Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/15/2022 9:12:19 pm • Time spent: 03:22

Score: 90% Passing Score: 80%

Question 1: ✔ Correct

Which of the following tools can you use on a Windows network to automatically distribute and install software and operating system patches on workstations? (Select two.)

- [ ] Security Configuration and Analysis
- [x] WSUS
- [x] Group Policy
- [ ] Security Templates

EXPLANATION

Windows Software Update Services (WSUS) is a patch management tool that allows clients on a network to download software updates from an internal WSUS server in their organization.

- The WSUS server receives a list of available updates from Microsoft.
- On the WSUS server, you identify allowed or required patches for your organization.
- Clients download only approved patches from an internal WSUS server or directly from Microsoft.

You can also use Group Policy to distribute and automatically install patches. You must use Group Policy to install updates to non-Microsoft software that is not supported with WSUS.

Use the Security Templates snap-in to create and edit templates that enforce system security settings. Use the Security Configuration and Analysis snap-in to compare the existing settings with the template or to apply a template to a single device. Use Group Policy to automatically apply security templates.

Question 2: ✔ Correct

Which of the following describes a configuration baseline?

- ➡ A list of common security settings that a group or all devices share
- The minimum services required for a server to function
- A collection of security settings that can be automatically applied to a device
- A set of performance statistics that identifies normal operating performance

EXPLANATION

A configuration baseline is a set of consistent requirements for a workstation or server. Configuration baselines include a component that ensures that all workstations and servers comply with the security goals of the organization.

A security template is a saved set of configuration values that produce the system configuration as specified in the configuration baseline. When you apply the security template to a system, the settings within the template are applied to the system.

A performance baseline is a set of performance statistics that identify normal operating performance.

Question 3: ✔ Correct

What should you consider security baselines?

- Suggestion
- Static
- ➡ Dynamic
- Unchangeable

EXPLANATION

Because most environments are constantly changing, security baselines must also be dynamic and react to the changes.

They are not static or unchangeable due to changes in the environment.

They are not a suggestion. If implemented correctly, they provide the rules for how to configure devices.

Question 4: ✔ Correct

By definition, what is the process of reducing security exposure and tightening security controls?

- ➡ Hardening
- Active scanning
- Passive reconnaissance
- Social engineering

EXPLANATION

Hardening is the process of securing devices and software by reducing security exposure and tightening security controls.

Social engineering is the act of exploiting human nature by convincing someone to reveal information or perform an activity. Active scanning and passive reconnaissance are types of reconnaissance attacks.

Question 5: ✔ Correct

Which of the following is the strongest form of multi-factor authentication?

- Two-factor authentication
- Two passwords
- A password and a biometric scan
- ➡ A password, a biometric scan, and a token device

EXPLANATION

A password, a biometric scan, and a token device together are the strongest form of multi-factor authentication listed here. Multi-factor authentication is any combination of two or more of the same or different authentication factors. The three common authentication factor types are something you know (such as a password), something you have (such as a smart card or a token device), and something you are (such as a biometric quality, like a fingerprint).

The other three options are all weaker forms of multi-factor authentication. A password and a biometric scan is a multi-factor authentication system, but this is also an example of two-factor authentication. Two-factor authentication is any combination of two or more different authentication factors. Two passwords is an example of multi-factor authentication, but since it uses two of the same type of factors, it is not a true two-factor authentication method.

Question 6: ✕ Incorrect

You have recently experienced a security incident with one of your servers. After some research, you determine that a new hotfix has recently been released, which would have protected the server.

Which of the following recommendations should you follow when applying the hotfix?

- Test the hotfix and then apply it to the server that had the problem.
- ~~Apply the hotfix immediately to all servers.~~
- Apply the hotfix immediately to the server. Apply the hotfix to other devices only as the security threat manifests itself.
- ➡ Test the hotfix and then apply it to all servers.

EXPLANATION

In this scenario, you should test the hotfix and only apply it to all other servers if the test is successful. Applying it only to the server that was compromised does not protect other servers with the same vulnerability. A common testing strategy is to:

1. Apply and test patches in a lab environment
2. Deploy patches to a set of systems, such as a single department
3. Deploy patches system-wide

Question 7: ✔ Correct

Which of the following actions should you take to reduce the attack surface of a server?

- Install anti-malware software.
- Install a host-based IDS.
- Install the latest patches and hotfixes.
- ➡ Disable unused services.

EXPLANATION

Attack surface reduction (ASR) cuts down on the software or services running on a system. By removing unnecessary software, features, or services, you eliminate possible attacks directed at those components. When removing unnecessary components, you should:

- Use role separation by installing services on separate physical systems. If a single system is compromised, only the few services on that system are affected.
- For many new systems, unnecessary services are often installed by default. Following installation, remove unneeded services, protocols, and applications.
- When removing existing services, determine the unneeded services and their dependencies before altering the system.

Adding anti-malware or a host-based intrusion detection system (IDS) adds a level of protection (defense in depth) but does not reduce the number of components running on the system. Applying patches is necessary to fix security problems with software or the operating system. But if the system is not running a specific piece of software, the patches that apply to that software are irrelevant and do not need to be applied.

Question 8: ✔ Correct

Which of the following do security templates allow you to do? (Select two.)

- [ ] Block malicious websites
- [x] Quickly apply settings to multiple computers
- [ ] Apply new software patches
- [x] Configure consistent security settings between devices
- [ ] Fix a specific software problem

EXPLANATION

Security templates allow you to quickly and consistently apply settings to multiple computers in order to bring them into compliance with a security baseline.

Security templates are not used to apply new patches, block malicious websites, or fix specific software problems.

Question 9: ✔ Correct

You have just purchased a new network device and are getting ready to connect it to your network. Which of the following actions should you take to increase its security? (Select two.)

- [x] Apply all patches and updates.
- [ ] Remove any backdoors.
- [x] Change default account passwords.
- [ ] Implement separation of duties.
- [ ] Conduct privilege escalation.

EXPLANATION

To secure new devices, apply all recent patches and updates and then change the default user account passwords. For some systems, you can also increase security by changing the default account usernames. Default account usernames and passwords are well known and can be easily discovered.

A backdoor is an unprotected access method or pathway. Backdoors are added by attackers or programmers during development. Backdoors that are present on new devices are typically hard-coded and must be removed by editing the code.

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. Separation of duties is the concept of requiring the participation of at least two people to complete a task. This helps prevent insider attacks because no one person has end-to-end control and no one person is irreplaceable.

Question 10: ✔ Correct

Which of the following is defined as an operating system that comes hardened and validated to a specific security level as defined in the Common Criteria for Information Technology Security Evaluation (CC)?

- UNIX
- Windows
- TOS
- OS X

EXPLANATION

A trusted operating system (TOS) is one that has been hardened and validated to a specific level as defined by the Common Criteria.

Windows, UNIX, and OS X are not TOSs by default.