AP CYBERSECURITY • EXERCISE SHEET

4.3 Protecting Devices

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

KEY WORDS acceptable use policy 可接受使用政策 • host-based firewall 主机防火墙 • anti-malware software 反恶意
• patch 补丁 • malware 恶意软件

Objective

Build the skills to answer exam questions on protecting a device with policies, anti-malware, patching, and a **host-based firewall** 主机防火墙.

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

1 Worked examples

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

■ 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.

■ 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.

2 Practice

2.1 Explain why keeping software updated makes a device safer. [2]

2.2 State what a **host-based firewall** protects. [1]

2.3 How does anti-malware software detect malicious files? [2]

3 Exam-style questions

3.1 A firewall that controls traffic for just one device is a [1]

- **A** network firewall
- **B** host-based firewall
- **C** stateless proxy
- **D** VPN

3.2 The policy listing what users may and may not do on company devices is the [1]

- **A** password policy
- **B** acceptable use policy
- **C** wireless policy
- **D** router policy

3.3 A host-based firewall on a laptop blocks outbound FTP.

(a) Explain how this could stop data theft. [2]

Solutions

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

2.2 traffic in and out of one single device.

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

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

3.2 B. the acceptable use policy sets device usage rules.

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