- Filename: eccouncil-ceh31250-v10-16-3-1-wireless_hacking_common_threats.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Wireless Hacking: Common Threats
- Description: In this episode, Daniel and Zach take you through an exploration of common threats against wireless networks. Here they will explain and demonstrate some of the more technically simple attacks like exploiting poorly configured devices, deploying Rogue APs, Evil Twins APs, Ad-hoc connections, and Honeypot APs.

==========

Wireless Hacking: Common Threats

- **I know that there are many different types of attacks that leverage wireless technologies. That being said, where does one begin?**
    - Simple to complex
        - Simple
            - Poorly configured APs
                - Default creds
                - Poor password strength
                    - Try the SSID as a password
                        - To broadcast or not to broadcast. That is the question.
            - Rogue Access Point
                - Example of an Access Control attack
                    - Access control bypassing
                - Setup an AP on target network
                - Wait for connections
                - Sniff traffic for goodies
                - Bonus points for planting AP inside target network
                    - Gives outside access to attacker
                        - Some employees inadvertently do this for you
            - Evil Twin
                - Mimics another AP on your target's network
                    - Standard AP or Wifi-Pumpkin/Pineapple to accomplish this
            - Ad-Hoc Connection
                - Attacker connects to a wireless adapter in ad-hoc mode
                    - Will have to use malware/trojan otherwise to enable ad-hoc mode
            - Honeypot AP
                - Attacker impersonates a popular hotspot