

Questão 1

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. ☐ Exploit.
- B. ☐ Ransomware
- C. ☐ Denial of Service.
- D. ☐ Sniffer.
- E. ☒ Engenharia Social.

Questão 2

Assinale a alternativa que identifica de forma correta, somente princípios relacionados de forma direta ao contexto de segurança à interconexão dos sistemas.

- A. ☐ Confiabilidade, integridade, disponibilidade, autenticação e confidencialidade.
- B. ☐ Confiabilidade, integridade, disponibilidade, autenticação e repúdio.
- C. ☒ **Confiabilidade, integridade, disponibilidade, autenticação e não repúdio.**
- D. ☐ Confidencialidade, integridade, disponibilidade, programação e configuração.
- E. ☐ Confidencialidade, integridade, disponibilidade, autenticação e configuração.

Questão 3

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.



Ransomware.

B.



Spyware.

C.



Vírus

D.



Adware.

E.



Worms.

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.

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. ☐ Spam
- B. ☐ Cavalo de Troia
- C. ☐ DDOS
- D. ☐ Cookie
- E. ☒ Ransomware

Questão 5

A forma de executar a auditoria é importante, com o uso das técnicas e ferramentas mais adequadas para cada objetivo.

O _____ da ISACA é um framework de auditoria de TI que define padrões para as auditorias de TI relacionadas aos papéis e responsabilidades, ética, comportamento esperado e conhecimento e qualificação requeridas, além de termos e conceitos específicos ao assunto.

O que completa corretamente a definição é:

A. ☐ Ansoff

B. ☐ ITIL

C. ☒ ITAF

D. ☐ COBIT

E. ☐ SWOT

Questão 6

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.

Ano: 2019 Banca: FURB Órgão: Câmara de Timbó - SC Prova: FURB - 2019 - Câmara de Timbó - SC
Afirma-se:

_____: software malicioso que ameaça publicar os dados da vítima ou bloquear perpetuamente o acesso a eles, a menos que um resgate seja pago. _____: software que parece oferecer funcionalidade legítima e benigna, mas, ao ser executado, executa função maliciosa diversa da original. _____: é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores. _____: maneira não documentada de acessar um sistema, ignorando os mecanismos normais de autenticação.

Os termos que preenchem correta e respectivamente as lacunas são:

- A. ☐ Ransomware, Adware, Exploit, Rootkit
- B. ☐ Malware, Adware, Exploit, Rootkit
- C. ☒ Ransomware, Cavalo de Troia, DoS, Backdoor

Questão 7

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, somente.

C. ☐ integridade, somente.

D. ☐ confidencialidade e integridade, somente.

E. ☐ confidencialidade e disponibilidade, somente.

Questão 8

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.

Banca: FGV, 2017, **Órgão:** MPE-BA, **Prova:** Analista Técnico - Tecnologia

Um ciber criminoso envia para sua vítima um e-mail falso, em que se passa por uma instituição conhecida, informando que seu cadastro está irregular e que, para regularizá-lo, é necessário clicar no link presente no corpo do e-mail.

Esse tipo de falsificação de uma comunicação por e-mail é uma técnica conhecida como:

A. ☐ Denial of Service;

B. ☐ Sniffing;

C. ☐ MAC Spoof;

D. ☐ SQL Injection.

E. ☒ Phishing;

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. São aplicações maliciosas caracterizadas por multiplicar-se e espalharem-se automaticamente em redes de computadores, assim como alterar seu próprio conteúdo para não serem identificadas.

- A. ☐ Sniffers
- B. ☐ Cavalos de Tróia (*Trojan Horses*)
- C. ☐ Porta dos Fundos (*Backdoor*)
- D. ☒ Worms (*Vermes*)
- E. ☐ Virus

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. ☒ Varredura de portas.

B. ☐ Ataque Smurf.

C. ☐ DNS spoofing.

D. ☐ Injeção SQL.

E. ☐ Man in the middle.

Questão 11

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 reuniões com profissionais de áreas-chave para a auditoria.

- A. ☐ Dinâmicas em grupo
- B. ☒ Entrevistas
- C. ☐ Questionários
- D. ☐ Pesquisas
- E. ☐ Perguntas e observação

Questão 12

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 interativa é um teste de segurança conhecido como, combinando os testes estáticos e dinâmicos.

O que preenche corretamente a coluna é:

A. ☐ DAST ou Análise dinâmica

B. ☐ SAST ou Análise estática

C. ☐ LDST ou Lógica dinâmica

D. ☐ LAST ou Lógica estática

E. ☒ IAST ou Forma interativa

Questão 13

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

- A. ☒ O protocolo HTTPS criptografa a sessão utilizando recursos de um certificado digital.
- B. ☐ O protocolo HTTP possui uma segurança implementada.
- C. ☐ O protocolo HTTP criptografa a sessão utilizando recursos de um certificado digital.
- D. ☐ O protocolo HTTP é mais seguro que o HTTPS.
- E. ☐ Para sua identificação o protocolo HTTP apresenta um cadeado mostrando que é seguro.

Questão 14

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.

Complete a lacuna e assinale a alternativa correta.

Antes, a _____ tinha como objetivo a comunicação secreta, e atualmente foram acrescentados objetivos de autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, leilões e eleições eletrônicas, dinheiro digital.

- A. ☐ Disponibilidade
- B. ☐ Política da Segurança
- C. ☐ Integridade
- D. ☐ Segurança da Informação
- E. ☒ Criptografia

Questão 15

A 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.

Ano: 2019 Banca: IADES Órgão: AL-GO Prova: IADES - 2019 - AL-GO - Segurança da Informação

Em essência, usa criptografia e autenticação em protocolos de camadas baixas para fornecer uma conexão segura por meio de uma rede insegura, tipicamente a internet.

STALLINGS, W. Cryptography and network security: principles and practice. Londres: Pearson, 2017.

Tradução livre, com adaptações.

O trecho apresentado refere-se a um(a):

- A. ☐ proxy.
- B. ☐ IP (do inglês, Internet Protocol).
- C. ☐ LAN (do inglês, Local Area Network).
- D. ☒ VPN (do inglês, Virtual Private Network).
- E. ☐ Firewall.

Questão 16

Ano: 2020 Banca: IDECAN Órgão: IF-RR Prova: IDECAN - 2020 - IF-RR - Informática

A Internet promove uma série de facilidades, e o estilo de vida moderno passa pela sua utilização. Existe uma série de ataques que podem comprometer a segurança e a disponibilidade da informação que acontecem através da Internet. Um desses ataques consiste em inundar uma máquina com requisições falsas a um serviço, consumindo os recursos dessa máquina (processamento, memória e espaço em disco, etc.), provocando a interrupção do serviço. Marque a opção que indica o ataque descrito.

- A. ☐ Varredura em redes (Scan)
- B. ☐ Força bruta (Brute force)
- C. ☐ Interceptação de tráfego (Sniffing)
- D. ☐ Falsificação de e-mail (E-mail spoofing)
- E. ☒ Negação de serviço (DoS)