- Filename: eccouncil-ceh31250-v11-18-5-1-ot-attacks-tools-and-countermeasures.md
- Show Name: CEHv11 (312-50)
- Topic Name: Mobile Platform, IoT, and OT Hacking - IoT and OT Hacking
- Episode Name: OT Attacks, Tools, and Countermeasures ================================================================================

# OT Attacks, Tools, and Countermeasures

## Objectives:

---

- OT Vulnerabilities
    - Internet-connected OT systems
    - OT System connected to system that is connected to Internet
    - Missing or Non-existent updates
    - Weak passwords and/or no authentication
    - Weak firewall rules (ingress/egress)
    - Non-existent network segmentation
    - Weak or non-existent encryption
- OT Threats
    - **Malware**
        - Introduced through
            - Removable Media
            - External hardware
            - via Internet
                - IT connected systems
                    - Web / Database
                    - Compromised Cloud
                    - Infected end-user devices
    - DoS/DDoS
    - Sensitive data exposure
    - **HMI-based Attacks**
        - Buffer Overflows
        - Authentication/Authorization
            - Creds in Clear-text
            - Hard-coded creds
            - Sensitive info transmitted in the clear
    - Human Error
    - **Side-Channel attacks**
        - Monitoring physical aspects of the OT
            - Timing Analysis
                - Observe the time it takes to complete password auth process
                    - Deduce password or crypto-key
            - Power Analysis
                - Attacker using a oscilloscope observes power consumption between clock cycles

  - **RF Connected controller attacks** (attacks against RF communications)
    - Replay attacks
      - Capture and replay legit command traffic
    - Command Injection
      - Create and inject malicious traffic
    - Malicious RF Controller Re-pairing attack
      - "Evil" Controller
    - Malicious Reprogramming attack
      - Evil firmware
- Tools
  - Shodan
  - SearchDiggity
  - s7scan
  - plcscan
  - smartrf packet sniffer (https://www.ti.com/tool/download/PACKET-SNIFFER-2)
  - ISF (ICS Exploitation Framework)
- Countermeasures
  - Updates/Patches
  - Secure Coding practices
  - Change defaults (passwords/configs)
  - Secure authentication (strong passwords/MFA)
  - Disable/Secure remote access
  - Encryption
  - Firewalls/IDS/IPS
  - Network Segmentation
  - Security training
  - OT Specific monitoring solutions
  - Honeypots/Honeynets (conpot)