

Module 1 - Ethical Hacking Overview

1. What type of testing procedure involves the tester(s) analyzing the company's security policy and procedures, and reporting any vulnerabilities to management?

- a. penetration test
- b. security test
- c. hacking test
- d. ethical hacking test

ANSWER:

b

2. What specific term does the U.S. Department of Justice use to label all illegal access to computer or network systems?

- a. Hacking
- b. Cracking
- c. Security testing
- d. Packet sniffing

ANSWER:

a

3. What penetration model should a company use if they only want to allow the penetration tester(s) partial or incomplete information regarding their network system?

- a. gray box
- b. white box
- c. black box
- d. red box

ANSWER:

a

4. What advanced professional security certification requires applicants to demonstrate hands-on abilities to earn their certificate?

- a. Offensive Security Certified Professional
- b. Certified Ethical Hacker
- c. Certified Information Systems Security Professional
- d. CompTIA Security+

ANSWER:

a

5. What common term is used by security testing professionals to describe vulnerabilities in a network?

- a. bytes
- b. packets
- c. bots
- d. holes

ANSWER:

d

6. What term refers to a person who performs most of the same activities a hacker does, but with the owner or

Module 1 - Ethical Hacking Overview

company's permission?

- a. cracker
- b. script kiddie
- c. ethical hacker
- d. hacktivist

ANSWER:

c

7. What derogatory title do experienced hackers give to inexperienced hackers who copy code or use tools created by knowledgeable programmers without understanding how the tools work?

- a. copy kiddie
- b. red team member
- c. packet monkey
- d. cracker

ANSWER:

c

8. What type of assessment performed by a penetration tester attempts to identify all the weaknesses found in an application or on a system?

- a. health
- b. technical
- c. vulnerability
- d. network

ANSWER:

c

9. Many experienced penetration testers will write a set of instructions that runs in sequence to perform tasks on a computer system. What type of resource are these penetration testers utilizing?

- a. kiddies
- b. packets
- c. scripts
- d. tasks

ANSWER:

c

10. How can a security tester ensure a network is nearly impenetrable?

- a. install a vendor's latest security patch
- b. update the operating systems
- c. eliminate unnecessary applications or services
- d. unplug the network cable

ANSWER:

d

11. What penetration model should be used when a company's management team does not wish to disclose that penetration testing is being conducted?

- a. black box

Module 1 - Ethical Hacking Overview

- b. white box
- c. red box
- d. silent box

ANSWER:

a

12. Why might companies prefer black box testing over white box testing?

- a. The white box model puts the burden on the tester to find information about the technologies a company is using.
- b. If a company knows that it's being monitored to assess the security of its systems, employees might behave more carelessly and not adhere to existing procedures.
- c. Black box testing involves a collaborative effort between a company's security personnel and penetration testers.
- d. Many companies don't want a false sense of security.

ANSWER:

d

13. What penetration model would likely provide a network diagram showing all the company's routers, switches, firewalls, and intrusion detection systems, or give the tester a floor plan detailing the location of computer systems and the OSs running on these systems?

- a. black box
- b. white box
- c. red box
- d. blue box

ANSWER:

b

14. What is the difference between penetration tests and security tests?

- a. These terms are synonymous
- b. In a penetration test, an ethical hacker attempts to break into a company's network or applications to find weak links. In a security test, testers do more than attempt to break in; they also analyze a company's security policy and procedures and report any vulnerabilities to management.
- c. Penetration testing takes security testing to a higher level
- d. In a security test, an ethical hacker attempts to break into a company's network or applications to find weak links. In a penetration test, testers do more than attempt to break in; they also analyze a company's security policy and procedures and report any vulnerabilities to management.

ANSWER:

b

15. Why should a company employ an ethical hacker?

- a. The benefit of an ethical hacker discovering vulnerabilities outweighs the cost of paying for the penetration/security test services.
- b. A company can hire an ethical hacker to promote political or social ideologies.
- c. Ethical hackers can help make a network impenetrable.
- d. Companies should never hire hackers.

ANSWER:

a

Module 1 - Ethical Hacking Overview

16. Which penetration model allows for an even distribution of time and resources along with a fairly comprehensive test?

- a. White box
- b. Black box
- c. Gray box
- d. Red box

ANSWER:

c

17. What is critical to remember when studying for a network security certification exam?

- a. Memorize answers to questions to ensure you pass.
- b. Security certifications are always relevant because it is a static profession.
- c. Certifications prove only technical skills are necessary to perform the job of a security professional effectively.
- d. Following the laws and behaving ethically are more important than passing an exam.

ANSWER:

d

18. What can be inferred about successful security professionals?

- a. Successful security professionals have strong technical skills.
- b. Successful security professionals have strong soft skills.
- c. Successful security professionals have a combination of technical and soft skills.
- d. Successful security professionals have multiple certifications.

ANSWER:

c

19. With which type of laws should a penetration tester or student learning hacking techniques be familiar?

- a. local
- b. state
- c. federal
- d. all of the above

ANSWER:

d

20. What policy, provided by a typical ISP, should be read and understood before performing any port scanning outside of your private network?

- a. Port Scanning Policy
- b. Acceptable Use Policy
- c. ISP Security Policy
- d. Hacking Policy

ANSWER:

b

21. What acronym represents the U.S. Department of Justice branch that addresses computer crime?

- a. GIAC

Module 1 - Ethical Hacking Overview

- b. OPST
- c. CHIP
- d. CEH

ANSWER:

c

22. What federal law makes it illegal to intercept any type of communication, regardless of how it was transmitted?

- a. The No Electronic Theft Act
- b. U.S. PATRIOT Act
- c. Electronic Communication Privacy Act
- d. The Computer Fraud Act

ANSWER:

c

23. Which of the following statements about port scanning is true?

- a. Port scanning violates the U.S. Constitution.
- b. Some states consider port scanning as noninvasive or nondestructive in nature and deem it legal.
- c. If you are found innocent of criminal port scanning charges, there are no financial repercussions.
- d. Port scanning while connected to a VPN will only allow you to scan your own personal network.

ANSWER:

b

24. Why have some judges dismissed charges for those accused of port scanning?

- a. Networks are private property.
- b. Usually, no damages are done when port scanning.
- c. Port scanning is legal everywhere.
- d. Port scanning is a federal offense, so hackers can be charged with greater offenses.

ANSWER:

b

25. Which of the following actions could be prosecuted under the Stored Wire and Electronic Communications and Transactional Records Act?

- a. An authorized employee of the FBI accesses classified records.
- b. An individual downloads copyrighted movies and makes copies for friends.
- c. A security contractor accesses computers that have classified information without authorization.
- d. An employee of a company copies records without permission with intent to sell the records to a competitor.

ANSWER:

c

26. How can a nondisclosure agreement allay management fears about password discovery?

- a. Nondisclosure agreements outline the scope of testing.
- b. Nondisclosure agreements assure clients that testers are certified to authenticate passwords.
- c. Nondisclosure agreements assure clients that testers will not change any passwords.
- d. Nondisclosure agreements assure clients that testers will not reveal or use any information they find.

ANSWER:

d

Module 1 - Ethical Hacking Overview

27. Even though a security professional might think they are following the requirements set forth by the client who hired them to perform a security test, management may be dissatisfied. Which of the following is an example of an ethical hacking situation that might upset a manager?

- a. The security testing reveals a vulnerability with the system, and the professional suggests that the company update their operating system to correct the vulnerability.
- b. The security tester uses a vulnerability that they discovered to steal secret company information and sell it to a competitor.
- c. The security testing reveals all the usernames and passwords of company personnel to the tester without the manager's prior consent.
- d. The security tester uses a port scanning technique outlined in a contract which both parties signed.

ANSWER:

c

28. When a security professional is presented with a contract drawn up by a company's legal department, which allows them to "hack" the company's network, they should proceed by performing what precautionary step?

- a. consult the company's lawyer
- b. consult their lawyer
- c. sign the contract
- d. begin testing immediately

ANSWER:

b

29. Which of the following activities is not illegal?

- a. Copying information without the owner's permission
- b. Installing a worm on a network
- c. Discovering passwords of company personnel when testing for vulnerabilities
- d. Destroying data

ANSWER:

c

30. Which of the following statements about written contracts is true?

- a. Written contracts are always a good business practice.
- b. Written contracts undermine relationships with clients.
- c. Written contracts can be omitted when doing business with a friend.
- d. Written contracts authored by the company's lawyers are always safe to sign.

ANSWER:

a

31. All of the following are good resources for finding more information about contracts for independent security consultants except one. Which is the exception?

- a. Your own attorney
- b. Books on working as independent contractor
- c. Free contract templates on the Internet
- d. The attorney of the company with which you will be contracting

ANSWER:

a

Module 1 - Ethical Hacking Overview

32. Which of the following is a possibility when you work as a security professional?

- a. Causing a DoS attack inadvertently
- b. Violating federal law
- c. Being sued for slowing down a company's network
- d. All are possibilities.

ANSWER:

d

33. What skills does a security professional need to be successful?

- a. Knowledge of network and computer technology
- b. Ability to communicate with management and IT personnel
- c. Both knowledge of network and computer technology and the ability to communicate with management and IT personnel.
- d. Multiple IT certifications

ANSWER:

c

34. Which of the following might be a violation of a contract between an independent contractor and a company that hires them to run security tests?

- a. The independent contractor runs a program that prevents the employees from doing their jobs.
- b. The company offers the independent contractor a role within their IT department.
- c. The independent contractor signs an agreement written by the company's attorneys.
- d. The company requests that the independent contractor sign a nondisclosure agreement should the security testing reveal sensitive information such as usernames and passwords.

ANSWER:

a

35. What skill is most important when developing a written agreement between a security professional and a company that will be hiring them to execute a security assessment?

- a. knowledge of network and computer technology
- b. the breadth of the target organization's security presence
- c. the ability to apply the necessary tools to perform your task
- d. an understanding of the laws that apply to your location

ANSWER:

d

36. Penetration testing can create ethical, technical, and privacy concerns for a company's management team. What can a security consultant do to ensure the client fully understands the scope of testing that will be performed?

- a. create a contractual agreement
- b. create a lab demonstration
- c. create a virtual demonstration
- d. create a slide presentation

ANSWER:

a

Name _____ Class _____ Date _____
: _____ : _____ e: _____

Module 1 - Ethical Hacking Overview

37. Why is it a challenge and concern for an ethical hacker to avoid breaking any laws?

- a. People do not like hackers.
- b. The laws are constantly changing.
- c. It costs too much money to hire a lawyer.
- d. To avoid breaking laws, it is important to get certifications.

ANSWER:

b