为什么学kali容易进局子—ARP断网攻击与监听

极客事纪
已认证账号

找资源 | 领资料 | 涨知识 | 学技能
mp.weixin.qq.com/s?__biz=MzkxNTI1OTc4…

最近我发现，有很多学员都对kali渗透非常感兴趣，有着一颗想要学习新知识的心，可却总是畏惧于对想要学习内容的未知，而这也是大多数人失败甚至后悔终身的原因：因为他们从未开始过！

小编在这里说一句：坑就在你面前，别总是犹豫徘徊，大胆一点，向前一步，入了这个坑，莽着头就是往前冲，别多想，别回头，终有一天，你也会成为别人眼里的前辈！

至于为什么说学kali容易进局子，看完这篇文章你就会有所了解~

本期主题

Kali渗透-ARP断网攻击与监听

演示如何借助Kali Linux系统内置的 nmap、arpspoof、driftnet、ettercap 等渗透测试工具对局域网内(同WIFI下)同一网段的PC主机、手机进行 ARP 欺骗 和 流量监听，实现对目标主机/手机的断网攻击、图片窃取、密码监听 等攻击目的。

使用工具：ARP欺骗、图片捕获、抓包

- **arpspoof**

ARP欺骗的工具，可毒化受害者ARP缓存，将网关MAC替换为攻击者MAC

- **driftnet**
  图片捕获工具，用于监听网络流量并从它观察到的TCP流中提取图像的程序
- **ettercap**
  网络抓包工具，利用ARP协议的缺陷进行中间人攻击，嗅探局域网数据流量

环境说明：主机及IP地址

- Kali Linux：192.168.0.198
- Win 10 物理机： 192.168.0.106
- honor 20 手机： 192.168.0.105
- 魅族 A5 手机： 192.168.0.100

Kali 虚拟机使用桥接模式，Win 10 物理机和 华为荣耀20、魅族A5 实体手机连接同一个WIFI，使得四者处于同一局域网同一网段之下，可互相(Ping)连通。

应用场景

- 室友半夜打游戏、看视频太吵了，忍无可忍的你“优雅”地使用ARP欺骗切断他的WIFI，然后舒服地睡觉，留他一脸蒙圈……；
- 室友半夜盯着手机疯狂偷笑，你可以通过使用 arpspoof+driftnet 将他手机正在浏览的图片保存到 Kali 主机内，好东西得分享……；
- 室友跟你吹嘘他高数考了100分，然而每天比他努力却只考了60分的你表示不服，通过使用 arpspoof+ettercap 监听他登陆教务管理系统时输入的账号密码，发现这货只考了10分…

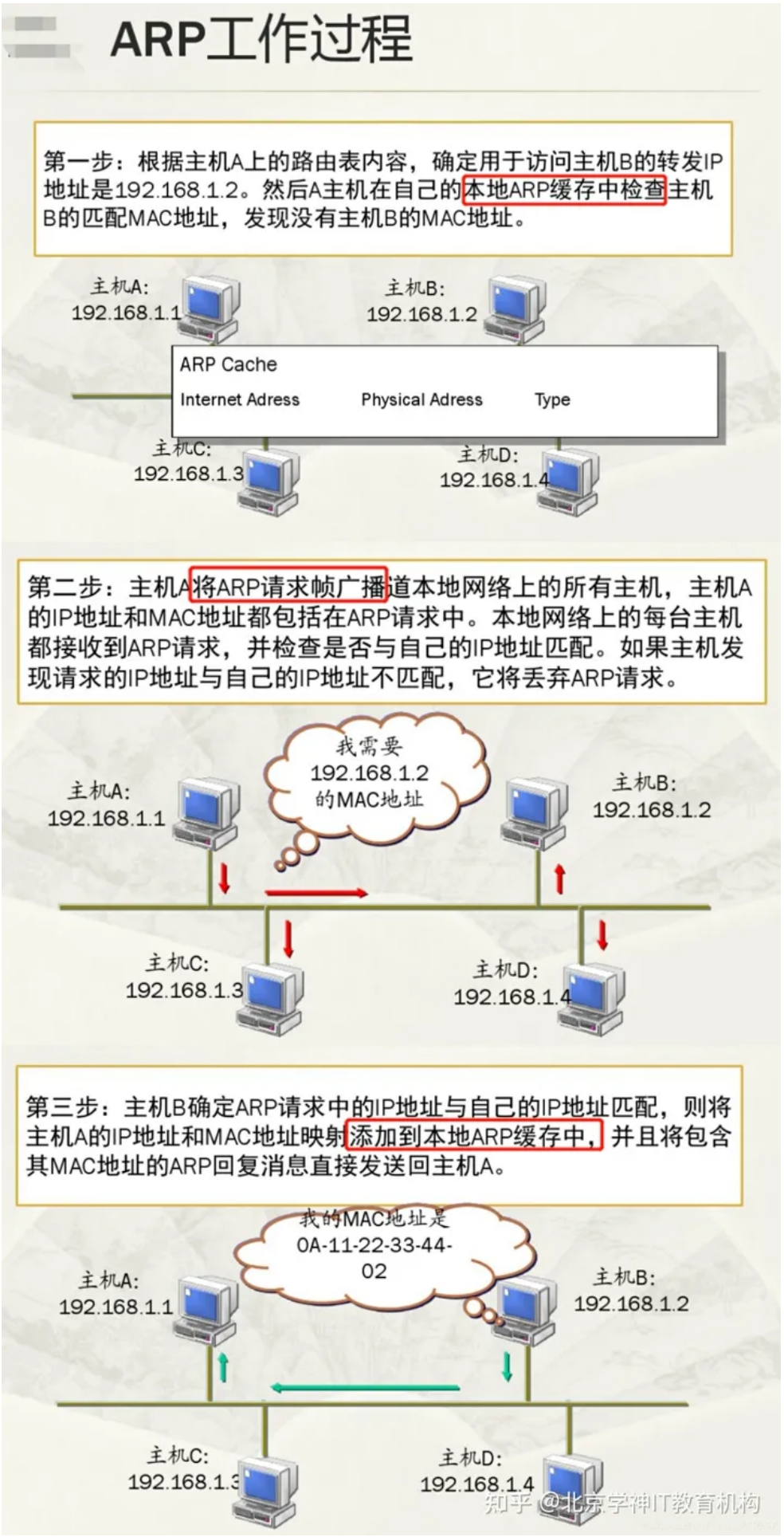
以上应用场景均假设与“被害人”处于同一WIFI(校园网)环境之中。再次强调下本文所述方法具有攻击性，各位同胞切不可以身试法……

1、断网攻击

在演示如何对局域网内部的主机进行断网攻击之前，我们先来了解下攻击原理——ARP欺骗。

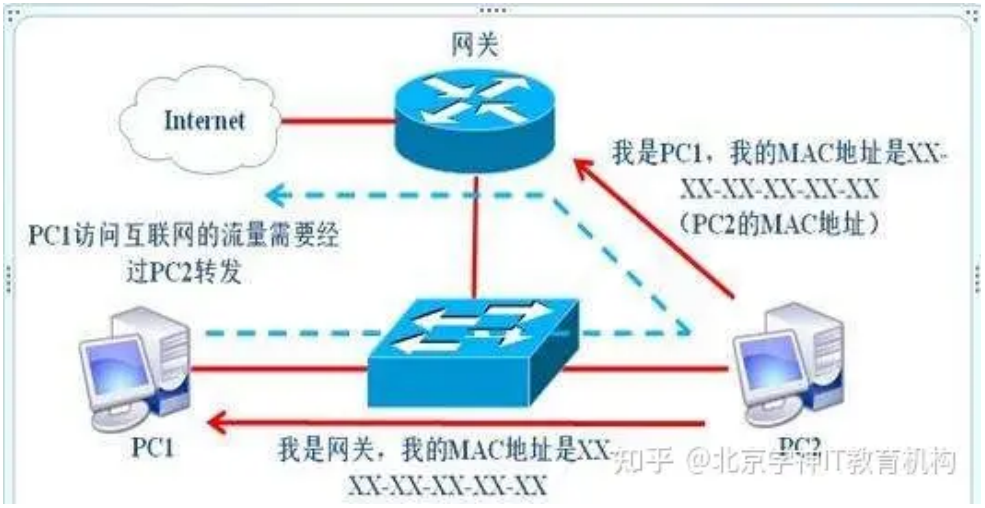
2、ARP欺骗

ARP(Address Resolution Protocol)即地址解析协议，是根据IP地址获取物理地址的一个TCP/IP协议。主机发送信息时将包含目标IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址；收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，下次请求时直接查询ARP缓存以节约资源。



ARP欺骗

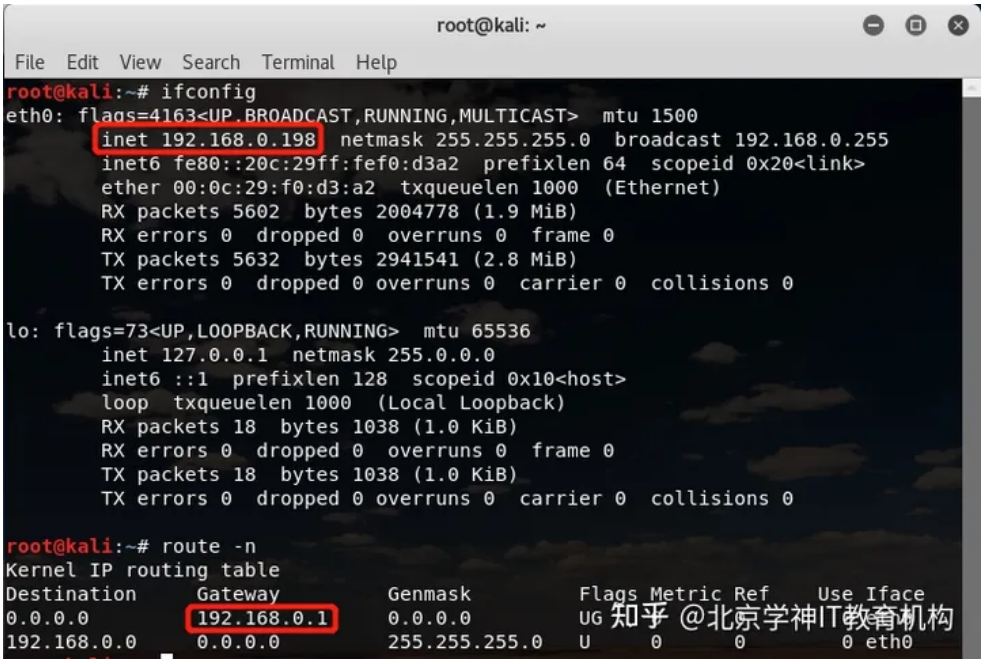
地址解析协议是建立在网络中各个主机互相信任的基础上的，局域网络上的主机可以自主发送ARP应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将其记入本机ARP缓存；由此攻击者就可以向某一主机发送伪ARP应答报文，使其发送的信息无法到达预期的主机或到达错误的主机，这就构成了一个ARP欺骗。



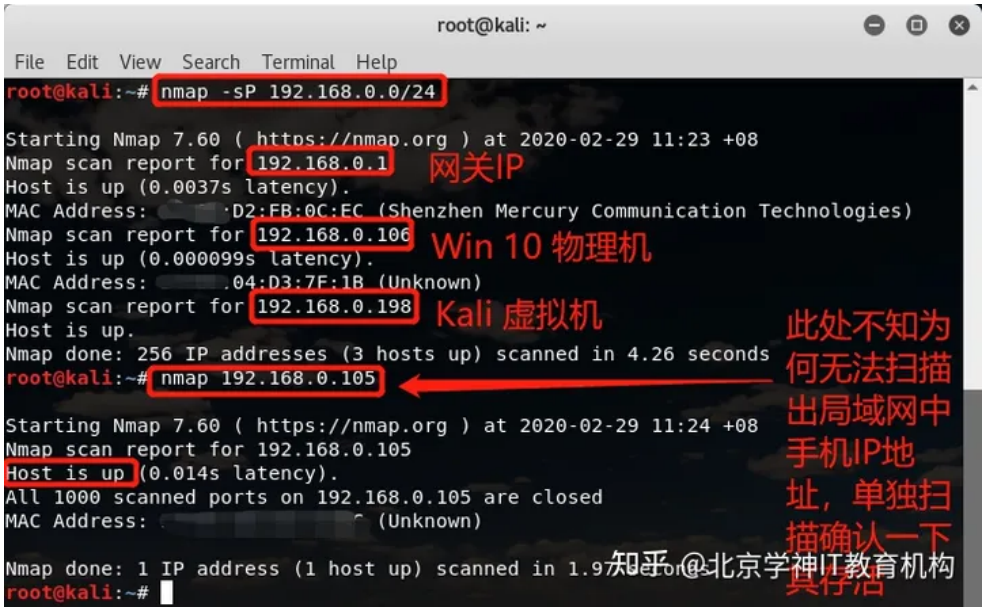
由于ARP缓存表不是实时更新的，如果在网络中产生大量的ARP通信量，攻击者只要持续不断的发出伪造的ARP响应包就能更改目标主机ARP缓存中的IP-MAC条目，造成网络中断或中间人攻击。

3、攻击演示

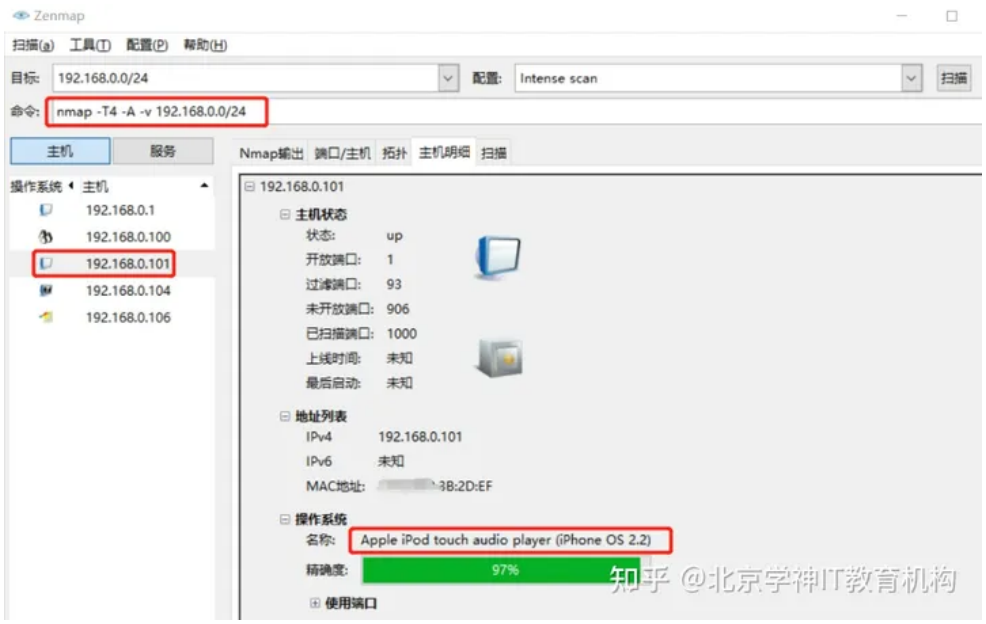
1、将 Kali 虚拟机配置为桥接模式，查看其IP地址和网关地址：



2、使用Nmap扫描局域网中存活的主机的信息（也可以使用 Kali 内置的 Nmap 图形化界面软件 Zenmap 扫描，结果是一样的）：



3、在 Win 10 主机使用 Zenamp 做下全面扫描，发现华为手机还是无法扫描到IP地址，但 IPhone 和 魅族手机可以扫描到：



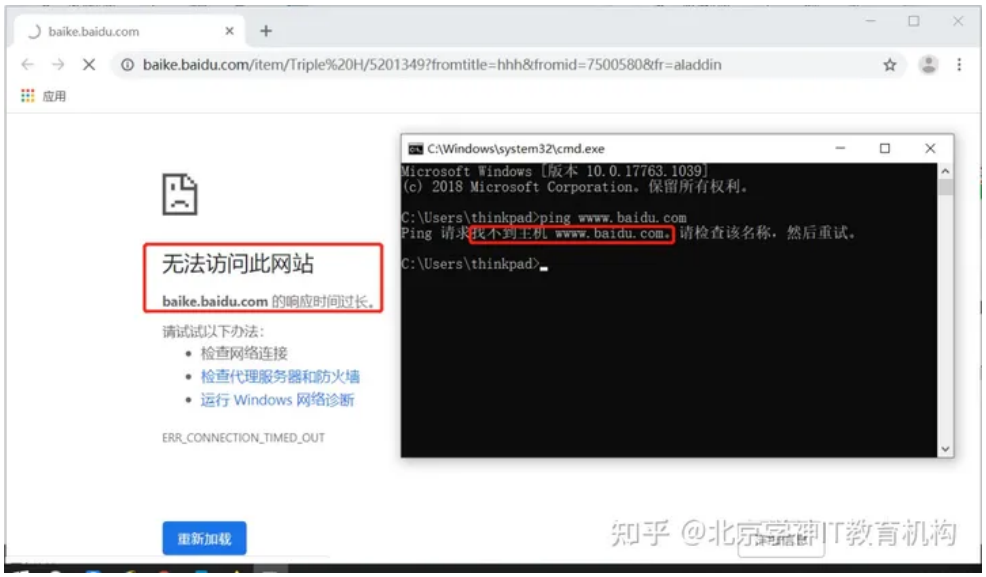
4、在Kali终端执行 arpspoof 命令：

arpspoof -i en0 -t 192.168.0.106(目标IP)

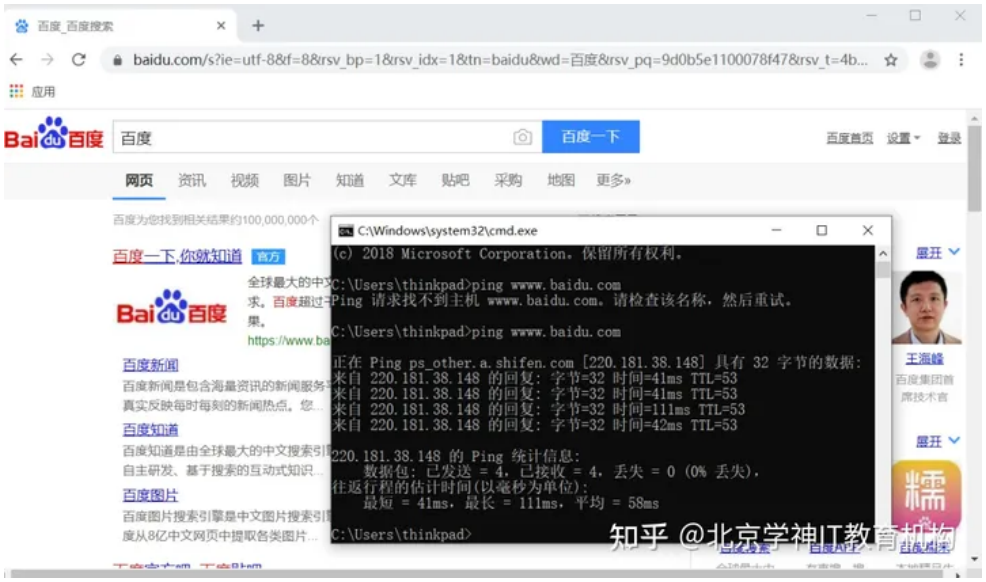
192.168.0.1(网关IP)

开始进行 ARP 断网攻击，攻击目标为 Win 10 物理主机：

5、此时 Win 10 主机已经无法正常连接互联网，访问百度后如下：



6、在 Kali 的终端中按下键盘 Ctrl+Z 组合键中断欺骗，物理机就可以恢复正常访问互联网了：



7、对华为荣耀20手机做了同样的断网攻击测试，结果没法完全断网……但是会极大地限制网速，刷网页、视频会十分卡顿。然而对 魅族 A5 手机进行测试，则可以正常实现断网：

华为手机在 Nmap 中扫描不出其 IP 地址、ARP欺骗也没法实现彻底的断网，具体原因待研究……在这里暂时先默默送给它一句Six Six Six吧……

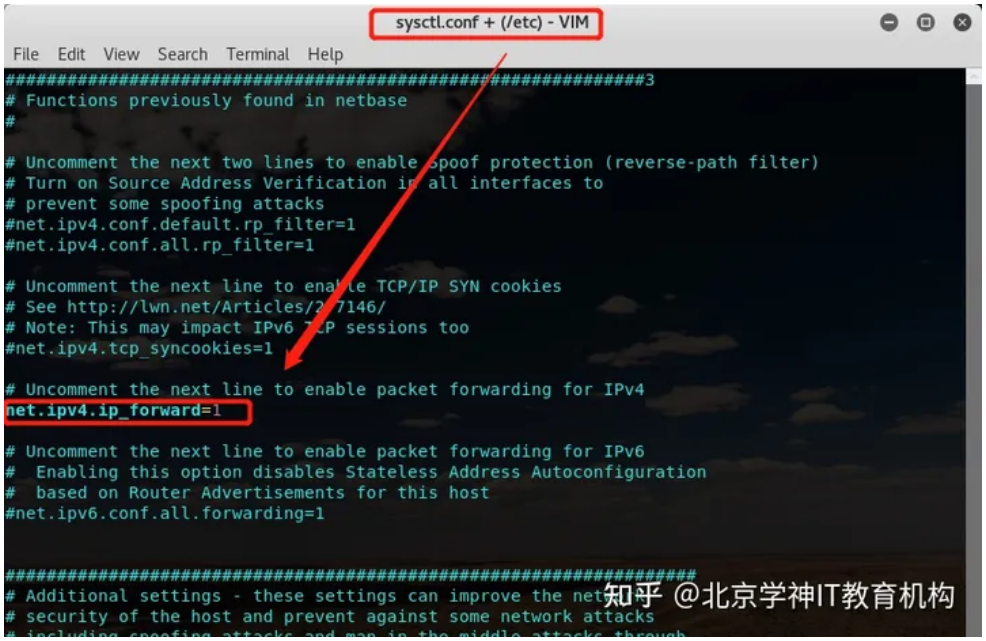
4、图片窃取

你以为Kali能做的仅仅是让局域网中主机断网这么简单？单纯截断受害者的数据流量可没多大意思，我们何不自己充当中间人将其数据流量转发出去，然后监听、获取受害者的数据流量呢（疯狂暗示）……

5、端口转发

在对受害者实施以上ARP欺骗实现断网攻击后，如果攻击者将自己的网卡开启流量转发，将截获的数据包传到真正网关，则可让受害主机不断网，同时可以监听到受害者主机的数据流量的内容。

1、编辑 Kali Linux 虚拟机/etc/sysctl.conf 配置文件，将net.ipv4.ip_forward配置项取消掉“#”注释符号，并将其值由 0 改为 1 即可开启端口转发：



2、接着在 Kali 终端重新执行 arpspoof 命令（注意网关IP和主机IP顺序此时需要对换一下）：

arpspoof -i en0 -t 192.168.0.1(网关IP)

192.168.0.106(目标IP)

重新对 Win 10 主机发动 ARP 欺骗攻击，此时其仍能正常联网，端口转发成功：

6、攻击演示

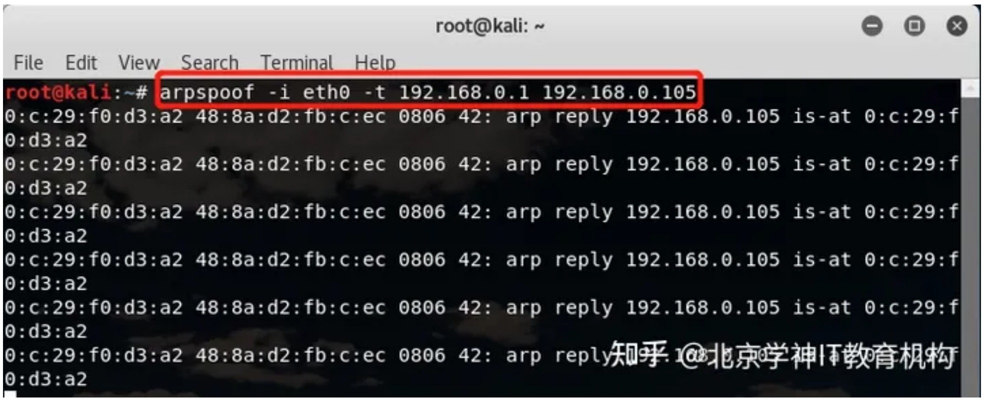
driftnet是一款简单而使用的图片捕获工具，可以很方便的在网络数据包中抓取图片，其使用语法：

driftnet [options] [filter code]。

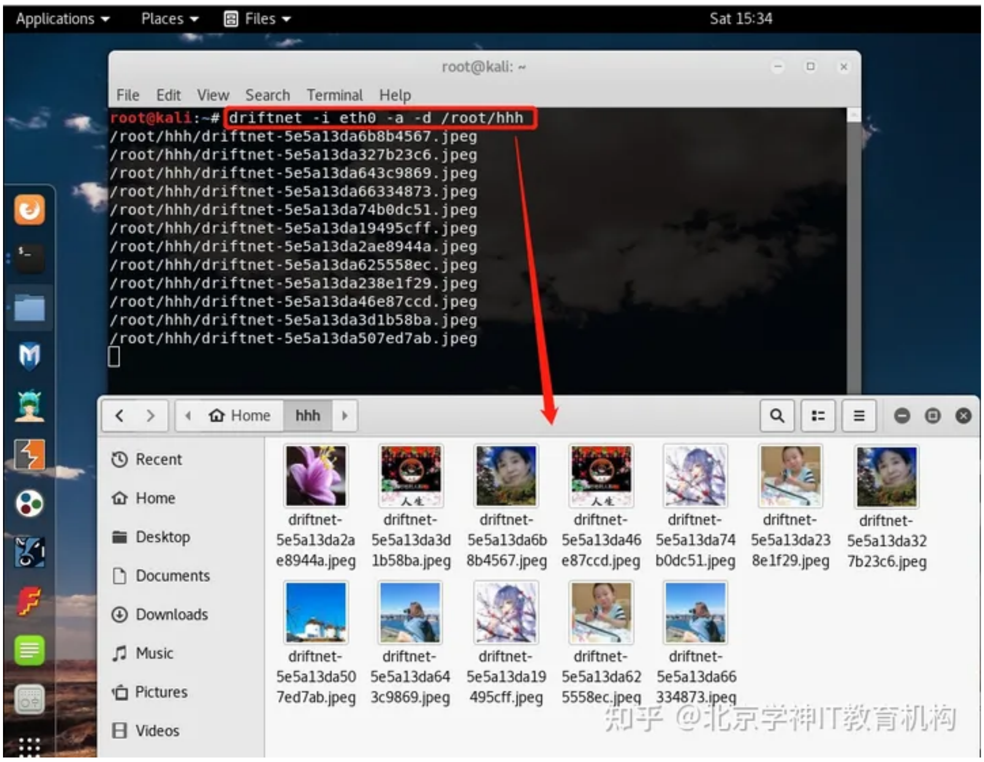
- -b： 捕获到新的图片时发出嘟嘟声
- -f： file 读取一个指定pcap数据包中的图片
- -i： interface 选择监听接口
- -p： 不让所监听的接口使用混杂模式
- -a： 后台模式：将捕获的图片保存到目录中（不会显示在屏幕上）
- -m： number 指定保存图片数的数目
- -d： directory 指定保存图片的路径

- -x： prefix 指定保存图片的前缀名

1、此次图片窃取的演示使用IP地址为192.168.0.105的华为荣耀20手机(前面断网不成功，本菜表示不服)，首先开启ARP欺骗：

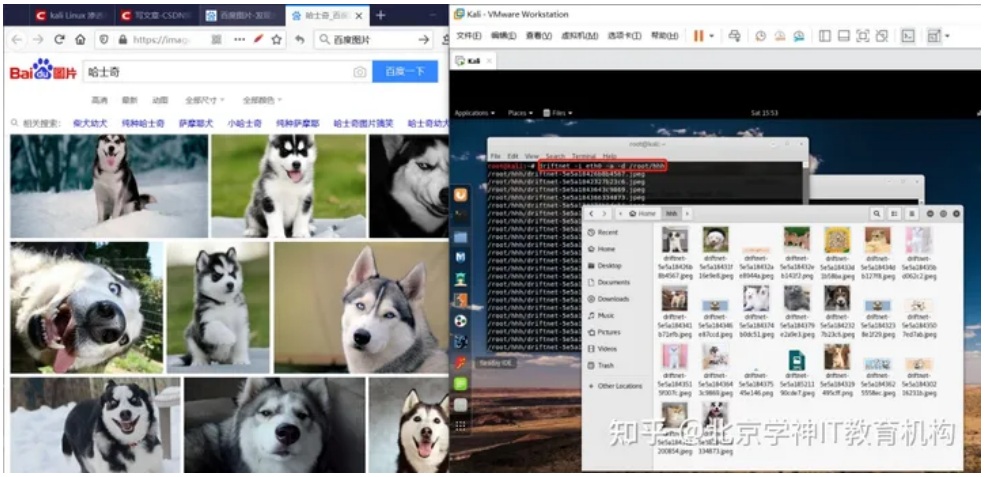


2、打开另外一个终端并执行 driftnet -i eth0 -a -d /root/hhh 命令，该命令会自动将手机浏览的图片保存到Kali虚拟机的/root/hhh路径下：



3、上图已成功获取到手机上正在访问的图片信息，而此时手机打开的是 “央视新闻” 微信公众号的新闻链接，图中保存了文章评论者的头像

4、此处还对 IPhone手机、Win 10物理主机均进行了测试，均可成功监听并保存受害主机的图片：



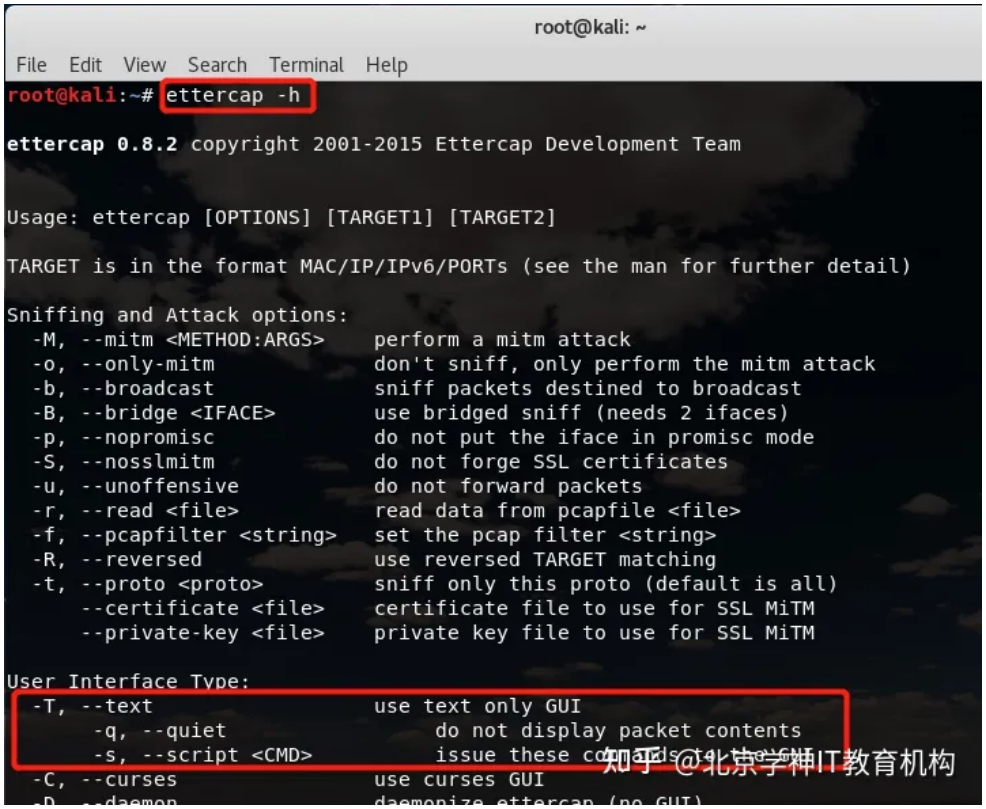
至此，图片监听窃取的攻击演示结束……骚年，看到这里，你还敢连着WIFI肆无忌惮地看“不可描述”的东西么？

7、密码监听

手机浏览的图片被监听窃取，想一想还是可以忍的（身正不怕影子斜）……但是如果连上网使用的账号密码也被监听了，兄die你还能稳得住么？

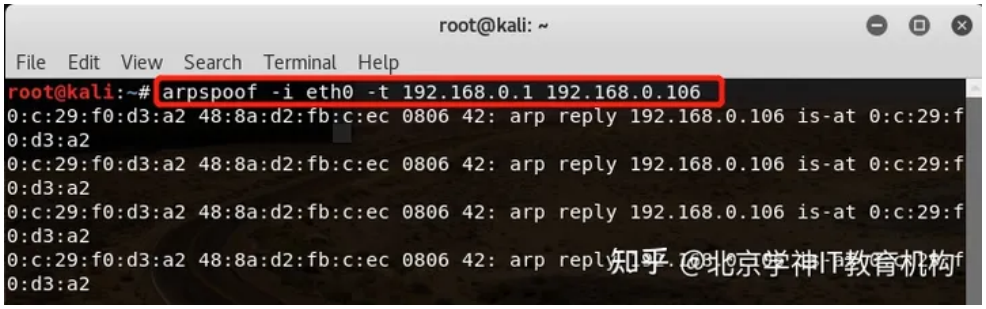
前面介绍了，ettercap是一款网络抓包工具，利用ARP协议的缺陷进行中间人攻击，可嗅探局域网数据流量。

其他命令和使用，我们可以直接在Kali 终端输入 ettercap -h打印：

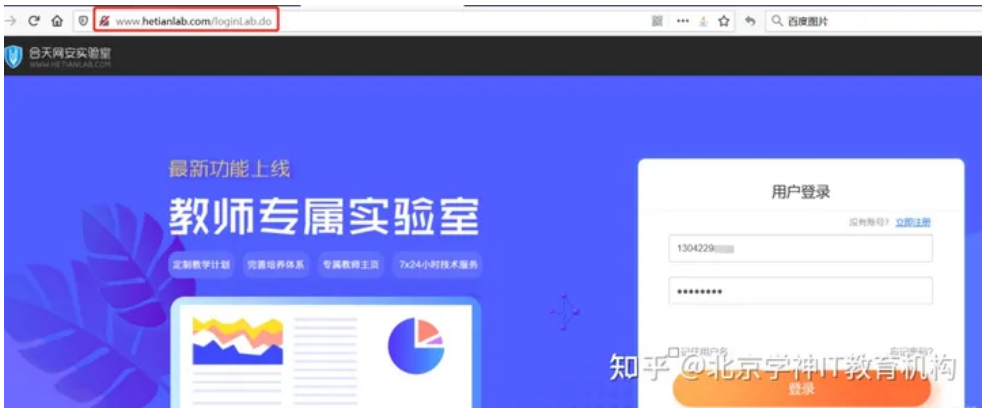


8、攻击演示

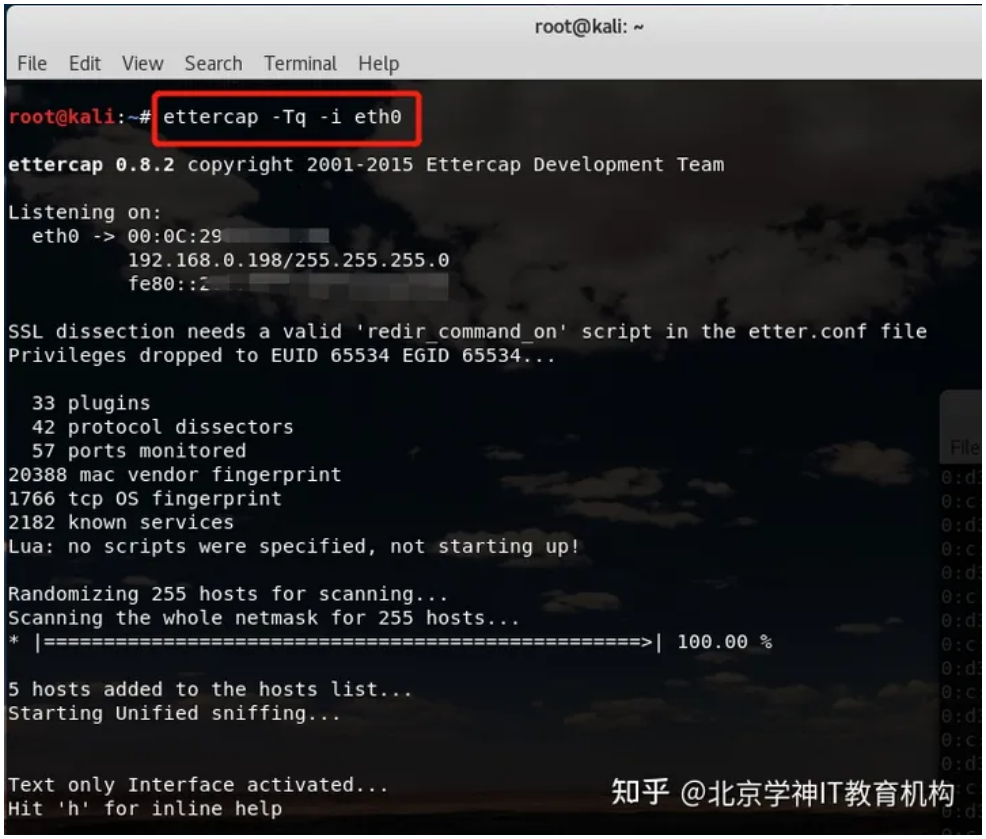
1、同样先在Kali终端执行 arpspoof 命令开启 ARP 欺骗攻击，攻击目标为 Win 10 物理主机：



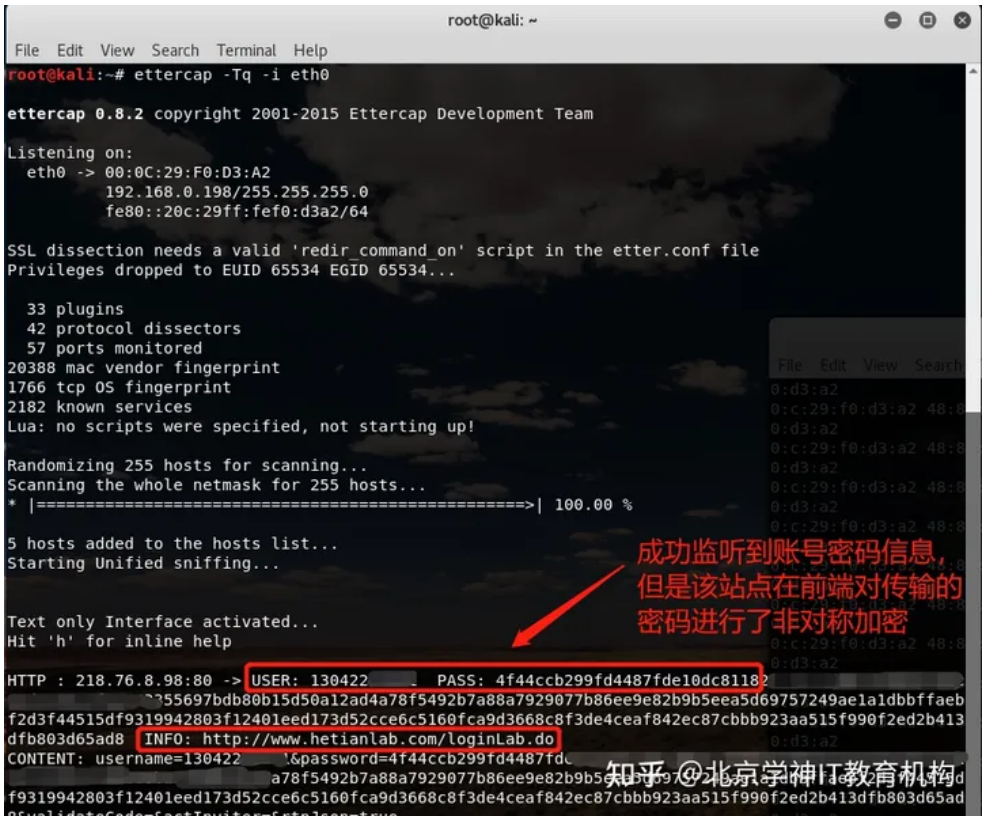
2、然后在物理机上打开一个合天网安实验室官网的登陆页面：



3、打开另一个 Kali 终端，开始利用 ettercap 来抓取账号密码，在终端输入命令ettercap -Tq -i eth0（这条命令表示监控 eth0 网卡的流量）即可，监听状态如下图：



4、此时在物理机输入正确的账号和密码后，即可在虚拟机终端输出打印其账号密码等登录信息：



5、至此，密码监听的攻击演示结束

9、总结

从上面的攻击演示可以看出，当你与攻击者处于同一局域网(同一WIFI)下面，攻击者可以借助ARP欺骗让你回到“村里还没接网线”的年代，同时还能让你的PC主机或者手机的部分隐私处于“裸

奔”状态……

防止ARP攻击是比较困难的，修改协议也是不大可能，但是有一些工作是可以提高本地网络的安全性和可提高电脑的安全系数，比如:

- 定期删除ARP缓存表
- 绑定静态的ARP表
- 安装ARP防火墙
- 拒绝连接安全性未知的WIFI等

我们可以在主机中使用以下命令查看本地的ARP缓存：

我们可以在浏览器进入网关管理页面（路由器后台管理地址），网络参数一栏有“IP与MAC绑定”一栏，把网关的mac地址与网关地址绑定就好了：

只要确定了对应关系，当攻击者发布ARP响应包时，就不会更新相应的IP-MAC缓存表。

到这里就全部结束了，想学习kali渗透的现在就可以行动起来了，为防止有些学员还不知道如何下手学习，小编特意整理了相关书籍以供各位交流学习。

总结，我的教学仅供大家学习使用，希望可以对kali linux有一些心得，到这里就结束了。

如果大家对黑客、kali、linux、K8S等小知识感兴趣，点击下方卡片直达~

编辑于 2023-03-28 09:58 • IP 属地北京

kali 渗透测试 黑客攻击

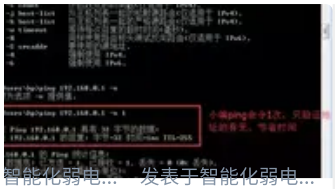
写下你的评论...

1 条评论 默认 最新

Horizon
sofa
02-12 • IP 属地江西 回复 喜欢

推荐阅读

第一次做弱网测试--fiddler模拟网络延迟



智能化弱电... 发表于智能化弱电...

macro... 发表于mall学...

玩转Linux内核

因为公司项目业务需要，前不久测试老大需要我这边对我们的性能测试apk做一下弱网测试，虽然以前弱网测试都有所了解。但是还没有实操过，作为一个三年工作经验的软

王大宝