Computer Security and Penetration Testing, Second Edition

Review Questions with Answers

Chapter 1: Ethics of Hacking and Cracking

1. Using the W/B Hat model, which hacker is more likely to make up a Web site to teach new hackers how to hack a network?

   Gray Hat

2. Using the W/B Hat model, which hacker is most likely to work as a network administrator?

   White Hat

3. Using the W/B Hat model, which hacker is most likely to share information?

   Gray Hat

4. Using the W/B Hat model, which hacker is selling credit card numbers to criminals online?

   Black Hat

5. When presenting a talk to a group of business leaders, are you more likely to use the W/B Hat model to explain the dangers posed by hackers or the Hacker Profiles model? If the business leaders were the Chief Information Officers of their respective companies, would you reverse your decision? (Short essay, no more than two pages, please.)

6. If your web site is hacked and all the pages call up the same anti-war slogan and picture, which profile of hacker has hit your site?

   Probably a Hactivist

7. If it is discovered that the CEO's e-mail browser is set to automatically copy all her outgoing mail to an unknown account called *asmith@thecompany.com*, what profile of hacker is probably responsible?

   Internal person (80% or more hacks are internal.)

8. What Hacker Profile tries out attack scripts they find on the internet, "just to see what happens?"

Novices. Another right answer, at least in the jargon used by IT people, is “scrtipt-kiddie.”

9. Name a trend that has arisen from the hacker mindset of the 1950s?

   Open-source software

10. What are the motivations for the Hacker Profile, “professional criminal?”

    Financial gain

Indicate whether the sentence or statement is true or false.

11. _____ As a security tester, you can make a network impenetrable.

    False

12. _____ An ethical hacker is a person who performs most of the same activities a cracker does, but only late at night.

    False

13. The SysAdmin, Audit, Network, Security (SANS) Institute offers training and IT security certifications through Global Information Assurance Certification (GIAC).

    True

14. _____ The GIAC program offers a certification that focuses on reverse-engineering malware.

    True

15. _____ All states look at port scanning as noninvasive or nondestructive in nature and deem it legal.

    False

16. _____ Old-Guard hackers brag incessantly about their successful exploits.

    False

Match each term with the correct statement below.

a.	script	c.	novice
b.	port scanning	d.	ethical hacker

17. _____ Way to find open ports on a system

    b

18. _____ Copies code from knowledgeable programmers instead of creating the code himself/herself

    c

19. _____ Set of instructions that runs in sequence to perform tasks on a computer system

    a

20. _____ Sometimes employed by companies to perform penetration tests

    d