1.2 Suspicious Website Logins

Name: _____ Class: _____ Date: _____ **Total: 15 marks**

KEY WORDS authentication • password attack • mfa • password manager • dictionary

Objective

Build the skills to answer exam questions on **password attacks** and stronger **authentication** .

You must be able to:

- identify signs of an online password attack in a log
- explain why weak, patterned passwords fail
- recommend stronger authentication: long unique passwords and **MFA**

1 Key knowledge and worked examples

Study these first. Each one shows the method for a task used later.

■ Signs in the log

Possible signs of an online password attack include many failed logins in a short time, logins at unusual hours, or logins from unknown devices.

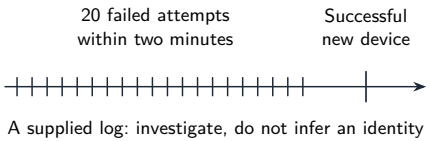
■ Making authentication stronger

Use long, random, unique passwords (a password manager helps), avoid names and dates, and enable multifactor authentication so a stolen password alone is not enough.

■ Worked application: A log pattern supports a hypothesis rather than proving it

A supplied fictional log contains 20 failed password attempts for one account in two minutes, followed by a successful login from an unfamiliar device. That pattern justifies investigation, but it does not prove who acted: typing mistakes, a shared network or a legitimate new device may also explain parts of it. Compare device and time records, confirm with the account owner through an established channel and preserve the log. A long unique password reduces reuse risk; a second independent authentication factor reduces the chance that possession of a password alone is sufficient.

Neither control proves that a later login is legitimate.



2 Practice

2.1 State two signs, visible in a log, of an online password attack. [2]

2.2 Explain why a password like `Summer2024!` is weak. [2]

2.3 State two ways to make authentication stronger. [2]

3 Exam-style questions

3.1 Which log pattern most strongly suggests an online password attack? [1]

☐ **A** one successful login
B many failed logins in a short time
C a file download
D a printer coming online

3.2 Which is the strongest password? [1]

☐ **A** your dog's name
B P@ssword!
C a 16-character random string
D your birthday

3.3 A company wants to reduce account takeovers.

(a) Name one authentication improvement they could require. [1]

(b) Explain how it helps even if a password is stolen. [2]

3.4 A fictional account has 15 failed logins and then one successful login from a new device. Give one suspicious feature, one legitimate alternative explanation, one additional evidence check and one authentication improvement. [4]