1Ahmed is a sales manager with a major insurance company. He has received an email that is

encouraging him to click on a link and fill out a survey. He is suspicious of the email, but it

does mention a major insurance association, and that makes him think it might be legitimate.

Which of the following best describes this attack?

A. Phishing

B. Social engineering

C. Spear phishing

D. Trojan horse

Answer: C

So spear phishing is the right response. A particular group, in this case insurance professionals, is the target of spear phishing. Even if this is a type of phishing, you should always choose the more precise response to inquiries like this. Phishing employs social engineering techniques in order to be successful, but because it is a more general solution than spear phishing, it is not the best option. Last but not least, a Trojan horse impersonates a trustworthy or desirable programme or file, which this scenario doesn't do.

2. You are a security administrator for a medium-sized bank. You have discovered a piece of

software on your bank’s database server that is not supposed to be there. It appears that the

software will begin deleting database files if a specific employee is terminated. What best

describes this?

A. Worm

B. Logic bomb

C. Trojan horse

D. Rootkit

Answer: B.

A logic bomb is malware that only starts acting maliciously when a certain criterion is satisfied. A worm is a type of malware that spreads itself. A rootkit is malware that gains root or administrative access, whereas a Trojan horse is malware that is bundled with a trustworthy programme.

3. You are responsible for incident response at Acme Bank. The Acme Bank website has been

attacked. The attacker used the login screen, but rather than enter login credentials, they

entered some odd text:

'

or

'1' = '1

. What is the best description for this attack?

A. Cross-site scripting

B. Cross-site request forgery

C. SQL injection

D. ARP poisoning

Answer: C.

This is a pretty simple SQL injection technique. JavaScript would be used in the text field for cross-site scripting, which aims to affect other websites while a user is logged in. ARP poisoning is the process of changing the ARP table in a switch; it is unrelated to website hacking, as would cross-site request forgery, which does not include any text being placed into the web page.

4. Users are complaining that they cannot connect to the wireless network. You discover that

the WAPs are being subjected to a wireless attack designed to block their Wi-Fi signals.

Which of the following is the best label for this attack?

A. IV attack

B. Jamming

C. WPS attack

D. Botnet

Answer: B.

This represents a jamming attack, in which another signal obstructs genuine flow. Jamming may be continuous or sporadic and can be purposeful or accidental. IV attacks are mysterious stream cypher cryptography attacks. WPS (Wi-Fi Protected Setup) connects to the wireless access point using a PIN (WAP). The WPS attack aims to connect to the WAP, intercept that PIN while it is being transmitted, and then steal the WPA2 password. A set of computers used in an attack without their permission is known as a botnet.

5. Frank is deeply concerned about attacks to his company’s e-commerce server. He is particular worried about cross-site scripting and SQL injection. Which of the following would best defend against these two specific attacks?

A. Encrypted web traffic

B. Input validation

C. A firewall

D. An IDS Threats, Attacks, and Vulnerabilities

Answer: B.

Input validation is the most effective option for preventing the attacks mentioned. Web traffic encryption will have no impact on these two attacks. Input validation would take precedence over web application firewall (WAF) mitigation of these attacks, and an intrusion detection system (IDS) will only be able to identify the attack—not prevent it.

6. You are responsible for network security at Acme Company. Users have been reporting that

personal data is being stolen when using the wireless network. They all insist they only con-

nect to the corporate wireless access point (AP). However, logs for the AP show that these

users have not connected to it. Which of the following could best explain this situation?

A. Session hijacking

B. Clickjacking

C. Rogue access point

D. Blue jacking

Answer: C.

Users may have been connecting to a fake access point if they have been doing so even though the AP does not show them doing so. This may be the root of an architecture and design flaw, such as an uncontrolled network with no segmentation of devices connected to it. The act of hijacking an authenticated session is known as session hijacking. Attacks that hijack sessions frequently use impersonation. By pretending to be another user, the attacker tries to get access to that user's session. The act of "clickjacking" includes tricking website users into clicking on the incorrect link. Lastly, a Bluetooth attack is known as blue jacking.

7. What type of attack depends on the attacker entering JavaScript into a text area that is

intended for users to enter text that will be viewed by other users?

A. SQL injection

B. Clickjacking

C. Cross-site scripting

D. Blue jacking

Answer: C.

Entering a script into text fields that other users will see is known as cross-site scripting. SQL injection involves inputting SQL commands rather than scripts. The goal of clickjacking is to deceive consumers into clicking on the incorrect link. A Bluetooth attack is called blue jacking.

8. Rick wants to make offline brute-force attacks against his password file very difficult

for attackers. Which of the following is not a common technique to make passwords

harder to crack?

A. Use of a salt

B. Use of a pepper

C. Use of a purpose-built password hashing algorithm

D. Encrypting password plain text using symmetric encryption

Answer: D.

Since keeping the actual password is not recommended, encrypting plain-text passwords is not a frequent way to make passwords more difficult to guess. Anyone with access to the encryption key could decrypt the passwords because the application needs it to read them. Common best methods to thwart offline brute-force attacks include using a salt, a pepper, and a cryptographic hashing algorithm created for passwords.

9. What term is used to describe spam over Internet messaging services?

A. SPIM

B. SMSPAM

C. IMSPAM

D. Two Face Timing

Answer: A.

Despite being one of the most out-of-date questions on the Security+ exam syllabus, you should be aware of the acronym SPIM, which stands for spam Internet messages. Though it is stated in the exam outline that the remaining answers were made up, this phrase is no longer often used.

10.Susan is analysing the source code for an application and discovers a pointer de-reference

and returns NULL. This causes the program to attempt to read from the NULL pointer and

results in a segmentation fault. What impact could this have for the application?

A. A data breach

B. A denial-of-service condition

C. Permissions creep

D. Privilege escalation

Answer: B.

A segmentation fault usually causes the programme to crash. Because a denial-of-service condition affects the service's availability, a NULL pointer or other pointer dereferencing error is seen as a potential security risk. Access creep happens when people accumulate more permissions over time in a single organisation because their permissions are not cleaned up when they switch jobs or responsibilities. This type of issue is unlikely to result in a data breach or allow privilege escalation.