CompTIA Cybersecurity Analyst (CySA+)

1. **Threat Management**
    a. Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes
    b. Given a scenario, analyze the results of a network reconnaissance
    c. Given a network-based threat, implement or recommend the appropriate response and countermeasure
    d. Explain the purpose of practices used to secure a corporate environment
2. **Vulnerability Management**
. Given a scenario, implement an information security vulnerability management process
    a. Given a scenario, analyze the output resulting from a vulnerability scan
    b. Compare and contrast common vulnerabilities found in the following targets within an organization
3. **Cyber Incident Response**
. Given a scenario, distinguish threat data or behavior to determine the impact of an incident
    a. Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation
    b. Explain the importance of communication during the incident response process
    c. Given a scenario, analyze common symptoms to select the best course of action to support incident response
    d. Summarize the incident recovery and post-incident response process
4. **Security Architecture and Tool Sets**
. Explain the relationship between frameworks, common policies, controls, and procedures
    a. Given a scenario, use data to recommend remediation of security issues related to identity and access management
    b. Given a scenario, review security architecture and make recommendations to implement compensating controls
    c. Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC)
    d. Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies