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 DoS attack.

The logs show that:

- A continuous stream of SYN requests originate from an unfamiliar IP address (203.0.113.0).
- The volume of SYN requests overwhelms the web server, resulting in a connection timeout error.

This event could be a SYN flood attack, causing an overflow of SYN requests to the network.

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 (Synchronize)**: The client initiates a connection by sending a SYN, ACK packet, indicating it willingless to establish a connection.

2. **SYN, ACK (Synchronize, Acknowledge)**: The server responds with AYN, ACK packet, indicating its willingness to establish a connection. The destination reserves resources fot the source to connect.

3. **ACK (Acknowledge)**: The client acknowledges the server's response with ACK packet, and the connection is established.

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

- When a malicious actor initiates a SYN flood attack, the web server, anticipating legitimate connection requests, allocates resources for each incoming SYN request.
- In a SYN flood attack the server or network is flooded with SYN packets from the attacker, disrupting the normal handshake process
- As a result, the server's resources are depleted, leading to worsening of performance and, eventually a loss of service.

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

- A stream of of SYN requests (log items 52- 152) from the attackers's IP address (203.0.113.0) and a few legitimate SYN requests from employees.
- Initially the server responds to both the legitimate (green) and malicious (red) SYN requests (log items 52 -79).
- As the attack intensifies, the server struggles to keep up which results in failed communications (yellow) with legitimate visitiors.
- The web server eventually stops responding to legitimate traffic, indicating a successful disruption caused by the SYN flood attack.
- The error messgaes included in the log are "504 Gateway Time out" and [RST, ACK] packets. This indicates the inibaility to establish connections and the dropping of connection attempts.

To prevent such an attack in the future the orginization should implement the following security measures:

- **Intrusion Prevention System (IPS):** Deploying IPS solutions can help identify an block malicious traffic. The IPS systems analyze network traffic patterns in real time and takes proactive measures to prevent unauthorized access. One example of an IPS is the Cisco Secure IPS.
- **Rate limiting**: Implementing rate-limiting measures on incoming SYN requests can help control the volume of requests from a single source. This can help mitigate the impact of SYN flood attacks by limiting the number of connection requests within a specific time frame. This will not protect the server from advanced DDoS attacks, especially those distributed across multiple sources. Attackers may use botnets to bypass the rate limit.
- **Web Application Firewalls (WAF)**: Deploying WAFs can add an additional layer of protection by filtering and monitoring HTTP traffic between a web application and the internet. WAFs can detect and block malicious traffic including attempts to exploit vumlrabilitites through SYN flood attacks.
- **Incident Response Plan**: Develop and regularly update an incident response plan that outlines the steps to be taken in the event of a cyber attack. This ensures a swift and coordinated response to minimize the impact of the attack and facilitate recovery.