Analyzing a Network Attack

Possible Attack on the Website:

One possible reason for the website's connection timeout error is a **Denial of Service (DoS) attack**. The server logs show that the web server stops responding after being flooded with too many **SYN packet requests**. This could indicate a specific type of DoS attack called **SYN flooding**.

How a Normal Connection Works:

When visitors try to connect to the website, their device and the web server go through a process called the **3-way handshake** to establish a connection. This process happens in three steps:

1. **SYN Packet:** The visitor's device sends a request (called a **SYN packet**) to the server, asking to connect.
2. **SYN-ACK Packet:** The server replies with a message (called **SYN-ACK**) saying, "I’m ready to connect. Here are some resources for the connection."
3. **ACK Packet:** The visitor’s device sends a final message (**ACK**) to confirm that the connection is established.

What Happens in a SYN Flood Attack:

In a **SYN flood attack**, a malicious person sends a large number of **SYN packets** all at once. This overwhelms the server’s ability to handle the requests, and it runs out of resources to manage them. As a result, the server can’t process the real connection requests from legitimate visitors.

The logs show that the server has been flooded with these **SYN requests**, making it unable to respond to new visitors, who then get the **connection timeout** error.