Nome: _____

Documento: _____

Questão 1:
A gestão segura de contas online é uma preocupação constante para usuários e empresas, visando proteger informações pessoais e acessos indevidos. Nesse sentido, qual das seguintes práticas é fundamental para proteger suas contas online?

A) Utilizar a mesma senha para todas as contas, desde que seja uma senha longa.
B) Anotar senhas em papéis e guardá-los próximos ao computador.
C) Criar senhas fortes, únicas para cada serviço, e habilitar a verificação em duas etapas sempre que possível.
D) Compartilhar senhas apenas com amigos ou familiares de confiança.

Questão 2:
Uma das práticas mais importantes para prevenir diversas vulnerabilidades em aplicações web, incluindo XSS e SQL Injection, envolve o tratamento cuidadoso e a verificação de todos os dados recebidos de fontes externas, como formulários de usuários ou parâmetros de URL, antes de serem processados ou armazenados. Qual é o nome genérico dessa prática essencial de programação segura?

A) Criptografia de ponta a ponta
B) Validação de Entrada (Input Validation) e Sanitização de Dados
C) Balanceamento de Carga
D) Virtualização de Servidores

Questão 3:
Quando um incidente de segurança é identificado, uma resposta rápida e estruturada é essencial para minimizar os impactos e restaurar a normalidade o mais breve possível. Considerando o processo de tratamento de incidentes, qual das etapas abaixo é crucial e geralmente uma das primeiras a ser realizada após a detecção?

A) Erradicação completa do agente causador do incidente.
B) Comunicação do incidente a todos os funcionários da empresa.
C) Contenção do incidente, para evitar que se espalhe e cause mais danos.
D) Análise forense detalhada para identificar o culpado.

Questão 4:
Para avaliar proativamente a segurança de sistemas e aplicações, empresas frequentemente recorrem a simulações de ataques, buscando identificar falhas antes que sejam exploradas por agentes mal-intencionados. Nesse contexto, qual é o principal objetivo da execução de um teste de penetração (pentest)?

A) Garantir que o sistema estará 100% seguro contra qualquer tipo de ataque.
B) Substituir a necessidade de outras medidas de segurança, como firewalls e antivírus.
C) Punir os desenvolvedores que introduziram falhas de segurança no sistema.
D) Identificar e explorar vulnerabilidades em um sistema ou aplicação de forma controlada, simulando um ataque real.

Questão 5:
Um princípio fundamental em segurança da informação estabelece que usuários, programas ou processos devem operar utilizando o menor conjunto possível de permissões necessárias para realizar suas tarefas legítimas. O objetivo é minimizar o dano potencial em caso de comprometimento. Como é conhecido este princípio?

A) Defesa em Profundidade
B) Princípio da Mínima Surpresa
C) Princípio do Menor Privilégio (Least Privilege)
D) Segurança por Obscuridade

Questão 6:
Muitas violações de segurança não exploram falhas técnicas complexas em software, mas sim a tendência humana a confiar ou a ser enganada. Essa abordagem foca em manipular psicologicamente indivíduos para que realizem ações ou divulguem informações confidenciais. Como é chamada essa técnica de ataque?

A) Engenharia Reversa
B) Engenharia Social
C) Ataque de Força Bruta
D) Ataque de Negação de Serviço Distribuído (DDoS)

Questão 7:
Diversos dispositivos e softwares são empregados para garantir a segurança de redes corporativas e domésticas, filtrando e monitorando o fluxo de informações. Dentre eles, o Firewall desempenha um papel crucial. Qual o principal objetivo de um Firewall em uma rede de computadores?

A) Criptografar todos os dados que trafegam na rede interna.
B) Detectar e remover vírus e malware dos computadores da rede.
C) Controlar o tráfego de dados entre redes distintas, permitindo ou bloqueando comunicações com base em regras predefinidas.
D) Autenticar usuários antes que acessem qualquer recurso da rede.

Questão 8:
Em sistemas de informação, especialmente em aplicações web, é crucial verificar corretamente quem é o usuário e, subsequentemente, o que ele tem permissão para fazer dentro do sistema. Qual a diferença fundamental entre os processos de Autenticação e Autorização?

A) Autenticação verifica "quem você é" (identidade), Autorização verifica "o que você pode fazer" (permissões).
B) Autenticação verifica "o que você pode fazer" (permissões), Autorização verifica "quem você é" (identidade).
C) Autenticação é o processo de registrar um novo usuário no sistema, Autorização é o processo de login de um usuário existente.
D) São termos sinônimos para o mesmo processo geral de controle de acesso a recursos.

Questão 9:
A proliferação de softwares maliciosos, conhecidos como malware, representa uma ameaça constante para dispositivos e dados, podendo causar desde lentidão até o roubo de informações sensíveis. Qual das seguintes ações é uma medida preventiva importante contra malware?

A) Clicar em todos os links recebidos por e-mail para verificar sua veracidade.
B) Baixar softwares apenas de fontes desconhecidas, pois geralmente são gratuitos.
C) Manter o sistema operacional e os aplicativos sempre atualizados e utilizar um bom software antivírus.
D) Desabilitar o firewall do sistema para melhorar a velocidade da conexão com a internet.

Questão 10:
Em aplicações web, uma vulnerabilidade comum permite que atacantes injetem scripts maliciosos, que são então executados no navegador de outros usuários, podendo roubar informações de sessão ou redirecioná-los para páginas fraudulentas. Como essa vulnerabilidade é conhecida?

A) SQL Injection
B) Man-in-the-Middle (MitM)
C) Denial of Service (DoS)
D) Cross-Site Scripting (XSS)

Gabarito

Questão	Alternativa Correta
1	C
2	B
3	C
4	D
5	C
6	B
7	C
8	A
9	C
10	D