网络安全工程实践：实验五

> 李家昊 2017011620
> 李文博 2017011447

代码使用手册

安装第三方库

```
pip install -r requirements.txt
```

在代理服务器上运行服务器代码

```
python socks_server.py
```

在本地机器运行客户端代码

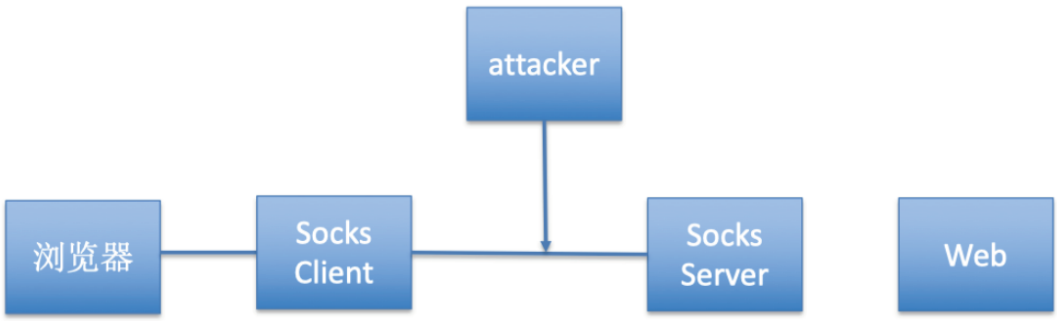
```
python socks_client.py
```

本地机器上通过 socks 代理访问百度主页

```
curl --socks5 127.0.0.1:1091 -U username:password http://www.baidu.com/
```

代码设计思路

考虑以下网络拓扑



其中攻击者能够监听 Socks Client 到 Socks Server 之间的通信，因此该链路需要加密。

1. 建立连接后，客户端与服务端首先应当交换密钥。服务端利用 RSA 算法生成公钥私钥对，并将公钥发送给客户端。客户端随机生成 DES 算法密钥，利用服务端的公钥将该密钥加密，并将加密后的密钥发送给服务端，服务端用私钥解密，得到双方的 DES 共同密钥
2. 密钥交换后，客户端与服务端之间使用 DES 算法对称加密 Socks5 协议的通信包，保证传输安全。

客户端与服务端之间的协议如下：

报文格式如下

```
+---------+-------------+-----------+
| TYPE(1) | DATA_LEN(4) | DATA(VAR) |
```

```
+---------+-------------+-----------+
TYPE (1 byte):
    0x00: send RSA public key
    0x01: send encrypted DES key
    0x02: encrypted socks message
DATA_LEN (4 bytes):
    Length of the DATA field
DATA (VARIABLE):
    Payload
```

对于 RSA 公钥类型（TYPE=0x00），Payload 为 pub key (512)
对于加密 DES 密钥类型（TYPE=0x01），Payload 为加密的 des key (8)
对于 Socks5 代理类型（TYPE=0x02），Payload 为加密的 Socks5 报文

功能测试截图

命令行通过 socks 代理访问百度主页，并通过用户名密码登录认证

```
liwenbodeMacBook-Air:socks5-proxy liwenbo$ curl --socks5 127.0.0.1:1091 -U username:password
http://www.baidu.com
<!DOCTYPE html>
<!--STATUS OK--><html> <head><meta http-equiv=content-type content=text/html;charset=utf-8><m
eta http-equiv=X-UA-Compatible content=IE=Edge><meta content=always name=referrer><link rel=s
tylesheet type=text/css href=http://s1.bdstatic.com/r/www/cache/bdorz/baidu.min.css><title>百
度一下，你就知道</title></head> <body link=#0000cc> <div id=wrapper> <div id=head> <div class
=head_wrapper> <div class=s_form> <div class=s_form_wrapper> <div id=lg> <img hidefocus=true
src=//www.baidu.com/img/bd_logo1.png width=270 height=129> </div> <form id=form name=f action
=//www.baidu.com/s class=fm> <input type=hidden name=bdorz_come value=1> <input type=hidden n
ame=ie value=utf-8> <input type=hidden name=f value=8> <input type=hidden name=rsv_bp value=1
> <input type=hidden name=rsv_idx value=1> <input type=hidden name=tn value=baidu><span class
="bg s_ipt_wr"><input id=kw name=wd class=s_ipt value maxlength=255 autocomplete=off autofocu
s></span><span class="bg s_btn_wr"><input type=submit id=su value=百度一下 class="bg s_btn"><
/span> </form> </div> </div> <div id=u1> <a href=http://news.baidu.com name=tj_trnews class=m
nav>新闻</a> <a href=http://www.hao123.com name=tj_trhao123 class=mnav>hao123</a> <a href=htt
p://map.baidu.com name=tj_trmap class=mnav>地图</a> <a href=http://v.baidu.com name=tj_trvide
o class=mnav>视频</a> <a href=http://tieba.baidu.com name=tj_trtieba class=mnav>贴吧</a> <nos
cript> <a href=http://www.baidu.com/bdorz/login.gif?login&amp;tpl=mn&amp;u=http%3A%2F%2Fwww.b
aidu.com%2f%3fbdorz_come%3d1 name=tj_login class=lb>登录</a> </noscript> <script>document.wri
te('<a href="http://www.baidu.com/bdorz/login.gif?login&tpl=mn&u='+ encodeURIComponent(window
.location.href+ (window.location.search === "" ? "?" : "&")+ "bdorz_come=1")+ '" name="tj_log
in" class="lb">登录</a>');</script> <a href=//www.baidu.com/more/ name=tj_briicon class=bri s
tyle="display: block;">更多产品</a> </div> </div> </div> <div id=ftCon> <div id=ftConw> <p id
=lh> <a href=http://home.baidu.com>关于百度</a> <a href=http://ir.baidu.com>About Baidu</a> <
/p> <p id=cp>&copy;2017 Baidu <a href=http://www.baidu.com/duty/>使用百度前必读</a>
  <a href=http://jianyi.baidu.com/ class=cp-feedback>意见反馈</a> 京ICP证030173号&n
bsp; <img src=//www.baidu.com/img/gs.gif> </p> </div> </div> </div> </body> </html>
```

通过 SwitchyOmega 插件，设置浏览器代理

在代理模式下访问 http://info.cern.ch ，成功加载出页面