# 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 indicating that the web server was subjected to a SYN flood attack. This type of attack involves overwhelming the server with a high volume of TCP SYN requests, which are the initial step in establishing a TCP connection. The logs show a large number of SYN requests originating from a single IP address (203.0.113.0), with very few completed TCP handshakes. The rapid succession of these SYN requests prevents legitimate users from completing their connections to the server. This event could be a Denial of Service (DoS) attack, specifically a SYN flood attack, designed to exhaust server resources by saturating the connection queue with half-open connections.  When determining what type of attack occurred, several questions are important to consider. First, understanding network attacks is crucial. Network attacks are malicious activities aimed at compromising, disrupting, or gaining unauthorized access to network resources. They can be executed in various forms, including but not limited to Denial of Service (DoS), Distributed Denial of Service (DDoS), phishing, man-in-the-middle attacks, and malware dissemination. Each type of attack has unique characteristics and methodologies, but the ultimate goal is often to disrupt services, steal data, or cause harm to the targeted network or systems.  Given the symptoms described in the scenario, the type of attack likely responsible is a Denial of Service (DoS) attack. Specifically, the SYN flood attack is a type of DoS attack that fits the observed symptoms and log data. The difference between a denial of service (DoS) and distributed denial of service (DDoS) attack lies in their execution. A DoS attack originates from a single source, such as one computer or network, and aims to overwhelm a server or network with a flood of requests, leading to resource exhaustion and service unavailability. In contrast, a DDoS attack involves multiple sources, often distributed across various locations, all targeting a single server or network simultaneously. The distributed nature of the attack makes it more challenging to mitigate, as it increases the volume of traffic and can evade simple filtering mechanisms.  The website is taking a long time to load and reporting a connection timeout error because the server is overwhelmed with an excessive number of SYN requests from the attacker. These requests occupy the server's resources, leaving it unable to respond to legitimate user requests. As the server’s connection queue fills up with half-open connections that never complete, it cannot process new connections efficiently, resulting in delays and timeout errors for users trying to access the site. By analyzing the logs and understanding the nature of the SYN flood attack, it becomes clear that this specific type of DoS attack is responsible for the current network interruption and the website's poor performance. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| A SYN flood attack is characterized by an attacker sending a succession of TCP/SYN packets to a target’s system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. The main symptoms of a SYN flood attack include a significant increase in the number of incomplete TCP connections, network congestion, and severe degradation in the performance of the targeted system. Specifically, the server’s connection table is overwhelmed with half-open connections, which prevents new connections from being established.  This SYN flood attack severely impacted the organization’s network by overloading the web server’s connection handling capacity. The server, inundated with a massive number of SYN requests, could not keep up with legitimate connection attempts. Consequently, legitimate users experienced significant delays, with the website taking an unusually long time to load, and many users faced connection timeout errors. This disruption hampered normal business operations, affected user experience, and potentially led to a loss of customer trust and revenue.  The potential consequences of a SYN flood attack on the organization are extensive. Firstly, the immediate impact is the disruption of service, leading to a poor user experience and potential loss of customers. The downtime and degraded performance can result in lost sales and damage to the organization’s reputation. Additionally, the resources required to mitigate the attack and restore normal operations can be significant, both in terms of time and cost. In some cases, prolonged attacks can lead to data corruption or loss, and sensitive information might be exposed if the attacker gains deeper access to the network. The overall trust and credibility of the organization can be compromised, leading to long-term financial and operational repercussions.  To prevent future SYN flood attacks and enhance network security, the organization can implement several measures:   * Firewall and Intrusion Detection Systems (IDS): Use advanced firewalls and IDS/IPS (Intrusion Prevention Systems) to detect and block abnormal traffic patterns indicative of SYN flood attacks. * Rate Limiting: Implement rate limiting on the server to control the number of incoming SYN requests from a single IP address. * SYN Cookies: Configure the server to use SYN cookies, a technique that allows the server to handle more SYN requests without allocating resources for each half-open connection. * Load Balancers: Deploy load balancers to distribute traffic evenly across multiple servers, thus reducing the impact on a single server. * Network Redundancy: Design the network with redundancy to ensure that if one server is attacked, others can take over its load. * Regular Security Audits: Conduct regular security audits and update systems to ensure they are protected against the latest threats.   By understanding the attack’s nature and implementing robust security measures, the organization can significantly reduce the risk of future disruptions and protect its network infrastructure. |