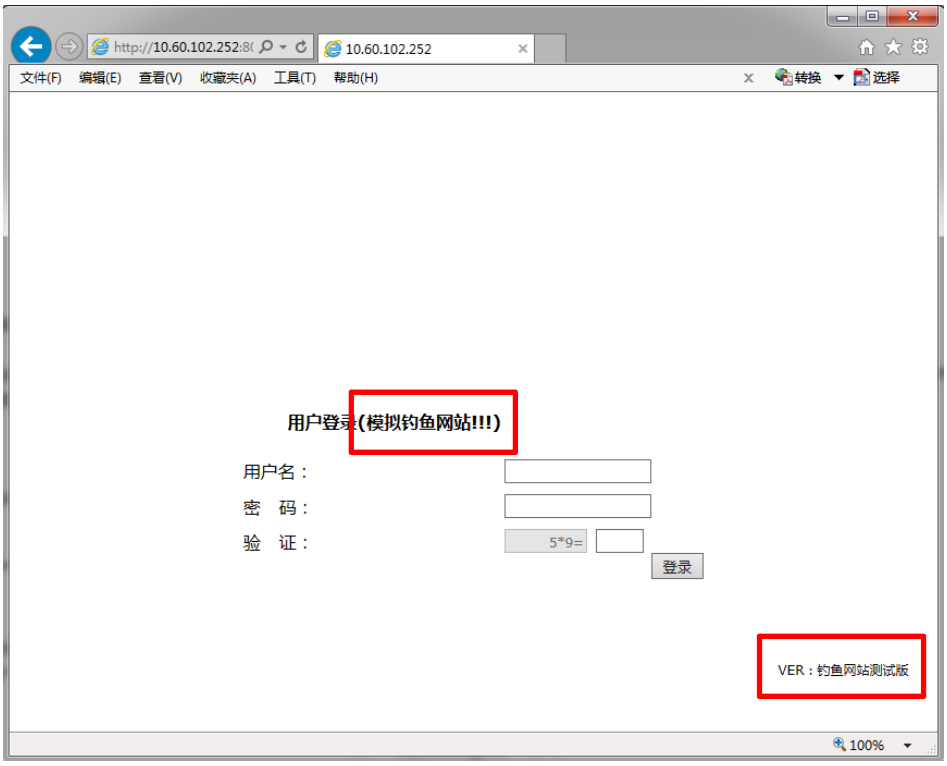
§.小组作业 - 编程技巧类 - 用 IP 代理方式实现一个简单的钓鱼网站

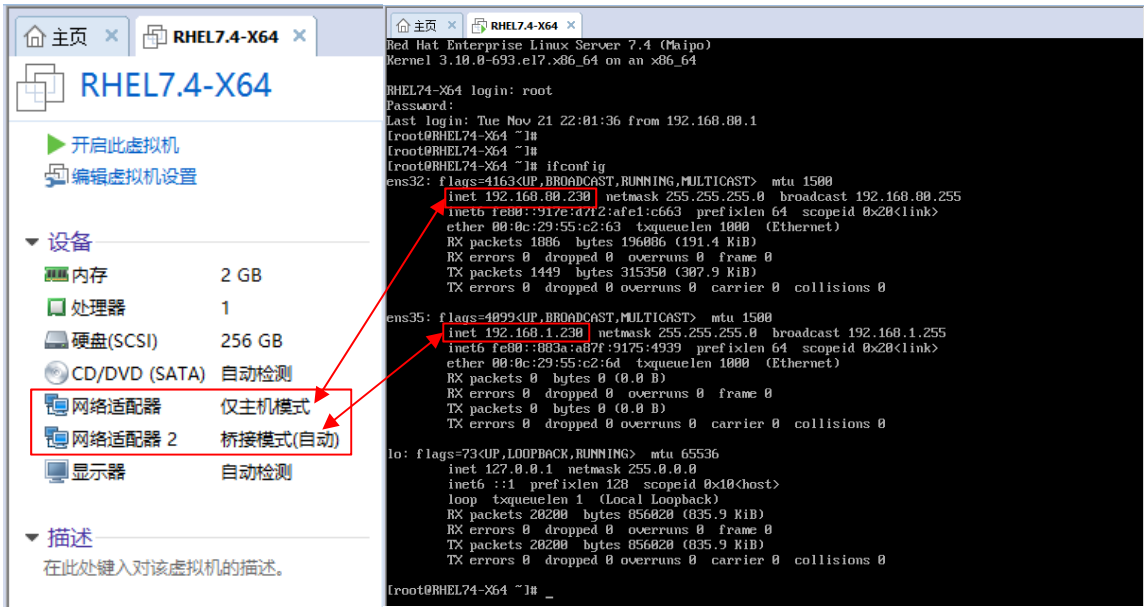
【应用场景:】模拟的应用场景如下所示:

- 假设 http://10.60.102.252:8080 上有一个 web 服务器在正常运行



【说明:】1、只有同济校园网内才能访问该地址
2、每人的初始账号和密码均为学号，登录后的内容与交作业网站相同
3、注意作业不要交到这个网页下!!!

- 一台 VMWare 虚拟机，配置双网卡，一个为桥接，一个为仅主机模式



【说明:】1、贴图中设置的桥接网卡地址为 192.168.1.230，NAT 网卡地址为 192.168.80.230，可以自行设置其它 IP 地址，但下面以这两个地址为例
2、设置宿主机的各网卡/虚拟机桥接网卡的 IP 地址及网关、DNS 等，要求 192.168.1.230 能 ping 通 10.60.102.252，宿主机能 ping 通 192.168.80.230（注意 1：仅主机模式是通过 VMnet1 网卡，注意 IP 网段的设置）
3、停用虚拟机上的 httpd 服务

【功能要求：】基于以上应用场景描述，在虚拟机上完成一个 IP 代理网站并分析代理传输的数据，从中找出用户登录时的用户名和密码

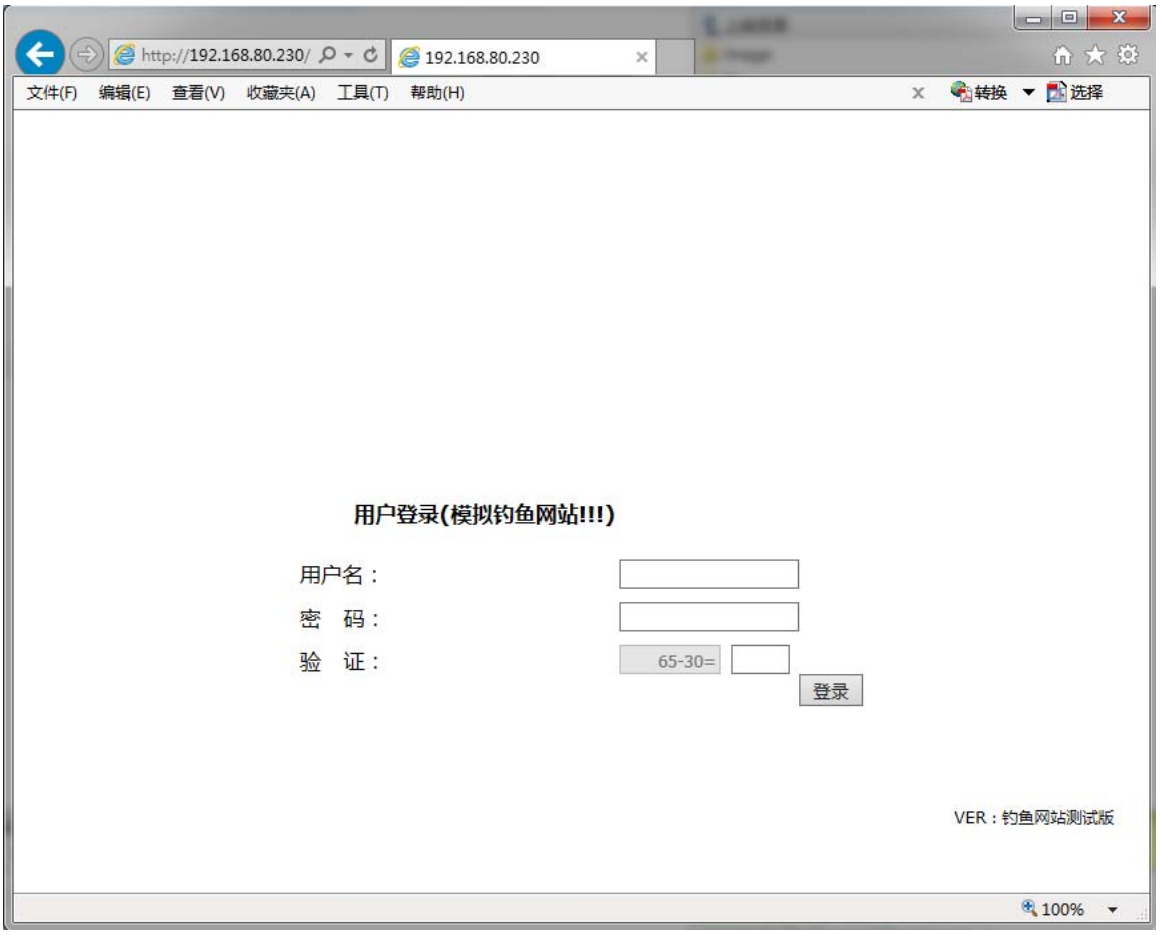
1、 写一个守护进程，监听 192.168.80.230 的 80 端口，但不能监听 192.168.1.230 的 80 端口

2、 守护进程每收到一个来自宿主机 IE 浏览器的 connect 请求，就 accept 并 fork 一个子进程，然后子进程通过 192.168.1.230 去连接 10.60.102.252 的 8080 端口

3、 连接成功后，在两个 socket 之间来回传递数据即可

4、 某条 socket 被关闭，则关闭另一条 socket

达到上述 1-4 要求后，如果在宿主机的 IE 浏览器中输入 http://192.168.80.230，则会显示 http://10.60.102.252:8080 的内容（假设 10.60.102.252:8080 代表 icbc 的真实网址，而 192.168.80.230 代表 1cbc 的假冒网址，那么...）



5、 分析在 socket 上传输的数据（明文），当发现有用户名和密码时，截获并打印出来

【小组作业的基本要求：】

1、每个小组的成员自由组合，最多三人

2、如果某个作业的分值为 n，则三人小组，每人得分为 n*得分率；两人小组，每人得分为 n*得分率*1.1；单人小组，每人得分为 n*得分率*1.2

3、每个小组成员的得分相同，不会因为贡献大小而区别给分

4、11 月 24 日前各小组上报分组名单，确定后不再变动（本次分组适用于知识拓展类及编程技巧类）

5、本次作业分值为 10 分（以小组成绩 100 分计算）

【作业提交内容：】

每个小组中任一人提交即可，文件名为 linux-proxy.tar.bz2，解压后目录结构如下：

```
1551234-G00102
  |-- ***.c/***.cpp
  |-- ***.h
  |-- ...
  `-- makefile        （make 即可在当前目录下生成可执行文件，名为 web-proxy）
```

【作业要求：】

1、 12 月 10 日前网上提交

2、 每个小组由学号最小的同学提交即可，其余同学不必提交（若同一小组多人提交，**取低分者**）

3、 超过截止时间提交作业则不得分

4、 **本次作业会安排现场测试验收（在浏览器中由其他人输入用户名和密码，各小组的程序能正确截获者为通过），具体时间另行通知（12.10 后）**