Teste de SIO 1

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 polícia, 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. **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 importantes

---

5. **Que medida endereça maioritariamente vulnerabilidades conhecidas?**
   (a) Reconhecimento
   (b) Legais
   (b) Ataque
   (b) 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 usam EDE com K1=K2 e 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 cifra?**
(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 numa 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 outro texto autenticamente assinado ao imitar outro texto

main carreta

---

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 uma MAC (Message Authentication Code) que algoritmos ou tipos de funções é normalmente usado?**
(a) Funções de cifra com excipiente
(b) Cifras simétricas contínuas
(c) Cifras simétricas por blocos
(d) Cifra de Verman

---

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 ? → Também pode ser

---

14. **Um dos objetivos 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 num documento de texto
(d) Impedir que uma entidade negue a autoria de um documento ou 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 detêm unicamente certificados expirados, mas a 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 no 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) A confiança de uma Entidade Certificadora (CA) intermediária foi resolvida após a data de criação do certificado assinado

---
Aqui estão as perguntas reescritas sem as respostas destacadas:

---

17. **Identifique uma das principais fontes de vulnerabilidades dos sistemas informáticos**:
(a) Comunicações não controladas
(b) Atualizações conhecidas
(c) Administradores
(d) Fornecedores

---

18. **Identifique uma das dimensões principais a considerar numa estratégia de segurança**:
(a) As pessoas
(b) O treino
(c) As vulnerabilidades
(d) As políticas

---

19. **Em relação à faceta ofensiva da segurança, assinale a correta**:
(a) Diz respeito ao software, mas não aos processos ✓
(b) Consiste em ofender pessoas ✗

(c) É de evitar, pois corresponde a atividades ilegais
(d) É usada pelos cibercriminosos

---

20. **As técnicas de branqueamento de uma cifra**:
(a) Aumentam a segurança de uma cifra
(b) Aplicam chaves no início e/ou criptogramas com XOR
(c) Anonimizam os dados depois de decifrados
(d) Renomeiam as chaves fixas

---

21. **Uma cifra híbrida consiste em**:
(a) Utilizar cifra com decifra
(b) Utilizar uma combinação de cifras contínuas
(c) Cifrar um texto com uma chave simétrica aleatória, que é cifrada com a chave pública do destinatário
(d) Utilizar uma qualquer combinação de algoritmos de cifra

---

22. **Qual dos seguintes modos de cifra permite paralelizar a cifra?**
(a) CFB (Cipher FeedBack)
(b) GCM (Galois/Counter Mode)
(c) CBC (Cipher Block Chaining)
(d) CTR (Counter)

---

23. **Ao utilizar o mecanismo PBKDF2, que informação deve ser privada?**
(a) A dimensão do resultado
(b) A senha
(c) O Pseudo Random Generator
(d) O tamanho dos blocos

---

24. **Quando se usa cifra tripla é normal usar o modo EDE (Encrypt, Decrypt and Encrypt). Porquê?**
(a) Porque permite que decifra possa anular uma cifra, resultando numa única cifra simples
(b) Porque caso se usasse 3 cifras seria mais simples de escolher as 3 chaves
(c) Porque aumenta a robustez da cifra, sem impacto de performance
(d) Porque usar uma decifra entre cifras aumenta muito a confusão do processo de cifra

---

25. **Tendo em conta apenas a resistência à descoberta de colisões em funções de síntese, qual destas expressões é verdadeira?**
(a) Duas funções que implementem algoritmos distintos não vão colidir
(b) Se for reduzida, representa um risco caso a função seja usada num MIC (Message Integrity Code)
(c) Pode ser muito elevada com funções de síntese pseudo-aleatórias
(d) Se for reduzida, o autor de uma assinatura poderá produzir vários documentos para a mesma

assinatura

---

26. **Uma assinatura digital de uma mensagem usando RSA**:
(a) Não tem qualquer vantagem em relação a uma autenticação com um MAC (Message Authentication Code)
(b) Permite que terceiros verifiquem a identidade de quem a envia
(c) Garante a identidade de quem a envia
(d) Garante a identidade de quem a cria

---

27. **Para se verificar uma assinatura digital de um documento é preciso**:
(a) A chave pública do verificador
(b) A identidade do assinante
(c) A chave pública do assinante
(d) O certificado de chave pública do verificador

---

28. **Tendo em conta o uso de CRL (Certificate Revocation List), qual destas afirmações é verdadeira?**

(a) As CRL delta constituem uma validação de integridade das CRL base
(b) As CRL base devem ser obtidas em conjunto com as CRL delta
(c) As CRL delta devem ser consultadas a cada acesso remoto
(d) Quando uma lista base é emitida, importa obrigatoriamente a lista delta imediatamente anterior

---

29. **Em qual dos seguintes casos é possível um utente realizar uma verificação incompleta, mas válida, de uma cadeia de certificação?**
(a) Existe uma Entidade Certificadora (CA) intermédia confiável no caminho de certificação
(b) Não é de todo possível
(c) O certificado de todas as Entidade Certificadoras (CA) intermédias ainda não expirou
(d) A data do certificado é válida

---

30. **As políticas de segurança de informação**:
(a) Não se aplicam aos equipamentos de uma organização
(b) São as tecnologias que permitem implementar um determinado objetivo de segurança
(c) São processos e mecanismos específicos a utilizar de forma a obter segurança
(d) São normas, regulamentos e orientações que definem o modelo de proteção num determinado domínio de segurança

---

31. **Uma vulnerabilidade é um estado de um sistema que permite**:
(a) Que um atacante negue a prestação de serviços
(b) Que um atacante consiga agir sem ser notado
(c) Que um atacante conheça o seu funcionamento
(d) Que um atacante venda acessos ilegítimos

---

32. **O OWASP Top 10 consiste**:
  (a) Na lista das 10 empresas mais relevantes na área de segurança
  (b) Numa previsão das 10 vulnerabilidades mais relevantes no próximo ano
  (c) Nos 10 mecanismos mais relevantes a implementar
  (d) Nas 10 fontes de vulnerabilidades mais populares em sistemas atuais/recentes

---

33. **Num ataque XSS (Cross-Site Scripting) e CSRF (Cross-Site Request Forgery), onde é executado o código malicioso?**
  (a) No servidor comprometido
  (b) Num servidor vulnerável
  (c) No servidor
  (d) No computador da vítima

---

34. **Qual é o objetivo principal de um plano de segurança numa organização?**
  (a) É um registo histórico de incidentes de segurança
  (b) É um manual de procedimentos de resposta a emergências
  (c) É um plano para a organização de recursos e atividades de segurança
  (d) É um documento ativo que descreve a postura de segurança da organização, permitindo que se acompanhe o estado atual e futuro de segurança

---

35. **Uma cifra simétrica**:
  (a) Permite não repúdio de quem cifra com a chave pública
  (b) Obriga a utilização de excipiente
  (c) Permite o não repúdio de quem cifra com a chave privada
  (d) Pode servir para implementar mecanismos de controlo de integridade

---

36. **O conceito de difusão, indicado por Shannon, significa**:
  (a) Que o algoritmo é implementado com técnicas de difusão
  (b) Que o método de cifra não faz uso de blocos
  (c) Que utiliza um IV
  (d) Que uma alteração do texto resulta numa grande alteração do criptograma

---

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

---

38. **Qual dos seguintes modos de cifra não usa um vetor de inicialização (Initialization Vector, IV) adicional à chave?**
  (a) CTR (Counter)

(b) CBC (Cipher Block Chaining)
(c) CFB (Cipher FeedBack)
(d) ECB (Electronic Code Book) → não usa IV.

---

39. **Tendo em conta apenas a resistência à descoberta de colisões em funções de síntese, qual destas expressões é verdadeira?**
(a) É definida apenas pela dimensão do resultado da função
(b) Duas funções que implementem algoritmos distintos não vão colidir
(c) Pode ser muito elevada com funções de síntese pseudo-aleatórias
(d) Se for reduzida, uma entidade terceira poderá produzir um texto alternativo compatível com a assinatura de outro texto

---

40. **Um MAC (Message Authentication Code) é calculado com uma chave secreta**
(a) Porque usa uma função de cifra
(b) Para que um atacante não consiga deduzir uma mensagem a partir do seu MAC
(c) Para impedir que terceiros possam gerar um MAC válido para uma outra mensagem
(d) Porque é necessário garantir o seu secretismo

---

41. **Qual das seguintes cifras não existe**:
(a) Cifras contínuas simétricas
(b) Cifras por blocos recorrendo a cifras contínuas
(c) Cifras por blocos assimétricas
(d) Cifras contínuas recorrendo a cifras por blocos

CFB, OFB, passam em cifras por blocos e transformam em contínuas

---

42. **Qual dos seguintes modos de cifra não usa um vetor de iniciação (Initialization Vector, IV) adicional à chave?**
(a) CFB (Cipher FeedBack)
(b) GCM (Galois/Counter Mode)
(c) CTR (Counter)
(d) ECB (Electronic Code Book)

aqui cada bloco é cifrado usando a mesma chave.

---

43. **Qual dos seguintes modos de cifra realiza uma cifra monoalfabética?**
(a) ECB (Electronic Code Book)
(b) CBC (Cipher Block Chaining) → não é monoalfabética, pq há uma difusão entre os blocos e a cifragem depende da posição e dos blocos anteriores, além de ter vetor de inicialização.

---

44. **Ao utilizar o mecanismo PBKDF2, que informação deve ser privada?**
(a) A senha
(b) A função de derivação
(c) O número de iterações (rounds)
(d) O Salt

---

45. **Qual das seguintes afirmações é correta?**
(a) No método Encrypt-then-MAC, a integridade do criptograma é determinada depois da sua decifragem
(b) O método MAC-then-Encrypt revela se o texto é igual a um outro já conhecido
(c) O método Encrypt-and-MAC permite validar a integridade do criptograma antes da sua decifragem
(d) O método Encrypt-then-MAC permite validar a integridade do criptograma antes da sua decifragem
↳ mais seguro

---

46. **No contexto das cifras, uma Substitution Box**: → adiciona confusão
(a) Substitui uma mensagem constituída por bits à entrada por uma outra mensagem gravada
(b) Aplica o conceito da difusão perfeita
(c) Altera a ordem de bits sem alterar o seu valor → isso é permutation Box
(d) Opera com base numa chave ✗

---

47. **Em que consiste a Integridade da informação?**
(a) Garantia que a informação não foi lida por terceiros
(b) Garantia que a informação não é convertida para outro formato
(c) Garantia que a informação é armazenada de forma integral
(d) Garantia que a informação não é alterada

---

48. **Em relação à faceta ofensiva da segurança, assinale a correta**:
(a) É ilegal ✗
(b) Diz respeito ao software, mas não aos processos ✗
(c) Foca-se em diminuir o custo de um sistema ✗
(d) É útil para validar a segurança de uma solução

---

49. **Tendo em conta o que é um registo CVE (Common Vulnerabilities and Exposures), é verdade que**:
(a) Um registo CVE estima o valor monetário da exploração da vulnerabilidade ✗
(b) Um registo CVE descreve vírus e outras aplicações maliciosas
(c) Um registo CVE identifica formas de proteção de uma vulnerabilidade
(d) Um registo CVE descreve como pode ser realizado um ataque a um software vulnerável

---

50. **O mecanismo de negociação de chaves Diffie-Hellman**:
(a) É robusto contra atacantes ativos
(b) Faz uso de valores públicos e privados
(c) Obriga a que os intervenientes distribuam chaves anteriormente à negociação
(d) Implementa um mecanismo de cifra híbrida

---

51. **As técnicas de branqueamento em cifras**:
(a) Aplicam-se a assinaturas de forma a esconder o assinante
(b) Aplicam chaves ao texto e/ou criptograma com XOR
(c) Anonimizam os dados depois de decifrados

(d) Aumentam a difusão de uma cifra

---

52. **Qual das seguintes cifras não existe**:
(a) Cifras por blocos recorrendo a cifras contínuas
(b) Cifras por blocos assimétricas
(c) Cifras por blocos simétricas
(d) Cifras contínuas simétricas

---

53. **Quando se diz que uma cifra é realizada em N-bit OFB (Output FeedBack), tal significa que**:
(a) Requer um mínimo de N bits de memória para o gerador
(b) Por cada cifra por blocos do seu gerador só são usados N bits do resultado
(c) A cifra por blocos do gerador possui N bits nos blocos de entrada e saída
(d) Evita a propagação de erros até N bits

---

54. **Tendo em conta apenas a resistência à descoberta de colisões em funções de síntese, qual destas expressões é verdadeira?**
(a) Será tanto menor quanto menor for a dimensão do resultado da função
(b) Se for reduzida, representa um risco caso a função seja usada num MIC (Message Integrity Code)
(c) Tem um limite superior que depende da dimensão da entrada da função
(d) Essa propriedade não é relevante para a robustez dos processos de criação e validação de assinaturas digitais

---

55. **Os mecanismos de derivação de chaves (PBKDF2, etc) são importantes para**:
(a) Aumentar o universo de pesquisa da palavra-passe
(b) Reduzir o universo de pesquisa da palavra-passe
(c) Evitar ataques por dicionário, em relação aos ataques por força bruta
(d) Aumentar o custo de ataques por força bruta

→ são gerados, usando hashes

56. **Um MIC (Message Integrity Code)**:
(a) É robusto contra modificações aleatórias de transmissão
(b) É implementado através de cifras assimétricas
(c) É implementado através de cifras contínuas
(d) Faz uso de uma chave conhecida apenas pelos locutores → isto é para o MAC

---

57. **A assinatura digital de um documento**:
(a) Tem de, forçosamente, incluir a identidade do assinante
(b) Pode ser copiada para outro documento desde que o assinante seja o mesmo
(c) Deixa de ser válida quando o par de chaves do assinante expira
(d) Impede que o documento possa ser compreendido por quem não estiver autorizado

---

58. **Uma assinatura digital de uma mensagem usando RSA**:

(a) Impede que o recetor aceite uma mensagem adulterada depois de assinada
(b) Garante a identidade de quem a recebe
(c) Permite que terceiros verifiquem a identidade de quem a envia
(d) Obriga a que cada mensagem contenha sempre o certificado de chave pública do assinante

---

59. **Tendo em conta o período de validade de um certificado, qual destas afirmações é verdadeira?**
(a) Não é uma informação obrigatória nos certificados
(b) Não permite que o certificado seja usado fora desse período
(c) Pode ser estendido pela respetiva Entidade Certificadora
(d) Serve para limitar, no tempo, o uso da correspondente chave privada

---

60. **Uma Entidade Certificadora raiz é confiável porque**:
(a) O software que faz a validação de uma cadeia de certificação o considera confiável
(b) Ninguém certifica o seu certificado
(c) Certifica muitas outras Entidades Certificadoras
(d) Tem o topo da cadeia de certificação
