EXEMPLO DE EXAME

CERTIFICAÇÃO BSTQB/ISTQB

CTAL-SEC

Certified Tester Advanced Level

Security Testing

EXAME A

Versão 1.0

BASEADO NO SYLLABUS 2018BR

Legal

Histórico

Versão	Data	Comentários
1.0 - Beta	22 Setembro 2015	Versão beta do exemplo exame
1.0 -GA Candidate	04 Março 2016	Atualizações após a revisão do WG de exame - questões 18 e 29 alterado para o nível K3, erro de digitação na questão 35 corrigido, alocações de pts para questões 25 a 32 corrigidos.
1.0 - GA	15 Março 2016	Versão GA com pequenas edições. LOs removidos.

Questão 1 (1 pt)

Qual das opções a seguir é o propósito de uma auditoria de segurança?

A) Evitar que os usuários usem senhas simples
B) Revelar atualizações de patch insuficientes fornecidas pelo fornecedor
C) Impedir que intrusos autorizados acessem o sistema
D) Exigir que os usuários alterem sua senha após um conjunto predeterminado de dias

Questão 2 (3 pt)

Você é responsável por garantir que os novos fornecedores contratados externamente para o projeto estejam em total conformidade com as diretrizes exigidas pelo governo como parte de sua avaliação de risco. Em quais stakeholders você deve se concentrar principalmente para garantir que esses fornecedores externos continuem a cumprir?

A) Clientes, usuários e fornecedores para garantir uma boa comunicação entre eles
B) Usuários públicos e fornecedores que seguirão a lei conforme ela se aplica à fonte de informações
C) Agências federais e locais que comunicam as diretrizes a serem seguidas
D) Ambas as fontes internas e externas que usarão as informações para uma análise mais aprofundada do risco

Questão (1 pt)

Qual das alternativas a seguir é uma consequência de uma política que minimiza o acesso a um sistema ou dispositivo a níveis aceitáveis?

E) Mais dispositivos são adicionados para mitigar o impacto
A) Controles adequados de dispositivos de auto-provisionamento como roteadores são proibidos
B) Os dispositivos que não estão em conformidade são removidos da rede sem fio
C) O acesso à VPN é severamente restrito

Questão 4 (3 pts)

Sua função como administrador de segurança é ajudar sua organização a compreender a eficácia das políticas e procedimentos de segurança em toda a empresa. Você relatará suas descobertas de eficácia ao gerenciamento sênior após a conclusão da análise.

Qual das alternativas a seguir é a estratégia ideal para fazer isso?

A) Implementar uma avaliação de análise estática de forma independente para políticas e procedimentos
B) Analisar os resultados de um teste de segurança para validar a eficácia
C) Avaliar os resultados dos testes de segurança que se concentram nas ameaças e ataques atuais
D) Avalie os resultados do teste estático para novas e emergentes ameaças de software

Questão 5 (1 pt)

Se uma organização sofre uma violação de segurança e resulta em uma ação legal, como isso ajuda a organização a fazer testes de segurança?

A) Pode mostrar que a organização fez a devida diligência para tentar evitar tal incidente
B) A documentação do teste de segurança pode ser usada para rastrear o autor criminoso
C) Visto que qualquer informação importante teria sido copiada antes dos testes de segurança, este backup pode ser usado para restaurar qualquer informação comprometida
D) Rastreando através dos testes documentados, a equipe de teste de segurança pode descobrir como a violação foi possível

Questão 6 (1 pt)

Qual das alternativas a seguir é uma afirmação correta?

A) A garantia da informação faz parte dos testes de segurança
B) A garantia da informação e o teste de segurança são dois termos para a mesma coisa
C) O teste de segurança faz parte da garantia da informação
D) Os dois termos referem-se a diferentes áreas de segurança

Questão 7 (2 pts)

Você está trabalhando em um banco como parte da equipe de testes de segurança. Durante uma recente auditoria de segurança, foi observado que as senhas do usuário não eram fortes o suficiente. Desde então, um novo conjunto de requisitos foi emitido para garantir a força da senha.

Com essas informações, qual seria um conjunto razoável de objetivos geral de segurança para o teste de regra de senha?

1) Verifique se as senhas atendem aos requisitos de extensão;
2) Verifique se as senhas atendem aos requisitos de uso de caracteres, números, letras minúsculas e maiúsculas;
3) Verifique se as senhas podem ser repetidas três vezes;
4) Verifique se as senhas não podem ser reutilizadas dentro de um período de um ano;
5) Verifique se as senhas devem ser redefinidas a cada três meses;
6) Verifique se o usuário pode solicitar o envio de sua senha por e-mail;
7) Verifique se o administrador do sistema pode redefinir uma senha bloqueada;

A) 1, 2, 3, 4
B) 1, 2, 4, 5
C) 3, 4, 6, 7
D) 4, 5, 6, 7

Questão 8 (2 pts)

Recentemente, sua empresa ganhou as manchetes depois que uma violação de segurança resultou no roubo de informações confidenciais de clientes. A gerência reagiu com um edital de que o escopo dos objetivos do teste de segurança precisa ser expandido imediatamente. Embora concorde que algo precisa ser feito, você está preocupado com a possibilidade de essa abordagem ser muito reativa e não resultar nos testes necessários.

De acordo com o Syllabus, o que é uma preocupação razoável se essas iniciativas forem implementadas?

A) O teste ainda perderá problemas porque não será bem focado
B) O teste será terceirizado para que possa ser feito de forma mais eficiente
C) O escopo do teste pode ser muito grande e pode não haver recursos adequados para completá-lo
D) Os objetivos de teste não são claramente definidos e podem perder os mesmos problemas que escaparam anteriormente para a produção

Questão 9 (3 pts)

Você acabou de aceitar um emprego para criar uma equipe de testes de segurança para uma empresa que lida com informações médicas confidenciais que são compartilhadas entre médicos e hospitais. Você notou que a segurança em torno dessas informações não é suficiente para protegê-las de hackers ou mesmo de exposição acidental. A pessoa que desempenhava seu trabalho anteriormente trouxe vários consultores para fazer o teste, mas as descobertas não foram documentadas e nenhuma mudança foi implementada. Na verdade, você nem sabe qual foi a cobertura do teste. Você apresentou suas descobertas à equipe de gerenciamento executivo. Embora tenham concordado em princípio que precisam de testes de segurança, eles não alocaram o orçamento ou o tempo necessários para o projeto. Parece que, embora eles pensem que a segurança é uma boa ideia, eles realmente não entendem o que deve ser feito ou como deve ser feito.

Qual deve ser o primeiro passo para alinhar os executivos com o trabalho que precisa ser feito?

A) Criar uma lista detalhada de todas as falhas de segurança possíveis e apresentar aos executivos
B) Fornecer um resumo da abordagem de teste que você propõe e dar exemplos de como o teste será conduzido
C) Convocar a equipe jurídica para explicar o que uma violação de segurança pode custar à organização
D) Criar uma política de segurança e uma política de teste de segurança e demonstrar como isso se alinha com sua abordagem de teste proposta

Questão 10 (2 pts)

Você acabou de chegar de uma reunião em que houve muita discussão sobre a abordagem de segurança da organização. Um dos pontos de destaque foi a importância dos testes para garantir que os dados sejam protegidos contra acessos fraudulentos, principalmente informações de cartão de crédito.

Você foi solicitado a preparar um conjunto de objetivos de teste que ajudarão a abordar essa área de risco. Uma de suas tarefas é garantir que você esteja cobrindo todas as preocupações dos stakeholders.

Qual grupo de stakeholders tem maior probabilidade de ver os benefícios de seus esforços?

A) Direção executiva
B) Agentes de conformidade
C) Clientes do negócio
D) Agentes reguladores

Questão 11 (2 pts)

Como administrador de segurança, você é responsável por todos os aspectos do processo de segurança, incluindo testes. Para este processo específico, você deve usar testes conceituais como base para testes manuais e executá-los da perspectiva de um fornecedor externo.

Qual processo de teste de segurança é o mais correspondente?

A) Criação de teste de segurança de condições e objetivos
B) Implementação de teste de segurança
C) Avaliação geral e relatórios de testes de segurança
D) Análise e design de teste de segurança

Questão 12 (3 pts)

Você está desenvolvendo um plano de teste de segurança para um sistema que armazena informações médicas de pacientes e transfere esses dados para médicos especialistas. Você cobriu as seguintes áreas em seu plano:

- Escopo (o que está dentro e fora do escopo)
- Funções e atribuições
- Responsabilidades (fornecedores vs. internos)
- Cronograma de alto nível
- Requisitos e configuração do ambiente
- Lista de autorizações e aprovações necessárias

Que informações você ainda precisa fornecer neste plano de teste para atender aos requisitos mínimos conforme observado no Syllabus?

A) Uma lista das credenciais e do treinamento necessários para o pessoal que realizará o teste.
B) Um cronograma mostrando o tempo que será necessário para projetar, executar e avaliar os testes de segurança.
C) Uma cópia das normas regulatórias que devem ser atendidas por este sistema.
D) Uma lista dos indivíduos que farão o teste e suas informações de contato em caso de violação de segurança.

Questão 13 (2 pts)

Qual dos casos de teste a seguir testaria melhor o procedimento de segurança de um sistema?

A) Três tentativas malsucedidas de login irão gerar uma mensagem de bloqueio. Entre em contato com seu gerente ou com o administrador do sistema para que eles possam fornecer uma senha temporária pelo telefone. Você deve então alterar a senha temporária ao fazer o login. Você sai e faz o login novamente usando a senha recém-criada.
B) Você recebe uma mensagem de bloqueio após várias tentativas de login. Você liga para o suporte de TI para obter uma nova senha. Você efetua login com a senha temporária, efetua log out, efetua login novamente e insere uma nova senha.
C) Após várias tentativas, você é bloqueado no sistema. Você usa uma senha que funcionou anteriormente. No entanto, ele não funciona mais. Você tenta criar uma nova senha, mas agora está bloqueado. Uma reinicialização completa da máquina é a próxima etapa para levá-lo ao prompt para redigitar a senha.
D) Após a primeira tentativa de usar uma senha inválida, você imediatamente abre uma lista de senhas no bloco de notas do PC para garantir que está usando a senha correta. Você tenta outra senha da lista e funciona.

Questão 14 (1 pt)

Quais das seguintes são características principais de um ambiente de teste de segurança eficaz?

A) Estritamente vinculado a sistemas de produção para aumentar a segurança em todos os pontos
B) Isola diferentes versões antigas dos sistemas operacionais para uso no ambiente
C) Imita o ambiente de produção em termos de direitos de acesso
D) Inclui todos os plug-ins do ambiente de produção, bem como outros plug-ins que não estão no ambiente de produção, a fim de garantir a configuração mais abrangente

Questão 15 (1 pt)

O que é uma preocupação significativa ao buscar aprovação para as ferramentas de teste de segurança?

A) Alguns países proíbem o uso de certas ferramentas de teste de segurança
B) Garantir que o processo de aprovação para ferramentas de teste de segurança possa ser ignorado como exceção nos casos em que um evento malicioso esteja em andamento

C) Os riscos da ferramenta raramente são conhecidos antes de ser adquirida e são mais bem exploradas quando as ferramentas estão em uso
D) Como os riscos da ferramenta de teste de segurança são geralmente conhecidos, não há necessidade de uma estratégia de mitigação

Questão 16 (3 pts)

Você está revisando um conjunto de resultados de teste de segurança executados em um produto que está passando pelo teste final antes de ser liberado para produção. Esta é uma atualização de uma versão que está atualmente em produção. O aplicativo que acabamos de testar é o seu site de comércio eletrônico e tem um defeito que permite a execução de scripts entre sites.

Qual das opções a seguir é o conjunto adequado de etapas que você deve seguir?

A) Relatar o problema ao desenvolvedor, adicioná-lo ao relatório dos stakeholders e continuar testando outros tipos de defeitos
B) Testar se o problema existe na versão de produção atual, documentar o defeito em um sistema seguro, notificar o desenvolvedor, continuar testando para outros XSS defeitos
C) Investigar a extensão do problema conduzindo testes adicionais no lançamento planejado com concentração particular em outros problemas de XSS, conduzir uma análise estática no código
D) Informar a gestão, documentar o defeito e inclui-lo em seu relatório de status semanal para os stakeholders, continuar testando outros defeitos de segurança para determinar a extensão dos problemas de segurança

Questão 17 (1 pt)

Em que ponto do SDLC deve haver verificação para garantir que as práticas de codificação seguras adequadas foram seguidas?

A) Teste de componentes
B) Teste de integração
C) Teste de sistema
D) Teste de aceite de segurança

Questão 18 (2 pts)

O analista de negócios pediu que você ajudasse a definir os requisitos para os aspectos de segurança de um sistema. Este é um sistema crítico de segurança que armazena informações médicas para pacientes e fornece essas informações para profissionais de saúde em hospitais, consultórios médicos e ambulâncias.

Em que ponto do ciclo de vida os requisitos de segurança devem ser documentados e em que nível de detalhes?

A) Não devem ser documentados formalmente devido à necessidade de proteger a implementação de segurança dentro do código estranho
B) Devem ser documentados de forma detalhada e inequívoca nos documentos de requisitos durante a fase de requisitos
C) Devem ser documentados durante a fase de design, quando a abordagem do código é conhecida, e não na fase de requisitos, quando a abordagem não é conhecida
D) Devem ser restritos ao acesso funcional e requisitos de disponibilidade da perspectiva do usuário e devem ser documentados durante a fase de requisitos

Questão 19 (3 pts)

Uma deficiência foi descoberta na produção. Se um usuário não autorizado copiar uma URL de uma sessão de um usuário autorizado, poderá colar a URL em sua sessão e continuar a processar com os direitos do usuário autorizado. No caso relatado, o usuário não autorizado foi capaz de usar a URL do usuário autorizado para

alterar a senha de administração do sistema. Para fechar esta lacuna, os desenvolvedores verificarão o ID da sessão e o ID do usuário sempre que uma URL for usada.

Qual é uma preocupação realista para essa correção?

A) Não resolverá o problema e o roubo de sessão ainda será possível
B) Resolverá o problema, mas a usabilidade poderá ser afetada negativamente
C) Resolverá o problema, mas o desempenho poderá ser adversamente afetado
D) Não resolverá o problema e exibirá uma nova vulnerabilidade com IDs de sessão

Questão 20 (1 pt)

Durante o teste de nível de componente, por que o testador de segurança deve revisar os avisos do compilador?

A) Porque indicam problemas de segurança que devem ser corrigidos
B) Porque indicam possíveis problemas que devem ser investigados
C) Porque indicam problemas de codificação que causarão defeitos funcionais
D) Porque indicam práticas de programação ruins que aumentarão a capacidade de manutenção

Questão 21 (2 pts)

Você testou um sistema que possui 20 componentes definidos. Você fez testes extensivos de segurança em cada um dos componentes. O sistema agora está pronto para passar para os testes de segurança de integração de componentes.

Como você deve abordar esse teste?

A) Uma vez que o teste de integração de componentes se preocupa com a soma das vulnerabilidades dos componentes individuais, a melhor abordagem é conduzir os mesmos testes nos componentes integrados.
B) O principal risco agora está na integração dos próprios componentes, então o teste deve cobrir cada interface e verificar se não há vulnerabilidades nas interfaces e os componentes também devem ser testados novamente.
C) É provável que novas vulnerabilidades estejam presentes com os componentes integrados, bem como com o sistema e a infraestrutura maiores que agora podem ser testados, portanto, os testes devem ser expandidos para incluir essas novas áreas.
D) Como os componentes agora estão integrados, os riscos de segurança serão reduzidos porque as possíveis interações agora são limitadas, portanto, apenas os pontos de integração devem ser testados e nenhum novo teste de componente é necessário.

Questão 22 (3 pts)

Você está criando casos de teste de segurança para verificar a injeção de SQL em um campo de entrada que permite até 5 caracteres alfanuméricos. Você está planejando aplicar o particionamento de equivalência para reduzir o número de casos de teste que precisará executar. om essas informações, qual das opções a seguir é o conjunto mínimo de entradas que você precisaria usar para testar este campo?

A) bbbbb, 12345, ‘
B) %, ‘, @, ab123
C) ‘, ab123
D) ‘

Questão 23 (2 pts)

Um usuário terá permissão para solicitar sua senha. Se ele fizer essa solicitação, deverá responder duas de suas três perguntas de segurança corretamente. Se responder corretamente, um link será enviado para seu e-mail. O link o levará a uma página onde redefinirá a senha. Depois de redefinido, poderá fazer o login com a nova senha. O link será desativado 1 hora depois de ser enviado. O usuário tem permissão para apenas duas solicitações de senha sem uma redefinição, após ele terá que ligar para o help-desk. Para quaisquer outros erros, o ID do usuário é bloqueado e deve ser desbloqueado pelo help-desk. Qual das seguintes é a lista mínima de condições de teste para testar adequadamente a segurança funcional coberta por este requisito?

A) usuário inválido; usuário válido; 2 respostas corretas; 2 respostas incorretas; bom e-mail; e-mail ruim; redefinir com uma boa senha; redefinir com senha ruim; link bom; Link expirado; duas solicitações sem reset; três solicitações sem reset
B) usuário válido; 2 respostas corretas; bom e-mail; redefinir com uma boa senha; link bom; duas solicitações sem reset
C) usuário inválido; 2 respostas incorretas; e-mail ruim; redefinir com senha ruim; Link expirado; três solicitações sem reset
D) Estouro de buffer em cada campo de entrada; Injeção SQL em cada campo de entrada; XXS na página de login e página de redefinição de senha, usuário inválido; usuário válido; 2 respostas corretas; 2 respostas incorretas; bom e-mail; e-mail ruim; redefinir com uma boa senha; redefinir com senha ruim; link bom; Link expirado; duas solicitações sem reset; três solicitações sem reset

Questão 24 (2 pts)

Um usuário terá permissão para solicitar sua senha. Se ele fizer essa solicitação, deverá responder duas de suas três perguntas de segurança corretamente. Se responder corretamente, um link será enviado para seu e-mail. O link o levará a uma página onde redefinirá a senha. Depois de redefinido, poderá fazer o login com a nova senha. O link será desativado 1 hora depois de ser enviado. O usuário tem permissão para apenas duas solicitações de senha sem uma redefinição, após ele terá que ligar para o help-desk. Para quaisquer outros erros, o ID do usuário é bloqueado e deve ser desbloqueado pelo help-desk. Qual das opções a seguir é um conjunto válido de critérios de aceite para este requisito?

1) O usuário pode redefinir a senha se menos de três solicitações tiverem sido feitas desde a última redefinição e duas perguntas de segurança forem respondidas corretamente e o link for usado para redefinir e uma senha válida for inserida no prompt de redefinição.
2) Mais de duas solicitações resultam em bloqueio de ID do usuário.
3) Mais de duas solicitações sem redefinição resultam em bloqueio de ID do usuário.
4) Mais de duas perguntas de segurança perdidas resultam em erro.
5) Mais de duas perguntas de segurança perdidas, o ID do usuário está bloqueado.
6) Se o sistema receber um erro de e-mail, o ID do usuário será bloqueado.
7) Se uma senha inválida for inserida na redefinição, o usuário será avisado com as regras adequadas.
8) A redefinição de senha pode ser usada para fazer login no sistema.

A) 1,2, 4, 6, 7, 8
B) 1, 2, 3, 4, 5, 6, 7, 8
C) 3, 5, 6, 7, 8
D) 1, 3, 5, 6, 8

Questão 25 (2 pts)

Você está implementando procedimentos para avaliar a proteção do sistema em um esforço para testar a eficácia da segurança do sistema. Que procedimento você deve seguir para garantir que os mecanismos de proteção implementados estejam funcionando conforme o esperado?

A) Monitorar cuidadosamente vários relatórios e métricas de desempenho de segurança para determinar se o nível correto de acesso e autenticação é alcançado
B) Auditar com frequência a consistência da autenticação para garantir que um alto nível de proteção contra intrusão seja mantido em todos os momentos
C) Avaliar os componentes de hardware que foram reforçados e os comparar com outros componentes de software reforçados para garantir que o equilíbrio está sendo alcançado
D) Recrutar um hacker conhecido para realizar uma avaliação independente da eficácia do reforço

Questão 26 (1 pt)

Quais são os principais atributos da autenticação de segurança de um sistema de TI de média complexidade?

A) Verificar se o usuário tem o perfil correto e os direitos correspondentes para acessar partes limitadas do sistema
B) Ser a chave para identificar a quantidade de recursos do sistema que o usuário pode utilizar
C) Verificar se o usuário que entra no sistema é legítimo
D) Usar credenciais comuns entre os usuários para obter entrada no sistema

Questão 27 (2 pts)

Os mecanismos de criptografia típicos são vulneráveis a ameaças, o que torna importante entender sua eficácia a qualquer momento.

Identifique qual das opções a seguir você deve implementar para ganhar confiança em seus mecanismos de criptografia?

A) Avaliar as chaves criptográficas para garantir que tenham pelo menos 256 bits de tamanho
B) Certificar-se de que está aplicando algoritmos aleatórios para gerar números sempre que possível
C) Desenvolver testes que garantam que a criptografia simétrica seja usada nos modos corretos
D) Remover todos os protocolos WEP para observar como o sistema funciona

Questão 28 (1pt)

O que se aplica à relação entre um firewall e uma zona de rede?

A) Tanto uma zona de rede e firewall se concentram no tamanho dos dados que estão sendo transmitidos
B) Uma zona de rede se comunica por meio de opções de protocolo seguras enquanto um firewall garante que esses protocolos sejam seguros
C) Uma sub-rede pode ser considerada uma zona de rede e um firewall pode ser um software de monitoramento de tráfego
D) Uma zona de rede bloqueia o tráfego malicioso de uma zona não confiável que o firewall não filtra

Questão 29 (2 pts)

Qual das seguintes opções você aplicaria para testar com mais eficácia as habilidades de uma ferramenta de detecção de intrusão?

A) Desenvolver uma série de cenários com base em experiências anteriores
B) Usar testes que gerem tráfego malicioso para adicionar novas especificações intrusivas
C) Aplicá-los a situações de tráfego malicioso conhecido
D) Usá-los em conjunto com outros produtos IDS, quando possível

Questão 30 (1pt)

Qual das opções a seguir é a principal desvantagem das ferramentas de verificação de malware?

A) Só detectam apenas certos níveis de malware
B) Só podem detectar malware conhecido pela ferramenta
C) Tendem a ser excessivamente complexos para executar
D) Não fornecem recursos de atualização e relatórios

Questão 31 (2 pts)

Você precisa remover os números de identificação pessoal de um sistema legado para reduzir o risco durante o teste. Parte do seu plano inclui a verificação da eficácia com que os dados são mascarados.

Qual das alternativas a seguir é a abordagem mais eficaz a ser usada?

A) Verificar manualmente no banco de dados se os dados direcionados para ocultação não são mais compreensíveis para interpretação humana lógica
B) Projetar um ataque de força bruta nos dados ocultados
C) Substituir os dados confidenciais por dados aleatórios de vários comprimentos de string
D) Convidar o desenvolvimento para criar um programa para testar o banco de dados em busca de vulnerabilidades

Questão 32 (1pt)

O que geralmente é considerado o elo mais fraco na segurança de software?

A) A falta de um plano de treinamento de segurança consistente e abrangente
B) O esforço necessário para manter as atualizações de documentos e procedimentos, a fim de acompanhar as ameaças de segurança contínuas
C) O comportamento dos humanos
D) O constante avanço em técnicas maliciosas

Questão 33 (1 pt)

Qual das opções a seguir é um risco potencial à segurança?

A) Publicar um organograma do departamento de contabilidade no site da empresa
B) Enviar votos de aniversário para um colega de trabalho no Facebook
C) Publicação da lista telefônica da empresa na intranet da empresa
D) Publicação de experiência profissional em um perfil do LinkedIn

Questão 34 (2 pts)

Você é responsável por testar a segurança do aplicativo financeiro de sua empresa. Recentemente, você recebeu um e-mail de uma pessoa que afirma ter invadido o sistema usando o Shodan e descobriu que você está executando um sistema operacional desatualizado e vulnerável em um de seus servidores. Você verificou e o hacker está correto. Você se certificou de que o servidor foi atualizado. Sua verificação preliminar não mostrou nenhum traço de como o hacker entrou em seu sistema.

Quais das opções abaixo você deveria se preocupar?

A) Não, este é um hacker de "white hat" e não significa nenhum dano para sua empresa
B) Não, você corrigiu a vulnerabilidade, então o sistema agora está seguro
C) Sim, o seu teste de segurança não é suficiente e você precisa refazer os testes para ver o que foi perdido
D) Sim, uma vez que o hacker não admitiu como entrou no sistema, ele ainda pode acessá-lo e pode decidir explorar a vulnerabilidade na próxima vez

Questão 35 (1 pt)

Por que um ataque de dentro da organização é particularmente preocupante?

A) O invasor provavelmente é movido pela curiosidade e será inflexível
B) O invasor provavelmente está entediado no trabalho e continuará hackeando o sistema para se divertir
C) O invasor já está dentro do firewall e é um usuário autorizado do sistema
D) O invasor provavelmente lançará um ataque DOS que irá paralisar os servidores

Questão 36 (3 pts)

Você está trabalhando em uma organização onde o acesso de administração do sistema aos servidores é altamente restrito. Apenas três funcionários confiáveis e de longa data conhecem as senhas de root. Recentemente, porém, houve várias ocorrências estranhas. Um programa desconhecido, chamado "IKnowYourBirthday" foi encontrado em execução e estava enviando saudações de aniversário para membros da equipe. As datas de nascimento estavam corretas e as saudações foram todas assinadas "Do seu servidor favorito". Este programa foi eliminado e ninguém conseguiu descobrir. Um segundo problema ocorreu quando a lista de telefones da empresa foi hackeada e todos os números de telefone foram alterados para 867-5309. A lista correta foi restaurada e novamente ninguém conseguiu descobrir como isso foi feito, embora o novo arquivo tenha sido criado pelo "root". Você acabou de receber uma ligação do administrador do sistema principal informando que a senha do root foi alterada. Foi determinado que a senha foi definida com o nome do cachorro do administrador do sistema principal.

Investigações posteriores descobriram que os problemas começaram logo depois que uma série de e-mails infectados por vírus foram detectados. Quando o primeiro foi encontrado, guardas de segurança foram imediatamente colocados em prática para impedir qualquer propagação do vírus, mas agora você está se perguntando se alguém conseguiu entrar no sistema por meio de um código que foi introduzido no sistema pelo vírus.

O que você deve fazer agora como sua próxima etapa de investigação?

A) Verificar se as informações de data de nascimento do RH foram acessadas de fora do sistema e, em caso afirmativo, rastrear o endereço IP
B) Verificar se o nome do cachorro do administrador principal do sistema está publicado em algum lugar nas redes sociais
C) Verificar o e-mail suspeito que foi enviado e tentar rastrear o endereço IP
D) Verificar os arquivos pessoais dos outros dois administradores de sistema para ver se há uma indicação de que eles estão insatisfeitos

Questão 37 (2 pts)

Durante o teste de uma atualização, você descobriu que é possível criar um ataque man-in-the-middle que pode alterar o valor cobrado dos clientes em seu site de comércio eletrônico. Seu testador alterou o valor com sucesso para que todos os clientes recebessem um desconto de 10%. O que você deve fazer primeiro?

A) O testador deve ser desencorajado de criar esses tipos de ataques, pois eles não são realistas no ambiente de produção
B) Informar imediatamente a gerência que o ataque foi criado pela equipe de teste como parte do teste, caso seja detectado
C) Trabalhar com os desenvolvedores para implementar verificações como SSL-trip para garantir que os certificados sejam válidos e não auto assinados
D) Verificar a produção para ver se a vulnerabilidade também está no código de produção

Questão 38 (1 pt)

Por que é importante reavaliar as expectativas de risco de segurança com frequência?

A) Os Stakeholders, devem ser instruídos sobre todos os riscos de segurança em todos os momentos
B) Os Stakeholders tomarão decisões de negócios com base nos níveis de risco de segurança associados
C) Os usuários devem desenvolver um plano de mitigação de risco com base manual
D) As expectativas do usuário e dos Stakeholders em relação à segurança devem ser impedidas de mudar

Questão 39 (1 pt)

Qual das opções a seguir é um aspecto importante dos resultados do teste de segurança?

A) Eles são publicados para usuários e stakeholders acessarem, a fim de ajudá-los a entender melhor os riscos
B) Eles devem ser compartilhados com desenvolvedores em toda a empresa, a fim de mitigar o risco de projetos de desenvolvimento futuros
C) Quanto menos pessoas souberem, melhor
D) Os resultados devem sempre ser classificados por criticidade

Questão 40 (3 pts)

Você está finalizando seu relatório de status de teste de segurança para um projeto que está pronto para implantação na produção. Existe um alto grau de risco para este projeto devido à natureza do sistema. Como resultado, você deseja dar ênfase especial ao risco.

Com base nisso, qual é a melhor forma de articular o risco em seu relatório?

A) Uma avaliação descritiva de risco incluída no resumo
B) Risco geral incluído na última seção do relatório
C) Impacto de risco descrito no resumo e posteriormente detalhado em termos de vulnerabilidades específicas
D) O impacto do risco não faz parte do resumo do relatório

Questão 41 (1 pt)

De que forma as ferramentas de análise dinâmica de segurança são diferentes das ferramentas de análise dinâmica geral?

A) As ferramentas de segurança investigam o sistema em vez de apenas o aplicativo em teste
B) As ferramentas de segurança funcionam da mesma forma no modo dinâmico ou estático
C) As ferramentas de segurança são mais adequadas para detectar problemas como vazamentos de memória
D) As ferramentas de segurança precisam ser adaptadas ao idioma em que o aplicativo é implementado

Questão 42 (3 pts)

Você recebeu a tarefa de testar o firewall da organização. Você revisou o plano e as etapas de implementação, verificou se a configuração foi definida conforme as instruções do fornecedor do firewall e realizou uma varredura de porta. Sua organização está particularmente preocupada com ataques de negação de serviço (DOS), principalmente porque eles tiveram um quando o antigo firewall estava instalado.

Que tipo de teste você deve realizar para ajudar a detectar um comportamento inesperado que pode ser explorado por um ataque DOS?

A) Criar testes que enviarão pacotes de rede malformados ou dados Fuzzing e verificar se eles serão detectados e rejeitados pelo firewall
B) Implementar testes automatizados para testar a carga dos servidores para testar os recursos de failover

C) Testar os algoritmos de criptografia e descriptografia para determinar se eles são rápidos o suficiente para lidar com a carga de um ataque DOS
D) Conduzir a proteção do componente de software para garantir que a superfície de ataque seja reduzida o máximo possível

Questão 43 (1 pt)

Se você adquiriu uma ferramenta que é usada sob a Licença Pública Geral GNU, qual das opções a seguir é uma consideração importante para a manutenção da ferramenta?

A) Confiabilidade do fornecedor e capacidade de fornecer suporte
B) Frequência e disponibilidade de atualizações do fornecedor
C) Capacidades técnicas de sua equipe para oferecer suporte e personalizar a ferramenta para seu ambiente
D) Custo da licença e custo do contrato de suporte

Questão 44 (1 pt)

Qual das opções a seguir é uma vantagem de estar em conformidade com os padrões de teste de segurança?

A) São consistentes e fáceis de seguir, pois são separados e independentes das metas e objetivos do projeto
B) São os blocos de construção para testes de segurança futuros, eliminando a necessidade de começar do zero
C) Descrevem uma ofensa eficaz para enfrentar as ameaças antes que elas entrem no sistema
D) Permitem latitude nas práticas de segurança, uma vez que as ameaças estão sempre mudando dinamicamente

Questão 45 (1 pt)

Quais são as vantagens de impor padrões de segurança em contratos?

A) Fornecem a cada parte uma saída legal quando um problema de segurança imprevisto afeta negativamente o produto
B) Fornecem um ponto de partida para ambas as partes começarem suas negociações
C) São uma maneira conveniente de tornar público o acordo entre as partes
D) Podem mudar conforme os padrões mudam, mesmo quando o contrato é finalizado

Gabarito e Comentários

(**Q**) Questão – (**RC**) Resposta correta – (**P**) Pts

Q	RC	Comentários	P
1	b	B é a correta, pois manter as atualizações do patch atualizadas no sistema é um dos propósitos de uma segurança auditoria. As outras são boas práticas, mas não são o objetivo da auditoria de segurança.	1
2	c	C é a correta, pois esta é a fonte das diretrizes. As diretrizes podem mudar, portanto é importante manter os canais de comunicação abertos com essa gente. A, B e D precisam todos ser informados, mas o as informações devem vir dos órgãos federais e locais	3
3	c	C é a correta. Quando esta política for implementada, os dispositivos não-conformes serão removidos até conformar. A não é correto, pois isso não seria um resultado esperado. B não é correto porque estes controles serão encorajados. D não é correto porque o acesso será controlado, não severamente limitado	1
4	b	B é a correta. Você deve analisar os resultados de um teste de segurança para ver se as políticas e procedimentos foram seguidas e são eficazes. A não é correto porque a análise estática deve estar sobre o código, se qualquer coisa. C não é correto porque o foco não deveria ser apenas nas ameaças e ataques atuais, mas também em configurações, etc. D não é correto porque o foco não está apenas nas ameaças emergentes	3
5	a	A é a correta de acordo com o programa. B não está correto porque esta informação provavelmente não seria útil. C não está correto porque o backup provavelmente estaria desatualizado e a informação não era necessariamente corrompido, mas sim roubado ou visto. D não é correto porque, embora isto possa ajudar a apontar áreas onde os testes não foram suficientes, não apoiará a defesa da organização em ações legais	1
6	c	C é a correta, os testes de segurança fazem parte de uma área maior de garantia da informação	1
7	b	B é a correta porque todos são objetivos de segurança válidos. A não é correto porque 3 é funcional em vez de relacionadas à segurança (a menos que isso as bloqueie, mas não sabemos isso a partir desta descrição). C é não correto porque 6 e 7 são ambos funcionais em vez de requisitos específicos de segurança. D não é correto pela mesma razão que a C	2
8	c	C é a correta de acordo com o syllabus, pois este é um problema comum quando os objetivos são definidos de forma ampla. A e D são preocupações razoáveis, mas você não sabe quando ou como os objetivos do teste serão definidos, portanto isto pode ser controlável. B é sempre uma possibilidade e pode ser a coisa certa a ser feita neste caso, mas não houve indicação de que a terceirização ocorrerá neste momento	2
9	d	D é a correta. Neste ponto, a organização precisa de uma política de alto nível e planeja seguir em frente. Sem esta política, os testes podem continuar a ser esporádicos e o apoio e financiamento de alto nível será difícil. A e C não estão corretas neste ponto, embora possam ser úteis se você tiver dificuldade em obter financiamento quando você trabalha para	3

Q	RC	Comentários	P
		implementar a política. B não está certo porque você precisa de uma política geral diante de você definir a abordagem	
10	c	C é a correta. Os clientes comerciais estarão mais preocupados com a proteção contra acesso fraudulento, pois são os dados deles que são vulneráveis. Você esperaria que A, B e D também estivessem envolvidos, mas isto não é geralmente seu principal benefício	2
11	b	B é a correta. O uso dos testes conceituais para criar os testes manuais e realizar a execução é parte da implementação do teste de segurança. A e D não estão corretas porque isso já foi feito com a criação dos testes conceituais. C ocorrerá após a execução dos testes	2
12	b	B é a correta de acordo com o syllabus. A pode ser necessário, mas isso não é um dos requisitos mínimos e já podem ser compreendidas na seção de papéis e responsabilidades. C não é correto porque as normas podem ser referenciadas, mas não incluídas no plano. D não é correto porque este nível de detalhe não faz parte do plano e os testadores individuais não devem ser contatados durante uma violação	3
13	a	A é a correta. B e C não estão corretas por causa da palavra "várias". D não está correto porque esta não seria definitivamente uma boa prática de segurança.	2
14	c	C é a correta porque quanto mais próximo o ambiente de teste imita a produção, mais válidos serão os testes. Isto é particularmente verdadeiro quando se trata de direitos de acesso e definições de delegação. A não é correta porque o sistema não precisa ser e provavelmente não deveria ser conectado. B pode ser útil, mas não é uma característica principal. D não é correto porque inclui plug-ins que não estão em produção, o que poderia resultar tanto em falsos positivos quanto em falsos negativos dos testes.	1
15	a	A é a correta. Embora algumas ferramentas sejam bastante boas e eficazes para testes, elas podem ser proibidas por alguns países e algumas organizações. B não é correta porque sempre há o perigo de se empregar uma ferramenta insuficiente para lidar com uma crise. Um processo de aprovação rápido faz sentido, mas um desvio completo é arriscado. C e D não são corretas porque pode haver riscos desconhecidos das ferramentas e é melhor fazer a devida diligência na seleção de ferramentas do que lidar com as consequências de uma ferramenta mal selecionada.	1
16	b	B é a correta. A primeira prioridade é ver se o problema existe na versão de produção. O defeito deve ser documentado apenas em um sistema seguro de rastreamento de defeitos, uma vez que o problema pode existir na produção. Como foi encontrado um problema XSS, pode haver outros, portanto, é necessário continuar os testes. A não é correto porque o defeito não deve ser divulgado no relatório das partes interessadas. C não é correto porque embora sejam necessários mais testes, a notificação é crítica. D não é correto porque o relatório das partes interessadas não deve ser divulgado.	3
17	a	A é a correta. A verificação deve ser feita assim que o código for escrito	1
18	b	B é a correta. A não é correto, embora seja importante que os requisitos documentados sejam protegidos daqueles que não precisam saber. C não é correto porque, embora possam ser refinados no nível de projeto, devem ser inicialmente capturados durante a fase de definição	2

Q	RC	Comentários	P
		dos requisitos. D não é correta porque os requisitos de segurança também precisam incluir práticas de codificação seguras, etc.	
19	c	C é a correta. É provável que este nível de verificação retarde o sistema porque ele terá que verificar em cada mudança de tela. A e D não estão corretas porque a correção deve consertar o problema. B não está correto porque não deve haver impacto na usabilidade (a menos que você seja o hacker!	3
20	b	B é a correta. Do ponto de vista dos testes de segurança, os avisos do compilador indicam problemas potenciais que podem levar a falhas de segurança. A não é correta porque as advertências não requerem necessariamente uma correção. C e D podem ser verdadeiras, mas não estão relacionadas aos testes de segurança.	1
21	c	C é a correta. Novas vulnerabilidades podem estar presentes com os componentes integrados e é provável que novas áreas de teste estejam disponíveis. A não é correta porque o teste de integração de componentes não é a soma dos componentes individuais. B não é correta porque o teste não deve ser limitado apenas às interfaces e aos componentes originais. D não é correta porque é provável que os riscos de segurança sejam maiores e não menores.	2
22	c	C é a correta, pois este tem um teste para injeção SQL e outro para uma entrada válida. Este é o número mínimo de testes. A e B têm mais do que o número mínimo e D não tem testes suficientes porque não testa a entrada válida. Seria aconselhável fazer mais testes nos vários caracteres que podem suportar injeção SQL, mas esta pergunta é para aplicar EP e obter o número mínimo de casos de teste.	3
23	a	A é a correta, pois cobre os principais cenários para a segurança funcional especificada na exigência. B testa somente os testes válidos. C testa somente as condições de erro. D se expande em testes de ataque, bem como em testes funcionais	2
24	d	D é a correta, porque fornece os critérios de aceitação com base na exigência. 7 é tentador e seria lógico, mas não está especificado na exigência. Os outros não são corretos porque não contêm os critérios adequados. 2 é incorreto onde 3 é correto. 4 é incorreto onde 5 é correto.	2
25	a	A é a correta. Há relatórios e métricas de desempenho de segurança disponíveis que podem ser usados para determinar se você atingiu o nível correto de endurecimento. B não é correto porque uma autenticação forte é apenas um aspecto do endurecimento. C não é correto porque o equilíbrio não é necessário. As áreas mais críticas podem justificar um endurecimento melhor. D não é correto porque existe o perigo de o hacker não lhe dizer o que é encontrado	2
26	c	C é a correta. Ele verifica que o usuário é legítimo e autorizado. A não é correto porque não está olhando para os direitos de acesso. B não é correta porque a utilização dos recursos do sistema não é uma consideração. D não é correta porque a verificação de credenciais comuns não deve ser usada - cada indivíduo deve ter credenciais únicas.	1
27	c	C é a correta de acordo com o syllabus. A não é correta porque deve ser usado um mínimo de 768 bits. B não é correta porque o algoritmo aleatório é fácil de quebrar. D não é correta porque os protocolos WEP devem ser deixados no lugar, não removidos.	2

Q	RC	Comentários	P
28	c	C é a correta de acordo com o syllabus. A não é correta porque as zonas da rede não se concentram no tamanho dos dados. B não é correta. As zonas de rede são partes da configuração do firewall e definem o fluxo autorizado de dados entre redes. D não é correta porque o firewall bloqueia o tráfego, não a zona da rede.	1
29	b	B é a correta porque estes testes podem ser usados para acrescentar novas especificações intrusivas que antes eram consideradas como tráfego autorizado. A e C podem ser úteis, mas não serão tão eficazes quanto B para garantir que a ferramenta funcionará tanto para o futuro quanto para o presente. D é verdadeiro para o uso, mas não para os testes.	2
30	b	B é a correta. A ferramenta malware só pode detectar malware que ela já conhece. B pode estar correta dependendo do foco particular da ferramenta, mas não é uma desvantagem principal. C geralmente não é verdade - as ferramentas são normalmente fáceis de executar. D não é correta porque as ferramentas fornecem a capacidade de se atualizar com novas descobertas e de produzir relatórios	1
31	b	B é a correta de acordo com o syllabus. Uma força bruta ou ataque de dicionário pode ser usada para ver se as informações pessoais ainda estão acessíveis. A não é correta porque geralmente não é viável devido à quantidade de dados e ao tempo que levaria. C não é correta porque isto é mais um exercício anônimo. Além disso, a extensão do campo pode ser limitada, o que pode corromper os dados. D não é correta porque não estamos tentando testar o banco de dados em si.	2
32	c	C é a correta. São as pessoas e seu comportamento que é o elo mais fraco. A, B e D são as preocupações, mas C é o elo mais fraco da cadeia de segurança.	1
33	a	A é a correta. Estas informações poderiam ser usadas para determinar cadeias de aprovação de faturas que poderiam então ser usadas para criar e aprovar faturas falsas se o sistema de contabilidade puder ser pirateado. B não está correta porque a data de nascimento não deve ser usada em nenhuma informação do funcionário, tal como uma senha. C não está correta porque a intranet da empresa deve estar por trás do firewall com outras informações protegidas. D não está correto porque é improvável que esta informação seja útil a um hacker	1
34	d	D é a correta e esse é o seu maior ponto de preocupação. A não é correta e pode ser uma suposição perigosa. B não é correta porque o hacker ainda tem acesso ao sistema. C pode ser verdade, mas a repetição dos mesmos testes não vai ajudar nesta questão	2
35	c	C é a correta. A maior ameaça aqui é que as proteções externas são inúteis porque o atacante já está dentro do sistema. A e B são mais prováveis de ocorrer com um atacante externo. D não é o ataque mais provável - geralmente os usuários internos estão atrás de informações que podem vender ou podem usar para embaraçar a empresa	1
36	c	C é a correta. É o melhor lugar para começar, pois parece que este poderia ter sido o local de origem do problema. Se C não encontrar nada, então A e D seriam os próximos caminhos prováveis a serem seguidos, pois é possível que se trate de um ataque interno (D) ou que os ataques sejam separados e as informações sobre a data de nascimento pode fornecer algumas informações sobre quem esteve perto dele. B poderia ser perseguido, mas seria mais fácil perguntar ao administrador do sistema quem saberia o nome do cão	3

Q	RC	Comentários	P
37	d	D é a correta. A primeira prioridade é ver se a vulnerabilidade está no código de produção e consertar o problema imediatamente. C deve ser o próximo passo para garantir que os desenvolvedores estejam codificando corretamente e usando todas as ferramentas disponíveis para verificar este tipo de problema. A não é correta porque é exatamente isso que os testadores de segurança deveriam estar fazendo. B não é correta porque a permissão da gerência deve ser sempre obtida antes dos testes, e não depois.	2
38	b	B é a correta. As partes interessadas frequentemente têm que tomar decisões comerciais relativas ao nível de risco de segurança que é aceitável e quaisquer planos de mitigação necessários. A não é correta porque todos não precisam saber de tudo. C não é correta porque um plano manual de mitigação de riscos não é viável e os usuários provavelmente não estariam implementando isto de qualquer forma. D não é correta porque as expectativas devem mudar	1
39	c	C é a correta. Os resultados dos testes de segurança devem ser mantidos em sigilo e o acesso aos resultados deve ser rigorosamente controlado. Isto porque o resultado dos testes frequentemente identifica fraquezas no sistema atual em teste e muitas vezes os mesmos problemas existem com o sistema de produção. A não é correta devido à necessidade de controlar rigidamente o acesso aos resultados. B não é correta porque apenas partes limitadas do relatório devem ser disponibilizadas aos desenvolvedores para melhorar sua codificação. Da mesma forma, partes limitadas devem ser disponibilizadas às pessoas da infraestrutura para corrigir quaisquer problemas de infraestrutura que possam ter sido encontrados. D é verdade, mas não é o aspecto mais importante	1
40	c	C é a correta. O impacto do risco deve ser descrito no resumo e detalhado mais adiante no relatório, discutindo vulnerabilidades específicas. A não está correta porque os detalhes não devem constar do resumo. B não é correta porque as informações não devem ser registradas somente no final do relatório. D não é correta porque esta é uma parte importante do relatório.	3
41	a	A é a correta. B não é correta porque existem ferramentas de segurança tanto de análise dinâmica como estática. C não é correta porque os vazamentos de memória são detectados pelas ferramentas de análise dinâmica geral, não pelas ferramentas específicas de segurança. D não é correta porque isto é verdade para todas as ferramentas de análise estática.	1
42	a	A é a correta, pois ambas as técnicas são usadas para testar firewalls. B e C não são corretas porque o objetivo é evitar o ataque em vez de deixá-lo passar pelo firewall. D não é correta porque o endurecimento dos componentes de software ajudará os componentes de software individuais, mas não o firewall e sua implementação.	3
43	c	C é a correta. A licença GNU é livre e é uma comunidade de código aberto, portanto não há fornecedor. A e B não são corretas porque não há fornecedor. D não é correta porque a ferramenta é gratuita, embora você possa ter custos de desenvolvimento na customização da ferramenta para suas necessidades	1
44	b	B é a correta. A não é correta porque os padrões de segurança podem ser mencionados nas metas e objetivos do projeto. C não é correta porque elas são defensivas por natureza. D não	1

Q	RC	Comentários	P
		é correta porque definem certas normas que ajudam a definir práticas - as normas devem ser responsivas a mudanças nas ameaças.	
45	b	B é a correta. Ao definir as normas de segurança, cada parte pode então determinar o que é necessário e especificar melhor esses requisitos. A não é correta porque então é tarde demais! C não é correta porque é provável que os acordos de segurança sejam mantidos privados. D não é correta porque os contratos normalmente não mudam desta forma	1