Riley Radici

1. **Explanation of how the TCP SYN flood attack works:**

   The TCP three-way handshake is exploited when the attacker sends multiple SYN (synchronization) requests without acknowledging them. When a SYN request is made, the server sends back a SYN-ACK (synchronization acknowledgment) to the client to confirm the synchronization. When the attacker sends a lot of SYN requests without acknowledging them, the server eventually crashes.

2. **Explanation of how SYN cookies work to prevent the denial-of-service effect from a SYN flood attack:**

   SYN cookies are used to prevent DoS attacks such as the SYN flood by limiting the number of connections at a time. This is done by keeping a table of the SYN requests. If the table reaches its maximum capacity, the subsequent requests are put into a queue until there is room to process them. If the request is valid, i.e., the SYN-ACK comes back to the server, the connection is performed. If the request is invalid, the connection is dropped.
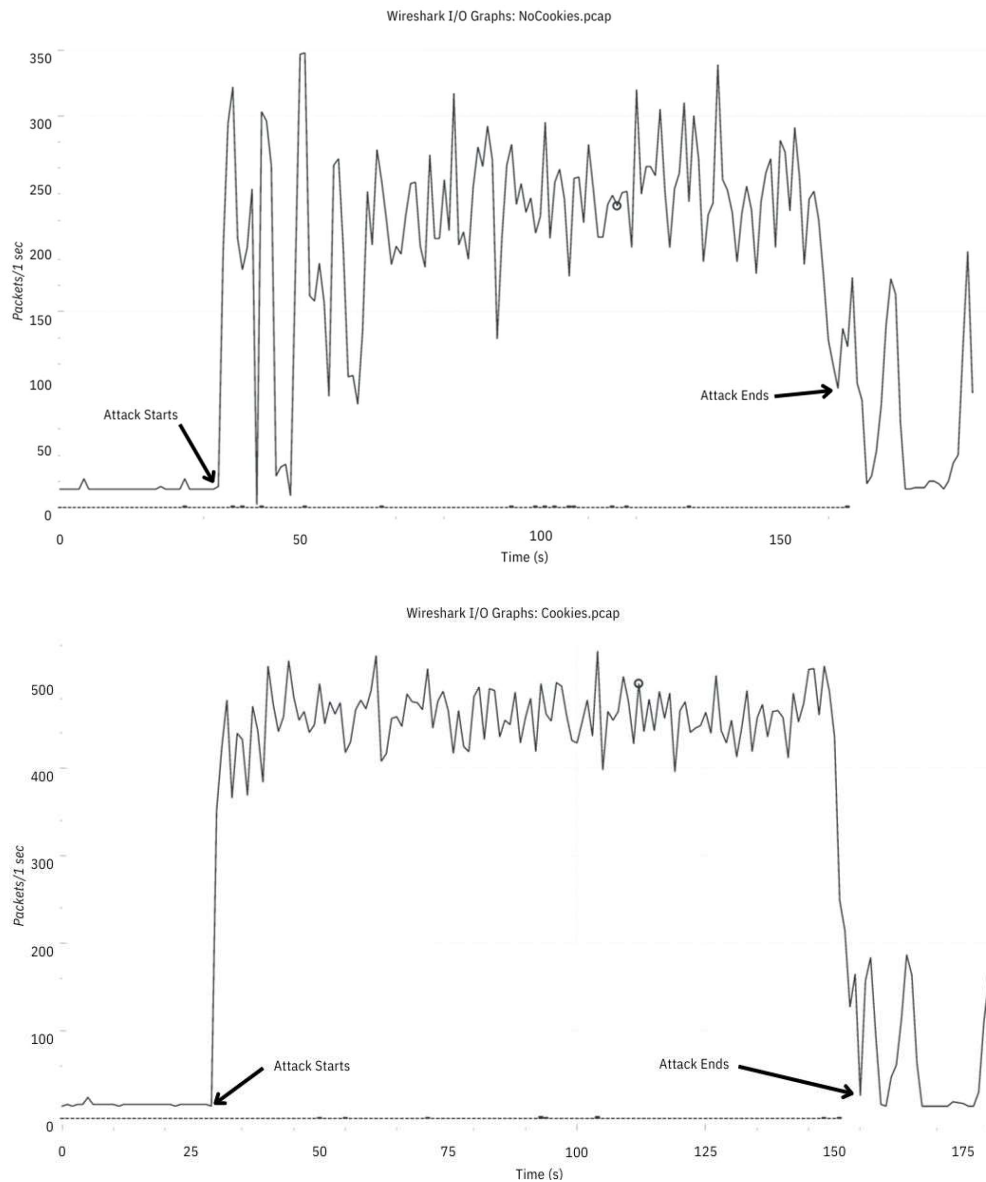
3. **Your legitimate client script:**

   ```
   #!/bin/bash
   for ((i=0; i < 100000; i++)); do
           curl -o index.html 5.6.7.8
           sleep 1
   done
   ```

4. **Your attack command (for flooder):**

   ```
   sudo flooder --dst 5.6.7.8 --highrate 1000 --proto 6 --dportmin 80 --dportmax 80 --src 1.1.2.0 --srcmask 255.255.255.0
   ```

5. Graphs:

Wireshark I/O Graphs: NoCookies.pcap

Wireshark I/O Graphs: Cookies.pcap

6. Explanation of graphs:

The first graph resembles the number of packets per second using no SYN cookies. The second graph resembles the number of packets per second **with** SYN cookies. The graph with no cookies shows how sporadic the connection is with no safeguard against the SYN flood. We can infer that the attack is successful in this case based on the graph since we since the hundreds of connections get periodically dropped within the attack phase. The second graph with cookies also shows a high volume of packets. However, this is a steadier and more predictable flow, meaning the SYN cookies helped prevent sudden drops in packet volume. Therefore, we can assume the attack worked with no SYN cookies and the attack failed with SYN cookies.