Chapter 3- Quiz

1. What is a vulnerability that allows criminals to inject scripts into web pages viewed by users?

- buffer overflow
- SQL injection
- XML injection
- Cross-site scripting

Explanation: Cross-site scripting (XSS) allows criminals to inject scripts that contain malicious code into web applications.

2. What type of attack targets an SQL database using the input field of a user?

- buffer overflow
- SQL injection
- XML injection
- Cross-site scripting

Explanation: A criminal can insert a malicious SQL statement in an entry field on a website where the system does not filter the user input correctly.

3. Which two reasons describe why WEP is a weak protocol? (Choose two.)

- WEP uses the same encryption features as Bluetooth.
- Everyone on the network uses a different key.
- The key is static and repeats on a congested network.
- The default settings cannot be modified.
- The key is transmitted in clear text.

Explanation:
The initialization vector (IV) of WEP is as follows:

Is a 24-bit field, which is too small
Is cleartext and readable
Is static and causes identical key streams to repeat on a busy network

4. What is the difference between a virus and a worm?

- Viruses hide in legitimate programs but worms do not.
- Worms self-replicate but viruses do not.
- Viruses self-replicate but worms do not.
- Worms require a host file but viruses do not.

Explanation: Worms are able to self-replicate and exploit vulnerabilities on computer networks without user participation.

5. A criminal is using software to obtain information about the computer of a user. What is the name of this type of software?

- phishing
- adware
- spyware
- virus

Explanation: Spyware is software that tracks the activity of a user and obtains information about that user.

6. What is the meaning of the term logic bomb?

- a malicious worm
- a malicious program that uses a trigger to awaken the malicious code
- a malicious virus
- a malicious program that hides itself in a legitimate program

Explanation: A logic bomb remains inactive until a trigger event occurs. Once activated, a logic bomb runs malicious code that causes harm to a computer.

7. What is the term used when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source?

- Trojan
- vishing
- phishing
- backdoor
- social engineering

Explanation: Phishing is used by malicious parties who create fraudulent messages that attempt to trick a user into either sharing sensitive information or installing malware.

8. What are two ways to protect a computer from malware? (Choose two.)

- Empty the browser cache.
- Use antivirus software.
- Delete unused software.
- Keep software up to date.
- Defragment the hard disk.

Explanation: At a minimum, a computer should use antivirus software and have all software up to date to defend against malware.

9. What occurs on a computer when data goes beyond the limits of a buffer?

- a buffer overflow
- a system exception
- an SQL injection
- cross-site scripting

Explanation: A buffer overflow occurs by changing data beyond the boundaries of a buffer and can lead to a system crash, data compromise, or cause escalation of privileges.

10. What is the term used to describe an email that is targeting a specific person employed at a financial institution?

- spam
- vishing
- spear phishing
- target phishing
- spyware

Explanation: Spear phishing is a phishing attack customized to reach a specific person or target.

11. An attacker is sitting in front of a store and wirelessly copies emails and contact lists from nearby unsuspecting user devices. What type of attack is this?

- RF jamming
- smishing
- bluejacking
- bluesnarfing

Explanation: Blusnarfing is the copying of user information through unauthorized Bluetooth transmissions.

12. What are two of the tactics used by a social engineer to obtain personal information from an unsuspecting target? (Choose two.)

- intimidation
- compassion
- honesty
- urgency
- integrity

Explanation:
Social engineering tactics include the following:

Authority
Intimidation
Consensus/Social Proof
Scarcity
Urgency
Familiarity/Liking
Trust

13. What are two common indicators of spam mail? (Choose two.)

- The email has keywords in it.
- The email has misspelled words or punctuation errors or both.
- The email is from your supervisor.
- The email is from a friend.
- The email has no subject line.
- The email has an attachment that is a receipt for a recent purchase.

Explanation: Spam is a common method of advertising through the use of unsolicited email and may contain malware.

14. Which term describes the sending of a short deceptive SMS message used to trick a target into visiting a website?

- spam
- smishing
- grayware
- impersonation

Explanation: Smishing is also known as SMS phishing and is used to send deceptive text messages to trick a user into calling a phone number or visiting a specific website.

15. A computer is presenting a user with a screen requesting payment before the user data is allowed to be accessed by the same user. What type of malware is this?

- a type of logic bomb
- a type of virus
- a type of worm
- a type of ransomware

Explanation: Ransomware commonly encrypts data on a computer and makes the data unavailable until the computer user pays a specific sum of money.

16. What is the name for the type of software that generates revenue by generating annoying pop-ups?

- spyware
- trackers
- pop-ups
- adware

Explanation: Adware is a type of malware that displays pop-ups on a computer to generate revenue for the creator of the malware.

17. What does a rootkit modify?

- Microsoft Word
- Notepad
- screen savers
- programs
- operating system

Explanation: A rootkit commonly modifies an operating system to create a backdoor to bypass normal authentication mechanisms.

18. What is the name given to a program or program code that bypasses normal authentication?

- virus
- worm
- ransomware
- Trojan
- backdoor

Explanation: A backdoor is a program or program code implemented by a criminal to bypass the normal authentication that is used to access a system.