# Cybersecurity Incident Report: IP spoofing(smurf possibily)

|  |
| --- |
| **Problem**: The company's web server is under attack, causing a connection timeout error on the website. |
| **Solution**: You use a packet sniffer to capture data packets and identify a large number of TCP SYN requests from an unfamiliar IP address. You take the server offline, block the IP address, and plan to inform your manager. |
| **Goal**: Analyze the attack, mitigate the issue, and communicate effectively with your manager. |

**Questions**  
  
What do you currently understand about network attacks?

**IP Spoofing:** Malicious actions or activities aimed at exploiting vulnerabilities in a network to compromise its security, disrupt services, steal information, or gain unauthorized access.  
Which type of attack would likely result in the symptoms described in the scenario?

**TCP SYN Flood Attack:** A malicious actor sends a large number of SYN requests to the target server, causing it to be unable to respond to legitimate connection requests and leading to service interruption.  
What is the difference between a denial of service (DoS) and distributed denial of service (DdoS)?  
**DoS attack**, a single source or a few sources flood the target with traffic, overwhelming its resources and causing service disruption.   
**DDoS attack**, multiple compromised devices, often part of a botnet, coordinate to flood the target with traffic, making it more difficult to mitigate and resulting in a more widespread and severe impact.  
  
Why is the website taking a long time to load and reporting a connection timeout error?

TCP SYN Flood Attack. In this attack, the web server is flooded with a large number of incomplete connection requests (SYN packets) from the attacker

|  |
| --- |
| TCP 3 way handshake |
| 1. SYN (Synchronize) Request: The client sends a SYN packet to the server, requesting a connection. |
| 2. SYN-ACK (Synchronize-Acknowledge) Response: The server responds with a SYN-ACK packet, acknowledging the request and reserving resources for the connection. |
| 3. ACK (Acknowledgment) Request: The client sends an ACK packet to the server, confirming the connection establishment. |

|  |  |
| --- | --- |
| This event could be: | Explain what the logs indicate and how that affects the server: |
| A coordinated attempt by a malicious actor to overwhelm the web server with SYN requests, known as a SYN Flood attack. | The logs indicate a high volume of incoming SYN requests from the unfamiliar IP address. This influx of SYN packets consumes the server's memory and processing capacity, leading to resource exhaustion. As a result, the server becomes unresponsive to legitimate connection requests, causing the website to malfunction and resulting in connection timeout errors for users. |