Cybersecurity Guided Notes (ANSWER KEY)

Lesson 1.2.16 - Cryptographic Attacks

1. What is the purpose of a cryptographic attack?

A malicious actor is attempting to break an encryption algorithm

2. What is a birthday attack?

A birthday attack is attempting to find collisions with hashes since there are only a limited number of possible hashes

3. What is a collision, and why are they dangerous?

A collision is when two hashes are the same even though the original files/strings do not match, thus potentially allowing access to something without the proper password

4. What is a downgrade attack?

A downgrade attack is when a malicious actor is able to attack a system by using an older version of the software

5. How can a person defend themselves against cryptographic attacks?

Answers will vary, example answers include:

- Upgrade your system and always make sure to update older software
- Use longer hashing algorithms to help avoid collisions