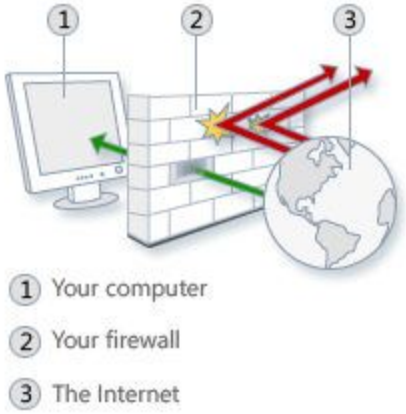
Firewall

Introduction

A firewall is a piece of software running on a system that isolates the trusted(internal-network) from the untrusted external network. It monitors incoming and outgoing traffic based on the predefined security rules. A firewall can work at any layer above the physical layer in the TCP/IP model. The firewall undertaken as the project here aims to implement major functionalities of a firewall(described below). The only difference is that rather than dropping(or blocking) any packets, it marks them as suspicious. This is because of the fact that to drop packets, a packet handling process should be running at kernel level inside a networking stack. This requires a high-level knowledge of writing kernel modules which is not feasible at for us at this moment.

Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.



The project will be developed in python language. Using a few famous libraries. Design details are described below.

Features

The firewall will provide following functionalities:

- Filtering any packets according to their IP address.
- Filtering any packets according to their ports numbers.
- Filtering any packets according to their Transport layer protocol.
- Filtering any packets according to their interfaces.
- Filtering any packets according to their MAC address.
- Filtering any packets according to a service (The service name mentioned should use a well-known port assigned by ICANN)
- Filtering DNS packets using a blacklist
- The firewall will provide a daemon interface.

Dependencies

The firewall be using following third-party dependencies to fulfill its tasks

- **Scapy**
  Scapy is a powerful interactive packet manipulation program. It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, match requests and replies. This tool provides the ability to sniff packets in real-time. It allows the developer to work with known protocol without the trouble of caring about minute details of the protocol.

Logging

The data is logged into the file named ‘/var/log/custom_firewall.log’. The settings can be changed from ‘config.py’ file.

PID File and Socket File

Pid file is stored under the name ‘custom_firewall.pid’ at location ‘/var/run’. In the same location socket file is stored under the name ‘custom_firewall.socket’.

Architecture