

PASSWORD GUESSING MONITOR USER MANUAL

COMP 8006

SPENSER LEE A00925785

THOMAS YU A00915638

Contents

About the Password Monitor..... 3

How to use..... 3

About the Password Monitor

This project was broken up into two separate executable files. One is the log-monitor, which is a console application that is responsible for monitoring a file like /var/log/secure for ssh login attempts. If more than a user specified number of failed login attempts occur, the log-monitor will block that IP for a user specified amount of time.

The second executable is a GUI application that can be used to control the log-monitor. It will call the log-monitor and pass in any user variables, as well as monitor the output files from the log-monitor to update a table of the IPs that attempt to login to the host machine.

How to use

Each application must be run as root.

To run the log-monitor application:

```
./log-monitor <log-file> <allowed-attempts> <reset-hr> <reset-min> <block-hr> <block-min>
```

For example:

```
./log-monitor /var/log/secure 3 0 1 0 5
```

The previous example will monitor the secure log file, and allow 3 login attempts before blocking the IP for 5 minutes. It will reset the attempt counter after 1 minute of no login attempts.

To use the GUI application, **each executable must be in the same directory.**

If there is already a log-monitor running, it will grab the current settings and update as necessary in the UI.

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	Attempts Reset	ssh	0	08:24:26 pm
2	192.168.0.6	Connected	ssh	1	08:26:18 pm
3	192.168.0.5	Failed Attempt	ssh	1	08:26:23 pm