中山大學 SUN YAT-SEN UNIVERSITY 移动网络安全技术实验报告

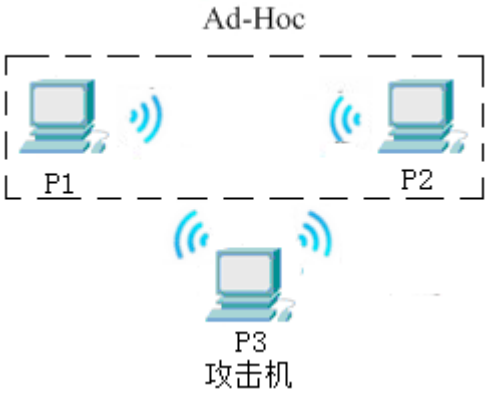
警示

1. 实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2. 当次小组成员成绩只计学号、姓名登录在下表中的。
3. 在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4. 实验报告文件以 PDF 格式提交。

院系	数据科学与计算机实验	班 级	14M3，14C1	组长	白冰
学号	14353355	14353002			
学生	杨金华	白冰			
实验分工					
杨金华	进行攻击实验，共同编写实验报告		白冰	下载软件，配置无限网络，共同编写实验报告	

无线网络攻击分析实验

【实验拓扑】



【实验内容】

在实验拓扑中，P1、P2 组成点对点 Ad-Hoc 网络，它们有相同的安全密钥、SSID、通道号，P3 是一台攻击机。

实验开始时，P3 对整个 WIFI 网络进行攻击。由于此时 P3 不在网络中且不知道 WIFI 的密码，因此需要通过程序对 WIFI 密码进行破解。WIFI 密码破解方法是借助一份可能是密码的密码表，通过程序的无限次的逐个尝试登陆，最终来进行密码破解。例如需要将已经认为可能是密码的字段加入到等待尝试的文本中，然后逐个进行尝试，比如在文本中加入“12345678”，如果和 WIFI 密码匹配，则可以登录 WIFI，若不匹配则进行下一次尝试。

进行 WIFI 破解的时候通常可是通过直接写程序或者在网上寻找相关破解软件，类似软件比如“WIFI 爆破”，这类软件就是通过枚举法尝试来达到破解 WIFI 的目的。

破解 WIFI 后，P3 便可侵入 Ad-Hoc 网络 WIFI，此后 P3 就可以通过 Omnipeek 等抓包软件对 WIFI 中的广播进行捕获，通过捕获广播，P3 可以知道整个网络中都有哪些设备在运行中，在 P3 定位到每一个 IP 地址所对应的设备后，就可以有针对性性的进行网络破坏。例如进行 ARP 攻击，使 P1 或 P2 脱离网络。

【实验要求】

请根据攻击过程，详细分析回答下列问题（指出结论是由那些攻击引起的，要有相应的验证测试截图）。

（1）攻击机使用了什么 WiFi 密码破解工具？简述此工具的功能和破解过程。请注意破解难度、破解时间等因素。

我们小组使用了很多所谓的破解工具进行破解，比如说 WLAN 无线 SDK(WIFI 破解)、wifi 暴力破解器电脑版等，但这些软件要么收费，要么不能正常工作，更离谱的是很多直接下载不了，全是广告。不过这类软件的原理还是比较简单的，要么是靠用户共享密码，要么是通过枚举进行破解，再者就是通过已有数据库（里面存有可能的密码）进行破解。这类软件进行破解的时间很不稳定，如果密码简单，则很快能破解，复杂一点的话，花费时间久指数上升了。

（2）破解后攻击机是否能连入 WiFi 网络？请给出测试截图。

PC1 和 PC2 截图：

攻击机截图：

显然，攻击机已经连入 wifi。

（3）攻击机使用什么抓包工具捕获 P1、P2 的通信包？简述此工具的功能和捕获包的过程。

抓包工具为 Omnipeek。

此工具的功能有以下：

基于信息包流的专家分析系统和应用分析、交互式节点图 · 完整的七层协议解码、应用响应、(ART) 分析、安全功能、监控与报表、RMON 分布式分析

捕获包的过程：

PC1 和 PC2 互 ping，启动 omnipeek 进行抓包，分析数据包。

以下为抓包截图：

1	169.254.254.2	169.254.255.255	96	51.739791	NB Name Svc	C QUERY NAME=WWW.GOOGLE.COM <00> ...
2	169.254.254.2	169.254.255.255	96	52.489598	NB Name Svc	C QUERY NAME=WWW.GOOGLE.COM <00> ...
3	169.254.254.2	169.254.255.255	96	53.239650	NB Name Svc	C QUERY NAME=WWW.GOOGLE.COM <00> ...
4	169.254.254.2	169.254.255.255	96	0:01:59.532085	NB Name Svc	C QUERY NAME=WWW.BAIDU.COM <00> W...
5	169.254.254.2	169.254.255.255	96	0:02:00.281098	NB Name Svc	C QUERY NAME=WWW.BAIDU.COM <00> W...
6	169.254.254.2	169.254.255.255	96	0:02:01.031136	NB Name Svc	C QUERY NAME=WWW.BAIDU.COM <00> W...
7	169.254.229.8	169.254.255.255	96	0:02:32.056510	NB Name Svc	C QUERY NAME=169 <00> Workstation
8	fe80::edb4:5180:...	LLMNR	88	0:02:55.918113	LLMNR	Src=54631,Dst= 5355 ,L= 22
9	169.254.112.101	LLMNR	68	0:02:55.918282	LLMNR	Src=51251,Dst= 5355 ,L= 22
10	169.254.112.101	169.254.255.255	96	0:02:56.118374	NB Name Svc	C QUERY NAME=WPAD <00> Workstation
11	169.254.112.101	169.254.255.255	96	0:02:56.874078	NB Name Svc	C QUERY NAME=WPAD <00> Workstation
12	169.254.112.101	169.254.255.255	96	0:02:57.630057	NB Name Svc	C QUERY NAME=WPAD <00> Workstation
13	0.0.0.0	IP Broadcast	346	0:03:21.022541	DHCP	C DISCOVER

（4）攻击机如何将 P1 或 P2 脱离 WiFi？写出实现过程。

先删除 ARP 表里的项目，即用命令行执行 arp -d。由于之前在测试过程中，PC 之间进行了互 ping，使得 APR 缓存表已经有列表项。

PC1 在网络上发送广播，攻击机接收到广播后制造假的应答，伪造 IP 地址与 Mac 地址的映射，使得 PC2 的 IP 地址未能映射到 PC2 的 Mac 地址。

PC2 则无法与 PC1 进行通信。

（5）如何防止这样的攻击？（需具体写出措施、理由）

1、强大的密码是 Wi-Fi 安全最重要的基石，可以通过设置强密码（密码长度长、组合复杂）保证 wifi 环境安全。

2、只要对 Wi-Fi 采用 WPA/WPA2 加密，并且设置强密码，就几乎不可能被攻破。

3、隐藏 SSID。隐藏 SSID 就是指在路由器管理界面进行相关的设置，使得无线网络的 SSID 不再广播出来，成为一个“隐形网络”，这样同样可以大大降低被黑客攻击的概率。

4、MAC 绑定。MAC 绑定是指在路由器中进行相关的设置，开启 MAC 地址黑名单或白名单功能。

5、关闭无线路由器的 QSS、WDS 功能。QSS/WDS 功能会大大降低无线路由器的安全性，因此如非必须，应将这两个功能关闭。