The server setup will be done on windows using a service provider and the implementation will be done using python. The GUI will be created using QT for better usage.

## Design and Implementation Constraints

The design will be mostly limited to the small scale servers and the prevention of attacks will also be dependent on the server quality and payload.

## User Documentation

The help and implementation is taken under the consideration of DOS attacks on a small server. The types and implementation help for the product is given under the reference in previous section.

## Assumptions and Dependencies

It is taken into consideration that the server is without any flaws and the payload delivery of the server is up to the mark for best results. The implementation will mostly be dependent on the attributes of the service providers such as load, capacity, firewalls and mechanisms to handle flow.

# External Interface Requirements

## User Interfaces

The Client User Interface consists of a single window with several Buttons to implement various types of DOS attacks on the server. A text-box is used to input server’s IP (Internet Protocol) Address and Port Address. On clicking a button a dialog box appears with a real-time graph of System and RAM Load in order to monitor the attack. A check box is provided to enable or disable the server side firewall rules which can be used to mitigate the DOS Attack.

## Hardware Interfaces

Server Setup → Server consists of a single core CPU with 512MB of RAM. The Operating System runs on a KVM Hyper-visor.

Client Hardware → Client Hardware must be able to run any Operating system with QT Toolkit Support.

## Software Interfaces

Server →

* Ubuntu 16.04 running on KVM Hyper-visor.
* IPTables – for controlling the firewall and log IP addresses.
* Apache Web Server

Client →

* Linux/Windows/Mac OS for running the client software.
* QT Toolkit 5.8 – UI Toolkit (Cross Platform)

## Communications Interfaces

Apache Web server is used to provide an interface to perform DOS attacks over port 80.

Communication Standards:

* HTTP
* ICMP
* UDP

# System Features

The software provides two major features – DOS Attack Implementation (Client Side) and Firewall Implementation (Server Side).

## DOS Attack Implementation

4.1.1 Description and Priority

Implementing various types DOS Attack Methods. Priority: High

4.1.2 Stimulus/Response Sequences

1. Open the Client Program.
2. Click the DOS Attack type.
3. A dialog box will open with logs and real-time load graph.

4.1.3 Functional Requirements

TBD

## Firewall Implementation

4.2.1 Description and Priority

Mitigation and Blocking of attacks based on IP Address. Priority: Medium

4.2.2 Stimulus/Response Sequences

TBD

4.2.3 Functional Requirements

TBD

# Other Nonfunctional Requirements

## Performance Requirements

The administrator should ensure the working of server before launching the software so as to authenticate the attack. The performance of the attack will be based on the connection of the user with server, high connection will yield better results. The performance will be dependent on the attributes of the server such as connectivity, payload, handling and prevention measures as specific as possible. You may need to state performance requirements for individual functional requirements or features.

## Safety Requirements

The safety of the server for administrator will be ensured as soon as the authentication of attack is done by the program. It is required to ensure the safety measures before launching the program such as checking for malware and Trojans or corrupted files transacting over the server.

## Security Requirements

The server will be secured by different DOS attacks when the administrator starts the program. The issue of securing under certain time will be dependent on the type of attack done by user or attacker. The firewall stops or halts the server as soon as it detects any false attack over the server.

## Software Quality Attributes

The software will be very interactive to users for both attack and prevention. The small size will ensure the working and it will be easily loadable on any machine with limited configurations. The effectiveness will be high when the connectivity will be good with the server. The speed of the attacks will be dependent on the type of server and thus its efficiency will vary according to the server.

## Business Rules

The User is expected to be Internet literate and should know about basic protocols over which Internet works for better efficiency of the implementation. The User is expected to be Windows literate and to be able to use button, pull-down menus, and similar tools.

The attack side of the software is for learning purpose only and it shouldn’t be used for any false actions.

# Other Requirements

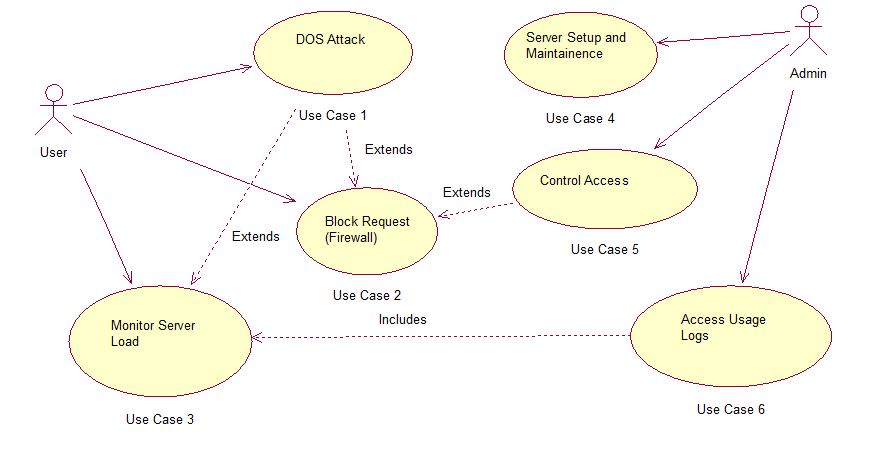
Legal: The project is licensed under GPLv3

Appendix A: Glossary

* IP Address: Internet Protocol Address.
* UDP: User Datagram Protocol
* ICMP: [Internet Control Message Protocol](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol)
* KVM: Kernel-based Virtual

Appendix B: Analysis Models

* Use Case Diagram



* Pert Schedule

