Kicho Yu
2025-02-14

Cybersecurity Incident Report

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 SYN flood attack which is a DoS attack. The logs show that the web server stops responding after it is overloaded with SYN packet requests.

In the case of 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.

It seems like that 203.0.113.0 is a malicious actor. In the logs, this IP address shows up at 3.390692 seconds and keeps showing up. It dominates sending SYN since 20.167744 seconds, and the web server cannot respond with any [SYN, ACK] packet but rather [RST, ASK] packets. I witnessed thirteen [RST, ACK] flagged packets in this capture and one "HTTP/1.1 504 Gateway Time-out (text/html)" packet at 7.330577 seconds. Those packets mean that normal traffic from employees of the company get timeouts from their SYN requests to the web server.

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. The three steps of the handshake consists of:

1. [SYN]: A packet with this flag indicates the website visitors try to make a handshake with the web server. SYN stands for "synchronize."

2. [SYN, ACK]: A packet with this flag indicates that the web server acknowledges a handshake attempted by the website visitor. SYN, ACK stands for "synchronize acknowledge."

3. [ACK]: A packet with this flag indicates that the website visitors from the company's employee can establish the final (aka the third) step of the handshake to synchronize with the web server. ACK stands for "acknowledge."

When a malicious actor sends a large number of SYN packets all at once, the web server is overwhelmed with that SYN flood. So it stops responding to any traffic. This is called a SYN flood attack and is a part of a DoS (denial of service) attack. This incident is a DoS attack and not DDoS (Distributed Denial of Service) attack, because there is only one malicious actor based on one IP address: 203.0.113.0.

At 6.230548 seconds, I witnessed the first [RST, ACK] flagged packet from the web server. This means that the web server cannot send the [SYN, ACK] flagged packet to the website visitor. It rather sends the [RST, ACK] flagged packet to "reset, acknowledge" the website visitor, who will receive a timeout error message in their browser and the connection attempt is dropped. The website visitor can refresh their browser to attempt to send a new SYN request.