- Filename: eccouncil-ceh31250-v11-16-4-1-wireless-hacking-countermeasures.md
- Show Name: CEHv11 (312-50)
- Topic Name: Wireless Network Hacking - Hacking Wireless Networks
- Episode Name: Wireless Hacking Countermeasures
==

Wireless Hacking Countermeasures

Objectives:

- Wireless Security Controls

    - Patches/Updates

        - Clients
        - Firmware for APs

    - Change AP defaults

        - Opt into the security features of your AP

            - APs are insecure by default so that you can access it out of the box

                - The assumption is that you will enable the security features

                    - Security features need to be unique to your environment

    - Strong PSK passwords/phrases

        - No dictionary words here
        - Sufficient length and complexity
        - Passwords are like underwear

            - They will eventually stink, so change often!

    - Use the strongest encryption possible

        - No less than WPA2

            - Enterprise is best

    - SSID Obfuscation

        - To broadcast or not to broadcast? That is the question!

            - aka SSID Cloaking

        - Change the default SSID

            - Can be too descriptive (make, model, etc)

    - Disable remote login!

    - Add extra layers of protection

        - NAC/NAP

            - https://www.packetfence.org/

        - VPN
        - Network segmentation

            - Firewall/IDS/IPS

                - https://www.cisco.com/c/en/us/products/wireless/adaptive-wireless-ips-software/index.html

- Forbid public wifi use!

- Physical security of devices

- Scheduled audits

  - Wifi surveys

    - Compare results to baselines
    - Update baselines whenever approved changes are made
    - Heat maps

      - Control AP placement and/or signal strength to keep signal from bleeding signal into untrusted areas

        - Parking lots
        - Adjacent buildings

  - Packet Capture and Analysis