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:

The server's resources are consumed by malicious half-open connections, leaving no capacity to serve legitimate traffic.

This event could be: SYN Flood Denial-of-Service (DoS) Attack.

The logs shows that:

1. Repetitive SYN Packets from Malicious Source:

- IP `203.0.113.0` sends hundreds of `SYN` packets to the server `192.0.2.1:443` (e.g., entries 52.0, 57.0, 59.0, and continuing through entry 214.0).
- These `SYN` packets have no follow-up `ACK` from the attacker, leaving connections half-open.

2. Server Overload Symptoms:

- The server sends `[RST, ACK]` packets (e.g., entries 73.0, 80.0, 85.0) to legitimate clients like `198.51.100.16` and `198.51.100.7`, indicating it is forcibly closing connections due to resource exhaustion.

- Legitimate HTTP requests (e.g., `GET /sales.html`) are interrupted, resulting in errors like `504 Gateway Time-out` (entry 77.0).

3. Pattern of Incomplete Handshakes:

- Normal TCP handshakes (green entries) complete the `SYN → SYN-ACK → ACK` sequence (e.g., entries 47–51).
- Malicious traffic (red entries) only completes `SYN → SYN-ACK`, exhausting the server's connection queue.

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.Normal TCP Three-Way Handshake:

- Step 1: The client sends a `SYN` (synchronize) packet to the server in order to initiate a connection.
- Step 2: The server responds with a `SYN-ACK` (synchronize-acknowledge) packet to confirm readiness.
- Step 3: The client sends a final `ACK` (acknowledge) packet to establish the connection.

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

Malicious SYN Flood Mechanics:

- Attack Description: A malicious actor (IP `203.0.113.0`) sent a massive volume of `SYN` packets to the server (IP `192.0.2.1:443`) without completing the handshake, never sent the final `ACK`

- Half-Open Connections: The server reserved resources for each incomplete handshake, exhausting its connection queue.

- Legitimate Traffic Blocked: Legitimate users (e.g., `198.51.100.23`) received `RST, ACK` packets (e.g., entry 73.0) as the server forcibly closed connections to free resources.

- HTTP Errors: Valid requests (e.g., `GET /sales.html`) timed out, resulting in errors like `504 Gateway Time-out` (entry 77.0).

- The server allocates resources to each half-open connection, eventually exhausting its available ports/memory.

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

Impact on the Server:

- Legitimate users (e.g., `198.51.100.23`) cannot complete handshakes because the server's connection queue is full.

- The server starts resetting legitimate connections (yellow entries) and fails to respond to valid HTTP requests, causing timeouts.

Network Devices and Activities Involved:

- Web Server: Overwhelmed by fake `SYN` requests, leaving no capacity to serve legitimate users.

- Firewalls/Routers: Failed to detect and block the abnormal traffic pattern from `203.0.113.0`.

- Load Balancers (if present): Could not mitigate the attack due to the sheer volume of malicious packets.

Impact on the Organization:

- Website Functionality:
    - Users experienced slow loading times or complete inability to access the site.
    - Critical services (e.g., sales pages) became unavailable, disrupting operations.
- Network Performance:
    - Bandwidth saturation degraded overall network performance.
    - Server CPU/memory usage spiked, risking hardware failure.
- Potential Consequences:
    - Financial Loss: Downtime halted revenue-generating activities (e.g., e-commerce transactions).
    - Reputation Damage: Customers lost trust due to unreliable service.
    - Secondary Attacks: The `SYN` flood could mask more severe intrusions (e.g., data exfiltration).
- Recommended Mitigation Strategies:
    - SYN Cookies: Enable `SYN` cookies on the server to handle connections without reserving resources.
    - Rate Limiting: Restrict the number of `SYN` packets per second from a single IP.
    - Firewall Rules: Block traffic from malicious IPs (e.g., `203.0.113.0`) and use intrusion detection systems (IDS).

    - DDoS Protection: Deploy cloud-based DDoS mitigation services to absorb large-scale attacks.
    - Network Monitoring: Implement real-time alerts for unusual traffic spikes.
- Conclusion:

The SYN flood attack exploited the TCP handshake’s design to overwhelm the server, causing widespread service disruption. Immediate implementation of SYN cookies and traffic filtering can restore stability and prevent future incidents.