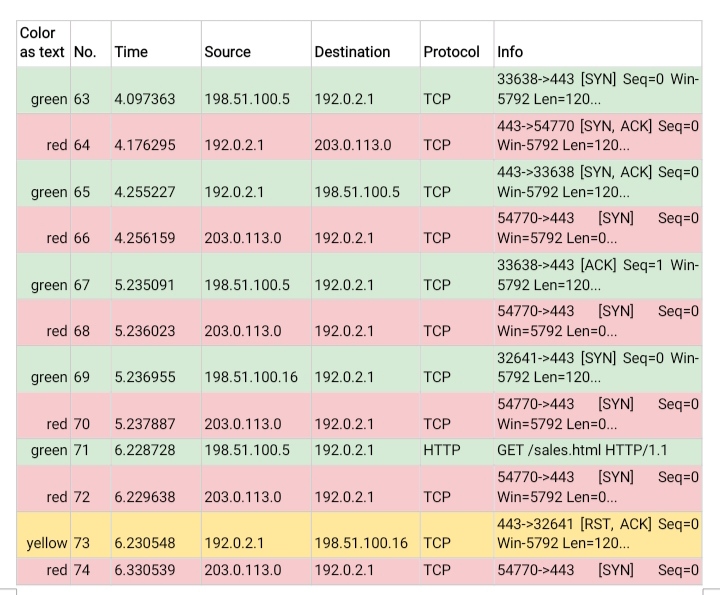
# Cybersecurity Incident Report

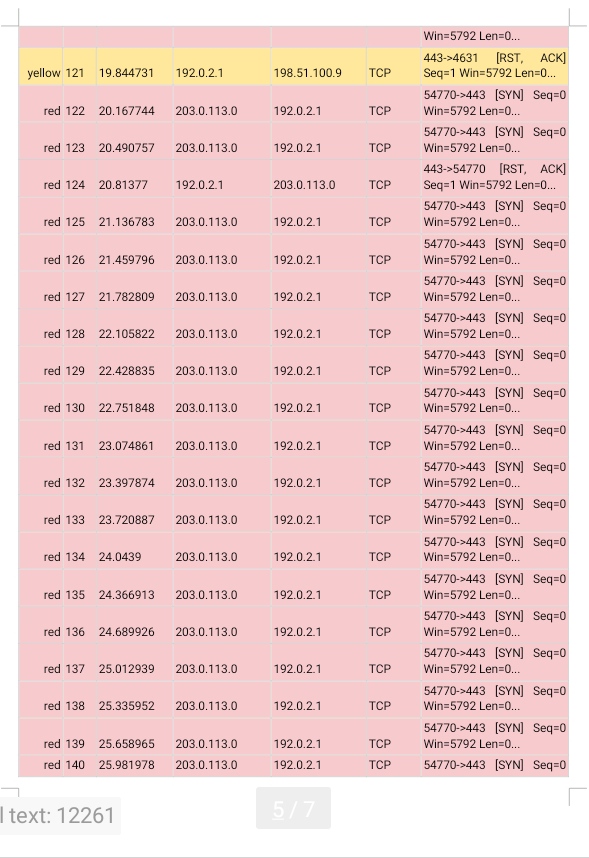
As a security analyst for a travel agency that advertises sales and promotions on the company’s website. The employees of the company regularly access the company’s sales webpage to search for vacation packages their customers might like.

One afternoon, i received an automated alert from my monitoring system indicating a problem with the web server. You attempt to visit the company’s website, but you received a connection timeout error message in my browser.

I used a packet sniffer to capture data packets in transit to and from the web server. I noticed 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.

I took the server offline temporarily so that the machine can recover and return to a normal operating status. I also configured the company’s firewall to block the IP address that was sending the abnormal number of SYN requests. I know that your IP blocking solution won’t last long, as an attacker can spoof other IP addresses to get around this block. I need to alert my manager about this problem quickly and discuss the next steps to stop this attacker and prevent this problem from happening again.





| **Identify the type of attack that may have caused this**  **network interruption** |
| --- |
| One potential explanation for the website's connection timeout error message is due to a delay in establishing connection with the web server in order for both the web browser and the server to communicate or exchange data. The logs show that large TCP SYN requests were been sent to the web server simultaneously. This event could be a Malicious DoS attack and specifically a SYN flood attack trying to prevent the real persons from accessing the website. |
|

| **Explain how the attack is causing the website to malfunction** |
| --- |
| When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol which is:  The [SYN] packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server. SYN stands for “synchronize.”  The [SYN, ACK] packet is the web server’s response to the visitor’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for “synchronize acknowledge.”  The [ACK] packet is the visitor’s machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection. ACK stands for “acknowledge.”  When a malicious actor sends a large number of SYN packets all at once, it is typically an attempt to execute a SYN flood attack, a type of Denial of Service (DoS) attack. Here's a detailed explanation of what happens:  1. SYN Packet Initiation: The attacker sends a large number of SYN (synchronize) packets to the target server. A SYN packet is the first step in the TCP three-way handshake process used to establish a connection between a client and a server.  2. Server Response: The target server, upon receiving a SYN packet, responds with a SYN-ACK (synchronize-acknowledge) packet. This response indicates that the server has received the request and is ready to establish a connection.  3. Half-Open Connections: The server then waits for an ACK (acknowledge) packet from the client to complete the handshake and establish a full connection. However, in a SYN flood attack, the attacker does not send this final ACK packet. As a result, the server is left with many half-open connections, each consuming resources.  4. Resource Exhaustion: Because the server is maintaining these half-open connections, it allocates resources (memory, CPU, and connection slots) for each one. Since the attacker sends a large number of SYN packets, the server's resources can quickly become exhausted.  5. Denial of Service: As the server’s resources are consumed by these half-open connections, it becomes unable to handle legitimate requests from other clients. This leads to a denial of service, where legitimate users cannot access the server or experience significant delays and disruptions.  The logs indicate that the web server has become overwhelmed and is unable to process the visitors’ SYN requests. The server is unable to open a new connection to new visitors who receive a connection tiymeout message. |