

### **Section 3: Identify the type of attack causing this network interruption**

What do you currently understand about network attacks?:

- Network attacks involve capturing packets to obtain valuable information, such as all kinds of PI or PII, etc.

What type of attack would likely cause the symptoms described in the scenario?:

- Validating the aforementioned scenario, the attack characterized by sending multiple packet requests to cause the network to collapse is the DOS or DDOS attack.

What is the difference between a denial of service (DoS) attack and a distributed denial of service (DDoS) attack?:

- A DOS attack involves sending multiple packet requests to a specific device from the same computer. The difference with DDOS is that they use botnets, or multiple devices in different locations, to make the attack more powerful and less detectable.

Why is the website taking a long time to load and reporting a connection timeout error?

- The server is suffering a heavy load of requests, which is why it is saturated. Since it cannot handle all the requests, the user trying to access the website will be on a waiting list to receive the SYN-ACK packet and establish the connection. When your browser's timeout limit passes, if the response from the host has not been received, it generates the aforementioned error.

**Christian Danglades**