
# Exame simulado

Edição 202203

# Conteúdo


| | |
|---|---|
| Introdução | 4 |
| Exame simulado | 5 |
| Gabarito de respostas | 16 |
| Avaliação | 35 |

# Introdução

Este é o modelo de exame de Cyber and IT Security Foundation (CISEF.PR). As regras e regulamentos do exame do EXIN se aplicam a este exame.

Este exame consiste de 40 questões de múltipla escolha. Cada questão de múltipla escolha possui um certo número de alternativas de resposta, entre as quais somente uma resposta é a correta.

O número máximo de pontos que pode ser obtido neste exame é 40. Cada resposta correta vale um ponto. Para ser aprovado você deve obter 26 pontos ou mais.

O tempo permitido para este exame simulado é de 60 minutos.

Boa Sorte!

# Exame simulado

**1 / 40**
Um hub representa o componente central, com o qual uma rede baseada em topologia em estrela pode ser construída.

Qual é o **principal** motivo pelo qual hubs quase nunca são usados?

**A)** Um hub só é capaz de reconhecer o endereço de hardware de um nó, não o endereço lógico (endereço IP). Por esse motivo, um hub não é adequado para ser usado em ambientes de rede local.
**B)** Um hub não é capaz de reconhecer nenhuma informação de endereço. Portanto, um hub envia trá fego de rede, que é destinado a um host específico, para todos os outros hosts na rede. Por esse motivo, a rede ficará sobrecarregada quando muitos hosts quiserem se comunicar.
**C)** Um hub é capaz de reconhecer o endereço de hardware de um nó, mas ignora isso e envia tráfego de rede, que é destinado a um host específico, para todos os outros hosts na rede. Por esse motivo, o trá fego de rede pode ser facilmente interceptado.
**D)** Um hub só é capaz de reconhecer o endereço lógico (endereço IP) de um nó. Por esse motivo, um hub não é adequado para ser usado em ambientes de rede local.

**2 / 40**
O ARP (Address Resolution Protocol) representa um dos mais importantes protocolos de rede em ambientes de rede baseados em TCP/IP.

O que o ARP faz, basicamente?

**A)** O ARP traduz o endereço de hardware de um nó para seu endereço IP.
**B)** O ARP responde com o endereço IP de um nó específico para qualquer nó que o solicite.
**C)** O ARP traduz o endereço IP de um nó para seu endereço de hardware.
**D)** O ARP responde com o endereço de hardware de um nó específico para o gateway padrão.

**3 / 40**
Atualmente, várias tecnologias são conectadas à Internet, por exemplo, smartphones, tablets e IoT. Portanto, o número de endereços IP públicos não será suficiente no futuro.

Com base neste cenário, qual afirmativa é correta?

**A)** IPv4 tem um espaço de endereçamento de 32 bits, o que é suficiente para o futuro.
**B)** O IPv4 com funcionalidade NAT (Tradução do Endereço da Rede) tem IP público suficiente para o futuro.
**C)** Endereços IPv6 serão suficientes somente trabalhando com endereços IPv4.
**D)** IPv6 tem um espaço de endereçamento de 128 bits, o que é suficiente para o futuro.

**4 / 40**
Qual protocolo pertence à Camada de Apresentação?

**A)** FTP
**B)** HTTP
**C)** S/MIME
**D)** SMTP

**5 / 40**
Um analista de segurança precisa realizar uma análise forense em um computador, pois esse computador foi usado para roubar informações estratégicas do servidor corporativo, que foram vendidas a um concorrente.

Qual é o componente-chave que precisa ser analisado?

**A)** Hardware
**B)** Software
**C)** Firmware
**D)** CPU

**6 / 40**
Qual família de CPUs foi desenvolvida pela Apple?

**A)** A5
**B)** Core i7
**C)** Power8
**D)** Sparc T5

**7 / 40**
Um consultor é contratado por uma empresa que deseja aconselhamento sobre como organizar e implementar o gerenciamento de patches. Ele recomenda que:

1. Os patches devem ser testados primeiro.
2. Os patches devem ser implementados o mais rápido possível após seu lançamento.

Que recomendação adicional ele deveria fazer?

**A)** Sistemas críticos devem ser corrigidos antes dos menos críticos.
**B)** Sistemas críticos e sistemas menos críticos devem ser corrigidos ao mesmo tempo.
**C)** Sistemas menos críticos devem ser corrigidos antes dos críticos.

**8 / 40**
Um Sistema de Detecção de Intrusão (IDS) pode ser usado para monitorar e filtrar o tráfego de rede.

Do ponto de vista de detecção, quais tipos **principais** de IDS podem ser identificados?

**A)** Baseado em anomalia e baseado em heurística
**B)** Baseado em anomalia e baseado em comportamento
**C)** Baseado em assinatura e baseado em conhecimento
**D)** Baseado em comportamento e baseado em conhecimento

**9 / 40**
Um sandbox representa um mecanismo bem conhecido que é usado para a execução de applets.

Qual é a **principal** função de um sandbox?

**A)** Fornece uma área de proteção para execução de código ou applet.
**B)** Fornece um ambiente de execução para o Gerenciador de segurança Java.
**C)** Garante que o malware não conseguirá sair do sandbox.
**D)** Reforça a execução de applets Java.

**10 / 40**
Um engenheiro de software está desenvolvendo um aplicativo da web, mas o gerente de segurança da informação está preocupado com os requisitos de segurança desse aplicativo.

Qual suposição feita pelo engenheiro de software está correta?

**A)** O lado do servidor de aplicação pode confiar nas informações provenientes do usuário.
**B)** A autenticação é o único controle necessário para garantir a segurança do usuário.
**C)** O certificado digital garante a segurança dos dados trocados entre cliente e servidor.
**D)** A configuração incorreta de segurança será abordada no ambiente de produção.

**11 / 40**
O Sistema de Gerenciamento de Banco de Dados Relacional é o modelo dominante de gerenciamento de banco de dados.

O que uma chave estrangeira representa ou fornece?

**A)** Representa uma coluna que identifica exclusivamente uma linha em uma tabela.
**B)** Fornece um método para integridade referencial.
**C)** Fornece um link ou referência para uma chave primária na mesma tabela.
**D)** Representa a relação entre colunas.

**12 / 40**
Após uma análise, um consultor recomenda ao cliente a implementação de um diretório de serviços para gerenciar centralmente usuários e grupos.

Qual é um exemplo de Serviços de diretório que o cliente precisará implementar?

**A)** Data Definition Language (DDL)
**B)** Directory Analysis Procedure (DAP)
**C)** Meta Data Dictionary (MDD)
**D)** Windows Active Directory (AD)

**13 / 40**
Bancos de dados são muito desafiadores de uma perspectiva de segurança. Uma das vulnerabilidades mais arriscadas é a inferência.

Como a inferência pode ser explicada?

**A)** Como a corrupção da integridade de dados por erros de dados de entrada ou processamento errôneo
**B)** Como processos executados simultaneamente, introduzindo, assim, o risco de inconsistência
**C)** Como o contorno (bypass) dos controles de segurança no front-end, a fim de acessar informações para as quais não se está autorizado
**D)** Como a dedução de informações confidenciais a partir das informações disponíveis

**14 / 40**
Os bancos de dados são importantes para o negócio, portanto, o acesso e as atividades devem ser monitorados.

Qual é o **principal** objetivo do monitoramento de Auditoria?

**A)** Determinar e proteger a quantidade de armazenamento necessária para dados de registro
**B)** Monitorar ações executadas por quem, a que horas, em qual objeto
**C)** Evitar incidentes de segurança, fornecendo tabelas de registro e auditoria
**D)** Verificar a retenção e o arquivamento de dados de registro prescritos legalmente

**15 / 40**
Uma assinatura digital é um dos métodos mais importantes para garantir a autenticidade das informações digitais.

Como uma assinatura digital é criada a partir da impressão digital (hash) das informações?

**A)** O hash é encriptado com a chave de sessão do remetente. A verificação é feita pelo receptor das informações, desencriptando a impressão digital com uma chave de sessão correspondente.
**B)** O hash é encriptado com a chave pública do remetente. A verificação é feita pelo receptor das informações, desencriptando a impressão digital com a chave privada correspondente.
**C)** O hash é encriptado com a chave privada do remetente. A verificação é feita pelo receptor das informações, desencriptando a impressão digital com a chave privada correspondente.
**D)** O hash é encriptado com a chave privada do remetente. A verificação é feita pelo receptor das informações, desencriptando a impressão digital com a chave pública correspondente.

**16 / 40**
Referindo-se às cifras de substituição famosas, como a Cifra de César, qual é o resultado da palavra “SECURITY” criptografada através do esquema a seguir?

ESQUEMA:
A = 1, B = R, C = @, D = /, E = T, I = (, R = !, S = 5, T = -, U = &, Y = X

**A)** 5T@&!(-X
**B)** 5T@-!(-@
**C)** ST@&!@-X
**D)** 5E@&!(@X

**17 / 40**
Um administrador de rede enviou uma mensagem assinada com sua chave privada.

Qual das opções a seguir é correta?

**A)** A origem dessa mensagem pode ser garantida porque ela foi assinada com a chave privada do remetente.
**B)** A origem desta mensagem pode ser garantida se ele usar o algoritmo AES antes de enviar esta mensagem.
**C)** A origem desta mensagem pode ser garantida se ele usar o algoritmo SHA-2 antes de enviar esta mensagem.
**D)** A origem dessa mensagem não pode ser garantida, porque ela foi assinada somente com uma chave privada.

**18 / 40**
Uma organização governamental deseja garantir a integridade das informações comunicadas entre as partes.

O que é necessário para conseguir isso?

**A)** Encriptação assimétrica
**B)** Encriptação simétrica
**C)** Hashing e encriptação simétrica
**D)** Hashing e encriptação assimétrica

**19 / 40**
A Infraestrutura de Chave Pública (PKI) consiste em hardware, software, protocolos, procedimentos, políticas e padrões para gerenciar a criação, a administração, a distribuição e a revogação dos certificados digitais e chaves.

Qual é o objetivo de uma Lista de Revogação de Certificados (CRL)?

**A)** A CRL apresenta certificados apenas com uma data de validade expirada.
**B)** Revogar, de forma irreversível ou temporária, os certificados que não são mais válidos ou que possuem comprometimento de chave.
**C)** Revogar, irreversivelmente, os certificados que não são mais válidos.
**D)** Revogar, temporariamente, os certificados que não são mais válidos.

**20 / 40**
Certificados digitais representam um componente importante em qualquer Infraestrutura de Chave Pública (PKI).

O que **nunca** deve ser incluído em um certificado digital?

**A)** A assinatura digital da Autoridade de Certificação (CA) que emitiu o certificado digital
**B)** A chave privada da parte à qual o certificado digital está vinculado
**C)** A identidade da parte que possui o certificado digital
**D)** A data inicial e final do período no qual o certificado digital é válido

**21 / 40**
Um canal seguro foi estabelecido entre dois hosts usando Transport Layer Security (TLS) versão 1.2.

Em relação a essa TLS, qual das afirmações a seguir está correta?

**A)** TLS é baseada em criptografia de chave assimétrica e opera somente na Camada de Transporte OSI.
**B)** TLS fornece encriptação e autenticação de dados, e é baseada em criptografia de chave assimétrica.
**C)** TLS fornece encriptação e autenticação de dados, e é baseada em criptografia de chave simétrica.
**D)** TLS fornece encriptação de dados, é baseada em criptografia de chave simétrica e opera somente na camada de transporte.

**22 / 40**
A especificação de segurança IPSec fornece vários métodos de implementação.

Para que finalidade e como o modo de túnel IPSec é usado?

**A)** Para proteção de uma ponta a outra. Somente a carga útil (Payload) do IP é protegida.
**B)** Para proteção de link. Somente a carga útil (Payload) do IP é protegida.
**C)** Para proteção de uma ponta a outra. Tanto a carga útil (Payload) do IP quanto o cabeçalho do IP são protegidos.
**D)** Para proteção de link. Tanto a carga útil (Payload) do IP quanto o cabeçalho do IP são protegidos.

**23 / 40**
O que Security Assertion Markup Language (SAML) oferece?

**A)** Autenticar usuários em ambientes corporativos
**B)** Autenticar usuários e aplicativos em ambientes corporativos
**C)** Usar redes sociais para autenticação (“Use sua conta do Facebook para fazer login”)
**D)** Trocar segura de informações de autenticação em um ambiente federado

**24 / 40**
A biometria se torna cada vez mais importante como meio de verificar a identidade de usuários.

Qual recurso da biometria representa uma das **principais** considerações para as organizações que desejam implementá-la?

**A)** A chamada taxa de cruzamento de erros, que é a taxa na qual os erros de aceitação e de rejeição são equivalentes.
**B)** A maneira como os usuários deslizam em seu tablet ou smartphone pode ser usada como um mecanismo comportamental para biometria.
**C)** A chamada taxa de cruzamento de erros, que é a taxa na qual os erros de aceitação e de rejeição estão dentro dos níveis aceitáveis.
**D)** O reconhecimento facial não pode ser usado como um mecanismo biométrico, porque é muito impreciso.

**25 / 40**
Muitas organizações buscam o Single sign-on (SSO) para seus usuários.

O que é **mais** importante considerar ao implementar o SSO?

**A)** Ao introduzir um conjunto de credenciais para todos os aplicativos, um cibercriminoso pode, ao obter as credenciais, conseguir acesso a todos os aplicativos de uma só vez.
**B)** O Enterprise wide Single sign-on (ESSO – sign-on único para toda a empresa) não é possível devido à diversidade de aplicativos existentes dentro da maioria das organizações.
**C)** Sistemas com Enterprise Single Sign-on (ESSO) são muito caros para aplicações web. Como a maioria dos aplicativos é baseada na web, não existe caso de negócio para ESSO.
**D)** O Single sign-on (SSO) usa um conjunto de credenciais que dão acesso a todos os aplicativos de uma só vez. Consequentemente, essas credenciais devem ser totalmente protegidas.

**26 / 40**
O que um invasor consegue fazer quando um único valor de salt é usado para todas as senhas em um banco de dados?

**A)** Adicionar o salt novamente e obter os valores de texto simples.
**B)** Remover os primeiros caracteres do hash para ignorar os salts.
**C)** Remover o salt e desencriptar as senhas.
**D)** Usar o mesmo salt e criar um banco de dados de senhas e seus valores de hash.

**27 / 40**
No contexto de autorização, o princípio da “necessidade de saber” (need-to-know) é um dos mais importantes a considerar.

O que significa o princípio da “necessidade de saber”?

**A)** As tarefas críticas só podem ser realizadas por pelo menos dois indivíduos, de modo que é necessário um conluio para poder cometer fraudes.
**B)** Os usuários devem ter um nível mínimo de direitos de acesso atribuído a eles para desempenhar suas tarefas.
**C)** Os usuários devem ter acesso apenas às informações necessárias para desempenhar suas tarefas.
**D)** Os usuários devem ter apenas direitos de acesso temporários atribuídos a eles para desempenhar suas tarefas.

**28 / 40**
Quantas partes (no mínimo) desempenham um papel em um fluxo de dados de autenticação do OpenID Connect?

**A)** 2
**B)** 3
**C)** 4
**D)** 5

**29 / 40**
Uma organização **não** está disposta a compartilhar nenhum recurso.

Que modelo de implantação na Computação em Nuvem representa o mais seguro?

**A)** Nuvem comunitária
**B)** Nuvem híbrida
**C)** Nuvem privada
**D)** Nuvem pública

**30 / 40**
Qual afirmação é verdadeira sobre a nuvem pública?

**A)** Partes são usadas por uma única organização e partes são usadas por um grupo de organizações.
**B)** É usada por uma única organização.
**C)** É usada por um pequeno grupo de organizações com interesses compartilhados.
**D)** É usada por qualquer organização que deseje utilizá-la.

**31 / 40**
Identidade como um Serviço (IDaaS) é um dos modelos de serviço emergentes na Computação em Nuvem.

O que IDaaS fornece?

**A)** Governança de identidade e autenticação para usuários internos
**B)** Governança de identidade e autenticação para clientes, parceiros de negócios e outros usuários externos
**C)** Governança de identidade e autenticação para usuários internos e externos
**D)** Single sign-on (SSO) para usuários externos

**32 / 40**
Uma organização deseja hospedar um serviço de web, mas não deseja lidar com a compra e manutenção de hardware, nem manter o sistema operacional atualizado.

Que tipo de modelo de serviço ela deve solicitar?

**A)** IaaS
**B)** PaaS
**C)** SaaS
**D)** SECaaS

**33 / 40**
Há sempre um risco quando um provedor de nuvem que fornece uma solução como SaaS ou PaaS fecha ou vai à falência.

Qual é esse risco para a empresa que usa essa solução de nuvem?

**A)** Risco de continuidade
**B)** Risco de jurisdição
**C)** Risco legal
**D)** Risco de armazenamento

**34 / 40**
Por que o CEO de uma empresa desejaria transferir os principais sistemas corporativos para a nuvem?

**A)** Para reduzir o custo com tecnologia
**B)** Para reduzir o vazamento de informações confidenciais
**C)** Para reduzir vulnerabilidades de segurança
**D)** Para reduzir o acesso não autorizado às informações dos clientes

**35 / 40**
Engenharia social é um dos métodos de ataque de cibercriminosos **mais** bem-sucedidos.

O que é considerado como uma forma de engenharia social?

**A)** Criptoware
**B)** Ataque de Negação de Serviço (DoS)
**C)** Phishing
**D)** Spam

**36 / 40**
Há quatro categorias principais de ataque quando se trata de explorar vulnerabilidades.

Qual **não** é uma das quatro principais categorias de ataque?

**A)** Invasão completa
**B)** Roubo ou revelação de informações
**C)** Uso indevido por insider

**37 / 40**
Certo tipo de invasor sabe como escrever exploits, usa engenharia social para obter informações sobre seu alvo e coleta dados. Os motivos do invasor não são claros, e o invasor nem sempre é malicioso.

Que tipo de invasor é esse?

**A)** Black Hat Hacker
**B)** Gray Hat Hacker
**C)** Hacktivista
**D)** White Hat Hacker

**38 / 40**
Qual ferramenta representa uma ferramenta de varredura?

**A)** Nessus
**B)** John the Ripper
**C)** Metasploit
**D)** Ophcrack

**39 / 40**
Hackers e cibercriminosos geralmente realizam suas atividades seguindo um plano bem estruturado.

Qual é a **melhor** ordem em que essas atividades são realizadas dentro de um plano bem estruturado?

**A)** Enumeração, footprinting, obtenção de acesso, escalonamento de privilégios, apagamento de rastros
**B)** Reconhecimento, enumeração, obtenção de acesso, escalonamento de privilégios, apagamento de rastros
**C)** Reconhecimento, varredura, obtenção de acesso, escalonamento de privilégios, manutenção de acesso
**D)** Varredura, enumeração, obtenção de acesso, escalonamento de privilégios, manutenção de acesso

**40 / 40**
Um hacker obteve acesso a um servidor de web usando um plano passo a passo pensado cautelosamente.

Que passo que ele deu imediatamente após “Invasão e acesso”?

**A)** Impressões digitais
**B)** Escalonamento de privilégios
**C)** Reconhecimento
**D)** Avaliação de vulnerabilidade

# Gabarito de respostas

**1 / 40**
Um hub representa o componente central, com o qual uma rede baseada em topologia em estrela pode ser construída.

Qual é o **principal** motivo pelo qual hubs quase nunca são usados?

**A)** Um hub só é capaz de reconhecer o endereço de hardware de um nó, não o endereço lógico (endereço IP). Por esse motivo, um hub não é adequado para ser usado em ambientes de rede local.
**B)** Um hub não é capaz de reconhecer nenhuma informação de endereço. Portanto, um hub envia trá fego de rede, que é destinado a um host específico, para todos os outros hosts na rede. Por esse motivo, a rede ficará sobrecarregada quando muitos hosts quiserem se comunicar.
**C)** Um hub é capaz de reconhecer o endereço de hardware de um nó, mas ignora isso e envia tráfego de rede, que é destinado a um host específico, para todos os outros hosts na rede. Por esse motivo, o trá fego de rede pode ser facilmente interceptado.
**D)** Um hub só é capaz de reconhecer o endereço lógico (endereço IP) de um nó. Por esse motivo, um hub não é adequado para ser usado em ambientes de rede local.

**A)** Incorreto. Um hub não é capaz de lidar com nenhuma informação de endereço (lógico/de hardware).
**B)** Correto. Um hub só é capaz de encaminhar pacotes de dados, sem reconhecer nenhuma informação de endereço nele. *Fundamentals of Information Systems Security, Capítulo 10: Local Area Networks*
**C)** Incorreto. Um hub não é capaz de lidar com nenhuma informação de endereço (lógico/de hardware).
**D)** Incorreto. Um hub não é capaz de lidar com nenhuma informação de endereço (lógico/de hardware).

**2 / 40**
O ARP (Address Resolution Protocol) representa um dos mais importantes protocolos de rede em ambientes de rede baseados em TCP/IP.

O que o ARP faz, basicamente?

**A)** O ARP traduz o endereço de hardware de um nó para seu endereço IP.
**B)** O ARP responde com o endereço IP de um nó específico para qualquer nó que o solicite.
**C)** O ARP traduz o endereço IP de um nó para seu endereço de hardware.
**D)** O ARP responde com o endereço de hardware de um nó específico para o gateway padrão.

**A)** Incorreto. O ARP é usado para transmitir a pergunta “quem tem ?”. O host com o endereço IP correto responderá com seu endereço de hardware (MAC).
**B)** Incorreto. O ARP é usado para transmitir a pergunta “quem tem ?”. O host com o endereço IP correto responderá com seu endereço de hardware (MAC).
**C)** Correto. Um host que deseja saber o endereço de hardware de outro host envia uma transmissão ARP no domínio de broadcast da rede dizendo “quem tem ? Diz ”. O host com o endereço IP correto responde com seu endereço de hardware. *Fundamentals of Information Systems Security, Capítulo 3: IP Address Spoofing*
**D)** Incorreto. O ARP é usado para transmitir a pergunta “quem tem ?”. O host com o endereço IP correto responderá com seu endereço de hardware (MAC).

**3 / 40**
Atualmente, várias tecnologias são conectadas à Internet, por exemplo, smartphones, tablets e IoT. Portanto, o número de endereços IP públicos não será suficiente no futuro.

Com base neste cenário, qual afirmativa é correta?

**A)** IPv4 tem um espaço de endereçamento de 32 bits, o que é suficiente para o futuro.
**B)** O IPv4 com funcionalidade NAT (Tradução do Endereço da Rede) tem IP público suficiente para o futuro.
**C)** Endereços IPv6 serão suficientes somente trabalhando com endereços IPv4.
**D)** IPv6 tem um espaço de endereçamento de 128 bits, o que é suficiente para o futuro.

**A)** Incorreto. IPv4 tem mais de 4 bilhões de endereços, mas isso não é suficiente para o futuro.
**B)** Incorreto. IPv4 tem mais de 4 bilhões de endereços, mas isso não é suficiente para o futuro, mesmo com o uso de NAT.
**C)** Incorreto. IPv6 é suficiente, não é necessário usar endereços IPv4.
**D)** Correto. IPv6 tem mais de 6 * 1023 endereços, o que será suficiente para as próximas décadas.
*Fundamentals of Information Systems Security, Capítulo 10: IP Addressing*

**4 / 40**
Qual protocolo pertence à Camada de Apresentação?

**A)** FTP
**B)** HTTP
**C)** S/MIME
**D)** SMTP

**A)** Incorreto. FTP pertence à Camada de Aplicativo.
**B)** Incorreto. HTTP pertence à Camada de Aplicativo.
**C)** Correto. S/MIME pertence à Camada de Apresentação.
**D)** Incorreto. SMTP pertence à Camada de Aplicativo.

**5 / 40**
Um analista de segurança precisa realizar uma análise forense em um computador, pois esse computador foi usado para roubar informações estratégicas do servidor corporativo, que foram vendidas a um concorrente.

Qual é o componente-chave que precisa ser analisado?

**A)** Hardware
**B)** Software
**C)** Firmware
**D)** CPU

**A)** Incorreto. A opção correta é o software, não o hardware.
**B)** Correto. Ele precisa analisar o sistema operacional, procurando evidências de informações roubadas.
**C)** Incorreto. A opção correta é o software, não o firmware.
**D)** Incorreto. A opção correta é o software, não a CPU.

**6 / 40**
Qual família de CPUs foi desenvolvida pela Apple?

**A)** A5
**B)** Core i7
**C)** Power8
**D)** Sparc T5

**A)** Correto. A5 foi desenvolvida pela Apple.
**B)** Incorreto. Core i7 é uma série específica de processadores Intel.
**C)** Incorreto. O Power8 foi desenvolvida pela IBM.
**D)** Incorreto. O Sparc T5 foi desenvolvida pela Oracle (anteriormente SUN Microsystems).

**7 / 40**
Um consultor é contratado por uma empresa que deseja aconselhamento sobre como organizar e implementar o gerenciamento de patches. Ele recomenda que:

1. Os patches devem ser testados primeiro.
2. Os patches devem ser implementados o mais rápido possível após seu lançamento.

Que recomendação adicional ele deveria fazer?

**A)** Sistemas críticos devem ser corrigidos antes dos menos críticos.
**B)** Sistemas críticos e sistemas menos críticos devem ser corrigidos ao mesmo tempo.
**C)** Sistemas menos críticos devem ser corrigidos antes dos críticos.

**A)** Incorreto. Como patches podem afetar um sistema de maneira negativa, sistemas menos críticos devem ser corrigidos primeiro para ver se o patch causa danos.
**B)** Incorreto. Como patches podem afetar um sistema de maneira negativa, sistemas menos críticos devem ser corrigidos primeiro para ver se o patch causa danos.
**C)** Correto. Como patches podem afetar um sistema de maneira negativa, sistemas menos críticos devem ser corrigidos primeiro para ver se o patch causa danos. *Fundamentals of Information Systems Security, Capítulo 6: Configuration Management*

**8 / 40**
Um Sistema de Detecção de Intrusão (IDS) pode ser usado para monitorar e filtrar o tráfego de rede.

Do ponto de vista de detecção, quais tipos **principais** de IDS podem ser identificados?

**A)** Baseado em anomalia e baseado em heurística
**B)** Baseado em anomalia e baseado em comportamento
**C)** Baseado em assinatura e baseado em conhecimento
**D)** Baseado em comportamento e baseado em conhecimento

**A)** Incorreto. Baseado em heurística não é uma característica de um IDS.
**B)** Incorreto. Baseado em anomalia e baseado em comportamento são sinônimos.
**C)** Incorreto. Baseado em assinatura e baseado em conhecimento são sinônimos.
**D)** Correto. Um IDS baseado em comportamento (também chamado de baseado em anomalia) é capaz de detectar desvios na quantidade e direção do tráfego e não conformidade a protocolos e convenções. O outro tipo é o IDS baseado em conhecimento (também chamado de baseado em assinatura), que compara o tráfego de rede com as informações em seu banco de dados com assinaturas de tráfego de rede malicioso. *Fundamentals of Information Systems Security, Capítulo 7: How to Verify Security Controls*

**9 / 40**
Um sandbox representa um mecanismo bem conhecido que é usado para a execução de applets.

Qual é a **principal** função de um sandbox?

**A)** Fornece uma área de proteção para execução de código ou applet.
**B)** Fornece um ambiente de execução para o Gerenciador de segurança Java.
**C)** Garante que o malware não conseguirá sair do sandbox.
**D)** Reforça a execução de applets Java.

**A)** Correto. Um sandbox é um ambiente virtualizado para a execução de códigos ou applets.
**B)** Incorreto. O Gerenciador de segurança Java é um exemplo de sandbox.
**C)** Incorreto. Um sandbox fornece uma área de proteção para a execução de applets.
**D)** Incorreto. Um sandbox impõe quantidades limitadas de recursos de memória e processador.

**10 / 40**
Um engenheiro de software está desenvolvendo um aplicativo da web, mas o gerente de segurança da informação está preocupado com os requisitos de segurança desse aplicativo.

Qual suposição feita pelo engenheiro de software está correta?

**A)** O lado do servidor de aplicação pode confiar nas informações provenientes do usuário.
**B)** A autenticação é o único controle necessário para garantir a segurança do usuário.
**C)** O certificado digital garante a segurança dos dados trocados entre cliente e servidor.
**D)** A configuração incorreta de segurança será abordada no ambiente de produção.

**A)** Incorreto. Os dados de entrada do usuário não são confiáveis, todos os controles de segurança devem ser feitos no lado do servidor.
**B)** Incorreto. Autorização e gerenciamento de sessão são outros controles importantes para garantir a segurança do usuário.
**C)** Correto. O certificado digital (protocolo HTTPS) garante que o tráfego seja seguro.
**D)** Incorreto. A configuração incorreta de segurança deve ser abordada no ambiente de GQ.

**11 / 40**
O Sistema de Gerenciamento de Banco de Dados Relacional é o modelo dominante de gerenciamento de banco de dados.

O que uma chave estrangeira representa ou fornece?

**A)** Representa uma coluna que identifica exclusivamente uma linha em uma tabela.
**B)** Fornece um método para integridade referencial.
**C)** Fornece um link ou referência para uma chave primária na mesma tabela.
**D)** Representa a relação entre colunas.

**A)** Incorreto. Esta é a definição de uma chave primária.
**B)** Correto. Uma chave estrangeira fornece um link para uma chave primária em outra tabela, fornecendo, assim, integridade referencial.
**C)** Incorreto. Uma chave estrangeira também pode fazer link com uma chave primária em outras tabelas.
**D)** Incorreto. Um registro representa uma relação entre colunas.

**12 / 40**
Após uma análise, um consultor recomenda ao cliente a implementação de um diretório de serviços para gerenciar centralmente usuários e grupos.

Qual é um exemplo de Serviços de diretório que o cliente precisará implementar?

**A)** Data Definition Language (DDL)
**B)** Directory Analysis Procedure (DAP)
**C)** Meta Data Dictionary (MDD)
**D)** Windows Active Directory (AD)

**A)** Incorreto. DDL descreve um modelo de dados em um banco de dados.
**B)** Incorreto. DAP significa Directory Access Protocol (Protocolo de Acesso ao Diretório).
**C)** Incorreto. Um MDD não existe, apenas um Dicionário de Dados ou Metadados em bancos de dados.
**D)** Correto. AD é um exemplo de serviços de diretório, baseado em X.500.

**13 / 40**
Bancos de dados são muito desafiadores de uma perspectiva de segurança. Uma das vulnerabilidades mais arriscadas é a inferência.

Como a inferência pode ser explicada?

**A)** Como a corrupção da integridade de dados por erros de dados de entrada ou processamento errôneo
**B)** Como processos executados simultaneamente, introduzindo, assim, o risco de inconsistência
**C)** Como o contorno (bypass) dos controles de segurança no front-end, a fim de acessar informações para as quais não se está autorizado
**D)** Como a dedução de informações confidenciais a partir das informações disponíveis

**A)** Incorreto. Inferência é definida como a dedução de informações confidenciais a partir das informações disponíveis.
**B)** Incorreto. Inferência é definida como a dedução de informações confidenciais a partir das informações disponíveis.
**C)** Incorreto. Inferência é definida como a dedução de informações confidenciais a partir das informações disponíveis.
**D)** Correto. Inferência pode ser explicada como a dedução de informações confidenciais a partir de informações agregadas de fontes públicas.

**14 / 40**
Os bancos de dados são importantes para o negócio, portanto, o acesso e as atividades devem ser monitorados.

Qual é o **principal** objetivo do monitoramento de Auditoria?

**A)** Determinar e proteger a quantidade de armazenamento necessária para dados de registro
**B)** Monitorar ações executadas por quem, a que horas, em qual objeto
**C)** Evitar incidentes de segurança, fornecendo tabelas de registro e auditoria
**D)** Verificar a retenção e o arquivamento de dados de registro prescritos legalmente

**A)** Incorreto. Determinar a quantidade mínima ou máxima de dados de registro continua sendo um desafio.
**B)** Correto. O monitoramento de Auditoria pode acompanhar os incidentes de segurança ocorridos. *Fundamentals of Information Systems Security, Capítulo 5: Policies and Procedures for Accountability*
**C)** Incorreto. O monitoramento de Auditoria é uma medida reativa, e não pode evitar incidentes de segurança.
**D)** Incorreto. O monitoramento de Auditoria pode verificar somente a conformação a termos legais.

**15 / 40**
Uma assinatura digital é um dos métodos mais importantes para garantir a autenticidade das informações digitais.

Como uma assinatura digital é criada a partir da impressão digital (hash) das informações?

**A)** O hash é encriptado com a chave de sessão do remetente. A verificação é feita pelo receptor das informações, desencriptando a impressão digital com uma chave de sessão correspondente.
**B)** O hash é encriptado com a chave pública do remetente. A verificação é feita pelo receptor das informações, desencriptando a impressão digital com a chave privada correspondente.
**C)** O hash é encriptado com a chave privada do remetente. A verificação é feita pelo receptor das informações, desencriptando a impressão digital com a chave privada correspondente.
**D)** O hash é encriptado com a chave privada do remetente. A verificação é feita pelo receptor das informações, desencriptando a impressão digital com a chave pública correspondente.

**A)** Incorreto. A encriptação do hash deve ser feita com a chave privada do remetente e verificada com a chave pública do remetente. Veja a Pasta de trabalho ITSF, capítulo Assinaturas digitais.
**B)** Incorreto. A encriptação do hash deve ser feita com a chave privada do remetente e verificada com a chave pública do remetente. Veja a Pasta de trabalho ITSF, capítulo Assinaturas digitais.
**C)** Incorreto. A encriptação do hash deve ser feita com a chave privada do remetente e verificada com a chave pública do remetente. Veja a Pasta de trabalho ITSF, capítulo Assinaturas digitais.
**D)** Correto. A encriptação do hash deve ser feita com a chave privada do remetente e verificada com a chave pública do remetente. *Fundamentals of Information Systems Security, Capítulo 9: Digital Signatures and Hash Functions*

**16 / 40**
Referindo-se às cifras de substituição famosas, como a Cifra de César, qual é o resultado da palavra “SECURITY” criptografada através do esquema a seguir?

ESQUEMA:
A = 1, B = R, C = @, D = /, E = T, I = (, R = !, S = 5, T = -, U = &, Y = X

**A)** 5T@&!(-X
**B)** 5T@-!(-@
**C)** ST@&!@-X
**D)** 5E@&!(@X

**A)** Correto. Envolve o processo simples de substituir um caractere por outro, baseado em uma variável de criptografia. *Fundamentals of Information Systems Security, Capítulo 9: Types of Ciphers*
**B)** Incorreto. Porque U = & e Y = X.
**C)** Incorreto. Porque I = ( e S = 5.
**D)** Incorreto. Porque E = T e T = -.

**17 / 40**
Um administrador de rede enviou uma mensagem assinada com sua chave privada.

Qual das opções a seguir é correta?

**A)** A origem dessa mensagem pode ser garantida porque ela foi assinada com a chave privada do remetente.
**B)** A origem desta mensagem pode ser garantida se ele usar o algoritmo AES antes de enviar esta mensagem.
**C)** A origem desta mensagem pode ser garantida se ele usar o algoritmo SHA-2 antes de enviar esta mensagem.
**D)** A origem dessa mensagem não pode ser garantida, porque ela foi assinada somente com uma chave privada.

**A)** Correto. Podemos garantir que a mensagem seja confiável, porque ela foi assinada com uma chave privada, o que garante o não repúdio. *Fundamentals of Information Systems Security, Capítulo 9: Digital Signatures and Hash Functions*
**B)** Incorreto. Não é necessário usar uma encriptação simétrica para garantir o não repúdio.
**C)** Incorreto. Não é necessário usar outras funções hash, porque a integridade da mensagem é garantida pela chave privada.
**D)** Incorreto. A mensagem foi assinada com uma chave privada, o que garante o não repúdio.

**18 / 40**
Uma organização governamental deseja garantir a integridade das informações comunicadas entre as partes.

O que é necessário para conseguir isso?

**A)** Encriptação assimétrica
**B)** Encriptação simétrica
**C)** Hashing e encriptação simétrica
**D)** Hashing e encriptação assimétrica

**A)** Incorreto. Além da Encriptação assimétrica, também é necessário hashing para garantir a integridade das informações.
**B)** Incorreto. Somente encriptação assimétrica pode ser usada para criar uma assinatura digital. A encriptação do hash deve ser feita com a chave privada do remetente e verificada com a chave pú blica do remetente.
**C)** Incorreto. Somente encriptação assimétrica pode ser usada para criar uma assinatura digital. A encriptação do hash deve ser feita com a chave privada do remetente e verificada com a chave pú blica do remetente.
**D)** Correto. O remetente deve criar um hash das informações, encriptar o hash com sua chave privada e enviar o hash para o destinatário, junto com as informações. O receptor pode verificar a autenticidade das informações, desencriptando o hash com a chave pública do remetente. Posteriormente, a integridade pode ser verificada, criando-se um segundo hash. Se os dois hashes coincidirem, a integridade das informações foi preservada. *Fundamentals of Information Systems Security, Capítulo 9: Symmetric and Asymmetric Key Cryptography and Digital Signatures and Hash Functions*

**19 / 40**
A Infraestrutura de Chave Pública (PKI) consiste em hardware, software, protocolos, procedimentos, políticas e padrões para gerenciar a criação, a administração, a distribuição e a revogação dos certificados digitais e chaves.

Qual é o objetivo de uma Lista de Revogação de Certificados (CRL)?

**A)** A CRL apresenta certificados apenas com uma data de validade expirada.
**B)** Revogar, de forma irreversível ou temporária, os certificados que não são mais válidos ou que possuem comprometimento de chave.
**C)** Revogar, irreversivelmente, os certificados que não são mais válidos.
**D)** Revogar, temporariamente, os certificados que não são mais válidos.

**A)** Incorreto. A CRL apresenta todos os certificados que não são mais válidos, com base nos incidentes com o certificado ou em uma data de validade expirada.
**B)** Correto. A CRL é responsável pela revogação de certificados que não são mais válidos, irreversivelmente se uma chave privada foi comprometida ou a data de validade expirou, e temporariamente se um usuário não tiver certeza se a chave privada foi perdida ou comprometida. *Fundamentals of Information Systems Security, Capítulo 9: Cryptographic Applications and Uses in Information System Security*
**C)** Incorreto. A CRL é responsável por revogar, de forma irreversível ou temporária, certificados que não são mais válidos.
**D)** Incorreto. A CRL é responsável por revogar, de forma irreversível ou temporária, certificados que não são mais válidos.

**20 / 40**
Certificados digitais representam um componente importante em qualquer Infraestrutura de Chave Pública (PKI).

O que **nunca** deve ser incluído em um certificado digital?

**A)** A assinatura digital da Autoridade de Certificação (CA) que emitiu o certificado digital
**B)** A chave privada da parte à qual o certificado digital está vinculado
**C)** A identidade da parte que possui o certificado digital
**D)** A data inicial e final do período no qual o certificado digital é válido

**A)** Incorreto. A assinatura digital da Autoridade de Certificação (CA) é vital para confiar no certificado.
**B)** Correto. A chave privada deve ser mantida em segredo em todos os momentos e, portanto, não deve ser publicada em um certificado digital. Em vez disso, a chave pública é publicada com o certificado digital. *Fundamentals of Information Systems Security, Capítulo 9: Cryptographic Applications and Uses in Information System Security*
**C)** Incorreto. A identidade da parte que possui o certificado digital é necessária para confiar no certificado.
**D)** Incorreto. O período no qual o certificado digital é válido é vital para confiar no certificado.

**21 / 40**
Um canal seguro foi estabelecido entre dois hosts usando Transport Layer Security (TLS) versão 1.2.

Em relação a essa TLS, qual das afirmações a seguir está correta?

**A)** TLS é baseada em criptografia de chave assimétrica e opera somente na Camada de Transporte OSI.
**B)** TLS fornece encriptação e autenticação de dados, e é baseada em criptografia de chave assimétrica.
**C)** TLS fornece encriptação e autenticação de dados, e é baseada em criptografia de chave simétrica.
**D)** TLS fornece encriptação de dados, é baseada em criptografia de chave simétrica e opera somente na camada de transporte.

**A)** Incorreto. TLS opera na camada de Transporte OSI, Sessão, Apresentação e Aplicativo.
**B)** Correto. TLS é um protocolo que protege a comunicação, como HTTPS, SMTP e outros, e é baseado em uma chave assimétrica. *Fundamentals of Information Systems Security, Capítulo 10: O Modelo de Referência OSI*
**C)** Incorreto. TLS é baseada em criptografia de chave assimétrica.
**D)** Incorreto. TLS é baseada em uma chave assimétrica e opera na camada de Transporte OSI, Sessão, Apresentação e Aplicativo.

**22 / 40**
A especificação de segurança IPSec fornece vários métodos de implementação.

Para que finalidade e como o modo de túnel IPSec é usado?

**A)** Para proteção de uma ponta a outra. Somente a carga útil (Payload) do IP é protegida.
**B)** Para proteção de link. Somente a carga útil (Payload) do IP é protegida.
**C)** Para proteção de uma ponta a outra. Tanto a carga útil (Payload) do IP quanto o cabeçalho do IP são protegidos.
**D)** Para proteção de link. Tanto a carga útil (Payload) do IP quanto o cabeçalho do IP são protegidos.

**A)** Incorreto. O modo de túnel IPSec é usado para proteger links e fornece encriptação de cabeçalho do IP e de carga do IP (Payload).
**B)** Incorreto. O modo de túnel IPSec é usado para proteger links e fornece encriptação de cabeçalho do IP e de carga do IP (Payload).
**C)** Incorreto. O modo de túnel IPSec é usado para proteger links e fornece encriptação de cabeçalho do IP e de carga do IP (Payload).
**D)** Correto. Com o modo de túnel IPSec, a carga útil do IP (Payload) é protegida (como em todos os modos). Além disso, as informações do cabeçalho do IP original também são protegidas. Um cabeçalho de IP alternativo com as informações do endereço IP do ponto final do túnel é colocado antes do pacote encriptado. *Fundamentals of Information Systems Security, Capítulo 9: Principles of Certificates and Key Management*

**23 / 40**
O que Security Assertion Markup Language (SAML) oferece?

**A)** Autenticar usuários em ambientes corporativos
**B)** Autenticar usuários e aplicativos em ambientes corporativos
**C)** Usar redes sociais para autenticação (“Use sua conta do Facebook para fazer login”)
**D)** Trocar segura de informações de autenticação em um ambiente federado

**A)** Incorreto. SAML é um padrão baseado em XML usado para trocar informações de autenticação e autorização.
**B)** Incorreto. SAML é um padrão baseado em XML usado para trocar informações de autenticação e autorização.
**C)** Incorreto. SAML é um padrão baseado em XML usado para trocar informações de autenticação e autorização.
**D)** Correto. SAML é usado para trocar informações de autenticação (chamadas de afirmações – assertions) em um ambiente federado. *Fundamentals of Information Systems Security, Capítulo: Centralized and Decentralized Access Control*

**24 / 40**
A biometria se torna cada vez mais importante como meio de verificar a identidade de usuários.

Qual recurso da biometria representa uma das **principais** considerações para as organizações que desejam implementá-la?

**A)** A chamada taxa de cruzamento de erros, que é a taxa na qual os erros de aceitação e de rejeição são equivalentes.
**B)** A maneira como os usuários deslizam em seu tablet ou smartphone pode ser usada como um mecanismo comportamental para biometria.
**C)** A chamada taxa de cruzamento de erros, que é a taxa na qual os erros de aceitação e de rejeição estão dentro dos níveis aceitáveis.
**D)** O reconhecimento facial não pode ser usado como um mecanismo biométrico, porque é muito impreciso.

**A)** Correto. Com a biometria deve haver um equilíbrio entre os erros de aceitação e de rejeição. *Fundamentals of Information Systems Security, Capítulo 5: Processes and Requirements for Authentication*
**B)** Incorreto. Que um método biométrico como a dinâmica swype possa ser usado não é uma consideração de segurança.
**C)** Incorreto. A taxa de cruzamento de erros é a taxa na qual os erros de aceitação e de rejeição são equivalentes.
**D)** Incorreto. O reconhecimento facial não é o método biométrico mais preciso, mas ainda pode ser usado se os falsos erros de aceitação forem menos importantes que os falsos erros de rejeição.

**25 / 40**
Muitas organizações buscam o Single sign-on (SSO) para seus usuários.

O que é **mais** importante considerar ao implementar o SSO?

**A)** Ao introduzir um conjunto de credenciais para todos os aplicativos, um cibercriminoso pode, ao obter as credenciais, conseguir acesso a todos os aplicativos de uma só vez.
**B)** O Enterprise wide Single sign-on (ESSO – sign-on único para toda a empresa) não é possível devido à diversidade de aplicativos existentes dentro da maioria das organizações.
**C)** Sistemas com Enterprise Single Sign-on (ESSO) são muito caros para aplicações web. Como a maioria dos aplicativos é baseada na web, não existe caso de negócio para ESSO.
**D)** O Single sign-on (SSO) usa um conjunto de credenciais que dão acesso a todos os aplicativos de uma só vez. Consequentemente, essas credenciais devem ser totalmente protegidas.

**A)** Correto. Por sua natureza, o SSO introduz a chamada chave para o reino. Portanto, medidas adicionais de segurança devem sempre ser consideradas com SSO. *Fundamentals of Information Systems Security, Capítulo 5: Processes and Requirements for Authentication*
**B)** Incorreto. É possível implementar ESSO para todos os tipos de aplicativos, por exemplo, usando SAML.
**C)** Incorreto. Não é muito caro implementar ESSO, mesmo para aplicações web, por exemplo, usando SAML.
**D)** Incorreto. Como as credenciais precisam ser totalmente protegidas o tempo todo, isso não é especí fico para SSO.

**26 / 40**
O que um invasor consegue fazer quando um único valor de salt é usado para todas as senhas em um banco de dados?

**A)** Adicionar o salt novamente e obter os valores de texto simples.
**B)** Remover os primeiros caracteres do hash para ignorar os salts.
**C)** Remover o salt e desencriptar as senhas.
**D)** Usar o mesmo salt e criar um banco de dados de senhas e seus valores de hash.

**A)** Incorreto. A senha de salt e texto simples é combinada e misturada. Voltar a adicionar o salt fornece dados sem sentido, que não podem ser usados. O problema é que um invasor pode gerar um banco de dados com senhas e seus valores de hash com salt (chamada de tabela arco-íris) e procurar cada valor de hash do banco de dados de senhas na tabela arco-íris. Com os salts aleatórios, o invasor teria que atacar cada valor de hash separadamente. *Veja o slide 65 do livro de slides para o dia 2.*
**B)** Incorreto. Remover os primeiros caracteres do hash transforma o hash em algo sem sentido. O problema é que um invasor pode gerar um banco de dados com senhas e seus valores de hash com salt (chamada de tabela arco-íris) e procurar cada valor de hash do banco de dados de senhas na tabela arco-íris. Com os salts aleatórios, o invasor teria que atacar cada valor de hash separadamente. *Veja o slide 65 do livro de slides para o dia 2.*
**C)** Incorreto. Depois de misturado, o salt não pode ser removido. O problema é que um invasor pode gerar um banco de dados com senhas e seus valores de hash com salt (chamada de tabela arco-íris) e procurar cada valor de hash do banco de dados de senhas na tabela arco-íris. Com os salts aleató rios, o invasor teria que atacar cada valor de hash separadamente. *Veja o slide 65 do livro de slides para o dia 2.*
**D)** Correto. Um invasor pode gerar um banco de dados com senhas e seus valores de hash com salt (chamado de tabela arco-íris) e procurar cada valor de hash do banco de dados de senhas na tabela arco-íris. Com os salts aleatórios, o invasor teria que atacar cada valor de hash separadamente.

**27 / 40**
No contexto de autorização, o princípio da “necessidade de saber” (need-to-know) é um dos mais importantes a considerar.

O que significa o princípio da “necessidade de saber”?

**A)** As tarefas críticas só podem ser realizadas por pelo menos dois indivíduos, de modo que é necessário um conluio para poder cometer fraudes.
**B)** Os usuários devem ter um nível mínimo de direitos de acesso atribuído a eles para desempenhar suas tarefas.
**C)** Os usuários devem ter acesso apenas às informações necessárias para desempenhar suas tarefas.
**D)** Os usuários devem ter apenas direitos de acesso temporários atribuídos a eles para desempenhar suas tarefas.

**A)** Incorreto. O princípio da “necessidade de saber” significa que os usuários devem ter acesso apenas às informações necessárias para desempenhar suas tarefas.
**B)** Incorreto. O princípio da “necessidade de saber” significa que os usuários devem ter acesso apenas às informações necessárias para desempenhar suas tarefas.
**C)** Correto. O princípio da "necessidade de saber" significa que os usuários têm acesso apenas às informações necessárias.
**D)** Incorreto. O princípio da “necessidade de saber” significa que os usuários devem ter acesso apenas às informações necessárias para desempenhar suas tarefas.

**28 / 40**
Quantas partes (no mínimo) desempenham um papel em um fluxo de dados de autenticação do OpenID Connect?

**A)** 2
**B)** 3
**C)** 4
**D)** 5

**A)** Incorreto. Há pelo menos o usuário (navegador da web), o site no qual se faz logon e o provedor OpenID – 3.
**B)** Correto. Há pelo menos o usuário (navegador da web), o site no qual se faz logon e o provedor OpenID – 3.
**C)** Incorreto. Há pelo menos o usuário (navegador da web), o site no qual se faz logon e o provedor OpenID – 3.
**D)** Incorreto. Há pelo menos o usuário (navegador da web), o site no qual se faz logon e o provedor OpenID – 3.

**29 / 40**
Uma organização **não** está disposta a compartilhar nenhum recurso.

Que modelo de implantação na Computação em Nuvem representa o mais seguro?

**A)** Nuvem comunitária
**B)** Nuvem híbrida
**C)** Nuvem privada
**D)** Nuvem pública

**A)** Incorreto. Uma nuvem comunitária é implantada por uma comunidade de organizações com interesses compartilhados.
**B)** Incorreto. Em uma nuvem híbrida, os recursos são compartilhados com outras partes.
**C)** Correto. Uma nuvem privada é o domínio exclusivo da própria organização. *Fundamentals of Information Systems Security, Capítulo 5: Centralized and Decentralized Access Controls*
**D)** Incorreto. Em uma nuvem pública, os recursos são compartilhados com outras partes.

**30 / 40**
Qual afirmação é verdadeira sobre a nuvem pública?

**A)** Partes são usadas por uma única organização e partes são usadas por um grupo de organizações.
**B)** É usada por uma única organização.
**C)** É usada por um pequeno grupo de organizações com interesses compartilhados.
**D)** É usada por qualquer organização que deseje utilizá-la.

**A)** Incorreto. Esta é uma nuvem híbrida.
**B)** Incorreto. Esta é uma nuvem privada.
**C)** Incorreto. Esta é uma nuvem comunitária.
**D)** Correto. Esta é uma nuvem pública. *Fundamentals of Information Systems Security, Capítulo 5: Centralized and Decentralized Access Controls*

**31 / 40**
Identidade como um Serviço (IDaaS) é um dos modelos de serviço emergentes na Computação em Nuvem.

O que IDaaS fornece?

**A)** Governança de identidade e autenticação para usuários internos
**B)** Governança de identidade e autenticação para clientes, parceiros de negócios e outros usuários externos
**C)** Governança de identidade e autenticação para usuários internos e externos
**D)** Single sign-on (SSO) para usuários externos

**A)** Incorreto. IDaaS fornece governança de identidade e autenticação para usuários internos e externos.
**B)** Incorreto. IDaaS fornece governança de identidade e autenticação para usuários internos e externos.
**C)** Correto. IDaaS fornece governança de identidade e autenticação para todos os grupos de usuários com os quais a organização tem um relacionamento. *Cyber & IT Security – Literatura adicional*
**D)** Incorreto. IDaaS fornece serviços para usuários internos e externos.

**32 / 40**
Uma organização deseja hospedar um serviço de web, mas não deseja lidar com a compra e manutenção de hardware, nem manter o sistema operacional atualizado.

Que tipo de modelo de serviço ela deve solicitar?

**A)** IaaS
**B)** PaaS
**C)** SaaS
**D)** SECaaS

**A)** Incorreto. Infraestrutura como Serviço exigiria que a organização mantivesse o sistema operacional.
**B)** Correto. Plataforma como Serviço fornece uma plataforma na qual a organização só precisa gerenciar seu serviço de web. *Cyber & IT Security – Literatura Adicional*
**C)** Incorreto. Software como Serviço não permite à organização criar seu próprio serviço de web.
**D)** Incorreto. Segurança como Serviço não permite que a organização hospede nenhum serviço de web.

**33 / 40**
Há sempre um risco quando um provedor de nuvem que fornece uma solução como SaaS ou PaaS fecha ou vai à falência.

Qual é esse risco para a empresa que usa essa solução de nuvem?

**A)** Risco de continuidade
**B)** Risco de jurisdição
**C)** Risco legal
**D)** Risco de armazenamento

**A)** Correto. Quando a empresa fecha ou vai à falência, todas as informações são perdidas (dados armazenados na nuvem etc.). *Cyber & IT Security – Literatura adicional*
**B)** Incorreto. Onde os dados são armazenados? São armazenados no país (região) onde a empresa está localizada ou não? Estas informações devem ser fornecidas pelo provedor de serviço.
**C)** Incorreto. Isso pode ser lido no EULA (Contrato de Licença de Usuário Final).
**D)** Incorreto. Este é um risco para o provedor, e não para a empresa que usa a nuvem.

**34 / 40**
Por que o CEO de uma empresa desejaria transferir os principais sistemas corporativos para a nuvem?

**A)** Para reduzir o custo com tecnologia
**B)** Para reduzir o vazamento de informações confidenciais
**C)** Para reduzir vulnerabilidades de segurança
**D)** Para reduzir o acesso não autorizado às informações dos clientes

**A)** Correto. Transferir para a nuvem reduz o custo com tecnologia. *Fundamentals of Information Systems Security, Capítulo 5: Centralized and Decentralized Access Controls*
**B)** Incorreto. Um vazamento de informações confidenciais é um risco ao se transferir para a nuvem.
**C)** Incorreto. Vulnerabilidades de segurança não controladas são um risco da transferência para a nuvem.
**D)** Incorreto. O acesso não autorizado às informações dos clientes é um risco da transferência para a nuvem.

**35 / 40**
Engenharia social é um dos métodos de ataque de cibercriminosos **mais** bem-sucedidos.

O que é considerado como uma forma de engenharia social?

**A)** Criptoware
**B)** Ataque de Negação de Serviço (DoS)
**C)** Phishing
**D)** Spam

**A)** Incorreto. Criptoware opera sem a supervisão do usuário do sistema.
**B)** Incorreto. Um ataque de DoS é um ataque para restringir o acesso a serviços, independentemente das ações do usuário.
**C)** Correto. Phishing pode ser considerado um meio de enganar as pessoas para que divulguem informações confidenciais. *Fundamentals of Information Systems Security, Capítulo 11: The Main Types of Malware*
**D)** Incorreto. Spam é uma mensagem comercial enviada a um grande grupo de destinatários.

**36 / 40**
Há quatro categorias principais de ataque quando se trata de explorar vulnerabilidades.

Qual **não** é uma das quatro principais categorias de ataque?

**A)** Invasão completa
**B)** Roubo ou revelação de informações
**C)** Uso indevido por insider

**A)** Incorreto. Esta é uma das quatro principais categorias de ataque.
**B)** Incorreto. Esta é uma das quatro principais categorias de ataque.
**C)** Correto. Esta é uma fonte de ataque, mas não uma das principais categorias de ataque. A categoria que falta é Negação de Serviço (DoS).

**37 / 40**
Certo tipo de invasor sabe como escrever exploits, usa engenharia social para obter informações sobre seu alvo e coleta dados. Os motivos do invasor não são claros, e o invasor nem sempre é malicioso.

Que tipo de invasor é esse?

**A)** Black Hat Hacker
**B)** Gray Hat Hacker
**C)** Hacktivista
**D)** White Hat Hacker

**A)** Incorreto. O black hat hacker quer ganhar algo com o hack: dinheiro, status etc.
**B)** Correto. O gray hat hacker nem sempre é malicioso, e a motivação às vezes é ambígua. Às vezes, o gray hat hacker hackeia apenas por diversão e, às vezes, ele quer mostrar a uma empresa que há vazamentos em seus sistemas. Mesmo assim, o gray hat hacker não é contratado (ou ético) como o white hat hacker. *EXIN Ethical Hacking Foundation*
**C)** Incorreto. O hacktivista ataca sistemas de um ponto de vista político.
**D)** Incorreto. A motivação do white hat hacker é sempre clara.

**38 / 40**
Qual ferramenta representa uma ferramenta de varredura?

**A)** Nessus
**B)** John the Ripper
**C)** Metasploit
**D)** Ophcrack

**A)** Correto. Nessus é uma das ferramentas mais conhecidas para fazer varredura à procura de vulnerabilidades. *EXIN Ethical Hacking Foundation*
**B)** Incorreto. John the Ripper é uma ferramenta para forçar senhas brutalmente.
**C)** Incorreto. Metasploit é uma caixa de ferramentas para hacking.
**D)** Incorreto. Ophcrack é uma ferramenta para forçar senhas do Windows brutalmente.

**39 / 40**
Hackers e cibercriminosos geralmente realizam suas atividades seguindo um plano bem estruturado.

Qual é a **melhor** ordem em que essas atividades são realizadas dentro de um plano bem estruturado?

**A)** Enumeração, footprinting, obtenção de acesso, escalonamento de privilégios, apagamento de rastros
**B)** Reconhecimento, enumeração, obtenção de acesso, escalonamento de privilégios, apagamento de rastros
**C)** Reconhecimento, varredura, obtenção de acesso, escalonamento de privilégios, manutenção de acesso
**D)** Varredura, enumeração, obtenção de acesso, escalonamento de privilégios, manutenção de acesso

**A)** Incorreto. 'Footprinting' não é um termo ligado a sistemas de hacking, 'impressões digitais' (fingerprinting) é.
**B)** Correto. Reconhecimento e enumeração podem ser definidos como as atividades para coletar informações, que devem ser concluídas primeiro, a fim de conseguir obter acesso. *EXIN Ethical Hacking Foundation*
**C)** Incorreto. Apagar rastros é essencial para ocultar violações do sistema.
**D)** Incorreto. Apagar rastros é essencial para ocultar violações do sistema.

**40 / 40**
Um hacker obteve acesso a um servidor de web usando um plano passo a passo pensado cautelosamente.

Que passo que ele deu imediatamente após “Invasão e acesso”?

**A)** Impressões digitais
**B)** Escalonamento de privilégios
**C)** Reconhecimento
**D)** Avaliação de vulnerabilidade

**A)** Incorreto. A identificação do sistema operacional e detecção de versões específicas de aplicativos ou protocolos é feita antes de entrar no sistema de aplicativo.
**B)** Correto. Depois de entrar no sistema ou aplicativo, ele ganha acesso administrativo. *EXIN Ethical Hacking Foundation*
**C)** Incorreto. Este é o primeiro passo: coletar informações preliminares.
**D)** Incorreto. A identificação e exploração de quaisquer vulnerabilidades é feita antes de entrar no sistema de aplicativo.

# Avaliação

A tabela a seguir mostra as respostas corretas às questões apresentadas neste exame simulado.

| Número | Resposta | Número | Resposta |
|---|---|---|---|
| **1** | B | **21** | B |
| **2** | D | **22** | D |
| **3** | C | **23** | D |
| **4** | C | **24** | A |
| **5** | B | **25** | A |
| **6** | A | **26** | D |
| **7** | C | **27** | C |
| **8** | D | **28** | B |
| **9** | A | **29** | C |
| **10** | C | **30** | D |
| **11** | B | **31** | C |
| **12** | D | **32** | B |
| **13** | D | **33** | A |
| **14** | B | **34** | A |
| **15** | D | **35** | C |
| **16** | A | **36** | C |
| **17** | A | **37** | B |
| **18** | D | **38** | A |
| **19** | B | **39** | B |
| **20** | B | **40** | B |


## Contato EXIN

www.exin.com