Questão 1

Um ataque só acontece porque vulnerabilidades são exploradas pelos atacantes. Temos que eliminar todos os pontos fracos de nosso ambiente, em todos os níveis.
Analise as afirmativas dentre as principais vulnerabilidades que devem ser evitadas, e assinale a alternativa correta:
I. Falhas de Injeção
II. Autenticação quebrada
III. Exposição de dados sensíveis
Estão corretas as afirmativas:

A. ○ Apenas II e III

B. ● **I, II e III**

C. ○ Apenas I e III

D. ○ Apenas I e II

E. ○ Apenas I

Questão 2

Engenharia social é uma técnica de ataque em segurança da informação.

I. Apesar do nome, a Engenharia Social nada tem a ver com ciências exatas ou sociologia. Na verdade, trata-se de uma das mais antigas técnicas de roubo de informações importantes de pessoas descuidadas, através de uma boa conversa (Virinfo,2002).

II. Consiste na habilidade de obter informações ou acesso indevido a determinado ambiente ou sistema, utilizando técnicas de persuasão (Vargas,2002).

III. Trata-se da arte de convencer, confundir para conseguir obter informações

Analise as afirmativas acima e assinale a correta:

A. ○ Apenas as afirmativas I e III estão corretas.

B. ○ Apenas as afirmativas II e III estão corretas.

C. ○ Apenas a afirmativa I está correta.

D. ○ Apenas as afirmativas I e II estão corretas.

E. ● **Todas as afirmativas estão corretas.**

Questão 3

As ferramentas de segurança visam à prevenção, detecção e resposta a ataques, protegendo os ativos contra ataques que comprometam uma das propriedades básicas de segurança da informação.
Prova: ESAF - CGU - Analista de Finanças e Controle - Tecnologia da Informação - Prova 3 Disciplina: Segurança da Informação | Assuntos: Auditoria de Sistemas;
Considere um sistema no qual existe um conjunto de informações disponível para um determinado grupo de usuários denominados "auditores". Após várias consultas com respostas corretas, em um determinado momento, um usuário pertencente ao grupo "auditores" acessa o sistema em busca de uma informação e recebe, como resposta à sua consulta, uma informação completamente diferente da desejada. Neste caso houve uma falha na segurança da informação para este sistema na propriedade relacionada à:

A. ○ Privacidade

B. ○ Confidencialidade

C. ● **Disponibilidade**

D. ○ Integridade

E. ○ Auditoria

Questão 4

O avanço dos ataques cibernéticos, que vitimam indivíduos, empresas e países, é motivado por uma série de fatores que tomam ainda mais desafiador o trabalho do profissional de segurança da informação.
Técnico de Nível Superior - Análise de Sistemas
https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-seguranca-da-informacao/ataques-e-ameacas
Considere que um *hacker* compromete milhares de *hosts* ao redor do mundo, criando uma *botnet* com intenção maliciosa. Em determinada ocasião, comandados por um computador mestre, estes *hosts* executam um ataque conjunto a um determinado servidor *web* ou DNS, consumindo a largura de banda do servidor e comprometendo seu funcionamento.
O cenário descrito é típico de um ataque denominado:

A. *spoofing*.

B. *phishing*.

C. *worms*.

D. *DoS*.

E. **DDoS**

Questão 5

O avanço dos ataques cibernéticos, que vitimam indivíduos, empresas e países, é motivado por uma série de fatores que tornam ainda mais desafiador o trabalho do profissional de segurança da informação.
Ano: 2020 Banca: FCC Órgão: AL-AP Prova: FCC - 2020 - AL-AP - Analista Legislativo - Administrador de Rede e Telecomunicações
A equipe que administra a infraestrutura de tecnologia da informação precisa liberar acesso sem filtros de proteção para navegação na internet através de dispositivos móveis autenticados na rede como pertencentes aos visitantes que regularmente comparecem à empresa para reuniões executivas. Para isso, um conjunto de equipamentos servidores de domínio WEB (DNS), servidores FTP e um conjunto de switches WiFi serão mapeados nessa rede de visitantes que implementa:

A. ○ um IPS

B. ◉ **uma DMZ.**

C. ○ um IDS.

D. ○ um certificado digital.

E. ○ uma criptografia.

Questão 6

O objetivo e o escopo da auditoria podem estar relacionados com a conformidade com normas, padrões, frameworks, leis e requisitos de negócios.

Analise as técnicas e ferramentas que envolvem interação com pessoas, então assinale o que preenche corretamente a lacuna (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):

_____ são a obtenção de dados via perguntas individuais ou para grupos.

A. ○ Perguntas e observação

B. ○ Questionários

C. ○ Dinâmicas em grupo

D. ○ Entrevistas

E. ● **Pesquisas**

Questão 7

A Criptografia tem como definição que é a arte de escrever ou resolver códigos. A criptografia deriva de duas palavras gregas: *kryptos*, que significa oculto, e *graphien*, que significa escrever. Seu objetivo não é esconder a existência da mensagem, mas sim de apenas ocultar o seu significado.
A respeito dos métodos de criptografia, assinale a opção correta.

A. Na criptografia simétrica, as chaves utilizadas para criptografar uma mensagem possuem o mesmo tamanho, todavia são diferentes na origem e no destino.

B. **Na utilização de chaves públicas, a chave é dividida em duas partes complementares, uma das quais é secreta, eliminando-se, dessa forma, o processo de geração e distribuição de chaves de cifragem.**

C. A cifragem é suficiente para garantir a integridade dos dados que são transmitidos, por isso é dispensável o uso de chaves de autenticação e de assinaturas digitais.

D. Esses métodos classificam-se em cifragem e decifragem de chaves, apenas.

E. Independentemente da técnica de criptografia empregada, a transmissão das chaves de cifragem do emissor para o receptor é desnecessária.

Questão 8

Segurança da informação só é possível se todos da organização seguirem os mesmos princípios e realizarem suas tarefas do dia a dia com base em preocupações comuns de manutenção das propriedades da segurança da informação.
Quando executamos o ataque :"Modificar imagens ou textos de um site ou substituí-los por informações ilegítimas". Estamos nos referindo ao ataque de:

A. ○ Fraude financeira.

B. ● **Phishing.**

C. ○ Ataque DoS (Denial of Service).

D. ○ Roubo de informações confidenciais.

E. ○ Vandalismo.

Questão 9

salvando

A proteção de uma empresa é feita com o uso de mecanismos de segurança tecnológicos, físicos, processuais e regulatórios. É com a sua implementação que as finalidades de prevenção, detecção e resposta a incidentes são cumpridas.
Um equipamento importante de rede utilizado para restringir o acesso a uma rede de computadores, evitando assim um ataque indesejado, é

A. *switch*.

B. chaveador.

C. ***firewall.***

D. roteador.

E. *gateway*.

Questão 10

Há diversas alternativas e elas refletem diretamente em como a segurança e privacidade deve ser tratada por sua empresa, principalmente quanto às responsabilidades.

_____deve ser aplicado no código-fonte, e é importante para remover as vulnerabilidades do código antes do software entrar em produção.

O que preenche corretamente a coluna é:

A. **SAST ou Análise estática**

B. LDST ou Lógica Dinâmica

C. LAST ou Lógica estática

D. IAST ou Forma interativa

E. DAST ou Análise dinâmica

apha

Questão 11

Há diversas alternativas e elas refletem diretamente em como a segurança e privacidade deve ser tratada por sua empresa, principalmente quanto às responsabilidades.

_____que realiza os testes de segurança de uma forma interativada um teste de segurança conhecido como, combinando os testes estáticos e dinâmicos.

O que preenche corretamente a coluna é:

A. ○ LAST ou Lógica estática

B. ○ LDST ou Lógica dinâmica

C. ○ DAST ou Análise dinâmica

D. ● **IAST ou Forma interativa**

E. ○ SAST ou Análise estática

Questão 12

Segurança da informação só é possível se todos da organização seguirem os mesmos princípios e realizarem suas tarefas do dia a dia com base em preocupações comuns de manutenção das propriedades da segurança da informação.

De um modo geral, a manutenção da segurança dos ativos de informação deve cuidar da preservação da:

A. integridade, somente.

B. confidencialidade e integridade, somente.

C. **confidencialidade, integridade e disponibilidade.**

D. confidencialidade, somente.

E. confidencialidade e disponibilidade, somente.

Questão 13

Assinale a alternativa correta que identifica a principal diferença entre os protocolos de internet HTTP e o HTTPS.

A. O protocolo HTTP criptografa a sessão utilizando recursos de um certificado digital.

B. O protocolo HTTP é mais seguro que o HTTPS.

C. Para sua identificação o protocolo HTTP apresenta um cadeado mostrando que é seguro.

D. **O protocolo HTTPS criptografa a sessão utilizando recursos de um certificado digital.**

E. O protocolo HTTP possui uma segurança implementada.

Questão 14

Para Nakamura.(2016), o termo *malware* vem do inglês malicious software, ou software malicioso, que causa, intencionalmente,danos à vítima.
Nakamura, Emílio Tissato. Segurança da Informação e redes. Londrina: Editora e Distribuidora Educacional S.A., 2016. 224 p.
Banca :IDECAN **Órgão:**PRODEB **Prova:**Assistente - Suporte **Analise as afirmativas sobre*softwares* maliciosos, marque V para as verdadeiras e F para as falsas.**
( )Para que o vírus se torne ativo e continue o processo de infecção, é necessário que o programa ou arquivo hospedeiro seja executado.
( )*Botnet* é o conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
( )*Worm* é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.
( )Cavalo de Troia é um programa que permite o retorno de um invasor a um computador comprometido por meio da inclusão de serviços criados ou modificados para este fim.
A sequência está correta em:

A. V, V, V, V.

B. F, V, F, V.

C. **V, F, V, F.**

Questão 15

Há diversas alternativas e elas refletem diretamente em como a segurança e privacidade deve ser tratada por sua empresa, principalmente quanto às responsabilidades.

O que preenche corretamente a coluna é:

_____ também deve ser realizado antes do software entrar em produção, e o teste é com o software funcionando, testando-se as interfaces existentes.

A. LDST ou Lógica dinâmica

B. SAST ou Análise estática

C. **DAST ou Análise dinâmica**

D. IAST ou Forma interativa

E. LAST ou Lógica estática

Questão 16

Com o crescimento da internet e o uso de dispositivos móveis nas empresas é inevitável a ocorrência de problemas de segurança, é preciso muito planejamento e muito trabalho da equipe de TI para ligar com tudo isso. É importante criar normas rígidas e principalmente treinar toda a equipe interna e externa.
A NBR ISO/IEC 27005 define risco como a combinação das consequências advindas da ocorrência de um determinado evento indesejado com a probabilidade de ocorrência desse mesmo evento. A análise e a avaliação de riscos capacitam os gestores a priorizar os riscos. De acordo com essa norma, a atividade de análise de riscos inclui:

A. a avaliação e o tratamento de riscos.

B. **a identificação e a estimativa de riscos.**

C. o tratamento e a aceitação de riscos.

D. a estimativa e o tratamento de riscos.

E. a comunicação e a avaliação de riscos.