Exam Report: 12.3.5 Practice Questions

Date: 11/20/2019 5:55:23 pm
Time Spent: 11:53

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 13%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Arrange the steps in the change and configuration management process on the left into correct completion order on the right.

Step 1
- ✓ Identify the need for a change.

Step 2
- ✓ Conduct a feasibility analysis.

Step 3
- ~~Test the implementation.~~ Define the procedure for implementing the change.

Step 4
- ~~Define the procedure for implementing the change.~~ Notify affected parties of the pending change.

Step 5
- ✓ Implement the change.

Step 6
- ~~Notify affected parties of the pending change.~~ Test the implementation.

Step 7
- ✓ Document the change.

Explanation

The change and configuration management processes used in most organizations include the following steps:

- Identify the need for a change.
- Conduct a feasibility analysis that includes technical and budgetary considerations. Identify any potential impacts to the network.
- Define a procedure for implementing the change.
- Notify all affected parties of the pending change.
- Implement the change. This includes identifying a maintenance window when the system will be unavailable.
- Test the implementation to make sure it conforms to the plan and does not adversely affect the network.
- Document the change.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm RT NP15_5.8-5]

Question 2: Incorrect

Match each third-party integration phase on the left with the tasks that need to be completed during that phase on the right. Each phase may be used once, more than once, or not at all.

Communicate vulnerability assessment findings with the other party.

Ongoing operations

Disable VPN configurations that allow partner access to your network.

Off-boarding

Compare your organization's security policies with the partner's policies.

~~Ongoing operations~~ Onboarding

Disable the domain trust relationship between networks.

Off-boarding

Identify how privacy will be protected.

Onboarding

Draft an ISA.

Onboarding

Conduct regular security audits.

Ongoing operations

Explanation

During the onboarding phase of a relationship you should take steps to ensure that the integration process maintains the security of each party's network by completing tasks, such as:

- Comparing your organization's security policies and infrastructure against each partner organization's policies and infrastructure.
- Identifying how privacy will be protected.
- Drafting an ISA to document how the information systems of each party in the relationship will be connected and how they will share data.

During the ongoing operations phase of the relationship you need to verify that all parties are abiding by the Interoperability Agreement documents. To do this, you should:

- Conduct regular security audits to ensure that each party in the relationship is following the security-related aspects of the IA documents.
- Communicate vulnerability assessment and security audit findings with all of the parties in the relationship to maintain risk awareness.

When the relationship with the third party ends, you need to ensure that all of the doors that were opened between organizations during the onboarding phase are closed by completing tasks, such as:

- Disabling any VPN, firewall, router, or switch configurations that allowed access to your network from the third-party network.
- Disabling any domain trust relationships that were established between the organizations.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm RT-4.10-4]

Question 3: Incorrect

What is the most common security policy failure?

- ~~Improperly outlined procedures~~
- Failure to assign responsibilities
- Overlooked critical assets
- Lack of user awareness

Explanation

The most common security policy failure is a lack of user awareness. If users are not aware of the policies to follow or procedures to comply with, they do not know how to perform their work tasks securely.

When an organization makes the effort to produce a security policy, improperly outlined procedures are rarely a problem. This issue is usually discovered and corrected early in the security policy development process. Overlooking critical assets is not a common problem. During the asset identification stage of risk analysis and security policy development, every asset is examined for importance. A security policy is not complete unless it assigns specific tasks and responsibilities to roles and individuals within the organization.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm SP02_5-8 [5]]

Question 4: Incorrect

Which business document is a contract that defines the tasks, time frame, and deliverables that a vendor must perform for a client?

- ~~Master service agreement~~
- Interconnection security agreement
- Memorandum of understanding
- Statement of work

Explanation

A statement of work is a contract that defines the tasks, time frame, and deliverables that a vendor agrees to before it provides services to a client. A statement of work usually includes specific requirements and a pricing structure for the work performed.

A master service agreement is a contract that defines terms that will govern future agreements between two parties. A memorandum of understanding provides a brief summary of which parties in the relationship are responsible for performing specific tasks. An interconnection security agreement documents how the information systems of each party in the relationship will be connected and how they will share data.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm RT NP15_5.5-2]

Question 5: Incorrect

A code of ethics accomplishes all but which of the following?

- ~~Establishes a baseline for managing complex situations.~~
- Improves the professionalism of your organization as well as your profession.
- Clearly defines courses of action to take when a complex issue is encountered.
- Serves as a reference for the creation of acceptable use policies.

Explanation

A code of ethics does not provide clear courses of action when faced with complex issues and situations. That's the whole problem with ethical dilemmas--a right or wrong answer is not always easily determined. A code of ethics describes best practices and helps steer intentions to allow individuals and organizations to respond to complex situations in the most appropriate manner.

A code of ethics does establish a baseline for managing complex situations, improve professionalism, and serve as a reference for the creation of acceptable use policies.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm SP02_5-4 [109]]

Question 6: Incorrect

Match each interoperability agreement document on the left with the appropriate description on the right. Each document may be used once, more than once, or not at all.

Specifies exactly which services will be performed by each party.

SLA

Binds a vendor in an agreement to provide services on an ongoing basis.

~~SLA~~ BPO

Provides a summary of which party is responsible for performing specific tasks.

~~ISA~~ MOU

Documents how the networks will be connected.

~~BPO~~ ISA

Defines how disputes will be managed.

~~MOU~~ SLA

Specifies a preset discounted pricing structure.

~~ISA~~ BPO

Explanation

Several key documents that may be included within an interoperability agreement (IA):

- A service level agreement (SLA) specifies exactly which services will be performed by the third party and what level of performance they guarantee. An SLA may also provide warranties, specify disaster recovery procedures, define how disputes will be managed, and specify when the agreement will be terminated.
- A blanket purchase order (BPO) is an agreement with a third party vendor that the vendor will provide services on an ongoing basis. BPOs are typically negotiated to take advantage of a preset discounted pricing structure.
- A memorandum of understanding (MOU) is a very important document that provides a brief summary of which party in the relationship is responsible for performing specific tasks. In essence, the MOU specifies who is going to do what and when.
- An interconnection security agreement (ISA) documents how the information systems of each party in the relationship will be connected and how they will share data.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm RT-4.10-1]

Question 7: Correct

Which of the following defines an acceptable use agreement?

- (●) An agreement that identifies the employee's rights to use company property, such as internet access and computer equipment, for personal use.
- ( ) An agreement that is a legal contract between the organization and the employee that specifies that the employee is not to disclose the organization's confidential information.
- ( ) An agreement that outlines the organization's monitoring activities.
- ( ) An agreement that prohibits an employee from working for a competing organization for a specified time after the employee leaves the organization.

Explanation

The acceptable use agreement identifies the employee's rights to use company property, such as internet access and computer equipment, for personal use.

The non-compete agreement prohibits an employee from working for a competing organization for a specified time after the employee leaves the organization. The employee monitoring agreement outlines the organization's monitoring activities. The non-disclosure agreement is a legal contract between the organization and the employee that specifies that the employee is not to disclose the organization's confidential information.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm SSCP-7 NEW [118]]

Question 8: Incorrect

Your organization entered into an interoperability agreement (IA) with another organization a year ago. As a part of this agreement, a federated trust was established between your domain and the partner domain.

The partnership has been in the ongoing operations phase for almost nine months now. As a

security administrator, which tasks should you complete during this phase? (Select two.)

- [x] Verify compliance with the IA documents.
- [ ] Negotiate the BPO agreement.
- [x] ~~Disable user and group accounts that the partner organization used to access your organization's data.~~
- [ ] Conduct periodic vulnerability assessments.
- [ ] Draft an MOU document.

Explanation

During the ongoing operations phase of the relationship, you should:

- Regularly verify compliance with the IA documents.
- Conduct periodic vulnerability assessments to verify that the network interconnections created by the relationship have not exposed or created security weaknesses.

BPO negotiations and MOU drafting should have taken place during the onboarding phase of the relationship. User and group accounts should have been disabled during the off-boarding phase.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm RT-4.10-2]

Question 9: Correct

Which of the following are typically associated with human resource security policies? (Select two.)

- [ ] Change management
- [x] Termination
- [ ] SLA
- [ ] Password policies
- [x] Background checks

Explanation

Human resource policies related to security might include the following:

- Hiring policies, which identify processes to follow before hiring. For example, the policy might specify that pre-employment screening include a background check.
- Termination policies and procedures, which identify processes to be implemented when terminating employees.
- A requirement for job rotation, which cross-trains individuals and rotates users between positions on a regular basis.
- A requirement for mandatory vacations, which require employees to take vacations of specified length.

Service level agreements (SLAs), sometimes called maintenance contracts, guarantee a subscriber a certain quality of a service from a network service provider. Password policies detail passwords requirements for the organization. A change and configuration management policy provides a structured approach to securing company assets and making changes.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm SP08_6-4 1]

Question 10: Incorrect

Which business document is a contract that defines a set of terms that will govern future agreements between two parties?

- ( ) ~~Memorandum of understanding~~
- ( ) Master service agreement

- Statement of work
- Interconnection security agreement

Explanation

A master service agreement is a contract that defines terms that will govern future agreements between two parties. The purpose of this document is to allow the parties to quickly negotiate future agreements without having to repetitively renegotiate the same terms over and over.

A statement of work is a contract that defines the tasks, time frame, and deliverables that a vendor agrees to with a client. A memorandum of understanding provides a brief summary of which party in the relationship is responsible for performing specific tasks. An interconnection security agreement documents how the information systems of each party in the relationship will be connected and how they will share data.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm RT NP15_5.5-1]

Question 11: Incorrect

Your organization is in the process of negotiating an interoperability agreement (IA) with another organization. As a part of this agreement, the partner organization proposes that a federated trust be established between your domain and their domain. This configuration will allow users in their domain to access resources in your domain and vice versa.

As a security administrator, which tasks should you complete during this phase? (Select two.)

- [ ] Conduct security audits on the partner organization.
- [x] Identify how data will be shared.
- [ ] Verify compliance with the IA documents.
- [ ] Identify how data ownership will be determined.
- [x] ~~Reset all passwords the third-party uses to access data or applications on your network.~~

Explanation

During the onboarding phase of a third-party relationship, several issues need to be considered and a plan formulated to address them, including:

- How data ownership will be determined.
- How data will be shared.

Security and compliance audits should be conducted during the ongoing operations phase of the relationship. Partner passwords should be reset during the off-boarding phase.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm RT-4.10-3]

Question 12: Incorrect

You have installed anti-virus software on computers at your business. Within a few days, however, you notice that one computer has a virus. When you question the computer's user, she says she did install some software a few days ago, but it was supposed to be a file compression utility. She admits she did not scan the file before running it.

What should you add to your security measures to help prevent this from happening again?

- Proxy server
- User awareness training
- ~~Account lockout~~
- Close unused firewall ports

Explanation

Many anti-virus prevention measures are ineffective if users take actions that put their computers at risk (such as downloading and running files or copying unscanned files to their

computers). If users are educated about malware and about the dangers of downloading software, the overall security of the environment improves.
A proxy server controls access to the internet based on username, URL, or other criteria.
Account lockout helps prevent attackers from guessing passwords. Firewall ports might be used by some malware, but will not prevent malware introduced by downloading and installing a file.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm AP09PA_4-1 D3]

Question 13: Incorrect

Which component of a change and configuration management policy specifies options for reverting a system back to the state it was in before a change was made?

- ~~Change request~~
- Feasibility analysis
- Authorized downtime
- Rollback

Explanation

In the event that a change unintentionally causes problems, your change and configuration management process should include provisions for a rollback. A rollback makes it possible to revert the system back to the state it was in before the change was put into effect.

Authorized downtime defines a maintenance window during which the system will be unavailable while the change is made. A change request identifies the need for a change. A feasibility analysis identifies technical and budgetary considerations for a change. It also identifies any potential impacts to the network.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm RT NP15_5.8-2]

Question 14: Incorrect

Which component of a change and configuration management policy identifies technical and budgetary considerations associated with a proposed change and also identifies any potential impacts to the network?

- Change request
- Feasibility analysis
- Authorized downtime
- ~~Rollback~~

Explanation

A feasibility analysis identifies technical and budgetary considerations associated with a proposed change. It should also identify any potential impacts to the network.

In the event that a change unintentionally causes problems, your change and configuration management process should include provisions for a rollback. A rollback makes it possible to revert the system back to the state it was in before the change was put into effect. Authorized downtime defines a maintenance window during which the system will be unavailable while the change is made. A change request identifies the need for a change.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm RT NP15_5.8-3]

Question 15: Incorrect

Which component of a change and configuration management policy identifies the need for a proposed change?

- ~~Authorized downtime~~
-

- Feasibility analysis
- Rollback
- Change request

Explanation

A change request identifies the need for a change. It also documents the specific change to be made.

A feasibility analysis identifies technical and budgetary considerations associated with a proposed change. It should also identify any potential impacts to the network. In the event that a change unintentionally causes problems, your change and configuration management process should include provisions for a rollback. A rollback makes it possible to revert the system back to the state it was in before the change was put into effect. Authorized downtime defines a maintenance window during which the system will be unavailable while the change is made.

References

LabSim for Network Pro, Section 12.3.
[netpro18v5_all_questions_en.exm RT NP15_5.8-4]