实验1-网络的使用与配置

实验目的

熟悉 TCP/IP 通信原理,熟练地掌握典型的 TCP/IP 应用程序的使用与设置，熟悉 Linux 下抓包工具 tcpdump 的使用。

预备知识

TCP/IP 通信的基本概念：IP 地址、IP 端口、子网屏蔽、IP 子网、路由器等。TCP/IP 应用协议族的内容和功能：DNS 名字/地址解析协议、ARP 协议、FTP 协议、HTTP 协议和 SMTP 协议。

实验内容

终端输出结果可以截图或者复制到文本文档，通过u盘或者邮箱带回去写报告。

助教会检查终端输出结果和你的记录。

wget 下载命令使用

说明

本实验使用的网址是科大的镜像站子目录`http://mirrors.ustc.edu.cn/debian/tools/`。实验中，涉及到文件夹下载的指令，都需要额外的三个选项：`-np`，`-l1`，`-e robots=off`。其中：

- `-np`是禁止下载父文件夹内容，`-l1`是禁止下载子文件夹内容。
  为了不对服务器造成过大压力，这两个选项是必须的。
- `-e robots=off`是防止 wget 被当成机器人而被禁止。
  有兴趣的同学可以去掉这个选项试试。

为了不让实验课变成对镜像站的 DDoS 攻击，如果发现因为输错指令导致大量下载，请尽快使用 ctrl+c 终止。

实验

学习“wget”的各种使用方法，完成以下功能并在实验报告中记录所使用的命令：

- 断点续传
  例子：`wget -c http://mirrors.ustc.edu.cn/debian/tools/loadlin.exe`
  终端会出现下载提示，显示下载流程。下载完成后，所下载文件会出现在当前文件夹下。
- 后台运行下载任务
  例子：`wget -b http://mirrors.ustc.edu.cn/debian/tools/loadlin.exe`
  这时候下载会自动在后台下载，和上一个命令的显示不同。下载的文件同样会在当前文件夹下。
- 利用编写下载 URL 列表文件的方法实现下载批量文件
  例子：在当前文件夹下，使用命令`touch list`来创建一个名为 list 的文件。使用`gedit list`命令，打开 list 文件，在其中输入 URL 列表。如：

  ```
  http://mirrors.ustc.edu.cn/debian/tools/loadlin.exe
  http://mirrors.ustc.edu.cn/debian/tools/loadlin.txt
  ```

  然后保存关闭，在终端中使用命令：`wget -i list`，就可以下载 list 中的两个文件。
- 下载指定后缀名的文件(需要与-m 或者-r 等参数结合使用) (创建目录结构和不创建目录结构两种情况)
  创建目录：`wget -x -r -A "*.txt" -np -l1 -e robots=off http://mirrors.ustc.edu.cn/debian/tools/`
  不创建目录：`wget -nd -r -A "*.txt" -np -l1 -e robots=off http://mirrors.ustc.edu.cn/debian/tools/`
- 下载除某后缀名之外的文件(需要与-m 或者-r 等参数结合使用) (创建目录结构和不创建目录结构两种情况)
  创建目录：`wget -x -r -R "*.txt" -np -l1 -e robots=off http://mirrors.ustc.edu.cn/debian/tools/`
  不创建目录：`wget -nd -r -R "*.txt" -np -l1 -e robots=off http://mirrors.ustc.edu.cn/debian/tools/`
- 下载某网站上一个完整的子目录（镜像）
  例子：`wget -m -np -l1 -e robots=off http://mirrors.ustc.edu.cn/debian/tools/`

分析

在实验报告中解释下列命令行的含义：

- `wget -r -nH ftp://10.1.1.1/movie/`
- `wget -r -R "*.htm*\?*" -k http://www.abc.com/blog`
- `wget -r -k http://www.abc.com/blog`
- `wget -r -l2 -k http://www.abc.com/blog`
- `wget -nc -r -k http://www.abc.org/help/`
- `wget -i your.file`

熟悉抓包工具 tcpdump

说明

tcpdump 可以将网络中传送的数据包的“头”完全截获下来提供分析。它支持针对网络层、协议、主机、网络或端口的过滤,并提供 and、or、not 等逻辑语句来帮助你去掉无用的信息。tcpdump 就是一种免费的网络分析工具，尤其其提供了源代码，公开了接口,因此具备很强的可扩展性，对于网络维护和入侵者都是非常有用的工具。

tcpdump 的命令格式为:

```
tcpdump [ -adeflnNOpqStvx ] [ -c 数量 ] [ -F 文件名 ] [ -i 网络接口 ] [ -r 文件名] [
-s snaplen ] [ -T 类型 ] [ -w 文件名 ] [ 表达式 ]
```

tcpdump 利用表达式作为过滤报文的条件，如果一个报文满足表达式的条件，则这个报文将会被捕获。如果没有给出任何条件，则网络上所有的信息包将会被截获。

表达式中需要注意的关键字:

1. 关于类型的关键字，主要包括 `host`、 `net`、 `port`。例如：
    1. `host 202.38.75.11`，指明 202.38.75.11 是一台主机
    2. `net 202.38.0.0`指明 202.38.0.0 是一个网络地址
    3. `port 23`指明端口号是 23
2. 确定传输方向的关键字，主要包括 `src`、 `dst`、 `dst or src`、 `dst and src`。例如：
    1. `src 202.38.75.11`指明 ip 包中源地址是 202.38.75.11
    2. `dst net 202.38.0.0`指明目的网络地址是 202.38.0.0

这些关键字可以组合起来构成强大的组合条件来满足人们的需要，例如 `tcpdump host 202.38.75.11 and port 80`。

实验

熟悉 tcpdump 的用法，会在下一节中使用，不需要记录。

观察 FTP 的两种数据传送模式

实验

使用 tcpdump 观察 FTP 的两种数据传输模式（主动模式和被动模式）的区别。

请同学们自己设计 tcpdump 的命令格式（注意使用-X 选项），并且使用上述 FTP 客户端程序连接某 FTP 服务器 (推荐 202.38.64.123 、debian.ustc.edu.cn 或 mail.ustc.edu.cn，大家可以自己随意选取)，然后分析 tcpdump 抓到的数据包，对比 ftp 主动模式和被动模式的区别。

在观察被动模式时请注意观察 FTP 的PASV 命令；在观察主动模式时请注意观察 FTP 的 PORT 命令。记录主动模式和被动模式的关键数据，并在实验报告中进行分析。

详情

首先需要打开两个终端,一个用来登录 ftp,一个用来使用 tcpdump 捕获数据包,观察结果。

进入一个终端1，输入命令`ftp home.ustc.edu.cn`，用户名是你的科大邮箱名(@mail之前的那几个字母)，密码是你的科大邮箱密码。登陆后，输入命令`passive`，打开passive模式。如果要退出，输入命令`exit`。

进入另一个终端2，输入命令`ip addr`查看本机 IPv4 地址，记录下来。之后在该终端(终端2)输入命令：`sudo tcpdump -vvnn -X host home.ustc.edu.cn and 本机IPv4地址`，密码填123456。

在终端1中输入`ls`命令，显示 ftp 当前目录，此时可以在终端2中观察捕获的数据包，在字符串中寻找相应的 PASV 和 PORT 命令。另外还需要在数据包中注意主被动态的端口使用情况。

了解 DNS 域名服务

实验

熟悉使用 nslookup 查找 DNS 服务器上登记的域名。

在终端中输入 nslookup，进入交互模式，完成以下实验，并记录几次查询的结果和服务器的 ip：

1. 某个子域下的一部分主机的名字-IP 地址对应关系，如 flame.nsrl.ustc.edu.cn—202.38.77.223
   直接输入 flame.nsrl.ustc.edu.cn 回车,就可以看到服务器返回的解析结果。
2. 通过 IP 地址查找主机名，即：反向查询,记录你的查询结果
   输入 202.38.75.11 回车，即可以看到相应的反向解析结果。(注意:有些地址不能反向解析)
3. 指定使用 202.38.75.11 作为 DNS 服务器,重复 2、3
   输入命令 lserver 202.38.75.11 回车，设定 202.38.75.11 为 dns 服务器,然后重复 1、2。
4. 查看当前的查询选项(set all)
5. 查询邮件交换记录 MX(如 mail.ustc.edu.cn)
   set type=MX，然后查询。
6. 查询某个域的域名服务器(如 ustc.edu.cn 的域名服务器)
   set type=ns，然后查询。

实验报告要求

实验报告在下次做实验时上交，必须手写版。

1. 完成实验内容中要求记录的部分。
2. 完成实验内容中要求记录部分的分析。
3. 说明在实验过程中遇到的问题和解决方法。
4. 完成以下思考题：
   1. `wget -m http://mirrors.ustc.edu.cn/debian/tools/`
      这条创建镜像的命令,如何在不使用-m 选项的条件下实现相同功能(用其他参数结合使用)。
   2. ftp 协议在客户端和服务器之间使用了几个 TCP 连接?这样做有何优点?“被动(passive)”方式是如何工作的?请用实验中记录的现象加以说明。
   3. 简要说明 tcpdump 的作用,在实验中用到了那些参数和表达式的关键字,说明这些参数和表达式的作用。
   4. DNS 服务器的功能是什么?人们为什么要使用它们?Internet 上的 DNS 服务器结构是怎么样的?*它们之间如何保持名字/地址数据的一致性?
   5. 请列举一些常用的下载工具及其软件编写公司或个人,这些软件各有什么优缺点。