



#MaratonaCiber2022_PUC Minas-Coração Eucarístico

Started on	Monday, 28 March 2022, 12:18 PM
State	Finished
Completed on	Monday, 28 March 2022, 12:32 PM
Time taken	13 mins 34 secs
Marks	40.00/40.00
Grade	100.00 out of 100.00

Question 1

Correct

Mark 2.00 out of 2.00

Alice e Bob usam a mesma senha para efetuar login na rede da empresa. Isto significa que os dois têm o mesmo hash exato para suas senhas. O que poderia ser implementado para impedir que os dois hashes das senhas sejam iguais?

Select one:

- ☐ gerador pseudoaleatório
- ☐ RSA
- ☒ salting
- ☐ granulação



Refer to curriculum topic: 5.1.2

Uma senha é armazenada como uma combinação de um hash e um salt.

The correct answer is: salting

Question 2

Correct

Mark 2.00 out of 2.00

Um usuário criou um novo programa e deseja distribuí-lo para todos na empresa. O usuário quer garantir que, quando o programa for baixado, não será alterado enquanto estiver em trânsito. O que o usuário pode fazer para garantir que o programa não será alterado quando for baixado?

Select one:

- ☒ Criar um hash do arquivo do programa que pode ser usado para verificar a integridade do arquivo depois que o download for feito.
- ☐ Distribuir o programa em um pen drive.
- ☐ Desativar o antivírus em todos os computadores.
- ☐ Criptografar o programa e exigir uma senha depois que o download for feito.
- ☐ Instalar o programa em computadores individuais.



Refer to curriculum topic: 5.1.1

Hash é um método para assegurar a integridade e ele garante que os dados não serão alterados.

The correct answer is: Criar um hash do arquivo do programa que pode ser usado para verificar a integridade do arquivo depois que o download for feito.

Question 3

Correct

Mark 2.00 out of 2.00

Um usuário é instruído por um chefe a encontrar um método melhor para proteger as senhas em trânsito. O usuário pesquisou vários meios para fazer isso e escolheu o uso de HMAC. Quais são os elementos principais necessários para implementar o HMAC?

Select one:

- ☐ message digest e chave assimétrica
- ☐ IPSec e soma de verificação
- ☒ chave secreta e message digest
- ☐ chave simétrica e chave assimétrica



Refer to curriculum topic: 5.1.3

A implementação de HMAC é uma chave secreta adicionada a um hash.

The correct answer is: chave secreta e message digest

Question 4

Correct

Mark 2.00 out of 2.00

Qual é o padrão para uma infraestrutura de chave pública gerenciar certificados digitais?

Select one:

- ☐ x.503
- ☐ NIST-SP800
- ☒ x.509
- ☐ PKI



Refer to curriculum topic: 5.3.2

O padrão x.509 é para uma infraestrutura PKI e x.500 é para estruturas de diretório.

The correct answer is: x.509

Question 5

Correct

Mark 2.00 out of 2.00

Qual é o processo passo a passo para criar uma assinatura digital?

Select one:

- ☐ Criar uma message digest; criptografar a digest com a chave pública do remetente e empacotar a mensagem, a síntese criptografada e a chave pública juntos para assinar o documento.
- ☐ Criar um hash de SHA-1; criptografar o hash com a chave privada do remetente e empacotar a mensagem, o hash criptografado e a chave pública juntos para o documento assinado.
- ☐ Criar uma mensagem, criptografar a mensagem com um hash MD5 e enviar o pacote com uma chave pública.
- ☒ Criar uma message digest; criptografar a digest com a chave privada do remetente e empacotar a mensagem, a digest criptografada e a chave pública juntos a fim de assinar o documento.



Refer to curriculum topic: 5.2.2

Para criar uma assinatura digital, devem ser seguidas estas etapas:

1. A mensagem e a message digest são criadas.
2. A digest e chave privada são criptografadas.
3. A mensagem, a message digest criptografada e a chave pública são empacotadas para criar o documento assinado.

The correct answer is: Criar uma message digest; criptografar a digest com a chave privada do remetente e empacotar a mensagem, a digest criptografada e a chave pública juntos a fim de assinar o documento.

Question 6

Correct

Mark 2.00 out of 2.00

Foi solicitado que um usuário implementasse o IPSec para conexões externas de entrada. O usuário planeja usar SHA-1 como parte da implementação. O usuário deseja garantir a integridade e a autenticidade da conexão. Qual ferramenta de segurança o usuário pode usar?

Select one:

- ☐ MD5
- ☐ ISAKMP
- ☒ HMAC
- ☐ SHA256



Refer to curriculum topic: 5.1.3

O HMAC fornece uma chave secreta como recurso adicional para garantir a integridade e a autenticação.

The correct answer is: HMAC

Question 7

Correct

Mark 2.00 out of 2.00

Um investigador encontra uma unidade de USB na cena do crime e quer apresentá-lo como prova no tribunal. O investigador leva a unidade de USB, cria uma imagem forense dela e leva um hash do dispositivo USB original e da imagem que foi criada. O que o investigador deseja provar sobre a unidade de USB quando a prova for apresentada no tribunal?

Select one:

- ☐ Não pode ser feita uma cópia exata de um dispositivo.
- ☐ O investigador encontrou uma unidade de USB e conseguiu fazer uma cópia dela.
- ☐ Os dados estão todos lá.
- ☒ Os dados da imagem são uma cópia exata, e nada foi alterado pelo processo.



Refer to curriculum topic: 5.1.1

Uma função hash garante a integridade de um programa, arquivo ou dispositivo.

The correct answer is: Os dados da imagem são uma cópia exata, e nada foi alterado pelo processo.

Question 8

Correct

Mark 2.00 out of 2.00

Quais são os três critérios de validação utilizados para uma regra de validação? (Escolha três.)

Select one or more:

- ✓ tamanho
- ✓ formato
- criptografia
- ✓ intervalo
- tipo
- chave



Refer to curriculum topic: 5.4.2

Os critérios utilizados em uma regra de validação incluem formato, consistência, alcance e dígito de verificação.

The correct answers are: tamanho, intervalo, formato

Question **9**

Correct

Mark 2.00 out of 2.00

Um usuário está avaliando a infraestrutura de segurança de uma empresa e percebe que alguns sistemas de autenticação não estão usando as melhores práticas relacionadas ao armazenamento de senhas. O usuário consegue decifrar senhas muito rápido e acessar dados confidenciais. O usuário deseja apresentar uma recomendação para a empresa sobre a implementação adequada de salting para evitar técnicas de violação de senha. Quais são as três melhores práticas na implementação de salting? (Escolha três.)

Select one or more:

- ☐ Salts não são uma prática recomendada eficiente. ✓
- ☒ Um salt deve ser exclusivo. ✓
- ☐ Salts devem ser curtos.
- ☒ Um salt não deve ser reutilizado. ✓
- ☐ O mesmo salt deve ser usado para cada senha.
- ☒ Um salt deve ser exclusivo para cada senha. ✓

Refer to curriculum topic: 5.1.2

O salting deve ser exclusivo e não reutilizado. Fazer o oposto fará com que senhas sejam quebradas facilmente.

The correct answers are: Um salt deve ser exclusivo para cada senha., Um salt não deve ser reutilizado., Um salt deve ser exclusivo.

Question **10**

Correct

Mark 2.00 out of 2.00

Um usuário baixa de um site um driver atualizado para uma placa de vídeo. Uma mensagem de aviso aparece na tela dizendo que o driver não é aprovado. O que está faltando nesta parte do software?

Select one:

- ☐ código fonte
- ☐ reconhecimento de código
- ☒ assinatura digital ✓
- ☐ ID válida

Refer to curriculum topic: 5.2.2

A assinatura de código é um método de verificação de integridade do código

The correct answer is: assinatura digital

Question **11**

Correct

Mark 2.00 out of 2.00

Qual das opções é um ponto forte do uso de uma função de hash?

Select one:

- ☐ Tem uma saída de tamanho variável.
- ☒ É uma função unidirecional e não reversível. ✓
- ☐ Não é usado comumente na segurança.
- ☐ Pode levar apenas uma mensagem de tamanho fixo.
- ☐ Dois arquivos diferentes podem ser criados com a mesma saída.

Refer to curriculum topic: 5.1.1

Compreender as propriedades de uma função hash mostra sua aplicabilidade como função unidirecional, tamanho de entrada arbitrária e saída fixa.

The correct answer is: É uma função unidirecional e não reversível.

Question **12**

Correct

Mark 2.00 out of 2.00

Uma violação recente em uma empresa foi atribuída à capacidade de um hacker de acessar o banco de dados corporativo por meio do site da empresa, com o uso de dados malformados em um formulário de login. Qual é o problema com o site da empresa?

Select one:

- ☐ falta de patches de sistema operacional
- ☐ nomes de usuário ruins
- ☐ criptografia fraca
- ☒ validação de entrada pobre



Refer to curriculum topic: 5.4.2

A capacidade de transmitir dados malformados através de um site é uma forma de validação de entrada pobre.

The correct answer is: validação de entrada pobre

Question **13**

Correct

Mark 2.00 out of 2.00

Quais são os três algoritmos de assinatura digital aprovados pelo NIST? (Escolha três.)

Select one or more:

- SHA1
- SHA256
- ✓ DSA
- ✓ RSA
- ✓ ECDSA
- MD5



Refer to curriculum topic: 5.2.2

O NIST escolhe algoritmos aprovados com base em técnicas de chave públicas e ECC. Os algoritmos de assinatura digital aprovados são DSA, RSA e ECDSA.

The correct answers are: DSA, RSA, ECDSA

Question **14**

Correct

Mark 2.00 out of 2.00

Qual a finalidade do CSPRNG?

Select one:

- ☐ processar buscas de hash
- ☐ impedir que um computador seja um zumbi
- ☒ gerar o salt
- ☐ proteger um site



Refer to curriculum topic: 5.1.2

O salting impede que alguém use um ataque de dicionário para adivinhar uma senha. O Gerador de Número Pseudo-Aleatório Protegido por Criptografia (CSPRNG) é uma forma (e é a melhor) de gerar o salt.

The correct answer is: gerar o salt

Question **15**

Correct

Mark 2.00 out of 2.00

Um usuário é o administrador do banco de dados de uma empresa. Foi solicitado que um usuário implementasse uma regra de integridade, que declarasse que todas as tabelas devem ter uma chave primária e que a coluna ou as colunas escolhidas como chave primária devem ser exclusivas e não nulas. Qual requisito de integridade o usuário está implementando?

Select one:

- ☐ integridade da anomalia
- ☐ integridade do domínio
- ☒ integridade da entidade
- ☐ integridade referencial



Refer to curriculum topic: 5.4.1

Existem três requisitos principais de integridade do banco de dados: entidade, referencial e integridade do domínio.

The correct answer is: integridade da entidade

Question **16**

Correct

Mark 2.00 out of 2.00

Quais são os três tipos de ataques que podem ser evitados ao utilizar salting? (Escolha três.)

Select one or more:

- ☒ tabelas de pesquisa reversa
- ☒ rainbow tables
- ☐ adivinhação
- ☐ engenharia social
- ☐ phishing
- ☒ tabelas de pesquisa
- ☐ navegação bisbilhoteira



Refer to curriculum topic: 5.1.2

O salting faz com que tabelas pré-calculadas não tenham efeito devido à sequência aleatória que é usada.

The correct answers are: tabelas de pesquisa, tabelas de pesquisa reversa, rainbow tables

Question **17**

Correct

Mark 2.00 out of 2.00

Um e-mail recente enviado para toda a empresa afirmou que haveria uma mudança na política de segurança. O oficial de segurança que acreditava-se ter enviado a mensagem afirmou que ela não foi enviada do departamento de segurança, e a empresa pode ter sido vítima de um e-mail falso. O que poderia ter sido adicionado à mensagem para garantir que ela de fato veio dessa pessoa?

Select one:

- ☐ não rejeição
- ☐ chave assimétrica
- ☒ assinatura digital
- ☐ hashing



Refer to curriculum topic: 5.2.1

As assinaturas digitais garantem a não rejeição ou a capacidade de não negar que uma pessoa específica enviou uma mensagem.

The correct answer is: assinatura digital

Question **18**

Correct

Mark 2.00 out of 2.00

Qual método tenta todas as senhas possíveis até que uma correspondência seja encontrada?

Select one:

- ☐ criptográfico
- ☐ rainbow tables
- ☒ força bruta
- ☐ data de nascimento
- ☐ nuvem
- ☐ dicionário



Refer to curriculum topic: 5.1.1

Dois métodos comuns para decifrar hashes são o dicionário e a força bruta. Depois de um tempo, o método de força bruta sempre decifrára uma senha.

The correct answer is: força bruta

Question **19**

Correct

Mark 2.00 out of 2.00

Um usuário está se conectando a um servidor de e-commerce para comprar alguns widgets para uma empresa. O usuário se conecta ao site e percebe que não há um cadeado na barra de status de segurança de navegador. O site solicita um nome de usuário e a senha e o usuário consegue fazer login. Qual é o perigo em prosseguir essa transação?

Select one:

- ☐ Um software bloqueador de anúncios está impedindo que a barra de segurança funcione corretamente, e, portanto, não há perigo com a transação.
- ☐ O certificado do site expirou, mas ele ainda é seguro.
- ☐ O usuário está usando o navegador errado para realizar a transação.
- ☒ O site não está usando um certificado digital para proteger a transação, o que significa que tudo fica não codificado.



Refer to curriculum topic: 5.3.1

O cadeado na janela do navegador garante que uma conexão segura foi estabelecida e não foi bloqueada por um complemento do navegador.

The correct answer is: O site não está usando um certificado digital para proteger a transação, o que significa que tudo fica não codificado.

Question **20**

Correct

Mark 2.00 out of 2.00

Identifique as três situações em que a função de criptografia pode ser aplicada. (Escolha três)

Select one or more:

- | | |
|---|---|
| <input checked="" type="checkbox"/> PKI | ✓ |
| <input type="checkbox"/> DES | |
| <input checked="" type="checkbox"/> IPsec | ✓ |
| <input checked="" type="checkbox"/> CHAP | ✓ |
| <input type="checkbox"/> PPOE | |
| <input type="checkbox"/> WPA | |

Refer to curriculum topic: 5.1.1

Três situações em que uma função hash pode ser usada são:

- Quando o IPSec estiver sendo usado
- Quando a autenticação por roteamento estiver ativada
- Nas respostas de desafios dentro de protocolos, como PPP CHAP
- Em contratos assinados digitalmente e certificados PKI

The correct answers are: IPsec, CHAP, PKI

[◀ Lançar Capítulo 5](#)

Jump to...

[Lançar Capítulo 6 ▶](#)

NetAcad, a Cisco Corporate Social Responsibility program, is an IT skills and career building program available to learning institutions and individuals worldwide.

[termosecondições](#)

[Privacy Statement](#)

[Cookie Policy](#)

[Data Protection](#)

[Trademarks](#)

[Data Protection](#)

[Accessibility](#)