

嵌入式网络安全实验平台用户手册

计算机系 55 班 席照炜 学号：2015011354， E-mail:xizw15@mails.tsinghua.edu.cn

计算机系 55 班 毛宇飞 学号：2015011364， E-mail:maoyf15@mails.tsinghua.edu.cn

计算机系 55 班 徐韧喆 学号：2015011350， E-mail:xrz199721@126.com

目录

一 嵌入式网络安全实验平台概述	2
二 网站访问使用	2
(一) 整体结构	2
(二) 主页	2
(三) 终端主页 & 题目页	3
三 增加题目	3
(一) 搭建对应题目网页	3
(二) 在服务器上部署	4
(三) 在网站上显示	5
四 举办竞赛	6
五 增加终端	6

一 嵌入式网络安全实验平台概述

嵌入式网络安全实验平台（以下简称平台）是基于多个 Intel Edison 小型嵌入式系统设备（以下简称终端设备）的用于网络安全实验及 CTF 竞赛的实验平台。目前由一台路由器和三台终端设备构成。其中网络框架为：

- 路由器：搭建局域网环境，让所有终端设备通过路由器接入公网，避免终端设备较多时过度占用 ip 资源。
- 主服务器：其中一台终端设备作为主服务器，部署网站主页，用于接收其他终端设备的 ip 心跳包，实现对于网络中所有可用终端设备的监听。
- 其他终端设备：其他终端设备部署终端主页和题目页面，每一个终端设备上可以部署多道题目，其他终端设备向主服务器发送 ip 和当前时间，用于验证登录，实现实时更新；题目的部署通过终端主页进行协调、展示和访问。

二 网站访问使用

主服务器使用固定 ip 地址 192.168.1.2，主页的端口号为 7070。想要访问的设备接入 NET-GEAR62 网络（密码 12345678）后，直接访问 <http://192.168.1.2:7070> 即可。其他终端设备则采用动态分配 ip 的模式，在接入网络后向主服务器发送心跳包，报告自己的 ip 和状态，使得主机知道当前有哪些设备接入了网络，且他们的 ip 都是多少。

（一） 整体结构

网站主要分为三层结构：主页，终端主页，题目页。主页部署在主服务器上，而终端主页及题目页部署在其他终端设备上。

（二） 主页

主页主要包括以下几个部分：

- Term：当前网络中所有可用终端，显示终端上的题目集合。

- **Contest** : 目前已有的相关比赛, 显示某一比赛中的题目集合, 目前由于题目数量少, 因此直接定向到不同终端上的所有题目, 在题目增加后允许设置部分题目显示。
- **Develop** : 帮助文档链接, 不仅是帮助用户使用网站, 更多的是帮助开发者了解如何在网站实现上传题目等操作, 包括 `answer problems`、`add problems`、`hold contest`、`add term` 等四个帮助文档。
- **Contact** : 其他联系信息, 包括项目介绍, 作者信息等其他网站相关信息。

(三) 终端主页 & 题目页

终端主页包含所有部署在该终端设备上的题目, 以列表的形式展现所有题目的名称、类型、端口号等信息。

题目页包含题目的题面、提示、下载链接、以及服务访问端口等, 大部分题目通过 `flag` 来判断题目是否做对, 有专门的 `flag` 检查服务, 像 `XSS` 这样的题目则有专门的判定机制, 来判断是否正确。

提交时需要先以某个用户名登录, 则提交结果正确与否保存在该用户名下, 正确时显示“you have solved this problem”。

三 增加题目

增加题目相当于新增一个题目页面。

如果作为开发者, 想要将自己的题目上传到网站上, 主要流程分为三步:(1) 搭建对应题目网页;(2) 在服务器上部署;(3) 在网站上显示; 为了实现增加题目, 请联系管理员获得终端的访问权限(在此, 一台主服务器和两台终端的密码均为 `edison123`)。访问方法为 `ssh root@192.168.1.X`, 然后输入密码, 即可登录到服务器或终端。

(一) 搭建对应题目网页

想要部署题目, 首先需要编写符合规范的网页。当然不符合规范也是可行的, 但需要对于配置环境和配置文件做更多的修改。

已有样题放在/usr/share/apache2 中，可以下载查看相应内容。以 index.html/index.php 作为网页的主页，文件打包在 prob 文件夹中，文件的组织方式为：

prob

index :

index.html/index.php : 网页的主页

other files needed to be visited by index.html/index.php

header.php / footer.php : 使用网站样题风格的页首页尾，符合网站的风格和相应功能，在template中，使用时利用<?php require_once("header.php/footer.php")?>加在index.html/index.php的开头/结尾即可

LogIn.php / LogOut.php : 实现在页首中的用户系统的配套支持服务，在template中

CheckFlag.php : 如果题目希望以flag的方式检验做题的正确性，可以直接使用CheckFlag.php，将正确答案存放在flag.txt中

css/js/images : 在相关服务中使用到的资源存储在template中，如果使用相关服务，也请将这些文件夹一并加入题目文件夹中

(对于想使用的上述资源，在template文件夹中，建议以软链接的方式拷贝，而非直接硬拷贝)

start.sh : 支持简易用户系统和自带CheckFlag.php服务判定的脚本，可从样题中拷贝，如果题目有需要开启的服务，也请将指令写在start.sh中，/usr/share/apache2/start_term.sh会检查start.sh脚本的存在并执行，且start_term.sh是开机自启动的。

other files needed by the problem

服务器终端使用 apache 引擎，支持 html+css+js+php 的基本设置，其他复杂框架并未安装，我们配置了简单的 python 环境，可以运行 python 脚本，因此请保证网页的开发符合服务器终端的设置。

实现后请使用 rsync 将对应题目上传到对应终端的/usr/share/apache2 路径下。指令的格式如下：

```
rsync -avz --progress ./prob root@192.168.1.X:/usr/share/apache2
```

在全部部署完毕后请手动调用一次/usr/share/apache2/start_term.sh，来完成相应配置和服务开启。

(二) 在服务器上部署

在完成了题目网页的搭建后，我们需要进行部署。首先打开/etc/apache2/httpd.conf 文件，找到端口监听部分，选择一个未被使用的端口，加上 Listen 该端口的设置。

再打开/etc/apache2/extra/httpd-vhosts.conf 文件，添加对于该端口网页的相关配置，可以参考

每台终端上已有的样题的配置：

```
<VirtualHost *:7074>
    DocumentRoot "/usr/share/apache2/prob4/index"
    ServerName localhost:7074
    ProxyPassMatch ^/(.*\.php(/.*?))$ fcgi://127.0.0.1:9000/usr/share/apache2/prob4/index/$1
    <Directory "/usr/share/apache2/prob4/index">
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
    </Directory>
    <Files ~ "\.py">
        Deny from all
    </Files>
    <Files ~ "\.txt">
        Deny from all
    </Files>
</VirtualHost>
```

主要需要配置资源文件的寻找路径，php 解释器的执行路径，端口的执行路径等路径，以及一些权限设定。

在完成上述配置后运行 `/usr/sbin/apachectl restart` 来刷新 apache 的配置更改。

（三） 在网站上显示

在完成了上述配置后已经可以通过 url 进行访问了，最后修改 `/usr/share/apache2/term_index` 中的 question 文件，question 的文件格式为：

```
port*/name*/type
```

即分别是题目的端口号，题目名，以及题目类型，将新增题目的信息加上，刷新终端主页界面题目就会出现。

四 举办竞赛

举办竞赛相当于新建一个题目集合。目前的显示是与终端相同的，但与添加新终端不同之处在于使用已经配置好的终端，省去了终端配置的过程。

首先需要将所有题目部署好，按照上述方法使得能够通过 url 访问。

其次是 term_index 文件夹，实现了终端主页。其文件结构为：

term_index：

css / js / images：用于终端主页的资源文件

header.php / footer.php：用于页首和页尾的php文件，和题目页的略有不同

LogIn.php / LogOut.php：用于用户系统登入登出的php文件，和题目页相同

question：用于存储题目信息的文件

index.php：主页

因此最简单的配置方法是按照复制 term_index，再按照添加题目页的修改配置方法，部署终端主页到某端口，最后修改 question 信息为想要展示的题目信息即可。

五 增加终端

如果开发者有新的完全相同的 Intel edison 嵌入式设备，为了使得它能够正常接入网络，除了举办比赛中的相关操作外，首先需要进行环境的搭建和配置。在我们拿到板子的时候已经进行了一些预配置，于此相关的内容请参考老师给出的参考资料。以下是我们对已有的两块板子做出的进一步配置。

首先需要将实验平台用 usb 线连接电脑，使用官网上提供的软件控制平台连接向一个 Wi-Fi，编写一个自启动脚本，这是我们的配置：

```
#!/bin/bash
systemctl enable wpa_supplicant
wpa_supplicant -B -Dnl80211 -iwlan0 -c/etc/wpa_supplicant/wpa_supplicant.conf
busybox udhcpc -i wlan0
source ~/.bashrc
/usr/share/apache2/start_term.sh
```

然后将这个脚本设置成开机自启动的，即在终端运行如下命令：

```
cp mystartup.sh /etc/init.d/  
update-rc.d mystartup.sh defaults
```

接下来需要将 `start_term.sh`、`update_ip.py` 拷贝到平台 `/usr/share/apache2` 文件夹下,其中 `start_term.sh` 会自动扫描文件夹下 `prob*` 的文件,启动其中的服务,创建运行每道题和配置平台必需的文件;
`update_ip.py` 是发送心跳包的脚本。

最后按照前面章节所述,配置好 `term_index`、题目和 Apache 服务即可。