WIFI HACKING

Objectives

- ✓ Wifi Basics
- ✓ WPA 2 wifi cracking
- ✓ Popular tools to hack and crack wifi passwords
- ✓ Hacking Wifi on Windows

HOW WIFI WORKS

The way Wi-Fi works is through the use of radio signals like in phones (GSM)

The **wireless adapter card** that is found inside of computers and smartphones converts the data that is to be sent to a **radio signal** and then transmits it by the **antenna**

A router then receives these signals and decodes them in order to send the information contained within to the Internet via a **Local Area Network or a wired Ethernet connection** like a cable network connection

WIFI SECURITY

- ✓ **WEP (Wired Equivalent Privacy) - Not used anymore**
- ✓ **WPA/WP2 - 99%**
- ✓ **WPA3 - Newest standard**

IMPORTANT TERMINOLOGY

- AP – Access Point (The wifi router)

- MAC – Media Access Control

A unique id assigned to wireless adapters and routers

(48 Bit)

- BSSID – Access Point's MAC Address
- ESSID - Access Point’s Broadcast name. (ie linksys, default, belkin etc)

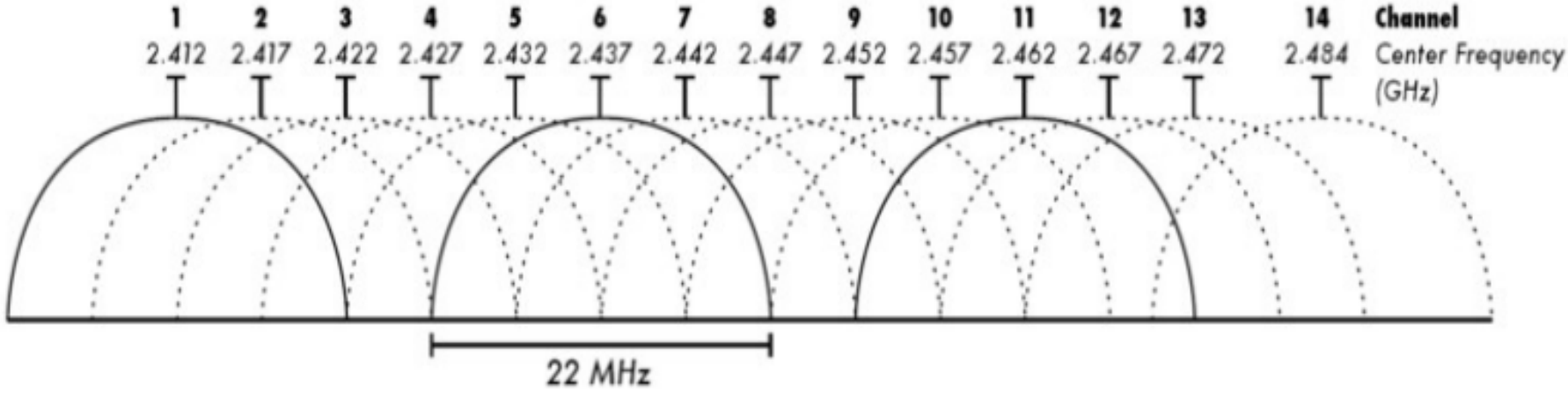
Some Aps will not broadcast their name, But wireless hacking tools can guess it.

```
CH -1 ][ Elapsed: 24 s ][ 2013-03-03 12:58

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

00:26:5A:F5:DA:B8  -38      194        0    0   3  54e. WPA2 CCMP   PSK  America
00:1B:9E:A7:D6:FA  -58        3        0    0   6  54e  WPA  TKIP   PSK  Bezeq
80:1F:02:4F:5F:78  -80        3        0    0  11  54e  WPA2 CCMP   PSK  temo
CC:B2:55:E7:F8:F7  -80        2        0    0   6  54e  OPN              Bezeq Free E7F8F3
98:FC:11:82:A8:41  -81       51        8    0   1  54e  WPA2 CCMP   PSK  Cisco04119
00:12:2A:33:88:CC  -83        2        0    0  11  54e. WPA2 CCMP   PSK  Avi
00:1F:1F:AE:D1:24  -83        3        0    0   6  54e  WEP  WEP         oskatz
30:46:9A:24:38:5A  -83       28        0    0   6  54e. WEP  WEP         Eli
C0:AC:54:F5:DD:D8  -86        2        0    0   9  54e  OPN              hatihon
```

WIFI CHANNELS

- The physical frequency of the wireless transmissions

- Channels are between 1-14 in 2.4 GHz range (1-11 in the USA)
- Some APs also use 5 GHz band



Monitor Mode and Packet Injection

- By default wireless cards listen only to traffic addressed to them. Enabling monitor mode enables the adapter to listen to all traffic in the area. Whereas packet injection help to inject packet into AP for advanced attacks

Not all wireless cards support these features and you need a wireless card supporting these features

The wireless card I am using TL-WN722N

Most people like to use Kali in a VM environment. So, you must have an external USB wireless card

BASIC Password cracking techniques

Brute Force

Dictionary

WHY DICTIONARY

A researcher from the security firm CyberArk has managed to crack 70% of Tel Aviv's Wifi Networks starting from a sample of 5,000 gathered WiFi

- The expert gathered 5,000 WiFi network hashes by strolling the streets in Tel Aviv with simple WiFi sniffing equipment composed of an AWUS036ACH ALFA Network card
- He cracked 1,359 passwords using Rockyou dictionary (which we will be using mostly)
- And another 2000 by masking attack with combination of dictionary

THANKS