Name: _____ Class: _____ Date: _____

Chapter 01: Ethical Hacking Overview

1. As a security tester, you can make a network impenetrable.

a. True
b. False

ANSWER: False

2. An ethical hacker is a person who performs most of the same activities a hacker does, but with the owner or company's permission.

a. True
b. False

ANSWER: True

3. Even though the Certified Information Systems Security Professional (CISSP) certification is not geared toward the technical IT professional, it has become one of the standards for many security professionals.

a. True
b. False

ANSWER: True

4. Penetration testers and security testers need technical skills to perform their duties effectively.

a. True
b. False

ANSWER: True

5. Port scanning is a noninvasive, nondestructive, and legal testing procedure that is protected by federal law.

a. True
b. False

ANSWER: False

6. 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

7. 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

Chapter 01: Ethical Hacking Overview

8. What derogatory title do experienced hackers, who are skilled computer operators, give to inexperienced hackers?

a. script kiddies
b. repetition monkeys
c. packet sniffers
d. crackers

ANSWER: a

9. What term best describes a person who hacks computer systems for political or social reasons?

a. cracktivist
b. hacktivist
c. sniffer
d. script kiddy

ANSWER: b

10. 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

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

ANSWER: a

12. What type of laws should a penetration tester or student learning hacking techniques be aware of?

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

ANSWER: d

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

Chapter 01: Ethical Hacking Overview

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

ANSWER: b

14. 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

15. 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

16. What security certification did the "The International Council of Electronic Commerce Consultants" (EC-Council) develop?

a. Security+
b. OSSTMM Professional Security Tester (OPST)
c. Certified Information Systems Security Professional (CISSP)
d. Certified Ethical Hacker (CEH)

ANSWER: d

17. What professional level security certification did the "International Information Systems Security Certification Consortium" (ISC2) develop?

a. Security+
b. OSSTMM Professional Security Tester (OPST)
c. Certified Information Systems Security Professional (CISSP)
d. Certified Ethical Hacker (CEH)

ANSWER: c

18. What subject area is not one of the 22 domains tested during the CEH exam?

a. Sniffers

Chapter 01: Ethical Hacking Overview

b. Social engineering
c. Footprinting
d. Trojan hijacking

ANSWER: d

19. What security certification uses the Open Source Security Testing Methodology Manual (OSSTMM) as its standardized methodology?

a. CEH
b. OPST
c. CISSP
d. GIAC

ANSWER: b

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

a. GIAC
b. OPST
c. CHIP
d. CEH

ANSWER: c

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

a. Fraud and Abuse Act
b. Interception Abuse Act
c. Electronic Communication Privacy Act
d. The Computer Fraud Act

ANSWER: c

22. What organization disseminates research documents on computer and network security worldwide at no cost?

a. EC-Council
b. SANS
c. ISECOM
d. ISC2

ANSWER: b

23. 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

Chapter 01: Ethical Hacking Overview

c. create a virtual demonstration
d. create a slide presentation

ANSWER: a

24. What 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

25. If you work for a company as a security professional, you will most likely be placed on a special team that will conduct penetration tests. What is the standard name for a team made up of security professionals?

a. pen team
b. blue team
c. red team
d. security team

ANSWER: c

26. 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

27. 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

28. What name is given to people who break into computer systems with the sole purpose to steal or destroy data?

a. packet monkeys
b. crackers
c. script kiddies
d. bots

Chapter 01: Ethical Hacking Overview

ANSWER: b

29. What professional level security certification requires five years of experience and is designed to focus on an applicant's security-related managerial skills?

a. Certified Information Systems Security Professional
b. Offensive Security Certified Professional
c. OSSTMM Professional Security Tester
d. Certified Ethical Hacker

ANSWER: a

30. 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

31. Why are ethical hackers employed or contracted by a company to conduct vulnerability assessments, penetration tests, and security tests?

ANSWER: Companies need to know what, if any, parts of their security infrastructure are vulnerable to attack. In a penetration test, an ethical hacker attempts to break into a company's network or applications to find weak links. In a vulnerability assessment, the tester tries to enumerate all the vulnerabilities found in an application or on a system. 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.

32. In the context of penetration testing, what is the gray box model?

ANSWER: The gray box model is a hybrid of the white and black box models. In this model, the company gives a tester only partial information. For example, the tester might get information about which OSs are used, but not get any network diagrams.

33. Why are employees sometimes not told that the company's computer systems are being monitored?

ANSWER: If a company knows that it's being monitored to assess the security of its systems, employees might behave more vigilantly and adhere to existing procedures. Many companies don't want this false sense of security; they want to see how personnel operate without forewarning that someone might attempt to attack their network.

34. List at least five domains tested for the Certified Ethical Hacker (CEH) exam.

ANSWER:
- Ethics and legal issues
- Footprinting
- Scanning
- Enumeration
- System hacking
- Trojan programs and backdoors
- Sniffers

Chapter 01: Ethical Hacking Overview

- Denial of service
- Social engineering
- Session hijacking
- Hacking Web servers
- Web application vulnerabilities
- Web-based password-cracking techniques
- Structured Query Language (SQL) injection
- Hacking wireless networks
- Viruses and worms
- Physical security
- Hacking Linux
- Intrusion detection systems (IDSs), firewalls, and honeypots
- Buffer overflows
- Cryptography
- Penetration-testing methodologies

35. What is the SANS Institutes "Top 25 Software Errors" list?

ANSWER: One of the most popular SANS Institute documents is the Top 25 Software Errors list, which describes the most common network exploits and suggests ways of correcting vulnerabilities. This list offers a wealth of information for penetration testers or security professionals.

36. A Security professional may think they are following the requirements set forth by the client who hired them to perform a security test, don't assume that management will be happy with the test results. Provide an example of an ethical hacking situation that might upset a manager.

ANSWER: One tester was reprimanded by a manager who was upset that the security testing revealed all the user names and passwords to the tester. The manager believed that the tester shouldn't know this information and considered stopping the security testing.

37. Describe some actions which security testers cannot perform legally.

ANSWER: Accessing a computer without permission, destroying data, or copying information without the owner's permission is illegal. Certain actions are illegal, such as installing worms or viruses on a computer network that deny users access to network resources. As a security tester, you must be careful that your actions do not prevent customers from doing their jobs. For example, DoS attacks should not be initiated on your customer's networks.

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

ANSWER: Because the job of an ethical hacker is fairly new, the laws are constantly changing. Even though a company has hired you to test its network for vulnerabilities, be careful that you aren't breaking any laws for your state or country. If you're worried that one of your tests might slow down the network because of excessive bandwidth use, that concern should signal a red flag. The company might consider suing you for lost time or monies caused by this delay.

39. What are four different skills a security tester needs to be successful?

ANSWER:
- Knowledge of network and computer technology
- Ability to communicate with management and IT personnel
- An understanding of the laws that apply to your location
- Ability to apply the necessary tools to perform your tasks

Chapter 01: Ethical Hacking Overview

40. Why should a security professional or student learning hacking techniques be aware of the local, state, and federal laws that apply to their field of study?

ANSWER: Laws are written to protect society, but often the written words are open to interpretation. Having some hacking tools on your computer might be illegal. You should contact local law enforcement agencies and ask about the laws governing your state or country before installing hacking tools on your computer. The point of mentioning laws and regulations is to make sure you're aware of the dangers of being a security tester.

Match each item with a statement below.

a. script kiddies
b. red team
c. black box model
d. crackers
e. vulnerability assessment
f. security test
g. hacker
h. gray box model
i. ethical hacker
j. penetration test

41. Inexperienced people who copy code or use tools created by knowledgeable programmers

ANSWER: a

42. A group of people with varied skills who perform penetration tests

ANSWER: b

43. A test that does not divulge to staff that penetration testing is being conducted or disclose what technologies the company is using to the security professional

ANSWER: c

44. A person who breaks into systems to steal or destroy data

ANSWER: d

45. An attempt to identify all the unprotected areas found in an application or on a system

ANSWER: e

46. Analysis of a company's security policy and procedures followed with a report disclosing any vulnerabilities to management

ANSWER: f

47. An individual who breaks into a computer system illegally

ANSWER: g

48. Hybrid of the white and black box models used for penetration testing

ANSWER: h

Chapter 01: Ethical Hacking Overview

49. An individual who breaks into a company's computer system legally when employed or contracted by that company
ANSWER: i

50. An ethical attempt to break into a company's network or applications to find weak links
ANSWER: j