1.3 Minimal Ubuntu Linux Security Checklist

Introduction

Outlined here are the minimal security steps the Bonsai Framework uses in server builds.

Disable Direct Login as Root Through SSH

On a fresh Ubuntu setup from scratch the default values in your /setch/ssh/sshd_config is,

```
PermitRootLogin prohibit-password
```

This prevents password and keyboard-interactive authentication using the root account. However, if in a hardened environment we prefer root to not be available at all.

In this example, we are using a canned **hosted** Ubuntu system where the automated setup has the root account is enabled. This is dangerous because there are attackers out there looking for Unix/Linux boxes and trying to login via ssh using the username root and then a list of common passwords.

> I do not like disabling the root account as this might break the hosted Ubuntu setup. For example, Slice's or Rackspace special terminal console login might stop working. In any event, the vector of attack is SSH login. To prevent users from using root, well don't provide the root password and provide sudo privileged accounts as shown in this article.

Connect to SSH as a staff user and edit sshd_config,

```
sudo nano /etc/ssh/sshd_config
```

Search for the line **"PermitRootLogin yes"** and change to **"PermitRootLogin no"**. You can still issue su to go in as root but only after logging in as a user belonging to the admin group.

Last restart the SSH service for the changes to take effect.

```
sudo service ssh restart
```

In older versions of Ubuntu (to determine) where Upstart is not available use,

```
sudo /etc/init.d/ssh restart
```

Install Fail2ban

Install fail2ban to prevent brute force attacks.

Switch to SSH Key Authentication

If you system is on the Internet, switching to SSH key authentication this is a must do step.