Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

According to the web connection logs from WireShark TCP/HTTP log, it is a DoS(Denial of service) attack.
The logs show that rapid SYN handshake protocols are being requested from the web server by “203.0.113.0” IP address.
At first, SYN requested from the web server, then the server sent back SYN, ACK protocol, then 203.0.113.0 sent ACK protocol. After this, usually HTTP connection between client and server has to be established, but there is another SYN request that comes from the 203.0.113.0 IP, which is abnormal. There are about 170 SYN requests in ~48 seconds of time, which indicates DoS attack.
Malicious actors use DoS attacks to flood a system to overwhelm it so the server/machine stops responding to requests.

Section 2: 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. Explain the three steps of the handshake:
1.First, a client sends a SYN(Synchronize) request to a WEB server to establish an HTTP connection.

2. Then, when the Web server receives the SYN request, and it goes through Firewall, it sends SYN/ACK(Synchronize, acknowledge) protocol back to the client.

3. Finally, after receiving SYN/ACK from the WEB server, the client sends the final protocol, which is ACK(Acknowledge), so the sides establish HTTP connection between them.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets rapidly, the web server gets overwhelmed by the requests and unable to respond to them, and eventually it shuts down.
Explain what the logs indicate and how that affects the server: Logs indicate that the web server is being flooded by malicious attack, namely with SYN packets flood. This is overwhelming the system and the Web server is unable to respond to the normal customer requests and it shuts down itself.