工欲善其事必先利其器，我们来介绍两款用于邮件伪造的测试工具，实现伪造任意用户邮箱。

### SimpleEmailSpoofer

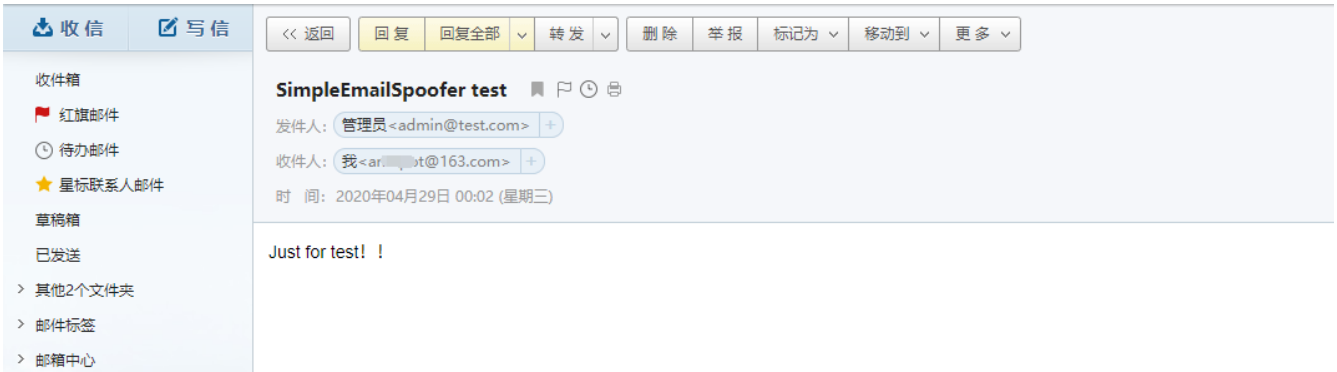
这是一个很简单的python脚本，帮助渗透测试人员进行电子邮件伪造。

Github项目地址：https://github.com/lunarca/SimpleEmailSpoofer

```
git clone https://github.com/lunarca/SimpleEmailSpoofer.git
cd SimpleEmailSpoofer/
pip install -r requirements.txt
#使用示例
./SimpleEmailSpoofer.py -e [Path to Email file] -t [To address] -f [From address] -n [From name] -j [Email subject]
```

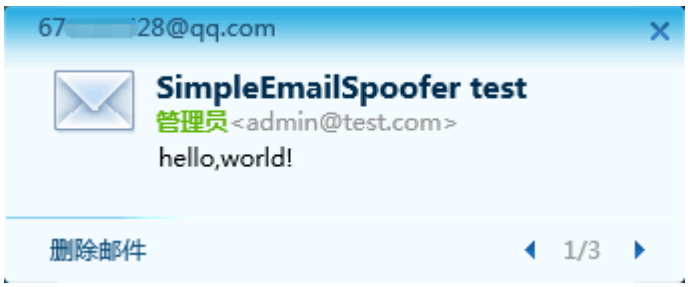
163邮箱测试：

```
python SimpleEmailSpoofer.py -t a******t@163.com  -n 管理员 -f admin@test.com -j "SimpleEmailSpoofer test"  -e 1.txt
```




QQ邮箱演示：

```
python SimpleEmailSpoofer.py -t 67*****28@qq.com  -n 管理员 -f admin@test.com -j "SimpleEmailSpoofer test"  -e 1.txt  -s 192.168.99.240 -p 25 --user test --pass abc123!
```




**Swaks - SMTP界的瑞士军刀**

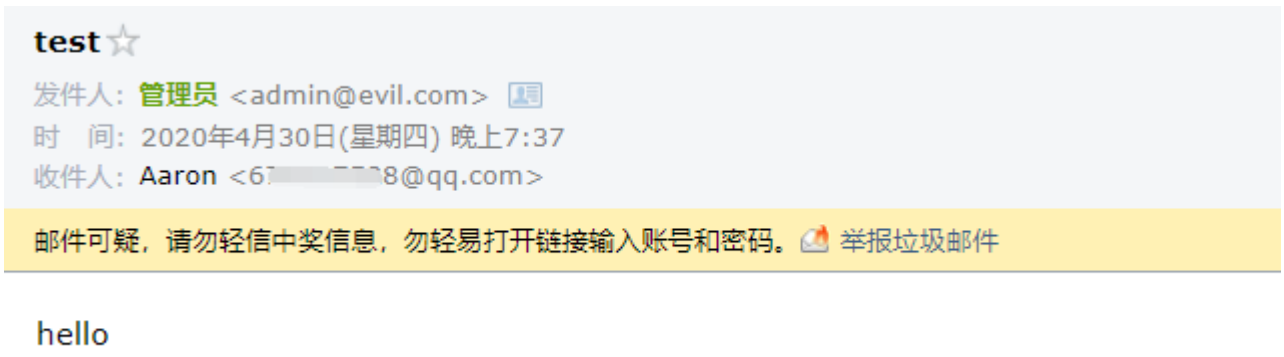
Swaks是由John Jetmore编写和维护的一种功能强大，灵活，可脚本化，可向任意目标发送任意内容的邮件的SMTP测试工具。

Swaks下载地址 ：http://www.jetmore.org/john/code/swaks/

```
#下载文件并解压
wget  http://www.jetmore.org/john/code/swaks/files/swaks-20190914.0.tar.gz
tar -zxvf swaks-20190914.0.tar.gz
cd swaks-20190914.0/
#测试邮箱的连通性
sudo ./swaks --to  67*****28@qq.com
```

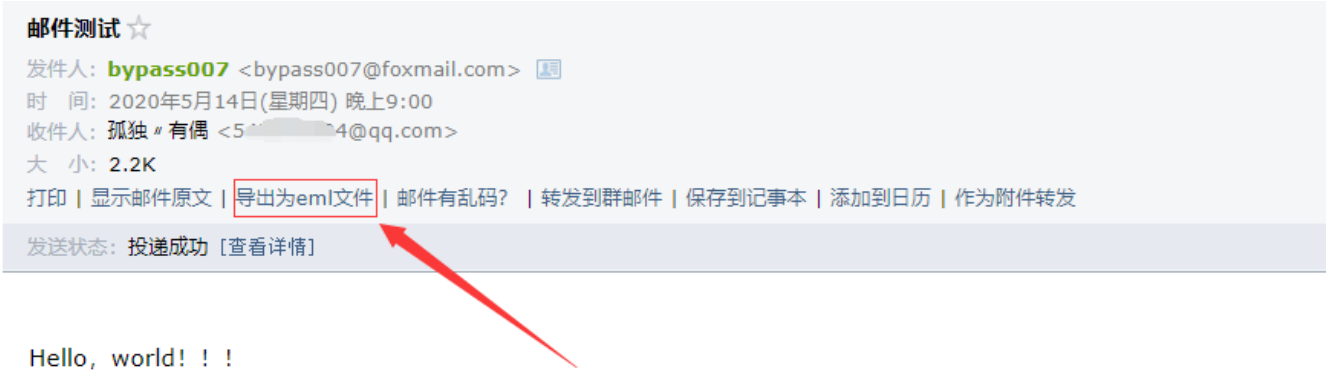
使用示例：

```
sudo ./swaks --to 67*****28@qq.com  --from admin@evil.com  --h-From: '=?GB2312?B?udzA7dSx?=
<admin@evil.com>' --ehlo qq.com --body hello --header "Subject: test"
```




高级用法：

1、首先，在QQ邮箱发送一封测试邮件，导出mail.eml文件




2、删除前面不必要的字段信息，如保留，接收到的邮件头部将会重复这些字段，根据自己的需要构造字段信息。

```
X-QQ-FEAT: ECcPpPTfzVBpKEQC9RgXL3YE9qNEjqv+4MTW/zwOVNdyQtQXWeuRKXkjXmgPB
    WQPkFho49MkkhPVNi5ZbLFw/y5VAoRTqfDtu/wPmfqKhZbVq7rqiBGLYo+WamSRM1gFk7bc
    FI3SUHM55ael2dss93zv8yraCZIUa8btC0xAcrkmtLc9y9faNl0BtMMGCwcX753ppL/dj73
    D2MVvOW7ngpn2Tp9MtxPz6ARQrDnjewJaudcPJ6vUMN/oJ4fDCqinSHW1xHt/RLtQi9jloG
    dqHw==
X-QQ-SSF: 00010000000000080000000000000002
X-QQ-XMAILINFO: NJJAqggpHpVvTTBXdrs2nfpvTuJ3u7IjBPqxBwOSsf8K1OkmR3TOXHEutoMHRz
     x+E7Mcb41JqQBTdKw0QyilbQAs7ai9s5TbRVUB45fgY8mVlENSZz2JCD6GY0eTAjJAVYSwueGF0WM
     K9vALzoaveVE6Ec8aYVmecQVEnOCRNpuaOUy22jrWKIKRE4MheIYhZlzgeZHfmJWwRPwnwtlplRbE
     gZo70HAApxu9b6Bb90RO190dMfmRDltc0IV/k0KNzSoAtg6zWRniXoaGvV9pF0tNcTcbmjrmubdec
     qpDhIUdBk+YVLvVt+KWIPQ8XlSGOLkulcMMjd/xjlJxWyAhXRvj5EJUJJE72UjpflOsz52f6t+gev
     FbplZjK2tPlctYTfrQExQx/cXWT7K2P4ck0InWMSO1EgRF78XuwYMfUL+n01PkioEzVLxPnC3nqVY
     QsEcbKE7eNZkxh0iNhf5Pkqu/xQyIz/s91lmp8a7fwQtZwQmYS/L4CvGafa4TB2b30ec3Ys9u3+gv
     K3DbcePGL96YouICepdIltFrJTOC9eBRHpExTPUnW7UZfxjvEYhyE5a3XeWgMTeDxDP9ibS3QKju5
     h9rMpLlH0QXUawp5My+m7dZMpSi6itS/EZsYKEn6w==
X-HAS-ATTACH: no
X-QQ-BUSINESS-ORIGIN: 2
X-Originating-IP: 120.36.248.144
X-QQ-STYLE:
X-QQ-mid: webmail226t1589461257t8605169
From: "=?gb18030?B?QWFyb24=?=" <bypass007@foxmail.com>
To: "=?gb18030?B?ucK2wKGo09DFvA==?=" <54[redacted]4@qq.com>
Sender: bypass007@foxmail.com
Subject: =?gb18030?B?08q8/rLiytQ=?=
Mime-Version: 1.0
Content-Type: multipart/alternative;
    boundary="----=_NextPart_5EBD4108_1075BD58_64D4E686"
Content-Transfer-Encoding: 8Bit
Date: Thu, 14 May 2020 21:00:56 +0800
X-Priority: 3
Message-ID: <tencent_B3B3AB29BD49C6DD40AEEB8DBB4B7E7B4907@qq.com>
X-QQ-MIME: TCMime 1.0 by Tencent
X-Mailer: QQMail 2.x
X-QQ-Mailer: QQMail 2.x
```

删除红线前面的字段信息

3、使用 --data参数发送邮件，就这样，我们就可以灵活的伪造邮件中的每一个参数。

```
sudo ./swaks --data mail.eml --to 676707628@qq.com --from admin@test.com
```

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。


Bypass