# 实验八:HTTP 协议分析

### 一、实验目的

- 1、了解 HTTP 协议;
- 2、理解 HTTP 协议的基本内容;

3、理解 HTTP 协议的通信过程。

#### 二、实验学时

2 学时

#### 三、实验类型

综合型

# 日四日本

# 四、实验需求

# 1、硬件

每人配备计算机1台,不低于双核CPU、8G内存、500GB硬盘。

### 2、软件

推荐 Ubuntu Desktop 操作系统,安装 Wireshark 抓包工具。 支持 Windows 操作系统,安装 Wireshark 抓包工具。

#### 3、网络

计算机使用固定 IP 地址接入局域网,并支持对互联网的访问。

# 4、工具

无。

#### 五、实验任务

- 1、通过 Wireshark 分析 HTTP 报文结构;
- 2、使用 Wireshark 分析 HTTP 协议工作原理;
- 3、使用 Wireshark 分析 HTTPS 协议工作原理。

# **六、**实验内容及步骤

### 1、HTTP 协议报文结构分析

(1) 获取数据报文

①打开 Wireshark, 在【Filter】选项中输入报文过滤条件:http contains "http://www.51x ueweb.cn",(注意冒号后面的引号为英文输入模式输入),选择【Start】,开始进行报文采集。

②打开浏览器,在地址栏中输入"http://www.51xueweb.cn",进行网页访问。

③在 Wireshark 的抓包窗体中,查看已获取的 HTTP 协议的数据报文。

(2) 数据报文分析

选择**任意一个 HTTP Get 请求报文**,对获取到的 HTTP 协议报文内容进行详细分析, 并填写表 8-1。

> (注意: HTTP Get 请求报文截图,填写下表之后保存成图片,共需要提供2张图片) 表 8-1 HTTP Get 请求报文分析

序号	字段名称	字段值	字段含义
1	<b>Request Method</b>		
2	Request URI		
3	<b>Request Version</b>		
4			
5			
6			
7			
8			

● 请自行填写不少于 5 个头部字段名称,以及该字段名称的值,并说明该字段的含义。

选择**任意一个 HTTP Get 响应报文**,对获取到的 HTTP 协议报文内容进行详细分析, 并填写表 8-2。

(注意: HTTP Get 响应报文截图,填写下表之后保存成图片,共需要提供2张图片)

表 8-2 HTTP Get 响应报文分析

序号	字段名称	字段值	字段含义
1	<b>Response Version</b>		
2	Status Code		
3	<b>Response Phrase</b>		
4			
5			
6			
7			
8			

• 请自行填写不少于5个头部字段名称,以及该字段名称的值,并说明该字段的含义。

#### 2、HTTPS 协议通信过程分析

(1) 获取数据报文

①打开 Wireshark, 在【Filter】选项中输入报文过滤条件"ip.addr == 211.69.33.161",
选择【Start】,开始进行报文采集。

②打开浏览器,在地址栏中输入 https://internet.hactcm.edu.cn/Templates/internet/Images/ header-logo-pc.png。为了方便分析,仅通过 HTTPS 协议访问一个单一的图片文件,进行网 页访问。访问到图片内容后,随即**关闭浏览器窗口**。

注意:本步骤要完全实现从连接建立到连接断开的全过程。建议发送请求时,关闭所有 的浏览器和页面,确保不产生多余的 HTTP 报文。

③在 Wireshark 的抓包窗体中,停止报文采集,查看已获取的 HTTP 协议的数据报文。 (2)通信过程的数据报文分析

请分析 HTTPS 方式访问一个单一图片的过程,并将通信过程填写到表 8-3 中。

(注意: Wireshark 中 TCP 连接界面截图,填写下表之后保存成图片,共需要提供2张图片)

No.	Time	Source	Destination	Protocol	TCP 连接阶段

表 8-3 HTTPS 访问一个单一图片的通信过程

#### ● 行数不够可以自行添加。

● TCP 连接阶段请填写: TCP 建立连接、TCP 连接释放、数据传输等。

(3) HTTP 和 HTTPS 通信报文对比分析

对比上述两个任务获取的 HTTP 和 HTTPS 通信报文,分析 HTTP 和 HTTPS 通信获取的报文存在的不同点。

# 七、实验考核

#### 1、任务说明

(1) 使用 Wireshark 分析 HTTP 报文结构;

- (2) 使用 Wireshark 分析 HTTP 协议工作原理;
- (3) 使用 Wireshark 分析 HTTPS 协议工作原理。

#### 2、任务要求

要求 1: 使用 Wireshark 完成 HTTP 报文分析;

要求 2: 完成 HTTP 通信分析;

要求 3: 完成 HTTPs 通信分析。

#### 3、考核要求

题目 1: 提供 HTTP Get 请求协议的报文截图,完成分析后并填写表 8-1,将表格转为 截图后提交。(共计提交 2 张图片,且内容相对应)

题目 2: 提供 HTTP Get 响应协议的报文截图,完成分析后并填写表 8-2,将表格转为 截图后提交。(共计提交 2 张图片,且内容相对应,Get 响应报文要和题目 1 提交的请求报 文相对应)

题目 3: 提供 HTTPS 协议分析的报文列表截图,完成分析后并填写表 8-3,将表格转为 截图后提交。(共计提交 2 张图片,且内容相对应)