# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| After conducting an analysis of the network interruption, it seems that the website malfunction is likely the result of a deliberate and targeted Distributed Denial of Service attack. This type of attack involves a coordinated effort to overload the website's servers and infrastructure with an enormous amount of traffic. Typically, attackers create a network of compromised devices, known as a botnet, which is then used to generate a massive influx of requests that overwhelms the website's resources. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| The DDoS attack has disrupted the normal functioning of the website by flooding it with an abnormally high volume of traffic. This flood of traffic places an immense burden on the website's infrastructure, including servers, routers, and network bandwidth. As a result, the website is unable to handle legitimate user requests efficiently, leading to slow loading times, timeouts, or even complete unavailability.  The attack works by exploiting the website's limited resources, such as CPU, memory, and network capacity, through the simultaneous submission of an overwhelming number of requests. This resource saturation prevents the website from effectively processing genuine user traffic, causing a significant degradation in service quality or a complete breakdown of the site's functionality.  Moreover, the DDoS attack may employ various tactics to further amplify the website's malfunction. For instance, the attackers may utilize IP spoofing techniques to conceal the true source of the attacking traffic, making it challenging to identify and block specific IP addresses. Additionally, they may employ different types of DDoS attacks, such as volumetric attacks that inundate the network with an enormous volume of traffic or application-layer attacks that exploit vulnerabilities in the website's software or infrastructure.  The combined impact of the overwhelming traffic, resource exhaustion, and potential exploitation of vulnerabilities contribute to the severe performance degradation or complete unavailability of the website, ultimately resulting in the observed network interruption. |