Cybersecurity Incident Report

1	No.	Time	Source	Destination	Protocol	Info
74	119	19.198705	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
75	120	19.521718	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
76	121	19.844731	192.0.2.1	198.51.100.9	TCP	443->4631 [RST, ACK] Seq=1 Win=5792 Len=0...
77	122	20.167744	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
78	123	20.490757	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
79	124	20.81377	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
80	125	21.136783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
81	126	21.459796	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
82	127	21.782809	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
83	128	22.105822	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
84	129	22.428835	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

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

One potential explanation for the website's connection timeout error message is: There is a big traffic taking place, overwhelming the server.

The logs show that: There is a flood of SYN messages trying to form a handshake.

This event could be: DoS SYN Flood.

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. SYN (A request to connect)
2. SYN-ACK (This is a respond from the server as it receives the connection request)
3. ACK (Acknowledging the respond from the destination server)

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a large number of SYN packets are sent to the server it is overwhelmed, becomes unable to respond to every single request and shuts down.

Explain what the logs indicate and how that affects the server: Since the server is under overload due to too many incoming SYN packets, it gives "connection timed out" error to new visitors who trying to connect. The server cannot establish new connections.