TESTE 1 21/22

1. As políticas de segurança:
   (a) Definem requisitos e regras para a proteção dos recursos de uma organização
   (b) São constituídas pelas leis que definem o âmbito do crime informático
   (c) São uma coisa de políticos e polícias, que não tem nada a ver com segurança de redes e sistemas informáticos
   (d) São as tecnologias que permitem implementar um determinado objetivo de segurança
2. O conceito de domínio de segurança:
   (a) Agrega pessoas com conhecimento ou tarefas semelhantes
   (b) Refere-se a um conjunto de políticas
   (c) Refere-se a um conjunto de controlos
   (d) É útil para gerir a segurança de forma agregada
3. Identifique uma das principais fontes de vulnerabilidades:
   (a) Comunicações internas
   (b) CVEs
   (c) Erros de hardware
   (d) Usuários

4. O OWASP Top 10 consiste:
   (a) Nas 10 vulnerabilidades mais populares em sistemas atuais
   (b) Nas 10 vulnerabilidades mais importantes para o desenvolvimento de sistemas
   (c) Nos 10 mecanismos mais relevantes a implementar
   (d) Nas 10 fontes de vulnerabilidades mais populares em sistemas atuais

5. Que medidas endereçam maioritariamente vulnerabilidades conhecidas?
   (a) Reconhecimento
   (b) Legais
   (c) Ataque
   (d) Ilusão

6. Um ataque Meet-in-the-Middle:
   (a) Permite interceptar a negociação de chaves com Diffie-Hellman
   (b) Permite encontrar a chave num cifra dupla com dificuldade inferior à esperada
   (c) Aplica-se a algoritmos que usem EDE com K1=K2 ou K2=K3
   (d) É um ataque de roubo de chaves assimétricas

7. Uma cifra híbrida consiste em:
   (a) Um mecanismo para aumento da performance no uso prático de chaves assimétricas
   (b) Cifrar um texto com uma chave assimétrica aleatória, que é cifrada com a chave pública do destinatário
   (c) Utilizar uma qualquer combinação de algoritmos de cifra
   (d) Realizar uma cifra com controlo de integridade

8. Qual das seguintes cifras não existe:
   (a) Cifras contínuas simétricas
   (b) Cifras contínuas assimétricas
   (c) Cifras por blocos assimétricas
   (d) Cifra de Vernam

9. Qual dos seguintes modos de cifra **não** permite paralelizar a decifra?
   (a) ECB (*Electronic Code Book*)
   (b) OFB (*Output FeedBack*)
   (c) CBC (*Cipher Block Chaining*)
   (d) GCM (*Galois/Counter Mode*)

10. Tendo em conta apenas a resistência à descoberta de colisões em funções de síntese, qual destas expressões é **verdadeira**?
   (a) Essa propriedade não é relevante para a robustez dos processos de criação e validação de assinaturas digitais
   (b) Se for reduzida, representa um risco caso a função seja usada num MIC (*Message Integrity Code*)
   (c) É definida apenas pela dimensão do resultado da função, de acordo com o paradoxo do aniversário
   (d) Se for reduzida, uma entidade terceira poderá produzir um texto alternativo compatível com a assinatura de outro texto

Uma síntese demasiado pequena vai produzir colisões very easily.

11. Ao utilizar o mecanismo PBKDF2, que informação pode ser pública?
   (a) O tamanho dos blocos
   (b) O *Pseudo Random Generator*
   (c) O número de blocos
   (d) O tipo de operações

12. No cálculo de um MAC (*Message Authentication Code*) qual dos seguintes tipos de funções é normalmente usado?
    (a) Funções de cifra com excipiente
    (b) Cifras simétricas contínuas
    (c) Cifras simétricas por blocos
    (d) Cifra de Vernam

13. Uma assinatura digital de uma mensagem:
    (a) Permite que terceiros verifiquem a identidade de quem a envia numa rede
    (b) Impede que o recetor aceite uma mensagem adulterada depois de assinada
    (c) Garante a identidade de quem a envia numa rede
    (d) Garante a identidade de quem a recebe

14. Um dos objectivos das assinaturas digitais é o não-repúdio, que consiste em:
    (a) Impedir a negação da criação de uma assinatura digital
    (b) Impedir o acesso não autorizado ao conteúdo das mensagens/documentos
    (c) Forçar o uso de *smartcards* na geração de assinaturas
    (d) Impedir que uma entidade negue a autoria de um documento de texto

15. Tendo em conta o uso de CRL (*Certificate Revocation List*), qual destas afirmações é **verdadeira**?
    (a) As CRL indicam a identidade dos sujeitos afetos aos certificados revogados
    (b) A localização da CRL de uma Entidade Certificadora faz parte de todos os certificados que ela revogar
    (c) As CRL delta incluem certificados expirados, mas as CRL base não
    (d) Quando uma lista base é emitida, importa obrigatoriamente a lista delta imediatamente anterior

16. Em qual dos seguintes casos é possível um utente realizar uma verificação incompleta, mas válida, de uma cadeia de certificação?
    (a) Existe confiança na Entidade Certificadora (CA) raiz do caminho de certificação
    (b) A validação via OCSP (*Online Certificate Status Protocol*) devolve indicação de que o certificado é válido
    (c) Não é de todo possível
    (d) O certificado de uma Entidade Certificadora (CA) intermédia foi revogado após a data do certificado por ela assinado

17. Considere o criptograma resultante de uma cifra por blocos no modo CBC. Assumindo que a transmissão do criptograma resultou na perda de um número desconhecido de bits iniciais, é possível obter alguma parte do texto original? Justifique.

- Cifra por blocos no modo CBC (Cipher Block Chaining)

A cifra por blocos no modo CBC, permite a cifra e a decifra de cada bloco tendo em conta o feedback de C_{i-1}, ou seja, com recurso ao feedback da cifra do bloco anterior. Como é usado este feedback, do bloco anterior, é necessário um IV (com o mesmo tamanho do bloco), para calcular a cifra do primeiro bloco. Deste modo, é possível obter o texto original, a partir do bloco seguinte ao bloco que não sofreu a perda bits, se este bloco estiver completo. Caso esse bloco não esteja completo, só se consegue obter o texto original a partir do bloco a seguir ao bloco seguinte antes mencionado.

18. Considerando uma cadeia de certificação, porque nem todos os certificados da cadeia são validados da mesma forma?

- Nem todos os certs da cadeia são validados da mesma forma

A