电子邮件欺骗（email spoofing）的根本原因是SMTP协议是不需要身份验证的，攻击者可以利用这个特性伪造电子邮件头，从任意电子邮件地址发送任何人，导致信息看起来来源于某个人或某个地方，而实际却不是真实的源地址。

如果要实现邮箱伪造发件人地址，首先，我们需要一个可以用来发送邮件的SMTP服务器。在这里，我们将介绍如何搭建一个匿名SMTP服务器。

0x01 在线邮件伪造

我们先来使用一个在线伪造邮件地址发送Email邮件的服务，来做一些简单的测试。

查看SPF配置情况：

```
nslookup -type=txt qq.com
```

Emkei's Fake Mailer：https://emkei.cz/

Free online fake mailer with attachments, encryption,
HTML editor and advanced settings...

From Name: 管理员
From E-mail: admin@test.com
To: 67 28@qq.com
Subject: test
Attachment: 选择文件 未选择任何文件
Attach another file
Advanced Settings
Content-Type: text/plain text/html Editor
Text: 您的密码已到期，请尽快修改密码！！！

Solve reCAPTCHA v2 instead of v3
Send Clear

1、test.com未配置SPF，伪造发件人邮件为`admin@test.com`，发送邮件，QQ邮箱成功接收到邮件：

2、某个域名xxx.net 配置了SPF，伪造`admin@xxx.net`发送邮件，邮件进入垃圾箱。

通过以上测试，我们可以得到一个简单的结论，QQ邮箱在接收到邮件时，会检查域名的SPF记录，未配置SPF的域名，邮箱容易被伪造并成功投递到目标邮箱；已经配置了SPF的域名，检验后会被投递到垃圾箱。

其实可以发现，这个在线邮件伪造emkei.cz，通过查看邮件头，可知它是用postfix搭建。那么，我们也可以使用postfix搭建匿名SMTP邮件服务器，以便更灵活地去伪造邮箱任意字段。

0x02 搭建匿名SMTP服务器

使用postfix搭建匿名SMTP服务器

环境：CentOS7

1、安装postfix

```
#安装postfix
yum install postfix
```

2、修改main.cf配置文件

```
vi /etc/postfix/main.cf
    # 75行:设置myhostname
    myhostname = mail.test.com
```

```
    # 83行：设置域名
    mydomain = test.com
    # 99行：设置myorigin
    myorigin = $mydomain
    # 116行：默认是localhost，修改成all
    inet_interfaces = all
    # 119行：推荐ipv4，如果支持ipv6，则可以为all
    inet_protocols = ipv4
    # 165行：设置mydestination
    mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
    # 264行：指定内网和本地的IP地址范围
    mynetworks = 192.168.0.0/16，127.0.0.0/8
    # 419行：取消注释，邮件保存目录
    home_mailbox = Maildir/
    # 572行：取消注释，设置banner。
    smtpd_banner = $myhostname ESMTP
```

3、启动postfix服务

```
systemctl start postfix

#关闭防火墙
systemctl stop firewalld.service
```

测试邮件搭建成功的几种方式：

第一种：使用mail发送邮件

```
#安装mailx
yum install mailx

#发送邮件测试
echo "email content" | mail -s "title" a*****t@163.com
```

查看邮件发送记录：

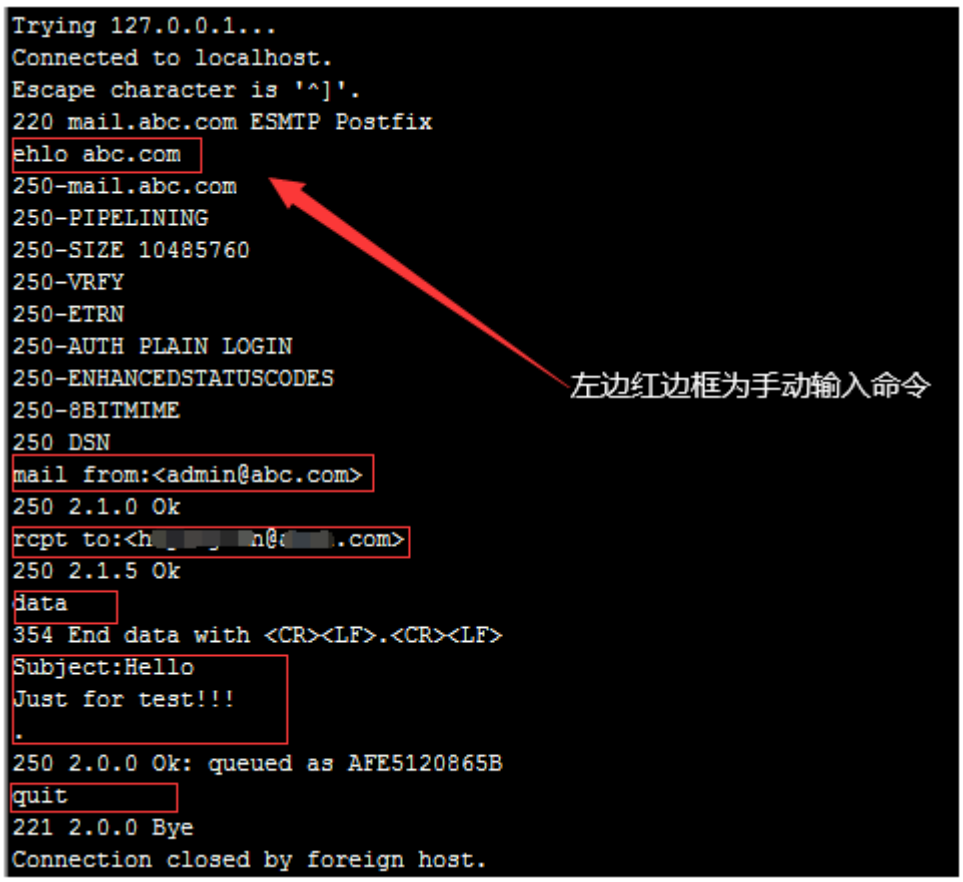
```
#tail -f /var/log/maillog

Apr 28 09:27:14 centos postfix/smtpd[108012]: connect from localhost[127.0.0.1]
Apr 28 09:27:15 centos postfix/smtpd[108012]: 0170D403916: client=localhost[127.0.0.1]
Apr 28 09:27:15 centos postfix/cleanup[108015]: 0170D403916: message-id=
<20200428012715.0170D403916@mail.abc.com>
Apr 28 09:27:15 centos postfix/qmgr[39469]: 0170D403916: from=<root@test.com>, size=716,
nrcpt=1 (queue active)
Apr 28 09:27:15 centos postfix/smtpd[108012]: disconnect from localhost[127.0.0.1]
Apr 28 09:27:15 centos postfix/smtp[108016]: connect to
mx3.qq.com[240e:ff:f101:10::127]:25: Network is unreachable
Apr 28 09:27:16 centos postfix/smtp[108016]: 0170D403916: to=<a*****t@163.com>,
relay=mx3.qq.com[58.251.110.111]:25, delay=1.5, delays=0.03/0.03/0.37/1, dsn=2.0.0,
status=sent (250 Ok: queued as )
Apr 28 09:27:16 centos postfix/qmgr[39469]: 0170D403916: removed
```

从邮件日志看到`status=sent`，确认邮件发送成功。

第二种：通过telnet使用smtp协议发送邮件

```
telnet localhost 25
```



测试邮箱成功接收到邮件：

第三种：使用Python脚本发送邮件

```
#!/usr/bin/python
# -*- coding: UTF-8 -*-
import smtplib
from email.mime.text import MIMEText
from email.header import Header
sender = 'admin@test.com'

receivers = ['antapot@163.com']

message = MIMEText('Just for test', 'plain', 'utf-8')
message['From'] = Header("admin")   # 发送者
message['To'] =  Header("test")        # 接收者

subject = 'SMTP 邮件测试'
message['Subject'] = Header(subject, 'utf-8')


try:
    smtpObj = smtplib.SMTP('localhost')
    smtpObj.sendmail(sender, receivers, message.as_string())
    print "邮件发送成功"
except smtplib.SMTPException:
    print "Error: 无法发送邮件"
```

使用第三方邮件服务器，往往会受限于SMTP服务商的限制，但也有一定的好处，这些权威的邮件服务商的地址往往会被大部分邮件服务商加入白名单。

国内主流的邮箱有：QQ邮箱（qq和foxmail）、网易邮箱（包括163、126和yeah邮箱）、新浪邮箱、搜狐闪电邮箱、移动139邮箱、电信189邮箱等等。

国外的第三方SMTP服务商：SendGrid、mailgun等

不同的邮箱系统，接收邮件安全策略是不同；不同的SMTP服务商，发送邮件的限制也是不一样，具体会发生什么样的化学作用，还需具体进一步去测试。