**Analyze Network Attacks**

**Scenario:**

You work as a security analyst for a travel agency that advertises sales and promotions on the company’s website. The employees of the company regularly access the company’s sales webpage to search for vacation packages their customers might like.

**One afternoon, you receive an automated alert from your monitoring system indicating a problem with the web server**. You attempt to visit the company’s website, but you 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 coming from an unfamiliar 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 large number of SYN requests. You suspect the server is under attack by a malicious actor.

**You take the server offline temporarily so that the machine can recover and return to a normal operating status.** **You also configure the company’s firewall to block the IP address that was sending the abnormal number of SYN requests.** You know that your IP blocking solution won’t last long, as an attacker can spoof other IP addresses to get around this block. You need to alert your manager about this problem quickly and discuss the next steps to stop this attacker and prevent this problem from happening again. You will need to be prepared to tell your boss about the type of attack you discovered and how it was affecting the web server and employees.

[**Wireshark TCP/HTTP log**](https://docs.google.com/spreadsheets/d/1enpRzrIao3J2Lp2tOI0hmu1Cu7D7CjLGhFAiTiR9J64/template/preview)

**CISCO TRAVELS**

**Cybersecurity Incident Report**

**Scenario:**

On July 31st, the security team at Cisco Travels received an automated alert from our monitoring system indicating a problem with the web server. Our team attempted to make a visit to the company’s website but received a connection timeout error message in our browser. We used Wireshark to capture data packets in transit to and from the company’s web server. We noticed a large number of TCP SYN requests coming from an unfamiliar IP Address.

This is indicative of the server appearing to be overwhelmed by the volume of incoming traffic and is facing difficulties responding to the large number of SYN requests. As a remedial measure, we first took the server offline so that the machine could recover and return to normal operating status. We also configured the company’s firewall to block the IP address that was sending the abnormal number of SYN requests. The efficacy of this measure is, however, questionable, as attackers could spoof other IP addresses to get around the block.

**Type of Attack:**

One potential explanation for the website’s connection timeout error message is a DoS attack. The logs show that the web server stops responding after it is overloaded with SYN packet requests. This event could be a type of Denial of Service (DoS) attack called SYN flooding.

**Effects of Attack:**

When the website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The handshake consists of three steps:

1. A **SYN packet** is sent from the source to the destination, requesting to connect.
2. The destination replies to the source with a **SYN-ACK packet** to accept the connection request. The destination will reserve resources for the source to connect
3. A final **ACK packet** is sent from the source to the destination acknowledging the permission to connect.

During a SYN flood attack, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server’s available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests.

The logs indicate the web server has become overwhelmed and is unable to process the visitors’ SYN requests. The server is unable to open a new connection who receive a connection timeout message.