**PURPOSE:**

Today, we live in the world of Internet which has made great impact on computing and communications. Because of this the impact of DDoS attacks on internet security is growing excessively. There are various ways by which attacks are done like flooding, (slow), etc

Here, we propose a model which will detect and mitigate TCP and HTTP flood attacks in a timely manner and in very efficient way. But to detect them we have to first make a system which will do these attacks.

**SCOPE:**

**PRODUCT NAME:**

**PURPOSE:**

**OBJECTIVE:**

**GOALS:**

**STAKEHOLDERS**: Network Admin

1.3PRODUCT PERSPECTIVE:

With rapid growth of networking communications, there is threat to financial data, business analytics data, etc by DDoS attacks. So the perspective of our system will be to detect and mitigate this attacks so that victim must not be affected. Because some system going down for a second may pose great threat. As many application layer protocols who don’t want their data to be lost uses TCP protocol, so our main aim will be to handle TCP flooding SYN/ACK attacks.

1.3.1SYSTEM INTERFACES

Desktop application which must be run along with system(victim machine) everytime, because attack can happen anytime

1.3.2USER INTERFACES

GUI depicting the coming packets one by one and shows the number of attacks happened in timebound frame.

Also it will give the graphical view of the traffic on the system.

1.3.3 SOFTWARE INTERFACES

Operating system: windows or linux (32-64 bit)

Database system: MySQL

Backend: JAVA

Frontend: JAVA

Dependencies: wireshark

1.3.4HARDWARE INTERFACES

All devices like personal computers, mainframe computers with linux or windows operating system

1.3.5COMMUNICATION INTERFACES

High level use of socket programming

Use http, icmp, tcp, protocols

To detect the packets, packet sniffing is done for all layers

1.3.6 MEMORY CONSTRAINTS

It requires memory to store the packets. Also the dynamic memory to store the ip address of attacker(if detected) for short period of time and then free the memory.

1.3.7OPERATION REQUIREMENTS

This software is compatible with Linux or Windows with JDK (32-64bit)

The system will not interrupt any other process though it will run continuously.

This software is developed in JAVA.

1.3.8INTERFACE WITH SERVICES

Socket(can cancel this section if you want)

1.4 PRODUCT FUNCTION

1)Demonstrating DDoS Attack:

It will perform DDoS Attack on one node in the network where other attackers may also attack at same time.

2)DDoS attack

1)Detection: By analysing the packets coming on node, software will detect the attack

2)MitiGation: after analysing and detecting attack, there is a need to firewall the packets coming from ip address of attacker for short period of time.

1.5 USER CHARACTERISTICS:

1)Network Administrators

2)Cloud Networking

3)Independent Servers

4)Companies, institutions, etc

1.6LIMITATIONS:

1)To segregate attack traffic from legitimate user traffic.

2)To detect all types of attacks .

3)MAC Spoofing is difficult to handle.

4)DNS Spoofing will not be maintained

1.7ASSUMPTIONS & DEPENDENCIES:

1)Assume that attackers are distributed by IP Spoofing.

2)full internet connection

3)JAVA Gcc

4)Wireshark

5)Server system

1.8DEFINITIONS

1)DDOS ATTACK:

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic to a web property by distributed system.

2)DOS ATTACK:

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

3)IP Spoofing:

 IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of impersonating another computing system.

4)MAC Spoofing:

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device.

5)HTTP FLOOD ATTACK:

HTTP flood is a type of Distributed Denial of Service (DDoS) attack in which the attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application

6)TCP FLOOD ATTACK:

TCP SYN/ACK flood  is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.