|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名： | | 学号： | 专业年级： | 班级： |
| 分组： | | 实验室： | 指导教师：郭念 | 实验日期： |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **网络协议分析与攻防技术** | | |
| **实验名称** | 实验三 FTP文件传输协议 | | |
| **实验目的** | 1)理解FTP协议的工作原理 | | |
| **实验内容** | 1) FTP协议特点：控制连接，服务器以被动方式打开众所周知的用于F T P的21端口 ，等待客户的连接。客户则主动方式打开TCP端口21来建立连接。控制连接始终等待客户与服务器之间的通信。该连接将命令从客户传给服务器，并传回服务器的应答；数据连接，每当一个文件在客户与服务器之间传输时，就创建一个数据连接。由于该连接用于传输目的，所以IP对数据连接的服务特点就是“最大限度提高吞吐量” 。  2) FTP协议交互过程：客户端打开一个随机的端口（端口号大于1024），同时一个FTP进程连接至服务器的21号命令端口。源端口为客户端随机端口，远程端口为服务器21。客户发出命令要求建立数据连接，所以数据连接是在客户的控制下建立的。客户通常在客户端主机上为所在数据连接端选择一个临时端口号。客户从该端口发布一个被动的打开。客户使用PORT命令从控制连接上把端口号（数据连接）发向服务器。服务器在控制连接上接收端口号，并向客户端主机上的端口发布一个主动的打开，服务器的数据连接端一直使用端口20。 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | FTP工作流程和报文格式 | | |
| **实验环境** | 绘图1  本次实验根据虚拟机的真实MAC地址进行实 | | |
| **实验的实施阶段** | **实验步骤及实验结果** | **一、利用网络协议分析软件抓取FTP协议数据包**  1.1  在打开主机A上的“网络协议分析软件，单击工具栏”过滤器“-〉”添加“-〉”类型过滤器“->”ftp协议“->”接受”->”设置参数”-〉”确定“，然后单击”开始“按钮，捕捉ftp数据包。**实验过程截图如下：**    1.2  单击工具栏中“TCP”按钮，打开TCP连接工具，在对话框中输入“192.168.1.3”-〉“21”->”FTP”，单击“连接“按钮。**实验过程截图如下：**    1.3  在命令对话框中选择“USER“，在输入框中输入登录用户名”administrator“(即USER administrator)，单击”发送“按钮。**实验过程截图如下：**    1.4  在命令对话框中选择“PASS“，在输入框中输入登录密码”Simplexue123“(即PASS Simplexue123)，单击”发送“按钮。**实验过程截图如下：**    1.5  在命令对话框中选择“SYST“，查看目标系统类型，单击”发送“按钮。**实验过程截图如下：**    1.6  在命令对话框中选择“QUIT“，退出FTP登录，单击”发送“按钮。**实验过程截图如下：**    1.7  单击会话树中的”192.168.1.2ó192.168.1.3[18]”,显示FTP登录过程中数据包交互过程。**实验过程截图如下：**    1.8  单击“协议视图”，在数据包列表区中显示出数据包抓取顺序。**实验过程截图如下：**    **二、分析FTP登录数据包**  2.1  单击“网络协议分析软件“数据包分类列表框中的第一个数据包，数据包的标志位为”SYN“，表示为三次握手包的第一个。**实验过程截图如下：**    l  **源端口**：1038，由于发起连接的是客户端，因此源端口为TCP程序随机出的短暂端口，在此连接中是1038。  l  **目的端口**：21，由于是向FTP服务发起连接，因此目的端口为FTP服务的熟知端口，为21。  l  **序列号**：0XD039D920，此序列号为TCP程序随机出的字节编号。  l  **确认序号**：0X00000000，第一个发出的连接请求中，确认号为0。  l  **TCP首部长度**：7，TCP首部长度包括TCP报头长度和数据长度，这个字段表示TCP报头长度，其中20字节为标准TCP报头长度，另有8字节选项字段长度，选项字段中和服务器端协商了最大报文段长度。  l  **标识位**：SYN位置1，只有TCP连接中三次握手第一次连接的报文段中SYN位置1。  l  **窗口大小**：65535，默认大小。  l  **校验和**：0X524C，校验和是对TCP报头、数据和伪首部进行计算得出的校验和。  l  **紧急指针**：0，当紧急标识位置1时，此16位字段才有效，说明此时报文段中包含紧急数据，紧急数据到达接受端后可以不按次序优先被接受程序处理。  2.2  单击“网络协议分析软件“数据包分类列表框中的第二个数据包，数据包的标志位为”SYN|ACK“，表示为三次握手包的第二个。**实验过程截图如下：**    l  **源端口**：21，服务端的源端口为相关服务的熟知端口，FTP服务端口为TCP21。  l  **目的端口**：1038，为客户端源端口复制过来得到。  l  **序列号**：0X435FA400，为服务端随机计算出的字节序号。  l  **确认序列号**：0XD039D921，确认序列号的功能是对发送端数据进行确认，为发送端序号0XD039D920+1得到。  l  **TCP首部长度**：7，包含20字节标准TCP首部长度和8字节选项长度。  l  **标志位**：SYN位和ACK位置1，表示此报文为TCP三次握手的第二个报文。  l  **窗口大小**：16384，为默认大小。  l  **校验和**：0X2ADB，TCP校验和为TCP首部、数据和伪首部三部分计算得出校验和。  l  **紧急指针**：0。  2.3  单击“网络协议分析软件“数据包分类列表框中的第三个数据包，数据包的标志位为”ACK“，表示为三次握手包的第三个。**实验过程截图如下：**    l  **源端口**：1038，同一个连接发送的数据，源端口保持不变。  l  **目的端口**：21，对同一个服务发送的数据段中的目的端口保持不变。  l  **序列号**：0XD039D921，为前一个数据段序列号加1。  l  **确认序号**：0X435FA401，由于此报文是对服务端发回的连接应答消息的确认，因此是上一个报文序号0X435FA400加1。  l  **TCP首部长**度：5，标准TCP首部长度为5\*4字节=20字节。  l  **标识位**：TCP三次握手第三个报文段ACK位置1。  l  **窗口大小**：65535，默认窗口大小。  l  **校验和**：0X979F，为TCP首部、数据、伪首部计算得出的校验和。  l  **紧急指针**：0，未使用紧急指针。  2.4  单击“网络协议分析软件“数据包分类列表框中的第四个数据包,表示FTP连接状态正常。**实验过程截图如下：**    2.5  单击“网络协议分析软件“数据包分类列表框中的第八个数据包,显示登录FTP服务器时,输入的用户名。**实验过程截图如下：**    2.6  单击“网络协议分析软件“数据包分类列表框中的第十一个数据包,显示登录FTP服务器时,输入的密码。**实验过程截图如下：**    2.7  单击“网络协议分析软件“数据包分类列表框中的第十六个数据包,显示输入的命令“SYST”，查看目标服务器系统类型。**实验过程截图如下：**  图16  2.8  单击“网络协议分析软件“数据包分类列表框中的第十六个数据包,显示输入的命令“QUIT”，推出FTP登录。**实验过程截图如下：**17所示 | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | **【实验思考】**  1．利用协议编辑软件中的FTP模板验证FTP交互过程。  打开协议编辑软件，并选择FTP模板。  在FTP模板中创建一个新的会话，填写FTP服务器的IP地址、端口号、用户名和密码等信息。  连接FTP服务器。可以点击协议编辑软件中的“连接”按钮，或者在命令行中输入“CONNECT”命令。  登录FTP服务器。可以使用“USER”和“PASS”命令登录FTP服务器。根据FTP服务器的设置，可能需要输入其他的命令或参数。  浏览FTP服务器的目录结构。可以使用“LIST”命令来列出FTP服务器上的文件和文件夹。还可以使用“CWD”命令来更改当前目录。  下载文件。可以使用“GET”命令下载FTP服务器上的文件。  上传文件。可以使用“PUT”命令将文件上传到FTP服务器。  断开FTP服务器的连接。可以使用“QUIT”命令来断开FTP服务器的连接。 | | |