CHAPTER10—PCI DSS COMPLIANCE

TRUE/FALSE

1.Because it is a perimeter defense strategy, a firewall is not a critical element of cardholder data security.
A. True
B. False

ANS: B

2. Use WEP to secure communications sent over a wired network.
A. True
B. False

ANS: B

3. PSS DSS is a set of standards designed to help organizations that process credit card payments prevent fraud by having increased control over data and its exposure.
A. True
B. False

ANS: A

4. Merchants should not develop a two-factor authentication scheme to protect access to cardholder data.
A. True
B. False

ANS: B

MULTIPLE CHOICE

1. You are tasked with designing a security policy for cardholder data. Which of the following is not a recommended security strategy for cardholder data?
A. Verify that data is retained for a limited period of time.
B. Verify that user groups are used to access sensitive data areas.
C. Verify that data is disposed of properly.
D. Verify that passwords are encrypted during transmission.

ANS: C

2. Which of the following firewall considerations is not recommended by the PCI Security Standards Council?
A. Use open source firewall systems.
B. Block unused ports.
C. Use host-based firewall systems on mobile computers.

D. Conduct periodic reviews of firewall and router set rules.

ANS: A

MULTIPLE RESPONSE

1. Which of the following elements are typically examined during a PCI DSS Security Assessment? (Select two.)
A. Firewalls
B. Network hardware
C. Employee background
D. Cached files

ANS: A,B

CHAPTER11—TESTING AND QA

TRUE/FALSE

1.The bounce rate identifies the percentage of people who leave your site from the page they initially visited.
A. True
B. False

ANS:A

2. Recovery testing analyzes how an application manages in the aftermath of failures and crashes.
A. True
B. False

ANS:A

3. Regulations are set by organizations and not by applicable laws.
A. True
B. False

ANS:B

4.Standards are typically non-enforceable while suggestions are used to guarantee a level of quality and performance.
A. True
B. False

ANS:B

MULTIPLE CHOICE

1. As a software developer, you have recently coded a security patch to a Web application. Which of the

following might you do after finishing the patch?
A. Perform a regression test
B. Perform a compatibility test
C. Perform a suitability test
D. Perform a gray box test

ANS:A

2.You have completed an application and now wonder if it will work with both the Microsoft Internet Explorer and Mozilla Firefox Web browsers. Which of the following tests might you perform?
A. Unit test
B. Universal acceptance test
C. Compatibility test
D. System test

ANS:C

3. You are using a testing mechanism that looks at the input and output of an application to determine potential problems. Which mechanisms may not be in use?
A. Black box testing
B. White box testing
C. Gray box testing
D. Brown box testing

ANS:D

4. Which of the following is often developed by first creating a risk analysis?
A. Web rules
B. Test software
C. Security policies
D. SDLCs

ANS:C

CHAPTER12—Vulnerability and Security Assessment

TRUE/FALSE

1.The "percentage of vulnerabilities not found" metric is a useful way of reporting assessment data.
A.True
B.False

ANS:F

2. Web site forms and user input felds are often attacked using cross-site scripting.

A.True
B.False
ANS:T

3.OWASP is the organization known for developing secure application development standards and practices.
A.True
B.False

ANS:T

4.Unauthenticated scanning requires the scanner logging onto the systems being assessed.
A.True
B.False

ANS:F

MULTIPLE CHOICE

1.How many tiers are commonly used for Web sites?
A. 2
B. 1
C. 3
D. 4

ANS:C

2.Ping sweeps are a part of what process?
A. Code review
B. Discovery
C. Attack vectors
D. Remediation

ANS:B

3.Which section of the assessment report is intended to be a high-level briefing of the findings?
A. Summary of findings
B. Vulnerability findings
C. Recommendations
D. Executive summary

ANS:D

4. An in-depth security assessment of a Web server application includes performing which of the following?
A. Error-based code compiling
B. OS patching
C. A source code review
D. TCP/IP routing

ANS:C

5.Nmap’s primary features doesn't include which of the following?
A. Password cracking
B. OS fingerprinting
C. Port scanning
D. Ping sweeps

ANS:A

6.What is the purpose of exploiting a vulnerability or a weakness in a system to gain access to resources not otherwise available to the attacker or tester?
A. Acceleration
B. Enumeration
C. Privilege escalation
D. Field injection

ANS:C

7. Which attack involves exploring the files and folders of a Web server by manipulating URLs?
A. Man-in-the-middle
B. Buffer underflow
C. Brute force password attacks
D. Directory traversal attacks

ANS:D