# SYN Flood: Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| The attack was noticed when our monitoring system sent an alert about a problem with the web server. Now, when you try to visit the company’s website, it just shows a connection timeout error.  Using Wireshark, a cybersecurity analyst found that a huge number of TCP SYN requests were coming from an unknown IP address. At first, the server could handle these requests and keep working, but eventually, the server got overloaded and couldn’t respond to real users.  This seems to be a Denial of Service (DoS) SYN flood attack. Since the requests are only coming from one IP address, it isn’t a Distributed Denial of Service (DDoS) attack yet, where multiple devices are used. The large number of SYN requests has now overwhelmed the server, stopping it from handling normal traffic, which is why anyone trying to access the site gets a connection timeout. |
|

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

**A SYN flood attack happens when an attacker misuses the process of connecting to a server. They send a lot of connection requests, but the server only has a limited number of ports to handle them. The attacker's goal is to overwhelm the server by sending more requests than it can handle.**

**At first, this will make the network slow down, causing long loading times for users. Eventually, the server becomes overloaded and stops working completely.**

**The effects of this attack include losing money because the server can't handle normal business, losing customer trust, and possibly harming the server or its data.**

**To prevent these kinds of attacks, you can:**

**1. Use a Next Generation Firewall (NGFW) to watch for suspicious activity.**

**2. Use VPNs and encryption to hide the web server’s IP address.**

**3. Divide the network into subnets so that if one part fails, the whole system isn't affected.**