# microsocks 技术分析报告

## 名词解释

服务器：指运行microsocks的主机

客户端：指主动连接microsocks服务器的主机

target：客户端连接服务器，而服务器作为中间人（代理）与之通信的主机

## 图示

客户端 ----------> 服务器 ----------> target

## microsocks介绍

microsocks是一个基于TCP/IP协议的代理程序。它非常轻巧，占用很少的资源。它还特意设置了资源占用保护，当系统资源不足时会拒绝新的客户端连接。它适合运行在路由器这样的小型设备中，因此，microsocks能够作为一个流量中转站。

microsocks支持IPv4和IPv6，对于客户端的身份验证，可以选择不需要验证、一次验证（记录登录IP）、每次输入用户名和密码验证。microsocks还支持日记记录，并可以开启和关闭。

项目地址：https://github.com/rofl0r/microsocks

## microsocks用法

```
useage : microsocks -1 -q -i listenip -p port -u user -P password -b binda
ddr

例如
microsocks -1 -i 127.0.0.1 -p 7777 -u admin -P admin123 -b 127.0.0.1
```

所有的参数都是可选的。以下是选项说明：

```
-1
```

激活一次验证模式。当这个选项开启，某个IP的用户经过用户名和密码认证后，microsocks会记录该IP。之后，若同样的客户端IP登录microsocks服务器，同时在客户端启用一次验证功能（根据身份认证协议），则可以不需要再次进行身份验证。

```
-q
```

默认情况下，microsocks会启用日志记录功能。当选择这个选项时，日志记录功能被关闭。

```
-i arg
```

当选择这个选项时，后面必须输入参数。如果没有指定参数，则默认参数为0.0.0.0 。该选项指定了microsocks的入站IP，即当一个客户端希望和microsocks服务器建立连接时，使用这个IP地址去连接。

```
-p arg
```

当选择这个选项时，后面必须输入参数（这里的p是小写）。如果没有指定参数，则默认参数为1080 。该选项指定了microsocks的入站端口，即当一个客户端希望和microsocks服务器建立连接时，使用这个端口去连接。

```
-u arg
```

当选择这个选项时，后面必须输入参数。该选项的参数指定了用户登录的名称，即用户名。用户名的长度最好大于5个字符，小于100个字符，以防极端情况下程序出现难以预测的错误。

```
-P arg
```

当选择这个选项时，后面必须输入参数（这里的P是大写）。该选项的参数指定了用户的密码，密码的长度最好大于5个字符，小于100个字符，以防极端情况下程序出现难以预测的错误。

```
-b arg
```

当选择这个选项时，后面必须输入参数。该选项的参数指定了microsocks服务器的出站IP。客户端通过入站IP连接microsocks服务器，而microsocks服务器通过出站IP连接target主机。根据作者提供的信息，在一些设备/主机中，有时会同时存在多个网卡/IP。所以，该选项为出站IP提供了选择。如果没有多网卡/多IP，设置为本机IP（-i选项指定的IP）即可。

## microsocks技术原理

- 读取用户输入，解析用户输入的选项和参数
- 根据用户输入的主机名或IP，创建套接字并监听
- 持续等待客户端的连接，并且为每个连接新建一个执行线程
- 新线程将验证客户身份，microsocks服务器和客户端之间的通信使用了简单的身份验证协议
- 根据客户端发送的地址连接指定的target主机，并为客户和target主机提供数据中转服务

## 源代码分析

对源代码的分析都体现在注释中，详见仓库

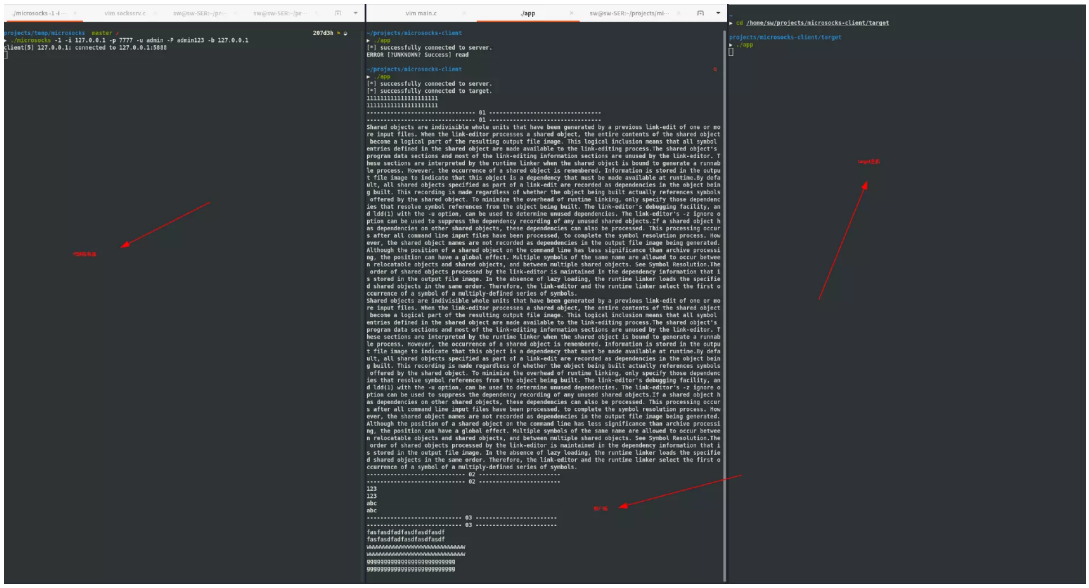
https://github.com/blues2600/sw-test/tree/master

## 环境与配置

不需要额外的环境和配置

## 测试和使用

1. 根据microsocks的身份认证协议，开发了一个测试用的客户端程序
2. 除此之外，还开发了一个程序扮演target主机
3. 按照仓库中介绍的使用方法，可以模拟客户端连接microsocks服务器与target主机通信
4. 通信方式很简单，客户端程序发送数据给microsocks服务器，服务器负责转发数据给target主机，随后target简单的将收到的数据送回给microsocks服务器，microsocks服务器再次转发给客户端


./microsocks -l 1 127.0.0.1 -p 7777 -u admin -P admin123 -b 127.0.0.1
client[8] 127.0.0.1: connected to 127.0.0.1:5080
./app
[+] successfully connected to server.
ERROR [!UNKNOWN] Success] read
./app
[+] successfully connected to server.
[+] successfully connected to target.
11111111111111111111
11111111111111111111
---------- 01 ----------
---------- 02 ----------
123
123
abc
abc
---------- 03 ----------
---------- 03 ----------
fasfasdfasdfasdfasdf
fasfasdfasdfasdfasdf
uAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
uAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
09999999999999999999999990
09999999999999999999999990
cd /home/su/projects/microsocks-client/target
./app