Chapter 1: Ethical Hacking Overview

TRUE/FALSE

1. As a security tester, you can't make a network impenetrable.

   ANS: T PTS: 1 REF: 2

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

   ANS: F PTS: 1 REF: 3

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.

   ANS: T PTS: 1 REF: 7

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

   ANS: T PTS: 1 REF: 8

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

   ANS: F PTS: 1 REF: 11

MULTIPLE CHOICE

1. In a(n) ____, the tester does more than attempt to break in; he or she also analyzes the company's security policy and procedures and reports any vulnerabilities to management.

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

   ANS: B PTS: 1 REF: 2

2. ____ takes penetration testing to a higher level.

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

   ANS: C PTS: 1 REF: 2

3. Some hackers are skillful computer operators, but others are younger inexperienced people who experienced hackers refer to as ____.

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

   ANS: A PTS: 1 REF: 3

4. The U.S. Department of Justice labels all illegal access to computer or network systems as "____".

   a. cracking c. sniffing
   b. hacking d. trafficking

ANS: B PTS: 1 REF: 3

5. Many experienced penetration testers can write computer programs or ____ in Perl or the C language to carry out network attacks.
a. kiddies
b. packets
c. scripts
d. crackers

ANS: C PTS: 1 REF: 3

6. The collection of tools for conducting vulnerability assessments and attacks is sometimes referred to as a "____".
a. black box
b. white box
c. gray box
d. tiger box

ANS: D PTS: 1 REF: 4

7. Penetration testers and security testers usually have a laptop computer configured with ____ and hacking tools.
a. multiple OSs
b. tiger boxes
c. packet sniffers
d. script kiddies

ANS: A PTS: 1 REF: 4

8. An April 2009 article in *USA Today* revealed that the federal government is looking for ____ to pay them to secure the nation's networks.
a. crackers
b. IT professionals
c. hackers
d. security testers

ANS: C PTS: 1 REF: 4

9. In the ____ model, the company might print a network diagram showing all the company's routers, switches, firewalls, and intrusion detection systems (IDSs) 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. gray box

ANS: B PTS: 1 REF: 4

10. In the ____ model, management does not divulge to staff that penetration testing is being conducted, nor does it give the tester any diagrams or describe what technologies the company is using.
a. gray box
b. white box
c. black box
d. red box

ANS: C PTS: 1 REF: 5

11. The International Council of Electronic Commerce Consultants (EC-Council) has developed a certification designation called ____.
a. CompTIA Security+
b. OSSTMM Professional Security Tester (OPST)
c. Certified Information Systems Security Professional (CISSP)
d. Certified Ethical Hacker (CEH)

ANS: D PTS: 1 REF: 6

12. Currently, the CEH exam is based on ____ domains (subject areas) with which the tester must be familiar.

a. 11
b. 22
c. 31
d. 41

ANS: B PTS: 1 REF: 6

13. “____” is not a domain tested for the CEH exam.
a. Sniffers
b. Social engineering
c. Footprinting
d. Red team testing

ANS: D PTS: 1 REF: 6

14. The ____ certification is designated by the Institute for Security and Open Methodologies (ISECOM), a nonprofit organization that provides security training and certification programs for security professionals.
a. CompTIA Security+
b. OSSTMM Professional Security Tester (OPST)
c. Certified Information Systems Security Professional (CISSP)
d. Certified Ethical Hacker (CEH)

ANS: B PTS: 1 REF: 7

15. The ____ certification for security professionals is issued by the International Information Systems Security Certifications Consortium (ISC^2).
a. Global Information Assurance Certification (GIAC)
b. OSSTMM Professional Security Tester (OPST)
c. Certified Information Systems Security Professional (CISSP)
d. Certified Ethical Hacker (CEH)

ANS: C PTS: 1 REF: 7

16. The ____ certification uses the Open Source Security Testing Methodology Manual (OSSTMM), written by Peter Herzog, as its standardized methodology.
a. CEH
b. OPST
c. CISSP
d. GIAC

ANS: B PTS: 1 REF: 7

17. The ____ disseminates research documents on computer and network security worldwide at no cost.
a. International Council of Electronic Commerce Consultants (EC-Council)
b. SysAdmin,Audit,Network, Security (SANS) Institute
c. Institute for Security and Open Methodologies (ISECOM)
d. International Information Systems Security Certifications Consortium (ISC^2)

ANS: B PTS: 1 REF: 8

18. The SysAdmin,Audit,Network, Security (SANS) Institute offers training and IT security certifications through ____.
a. Global Information Assurance Certification (GIAC)
b. OSSTMM Professional Security Tester (OPST)
c. Certified Information Systems Security Professional (CISSP)
d. Certified Ethical Hacker (CEH)

ANS: A PTS: 1 REF: 8

19. The ____ Institute Top 20 list details the most common network exploits and suggests ways of correcting vulnerabilities.

a. SANS
b. CompTIA
c. CERT
d. ISECOM

ANS: A PTS: 1 REF: 8

20. Some of the most infamous cases are hacks carried out by ____ students, such as the eBay hack of 1999.
a. graduate
b. high-school
c. college
d. engineering

ANS: C PTS: 1 REF: 10

21. A ____ can be created that welcomes new users joining a chat session, even though a person isn't actually present to welcome them.
a. byte
b. packet
c. switch
d. bot

ANS: D PTS: 1 REF: 13

COMPLETION

1. In a(n) ____________________, an ethical hacker attempts to break into a company's network to find the weakest link in that network or one of its systems.

ANS: penetration test

PTS: 1 REF: 2

2. Those who break into systems to steal or destroy data are often referred to as ____________________.

ANS: crackers

PTS: 1 REF: 3

3. In the ____________________ model, the tester is told what network topology and technology the company is using and is given permission to interview IT personnel and company employees.

ANS: white box

PTS: 1 REF: 4

4. The U.S. government now has a new branch of computer crime called ____.

ANS:
computer hacking and intellectual property (CHIP)
CHIP
computer hacking and intellectual property

PTS: 1 REF: 13

5. Employees of a security company are protected under the company's ____________________ with the client.

ANS: contract

PTS: 1 REF: 15

MATCHING

Match each term with the correct statement below.

a. script
b. red team
c. black box model
d. packet monkey
e. IRC "bot"
f. packet monkey
g. hacker
h. gray box model
i. ethical hacker

1. Derogatory term referring to people who copy code from knowledgeable programmers instead of creating the code themselves.
2. the tester might get information about which OSs are used, but not get any network diagrams
3. copies code from knowledgeable programmers instead of creating the code himself/herself
4. set of instructions that runs in sequence to perform tasks on a computer system
5. sometimes employed by companies to perform penetration tests
6. puts the burden on the tester to find out what technologies the company is using
7. program that sends automatic responses to users, giving the appearance of a person being present on the other side of the connection
8. composed of people with varied skills who perform penetration tests
9. accesses a computer system or network without the authorization of the system's owner

1. ANS: D PTS: 1 REF: 3
2. ANS: H PTS: 1 REF: 5
3. ANS: F PTS: 1 REF: 3
4. ANS: A PTS: 1 REF: 3
5. ANS: I PTS: 1 REF: 2
6. ANS: C PTS: 1 REF: 5
7. ANS: E PTS: 1 REF: 13
8. ANS: B PTS: 1 REF: 6
9. ANS: G PTS: 1 REF: 3

SHORT ANSWER

1. Ethical hackers are employed or contracted by a company to do what illegal hackers do: break in. Why?

   ANS:
   Companies need to know what, if any, parts of their security infrastructure are vulnerable to attack. To protect a company's network, many security professionals recognize that knowing what tools the bad guys use and how they think enables them to better protect (harden) a network's security.

   PTS: 1 REF: 2

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

   ANS:

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.

PTS: 1 REF: 5

3. Why are employees sometimes not told that the company is being monitored?

ANS:
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.

PTS: 1 REF: 5

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

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

PTS: 1 REF: 6

5. What is the SANS Institute Top 20 list?

ANS:
One of the most popular SANS Institute documents is the Top 20 list, which details the most common network exploits and suggests ways of correcting vulnerabilities. This list offers a wealth of information for penetration testers or security professionals.

PTS: 1 REF: 8

6. Even though you might think you're following the requirements set forth by the client who hired you to perform a security test, don't assume that management will be happy with your results. Provide an example of an ethical hacking situation that might upset a manager.

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

   PTS: 1 REF: 14

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

   ANS:
   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 don't prevent customers from doing their jobs. For example, DoS attacks should not be initiated on your customer's networks.

   PTS: 1 REF: 14-15

8. Why is it hard for an ethical hacker to avoid breaking any laws?

   ANS:
   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.

   PTS: 1 REF: 16

9. What are four different skills a security tester needs?

   ANS:
   - 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

   PTS: 1 REF: 16

10. If being liked by others is important to you, you might want to consider a different profession than penetration testing. Why?

    ANS:
    If you're good at your job, many IT employees resent you discovering vulnerabilities in their systems. In fact, it's the only profession in which the better you do your job, the more enemies you make!

    PTS: 1 REF: 17