Cybersecurity Incident Report

Type of attack that may have caused this network interruption

Network attacks refer to malicious actions done to exploit the vulnerabilities in a network, with the intent to disrupt, damage or gain unauthorized access to data. Common attacks are DoS, DDoS, MITM, phishing, etc.

This afternoon, we were under a SYN flood attack, which overwhelms the target server with a high volume of SYN packets, initiating connection requests without completing the TCP three-way handshake. The attacker sends multiple SYN packets, ignoring the server's SYN-ACK or using spoofed IP addresses, ensuring the final ACK never reaches the server, causing the servers to crash or become unavailable.

The logs show that the IP address, “203.0.113.0” sent a large number of SYN requests which caused the system to crash.

How the attack is causing the website to malfunction and suggestions

When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The 3-way handshake is a process used by TCP to establish a reliable connection between a client and a server. It ensures that both parties are ready to communicate and synchronizes the connection between them. The process begins when the client sends a SYN (synchronize) message to the server. The server responds with a SYN-ACK (synchronize-acknowledgment) message, which acknowledges the client's request and also sends its own sequence number. Finally, the client sends an ACK (acknowledgment) message back to the server, confirming the receipt of the server’s sequence number. When a malicious actor sends a large number of SYN packets all at once, it is typically part of a SYN flood attack, a type of Denial of Service (DoS) attack. The goal of this attack is to overwhelm the target server and prevent legitimate users from establishing connections.

The log indicates that the IP address “203.0.113.0” sent multiple requests which caused the system to crash. The user started sending the requests slowly and gradually increased the flow of requests, which caused the server to crash.

This can be fixed as follows:

- Implementing rate limiting to control the number of requests from any single IP address within a given time frame.
- Use a WAF to filter out malicious traffic before it reaches the server.
- Load balancing to distribute incoming traffic across multiple servers to prevent a single server from being overwhelmed.