**Chapter 3 Review Questions**

1. A \_\_\_\_\_\_\_\_\_\_ attack exploits previously unknown vulnerabilities.

a. virus resource

b. shock and awe

c. surprise

d. zero day – PG83

2. Why can traditional networking security devices NOT be used to block Web application attacks?

a. Traditional network security devices ignore the content of HTTP traffic, which is the vehicle of Web application attacks. – PG84

b. Web application attacks use Web browsers that cannot be controlled on a local computer.

c. Network security devices cannot prevent attacks from Web resources.

d. The complex nature of TCP/IP allows for too many ping sweeps to be blocked.

3. Attackers use buffer overflows to \_\_\_\_\_\_\_\_\_\_.

a. corrupt the kernel so the computer cannot reboot

b. point to another area in data memory that contains the attacker’s malware code – PG96

c. place a virus into the kernel

d. erase buffer overflow signature files

4. What is unique about a cross-site scripting (XSS) attack compared to other injection attacks?

a. SQL code is used in an XSS attack.

b. XSS requires the use of a browser.

c. XSS does not attack the Web application server to steal or corrupt its information. – PG85

d. XSS attacks are rarely used anymore compared to other injection attacks.

5. Each of the following can be used in an XSS attack except .

a. HTML

b. JavaScript

c. Adobe Flash

d. ICMP – PG86

6. A cookie that was not created by the Web site being viewed is called a \_\_\_\_\_\_\_\_.

a. first-party cookie

b. second-party cookie

c. third-party cookie – PG93

d. fourth-party cookie

7. The basis of a SQL injection attack is \_\_\_\_\_\_\_\_\_\_\_.

a. to inject SQL statements through unfiltered user input – PG88

b. to have the SQL server attack client Web browsers

c. to link SQL servers into a botnet

d. to expose SQL code so that it can be examined

8. Which of the following cannot be performed through a successful SQL injection attack?

a. Display a list of customer telephone numbers.

b. Discover the names of different fields in a table.

c. Erase a database table.

d. Reformat the Web application server’s hard drive. – PG89

9. A markup language that is designed to carry data is \_\_\_\_\_\_\_\_.

a. ICMP

b. HTTP

c. HTML

d. XML – PG89

10. When an attacker can access files in directories other than the root directory, this is known as a(n) \_\_\_\_\_\_\_\_\_\_\_ attack.

a. Command injection

b. Directory traversal – PG90

c. SQL injection

d. XML injection

11. A(n) \_\_\_\_\_\_\_ attack modifies the fields that contain the different characteristics of the data that is being transmitted.

a. HTML packet

b. SQL injection

c. XML manipulation

d. HTTP header – PG92

12. Which of the following cookies only lasts for the duration of visiting the Web site?

a. Session – PG93

b. Persistent

c. Temporary

d. RAM

13. What is a session token?

a. A random string assigned by a Web server – PG94

b. The same as a third-party cookie

c. A unique identifier that includes the user’s e-mail address

d. XML code used in an XML injection attack

14. Which of the following is not a security concern of the ActiveX add-on?

a. The person who signed the control may not have properly assessed the control’s safety.

b. A malicious ActiveX control can affect all users of that computer.

c. ActiveX can be integrated with JavaScript. – PG96

d. ActiveX does not have safeguards and has full access to the Windows operating system.

15. Which of the following is not a DoS attack?

a. Ping flood

b. SYN flood

c. Push flood – PG98

d. Smurf

16. What type of attack intercepts legitimate communication and forges a fictitious response to the sender?

a. Man-in-the-middle – PG99

b. Interceptor

c. SQL intrusion

d. SIDS

17. A replay attack \_\_\_\_\_\_.

a. makes a copy of the transmission for use at a later time – PG100

b. replays the attack over and over to flood the server

c. can be prevented by patching the Web browser

d. is considered to be a type of DoS attack

18. \_\_\_\_\_\_\_\_\_ is used to discover the MAC address of a client based on its IP address.

a. Ping

b. ICMP

c. DNS

d. ARP – PG101

19. DNS poisoning \_\_\_\_\_\_\_.

a. is rarely found today due to the use of host tables

b. can attack an external DNS server – PG102

c. is the same as ARP poisoning

d. floods a DNS server with requests until it can no longer respond

20.\_\_\_\_\_\_\_\_\_ involves using a third party to gain access rights.

a. Transitive access – PG105

b. Privilege escalation

c. Active Rights Scaling (ARS)

d. Directory traversal

**Chapter 4 Review Questions**

1. A \_\_\_\_\_\_\_ is a systematic and methodical evaluation of the exposure of assets to attackers, forces of nature, or any other entity that is a potential harm.

a. penetration test

b. vulnerability scan

c. vulnerability assessment – PG125

d. risk appraisal (RAP)

2. Each of the following can be classified as an asset except .

a. business partners

b. buildings

c. employee databases

d. accounts payable – PG125

3. Each of the following is a step in risk management except \_\_\_\_\_\_\_.

a. attack assessment – PG125

b. vulnerability appraisal

c. threat evaluation

d. risk mitigation

4. Which of the following is true regarding vulnerability appraisal?

a. Vulnerability appraisal is always the easiest and quickest step. – PG128

b. Every asset must be viewed in light of each threat.

c. Each threat could reveal multiple vulnerabilities.

d. Each vulnerability should be cataloged.

5. A threat agent \_\_\_\_\_\_\_.

a. is limited to attacks using viruses and worms

b. does not include natural disasters

c. is something that cannot be determined in advance

d. is a person or entity with the power to carry out a threat against an asset – PG126

6. \_\_\_\_\_\_\_\_\_ constructs scenarios of the types of threats that assets can face in order to learn who the attackers are, why they attack, and what types of attacks may occur.

a. Vulnerability prototyping

b. Risk assessment

c. Attack assessment

d. Threat modeling – PG126

7. What is a current snapshot of the security of an organization?

a. Vulnerability appraisal – PG127

b. Risk evaluation

c. Threat mitigation

d. Liability reporting

8. The \_\_\_\_\_\_\_\_\_\_ is the proportion of an asset’s value that is likely to be destroyed by a particular risk.

a. Exposure Factor (EF) – PG129

b. Single Loss Expectancy (SLE)

c. Annualized Rate of Occurrence (ARO)

d. Annualized Loss Expectancy (ALE)

9. Which of the following is NOT an option for dealing with risk?

a. Eliminate the risk – PG130

b. Accept the risk

c. Diminish the risk

d. Transfer the risk

10. \_\_\_\_\_\_\_\_\_\_\_ is a comparison of the present security state of a system compared to a standard established by the organization.

a. Risk mitigation

b. Baseline reporting – PG132

c. Comparative Resource Appraisal (CRA)

d. Horizontal comparables

11. Each of the following is a state of a port that can be returned by a port scanner except \_\_\_\_\_\_\_\_.

a. open

b. busy – PG135

c. blocked

d. closed

12. Each of the following is true regarding TCP SYN port scanning except \_\_\_\_\_\_\_\_.

a. it uses FIN messages that can pass through firewalls and avoid detection – PG136

b. instead of using the operating system’s network functions, the port scanner generates IP packets itself and monitors for responses

c. the scanner host closes the connection before the handshake is completed

d. this scan type is also known as “half-open scanning” because it never actually opens a full TCP connection

13. The protocol File Transfer Protocol (FTP) uses which two ports?

a. 19 and 20

b. 20 and 21 – PG134

c. 21 and 22

d. 22 and 23

14. A protocol analyzer places the computer’s network interface card (NIC) adapter into \_\_\_\_\_\_ mode.

a. promiscuous – PG 137

b. full

c. view

d. real

15. Each of the following is a function of a vulnerability scanner except \_\_\_\_\_\_\_\_\_.

a. detect which ports are served and which ports are browsed for each individual system

b. alert users when a new patch cannot be found – PG138

c. maintain a log of all interactive network sessions

d. detect when an application is compromised

16. Which of the following is true of the Open Vulnerability and Assessment Language

(OVAL)?

a. It only functions on Linux-based computers.

b. It attempts to standardize vulnerability assessments. – PG139

c. It has been replaced by XML.

d. It is a European standard and is not used in the Americas.

17. Which of the following is not true regarding a honeypot?

a. It is typically located in an area with limited security.

b. It contains real data files because attackers can easily identify fake files. – PG140

c. It cannot be part of a honeynet.

d. It can direct an attacker’s attention away from legitimate servers.

18. Which of the following is true of vulnerability scanning?

a. It uses automated software to scan for vulnerabilities. – PG140

b. The testers are always outside of the security perimeter.

c. It may disrupt the operation of the network or systems.

d. It produces a short report of the attack methods and value of the exploited data.

19. If a tester is given the IP addresses, network diagrams, and source code of customer applications, then she is using which technique?

a. Black box

b. White box – PG142

c. Gray box

d. Blue box

20. If a software application aborts and leaves the program open, which control structure is it using?

a. Fail-safe

b. Fail-secure

c. Fail-open – PG144

d. Fail-right