Cybersecurity Incident Report

Maria Audu

Section 1: Identify the type of attack that may have caused this network interruption
TCP SYN Flood (Denial-of-Service attack) A TCP SYN flood attack overwhelms a server by sending a large number of SYN requests without completing the TCP three-way handshake. This consumes server resources and prevents legitimate users from establishing connections.

Section 2: Explain how the attack is causing the website to malfunction
• High volume of TCP SYN packets from an unfamiliar IP address • Incomplete TCP handshakes • Web server becomes unresponsive • Users experience connection timeout errors The server's connection table was overwhelmed with half-open connections, reducing its ability to respond to legitimate traffic. As a result, employees could not access the company website. **Negative Impact on the Organization** • Website downtime and service interruption • Reduced employee productivity • Potential loss of customer trust and revenue • Increased risk of future attacks if not mitigated **Difference Between DoS and DDoS** • **DoS**: Attack originates from a single source • **DDoS**: Attack originates from multiple compromised systems (botnet) •

Why the Website Timed Out

The server was unable to process legitimate connection requests due to resource exhaustion caused by excessive SYN packets.

Potential Mitigation Strategies

- Enable SYN cookies on the server
- Implement rate limiting on firewalls
- Use intrusion detection/prevention systems (IDS/IPS)
- Deploy DDoS protection services