Cracking WEP and WPA wireless networks and How to Better Secure Wireless Networks



Overview

- How to crack WEP and WPA
- Tactics to better secure your network
- Use this for educational and informational purposes only

WEP cracking

- WEP is outdated and week
- Novice hackers will hack WEP very easily
- WEP uses a 3-byte vector (IV) Initialization Vector – IV is placed in packets – based on pre-shared key
- Capturing thousands of these packets from the client or AP you will have enough data gathered to crack WEP

Tools

- AirCrack,
  - Aircrack contains several tools
    - Tools will be using
      - Airodump – capturing IVs
      - Aircrack – cracking IVs
- Kismet
  - For sniffing and locating networks

Getting Started

- The device (laptop) wireless card must be put into “monitor mode” aka. (promiscuous mode)
  - allows wireless card to locate and crack wlan network
  - putting wireless card in this mode is not very easy. Web browsing will not be possible.
  - Rollback wireless card drivers to undo monitor mode.

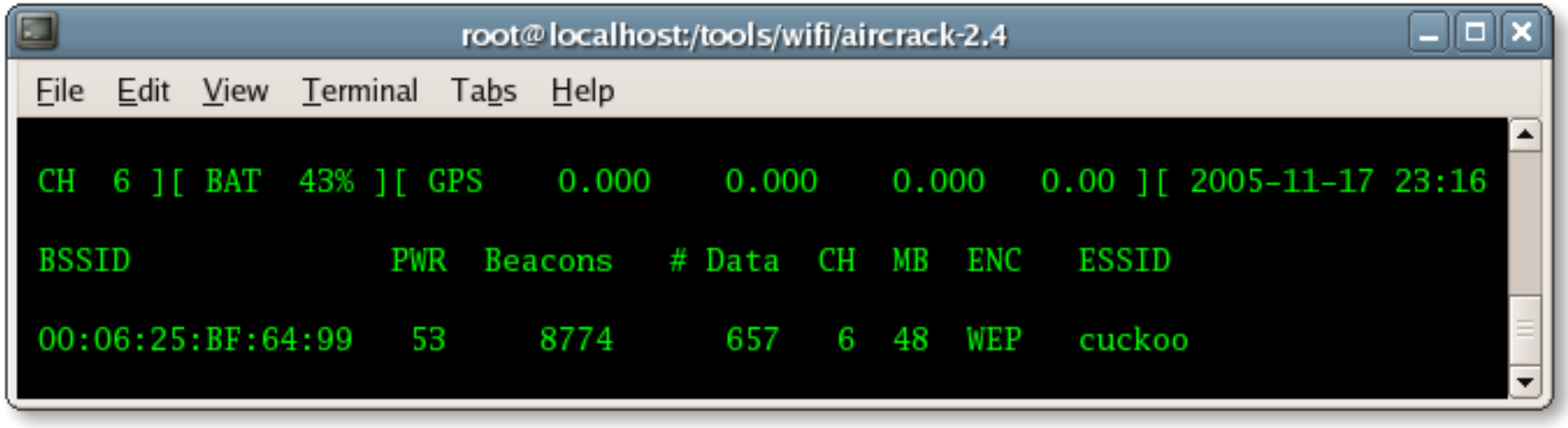
Getting Started – cont.

- Run kismet or airodump and locate nearby networks
- The info we need:
  - Encryption type
  - Channel no.
  - IP address
  - BSSID
- Ie. Let’s use a channel 6 – and BSSID (MAC) 00:23:1F:55:04:BC

Capturing

- Capturing IVs
  - Use airodump – type command: /airodump <interface> <output prefix> [channel] [IVs flag]
- Example
  - /airodump cardname **test** 6 1
    - "**test**" is the filename with our captured IVs
    - "1" is always used for IVs flag when cracking WEP
    - Note: (the more the merrier) meaning: we will need over 100,000 IVs to crack the WEP key

Airodump or Kismet output

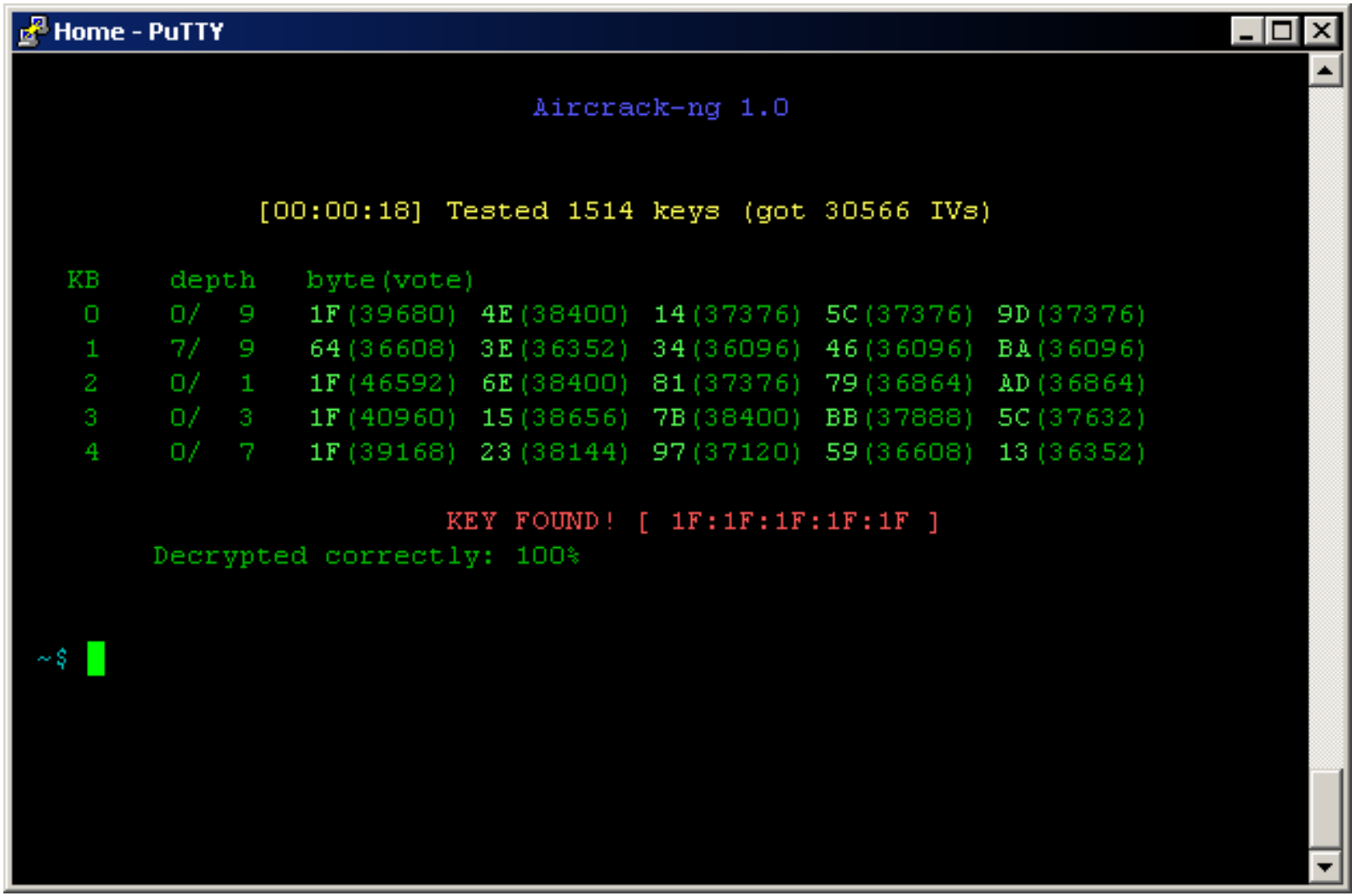


1. BSSID = MAC
2. CH = Channel Number
3. # Data = Number of IVs captured so far

Cracking

- Cracking IVs
  - Using aircrack command: /aircrack [option] <input file>
    - The options are
      - -a 1 for WEP
      - -b for BSSID
      - (the input file is the file we generated using airdump command earlier) : Ie. /aircrack –a 1 –b 00:23:1F:55:04:BC test.ivs

Screenshot from aircrack



- Info from airodump is fed into aircrack the program will return the WEP key used on that network. Program gave out over 30566 IVs in 18 seconds. Could do 3000000 in less than 3 min.

WEP finale

- The time needed for cracking the WEP key is determined by the number of the IVs collected.
- Any number of IVs over 100000 is reasonable and should yield the WEP key within minutes.

Intro to cracking WPA

- WPA keys are much harder than WEP to crack
- WPA cracking nearly impossible
- WPA fills out holes that WEP can’t

Getting started

- WPA passwords are real words
  - dictionary word list

Capturing

- Run kismet to gather network info required
- Open airodump, enter command: /airodump cardname test 2
  - Cardname is the name of the wireless card
  - Test is the name of the output file
  - 2 is the channel we retrieved using Kismet

Cracking

- Open aircrack and type: /aircrack –a 2 –b 00:25:1G:45:02:ad –w/path/to/wordlist
  - to crack WPA use –a 2
  - -b is the MAC (BSSID)
  - -w is path on your computer to the dictionary word list

- If the command yields the WPA passkey you are one lucky hacker. Else you are out of luck..

Conclusion

- WEP is easier to crack than WPA
- AirCrack is one tool used to crack WEP

Reasons you should secure your network

- Your resources are exposed to unknown users
- Your network can be captured, examined
- Your network and connectivity may be used for illegal activities

Countermeasures

- Use these tips to prevent unwanted users
  - Change default setting on your router
    - When you install router modify id and pwd to something else rather than default
  - Disable SSID broadcast
    - Hides network from beginner intruder. Ie. Windows Wireless Zero config utility
    - Will not keep you safe from more advance hackers
  - Turn off network when not in use
    - Impossible to hack a network that it is not running
  - MAC address filtering
    - AP grants access to certain MAC addresses
    - Not fully proof, but good countermeasure
  - Encryption
    - Use of WPA
    - Use long and random WPA keys