Incident handler's journal

Date: 11-05-2024	Entry: 001 SYN Flood Denial of Service Incident on Company Web Server
Description	An abnormal increase in TCP SYN packets from a specific external IP address (203.0.113.0) caused the web server to become unresponsive. This led to a service disruption affecting both employees and customers attempting to access the company's sales webpage.
Tool(s) used	Packet sniffer Web browser Monitoring/Alerting system Firewall
The 5 W's	**Who** caused the incident? A malicious actor using the IP address 203.0.113.0 (source may be spoofed). **What** happened? A TCP SYN flood attack overwhelmed the web server with half-open TCP connections, leading to a denial of service and eventual HTTP 504 Gateway Time-out errors for legitimate users. **When** did the incident occur? 11-05-2024, early afternoon (as per system alert timestamp and packet capture logs) **Where** did the incident happen? On the company's external web server hosting the sales and promotions page (192.0.2.1). **Why** did the incident happen? The attacker exploited the server's lack of SYN flood mitigation by sending a high volume of SYN requests without completing the TCP handshake, exhausting system resources.
Additional notes	Temporary IP blocking was implemented but acknowledged as a short-term solution. Future mitigation steps discussed include enabling SYN cookies, rate limiting, and upstream DDoS protection. Incident to be documented and used as a basis to update the organization's risk strategy and response playbooks (per NIST CSF mappings: RS.MA, GV.RM, PR.PS, DE.CM, RC.RP).