Exercise walk-through

Protecting Devices ▪ 4.3

eXercise

You must be able to

- give managerial controls: acceptable use, password, software installation policies
- explain how anti-malware and patching protect a device
- describe what a host-based firewall does

Method — Patching

When a vendor releases a patch, they reveal the hole it fixes - so adversaries target anyone who has not updated. Prompt patching closes known holes before they are exploited.

Method — Host-based firewall

A host-based firewall controls traffic in and out of one single device, blocking ports and services it does not need - adding a layer even on a compromised network.

Practice 2.1 ▪ 2 marks

Explain why keeping software updated makes a device safer.

Solution 2.1

Worked steps

a patch closes a known vulnerability B1 before an adversary can exploit it B1.

Practice 2.2 ▪ 1 mark

State what a **host-based firewall** protects.

Solution 2.2

Method: Host-based firewall

Worked steps

traffic in and out of one single device B1.

Practice 2.3 ▪ 2 marks

How does anti-malware software detect malicious files?

Solution 2.3

Worked steps

it keeps a database of malware signatures B1 and quarantines files that match a signature B1.

Exam-style 3.1 ▪ 1 mark

A firewall that controls traffic for just one device is a

A network firewall

B host-based firewall

C stateless proxy

D VPN

Solution 3.1

Method: Host-based firewall

A network firewall

B host-based firewall ✓

C stateless proxy

D VPN

Worked steps

B. a host-based firewall guards a single device.

Exam-style 3.2 ▪ 1 mark

The policy listing what users may and may not do on company devices is the

A password policy

B acceptable use policy

C wireless policy

D router policy

Solution 3.2

A password policy

B acceptable use policy ✓

C wireless policy

D router policy

Worked steps

B. the acceptable use policy sets device usage rules.

Exam-style 3.3 ▪ 2 marks

A host-based firewall on a laptop blocks outbound FTP.
(a) Explain how this could stop data theft.

Solution 3.3

Method: Host-based firewall

Worked steps

(a) if malware infects the laptop and tries to exfiltrate files over FTP B1, the host firewall blocks the outbound connection even though the network allowed FTP B1.