Computer Networks Project Synopsis

Semi-Permeable and Flood Attack Detecting Firewall

Basics of Firewall and Flood Attacks

Firewalls

A firewall is a network security system designed to prevent unauthorised access to or from a private network.

Firewalls can be implemented in both hardware and software, or a combination of both.

Network firewalls are frequently used to prevent unauthorised Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

The project would mainly focus on the development of the software firewall.

Software firewalls are installed on your computer (like any software) and you can customise it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.

Flooding and Flooding Attacks

Flooding

Flooding is a simple routing technique in computer networks where a source or node sends packets through every outgoing link.

Flooding Attacks

Flooding is also used as a denial of service attack by flooding network traffic to bring down a network service. The service is flooded with many incomplete server connection requests. Due to the number of flooded requests, the server or host is not able to process genuine requests at the same time.

A flooding attack fills the server or host memory buffer; once it is full, further connections cannot be made, which results in denial of service.

There are many kinds of Flooding attacks such as UDP flood,SYN floods, DOS attacks etc.

Project Purpose

The project mainly focuses on the development of a semi-permeable firewall which would provide access to only the authorised clients and would reject unauthorised access requests. Along with it would detect a flood attack (mainly SYN flood) as and when the attack is attempted.

Technologies Used

C Language- For the socket programming and building the firewall.

Wireshark or Scapy - A packet analyser tool used to predict the number of packets in order to detect whether the attack is being predicted or not.

Python - For the programming of the GUI.

Network Requirements

Linux Environment

Network Switches (If required)

Routers(If required)

Team Members

Harshil Gupta (Roll No- 27)
Bhoomika Hasija (Section C)
Tuhin Khare (Roll No -9)