Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
This attack is a SYN flood attack. The attacker is sending too many SYN requests in a TCP connection for the host server to acknowledge, using up all its resources.

Section 2: Explain how the attack is causing the website to malfunction
This attack is causing the website to malfunction by flooding the server with SYN requests which it does not have the capacity to acknowledge. When too many requests are received the server cannot respond to genuine requests as it is still trying to acknowledge all of the disingenuous requests.

Section 1: Identify the type of attack that may have caused this network interruption

- What do you currently understand about network attacks? - network attacks occur when attackers overload a network or system on a network by sending unwanted traffic. A common type of network attack is known as a DoS attack.
- Which type of attack would likely result in the symptoms described in the scenario? - This scenario is typical of a SYN flood attack.
- What is the difference between a denial of service (DoS) and distributed denial of service (DDoS)? - A DoS attack is carried out on a smaller scale than a DDoS attack. A DDoS attack is much harder to detect/source as the attacks can be coming from many systems / networks of systems around the world.
- Why is the website taking a long time to load and reporting a connection timeout error? - The server running the website does not have the capacity to process all of the incoming requests and is slowing down as a result. This in turn slows down normal requests and produces timeout errors.

Section 2: Explain how the attack is causing the website to malfunction

- Describe the attack. What are the main symptoms or characteristics of this specific type of attack? - The attack consists of an attacker initiating a TCP connection with the host server, contained within the TCP connection is a flood of SYN requests. The host server is not able to acknowledge all of the requests and uses up its resources causing it to malfunction.
- Explain how it affected the organization's network. How does this specific network attack affect the website and how it functions? - This attack affected the organisation's network by slowing down genuine requests due to insufficient resources.
- Describe the potential consequences of this attack and how it negatively affects the organization. - This type of attack has the potential to affect the organisation financially as it slows down their normal business operations. It could also affect their reputation because if attacks like this keep happening, they could be known for their lack of security and users might be hesitant to use their online services.
- *Optional:* Suggest potential ways to secure the network so this attack can be prevented in the future. -