1/9/2020 TestOut LabSim

1912020 IESTOUL LADSITI	
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: <u>Correct</u>	
Which of the following is the single greatest threat to r	network security?
 Insecure physical access to network resource 	es s
Weak passwords	
Email phishing	
→ ○ Employees	
Explanation	
Employees are the single greatest threat to network section important. • Employees need to be aware that they are the printer in the printer	nary targets in most attacks. cks directed toward employees. mail, instant messages, downloads, and websites. nd passwords should not be written down. l and external threats.
References	
LabSim for Security Pro, Section 2.2. [All Questions SecPro2017_v6.exm DEF_PLAN_02]	
▼ Question 2: <u>Correct</u>	
Which of the following is a security approach that consometime called defense in depth?	abines multiple security controls and defenses and is
→	
Cumulative security	
Network security	

Explanation

Perimeter security

Countermeasure security

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,

1/9/2020 TestOut LabSim

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

LabSim for Security Pro, Section 2.2.

[All Questions SecPro2017_v6.exm DEF_PLAN_01]

▼ Question 3:

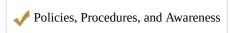
Correct

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



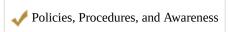
Includes how to manage employee onboarding and off-boarding



Includes cryptography and secure transmissions



Includes user education and manageable network plans



Includes firewalls using ACLs and securing the wireless network



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



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

1/9/2020 TestOut LabSim

- Should beginde praintiental of norther indergreation
- 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.



Includes each individual workstation, laptop, and mobile device.



Host

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



Includes cameras, motion detectors, and even environmental controls.



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



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

 $Lab Sim\ for\ Security\ Pro,\ Section\ 2.2.$

[All Questions SecPro2017_v6.exm DEF_PLAN_04]