Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
Uma análise dos logs do Wireshark identificou, em meio aos acessos de usuários autênticos à página web, um IP específico, localizado fora da rede interna, que realizou diversas requisições ao servidor em um curto período de tempo (alguns segundos) até que ele parasse de responder apropriadamente. Esse caso se refere a um ataque de DoS SYN flood.

Section 2: Explain how the attack is causing the website to malfunction
O ataque de DoS SYN Flood prejudica o acesso ao site pois, durante sua execução, são enviadas múltiplas e rápidas requisições ao servidor web. Isso inicia diversos processos de *three-way handshake* (com pacotes SYN) que forçam o servidor a responder (com SYN-ACK) e aguardar uma conclusão (o pacote ACK final). Como esse ACK nunca é enviado pelo atacante, as conexões permanecem em um estado “meio-aberto”. Inicialmente, o servidor tenta responder, mas conforme o número de conexões pendentes excede os recursos disponíveis, ele começa a demorar para responder a usuários legítimos (causando um erro de *Time-out*) até não conseguir mais e parar de funcionar. Esse ataque fere a disponibilidade, um dos princípios da tríade CIA, e pode trazer prejuízos financeiros à organização se não resolvido em tempo hábil, e, principalmente, prevenido, para que não ocorra mais vezes futuramente. Sugestões para evitá-lo são a implementação de SYN Cookies no servidor e, caso haja viabilidade orçamentária, a contratação de um serviço de proteção DDoS/WAF.