SSH Intrusion Detector
User Manual

Gary Khodayari
February 27th, 2022

Requirements:

iptables
ipset
bash
ssh

Optional:
git

Initial Setup:

Please make usre to run before executing this script
apt update && apt upgrade

You can update the newest version by cloning https://github.com/d0ntblink/g8keep3r
repository

git clone https://github.com/d0ntblink/g8keep3r
git fetch && git pull

Warnings:

Please keep in mind if the location of the script has moved, this application will stop working properly.

This program must be uses with root privileges.

You will only to run the g8keep3r script, parser is just a helping script

In case the program is misbehaving, please reset crontab and then try again.

This program will not work properly if its not ran by bash. Shell and kornshell will not work.

Usage:

If you don't use chmod to give executive rights to this program, you will need to add bash to the biggening of every command

Get help:
./g8keep3r –help

Output:
use --help to display this message
Correct Usage:
  g8keepr --add <username> <maximum failed attempts in 1 minute allowed> <timeout durations in seconds>
  g8keepr --remove <username>

adding a new user to the watch list:

  g8keepr --add <username> <maximum failed attempts in 1 minute allowed> <timeout durations in seconds>

example:
./g8keep3r.sh --add testuser 4 100

removing an exiting user in the watchlist:

  g8keepr --remove <username>

example:
./g8keep3r.sh –remove testuser