Exercise walk-through

Protecting Networks: Managerial Controls and Wireless Security ▪ 3.2

eXercise

You must be able to

- give managerial controls: router, switch, VPN, and wireless security policies
- harden wireless: disable beacon frames, control signal, enable WPA3, MAC filtering
- explain why WEP and the original WPA are insecure

Method — Wireless hardening

Disable beacon frames so the network is harder to find, control signal strength so it does not leak outside, enable WPA3 (WEP and original WPA are broken), and use MAC filtering plus authentication.

Method — Choosing encryption

WPA3 is today's strongest wireless encryption. WEP and the original WPA have known, unfixable weaknesses and must not be used for a secure network.

Practice 2.1 ▪ 1 mark

State the strongest current wireless encryption protocol.

Solution 2.1

Method: Choosing encryption

Worked steps

WPA3 B1.

Practice 2.2 ▪ 2 marks

Give two ways to harden a wireless network.

Solution 2.2

Worked steps

any two of: enable WPA3 **B1**; disable beacon frames; control signal strength; MAC filtering **B1**.

Practice 2.3 ▪ 2 marks

Explain why controlling a WAP's signal strength improves security.

Solution 2.3

Method: Wireless hardening

Worked steps

it stops the signal leaking outside the building **B1**, so attackers outside cannot detect or probe it **B1**.

Exam-style 3.1 ▪ 1 mark

Which wireless encryption is insecure and should be avoided?

A WPA3

B WEP

C WPA3-Enterprise

D AES-256

Solution 3.1

Method: Choosing encryption

A WPA3

B WEP ✓

C WPA3-Enterprise

D AES-256

Worked steps

B. WEP is broken; WPA3 is the strong choice.

Exam-style 3.2 ▪ 1 mark

A VPN policy typically forbids

- **A** strong encryption
- **B** split tunneling
- **C** MAC filtering
- **D** authentication

Solution 3.2

A strong encryption

B split tunneling ✓

C MAC filtering

D authentication

Worked steps

B. split tunneling can bypass the corporate VPN protections.

Exam-style 3.3 ▪ 1 mark

A company writes a wireless security policy.
(a) State one requirement the policy should include.
(b) Explain how MAC filtering helps.

Solution 3.3

Method: Wireless hardening

Worked steps

(a) e.g. require WPA3 / require authentication **B1**. (b) MAC filtering allows only known hardware addresses **B1**, so unknown devices cannot join the network **B1**.