Exercicios de Revisão

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

Um **pentest (teste de penetração)** é um teste simulado de ataque a um sistema para identificar vulnerabilidades. As principais etapas são:

1. Planejamento e reconhecimento;
2. Varredura (scanning);
3. Obtenção de acesso;
4. Manutenção de acesso;
5. Análise e relatório.

---

2) Explique o funcionamento de 3 ataques que comprometem a *DISPONIBILIDADE* dos sistemas.

- **DDoS (Distributed Denial of Service):** Envia grande volume de tráfego para sobrecarregar servidores e tirar o sistema do ar.
- **Ransomware:** Sequestra os dados e impede o acesso até que um resgate seja pago.
- **Exploração de bugs (como buffer overflow):** Pode travar o sistema e tornar o serviço indisponível.

---

3) Conceito referido no texto:

Conformidade.
As empresas devem estar em **conformidade** com leis, regulamentos e contratos para garantir a segurança da informação.

---

4) Quadro comparativo: Firewalls, IDS e IPS

Recurso	Função	Atuação	Ação
Firewall	Controla o tráfego de entrada e saída	Preventiva	Bloqueia ou permite pacotes

Recurso	Função	Atuação	Ação
IDS (Intrusion Detection System)	Detecta intrusões	Monitoramento passivo	Gera alertas
IPS (Intrusion Prevention System)	Previne intrusões	Monitoramento ativo	Bloqueia ações maliciosas automaticamente

---

5) Três conselhos para proteger senhas:

1. Use senhas longas e complexas (com letras, números e símbolos).
2. Não reutilize senhas em diferentes serviços.
3. Utilize um gerenciador de senhas confiável.

---

6) Imagem 1 – Segurança da Informação

a) **Vulnerabilidade:** Falta de autenticação ou senhas fracas.
b) **Ameaça:** Acesso não autorizado ao sistema.
c) **Ação defensiva:** Implementar autenticação multifator (MFA) e exigir senhas fortes.

---

7) Imagem 2 – Segurança da Informação

a) **Vulnerabilidade:** Porta USB destrancada ou sistema sem bloqueio físico.
b) **Ameaça:** Inserção de dispositivos maliciosos (ex: pendrive com malware).
c) **Ação defensiva:** Desabilitar portas USB ou usar software de controle de dispositivos.

---

8) Criptografia com Bob e Carlos:

a) Para Bob: Ana deve **cifrar a mensagem com a chave pública de Bob**.
b) Bob decifra: usando **sua chave privada**.
c) Para Carlos: Ana deve **cifrar com sua própria chave privada** (garantia de autoria).
d) Carlos decifra: usando a **chave pública de Ana** para verificar a autenticidade.

---

9) Certificado Digital do Banco do Brasil

9.a)

- **Origem (cliente):** Usa a **chave pública do Banco** para cifrar.
- **Destino (Banco):** Usa sua **chave privada** para decifrar.

9.b) Benefícios de segurança:

1. Garante a **autenticidade** do site.
2. Garante **criptografia segura** na comunicação, protegendo os dados.

---

10) Três registros importantes para auditoria:

1. Tentativas de login (bem-sucedidas e falhas).
2. Acessos a arquivos e sistemas críticos.
3. Alterações em configurações de segurança ou políticas do sistema.