Computer Systems Technology

British Columbia Institute of Technology

COMP 8006 - Assignment3- Design

Albert Huang &

Aiyan Ma

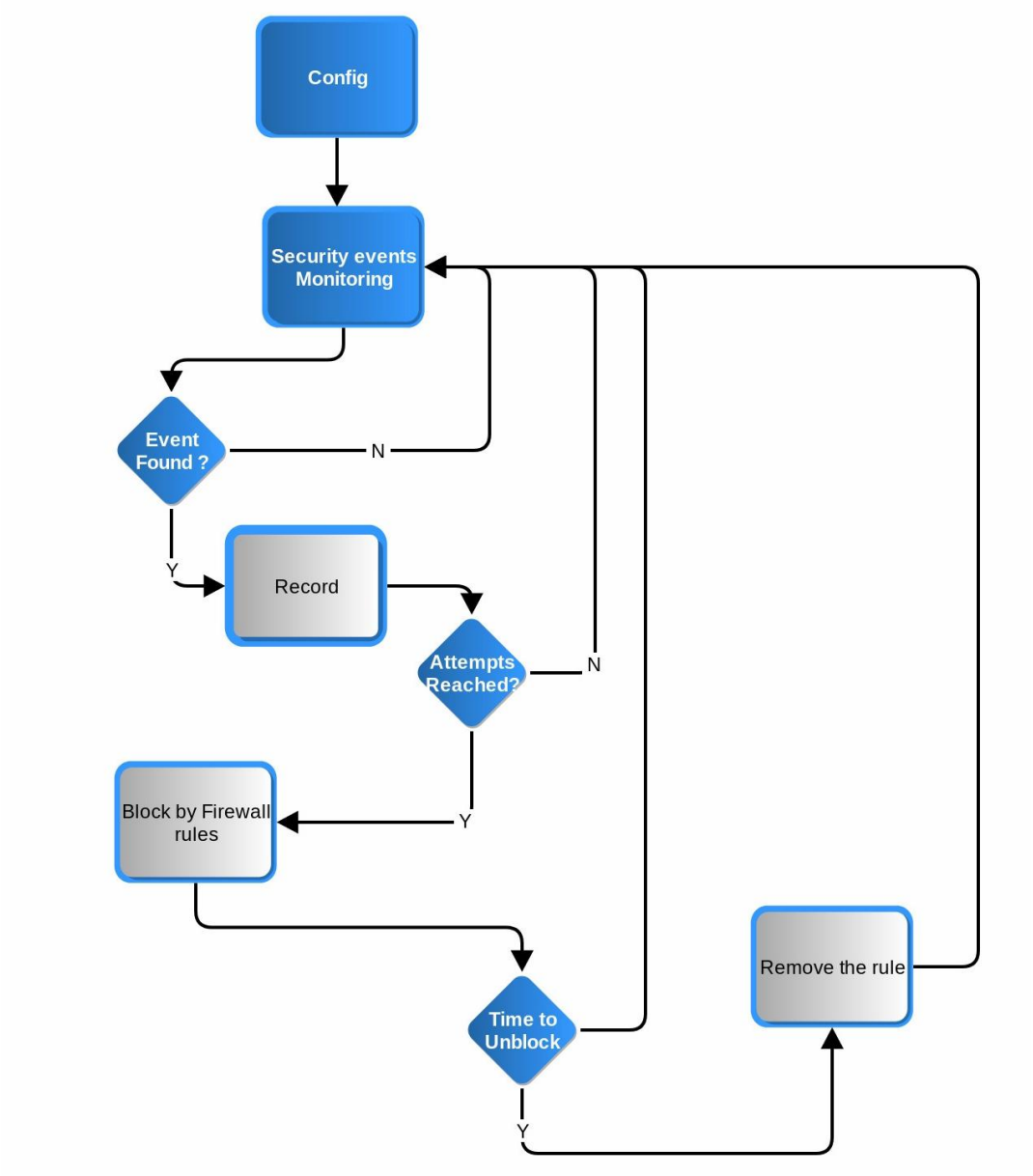
Feb 20, 2018

Table of Contents

Design

1.1 Main Flow

1.1.1 Flowchart



1.1.2 Description

1. Setting vary variables of in configure session

2. Monitoring dynamically to get the incremental part of the logs

3. Make the analysis for the sensitive words are in or not

Read each new line of the log file and compare with the keywords, if find one then go down ,if not continue search.

4. When the critira triggered, the client IP, times attempted is recorded.

While after program get target ip, manage the data into array

5. When the threshold reached, the blocking action will be taken by using iptables rule.

While attempt time reach threshold, in this case, the program will block the connection when asked by the monitor module. It calls the *iptables* to setup the rule to indeed take the action.

6. When the blocking time passed, the unblock action will be taken by using crontab task.

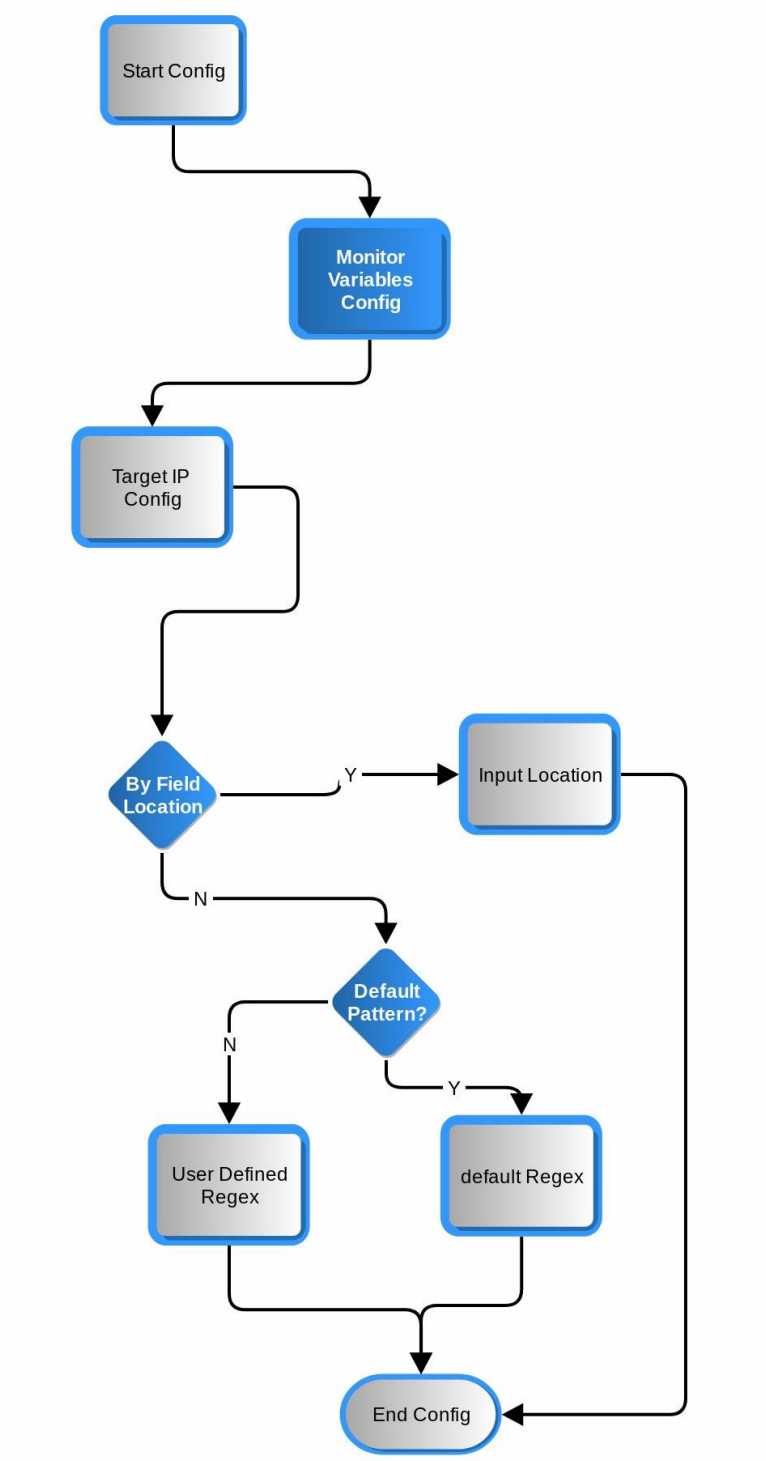
Unlbock is triggered automatically by crontab when the time limit is reached. When it's time to unblock, the crontab job is cleared and the rules on the firewall is removed to allow the access again.

7. During the whole time, the program maintaining an Array as blacklist.

Program using adding, deleting and updating functions to make the array data accurate and in time.

1.2 Configure Flow

1.2.1 Flowchart



1.2.2 Description

1. Program provides both GUI and command line user interface for user to input and configure the required parameters

Program supply a gui by using yad, it allow user input variables easier than command line interface. User can play with it even they never read how-to

2. Setup the monitor variables

Set most of the variables in here beside target ip related variables.

3. IP address Handling by using awk

Program default ip capture method is by location(fields number of the record in the log file). The only thing user need to input is the field number. It's easy and works for some log. While this method is not fit for every log, it is too much straight forward. Sometimes the part contain ip information is complex, it mixed with other characters.

4. IP address Handling by using regular expression

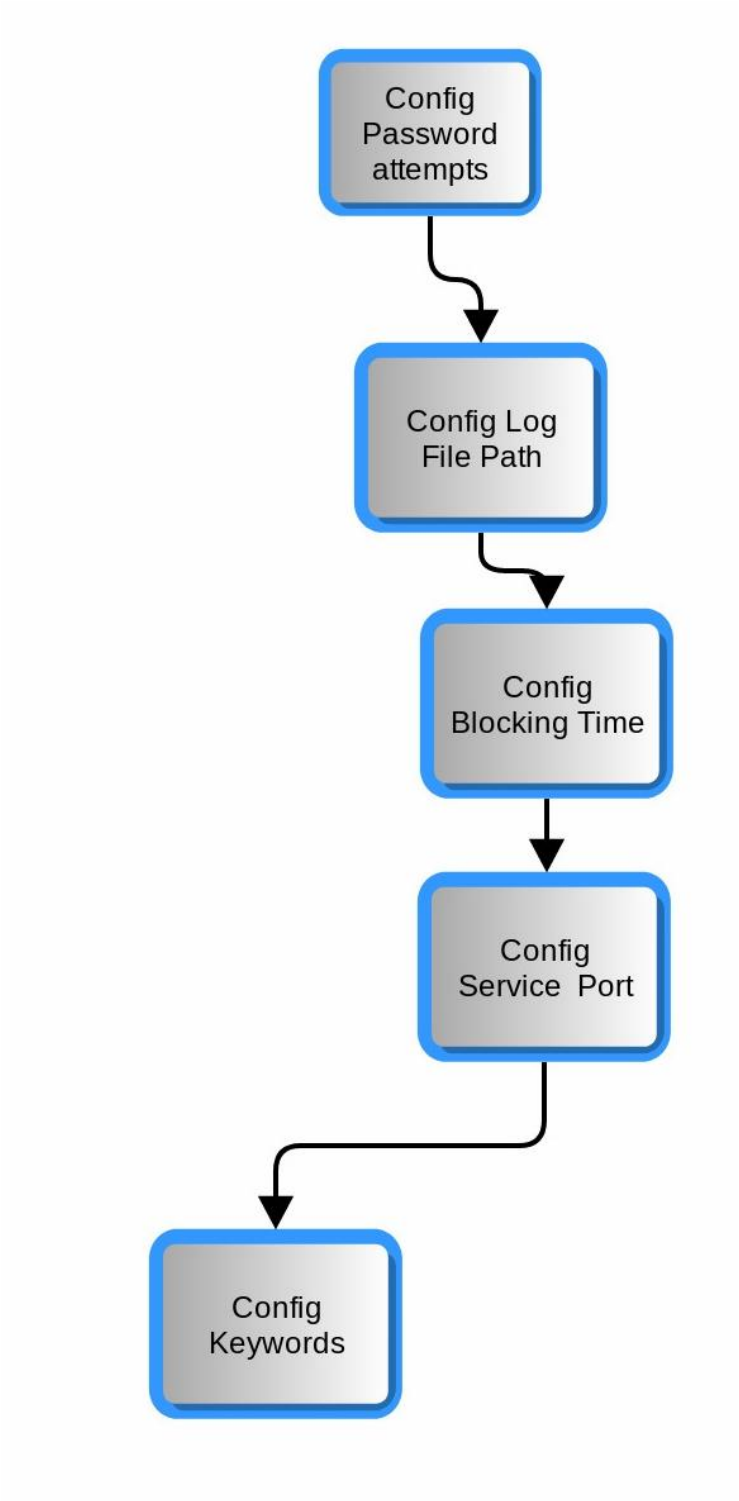
As an alternative ip capture method, it is by regular expression. It also very nice to provide a system default pattern can be applied for almost all the cases. Of course, user defined patterns also supported. User will asked to input a regular expression to match the keywords.

5. Regular expression tester

Due to the error pron design, a test (verify) function is provided for end use to test the pattern before really applied in it.

1.3 General Variables Configure Flow

1.3.1 Flowchart



1.3.2 Description

1. Set attempt times as a threshold to measure if trigger any action

2. Set Log file path to make sure which file will be analyzed

3. Set blocking time to make sure how long the blocking action would last if triggered

4. Set service port number to specify the service it monitored

5. Set keywords which is used to find the password attempt information