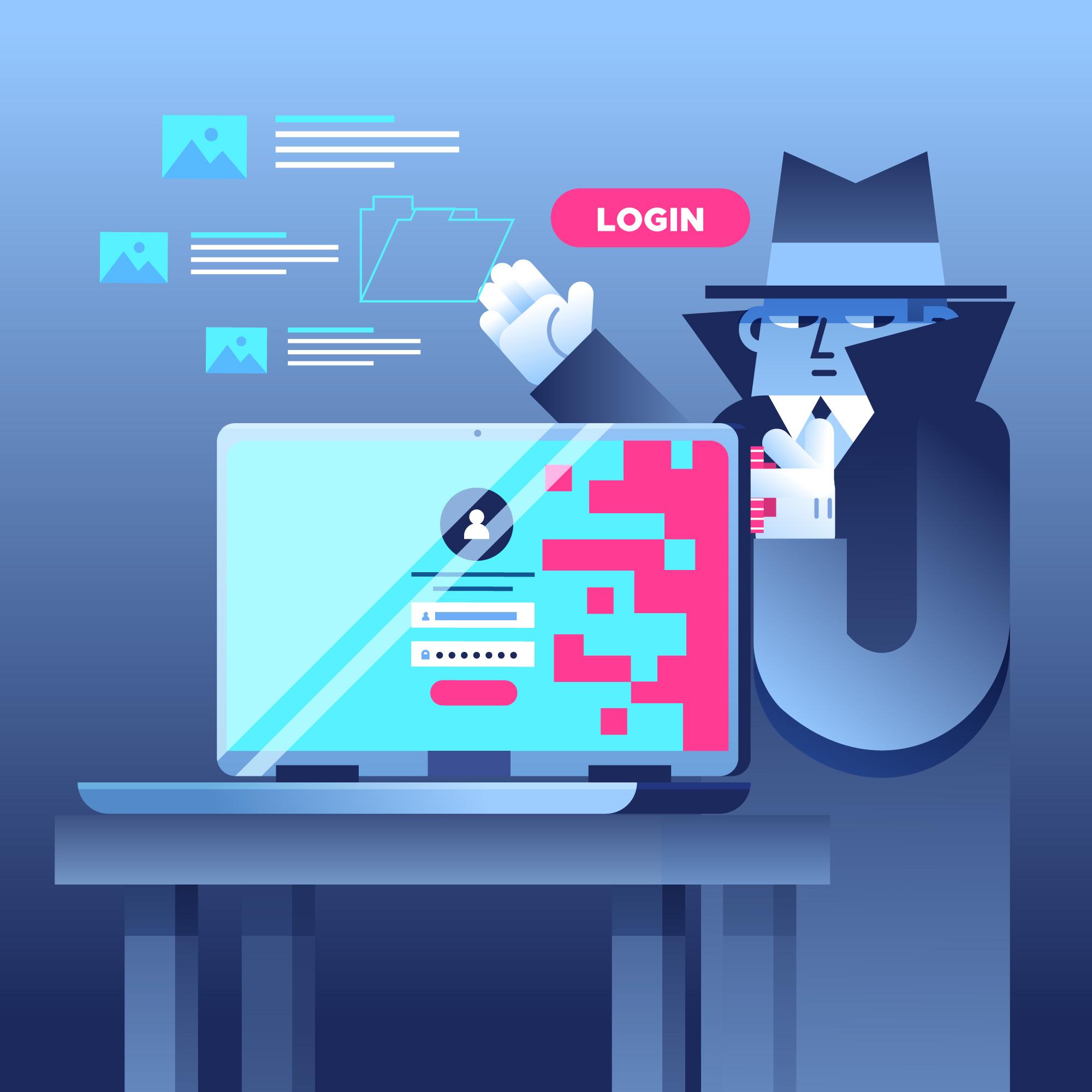
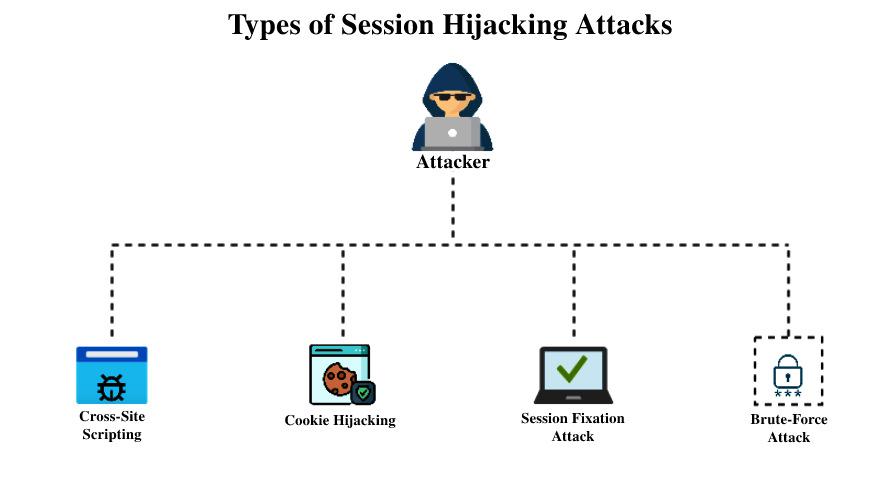
**CTF Challenge: Session Hijacking**

**What is Session Hijacking?**

****

"Session hijacking" refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. In a session hijacking attack, the attacker takes over a user's session and assumes their identity to perform actions as the user. Here are some key points about session hijacking:

### **Types of Session Hijacking**



1. **Active Hijacking**: The attacker takes over the session while it is still active, potentially disrupting the legitimate user's experience.
2. **Passive Hijacking**: The attacker monitors the session without disrupting the legitimate user’s activity to gather information.

### **Techniques for Session Hijacking**

1. **Session Fixation**: The attacker sets a known session ID and tricks the user into using it, allowing the attacker to hijack the session once the user logs in.
2. **Session Sidejacking**: The attacker uses packet sniffing to steal session cookies, often on unencrypted networks.
3. **Cross-Site Scripting (XSS)**: Injecting malicious scripts into web pages to steal session cookies.
4. **Man-in-the-Middle (MitM)**: Intercepting communication between the user and server to hijack the session.

### **Tools for Session Hijacking**

* **Firesheep**: A Firefox extension that intercepts unencrypted session cookies.
* **Ettercap**: A comprehensive suite for man-in-the-middle attacks on LAN.
* **Burp Suite**: An integrated platform for performing security testing of web applications, including session hijacking.

# **Capture the Flag (CTF) Challenges**

**Flag 1. Which type of hijacking involves the attacker taking over an active session, potentially disrupting the user’s experience?**

Answer: Active

**Flag 2. What technique involves using packet sniffing to steal session cookies on unencrypted networks?**

Answer: Sidejacking

**Flag 3. Which Firefox extension can intercept unencrypted session cookies?**

Answer: Firesheep

**Flag 4. What method injects malicious scripts into web pages to steal session cookies?**

Answer: XSS

**Flag 5. What is the term for intercepting communication between the user and server to hijack the session?**

Answer: MitM