D2_4_14 Password Attacks

Amanda Success (Period 9) (replace with your information)
Monday December 25, 2023
Seat 99 (Grade level 13)
Cyber Capstone

1. What is the main purpose of a password attack?
A. To encrypt passwords
B. To authenticate users on a system
C. To gain a victim's password
D. To enhance password security
___ <- Type answer here

2. Why should plaintext passwords never be sent or stored?
A. They are more secure than encrypted passwords
B. They can be intercepted or compromised easily
C. They are required for secure authentication
D. They are less prone to brute force attacks
___ <- Type answer here

3. What is a Brute Force attack?
A. An attack that uses commonly used words or passwords from a list
B. An attack that tries all possible combinations until the right guess works
C. An attack that tries a few passwords at a time to get lucky
D. An attack that attempts to crack passwords using precalculated series of hashes
___ <- Type answer here

4. How does a Dictionary attack differ from a Brute Force attack?
A. Dictionary attacks are slower and more exhaustive
B. Dictionary attacks attempt to crack passwords using precalculated hashes
C. Dictionary attacks try all possible combinations until the right guess works
D. Dictionary attacks use commonly used words or passwords from a list
___ <- Type answer here

5. What is spraying in the context of password attacks?
A. Trying a few passwords at a time to get lucky
B. Using commonly used words or passwords from a list
C. Trying all possible combinations until the right guess works
D. Attempting to crack passwords using precalculated series of hashes
___ <- Type answer here

6. How do Rainbow Tables aid in password cracking?
A. They generate random passwords for dictionary attacks
B. They use brute force to crack passwords
C. They precalculate a series of hashes using known algorithms
D. They encrypt passwords for secure storage

___ <- Type answer here

7. What defense measure can be used to combat rainbow table attacks?
A. Using a salt with passwords
B. Increasing the time required between password attempts
C. Implementing password lockout policies
D. Enforcing strong password complexity requirements

___ <- Type answer here