- Filename: eccouncil-ceh31250-v12-11-4-1-session-hijacking-countermeasures.md
- Show Name: CEHv12 (312-50)
- Topic Name: Network and Perimeter Hacking: Session Hijacking
- Episode Name: Session Hijacking Countermeasures
  ==

Session Hijacking Countermeasures

Objectives:

- List and describe session hijacking detection methods
- Explain commonly employed protections against session hijacking attacks
- Define session hijacking specific security control mechanisms

---

- How do we protect against session hijacking attacks?
    - Detection
        - Manually detect
            - More network traffic than normal
            - Packet inspection with Wireshark
            - ARP Cache Entries
        - Automation
            - IDS/IPS
            - SIEM w/real-time threat protection
- What about preventative measures?
    - Switch to encrypted protocols and applications
        - Telnet < SSH
        - HTTP < HTTPS
        - IP < IPsec
    - Web Apps
        - End-Users
            - ALWAYS LOG OUT!
            - Don't click links in emails
        - Web App Devs/Admins
            - Use randomization for session IDs
            - No session for unauthenticated users if possible
            - Generate new session IDs after login
            - Verify session is coming from same host
                - Look at things like source IP and User Agent string
            - Set sessions to expire after logout
                - Set sessions to expire more quickly