**Computer Systems Technology**

British Columbia Institute of Technology

COMP 8006 - Assignment3- How-to

Albert Huang &

Aiyan Ma

Feb 20, 2018

# Table of Contents

[Table of Contents 2](#_Toc813833444)

[1. Config the Monitor by hard code 3](#_Toc631476044)

[2. Config the Monitor in GUI 4](#_Toc208200676)

[3. Running the Monitor 5](#_Toc41015193)

# Config the Monitor by hard code

1. Ensure you are running the terminal as root.
2. Set variables key words for filter information from log file; for example:

Keywords=’Failed password’



1. Set variable ip by using awk, set field number; for example:

fieldNo=13 (if you are trying to monitor secure file , this value should be 11)



1. Set variable target ip by using regular expression: set regular expression switch and pattern.

Regx\_on=1 (0 means off, 1 means on)

Ex='[0-9]+(\.[0-9]+){3}'



1. Set variables attempt times, blocking time, log file path and service port number and run:

#./monitor.sh -set 3 30 /var/log/secure 22

This command set :

attempt time = 3;

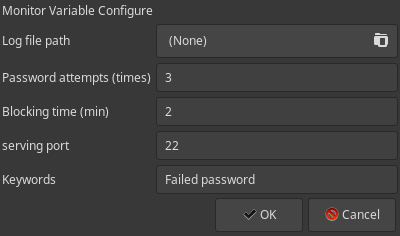
blocking time = 30 min;

log file path = /var/log/secure;

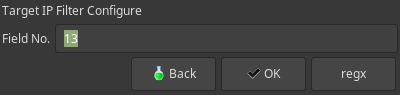
service port number = 22 (ssh service)

# Config the Monitor in GUI

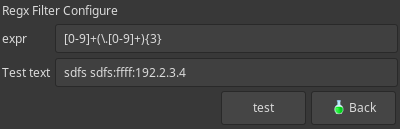
1. Set vary information which including attempt times, blocking time, port number, key words etc; see below



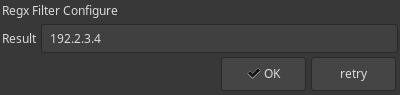
1. If use awk to get the target ip, input field number:



1. Set regular expression to get target ip, click regx button on above dialog then you will see:



The expr is regular expression pattern; the second line is testing text for you to try if your pattern works or not; for example click button test:



It works! This pattern catch the ip part from the line!

# Running the Monitor

1. Ensure the file has executable permission by the root user with the command:

**#chmod 755 monitor.sh**

**#./monitor.sh -gui**

1. Ensure you already installed yad, if not, run the command below:

**#dnf install yad**

1. Input the following arguments while executing the file:

**#./monitor.sh [ -set | timelimit | -gui ]**

1. Arguments list:

**-set**  //start in command line interface

**timelimit** //call to clear a firewall rule and cron task

**-gui //**start gui for user