# Cybersecurity Incident Report

|  |
| --- |
| **Session 1: Identify the type of attack that may have caused this**  **network interruption** |
| A possible direct DoS attack of SYN flood is overloading the web server, making it impossible to access the pages of the company's website.  Site visitors, including employees, are unable to connect to the pages, receiving a **timeout** error message, which indicates that the gateway server has not received a response from the web server. After analysis of the log record it was identified that a single IP address is flooding the web server with more SYN requests than it can handle, this explains the overload and the inability to respond effectively to the gateway server and visitors. |
|

|  |
| --- |
| **Session 2: Explain how the attack is causing the website to malfunction** |
| After receiving a monitoring alert indicating a problem with the web server, the security team tried to access the company's website and was unable to do so, receiving a **timeout** error message.  A packet sniffer was used to capture data packets and log analysis showed that:   * A single IP address was sending a large number of TCP SYN requests in a very short space of time. * The information from legitimate visitor requests contained the error message *HTTP/1.1 504 Gateway Time-out (text/html)* indicating that the gateway server was not getting response from the web server and [RST, ACK] packets because the web server was not receiving its sent [SYN, ACK] packets.   These facts justify the overloading of the web server and become strong indications that it is a direct DoS attack of SYN flood.  The server has been taken offline temporarily so that it can recover and return to normal operations, the firewall has also been configured to block the IP address that was sending the TCP SYN requests.  As it is a company in the service sales segment, with a focus on travel promotions, the suspension of access to the site can cause loss of customers, who in many cases need this type of service urgently, going to seek the service in other companies. Employees do not have access to the website, where they search for the best deals for customers, can also lose clients with this inaccessibility. |