Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/24/2022 7:57:09 pm • Time spent: 00:09

Score: 0% Passing Score: 80%

Question 1: ✕ Incorrect

While developing a network application, a programmer adds functionally that allows her to access the running program without authentication so she can capture debugging data. The programmer forgets to remove this functionality prior to finalizing the code and shipping the application.

Which type of security weakness does this describe?

- Buffer overflow
- Privilege escalation
- Weak password
- Backdoor

EXPLANATION

A backdoor is an unprotected access method or pathway. Backdoors may include hard-coded passwords or hidden service accounts. They are often added during development as a shortcut to circumvent security. If they are not removed, they present a security problem.

Privilege escalation allows a user to take advantage of a software bug or design flaw in an application to gain access to system resources or additional privileges that would typically not be available to the user.

Weak passwords are passwords that are blank, too short, dictionary words, or not complex enough. This allows them to be quickly identified using password-cracking tools.

A buffer overflow occurs when the operating system or an application does not properly enforce boundaries for how much and which type of data can be inputted.

REFERENCES

5.9.2 Device Vulnerability Facts

q_dev_vuln_backdoor_01_secp7.question.fex

Question 2: ✕ Incorrect

An attacker was able to gain unauthorized access to a mobile phone and install a Trojan horse so that he or she could bypass security controls and reconnect later.

Which type of attack is this an example of?

- Social engineering
- Backdoor
- Privilege escalation
- Replay

EXPLANATION

A backdoor is an unprotected access method or pathway. Backdoors:

- Include hard-coded passwords and hidden service accounts.
- Are often added during development as a shortcut to circumvent security. If they are not removed, they present a security problem.
- Can be added by attackers who have gained unauthorized access to a device. When added, the backdoor can be used at a future time to easily bypass security controls.
- Can be used to remotely control the device at a later date.
- Rely on secrecy to maintain security.

Social engineering attacks involve stealing information or convincing someone to perform an inappropriate activity via email, via phone, or in person.

A replay attack is a network attack that occurs when an attacker intercepts data and fraudulently delays or re-transmits it.

Privilege escalation allows a user to take advantage of a software bug or design flaw in an application to gain access to system resources or additional privileges that aren't typically available to that user.

REFERENCES

5.9.2 Device Vulnerability Facts

q_dev_vuln_backdoor_02_secp7.question.fex

Question 3: ✕ Incorrect

In an effort to increase the security of your organization, programmers have been informed they can no longer bypass security during development.

Which vulnerability are you attempting to prevent?

- Privilege escalation
- Social engineering
- Replay
- ➡ Backdoor

EXPLANATION

A backdoor is an unprotected access method or pathway. Backdoors:

- Include hard-coded passwords and hidden service accounts.
- Are often added during development as a shortcut to circumvent security. If they are not removed, they present a security problem.
- Can be added by attackers who have gained unauthorized access to a device. When added, the backdoor can be used at a future time to easily bypass security controls.
- Can be used to remotely control the device at a later date.
- Rely on secrecy to maintain security.

Social engineering attacks involve stealing information or convincing someone to perform an inappropriate activity via email, phone, or in person.

A replay attack is a network attack that occurs when an attacker intercepts data and fraudulently delays or re-transmits it.

Privilege escalation allows a user to take advantage of a software bug or design flaw in an application to gain access to system resources or additional privileges that aren't typically available to that user.

REFERENCES

5.9.2 Device Vulnerability Facts

q_dev_vuln_backdoor_03_secp7.question.fex

Question 4: ✕ Incorrect

Which of the following are characteristics of a complex password? (Select two.)

- [x] Consists of letters, numbers, and symbols
- [ ] Consists of letters and numbers only
- [ ] Has a minimum of six characters
- [ ] Has a maximum of fifteen characters
- [x] Has a minimum of eight characters

EXPLANATION

Complex passwords require a certain length (typically over eight characters) and a mix of character types (numbers and symbols) along with requirements that the password not consist of words, variations of words, or derivatives of the username.

There is no maximum character limit for a complex password.

REFERENCES

5.9.2 Device Vulnerability Facts

q_dev_vuln_complex_secp7.question.fex

Question 5: ✕ Incorrect

An attacker has gained access to the administrator's login credentials. Which type of attack has most likely occurred?

- Buffer overflow
- Privilege escalation
- Backdoor
- ➡ Password cracking

EXPLANATION

Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system. If an attacker has gained access to the administrator's login credentials, this is most likely the cause of a password-cracking attack.

Privilege escalation allows a user to take advantage of a software bug or design flaw in an application to gain access to system resources or additional privileges that would typically not be available to the user.

A backdoor is an unprotected access method or pathway. Backdoors may include hard-coded passwords or hidden service accounts.

A buffer overflow attack occurs when the operating system or an application does not properly enforce boundaries for how much and which type of data can be inputted.

REFERENCES

5.9.2 Device Vulnerability Facts

11.7.2 Password Attack Facts

11.7.5 Crack Passwords

11.7.6 Crack Password Protected Files

11.7.7 Crack a Password with John the Ripper

q_dev_vuln_cracking_secp7.question.fex

Question 6: ✕ Incorrect

When setting up a new wireless access point, what is the first configuration change that should be made?

- Encryption protocol
- SSID
- MAC filtering
- Default login

EXPLANATION

Whenever any new network device is turned on for the first time, the default login information should be changed immediately.

Neither the SSID, encryption protocol, nor MAC filtering is the first configuration change that should be made when setting up a new wireless access point.

REFERENCES

5.9.2 Device Vulnerability Facts

q_dev_vuln_default_secp7.question.fex

Question 7: ✕ Incorrect

You've just deployed a new Cisco router that connects several network segments in your organization.

The router is physically located in a server room that requires an ID card to gain access. You've backed up the router configuration to a remote location in an encrypted file. You access the router configuration interface from your notebook computer by connecting it to the console port on the router. You've configured the management interface with a username of admin and a password of password.

What should you do to increase the security of this device?

- Move the device to a secure data center.
- ➡ Use a stronger administrative password.
- Include hard-coded passwords and hidden service accounts.
- Use an SSH client to access the router configuration.

EXPLANATION

In this scenario, the password assigned to the device is weak and can be easily guessed. The password should be replaced with a strong one that is at least eight characters long, uses uppercase and lowercase letters, and uses numbers or symbols.

Including hard-coded passwords and hidden service accounts is an option for avoiding backdoor vulnerabilities.

Using the console port to access the device creates a dedicated connection, making the use of SSH unnecessary.

Because the device has been installed in a secured room, it's not necessary to move it to a data center.

REFERENCES

5.9.2 Device Vulnerability Facts

q_dev_vuln_password_secp7.question.fex

Question 8: ✕ Incorrect

A relatively new employee in the data entry cubical farm was assigned a user account similar to the other data entry employees' accounts. However, audit logs have shown that this user account has been used to change ACLs on several confidential files and has accessed data in restricted areas.

This situation indicates which of the following has occurred?

- Social engineering
- Physical security
- External attack
- ➡ Privilege escalation

EXPLANATION

This situation describes the result of a successful privilege escalation attack. If a low-end user account is detected performing high-level activities, it is obvious that the user account has somehow gained additional privileges.

Physical security is the protection of corporate assets from threats such as theft or damage.

Social engineering attacks involve stealing information or convincing someone to perform an inappropriate activity via email, phone, or in person.

External attacks are when unauthorized individuals try to breach a network from off-site.

REFERENCES

2.4.2 Vulnerability Concerns Facts

5.9.2 Device Vulnerability Facts

6.1.4 Access Control Best Practices

q_dev_vuln_privilege_01_secp7.question.fex

Question 9: ✕ Incorrect

An attacker has obtained the logon credentials for a regular user on your network. Which type of security threat exists if this user account is used to perform administrative functions?

- Social engineering
- Replay
- Impersonation
- Privilege escalation

EXPLANATION

Privilege escalation allows a user to take advantage of a software bug or design flaw in an application to gain access to system resources or additional privileges that are typically not available to normal users. Examples of privilege escalation include:

- A user accessing a system with a regular user account and successfully accessing functions reserved for higher-level user accounts (such as administrative features).
- A user who is able to access content that should be accessible only to a different user.
- A user who should have only administrative access being able to access content that should only be accessible to a regular user.

Privilege escalation does not occur when a user is able to steal or hack administrator credentials and is, therefore, able to access administrative functions. Privilege escalation refers to accessing features with an account that normally should not have access to those features.

REFERENCES

2.4.2 Vulnerability Concerns Facts

5.9.2 Device Vulnerability Facts

6.1.4 Access Control Best Practices

q_dev_vuln_privilege_02_secp7.question.fex

Question 10: ✕ Incorrect

Travis and Craig are both standard users on the network. Each user has a folder on the network server that only they can access. Recently, Travis has been able to access Craig's folder.

This situation indicates which of the following has occurred?

- ➡ Privilege escalation
- Social engineering
- Replay
- External attack

EXPLANATION

This situation describes the result of a successful privilege escalation attack. If a user is able to access content that should only be accessible to a different user, it is obvious that a privilege escalation attack has occurred.

Social engineering attacks involve stealing information or convincing someone to perform an inappropriate activity via email, phone, or in person.

A replay attack is a network attack that occurs when an attacker intercepts data and fraudulently delays or re-transmits it.

External attacks are when unauthorized individuals try to breach a network from off-site.

REFERENCES

2.4.2 Vulnerability Concerns Facts

5.9.2 Device Vulnerability Facts

6.1.4 Access Control Best Practices

q_dev_vuln_privilege_03_secp7.question.fex