最亲近的陌生人

原创先锋情报站 酒仙桥六号部队
2020-09-23原文

这是 **酒仙桥六号部队** 的第 **83** 篇文章。
全文共计2449个字，预计阅读时长9分钟。

1 为什么最亲近?

随着近些年国内网络基础建设的飞速发展，无线WiFi的覆盖面已经很广了。几乎每个人每天都会有所接触，办公也好、下班后刷剧打游戏也好。不知道算不算最亲近？

2 为什么又是陌生人

想一下下面几个场景：

1. 你独自一人出差，住某酒店并且连接酒店WiFi，半夜醒来忽然发现手机在录像！
2. 隔壁没说过话的老王对自己最近追的剧一清二楚！
3. 周末邀请刚认识的妹子到家里用智能电视看剧，屏幕上突然弹出小视频（你懂的那种视频）！　想想吧，惊吓中又带着尴尬。

下面再来看几个场景：

自201x年以来，每年都会有一个特殊的活动。前期准备中，web应用、主机、各种云主机服务器、各种平台等等，漏洞该修的修了，该删的删了，该关的关了。外部可谓铁桶一般，万事大吉。某个夜黑风高的晚上，一个人穿着黑色连帽卫衣，黑色裤子和黑色袜子蹲到你们公司楼下墙角，只见他一言不发的默默打开了kali，电脑的usb口还插着个天线。第二天公司收到通告”已出局“。

这些场景有一个共同点，都跟WiFi有关。平时我们接触到的WiFi，也就是找到WiFi名字，输入对应的密码，连接成功，开始愉快的网上冲浪。也不能拿它怎么着，真的是这样吗？

3 WiFi常见加密方式

WEP

WEP 是针对无线网络而开发的，1999年9月获准成为Wi-Fi安全标准。WEP理论上应当提供与有线网络同等的安全等级，但是其中却存在很多众所周知的问题，而且这些问题同样也易于破解且配置困难。

WPA

在802.11i无线安全标准的开发过程中，WPA被用作WEP的临时安全增强措施。在WEP被正式放弃的前一年，WPA正式被采用。大多数现代WPA应用程序使用预共享密钥（PSK）（通常称为WPA

Personal）和临时密钥完整性协议（TKIP（/ti k p/））进行加密。WPA Enterprise使用身份验证服务器生成密钥和证书。

WPA2

基于802.11i无线安全标准的协议于2004年推出。WPA2相对于WPA最重要的改进是使用高级加密标准（AES）。

详见：https://www.netspotapp.com/cn/wifi-encryption-and-security.html

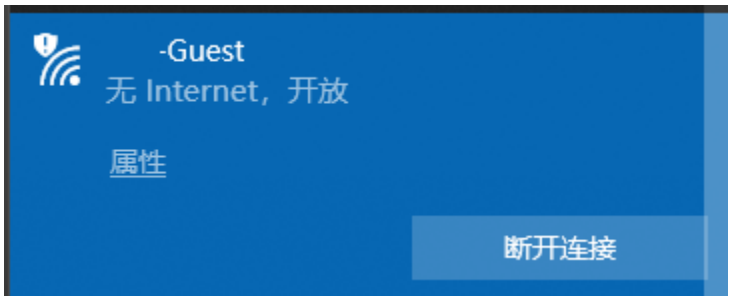
4 如何攻破WiFi

我们平时接触到的WiFi大致分为三种：

第一种 WiFi连接无验证

常见于咖啡馆、酒店等场景，WiFi为公开WiFi，连接WiFi无需密码，但是连接之后会弹出一个网页来输入账号密码认证。

直接连接WiFi。



连接WiFi后，弹出如下认证页面。

正常情况下，酒店会直接把账号密码写在房卡上面。这种情况下酒店里的人都在同一网段，可以互相访问，很不安全。

还有就是在逛街的时候，也会碰到无验证的WiFi，并且连接WiFi后没有跳转认证，直接就可以联网，这种情况很有可能就是就是钓鱼WiFi。连接这个WiFi过程中的操作，比如：转账、购物等都会被攻击者截获，从而造成财产损失。具体攻击原理参考下文“数据截获”。

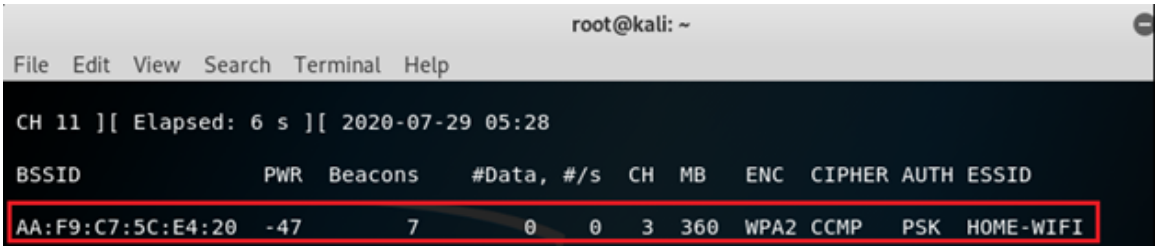
第二种WiFi连接单密码验证

常见于在家，公司等场景，找到WiFi名字，输入正确密码，便可以正常使用。

WiFi界面

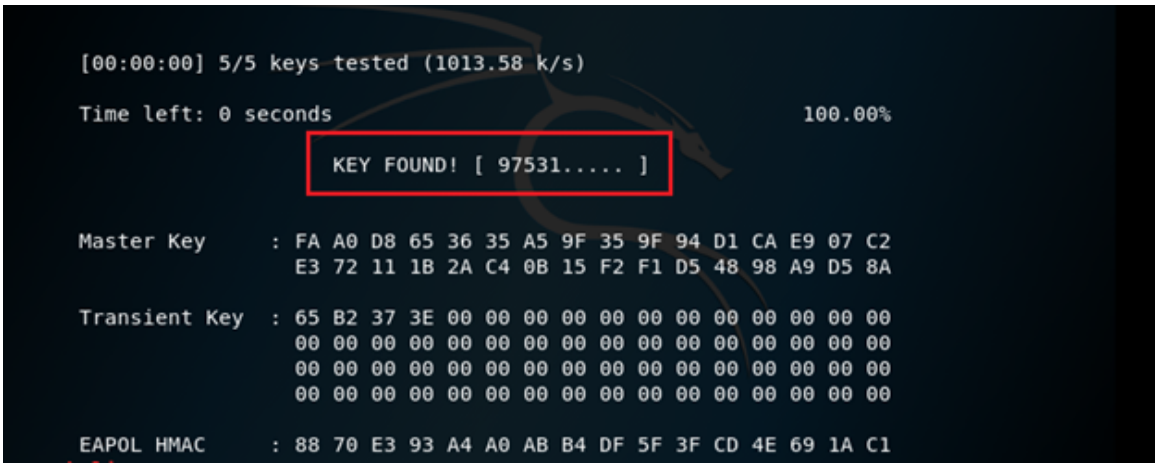
利用工具aircrack-ng抓WiFi握手包，然后通过遍历字典的方式,爆破wifi连接密码。

先搜索WiFi；



抓取握手包（含有密钥的数据包）；

破解（爆破）。



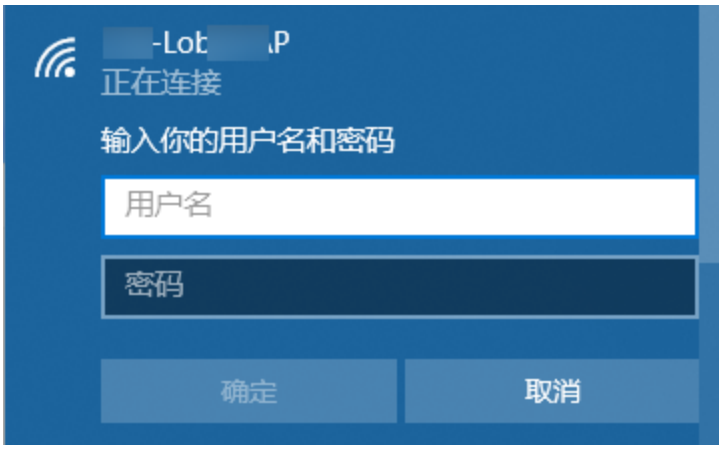
WiFi：HOME-WIFI

KEY ：97531.....

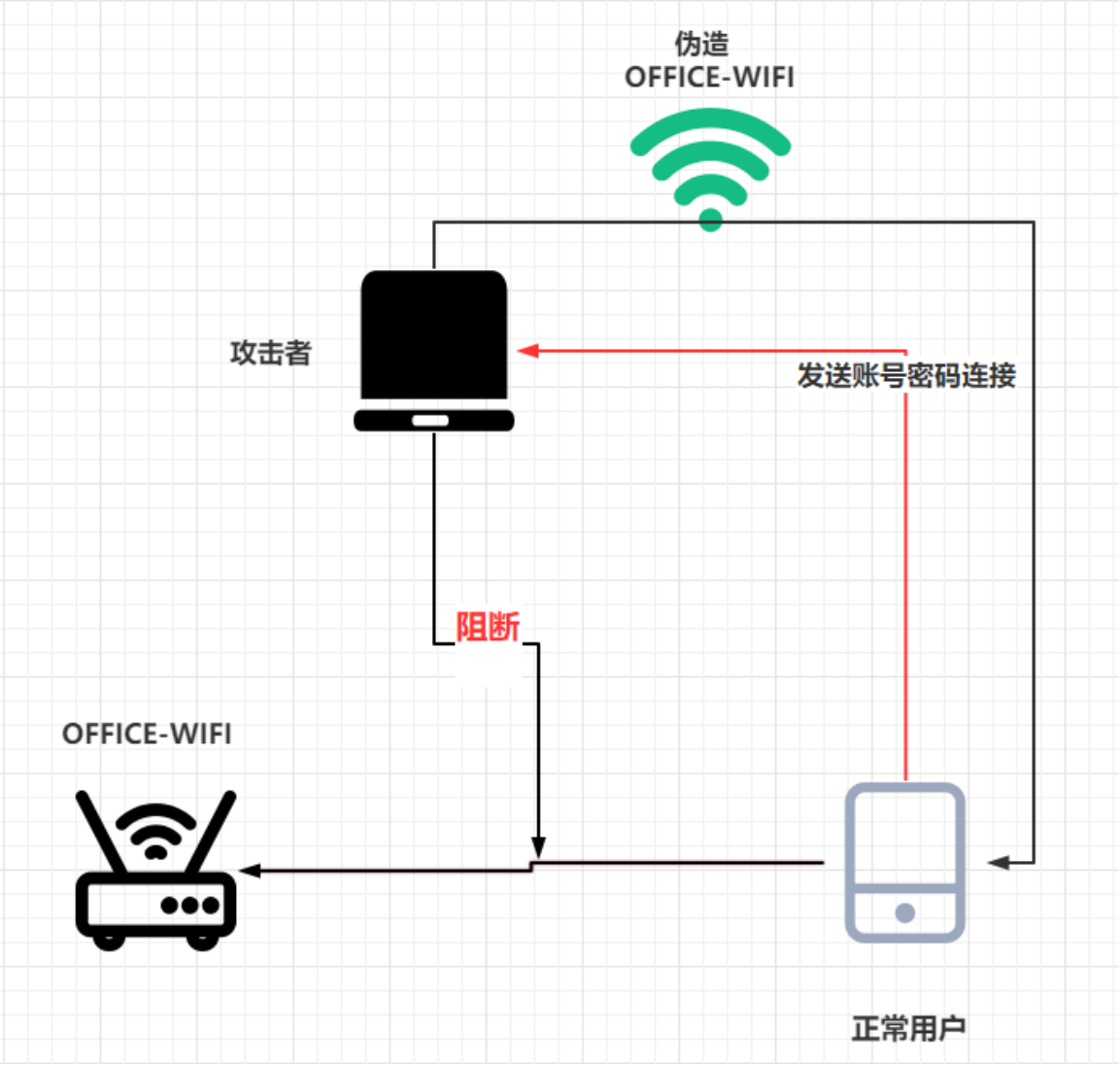
第三种WiFi连接账号密码验证

常见于企业级的WiFi，连接时，先找到WiFi名，然后输入账号，密码才能连接WiFi，然后正常使用，这种WiFi往往是可以直接访问公司内网的。

WiFi登陆窗口是这样的。



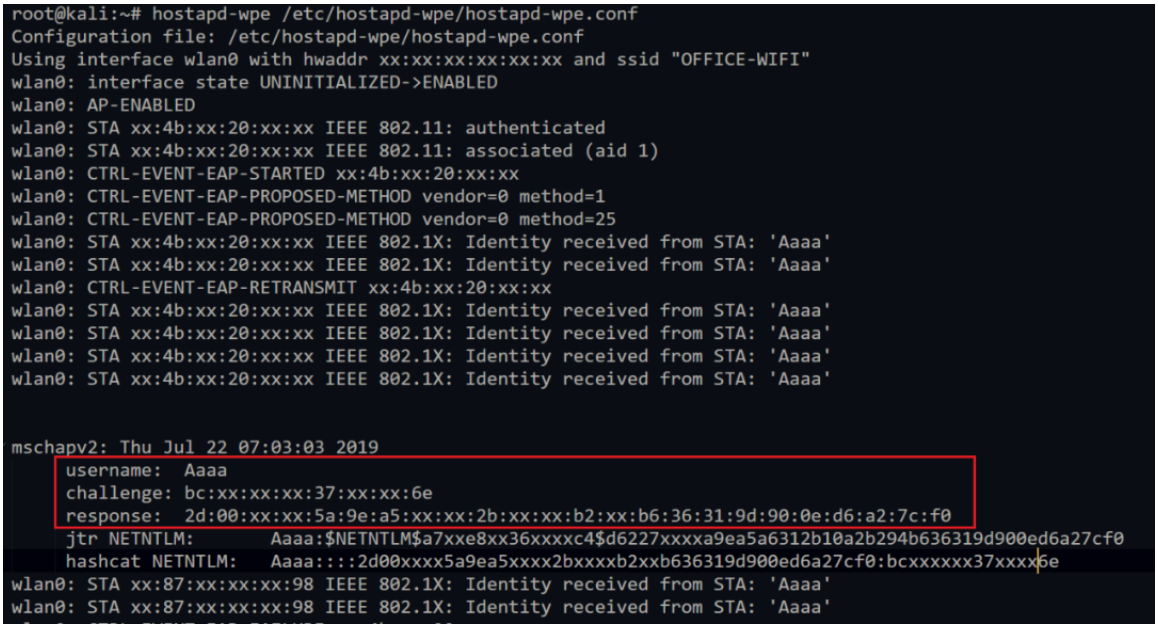
使用hostapd-wpe工具伪造一个同名的WiFi，然后劫持正常用户跟真WiFi之间的流量。比如下图：



工具下载后，只配置WiFi名就可以了。

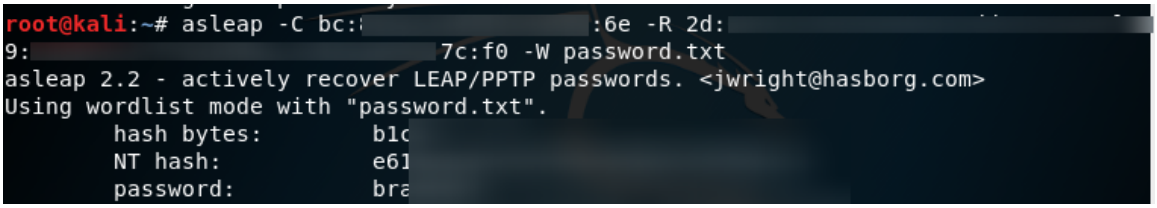
```
sudo vim /etc/hostapd-wpe/hostapd-wpe.conf
```

启动工具hostapd-wpe就可以抓取新连接WiFi的用户名密码了。



抓到了用户名和NTLM加密的密码，然后利用工具asleap破解密码就可以了。

```
asleap -C <challenge> -R <response> -W 字典
```



aername：Aaaa

passowrd：braxxxx

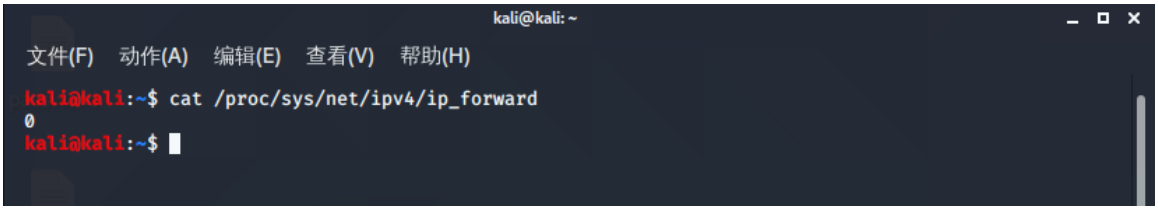
现在账号、密码都有了，就可以直接登陆了。

5 攻破之后

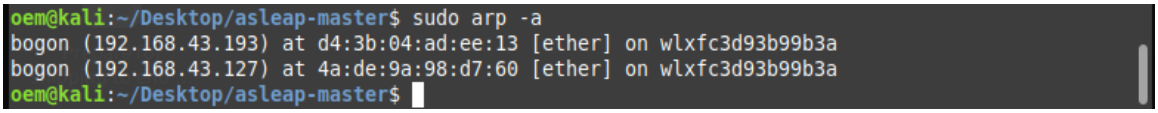
下面均为隔壁老王所为，我只是帮忙做记录。

A. 断网

可造成被攻击者网络中断，需要在同一网段内。命令：`arpspoof -i 网卡 -t 目标ip 目标网关` `cat /proc/sys/net/ipv4/ip_forward` 输出为“0”时，为阻断状态。



获取目标IP的方法：`工具扫描`、`Ping`、`arp -a`等，最好使用工具扫描，这样可以获得更多信息，进一步确定目标。`apr -a`

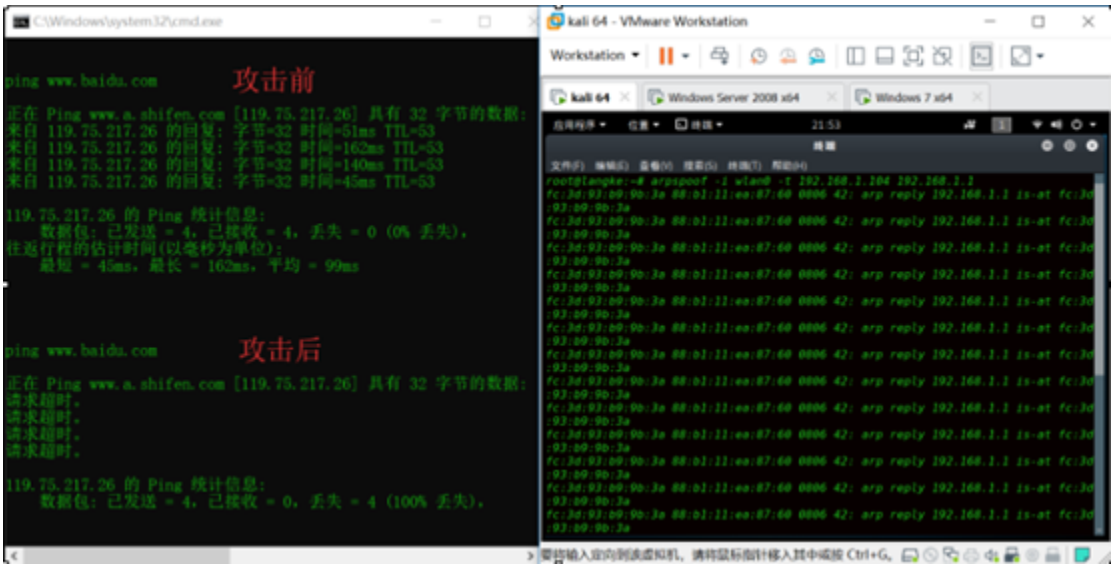


工具扫描

```
File  Edit  View  Search  Terminal  Help
Nmap scan report for bogon (192.168.43.193)
Host is up (0.020s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
1080/tcp open  socks
MAC Address: D4:3B:04:AD:EE:13 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 close
d port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (87%), FreeBSD 6.X|10.X (8
6%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), Microsoft Windows XP
SP2 (87%), FreeBSD 6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for bogon (192.168.43.90)
Host is up (0.000030s latency).
All 1000 scanned ports on bogon (192.168.43.90) are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 close
d port
Device type: phone|general purpose|webcam|storage-misc
Running: Google Android 2.X, Linux 2.6.X, AXIS embedded, ZyXEL embedded
OS CPE: cpe:/o:google:android:2.2 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.6.1
7 cpe:/h:axis:210a_network_camera cpe:/h:axis:211_network_camera cpe:/h:zyxel:nsa-210
OS details: Android 2.2 (Linux 2.6), Linux 2.6.14 - 2.6.34, Linux 2.6.17, Linux 2.6.17 (Mandriv
a), Linux 2.6.32, AXIS 210A or 211 Network Camera (Linux 2.6.17), ZyXEL NSA-210 NAS device
```

下面演示断网，宿主机IP：192.168.1.104。

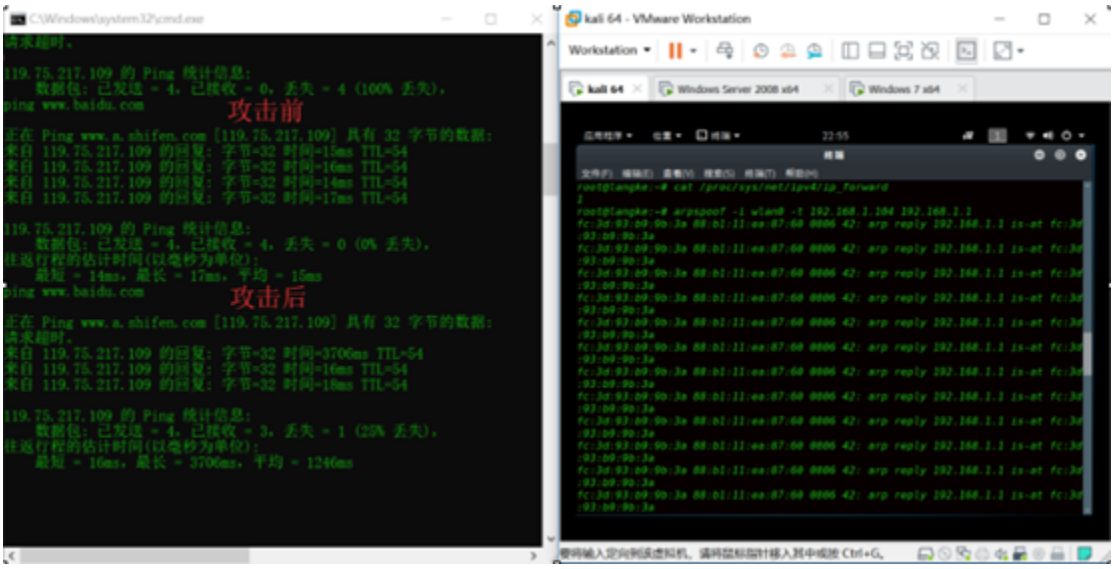


B. 欺骗

ARP欺骗的运作原理是由攻击者发送假的ARP数据包到网络上，尤其是送到网关上。其目的是要让送至特定的IP地址的流量被错误送到攻击者所取代的地方。因此攻击者可将这些流量另行转送到真正的

网关（被动式数据包嗅探，passive sniffing）或是篡改后再转送（中间人攻击，man-in-the-middle attack）。

攻击者亦可将ARP数据包导到不存在的MAC地址以达到阻断服务攻击的效果，`cat /proc/sys/net/ipv4/ip_forward` 输出为“1”时，把传送到攻击者的流量转送到网关。

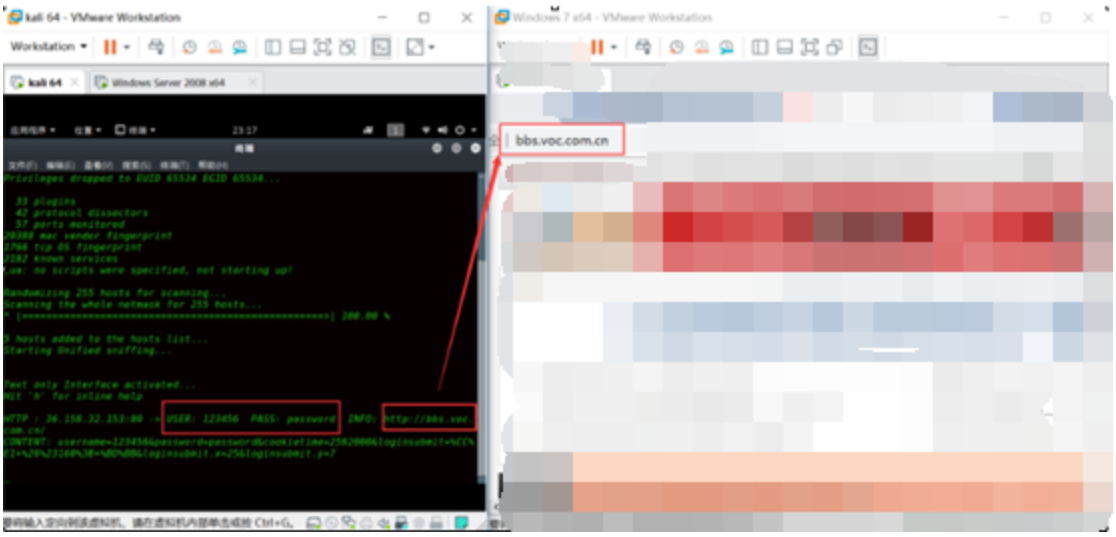


C. 数据截获

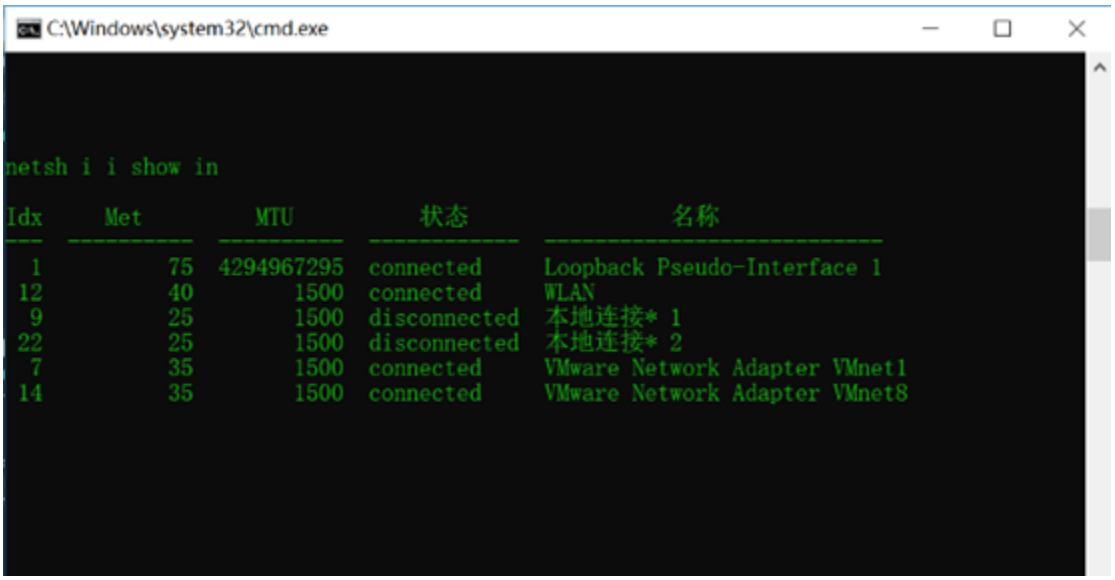
传输报文的截取

利用自带的工具演示

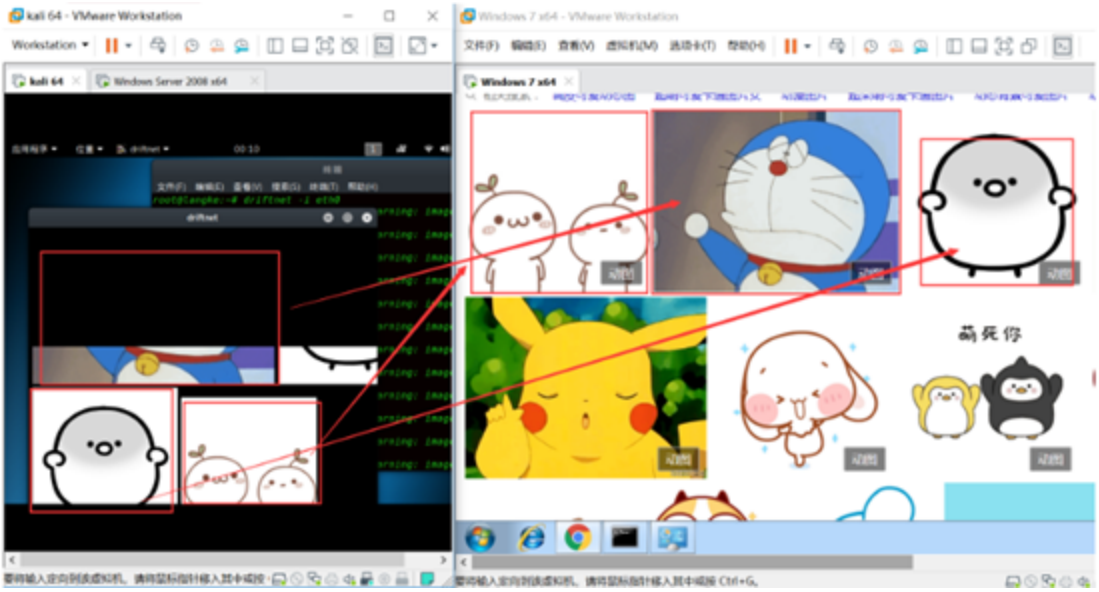
命令：`ettercap -Tq -i 网卡`



如果网卡比较多，可以用命令查看网卡`Idx`号命令：`netsh i i show in`



图片截取 命令：`driftnet -i 网卡`



6 反击

虽然某科等网络设备生产商也有相应的防护设备，之前有所接触。但是这些设备并不是那么好用，从检测到攻击到压制再到显示出攻击，中间相隔5分钟之久。

这么说，护网期间，企业遇到WiFi钓鱼攻击的情况下，只能坐以待毙了吗？

NO！

首先，利用钓鱼WiFi检测工具实时监测，以便发现钓鱼WiFi。由于WiFi钓鱼攻击属于物理攻击，攻击者需要在企业附近才能实施攻击，所以可以利用WiFi信号探测工具找到攻击者物理位置。如下图，右侧数值越大，信号越强。通过在公司附近不断移动，再依靠信号值，确定攻击者大概位置。然后找目标位置附近具有如下特点的人：

- 一个人拿着电脑独自站在风中。
- 或者拿着树莓派一类的设备，在附近一呆就是很长时间

◆ 或者手机上边带着类似路由器上的天线。

拍照留作证据。 最后形成溯源报告，还可以为防守方加分。


List
2.4 Ghz
5 Ghz
channel filter
order: 质量
CM
MAC: 54:b :4b
Freq.: 2437 (ch: 6) (w: 20Mhz)
WPA2 RSN ESS WPS
-40 dBm
骑着
MAC: ea: :20
Freq.: 2447 (ch: 8) (w: 20Mhz)
WPA2 RSN ESS
-46 dBm
ak
MAC: da: :33
Freq.: 2422 (ch: 3) (w: 20Mhz)
WPA2 RSN ESS
-46 dBm
vivo x50 pro
MAC: 8a: :2a
Freq.: 2437 (ch: 6) (w: 20Mhz)
WPA2 RSN ESS
-51 dBm
HUAWEI Mate 20 Pro
MAC: f4: :ec
Freq.: 2412 (ch: 1) (w: 20Mhz)
HUAWEI TECHNOLOGIES CO.,LTD
WPA2 RSN ESS
-54 dBm
696
MAC: a8: :34
Freq.: 2437 (ch: 6) (w: 20Mhz)
HUAWEI TECHNOLOGIES CO.,LTD
WPA2 RSN ESS
-63 dBm

7 总结

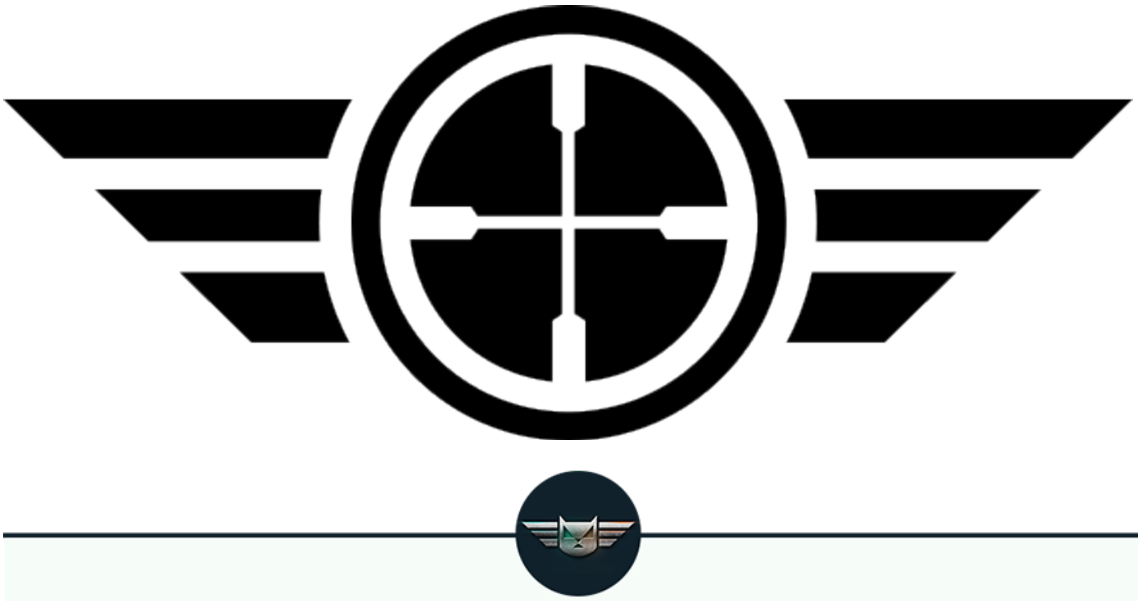
这些针对WiFi的攻击，我们防不胜防。

对于个人建议：

1. 外出时尽量保持手机WiFi功能关闭。
2. 尽量不使用陌生WiFi网购，在公共WiFi下最好不要登陆网银或支付。拒绝来源不明的WiFi。
3. 家用WiFi尽量设置复杂的密码，包含大小写字母、数字、特殊字符等多种字符，长度20位左右。虽然20位的密码有点长，毕竟WiFi密码一般只输入一次，就可以用到下次修改密码，也不会很麻烦。
4. 使用360手机卫士对WiFi进行安全检测。

对于企业建议：

1. 提升密码复杂度，参考上条。
2. 企业会有一些网络设备，可以绑定MAC地址、设置IP白名单、设置联网时间段等等。
   虽然说增加密码复杂度依然无法防止破解，但是可以增加破解的成本。



精选留言

用户设置不下载评论