Questão 1

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 a afirmativa I está correta.

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

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

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

Questão 2

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 d 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 certificado digital.

B. ● **uma DMZ.**

C. ○ um IPS

D. ○ um IDS.

Questão 3

Engenharia social é uma técnica de ataque em segurança da informação.
Considere o recebimento de um e-mail que informa o usuário a respeito de uma suposta contaminação do computador dele por um vírus, sugerindo a instalação de uma ferramenta disponível em um site da Internet para eliminar a infecção. Entretanto, a real função dessa ferramenta é permitir que alguém tenha acesso ao computador do usuário e a todos os dados lá armazenados. Este método de ataque trata-se de:

A. **Engenharia Social.**
B. Denial of Service.
C. Exploit.
D. Ransoware
E. Sniffer.

Questão 4

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.
Quando *sites* de diversos sofrem ataques através da Internet com o objetivo de deixá-los inacessíveis. Este tipo de ataque é conhecido como:

A. *port scanning.*
B. *cookie hijacking.*
C. ***denial of service.***
D. *phishing.*
E. *backdoor.*

Questão 5

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 exercícios ou atividades especializadas direcionadas a grupos.

A. **Dinâmicas em grupo**
B. Pesquisas
C. Perguntas e observação
D. Questionários
E. Entrevistas

Questão 6

Foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio, pela Internet, de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários.
O ataque definido é conhecido como:

A. *Flood.*
B. ***Phishing.***
C. *Spoofing.*
D. *Botnet.*
E. DoS.

Questão 7

E os testes de segurança são uma das principais atividades de empresas especializadas em segurança e privacidade, com a oferta de serviços de análise de vulnerabilidades e pentests, por exemplo.
Vulnerabilidade é o (a)

A. resultado de um evento que afetou um ativo.

B. potencial causa de um incidente não desejado que pode resultar em danos à organização.

C. efeito da incerteza quanto aos objetivos.

D. **ponto fraco de um ativo que pode ser explorado por uma ameaça.**

E. processo de identificar, reconhecer e tratar riscos.

Questão 8

A forma de executar a auditoria é importante, com o uso das técnicas e ferramentas mais adequadas para cada objetivo.
Analise as afirmativas sobre métodos para avaliar controles conforme (ISACA, 2016) e assinale a alternativa correta:
I. Software de auditoria para analisar o conteúdo de arquivos de dados, como os logs de sistemas e a lista de acesso de usuários.
II.Software especializado para avaliar conteúdo de sistemas operacionais, banco de dados e arquivos de parâmetros de aplicações.
III. Técnicas de desenho de fluxos para documentar processos de negócios e controles automatizados.
Estão corretas as afirmativas:

A. Apenas I

B. **I, II e III**

C. Apenas I e II

D. Apenas I e III

Questão 9

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: GUALIMP Órgão: Prefeitura de Areal - RJ Prova: GUALIMP - 2020 - Prefeitura de Areal - RJ - Técnico em Informática
Qual o malware que sequestra arquivos (e, às vezes, todo o HD), criptografa-os e exige dinheiro de sua vítima em troca de uma chave de descriptografia?

A. ○ *Spyware*.

B. ○ *Worms*.

C. ○ Vírus

D. ○ *Adware*.

E. ● ***Ransomware.***

Questão 10

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.
Aplicada em: 2017 **Banca:** FCC **Órgão:** TST **Prova:** Analista Judiciário – Suporte em Tecnologia da Informação
No contexto da segurança de redes de computadores existem basicamente dois tipos de ataques, o passivo e o ativo. Dentre os ataques do tipo passivo, inclui-se

A. ○ Injeção *SQL*.

B. ○ *Man in the middle*.

C. ○ *DNS spoofing*.

D. ● **Varredura de portas.**

E. ○ Ataque *Smurf*.

Questão 11

A análise de segurança física se inicia com a visita técnica nos ambientes onde são realizadas as atividades relacionadas direta ou indiretamente com os processos de negócio que estão sendo analisados. Esses ambientes devem ser observados com relação a diversos aspectos, sendo que a principal premissa para garantir o controle de acesso é:

A. ○ Tudo é proibido, desde que expressamente declarado.

B. ○ Tudo é permitido, desde que expressamente declarado.

C. ○ Tudo é permitido, menos o que é expressamente proibido.

D. ● **Liberar apenas o estritamente necessário para o uso do usuário.**

E. ○ Liberar tudo para o uso do usuário, mas com senha.

Questão 12

A segurança da informação é direcionada também por aspectos legais, regulatórios e contratuais, como os do setor médico, de telecomunicações ou financeiro
Ano: 2018 Banca: IADES Órgão: APEX Brasil Prova: IADES - 2018 - APEX Brasil - Analista - Serviços Técnicos em Tecnologia da Informação
Acerca do sistema de gestão de segurança da informação (SGSI), é correto afirmar que ele:

A. ○ não inclui processos.

B. ○ não inclui estrutura organizacional.

C. ● **analisa criticamente a segurança da informação.**

D. ○ lida diretamente com riscos de problemas de saúde dos desenvolvedores.

E. ○ tem foco em remover quaisquer riscos do negócio.

Questão 13

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. **confidencialidade, integridade e disponibilidade.**

B. confidencialidade e integridade, somente.

C. confidencialidade e disponibilidade, somente.

D. integridade, somente.

E. confidencialidade, somente.

Questão 14

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

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

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

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

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

E. O protocolo HTTP possui uma segurança implementada.

Questão 15

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.
Diversos recursos e ferramentas são utilizados para melhorar a segurança da informação, principalmente transmissão de informações pela rede de computadores. Nesse contexto, o *hash* é utilizado para:

A. **verificar a autenticidade da mensagem utilizando a chave simétrica gerada no processo de *hashing*.**

B. checar a veracidade de uma assinatura digital junto a uma Autoridade Certificadora.

C. criar uma chave criptográfica específica e personalizada para o arquivo a ser transmitido pela rede.

D. gerar um conjunto de dados de tamanho fixo independentemente do tamanho do arquivo original.

Questão 16

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: 2017 Banca: CIEE Órgão: TJ-DFT Prova: CIEE - 2017 - TJ-DFT - (adaptada)
É um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso.

A. **Cavalo de Troia**

B. ***Spam***

C. ***DDOS***

D. ***Ransonware***

E. ***Cookie***