Cybersecurity Incident Report - Network Attack

Section 1: Identify the type of attack that may have caused this network interruption

One potential explanation for the website's connection timeout error message is: A **Denial of Service (DoS) attack**, specifically a **TCP SYN flood**, which overwhelms the server by sending a large number of SYN requests that the server cannot handle.

The logs show that: A very high volume of **TCP SYN packets** are coming from an unfamiliar IP address. The server is unable to respond to all the incoming requests, indicating that it is being intentionally flooded.

This event could be: A **SYN flood attack**, a type of DoS attack that targets the TCP handshake process. It causes the server to hang or crash because it has too many half-open connections waiting for completion.

Section 2: Explain how the attack is causing the website to malfunction

When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:

1. **SYN**: The client sends a synchronize (SYN) packet to the server to initiate the connection.
2. **SYN-ACK**: The server responds with a synchronize-acknowledge (SYN-ACK) packet.
3. **ACK**: The client replies with an acknowledgment (ACK) packet to complete the connection.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server receives numerous SYN requests but never receives the final ACK responses needed to complete the handshake. These incomplete handshakes remain open, consuming server resources and eventually leading the server to become unresponsive to legitimate users.

Explain what the logs indicate and how that affects the server: The packet sniffer logs show an unusually high number of SYN packets from a suspicious IP address without corresponding ACKs. This prevents the server from completing normal TCP handshakes, leading to performance degradation and eventual downtime, which explains the connection timeout error experienced by users.

Difference between DoS and DDoS: A **Denial of Service (DoS)** attack typically comes from

a **single source**, overwhelming a server with traffic. A **Distributed Denial of Service (DDoS)** attack, on the other hand, involves **multiple sources** (often compromised systems or bots) attacking the server simultaneously, making it harder to block.

Suggest ways to secure the network in future:

1. Use SYN cookies to validate handshakes.
2. Implement rate limiting on SYN requests.
3. Deploy a Web Application Firewall (WAF) with DoS protections.
4. Monitor network traffic for anomalies in real-time.
5. Consider intrusion detection/prevention systems (IDS/IPS).

What do you understand about network attacks?

Network attacks are attempts to disrupt, damage, or gain unauthorized access to systems or data. They include DoS/DDoS attacks, phishing, spoofing, and exploitation of software vulnerabilities. The goal is often to steal information, interrupt service, or gain control.

Why is the website showing timeout errors?

The web server is overwhelmed with half-open TCP connections due to the SYN flood. It uses up resources to wait for connections that never complete, eventually making it unable to respond to real users.

What are the possible consequences of this attack?

- Service downtime and user frustration
- Financial losses from missed sales
- Damage to the organization’s reputation
- Potential data breach if the attacker exploits other vulnerabilities