四步教你破解隔壁老王的Wi-Fi密码

2015-10-15 萌码

对于想在很多人来说，WiFi就如同空气中的氧气般，必不可少；因此时不时的需要蹭网救命。当然，如果你有个不设WiFi密码的好邻居，那么可以说你是世界上最幸运的人了。然而问题是WiFi长蹭，好邻居却不常有。

不过没有关系啦，作为会编程或者正在学习编程的你们当然有办法啦！！！今天萌小妹就给大家分享一个破解隔壁家老王WiFi密码的方法，以备你们救命之需。

主要原理

创建一个伪AP来“狸猫换太子”，然后撤销用户AP的授权，

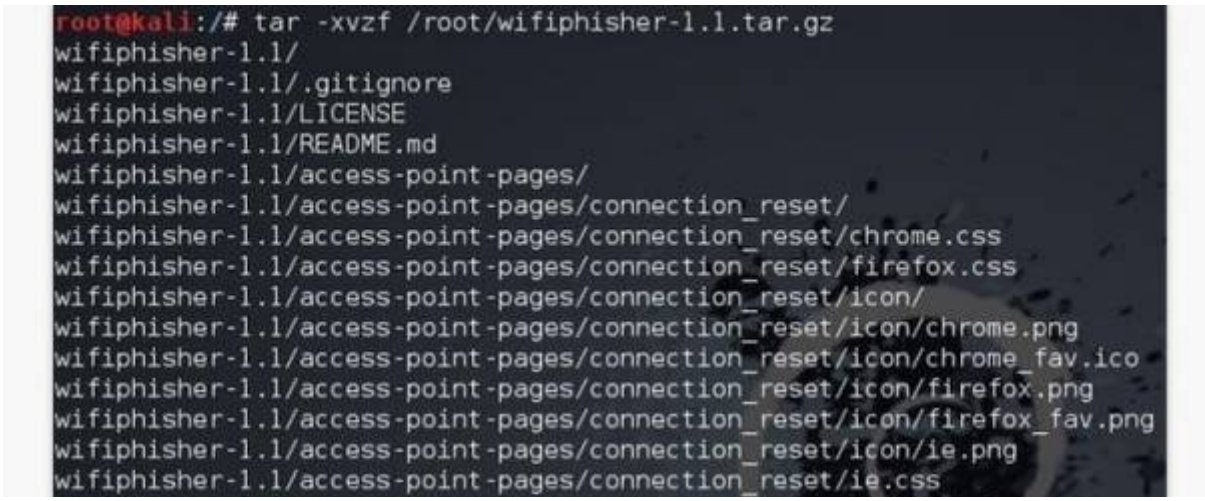
通知用户需要进行“固件升级”，需要重新验证密码。你的假AP由于具有相同的SSID，用户便会“交代”密码。

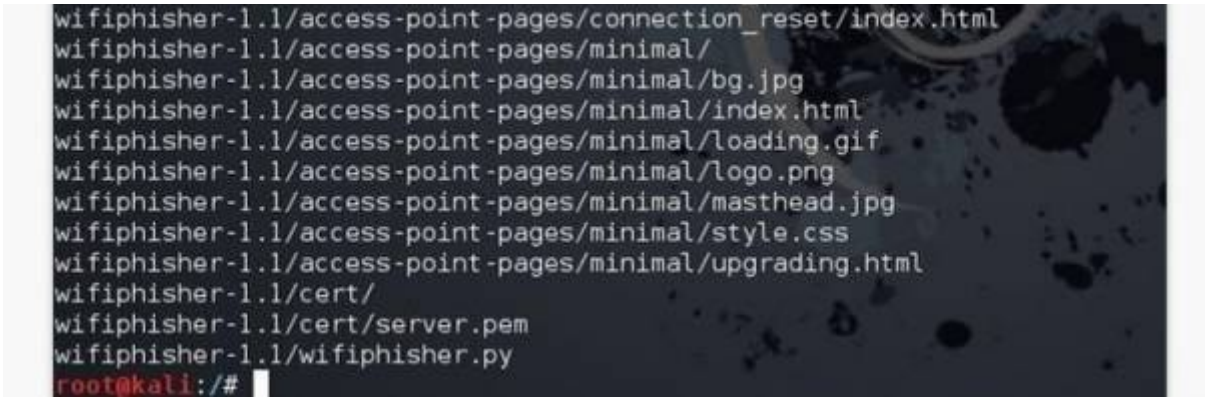
这样你就能得到用户的密码，并且让用户采用你的伪AP做为自己的接入点。而对方一无所知。

要完成上述“大业”，你需要Kali Linux和两个无线适配器，其中一个必须能支持数据包注入。

第一步：下载Wifiphisher

如图所示，这是已经解开了的Wifiphisher源代码。



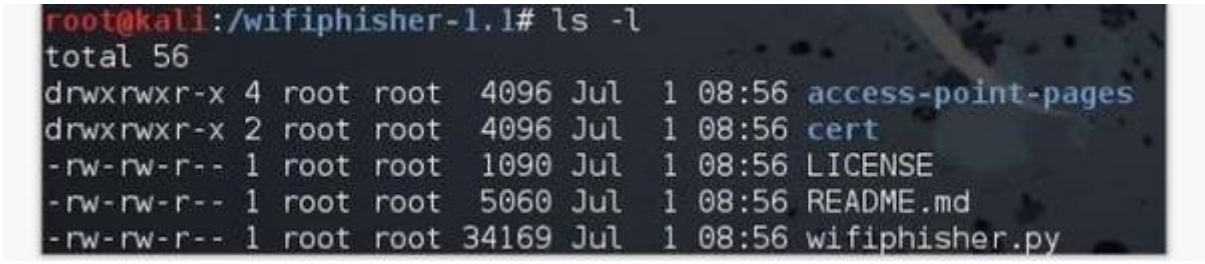


当然，如果你懒，也可以复制GitHub上的代码，不用谢~

第二步：导航到该目录

接下来，导航到Wifiphisher创建时被解压的目录。就图示而言，为/wifiphisherWi-Fi1.1。

当你看到目录内容时，你会看到wifiphisher.py的脚本。



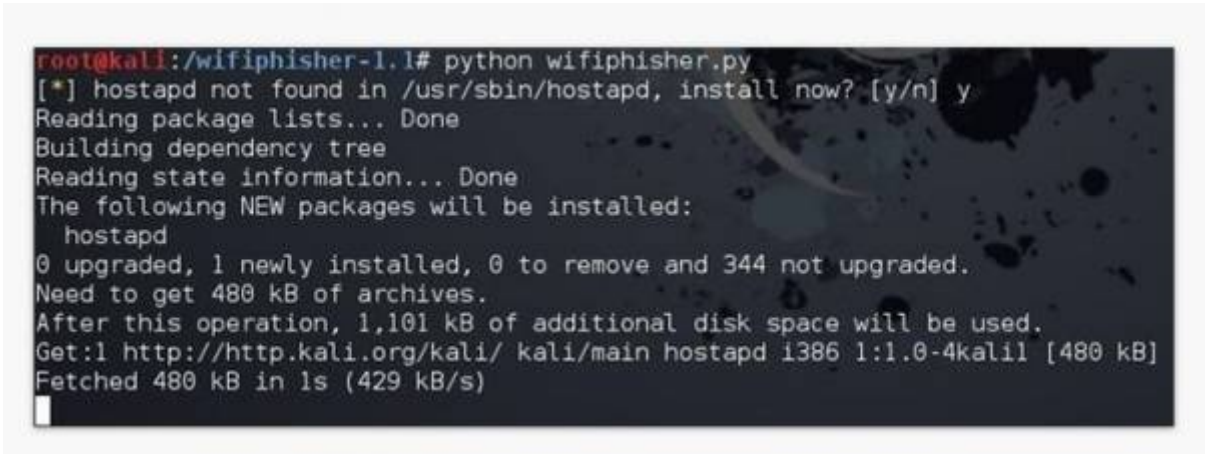
第三步：运行脚本

可以键入下面的脚本实现。

kali > python wifiphisher.py

注意这里有一个问题：

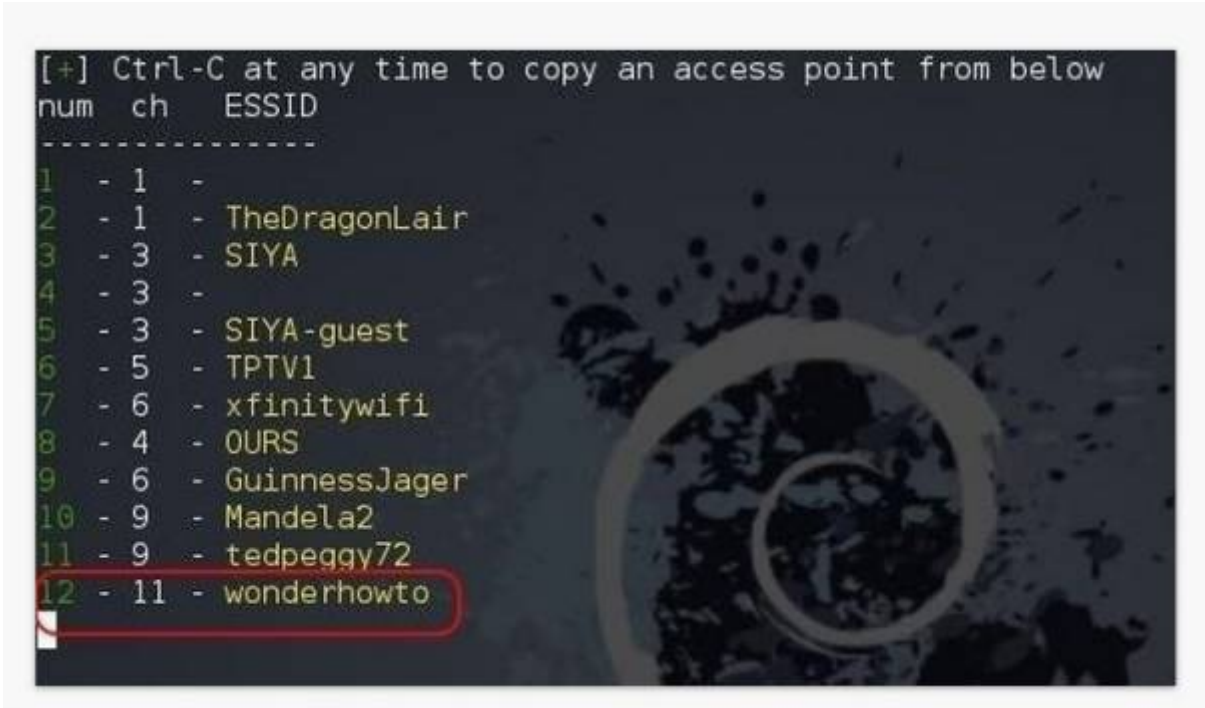
如果是第一次运行脚本的话，它可能会出现提示安装hostpad的信息，键入Y继续安装即可。



完成的时候，再次运行Wifiphisher脚本。

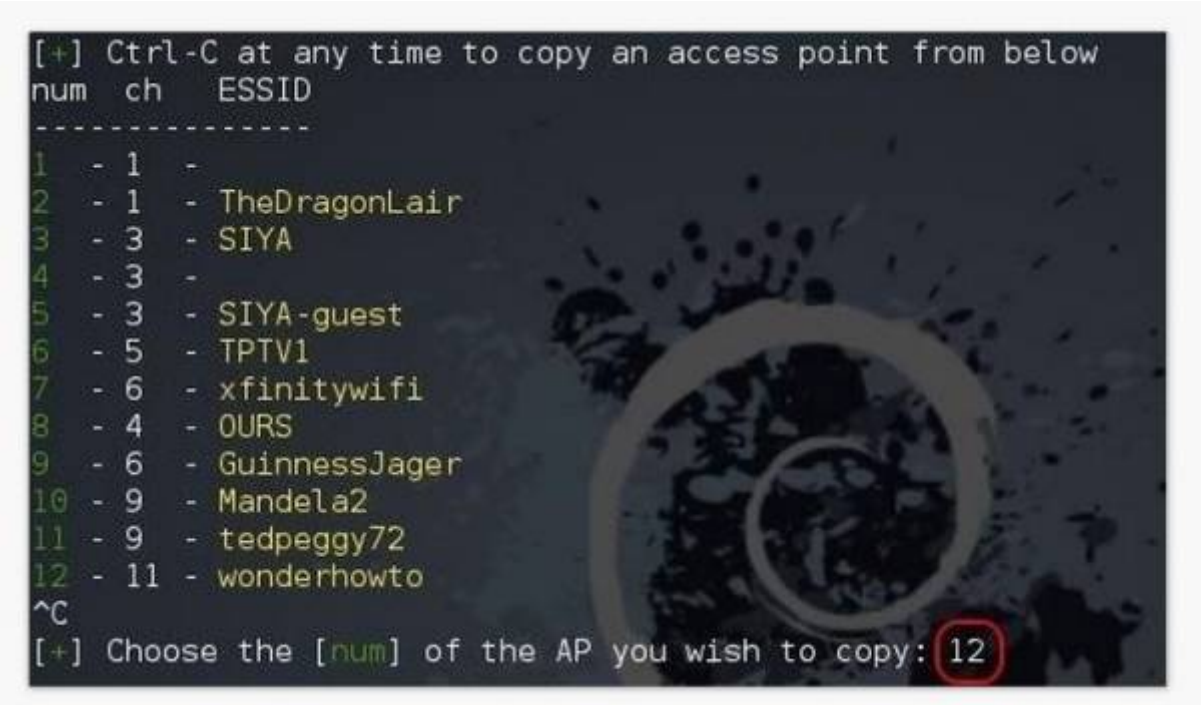
这次将运行8080和43端口的Web服务器，然后开始搜索附近的Wi-Fi网络。

等待搜索完成，我们会发现一系列Wi-Fi网络名。最下方的wonderhowto就是我们的目标。



第四步：获取密码

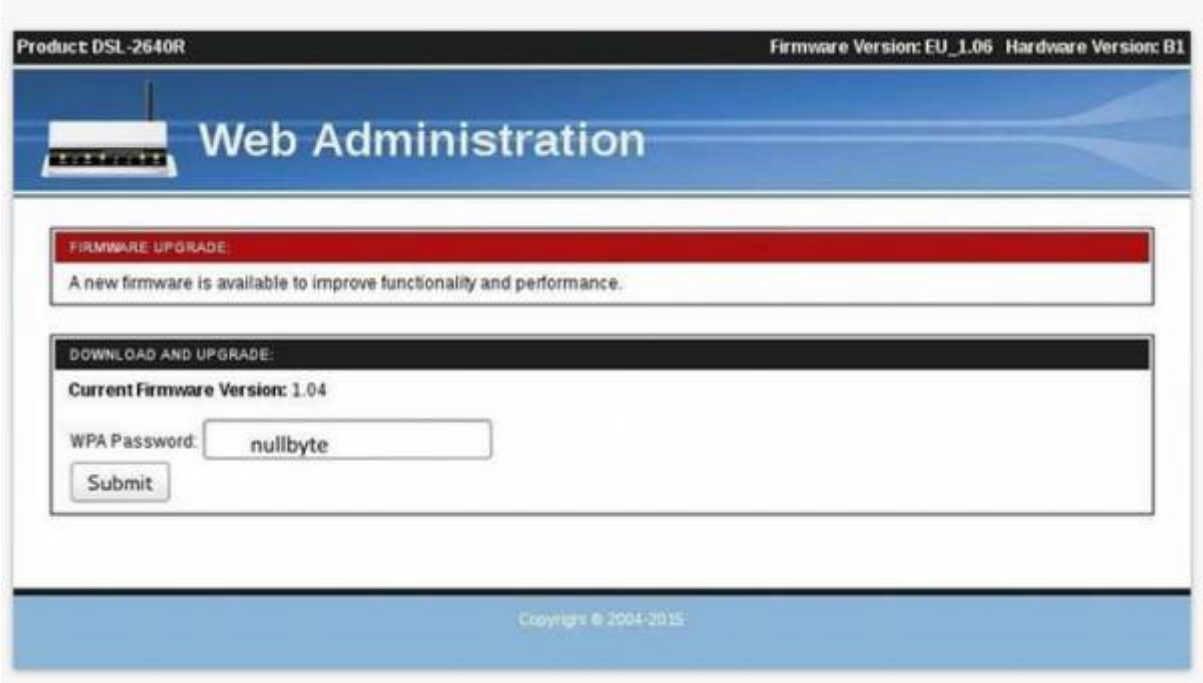
按下Ctrl + C，键入想要复制的AP数，在这里我们选择12。



敲下回车，Wifiphisher会显示如下结果，显示了正在使用的界面，还有正被攻击及复制的AP所在的SSID。

目标用户已经取消验证他们的AP，随后会出现一个固件升级的信息，请求他们重新验证。一旦重新验证，他们

目标用户已经取消验证他们的AP，随后会出现一个固件升级的信息，请求他们重新验证。一旦重新验证，他们接入的就是伪接入点了。



当用户输入密码，它会通过Wifiphisher的开放终端传输给你，随后他们依然像平时一样上网，风平浪静，然而他们并不知道我们已经获得了密码。

现在你可以开始愉快地蹭Wi-Fi了!

源：网络


www.mengma.com
扫一扫，开始计算机二级修炼之路
少壮不编程，老大徒伤悲