Cybersecurity Incident Report -

Denial of Service (DoS) Attack

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**, specifically a **SYN Flood attack**. The logs show that: ● Multiple SYN packets were sent from the IP address `203.0.113.0` to the web server (`192.0.2.1`) on port **443 (HTTPS)**. ● The server responded with SYN-ACKs, but no **final ACK** was received, indicating an incomplete handshake. ● A high number of **RST (Reset) packets** were sent by the server to various clients, suggesting excessive connection failures. ● A **504 Gateway Timeout** error was recorded, indicating the server was unable to process requests in a timely manner. This event could be: ● A **SYN Flood DoS attack**, where an attacker sends a massive number of SYN packets to exhaust the server's resources. ● A potential precursor to a **Distributed Denial of Service (DDoS) attack**, where multiple IPs would be involved. ● An **aggressive network scan** or misconfigured client flooding the server with connection attempts.

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. The three steps of the handshake are:

1. **SYN (Synchronization):**
    - The client sends a **SYN** packet to the server to initiate a connection.
2. **SYN-ACK (Synchronization-Acknowledgment):**
    - The server responds with a **SYN-ACK** packet, acknowledging the request.
3. **ACK (Acknowledgment):**
    - The client sends an **ACK** packet, completing the handshake, and communication begins.

When a malicious actor sends a large number of SYN packets all at once:

- The server allocates memory and resources to track each incoming SYN request.
- If the attacker **never responds with an ACK**, the server keeps these half-open connections in its queue.
- When the queue is full, the server **cannot accept new legitimate connections**, causing delays and failures.
- The system may eventually **crash or become unresponsive**, leading to **timeouts (504 errors)** and connection resets.

The logs indicate that:

- The server is receiving SYN packets without completing the handshake.
- **Numerous RST packets** suggest the server is overwhelmed and rejecting connections.
- **504 errors show degraded performance**, meaning legitimate users cannot access the website.

Conclusion & Next Steps:

This is a **suspected SYN Flood DoS attack**. To mitigate the impact, the following steps should be taken:

- **Enable SYN cookies** to prevent resource exhaustion.
- **Implement rate limiting** to restrict the number of SYN packets from a single IP.
- **Block suspicious IPs** at the firewall.
- **Monitor for potential DDoS escalation** and deploy mitigation strategies if necessary.