Exam Report: 13.4.3 Practice Questions

Date: 4/15/2020 4:25:39 pm
Time Spent: 1:26

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 50%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

An unauthorized person gains access to a secured area by following an authorized person through a door controlled by a badge reader.

Which of the following security threats does this sentence describe?

- Phishing
- Brute forcing
- Shoulder surfing
- Tailgating

Explanation

Tailgating describes the actions of an unauthorized person closely following an authorized person to gain access to a secure area.

Shoulder surfing occurs when a one person obtains usernames, passwords, and other data by looking over the shoulder of another person. Brute forcing describes the process of cracking a username, password, decryption key, or network protocols using the trial-and-error method, often by testing all possible character combinations. Phishing is an attempt to trick a user into compromising personal information or downloading malware. Most often, it involves an email containing a malicious attachment or hyperlink.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_01]

Question 2: Correct

Joe, an executive, receives an email that appears to be from the financial institution that provides his company credit card. The text of the email includes Joe's name and the company name and states that there is a problem with Joe's credit card. The email provides a link to verify the credit card, but when Joe hovers over the link, he thinks the web address seems strange.

Which of the following BEST describes this type of attack?

- Brute forcing
- Zero-day attack
- Man-in-the-middle attack

Explanation

Social engineering is the use of deception to manipulate individuals into sharing confidential or personal information that can be used for unlawful purposes.

A zero-day attack is an exploit of an operating system or software vulnerability that is unknown and unpatched by the author. Brute force can be used to crack a username, password, or other authentication using trial and error, usually by trying all possibly permutations. A man-in-the-middle (MITM) attack intercepts communications between two systems and alters the message before sending it on to the original recipient.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_02]

Question 3: Correct

Which of the following are common forms of social engineering attacks?

- Using a sniffer to capture network traffic.
- Distributing false information about your organization's financial status.
- Stealing the key card of an employee and using that to enter a secured building.
- Sending hoax virus information emails.

Explanation

Hoax virus information emails are a form of social engineering attack. This type of attack preys on email recipients who are fearful and will believe most information if it is presented in a professional manner. The victims of these attacks usually fail to double-check the information or instructions with a reputable third party anti-virus software vendor before implementing the recommendations. Usually, these hoax messages instruct the reader to delete key system files or download Trojan horses. Social engineering relies on the trusting nature of individuals to take an action or allow unauthorized action.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_03]

Question 4: Correct

Which of the following is a form of attack that tricks victims into providing confidential information, such as identity information or logon credentials, through emails or websites that impersonate an online entity that the victim trusts, such as a financial institution or well-known e-commerce site?

- Session hijacking

- Phishing
- Fraggle attack

Explanation

Phishing tricks victims into providing confidential information, such as identity information or logon credentials, through emails or websites that impersonate an online entity that the victim trusts, such as a financial institution or well-known e-commerce site. Phishing is a specific form of social engineering. A fraggle attack uses spoofed UDP packets to flood a victim with echo requests using a bounce network, much like a Smurf attack. Session hijacking takes over a logon session from a legitimate client, impersonating the user and taking advantage of their established communication link.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_04]

Question 5: Incorrect

Which of the following are examples of social engineering? (Select TWO).

- [ ] Brute force password cracking
- [ ] Port scanning
- [ ] Dumpster diving
- [x] Shoulder surfing
- [x] ~~War dialing~~

Explanation

Social Engineering leverages human nature. Internal employees are often the target of trickery, and false trust can quickly lead to a serious breach of information security. Shoulder surfing and dumpster diving are examples of social engineering. Shoulder surfing is the act of looking over an authorized user's shoulder in hopes of obtaining an access code or credentials. Dumpster diving involves searching through trash or other discarded items to obtain credentials or information that may facilitate further attacks. These low-tech attack methods are often the first course of action that a hacker pursues.

Port scanning and war dialing are technical attacks that seek to take advantage of vulnerabilities in systems or networks. Brute force password-cracking software tries to identify a password by trying every possible letter, number, and symbol combination until the correct one is found.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_05]

Question 6: Incorrect

What is the best countermeasure against social engineering?

- Acceptable use policy

- User awareness training
- Strong passwords
- ~~Access auditing~~

Explanation

The best countermeasure to social engineering is user awareness training. If users understand the importance of security and the restrictions on types of information, they are less likely to reveal confidential information or perform unauthorized activities at the prompting of a stranger or a claimed identity over the phone.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_06]

Question 7: Incorrect

You are a security consultant. An organization has hired you to review their security measures. The organization is chiefly concerned that it could become the victim of a social engineering attack.

Which of the following actions would you MOST likely recommend to mitigate the risk?

- Implement a border firewall to filter inbound network traffic.
- ~~Train managers to monitor user activity.~~
- Establish a written security policy.
- Teach users how to recognize and respond to social engineering attacks.

Explanation

The best way to combat social engineering is to train users how to recognize and respond to social engineering attacks. For example, most organizations train employees to forward any calls or emails requesting a password or other network information to their help desk.

Filtering network traffic with a firewall fails to address the human element involved in social engineering. While a written security policy is a necessary measure, it will do little to defend your network if your users don't know how to recognize social engineering attempts. Management oversight is expensive and unlikely to detect a social engineering attempt until it is too late. Raising user awareness of the issue tends to be much more effective.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_07]

Question 8: Correct

Several users have forwarded you an email stating that your company's health insurance provider has just launched a new website for all employees. To access the site, they are told to click a link in the email and provide their personal information.

Which of the following BEST describes the type of attack that just occurred?

- Denial of service
- Phishing
- Piggybacking
- Smurf

Explanation

A phishing attack has occurred. In a phishing attack, a spoofed email containing a link to a fake website is used to trick users into revealing sensitive information, such as a username, password, bank account number, or credit card number. Both the email and the website used in the attack appear to be legitimate on the surface.

Piggybacking occurs when an unauthorized person follows an authorized person to enter a secured building or area within a building. Piggybacking is also sometimes called tailgating. A denial of service (DoS) attack involves using network mechanisms to flood a particular host with so many bogus requests that it can no longer respond to legitimate network requests. A Smurf attack is a distributed type of DoS attack that inserts a target system's IP address for the source address of ICMP echo request packets, causing a flood of ICMP echo response packets to be sent to a victim system.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_08]

Question 9: Incorrect

An intruder waits near an organization's secured entrance until an employee approaches the entrance and unlocks it with a security badge. The intruder falls in line behind the employee, who assumes the intruder is another employee and holds the door open for her.

Which of the following BEST describes the type of attack that just occurred?

- Tailgating
- Smurf
- Phishing
- ~~Denial of service~~

Explanation

A tailgating attack has occurred. Tailgating occurs when an unauthorized person follows behind an authorized person to enter a secured building or area within a building. Tailgating is also sometimes called piggybacking.

In a phishing attack, a spoofed email containing a link to a fake website is used to trick users into revealing sensitive information, such as a username, password, bank account number, or credit card number. Both the email and the website used in the attack appear on the surface to be legitimate. A denial of service (DoS)

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_09]

Question 10: Correct

A malicious person calls an employee from a cell phone. She tells the employee that she is the vice president over the accounting department in the employee's company. She relates that she has forgotten her password and demands that the employee give her his password so that she can access the reports she needs for an upcoming presentation. She threatens to fire the employee if he does not comply.

Which of the following BEST describes the type of attack that just occurred?

- Eavesdropping
- Masquerading
- Piggybacking
- Phishing

Explanation

A masquerading attack has occurred. Masquerading involves an attacker convincing authorized personnel to grant them access to protected information by pretending to be someone who is authorized and/or requires that access. Usually, the attacker poses as a member of senior management. A sense of urgency is typically fabricated to motivate the user to act quickly.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_10]

Question 11: Incorrect

A user within your organization received an email relating how an account containing a large sum of money has been frozen by the government of a small African nation. The user was offered a 25 percent share of this account if she would help the sender transfer it to a bank in the United States. The user responded to the sender and was instructed to send her bank account number so that it could be used to facilitate the transfer. She complied, and then the sender used the information to drain her bank account.

What type of attack occurred?

- Phishing
- Piggybacking
- ~~Eavesdropping~~
- Man-in-the-middle

Explanation

A phishing attack has occurred in this scenario. This particular attack is sometimes referred to as a Nigerian 419 attack and is very common.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_11]

Question 12: Incorrect

While organizing a storage cabinet, a technician discovers a box of hard drives that are incompatible with current hardware and may contain sensitive data.

Which of the following is the BEST method for disposing of these drives?

- Partitioning
- Overwriting
- Shredding
- ~~Formatting~~

Explanation

A physical method of destroying the hard drives is best. This includes shredding, drilling, pulverizing, degaussing, and incinerating.

If not done repeatedly, overwriting may leave recoverable data on the disk.

Formatting will leave recoverable data on the disk.

Partitioning will leave recoverable data on the disk.

References

TestOut PC Pro - 13.4 Social Engineering
[e_social_pp6.exam.xml Q_SEC_SOCE_DATA_DESTRUCTION_02]