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 is flooded with an overwhelming number of SYN requests and hence is unable to respond to genuine SYN requests.
After investigating the Wireshark TCP/HTTP log it is known that:

1. The protocol used is TCP
2. Initially, the attacker's SYN request gets responded normally by the web server (log items 52-54).
3. However, the attacker (IP: 203.0.113.0) keeps sending more SYN requests. After sending an overwhelming number of SYN requests to the web server - the log begins to reflect the struggle the web server has to keep up with the rapid pace of the SYN requests.
4. The attacker sends several SYN requests every second. After a while the server fails to respond even to legitimate employee website visitors.

This is the SYN Flood attack and it is a direct DoS attack since there is single device used for the attack as indicated by the IP address.

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. Client **->** [SYN] packet **-->** server
   The client sends SYN requests to the server which is the first step in a TCP handshake process. SYN = Synchronise
2. Client **<-** [SYN, ACK] packet **<-** Server
   The server then responds to the client with SYN/ACK. This indicates that the server has agreed to connect. SYN/ACK = Synchronize acknowledge
3. Client **->** [ACK] packet **->** Server
   The Client then sends an ACK packet acknowledging the permission for connection. ACK = Acknowledge

When malicious actor tries a SYN flood attack:

A malicious actor sends multiple SYN packets to the server, the server - assuming all are genuine requests to connect - tries to respond to each request with the SYN/ACK packet. But soon in this attack, since there is a deliberate attempt to overwhelm the server with SYN requests, the server gets flooded with requests larger than available resources to handle such requests. This renders the server unable to respond.

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

The server once overwhelmed with too many SYN requests is unable to respond and unable to service any requests.The logs indicate that initially when an attacker sends the SYN request it is treated like a normal SYN request and responded with SYN-ACK. Soon the attacker bombards the server with SYn requests rendering the web server overwhelmed resulting in a situation where it cannot respond to any request.

There are two types of error responses we can see after server is unable to respond due to the SYN flood attack

1. HTTP/1.1 504 Gateway Time-out (text/html) error message
    a. The gateway server that was waiting for a response from the web server sends this message.
    b. If the web server takes too long to respond, the gateway server sends a timeout error message to the requesting browser.
2. [RST, ACK] packet
    a. This is sent to the requesting client, if the [SYN, ACK] packet is not received by the web server.
    b. RST,ACK stands for reset, acknowledge.
    c. The client receives a timeout error message in their browser and the connection attempt is dropped.
    d. The visitor can refresh their browser to attempt to send a new SYN request.