Identificação, Autenticação e Autorização
2º Semestre, 2021/22

2º Teste
4 de julho de 2022

- Todas as perguntas têm a mesma cotação.
- A duração total do teste é de 2 horas.

1. Imagine que se decidia pelo uso de biometria para obter a identidade de uma pessoa. Nesse caso:
    a. O que seria preciso fazer para realizar uma operação de autenticação e não de identificação?
    b. Que riscos minimizaria se optasse por uma autenticação em vez de uma identificação?

2. Os ataques com dicionários só são possíveis com determinadas estratégias de autenticação, que são usadas em diversos protocolos de autenticação.
    a. Que estratégias são essas e o que as torna vulneráveis a esses ataques?
    b. Indique duas estratégias alternativas que eliminam essa vulnerabilidade.

3. Explique, de uma forma sucinta mas completa, como funciona o protocolo de autenticação TOTP (*Time-based One-Time Password*).

4. Explique porque razão se escolheu a autenticação com credenciais assimétricas e certificados X.509 da respetiva componente pública para autenticar servidores Web.

5. O SSH (*Secure Shell*) permite uma autenticação mútua dos interlocutores, mas não segundo o mesmo paradigma nos dois sentidos. Descreva:
    a. De que forma se autentica o extremos servidor.
    b. De que forma se autentica o extremo cliente.

6. A infraestrutura PAM (*Pluggable Authentication Modules*) permite configurar de forma flexível e rápida a forma como se realizam diversas operações de autenticação que podem ser realizadas num sistema operativo Linux. Explique:
    a. Como se pode modificar apenas o processo de autenticação relativo a uma aplicação?
    b. De que forma é possível adicionar e parametrizar a execução de um novo mecanismo de autenticação?

7. O padrão PKCS #11 define uma interface para acesso a dispositivos criptográficos (*crypto tokens*). Mas embora a interface seja apenas uma, é normal que a mesma seja concretizada por bibliotecas diferentes, tipicamente uma para cada tipo de dispositivo. Explique porquê.

8. Explique como é realizada a autenticação de uma pessoa através do seu Cartão de Cidadão.

9. O Kerberos é um sistema que consegue autenticar pessoas (utentes) perante serviços. Explique, com pormenor, como tal é realizado.

10. No cenário de autenticação *enterprise* do 802.1X usa-se EAP (*Extensible Authentication Protocol*) para encapsular a autenticação entre um suplicante e um Servidor de Autenticação. Explique:
    a. Que vantagens advêm desse encapsulamento?
    b. Que elementos críticos resultam de uma autenticação sobre EAP para a prossecução da autenticação com 802.1X?