3/2/2016

COMP8006 Assignment 3

Design Document

Rizwan Ahmed

Vishavpreet Singh

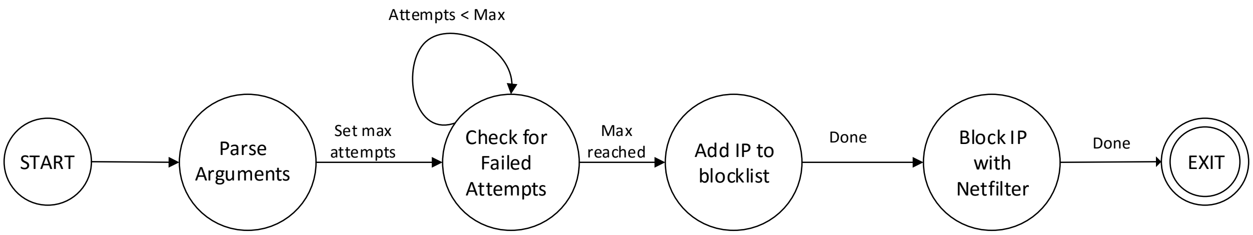
COMP6D

Design

The IPS will be activated through the crontab periodically.

The IPS will first parse arguments from crontab for the maximum number of allowed attempts before blocking an IP address. The IPS will then use terminal commands to create a file containing a list of failed password attempts from the /var/log/secure file. The list of failed password attempts is sorted by IP addresses. The IPS will track the number of attempts for each IP address. If the number of attempts exceeds the limit, the IPS will then use Netfilter to block that IP address indefinitely. A list of banned IP addresses will be written to another file.

Finite State Machine



Name	Description
Start	The script executes through cron
Parse Arguments	Get maximum number of attempts from arguments
Check for Failed Attempts	Read from file of failed attempts and track number of attempts for each IP if they exceed the maximum limit.
Add IP to block list	Add IP address to file containing list of blocked IPs
Block IP with Netfilter	Use iptables to block IP indefinitely
EXIT	The script terminates execution

Pseudocode

Main – entry point

```
Script is executed by cron
Write failed attempts from /var/log/secure to a file
Count attempts for each IP address
Add the IP’s to a file with a list of blocked addresses
Use iptables to block IP addresses exceeding maximum attempts
Exit
```