CPRE 431

M03 HW

Assignments will be submitted in PDF format via Canvas.

Please submit your homework online through Canvas. Late homework will not be accepted.
Important: Your submission must be in .pdf format ONLY!
Please ensure that you support all your answers with the correct screenshots showing your solutions.

1. Briefly state the differences between DAC and MAC access control mechanisms.

2. The inclusion of the salt in the UNIX password scheme increases the difficulty of guessing by a factor of 4096. But the salt is stored in plaintext in the same entry as the corresponding ciphertext password. Therefore, salt is known to the attacker. Based on that, why is it asserted that the salt increases security?

3. In the traditional UNIX file access model, UNIX systems provide a default setting for newly created files and directories, which the owner may later change. The default is typically full access for the owner combined with one of the following: no access for group and other, read/execute access for group and none for other, or read/execute access for both group and other. Briefly discuss the advantages and disadvantages of each of these cases, including an example of a type of organization where each would be appropriate.

4. Provide short answers to the following questions:
    a. Why should system administrators remove unnecessary services, applications, and protocols?
    b. Where is application and service configuration information stored on Unix and Linux systems?
    c. How does “chroot jail” used to improve application security? And what are its limitations?

5. Logging is a very important control for operating system and network security, explain the following:
    a. Why is logging important?
    b. What are its limitations as a security control?
    c. What are the pros and cons of remote logging?

Why is it important to rotate log files (overwrite old log files)?

6. Consider an automated audit log analysis tool (e.g., swatch). Can you propose some generic rules which could be used to distinguish “suspicious activities” from normal user behavior on a system for some organization, for the following activities:
    a. User Authentication
    b. Website Access