Homework Assignment 7: Identity and Access Management

1. Describe three types of authentication credentials and provide an example of each.

2. What makes passwords weak, and why are they commonly targeted by attackers?

3. Explain the differences between brute force attacks, dictionary attacks, and credential stuffing.

4. What is a rule attack, and how does it statistically increase the chances of password cracking?

5. How do security keys and smart cards improve authentication security?

6. Compare physiological and behavioral biometrics. Provide one example of each.

7. What are two disadvantages of biometric authentication systems?

8. Explain the difference between salting and peppering in securing password digests.

9. Name and describe two key stretching algorithms used to secure password hashes.

10. What is the purpose of password vaulting and user password managers?

11. Describe two best practices for password management in an organization.

12. What is single sign-on (SSO), and how does SAML support it?

13. Explain the difference between OAuth and OpenID in identity management.

14. What are passkeys and how do they improve upon traditional password-based authentication?

15. Compare DAC, MAC, RBAC, and ABAC access control models.