Cybersecurity Incident Report

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 SYN flood attack, a type of Denial-of-Service (DoS) attack that overwhelms a target server with numerous TCP connection requests.

The logs show that:

- **A significant number of TCP SYN requests originated from an unfamiliar IP address.**
- **The web server was unable to complete connections due to an excessive number of half-open TCP sessions.**
- **This resulted in exhaustion of server resources, preventing legitimate users from accessing the website.**
- **Increased CPU usage and memory consumption on the server were observed, further contributing to performance degradation.**

This event could be a Distributed Denial-of-Service (DDoS) attack if multiple IP addresses are involved, or a single-source SYN flood attack if only one IP address is responsible.

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:

1. **SYN (Synchronize) – The client sends a SYN request to initiate a connection.**
2. **SYN-ACK (Synchronize-Acknowledge) – The server responds with a SYN-ACK to acknowledge the request.**
3. **ACK (Acknowledge) – The client sends an ACK, completing the connection establishment.**

How the attack disrupts this process:

- **A malicious actor floods the server with a large number of SYN packets but never completes the handshake by sending the final ACK.**
- **This causes the server to keep waiting for responses, consuming its connection slots and preventing legitimate users from establishing connections.**
- **The server eventually becomes overwhelmed, leading to performance degradation and eventual failure to respond.**
- **High network congestion is observed, with increased packet drops and latency spikes.**

What the logs indicate and how it affects the server:

- **The logs show numerous half-open TCP connections, meaning requests are being initiated but never completed.**
- **The server is exhausting system memory and connection queues, leading to resource depletion.**
- **The result is a denial of service, preventing employees and customers from accessing the website.**
- **Prolonged attacks can cause business revenue loss, customer dissatisfaction, and damage to the organization's reputation.**

Next Steps to Mitigate and Prevent Future Attacks:

1. **Implement SYN Cookies – This helps protect against SYN flood attacks by allowing the server to respond without allocating resources for half-open connections.**
2. **Use a Web Application Firewall (WAF) – To detect and filter out malicious traffic.**
3. **Rate Limiting & Traffic Filtering – Restrict the number of requests per IP and block suspicious patterns.**
4. **Enable Intrusion Detection Systems (IDS) – To monitor and alert on unusual network activity.**
5. **Deploy a Content Delivery Network (CDN) – To help absorb excess traffic and mitigate DoS attacks.**
6. **Engage ISP for DDoS Mitigation Services – If the attack continues, contacting the ISP for additional protection may be necessary.**
7. **Geo-blocking & IP Reputation Filtering – Block traffic from known botnet regions and suspicious IPs.**

By implementing these security measures, we can reduce the impact of SYN flood attacks and ensure continued website availability for employees and customers.