Cybersecurity Incident Report

Prepared by: Security Analyst
Date: [Insert Date]
Affected System: Company sales web server (192.0.2.1)

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. Wireshark logs show the web server being flooded with an abnormally large number of TCP SYN packets from a single external IP address, 203.0.113.0, starting a few seconds into the capture and continuing steadily for the rest of the find. Because all of the flooding traffic comes from one source rather than many distributed sources, this is a DoS attack rather than a distributed Denial of Service (DDoS) attack. Along with the excessive SYN traffic, the logs never show that attacking IP completing the final acknowledgment step of the TCP handshake, which indicates specifically to a SYN flood, a common type of DoS attack. As the flood continues, the server begins failing to respond to legitimate visitors, sending connection resets and eventually a 504 Gateway Time-out, until it stops accepting new legitimate connections altogether.

Section 2: Explain how the attack is causing the website malfunction
When a website visitor tries to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. First, a SYN packet is sent from the source to the destination, requesting to connect. Second, the destination answer back with a SYN-ACK packet to accept the request and reserves resources in memory for that connection. Third, the source sends a final ACK packet, completing the handshake and opening the connection. In a SYN flood attack, a malicious actor sends a large number of SYN packets without ever sending the final ACK. Each of these incomplete requests still causes the server to reserve resources and hold the connection open while it waits for a response that never comes. The logs confirm this pattern: the attacking IP address repeatedly sent SYN packets that were never followed by a completing ACK, while legitimate employees and customers in the 198.51.100.0/24 range were initially able to complete handshakes and load the sales page normally. As the volume of fraudulent SYN requests grew, the server's pool of available connection resources became exhausted holding open connections for the attacker that would never be completed. With no resources left to reserve, the server could no longer respond to new SYN requests from legitimate visitors, so their browsers received a connection timeout error, and at least one in-progress legitimate session failed with an HTTP 504 Gateway Time-out. In short, the server was not hacked or breached — its capacity to accept new visitors was consumed entirely by fake, partially open connections from the attacker. If left unresolved, this type of service disruption risks lost sales, reduced customer trust, and staff time spent responding to future recurrences, since blocking one IP address is only a temporary fix an attacker could bypass by spoofing new source addresses. Longer-term, the risk can be reduced by enabling SYN cookies so the server does not reserve resources until a connection is verified, adding rate limits on incomplete connections per source IP at the firewall, and considering a cloud-based DDoS protection service to filter this kind of traffic before it reaches the server.