Short notes on **WIFI Hacking**

Source: Wi-Fi hacking for beginners

Author: James Wells

Notes taken by: Mohd Mehdi (Khan)

Points:

1. **Become untrace-able**.
    a. Use *macchanger* to change MAC address of your network interface.
        i. MAC address is the unique identifier for every computer.
        ii. We will not change MAC address on hardware level. We will change it, when MAC address is loaded in the RAM. So, the change will be temporary. Once you power-off or reboot your computer, new MAC address will be replaced by original MAC address.
2. **Change wireless mode.**
    a. Use following commands to enable Monitor mode.

```
iwconfig wlan0 down
iwconfig wlan0 mode monitor
iwconfig wlan0 up
```

    ***wlan0 –** replace with your wireless interface.
        i. Generally, we can capture those packets, on the network, that was intentionally sent to us.
        ii. There are two modes in wireless networks: Managed and Monitor.
        iii. Using Monitor mode, we can capture all packets even if, those packets are not sent to our computer.
3. Catch handshake.
    a. Handshake packets are packets sent every time when a device connects to Access Point (AP).
    b. Handshake packets **contains hashed passwords**.
        There are two STEPS to catch handshake:
        i. Start airodump-ng to an AP.
        airodump-ng –channel channel –bssid bssid –write filename <interface>
        ii. Wait a client to connect the AP or de-authenticate a connected client so that their system will connect automatically.
        Airodump-ng –deauth <# of packets> -a <AP> -c <target> <interface>
4. Cracking wireless network.

a. Use aircrack-ng.
   [aircrack-ng handshake-file -w wordlist <interface>]
   i. It uses *pdkdf2* algorithm to combine each password in the wordlist with Access Point (ESSID) to compute a PMK (Primary Master Key).

5. Secure yourself from WI-FI hacking.
   a. Use WPA with complex password having uppercase, lowercase, special characters and alphanumeric form.
   b. Ensure that WPS feature is disabled.
