**Pergunta # 1 (1 pt)**

Qual das seguintes opções é uma finalidade de uma auditoria de segurança?

a. Impedir que os usuários usem senhas simples

b. Revelar atualizações de patch insuficientes fornecidas pelo fornecedor

c. Impedir que intrusos não autorizados acessem o sistema

d. Exigir que os usuários alterem sua senha após um conjunto de dias predeterminado

**Pergunta # 2 (3 pts)**

Você é responsável por garantir que os novos fornecedores trazidos do exterior para o projeto estejam totalmente em conformidade com as diretrizes do governo como parte de sua avaliação de risco. Em qual das partes interessadas devem prioritariamente se concentrar para garantir que esses fornecedores externos continuem cumprindo?

a. Clientes, usuários e fornecedores para garantir que haja uma boa comunicação entre eles

b. Usuários públicos e fornecedores que seguirão a lei conforme aplicável à fonte de informações

c. Agências federais e locais que comunicam diretrizes a seguir

d. Fontes internas e externas, que usarão as informações para analisar ainda mais o risco

**Pergunta # 3 (1 pt)**

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

a. Mais dispositivos são adicionados para mitigar o impacto

b. Os controles adequados de dispositivos de auto provisionamento, como roteadores, são proibidos

c. Dispositivos que não estão em conformidade são removidos da rede sem fio

d. O acesso à VPN é severamente restrito

**Pergunta # 4 (3 pts)**

Sua função como Administrador de Segurança é ajudar sua organização a entender a eficácia de políticas e procedimentos de segurança em toda a empresa. Você relatará suas descobertas de eficácia para Administração Sênior após a conclusão da sua análise. Qual das seguintes é a melhor estratégia para conseguir isso?

a. Implementar uma avaliação de análise estática independentemente para políticas e procedimentos

b. Analise 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 de testes estáticos para ameaças de softwares novos e emergentes

**Pergunta # 5 (1 pt)**

Se uma organização tiver uma violação de segurança e resultados de ação legal, como ajudar a organização de que ela fez os 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 perpetrador

c. Uma vez que qualquer informação importante teria sido copiada antes dos testes de segurança, backup pode ser usado para restaurar qualquer informação comprometida

d. Ao rastrear os testes documentados, a equipe de testes de segurança pode descobrir como violação foi possível

**Pergunta # 6 (1 pt)**

Qual das seguintes afirmações é correta?

a. A garantia da informação é uma parte do teste de segurança

b. Garantia de informação e testes de segurança são dois termos para a mesma coisa

c. O teste de segurança é uma parte da garantia da informação

d. Os dois termos referem-se a diferentes áreas de segurança

**Pergunta # 7 (2 pts)**

Você está trabalhando em um banco como parte da equipe de testes de segurança. Durante uma recente auditoria de segurança, observou 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. Dada esta informação, o que seria um conjunto razoável dos objetivos de segurança para o teste geral de regras de senha?

1. Verifique se as senhas atendem aos requisitos de comprimento

2. Verifique se as senhas atendem aos requisitos de uso de caracteres, números, letras e capitalização

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 que sua senha seja enviada por e-mail para eles

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

**Pergunta # 8 (2 pts)**

Sua empresa recentemente ganhou as manchetes depois que uma violação de segurança resultou em roubo de informações confidenciais de clientes. A gerência reagiu com um decreto que diz que o escopo dos objetivos de testes de segurança precisa ser expandido imediatamente. Enquanto você concorda que algo precisa ser feito, você teme que essa abordagem seja muito reativa e não resulte no teste necessário.

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

a. O teste ainda vai perder problemas porque não será bem focado

b. O teste será terceirizado para que possa ser feito de forma mais eficiente

c. O escopo de teste pode ser muito grande e pode não haver recursos adequados para concluí-lo

d. Os objetivos do teste não estão claramente definidos e podem perder os mesmos problemas que escapou para a produção

**Pergunta # 9 (3 pts)**

Você acabou de aceitar um trabalho para criar uma equipe de testes de segurança para uma empresa cuja informações médicas são compartilhadas entre médicos e hospitais. Você notou que a segurança em torno desta informação não é suficiente para protegê-lo contra hackers ou até mesmo a exposição acidental. A pessoa que teve o seu trabalho anteriormente trouxe um número de consultores para fazer testes, mas as conclusões não foram documentadas e nenhuma alteração foi implementada. Na verdade, você nem sabe qual foi a cobertura do teste. Você apresentou suas descobertas para a equipe de gerenciamento executivo.

Embora tenham concordado em princípio que precisam de testes de segurança, eles não alocaram orçamento necessário ou tempo para o projeto. Parece que enquanto eles pensam que a segurança é uma boa ideia, eles realmente não têm compreensão do que deve ser feito ou como deve ser feito. Qual deve ser o seu primeiro passo para alinhar os executivos ao trabalho que precisa ser feito?

a. Crie uma lista detalhada de todos os possíveis furos de segurança e apresente-os aos executivos

b. Forneça um resumo da abordagem de teste que você propõe e dê exemplos de como o teste será conduzido

c. Traga a equipe jurídica para explicar o que uma violação de segurança poderia custar à organização

d. Crie uma política de segurança e testes de segurança e demonstre como isso se alinha com a sua abordagem de teste proposta

**Pergunta # 10 (2 pts)**

Você acabou de vir de uma reunião em que houve muita discussão sobre a abordagem de segurança da organização. Um dos pontos de ênfase foi a importância do teste para garantir que os dados sejam protegidos de acesso fraudulento, especialmente informações de cartão de crédito. Você foi convidado a preparar um conjunto de objetivos de teste que ajudará a abordar essa área de risco. Uma de suas tarefas é garantir que você está cobrindo todas as preocupações das partes interessadas. Qual grupo de stakeholders tem maior probabilidade de ver os benefícios de seus esforços?

a. Gestão executiva

b. Agentes de Compliance

c. Clientes empresariais

d. Agentes reguladores

**Pergunta # 11 (2 pts)**

Como administrador de segurança, você é responsável por todos os aspectos do processo de segurança, incluindo testes. Para este processo em particular, você deve usar testes conceituais como base para testes manuais e executar estes da perspectiva de um fornecedor externo. Qual processo de teste de segurança faz isso mais paralelo?

a. Criação de testes de segurança de condições e objetivos

b. Implementação de teste de segurança

c. Avaliação geral e relatório de testes de segurança

d. Análise e design de teste de segurança

**Pergunta # 12 (3 pts)**

Você tem desenvolvido um plano de teste de segurança para um sistema que armazenará informações médicas para pacientes e transferirá esses dados para médicos especialistas. Você cobriu as seguintes áreas em seu plano:

• Escopo (o que está no escopo e fora do escopo)

• Papéis e atribuições

• Responsabilidades (fornecedores vs. internos)

• Cronograma de alto nível

• Requisitos de ambiente e configuração

• Lista de autorizações e aprovações necessárias

Quais informações você ainda precisa fornecer neste plano de teste para atender aos requisitos mínimos anotado no programa?

a. Uma lista das credenciais necessárias e treinamento para o pessoal que estará conduzindo o testando

b. Um cronograma mostrando o tempo que será necessário para projetar, executar e avaliar os testes de segurança

c. Uma cópia dos padrões regulamentares que devem ser cumpridos por este sistema

d. Uma lista dos indivíduos que farão o teste e suas informações de contato no evento de uma violação de segurança

**Pergunta # 13 (2 pts)**

Qual dos seguintes casos de teste melhor seria testar o procedimento de segurança de um sistema?

a. Três tentativas de login malsucedidas geram uma mensagem de bloqueio. Entre em contato com seu gerente ou o administrador do sistema para que eles possam lhe dar uma senha temporária pelo telefone. Você deve, então, alterar a senha temporária ao efetuar login. Você efetua logout e, em seguida, efetua login novamente usando sua senha recém-criada.

b. Você recebe uma mensagem de bloqueio após várias tentativas de login. Você chama o suporte de TI para obter uma Nova senha. Você efetua login com a senha temporária, efetua o logout e, em seguida, efetua login novamente. Insira uma nova senha.

c. Depois de várias tentativas, você é bloqueado do sistema. Você usa uma senha que funcionou anteriormente. No entanto, não funciona mais. Você tenta criar uma nova senha, mas você está agora bloqueado. Uma reinicialização completa da máquina é o próximo passo para levá-lo ao prompt de digite novamente a senha.

d. Após a primeira tentativa de usar uma senha inválida, você imediatamente exibe uma lista de senhas seu bloco de notas no seu PC para garantir que você está usando o correto. Você tenta outra senha da lista e funciona.

**Pergunta # 14 (1 pt)**

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

a. Intimamente ligado aos 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 na produção ambiente, a fim de garantir a configuração mais abrangente

**Pergunta # 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 com base em exceções nos casos em que um evento malicioso está em andamento

c. Os riscos da ferramenta raramente são conhecidos antes de serem adquiridos e são melhor descobertos em ferramentas que já estão em uso

d. Como os riscos da ferramenta de teste de segurança são geralmente conhecidos, não há necessidade de uma estratégia de mitigação

**Pergunta # 16 (3 pts)**

Você está revisando um conjunto de resultados de testes de segurança executados em um produto que está passando pelo teste final antes de liberação para produção. Esta é uma atualização de uma versão que está atualmente em produção. A aplicação testada foi o seu site de comércio eletrônico, e ele tem um defeito que permite a criação de scripts entre sites. Qual dos itens a seguir, é o conjunto adequado de etapas que você deve seguir?

a. Relate o problema ao desenvolvedor, inclua-o no relatório de stakeholder e continue testando outros tipos de defeitos

b. Teste se o problema existe na versão de produção atual, documente o defeito em um sistema, notifique o desenvolvedor, continue testando outros defeitos XSS

c. Investigar a extensão do problema, realizando testes adicionais sobre a liberação planejada com concentração particular em outros XSS isses, realizar análise estática no código

d. Informar o gerenciamento, documentar o defeito e incluí-lo em seu relatório de status semanal para partes interessadas, continue testando outros defeitos de segurança para determinar a extensão da segurança problemas

**Pergunta # 17 (1 pt)**

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

a. Teste de componentes

b. Teste de integração

c. Teste do sistema

d. Teste de aceitação de segurança

**Pergunta # 18 (2 pts)**

Você foi convidado pelo analista de negócios para ajudar a definir os requisitos para os aspectos de segurança de um sistema. Este é um sistema de segurança crítico que armazena informações médicas para pacientes e fornece essas informações para profissionais de saúde em hospitais, consultórios médicos e ambulâncias. Em que ponto no ciclo de vida, os requisitos de segurança devem ser documentados e em que nível de detalhe?

a. Eles não devem ser documentados formalmente por causa da necessidade de proteger a segurança da implementação dentro do código de estranhos

b. Devem ser documentados de forma detalhada e inequívoca nos documentos de requisitos durante a fase de requisitos

c. Eles devem ser documentados durante a fase de design, quando a abordagem de código é mais conhecida do que na fase de requisitos, quando a abordagem não é conhecida

d. Eles devem estar restritos aos requisitos funcionais de acesso e disponibilidade da perspectiva do usuário e deve ser documentada durante a fase de requisitos

**Pergunta # 19 (3 ​​pts)**

Uma deficiência foi descoberta na produção. Se um usuário não autorizado copiar um URL de uma sessão de um usuário autorizado, o usuário não autorizado pode colar o URL em sua sessão e continuar o processo com os direitos do usuário autorizado. No caso que foi relatado, o usuário não autorizado foi capaz de usar o URL do usuário autorizado para alterar a senha de administração do sistema. Para fechar essa lacuna, os desenvolvedores verificarão o ID da sessão e o ID do usuário sempre que um URL for usado.

O que é uma preocupação realista para essa correção?

a. Isso não corrigirá o problema e o sequestro de sessão ainda será possível

b. Isso consertará o problema, mas a usabilidade pode ser afetada negativamente

c. Isso resolverá o problema, mas o desempenho pode ser afetado negativamente

d. Isso não corrigirá o problema e exporá 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 estes indicam problemas de segurança que devem ser corrigidos

b. Porque estes indicam potenciais problemas que devem ser investigados

c. Porque isso indica problemas de codificação que causam defeitos funcionais

d. Porque estas indicam práticas de programação deficientes que aumentam a manutenibilidade

**Pergunta # 21 (2 pts)**

Você está testando um sistema que possui 20 componentes definidos. Você fez um extenso teste de segurança em cada um dos componentes. O sistema está agora pronto para entrar nos testes de segurança de integração de componentes. Como você deve abordar esse teste?

a. Como o teste de integração de componentes está relacionado ao somatório das vulnerabilidades dos componentes individuais, realizando os mesmos testes nos componentes integrados é a melhor abordagem.

b. O principal risco agora é a integração dos próprios componentes, então os testes devem cobrir cada interface e verifique se não há vulnerabilidades nas interfaces e nos componentes também deve ser retestado.

c. É provável que novas vulnerabilidades estejam presentes com os componentes integrados, bem o sistema e a infraestrutura maiores que agora são testáveis, por isso os testes devem se expandir para incluir essas novas áreas.

d. Como os componentes agora estão integrados, os riscos de segurança serão reduzidos interações possíveis agora são limitadas, então apenas os pontos de integração devem ser testados e o teste de componente não é necessário.

**Pergunta # 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, você precisará executar. Dada esta informação, qual dos seguintes 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)**

Você recebeu o seguinte requisito para testes de segurança.

Um usuário poderá solicitar sua senha. Se eles fizerem esse pedido, eles devem responder a duas de suas três questões de segurança corretamente. Se eles responderem corretamente, um link será enviado para o email. O link irá levá-los para uma página onde eles podem redefinir sua senha. Depois de redefinir, eles podem fazer login com a nova senha. O link deve ser desativado 1 hora após o envio. O usuário é permitido a apenas duas solicitações de senha sem um reset, após o qual eles terão que ligar para o help desk. Para quaisquer outros erros, o ID do usuário está bloqueado e deve ser desbloqueado pelo suporte técnico.

Qual das alternativas a seguir é a lista mínima de condições de teste para testar adequadamente a segurança funcional coberto por este requisito?

a. Usuário Inválido; usuário válido; 2 respostas corretas; 2 respostas incorretas; bom email; e-mail ruim; restabelecer com boa senha; redefinir com senha incorreta; link bom; Link expirado; dois pedidos sem restabelecer; três pedidos sem reposição

b. Usuário válido; 2 respostas corretas; bom email; redefinir com boa senha; link bom; dois pedidos sem redefinir

c. Usuário Inválido; 2 respostas incorretas; e-mail ruim; redefinir com senha incorreta; Link expirado; três solicitações sem redefinir

d. Estouro de buffer em cada campo de entrada; Injeção de SQL em cada campo de entrada; XXS na página de login e redefinir a página de senha, usuário inválido; usuário válido; 2 respostas corretas; 2 respostas incorretas; Boa o email; e-mail ruim; redefinir com boa senha; redefinir com senha incorreta; link bom; Link expirado; dois pedidos sem reset; três pedidos sem reposição

Pergunta # 24 (2 pts)

Um usuário poderá solicitar sua senha. Se eles fizerem esse pedido, eles devem responder a dois de suas três questões de segurança corretamente. Se eles responderem corretamente, um link será enviado para o e-mail deles. O link os levará para uma página onde eles podem redefinir sua senha. Depois de redefinir, eles podem fazer o login com a nova senha. O link deve ser desativado uma hora após o envio. O usuário é permitido apenas dois pedidos de senha sem um reset, após o qual ele terá que chamar o helpdesk. Para qualquer outro erro, o ID do usuário é bloqueado e deve ser desbloqueado pelo suporte técnico. Qual das seguintes opções é um conjunto válido de critérios de aceitação para esse requisito?

1. O usuário pode redefinir a senha se menos de três solicitações tiverem sido feitas desde a última reinicialização e questões de segurança são respondidas corretamente, e o link é usado para redefinir e uma senha válida é inserido no prompt de redefinição.

2. Mais de dois pedidos resultam no ID do usuário bloqueado.

3. Mais de duas solicitações sem uma redefinição resultam em ID do usuário bloqueado.

4. Mais de duas questões de segurança perderam resultados em erro.

5. Mais de duas questões de segurança perdidas, o ID do usuário está bloqueado.

6. Se um erro de e-mail for recebido pelo sistema, o ID do usuário será bloqueado.

7. Se a senha inválida for inserida na redefinição, o usuário será solicitado com as regras apropriadas.

8. A senha de redefinição pode ser usada para efetuar 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 o endurecimento do sistema em um esforço para testar o sistema a eficácia da segurança. Que procedimento você pode seguir para garantir que os mecanismos de endurecimento lugar está funcionando como esperado?

a. Monitore de perto vários relatórios e métricas de desempenho de segurança para determinar se o nível de acesso e autenticação é alcançado

b. Audite com frequência uma autenticação forte para garantir um alto nível de proteção contra intrusões mantido em todos os momentos

c. Avalie os componentes de hardware que foram endurecidos e compare-os com outros componentes de software reforçados para garantir que o equilíbrio está sendo alcançado

d. Peça a um hacker conhecido que realize uma avaliação independente da eficácia do endurecimento

**Questão # 26 (1 pt)**

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

a. Ele verifica se o usuário tem o perfil correto e os direitos correspondentes para acessar partes limitadas de o sistema

b. É fundamental para identificar a quantidade de recursos do sistema que o usuário pode utilizar

c. Ele verifica se o usuário que entra no sistema é legítimo

d. Ele usa credenciais comuns entre os usuários para entrar no sistema

**Pergunta # 27 (2 pts)**

Mecanismos típicos de criptografia são vulneráveis ​​a ameaças, o que torna importante entender eficácia a qualquer momento. Identifique qual dos seguintes você deve implementar para obter confiança em seus mecanismos de criptografia?

a. Avaliar chaves criptográficas para garantir que elas tenham pelo menos 256 bits de tamanho

b. Certifique-se de estar aplicando algoritmos aleatórios para gerar números aleatórios onde possível

c. Desenvolver testes que garantam que a criptografia simétrica seja usada nos modos corretos

d. Remova todos os protocolos WEP para ver como o sistema executa

**Pergunta # 28 (1 pt)**

Qual é o verdadeiro relacionamento entre um firewall e uma zona de rede?

a. Tanto uma zona de rede quanto um firewall focam no tamanho dos dados que estão sendo transmitidos

b. Uma zona de rede se comunica através de opções seguras de protocolo, enquanto um firewall garante que protocolos são seguros

c. Uma sub-rede pode ser considerada uma zona de rede e um firewall pode ser um monitoramento de tráfego de programas

d. Uma zona de rede bloqueia o tráfego mal-intencionado de uma zona não confiável que o firewall não filtra

**Pergunta # 29 (2 pts)**

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

a. Desenvolver uma série de cenários baseados em experiências passadas

b. Use testes que geram tráfego mal-intencionado para adicionar novas especificações intrusivas

c. Aplique-o a situações de tráfego malicioso conhecido

d. Use-o em conjunto com outros produtos IDS quando possível

**Questão # 30 (1 pt)**

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

a. Eles só detectam certos níveis de malware

b. Eles só podem detectar malwares conhecidos pela ferramenta

c. Eles tendem a ser excessivamente complexos para executar

d. Eles não fornecem recursos de atualização e geração de relatórios

**Pergunta # 31 (2 pontos)**

Você precisa remover os números de identificação pessoal de um sistema legado para reduzir o risco durante teste. Parte do plano de ofuscação de dados inclui a verificação da eficácia com que os dados são mascarados. Qual das seguintes é a abordagem mais eficaz para usar?

a. Verificar manualmente no banco de dados que os dados segmentados para ofuscação não são mais compreensíveis para interpretação humana lógica

b. Projetar um ataque de força bruta nos dados ofuscados

c. Substitua os dados sensíveis por dados aleatórios de comprimentos de string variáveis

d. Recrute as equipes de desenvolvimento para gerar um programa para enfatizar o banco de dados em busca de vulnerabilidades

**Questão # 32 (1 pt)**

O que é frequentemente 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 continuando ameaças de segurança

c. O comportamento dos seres humanos

d. O constante avanço em técnicas maliciosas

**Questão # 33 (1 pt)**

Qual dos seguintes é um risco de segurança em potencial?

a. Publicação do organograma de um departamento de contabilidade no site da empresa

b. Postando desejos de aniversário para um colega de trabalho no Facebook

c. Postando o diretório de telefone da empresa na intranet da empresa

d. Postando experiência profissional em um perfil Linked In

**Pergunta # 34 (2 pts)**

Você é responsável pela segurança que testa o aplicativo financeiro de sua empresa. Você recentemente recebeu 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 dos seus servidores. Você tem verificado e o hacker está correto. Você certificou-se de que o servidor foi atualizado. Sua verificação preliminar não mostrou nenhum traço de como o hacker entrou em seu sistema. Qual deve ser sua preocupação?

a. Não, isso é um hacker de "chapéu branco" e não significa nenhum dano à sua empresa

b. Não, você corrigiu a vulnerabilidade para que o sistema agora esteja seguro

c. Sim, seu teste de segurança não é suficiente e você precisa executar novamente seus testes para ver o que foi perdido

d. Sim, desde que o hacker não admitiu como ele entrou no sistema, ele ainda pode acessá-lo e pode decidir explorar a vulnerabilidade na próxima vez

**Pergunta # 35 (1 pt)**

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

a. O atacante é provavelmente motivado pela curiosidade e será implacável

b. O atacante provavelmente está entediado no trabalho e continuará a invadir o sistema por entretenimento

c. O invasor já está dentro do firewall e é um usuário autorizado do sistema

d. O invasor provavelmente lançará um ataque do DOS que enfraquecerá os servidores

**Pergunta # 36 (3 pts)**

Você está trabalhando em uma organização onde o acesso de administração do sistema aos servidores é altamente restrito. Apenas três funcionários de longo prazo e confiáveis ​​conhecem as senhas raiz. Recentemente, porém, houve várias ocorrências estranhas. Um programa desconhecido, chamado "IKnowYourBirthday" era encontrado para ser executado e estava enviando saudações de aniversário para os membros da equipe. As datas de nascimento estavam corretas e as saudações foram assinadas "Do seu servidor favorito". Este programa foi morto e ninguém poderia descobrir de onde veio. Um segundo problema ocorreu quando a lista de telefones corporativos hackeado e todos os números de telefone foram alterados para 867-5309 (aparentemente retirado da música pelo mesmo nome). A lista correta foi restaurada e, novamente, ninguém conseguiu descobrir como foi feito, embora o novo arquivo tenha sido criado por “root”. Você acabou de receber uma ligação do líder administrador do sistema informando que a senha raiz foi alterada. Foi determinado que a senha foi definida para o nome do cão do administrador do sistema principal.

Outras investigações descobriram que os problemas começaram logo após uma série de infecções e-mails foram detectados. Quando o primeiro foi encontrado, salvaguardas foram imediatamente colocadas em prática para parar qualquer propagação do vírus, mas agora você está se perguntando se alguém conseguiu entrar no sistema via código que foi introduzido no sistema pelo vírus.

O que você deve fazer agora como seu próximo passo de investigação?

a. Verifique se as informações de "IKnowYourBirthday" do RH foram acessadas de fora do sistema e, em caso afirmativo, traçar o endereço IP

b. Verifique se o nome do cachorro do administrador do sistema principal está postado em algum lugar nas mídias sociais

c. Verifique o e-mail suspeito que foi enviado e tente rastrear o endereço IP

d. Verifique os arquivos pessoais dos outros dois administradores do sistema para ver se há uma indicação que eles estão infelizes

**Pergunta # 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 aos clientes em seu site de comércio eletrônico. Seu testador mudou com sucesso o valor para que os clientes recebessem um desconto de 10%. O que você deveria faça primeiro?

a. O testador deve ser desencorajado de criar esses tipos de ataques, pois eles não são realistas no ambiente de produção

b. Informe imediatamente a gerência que o ataque foi criado pela equipe de teste como parte do teste, no caso de ser detectado

c. Trabalhe com os desenvolvedores para implementar verificações, como SSL-trip, para garantir que os certificados sejam válidos e não auto-assinado

d. Verifique a produção para ver se a vulnerabilidade também está no código de produção

**Pergunta # 38 (1 pt)**

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

a. As partes interessadas devem ser educadas sobre todos os riscos de segurança em todos os momentos

b. As partes interessadas tomarão decisões de negócios com base nos níveis de risco de segurança associados

c. Os usuários devem desenvolver um plano de mitigação de riscos baseado em manual

d. As expectativas dos usuários e das partes interessadas em relação à segurança devem ser impedidas de mudar

**Questão # 39 (1 pt)**

Qual das alternativas a seguir é um aspecto importante dos resultados dos testes de segurança?

a. Eles são publicados para usuários e partes interessadas acessarem para ajudá-los melhor entender risco

b. Eles devem ser compartilhados com os desenvolvedores em toda a empresa, a fim de reduzir os riscos para o futuro projetos de desenvolvimento

c. Quanto menos pessoas souberem melhor

d. Os resultados devem ser sempre 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 em produção. Existe um alto grau de risco para este projeto devido à natureza do sistema. Como um resultado, você quer dar ênfase especial ao risco. Com base nisso, qual é a melhor maneira de articular o risco seu relatório?

a. Uma avaliação de risco descritiva incluída no resumo

b. Risco geral incluído na última seção do relatório

c. Impacto ao risco descrito no resumo e posteriormente detalhado em termos de vulnerabilidades específicas

d. O impacto de risco não faz parte do resumo do relatório

**Pergunta # 41 (1 pt)**

De que maneira as ferramentas dinâmicas de análise de segurança são diferentes das ferramentas dinâmica de análise gerais?

a. As ferramentas de segurança investigam o sistema em vez de apenas o aplicativo em teste

b. As ferramentas de segurança funcionam da mesma maneira 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 para o idioma em que o aplicativo é implementado

**Pergunta # 42 (3 pts)**

Você recebeu o trabalho de testar o firewall da organização. Você revisou o plano de implementação e etapas, verificou que a configuração foi configurada conforme instruído pelo fornecedor de firewall e realizou a varredura de portas. Sua organização está particularmente preocupada com ataques de negação de serviço (DOS), particularmente porque eles tinham um quando o antigo firewall estava em vigor. Que tipo de testes você deve realizar para ajudar a detectar comportamentos inesperados que poderiam ser explorados por um ataque DOS?

a. Crie testes que enviem pacotes de rede malformados ou dados difusos e veja se eles são detectados e rejeitados pelo firewall

b. Implementar testes automatizados para testar os servidores para testar os recursos de failover

c. Teste os algoritmos de criptografia e descriptografia para determinar se eles são rápidos o suficiente para lidar com a carga de um ataque do DOS

d. Conduzir o endurecimento dos componentes de software para garantir que a superfície de ataque seja reduzida tanto quanto possível

**Questão # 43 (1 pt)**

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

a. Confiabilidade do fornecedor e capacidade de fornecer suporte

b. Frequência e disponibilidade de atualizações do fornecedor

c. Capacidades técnicas de sua equipe para apoiar e personalizar a ferramenta para o seu ambiente

d. Custo de 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. Eles são consistentes e fáceis de seguir, pois são separados e independentes do projeto metas e objetivos

b. Eles são os blocos de construção para futuros testes de segurança, eliminando a necessidade de começar desde o início

c. Eles descrevem uma ofensa efetiva para enfrentar ameaças antes de entrarem no sistema

d. Eles permitem a latitude nas práticas de segurança, já que as ameaças estão sempre mudando dinamicamente

**Questão # 45 (1 pt)**

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

a. Eles fornecem a cada parte uma saída legal quando um problema de segurança imprevisto afeta produtos

b. Eles fornecem um ponto de partida para ambas as partes iniciarem suas negociações.

c. Eles são uma maneira conveniente de tornar público o acordo entre as partes

d. Eles podem mudar conforme os padrões mudam, mesmo quando o contrato é finalizado

1)B

2)C

3)C

4)B

5)A

6)C

7)B

8)C

9)D

10)C

11)B

12)B

13)A

14)C

15)A

16)B

17)A

18)B

19)C

20)B

21)C

22)C

23)A

24)D

25)A

26)C

27)C

28)C

29)B

30)B

31)B

32)C

33)A

34)D

35)C

36)C

37)D

38)B

39)C

40)C

41)A

42)A

43)C

44)B

45)B