信息安全实验：实现一个fake-wifi

原创

zekdot 于 2018-10-17 00:56:16 发布 1735 收藏 9
文章标签： 信息安全 WIFI

一、引言

这是信息安全课上老师讲的一个案例吧，某人创建一个假的热点，然后等待人来连接，然后去获取连接者的数据。

这个实验感觉还是比较有意思的，毕竟以前总听说过假WIFI泄露数据的案例但从来没有亲手实验过，所以这也算是一个比较好的机会吧，更何况交实验报告还能拿分。。

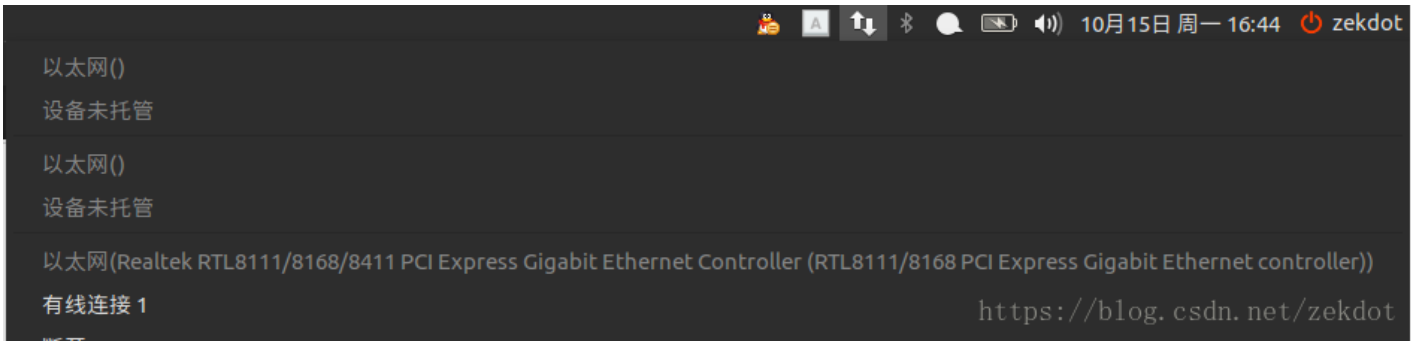
二、开放新的热点：

虽然这个实验名称叫做fake-wifi,但本质上这是一个真正的wifi，只是开放者可以监听到其中的数据包而已，所以我们首先要做的是开放一个热点。

这里我用的是Ubuntu 16.04来开放热点，尽管老师说过Linux下一行命令就可以实现热点的开放，但是我没有找到这样的方法，一位博主给出了命令行的开放方法，不过要下额外的软件，并且配置也比较多：

Ubuntu16.04命令行方式开放热点

这里我使用了一种图形化的方法，首先保证自己有了有线连接，在右上角点击左数第三个网络连接的图标，然后出现很多选项，选择"编辑链接"。



编辑所有链接

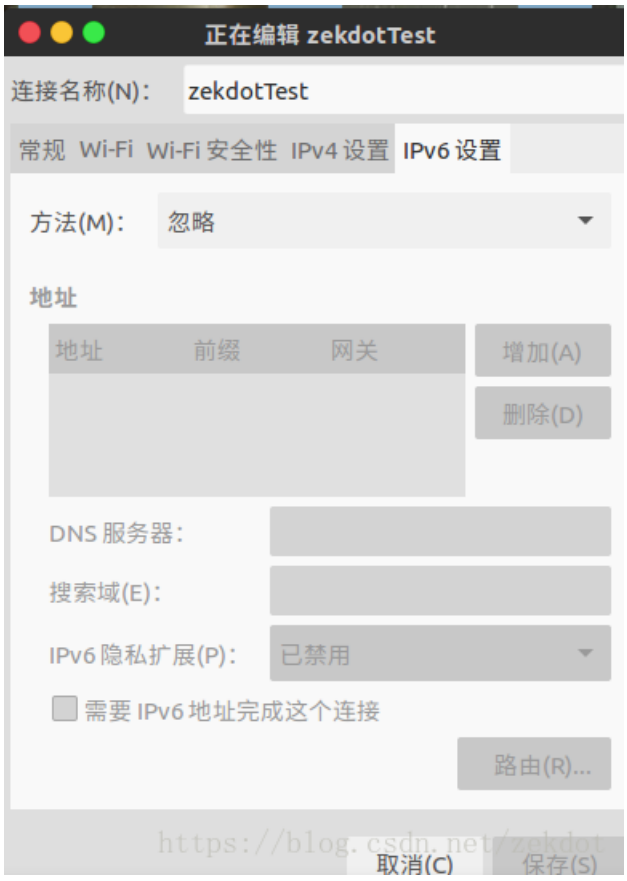
在这个界面选择增加，然后选择WIFI类型。

选择WIFI类型

连接名称自己起，这里展示一下各标签卡的配置：


正在编辑 zekdotTest
连接名称(N)：
zekdotTest
常规
Wi-Fi
Wi-Fi 安全性
IPv4 设置
IPv6 设置
SSID：
zekdotTest
模式(O)：
热点
波段(D)：
自动
频道(H)：
默认
设备(D)：
克隆 MAC 地址(L)：
MTU：
自动
字节
取消(C)
保存(S)


正在编辑 zekdotTest
连接名称(N)：
zekdotTest
常规
Wi-Fi
Wi-Fi 安全性
IPv4 设置
IPv6 设置
安全(E)：
WPA 及 WPA2 个人
密码(P)：
123456789
显示密码(W)
取消(C)
保存(S)



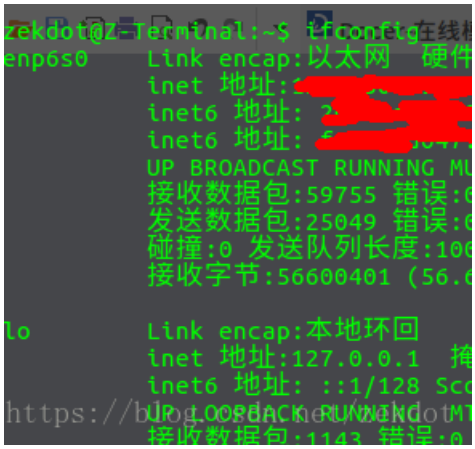
点击保存即可，然后用电脑连接到新创建的WIFI，如果找不到的话，可以链接到隐藏的WIFI网络。

选择刚创建的热点

点击连接即可，然后就可以用手机去连接这个热点了，这里我连接的时候手机上显示WIFI不能上网，重启了一下电脑然后再连接就正常了。

三、监听流量

首先要做的的是找到要监听的接口，这里我们可以使用tcpdump命令，在使用该命令之前，我们需要先找到要监听的接口，这里使用ifconfig命令，可以看到：



使用ipconfig命令之后

那么接口的名称就可以使用enp6s0，后面其实还有一个名称为wlp7s0的，监听这个也是可以的。个人感觉后者应该就是WIFI对应的接口，前者则是主接口，而本电脑开热点的话数据包一定要经过主接口，所以监听哪个应该都可以。

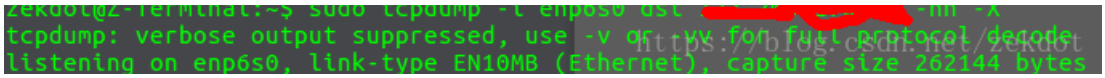
在去尝试更多的命令之前，我首先尝试去窃取一下向自己之前做的网站发送的密码，因为我的网站没用https，而且ip地址什么的我也都知道，所以比较好实现，这里使用的命令如下：

```
sudo tcpdump -i enp6s0 dst xxx.xxx.xx.xxx -nn -X
```

这里解释一下这个命令：

tcpdump属于特权命令，因此需要sudo来执行，-i参数来指定接口，也就是之前找到的enp6s0，dst则是数据包的目标点，后面接的是我服务器的地址，-nn指直接用IP名称及端口而不是服务来显示，-X指的是以16进制方式显示封包的内容。

开启之后，会进入到如下的状态：

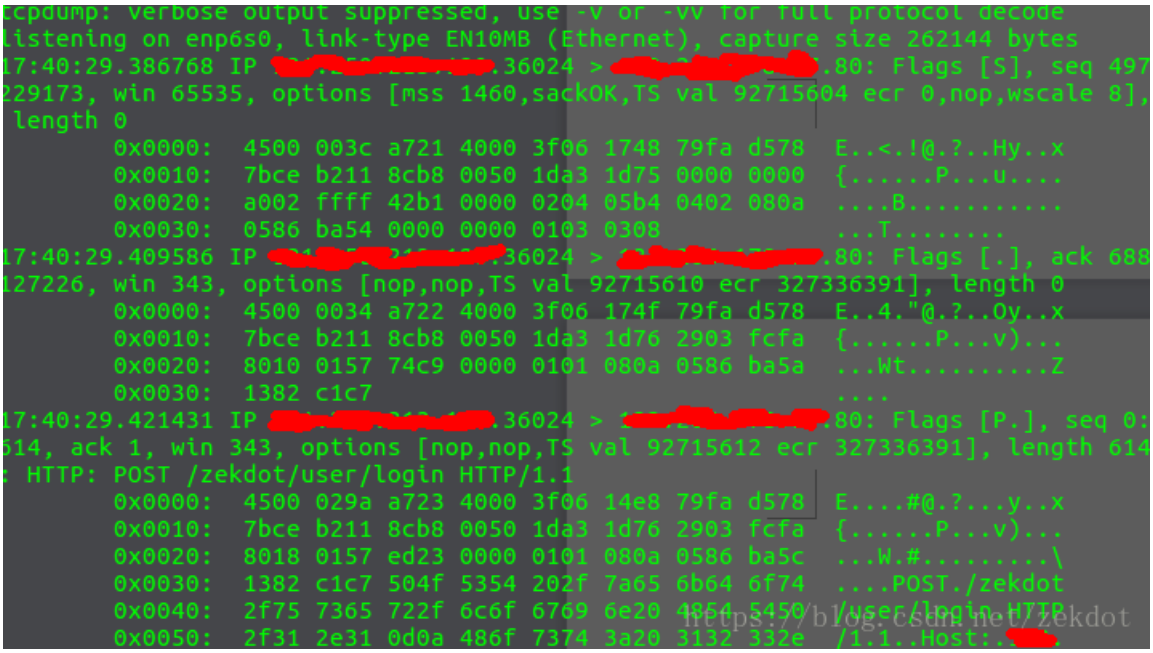


使用tcpdump之后显示的内容

这个时候，用连上热点的手机给我的网站发送一条数据，填好信息，然后点击提交：

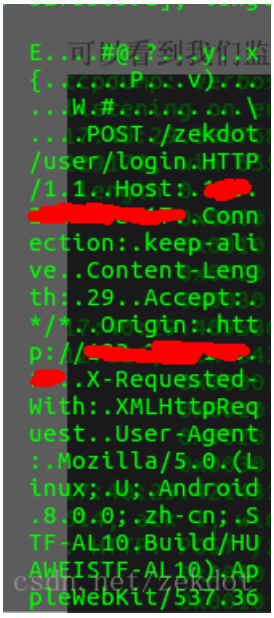
网站的样式，只有一个表单

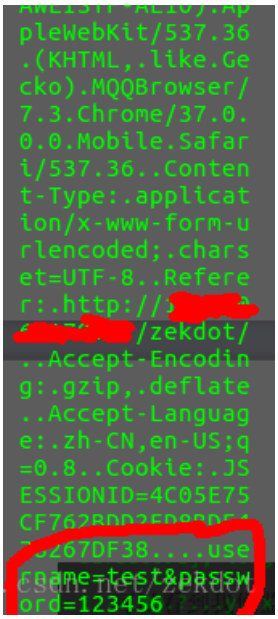
可以看到我们监听的界面出现了很多数据：



监听到了数据

这里也表明我们监听到了数据包，然后我们需要分析的是HTTP的POST请求，就是我刚才没有截完图的部分，如图：





从数据中可以看到密码明文

这里我圈出来的部分就是刚才发送的用户名和密码，这也说明我们成功监听到了关键数据。

四、重定向页面到某网站上

由于https协议下，传输的数据是加密的，所以直接窃听是不可取的，因此本实验的目的更多是通过钓鱼网站来获取https协议的传输数据。

1.源网站使用HTTP头

这个比较好实现，由于现在使用HTTP协议的网站不多了，所以我还是使用我自己的云服务器来演示，由于知道服务器的ip地址，这个实验更加的容易了，现在是在没有重定向的情况下访问该网站的某个页面。

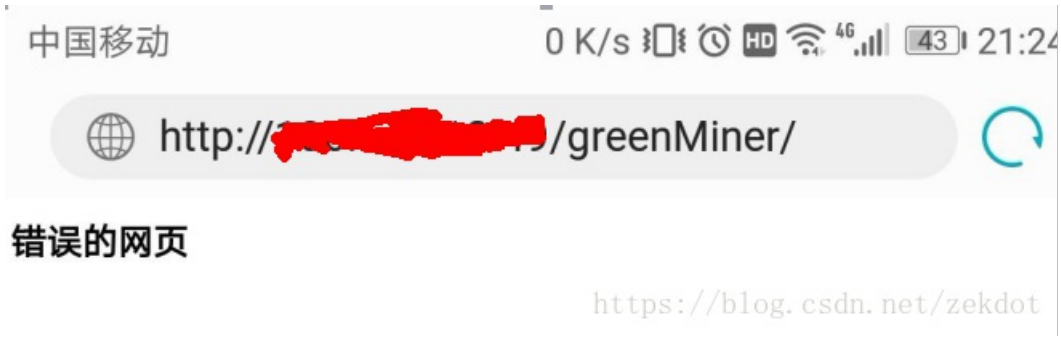
访问原来的网址

如图，这是在正常访问情况下的结果，然后我们开始进行配置，使得使用我们热点的人访问该页面时重定向到某个我们想展示给他的网页，这个与本来要访问的页面对应的网页我建立在了我本机的tomcat服务器的目录下，内容只有一行字”错误的页面”。

使用iptables命令来重定向ip

如图所示，我们使用了iptables命令，这里的关键在于-d后面的是原本要访问的ip地址，--to-destination后面的是重定向后的地址，回车之后就实现了一个重定向。

当设置之后我们再访问原来的URL：



再次访问该网址的对应页面

可以看到，此时已经跳转到了我们想要展示给对方的页面，即重定向页面成功。

*这里iptables命令重定向之后，如果想要删除这条重定向，可以用如下命令（具体原理可以百度）：

```
sudo iptables -nt nat -L --line-numbers    #查看PREOUTING下的所有规则
sudo iptables -t nat -D PREROUTING 1    #删除对应的规则
```

2.源网站使用HTTPS头

其实HTTPS现在位置还算是一个比较好的协议了，虽然本实验能在一定程度上来进行欺骗，但实际上我们用手机去访问这个冒牌网站时，还是有警告信息的，这也一定程度上证明了HTTPS协议的安全性，这里我用到了tomcat服务器，别的服务器应该也可以，关键是前者用习惯了。

首先我们要做的是DNS劫持，即将用户本来要访问的网址解析为一个放有钓鱼网站的地址上去，在Linux上可以通过一个叫做dnsmasq的软件来实现，通过apt-get就能下载并安装这款软件。

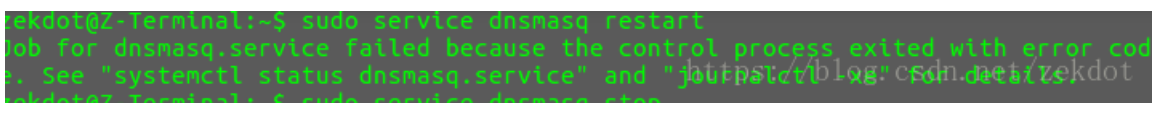
安装好之后我们首先需要修改其配置文件，即/etc/dnsmasq.conf，这里我针对的是QQ空间的手机网址，因此我把手机浏览器上登录QQ空间的所有域名都解析为了本机地址，如图：

书写解析规则

然后重启dnsmasq服务即可，在Ubuntu下命令为

```
sudo service dnsmasq restart
```

*这里有必要说一下，如果之后又修改了配置文件然后重启之前，要断掉WIFI，关掉相关链接的网页，否则重启可能失败，出现如图情况：



失败的重启

这些操作做完以后，再去访问手机QQ登录页面时，会发现如图的情况：

访问手机QQ登录页面

证明域名劫持成功，可以ping一下网址来进行验证：

ping qq.com

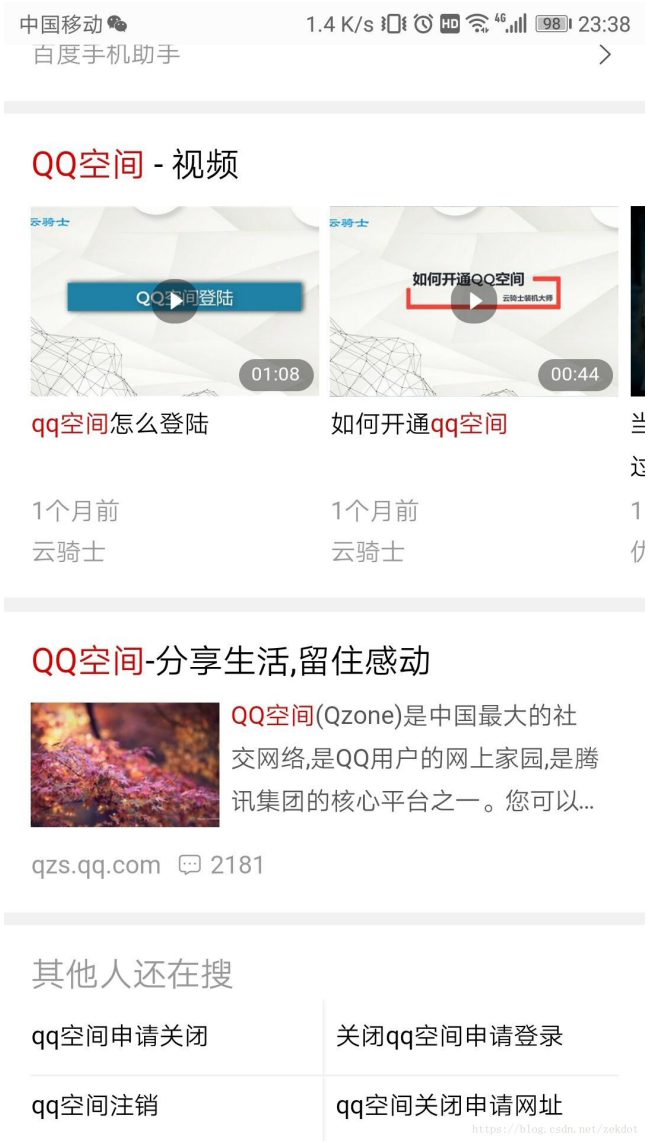
下一步就是要换上自己的钓鱼网站，这里我使用了tomcat服务器，所以面对的最主要的问题就是如何让其支持https访问，网上的教程还是挺多的，基本思路就是制作证书，然后修改端口为443，这样用https访问tomcat就能出现结果了，这里具体过程就不再详述了，可以参考这篇博客：

tomcat配置https协议

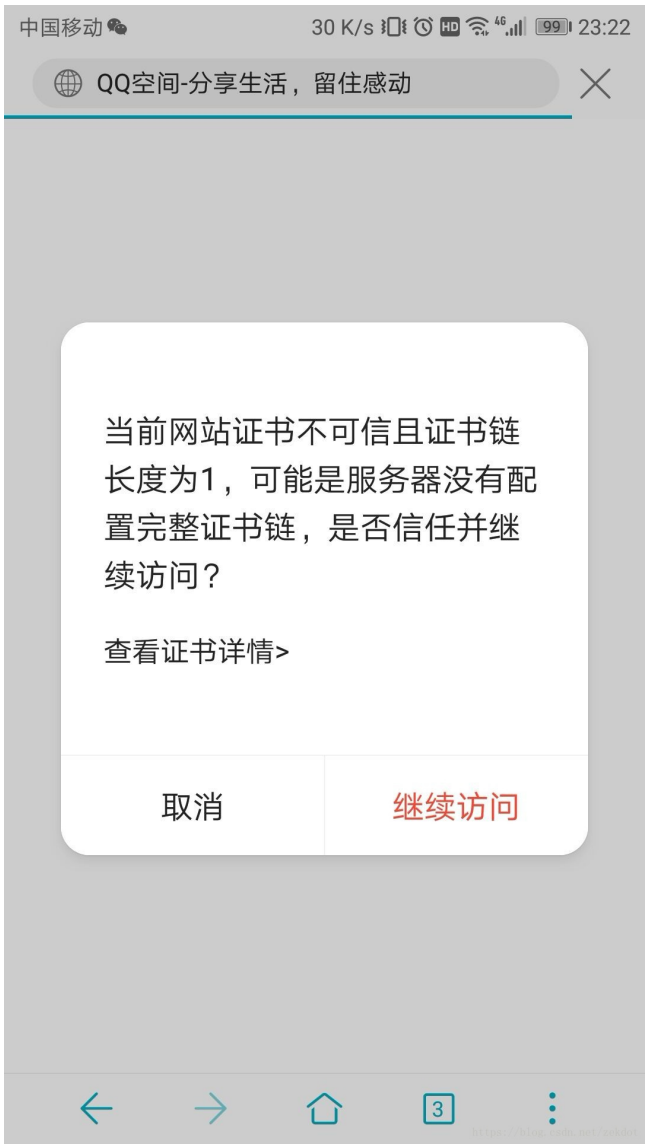
最后就是换上我们自己的假网页了，这里我随便写了一个，意思到了就行：

自己写的假网页

结束这些之后，我们开启tomcat服务器，然后尝试从连上了fake-wifi热点的手机上面去访问QQ空间登录页面，如图：



当我们去访问“QQ空间-分享生活，留住感动”时：



浏览器发出警告

这里浏览器已经出现了警告，因此这种欺骗可能在现实中不会成功或者对一些安全意识极差的用户能够成功，这里出于实验的原因我们按下继续访问：


中国移动
8.3 K/s
23:38
QQ空间-分享生活，留住感动
我是个假网站emmm
QQ号码:
密码:
3
https://blog.csdn.net/zekdot

显示出了假网页

网址却是真的

如图，重定向到了之前我们设置的钓鱼网站上，并且域名也是一本正经的QQ空间登录域名了。

五、总结

在本次试验中，我搭建了一个fake-wifi，并尝试在http协议下监听了用户数据，以及在http/https协议下将用户访问的正常网站重定向到钓鱼网站上。

这个实验中的欺骗其实在现实中不太行得通，因为这个欺骗成功的前提是用户的安全意识极低，可以随便连没有加密的未知WIFI，并且在浏览器预警时选择忽略。而现在的网民的安全意识还是比较高的，并且WIFI安全问题也频繁被报道，这也更让人们在连接WIFI以及使用WIFI时更加谨慎了。不过这个实验至少对我这样经常忽略各种警告的人还是有一定的警示作用的。

本次的实验虽然不是很复杂，不过对我个人还是有一定的帮助的。它为我开启了信息安全这一领域的一扇门，让我认识到要实现某些攻击手段，不一定要写很多的代码，也不一定要有很高超的计算能力，而在于知识的积累，懂得技术越多，能做的事也就越多，这也充分说明了学习的重要性。