# 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: **An abnormal number of SYN requests are flooding the web server every second causing failed communications between legitimate employee website visitors and web servers.**  The logs show that: **There’s an abnormally high number of SYN requests flooding the web server, an HTTP/1.1 504 Gateway Time-out error message, a [RST, ACK] Reset and acknowledge packet.**  This event could be: **direct DoS SYN flood attack** |
|
|  |

|  |
| --- |
| **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 (Synchronize): Client sends a SYN packet to server to initiate a connection**   **2. SYN-ACK (Synchronize-Acknowledge): Server responds with SYN-ACK packet to acknowledge request**  **3. ACK (Acknowledge): Client sends an ACK packet back to the server, confirming connection is established.**  Explain what happens when a malicious actor sends a large number of SYN packets all at once:   * **Web server struggles to keep up with abnormal number of SYN requests b/c several SYN requests are sent every second** * **Web server stops responding to legitimate traffic and stops responding** * **Visitors receive more error messages indicating they cannot establish/maintain connection to web server**   Explain what the logs indicate and how that affects the server:   * **SYN requests are flooding (in red) in the next 20 lines which shows web server stops responding to legitimate employee visitor traffic** * **HTTP/1.1 504 Gateway Time-out (text/html) error message: generated by gateway server saying that the web server took too long to respond** * **[RST, ACK] packet sends out timeout error message to visitor in their browser and connection attempt is dropped** |