Cybersecurity Incident Report

Link to material: How to read a Wireshark TCP/HTTP log - Google Docs

Section 1: Identify the type of attack that may have caused this network interruption
The TCP/HTTP logs indicate that a single IP address is sending a very large number of SYN packets to the web server. This large amount of SYN packets being sent to the web server is most likely the cause of the problems with the company website. Because these SYN packets are being sent from a single IP address, the web server is most likely experiencing a SYN flood attack from a malicious actor using this IP address.

Section 2: Explain how the attack is causing the website to malfunction
When a website visitor attempts to establish a connection with the web server, a three-way handshake takes place using the TCP protocol. In the first step of the handshake, the visitor's computer sends a SYN packet requesting a connection to the web server. In the second step, the web server will respond with a SYN-ACK packet back to the requesting computer if the web server has open ports and is able to accept the connection. Finally, after receiving the SYN-ACK packet, the requesting computer will send an ACK packet to the web server and the connection is established. In this case, the malicious actor is sending an abnormally large number of SYN packets to the web server in a short amount of time from a single IP address. This is known as a SYN flood attack, a type of denial of service (DOS) attack that disrupts a server or network by flooding it with SYN packets. When a malicious actor sends this large number of SYN packets to a web server, the server will attempt to complete the handshake process for each SYN packet. Because there are so many SYN packets being sent in a very short period of time, the server is not able to keep up and becomes very slow or crashes altogether. The result is what we are now experiencing with the timeout error message. The server is attempting to complete the handshake process for the high number of SYN packets that have been sent and loses the ability to respond to other new SYN packets that are being sent from other IP addresses in a timely manner. Because of this, employees and clients are not able to access the company website, disrupting business operations. In an attempt to stop this SYN flood attack, we have shut down the web server to give it a chance to recover and have configured the firewall to block any SYN packets being sent from the IP address that the malicious actor was using. However, this is only a temporary solution since the malicious actor can simply use a different IP address. Some steps that we can take to prevent this attack from continuing would be to first configure our firewall to block any SYN packets from suspicious IP addresses. Furthermore, we can use rate limiting to limit the number of

incoming connections from a single IP address. In doing so, we can prevent any single IP address from sending a very high number of SYN requests to the web server. :