**UNIVERSIDADE SÃO JUDAS TADEU SISTEMAS DE INFORMAÇÃO**

**Henrique Lima Candido**

**UC SISTEMAS COMPUTACIONAIS E SEGURANÇA**

**Atividade 1 - Resolução da revisão**

1. Pentest (Teste de Penetração) é uma simulação controlada de ataque para identificar vulnerabilidades em sistemas. Suas etapas são: Planejamento;

Reconhecimento; Varredura e Enumeração; Exploração; Pós-exploração e

Relatório.

1. DDoS: Envia tráfego excessivo para derrubar o sistema;

Ransomware: Bloqueia acesso aos dados até pagamento;

Desfiguração (Defacement): Modifica páginas web e pode tirar o site do ar.

1. O conceito no qual o texto se refere é conformidade.

**4-**

|  |  |  |  |
| --- | --- | --- | --- |
| Quadro comparativo | |  | |
| Recurso | Função Principal | Tipo | Atua em tempo real |
| Firewall | Filtrar tráfego (entrada e saída) | Software/Hardware | Sim |
| IDS | Detectar intrusões | Somente monitoramento | Sim |
| IPS | Detectar e bloquear intrusões | Preventivo (ação imediata) | Sim |
|  |  |  |  |

1. Conselhos importantes seriam: Usar senhas fortes (mistura de letras, números e símbolos); Ativar autenticação de dois fatores (2FA); Nunca reutilizar senhas em diferentes serviços.

1. a) A vulnerabilidade: Uso de sistema operacional sem licença original (pirata).
2. A ameaça: A ameaça é a possibilidade de o sistema estar comprometido por causa da falsificação de software.
3. Ação defensiva: Usar software original e manter o sistema atualizado.

**7-** a) Vulnerabilidade: Uso de credenciais padrão (ex: "admin") e possível senha fraca.

1. Ameaça: Invasores podem acessar o servidor Tomcat e controlar a aplicação.
2. Ação defensiva: Trocar usuário/senha padrão, usar senha forte e limitar acesso à interface de administração.

**8-** a) Como Ana deverá cifrar a mensagem para Bob:

Ana deve criptografar com a chave pública de Bob, garantindo que só ele possa decifrar.

b) Como Bob deverá decifrar a mensagem de Ana corretamente: Bob usa sua chave privada para decifrar a mensagem recebida. c) Como Ana deverá cifrar a mensagem para Carlos:

Ana deve assinar digitalmente com sua chave privada (para garantir autenticidade). d) Como Carlos deverá decifrar a mensagem de Ana corretamente:

Carlos usa a chave pública de Ana para verificar a assinatura e garantir que foi ela quem enviou.

**9-** a) O certificado é usado para identificar o site do Banco do Brasil (origem) e garantir que o usuário (destino) está se conectando com segurança. A chave privada assina e a pública valida a identidade.

b) Dois benefícios de segurança do uso do certificado digital:

Autenticidade - Garante que o site acessado é realmente do Banco do Brasil. Confidencialidade - Criptografa os dados trocados, protegendo contra interceptações.

**10-** 1. Login e logout dos usuários - Identifica quem acessou o sistema e quando.

1. Acesso a arquivos ou sistemas sensíveis- Mostra quais dados foram consultados ou modificados.
2. Tentativas de acesso não autorizado - Ajuda a detectar possíveis ataques ou uso indevido.