AP CYBERSECURITY • EXERCISE SHEET

4.4 Detecting Attacks on Devices

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

KEY WORDS indicator of compromise (ioc) 入侵指标 • credential stuffing 撞库 • password spraying 密码喷洒 • hash 散列值 • malware 恶意软件

Objective

Build the skills to answer exam questions on **indicators of compromise (IoCs)** 入侵指标 and reading authentication logs.

You must be able to:

- define an IoC and name host-, file-, and behaviour-based IoCs
- read auth logs to tell guessing, spraying, and stuffing apart
- explain why offline password attacks cannot be detected

1 Worked examples

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

■ Reading auth logs

One user with many wrong passwords = a guessing attack. Many users failing from one IP = password spraying. A burst of default credentials = credential stuffing.

■ Offline attacks

Offline password attacks cannot be detected because the adversary already stole the hash database and is cracking it on their own computer, far from your logs.

2 Practice

2.1 Define an **indicator of compromise (IoC)**. [2]

2.2 A log shows 50 failed logins for user 'admin' from one IP in 30 seconds. What does this indicate? [2]

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

3 Exam-style questions

3.1 Many different users failing to log in from ONE IP address suggests [1]

- **A** credential stuffing
- **B** password spraying
- **C** salting
- **D** patching

3.2 A file whose hash matches known malware is an example of a [1]

- **A** host-based IoC
- **B** file-based IoC
- **C** behaviour-based IoC
- **D** network segment

3.3 An analyst reviews authentication logs after an alert.

(a) State one pattern that would indicate credential stuffing. [1]

(b) State one pattern that would indicate a single-account guessing attack. [1]

Solutions

2.1 evidence in logs or files that an adversary has compromised a device or network.

2.2 an online password-guessing attack on one account; many wrong passwords fast for one user is the signature.

2.3 the cracking happens on the adversary's own computer, away from the victim's systems and logs.

3.1 B. one IP, many users = password spraying.

3.2 B. matching a known-malware hash is a file-based IoC.

3.3 (a) a burst of default username:password pairs tried in quick succession. (b) many wrong passwords for one user account.