

本文档对实验一相关操作做说明（**仅供参考!!!**）。

另外，使用命令和所得数据，一定要用纸记录（可以简单记录要点），方便助教检查，至于详细数据，使用 **txt** 文本保存，放到自己的邮箱中，方便回去仔细分析。

实验报告在下次做实验时上交，必须手写版!!!

1. wget 实验

同学们可以根据后面附录的参数表，查找对应的参数，完成实验。

基本使用方法： **wget + 参数 + URL 或者文件名**

➤ 断点续传

例子： `wget -c ftp://debian.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 ftp://debian.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：可以在当前文件夹下建立一个新的文件，如 `list`，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：

`ftp://debian.ustc.edu.cn/debian/tools/loadlin.exe`

`ftp://debian.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" ftp://debian.ustc.edu.cn/debian/tools/`

此时下载的文件和服务器上的文件目录保持一致，在本地创建了 `debian.ustc.edu.cn/debian/tools/`，里面只有 `loadlin.txt` 文件

不创建目录：

`wget -nd -r -A "*.txt" ftp://debian.ustc.edu.cn/debian/tools/`

此时下载的文件就在当前文件夹

➤ 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" ftp://debian.ustc.edu.cn/debian/tools/`

不创建目录：

`wget -nd -r -R "*.txt" ftp://debian.ustc.edu.cn/debian/tools/`

➤ 下载某网站上一个完整的子目录（镜像）eg: `ftp://debian.ustc.edu.cn/debian/tools/`

例子: `wget -m ftp://debian.ustc.edu.cn/debian/tools/`

注意:

1. 下载的时候, 不要选择太大的文件, 以免超出硬盘配额。尤其是 `-m` 命令, 是对整个站作镜像, 如果直接使用 `wget -m ftp://debian.ustc.edu.cn` 肯定会超出硬盘使用量, 使用 `-m` 参数一定要注意后面 URL 中的大小。

2.ftp地址如果连不上, 可以换成各个任课老师的课件地址。

思考题 (需要在实验报告中给出):

`wget -m ftp://debian.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&3 tcpdump 使用和观察 FTP 的主被动态模式

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。【附: 如要退出, 输入 `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 -vnn -X host home.ustc.edu.cn and 本机IP` (你刚才记下的 IPv4 地址), 密码填 123456。

在终端一中输入 `ls` 命令, 显示 ftp 当前目录, 可以在终端二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。

4 nslookup 命令使用

该实验只需要完成在 linux 下的操作即可。

在终端中输入 `nslookup`, 进入交互模式。

o 某个子域下的一部分主机的名字—IP 地址对应关系

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。

o 通过 IP 地址查找主机名

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)

o 指定使用 202.38.75.11 作为 DNS 服务器, 重复 2、3

输入命令 `server 202.38.75.11` 回车, 设定 202.38.75.11 为 dns 服务器, 然后重复 1, 2.

o 查看当前的查询选项

`set all`

o 查询邮 交换记录 MX

set type=MX

o 查询某 域的域名服务器

set type=ns

o 查询域 对应的 IPv6 地址(查询 bbs6.ustc.edu.cn 的地址)

set type=AAAA

在查询 IPV6 地址后，如果要查询 IPV4 地址，输入命令 set type=A