Chp 2 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 1/30/2022 12:04:27 pm • Time spent: 04:35

Score: 97%

Passing Score: 80%

Question 1: ✓ Correct

The IT manager in your organization proposes taking steps to deflect a potential threat actor. The proposal includes the following:

- Create and follow onboarding and off-boarding procedures.
- Employ the principal of least privilege.
- Have appropriate physical security controls in place.

Which type of threat actor do these steps guard against?

➡ ● Insider

○ Hacktivist

○ Script kiddie

○ Competitor

EXPLANATION

Because insiders are one of the most dangerous and overlooked threats to an organization, you need to take the appropriate steps to protect against them, such as requiring mandatory vacations, creating and following onboarding and off-boarding procedure, employing the principal of least privilege, and having appropriate physical security controls in place.

A script kiddie is an individual who carries out an attack by using scripts or programs written by more advanced hackers.

A hacktivist is any individual whose attacks are politically motivated.

A competitor threat actor carries out attacks on behalf of an organization and targets competing companies.

Question 2: ✓ Correct

Which of the following is a common social engineering attack?

- ➡ ● Distributing hoax virus-information emails
- ○ Using a sniffer to capture network traffic
- ○ Distributing false information about an organization's financial status
- ○ Logging on with stolen credentials

EXPLANATION

Distributing hoax virus-information emails are 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 Trojans.

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

Question 3: ✓ Correct

When confidential or protected data is exposed, either intentionally or accidentally, it is considered to be which of the following?

- ○ Data loss
- ➡ ● Data breach
- ○ Availability loss
- ○ Data exfiltration

EXPLANATION

A data breach is when confidential or protected data is exposed. Data loss involves the loss of important data, such as a file being deleted. Data exfiltration could be used during a data breach, but it in itself is not the definition of a data breach. Availability loss would be an attack where the attacker is preventing authorized users from accessing the systems.

Question 4: ✓ Correct

A hacker scans hundreds of IP addresses randomly on the internet until they find an exploitable target. What kind of attack is this?

○ Insider attack

○ Nation state attack

○ Targeted attack

➡ ● Opportunistic attack

EXPLANATION

In this scenario, the hacker is looking for an easy target and doesn't care what they are attacking. This is considered an opportunistic attack.

If the hacker had been targeting a certain individual, company, organization, or nation, it would have been considered a targeted attack.

An insider attack is accomplished by a threat agent who has authorized access to an organization and either intentionally or unintentionally carries out an attack.

A nation state attack is accomplished by a threat agent that is a sovereign state who may wage an all-out war on a target and have significant resources and money at their disposal.

Question 5: ✓ Correct

The root account has all privileges and no barriers. Which of the following is another name for the root account?

○ Default account

○ Backdoor account

○ User account

➡ ● Superuser account

EXPLANATION

The root account is also known as the superuser account because it has the privilege to do anything on the system.

It is possible that a default account or a backdoor account could have superuser privileges, but these accounts are not inherently root accounts.

Question 6: ✓ Correct

Which of the following is the BEST example of the principle of least privilege?

- ○ Lenny has been given access to files that he does not need for his job.
- ➡ ● Wanda has been given access to the files that she needs for her job.
- ○ Mary has been given access to all of the file servers.
- ○ Jill has been given access to all of the files on one server.

EXPLANATION

Wanda being given access only to what she needs to do her job is an example of the principle of least privilege.

The principle of least privilege states that users or groups are given only the access they need to do their jobs and nothing more.

Question 7: ✓ Correct

Every ACME computer comes with the same account created at the factory. Which kind of vulnerability is this?

- ○ Weak passwords
- ○ Backdoor
- ○ Misconfigurations
- ➡ ● Default accounts and passwords

EXPLANATION

The factory account is considered a default account and would be a well-known default password.

This is not a backdoor, as it is not hard-coded.
This is not a misconfiguration because it is the factory default setting.
Although the password is weak because it is well-known, a default password could still be considered complex if it meets password complexity requirements.

Question 8: ✓ Correct

Social engineers are master manipulators. Which of the following are tactics they might use?

- ➡ ◉ Moral obligation, ignorance, and threatening
- ○ Shoulder surfing, eavesdropping, and keylogging
- ○ Eavesdropping, ignorance, and threatening
- ○ Keylogging, shoulder surfing, and moral obligation

EXPLANATION

Social engineers are master manipulators. Some of the most popular tactics they use are moral obligation, innate human trust, threatening, an easy reward, and ignorance.

Social engineering attacks include shoulder surfing, eavesdropping, USB and keyloggers, spam and spim, and hoaxes.

Question 9: ✓ Correct

Jason is at home, attempting to access the website for his music store. When he goes to the website, it has a simple form asking for a name, email, and phone number. This is not the music store website. Jason is sure the website has been hacked. How did the attacker accomplish this hack?

- ○ Social networking
- ➡ ● DNS cache poisoning
- ○ Host file modification
- ○ Feigning ignorance

EXPLANATION

In DNS cache poisoning, the attacker launches the attack on the chosen DNS server. Then the attacker changes a target website's IP address to a fake IP address. When the user enters the target website's URL, the DNS server redirects them to the fake IP address that was modified by the attacker. This ends up taking the target to a fake website controlled by the attacker.

In host file modification, the attacker sends a malicious code as an email attachment. When the user opens the attachment, the malicious code executes and modifies local host files on the user's computer.

Many social engineers use applications such as Facebook, Twitter, and Instagram to gather information and steal identities, among other nefarious acts.

An attacker feigning ignorance might make a wrong statement and then admit to not knowing much about the subject, but that event does not occur in this attack scenario.

Question 10: ✓ Correct

A collection of zombie computers have been set up to collect personal information. Which type of malware do the zombie computers represent?

- ➡ ◉ Botnet
- ○ Logic bomb
- ○ Trojan horse
- ○ Spyware

EXPLANATION

A botnet is a collection of zombie computers that are controlled from a central control infrastructure to propagate spam or to collect usernames and passwords to access secure information.

A logic bomb is malware that lies dormant until triggered.

A Trojan horse is a malicious program that is disguised as legitimate software.

Spyware monitors the actions performed on a machine and then sends the information back to its originating source.

Question 11: ✓ Correct

You have installed antivirus software on the computers on your network. You update the definition and engine files and configure the software to update those files every day.

What else should you do to protect your systems from malware? (Select two.)

- ➡ ☑ Educate users about malware.
- ☐ Disable UAC.
- ☐ Enable chassis intrusion detection.
- ➡ ☑ Schedule regular full-system scans.
- ☐ Enable account lockout.

EXPLANATION

You should schedule regular full-system scans to look for any malware. In addition, educate users about the dangers of downloading software and the importance of anti-malware protections.

You should enable User Account Control (UAC) to prevent unauthorized administrative changes to your system.

Use account lockout to help protect your system from hackers trying to guess passwords.

Use chassis intrusion detection to identify when the system case has been opened.

Question 12: ✓ Correct

Having a legitimate reason for approaching someone to ask for sensitive information is called what?

- ○ Preloading
- ○ Pretexting
- ○ Footprinting
- ➡ ● Impersonation

EXPLANATION

Impersonation is pretending to be somebody else and approaching a target to extract information.

Pretexting is using a fictitious scenario to persuade someone to perform an action or give information they aren't authorized to share.

Footprinting is similar to stalking, but in a social engineering context.

Preloading is influencing a target's thoughts, opinions, and emotions before something happens.

Question 13: ✓ Correct

Which of the following best describes spyware?

○ It monitors user actions that denote personal preferences and then sends pop-ups and ads to the user that match their tastes.

➡ ● It monitors the actions you take on your machine and sends the information back to its originating source.

○ It is a malicious program disguised as legitimate software.

○ It is a program that attempts to damage a computer system and replicate itself to other computer systems.

EXPLANATION

Spyware monitors the actions you take on your machine and sends the information back to its originating source.

Adware monitors the actions of the user that denote their personal preferences and then sends pop-ups and ads to the user that match their tastes.

A virus is a program that attempts to damage a computer system and replicate itself to other computer systems.

A Trojan horse is a malicious program disguised as legitimate software.

Question 14: ✓ Correct

Which of the following is the BEST definition of the term *hacker?*

○ A threat actor whose main goal is financial gain.

➡ ● A general term used to describe any individual who uses their technical knowledge to gain unauthorized access to an organization.

○ Any individual whose attacks are politically motivated.

○ The most organized, well-funded, and dangerous type of threat actor.

○ A threat actor who lacks skills and sophistication but wants to impress their friends or garner attention.

EXPLANATION

The term *hacker* is a general term used to describe any individual who uses their technical knowledge to gain unauthorized access to an organization.

The following are specific types of hackers, also known as threat actors:

- A hacktivist is any individual whose attacks are politically motivated.
- A nation state is the most organized, well-funded, and dangerous type of threat actor.
- An organized crime threat actor is a group of cybercriminals whose main goal is financial gain.
- A script kiddie is a threat actor who lacks skills and sophistication but wants to impress their friends or garner attention. Script kiddies carry out an attack by using scripts or programs written by more advanced hackers.

Question 15: ✓ Correct

Which security control, if not applied, can allow an attacker to bypass other security controls?

○ Changing default passwords

➡ ● Physical access control

○ Updating firmware or software

○ Principle of least privilege

EXPLANATION

With physical access to a system, many security controls can be circumvented. It is important to secure access to devices.

Question 16: ✓ Correct

Which impact of vulnerabilities occurs when an attacker uses information gained from a data breach to commit fraud by doing things like opening new accounts with the victim's information?

➡ ● Identity theft

○ Availability loss

○ Data loss

○ Data exfiltration

EXPLANATION

Identity theft is when an attacker uses data from a victim to commit fraud. Data loss is the loss of files and documents, either accidentally or through malicious acts. Data exfiltration is the transfer of information or files from a computer without authorization. Availability loss is when an attacker performs a malicious act to make a network so busy that the whole system goes down.

Question 17: ✓ Correct

Sometimes, an attacker's goal is to prevent access to a system rather than to gain access. This form of attack is often called a denial-of-service attack and causes which impact?

➡ ● Availability loss

○ Identity theft

○ Data exfiltration

○ Data loss

EXPLANATION

Denial-of-service (DoS) attacks intend to create availability loss to an important service. An example would be a botnet being used to exhaust the resources of a web server in order to deny access to the websites that it hosts.

Data loss, data exfiltration, and identity theft are not the main purposes of denial-of-service attacks.

Question 18: ✓ Correct

To answer this question, complete the lab using the information below.
You have already answered this question.
You are not allowed to view the lab again.

Launch Lab

You completed the lab correctly.

View Lab Report

Question 19: ✓ Correct

A wireless access point configured to use Wired Equivalent Privacy (WEP) is an example of which kind of vulnerability?

- ○ Zero-day exploit
- ○ Unpatched software
- ➡ ● Weak security configurations
- ○ Default settings

EXPLANATION

Configuring a wireless access point with WEP would be considered a weak security configuration because WEP has been shown to be insecure.

WEP is not a zero-day exploit because it is known to be a vulnerability. WEP is not a default setting on modern wireless access points and cannot be patched to become secure, so it is not an example of unpatched software.

Question 20: ✓ Correct

Which kind of malware provides an attacker with administrative control over a target computer through a backdoor?

- ○ Crypto-malware
- ➡ ● Remote Access Trojan (RAT)
- ○ Potentially Unwanted Program (PUP)
- ○ Trojan horse

EXPLANATION

A Remote Access Trojan (RAT) provides a backdoor for an attacker to remotely control a computer with administrative control. The other types of malware could be used in conjunction with a RAT, but they do not provide the remote control access.

PUP is software that contains adware, installs toolbars, or has other unclear objectives.

Crypto-malware is ransomware that encrypts files until a ransom is paid.

A Trojan horse is a malicious program that is disguised as legitimate or desirable software.

Question 21: ✓ Correct

Which kind of virus operates only in memory and usually exploits a trusted application like PowerShell to circumvent traditional endpoint security solutions?

- ○ Remote Access Trojan (RAT)
- ➡ ● Fileless virus
- ○ Ransomware
- ○ Worm

EXPLANATION

Fileless viruses operate only in memory to avoid detection by traditional endpoint security solutions that are focused on matching signatures to files that have been written to the hard drive.

A worm is a self-replicating program.

Ransomware denies access to a computer system until the user pays a ransom.

A Remote Access Trojan (RAT) is a malware program that includes a backdoor that allows administrative control over the target computer.

Question 22: ✓ Correct

A user is able to access privileged administrative features with an account that is not granted administrator rights. Which type of vulnerability is this?

➡ ● Privilege escalation

○ Stealing administrator credentials

○ Weak passwords

○ Backdoor account

EXPLANATION

Privilege escalation allows a user to gain privileges that aren't normally available to that user.

A backdoor account vulnerability would imply that the user knew a secret password in addition to their account.

Stealing administrator credentials is not privilege escalation because the account used already-granted privileges.

Weak passwords would not grant a user more privileges than what the account is configured for.

Question 23: ✓ Correct

DNS tunneling is a common method that allows an attacker to accomplish which attack?

○ Medical identity theft

➡ ● Data exfiltration

○ Data loss

○ Availability loss

EXPLANATION

A common tactic attackers use for data exfiltration is DNS tunneling. DNS tunneling is a method that allows an attacker to hide data being sent to an outside host by disguising it as DNS traffic on UDP port 53. Because DNS is critical to most network operations, it is generally not blocked on the firewall.

The other answers are not directly associated with DNS tunneling.

Question 24: ✓ Correct

In healthcare, regulations often dictate that important systems remain unpatched to maintain compliance. Which kind of vulnerability does this introduce?

➡ ◉ Inherent vulnerabilities

○ Application flaws

○ Weak passwords

○ Misconfigurations

EXPLANATION

Important systems may have to be left unpatched to comply with regulations or other constraints. This leads to these systems having inherent vulnerabilities that must be mitigated through other security controls.

Weak passwords are passwords that are blank, too short, dictionary words, or overly simple.

Application flaws are flaws in the validation and authorization of users. These flaws present the greatest threat to security in transactional applications.

The primary cause of misconfiguration is human error.

Question 25: ✓ Correct

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

- ➡ ☑ Impersonation
- ➡ ☑ Keylogging
- ➡ ☑ Shoulder surfing
- □ War dialing
- □ Port scanning

EXPLANATION

Social engineering leverages human nature. Internal employees are often the targets 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. Social engineers often employ keystroke loggers to capture usernames and passwords. Impersonation is pretending to be trustworthy and having a legitimate reason for approaching the target. This is done with the purpose of asking for sensitive information or access to protected systems. 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.

Question 26: ✕ Incorrect

Compliments, misinformation, feigning ignorance, and being a good listener are tactics of which social engineering technique?

○ Preloading

➡ ○ Elicitation

● ~~Interrogation~~

○ Impersonation

EXPLANATION

Elicitation is a technique that aims to extract information from a target without arousing suspicion. Some elicitation tactics are giving compliments, delivering misinformation, feigning ignorance, and being a good listener.

Preloading is used to set up a target by influencing the target's thoughts, opinions, and emotions.

In the interrogation phase, the attacker talks to the target about their statements.

Impersonation is pretending to be trustworthy and approaching the target to ask him or her for sensitive information or convincing him or her to grant access to protected systems.

Question 27: ✓ Correct

Any attack involving human interaction of some kind is referred to as what?

○ An opportunistic attack

○ A white hat hacker

➡ ◉ Social engineering

○ Attacker manipulation

EXPLANATION

Social engineering refers to any attack involving human interaction of some kind. Attackers who use social engineering try to convince a victim to perform actions or give out information they wouldn't under normal circumstances.

An opportunistic attack is typically automated and involves scanning a wide range of systems for known vulnerabilities, such as old software, exposed ports, poorly secured networks, and default configurations.

A white hat hacker helps companies find vulnerabilities in their security infrastructure.

Social engineers are master manipulators and use multiple tactics on their victims.

Question 28: ✓ Correct

In which phase of an attack does the attacker gather information about the target?

○ Breach the system

○ Exploit the system

➡ ◉ Reconnaissance

○ Escalating privileges

EXPLANATION

Reconnaissance is the phase of an attack where the attacker is gathering information about the target. This can be done electronically using scanning tools or even physically by going through dumpsters.

Escalation of privileges comes at the end of the attack when the attacker gains access to unauthorized data.

Breaching or exploiting the system is when the attacker gains access to a system on the target network using a vulnerability.

Question 29: ✓ Correct

A type of malware that prevents the system from being used until the victim pays the attacker money is known as what?

○ Denial-of-service attack (DoS attack)

○ Fileless virus

○ Remote Access Trojan (RAT)

➡ ● Ransomware

EXPLANATION

A type of malware used to prevent the system from being used until a ransom is paid by the victim is known as ransomware.

While it does perform a denial of service, a DoS attack doesn't necessarily demand payment.

A Remote Access Trojan (RAT) is a malware program that includes a backdoor that allows administrative control over the target computer.

A fileless virus uses legitimate programs to infect a computer.

Question 30: ✓ Correct

Which of the following is a program that appears to be a legitimate application, utility, game, or screensaver, but performs malicious activities surreptitiously?

○ ActiveX control

○ Worm

➡ ● Trojan horse

○ Outlook Express

EXPLANATION

A Trojan horse is a program that appears to be a legitimate application, utility, game, or screensaver, but performs malicious activities surreptitiously. Trojan horses are very common on the internet. To keep your systems secure and free from such malicious code, you need to take extreme caution when downloading any type of file from just about any site on the internet. If you don't fully trust the site or service that is offering a file, don't download it.

Outlook Express is an email client found on Windows.

A worm is a type of malicious code similar to a virus. A worm's primary purpose is to duplicate itself and spread while not necessarily intentionally damaging or destroying resources.

ActiveX controls are web applications written in the ActiveX framework.