Misc 总结 ----流量分析 TCP协议的认识

M1n3 / 2018-01-14 19:57:00 / 浏览数 3214 安全技术 CTF 顶(0) 踩(0)

网络协议——TCP报文

实验目的

掌握TCP建立连接的方式
了解TCP报文中不同字段的作用
了解TCP报文中标志位的作用
掌握使用wireshark分析数据包的基本方法

实验环境

- 操作机：Windows 7
  - 实验工具：
    - Wireshark2.2

实验内容

从网络协议最基本的TCP开始讲起。TCP是基于连接的，一种可靠的通信方式。TCP连接的建立必须经过三次握手，建立连接之后才开始发送数据，且可以保证数据的完整性

序号为多少的包里传输了"endendend"结尾的文件最后一部分？

了解TCP三次握手建立连接的具体过程。

首先，先具体了解TCP三次握手建立的过程，以及判别TCP三次握手

方法一 观察标志位

- 操作步骤详解

我们首先要理解的是TCP连接三次握手，如下图，A主动打开本地一个端口，向B发送一个SYN标志位为1，seq=x的包。B在监听一个端口，当这个端口收到A发送的第一个包

我们先通过TCP连接建立的过程，理解一下ACK，SYN，标志位的作用。

使用wireshark载入TCP.pcapng流量包，wireshark分三栏，会很直观的呈现给我们数据包的分组列表，分组详情和分组字节流。我们从第一个数据包开始看。Source源IP地
，等等：

上图当前选中的第二个数据包，我们打开了分组详情，并打开了Flags这个字段。我们可以看到在这个字段中，SYN和ACK(Acknowledgment)是置为1的。同理我们看第一个
Control Protocol的详细信息，包含Source Port和Destination
Port字段，分别为2333和47638，我们可以得到第二个数据包是192.168.233.129从2333端口向192.168.233.128的47638端口发送的连接建立的确认信息，即第二个握手包

注释

方法二 通过seq和ack的值了解建立过程

我们刚才只了解了标志位，现在了解一下TCP连接中，数据包是如何计数的，并确认完整性。

上图中可以看出，wireshark在分组列表中info字段为我们呈现了一个seq的值，为0，分组详情中也呈现出来。但是0如分组详情中括号内容解释的一样，是一个相对的值。有
number字段，响应位置的信息会在分组字节流中显示出来，我们就可以看到seq这个随机数了：

紧接着往下，在A发送了seq为0(相对)的建立连接请求后，B同样发送了一个含有seq的包，这个seq就是B端对于TCP数据包的计数，并且在ack
number给A回复了A发送的seq，表示A发送的第seq个数据包已经收到：

思考

1. 如果A发送的seq没有收到对应的ack会怎样呢？(触发重传机制)
2. 如果建立连接的时候，A直接发送了一个ACK标志位为1的数据包没有SYN的过程，又会怎样？(连接建立失败)

实验二

TCP连接的数据传输过程

方法 根据标志位进行判断

TCP还有有一个名叫Push(PSH)的标志位，我们观察载入的流量包分组列表，在info列我们可以看到有两个包是含有PSH标志位的：

注意序号为5和13的数据包。详情可以通过上面的，展开对应数据包的Flags字段，可以看到Push标志位被置为1。当PSH标志位为1时意味着有数据的传输，我们可以通过分

实验三

TCP连接的断开过程

方法 根据标志位判断

同样涉及到seq和ack number的变化，连接释放(断开)的过程涉及到FIN标志位。TCP连接释放过程如下图：

TCP连接释放的过程可以由A或B主动断开连接均可，上图我们展示的是A(主动建立连接的一方)主动断开TCP连接。A发送一个FIN标志位置为1，seq=u的数据包，并进入FIN

序号为17的数据包是192.168.233.128向192.168.233.129发送的TCP连接关闭请求。我们注意到这个数据包的FIN字段为1同时ACK字段也为1，这个数据包的目的在于告知

思考

1. 主动释放连接的一方发送了最后的一个ACK之后，还要等待一个极短的时间是什么目的？（保证报文到达；防止已失效的连接请求报文段出现在当前连接中）
2. 被动建立连接的一方(B)主动关闭连接又会是什么样的情况？

根据PSH标志位，定位到序号为5和13的两个数据包，查看分组字节流即可得到答案。
答案：13

上一篇：DNS外带查询怎么防。。。 下一篇：AlphaJump - 如何用机器...
1. 1 条追加内容
追加 于 2018年1月14日 20:00

加上流量包文件

TCP.pcapng.zip(0.001 MB) 下载附件

---

1. 2 条回复


暮秋初九 2019-09-17 17:37:17

支持

0 回复Ta

id0044**** 2019-10-21 15:00:54

太详细了，非常感谢你。学习了。

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