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 logs show that: There is a large number of TCP SYN requests coming from an unfamiliar IP address. This appears to be overwhelming the web server due to the large volume of incoming traffic. The attacker SYN request is initially answered normally, however multiple requests keep coming in, which is abnormal. At this point the web server can still respond to requests, but as more and more packets keep coming in from the same source, the log begins to show signs of struggle. The attacker is sending several SYN requests every second, and log entries (highlighted in yellow = failed) are appearing. These yellow entries contain errors in the info column. I.e HTTP/1.1 504 Gateway Time-out (text/html). Generated by a gateway server that was waiting for a response from the web server, but it took too long to respond. The second error is shown as [RST, ACK] packet, which would be sent to the requesting visitor if the [SYN, ACK] packet is not received by the web server. The visitor would then receive a timeout message in their browser.

This event could be: This is a SYN flood attack - A type of DoS attack that simulates a TCP connection and floods a server with SYN packets.

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. First the [SYN] packet is initially requested, in this case from an employee trying to connect to the web page. SYN means synchronize.

2. Next, indicated by [SYN, ACK] this packet is the web server's response to the visitor's request agreeing to the connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for synchronize and acknowledge.

3. In this final part of the log entry, [ACK] packet is the visitor's machine acknowledging the permission to connect, and is the final step needed to make a successful TCP connection.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: Malicious actors take advantage of the TCP protocol by sending a large number of SYN packet requests, flooding the server. If this number is greater than the server resources available, the server can become overwhelmed and unable to respond to the requests.

Explain what the logs indicate and how that affects the server: The log shows that as the initial SYN packet flooding began, traffic was still able to send but things worsened as more and more SYN packet requests came in, overwhelming the server. More and more entries went to red status. We started to see two kinds of errors in the info column of the log: HTTP/1.1 504 Gateway Time-out (text/html) & [RST, ACK], which indicate time out errors. As there is only one IP address attacking the web server (203.0.113.0) we can assume this is a DoS, SYN flood attack, and not a DDoS. The website is taking a long time to respond/load and is reporting a connection time out error due to the overwhelming number of SYN packet requests. The consequences of this attack would be:

Service disruption & Downtime
Financial losses
Reputational Damage
Resource Exhaustion

Overall this attack poses a significant threat to availability, integrity, and confidentiality of the organisations IT infrastructure and data.

Some recommended preventions:

Use a VPN tunnel to encrypt network traffic.
Ensure use of HTTPS: https uses ssl/tls protection.
NGFW (Next-gen firewall) enhanced security capabilities.