Exercise walk-through

Authentication ▪ 4.2

eXercise

You must be able to

- state the properties of a cryptographic hash (one-way, fixed length, repeatable)
- explain how salt protects stored passwords
- classify authentication factors (know / have / are / where) and password attacks

Method — Hashing and salt

A service stores the hash of a password, never the plaintext. Salt (random bits) is added before hashing so two identical passwords produce different stored hashes.

Method — Password attacks

Password spraying = one common password against many accounts. Credential stuffing = stolen or default credentials. A rainbow table = a precomputed table of passwords and their hashes.

Practice 2.1 ▪ 2 marks

State two properties of a cryptographic hash function.

Solution 2.1

Worked steps

any two of: one-way/cannot reverse B1; fixed-length output; repeatable/same input same output B1.

Practice 2.2 ▪ 2 marks

Explain how **salt** protects stored passwords.

Solution 2.2

Method: Hashing and salt

Worked steps

salt adds unique random bits before hashing B1, so two identical passwords have different stored hashes B1.

Practice 2.3 ▪ 1 mark

Classify each authentication factor as know / have / are / where.
(a) A fingerprint
(b) A code sent to your phone
(c) A PIN

Solution 2.3

Worked steps

(a) are / biometric B1. (b) have B1. (c) know B1.

Exam-style 3.1 ▪ 1 mark

A cryptographic hash output is

A variable length

B a fixed length regardless of input

C the original password

D always longer than the input

Solution 3.1

A variable length

B a fixed length regardless of input ✓

C the original password

D always longer than the input

Worked steps

B. a hash is fixed length and one-way.

Exam-style 3.2 ▪ 1 mark

Trying one common password against many accounts is

A credential stuffing

B password spraying

C salting

D a rainbow table

Solution 3.2

Method: Password attacks

A credential stuffing

B password spraying ✓

C salting

D a rainbow table

Worked steps

B. one password, many users = password spraying.

Exam-style 3.3 ▪ 1 mark

A company enables multifactor authentication (MFA).
(a) State what MFA requires.
(b) Explain why it is stronger than a password alone.

Solution 3.3

Worked steps

(a) two or more different authentication factors B1. (b) an adversary must defeat two factors B1, so a stolen password alone cannot log in B1.