Misc 总结 ----流量分析 HTTP认识

M1n3 / 2018-01-17 23:23:46 / 浏览数 3833 安全技术 CTF 顶(0) 踩(0)

网络协议——HTTP

实验目的

掌握HTTP协议的通信方式
了解HTTP请求中不同字段的作用
了解HTTPheader中状态码的作用
掌握使用wireshark提取HTTP传输文件的方法

实验环境

- 操作机：Windows XP
  - 实验工具：
    - Wireshark2.2
    - chrome
    - notepad++
    - 看图工具

实验内容

听说用户在网站上下载了一个好玩的图片？是什么呢？

实验一 了解HTTP协议

HTTP协议即超文本传输协议，由TCP承载，实际上是基于TCP建立的可靠连接，进行数据传递。wireshark根据一个数据包既是TCP包，它的来源和目的端口是80(HTTP端口

实验二 HTTP状态码-重定向

方法一 理解http请求

wireshark载入HTTP.pcapng流量包。根据上节实验，我们可以得到前三个数据包是192.168.233.1向192.168.233.131请求建立一个TCP连接的过程。请求连接的目的端口是

我们打开Hypertext Transfer Protocol，可以看到分组详情中`GET /move.php HTTP/1.1\r\n`，展开之后，GET即请求方法，请求的URL是/move.php，采用的HTTP协议版本是1.1。

紧接着是请求的Host字段，即请求的ip地址或域名。后面的字段内容我们等下会讲到。

注释

HTTP请求的方法有很多：GET、HEAD、POST、PUT、DELETE等等，常用的有GET,POST等等。GET常用语请求某种资源，而POST则常用于向服务器发送数据等等。HTTP

方法二 分析HTTP返回包

我们可以通过刚才第四个数据包分组详情中的Response in frame：6
判断这个请求包的响应包位置，也可以通过wireshark在分组列表点击对应包，前面的小箭头确认发送包和回包，如下图中分组列表中No列的小箭头：

现在分析这个返回的数据包，同样展开分组详情中`HTTP/1.1 301 Moved Permanently\r\n`，可以得到HTTP版本1.1，Status Code(状态码)301，状态报告：临时移动(重定向)。

注意下面有一个Location，当我们的状态码是301/302重定向的时候，Location字段的内容告诉浏览器应该去请求这里的内容，浏览器转而向这个地址发送GET请求。就是将

实验三 404和200状态码

方法

在这个流量包中，序号8，14，19都返回了HTTP状态码200.200表示OK，即没有问题的把你请求的东西给你。序号11的数据包返回的HTTP状态码404，404表示没有找到，

实验四 HTTP协议字段详解

请求中常见：

Referer，这个字段的作用是标记来源页面，允许服务器生成回退链表，可用来登陆、优化cache等。在这个流量包中，序号16的数据包是包含referer字段的，因为我们通过

User-Agent，用于发送用户端信息，如当前操作系统版本，浏览器版本，内核版本等等，方便服务端根据不同UA判断浏览器，提供更好的服务，也常被用来绕过一些浏览限
(■■■■■■; ■■■■■■; ■■■■■) ■■■■■■ ■■■■。见上图Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36，我们可以得到使用了chrome54.0.2840.99，浏览器内核WebKit 537.36，windows 10 64位操作系统(Windows NT 10.0内核版本号)等等。
Cookie，用于辨别用户身份。
Cache-Control，指定请求和响应遵循的缓存机制。
Accept，指定可以接收的内容：

- accept_encoding，接受的压缩方法等等
- accept_language，接受的语言

响应中常见：

Server，标识服务器信息
Date，时间信息
Content_type，返回内容类型
Content_length_header，内容长度
Last_modified，最后编辑，用于优化缓存
Connection，是否终止TCP连接

实验五 HTTP信息提取

网页提取：

比如我们要提取download.html也买年内容，可以选择返回的HTTP内容的包，即序号为14的数据包。展开分组详情，最下面是Line-based text data: text/html。在这里右键，选择导出分组字节流，或者选中之后Ctrl+H，将内容导出，并命名成对应的文件类型，使用浏览器打开。

图片提取：

同理，在当前流量包中包含有一个xianyu.jpg的图片请求，我们找到对应的返回包。在wireshark的分组详情中，显示为JPEG File Interchange Format，同理右键导出分组字节流，保存为jpg格式，打开即可。我们得到了：

根据download.html的内容即可获知xianyu.jpg为用户下载的文件。

HTTP.pcapng.zip (0.006 MB) 下载附件
点击收藏 | 0 关注 | 1
上一篇：DEDECMS 任意重置管理员密码 下一篇：DeDecms 任意用户登录,管理...
1. 2 条回复


1815837370479554 2018-05-29 14:03:43

支持 支持

0 回复Ta

暮秋初九 2019-09-17 17:24:00

支持 支持

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板