Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| Based on the information provided, the network interruption was likely caused by a Distributed Denial of Service (DDoS) attack. The large number of TCP SYN requests coming from an unfamiliar IP address and overwhelming the web server's ability to respond is a common tactic used in DDoS attacks. The attacker sends a flood of SYN requests to the targeted server with fake or spoofed IP addresses, which consumes server resources and ultimately leads to a denial of service for legitimate users. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| It is possible that the attack caused the website to malfunction by overwhelming the website's servers with a high volume of traffic or requests, known as a distributed denial-of-service (DDoS) attack. This flood of traffic can cause the server to become overloaded and unable to respond to legitimate requests, resulting in slow or unresponsive website performance or even a complete outage.  Another possibility is that the attack may have involved the injection of malicious code or software onto the website's servers or network, such as a virus or malware. This could cause the website to display unexpected or incorrect information, or to redirect users to malicious websites or phishing pages.  In either case, the attack can cause significant disruption to the website's normal operations, leading to decreased functionality and user experience, and potentially even loss of data or sensitive information.  There are several potential ways to secure the network and prevent similar attacks in the future. Here are some suggestions:  Use a Web Application Firewall (WAF): A WAF can protect the website against various types of attacks, including SQL injection and cross-site scripting. It can detect and block malicious traffic before it reaches the web server.  Implement SSL/TLS: SSL/TLS can encrypt the communication between the web server and the client, preventing eavesdropping and tampering.  Keep the software up to date: It's important to keep the web server software and its components up to date with the latest security patches. This will ensure that known vulnerabilities are addressed and the system is protected against known attacks.  Implement strong authentication: Strong authentication mechanisms such as two-factor authentication can help prevent unauthorized access to the system.  Conduct regular security audits: Regular security audits can help identify vulnerabilities and weaknesses in the system, allowing the organization to address them before they can be exploited by attackers.  Educate employees: Employees should be educated on how to identify and report suspicious activities and be aware of basic security practices such as strong passwords, avoiding suspicious emails, and not sharing login credentials.  By implementing these measures, the organization can significantly reduce the risk of a similar attack occurring in the future. |