AP CYBERSECURITY • EXERCISE SHEET

5.2 Protecting Applications and Data: Managerial Controls and Access Controls

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

KEY WORDS access control models 访问控制模型 • principle of least privilege 最小权限原则

Objective

Build the skills to answer exam questions on **access control models** 访问控制模型 and **Linux permissions** Linux 权限.

You must be able to:

- choose the right access model (RBAC, RuBAC, DAC, MAC) from a scenario
- read and write Linux permissions using read 4 / write 2 / execute 1
- apply the **principle of least privilege** 最小权限原则

1 Worked examples

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

■ Choosing the model

RBAC follows your role; RuBAC follows a condition (like time); DAC lets the owner decide; MAC uses central levels. Match the scenario's decider to the model.

■ Linux permissions

Each group's number adds read (4) + write (2) + execute (1). chmod 640 = owner read+write (6), group read (4), others none (0).

2 Practice

2.1 "Access allowed only during business hours" - name the access-control model. [1]

2.2 Write the chmod number that gives the owner read+write, the group read, and others nothing. [2]

2.3 A file needs: owner read+write+execute, group read+execute, others none.

(a) Write the chmod number. [1]

(b) State what the ’7’ means. [1]

3 Exam-style questions

3.1 “Every user with the role ‘nurse’ can open patient charts” describes [1]

- **A** RuBAC
- **B** RBAC
- **C** DAC
- **D** MAC

3.2 The permission string -rw-r—— corresponds to which chmod number? [1]

- **A** chmod 444
- **B** chmod 640
- **C** chmod 740
- **D** chmod 777

3.3 An administrator applies the principle of least privilege.

(a) State what least privilege means. [1]

(b) Explain one security benefit. [1]

Solutions

2.1 RuBAC / rule-based access control.

2.2 640: owner 6 = 4+2, group 4, others 0.

2.3 (a) 750. (b) 7 = 4+2+1 = read + write + execute.

3.1 B. access follows the role, so RBAC.

3.2 B. owner rw = 6, group r = 4, others none = 0 → 640.

3.3 (a) each entity gets exactly the access it needs and no more. (b) if an account is compromised, the damage is limited to that minimal access.