Analyze network attacks

Incident Title:
Unusually High TCP SYN Request from Unfamiliar IP Address to The Company Web Server

1. Incident Summary
During afternoon, company's monitoring system gave an automating alert indicated a problem with company web server. A connection timeout error message received in browser when the host attempted to visit the company's website. The host noticed a large number of TCP SYN requests coming from an unfamiliar IP address.

2. Evidence / Observation
Summarize what the logs or tools show.

- Source IP: 203.0.113.0
- Destination IP: 192.0.2.1
- Protocol: TCP
- Response: HTTP/1.1 504 Gateway Time-out (text/html) error message.
- Behavior: Repeated SYN request from unfamiliar IP address (203.0.113.0) is observed.

3. Analysis

In the Wireshark TCP/HTTP log, the SYN request are repeated from unfamiliar IP address. Too much SYN request at a time is observed.

Section 1: Identify the type of attack that may have caused this network interruption
• From the packet capture in the WIRESHARK logs, a connection timeout error message appeared as there were too many SYN request at a time. • This causes the website stopped responding after receiving too many requests at a rapid pace. • The web server cannot handle it as web server has less resources to handle the request. • It turns out the request was from unfamiliar IP address. • This looks like a Denial-Of-Service (DoS) attack, called a SYN flood attack. • This attack targets network bandwidth to slow traffic and causes website to stopped responding/crashes. • A DoS direct attack originates from a single source. A distributed denial of service (DDoS) attack comes from multiple sources, often in different locations, making it more difficult to identify the attacker or attackers.

Section 2: Explain how the attack is causing the website malfunction
• Normally, when someone visits a website, TCP three-way handshake process will occur to start a safe connection: 1. Visitor's device will send SYN request to the company's website server. 2. The server replies with SYN/ACK. 3. Visitor's device responded with ACK to establish connection. • In SYN flood attack, the attacker sends many SYN request but never complete the handshake. • This attack causes the web server to crash/stop responding to request. • This is because the server keeps port open waiting for responses, eventually, running out of available port and crashing. • The logs show that the web server has become overwhelmed and unable to process visitor's SYN requests. • The server is unable to open a new connection to new visitors who received a connection timeout message. • To secure the network so this attack can be prevented in the future, it's suggested to: 1. Enable **firewall SYN flood protection** (rate limiting, SYN cookies) 2. Continue using **HTTPS/TLS** for secure data. 3. Monitor **logs** for early warning. 4. Use DDoS mitigation services (like Cloudflare/AWS Shield) 5. Use Intrusion Detection System (**IDS) /** Intrusion Prevention System (**IPS)** to detect unusual traffic.