Exam Report: 6.2.6 Practice Questions

Date: 1/21/2020 4:08:30 pm
Time Spent: 3:22

Candidate: Garsteck, Matthew
Login: mGarsteck

## Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

## Individual Responses

**Question 1:** Correct

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
- Man-in-the-middle attack
- Privilege escalation
- Smurf attack

### 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 user account has somehow gained additional privileges.

A man-in-the-middle attack involves a third party placing themselves between two legitimate communication partners in order to intercept and possibly alter their transmissions. Social engineering attacks involve stealing information or convincing someone to perform an inappropriate activity via email, phone, or in person. A smurf attack is a form of distributed reflective denial of service where spoofed ICMP packets are bounced and multiplied off another network to flood the victim's communication pipeline.

### References

LabSim for Security Pro, Section 6.2.
[All Questions SecPro2017_v6.exm NET_DEVICE_VULN_01]

**Question 2:** Correct

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
- Privilege escalation
- Impersonation
- Replay

### 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 who is able to access 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.

**Note**: 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

LabSim for Security Pro, Section 6.2.
[All Questions SecPro2017_v6.exm NET_DEVICE_VULN_02]

**Question 3:** Correct

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 configured the management interface with a user name of **admin** and a password of **password**.

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

- (selected) Use a stronger administrative password.
- Move the device to a secure data center.
- Use an SSH client to access the router configuration.
- Use a web browser to access the router configuration using an HTTP connection.

## Explanation

In this scenario, the password assigned to the device is weak and easily guessed. It should be replaced with a strong password that is at least eight characters long, uses upper- and lower-case letters, and uses numbers or symbols.

Using HTTP to manage the router configuration could expose sensitive information to sniffers, as it transmits data in cleartext. 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

LabSim for Security Pro, Section 6.2.
[All Questions SecPro2017_v6.exm NET_DEVICE_VULN_03]

**Question 4:** Correct

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.

What type of security weakness does this represent?

- Buffer overflow
- Privilege escalation
- (selected) Backdoor
- Weak passwords

## 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, which 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 what type of data can be inputted.

## References

LabSim for Security Pro, Section 6.2.
[All Questions SecPro2017_v6.exm NET_DEVICE_VULN_04]

**Question 5:** Correct

You've just deployed a new Cisco router so you can connect a new segment to your organization's network.

The router is physically located in a server room that can only be accessed with an ID card. You've backed up the the router configuration to a remote location in an encrypted file. You access the router configuration from your notebook computer by connecting it to the console port on the router. The web-based management interface uses the default user name of **cusadmin** and a password of **highspeed**.

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

- (●) Change the user name and create a more complex password.
- ( ) Remove any backdoors that might have been created by a programmer.
- ( ) Change the user name.
- ( ) Create a more complex password.

## Explanation

You should change the user name and create a more complex password. The default user name and password for Cisco routers and other routers can be found on the internet, so they should both be changed when the router is put into production.

## References

LabSim for Security Pro, Section 6.2.
[All Questions SecPro2017_v6.exm NET_DEV_VULN_05]