A Packet-Filtering Firewall WebApp

[1]Urvashi Dharne, [2]Vaishnavi Shivankar, [3]Dhiraj Balpande, [4]Satvik Sherekar, [5]Archana Bhade

[1,2,3,4]Department Of Information Technology, GCE Amravati, Maharashtra 444604, India

[5]Asst.Prof. Department of Information Technology, GCE Amravati, Maharashtra 444604, India

Abstract- The goal of this paper is to create a Packet-Filtering Firewall WebApp which can be deployed over a web-server to monitor the local network interface. Since there are several different network interfaces, we can select a particular interface to monitor all the data flowing through the interface by inspecting the packets that are being transferred into or out of the system by simply sorting them according to some pre-defined set of rules such as the source, destination, port number or the sequence number. This paper will thoroughly guide you on how exactly the sorting of packets works on network basis.

Introduction

Today's networks regularly change and evolve to accommodate new business situations such as reorganizations, acquisitions, outsourcing, mergers, joint ventures and strategic partnerships, and the increasing rate of internal networks being connected to the Internet. The resulting increased complexity and openness of the network makes the issue of security more complicated than before and requires the development of sophisticated security technologies at the interface between networks of different security domains, e.g., between an intranet and the Internet or an extranet. The best way to ensure interface security is to use a firewall. A firewall is a computer, router or other communication device that filters access to a protected network. Cheswick and Bellovin [2] define a firewall as a set of components or a system that sits between two networks and has the following characteristics:

- All traffic from the inside to the outside and vice versa must pass through it.
- Only authorized traffic, as defined in the local security policy, can pass through it.
- The firewall itself is immune to penetration.

A network works when number of packets are transferred from one computer to another computer via a medium (wired/ wireless). A typical packet looks like the figure (1) below –

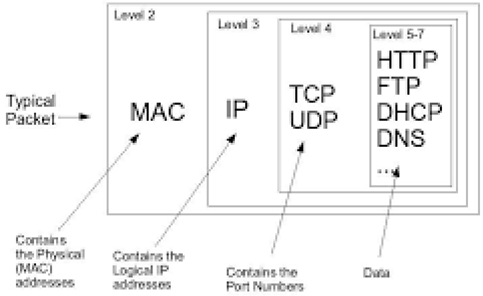
Typical Packet
Level 2
MAC
Level 3
IP
Level 4
TCP
UDP
Level 5-7
HTTP
FTP
DHCP
DNS
...
Contains the Physical (MAC) addresses
Contains the Logical IP addresses
Contains the Port Numbers
Data

Fig. – 1

In networks, a packet [3] is a small segment of a larger message. Data sent over computer networks such as the Internet is divided into packets. These packets are then recombined by the receiving computer or device.

A packet basically constitutes of the following components –

1. Header: -

   It is the part of the packet which contains all the necessary information such as the source, destination, port number, sequence number, etc.

2. Payload: -

   It is the part of the packet which contains the main data that needs to be transferred from one computer to another.

3. Tail: -

   It is the part of the packet which contains the data redundancy checks such as CRC, SHA256, MD5, etc.

These packets can be transferred over different network interfaces [4] and can be requested by different software and gets transferred according the Standard OSI-Model [5]. The OSI-Model is shown in the figure (2) below-

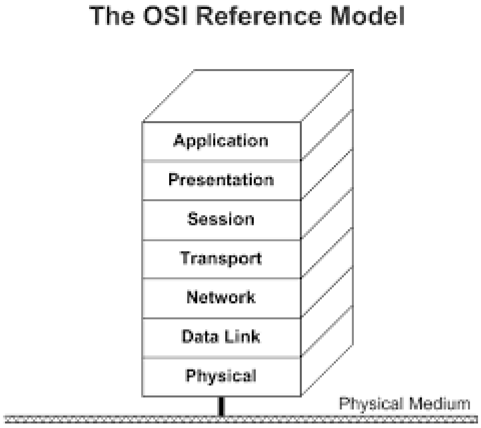

Fig. – 2

The network interfaces [4] can be termed as the communication points for the computer through which data is transmitted or received.

The different types of network interfaces [4] that work according to the OSI-Model are –

- MAC (Medium Access Control)
- IP (Internet Protocol)
  - IPv4 (Version 4)
  - IPv6 (Version 6)
- ICMP (Internet Control Message Protocol)
- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- DNS (Domain Name System)
- SSH (Secure Shell)

Methodology

1. **Workflow Diagram** -

   The following figure (3) shows the proper workflow of the intended program.

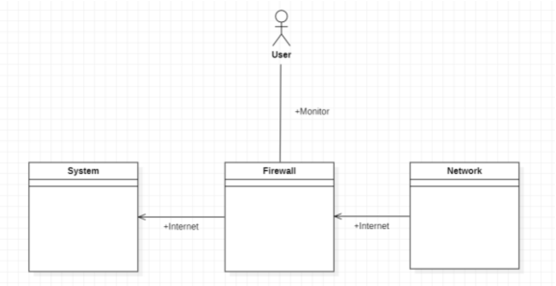

Fig. – 3

2. **Monitoring The Network** –

   We use the ‘psutil’ module from python to actively monitor the network at the first glance. Later we carry out the necessary actions according to our assumptions.

3. **Sorting The Packets** –

   We use a python module called ‘scapy’ [6] to sort the packets captured in the ‘.pcap’ file.

   We can sort the packets in various ways such as –

   - Source Address
   - Destination Address
   - Port Number
   - Sequence Number
   - Time

   This module uses the basic combination of ‘Merge Sort’ and ‘Insertion Sort’.

   The syntax for sorting is given below –

   sorted_packets = sorted(pcap, key=lambda x: x.time)

4. **Displaying The Sorted Data** –

   We make use of ‘Django’ Framework to create a dynamic website which can help us select the various network interfaces and display the needed data.

Conclusion

This paper proposes the design of a Packet-Filtering Firewall WebApp. This solely works on sniffing the packets and sorting them according to our needs and analyze the network.

Packet sniffing is a powerful technique for analyzing network traffic and extracting information from it. By capturing and analyzing packets, it is possible to gain an overview of the structure, behavior and vulnerabilities of network systems.

Python provides a flexible and powerful platform for packet sniffing using libraries such as ‘scapy’ that allow easy capture, manipulation and analysis of network packets. These tools can be used to perform a wide range of tasks, from detecting and analyzing network attacks to monitoring network performance and troubleshooting connectivity issues.

All in all, in today's fast-paced and connected world, the use of packet sniffing and Python-based tools for network analysis and monitoring is becoming increasingly important. As the volume and complexity of network traffic continues to grow, the need for effective and efficient packet sniffing techniques will only increase, making Python an essential tool for network professionals and researchers alike.

References

1. Abie, Habtamu. (2000). An Overview of Firewall Technologies.
2. W. R. Cheswick and S. M. Bellovin, Firewalls and Internet Security, Repelling the Wily Hacker, Addison-Wesley Publishing Company, 1994.
3. What is a Packet? | Network Packet Definition | Cloudflare. Available at: https://www.cloudflare.com/learning/network-layer/what-is-a-packet/
4. An Introduction to Networking Terminology, Interfaces, and Protocols | Digital Ocean (2023). Available at: https://www.digitalocean.com/community/tutorials/an-introduction-to-networking-terminology-interfaces-and-protocols
5. What is the OSI model? | Cloudflare (no date). Available at: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/
6. Welcome to Scapy’s documentation! — Scapy 2.5.0. documentation (2023). Available at: https://scapy.readthedocs.io/en/latest/

DOI: 10.55041/IJSREM19957