Scene
You work as a security analyst for a travel agency that advertises sales and promotions on the company's website. Company employees regularly access the company's sales website to research vacation packages their clients might like. One afternoon, you receive an automatic alert from your monitoring system indicating a problem with the web server. You attempt to visit the company's website but receive a connection timeout error message in your browser. You use a packet sniffer to capture data packets in transit to and from the web server. You notice a large number of TCP SYN requests from an unknown IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally high number of SYN requests. You suspect the server is being attacked by a malicious actor. You temporarily take the server offline so the machine can recover and return to a normal operating state. You also configure the company's firewall to block the IP address that was sending the abnormal number of SYN requests. You know your IP blocking solution won't last long, as an attacker can spoof other IP addresses to bypass it. You need to quickly alert your boss about this problem and discuss the steps to take to stop this attacker and prevent this problem from happening again. You'll need to be prepared to tell your boss the type of attack you discovered and how it was affecting the web server and employees. **Christian Danglades**