AP CYBERSECURITY • EXERCISE SHEET

5.6 Detecting Attacks on Data and Applications

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

KEY WORDS honeypot 蜜罐 • accounting 审计记录 • sql injection SQL 注入 • directory traversal 目录遍历 • cross-site scripting (xss) 跨站脚本

Objective

Build the skills to answer exam questions on detecting data attacks with **honeypots** 蜜罐 and log analysis.

You must be able to:

- describe accounting, honeypots, and hash checks as detective controls
- read application logs to identify SQL injection, XSS, and traversal
- weigh cost against sensitivity when choosing detection

1 Worked examples

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

■ The honeypot

A honeypot is a fake valuable file. Because no one has a legitimate reason to open it, any access is an unambiguous alarm - but it only catches an attacker who tries to open it.

■ Reading log signatures

SQL injection shows OR 1=1 and –. XSS shows <script> tags. Directory traversal shows ../. A buffer overflow shows very long input strings.

2 Practice

2.1 Explain how a **honeypot** detects an attacker. [2]

2.2 How can a cryptographic hash reveal that a file was altered? [2]

2.3 Match each log signature to its attack.

(a) OR 1=1 and – [1]

(b) a <script> tag [1]

(c) ../ in a request path [1]

3 Exam-style questions

3.1 A fake valuable file whose access signals an attack is a [1]

- **A** firewall
- **B** honeypot
- **C** baseline
- **D** patch

3.2 Seeing <script> tags in user input in the logs indicates [1]

- **A** SQL injection
- **B** cross-site scripting (XSS)
- **C** directory traversal
- **D** a smurf attack

3.3 A company wants cheap detection for tampering with sensitive files.

(a) Name one low-cost detective control. [1]

(b) Explain one limitation of a honeypot. [1]

Solutions

2.1 it is a fake valuable file no one should open, so any access is a clear sign of malicious activity.

2.2 re-hash the file and compare to the recorded hash; if the hash changed, the file changed.

2.3 (a) SQL injection. (b) XSS. (c) directory traversal.

3.1 B. a honeypot has no legitimate reason to be opened.

3.2 B. an injected <script> tag is the XSS signature.

3.3 (a) a honeypot or a cryptographic hash check. (b) a honeypot only catches an attacker who actually tries to open it.