# 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 show that: on-attack ip spoofing  This event could be:exploit customers personal details | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:  1.syn  2. syn-ack  3.ack  Explain what happens when a malicious actor sends a large number of SYN packets all at once:the server will consume lots of bandwidth and make it slow  Explain what the logs indicate and how that affects the server:the server will crash and shutdown |
| * What do you currently understand about network attacks?   Middleman attack  Replay attack  Smurf attack   * Which type of attack would likely result in the symptoms described in the scenario? Middleman attack * What is the difference between a denial of service (DoS) and distributed denial of service (DDoS)? Direct or single device on dos on the other hand the ddos have multiple devices on different location so its hard to find * Why is the website taking a long time to load and reporting a connection timeout error?because someone was meddling with dns and because of flood of syn it makes the server crash and consume lots of bandwidth and it could lead to shutdown of dns server |

Review the Wireshark reading from step 2, then write your analysis in section two of the Cybersecurity incident report template provided.

When writing your report, discuss the network devices and activities that are involved in the interruption. Include the following information in your explanation:

* Describe the attack. What are the main symptoms or characteristics of this specific type of attack? Syn attack
* Explain how it affected the organization’s network. How does this specific network attack affect the website and how it functions? This attack can make the server to load long due to lots of request on server
* Describe the potential consequences of this attack and how it negatively affects the organization. It could lead to crash of website and the server could shutdown
* *Optional:* Suggest potential ways to secure the network so this attack can be prevented in the future. firewall

Solution:

# Activity Exemplar: Analyze network attacks

| **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 DoS attack. The logs show that the web server stops responding after it is overloaded with SYN packet requests. This event could be a type of DoS attack called SYN flooding. |

| **Section 2: Explain how the attack is causing the website malfunction** |
| --- |
| When the website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The handshake consists of three steps:   1. A SYN packet is sent from the source to the destination, requesting to connect. 2. The destination replies to the source with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect. 3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect.   In the case of a SYN flood attack, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server’s available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests.  The logs indicate that the web server has become overwhelmed and is unable to process the visitors’ SYN requests. The server is unable to open a new connection to new visitors who receive a connection timeout message. |