Exam Report: 7.3.9 Practice Questions

Date: 1/22/2020 2:04:01 pm
Time Spent: 15:15

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 50%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

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

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

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:

- Use role separation by installing services on separate physical systems. If a single system is compromised, only the few services on that system will be 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 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.

References

LabSim for Security Pro, Section 7.3.
[All Questions SecPro2017_v6.exm WINDOWS_SYS_HARDEN_01]

Question 2: Incorrect

Which of the following describes a configuration *baseline*?

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

Explanation

A *configuration baseline* is a set of consistent requirements for a workstation or server. A *security baseline* is a component of the configuration baseline 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.

References

LabSim for Security Pro, Section 7.3.
[All Questions SecPro2017_v6.exm WINDOWS_SYS_HARDEN_02]

Question 3: Incorrect

You have recently experienced a security incident with one of your servers. After some research, you determine that the hotfix #568994 that has recently been released would have protected the server.

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

- 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.
- ~~Apply the hotfix immediately to all servers.~~
- Test the hotfix and then apply it to the server that had the problem.

Explanation

In this scenario, you should test the hotfix, and apply it to all other servers only if the test is successful. Applying it only to the server that was compromised will 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

References

LabSim for Security Pro, Section 7.3.
[All Questions SecPro2017_v6.exm WINDOWS_SYS_HARDEN_03]

Question 4: 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.)

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

Explanation

To secure new devices, apply all recent patches and updates and change the default user account passwords. For some systems, you can also increase security by changing the default account user names. Default account names 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 having 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.

References

LabSim for Security Pro, Section 7.3.
[All Questions SecPro2017_v6.exm WINDOWS_SYS_HARDEN_04]

Question 5: Correct

Which of the following terms describes a Windows operating system patch that corrects a specific problem and is released on a short-term, periodic basis (typically monthly)?

- (selected) Hotfix
- Kernel fix kit
- Service pack
- Targeted software patch

Explanation

A *hotfix* is an operating system patch that corrects a specific known problem. Microsoft typically releases hotfixes monthly.

Service packs include a collection of hotfixes and other system updates. Service packs are not released as often, but contain all hotfixes released up to that time.

References

LabSim for Security Pro, Section 7.3.
[All Questions SecPro2017_v6.exm WINDOWS_SYS_HARDEN_05]

Question 6: Incorrect

Which of the following is the best recommendation for applying hotfixes to your servers?

- Apply hotfixes immediately as they are released
- (selected) Apply only the hotfixes that affect to software running on your systems
- (selected) ~~Apply all hotfixes before applying the corresponding service pack~~
- Wait until a hotfix becomes a patch, then apply it

Explanation

Be sure to test patches before applying them within your organization. A common 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

You do not necessarily need to install every hotfix, patch, or service pack that is released. For example, if a hotfix applies to a service that you have disabled on your servers, applying that hotfix is not required. Service packs typically include all hotfixes and patches that have been released up to that point in time.

References

LabSim for Security Pro, Section 7.3.
[All Questions SecPro2017_v6.exm WINDOWS_SYS_HARDEN_06]

Question 7: Correct

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

- Passive reconnaissance
- (selected) Hardening
-

Active scanning

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.

References

LabSim for Security Pro, Section 7.3.
[All Questions SecPro2017_v6.exm WINDOWS_SYS_HARDEN_07]

Question 8: Incorrect

When securing a newly deployed server, which of the following rules of thumb should be followed?

Disable all services not associated with supporting shared network services

Disable each service in turn and then test the system for negative effects

Determine unneeded services and their dependencies before altering the system

~~Disable all unused services~~

Explanation

The best rule of thumb when securing a system is to determine the unneeded services and their dependencies before altering the system. If you don't perform the research before altering the system, you may inadvertently disable an essential service or fail to disable a service with significant vulnerabilities.

Altering a system without researching, performing a change and test method, or even blindly disabling all services of a specific type are not reliable means to improve security on a system.

References

LabSim for Security Pro, Section 7.3.
[All Questions SecPro2017_v6.exm WINDOWS_SYS_HARDEN_08]

Question 9: Incorrect

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.)

WSUS

Security Configuration and Analysis

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.

References

LabSim for Security Pro, Section 7.3.
[All Questions SecPro2017_v6.exm WINDOWS_SYS_HARDEN_09]

Question 10: Correct

You have contracted with a vendor to supply a custom application that runs on Windows workstations. As new application versions and patches are released, you want to be able to automatically apply them to multiple computers.

Which tool is your best choice for accomplishing this task?

- WSUS
- Group Policy
- Security Configuration and Analysis
- Security Templates

Explanation

Use Group Policy to distribute and install software updates. You must use Group Policy to install updates to non-Microsoft software that is not supported with Windows Software Update Services (WSUS).

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 within 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.

References

LabSim for Security Pro, Section 7.3.
[All Questions SecPro2017_v6.exm WINDOWS_SYS_HARDEN_10]