Exercise walk-through

Detecting Attacks on Data and Applications ▪ 5.6

eXercise

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

Method — 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.

Method — 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.

Practice 2.1 ▪ 2 marks

Explain how a **honeypot** detects an attacker.

Solution 2.1

Method: The honeypot

Worked steps

it is a fake valuable file no one should open B1, so any access is a clear sign of malicious activity B1.

Practice 2.2 ▪ 2 marks

How can a cryptographic hash reveal that a file was altered?

Solution 2.2

Worked steps

re-hash the file and compare to the recorded hash B1; if the hash changed, the file changed B1.

Practice 2.3 ▪ 1 mark

Match each log signature to its attack.
(a) OR 1=1 and –
(b) a <script> tag
(c) ../ in a request path

Solution 2.3

Worked steps

(a) SQL injection B1. (b) XSS B1. (c) directory traversal B1.

Exam-style 3.1 ▪ 1 mark

A fake valuable file whose access signals an attack is a

A firewall

B honeypot

C baseline

D patch

Solution 3.1

Method: The honeypot

A firewall

B honeypot ✓

C baseline

D patch

Worked steps

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

Exam-style 3.2 ▪ 1 mark

Seeing <script> tags in user input in the logs indicates

A SQL injection

B cross-site scripting (XSS)

C directory traversal

D a smurf attack

Solution 3.2

Method: Reading log signatures

A SQL injection

B cross-site scripting (XSS) ✓

C directory traversal

D a smurf attack

Worked steps

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

Exam-style 3.3 ▪ 1 mark

A company wants cheap detection for tampering with sensitive files.
(a) Name one low-cost detective control.
(b) Explain one limitation of a honeypot.

Solution 3.3

Worked steps

(a) a honeypot or a cryptographic hash check B1. (b) a honeypot only catches an attacker who actually tries to open it B1.