- Filename: eccouncil-ceh31250-v12-18-3-1-iot-attacks-tools-and-countermeasures.md
- Show Name: CEHv12 (312-50)
- Topic Name: Mobile Platform, IoT, and OT Hacking - IoT and OT Hacking
- Episode Name: IoT Attacks, Tools, and Countermeasures
  ==========

IoT Attacks, Tools, and Countermeasures

Objectives:

- Standard-issue threats
    - SQLi
    - Ransomware
    - DoS
    - MitM
    - RCE
- Tools
    - Shodan
    - Censys
    - Thingful
    - Wireshark
    - TCPDump
    - Attack Proxy
    - SDR tools (Parrot)
- DEMO hacking the Foscam
    - NTP Server Command Injection
        - `;/usr/sbin/telnetd -p37 -l /bin/sh;`
- Interesting IoT Attacks
    - HVAC
        - Shodan search for Metasys
    - Rolling Code Attack
        - Automobile hacking
            - Key fob for door locks
                - Uses rolling code (code can't be used twice in a row)
                - Attacker blocks/sniffs the unlock signal
                - Repeat the process
                - Attacker then sends first code to car
                - Car unlocks
                - Attacker then uses 2nd code to unlock car later
                  - Blueborne
                  + Bluetooth vuln
                  - Allows for complete takeover of a device
                  - DoS by Jamming Attack
                  - Sybil Attack
                  + VANET(Vehicular Ad-Hoc Network)
                  - Used to send traffic updates and safety messages between vehicles
                  + Sybil disrupts this by simulating traffic congestion
- Countermeasures
    - The Standards
        - Change Defaults
        - Updates and Patches

        - Encryption
        - Disable unnecessary services
        - Physical Security
        - Logging and Monitoring
        - Lockouts
    - SDR Security
        - Don't use 'Rolling Code'
        - Utilize preamble and synchronization nibbles
        - Use encryption
    - Manufacturer Security
        - Secure boot chain
            - Software verification technique
        - Chain of trust the update process
    - Other Defenses
        - IoT Device Management
            - IBM Watson IoT
            - Predix
            - AT&T
            - Oracle