Identificação, Autenticação e Autorização
2º Semestre, 2022/23

Exame de Recurso
26 de junho de 2023

- Todas as perguntas têm a mesma cotação.
- A duração total do exame é de 3 horas; a duração do teste é de 2 horas.
- Melhoria do 1º Teste: perguntas 1-10; melhoria do 2º Teste: perguntas 11-20.

1. Explique em que consiste o princípio do privilégio mínimo.

2. O controlo de acesso imposto ao super-utilizador do Linux (UID = 0) segue uma politica discricionária (*Discritionary Access Control*, DAC) ou obrigatória (*Mandatory Access Control*, MAC)? Justifique.

3. As políticas de controlo de acesso baseadas em papéis (*Role-Based Access Control*, RBAC) possuem um elemento central que é um papel, ou função (*role*). Explique por que razão o mesmo não se equipara a um grupo de utilizadores, tal como os que normalmente se usam na definição de proteções de ficheiros em sistemas operativos.

4. Considere o controlo de acesso através de capacidades (*capabilities*).
   a. Um bilhete (*ticket*) do Kerberos pode ser considerado uma capacidade? Justifique. ✗
   b. Um *Access Token* do OAuth 2.0 pode ser considerado uma capacidade? Justifique. ✓

5. Considere o conceito de Set-UID bit. Explique:
   a. Para que serve?
   b. Em que casos um utilizador comum (não privilegiado) pode manipular este bit?

6. Considere o conceito de *Control Groups* (cgroups) do Linux. Um processo com privilégios (*delegator*) pode criar um cgroup para um processo não privilegiado (*delegatee*) poder criar a sua própria sub-árvore de cgroups (*delegated subtree*). Explique o racional desta funcionalidade e dê um exemplo útil do seu uso.

7. No fluxo *implicit flow* do OAuth 2.0 não é realizada a autenticação do cliente. Explique porquê.

8. Um *access token* do OAuth 2.0 é uma credencial ao portador (*bearer token*) para acesso a um recurso protegido. Explique:
   a. O que é que isto significa, ser uma credencial ao portador?
   b. Que problemas podem ser criados com o roubo destas credenciais?

9. Que problema fundamental se procura resolver com a autenticação multifator?

10. Considere os paradigmas de autenticação com apresentação direta de credenciais. Explique que problemas têm relativamente ao roubo de credenciais.