**Lab 3\_2: An advanced WEP key cracking approach: active injection**

201311211918 汪大洋

其他组员：杜蓉、任梅、汪大洋

**一、实验介绍**

The purpose of this lab is to continue exploring the vulnerabilities of the WEP protocol. It is well known that the WEP protocol is crippled with numerous security flaws. Most of these weaknesses are described in Weaknesses in the Key Scheduling Algorithm of RC4 by Scott Fluhrer, Itsik Mantin and Adi Shamir. In our previous lab, we crack the WEP key by passively collecting data frames. Yet, it is unlikely that there always exist a large amount of data traffic. Therefore, we need to use more efficient techniques to crack a WEP key. In this lab, we will practice these advanced techniques. The detailed steps are as follows:

这个实验的目的是继续探索WEP协议的漏洞。众所周知,WEP协议被许多安全漏洞削弱。在Scott Fluhrer、Itsik Mantin和Adi Shamir的Weaknesses in the Key Scheduling Algorithm of RC4中有这些弱点中的大多数的描写。在我们之前的实验中,我们通过被动搜集数据包来破解WEP密钥。然而，一直存在大量的数据流量是不可能的。因此,我们需要使用更高效的技术来破解WEP密钥。在这个实验中,我们将尝试使用这些更高一级的技术。详细的步骤如下:

Section 1: Information Gathering 第一部分：信息搜集

Section 2: Test the Injection Functionality 第二部分：注入测试

Section 3: Start Airodump-ng to Capture Data 第三部分：抓IVs

Section 4: Fake Authentication and Association 第四部分：伪造身份认证并连接

Section 5: Traffic Generation via ARP Replay 第五部分：通过ARP产生通信信息

Section 6: Key Cracking 第六部分：破解密钥

Section 7: Network Reconnaissance 第七部分：网络侦测

Section 8: Discussion Questions 第八部分：问题讨论

Section 9: General Questions 第九部分：常规问题

Reference: <http://www.aircrack-ng.org/doku.php?id=simple_wep_crack>

**二、实验过程**

**Section 1: Information Gathering 第一部分：搜集信息**

这一步和之前的实验一样，搜集所需信息并记录。

1、打开终端，输入chkconfig NetworkManager off 和 service NetworkManager stop来关闭网络服务。

2、输入airmon-ng start wlp0s20u3，开启监听模式。

3、输入iwconfig，看到当前网卡名称是wlp0s20u3mon，输入airodump-ng wlp0s20u3mon，可以看到很多无线的信息，找到CIST2015\_2，在频道1。

记录信息如下：

For the AP named CIST2015\_2

Channel: 1

BSSID: 04:A1:51:B2:17:FF

For an associated client of this AP

MAC: 6C:B0:CE:20:FA:16



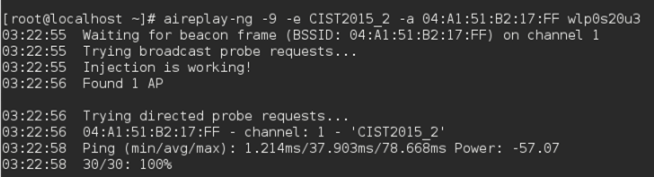
**Section 2: Test the Injection Functionality 第二部分：注入功能测试**

这一步的目的是确认自己的网卡在AP的距离范围内，并且可以向AP注入包。

输入aireplay-ng -9 -e CIST2015\_2 -a 04:A1:51:B2:17:FF wlp0s20u3mon

//9是注入测试

在老师发出信息后，可以看到正确的信息。



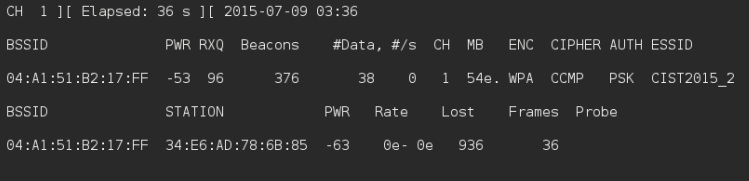
**Section 3: Start Airodump-ng to Capture Data 第三部分：抓IV数据**

这一步是通过Airodump-ng命令来抓IVs。

重新打开一个终端，输入airodump-ng -c 1 --bssid 04:A1:51:B2:17:FF wlp0s20u3mon

//1是指频道1

可以看到如下内容：



**Section 4: Fake Authentication and Association**

**第四部分：伪造身份认证并连接**

在这一步中，为了和AP连接，我们要使用aireplay-ng命令来伪造身份认证。

打开新的终端，输入

aireplay-ng -1 0 -e CIST2015\_2 -a 04:A1:51:B2:17:FF –h 6C:B0:CE:20:FA:16 wlp0s20u3mon

//-1是指伪造身份认证

可以看到屏幕上有正确的信息。

**Section 5: Traffic Generation via ARP Replay**

**第五部分：通过ARP来产生通信信息**

这一步的目的是通过aireplay-ng在监听模式下搜集ARP信息并将它们注回网络中。

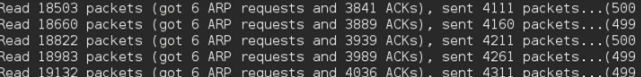
打开新的终端，输入

aireplay-ng -3 -b 04:A1:51:B2:17:FF –h 6C:B0:CE:20:FA:16 wlp0s20u3mon

//3指ARP

可以看到屏幕上有正确的信息。

**5.1.1 Provide a screenshot of an ongoing successful ARP injection/replay.**



**5.1.2 What will happen if there are no ARP packets sent over the air?**

答：会一直收不到ARP信息

**5.1.3 If the instructor did not create the ARP traffic for you, what will do to create the ARP traffic? Remember, you are not joined the network yet.**

答：伪装成AP向client发送断开连接的信息，这样client会重新连接AP，从而得到ARP traffic。

**Section 6: Key Cracking 第六部分：破解密钥**

这一步使用和上一个实验中相同的办法来破解密钥。

打开三个新的终端，分别输入三个不同的命令在抓IVs的同时破解密钥。

aircrack-ng -z -b 04:A1:51:B2:17:FF collection\*.cap

//this is PTW

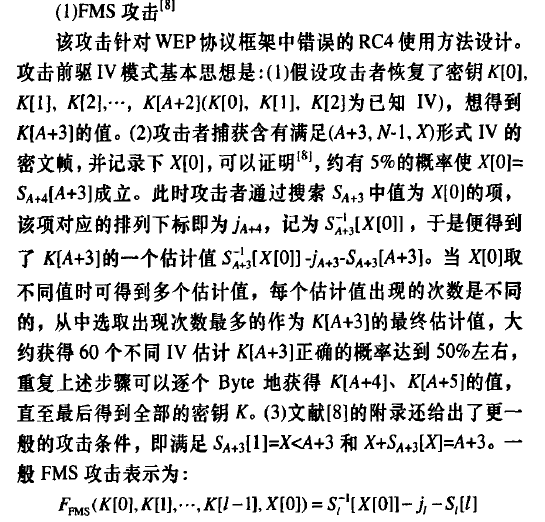
aircrack-ng –K -b 04:A1:51:B2:17:FF collection\*.cap

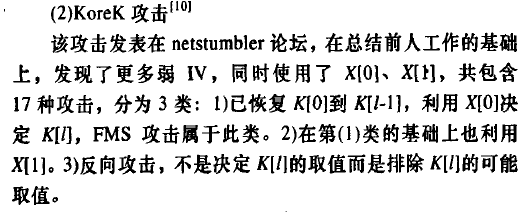
//this is FMS/Korek

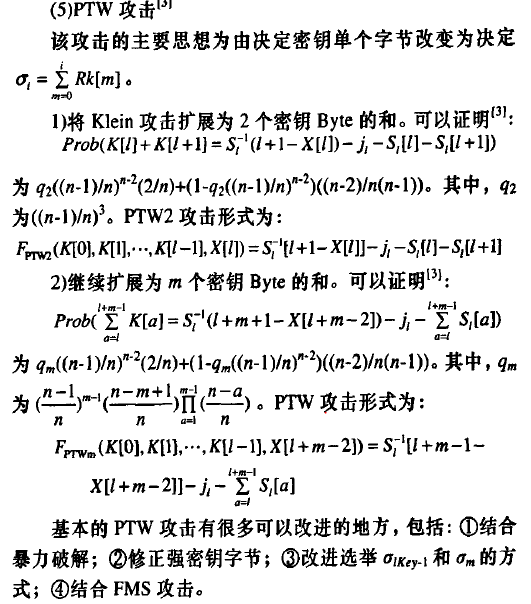
aircrack-ng –b 04:A1:51:B2:17:FF collection\*.cap

一段时间后，发现这次是第一个命令最先破解到密钥。

**6.1.1 Explain the following attacking techniques: FMS/Korek and PTW.**



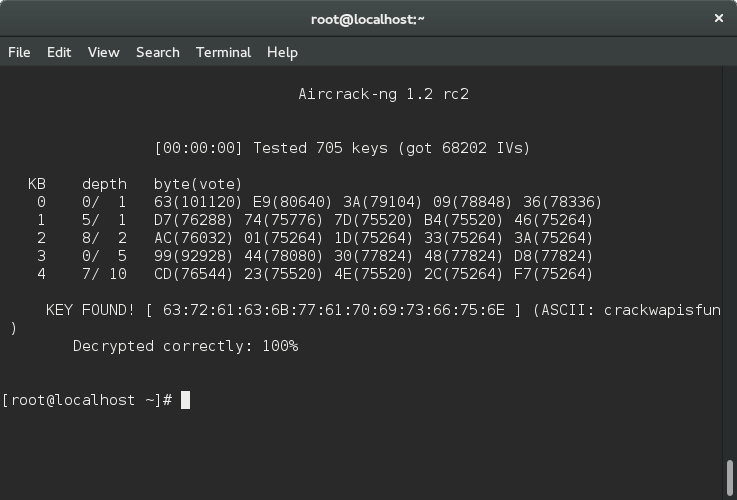




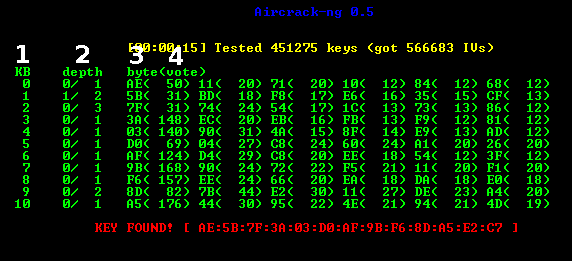
（参考文献：WEP协议攻击方法研究——刘永磊、金志刚）

**6.1.2 What is the WEP key (in ASCII format)? Provide a screenshot of the recovered key.**

答：密钥是crackwapisfun



**6.1.3 Explain the meaning of the Depth Field and Fudge Factor.**



The best explanation is an example. We will look at a specific byte. All bytes are processed in the same manner.

最好的解释是举个例子来说明。我们可以分析具体的一位数据，所有位的过程都是一样的。

You have the votes like in the screen shot above. For the first byte they look like: AE(50) 11(20) 71(20) 10(12) 84(12)

现在有如上截图的各数据出现次数分布情况。第一位的内容是：AE(50) 11(20) 71(20) 10(12) 84(12)

The AE, 11, 71, 10 and 84 are the possible secret key for key byte 0. The numbers in parentheses are the votes each possible secret key has accumulated so far.

AE、11、71、10和84都是第0位密钥可能出现的值。括号中的数据是到目前为止每位所得到的票数（即出现次数）。

Now if you decide to use a fudge factor of 3. Aircrack-ng takes the vote from the most possible byte AE(50):50 / 3 = 16.666666

如果你现在决定使用猜测因子3，aircrack-ng就会选出最可能的那个数据AE(50)的票数进行运算：:50 / 3 = 16.666666

Aircrack-ng will test (brute force) all possible keys with a vote greater than 16.6666, resulting inAE, 11, 71 being tested, so we have a total depth of three: 0 / 3 AE(50) 11(20) 71(20) 10(12) 84(12)

Aircrack-ng将测试（使用brute force算法）所有的备选密钥的票数是否大于16.6666，结果是AE、11、71将要被测试，因此我们得到总测试深度（测试次数）为3，（第一行信息为：）0/3、AE(50) 11(20) 71(20) 10(12) 84(12)。

When aircrack-ng is testing keys with AE, it shows 0 / 3, if it has all keys tested with that byte, it switches to the next one (11 in this case) and displays: 1 / 3 11(20) 71(20) 10(12) 84(12)

当aircrack-ng测试AE时，会显示深度是0/3，如果这一个数据的所有密钥都被测试完（仍然没有破解密码），就选择下一个（在这个例子里是11）来测试，并显示：1 / 3 11(20) 71(20) 10(12) 84(12)

**6.1.4 What is the default fudge factor in aircrack-ng?**

答：是2。

**6.1.5 Which method gives a better performance (i.e., quicker to recover the WEP key)? Why?**

答：PTW方法更快，因为这个算法更适合weak的IVs。

**Section 7: Network Reconnaissance**

因为时间原因，这一部分没有做。

**Section 8: Discussion Questions**

**8.1.1 What is the most significant advantage of this WEP key crack approach?**

答：不需要client频繁制造traffic信息。

**8.1.2 What is the basic requirement for this WEP key crack approach?**

答：需要client发送包至少一次。

**8.1.3 What is the biggest problem of this key crack approach?**

答：容易受到干扰。

**8.1.4 How would you to prevent this type attack on WEP key cracking?**

答：使用动态密码。

**8.1.5 Once the WEP key is discovered by adversaries, what can you do to protect a Wi-Fi network?**

*It is dangerous that someone can easily gain access to you wireless work because your security defense parameter can then be easily circumvented.*

答：改变密码，使用MAC白名单方式。

**8.1.6 Assume that a MAC filter is enabled on the AP of this wireless network. In addition, there is no traffic in the network. What will you do differently to crack the WEP key?**

答：等合法用户发出信息，搜集合法用户的信息，把自己的MAC伪装成合法用户。

**Section 9: General Questions**

**9.1.1 How long did it take you to complete this lab?**

答：大约两个小时。

**9.1.2 Was the lab challenging enough?**

答： 有一定难度。

**9.1.3 Are there any corrections needed to apply to this lab？**

答：无。

**三、遇到的问题**

1、在输入aircrack-ng命令时，时常因为‘-’这个符号出错。

2、一开始始终无法抓到IVs，后来换了无线网卡成功了。

**四、实验体会**

1、不同的算法适用于不同情况的密钥破解，找对方法可以很快得到密钥；

2、WEP加密方式很不安全，在平时看到的wifi中，大多都是WPA2或802.1x加密方式，没有见到过WEP加密。

**五、参考资料**

1、<http://www.aircrack-ng.org/doku.php?id=aircrack-ng#explanation_of_the_depth_field_and_fudge_factor>

2、AIrcrack中文手册（百度文库）

3、WEP协议攻击方法研究 <http://www.docin.com/p-380196788.html>