User Guide

Eric Tsang & Manuel Gonzales, 6D

1 Table of Contents

March 2, 2016

2 Configure setjob.sh

This section describes how to configure setjob.sh for your environment:

1. Open `setjob.sh` with your favorite test editor:

```
# gedit setjob.sh
```

2. Configure the variables to your preferences in the user-configurable section located near the top of `setjob.sh`.

3 Deploying the IPS via setjob.sh

This section describes how to deploy the IPS system, then verify that it is working (before deploying the IPS, make sure that `setjob.sh` has been configured. Setting up setjob.sh is described in section 2 of this guide):

1. Make sure there is no previous `crontab` entry for running `ips.sh`; enter the following command into a Terminal:

```
# crontab -r
```

2. Make sure that the database file referred to in `setjob.sh` is completely empty, or does not exist. If one exists, delete it, or delete all of its content.
3. Make sure there are no previous firewall rules from any previous instance of the IPS in `iptables`. Execute the following commands into a Terminal:

```
# iptables -X
# iptables -F
```

4. Run `setjob.sh` to deploy the IPS; enter the following commands into a Terminal:

```
# setjob.sh [path/to/log/file] [max allowed attempts] [ban
duration in seconds]
```

5. Verify that the IPS is running by checking that the archive log specified in `setjob.sh` exists, and is updated every minute or so.