Session Hijacking

Session Hijacking

Session hijacking involves exploiting the web session control mechanism to gain unauthorized access to a web server. The session token, often managed through a session ID, plays a crucial role in identifying and maintaining user connections.

Common Attack Vectors:

1. **Predictable Session Token:**
    - Exploits weak session ID generation.
    - Attackers predict or guess session tokens to gain unauthorized access.
2. **Session Sniffing:**
    - Involves capturing session IDs from non-encrypted communication.
    - Tools like Wireshark can be used to intercept and collect sensitive data packets.
3. **Cross-Site Scripting (XSS):**
    - Malicious code injected into a website, executed on the victim's browser.
    - Allows attackers to steal session information.
4. **Cross-Site Request Forgery (CSRF):**
    - Forces users to perform unwanted actions on a web application.
    - Social engineering is often involved to trick users into executing actions.
5. **Session Fixation:**
    - An attacker sets or fixes a session ID for a victim.
    - Exploits the way web applications manage session IDs.
6. **Man-in-the-Browser Attack:**
    - Similar to Man-in-the-Middle but uses a Trojan Horse to manipulate calls.
    - Intercept and modify communication between the application and the user.

Other Attacks:

- **Compression Ratio Info-leak Made Easy (CRIME):**
  - Targets secret web cookies over HTTPS connections using data compression.
  - Allows attackers to perform session hijacking.
- **BREACH:**
  - A security exploit against HTTPS using HTTP compression.
  - Built on the CRIME security exploit.
- **Forbidden Attack Vulnerability in TLS:**
  - Exploits TLS vulnerabilities related to cryptographic nonces.
- **Network Layer Attacks:**
  - TCP Hijacking involves gaining access to another user's network connection.
  - Tools like Ettercap and Shijack are used for TCP/IP hijacking.

Tools

- **Ettercap** - MiTM tool and packet sniffer on steroids
- **Hunt** - sniff, hijack and reset connections
- **T-Sight** - easily hijack sessions and monitor network connections
- **Zaproxy**
- **Burp Suite**
- **Paros**
- **Shijack** - TCP/IP hijack tools
- **Juggernaut**
- **Hamster**
- **Ferret**

Countermeasures:

- **Session IDS:**
  - Intrusion Detection Systems to monitor and detect suspicious session activity.
- **Randomized Session IDs:**
  - Session IDs should be unpredictable to prevent guessing attacks.
- **Avoid URL Sessions:**
  - Do not include session IDs in URLs to prevent exposure.
- **HTTP-Only Cookies:**
  - Restrict cookie access to JavaScript, preventing XSS attacks.
- **HTTPS Usage:**
  - Encrypt communication using TLS/SSL to secure data in transit.
- **Session Key Regeneration:**
  - Regenerate session keys after user authentication.
- **Time Limits:**
  - Implement session timeout to log users out after a period of inactivity.
- **Multi-Factor Authentication (MFA):**
  - Adds an extra layer of security beyond passwords.
- **IPSec Encryption:**
  - Provides network-layer security through encryption.
- **Architecture Protocols:**
  - Authentication Header, Encapsulating Security Payload (ESP), IKE, Oakley, ISAKMP for secure communication.