|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 TELNET协议 | | |
| **实验目的** | 1) 理解Telnet协议的工作原理。 | | |
| **实验内容** | 1) Telnet是一个简单的远程终端协议,通过TCP连接远程服务器。Telnet客户进程把收到的数据传送给TCP，由TCP负责在客户端和服务器端建立TCP连接，数据就通过TCP连接送到了服务器端，服务器的TCP层将收到的数据送到相应的应用层Telnet服务器进程。 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | Telnet工作流程和报文格式 | | |
| **实验环境** | telnet  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Telnet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“->”telnet协议“->”接受”->”设置参数”-〉”确定“，然后单击”开始“按钮，捕捉telnet数据包。**实验过程截图如下：**    1.2  在主机A上,单击”开始”->”运行”-〉输入“cmd”->”telnet 192.168.1.200”,telnet目标主机B，输入账号root,密码Simplexue123，“回车”后登录到远程服务器上。**实验过程截图如下：**    1.3  在命令行窗口输入“ifconfig”,显示目标主机网卡信息。**实验过程截图如下：**    1.4  网络协议分析软件捕获telnet协议数据包。**实验过程截图如下：**    1.5  单击“协议视图”，在数据包列表区逐个数据包查看telnet数据包交互过程。**实验过程截图如下：**    1.6  在数据包中发现“r”字母，在随后的数据报包中会陆续出现字母“o”、“o”……..等，这是因为telnet在传输用户输入的内容时一次只传输1个字节，因此每个报文中只能看到一个字母。**实验过程截图如下：**    **二、利用数据包发送器发送Telnet数据包**  2.1  在主机A上打开数据包发送器，单击工具栏“添加”按钮，选择“TELNET协议模板”，单击“确认”按钮，建立一个Telnet数据包。**实验过程截图如下：**    2.2  填写以太网帧头、IP首部、TCP首部和TELNET报文的内容。**实验过程截图如下：**8所示  填写以太网协议首部信息：  l  **目的物理地址**：在地址本中选择主机B的IP地址(192.168.1.200)，确认后自动填入主机B的MAC地址：00-55-55-55-55-55；  l  **源物理地址**：在地址本中选择主机A(192.168.1.2)，确认后自动填入主机A的MAC地址：00-22-22-22-22-22；  l  **类型或长度**：该字段应为0800(即IP协议的类型值)。  填写IP协议头信息：  l  **总长度字段**：包括TCP段内容的总长度，20 IP+20 TCP+6 TELNET = 46；  l  **高层协议字段**：即上层协议类型为6(TCP协议的类型为6)；  l  **发送IP地址**：在地址本中选择主机A的IP地址，确认后自动填入主机A的IP地址192.168.1.2；  l  **目标IP地址**：在地址本中选择交换机的管理IP地址，确认后自动填入交换机的IP地址192.168.1.200；  填写TCP协议的各个字段信息：  l  **16位源端口号**：任意大于1024的数；  l  **16位目的端口号**：23；  l  **32位序号**：选择一个序号(例如：11112222)；  l  **32位确认序号**：设置为0；  l  **首部长度**：首部长度设为5，即长度为20字节；  l  **标志位**：标志位设为2，即标志位SYN=1；  l  **窗口大小**：任意，例如填入32733；  l  **紧急指针**：0；  l  填写TELNET协议报文的内容：可填入Telnet命令或者单字节的字母，例如构造一个传输Will命令的报文可填入FF FB 01 FF FB 03。  2.3  在数据包列表区中选中编辑完的数据包,单击工具栏中的”校验和”,自动计算数据包效验和。**实验过程截图如下：**    2.4  选中发送的数据包，单机工具栏“发送”按钮，设置发送次数5。**实验过程截图如下：**    2.5  在协议结构树显示TCP报文的标志位是SYN，Telnet报文是Will。**实验过程截图如下：** | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | **【实验思考】**  1．FF FB 01 FF FB 03如何转换成Will  在TCP协议中，FF FB 01代表"Will"，FF FB 03代表"Won't"。  这些字节都是Telnet协议中的命令字节，用于在Telnet会话期间进行通信。Telnet协议是一种远程终端协议，用于在计算机之间进行网络连接，并提供类似于本地终端的功能。  在TCP报文中，Telnet协议通常是通过在TCP数据中包含特殊的Telnet控制字符来实现的。这些控制字符由前缀字节0xFF标识，后面跟着一个命令字节。对于Telnet的"Will"和"Won't"命令，它们的命令字节分别是0x01和0x03。  因此，当在TCP数据中看到0xFF 0xFB 0x01的字节序列时，它被解释为"Will"命令，表示发送方愿意启用指定的Telnet选项。类似地，当看到0xFF 0xFB 0x03时，它被解释为"Won't"命令，表示发送方不希望启用指定的Telnet选项。 | | |