Teste 2021/22 SIO

10-fev-2022

1º Exame

### 1. Identifique uma das principais fontes de vulnerabilidade em sistemas informáticos:

* 1. Comunicações não controladas
  2. Comunicações conhecidas
  3. Administradores
  4. Fornecedores

### 2. Identifique umas das **dimensões** principais a considerar numa estratégia de segurança:

* 1. As pessoas
  2. O treino
  3. A vulnerabilidade
  4. As políticas

### 3. Em relação à faceta ofensiva da segurança, assinale a correta:

* 1. Diz respeito ao software, mas não aos processos
  2. Consiste em ofender pessoas
  3. É de evitar, pois corresponde a atividades ilegais
  4. É usada pelos ciber-criminosos

### 4. O OWASP Top 10 consiste:

* 1. Nas 10 vulnerabilidades mais populares em sistemas atuas
  2. Nos 10 mecanismos mais relevantes a implementar
  3. No ranking de um concurso de exploração de vulnerabilidades
  4. Nas fontes de vulnerabilidades mais populares em sistemas atuais

### 5. (… )vulnerabilidades:

* 1. (…) comunicação com criminosos
  2. Considera a análise *(estatística)* para análise de aplicações em execução
  3. Está *(limitada)* a vulnerabilidades conhecidas
  4. Considera a análise *(estatica)* para análise do código (…)

### 6. Quando se usa cifra tripla é normal usar o modo EDE. Porquê?

* 1. Porque permite que decifra possa anular uma cifra, resultando numa única cifra simples
  2. Porque case se usasse 3 cifras seria mais simples de descobrir as 3 chaves
  3. Porque aumenta robustez da cifra, sem impacto de performance
  4. Porque usar uma decifra entre cifras aumenta muito a confusão do processo de cifra

### 7. As técnicas de branqueamento em cifras:

* 1. Aumentam a difusão de uma cifra
  2. Aplicam chaves ao texto e/ou criptograma com XOR
  3. Anonimizam os dados depois de decifrados
  4. Removem a maioria dos padrões do texto, mesmo usando uma chave fixe

### 8. Uma cifra híbrida consiste em:

* 1. Utilizar cifra com decifra
  2. Utilizar uma combinação de cifras por blocos e continuas
  3. Cifrara um texto com uma chave simétrica aleatória, que é cifrada com a chave pública do destinatário
  4. Utilizar uma qualquer combinação de algoritmos de cifra

### 9. Qual dos Seguintes modo de cifra permite paralelizar a cifra e a decifra:

* 1. CFB (Cipher FeedBack)
  2. GCM (Galois/Counter Mode)
  3. CBC (Cipher Block Chaining)
  4. CTR (Counter Mode)

### 10. Ao utilizar o mecanismo PBKDF2, que informação deve ser privada?

* 1. A dimensão do resultado
  2. A senha
  3. O Pseudo Random Generator
  4. O tamanho dos blocos

### 11. Tendo em conta apenas a resistência à descoberta de colisões em funções de síntese, qual destas expressões é **verdadeira**?

* 1. Duas funções que implementam algoritmos distintos vão colidir
  2. Se for reduzida, representa um risco caso a função seja usada num MIC (Message Integrity Code)
  3. Pode ser muito elevada com funções de síntese pseudo-aleatórias
  4. Se for reduzida, o autor de uma assinatura poderá produzir vários documentos para a mesma assinatura

### 12. Um MAC (Message Authentication Code) é calculado com uma chave secreta:

* 1. Para que um atacante não consiga (…) -sagem a partir do seu MAC
  2. Porque a (…) MAC precisa de ser confiável.
  3. Para evitar que um atacante possa validar um MAC
  4. Para verificar que uma mensagem e o seu MAC, proveem de um (…) conhecido

### 13. Uma assinatura digital de uma mensagem usando RSA:

* 1. Não tem qualquer vantagem em relação a uma autenticação com um MAC
  2. Permite que terceiros verifiquem a identidade de quem a envia
  3. Garante a identidade de quem a envia
  4. Garante a identidade de quem a cria

### 14. Para se verificar uma assinatura digital de um documento é preciso:

* 1. A chave pública do verificador
  2. A identidade do assinante
  3. A chave pública do assinante
  4. O certificado de chave pública do verificador

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

* 1. As CRL delta constituem uma validação de integridade das CRL base
  2. AS CRL base devem ser obtidas em conjunto com as CRL delta
  3. As CRL delta devem ser consultadas a cada acesso remoto
  4. 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?

* 1. Existe uma Entidade Certificadora (CA) intermédia confiável no caminho de certificação
  2. Não é de todo possível
  3. O certificado de todas as Entidades Certificadoras (CA) intermédias ainda não expirou
  4. A data do certificado é válida

### 17. Uma cifra contínua não deve ser reutilizada com a mesma configuração inicial (IV e chave). Explique porquê

### 18. Considere a gestão de chaves públicas. Explique por que razão não é necessário consultar o serviço de OCSP a cada validação realizada.