SEC 150 Midterm Project: Securing Web Servers with SSL

Titus Barik (tbarik@staff.waynecc.edu)

Version 1.4

1 Project Description

In this assignment, you will use the Tiny Core Linux distribution to create a virtual machine that hosts a secure web server and delivers some simple static content. The web server for this project will be the popular `lighttpd`.

Upon completion of this project, you will be able to generate an SSL certificate, install and configure `lighttpd`, and gain further familiarity with working within the Linux operating system.

Because this is a project, rather than an assignment, you are expected to discover and learn about much of the system on your own. Therefore, several assumptions may have been made and not every step is explicitly written out. You should therefore actively use the Discussion Board to seek clarification when needed.

2 Pre-Requisites

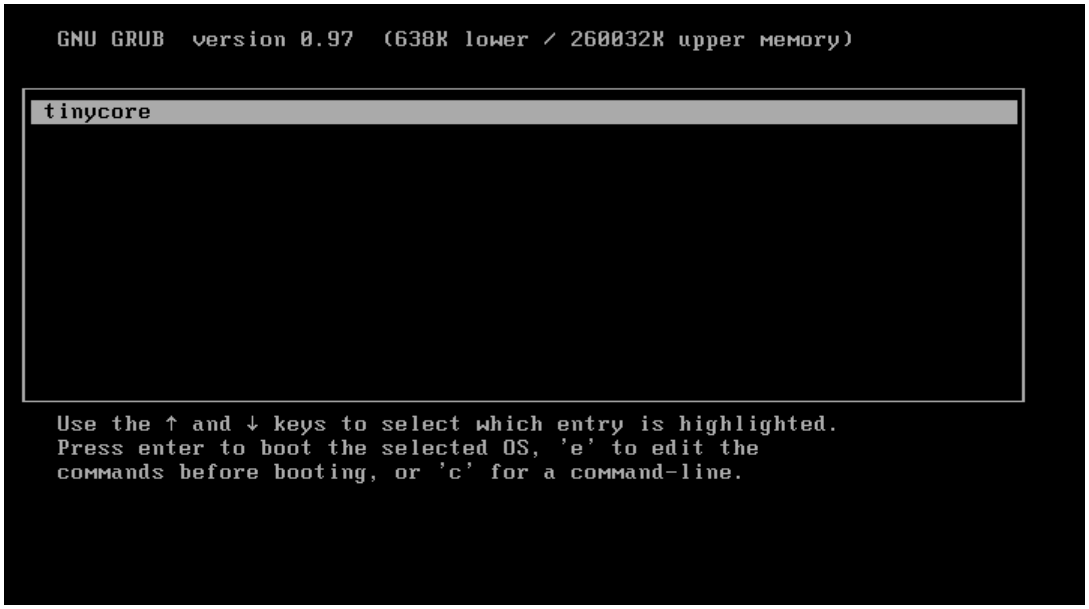
Before starting this assignment, you will need VMWare Player or VMWare Workstation. You will also need to download the Tiny Core ISO file (`tinycore_3.5.iso`).

3 Instructions

1. Create a virtual machine for your Tiny Core system. Create a virtual IDE (not SCSI) hard disk with approximately 100 MB of disk space (0.1 GB). Follow the Tiny Core Installation instructions to create an actual bootable installation, instead of a Live CD image (we want changes to be persistent).[1] Note that you may have to reboot after running the `cfdisk` command, though the instructions don't mention this key step.

[1] `http://distro.ibiblio.org/tinycorelinux/install.html`

2. After setup, you may wish to go into VMWare and ensure that Tiny Core is not inadvertently booting from the CD. You will know that you have (likely) followed the installation instructions correctly if you get to the GRUB boot screen instead:



3. Install the `lighttpd` package using the Apps tool. You may also need to install the OpenSSL package. If you are not comfortable using the `vi` text editor, you will also want to install `nano` at this point.

4. Create a directory called `/mnt/hda1/tce/midterm`. This directory will contain **all** of your files for the project.

5. Within this directory, generate RSA keys and a self-signed SSL certificate using the OpenSSL Keys HOWTO[2] and the OpenSSL Certificate HOWTO[3]. When generating the certificate, fill in the details with your information (such as your e-mail address).

6. For `lighttpd`, you will need to combine these files (the documentation doesn't mention this) using `cat privkey.pem cacert.pem > host.pem`. You will then use `host.pem` in your configuration.

7. Create a folder within midterm called `www`. This folder should contain a simple text file such as `index.txt`. The contents of this file will be your name.

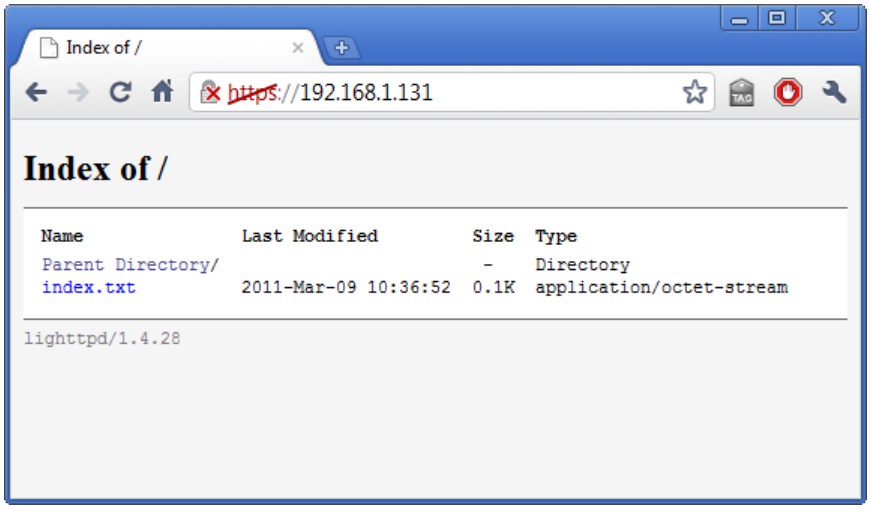
8. Using `nano`, or another text editor, create an `httpd.sh` script file, and then add support for SSL. To do this, see the Configuration section of How to Install SSL.[4] Be sure you include the `server.dir-listing` option as well. Remember that SSL uses port 443, not 80.

[2] `http://www.openssl.org/docs/HOWTO/keys.txt`
[3] `http://www.openssl.org/docs/HOWTO/certificates.txt`
[4] http://redmine.lighttpd.net/projects/1/wiki/Docs:SSL

9. Finally, start your server with the following command: `sudo sh httpd.sh`.

10. If you have done everything correctly, you should see a message such as `(log.c.166) server started`. Be aware that this is not a true background service at this point; hitting CTRL + C will kill the process.

11. You can now determine your IP address by opening a terminal and typing `ifconfig`. Open a web browser and navigate to `http://192.168.1.131` (replace 192.168.1.131 with your actual IP address). Your browser will complain that the certificate is untrusted; this is okay, as your connection is still encrypted (recall that verification and encryption are two different issues). Accept the certificate and you will be presented with a screen similar to the following:



12. Congratulations, you've successfully completed the midterm project!

4 Milestone

Submit a screen capture that shows what you've completed so far.

5 Submission

Submit all of your files as a single zip archive using Dropbox (unless you have personally made other arrangements with me). This archive should contain your entire VMWare image directory. Under Moodle, post the URL of your Dropbox location, as well as a file called `md5.txt` containing the MD5 signature of your zip file. This is to prevent tampering after the deadline.

Students are encouraged to help each other; please post issues to the Discussion Board.