Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/15/2022 7:39:19 pm • Time spent: 05:22

Score: 80% Passing Score: 80%

Question 1: ✔ Correct

You have hired 10 new temporary workers who will be with the company for three months. You want to make sure that the user accounts cannot be used for login after that time period. What should you do?

- Configure account lockout in Group Policy.
- Configure account policies in Group Policy.
- ➡ Configure account expiration in the user accounts.
- Configure day/time restrictions in the user accounts.

EXPLANATION

You should configure account expiration to disable an account after a specific date.

Use day/time restrictions to limit the days and hours when users can log on. Use account policies in Group Policy to configure requirements for passwords. Use account lockout settings in Group Policy to automatically lock accounts when a specific number of incorrect passwords are entered.

Question 2: ✔ Correct

Which Microsoft tool can be used to review a system's security configuration against recommended settings?

- Windows Defender
- Microsoft Internet Explorer
- ➡ Microsoft Security Compliance Toolkit
- Registry Editor

EXPLANATION

The Microsoft Security Compliance Toolkit allows enterprise security administrators to download, analyze, test, edit, and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products.

Internet Explorer is a web browser.

Registry Editor is used to change settings in the Windows Registry.

Windows Defender uses signatures to identify malicious applications.

Question 3: ✔ Correct

Which type of update should be prioritized even outside of a normal patching window?

- Microsoft updates
- Monthly updates
- ➡ Critical updates
- Security updates

EXPLANATION

The correct answer is critical updates. These updates are often marked critical because of the severity of the exploit or how widespread it is.

Microsoft, monthly, and security updates do not necessarily demand to be installed outside of a normal patching window.

Question 4: ✕ Incorrect

Prepare to Document means establishing the process you will use to document your network.

Which of the following makes this documentation more useful?

- Identify the choke points on the network.
- ➡ Have a printed hard copy kept in a secure location.
- Automate administration as much as possible.
- ~~Identify who is responsible for each device.~~

EXPLANATION

Prepare to Document means establishing the process you will use to document your network. A useful document:

- Is easy to use
- Includes enough detail
- Documents the important things
- Uses timestamps
- Is protected with restricted access and possibly encryption
- Has a printed hard copy kept in a secure location

Identifying who is responsible for each device is included in the Map Your Network milestone.

Identifying the choke points on the network is included in the Protect Your Network milestone.

Automating administration as much as possible is included in the Reach Your Network milestone.

Question 5: ✔ Correct

Documenting procedures and processes are part of which milestone in the NSA's Manageable Network Plan?

- ➡ Document Your Network
- Reach Your Network
- Prepare to Document
- Control Your Network

EXPLANATION

Milestone 8 (Document Your Network) is the milestone of the plan that includes documenting procedures and processes.

Milestone 1 (Prepare to Document) establishes the guidelines for how to create documentation.

Milestone 4 (Reach Your Network) defines how to maintain secure access to network devices.

Milestone 5 (Document Your Network) defines how to limit access to network devices.

Question 6: ✔ Correct

In which milestone should you use a network scanner and then confirm the scan manually with a room-by-room walkthrough?

- Prepare to Document
- Map Your Network
- Protect Your Network
- Reach Your Network

EXPLANATION

The Map Your Network milestone ensures that you are aware of all the components of the network and that you know where the physical devices are. The steps are:

- Create a map of the network topology.
- Create a list of all devices.
  - Don't forget to include wireless devices.
  - Use a network scanner and then confirm the scan manually with a room-by-room walkthrough.
  - Identify who is responsible for each device and detail other information, such as IP address, service tag, and physical location.
  - Consider using a database file to store the information.
- Create a list of all protocols being used on the network by using a network analyzer. Consider removing unauthorized devices and protocols from your network.

The Prepare to Document milestone means establishing the process you will use to document your network.

The Protect Your Network (network architecture) milestone identifies the necessary steps to protect your network.

The Reach Your Network (device accessibility) milestone helps to ensure that all of the devices on your network can be easily accessed while still maintaining each device's security. Accessibility includes physical access as well as remote access.

Question 7: ✔ Correct

Windows Server Update Services (WSUS) is used to accomplish which part of a manageable network?

- User access
- Documentation
- Patch management
- Device accessibility

EXPLANATION

Patch management is managed by Windows Server Update Services (WSUS) by keeping Windows systems up to date.

WSUS does not help with documentation, controlling user access, or ensuring devices are accessible.

Question 8: ✕ Incorrect

You have recently been hired as the new network administrator for a startup company. The company's network was implemented prior to your arrival. One of the first tasks you need to complete in your new position is to develop a manageable network plan for the network.

You have already completed the first and second milestones, in which documentation procedures were identified and the network was mapped. You are now working on the third milestone, which is identifying ways to protect the network.

Which tasks should you complete as a part of this milestone? (Select two.)

- ➡ ☑ Physically secure high-value systems.
- ☐ Apply critical patches whenever they are released.
- ➡ ☐ Identify and document each user on the network.
- ☐ Create an approved application list for each network device.
- ☑ ~~Set account expiration dates.~~

EXPLANATION

In the third milestone (Protect Your Network), you should take the following steps:

- Identify and document each user on the network and the information he or she has access to.
- Identify high-value network assets.
- Document the trust boundaries.
- Identify the choke points on the network.
- Segregate and isolate networks.
- Isolate server functions.
- Physically secure high-value systems.

Setting account expiration dates is part of the fifth milestone (Control Your Network).

Applying critical patches and creating an approved application list are both tasks associated with the sixth milestone (Manage Your Network).

Question 9: ✔ Correct

For Milestone 4 (Reach Your Network), which of the following would be considered a secure protocol to use to reach your network?

- ➡ SSH
- FTP
- HTTP
- Telnet

EXPLANATION

Of the protocols listed, only Secure Shell (SSH) is encrypted. The other protocols would expose data to being easily intercepted.

Question 10: ✔ Correct

As you go through the process of making your network more manageable, you discover that employees in the sales department are on the same network segment as the human resources department.

Which of the following steps can be used to isolate these departments?

- Implement the principle of least privilege for the human resources department.
- ➡ Create a separate VLAN for each department.
- Identify the choke points on your network.
- Move the sales department into the DMZ.

EXPLANATION

VLANs can be used to isolate these departments.

The sales department is not a lower-trust part of the network, so they do not belong in the DMZ.

You would identify choke points as part of the process of limiting the number of internet access points on your network in order to decrease the attack surface.

The principle of least privilege is used to control user access to network resources. However, this principle does not segregate and isolate network segments from each other.