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: that the TCP handshake is unable to be completed, so a connection cannot be established with the web server. The logs show that: several SYN packets are being sent per second from a single IP address. The server's ability to respond to legitimate employee requests slows and then halts as the server becomes overwhelmed with SYN packets. This event could be: A direct DoS SYN flood attack.

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. The [SYN] packet is initially sent from the employee visitor to the web server, requesting to form a connection. 2. The web server responds with a [SYN, ACK] packet consenting to forming the connection. The destination reserves resources for the source to connect. 3. The employee visitor’s machine acknowledges the permission to connect with a final [ACK] packet. Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a greater number of SYN requests than the server can handle, the server becomes overwhelmed and unable to respond to requests, including requests from legitimate sources, leading to slowed or even halted network traffic. No server resources are available for legitimate TCP connection requests because the server has tried to reserve all its resources for the flood of connection requests. Explain what the logs indicate and how that affects the server: The logs indicate that the attacker’s initial SYN request is answered normally by the server, and the server is able to respond to an employee’s legitimate request. However, as the number of SYN requests sent by the attacker increases, the web server struggles to address the large number of rapidly

arriving SYN requests as the attacker is sending several SYN requests per second. The logs show HTTP/1.1 504 Gateway Time-out error messages and [RST, ACK] packets, indicating that the web server is taking so long that the gateway server times out and that the [SYN, ACK] packet is not being received by the web server, causing a timeout error message in the browser. Eventually, the overwhelmed server stops responding to legitimate employee traffic, and more error messages are received indicating that a connection cannot be established or maintained with the web server. The organization's website cannot function. Potential consequences of this attack are loss of clients to competitors and reputational damage. Clients may not trust a company that has been successfully victimized by a malicious actor, and if employees are unable to search for vacation packages for customers while the server is down, customers may take their business elsewhere. One way to secure the network against this type of attack is to distribute network operations across hosts that can be dynamically scaled so that even if one server is overwhelmed, other servers are able to support continued network operations.