Personal Firewall Using Python

---

Abstract

This project, Personal Firewall Using Python, demonstrates how Python can be used to build a simple yet effective firewall on a Windows system. The firewall monitors active network connections, applies allow/deny rules using system commands, and gives the user greater control over which applications can access the internet. The project shows how Python can be leveraged to integrate system-level security with user-friendly control.

---

Introduction

A firewall is a security mechanism that filters incoming and outgoing network traffic based on predefined rules. Personal firewalls are particularly useful for individuals who want to protect their devices from unauthorized access.

This project implements a basic personal firewall using Python on Windows 10. It uses Python libraries to monitor connections and integrates with the Windows netsh utility to enforce security rules. Python was chosen due to its simplicity, flexibility, and extensive support for networking modules.

---

Tools Used

Python 3.x (programming language)

Windows 10 Home Edition (operating system)

Libraries: socket, psutil, subprocess

Command-line utility: netsh for applying firewall rules

---

Steps Involved

1. Environment Setup

Installed Python 3 on Windows 10

Verified pip and installed required libraries

2. Monitoring Active Connections

Used psutil and socket to fetch active network connections

3. Firewall Rules

Integrated with Windows netsh advfirewall to block or allow specific applications and ports

4. Testing

Ran applications to check which ones were blocked/allowed

Verified firewall rules were applied successfully

---

Conclusion

The project successfully demonstrates how Python can be used to build a personal firewall that allows or blocks applications based on user-defined rules.

Achievements:

Learned to integrate Python with Windows firewall

Built a simple, functioning personal firewall

Limitations:

Only basic allow/deny rules

Requires administrator privileges

Future Improvements:

Add a graphical user interface (GUI)

Implement logging of blocked/allowed attempts

Advanced packet inspection for deeper security

---

📌 End of Report