AP CYBERSECURITY • EXERCISE SHEET

3.5 Detecting Network Attacks

Name: _____ Class: _____ Date: _____ **Total: 11 marks**

Objective

Build the skills to answer exam questions on network detection systems and **signature-based** 基于特征 vs **anomaly-based** 基于异常 detection.

You must be able to:

- distinguish a NIDS (alerts) from a NIPS (blocks) and a SIEM
- compare signature-based and anomaly-based detection
- state the trade-offs (speed, cost, false alarms, novel attacks)

1 Worked examples

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

■ IDS vs IPS

An intrusion detection system (NIDS) only alerts - a human must act. An intrusion prevention system (NIPS) can also block the attack itself. A SIEM correlates data from many sources to spot patterns.

■ Signature vs anomaly

Signature-based matches known attack signatures - fast, few false alarms, but blind to new attacks. Anomaly-based compares to a normal baseline - catches novel attacks but costs more and raises more false alarms.

2 Practice

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

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

2.3 Why does anomaly-based detection need a recorded baseline? [2]

3 Exam-style questions

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

- **A** signature-based
- **B** anomaly-based
- **C** no detection
- **D** a firewall log

3.2 Which system detects an attack and alerts staff but does NOT block it? [1]

- **A** NIPS
- **B** NIDS
- **C** VPN
- **D** UPS

3.3 A manufacturing plant deploys a signature-based network detection system.

(a) State one potential drawback compared with anomaly-based detection. [1]

(b) Explain why this drawback occurs. [2]

4 Go further

- work through the **3.5 Detecting Network Attacks** lesson on the **Learn** page;
- read the **Securing Networks** section of the AP Cybersecurity handout on the **Know** page.

Solutions

2.1 a NIDS detects and alerts only; a NIPS can also block/stop the attack.

2.2 advantage: fast, few false positives; disadvantage: cannot catch brand-new attacks.

2.3 it flags traffic that deviates from normal, so it must first know what normal looks like.

3.1 B. anomaly-based flags the unusual; signatures miss the new.

3.2 B. a NIDS alerts only; a NIPS can block.

3.3 (a) more false negatives / misses new attacks. (b) signature-based needs a known signature, so an attack with no signature yet slips through.