TESTING SCENARIO

You are tasked with conducting a penetration test on a simulated e-commerce website, "Cybermart." The goal is to identify and address potential security vulnerabilities in the web application and associated infrastructure.

Virtual Environment Components:

Cybermart Web Application:

The Cybermart Web Application is a simulated e-commerce platform designed for the purpose of penetration testing. It imitates the functionality of a real online marketplace, allowing users to browse products, make purchases, and manage their accounts. This web application is created using common web technologies such as HTML for structuring content, CSS for styling, and JavaScript for dynamic interactions. The backend of the Cybermart application is developed using a server-side technology, for instance, Node.js.

Key Features:

- User authentication and account management.
- Product catalog with details and pricing.
- Shopping cart functionality.
- Order processing and order history.

Web Server (Nginx):

Nginx is utilized as the web server for the Cybermart application. Nginx is a high-performance web server that also functions as a reverse proxy server and load balancer. In this context, it is responsible for handling HTTP requests from clients (such as web browsers) and forwarding them to the Cybermart Web Application. Nginx plays a crucial role in serving static content, managing connections, and optimizing overall web application performance.

Key Functions:

- Handling incoming HTTP requests.
- Directing traffic to the appropriate components of the Cybermart application.
- Enhancing performance through load balancing and caching.

Database Server (MySQL):

The MySQL database server is employed to store and manage the data associated with the Cybermart Web Application. It serves as the backend storage for user information, product details, and order history. MySQL is a popular relational database management system (RDBMS) that ensures the secure and efficient storage of structured data.

Key Data Stored:

- User credentials and authentication information.
- Product details, including descriptions and pricing.
- Order history and transaction records.

TESTING SCENARIO

Firewall:

The firewall is a critical component of the virtual environment, configured to enhance security by controlling and monitoring network traffic. It is designed to restrict unnecessary or unauthorized access to the Cybermart application and associated servers. The firewall acts as a barrier between the internal network and external threats, preventing malicious activity and unauthorized access.

Firewall Configuration:

- Restricting incoming and outgoing traffic based on predefined rules.
- Blocking potential security threats and unauthorized access attempts.
- Monitoring and logging network activity for analysis.

Logging System:

A centralized logging system is implemented to monitor and analyze the activity within the virtual environment. It collects and stores logs generated by various components, including the web server, database server, and firewall. Centralized logging is crucial for security analysis, troubleshooting, and identifying potential security incidents.

Logging Activities:

- Recording login attempts, access requests, and system events.
- Storing error logs and security-related information.
- Providing a comprehensive view of system activity for analysis and audit purposes

In summary, the virtual environment for the Cybermart Web Application is a comprehensive setup that includes a web application mimicking an e-commerce platform, a web server (Nginx), a database server (MySQL), a firewall for security, and a centralized logging system for monitoring and analysis. This environment is designed for penetration testing, allowing security professionals to identify and address potential vulnerabilities within the simulated infrastructure.