Exam Report: 3.5.6 Practice Questions

Date: 1/15/2020 8:50:10 pm
Time Spent: 12:56

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 80%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

What is the primary countermeasure to social engineering?

➡ ● Awareness

○ Traffic filters

○ Heavy management oversight

○ A written security policy

Explanation

The primary countermeasure to social engineering is awareness. If users are not aware of security needs and able to meet them, they are vulnerable to numerous social engineering exploits. Awareness training focused on preventing social engineering should include methods for authenticating personnel over the phone, assigning classification levels to information and activities, and educating your personnel on what information should not be distributed over the phone.

A written security policy is a countermeasure against social engineering. However, without awareness training, it is useless. Heavy management oversight may provide some safeguards to social engineering, but it is less effective than awareness. Traffic filters are not countermeasures for social engineering because they do not focus on solving the human problem inherent in social engineering attacks.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_01]

Question 2: Correct

How can an organization help prevent social engineering attacks? (Select two.)

➡ ☑ Educate employees on the risks and countermeasures.

□ Close all unneeded ports on firewalls.

➡ ☑ Publish and enforce clearly-written security policies.

□ Implement IPsec on all critical systems.

Explanation

User training and policy enforcement are the keys to preventing social engineering attacks. Many users are not aware of the risks involved. Training raises awareness, provides clear instructions for dealing with and reporting suspicious activity, and directly supports all published security policies.

Technical countermeasures, such as using IPsec or closing unused ports, protect against automated attacks. Social engineering attacks gain access by exploiting human nature.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_02]

▼ Question 3: Correct

Which of the following attacks tricks victims into providing confidential information (such as identity information or login credentials) through emails or websites that impersonate an online entity that the victim trusts?

○ Man-in-the-middle

○ Adware

➡ ● Phishing

○ Session hijacking

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.

Session hijacking takes over a login session from a legitimate client, impersonating the user and taking advantage of their established communication link. A *man-in-the-middle* attack is where an attacker intercepts a data stream, slightly modifies it, then forwards that data stream to the destination. *Adware* is a type of malware that sends you advertisements that you do not request.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_03]

▼ Question 4: Correct

Match the social engineering description on the left with the appropriate attack type on the right.

Phishing

✓ An attacker pretending to be from a trusted organization sends an email asking users to access a website to verify personal information.

Whaling

✓ An attacker gathers personal information about the target individual, who is a CEO.

Spear phishing

✓ An attacker gathers personal information about the target individual in an organization.

Dumpster diving

✓ An attacker searches through an organization's trash looking for sensitive information.

Piggybacking

✓ An attacker enters a secured building by following an authorized employee through a secure door without providing identification.

Vishing

✓ An attacker uses a telephone to convince target individuals to reveal their credit card information.

Explanation

Specific social engineering attacks include:

- **Phishing**: a scam where an email pretending to be from a trusted organization that asks receivers to verify personal information or send money. A phishing attack usually uses a fraudulent message (which appears to be legitimate) is sent to a target. The message requests that the target visit a fraudulent website (which also appears to be legitimate). Graphics, links, and websites look almost identical to legitimate requests and web sites they are trying to represent. The fraudulent website requests that the victim provide sensitive information, such as the account number and password.

- **Whaling**: targets senior executives and high-profile victims.
- **Spear phishing**: where an attacker tries to gain access to information that will allow the attacker to gain commercial advantage or commit fraud. Spear phishing frequently involves sending seemingly genuine emails to all employees or members of specific teams.
- **Dumpster Diving**: the process of looking in the trash for sensitive information that has not been properly disposed of.
- **Tailgating and Piggybacking**: where an attacker entering a secured building by following an authorized employee through a secure door and not providing identification. Piggybacking usually implies the authorized employee's consent; tailgating implies no consent.
- **Vishing**: exploits VOIP telephone services.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_04]

▼ **Question 5:** Correct

Which of the following is a common social engineering attack?

○ Using a sniffer to capture network traffic

○ Logging on with stolen credentials

○ Distributing false information about your organization's financial status

➡ ● Distributing hoax virus information emails

Explanation

Distributing hoax virus information emails is a 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 fail to double-check the information or instructions with a reputable third-party antivirus software vendor before implementing the recommendations. Usually, these hoax messages instruct the reader to delete key system files or download Trojan horse viruses.

Social engineering relies on the trusting nature of individuals to take an action or allow an unauthorized action.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_05]

▼ **Question 6:** Incorrect

You have just received a generic-looking email that is addressed as coming from the administrator of your company. The email says that, as part of a system upgrade, you are to go to a website and enter your user name and password at a new website so you can manage your email and spam using the new service.

What should you do?

○ Click on the link in the email and look for company graphics or information before entering the login information.

○ Open a web browser and type the URL included in the email. Follow the directions to enter your login credentials.

➡ ○ Verify that the email was sent by the administrator and that this new service is legitimate.

○ Click on the link in the email and follow the directions to enter your login information.

● ~~Delete the email.~~

Explanation

You should verify that the email is legitimate and has come from your administrator. It is possible that the network administrator has signed up for a new service. If you ignore the message or delete it, you might not get the benefits the company has signed up for. However, the email might be a phishing attack. An attacker might be trying to capture personal information. By verifying the email with the administrator, you will be able to tell if the email is legitimate.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_07]

Question 7: Correct

Dumpster diving is a low-tech way to gathering information that may be useful in gaining unauthorized access or as a starting point for more advanced attacks. How can a company reduce the risk associated with dumpster diving?

○ Create a strong password policy

➡ ● Establish and enforce a document destruction policy

○ Mandate the use of Integrated Windows Authentication

○ Secure all terminals with screensaver passwords

Explanation

Dumpster diving is best addressed by a document destruction policy. All sensitive documents should be shredded or burned, and employees should be trained on the proper use of disposal equipment and the policies governing disposal of sensitive information.

A strong password policy, authentication types, and screensaver passwords do not prevent the risk associated with dumpster diving. User name and password complexity efforts are wasted if employees are documenting and disposing of paper information in an insecure fashion.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_08]

Question 8: Correct

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

➡ ☑ Shoulder surfing

□ Port scanning

➡ ☑ Dumpster diving

□ 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.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_09]

Question 9: Correct

Which of the following social engineering attacks use Voice over IP (VoIP) to gain sensitive information?

○ Masquerading

○ Tailgating

○ Spear phishing

➡ ● Vishing

Explanation

Vishing is a social engineering attack that uses Voice over IP (VoIP) to gain sensitive information. The term is a combination of *voice* and *phishing*.

In spear phishing, attackers gather information about the victim, such as identifying which online banks they use. They then send phishing emails for the specific bank. Masquerading refers to convincing personnel to grant access to sensitive information or protected systems by pretending to be someone who is authorized and/or requires that access. Tailgating refer to an attacker entering a secured building by following an authorized employee without their consent.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_10]

Question 10: Incorrect

A senior executive reports that she received a suspicious email concerning a sensitive internal project that is behind production. The email was sent from someone she doesn't know, and he is asking for immediate clarification on several of the project's details so the project can get back on schedule.

Which type of an attack best describes the scenario?

○ MAC spoofing

➡ ○ Whaling

● ~~Masquerading~~

○ Passive

Explanation

Whaling is a social engineering attack that targets senior executives and high profile victims. Social engineering is an attack that exploits human nature by convincing someone to reveal information or perform an activity.

Masquerading refers to convincing personnel to grant access to sensitive information or protected systems by pretending to be someone who is authorized and/or requires that access. Passive social engineering attacks take advantage of the unintentional actions of others to gather information or gain access to a secure facility. MAC spoofing is changing the source MAC address on frames sent by the attacker and can be used to hide the identity of the attacker's computer or impersonate another device on the network.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_11]

Question 11: Incorrect

Identify and label the following attacks by dragging the term on the left to the definition on the right. Not all terms are used.

An attacker convinces personnel to grant access to sensitive information or protected systems by pretending to be someone who is authorized and/or requires that access.

~~Phishing~~ Masquerading

An attacker pretending to be from a trusted organization sends emails to senior executives and high-profile personnel asking them to verify personal information or send money.

✓ Whaling

Attackers use Voice over IP (VoIP) to pretend to be from a trusted organization and ask victims to verify personal information or send money.

✓ Vishing

Attackers send emails with specific information about the victim (such as which online banks they use) that ask them to verify personal information or send money.

~~Masquerading~~ Spear phishing

Attackers attempts to make the person believe that if they don't act quickly, they will miss out on an item, opportunity or experience.

~~Urgency~~ Scarcity

Explanation

Masquerading is convincing personnel to grant access to sensitive information or protected systems by pretending to be someone who is authorized and/or requires that access. Masquerading passive when compared to impersonating.

Urgency is an active social engineering technique that attempts to make the people believe they must act quickly to avoid imminent damage or suffering.

Scarcity is an active social engineering technique that attempts to make the people believe that if they don't act quickly, they will miss out on an item, opportunity or experience.

Tailgating refers to an attacker who enters a secured building by following an authorized employee through a secure door without providing identification.

Piggybacking usually implies consent of an authorized employee, whereas tailgating implies no such consent.

Phishing is an email pretending to be from a trusted organization that asks the receiver to verify personal information or send money.

Whaling is another form of phishing that targets senior executives and high-profile victims.

Vishing is similar to phishing, but instead of an email, the attacker uses Voice over IP (VoIP) to gain sensitive information.

Spear phishing is an attack that uses specific information about the victim, such as identifying which online banks they use.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_12||/]

▼ **Question 12:** Correct

The receptionist received a phone call from an individual claiming to be a partner in a high-level project and requesting sensitive information. The individual is engaging in which type of social engineering?

○ Social validation

○ Persuasive

○ Commitment

➡ ● Authority

Explanation

Authority social engineering entails an attacker either lying about having authority or using their high status in a company to force victims to perform actions that exceed their authorization level.

Persuasive social engineering entails an attacker convincing a person to give them information or access that they shouldn't. *Social validation* entails an attacker using peer pressure to coerce someone else to bend rules or give information they shouldn't. *Commitment* social engineering entails convincing someone to buy into an overall idea, then demanding or including further specifics that were not presented up front.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_13]

▼ Question 13: Correct

You've just received an email message explaining that a new and serious malicious code threat is ravaging across the internet. The message contains detailed information about the threat, its source code, and the damage it can inflict. The message states that you can easily detect whether or not you have already been a victim of this threat by the presence of three files in the \Windows\System32 folder. As a countermeasure, the message suggests that you delete these three files from your system.

In response to this message, which action should you take first?

○ Perform a complete system backup

➡ ◉ Verify the information on well-known malicious code threat management websites

○ Distribute the message to everyone in your address book

○ Reboot the system

○ Delete the indicated files if present

Explanation

The best first step to take after receiving an email message about a new malicious code threat is to verify the information it contains. You can easily verify information by visiting two or more well-known malicious code threat management websites. These sites can be your anti-virus vendor or a well-known and well-regarded internet security watch group. All too often, messages of this type are hoaxes. It is important not to fall prey to email hoaxes or spread them to others.

Your first step should not be to follow any directions included in the email, especially deleting files. You should never forward email warnings until you have firmly established the authenticity and validity of such information. Even then, it is not your responsibility to inform anyone about such a threat except for the security personnel in your organization. Let those responsible for such activities, such as anti-virus vendors or your security team, inform the general public. Making a full backup is often a good idea, but it is not necessary in this instance.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_14]

▼ Question 14: Correct

What is the weakest point in an organization's security infrastructure?

➡ ◉ People

○ Technology

○ Procedures

○ Physical structure

Explanation

People are usually the weakest point in an organization's security infrastructure.

Procedures, technology, and physical security are often reasonably secure when controlled under a well-designed security policy.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_15]

Question 15: Correct

Which of the following is **not** a form of social engineering?

➡ ● Impersonating a user by logging on with stolen credentials

○ A virus hoax email message

○ Impersonating a utility repair technician

○ Impersonating a manager over the phone

Explanation

Impersonating a user by logging on with stolen credentials is not a social engineering attack. It is an intrusion attack made possible by network packet capturing or obtaining logon credentials through social engineering.

Impersonating someone over the phone or in person are easily recognizable forms of social engineering. A virus hoax email message is also a form of social engineering because it attacks people by exploiting the common weaknesses of fear and ignorance.

References

LabSim for Security Pro, Section 3.5.
[All Questions SecPro2017_v6.exm SOCIAL_ENGR_06]