3 Wireless security and detecting attacks – 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)		
WPA3	无线加密协议			
MAC filtering	地址过滤			
NIDS	网络入侵检测系统			
NIPS	网络入侵防御系统			
SIEM	安全信息与事件管理			
Signature-based	基于特征			
Anomaly-based	基于异常			
baseline	基线			

Recall

- You choose a Wi-Fi network by its name and enter a password.
- You know some networks are open and some are locked.
- You understand that alarms should only go off when something is really wrong.

New ideas

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

1 Wireless security

Use **WPA3** 无线加密协议 encryption - old **WEP** and the original **WPA** are broken. Disable beacon frames, control the signal so it does not leak outside, and use **MAC filtering** 地址过滤.

Worked example. A café controls its signal strength so the Wi-Fi stops at the walls, not the car park.

2 Detection systems

A **NIDS** 网络入侵检测系统 detects and alerts; a **NIPS** 网络入侵防御系统 can also block; a **SIEM** 安全信息与事件管理 correlates data from many sources.

Worked example. A NIDS raises an alert but waits for a human; a NIPS closes the port itself.

3 Detection methods

Signature-based 基于特征 detection matches known attacks - fast, few false alarms, but misses new ones. **Anomaly-based** 基于异常 compares to a normal **baseline** 基线 - catches new attacks but costs more.

Worked example. A brand-new worm slips past signature detection but trips the anomaly detector.

Watch out: The one-letter difference matters: an IDS only alerts, an IPS can block. Read which the question means.

Practice

2.1 State the strongest current wireless encryption protocol. [1]

2.2 Explain why controlling a Wi-Fi signal's strength improves security. [2]

2.3 State the difference between a NIDS and a NIPS. [2]

2.4 Which detection method is more likely to catch a brand-new attack? [1]

2.5 Give one advantage and one disadvantage of signature-based detection. [2]