## 实验五 网络相关命令的使用以及TCP协议分析

|  |  |
| --- | --- |
| 班级：信息2002 | 日期：2022年11月3日 |
| 学号：4201118033 | 姓名：刘凯 |
| **一、实验目的**   1. 掌握常用的（TCP/IP）网络命令netstat、route、tracert的使用。 2. 分析TCP协议的基本原理 | |
| **二。实验前的准备**   1. 熟悉TCP/IP网络命令的基本使用方法。 2. 熟悉TCP协议的基本原理和作用。 | |
| **三．实验内容和步骤。**  **1. 网络相关命令的使用**  **1.1 netstat命令**  1.1.1 netstat命令的基本功能是什么，有哪些参数，这些参数的作用是什么。（可以通过netstat /h 命令来观察其说明）  1netstat命令是一个观察网络连接状态的实用工具。 它能检验IP的当前连接状态，在断定你的基本级通信正在进行后，就要验证系统上的服务。这个服务包括检查正在收听输入的通信量和／或验证你正在创建一个与远程站点的会话，它可以很轻松地做到这一点。—R显示本机路由内容 ——S每个协议的使用状态 ——N以数字表格形式显示地址和端口 这个命令的具体用法如下： NETSTAT 〔-a〕 〔-e〕 〔-n〕 〔-s〕 〔-p proto〕 〔-r〕 〔interval〕 -A 显示任何关联的协议控制块的地址。主要用于调试 -a 显示所有套接字的状态。在一般情况下不显示与服务器进程相关联的套接字 -i 显示自动配置接口的状态。那些在系统初始引导后配置的接口状态不在输出之列 -m 打印网络存储器的使用情况 -n 打印实际地址，而不是对地址的解释或者显示主机，网络名之类的符号 -r 打印路由选择表 -f address -family对于给出名字的地址簇打印统计数字和控制块信息。  1.1.2在CMD窗口中运行netstat 命令查看本机的网络连接，将运行的结果截屏，并解释其结果。（注意连接中的端口）    2Proto：协议名recv-Q：网络接收队列send-Q：网路发送队列  Local Address：本地地址   Foreign Address：外部地址  State：状态  ESTABLISHED：此套接字已建立连接  TIME\_WAIT关闭之后，此套接字正等待处理仍在网络上的数据包  127.0.0.1：xxx:开放的端口号  1.1.3 运行netstat –an命令，将结果截图并解释该命令的作用是什么。再试试netstat –ano，看看有什么结果。    3netstat -an 来显示所有连接的端口并用数字表示。  **1.2 route命令**  1.2.1在CMD窗口中输入route，观察 route命令的基本功能是什么，有哪些参数，这些参数的作用是什么    **基本功能：**  Route命令是用于操作基于内核ip路由表，它的主要作用是创建一个静态路由让指定一个主机或者一个网络通过一个网络接口  **参数：**  **-f 清除所有网关入口的路由表。**  **-p 与 add 命令一起使用时使路由具有永久性。**  **-4表示强制使用IP v4。**  **-6表示强制使用IP v6。**  **-netmask:当添加一个网络路由时，需要使用网络掩码。**  **-metric：设置路由跳数。**  **-Command 指定您想运行的命令 (Add/Change/Delete/Print)。**  1.2.2 运行route print命令查看本地路由表。将运行的结果截屏，并简单解释其结果。    第一行表示向任意网段的数据通过本机接口192.168.43.90被送往一个默认的网关：192.168.43.1，它的管理距离是55。  **1.3 tracert命令**  1.3.1 在CMD窗口中输入tracert，观察tracert命令的基本功能是什么，有哪些参数，这些参数的作用是什么。    1.3.2 对于某个主机（如百度），利用tracert www.baidu.com命令跟踪和这些主机之间的路由信息。将运行的结果截屏，并解释其结果。  （如果想用ip地址，则可以利用nslookup [www.baidu.com](http://www.baidu.com)命令查询得到该域名对应的ip地址）    该命令列出从自己的上网IP地址到访问www.baidu.com网站IP所经过的所有服务器（路由）。  **2. TCP协议的分析**  2.1 启动Wireshark 软件。在“Capture”菜单中选择“Options”菜单选项，在Options 设置窗口中把捕获参数设置为非混杂模式。且捕获过滤器设置为“not arp”。    2.2 点击“Start”按钮开始捕获数据包。    2.3 将显示的结果截屏，选择显示过滤器为“tcp”，观察和分析TCP 报文段的结构以及各项信息的含义。    源端口：57437  目的端口：80  序号：2  确认号：1  数据偏移0  2.4 设置捕获过滤器为“tcp port https”说明只监听443端口的tcp请求。来捕获与网站之间的数据交互。  在浏览器的地址兰输入“www.baidu.com”浏览该网站的主页，待主页信息显示完毕后，点击“Stop”按钮停止捕获。  通过实验过程和结果．分析TCP 建立连接、传送数据的过程。以及http协议的相关数据。  传输数据的简要过程如下:  (1）发送数据:服务器向客户端发送一个带有数据的数据包，该数据报的序列号和确认号与建立连接第三步的数据包中的序列号和确认好相同。  (2）确认收到:客户端收到该数据报，向服务器发送一个确认数据包。该数据包中，序列号是为上一个数据报中的确认号的值，而确认号为服务器发送的上一个数据包中的序列号+该数据包中的所带数据的大小。  第一次握手    第二次握手    第三次握手    设置显示过滤器为“tcp.flags.fin==1”，查看释放连接的过程。将结果显示在下方，并解释。（也可以用类似的方法来查看syn标志的相关数据） | |