Questões para Autoavaliação sobre Conceitos e Noções Introdutórias

Questões em português

1. Considere as noções de "política de segurança" e "mecanismo de segurança". Uma das noções (A) está associada e foca na segurança que se quer garantir, enquanto que a outra noção (B) está associada a fundamentos, técnicas e tecnologias que permitem pôr em prática as garantias de segurança. Identifique as noções nos casos A e B.
2. Dê um ou mais exemplos de política de segurança e mecanismo de segurança quando observa um sistema, como por exemplo o sistema CLIP.
3. No contexto de um sistema distribuído, diga o que entende por defesa de perímetro e defesa de profundidade ? Dê exemplos de um e outro caso.
4. Explique e relacione os seguintes conceitos:
    - Vulnerabilidade.
    - Ataque.
    - Risco
    - Ameaça.
    - Defesa.
5. Dê exemplos que caracterizem cada um dos conceitos explicados em 4.
6. Quais as vantagens e desvantagens de eliminar riscos em vez de eliminar vulnerabilidades.
7. No âmbito dos sistemas computacionais:
    a) Explique o conceito de domínio de segurança.
    b) Qual a relação que deverá existir entre (i) o desenho e planeamento de redes locais e da sua ligação à Internet e (ii) a implantação de domínios de segurança.
8. Considere o princípio do privilégio mínimo. Indique vantagens e desvantagens operacionais decorrentes da sua aplicação em abstrato.
9. Enuncie um ou mais requisitos de segurança que estejam associados a políticas de segurança ou reforços de políticas de segurança.
10. De entre as áreas de segurança relativas ao padrão ISO 17999 e seus objetivos (e que também se inscrevem na mais vasta base documental ISO 27000), quais das áreas cobrem o seguinte tipo de requisitos:
    a) Impedir lacunas em leis civis ou criminais, bem como obrigações estatutárias, regulatórias ou contratuais associadas a requisitos de segurança
    b) Educação de recursos humanos para redução de risco de erros, fraudes, ou uso incorreto de sistemas ou componentes de sistemas por parte de equipas operacionais
    c) Proteger a integridade de software e dados geridos (ou mantidos) por esse software
    d) Minimizar o risco de falhas de sistemas, por exemplo envolvendo soluções de discos replicados (com tipologias de soluões de armazenamento em RAID)
11. Em que área ou áreas de objetivos do padrão ISO/IEC 1799 enquadraria a implementação de soluções associadas ao regulamento geral de privacidade de dados (RGPD). Justifique

12. Considerando a tipologia de mecanismos usados para implementação de políticas de segurança, os sistemas de defesa de perímetro como sejam os sistemas de prevenção de intrusões (*Intrusion Prevention Systems ou IPS*) ou sistemas corta-fogo (ou sistemas Firewalls) constituem mecanismos de inspeção. Verdadeiro ou Falso ? Considerando ser Falso corrija a afirmação

13. Dê um exemplo de um mecanismo de segurança que caracterize como sendo um mecanismo de execução privilegiada no caso de um sistema operativo LINUX ou MAC-OS.

14. De acordo com a tipologia de mecanismos de segurança, dê exemplo de um mecanismo de registo que identifique no seu computador pessoal.

15. Um ataque associado ao risco de personificação em redes de computadores pode ter um de dois propósitos: despiste ou apropriação. Dê exemplo de um ou outro propósito num ataque deste tipo.

16. Se um atacante quer realizar um ataque por reprodução a um fluxo de dados trocados por dois principais corretos, não o conseguirá fazer se o canal de comunicação for cifrado e assim assegurando confidencialidade. Verdadeiro ou Falso ?

17. Um sistema Firewall é um exemplo de uma defesa de perímetro que permite detectar se uma intrusão num sistema (nó de um sistema distribuído) teve lugar.

18. O protocolo IPSec é um protocolo de segurança que atua ao nível transporte, considerando a pilha TCP/IP. Verdadeiro ou Falso ?

19. Numa conexão HTTPS, os *endpoints* que representam um cliente (browser) e um servidor (servidor WEB) são sempre autenticados mutuamente.

20. O protocolo TLS, ao assegurar propriedades de segurança, assegura as mesmas em contexto de segurança extremo-a-extremo ou ponto-a-ponto ? Justifique.

Questões em inglês

21. Answer to review questions after reading Chapter 1 of the following book: W. Stallings, L. Brown, Computer Security, Principles and Paradigms and Chapter 1 of the following book: W. Stallings, Network Security Essentials.
    a) Define *computer security*.
    b) What is the OSI security architecture?
    c) What is the difference between passive and active security threats?
    d) List and briefly define categories of passive and active network security attacks.
    e) List and briefly define categories of security services.
    f) List and briefly define categories of security mechanisms.
    g) List and briefly define the fundamental security design principles.
    h) Explain the difference between an attack surface and an attack tree.

22. Review matrices similar to the ones presented and discussed in class (Introduction) to understand the mappings between attack types, security services and security mechanisms

23. From the security mechanisms in the matrices before, which ones we consider as pervasive or specific mechanisms. Why ?

24. Try to instantiate the security mechanisms with concrete mechanisms and techniques and related solutions

25. From your experience in using the CLIP system (as a user), try to recognize the security mechanisms used for the following security services: authentication, access-control, confidentiality, integrity and availability (considering that are mechanisms you feel as countermeasures against attacks against such security properties).

26. When you use TLS (or SSL) in an HTTPS connection, authenticating the server, what kind of authentication is it ? Peer-Authentication or Data-Origin Authentication ?

27. Do you believe that TLS (or SSL) can provide defenses against Denial Of Service Attacks ? What about SSH ? Explain.

28. When you are analyzing the security properties at the level of IPSec, what is the principals involved ?

29. What means the principle of the least privilege? Give an example of the applicability of this principle.

30. What means the principle of the least common mechanism? Give an example of the applicability of this principle.

31. What means the principle of complete mediation? Give an example of the applicability of this principle.

32. From what you learned in the introduction class, explain mechanisms that instantiate the principle of isolation at hardware level in a computer system.

33. Explain the principle of the separation of privileges.

34. Explain the notion of attack surface

35. Give an example of a software attack surface, considering attacks to web-applications.