

Exam Report: 7.7.4 Practice Questions

Date: 1/22/2020 6:57:57 pm
Time Spent: 3:24

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1:

Incorrect

You manage the information systems for a large manufacturing firm.

Supervisory control and data acquisition (SCADA) devices are used on the manufacturing floor to manage your organization's automated factory equipment. The SCADA devices use embedded smart technology, allowing them to be managed using a mobile device app over an internet connection.

You are concerned about the security of these devices. What can you do to increase their security posture? (Select two.)

- ☒ Verify that your network's existing security infrastructure is working properly.
- ☐ Install a network monitoring agent on each device.
- ☐ Install anti-malware software on each device.
- ☒ Install the latest firmware updates from the device manufacturer.
- ☐ Enroll each device in a mobile device management system.

Explanation

Since you generally have little or no control over the smart technology embedded within SCADA devices, they are referred to as *static environments*. As a result, there is, typically, very little you can do to increase the security posture for these types of devices. For SCADA devices, you may be able to perform the following, depending on the the device manufacturer:

- Install the latest firmware updates from the device manufacturer
- Verify that your network's existing security infrastructure is working properly

Because these devices operate in a static environment, you typically can't install third-party software on them, including anti-malware scanners, monitoring agents, or mobile device management (MDM) agents.

References

LabSim for Security Pro, Section 7.7.
[All Questions SecPro2017_v6.exm EMBED_SYSTEMS_01]

▼ Question 2:

Correct

You manage information systems for a large co-location data center.

Networked environmental controls are used to manage the temperature within the data center. These controls use embedded smart technology that allows them to be managed over an internet connection using a mobile device app.

You are concerned about the security of these devices. What can you do to increase their security posture? (Select two.)

- ☐ Enroll each device in a mobile device management system.

- ➡ ☒ Verify that your network's existing security infrastructure is working properly.
- ☐ Install anti-malware software on each device.
- ☐ Rely on the device manufacturer to maintain device security with automated firmware updates.
- ➡ ☒ Install the latest firmware updates from the device manufacturer.

Explanation

Since you generally have little or no control over the embedded technology within smart environmental control devices, they are referred to as *static environments*. As a result, there is typically very little you can do to increase the security posture for these types of devices. For environmental controls, you may be able to perform the following, depending upon the device manufacturer:

- Install the latest firmware updates from the device manufacturer
- Verify that your network's existing security infrastructure is working properly

Because these devices operate in a static environment, you typically can't install third-party software on them, including anti-malware scanners or mobile device management (MDM) agents. Relying upon the device manufacturer for security updates is problematic because manufacturers can be slow to take steps to protect their products against security threats. Manufacturers tend to only respond after an exploit has occurred, instead of proactively defending their systems.

References

LabSim for Security Pro, Section 7.7.

[All Questions SecPro2017_v6.exm EMBED_SYSTEMS_02]

▼ Question 3: Incorrect

Why do attackers prefer to conduct distributed network attacks in static environments? (Select two.)

- ➡ ☒ Devices tend to employ much weaker security than traditional network devices.
- ☐ Smart device vendors tend to proactively protect their products against security threats.
- ➡ ☐ Devices are, typically, more difficult to monitor than traditional network devices.
- ☐ It is difficult to update the virus definitions used to protect these devices.
- ☒ ~~These devices are typically installed in the DMZ outside an organization's perimeter firewall.~~

Explanation

Attackers prefer static environment devices to conduct distributed network attacks for the following reasons:

- Static devices tend to employ much weaker security and are easier to exploit than traditional targets, such as desktops, notebooks, tablets, and smartphones.
- Smart device vendors tend to reactively protect their products against security threats, responding only after an exploit has occurred, instead of proactively defending systems.
- Static devices are, typically, more difficult to monitor than traditional network devices.

Because these devices operate in a static environment, you typically can't install third-party software on them, including anti-malware scanners. Because of their relatively weak security, these devices should not be deployed in an unsecure area of a network, such as the DMZ.

References

LabSim for Security Pro, Section 7.7.


[All Questions SecPro2017_v6.exm EMBED_SYSTEMS_03]

▼ Question 4: Correct

You notice a growing number of devices, such as environmental control systems and wearable devices, are connecting to your network. These devices, known as smart devices, are sending and receiving data via

wireless network connections.

Which of the following labels applies to this growing ecosystem of smart devices?

- ☐ Internet of smart devices
- ☐ Dynamic environment
-  ☒ Internet of things
- ☐ The smartnet

Explanation

These smart devices are part of a growing ecosystem known as the internet of things (IoT).

Environments that contain these types of devices are known as static environments. A static environment is one that never changes (or changes very infrequently) and that a network administrator has very little control over. For example, a smart television in an office has embedded technology that might never be updated, which creates a security hole in the company's network.

References


LabSim for Security Pro, Section 7.7.

[All Questions SecPro2017_v6.exm EMBED_SYSTEMS_04]

▼ Question 5: Correct

Smart devices are attractive targets for cyber criminals because they typically have minimal security and are not protected with anti-malware software. This makes it easier to exploit these types of devices and perpetrate attacks. Many smart devices can be utilized to conduct a single coordinated attack.

What is this type of attack usually called?

-  ☒ A highly distributed attack
- ☐ A brute force attack
- ☐ A highly centralized attack
- ☐ A smartnet attack

Explanation

Using many smart devices to conduct a single coordinated attack is referred to as a highly distributed attack. Hundreds of thousands, or even millions, of smart devices from all over the world have been exploited to carry out a single attack.

References

LabSim for Security Pro, Section 7.7.

[All Questions SecPro2017_v6.exm EMBED_SYSTEMS_05]