Respostas - Atividade de Segurança da Informação

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

Pentest (ou Teste de Penetração) é uma simulação controlada de ataque a um sistema ou rede, com o objetivo de identificar vulnerabilidades que poderiam ser exploradas por invasores reais.

Etapas:

1. Planejamento e Reconhecimento

2. Varredura

3. Ganho de Acesso

4. Manutenção de Acesso

5. Análise e Relatório

## 2) Três ataques que comprometem a DISPONIBILIDADE de sistemas:

1. DDoS: Sobrecarga de tráfego que torna um serviço inacessível.

2. Ransomware: Criptografa os dados e exige resgate, paralisando o sistema.

3. Ping da Morte: Envio de pacotes ICMP malformados que travam o sistema.

## 3) Conceito abordado no texto de Hintzbergen (2018):

Conformidade.

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

| Recurso | Função Principal | Atua em Tempo Real? | Toma Ação? |

|-----------|--------------------------------------|----------------------|----------------|

| Firewall | Controla tráfego com base em regras | Sim | Sim |

| IDS | Detecta atividades suspeitas | Sim | Não (só alerta)|

| IPS | Detecta e bloqueia ataques | Sim | Sim |

## 5) Três conselhos para proteger senhas:

1. Use senhas fortes e variadas.

2. Ative a autenticação de dois fatores (2FA).

3. Utilize um gerenciador de senhas.

## 6) Imagem 1 - Cópia do Windows não original:

a) Vulnerabilidade: Uso de software pirata.

b) Ameaça: Malware embutido e falta de atualizações.

c) Ação defensiva: Utilizar software original e atualizado.

## 7) Imagem 2 - Instalação do Apache Tomcat:

a) Vulnerabilidade: Uso de credenciais padrão (admin/admin).

b) Ameaça: Acesso não autorizado ao servidor.

c) Ação defensiva: Alterar credenciais e restringir acesso.

## 8) Envio de mensagens criptografadas:

a) Ana cifra com a chave pública de Bob.

b) Bob decifra com sua chave privada.

c) Ana cifra com sua chave privada.

d) Carlos decifra com a chave pública de Ana.

## 9) Certificado digital - www.bb.com.br:

9.a) O servidor apresenta o certificado.

O navegador valida e usa a chave pública para criptografia.

9.b)

1. Confidencialidade da comunicação.

2. Autenticidade do site acessado.