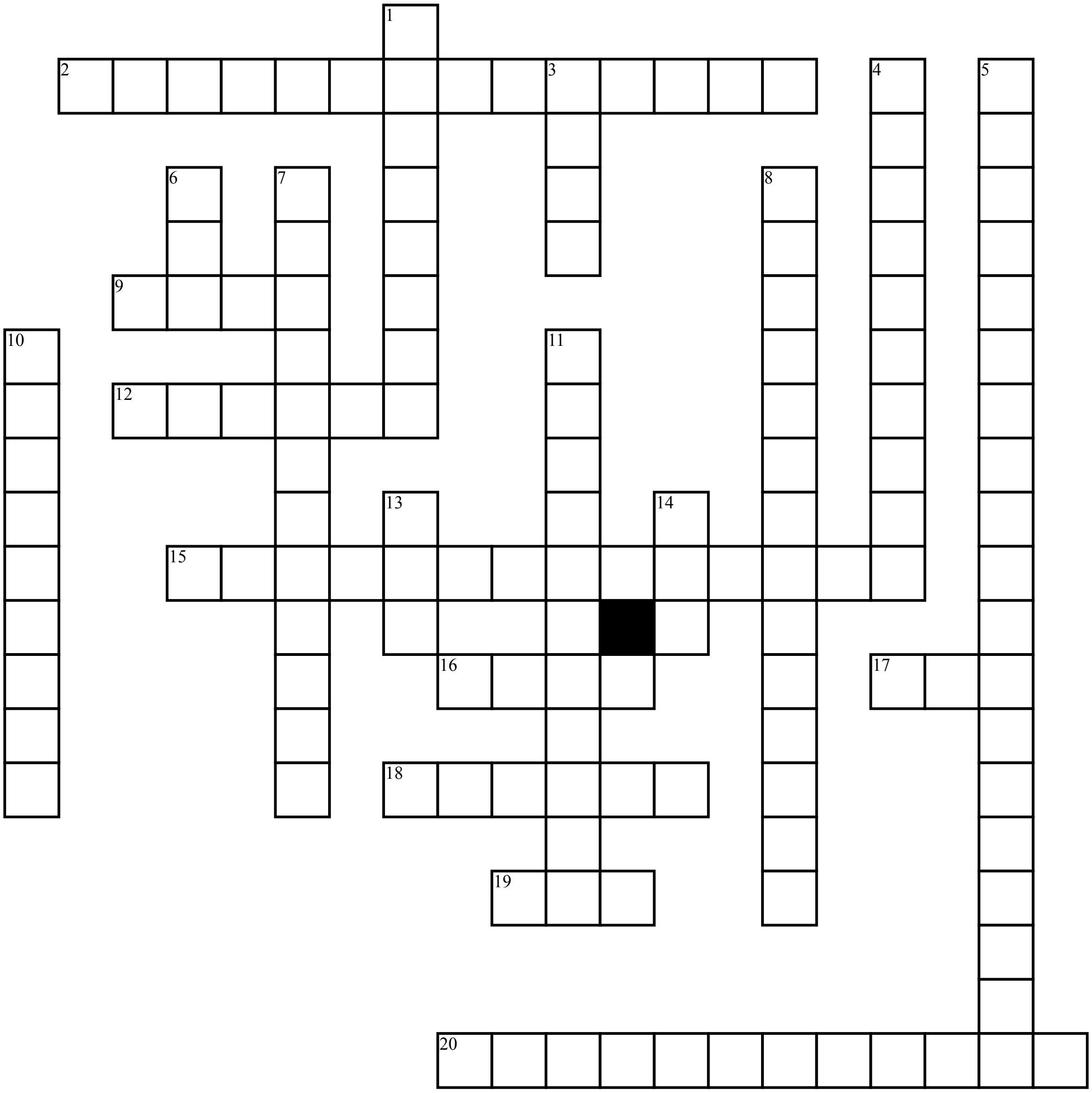
Name: ______________________________________ Date: _______ Period: _______

Access Control and Identity Management



Across

2. individual gains a higher level of access than they normally need usually caused by temporary or accidental access

9. algorithm uses a time-based fact to create unique passwords

12. authenticates remote users, authorizes their access, and enables remote access servers to communicate with a central server

15. prove that a user or system is actually who they say they are

16. standardized directory access protocol allowing queries to be made of directories

17. access policy that restricts subjects' access to objects based on security clearance of the subject and the classification of the object

18. token that gives user a complex password that is used to log onto the system

19. type 1 error

20. by not specifically allowing access, you have denied access

Down

1. authentication protocol that uses port 88

3. challenge/response method of authentication

4. collection of computer networks that agree on standards of operation, such as security standards

5. act of exploiting a bug or design flaw in a software application to gain access (hint: two types - vertical or horizontal)

6. provide access to all authorized resources with a single instance of authentication

7. specifically deny a subject (person, IP address, etc.) access to an object (file, server, etc.)

8. give users only the permissions they need to do their work and no more

10. allow users to authenticate with an alternate factor who have forgotten their password

11. verification using at least two different of the three factors of authentication

13. point at which the FRR equals the FAR

14. type 2 error