CHAPTER 6

1. _____ is an example of the insufficiency of security by obscurity.

    a. Broken authentication and session management
    b. Insecure cryptographic storage
    c. ID or password login failure
    d. Failure to restrict URL access

2. _____ enables attackers to inject client-side scripts into Web pages.

    a. XSS
    b. Malicious file execution
    c. Insecure direct object reference
    d. Cross-site request forgery

3. _____ exploits a Web site's trust for the user's browser.

    a. XSS
    b. Malicious file execution
    c. Insecure direct object reference
    d. Cross-site request forgery

4. _____ involves protecting sensitive data through encryption.

    a. Broken authentication and session management
    b. Insecure cryptographic storage
    c. Insecure communications
    d. Failure to restrict URL access

5. Which of the following helps to ensure the confidentiality and integrity of data communications?

    a. DNS
    b. SNMP
    c. IPSec
    d. TCP/IP

6. Which of the following is the standard security technology for establishing an encrypted link between a Web server and a Web browser?

    a. DNS
    b. SSL
    c. IPSec
    d. XSS

7. What uses Authentication Header (AH) and Encapsulating Security Payload (ESP) to create secure data transmissions?

a. DNS
b. SSL
c. IPSec
d. XSS

8. What does a Web server require to create SSL connections?

    a. A certificate
    b. IPSec
    c. Error-tracing functionality
    d. A stored XSS script

9. Which of the following is a means of authentication?

    a. Public key infrastructure (PKI)
    b. Kerberos
    c. Both A and B
    d. Neither A nor B

10. DES and Triple DES are forms of _____.

    a. attacks
    b. authentication systems
    c. online security protocols
    d. encryption

11. Your sales and marketing department wants to know which Web sites your visitors browse before coming to your site. Which type of tool is the best choice for providing this information?

    a. Cross-site scripting
    b. Web site analytics
    c. A user input form
    d. A search engine

12. You are designing your first Web site and want to be sure your design is useful and appealing to the appropriate audience. Which tool is the best choice?

    a. Web site analytics
    b. A Contact Us form
    c. A customer profile
    d. An online survey

13. On your e-commerce ticket-selling Web site, your Web site developer set a short time period for trusted user sessions. A user who doesn't respond to prompts within two minutes is automatically logged off the system. Which type of attack can this help prevent?

    a. Cross-site request forgery
    b. XSS
    c. Insecure direct object reference

d. Malicious file execution

14. Which of the following is **not** true of input validation?

a. Server-side input validation is easier to exploit than client-side validation.
b. It is a form of filtering.
c. Unexpected or unwanted input is automatically rejected and the underlying database remains inaccessible.
d. It is a good first line of defense against injection flaw attacks.

15. Which of the following generally does **not** help to mitigate cross-site request forgery attacks?

a. Log out of all secure Web sites immediately after finishing the session.
b. Periodically delete cookies in the local browser.
c. Ensure Web browsers are up to date.
d. Disable USB ports on all servers.

Chapter 6 Answer Key

Question Number	Correct Answer	Reference in Course	
		Source	Page (s)
1.	d	Chapter 6	163
2.	a	Chapter 6	150
3.	d	Chapter 6	154
4.	b	Chapter 6	159
5.	c	Chapter 6	160-161
6.	b	Chapter 6	162
7.	c	Chapter 6	161
8.	a	Chapter 6	162
9.	c	Chapter 6	161
10.	d	Chapter 6	162
11.	b	Chapter 6	143-144
12.	c	Chapter 6	146-147
13.	a	Chapter 6	154-155
14.	a	Chapter 6	152
15.	d	Chapter 6	154-155

CHAPTER 7

1. Which of the following best describes a brute-force attack?

    a. An attempt to overwhelm a Web server with service requests
    b. An attack that takes advantage of a Web server's unpatched vulnerabilities
    c. An attack that attempts to crack a cryptographic key or password simply by guessing
    d. An attempt to physically break into a system by manual force

2. A common attack in which a client's cookies, security tokens, or other personal information is obtained and used to impersonate the user is referred to as _____.

    a. cross-site scripting
    b. rootkitting
    c. Denial of Service
    d. fingerprinting

3. Which of the following is a root cause of SQL injection attacks?

    a. A database server that runs on a standard port
    b. An input data that is not properly filtered
    c. An SQL query that has too many joins
    d. A client's browser that is still using the older HTTP protocol

4. Which of the following techniques would help a Web application to properly validate user input?

    a. Cleansing all data in the database
    b. Blacklisting unknown IP addresses
    c. Whitelisting and accepting only known good characters
    d. Using SSL for all user input

5. Which of the following could be the end result for a Web application that doesn't have proper Transport layer protection?

    a. Personal data sent from the browser could be intercepted and read by others.
    b. IP addresses could be redirected to a malicious Web site.
    c. The Web site is vulnerable to cross-site scripting attacks.
    d. The Web site is vulnerable to SQL injection attacks.

6. Which type of attack primarily gathers information about a target system, such as the operating system version and network architecture?

    a. Cross-site scripting
    b. Content spoofing
    c. Denial of Service
    d. Fingerprinting

7. Which type of attack uses a fake Web site or Web application to fool victims into thinking it is a legitimate one?

    a. Cross-site scripting
    b. Content spoofing
    c. Denial of Service
    d. Fingerprinting

8. Password policies, such as account lockout duration and maximum password age, are helpful in protecting against what type of attack?

    a. Content spoofing
    b. Denial of Service
    c. Brute force
    d. Fingerprinting

9. What is the primary vulnerability of buffer overflow attacks?

    a. Hardware malfunctions
    b. Application programming errors
    c. Weak passwords
    d. Web browser cookies

10. Which of the following attacks does **not** use impersonation techniques?

    a. Credential/session prediction
    b. Cross-site scripting
    c. Session fixation
    d. Denial of Service

11. You want to determine if your Web site has been under a brute-force attack. Which of the following should you review first?

    a. Log files
    b. Web server backup files
    c. Web site analytics results
    d. Web server directory structure

12. You are increasing the security of your Windows 7 computers by configuring an account lockout duration. You want users who enter the wrong credentials to remain locked out until an administrator unlocks the account. Which value should you use?

    a. 0
    b. 1
    c. 5
    d. 30

13. Which of the following is generally **not** a result of a buffer overflow attack?

a. The attacker crashes an application or process.
b. The attacker modifies an application or process.
c. The attacker takes temporary pwnership of an application or process.
d. The attacker upgrades the application.

14. An e-mail spammer exploits SMTP and IMAP injection vulnerabilities to obtain e-mail addresses. Which attack is being described?

    a. SQL injection
    b. Fingerprinting
    c. Mail command injection
    d. HTTP request splitting

15. In a path traversal attack, the attacker commonly uses _____ to navigate the directory tree to access files in other directories.

    a. Windows Explorer
    b. ../
    c. boolean characters
    d. None of the above

16. Which of the following is **not** commonly a source of data leakage?

    a. Encrypted data
    b. Error messages
    c. Employee e-mails
    d. Unsecured backups

17. Which term refers to the way an application controls the data it produces, such as log data, error messages, or raw data passed to another application?

    a. Input handling
    b. Whitelisting
    c. Output handling
    d. Output stripping

Chapter 7 Answer Key

Question Number	Correct Answer	Reference in Course	
		Source	Page (s)
1.	c	Chapter 7	170
2.	a	Chapter 7	174-175
3.	b	Chapter 7	184
4.	c	Chapter 7	191
5.	a	Chapter 7	195
6.	d	Chapter 7	176
7.	b	Chapter 7	172
8.	c	Chapter 7	170-173
9.	b	Chapter 7	172
10.	d	Chapter 7	174, 175, 182,
11.	a	Chapter 7	170
12.	a	Chapter 7	171
13.	d	Chapter 7	172
14.	c	Chapter 7	179
15.	b	Chapter 7	180-181
16.	a	Chapter 7	191
17.	c	Chapter 7	191

CHAPTER 8

1. Developers should assume all data entered by a user is _____.

    a. malicious
    b. string character type
    c. verifiable
    d. validated

2. Which of the following is the oldest and best-known model of SDLC?

    a. Agile
    b. Waterfall
    c. Extreme
    d. Rational unified process

3. What is one of the most commonly exploited areas of interactive Web applications today?

    a. HTTP header manipulation
    b. User input
    c. Session information
    d. None of the above

4. How are dynamic Web applications that accept user input susceptible to insecure coding practices?

    a. User data can be authenticated but not validated.
    b. Developers can fail to properly validate data on the server side.
    c. Developers can fail to properly validate input on the client side.
    d. Encrypted user connections expose programming security holes.

5. What type of validation is more important from a security perspective for a Web application?

    a. Server side
    b. Client side
    c. Browser side
    d. Network side

6. What protocol should be used when transferring confidential data in a Web application?

    a. HTTP
    b. SMTP
    c. HTTPS
    d. FTP

7. Consider a person who logs into a Web site with a username and password. Which process allows the user access based upon correct credentials?

a. Authorization
b. Accountability
c. Authentication
d. Auditing

8. Consider a person who logs into a Web site with a username and password. Which process tracks mechanisms used to keep a record of events on the system?

a. Authorization
b. Accountability
c. Authentication
d. Auditing

9. What is a markup language that uses code for formatting a Web site within a text file?

a. HTML
b. HTTP
c. SSL
d. TCP/IP

10. What is one of several HTML tags that an attacker can place in a message posted to a message board to run malicious content?

a. <body>
b. <h1>
c. <script>
d. <p>

11. What is Common Gateway Interface (CGI)?

a. A programming language
b. Another name for JavaScript
c. A type of Web-based attack
d. A standard

12. Sanitization is commonly associated with which of the following?

a. Bank account protection
b. User input
c. HTML tagging
d. Software testing

13. During which stage of the software development life cycle do developers generally incorporate security coding?

a. Systems Analysis
b. Design
c. Implementation

d. Testing

14. During which stage of the software development life cycle do developers clearly establish an application's features and operational functions?

    a. Maintenance
    b. Design
    c. Implementation
    d. Testing

15. During which stage of the software development life cycle do developers create service packs, review logs, and review error reports?

    a. Maintenance
    b. Design
    c. Implementation
    d. Testing

16. What is the secure version of Hypertext Transfer Protocol?

    a. SFTP
    b. E-HTTP
    c. SSH
    d. HTTPS

17. Secure Sockets Layer (SSL) uses what type of process to authenticate a service to a client?

    a. Handshake
    b. High five
    c. Accounting
    d. Labeling

18. Which access control method assigns sensitivity labels to objects and compares them to the user's assigned level of sensitivity?

    a. Discretionary access control (DAC)
    b. Mandatory access control (MAC)
    c. Both A and B
    d. Neither A nor B

19. Which of the following is a type of mandatory access control (MAC)?

    a. Rule-based access control
    b. Role-based access control
    c. Both A and B
    d. Neither A nor B

20. Of the following, what is the best method of preventing log files and audit files from being read by a malicious user?

    a. Implement access controls and use the principle of least privilege.
    b. Santize the log and audit files.
    c. Validate the log and audit files.
    d. Hide the log and audit files in a deeply nested folder on the server.

Chapter 8 Answer Key

Question Number	Correct Answer	Reference in Course	
		Source	Page (s)
1.	a	Chapter 8	201-202
2.	b	Chapter 8	207
3.	b	Chapter 8	201
4.	b	Chapter 8	202, 210
5.	a	Chapter 8	202
6.	c	Chapter 8	212-213
7.	c	Chapter 8	216
8.	b	Chapter 8	216
9.	a	Chapter 8	204
10.	c	Chapter 8	204-205
11.	d	Chapter 8	205
12.	b	Chapter 8	202
13.	c	Chapter 8	210
14.	b	Chapter 8	210
15.	a	Chapter 8	211
16.	d	Chapter 8	212
17.	a	Chapter 8	213
18.	b	Chapter 8	218
19.	c	Chapter 8	218-219
20.	a	Chapter 8	221

CHAPTER 9

1. _____ can be used to prevent users or processes in a particular area of an application from damaging the wider system.

    a. HTML
    b. HTTPS
    c. Sandbox security
    d. Buffer overflows

2. Which layer of a Web application is exploited by an SQL injection?

    a. Database
    b. File system
    c. Application server
    d. Web server

3. Which of the following is **not** an advantage of software configuration management (SCM)?

    a. Ensures greater control
    b. Prevents unauthorized changes
    c. Allows easier management of the software
    d. Can be used in the place of traditional backups

1. What does XSS exploit in a Web application?

    a. Weak accountability
    b. Misconfigured servers
    c. Buffer overflows
    d. Invalidated user input

2. Which Web technology allows a Web application's logged-on users to use the application continuously without having to log in each time a page is refreshed?

    a. Session management
    b. Elevation of privileges
    c. Fault tolerance
    d. HTTP management

3. Poorly written code that sends the processor into panic, consumes all resources, and ends as a denial of service is referred to as a _____.

    a. Integer wraparound
    b. lock
    c. race condition
    d. buffer overflow

4. What secure coding best practice dictates that users are restricted to necessary permissions and access levels?

    a. Authentication
    b. Principle of least privilege
    c. Layered Security
    d. Accountability

5. Which of the following is **not** an advantage of revision-level tracking?

    a. Prevents unauthorized changes
    b. Provides ease of management
    c. Provides quality control
    d. Provides automated code reviews

6. Which of the following is **not** a fundamental aspect of the JavaScript secure coding standards?

    a. Prefer to have obviously no flaws than no obvious flaws.
    b. Avoid duplication.
    c. Restrict privileges.
    d. Use dynamic SQL.

7. Which of the following is true of Common Gateway Interface (CGI)?

    a. It is a programming language.
    b. It is type of encrypted communication.
    c. You can create CGI scripts in C, C++, Perl, and Java.
    d. You use CGI mainly to create static Web pages.

8. Your company is preparing to launch a SQL database with a custom front-end interface. You are working with the development team on protection strategies. Of the following, which is the best choice for protecting your new SQL database and its contents?

    a. Use input validation.
    b. Allow only administrative accounts to access the database.
    c. Use many different and detailed error messages so users can be exact when reporting problems to tech support.
    d. Duplicate data within the database for redundancy purposes.

9. Which of the following is a best practice for coding in HTML?

    a. Do not encrypt the HTML code.
    b. Keep the code clean and simple.
    c. Constantly check all source code for unexpected changes.
    d. For efficiency, validate forms or URLs, but not both.

10. What is **not** a secure coding practice?

a. Pay attention to compiler warnings.
b. Plan and design for security policies.
c. Allow access by default.
d. Sanitize data sent to other systems.

11. You are developing a Web application that will capture data input by users, and then transfer that data to other systems in your company. Which of the following should you avoid when creating the application?

    a. A secure coding standard
    b. Data sanitization
    c. Layered security
    d. Open directories

12. You are a disgruntled software coder. You are designing an authentication process for a Linux-driven Web application that will allow commands to run the application as the account with the highest privileges—the root user in Linux. After you leave the company, you plan to sabotage the company's data. What is this type of access called?

    a. Elevation of privilege
    b. Data tampering
    c. Run as administrator
    d. Session privilege

Chapter 9 Answer Key

Question Number	Correct Answer	Reference in Course	
		Source	Page (s)
1.	c	Chapter 9	239
2.	a	Chapter 9	228
3.	d	Chapter 9	242
4.	d	Chapter 9	228
5.	a	Chapter 9	228-229
6.	c	Chapter 9	230
7.	b	Chapter 9	232, 236
8.	d	Chapter 9	242
9.	d	Chapter 9	238-239
10.	c	Chapter 9	240
11.	a	Chapter 9	241
12.	b	Chapter 9	237-238
13.	c	Chapter 9	236-237
14.	d	Chapter 9	236-238
15.	a	Chapter 9	227

CHAPTER 10

1. Which of the following statements best describes the PCI DSS?

    a. A set of widely accepted requirements set by major credit card companies to enhance data security for online payments
    b. A federal law to enhance data security for online payments
    c. A standard set of requirements by credit card companies to enforce an encryption algorithm during online payments
    d. A federal law to enforce an encryption algorithm during online payments

2. What type of network topology does PCI DSS recommend for services that need to be accessed by both internal and external sources?

    a. Switches
    b. Hubs
    c. DMZ
    d. VLAN

3. Which of the following will result in noncompliance with the requirements of PCI DSS?

    a. Not storing card account number in an unreadable format
    b. Not maintaining a password change policy
    c. Not encrypting transmission when a user changes his or her e-mail preferences on the Web site
    d. Not providing the ability to refund card charges on the Web site

4. Which of the following merchant levels must scan the networks at least quarterly to be in compliance with PCI DSS?

    a. Level 1 (more than 6 million transactions a year)
    b. Level 2 (1 million to 6 million transactions a year)
    c. Level 3 (20,000 to 1 million transactions a year)
    d. All merchants, no matter the size, must scan at least quarterly

5. Storing which of the following data items is prohibited in PCI DSS requirements?

    a. Card validation codes
    b. Card expiration dates
    c. Card account number
    d. Card holder name

6. The Payment Card Industry Security Standards Council (PCI SSC) was formed by _____.

a. the federal government
b. the SEC
c. five major credit card companies
d. a consortium of nonprofit organizations

7. Handling of several transactions at one time is referred to as _____.

a. batch processing
b. real-time processing
c. transactional processing
d. delayed processing

8. An online merchant that experiences a security breach and found not to be in compliance with PCI DSS can:

a. Suffer monetary loss
b. Have lawsuits directed against them
c. Lose their reputation
d. All of the above

9. Which of the following merchant levels requires an annual onsite audit and quarterly network scans?

a. Level 1
b. Level 2
c. Levels 3 and 4
d. All of the above

10. Who performs the assessment to determine whether a merchant complies with PCI DSS standards?

a. A government representative
b. A QSA
c. A licensed CPA
d. A certified CISSP

11. The standard protocol used to allow systems across networks to synchronize their internal clocks is:

a. TLS
b. NTP
c. NIP
d. SNMP

12. Which of the following is **not** one of the twelve requirements for PCI DSS compliance?

a. Track and monitor all access to network resources and cardholder data.
b. Regularly test security systems and processes.

c. Maintain a policy that addresses security for employees and contractors.
d. Never store any of the cardholder's information in a database or other storage mechanism.

13. A consumer makes a credit card purchase at a gas station and the credit card is credited immediately. What is the name of this process?

    a. Batch processing
    b. Real-time processing
    c. Cash processing
    d. Delayed processing

14. During a PCI DSS compliance audit, the auditor selects representative elements of all the computer components in a merchant’s network and tests them for compliance. What is the name of this process?

    a. Imaging
    b. Batching
    c. Sampling
    d. Transactional metering

15. You are an auditor conducting a PCI DSS compliance audit. In addition to examining computer systems, you must also assess other components. Which of the following does not need to be assessed?

    a. Third-party services that store, process, or transmit cardholder information on behalf of your company
    b. The wireless network, if used to store, process, or transmit cardholder information
    c. Both A and B
    d. Neither A nor B

Chapter 10 Answer Key

Question Number	Correct Answer	Reference in Course	
		Source	Page (s)
1.	a	Chapter 10	248-250
2.	c	Chapter 10	254-257
3.	a	Chapter 10	257
4.	d	Chapter 10	250
5.	a	Chapter 10	257
6.	c	Chapter 10	248
7.	a	Chapter 10	247
8.	d	Chapter 10	250
9.	a	Chapter 10	250
10.	b	Chapter 10	251
11.	b	Chapter 10	252
12.	d	Chapter 10	255-263
13.	b	Chapter 10	248
14.	c	Chapter 10	253
15.	c	Chapter 10	252-253

CHAPTER 11

1. Which of the following best describes the difference between an organization's policies and an organization's guidelines?

    a. Guidelines are enforceable while policies are not.
    b. Policies are enforceable while guidelines are not.
    c. Policies define how procedures should be performed at a detailed level, while guidelines provide a general overview.
    d. The terms “policies” and “guidelines” may be used interchangeably.

2. Which best describes the white box testing methodology?

    a. The person testing assumes no knowledge of the inner code or application processing.
    b. The person testing examines the code of an application.
    c. The person testing checks for additional errors that may have been introduced in the process of upgrading or patching to fix other problems.
    d. The person testing combines individual software modules and tests as a group.

3. Which of the following would be a role of the software developer when an application is deployed to production?

    a. Handle customer support calls
    b. Monitor error messages
    c. Perform penetration testing
    d. Monitor system performance

4. Which of the following statements best describes bounce rate?

    a. The rate of users who have experienced an error message
    b. The rate of users who have server reset timeouts
    c. The rate of users who reload the Web page
    d. The rate of single-page visits to the Web site

5. Testing modified applications to ensure that no new errors have been introduced is commonly referred to as _____.

    a. regression testing
    b. unit testing
    c. penetration testing
    d. vulnerability testing

6. Which of the following can help you pinpoint problems with an e-commerce site?

a. Bounce rate
b. Shopping cart abandonment statistics
c. Visitor paths
d. All of the above

7. Testing an application to verify how well it functions with other software is commonly referred to as _____.

a. regression testing
b. unit testing
c. compatibility testing
d. software stress testing

8. Which best describes the integration testing methodology?

a. The person testing assumes no knowledge of the inner code or application processing.
b. The person testing examines the code of an application.
c. The person testing checks for additional errors that may have been introduced in the process of upgrading or patching to fix other problems.
d. The person testing combines individual software modules and tests as a group.

9. Testing an application by pushing it to its limits to detect breaking points is commonly referred to as _____.

a. regression testing
b. unit testing
c. compatibility testing
d. software stress testing

10. What is the primary purpose of the headline on a Web page?

a. To attract visitors' attention and entice them to keep reading
b. To ensure a higher SEO ranking
c. To show how your product or service solves an immediate problem
d. To tell your visitors what to do on your Web site

11. What is the primary purpose of the call to action on a Web page?

a. To attract visitors' attention and entice them to keep reading
b. To ensure a higher SEO ranking
c. To show how your product or service solves an immediate problem
d. To tell your visitors what to do on your Web site

12. You are designing a Web site that showcases and sells fine jewelry. Which of the following will be the most useful to your visitors?

a. A benefits statement
b. Clear images

c. A link to the About Us tab
d. A call to action

13. A programmer is coding a large Web application that has not yet gone live but wants to check only a small piece of the application. Which type of testing is most appropriate?

    a. Integration testing
    b. Black box test
    c. Unit testing
    d. Regression testing

14. The programming team has finished coding a large Web application that consists of multiple components. They want to check how individual components of the application work as a group. Which type of testing is most appropriate?

    a. Integration testing
    b. Black box test
    c. Unit testing
    d. Regression testing

15. The programming team has a prototype of a new, custom database interface for the company's SQL database. They want to determine whether it is intuitive or needs to be modified. Which type of testing is most appropriate?

    a. Performance testing
    b. Software stress testing
    c. Usability testing
    d. Recovery testing

16. You tested an application and found security holes. What is the first step you should take to mitigate the security deficiencies?

    a. Develop a mitigation plan.
    b. Outline vulnerabilities.
    c. Classify vulnerabilities and establish a priority.
    d. Retest.

17. After deploying a Web site application in a production environment, which of the following requires the quickest response time by developers?

    a. Responding to intermittent error messages about a resource limitation
    b. Responding to user feedback regarding a usability suggestion
    c. Responding to a security breach
    d. Enhancing features

18. Your e-commerce Web site analytics software indicates a high rate of shopping cart abandonment. What does this most likely indicate?

    a. A confusing checkout procedure on your Web site
    b. A lack of available consumer credit
    c. Unappealing products
    d. The wrong visitor demographic

19. You suspect that visitors are having difficulties navigating your Web site. Which Web site analytic statistic can help you determine if this is true?

    a. Visitor location
    b. Network performance
    c. Shopping cart abandonment
    d. Visitor path

20. You want to know which geographic areas your Web site visitors come from. Which Web site analytic statistic can provide this information?

    a. Visitor location
    b. Browser statistics
    c. Bounce rate
    d. Visitor path

Chapter 11 Answer Key

Question Number	Correct Answer	Reference in Course	
		Source	Page (s)
1.	b	Chapter 11	269-271
2.	b	Chapter 11	275
3.	b	Chapter 11	278
4.	d	Chapter 11	279
5.	a	Chapter 11	280
6.	d	Chapter 11	278-279
7.	c	Chapter 11	276
8.	d	Chapter 11	275
9.	d	Chapter 11	276
10.	a	Chapter 11	274
11.	d	Chapter 11	274
12.	b	Chapter 11	273-275
13.	c	Chapter 11	275
14.	a	Chapter 11	275
15.	c	Chapter 11	276
16.	b	Chapter 11	277
17.	c	Chapter 11	278
18.	a	Chapter 11	279
19.	d	Chapter 11	279
20.	a	Chapter 11	279

CHAPTER 12

1. What is the first step when performing a Web site security assessment?

    a. Perform penetration testing to discover vulnerabilities.
    b. Identify the components that make up the Web site.
    c. Attempt to escalate privileges on the Web site.
    d. Test forms for input validation.

2. When a Web site vulnerability assessment is completed, the report typically contains a CVE for each vulnerability. What does this represent?

    a. The vulnerability name and description
    b. The amount of exposure the vulnerability has gained in the past year
    c. The number that is used to determine its criticality or importance
    d. The number that uniquely identifies it across various security vendors and applications

3. Inserting unexpected data into a Web site's database query is commonly referred to as_____.

    a. SQL injection
    b. cross-site scripting
    c. database drafting
    d. phishing

4. Which of the following is typically the last step in performing a Web site security assessment?

    a. Ping sweeping
    b. Operating system detection
    c. Pen testing
    d. Reporting

5. When identifying components of a single-server Web site environment to test in a security assessment, you typically need to identify the Web server application, Web server front end, Web Server operating system, and _____.

    a. Web site forms
    b. network bandwidth
    c. firewall type
    d. wireless capabilities

6. Web sites typically consist of Web server software, a hardware server and operating system, a software application, and _____.

a. a POP3 server
b. an authentication server
c. a database server
d. a print server

7. Which phase of a Web security assessment involves conducting fingerprinting to help identify the components of the Web site platform?

a. Enumeration
b. Attack
c. Report
d. Penetration

8. Network Mapper (Nmap) would be a good tool choice to use for:

a. Port scanning
b. Validating data
c. Rootkit scanning
d. Penetration testing

9. Nessus® is a popular tool used primarily for _____.

a. ping sweeping
b. brute-force attacks
c. intrusion detection
d. vulnerability scanning

10. An e-commerce Web site that processes credit cards must comply with:

a. PCI DSS
b. HIPAA
c. Federal regulations
d. World Wide Web consortium standards

11. A planned attack performed during a Web site assessment is called:

a. Black-hat hacking
b. Penetration testing
c. Denial of Service
d. Gap analysis

12. The strategy used in a planned attack usually consists of developing attack plans, identifying security holes and gaps, and _____.

a. writing the report
b. attempting to escalate privilege
c. discovering the Web server type

d. creating automated attack plans

13. When performing an SQL injection attack, data is usually placed in form fields or in _____.

    a. JavaScript
    b. HTTP header
    c. URL
    d. CSS

14. Which of the following is a best practice for performing a security assessment and vulnerability scan?

    a. Ignoring authenticated testing and relying on non-authenticated scans.
    b. Hiring a black-hat hacker to perform the planned attacks.
    c. Using multiple tools for the same function.
    d. Ensuring that system administrators are unaware of the planned attacks.

15. Which section of a vulnerability and security assessment report is designed for management and highlights the most critical points throughout the report?

    a. Executive summary
    b. Summary of findings
    c. Recommended remediations
    d. None of the above

Chapter 12 Answer Key

Question Number	Correct Answer	Reference in Course	
		Source	Page (s)
1.	b	Chapter 12	285
2.	d	Chapter 12	303
3.	a	Chapter 12	300
4.	d	Chapter 12	301
5.	a	Chapter 12	291
6.	c	Chapter 12	285
7.	a	Chapter 12	285
8.	a	Chapter 12	287
9.	d	Chapter 12	289-290
10.	a	Chapter 12	295
11.	b	Chapter 12	297
12.	b	Chapter 12	297-298
13.	c	Chapter 12	300
14.	c	Chapter 12	305-306
15.	a	Chapter 12	301

CHAPTER 13

1. Which mobile network technology introduced the concept of global roaming, made data download speed up to 2 Mbps possible, and coined the term “mobile broadband”?

    a. 1G
    b. 2G
    c. 3G
    d. 4G

2. What advantage can whole-device encryption provide to the owner of a mobile device?

    a. The device is rendered inaccessible when away from the owner.
    b. Data is encrypted across the network.
    c. E-mail is encrypted.
    d. Data encryption is not needed when the device is in use.

3. What new risk will users of 4G networks encounter?

    a. Weaker encryption as compared to 3G networks
    b. Threat from viruses and other malware from IP-based systems
    c. Increased threat of eavesdropping from mobile network scanners
    d. Proprietary nature of the network can lock in customers

4. Which of the following mobile communication methods is subject to the least security risk?

    a. Voice calls
    b. Text messaging
    c. IM chat
    d. E-mail

5. Which of the following is **not** considered a best practice for improving the security of Web browsing on a mobile device?

    a. Enable JavaScript.
    b. Use a proxy server.
    c. Disable nonessential functions on the browser.
    d. Implement anti-phishing capabilities.

6. Which of the following is **not** considered a best practice for improving the security of a mobile device?

    a. Install or enable anti-malware functionality.
    b. Install or enable a firewall.
    c. Disable the encryption feature.
    d. Ensure the browser supports SSL.

7. Which feature generally distinguishes a smartphone from an ordinary cell phone?

a. Voice mail
b. SIM chip
c. Operating system
d. Numeric keypad

8. Which of the following is **not** considered an endpoint device?

    a. Server
    b. Smartphone
    c. Computer
    d. E-reader

9. You are responsible for acquiring networking equipment at work. One of your users would like a very lightweight, highly portable device to take on the road for checking e-mail and browsing the Internet. The device needs Wi-Fi and cellular connectivity, and an 8- to 10-inch screen. Value-add items include an MP3 player, an e-reader, and PDA features. Which would be the best choice for this user?

    a. Tablet PC, such as an iPad
    b. Smartphone
    c. Laptop computer
    d. E-reader

10. Which of the following is **not** true of mobile broadband?

    a. Includes WiMAX
    b. Includes Digital Enhanced Cordless Telecommunications (DECT)
    c. Is 3G technology
    d. Does not support video streaming

11. How does Multimedia Messaging Service (MMS) differ from Short Message Service (SMS)?

    a. Supports text messages and multimedia files
    b. Supports text messages only
    c. Works over a 3G connection
    d. Messages are generally smaller in size than SMS

12. Which type of endpoint communication is least susceptible to Denial of Service (DoS) attacks?

    a. E-mail
    b. Instant messaging/chat
    c. Internet browsing
    d. SMS messaging

13. Which type of endpoint communication is unlikely to experience data compromise?

    a. E-mail
    b. Instant messaging/chat

c. Internet browsing
d. SMS messaging

14. Which type of endpoint communication is not susceptible to malware (virus) infection?

    a. E-mail
    b. Instant messaging/chat
    c. Internet browsing
    d. SMS messaging

15. When using an endpoint device, for which type of communication do you need to install software to encrypt communications?

    a. Cellular voice
    b. Internet browsing
    c. E-mail
    d. Instant messaging/chat

Chapter 13 Answer Key

Question Number	Correct Answer	Reference in Course	
		Source	Page (s)
1.	c	Chapter 13	316
2.	a	Chapter 13	328
3.	b	Chapter 13	319
4.	b	Chapter 13	323
5.	a	Chapter 13	326
6.	c	Chapter 13	326
7.	c	Chapter 13	314
8.	a	Chapter 13	311
9.	a	Chapter 13	313
10.	d	Chapter 13	316
11.	a	Chapter 13	323-324
12.	b	Chapter 13	325
13.	d	Chapter 13	325
14.	d	Chapter 13	325
15.	c	Chapter 13	326

CHAPTER 14

1. Which of the following statements is true as it relates to mobile device messaging?

    a. SMS messages are guaranteed delivery
    b. MMS message are guaranteed delivery
    c. Both SMS and MMS messages are guaranteed delivery
    d. Neither SMS nor MMS are guaranteed delivery

2. Which of the following C-I-A triad tenets is the most vulnerable while introducing VoIP to an organization?

    a. Confidentiality
    b. Integrity
    c. Availability
    d. All equally the same

3. Which technique can an organization introduce to mitigate the risk of others “eavesdropping” on e-mail from mobile devices?

    a. Ensure antivirus is up to date.
    b. Add nonrepudiation with digital signatures.
    c. Use modern spam filtering.
    d. Implement encryption.

4. Which of the following is a risk that an organization encounters when allowing anyone to post messages to the organization’s social networking site?

    a. Competitors can eavesdrop.
    b. Regulators can eavesdrop.
    c. The organization’s confidential data could get posted.
    d. There is no risk because organizations are not allowed to post messages to social networking sites.

5. Which of the following techniques is recommended for VoIP traffic to avoid attacks on the data network?

    a. Purchase a different domain name for the IP address use.
    b. Use VLANs.
    c. Use an IDS.
    d. Disallow network traffic from the firewall.

6. What is the recommended mitigation technique for users to avoid becoming victims of phishing attacks?

a. Increase user awareness.
b. Install firewalls on the users' machines.
c. Employ use of the Nessus® vulnerability scanner.
d. Validate source code on the Web application.

7. An extension of SMS that allows a user to send and receive multimedia is called _____.

a. LMS
b. BMS
c. MMS
d. VMS

8. _____ is a real-time service that allows voice telephone communications over an IP network, such as the Internet.

a. IRC
b. DNS
c. SS
d. VoIP

9. The central router or switching device for handling telephone traffic is referred to as _____.

a. PBX
b. TRX
c. TSX
d. PTX

10. Which protocol was developed to manage communication sessions, particularly those involving multimedia, across the Internet?

a. HTTP
b. SMTP
c. SIP
d. CSOP

11. Which of the following is **not** an example of store-and-forward communication?

a. A message on Facebook
b. Presence/availability
c. Voice mail
d. E-mail

12. Which of the following is **not** an example of a real-time communication?

a. Voice mail
b. Presence/availability
c. Collaboration

d. An ordinary telephone call

13. Which of the following negatively affects the quality of real-time communications?

    a. Persistence
    b. Centralization
    c. SIP
    d. Latency

14. In which type of environment is store-and-forward communication a better choice than real-time communication?

    a. On networks with moderate to high latency
    b. Where the recipient is always available
    c. When source and destination are not in the same country
    d. None of the above

15. Which type of communication involves the SIP, H.323, MGCP, IP, and RTP protocols?

    a. SMS
    b. Cellular voice mail
    c. VoIP
    d. Fax

16. Which of the following is **not** a common technique for securing a PBX system?

    a. Physical isolation from unauthorized users
    b. Remote management
    c. Document control
    d. Patching and antivirus software

17. What is generally **not** a best practice for implementing VoIP?

    a. Do not use VPNs.
    b. Segregate traffic from data network.
    c. Use VLANs to protect and prioritize VoIP traffic.
    d. Patch systems and keep antivirus software up to date.

18. During which aspect of a multimedia connection does SIP discover and detect the user to be reached?

    a. User location
    b. User availability
    c. User capabilities
    d. Session setup

19. During which aspect of a multimedia connection does SIP notify the end device or user agent, also known as “ringing,” and set up the parameters between both ends?

    a. User location
    b. User availability
    c. User capabilities
    d. Session setup

20. When SIP controls a session with three SIP user agents, one of the agents acts as a _____.

    a. PBX
    b. IM client
    c. SIP user agent server (UAS)
    d. DNS server

Chapter 14 Answer Key

Question Number	Correct Answer	Reference in Course	
		Source	Page (s)
1.	b	Chapter 14	347
2.	c	Chapter 14	348
3.	d	Chapter 14	338
4.	c	Chapter 14	340-341
5.	b	Chapter 14	351
6.	a	Chapter 14	338
7.	c	Chapter 14	346
8.	d	Chapter 14	348
9.	a	Chapter 14	348
10.	c	Chapter 14	351
11.	b	Chapter 14	334-341
12.	a	Chapter 14	341-345
13.	d	Chapter 14	341
14.	a	Chapter 14	349, 354
15.	c	Chapter 14	348
16.	d	Chapter 14	348-349
17.	a	Chapter 14	350-351
18.	a	Chapter 14	351
19.	d	Chapter 14	351
20.	c	Chapter 14	352

CHAPTER 15

1. The National Cyber Security Division (NCSD) is part of which U.S. federal agency?

    a. Federal Communications Commission
    b. Department of Homeland Security
    c. Department of Commerce
    d. Federal Trade Commission

2. Which technology does US-CERT use primarily to keep you up to date on security tips, bulletins, and alerts, as well as the most recent security activities with leading vendors?

    a. RSS
    b. PDFs
    c. Webinars
    d. Windows Updates

3. Which organization maintains the Common Vulnerabilities and Exposures (CVE) list?

    a. US-CERT
    b. CERT/CC
    c. The MITRE Corporation
    d. National Institute of Standards and Technology (NIST)

4. Which of the following does NIST offer?

    a. CISSP certification
    b. Common Vulnerabilities and Exposures (CVE) list
    c. Federal Information Processing Standards (FIPS)
    d. Web-Hacking Incident Database

5. What is included on the OWASP Top 10 list?

    a. Web application vulnerabilities
    b. Accredited vulnerability testing products
    c. Security bulletins
    d. Open source security software products

6. What is the purpose of a honeypot?

    a. To analyze attack sources and methods
    b. To act as a repository of the most current anti-malware alerts
    c. Both A and B
    d. Neither A nor B

7. Which $(ISC)^2$ certification offers three concentrations in security architecture, engineering, and management?

a. Associate
b. CAP
c. SSCP
d. CISSP

8. What is the primary focus of U.S. DoD Directive 8570?

a. Timely dissemination of security alerts
b. Security certification for federally related workers
c. Anti-spam efforts
d. Standards for federal IT equipment

Chapter 15 Answer Key

Question Number	Correct Answer	Reference in Course	
		Source	Page (s)
1.	b	Chapter 15	360
2.	a	Chapter 15	360
3.	c	Chapter 15	362
4.	c	Chapter 15	364
5.	a	Chapter 15	372
6.	a	Chapter 15	371
7.	d	Chapter 15	368
8.	b	Chapter 15	367