11. A autenticação biométrica é normalmente muito vulnerável a ataques baseados no roubo de credenciais. Explique porquê.

12. Os protocolos de autenticação baseados em desafio-resposta são muito dependentes de valores designados por *nonces* (abreviatura de *not once*). Explique porquê.

13. A infraestrutura PAM (*Pluggable Authentication Modules*) usa ficheiros de orquestração para configurar de forma flexível a forma como se realizam diversas operações de autenticação que podem ser realizadas num sistema operativo Linux. Explique
    a. Como se pode concretizar uma política multifator?
    b. Como se pode concretizar uma política em que há várias alternativas de autenticação?

14. O padrão PKCS #11 é uma das interfaces que existe para interagir com o Cartão de Cidadão. Explique:
    a. Para que serve?
    b. Qual é a outra interface e por que razão é diferente?

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

16. O SSH autentica o extremo servidor usando chaves públicas não certificadas, enquanto o TLS usa certificados de chaves públicas X.509. Justifique a adequação de ambas as estratégias.

17. O Kerberos é um sistema que depende muito da sincronização dos relógios de clientes e servidores. Explique porquê.

18. No cenário de autenticação *enterprise* do 802.1X, explique quando e como é que um nó móvel (*supplicant*) sabe que está a interagir com um elemento genuíno (*Access Point*, AP) da rede a que pretende aceder.

19. Explique a diferença que existe entre um Gestor de Identidades (*Identity Manager*, IdM) e um Fornecedor de Identidade (*Identity Providers*, IdP).

20. Considere o conceito de quasi-identificador. Explique:
    a. Em que consiste?
    b. Que problemas levanta relativamente a requisitos de anonimato?