我在实验室电脑上玩Kali（中间人攻击、ARP，顺便断了同学的网）

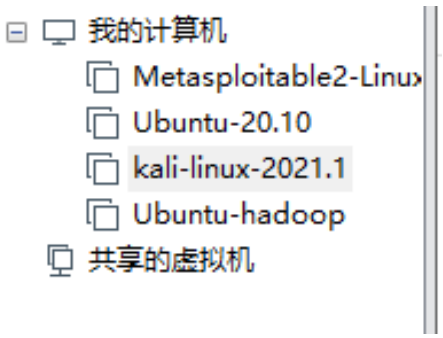
高星熠

前言

那天，我跑到实验室，打开了Kali。话说，在外地上学，我还一直没有在台式机上开过Kali，虽然实验室的也是虚拟机，但感觉还是超好的

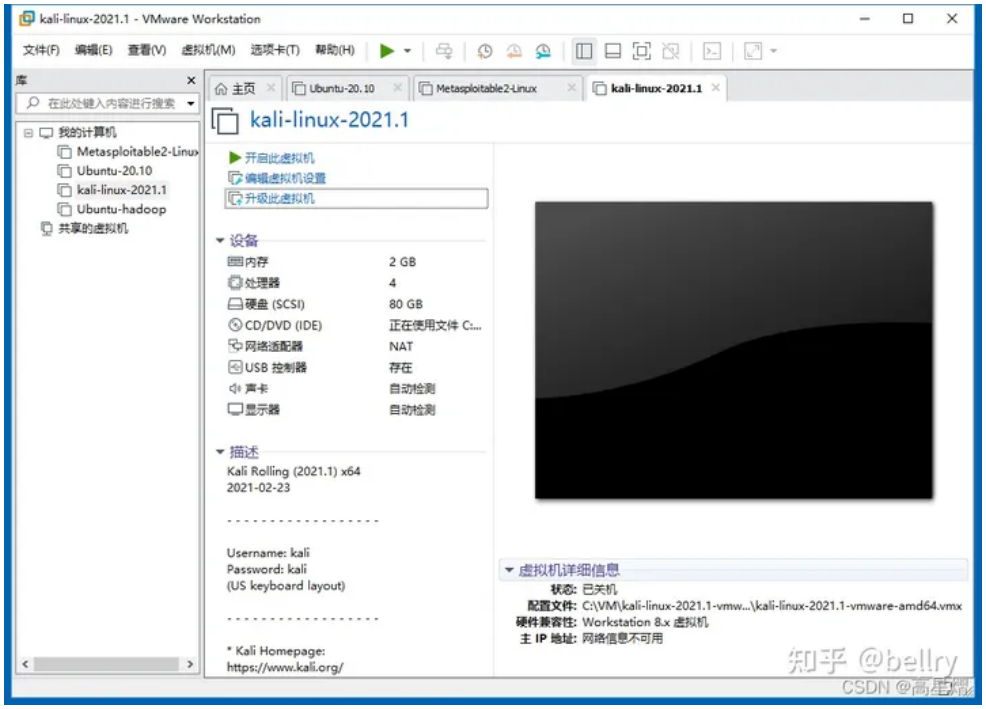
然后，就在实验室小玩了一波Kali，但是，你若因此觉得我是一个精通Kali的骇客，那还真的不是，只是为了应付这几天正在结课的系统测试，熟练的掌握了几个工具（Ettercap、Burp Suite）的操作方法罢了 。

话说那天，是上完篮球课，有一个同学要找我solo，然后我们打了11个球，我把他给打爆了 ，挺高兴的一件事，我就去超市排了个队，买了瓶水。突然发现 ，有节计网的实验课要去上，当我飞奔过去，还迟到一分钟 主要是太急，没回去取电脑 ，我就用实验室的电脑开始了操作。但是，最后无聊就开始找实验室电脑上的程序，直到打开了虚拟机，然后



有kali,直接DNA动了 。直接点开，再我赞叹2021版的炫酷背景时（高考完装的Kali，一直没怎么用，还是2020版的。。。） 遇到了这个

于是，我尝试了几个密码，结果都不对。我突然想，这个装着不就是给人用的，账号密码什么的应该是写在什么地方，于是，我去翻找了根目录和bin，想看看有没有readme之类的文件。 最后，啥也没找到回到了VMWare Workstation



等等，我好像看到了什么

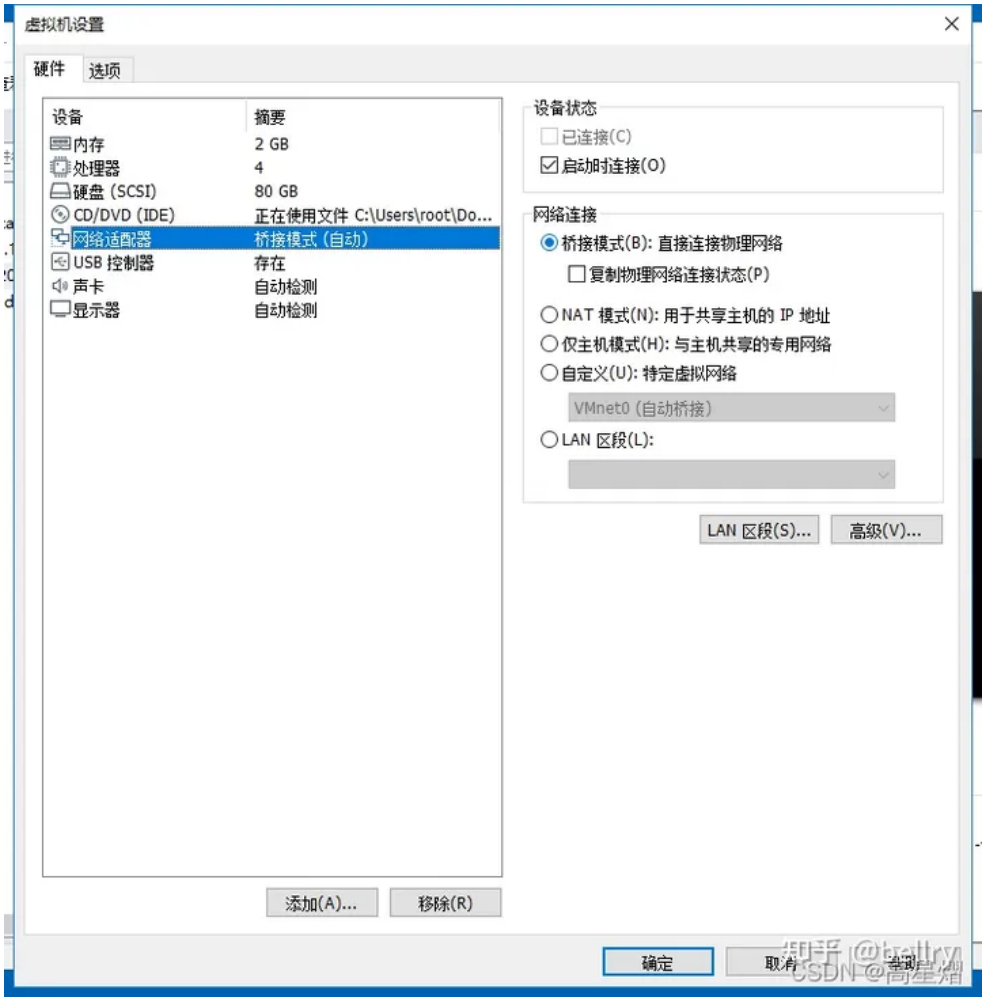
我真是大聪明啊

终于还是进来了，

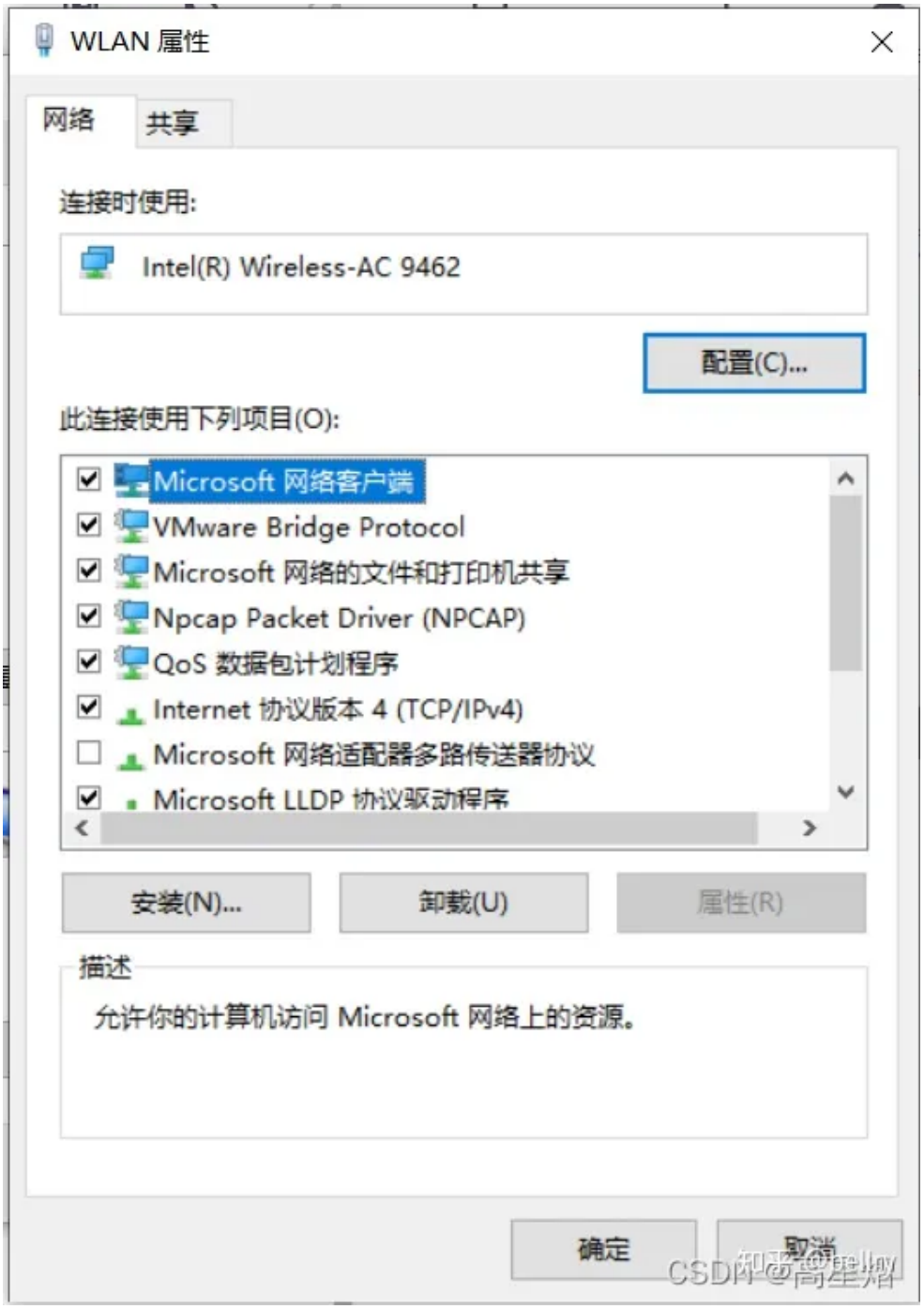
准备工作

网络环境的外部桥接

首先，我们知道一点要做中间人、arp欺骗或者是直接去断人家的网，前提是发起攻击的设备要和受害者在一个局域网内。这样才能通过去嗅探、伪造网关去欺骗。所以，我们得先把虚拟机的网络配置到和物理机的网络环境一致才行。 我们先出去进入到虚拟机设置



点击网络适配器，把原先的NAT模式改为==桥接模式==。 点击确认后，点击**编辑**，选择**虚拟网络编辑器**，进去后把VMnet桥接到网卡上去。网卡是用来放到网段里去监听用的。这个要看自己的网卡编号，可以在控制面板的网络里面，点进去后查看属性，就可以看到



上面那是我笔记本的网卡，不是实验室那台的。 这样设置完了以后，在启动Kali进去以后就可以看到已经连上校园网了。

基础的命令语句

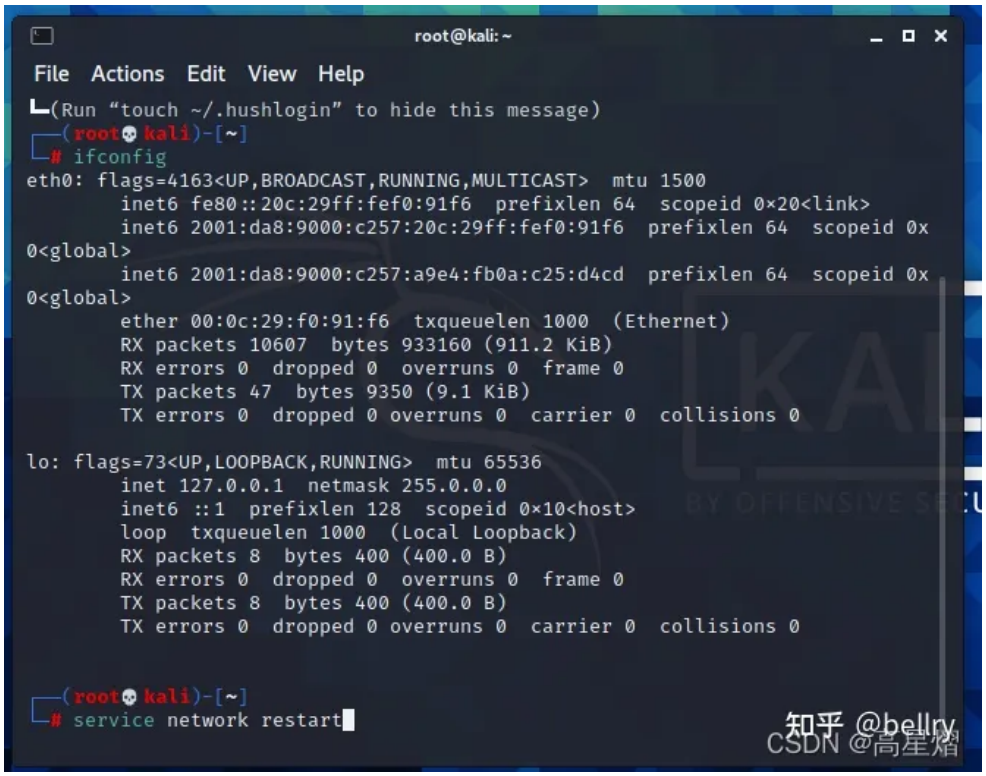
大一的时候，用过树莓派的虚拟机，Linux的命令知道一些

启动权限：

```
sudo -i
```

因为Kali里面大部分的工具都是要权限运行的，所以需要先赋权。 这里先说说我当时在实验室干了啥吧 我就很正常的在查看了一下ip 查看ip

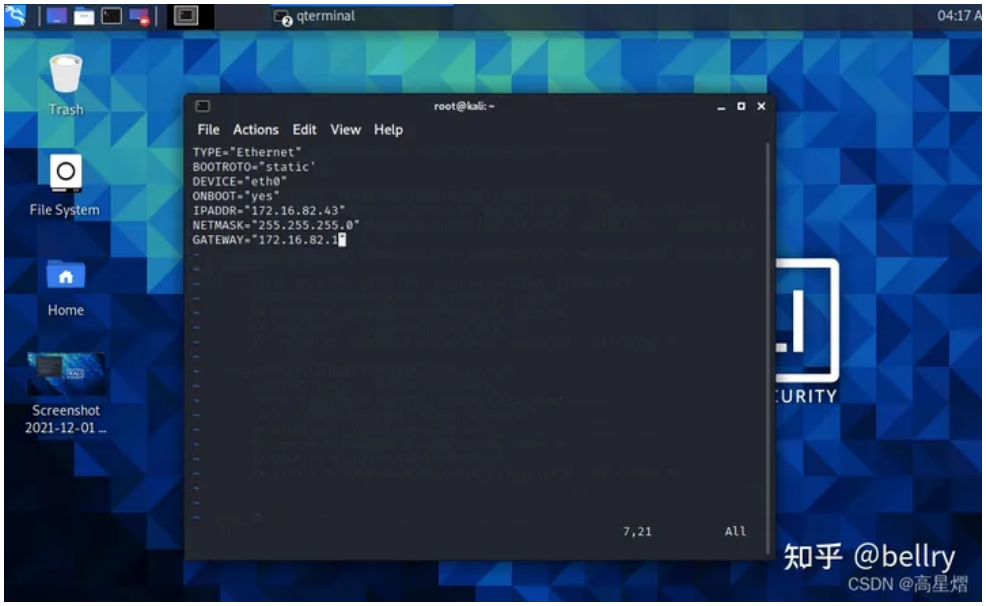
```
ifconfig
```

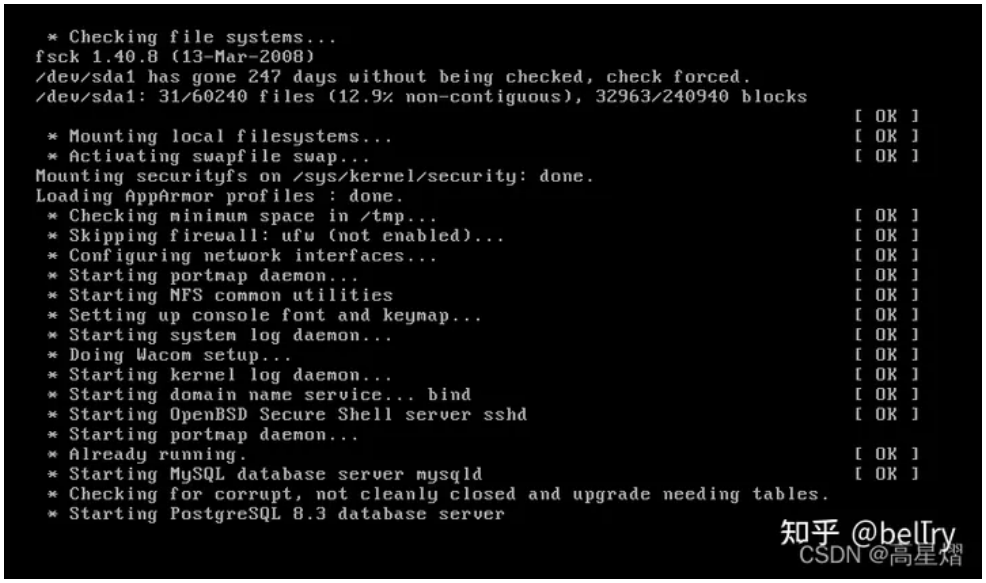


大家应该还看到了这个命名 刷新网络

```
network restart
```

这是因为上面出来的ip只有ipv6的，我改了一下配置文件，然后刷新了一下。



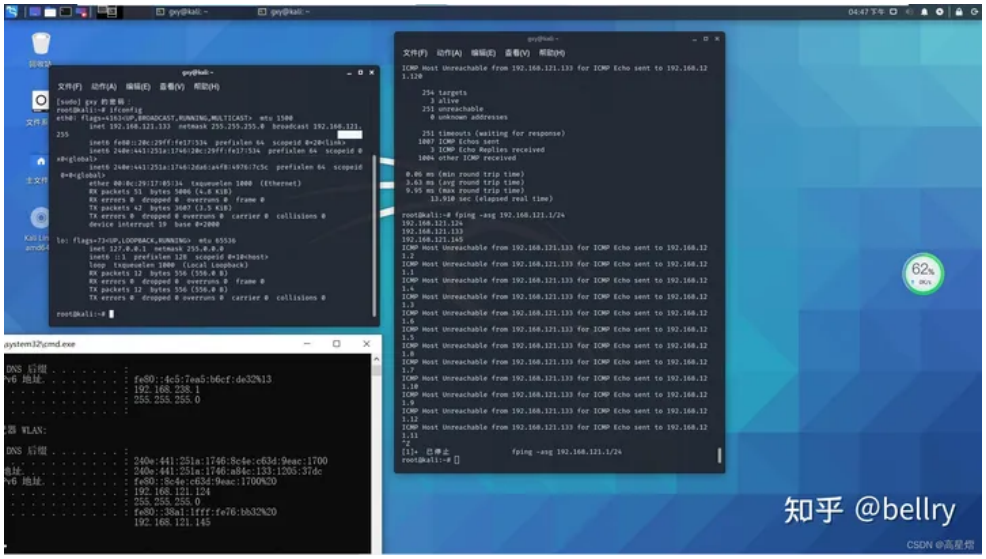


然后，我扫描了一下，周围的ip,发现存活的ip就只有4个。。。我抬头望了下四周，除了老师，大家好像确实都在用自己的电脑。好吧

```
fping -g ip/24
```

后者是

```
fping -ags ip/24
```



这里，其实我推荐使用Ettercap这个工具去扫描周围的IP，因为他是有机器的描述反馈的，这样就非常方便定位到目标攻击的机器（~~同学的机器 ~~）了。 然后，在实验室里，我就啥也不敢再干了，毕竟就只有4个ip，我想了一下，一个是网关，一个是Kali的ip，一个是物理机的ip，还有一个就是老师的机器。得，旁边就是网安实验室，在综合楼还是不太敢造次 于是，下了实验课，到了上军事理论课要去工学馆的时候。。

中间人攻击与ARP欺骗

上军理课，我早早去了工学馆打开了Kali，点开了Ettercap，打算先进行一下中间人

什么是中间人攻击（Man-in-the-MiddleAttack， MITM）

其实，这个名字就挺形象，在端系统和服务器中间还存在一个中间人，进行窃听、甚至是篡改、劫持，端系统与服务器的交互。

这其实是一件很危险的事情，尤其是在网络已是十分发达的现在，以及未来的物联网与区块链不断发展。它可以通过任何一个可以联网的设备找到你（例如：手机、手表）；它也会去窃听我们输入的用户账号及密码；它甚至可以控制但凡能联网的设备，让它非正常的工作（比如：无人机、心脏起搏器）。所以我们要当心这种攻击方式。

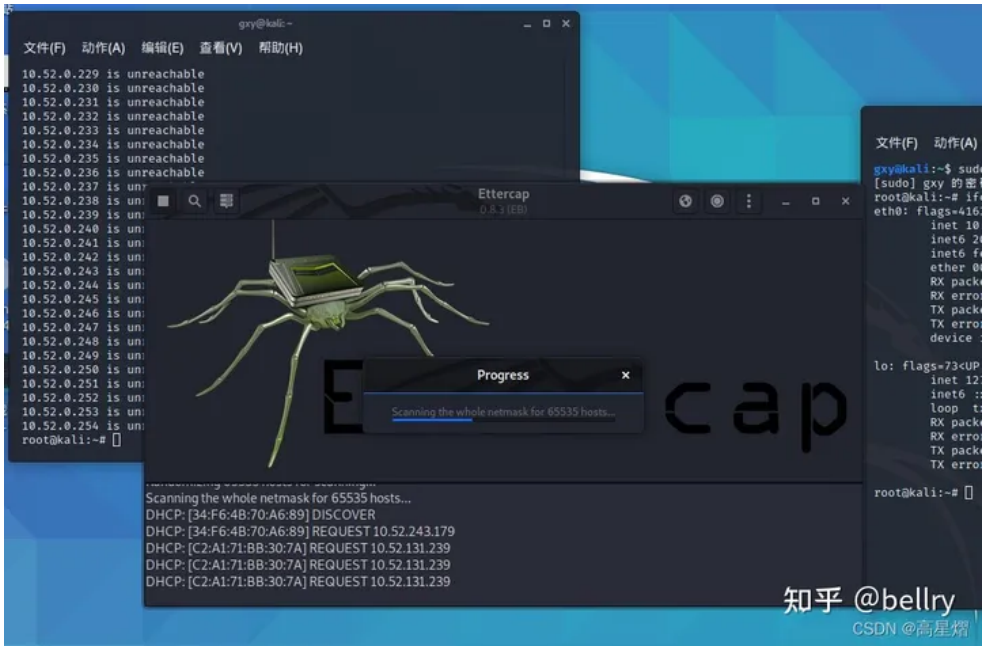
Ettercap的使用

Kali为我们提供了一个很好用的中间人攻击工具——Ettercap。在嗅探/欺骗里面

当然，你也可以通过命名行进行操作，那样体验感会更好，但是这样操作会更加直观。

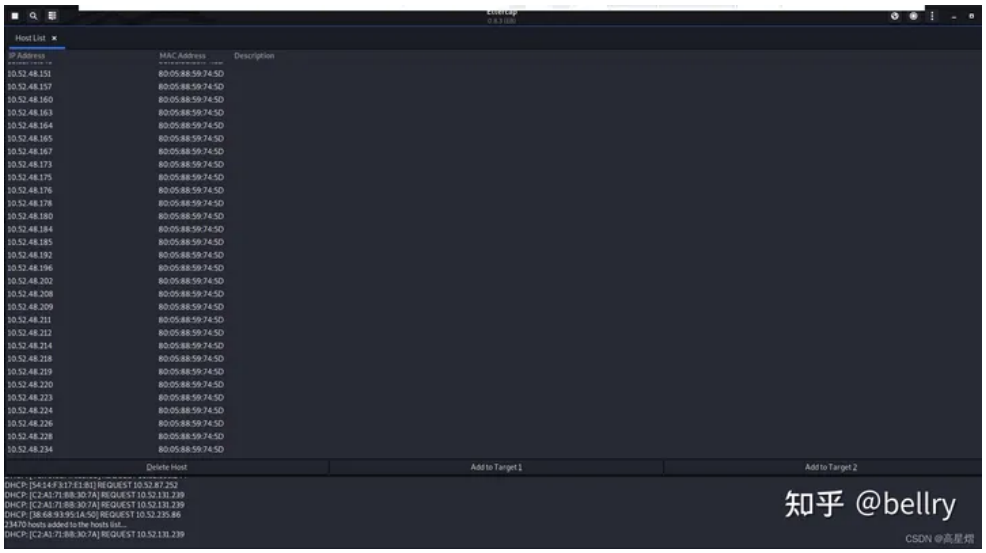
打开后，我们可以看到这个eth0就是我们用来监听的网卡，下面有一个Bridged sniffing 的选项，这个是用来桥接到现网上嗅探的，在后面我们进行Arp欺骗真实网站时是需要勾选的，我们这里先不选，先进行网段内的用户扫描。 于是，我连上校园网，开始扫描主机， 扫描主机，要点击左上角的小放大镜（scan for hosts）

干这件事确实是花费了我一些时间

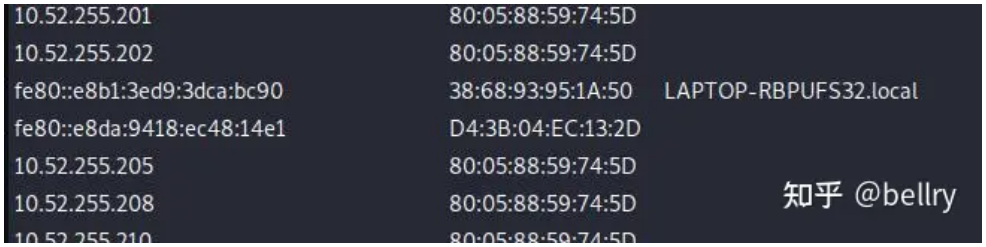


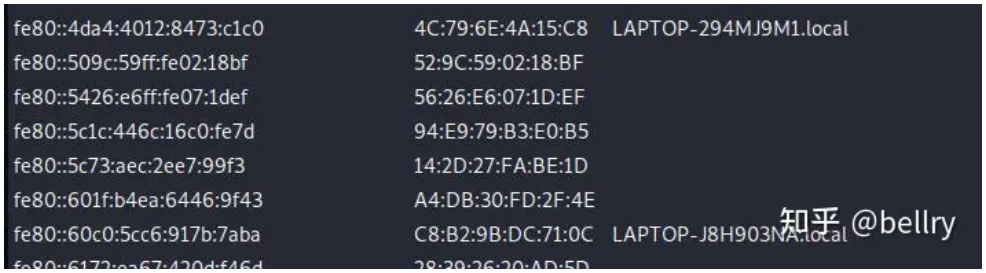
6.5万个ip，扫描了将近10分钟。 扫描完成后，要就可以把这些ip给呈现出来，点击左上角的第个标识，host list

我们就可以得到一堆ip

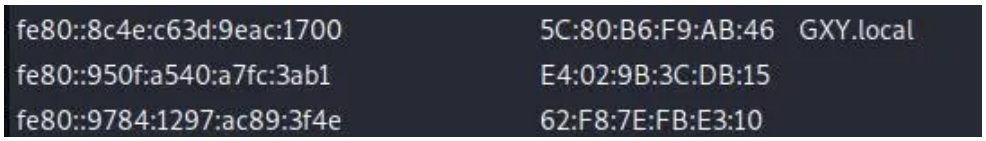


然后，我就翻找了一下那些带description的。 发现了几个熟悉的名字

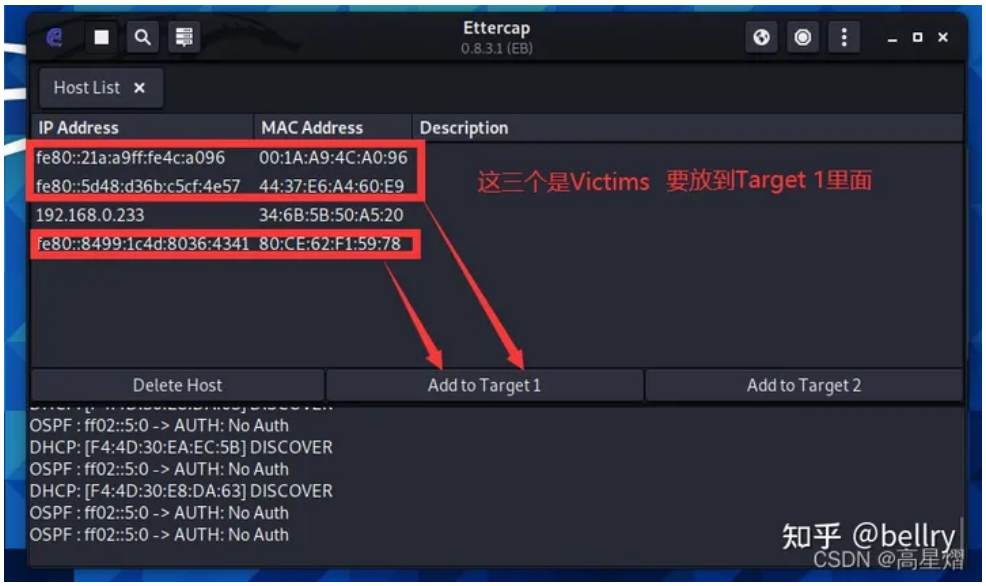




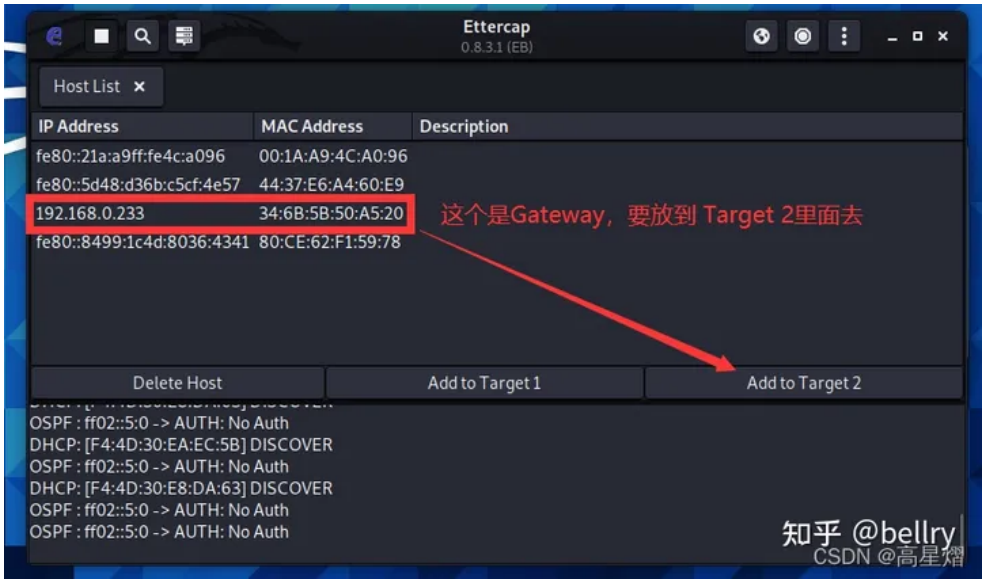
然后，这个是我的物理机



现在，我们要做的就是将划分网关和受害者了。 我们把上面的那些ip选中放到target 1中，再把网关放到target 2中，由于这一步当时没有截图，我就用连接其它网络环境时的操作演示。



然后，在把需要我们伪造的网关放到Target 2 里面去



然后，就可以点击左上角的小地球（MITM），再点击ARP欺骗。

弹出来的这个框，选择嗅探远程连接后点击OK就行了。

这一个可以用来嗅探其他端系统登录本地服务器网站时的操作的ARP欺骗就做好了，但是它并不能实现现有网络的嗅探，这个就要回到最初，选上Bridged Sniffing

然后。。。==就别点小勾了 ==。这个就是在ARP攻击校园网了，这样做挺不好的，而且，校园网应该是有防ARP的机制，攻击也应该攻击不了，只会发出报文占用更多的带宽，到时候就会巨卡无比。 我可以使用其他热点网络进行一下继续的操作。这个ARP是可以欺骗HTTP协议的网站的，HTTPS是有加密的无法窃听。 我先试了一下，arp欺骗校园网的登录界面。就是这个

然后，就可以再输完密码后，被窃听到。

再试试超星学习通

一样的，

不要问我，为什么遮User，因为User是手机号。。。 我们得到的密码是：YWJjZDEyMzQ1Ng==，
这明显是加密过的 而且，一看就知道是==base64 == 解密，得到密码

但是在去试我们学校的统一身份认证的网站时，

就发现这个网站是采用了==非对称的加密技术== **非对称加密技术：**就是有两个密钥，一个公钥一个私钥，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。 由于每次传递的私钥是不一样的，所以每次密文都会改变，我怀疑身份认证就是用了AES加密

可以看到这每次登录密码的密文是不一样的，所以拿不到公私钥，它是不会被破解的。 而且，我感觉他好像感知到了什么东西一样 我一进去就到了这个页面

按道理我是要连接VPN的，正常进去是这个页面

这个网页，安全性挺高，但是不知道为什么校园网登录页面怎么直接密码明文出现，我怀疑可能还是因为校园网有安全机制，没有必要在对登录信息进行加密，即便我们可以用热点网络可以嗅探到自己登录校园网网页的账号和密码。 所以，话说回来这是跟网络环境有关，他想要中间人攻击肯定是要和你在一个网段的，因此陌生不熟悉的WiFi最好别连 。而且，是不是大部分的计科学生都把杀毒软件给删干净了 ，最好还是留一个。

ARP断同学的网

这个其实很简单，一个命令就可以实现，但是你还是要和对方在一个局域网内

```
arpspoof -i eth0(网卡名) -t 受害者的ip 网关
```

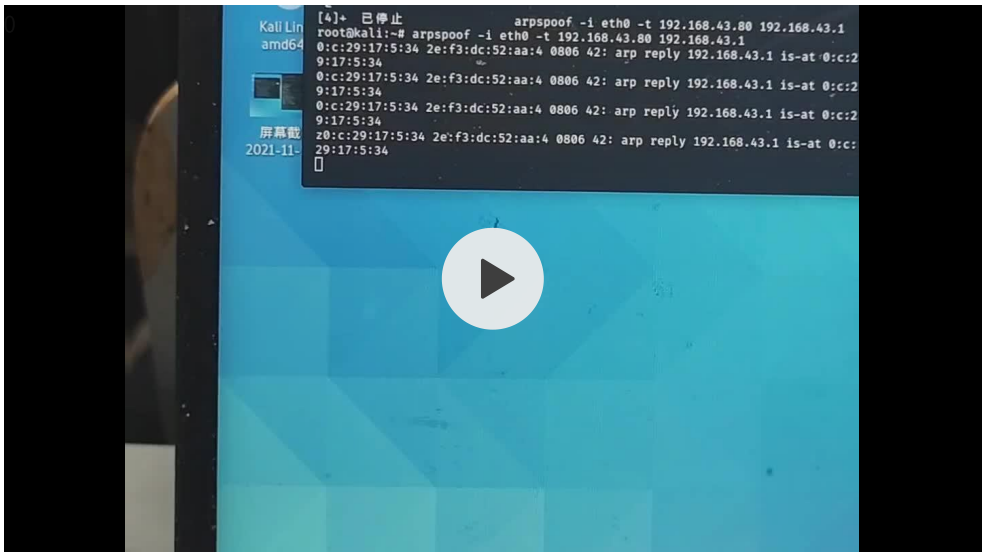
大家是不是觉得有点眼熟 ，对的 上面arp欺骗的时候，命令就是把受害人ip和网关反过来。

```
arpspoof -i eth0(网卡名) -t 网关 受害者的ip
```

直接开始 ，先我断我自己

可以看到

然后，不是在上军理课吗，这两个家伙尽然在下棋。我先偷偷连入他的WiFi 然后



后记

Kali确实好用，爆破密码等等巨爽无比，但是，可不能瞎用啊，Kali从入门到入狱不是没有道理的，最近，真的巨忙无比，上周考了Cornell听力笔记，还考了口语，而且业务需求结课的PBL，明天就要presentation了，系统测试也要presentation了，还有几天还有Research Reprort的presentation。我还想复习计网和数据结构还有6级。人麻了 woc，刚刚找表情包的时候看到了马克思和恩格斯的表情包。。。我马原还没复习啊啊啊

好吧，那个系统测试搞完就把Kali卸了，最近越用越心惊，怕被别人给肉鸡了，毕竟黑暗森林理论，在足够强大前，还是不要暴露自己为好。

编辑于 2022-02-05 00:52

Kali Linux　网络安全　中间人攻击

写下你的评论...

99 条评论　默认　最新

h87d
kali玩得好，牢饭吃到饱
2021-12-04　回复　149

来自灰暗
kali 玩得好，监狱进的早
2021-12-06　回复　12

高星熠 作者
CSDN不让发这篇blog就离大谱
2021-12-04　回复　100

初星梦
怪不得搜不到 原来是被扼杀在摇篮里 还有其他地方可以搜到相关内容吗
2021-12-06　回复　19

命运之轮
应该是太详细了，现在都没用太详细的经验贴，只有原理贴，把相关的攻击目标称为自己搭建的靶机应该就行了。

2021-12-07 回复 18

查看全部 9 条回复 >

谁的影子
看到自强不息知行合一才发现是校友😅
2021-12-06 回复 28

高星熠 作者
😄
2021-12-06 回复 3

icvuln
kali默认安装后账号密码都是kali
2021-12-06 回复 24

高星熠 作者
喔，学到了
2021-12-06 回复 2

高星熠 作者 ▸ **蒸汽动力长颈鹿**
有的
2021-12-09 回复 喜欢

展开其他 1 条回复 >

无所谓
兄弟，你这学得有点杂啊。马原不是大一下学的，数据结构是大二上，计算机网络是大三上，这都是怎么学到一起的？（难得在知乎碰到同校的）
2021-12-06 回复 8

高星熠 作者
现在大二上，我也不太清楚学校的课程安排
2021-12-06 回复 1

去冰三分糖
东秦的呀
2021-12-06 回复 8

去冰三分糖 ▸ **高星熠**
看到工学管就想其他学校也有这个管的？不过我毕业好几年了，校园网什么的都没有用过哈哈哈
2021-12-06 回复 1

高星熠 作者 ▸ **去冰三分糖**
哦，原来是学长啊
2021-12-06 回复 喜欢

展开其他 1 条回复 >

程序员波吉
感谢分享，学习了。请问一下，我公司的网络环境，IT部门统一每台工作电脑都装了Trend Micro的杀毒软件。就是一般用户关不了的那种。这种环境是否可以有机会搞一搞？毕竟每个月总有那么几天不太想干活的
2021-12-04 回复 5

高星熠 作者
Trend Micro是有ARP的防火墙的，建议还是通过和公司协商解决问题
2021-12-04 回复 5

白昼冷光
笑死 我们的产品
09-14 回复 喜欢

展开其他 1 条回复 >

LogyJ
兄弟厉害，同是大二，同是网安，自愧不如👍😜
2021-12-10 回复 6

卡冈图雅 ‣ **柳涟漪**
自己写都是大神喽，能了解那些工具基本原理就不错
2022-10-27 回复 1

柳涟漪
工具大师，还是要自己写才好玩
2022-10-24 回复 喜欢

一阵风
刚开局你就给人切啦😄😄
2022-03-23 回复 5

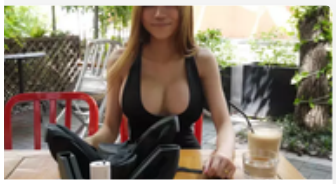
高星熠 作者
😪
2022-03-24 回复 1

Misakanet
问题来了为啥你这么忙还能抽空写长文
2021-12-07 回复 5

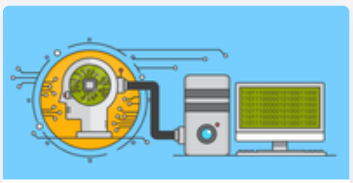
高星熠 作者
这不是肝完一项干点别的等个cd😪
2021-12-08 回复 5

点击查看全部评论 >

推荐阅读



Hacker，没有坚持3个月以上，就没有发言权
怪狗 发表于黑白之道



Hacker News热议：封装包那么多，程序员还用学习算法吗？
机器之心

Hacker技术学的再好，却无法侵入你的心！
怪狗 发表于黑白之道

The Hacker 2.0 | 用策略破译重重难关，化身黑客穿梭未来科…
红菱 发表于TapTa...