# 简介

WiFi钓鱼踩坑指南，文章选取了GitHub Stars靠前的5个工具进行对比，讲述的是本人在使用这5个工具时所遇到的坑，同时说说各个工具的使用体验。

# 准备工作

## 系统选择

毋庸置疑是Kali Linux了，当然如果大佬已有趁手的Linux也可以。

然后就是更新一波apt

apt-get update

分享一下我用的源/etc/apt/sources.list

#清华源

deb http://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling main contrib non-free

deb-src https://mirrors.tuna.tsinghua.edu.cn/kali kali-rolling main contrib non-free

#中科大源

deb http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib

deb-src http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib

#阿里云

deb http://mirrors.aliyun.com/kali kali-rolling main non-free contrib

deb-src http://mirrors.aliyun.com/kali kali-rolling main non-free contrib

#浙大源

deb http://mirrors.zju.edu.cn/kali kali-rolling main contrib non-free

deb-src http://mirrors.zju.edu.cn/kali kali-rolling main contrib non-free

#官方源

deb http://http.kali.org/kali kali-rolling main non-free contrib

deb-src http://http.kali.org/kali kali-rolling main non-free contrib

## 外置网卡

至少一个外置无线网卡，需支持Monitor模式，兼容Linux系统（市面上只兼容Windows的比较多）

在下用的是TL-WN722N，150Mbps，大约100RMB，买了几年了依然坚挺。

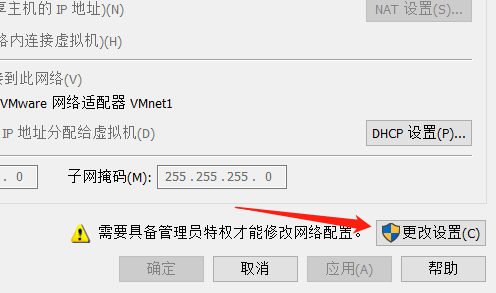
## 配置技巧

分享个配置技巧，有两个外置无线网卡的大佬请无视并留下联系方式。

以下步骤建议在开启虚拟机前配置。

遇到需要双网卡的钓鱼工具，可将虚拟机桥接无线网卡，当作第二外置网卡使用。

编辑 - 虚拟网络编辑器 - 更改配置



步骤一：添加网络。

步骤二：选择桥接模式，同时选择桥接物理机无线网卡。

步骤三：生成



# wifi-cracking（8.2k+ Stars）

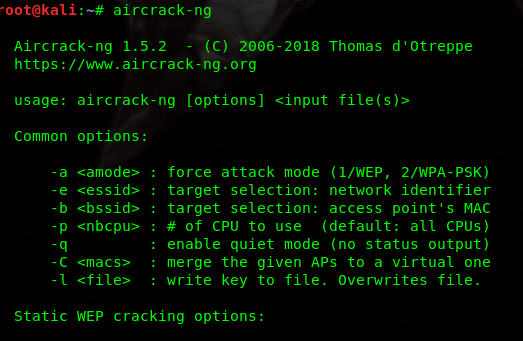
整合aircrack-ng、airmon-ng、airodump-ng、aireplay-ng、airbase-ng的攻击套件，可以说是

WiFi攻击组件中骨灰级的存在。

GitHub地址：https://github.com/brannondorsey/wifi-cracking

## 安装流程

apt-get install aircrack-ng

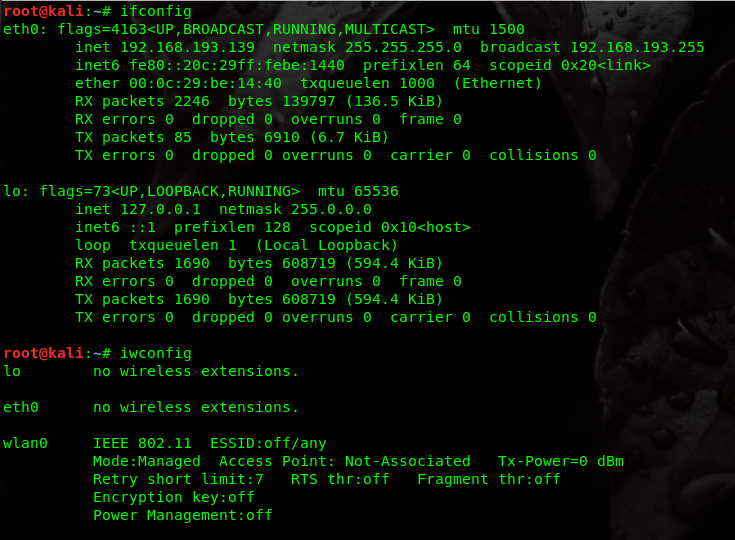


## 使用教程

### 准备阶段

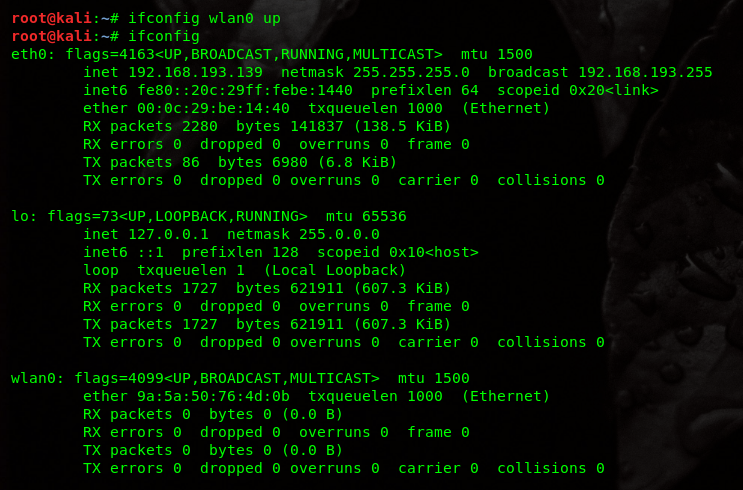
步骤一：查看wlan0是否准备完毕（注意此时的Mode是Managed，而且ifconfig是看不到wlan0网卡的）。

iwconfig



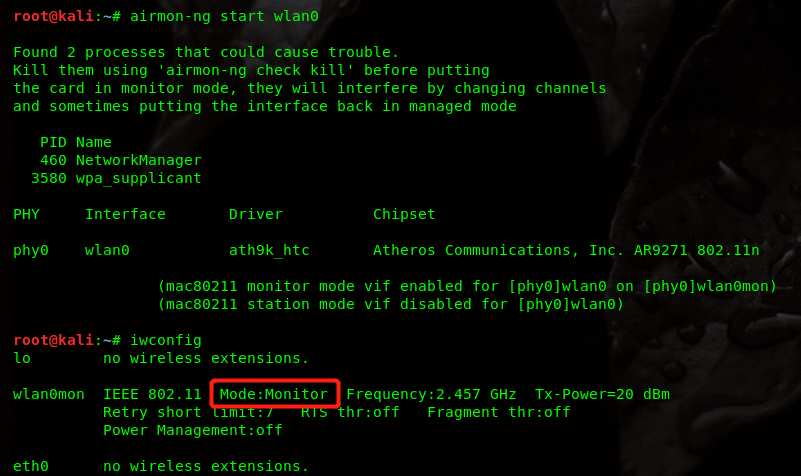
步骤二：启动wlan0网卡

ifconfig wlan0 up



步骤三：开启Monitor模式

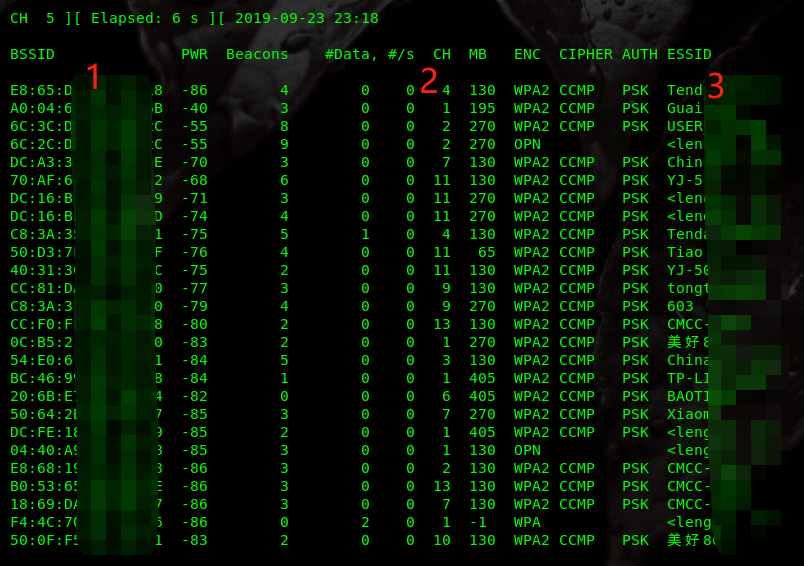
airmon-ng start wlan0



### 探测阶段

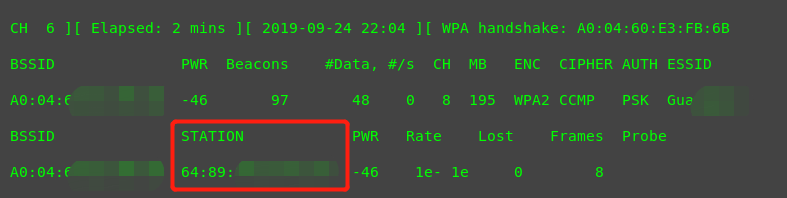
目的：记录有效信息BSSID（AP物理地址）、CH（信道）、ESSID（AP名称）

airodump-ng wlan0mon



进行针对探测

airodump-ng --bssid AA:AA:AA:AA:AA:AA wlan0mon



### 抓包阶段

目的：抓握手包 -> 破解密码 -> 伪造AP -> 嘿嘿嘿

选项解释：--bssid和-c分别对应选中ESSID的BSSID和CH。

注意：抓包阶段需一直开启，直到攻击阶段成功抓到握手包

情景一：抓ivs包（一般用作下一阶段的爆破）

airodump-ng --bssid AA:AA:AA:AA:AA:AA -w ./hackivs -c 1 wlan0mon --ivs



情景二：抓pcap, ivs, csv, gps, kismet, netxml, logcsv包

airodump-ng --bssid AA:AA:AA:AA:AA:AA -w ./hackpcap -c 1 wlan0mon --output-format pcap

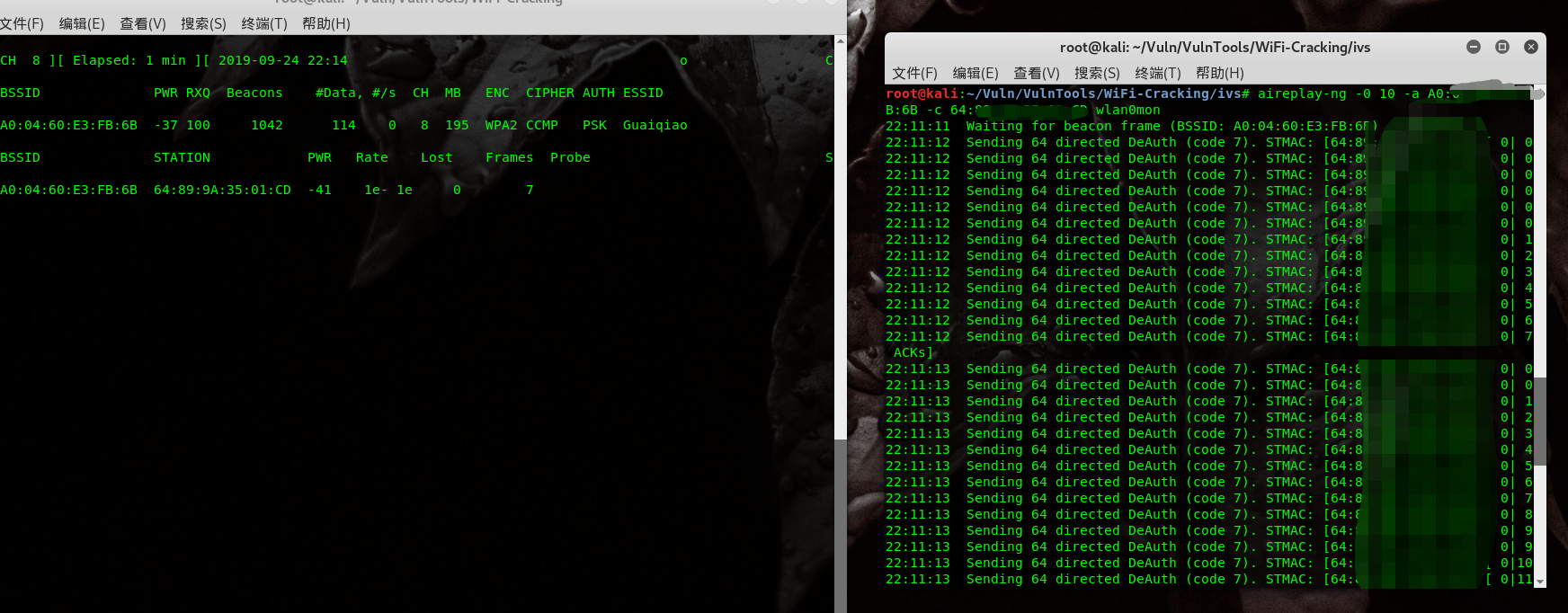


### 攻击阶段

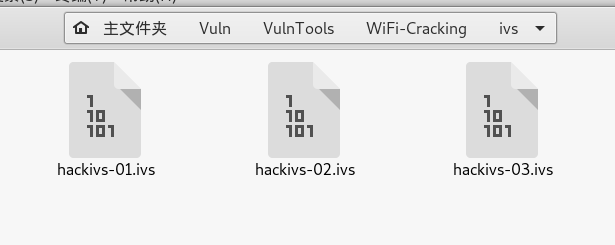
目的：打掉目标AP正在连接的用户，等待其重新连接回目标AP，抓取这个过程的handshak握手包。

选项解释：-a是目标AP的BSSID，-c是目标AP下Station的BSSID，-0是deauth包个数（10代表发10次）

aireplay-ng -0 10 -a 24:05:0F:22:EF:82 -c 20:08:ED:BE:D4:2B wlan0mon



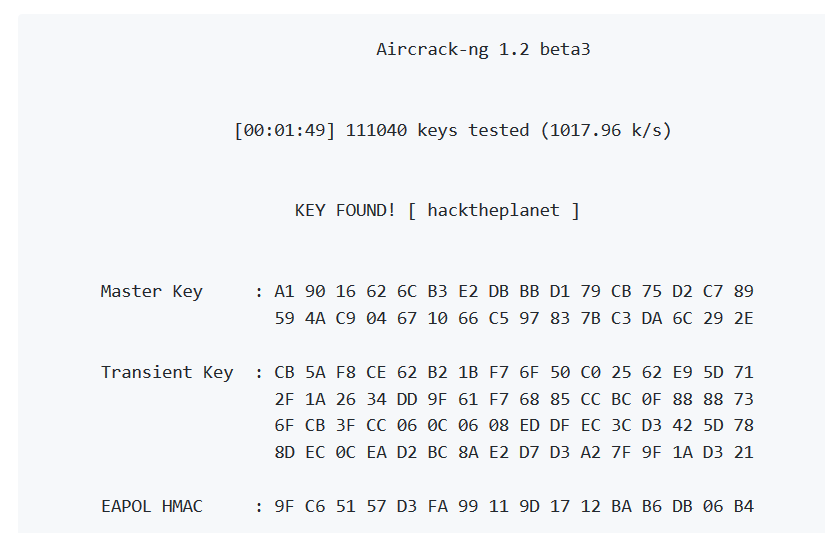
直到目录有握手包



### 爆破阶段

作用：根据抓包阶段获取的握手包进行密码暴力破解。

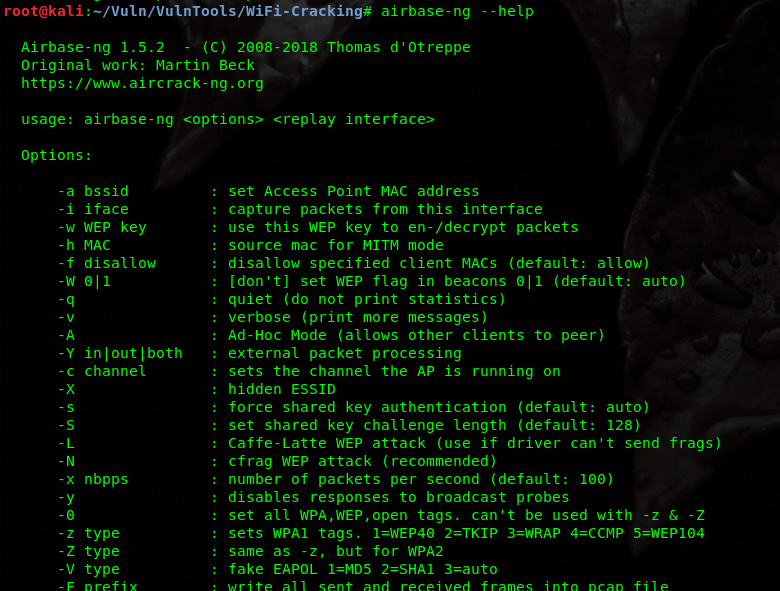
aircrack-ng -w dict.txt ./hackivs.ivs



### 伪造阶段

选项解释：-a是伪造AP的BSSID（一般用目标AP的BSSID）

airbase-ng -a AA:AA:AA:AA:AA:AA --essid fakename -c 11 -Z 4 wlan0mon



作用：宏范式攻击打目标AP，使得受害者连接伪造AP

aireplay-ng --deauth 0 -a AA:AA:AA:AA:AA:AA wlan0mon

### 结束阶段

还原外置无线网卡模式

airmon-ng stop wlan0mon

## 结束语

优点：骨灰级工具

缺点：

1、airbase-ng针对的是WEP协议的数据，现在大多都是WPA2加密，仿真度不高。

2、DHCP需要另外配置，需要修改各种配置文件，较为繁琐。

3、伪造AP时没得设置密码（可能我姿势不对）。

# flusion（1.9k+ Stars）

Fluxion是一种安全审核和社会工程研究工具。 这是vk496对linset的翻版，（希望）有更少的错误和更多的功能。 该脚本尝试通过社会工程（网络钓鱼）攻击从目标访问点检索WPA / WPA2密钥。 它与最新版本的Kali（滚动）兼容。 Fluxion的攻击设置大部分是手动的，但是实验性自动模式可以处理某些攻击的设置参数。

GitHub地址：https://github.com/FluxionNetwork/fluxion



## 前景提要

虚拟机必须提前备份，因为安装完组件后，下次启动系统会大概率报以下错误。猜测可能是和我之前安装的某些包冲突了。

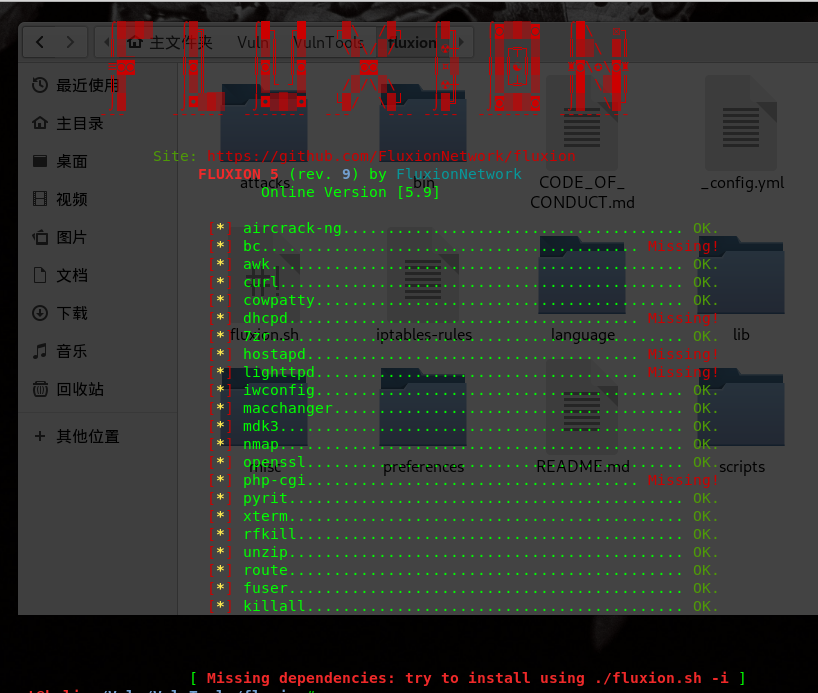


## 安装流程

git clone https://github.com/FluxionNetwork/fluxion.git

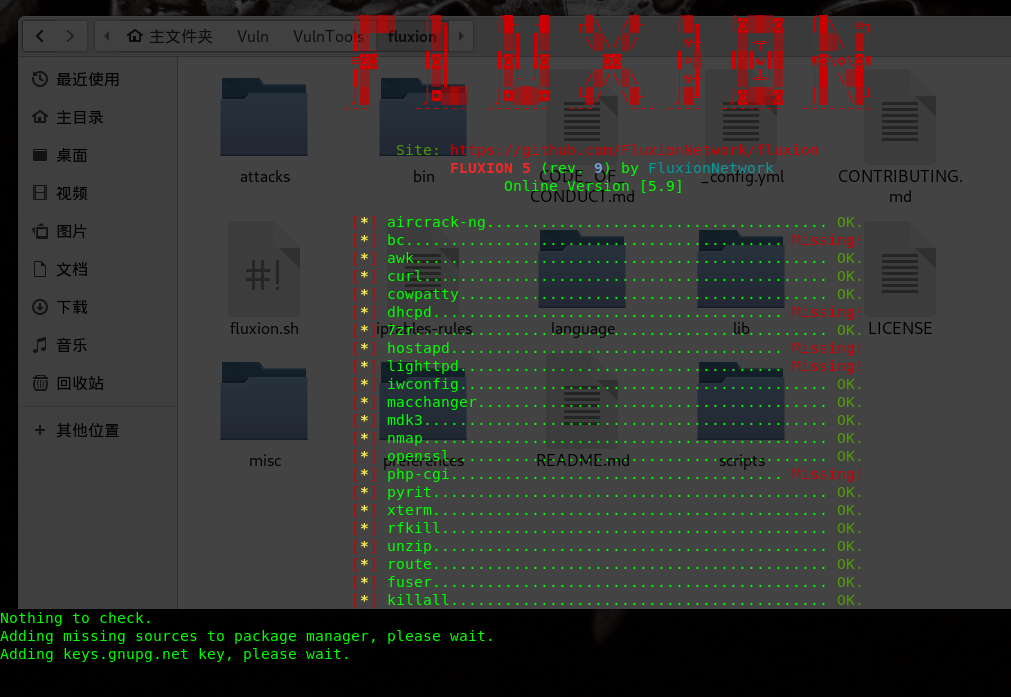
第一次启动时会有许多依赖组件未缺失。

./fluxion.sh



启动安装

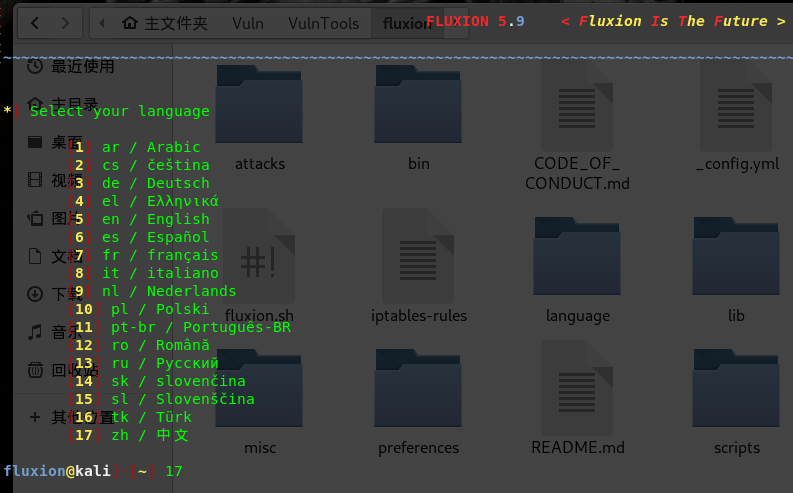
./fluxion.sh -i



## 使用教程

### 启动fluxion

选中文



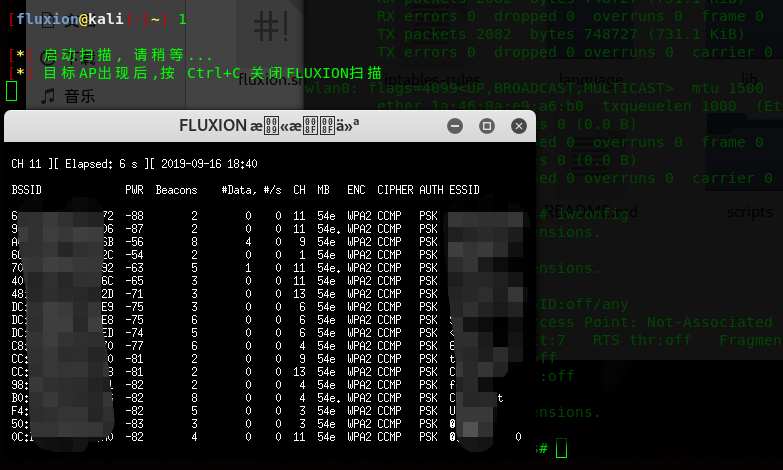
选择攻击方式，伪造钓鱼WiFi当然选1了



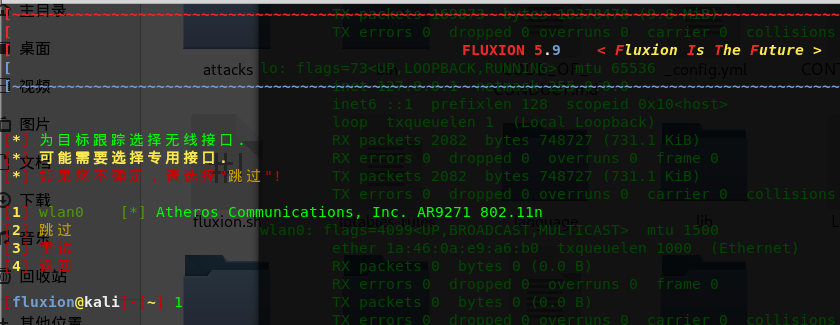
选择扫描信道的频率



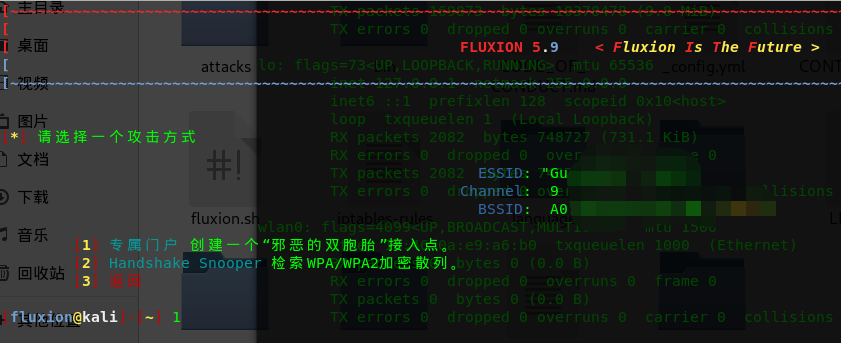
启动扫描，当你看到ESSID出现目标AP就可以Ctrl+C结束扫描。



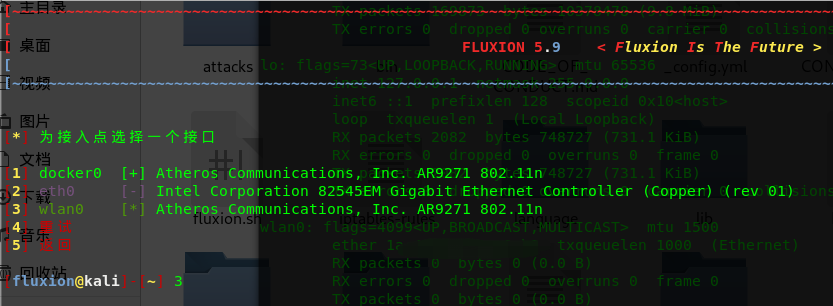
选wlan0



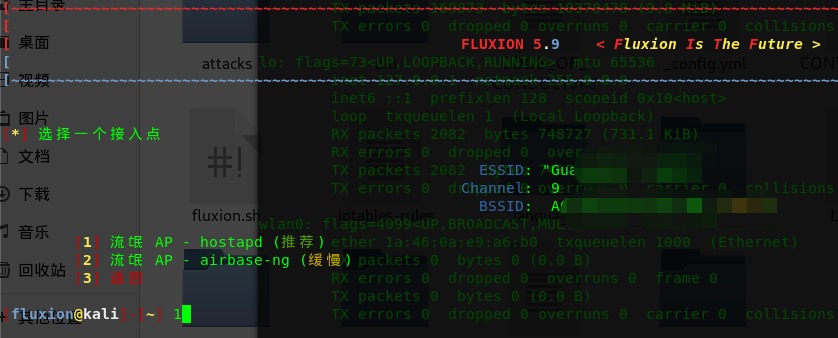
构造伪造AP



原本打算选择eth0作为第二个外置网卡，但没能成功，所以应该用第二个外置网卡会好些。



选择伪造AP接入点模式



后面处于懵逼状态，怎么都不能成功建立钓鱼AP，当时猜测是需要两个外置无线网卡才搞得动。再后来重启直接嗝屁，虽然作者有详细的解决方案说明，但我还是选择放弃治疗。

## 结束语

一开始用的时候感觉很高大上，但当我第一次重启后就懵逼了，虚拟机直接启动不了。后面尝试了很多次，安装完重启就歇菜。

优点：

1、将WiFi-cracking的各个步骤整合到一起，省去很多复制粘贴的操作。

2、语言兼容性强。

缺点：

1、自带抓包工具很弱鸡，没成功过一次，最后是用WiFi-cracking抓的包。

2、安装完重启就嗝屁，很迷。

3、需要两个外置无线网卡，可能可以只用一个外置，不过没试成功。

4、会给网卡重命名，估计是为了启动Monitor模式改的名。但后面有个操作没有返回按钮，又不能命令行结束掉，只能关掉整个CMD。此时网卡名字还是乱的，没有触发网卡恢复，如果对系统操作不熟悉的话，就很难受。

# WiFi-Pumpkin（2.6k+ Stars）

WiFi南瓜（我猜作者很喜欢过万圣节）是一个恶意AP框架，可轻松创建这些虚假网络，同时将合法流量往返于毫无戒心的目标之间。 它具有各种功能，包括流氓Wi-Fi接入点，对客户端AP的取消身份验证攻击，探测请求和凭据监视器，透明代理，Windows更新攻击，网络钓鱼管理器，ARP中毒，DNS欺骗，南瓜代理和图像捕获 在飞行中。 此外，WiFi-Pumpkin是一个非常完整的框架，用于审核Wi-Fi安全性，功能列表非常广泛。

Github地址：https://github.com/P0cL4bs/WiFi-Pumpkin

## 安装流程

git clone https://github.com/P0cL4bs/WiFi-Pumpkin.git

cd WiFi-Pumpkin

chmod +x installer.sh

./installer.sh -install

pip install config

pip install netifaces

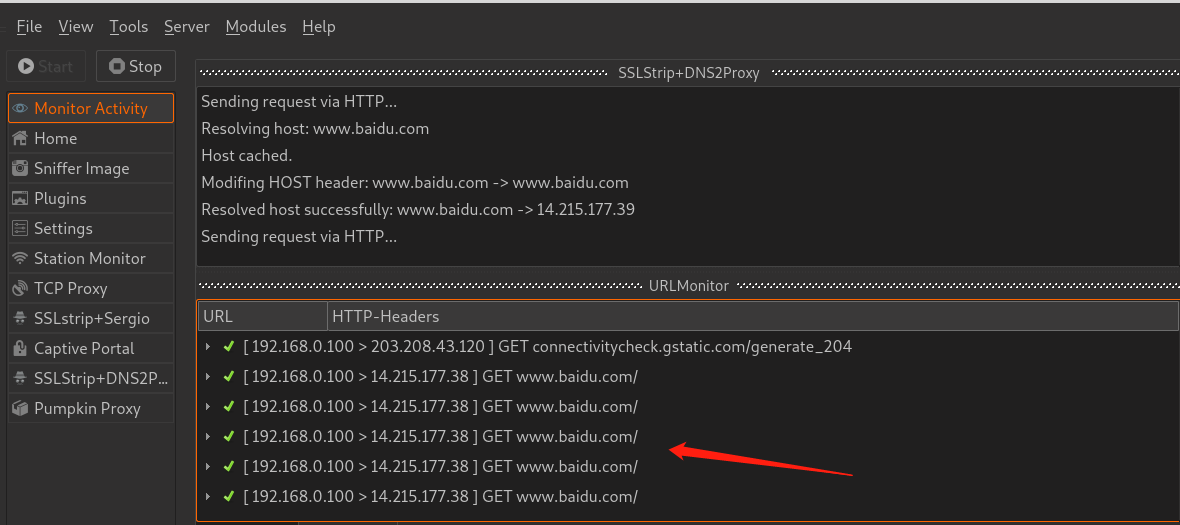
python wifi-pumpkin.py

听说可以创建MySQL数据库来存储数据，但我觉得没那个必要，感兴趣的童鞋可以自己操作一波。

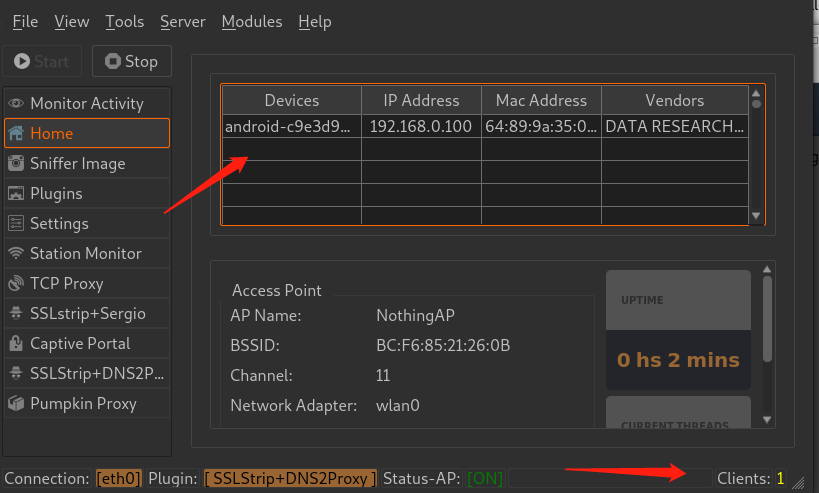
## 使用教程

### 主界面介绍

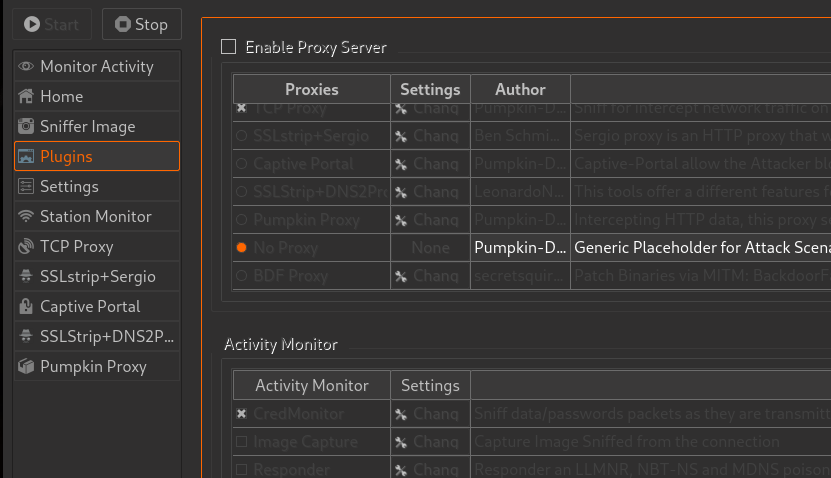
Monitor Activity用来直观显示伪造AP中用户都访问了那些站点。



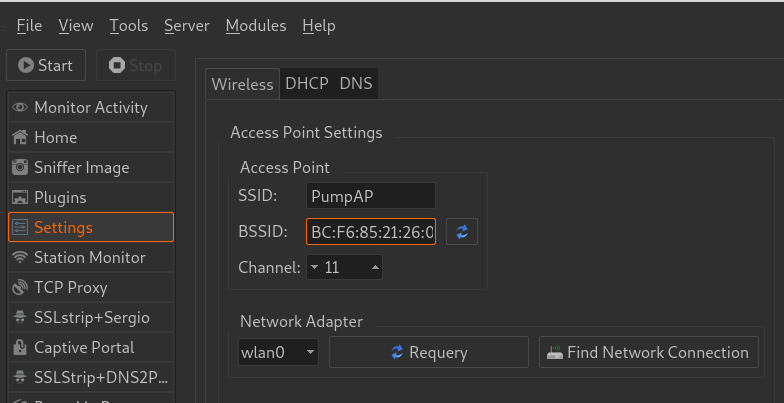
Home显示连接用户信息、伪造AP名字、BSSID、信道Channel和建立AP的网卡



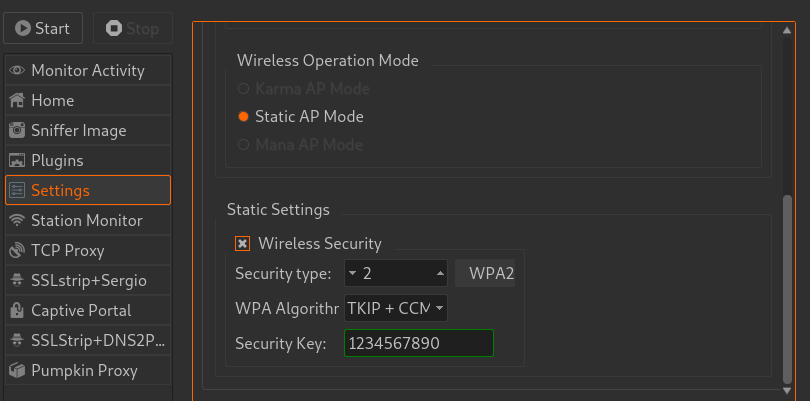
Plugins不常用，我直接不启用。



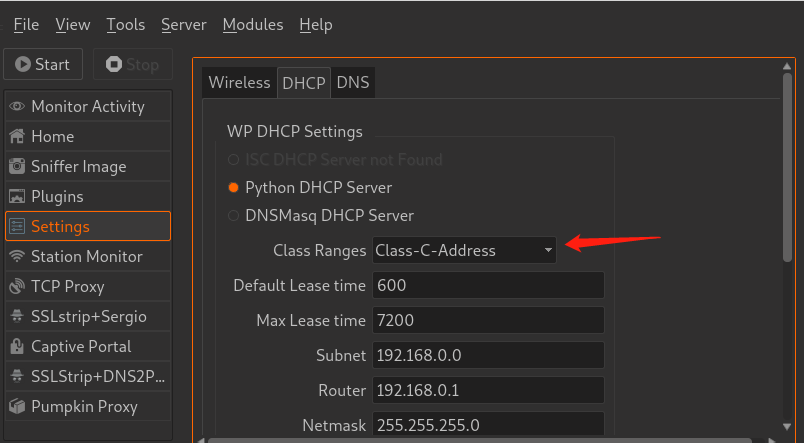
Settings用来设置伪造AP的信息。



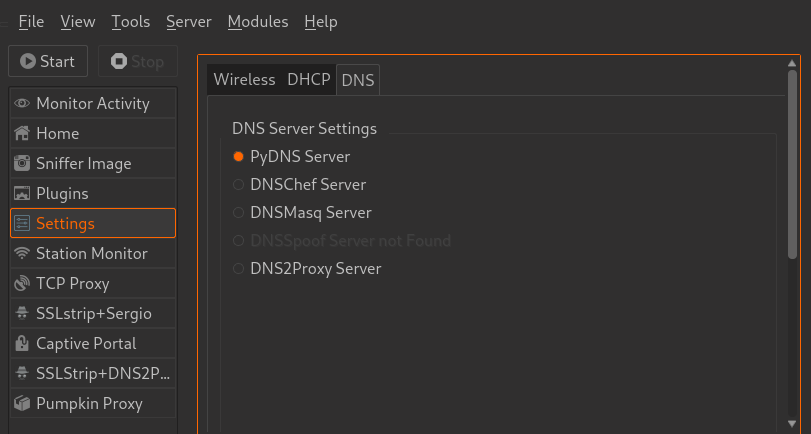
往下拉可以设置密码和加密方式。



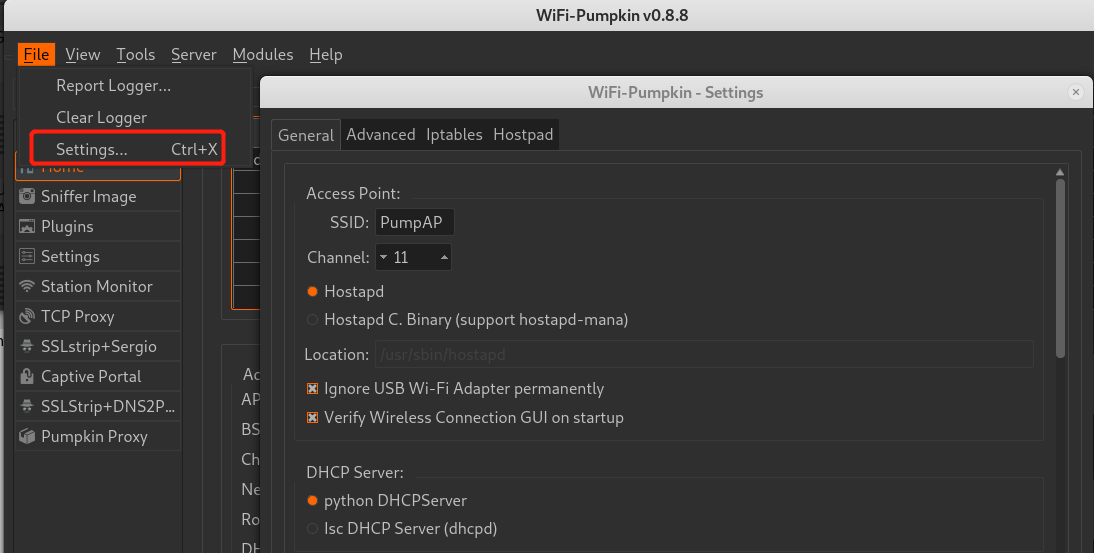
设置DHCP的IP段，舒服。



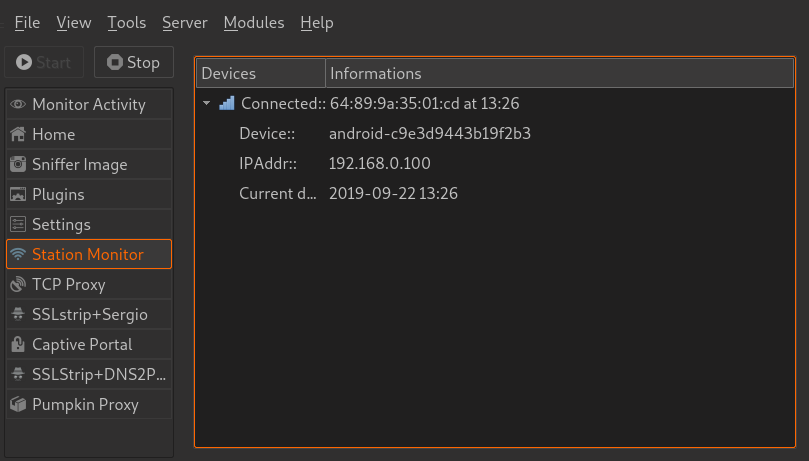
设置dns服务器。



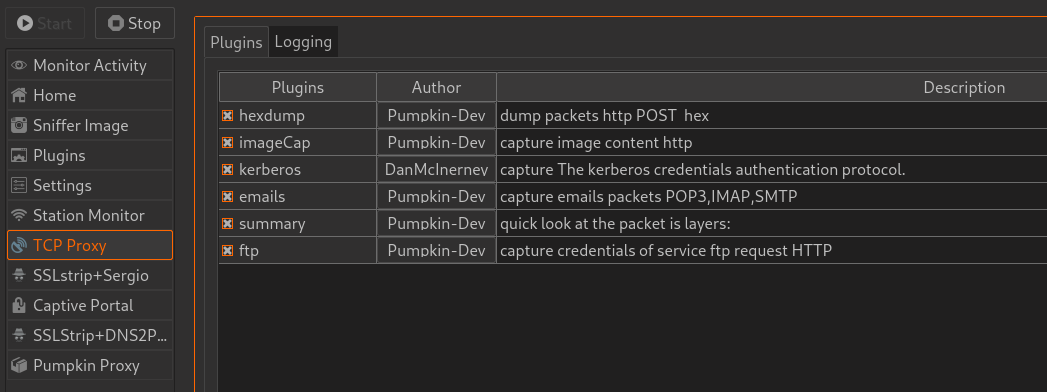
启动AP后，主界面的Setting不能修改，可以在File - Settings中修改固定信息。



Station Monitor查看连接用户信息，功能和Home差不多。



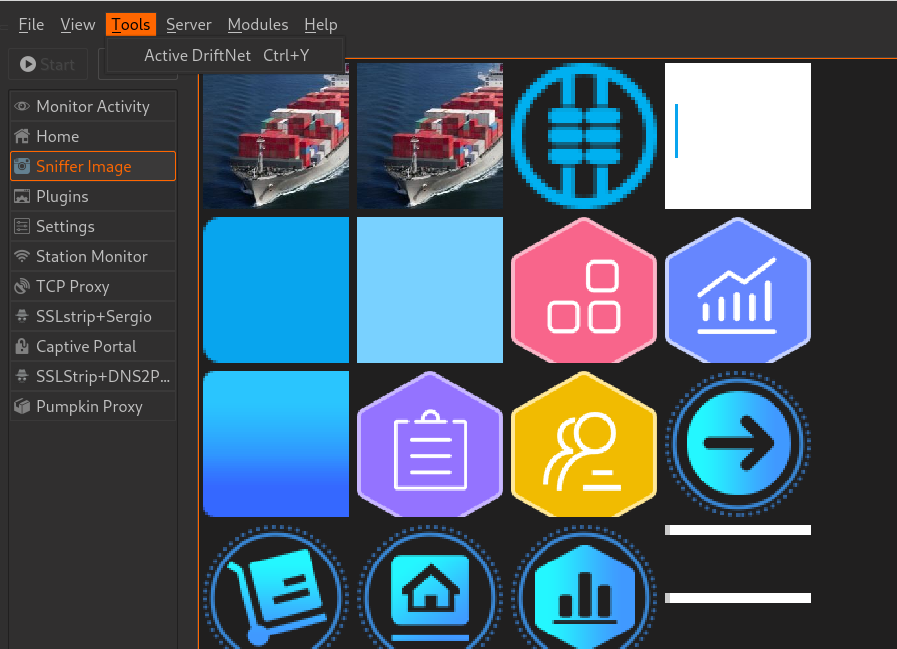
剩下的不常用，就不一一介绍。



### Tools选项卡

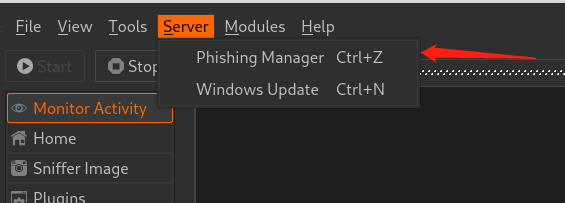
启动Active DriftNet，主界面转到Sniffer Image收取图片。

相当于driftnet -i wlan0

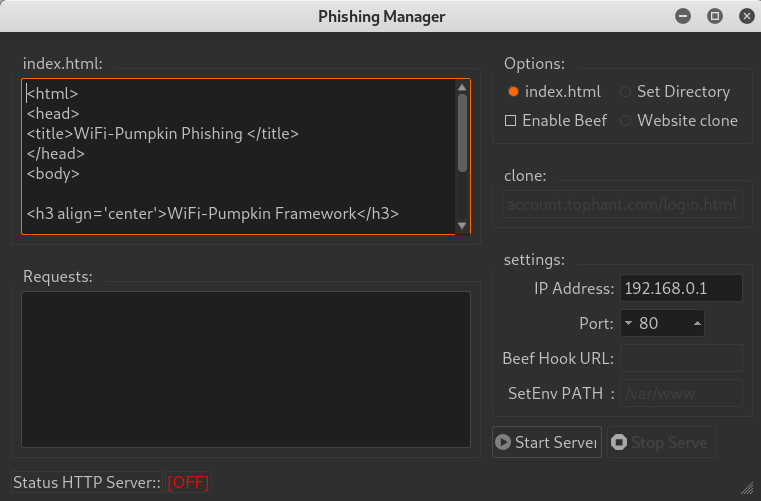


### Server选项卡

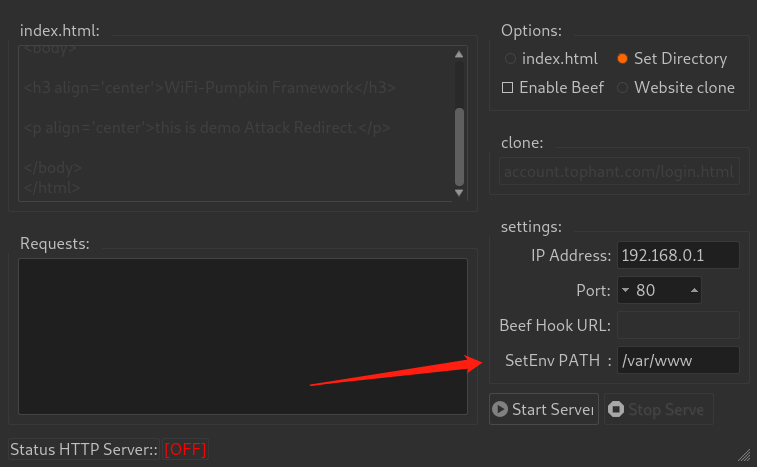
#### Phishing Manager钓鱼管理器



可以自定义index.html钓鱼页面。

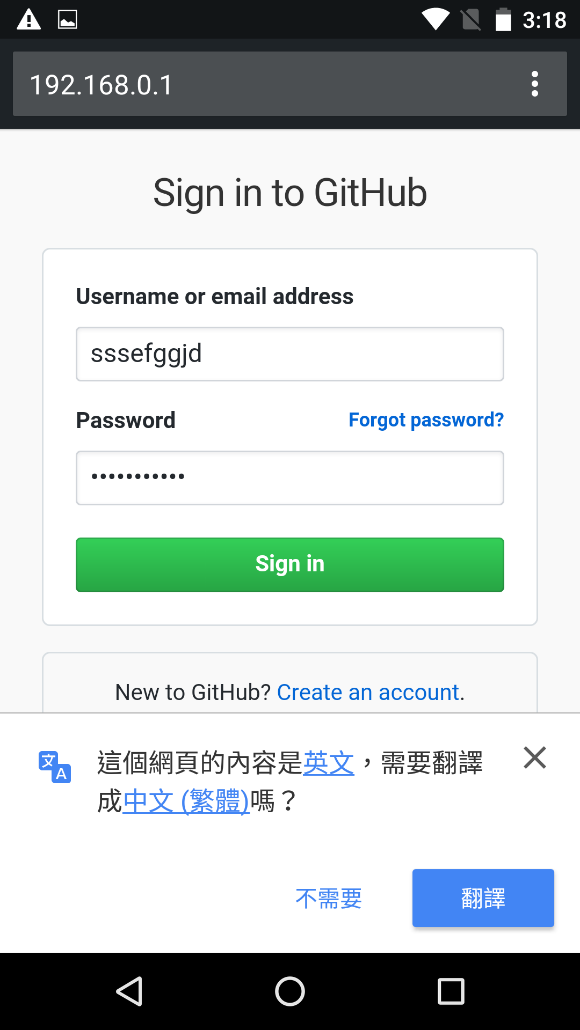


可以事先将目标源码dump下来作为完整的钓鱼站点。

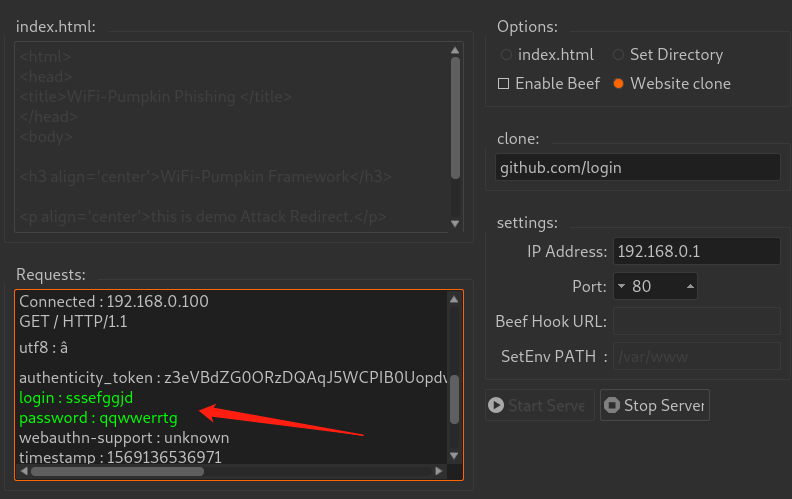


按照www.example/xxxx格式复制登录页面站点，这里以github.com/login为例。

下图：模拟攻击者输入账号密码。



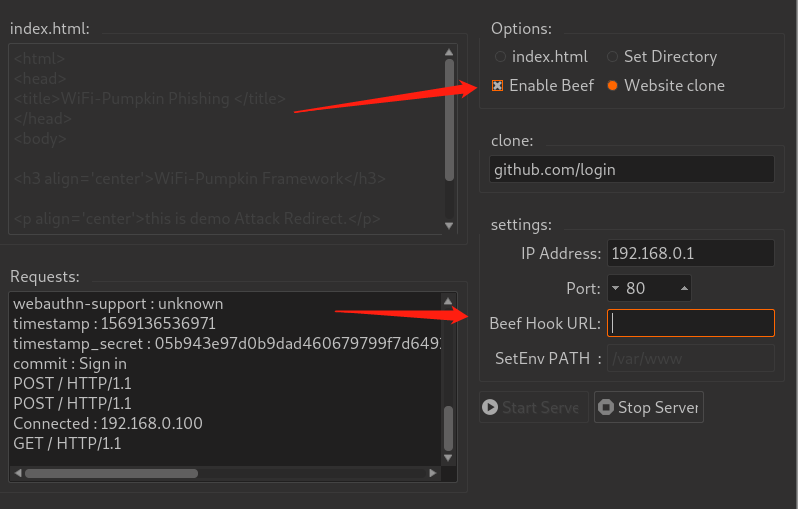
高亮密码，同时登录后自动跳转到真实站点。这界面可以说非常友好了。



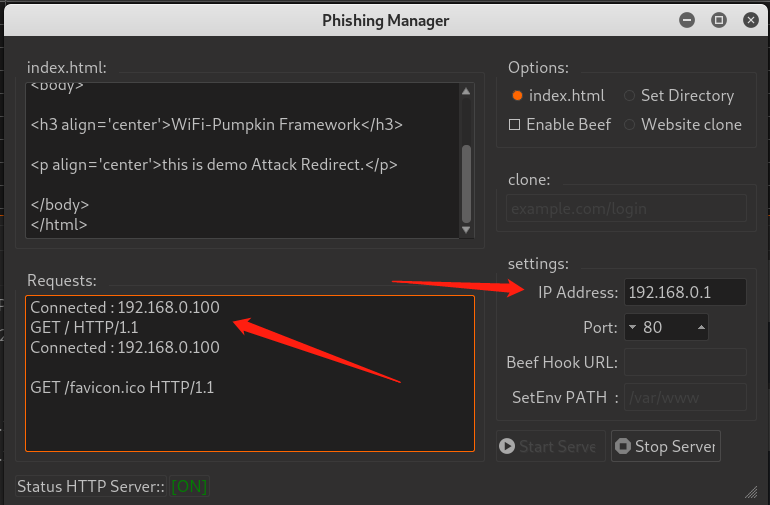
碰到https的站点不能设置https://github.com，不然会报错。



同时还支持BeEF攻击组件，大家自由发挥，这里不展开。



选择站点搭建IP和端口，然后Start Server，钓鱼页面就启动了。



附上几个测试图片

百度钓鱼站

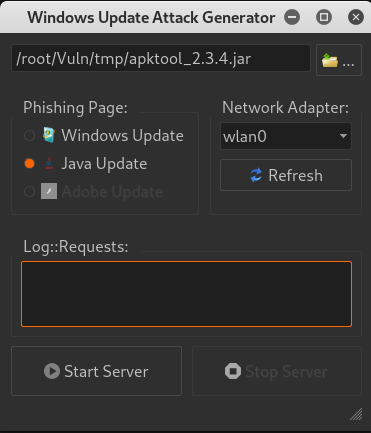
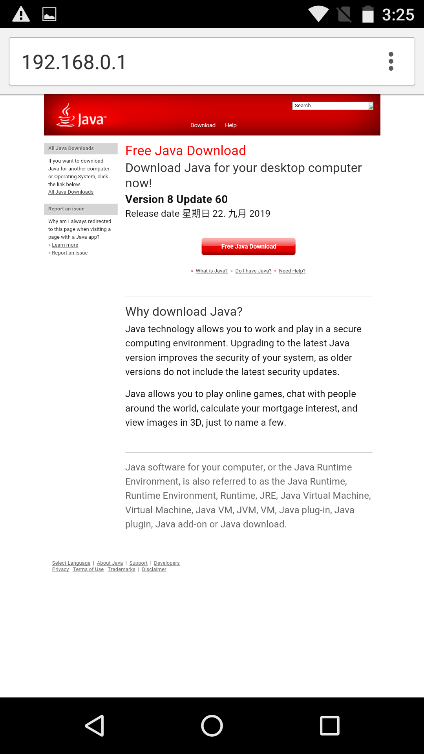


建议使用登录界面简单的站点作为钓鱼站点。像吐司的站就比较繁琐，效果不好。

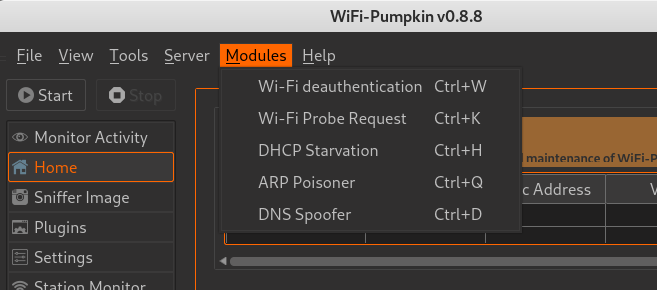


#### Windows Update攻击生成器

还可以设置升级页面诱导下载。

### Modules选项卡

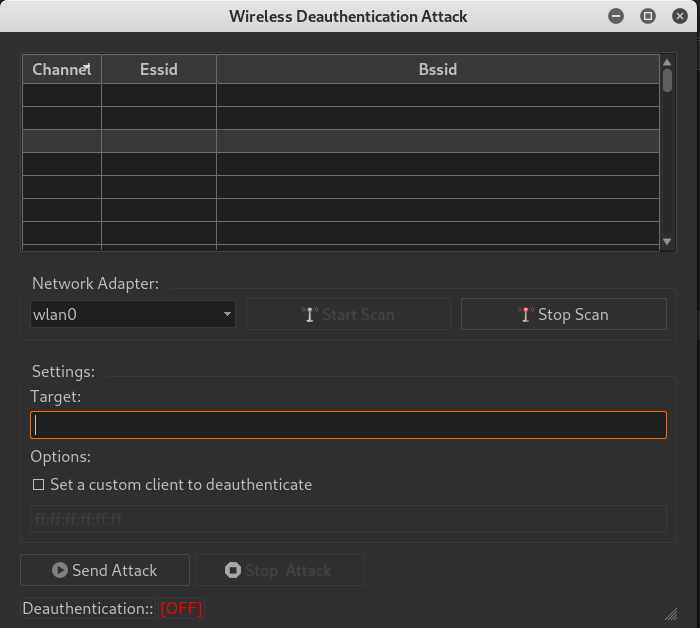


#### WiFi deauthentication

相当于WiFi-cracking攻击指令

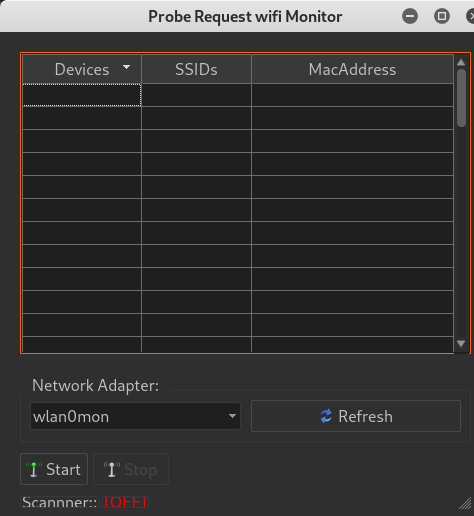
aireplay-ng --deauth 0 -a AA:AA:AA:AA:AA:AA wlan0mon

我测试时扫了几次都没成功，遂放弃。



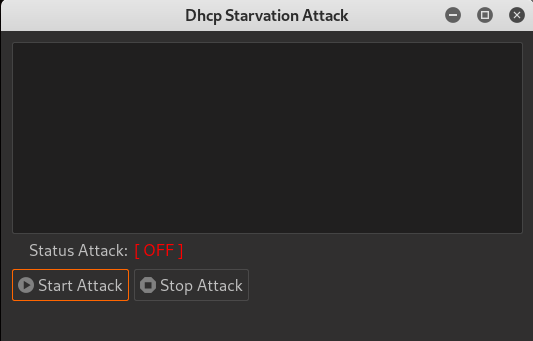
#### WiFi Probe Request

WiFi探针请求，感觉和主界面的Home差不多。

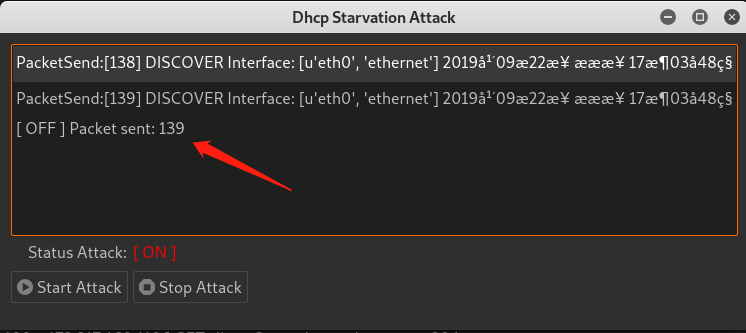


#### DHCP Starvation Attack

DHCP饥饿攻击



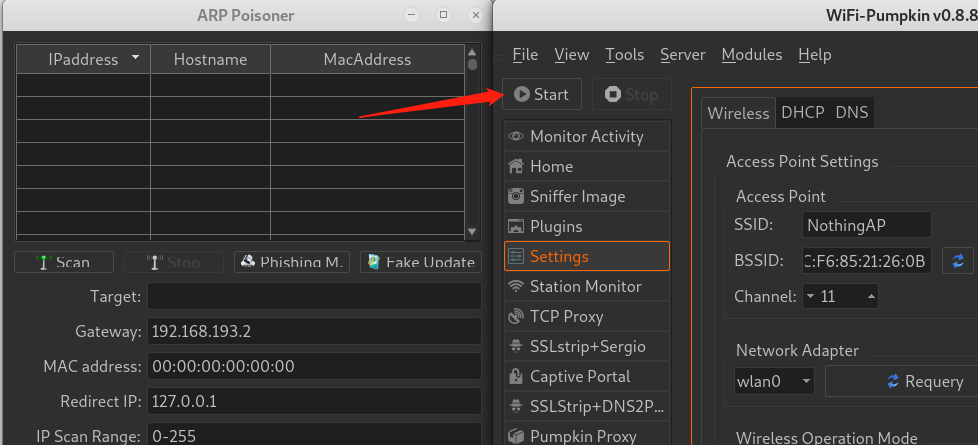
启动攻击后会不停的发包

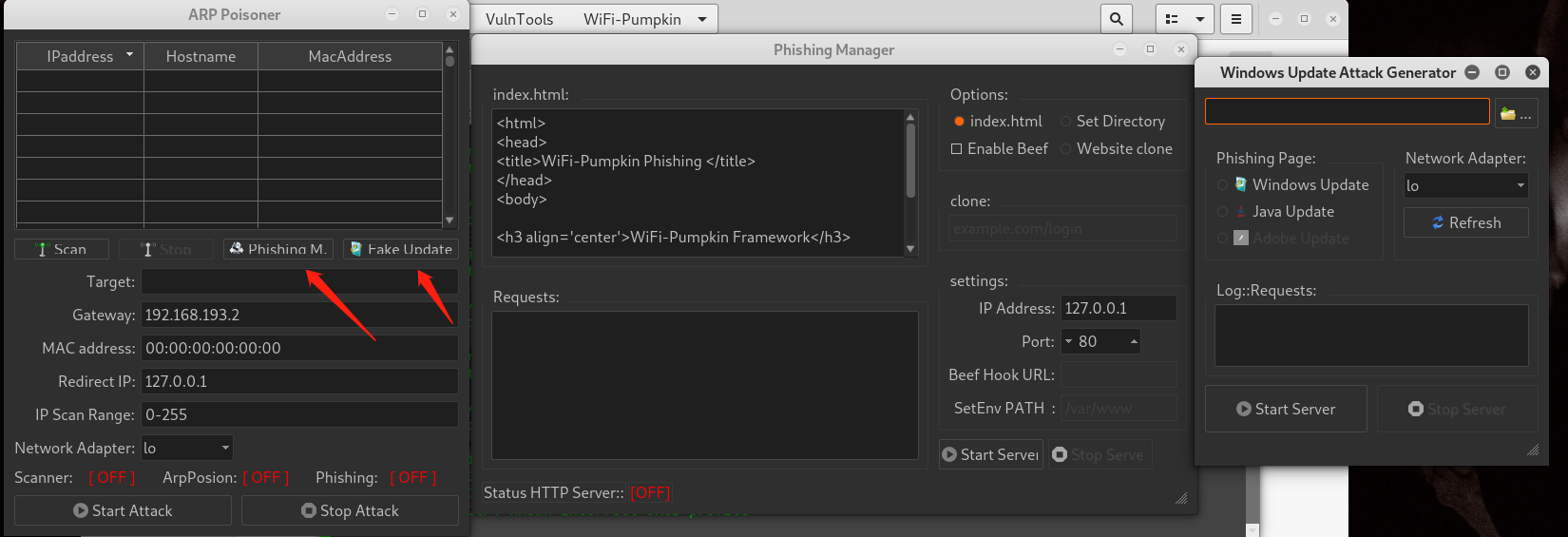


#### ARP Poisoner

ARP投毒，附带钓鱼管理器和Windows Update攻击生成器的攻击套件。

注意：该功能要在未启用钓鱼AP时才能使用（一般是已经打入目标AP，进行同局域网下目标攻击）。



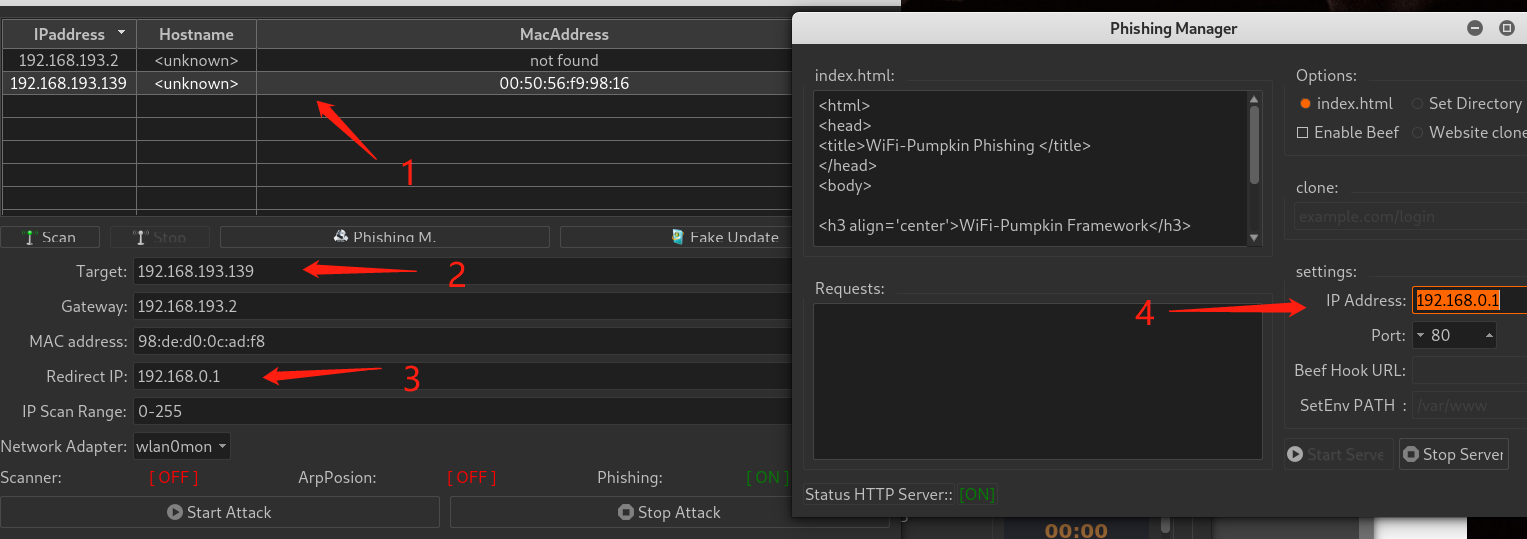


步骤一：点击扫描按钮进行扫描

步骤二：选择ARP投毒目标，点击列表中目标自动填充

步骤三：选择重定向IP

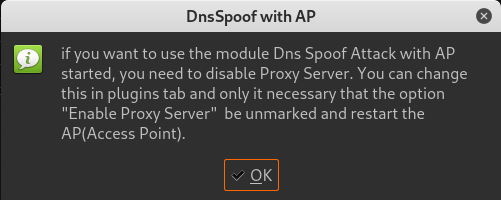
步骤四：配置钓鱼站点



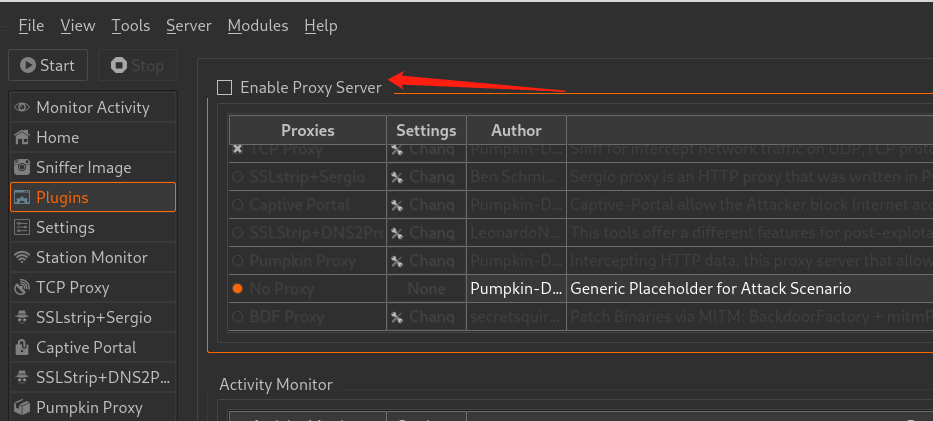
该功能没成功，不知道啥原因。

#### DNS spoofer

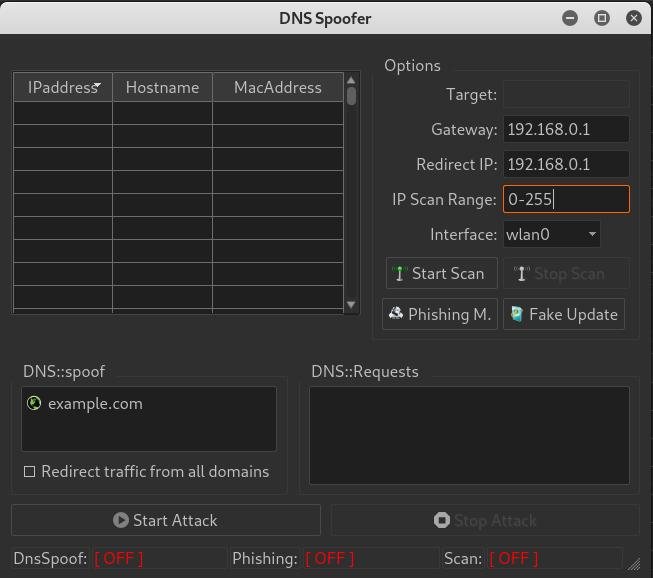
DNS欺骗，需要不勾选主界面中的Plugin的Enable Proxy Server复选框才能成功开启功能。



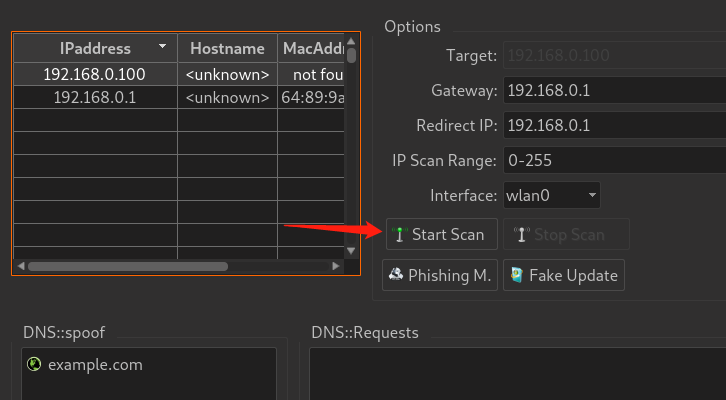
不勾选Enable Proxy Server



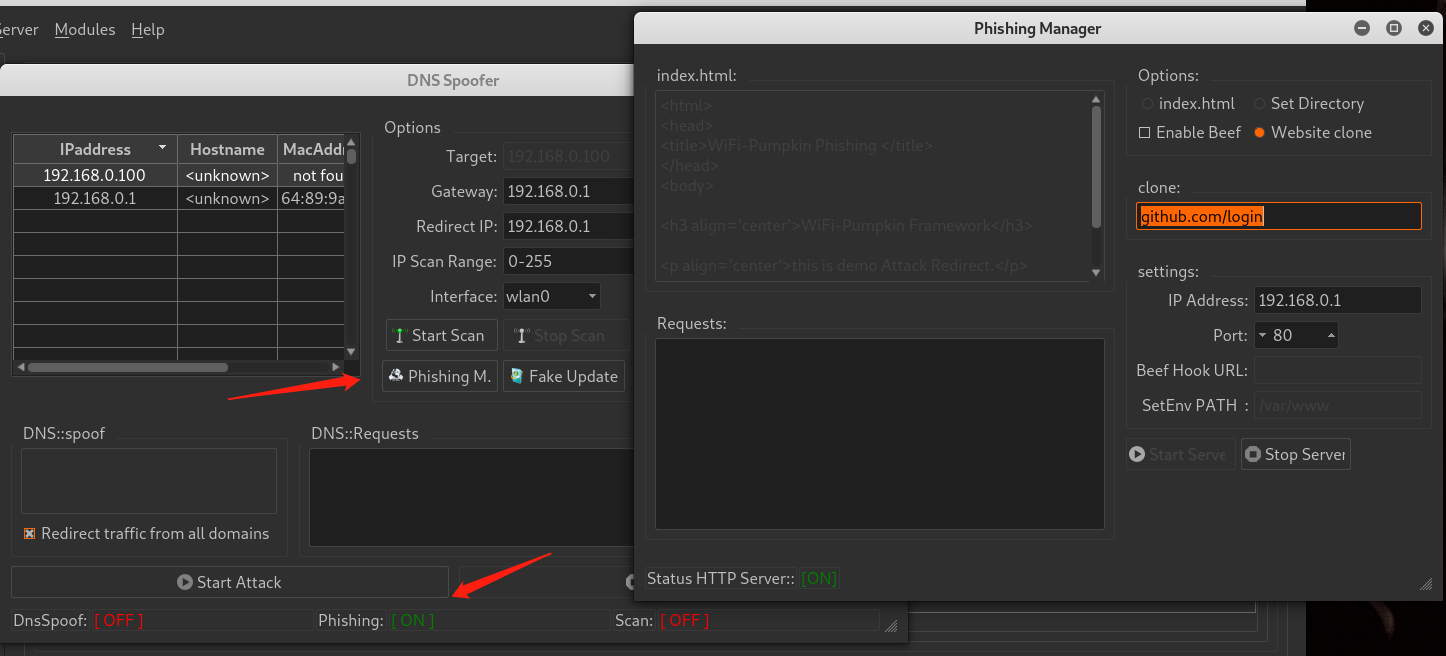
成功打开DNS投毒的界面如下。可以设置扫描IP段



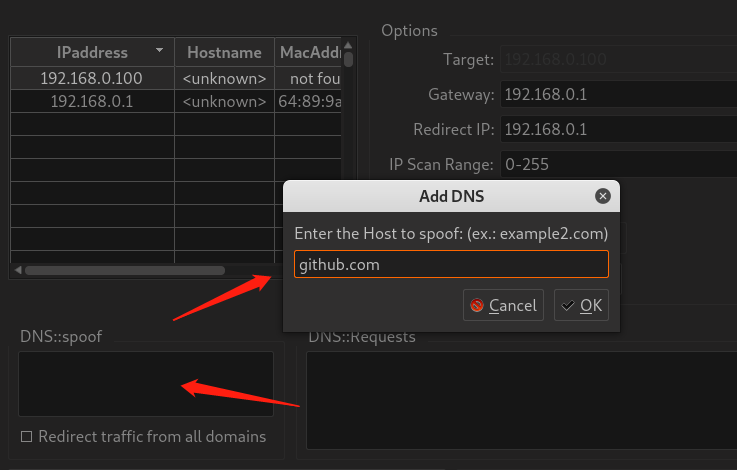
扫描结果会在左边显示



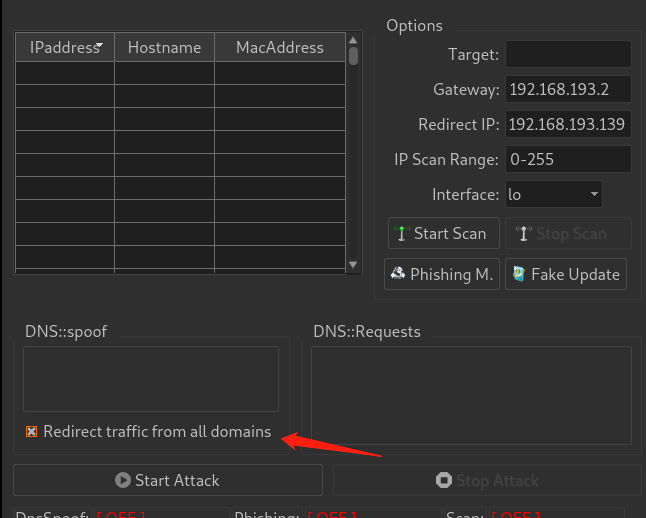
同时配合Phishing Manager和Fake Update扩大攻击



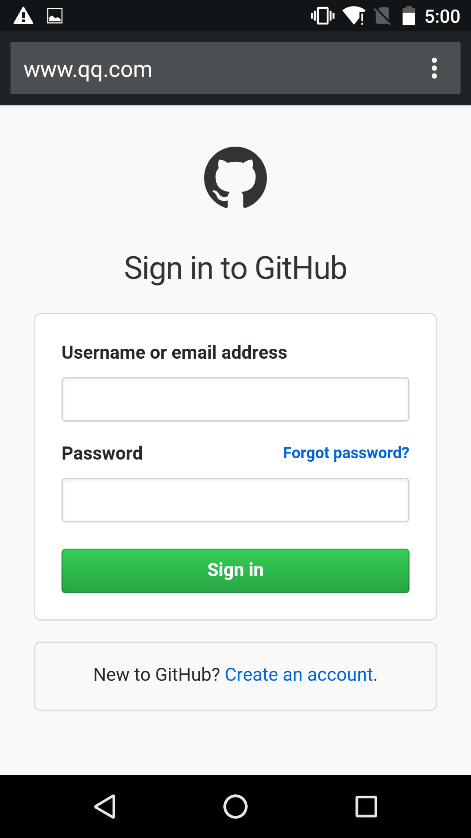
添加指定域名进行投毒



或者全域名投毒



成功利用DNS欺骗，把www.qq.com作为钓鱼站点的域名。



## 结束语

优点

1、完整的测试框架，集合常用的WiFi攻击套件，而且交互友好。

2、Phishing Manager设计很友好，基本能想到的都覆盖了，而且在进行ARP投毒和DNS欺骗时，可以同时设计钓鱼站，可以说很良心了。

缺点：

1、WiFi deauthentication貌似不能用，扫了几次没反应。

2、DNS欺骗功能，如果钓鱼站是复制的是github.com/login，如果受害者访问github.com时，并不会跳转到钓鱼站，更多时候会超时访问。

3、克隆钓鱼站时，对于https的站点兼容性有些欠缺，但对于页面简单的钓鱼站还是可以很好胜任的。

# wifiphisher（8k+ Stars）

GitHub地址：https://github.com/wifiphisher/wifiphisher

## 安装流程

git clone https://github.com/wifiphisher/wifiphisher.git

cd wifiphisher

python setup.py install

## 工具介绍

通过运行没有任何选项的工具，它将找到正确的界面，并交互地要求用户选择目标网络的ESSID（从周围区域的所有ESSID列表中选择）以及要执行的网络钓鱼方案。 默认情况下，该工具将同时执行Evil Twin和KARMA攻击。

wifiphisher -i wlan0 -e ESSID -hC handshake.pcap -iAM 38:EC:11:00:00:00 -dE PumpAP -dC 1,2,3 -pPD /tmp/wifiphisher/phishingPages/test.html

-i wlan0

手动选择一个既支持AP又支持监控模式的界面，以生成恶意AP以及从Extensions发起其他Wi-Fi攻击（即deauth）。

-aI wlan0

使用wlan0产生恶意访问点（一般用外置无线网卡）。

-e ESSID

使用ESSID作为钓鱼AP的名称（如果名字中有空，可用单/双引号-e "FREE WI-FI"）。

-hC handshake.pcap

通过与handhake.pcap文件中的握手进行检查，验证所捕获的预共享密钥是否正确。

-pK 1234567890

设置登录钓鱼AP的密码（一般不和-hC联用，知晓了密码才用这个选项）。

-iAM 38:EC:11:00:00:00

给钓鱼AP设置Mac地址（可选）。

-dE ESSID

解除WLAN中所有使用ESSID为AP名称的BSSID的身份验证（常用来打掉想要模拟的AP站点，这样就可以让受害者连接钓鱼AP）。

-dC 1,2,3

选择想要Deauth的信道（估计打全信道动作太大，直接打固定信道会省事）。

-pPD /var/www/login.html

设置钓鱼页面链接。

-p oauth-login

Oauth-login登录方式

# create\_ap（3.2k+ Stars）

看名字就知道是个单纯建AP的工具。

Github地址：https://github.com/oblique/create\_ap

## 安装流程

git clone https://github.com/oblique/create\_ap.git

cd create\_ap

make install

网卡设置：NAT模式+外置无线网卡

## 使用教程

### 常用命令

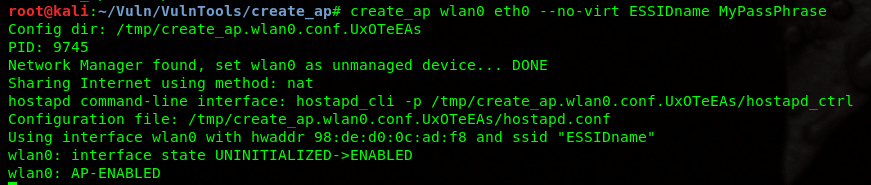
开放连接（无密码，不能正常上网）

create\_ap wlan0 eth0 --no-virt ESSIDname



WPA + WPA2加密（不能正常上网）

create\_ap wlan0 eth0 --no-virt ESSIDname MyPassPhrase



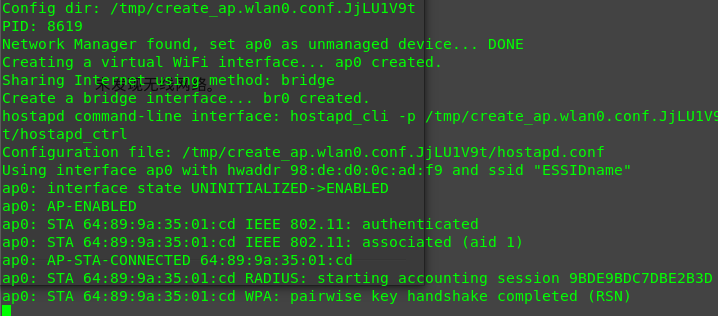
同WiFi接口（无法正常上网）

create\_ap wlan0 wlan0 ESSIDname MyPassPhrase

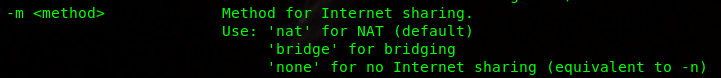


使用桥接模式分享网络（可以正常上网）

create\_ap -m bridge wlan0 eth0 ESSIDname MyPassPhrase



-m命令解释，可以用NAT、桥接Bridge和none模式



### 其他选项

1、不创建虚拟网卡（需用两个不同的网卡）

--no-virt

2、设置Mac地址

--mac AA:AA:AA:AA:AA:AA

3、设置DHCP返回的DNS

--dhcp-dns <IP1[,IP2]>

4、关闭工具后网卡没恢复，可用该选项修复。

--fix-unmanaged

5、选择信道（默认信道为1）

-c 1

6、选择加密方式（1代表WPA，2代表WPA2，1+2代表WPA+WPA2，默认1+2）

-w 1+2

## 结束语

优点：

1、操作方便，命令简单

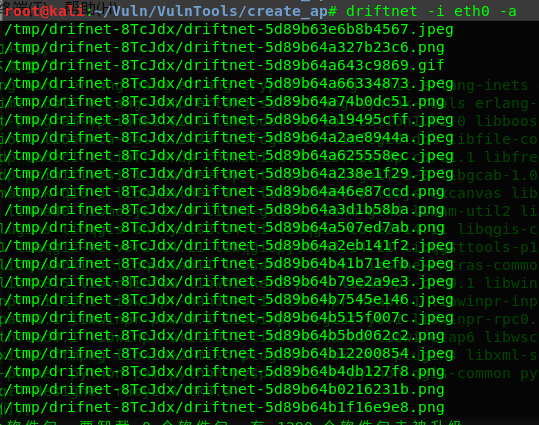
2、使用时创建临时配置文件，结束后会还原配置，不用担心配置问题。还配置了修复网卡功能。

作为一个专注于伪造AP的工具，在操作、功能、交互上是一款优秀的软件。如果和WiFi-Pumpkin这种完整框架比，在功能上的确是存在不足。但对于想自组一套攻击框架的朋友来说，这是个值得推荐的工具。

# 延伸攻击driftnet

使用driftnet监听网卡截取图片（不加-i的话，默认全网卡都监听），并保存-a

driftnet -i eth0 -a





# 踩坑后话

最满意的是WiFi-Pumpkin，UI界面+各种工具的集合，省力又省心，符合“一把梭”核心价值观，配合其他工具可以打出几种攻击链，不愧是完整WiFi测试框架。

最便捷的是create\_ap，适用于突发情况，延展性好。在该工具的基础上，可以组合一套自己的WiFi渗透框架。