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

1º Exame (Época Normal)
12 de junho de 2023

- Todas as perguntas têm a mesma cotação.
- A duração total do exame é de 3 horas.

1. O Linux possui dois mecanismos de elevação de privilégios associáveis a aplicações específicas: set-UID/Set-GID e capacidades (*capabilities*). Explique:
   a. O que permite cada um deles?
   b. Em que casos se deve usar cada um deles?

2. As políticas de controlo de acesso dependentes do contexto (*Context-Based*) condicionam as decisões a eventos passados. Explique a relevância deste facto no controlo de tráfego realizado pelas firewalls.

3. A política de controlo de acesso *break-the-glass* é muito importante em determinados cenários operacionais. Explique em quais, e ilustre a sua explicação com um exemplo.

4. O Linux possui um comando, sudo, que permite realizar a execução privilegiada de um comando arbitrário. Explique como é que o sudo permite que isso seja feito.

5. Considere o conceito de *Control Groups* (cgroups) do Linux. Estes permitem concretizar políticas de controlo de acesso quantitativos a recursos dos sistema. Explique:
   a. Como funciona genericamente esta política de controlo de acesso?
   b. Qual é a sua relevância para a proteção de um sistema Linux?

6. O OAuth 2.0 permite o acesso a recursos protegidos através de uma variante designada por *Device Authorization Grant*. Esta variante foi concebida para lidar com uma determinada limitação. Indique:
   a. Qual é essa limitação?
   b. Como é que a mesma é ultrapassada?

7. Considere a autenticação de pessoas com chaves partilhadas HOTP (*HMAC-based One-Time Password*). Explique:
   a. Como funciona?
   b. Quais as suas principais vulnerabilidades?

8. A arquitetura de autenticação PAM (*Pluggable Authentication Modules*) tem várias vantagens no âmbito da gestão da autenticação realizada numa máquina Linux. Indique duas dessas vantagens.

9. Os dispositivos individuais de autenticação usados no FIDO (*Fast Identity Online*) permitem gerar uma credencial de acesso diferente por cada prestador de serviço. Explique:
   a. Qual é o interesse desta funcionalidade?
   b. Que tipo de credenciais são usadas e como é que as mesmas são validadas?

10. Considere o padrão PKCS #11: Explique:
    a. Para que serve?
    b. Dê um exemplo da sua utilização.