Cybersecurity Incident Report Analysis

Section 1: Identify the type of attack that may have caused this network interruption
Type of Attack: Denial-of-Service (DoS) Attack **Description:** The website's connection timeout error message indicates a DoS attack. Packet sniffing revealed heavy network traffic from a single IP address, overwhelming the server and preventing it from responding to legitimate requests. **Evidence:** Logs show a surge of TCP SYN requests from an unknown IP address during the incident, indicative of a coordinated attack. **Impact:** The attack disrupted business operations and impacted customer experience. **Explanation:** One potential explanation for the website's connection timeout error message is that upon using the Packet Sniffing method, it was deduced that the server was receiving heavy network traffic from the same IP address, thus it was unable to respond to requests from the employees. All of these circumstances led to this event being a DoS Attack. The logs show that around the afternoon, the company’s server received an overwhelming amount of TCP SYN Requests from an unknown IP Address. **Conclusion:** This event could be an indication that a malicious actor has targeted our company’s server to slow down our business operations, resulting in customers being unsatisfied.

Section 2: Explain how the attack is causing the website to malfunction

Attack Method: SYN Flood Attack

Description: The attacker flooded the server with SYN packets, occupying all available ports and causing network congestion. This prevented legitimate connection requests from being processed.

Impact on Server: The server had to be temporarily taken down to mitigate the attack, resulting in downtime and loss of productivity.

Explanation: 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. The client initiates the connection by sending a TCP segment with the SYN (synchronize) flag set to the server.

2. The server acknowledges the client's sequence number (Seq), and it also selects its initial sequence number (ISN).

3. Finally, the client acknowledges the server's response by sending a TCP segment with the ACK flag set.

When a malicious actor sends a large number of SYN packets all at once, all of the ports get occupied which causes Network Traffic congestion which causes legitimate connection requests to be unable to process.

Explain what the logs indicate and how that affects the server: The logs indicate that a large amount of SYN-ACK requests were received by the server. This attack had an immense impact on the company’s productivity as the server had to be taken down temporarily in order to return to normal operating status.

Conclusion: The attack targeted our company's server, aiming to disrupt operations. Immediate action was taken to mitigate the impact, and measures are being implemented to prevent future attacks.