SSH Intrusion Detector
Report

Gary Khodayari
February 27th, 2022

Purpose

The SSH Intrusion Detector program is a simple monitoring application that will detect password-guessing attempts then call iptables script to block that IP on the base of username.

Requirements

Task	Status
Will monitor the /var/log/auth.log and detect password-guessing attempts then use iptables to block that IP	Implemented
Will get user-specified parameters then continuously monitor the log file specified.	Implemented
As soon as the monitor detects the number of attempts from a particular IP gone over a user-specified threshold.	Implemented
Application will flush the rule from Firewall rules set upon expiration of the block time limit.	Implemented
Design the system to test SSH Intrusion Detector	Implemented

Platforms

SSH Intrusion Detector has been tested on:

- Ubuntu 20 LTS

Language

- Bash script (WILL NOT WORK WITH SHELL)

Documents

- Design
- Testing
- User Manual
- The GitHub link