Cybersecurity Incident Report

SYN Flood attack, a form of Denial-of-Service (DoS) aimed at overwhelming the network and disrupting legitimate access. The logs reveal that an unauthorized external IP address (203.0.113.0) has repeatedly initiated suspicious TCP connections, simulating a three-way handshake but failing to complete it, thereby exhausting server resources.

Technical Description of the Attack:

A SYN Flood attack exploits the TCP handshake process by sending a rapid succession of SYN requests from a spoofed or malicious IP address without completing the handshake (i.e., without sending ACK). This causes the server to keep connections in a half-open state, consuming memory and bandwidth.

In our case:

The attacker’s IP 203.0.113.0, using port 54770, initiated a connection to port 443 of the web server.

The server, attempting to follow the TCP protocol, replied with SYN-ACK (Log entry #53)

However, the attacker either didn't respond with an ACK or continued spamming SYNs, never completing the handshake, leading to excessive half-open connections.

At log entry #73, RST-ACK responses began appearing, indicating that the server attempted to reset connections, likely due to overload or timeout.

Finally, at log entry #77, the server showed a connection timeout, signaling degradation of service.

Indicators in the Logs:

70	5.237887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
71	6.228728	198.51.100.5	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
72	6.229638	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
73	6.230548	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=0 Win=5792 Len=120...
74	6.330539	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
75	6.330885	198.51.100.7	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=0...
76	6.331231	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
77	7.330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)
78	7.351323	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

Here are the critical log entries illustrating the attack:
#52: Attacker IP 203.0.113.0 initiates SYN to web server (192.0.2.1) on port 443.
#53: Server responds with SYN-ACK, acknowledging the attacker.

#54–72: Repeated SYNs from attacker; multiple half-open connections.
#73: RST-ACK from server shows forced reset due to unresponsiveness.
#77: Connection timeout recorded — signs of denial of service.

70	5.237887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
71	6.228728	198.51.100.5	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
72	6.229638	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
73	6.230548	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=0 Win=5792 Len=120...
74	6.330539	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
75	6.330885	198.51.100.7	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=0...
76	6.331231	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
77	7.330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)
78	7.351323	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

Affected Systems:
Web Server IP: 192.0.2.1
Employee Devices IP Range: 198.

The network logs clearly indicate a SYN Flood attack targeting our web server (IP: 192.0.2.1), originating from an unauthorized external IP address (203.0.113.0). The attack successfully initiated multiple TCP handshake requests without completing them, leading to resource exhaustion and eventual service unavailability. The abnormal volume of SYN packets, reset acknowledgments, and timeouts observed in the logs (particularly between packet numbers 52 to 77) confirms the disruption.

This incident highlights the critical need for implementing advanced threat detection and prevention mechanisms such as firewalls, intrusion detection/prevention systems (IDS/IPS), SYN cookies, and network traffic filtering. Immediate action is recommended to mitigate current threats and strengthen our network's security posture to prevent similar attacks in the future.