Scenario

I work as a security analyst for a travel agency that promotes sales and promotions on the company's website. Employees regularly access the company's sales page to search for vacation packages that may interest their clients.

One afternoon, I receive an automated alert from my monitoring system indicating a problem with the web server. I try to visit the company's website but receive a connection timeout error message in my browser.

I use a packet sniffer to capture the data packets in transit to and from the web server. I notice a large number of TCP SYN requests coming from an unknown IP address. The web server seems overwhelmed by the incoming traffic volume and loses its ability to respond to the abnormally high number of SYN requests. I suspect that the server is being attacked by a malicious actor.

I decide to temporarily take the server offline to allow it to recover and return to its normal operational state. I also configure the company's firewall to block the IP address that was sending the abnormal amount of SYN requests. I am aware that this IP blocking solution will not last long, as an attacker can spoof other IP addresses to bypass this block.

I need to quickly alert my supervisor about this issue and discuss the next steps to stop this attacker and prevent this problem from happening again. I must be prepared to report to my boss about the type of attack I discovered and how it was impacting the web server and employees.