# Module 18: IoT & OT Hacking - Practical Guide

This guide details the specialized tools and step-by-step procedures for the hands-on lab sessions required to master the auditing of Internet of Things (IoT) and Operational Technology (OT) environments.

## 1. Comprehensive IoT & OT Toolset

### Discovery & Reconnaissance (OSINT)

* **Shodan:** The primary search engine for finding internet-connected devices. It allows you to search by port, service banner, and geographic location.
* **Censys:** Used to identify certificates and protocol versions on exposed IoT devices.
* **Wireshark:** Essential for capturing and analyzing traffic from IoT-specific protocols like MQTT or Modbus.

### Firmware Analysis & Reverse Engineering

* **Binwalk:** The industry-standard tool for searching binary files for embedded files and executable code. It is used to extract filesystems from firmware update files.
* **Firmwalker:** A script that automates the process of searching through an extracted firmware filesystem for sensitive strings (passwords, API keys, certificates).
* **Ghidra / IDA Pro:** Advanced disassemblers used to analyze the machine code within IoT binaries to find logic flaws or hardcoded credentials.

### Protocol & Hardware Exploitation

* **MQTT Explorer:** A GUI-based client used to connect to MQTT brokers, subscribe to topics, and visualize the data flow from sensors.
* **KillerBee:** A specialized framework and toolset for attacking Zigbee wireless networks.
* **Attify Badge:** A hardware tool used to interface with physical debugging pins on a circuit board (UART and JTAG).

## 2. Hands-On Lab Sessions

### Lab 1: IoT Reconnaissance with Shodan

**Goal:** Locate exposed Industrial Control Systems (ICS) and IoT devices globally.

1. **Search for PLCs:** Use the query port:502 to find devices running the Modbus protocol.
2. **Filter by Vendor:** Use port:502 "Schneider Electric" to find specific brands of industrial controllers.
3. **Search for Webcams:** Use "Server: SQ-WEBCAM" to find vulnerable camera systems.
4. **Identify Vulnerabilities:** Check the "Vulnerabilities" section in the Shodan results to see if the device is susceptible to known CVEs.

### Lab 2: Firmware Extraction with Binwalk

**Goal:** Extract the internal filesystem from an IoT firmware update binary.

1. **Obtain Firmware:** Download a sample firmware file (e.g., camera\_update.bin).
2. **Initial Scan:**  
   binwalk camera\_update.bin  
     
   *Note: This identifies the offset of various file systems (like SquashFS).*
3. **Extraction:**  
   binwalk -e camera\_update.bin
4. **Post-Extraction Analysis:** Navigate into the \_camera\_update.bin.extracted directory and look for the /etc/shadow file to find root password hashes.

### Lab 3: Intercepting and Spoofing MQTT Traffic

**Goal:** Sniff unencrypted MQTT messages and publish fake data to an IoT broker.

1. **Connect:** Open **MQTT Explorer** and connect to a local or public MQTT broker (e.g., broker.hivemq.com).
2. **Subscribe:** Use the wildcard topic # to see all messages being sent across the broker.
3. **Analyze Payloads:** Look for topics like sensor/temperature and observe the JSON data.
4. **Spoof Data:** Use the "Publish" section to send a fake value to the topic:
   * **Topic:** sensor/temperature
   * **Payload:** {"value": 100}
5. **Observation:** Notice how the receiving application reacts to the artificial "100 degree" reading.

### Lab 4: OT Discovery with Nmap NSE

**Goal:** Identify industrial services and extract PLC information.

1. **Modbus Discovery:**  
   nmap -sV -p 502 --script modbus-discover [Target\_IP]
2. **BACnet (Building Automation) Discovery:**  
   nmap -sU -p 47808 --script bacnet-info [Target\_IP]
3. **Analysis:** The results will often reveal the device vendor, hardware version, and firmware version directly from the PLC.

### Lab 5: Hardware Recon (UART Identification)

**Goal:** Identify the correct pins on a hardware device to gain console access.

1. **Visual Inspection:** Locate a row of 4 pins on the PCB labeled VCC, GND, TX, RX.
2. **Multimeter Check:** Use a multimeter to find the GND (Ground) pin by checking for continuity with the metal shield.
3. **Connect:** Attach a USB-to-TTL adapter to the TX and RX pins.
4. **Access:** Open a serial terminal (like **Minicom** or **PuTTY**) at a standard baud rate (e.g., 115200) to see if the device provides a root shell upon boot.

## 3. CEH Exam Technical Nuance

* **The Purdue Model:** Remember that the **Process Control Layer (Level 1/2)** is where the PLCs live, while the **Enterprise Layer (Level 4/5)** is the corporate IT network.
* **Rolling Code Attack:** This is a wireless attack against IoT car fobs. The counter-attack is **Rolljam** (Jam-and-Replay).
* **Availability:** Always prioritize Availability and Safety over Confidentiality when discussing OT environments.