Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 1/30/2022 11:59:05 am • Time spent: 00:59

Score: 100%

Passing Score: 80%

Question 1: ✓ Correct

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

➡ ● Default accounts and passwords

○ Backdoor

○ Misconfigurations

○ Weak 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 2: ✓ Correct

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

- ○ Misconfigurations
- ○ Application flaws
- ○ Weak passwords
- ➡ ◉ Inherent vulnerabilities

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 3: ✓ Correct

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

- ○ Changing default passwords
- ○ Principle of least privilege
- ○ Updating firmware or software
- ➡ ◉ Physical access control

EXPLANATION

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

Question 4: ✓ 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?

- ○ Weak passwords
- ○ Stealing administrator credentials
- ➡ ◉ Privilege escalation
- ○ 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 5: ✓ Correct

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

- ➡ ◉ Superuser account
- ○ User account
- ○ Default account
- ○ Backdoor 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

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

○ Zero-day exploit

○ Default settings

○ Unpatched software

➡ ● Weak security configurations

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 7: ✓ 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?

○ Data loss

➡ ● Availability loss

○ Data exfiltration

○ Identity theft

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 8: ✓ Correct

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

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

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 9: ✓ Correct

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

- ○ Availability loss
- ○ Data loss
- ➡ ● Data exfiltration
- ○ Medical identity theft

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 10: ✓ 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 exfiltration
- ○ Data loss

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.