Exam Report: 2.2.4 Practice Questions

Date: 1/9/2020 2:36:42 pm
Time Spent: 10:31

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following is the single greatest threat to network security?

- Insecure physical access to network resources
- Weak passwords
- Email phishing
- Employees

Explanation

Employees are the single greatest threat to network security. Therefore, user education is very important.

- Employees need to be aware that they are the primary targets in most attacks.
- Phishing attacks are one of the most common attacks directed toward employees.
- Employees should be able to identify attacks by email, instant messages, downloads, and websites.
- Effective password policies should be enforced, and passwords should not be written down.
- Employees should be able to identify both internal and external threats.
- Employees need to be aware of the company's security policies.

References

LabSim for Security Pro, Section 2.2.
[All Questions SecPro2017_v6.exm DEF_PLAN_02]

Question 2: Correct

Which of the following is a security approach that combines multiple security controls and defenses and is sometime called defense in depth?

- Layered security
- Cumulative security
- Network security
- Perimeter security
- Countermeasure security

Explanation

Layered security, sometimes called defense in depth security, is a security approach that combines multiple security controls and defenses to create a cumulative effect.

Perimeter security includes firewalls using ACLs and securing the wireless network. Network security includes the installation and configuration of switches and routers, implementation of VLANs,

penetration testing, and the utilization of virtualization. A countermeasure is a means of mitigating the potential risk. Countermeasures reduce the risk of a threat agent exploiting a vulnerability.

References

LabSim for Security Pro, Section 2.2.
[All Questions SecPro2017_v6.exm DEF_PLAN_01]

Question 3: Correct

Drag the security layer on the left to the appropriate description on the right. (Security layers may be used once, more than once, or not at all.)

Includes OS hardening, patch management, malware, and password attacks

✔ Host

Includes how to manage employee onboarding and off-boarding

✔ Policies, Procedures, and Awareness

Includes cryptography and secure transmissions

✔ Data

Includes user education and manageable network plans

✔ Policies, Procedures, and Awareness

Includes firewalls using ACLs and securing the wireless network

✔ Perimeter

Explanation

Layered Security includes the following layers:

- Policies, Procedures, and Awareness: Includes user education, manageable network plans, and how to manage employee onboarding and off-boarding.
- Perimeter: Includes firewalls using ACLs and securing the wireless network.
- Host: Includes log management, OS hardening, patch management and implementation, auditing, malware, and password attacks.
- Data: Includes storing data properly, destroying data, classifying data, cryptography, and securing data transmissions.

References

LabSim for Security Pro, Section 2.2.
[All Questions SecPro2017_v6.exm DEF_PLAN_03]

Question 4: Incorrect

Which of the following reduce the risk of a threat agent being able to exploit a vulnerability?

- ○ Implementation of VLANs
- ◉ ~~Manageable network plans~~
- ○ Secure data transmissions
- ➡ ○ Countermeasures

Explanation

A countermeasure is a means of mitigating potential risk. Countermeasures reduce the risk of a threat agent being able to exploit a vulnerability. An appropriate countermeasure:

- Must provide a security solution to an identified problem
- Should not depend on secrecy
- Must be testable and verifiable
- Must provide uniform or consistent protection for all assets and users

- Should be independent of other safeguards
- Should require minimal human intervention
- Should be tamper-proof
- Should have overrides and fail-safe defaults

References

LabSim for Security Pro, Section 2.2.
[All Questions SecPro2017_v6.exm DEF_PLAN_05]

Question 5: Incorrect

Drag the security layer on the left to the appropriate description on the right. (Security layers may be used once, more than once, or not at all.)

Includes fences, door locks, mantraps, turnstiles, device locks, and server cages.

✓ Physical

Includes each individual workstation, laptop, and mobile device.

~~Network~~ Host

Includes authentication and authorization, user management, and group policies.

✓ Application

Includes cameras, motion detectors, and even environmental controls.

✓ Physical

Includes implementation of VLANs, penetration testing, and the utilization of virtualization.

~~Host~~ Network

Explanation

Layered Security includes the following layers:

- Physical: Includes fences, door locks, mantraps, turnstiles, device locks, server cages, cameras, motion detectors, and environmental controls.
- Network: Includes the installation and configuration of switches and routers, implementation of VLANs, penetration testing, and the utilization of virtualization.
- Host: Includes each individual workstation, laptop, and mobile device.
- Application: Includes authentication and authorization, user management, group policies, and web application security.

References

LabSim for Security Pro, Section 2.2.
[All Questions SecPro2017_v6.exm DEF_PLAN_04]