05 WIFI安全实验报告模板

《信息安全综合实践》实验报告

Wifi安全实验

一、实验目的

1. 掌握无线AP的设置；
2. 认识无线WPA/WPA2安全原理，熟悉无线WPA破解方法；
3. 了解无线Dos攻击的原理、流程及防范方法。

二、实验内容

序	内容	实验结果
1)	无线AP配置	- [ ] 失败 - [√] 成功
2)	破解准备（无线网卡、口令字典）	- [ ] 失败 - [√] 成功
3)	aircrack-ng口令破解	- [ ] 失败 - [√] 成功
4)	wifite口令破解	- [ ] 失败 - [√] 成功
5)	无线DOS攻击（选做）	- [ ] 未做 - [√] 失败 - [] 成功

注：未能使得WIFI或者手机热点断网，但是使得网络访问速度明显下降

三、分析和思考（90分）

1. **使用Crunch可以基于用户指定的特殊规范而生成一个密码字典，以配合其他工具使用进行暴力破解。学习并尝试使用crunch命令生成下列类型的密码字典，给出相应命令，并给出相应的结果截图（可为部分截图）。(20分)**
    1. **生成由1896、0408、YSSY、sjtu这4个词组合而成的密码**

       命令： `crunch 4 16 -p 1896 0408 YSSY sjtu`

```
File  Actions  Edit  View  Help
└─$ crunch 4 16 -p 1896 0408 YSSY sjtu
Crunch will now generate approximately the following amount of data: 408 byte
s
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 24
04081896YSSYsjtu
04081896sjtuYSSY
0408YSSY1896sjtu
0408YSSYsjtu1896
0408sjtu1896YSSY
0408sjtuYSSY1896
18960408YSSYsjtu
18960408sjtuYSSY
1896YSSY0408sjtu
1896YSSYsjtu0408
1896sjtu0408YSSY
1896sjtuYSSY0408
YSSY04081896sjtu
YSSY0408sjtu1896
YSSY18960408sjtu
YSSY1896sjtu0408
YSSYsjtu04081896
YSSYsjtu18960408
sjtu04081896YSSY
```

2. **5位密码，格式为3个字母+2个数字，并要求每个密码中的字母不得完全相同**

   命令：`crunch 5 5 -d 2@ -t @@@%% -d 1@ -o pass-2.txt`

```
┌──(kali㉿kali)-[~]
└─$ crunch 5 5 -d 2@ -t @@@%% -d 1@ -o pass-2.txt
Crunch will now generate the following amount of data: 9750000 bytes
9 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1625000

crunch: 100% completed generating output
```

```
zyw29
zyw30
zyw31
zyw32
zyw33
zyw34
zyw35
zyw36
zyw37
zyw38
zyw39
zyw40
zyw41
zyw42
zyw43
zyw44
```

2. **简要总结描述实验中手工无线口令破解的步骤，并说明下列命令的含义和其中关键字段的意义（30分）。**

```
$ sudo aireplay-ng -3 -b <ap mac> -h <my mac> wlan0mon
$ sudo aireplay-ng -0 10 -a <ap mac> wlan0mon
```

- 无线口令破解的步骤：
  - step1：配置无线网卡至监听模式：`sudo airmon-ng start wlan0`
  - step2：查看USB无线网卡MAC：`ip addr show`，本实验中网卡 MAC为：`00:e0:4c:81:a3:b5`
  - step3：启动监听, 查看确定目标 AP 的相关信息：`sudo airodump-ng wlan0`，本实验中AP MAC为：`D8:15:0D:A4:E8:78`，信道为6
  - step4：截获握手包：`sudo airodump-ng -w ~/bags.cap -c 6 --bssid D8:15:0D:A4:E8:78 wlan0`
  - step5：获取握手包并破解密码：`sudo aircrack-ng -w ~/small.txt ~/bags.cap`
- 第一条用于在无线网络上执行去认证攻击。
  - "sudo" 用于以管理员权限运行命令。
  - "aireplay-ng" 是用于数据包注入和其他无线攻击的工具名称。
  - "-3" 是指定去认证攻击模式的选项。
  - "-b <ap mac>" 是指定目标接入点（AP）的 MAC 地址的选项。
  - "-h <my mac>" 是指定攻击设备的 MAC 地址的选项。
  - "wlan0mon" 是正在用于攻击的无线网络接口的名称。
- 第二条用于在无线网络上执行去认证攻击。
  - "sudo" 用于以管理员权限运行命令。
  - "aireplay-ng" 是用于数据包注入和其他无线攻击的工具名称。
  - "-0" 是指定去认证攻击模式的选项。
  - "10" 是指定发送的去认证数据包的数量。
  - "-a <ap mac>" 是指定目标接入点（AP）的 MAC 地址的选项。
  - "wlan0mon" 是正在用于攻击的无线网络接口的名称。

3. **有人认为隐藏无线AP的SSID可以让无线AP不易被发现和破解。其实利用airodump-ng命令可以简单地发现隐藏的无线AP，其它破解步骤与公开SSID的情况相同。请写出发现隐藏的无线AP命令，并说明提升无线AP安全的主要保护措施。（20分）**

- `sudo airodump-ng wlan0` :发现隐藏的无线AP
- `sudo airodump-ng --bssid D8:15:0D:A4:E8:78 wlan0`：对隐藏的AP进行扫描，其中`D8:15:0D:A4:E8:78`为此次试验的ap mac
- 主要保护措施：
  - 隐藏无线SSID，关闭SSID广播：隐藏无线AP的SSID，关闭无线网络的SSID广播，这样其他人就无法轻易看到网络名称，降低被发现和被攻击的概率。
  - 使用强密码：将Wi-Fi网络的密码设置为复杂的、随机的、尽可能少使用重复元素字符的密码，并定期更换密码。同时使用WPA2加密。

- MAC地址过滤：通过配置无线接入点，只允许特定的MAC地址访问网络进行访问控制。这样，即使攻击者知道了无线AP口令，也无法访问目标网络

4. **无线DOS攻击一般有哪些攻击方式，利用的是无线网络的何种特性/安全弱点，可以采取哪些防御措施？（20分）**

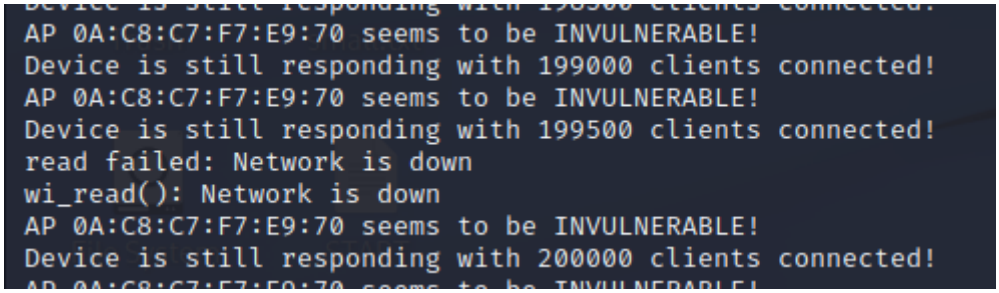
- Authentication DOS：
  - 验证洪水攻击，国际上称之为Authentication Flood Attack，全称即身份验证洪水攻击， 通常被简称为Auth D.O.S攻击，是无线网络拒绝服务攻击的一种形式。该攻击目标主要针对那些处于通过验证、和AP建立关联的关联客户端，攻击者将向AP发送大量伪造的身份验证请求帧（伪造的身份验证服务和状态代码），当收到大量伪造的身份验证请求超过所能承受的能力时，AP将断开其他无线服务连接。
  - 安全弱点：
    - 简单密码：用户可能使用简单密码或者是弱密码进行认证，这使得攻击者可以通过暴力破解或者字典攻击等方式轻松地获得正确的密码。
    - 日志记录不足：日志记录不足使得攻击者可以通过多次无效的认证尝试而不被系统检测到，从而导致攻击者可以继续攻击。
    - 系统安全漏洞：利用目标系统的认证机制的安全漏洞进行攻击，以导致系统无法正常工作或服务不可用。
  - 防御措施：
    - 强化密码策略:：要求用户使用强密码，并通过强密码策略要求用户在密码方面采取必要的安全措施，如密码长度、复杂性和周期性更改等
    - 增强日志记录和防止暴力破解：及时记录和监控所有的认证尝试，实时检测异常活动并及时发现和应对潜在的攻击，同时限制失败登录尝试次数，并通过增加验证机制如验证码或者多因素认证等方式增强认证安全性。
    - 更新系统软件：及时更新操作系统、应用程序和认证系统软件以修补已知的漏洞和提高系统的安全性。
- Beacon Flood：
  - 安全弱点：
    - 无限制信标帧的接受：某些网络设备可能没有限制信标帧的接收，这使得攻击者可以发送大量的伪造信标帧以引起网络拥塞。
    - 信道资源有限：无线网络中的信道是有限的，攻击者可以通过向网络中发送大量的无用数据包来占用信道，从而使得网络中的通信变得异常缓慢或完全中断。
    - 广播信号：无线网络中的数据包是通过广播信号进行传输的，这使得攻击者可以通过发送虚假的数据包来干扰网络中的通信和连接。
  - 防御措施：
    - 限制信标帧的接收：可以通过设置设备的过滤器和访问控制列表来限制接收的信标帧数量，这有助于防止Beacon Flood攻击。
    - 启用流量管理：在网络设备上启用流量管理器，以防止过量的信标帧和其他类型的流量进入网络。

        - 信道管理：无线网络中的信道数量是有限的，可以采取信道管理的措施来降低DoS攻击的影响。例如，可以启用动态信道选择（Dynamic Channel Selection）功能，当检测到信道拥塞时自动更换使用信道。
- Deauthentication Attack：
    - 攻击者通过向目标设备发送伪造的断开连接请求，强制目标设备断开与AP的连接，从而使其无法正常工作。
    - 安全弱点：
        - 广播信号：无线网络中的数据包是通过广播信号进行传输的，这使得攻击者可以通过发送虚假的数据包来干扰网络中的通信和连接。
    - 防御措施：
        - 使用WPA2加密，启用802.1x认证，使用频率跳跃技术可以避免暴力攻击。
        - 信道管理：无线网络中的信道数量是有限的，可以采取信道管理的措施来降低DoS攻击的影响。例如，可以启用动态信道选择（Dynamic Channel Selection）功能，当检测到信道拥塞时自动更换使用信道。
- Spoofing Attack：
    - 欺骗攻击指攻击者假装是合法用户或服务来进行网络访问或数据传输活动。
    - 安全弱点：
        - MAC地址欺骗：无线网络中的MAC地址可以被攻击者轻松地伪造，从而使得攻击者可以冒充合法设备进行攻击。
        - 认证和加密弱点：无线网络中的认证和加密机制存在一些漏洞和弱点，使得攻击者可以伪造认证请求或绕过加密措施，从而获得网络中的访问权限并进行攻击。
        - 无限制信标帧的接受：某些网络设备可能没有限制信标帧的接收，这使得攻击者可以发送大量的伪造信标帧以引起网络拥塞。
    - 防御措施：
        - 强化密码策略:：要求用户使用强密码，并通过强密码策略要求用户在密码方面采取必要的安全措施，如密码长度、复杂性和周期性更改等
        - 限制信标帧的接收：可以通过设置设备的过滤器和访问控制列表来限制接收的信标帧数量，这有助于防止Beacon Flood攻击。
        - 信道管理：无线网络中的信道数量是有限的，可以采取信道管理的措施来降低DoS攻击的影响。例如，可以启用动态信道选择（Dynamic Channel Selection）功能，当检测到信道拥塞时自动更换使用信道。
- 泛用的防御方式是定期更新固件和安全软件，限制无线网络范围，限制无线网络访问和授权，使用强密码和加密技术等。

四、实验总结（收获和心得）（5分）

这次是首次团队合作做实验，和同学朋友们一起做实验氛围很不错。这次实验中我们成功破解了口令，这让我们团队十分有成就感。我们也尝试对手机热点和WIFI进行dos攻击，但是二者似乎都经受住了百万甚至千万级别的clients连接请求而没有断联，但是也成功使得网络访问速度下降，还是有一定成效的。

五、尚存问题或疑问、建议（5分）



- 不知道中间的消息“read failed: Network is down /n wi read(): Network is down”是否是dos攻击成功的意思，感觉效果不是很好，但是网速确实下降了很多。