工具的使用 | BeEF的使用

谢公子学安全 2020-05-29 09:33:37

目录

BeEF的简单介绍

BEEF (The Browser Exploitation Framework)：一款浏览器攻击框架，用Ruby语言开发的，Kali中默认安装的一个模块，用于实现对XSS漏洞的攻击和利用。

BeEF主要是往网页中插入一段名为hook.js的JS脚本代码，如果浏览器访问了有hook.js(钩子)的页面，就会被hook(勾住)，勾连的浏览器会执行初始代码返回一些信息，接着目标主机会每隔一段时间（默认为1秒）就会向BeEF服务器发送一个请求，询问是否有新的代码需要执行。BeEF服务器本质上就像一个Web应用，被分为前端和后端。前端会轮询后端是否有新的数据需要更新，同时前端也可以向后端发送指示， BeEF持有者可以通过浏览器来登录 BeEF 的后端，来控制前端(用户的浏览器)。BeEF一般和XSS漏洞结合使用。
BeEF的目录是：/usr/share/beef-xss/beef

```
root@kali:~# cd /usr/share/beef-xss/
root@kali:/usr/share/beef-xss# ls
arerules  beef_cert.pem  config.yaml  db          Gemfile       modules
beef      beef_key.pem   core         extensions  Gemfile.lock
```

BeEF-XSS的使用

在使用之前，先修改/usr/share/beef-xss/config.yaml配置文件，将ip修改成我们kali的ip地址。后续我们进行其他实验也是需要修改这个配置文件

```
25    # HTTP server
26    http:
27        debug: false #Thin::Logging.debug, very verbose. Prints also full exception stack trace.
28        host: "192.168.10.25"
29        port: "3000"
```


打开方式：

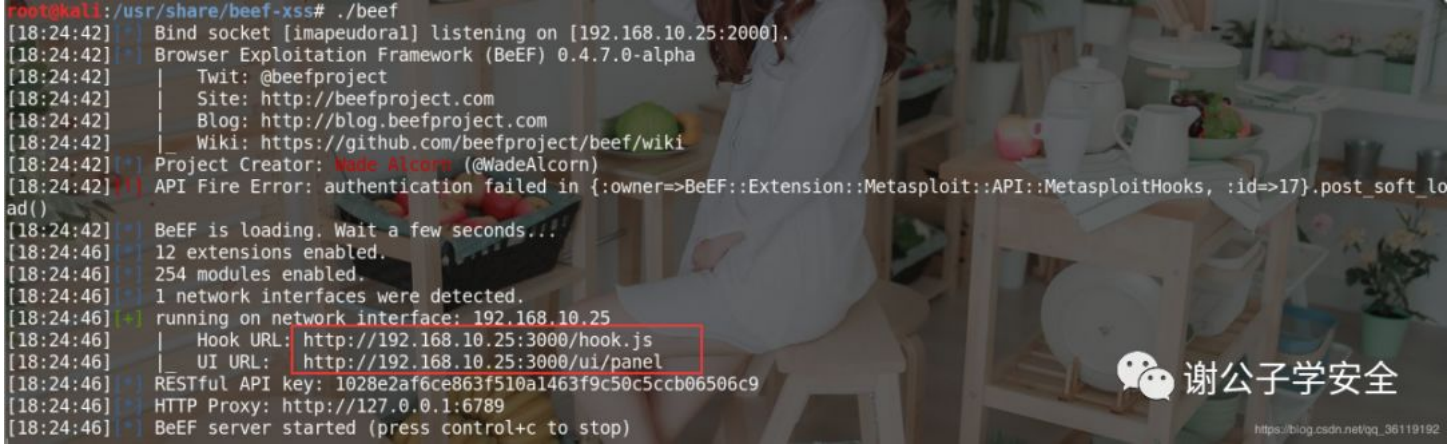
- 直接点击桌面上的图标，过5秒左右，然后它自动会打开命令行和浏览器beef的登录框
- 任意目录，直接输入命令：**beef-xss**打开 ，过5秒左右，然后它自动会打开命令行和浏览器beef的登录框
- 进入/usr/share/beef-xss/，输入命令：**./beef-xss**打开 ，然后手动打开浏览器链接

kali已经把beef-xss做成服务了，我们也可以使用systemctl 命令来启动或关闭beef服务

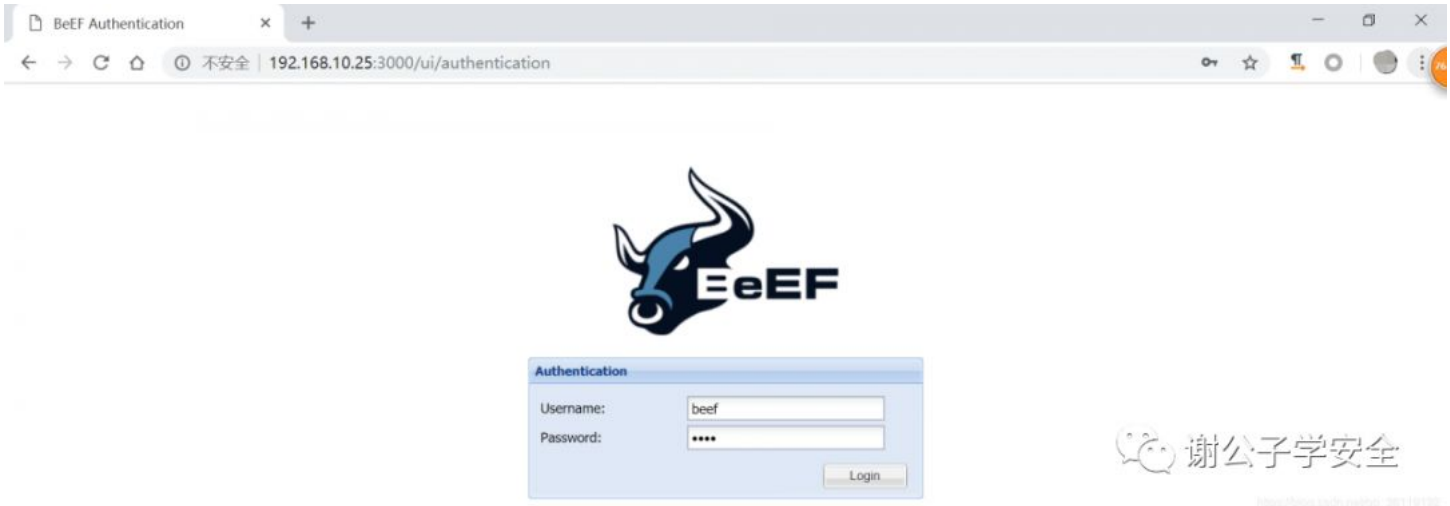
- systemctl start beef-xss.service #开启beef服务
- systemctl stop beef-xss.service #关闭beef服务
- systemctl restart beef-xss.service #重启beef服务

我直接进入该目录，**./beef**

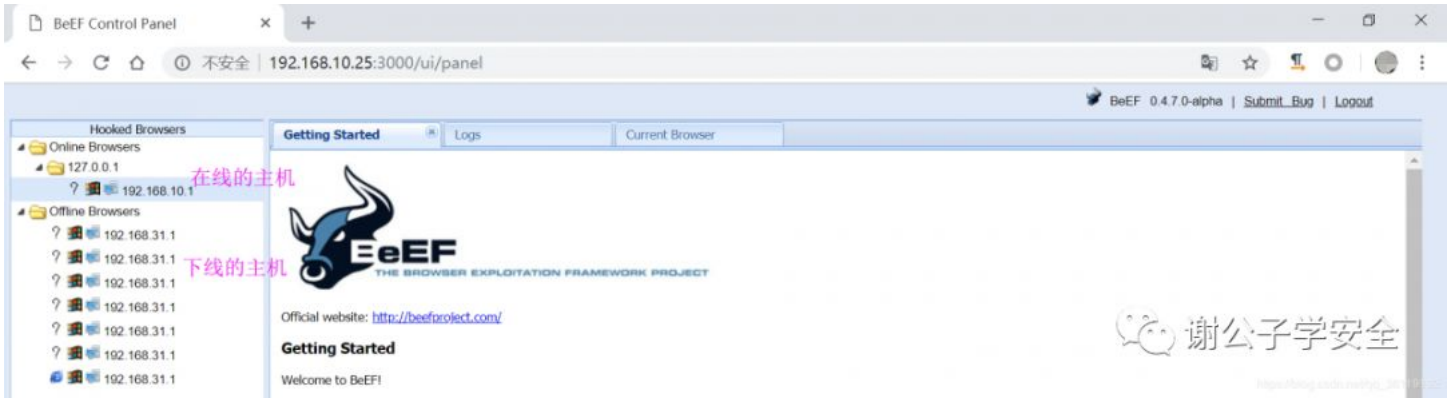
回到顶部



手动打开浏览器，登录名和密码默认都是：beef

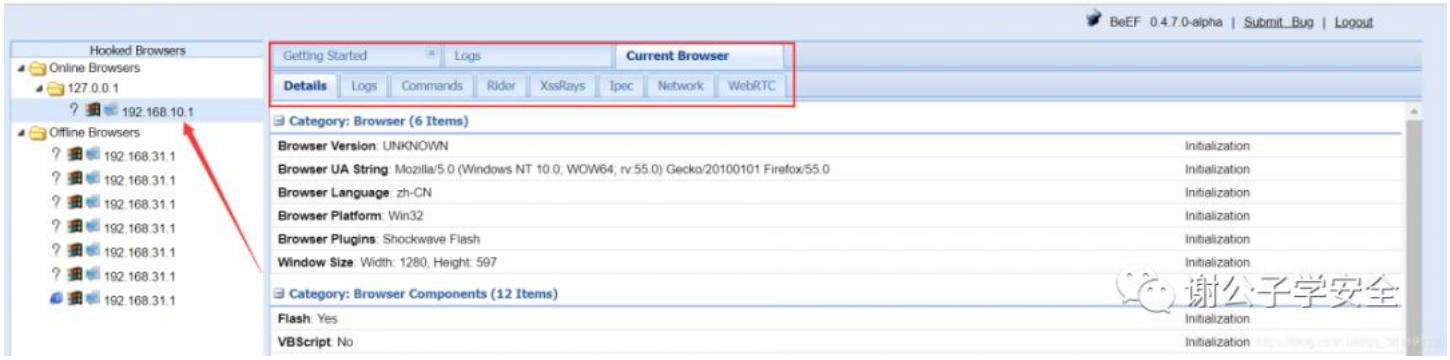


登录成功后，这里会显示在线的主机和不在线的主机。在线的就是现在该主机浏览器执行了我们的JS脚本代码，不在线的就是该主机曾经执行过我们的JS脚本代码，但是现在叉掉了该页面



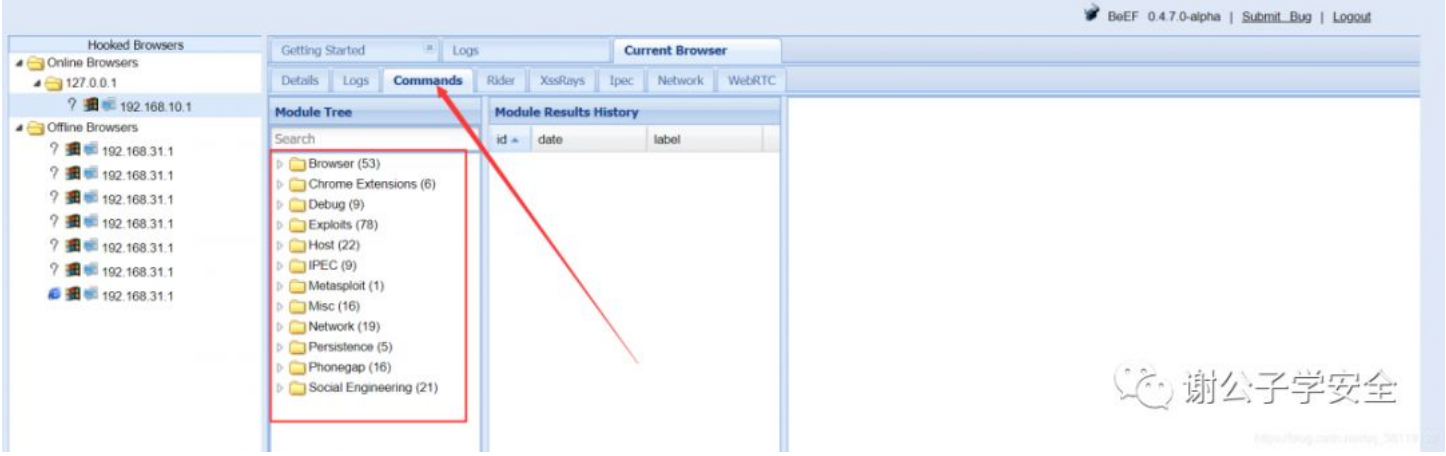
我们点击当前在线的主机，然后右边会有选择框，我们点击Current Browser，然后下面就有一些功能项：Details、Logs、Commands、Rider、XssRays、Ipec、Network、WebRTC

- Details是浏览器信息详情
- Logs能记录你在浏览器上的操作，点击，输入操作都能记录
- Commands是你能对该浏览器进行哪些操作



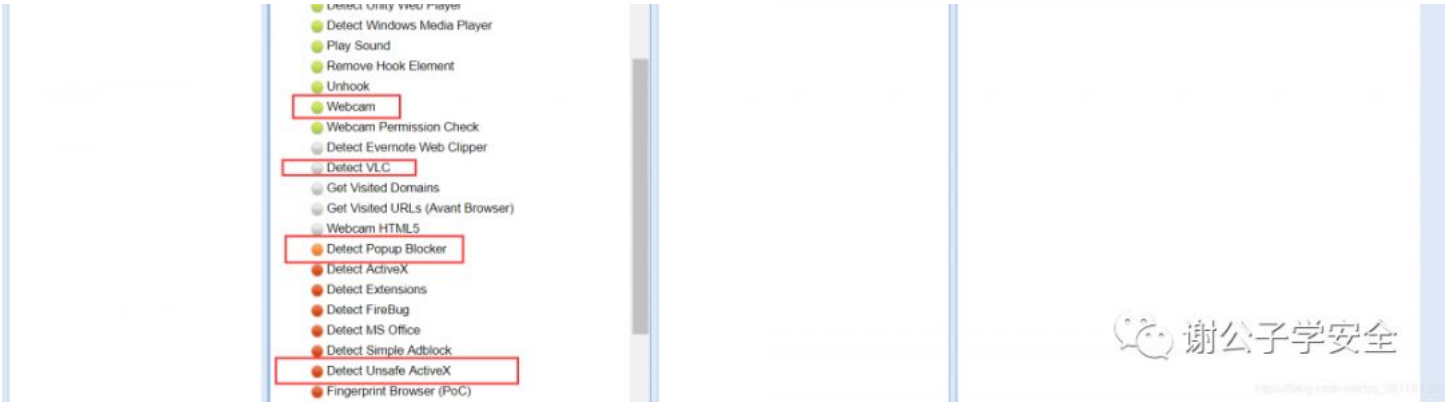
我们点击Command，这里有一些我们可以使用的功能分类，一共有12个大的功能，括号里面的是每个功能分类里面的个数。

回到顶部



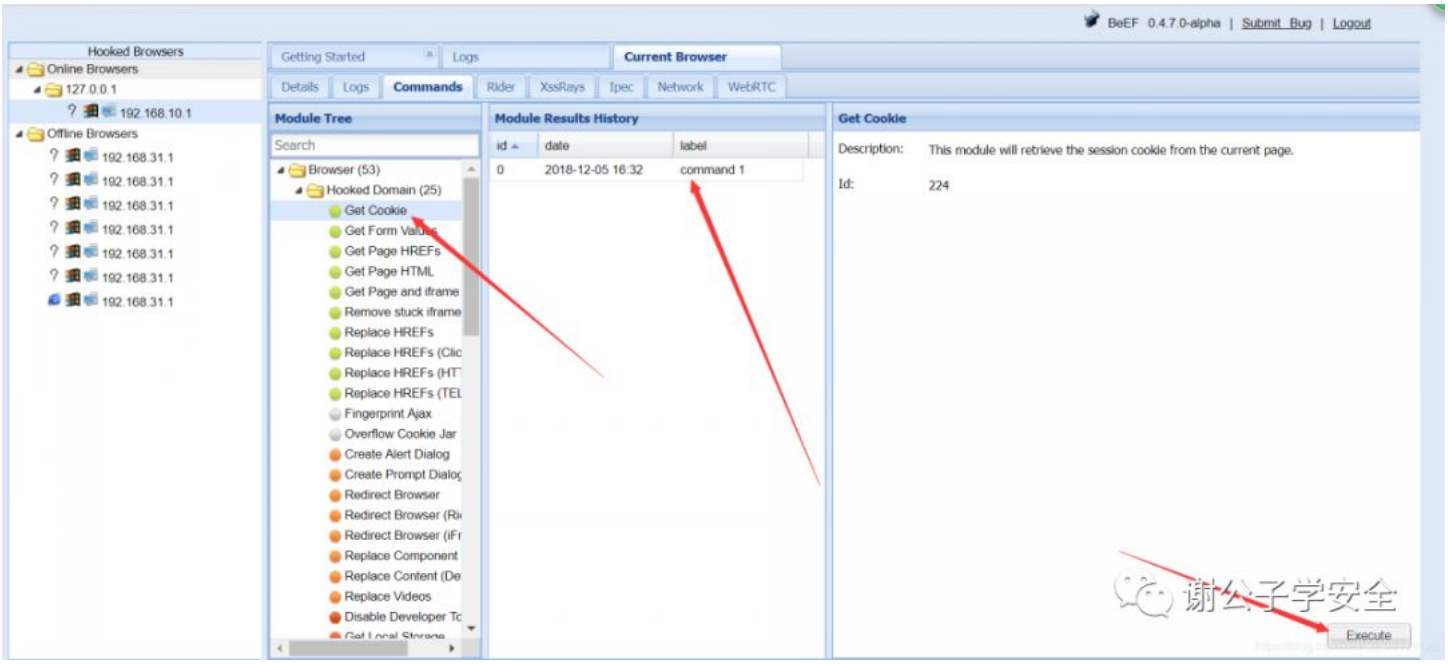
我们随便点开一个看看，发现有四种颜色的功能。

- •绿色的代表该功能有效，并且执行不会被用户所发现
- •橙色的代表该功能有效，但是执行会被用户所发现
- •白色的代表该功能不确定是否有效
- •红色的代表该功能无效



获取用户Cookie

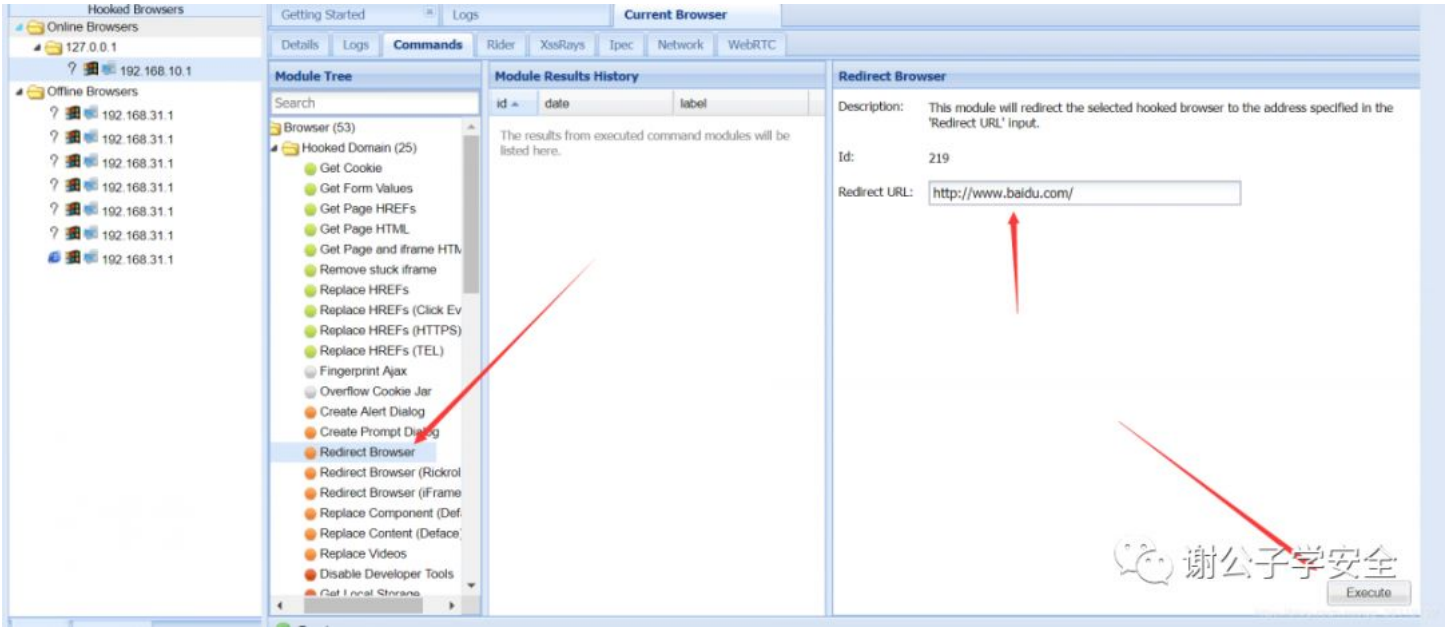
我们点击Browser—>Hooked Domain —>Get Cookie，然后点击右下角的Execute



然后点击我们执行的那条命令，右边就可以看到浏览器的 Cookie 了。

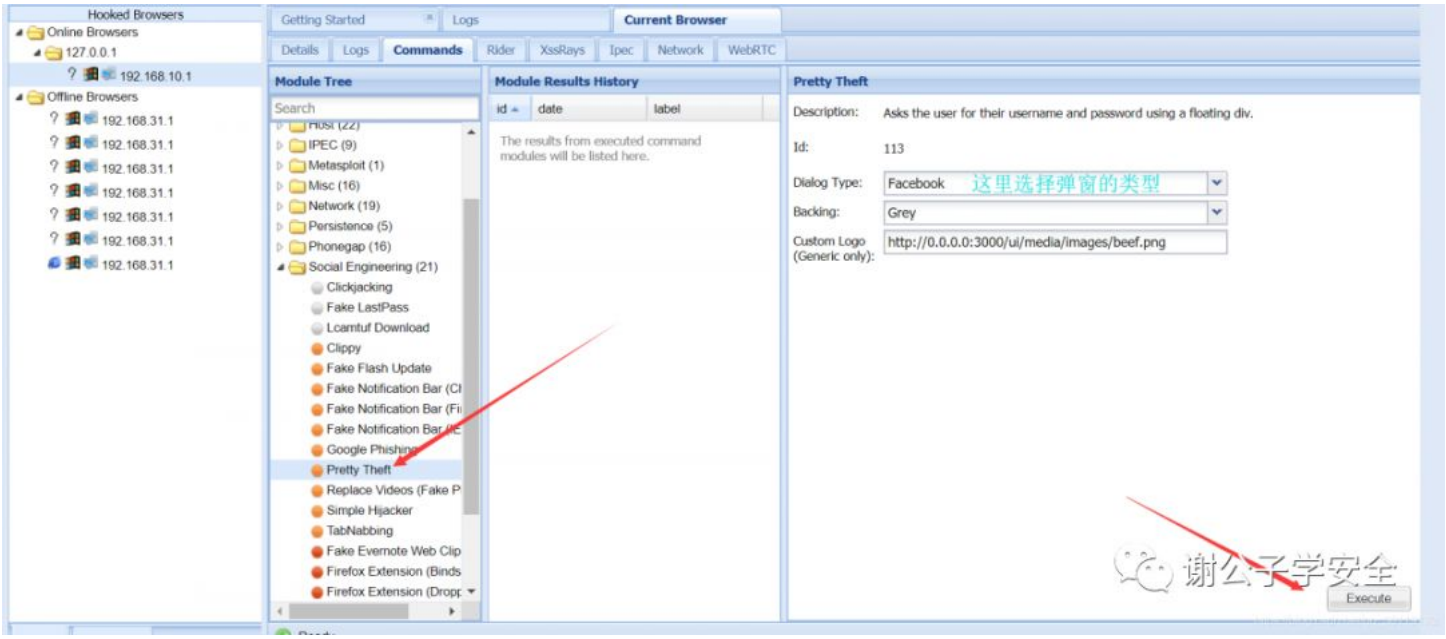
网页重定向

我们点击Browser—>Hooked Domain —>Redirect Browser，然后点击右下角的Execute，然后用户的浏览器的该页面就会跳转到百度的页面了。

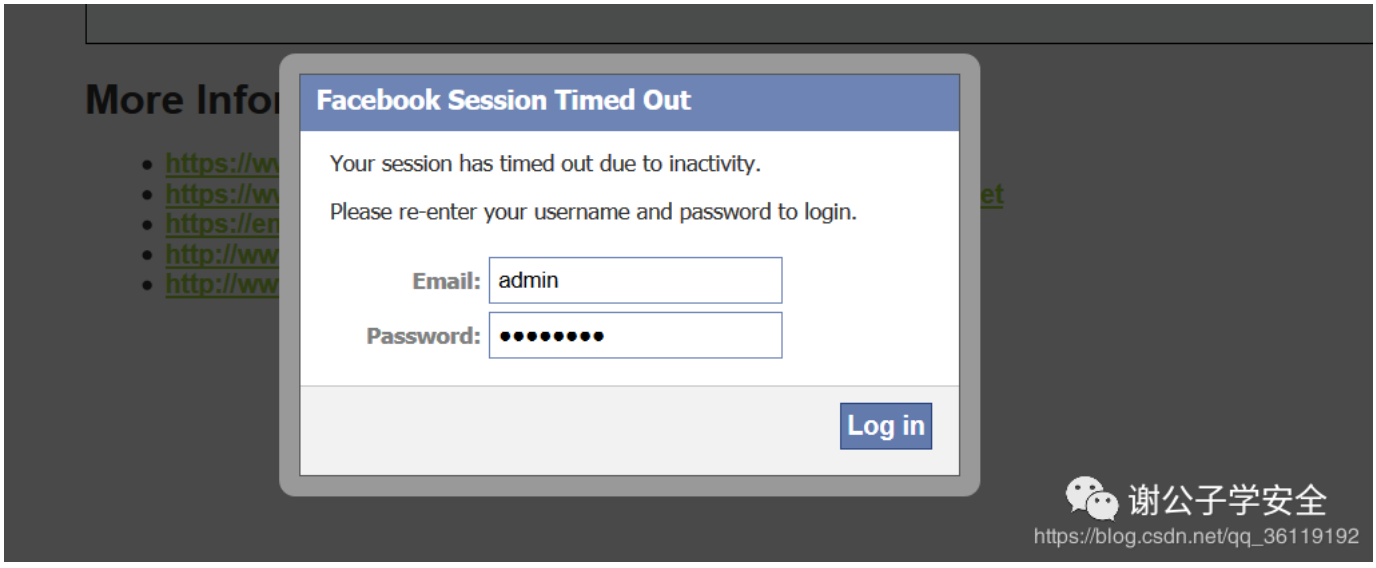


社工弹窗

我们点击Social Engiineering——>Pretty Theft ，然后右上角选择弹窗的类型，右下角点击 Execute

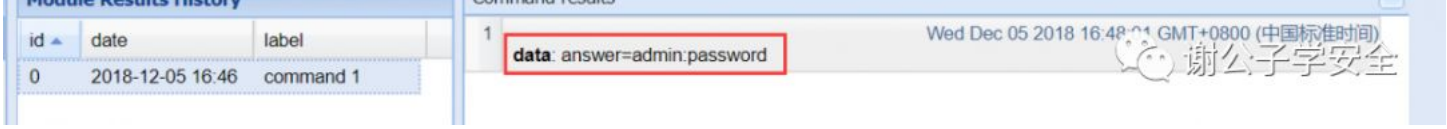


然后浏览器那边就会弹出框，如果你在框内输入了用户名和密码的话



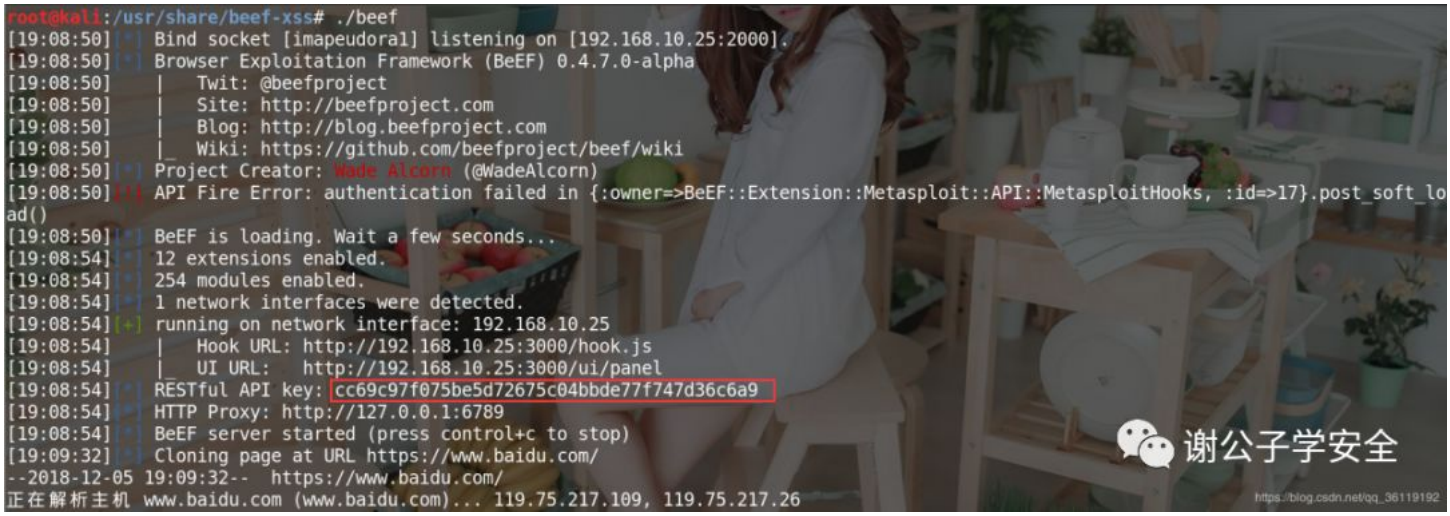
如果用户输入了用户名和密码，点击了Login的话，我们后台是可以收到密码的

回到顶部



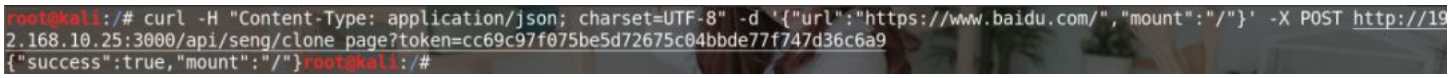
钓鱼网站(结合DNS欺骗)

进入/usr/share/beef-xss/目录下，执行命令：**./beef**u3000启动 beef ， API Token值

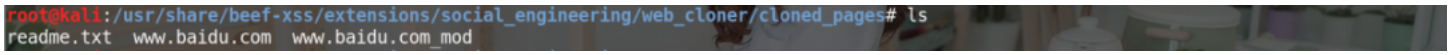


新打开一个页面，执行下面的命令

```
curl -H "Content-Type: application/json; charset=UTF-8" -d '{"url":"https://www.baidu.com/","mount":"/"}' -X POST http://192.168.10.25:3000/api/seng/clone_page?token=cc69c97f075be5d72675c04bbde77f747d36c6a9   #这里的地址token是我们上一步获取到的token
```



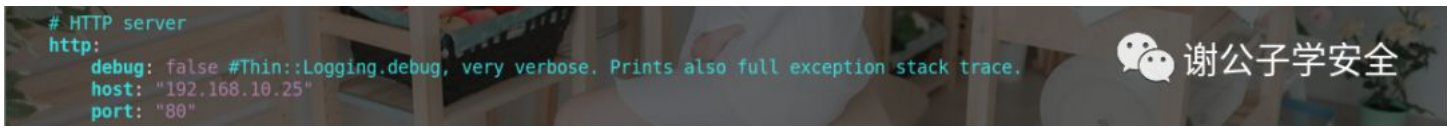
我们克隆的网站在目录：/usr/share/beef-xss/extensions/social_engineering/web_cloner/cloned_pages 下



我们访问：http://192.168.10.25:3000/， 可以看到和百度一模一样。只要别人访问了该链接，这个浏览器就可以被我们控制了！

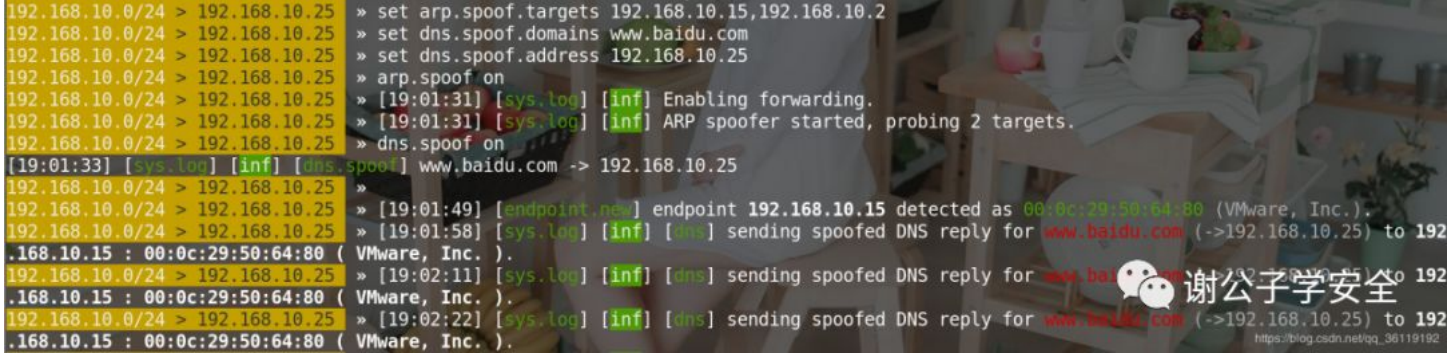
那么，如何让其他人访问我们的这个链接呢？我们可以结合DNS欺骗，将百度的地址解析到我们的这个链接上，这样，别人访问百度的时候就自动跳转到我们的这个页面了？

进行DNS欺骗之前，先去配置文件中把3000端口改成80端口



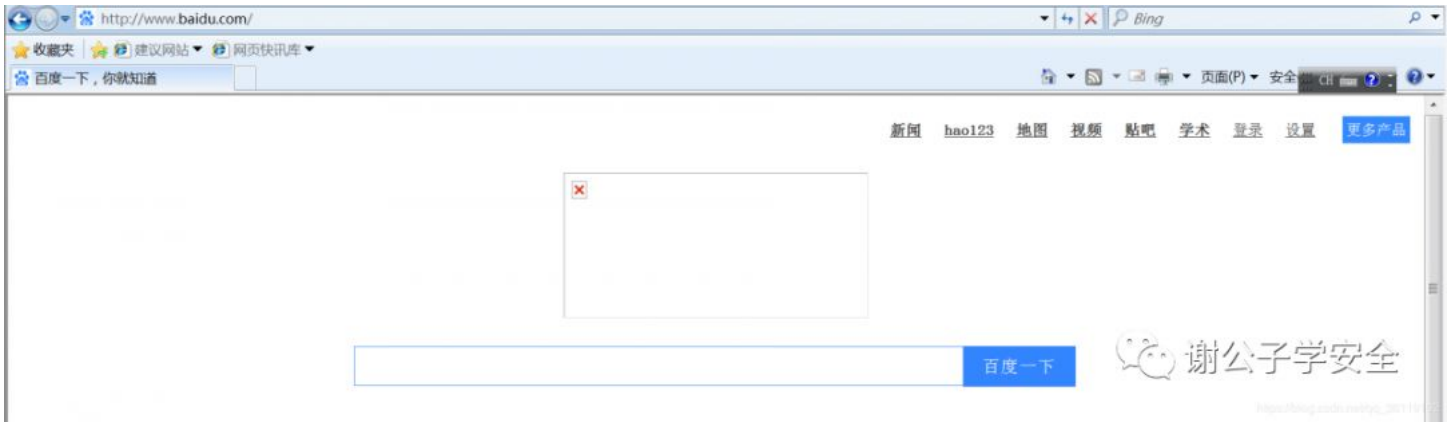
然后利用bettercap进行DNS欺骗。

回到顶部



然后重新打开beef，然后克隆www.baidu.com网站

只要被欺骗的主机访问www.baidu.com，其实跳转到了我们克隆的网站。这里百度的图片没加载出来，有点尴尬。



更多的关于BeEF的使用，参考Freebuf大佬的文章，写的很详细，很好！传送门——>https://www.freebuf.com/sectool/178512.html

相关文章：Bettercap2.X版本的使用

来源：谢公子的博客
责编：梁粉