

Each question is worth 3 points. Brief means brief, but not incomplete. Show your work on the back of test pages or additional sheets if necessary.

1. You work as an information security engineer for AdvanceCo. The CEO wants to announce his plan to deploy a public key infrastructure throughout the company's hundreds of locations to totally replace the use of symmetric cryptography. You must assist the Chief InfoSec Officer in preparing a brief to the CEO. List below 3 key points you believe should be included in the brief.
2. $x = \text{GCD}(18, 27), x = ?$
3. $15 \bmod x \equiv 20 \bmod x, x = ?$
4. Briefly describe 3 difficulties associated with symmetric key cryptosystems.
5. Name 3 procedural controls that have applicability in mitigating vulnerabilities in different realms of computer security.
6. Distinguish between threats, vulnerabilities, and controls as they relate to computer systems.
7. Briefly describe 3 vulnerabilities inherent in the GMU computer environment.
8. Define:
 - a. Virus
 - b. Trojan Horse
 - c. Trapdoor
 - d. Worm
 - e. Rootkit

9. Mr. Rich, the CEO of AdvanceCo, wants to ensure that construction plans for the new employee lounge are not released until his big announcement, and wants to protect them with the most sophisticated security system availability. What should the CISO advise in this case?

10. AdvanceCo information systems are protected by strong passwords, antivirus software, firewalls, and intrusion detection systems. What term describes this set of controls?

11. Define “protocol”. What are 3 characteristics of a successful protocol?

12. Briefly describe 3 possible attacks against a password system.

13. Describe 3 mitigating controls against password attacks.

14. What basic question didn't I ask?