登录

Misc 总结 ----流量分析 FTP认识

M1n3 / 2018-01-19 14:21:00 / 浏览数 4086 安全技术 CTF 顶(2) 踩(0)

网络协议—FTP

实验目的

了解FTP返回码的作用
了解FTP登录，认证的过程
掌握FTP操作是如何体现在流量包中
学会从FTP中找到传输的文件并提取

实验环境

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

实验内容

FTP即File Transfer
Protocol，文件传输协议。常用与互联网上对文件的操作，方便用户上传与下载，并对服务器的文件进行操作。用户通过一个支持FTP协议的客户端程序，连接到在远程主机

听说用户使用FTP客户端下载了一个文件？而且开放了一个本地端口来接收文件？能找到这个文件和端口吗？(flag格式flag{本地端口号_传输文件名}，例如flag{21_file.jpg})

实验一

FTP的认证过程

方法 查看执行的具体命令

- 操作步骤详解

打开wireshark导入FTP.pcapng流量包，可以先整体浏览一下，FTP协议也是通过TCP协议来承载，wireshark对于这个流量包解析成了三种协议来显示：TCP,FTP,FTP-DAT

按顺序从开始看数据包，序号1-3的数据包建立了到192.168.233.131的TFP连接，192.168.233.131等待连接建立成功之后，主动发送了如下数据：

全部展开这个数据包分组详情，可以看到`Response code: Service ready for new user (220)`，意思是FTP返回码220，FTP服务做好了用户登录的准备。紧接着是FTPserver的banner，欢迎信息，展示了服务器程序Pure-FTPd，当前时间，端口，登录模式(不

上图打开的数据包是客户端向服务端发送的命令，FTP命令传输的格式均为：`command arg`即■■ ■■。可以看到客户端发送了USER
ftp，使用用户名ftp登录这台FTP服务器，同理下面发送密码也是如此。

客户端发送请求以FTP用户名登录后，服务端回复，要求密码。返回码331，用户是ftp，要求密码。

注释

FTP服务不论这个用户存在与否，都会要求输入密码。

客户端发送密码后，认证成功，服务端回复230用户成功登陆，并返回当前目录/在FTP根目录，见序号12的数据包。

14：客户端发送SYST请求目标服务器操作系统，服务器返回215和UNIX Type。这一步是客户端程序主动发送的。

18：然后客户端给服务端发送PORT命令，指定了客户端的一个端口，随后服务端主动连接该端口，并随后传输的数据均通过新端口建立的TCP连接发送。

注释

21：客户端连接服务端21端口用于传输命令，服务端连接客户端端口用于传输数据，可以通过流量包FTP和FTP-DATA的端口号进行判断。

25：然后客户端发送命令LIST，请求文件列表，服务端说文件正常，准备发送列表，通过刚刚建立的TCP连接，端口

紧接着可以看到第一个FTP-DATA数据包发送到了新建立的端口，带着FTP服务器跟目录的信息，在分组字节流中：

29：发送完目录之后，服务端主动发送了一个226，表示关闭数据传输。

33：客户端发送CWD命令default为参数，切换目录到default并列出文件列表，服务端切换成功之后再次建立连接，通过FTP-DATA传回文件列表。

在序号为57的数据包中，客户端发送RETR www.tgz
获取FTP服务器上的一个文件，服务器建立连接，并在序号62的FTP-DATA给客户端传输了这个文件的数据。且客户端开放了49626端口接收文件。

69：客户端发送QUIT命令，退出FTP服务器，服务器回复221，服务断开，并包含了上传和下载文件大小的信息：

实验二 提取数据

在我们想要导出数据的FTP-DATA包，例如导出www.tgz这个文件，可以在序号62这个数据包分组详情，FTP Data字段右键导出分组字节流即可。

思考

这种FTP服务安全吗？
如何让FTP变的更安全？

Flag:
flag{49623_www.tgz}

FTP.pcapng.zip (0.003 MB) 下载附件
点击收藏 | 2 关注 | 2
上一篇：渗透测试技巧之一个XSS引发的漏洞... 下一篇：Misc 总结 ----流量分析 ...
1. 3 条回复


1815837370479554 2018-05-29 15:00:10

学习 学习

0 回复Ta


胖丫胖丫丶 2018-11-05 11:30:10

学习学习、

0 回复Ta

暮秋初九 2019-09-17 18:31:25

学习学习、

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