**Attacker’s Client (ex2\_client.c)**

The attacker’s client (ex2\_client.c) performs the following tasks:

* **Send Initial Query:** The client sends a DNS query for www.attacker.cybercourse.com to the vulnerable BIND9 resolver to initiate the attack sequence.
* **Receive TXID and Port Information:** It listens(in port 1024) for a UDP message from the attacker’s server containing the TXID and source port.
* **Predict TXIDs:** Using the TXID received, the client predicts the next 10 TXIDs using a linear-feedback shift register (LFSR) model, based on known taps (TAP1 and TAP2) like seen in the Amit Klien’s article.
* **Send Spoofed Responses:** The client crafts raw DNS packets with the predicted TXIDs, spoofing the source IP address (192.168.1.204) to simulate the root server. Each packet contains:
  1. An A record mapping www.example.cybercourse.com to 6.6.6.6.
  2. An authority section with NS records for cybercourse.com.
  3. An additional section with the IP address of the fake NS server (192.168.1.204).
* **Raw Socket Implementation:** The client uses raw sockets to send spoofed packets directly, including custom IP and UDP headers and calculate the checksum.

**Key Implementation Details:**

* The client uses ldns\_pkt to construct DNS payloads and raw sockets for packet transmission.
* Checksums for IP and UDP headers are calculated manually.
* A sleep interval (usleep) ensures the spoofed responses arrive before the legitimate response.

**Attacker’s Authoritative Name Server (ex2\_server.c)**

The attacker’s server (ex2\_server.c) performs the following tasks:

* **Handle DNS Queries:** It listens for incoming DNS queries and responds with either:
  1. A CNAME record pointing to a subdomain for odd TXIDs.
  2. A CNAME record pointing to the target domain for even TXIDs.
* **Simulate DNS Authority:** It constructs and sends DNS responses using the ldns library, including CNAME, OPT records, and question sections.
* **Send TXID and Port Information:** When an even TXID is encountered, the server extracts the TXID and source port and sends this information to the attacker’s client to assist with spoofing responses.
* **Stop on Success:** After notifying the attacker’s client of a valid TXID, the server stops further processing.

**Key Implementation Details:**

* The server uses ldns\_pkt to construct and serialize DNS packets.
* OPT records are included for EDNS0 compatibility.
* A loop continues handling incoming queries until the server sends a valid TXID and port to the attacker’s client.