14. Considere o protocolo de autenticação HOTP (*HMAC-based One Time Password*), que permite calcular OTPs a partir de uma chave partilhada e de um contador fracamente sincronizado. Esplique:
    a. Como evolui o contador ao longo da utilização de OTPs geradas com este protocolo?
    b. Que configurações podem ser feitas no validador para lidar com essa evolução.

15. O Kerberos usa um KDC (*Key Distribution Center*) baseado em dois serviços: AS (*Authentication* Service) e TGS (*Ticket Granting* Service). Explique para que serve cada um deles.

16. O Kerberos é um sistema que faculta a autenticação entre clientes (pessoas que usam aplicações cliente Kerberizadas) e serviços (igualmente Kerberizados). Explique o que significa essa Kerberização?

17. Considere o conceito de Control Groups (cgroups) do Linux. Explique de que a sua organização hierárquica é usada para controlar o uso de recursos por processos.

18. De que forma é que a técnica de k-anonimato contribui para o anonimato na análise de um conjunto de registos?

19. Os sistemas de gestão de identidade baseados em IdP (*Identity Providers*) agregam diversos atributos de identidade para vários serviços (*Service Providers*). Explique por que razão esse modelo pode criar problemas de privacidade para os utentes identificados através desses IdPs?

20. O IKE2 é um protocolo que permite negociar *Security Associations* IKE e IPSec. O protocolo tem duas fases. Indique para que serve cada uma.