Aula 22/11/2021 – Exercícios de Fixação

Prof. Felipe Oliveira

1. Segurança de Acesso é hoje:
   a. Somente para instalações físicas.
   b. Apenas para equipamentos computacionais.
   c. Somente para equipamentos de rede
   d. Tanto para acesso físico à instalações quanto para acessos lógicos a plataformas computacionais ou equipamentos de rede.

2. Sobre senhas, todas as alternativas estão corretas **exceto**:
   a. Uma senha serve para autenticar uma conta
   b. Assegura que você é quem diz ser e que possui o direito de acessar o recurso.
   c. A senha não faz parte dos mecanismos de autenticação.
   d. É um dos principais mecanismos de autenticação

3. Ao gerar uma senha de acesso você **não deve:**
   a. Utilizar números aleatórios.
   b. Utilizar dados pessoais como a placa do seu carro.
   c. Usar uma grande quantidade de caracteres.
   d. Usar uma senha com diferentes tipos de caracteres.

4. São exemplos de controle de acesso físico:
   a. O portas eletrônicas, cancelas e catracas.
   b. O sistema de login do sistema operacional.
   c. O registro de ações (log) em um roteador.
   d. A autenticação em uma rede wi-fi.

5. Biometria é ramo da ciência que estuda:
   a. Os biomas existentes na natureza.
   b. Os efeitos biológicos das ações humanas.
   c. As medidas dos seres vivos.
   d. Estuda as medidas das árvores.

6. São exemplos de informações biométricas, **exceto**:
   a. Geometria das mãos.
   b. Reconhecimento da voz.
   c. O odor ou cheiro de uma pessoa.
   d. Uma senha forte.

7. Sobre controle de acesso lógico é correto dizer que:
   a. Pode ser entendido como o conjunto de procedimentos relacionados aos softwares utilizados para controlar o acesso à um recurso computacional.
   b. É uma forma de impedir que uma pessoa tenha acesso físico à um recurso.
   c. É a utilização de lógica para impedir que pessoas não autorizadas acessem recursos restritos.
   d. Todas as alternativas estão corretas.

8. A partir da análise de informações presentes em *Logs* é é possível:
   a. Detectar problemas.
   b. Rastrear as ações executadas por um usuário.
   c. Detectar um ataque e usos indevidos de um computador.
   d. Todas as alternativas anteriores.

9. Sistemas de detecção de intrusão (IDS) são fundamentais para garantir visibilidade em computadores e redes. Sobre eles é correto dizer:
   a. Um IDS é um sistema onde um segurança aponta intrusos em uma sala.
   b. IDS é a pessoa responsável por monitorar uma rede e identificar possíveis ataques.
   c. IDS são programas de computador que monitoram uma rede ou um servidor a procura de sinais ou padrões de comportamento que sejam considerados maliciosos.
   d. Um IDS atua para impedir que atacantes invadam um sistema.

10. Em um sistema Linux o utilitário *syslog* é responsável por registrar tudo que ocorre no sistema. Os logs são salvos no diretório:
   a. /usr/bin
   b. /tmp/sistema
   c. /home/usuário
   d. /var/logs