Cybersecurity Incident Report

Subject: Analysis of Network Intrusion Attack

To: Manager

From: Adjei Yaw Osei

Date: 23rd September, 2024.

Time: 2:49pm (GMT)

Section 1: Analysis of the Network Attack

Understanding Network Attacks:

Network attacks can take various forms, including malware, phishing, and intrusion attempts aimed at exploiting vulnerabilities in systems and networks. A thorough understanding of these attacks is essential for effectively identifying and mitigating potential threats.

Type of Attack Indicated:

The symptoms described in the scenario suggest a **SYN flood attack**. This type of attack overwhelms a server with an excessive number of SYN requests, preventing it from establishing legitimate connections with users.

Difference Between DoS and DDoS:

- **Denial of Service (DoS):** Involves a single source flooding a target system with requests, causing it to become overwhelmed and unavailable.

- **Distributed Denial of Service (DDoS):** Involves multiple compromised devices (often a botnet) targeting a single system, significantly increasing the volume of traffic and complicating defense measures.

Reason for Connection Timeout Errors:

The website is taking a long time to load and reporting connection timeout errors due to the server's inability to handle legitimate requests while being bombarded with SYN packets from the attacker. This overwhelming traffic causes resource exhaustion, resulting in failed connection attempts for legitimate users.

Wireshark Traffic Analysis:

Upon reviewing the Wireshark logs, a distinct pattern emerged showing a high volume of SYN packets from a specific IP address with minimal SYN-ACK responses. This confirms a SYN flood attack, as legitimate connection handshakes are disrupted by excessive traffic.

Section 2: Impact of the Attack and Recommendations

Description of the Attack:

The SYN flood attack is characterized by a barrage of SYN packets sent to the server. Symptoms include high network traffic, connection timeouts for legitimate users, and server resource exhaustion. This specific attack does not require sophisticated tools, making it easily executed by malicious actors.

Effects on the Organization's Network:

This attack significantly impacts the organization's network by rendering the website inaccessible to employees and customers. It disrupts business operations, as employees cannot access the sales page to assist clients, leading to potential lost revenue and decreased customer satisfaction.

Potential Consequences:

- **Operational Disruption:** Inability to access the website hampers employees' ability to assist customers, which can lead to lost sales and a negative customer experience.

- **Reputational Damage:** Frequent outages may damage the company's reputation, leading to decreased trust among customers and stakeholders.

- **Financial Loss:** Prolonged downtime can result in direct financial losses from missed sales opportunities.

Recommendations for Future Security:

1. **Implement Rate Limiting:** Configure the firewall to limit the number of SYN requests from any single IP address.

2. **Deploy Intrusion Detection and Prevention Systems (IDPS): Utilize** IDPS to monitor for abnormal traffic patterns and take automatic actions against identified threats.

3. **Consider Anti-DDoS Services:** Engage third-party services that specialize in DDoS mitigation to enhance protection against future attacks.

4. **Regular Security Audits:** Conduct regular security assessments to identify vulnerabilities and improve overall network defenses.

Preparedness for Discussion:

I am ready to discuss the nature of the attack, its impact on our operations, and the proposed next steps in our security strategy. Please let me know when you would like to meet to review this matter further.

Thank you,

Adjei Yaw Osei

Cybersecurity Analyst

adjeiyawosei@gmail.com