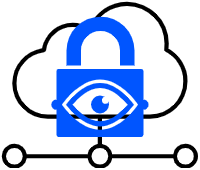
SSH Intrusion Detector

Report

Gary Khodayari

February 27th, 2022



[**Purpose**](#_erqf6cc0mwy3) **3**

[**Requirements**](#_i67my87iux23) **3**

[**Platforms**](#_79c42v75ayev) **3**

[**Language**](#_b09w09v20pc0) **3**

[**Documents**](#_pd8mtjyje9ia) **3**

# 

# 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](https://docs.google.com/document/d/1UgzGO7_8WykZgQOdwCeiXYXXF-IRlMPa2QXLsHwcR_M/edit#heading=h.ruvzfmj54yve)
* [Testing](https://docs.google.com/document/d/1O-6aVtDoS7y3dOlSLjy-UW34zzA28VlKv_qL0ks0vXw/edit#heading=h.ruvzfmj54yve)
* [User Manual](https://docs.google.com/document/d/1JLMY_bq4Fr3KnSHzlwp2mpi97TC6vCcAdw7uFq-9xRQ/edit)
* [The GitHub link](https://github.com/d0ntblink/g8keep3r)