4 Protecting and monitoring devices – Part 2

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	中文	Write it 3 times (English)		
Anti-malware software	反恶意软件			
patching	打补丁			
host-based firewall	主机防火墙			
password spraying	密码喷洒			
credential stuffing	撞库			

Recall

- You get reminders to update your phone or laptop.
- You may have antivirus software installed.
- You know a log records what happened, like a diary.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

■ 1 Protecting devices

Anti-malware software 反恶意软件 quarantines files matching known signatures. Prompt **patching** 打补丁 closes known holes. A **host-based firewall** 主机防火墙 guards one device by blocking unneeded ports.

Worked example. A host firewall blocks outbound FTP, stopping malware from sending files out.

■ 2 Reading authentication logs

Many wrong passwords for one user = guessing. Many users failing from **one IP** = **password spraying** 密码喷洒. Default credentials in bursts = **credential stuffing** 撞库.

Worked example. 50 failed logins for 'admin' from one IP in 30 seconds is an online guessing attack.

■ 3 What cannot be detected

Offline password attacks cannot be detected, because the attacker cracks the stolen hash on their own computer, away from your logs.

Worked example. Once a hash database is stolen, cracking it happens off-site and leaves no trace on you.

Watch out: Offline password attacks leave no trace on your systems - the only defence is strong, salted hashing in the first place.

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 Many users failing to log in from one IP address suggests which attack? [1]

2.4 Explain why offline password attacks cannot be detected. [2]

2.5 How does anti-malware software detect a malicious file? [2]