## QUESTIONS

1. Which of the following would be found in a final report from a full penetration test? (Choose all that apply.)
   - A. The names of all the participants
   - B. A list of findings from the assessments
   - C. An executive summary of the assessments
   - D. A list of vulnerabilities that were patched by the team
2. A team is starting a security assessment and has been provided a system on an internal subnet. No other previous knowledge of any pertinent information has been given. Which of the following best describes the type of test the team will be performing?
   - A. Internal, white box
   - B. Internal, black box
   - C. External, white box
   - D. External, black box
3. Which of the following provide automated pen test–like results for an organization? (Choose all that apply.)
   - A. Metasploit
   - B. Nessus
   - C. Core Impact
   - D. CANVAS
   - E. SAINT
   - F. GFI Languard
4. Which of the following best describes an assessment against a network segment that tests for existing vulnerabilities but does not attempt to exploit any of them?
   - A. Penetration test
   - B. Partial penetration test
   - C. Vulnerability assessment
   - D. Security scan
5. A spouse of an employee illegally uses the employee's credentials to gain access to the organization and carry out an attack. Which of the following best defines the attacker?
   - A. Outside affiliate
   - B. Outside associate
   - C. Insider affiliate
   - D. Insider associate

6. In which phase of a pen test is scanning performed?

   A. Pre-attack

   B. Attack

   C. Post-attack

   D. Reconnaissance

7. Which of the following tests is generally faster and costs less than a manual pen test?

   A. Automatic

   B. Internal

   C. Black box

   D. External

8. Which of the following best defines an attack against the organization by an internal user?

   A. External, black box

   B. Internal, gray box

   C. Internal, announced

   D. External, white box

9. Brad is part of an environmental group protesting SomeBiz, Inc., for the company's stance on a variety of issues. Frustrated by the failure of multiple attempts to raise awareness of his cause, Brad launches sophisticated web defacement and denial-of-service attacks against the company, without attempting to hide the attack source and with no regard to being caught. Which of the following terms best defines Brad?

   A. Hactivism

   B. Ethical hacker

   C. Script kiddie

   D. Suicide hacker

10. A security team has been hired by upper management to assess the organization's security. The assessment is designed to emulate an Internet hacker and to test the behavior of the security devices and policies in place as well as the IT security staff. Which of the following best describe this test? (Choose all that apply.)

    A. Internal

    B. External

    C. Announced

    D. Unannounced

11. In which phase of a pen test will the team penetrate the perimeter and acquire targets?

    A. Pre-attack

    B. Attack

    C. Post-attack

    D. None of the above

12. Which of the following test types presents a higher probability of encountering problems and takes the most amount of time?

    A. Black box

    B. Gray box

    C. White box

    D. Internal

13. Which of the following best describes the difference between a professional pen test team member and a hacker?

    A. Ethical hackers are paid for their time.

    B. Ethical hackers never exploit vulnerabilities; they only point out their existence.

    C. Ethical hackers do not use the same tools and actions as hackers.

    D. Ethical hackers hold a predefined scope and agreement from the system owner.

14. Sally is part of a penetration test team and is starting a test. The client has provided a network drop on one of their subnets for Sally to launch her attacks from. However, they did not provide any authentication information, network diagrams, or other notable data concerning the systems. Which type of test is Sally performing?

    A. External, white box

    B. External, black box

    C. Internal, white box

    D. Internal, black box

15. Joe is part of a pen test team that has been hired by AnyBiz to perform testing under a contract. As part of the defined scope and activities, no IT employees within AnyBiz know about the test. After some initial information gathering, Joe strikes up a conversation with an employee in the cafeteria and steals the employee's access badge. Joe then uses this badge to gain entry to secured areas of AnyBiz's office space. Which of the following best defines Joe in this scenario?

    A. Outside affiliate

    B. Outside associate

    C. Insider affiliate

    D. Insider associate

16. In which phase of a penetration test would you compile a list of vulnerabilities found?

    A. Pre-attack
    B. Attack
    C. Post-attack
    D. Reconciliation

17. Which of the following has a database containing thousands of signatures used to detect vulnerabilities in multiple operating systems?

    E. Nessus
    F. Hping
    G. LOIC
    H. SNMPUtil

18. Cleaning registry entries and removing uploaded files and tools are part of which phase of a pen test?

    A. Covering tracks
    B. Pre-attack
    C. Attack
    D. Post-attack

19. Jake, an employee of AnyBiz, Inc., parks his vehicle outside the corporate offices of SomeBiz, Inc. He turns on a laptop and connects to an open wireless access point internal to SomeBiz's network. Which of the following best defines Jake?

    A. Outside affiliate
    B. Outside associate
    C. Insider affiliate
    D. Insider associate

20. Which of the following are true regarding a pen test? (Choose all that apply.)

    A. Pen tests do not include social engineering.
    B. Pen tests may include unannounced attacks against the network.
    C. During a pen test, the security professionals can carry out any attack they choose.
    D. Pen tests always have a scope.
    E. The client is not notified of the vulnerabilities the team chooses to exploit.

21. Which of the following causes a potential security breach?

    A. Vulnerability

    B. Threat

    C. Exploit

    D. Zero day

22. Which Metasploit payload type operates via DLL injection and is difficult for antivirus software to pick up?

    A. Inline

    B. Meterpreter

    C. Staged

    D. Remote

23. Metasploit is a framework allowing for the development and execution of exploit code against a remote host and is designed for use in pen testing. The framework consists of several libraries, each performing a specific task and set of functions. Which library is considered the most fundamental component of the Metasploit framework?

    A. MSF Core

    B. MSF Base

    C. MSF Interfaces

    D. Rex

24. EC-Council defines six stages of scanning methodology. Which of the following correctly lists the six steps?

    A. Scan for vulnerabilities, check for live systems, check for open ports, perform banner grabbing, draw network diagrams, prepare proxies

    B. Perform banner grabbing, check for live systems, check for open ports, scan for vulnerabilities, draw network diagrams, prepare proxies

    C. Check for live systems, check for open ports, perform banner grabbing, scan for vulnerabilities, draw network diagrams, prepare proxies

    D. Prepare proxies, check for live systems, check for open ports, perform banner grabbing, scan for vulnerabilities, draw network diagrams

25. Which of the following may be effective countermeasures against an inside attacker? (Choose all that apply.)

    A. Enforce elevated privilege control.

    B. Secure all dumpsters and shred collection boxes.

    C. Enforce good physical security practice and policy.

    D. Perform background checks on all employees.

26. The IP address 132.58.90.55/20 is given for a machine your team is to test. Which of the following represents an address within the same subnet?

   A. 132.58.88.254

   B. 132.58.96.20

   C. 132.58.254.90

   D. 132.58.55.90