Reflection Activity

A medium-sized e-commerce company experiences a sudden surge in customer complaints about website performance degradation, with constant customer request failure and unauthorised access to their accounts. It was shown upon investigation, that the front desk team mistakenly shared the information with an unauthorised client who is now using it to access customers' accounts and flood traffic on the -e-commerce company site hijacking their normal transactional operation, the company's cybersecurity team discovered the following issues:

Network segmentation failure: The company's database servers, containing sensitive customer information, were not properly isolated from the public-facing web servers. This allowed an attacker who compromised a web server to easily access customer data.

Lack of Least privilege implementation: The front desk team has access to many sensitive information.

DDoS attack: The website slowdown was caused by a Distributed Denial of Service (DoS) attack, which the company's network infrastructure was ill-equipped to handle.

Weak encryption: Customer data was being transmitted using outdated encryption protocols, making it vulnerable to interception.

Now based, on these factors pointed out by the security team which also you have a working knowledge of based on our learning outcome from weeks 1 to 4 can we attempt linking networking fundamentals to cybersecurity using the following questions?

Exercise

1. Recommend security measures for the given scenario and how can understanding networking concepts enhance your recommendations.

2. How does the OSI model help in the identification of network vulnerabilities?

3. How can basic networking skills improve incident response in cybersecurity?

4. What do you understand network segmentation to be and what was its role in the stated scenario?

5. What are some common networking protocols used in cybersecurity and which of them played a role in this scenario?