Exercícios de Revisão – Sistemas Computacionais e Segurança

Respostas elaboradas para fins acadêmicos.

# **1) O que é um pentest? Quais são as etapas de um pentest?**

Pentest é um teste de invasão autorizado, feito para identificar vulnerabilidades em sistemas, redes ou aplicações. As etapas principais incluem: planejamento, reconhecimento, varredura, exploração, pós-exploração e relatório.

# **2) Explique o funcionamento de 3 ataques de segurança cibernética que podem comprometer diretamente a DISPONIBILIDADE de sistemas.**

- Ataques DDoS: sobrecarregam servidores com tráfego falso, deixando o serviço fora do ar.  
- Ransomware: criptografa dados e bloqueia acesso ao sistema.  
- Falhas de software (como buffer overflow): podem travar ou derrubar o sistema.

# **3) Qual o conceito abordado no texto de Hintzbergen?**

Conformidade.

# **4) Quadro comparativo entre Firewall, IDS e IPS:**

Firewall: controla o tráfego de rede, filtrando pacotes com base em regras.  
IDS (Sistema de Detecção de Intrusão): monitora e detecta atividades suspeitas, mas não reage automaticamente.  
IPS (Sistema de Prevenção de Intrusão): detecta e reage automaticamente, bloqueando tráfego malicioso.

# **5) Três conselhos para proteger senhas:**

- Use senhas fortes com letras, números e símbolos.  
- Ative autenticação de dois fatores (2FA).  
- Não reutilize senhas e use um gerenciador de senhas.

# **6) Questão com imagem – Segurança da informação:**

a) Vulnerabilidade: uso de software pirata.  
b) Ameaça: instalação de malware disfarçado.  
c) Ação defensiva: utilizar apenas softwares licenciados e originais.

# **7) Questão com imagem – Segurança na configuração de sistemas:**

a) Vulnerabilidade: uso de credenciais padrão (admin/admin).  
b) Ameaça: acesso não autorizado ou ataques automatizados.  
c) Ação defensiva: trocar as credenciais padrão, usar senhas fortes e restringir o acesso à interface administrativa.

# **8) Criptografia:**

a) Ana deve cifrar com a chave pública de Bob para garantir sigilo.  
b) Bob usará sua chave privada para decifrar.  
c) Para garantir autenticidade para Carlos, Ana deve assinar com sua chave privada.  
d) Carlos verifica a assinatura usando a chave pública de Ana.

# **9) Certificado digital do Banco do Brasil:**

a) O cliente recebe o certificado contendo a chave pública do banco. Ele usa essa chave para criptografar uma chave de sessão, que o servidor descriptografa com sua chave privada.  
b) Benefícios: autenticidade (confirma a identidade do banco) e confidencialidade (protege os dados da transação).

# **10) Três registros importantes para auditoria de segurança:**

- Log de acessos ao sistema (data, hora, IP, usuário).  
- Registro de alterações em arquivos sensíveis.  
- Tentativas de login mal-sucedidas ou acessos negados.