

- Filename: eccouncil-ceh31250-v11-11-2-1-network-level-session-hijacking.md
 - Show Name: CEHV11 (312-50)
 - Topic Name: Network and Perimeter Hacking: Session Hijacking
 - Episode Name: Network Level Session Hijacking
- =====

Network Level Session Hijacking

Objectives:

- List and define common Network-Level Session Hijacking attacks
-
- What are some of the common Network-Level Session Hijacking attacks we should be aware of?
 - Blind Hijacking
 - Kind of a 'hail Mary'
 - Attacker must correctly guess/predict the next *Initial Sequence Number*(ISN) of the device attempting to establish a session/connection
 - Attacker can then inject malicious stuff
 - Attacker cannot see responses (aka BLIND)
 - UDP
 - Attacker intercepts UDP replies
 - Modifies UDP replies and sends them on to intended endpoint
 - Modification is difficult to detect
 - UDP doesn't have the error correcting like TCP
 - TCP
 - **DEMO**: 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 (first try wont work)
 - This specific example is a **BLIND** attack
 - We can't see the response from the target
 - 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
- MitM Packet Sniffing
 - **DEMO**
 - Use Ettercap to ARP poison Bee-box and Websploit2018
 - Start wireshark
 - Bee-box is playing the Target
 - Bee-box login to to Websploit2018/bwapp
 - Check Wireshark for session token
 - Insert new token into Parrot browser and refresh page
 - User should have changed from Bee to AIM