- Filename: eccouncil-ceh31250-v10-11-1-3-session_hijacking_pt3.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Session Hijacking Pt.3
- Description: In this episode, Daniel and Zach finish exploring session hijacking. Here they discuss and demonstrate network-layer session hijacking, specifically showing you how to hijack an active telnet session. Finally, they go over the possible mitigation strategies to protect against these types of attacks.

==========

Session Hijacking Pt.3

- **Any other Application-layer session attacks we should be aware of?**
    - CRIME/BREACH
        - Exploits a vulnerability in the use of compression features found in
            - HTTPS/SSL/TLS
            - SPDY
    - Forbidden Attack
        - Attacker intercepts the nonce(Number Used Once)
        - Attacker uses nonce to hijack a session
        - This sets up a MITM attack
- **These have all been Application-layer attacks, but what about Network-layer attacks?**
    - TCP Hijacking
        - Hijack Telnet session
            1. Establish telnet session between client and server
            2. Start Ettercap GUI ARP spoof attack
                - Sniff > Unified Sniffing
                - Targets > Select Targets
                - Mitm > ARP Poisoning > Sniff Remote Connections
            3. Find session information with Wireshark
                - Look for Client to Server connection
                - Record Source IP/Port && Destination IP/Port
            4. Use *shijack* to hijack the session
                - `shijack-lnx eth0 10.0.0.200 48895 10.0.0.165 23`
            5. Wait for *shijack* to capture SEQACK
            6. Now you can run any command as that victim
                - This specific example is a **BLIND** attack
                    - We can't see the response from the target
    - Other network attack include
    - RST Hijacking
        - Sniff network for session packet with ACK flag set
        - Also need the Source/Dest IP/Port, Sequence number and Acknowledgement number
        - If you can correctly guess the next sequence number to the server...
            - You can reset the session by sending RST packet
                - Allowing you to hijack the session
    - UDP Hijacking

        - Race UDP service responses with forged/malicious responses
            - DNS
                - Gets a victim to update their DNS cache with false info
                    - Sends victim to cloned sites
- **How do we protect ourselves from Session Hijacking?**
    - Use end-to-end encryption
        - IPSec
        - SSL/TLS
    - Use random session IDs
    - Don't deliver session IDs via the URL or query string
    - Employ protective software apps
    - Auto-expire sessions with reasonably short session life
    - Use HSTS (HTTP Strict Transport Security)
        - Requires the use of HTTPS
    - Certificate and/or Public Key Pinning
        - Clients check Public Key or SSL Cert before creating a session