# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| Using a packet sniffer, the server log shows that there is a DoS attack. The logs show that the TCP protocol is being abused using a SYN flood attack by a malicious actor from outside the company (because the source IP address of the actor is not in the range for internal IP addresses from authorized groups). It appears that it is a DoS attack and not a DDoS attack because the malicious SYN requests are from a single IP address. The abnormal amount of requests is making the website slower at dealing with real/productive requests. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| The website is unable to be accessed due to a high volume of network traffic. Most of this network traffic is from SYN requests, which are the initial requests to set up a TCP connection. As these flood the website, it is too busy dealing with all the requests from this one source, and unable to deal with legitimate SYN requests for business operations. Since people with authorized access are unable to use the website, this leads to a loss of time and company resources with no productivity. Inability to fix this issue will lead to longer downtime and further monetary losses. To prevent this from happening again, there should be a firewall feature which locks out users from accessing the website if they send too many requests in a short amount of time. For further security, the firewall could also only allow requests from certain IP addresses or networks reach the server. |