Cybersecurity Incident Report (My Responses)

Section 1: Identify the type of attack that may have caused this network interruption
One potential explanation for the website's connection timeout error message is: A Denial of Service (DoS) attack which is a SYN flooding attack. Based on the scenario given and the support documents, it demonstrates that when a user attempts to visit a website, the user's request is handled by the web server, which responds by establishing a connection using the Transmission Control Protocol (TCP). With the definitions and the documents given for this case, I predict that during this attacking process and the TCP, the server's resources are engaged to handle the request. However, in the case described, the logs indicate that the web server stopped responding due to a large number of incoming TCP SYN requests (attacking it). **The logs show that:** the web server stops responding after being overloaded with SYN packet requests. With the sequences of events that happened, I predict that this means that there is a high volume of SYN requests from an unfamiliar IP address, which matches the signature of a SYN flood attack, where an attacker can send a lot of SYN packets to the server to overload it till it can't handle it anymore. With the documents given, I learned that a SYN flood is a type of DoS attack (Denial of Service) where the attacker floods the server with connection requests without completing the handshake, preventing the server from responding to legitimate user requests. The definition and the scenario match what are happening for this case. **This event could be:** hypothetically a type of DoS attack, specifically SYN flooding, where a bad person sends a large number of SYN packets to the server causing it to become overloaded (like a very old engine that suddenly stops in a car) and unable to responds. Usually, if the site is operational, the server would respond to the visitor's navigation to the site. However, in this case, the server is overflooded with half-open connections, increasing the processing power to connect the two areas, leading to a connection timeout error message when attempting to access the website. Upon investigating and the evidences provided, this event of overwhelming the server's ability to handle legitimate traffic clearly foreshadows a SYN flooding attack as the causation to these issues and the scenario given.

Section 2: Explain how the attack is causing the website to malfunction
When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake: 1. **SYN Packet Sent**: The client (source) sends a SYN (synchronize) packet to the server (destination), requesting a connection and is asking the server to allow

the user to communicate with the packet sent.

2. **SYN-ACK Sent**: Then after the SYN packet is sent by the client; the server sends a reply back which is a SYN-ACK (synchronize-acknowledge) packet back to the client to acknowledge the request to connect and indicates that the server is ready to establish the connection. Based on the documents provided it taught me that this tells the server also allocates system resources (such as memory and process threads) to handle the new connection.
3. **ACK Sent**: After the SYN-A CK is sent back to the client and the client receives it, then the client sends an ACK (acknowledgment) packet back to the server, confirming that the connection has been established and the communication can proceed (data/packets are allowed/confirmed to be exchanged).

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

In the case of a SYN flood attack, a malicious actor sends a large number of SYN packets (step 1 of the handshake) all at once, without completing the handshake by sending the final ACK packet (never sends the final ACK packet (step 3).). This causes the server to reserve resources for each of these incomplete connections and it eventually runs out of resources by leaving the server in a state where it has many half-open connections, each waiting for the final acknowledgment from the client. Due to this, I believe that this causes the user to have a time out message as the server is unable to process the connection request.

My shortened version of the events that happened in this case are below:

- The server allocates resources (such as memory and threads) for each incoming SYN request in anticipation of completing the handshake.
- Since the attacker does not send the final ACK, the server is unable to complete the connection for these requests.
- The server continues to reserve resources for these half-open connections, but they do not get completed, leading to a resource exhaustion scenario.
- As a result, the server to become unresponsive and users receive a connection timeout error message in their browsers because the server is unable to process their requests.

Explain what the logs indicate and how that affects the server:

Based on all the evidences, supporting documents given, and the sequences of events that happened, I believe that the logs indicate that the web server has become overwhelmed by these excessive high number of SYN requests from a specific, unfamiliar IP address. and is unable to process the legitimate visitors' SYN packets. Due to this, I conclude that the attack is targeting the server by exploiting its TCP connection management process and consuming its resources. Overall with all of these evidences in mind, the server to become unresponsive and users receive a connection timeout error message (website error) in their browsers because the server is unable to process their requests.

Supporting Additional Information:

Scenario: You work as a security analyst for a travel agency that advertises sales and promotions on the company's website. The employees of the company regularly access the company's sales webpage to search for vacation packages their customers might like.

One afternoon, you receive an automated alert from your monitoring system indicating a problem with the web server. You attempt to visit the company's website, but you receive a connection timeout error message in your browser.

You use a packet sniffer to capture data packets in transit to and from the web server. You notice a large number of TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. You suspect the server is under attack by a malicious actor.

You take the server offline temporarily so that the machine can recover and return to a normal operating status. You also configure the company's firewall to block the IP address that was sending the abnormal number of SYN requests. You know that your IP blocking solution won't last long, as an attacker can spoof other IP addresses to get around this block. You need to alert your manager about this problem quickly and discuss the next steps to stop this attacker and prevent this problem from happening again. You will need to be prepared to tell your boss about the type of attack you discovered and how it was affecting the web server and employees.

Links to supporting materials:

- Wireshark TCP/HTTP log
- How to read a Wireshark TCP/HTTP log

Step 3: Identify the type of attack causing this network interruption

Reflect on the types of network intrusion attacks that you have learned about in this course so far. As a security analyst, identifying the type of network attack based on the incident is the first step to managing the attack and preventing similar attacks in the future.

Here are some questions to consider when determining what type of attack occurred:

- What do you currently understand about network attacks?
- Which type of attack would likely result in the symptoms described in the scenario?
- What is the difference between a denial of service (DoS) and distributed denial of service (DDoS)?
- Why is the website taking a long time to load and reporting a connection timeout error?

Review the Wireshark reading from step 2 and try to identify patterns in the logged network traffic. Analyze the patterns to determine which type of network attack occurred. Write your analysis in section one of the Cybersecurity incident report template provided.

Step 4: Explain how the attack is causing the website to malfunction… Review the Wireshark reading from step 2, then write your analysis in section two of the Cybersecurity incident report template provided.When writing your report, discuss the network devices and activities that are involved in the interruption. Include the following information in your explanation:

- Describe the attack. What are the main symptoms or characteristics of this specific type of attack?
- Explain how it affected the organization's network. How does this specific network attack affect the website and how it functions?

- Describe the potential consequences of this attack and how it negatively affects the organization.
- Optional: Suggest potential ways to secure the network so this attack can be prevented in the future.

Be sure to address the following in your completed activity:

- The name of the network intrusion attack
- A description of how the attack negatively impacts network performance