Example Test Questions:

3) Angela reviews bulletins and advisories to determine what threats her organization is likely to face. What type of activity is this associated with?

a. Incident response

\*b. Threat hunting

c. Penetration testing

d. Vulnerability scanning

7) Charles has been tasked with building a team that combines techniques from attackers and defenders to help protect his organization. What type of team is he building?

a. A red team

b. A blue team

c. A white team

\*d. A purple team

8) Allison wants to aggregate her logs and have them automatically correlated and reported on. What sort of tool should she acquire for her organization?

a. MDM

b. A jump server

c. SDN

\*d. SIEM

18) As part of the early stages of a penetration test, Hui has researched her target organization’s domain names and IP addresses, and has conducted a port scan. What type of activity is Hui engaging in?

\*a. Reconnaissance

b. An unknown environment test

c. A known environment test

d. OSINT gathering

29) John has been asked to do a penetration test of a company. He has been given general information but no details about the network. What kind of test is this?

\*a. Partially known environment

b. Known environment

c. Unknown environment

d. Masked

38) Eric manages his organization’s internal security team and wants to leverage a penetration test as part of his team’s testing that allows them to respond to simulated attacks. What type of model best describes this?

a. Physical

b. Offensive

\*c. Defensive

d. Integrated

51) What type of penetration test is being done when the tester is given extensive knowledge of the target network?

\*a. Known environment

b. Full disclosure

c. Unknown environment

d. Red team

63) You have been asked to test your company network for security issues. The specific test you are conducting involves primarily using automated and semiautomated tools to look for known vulnerabilities with the various systems on your network. Which of the following best describes this type of test?

\*a. Vulnerability scan

b. Penetration test

c. Security audit

d. Security test

70) Jason’s organization has engaged a penetration testing firm that specializes in using techniques commonly employed by nation-state actors, including using social engineering techniques, advanced tools, and methods that will provide significant footholds within his infrastructure. What type of penetration test best describes this?

a. Physical

\*b. Offensive

c. Defensive

d. Integrated

77) Kelly’s organization has created an incident response policy that outlines the high-level goals of the IR process. Next, she wants to create detailed documents that describe the steps to handle specific incident types like denial-of-service attacks. What document should she create?

a. Standards

\*b. Playbooks

c. Regulations

d. Guidelines

89) The type and scope of testing, client contact details, how sensitive data will be handled, and the type and frequency of status meetings and reports are all common elements of what artifact of a penetration test?

a. The unknown environment (black-box) outline

\*b. The rules of engagement

c. The known environment (white-box) outline

d. The close-out report