**Instituto Federal Sul-rio-grandense – Campus Camaquã**
**Disciplina: Administração e Segurança em Redes de Computadores – Turma 2024**
**Professor: Vinícius Alves Hax**
**Assunto: Revisão do conteúdo do 3º bimestre**

**1. Cite e explique os pilares da segurança da informação.**

Os principais pilares da segurança da informação são:

- Confidencialidade: Garante que a informação seja acessível apenas a pessoas autorizadas. Por exemplo, dados bancários de clientes devem ser acessíveis apenas pelos próprios clientes e funcionários autorizados do banco;
- Integridade: Assegura que a informação não seja alterada de maneira não autorizada. Isso significa que, quando um dado é enviado, ele deve chegar ao destino sem modificações. E lá permanecer sem modificações indevidas;
- Disponibilidade: A informação deve estar disponível quando for necessária. Se um servidor de banco de dados ficar fora do ar, por exemplo, isso comprometeria a disponibilidade da informação.

Um outro pilar que não é elencado com tanta frequência é o não-repúdio. O não-repúdio se refere a pessoa não poder negar que realizou alguma ação digital.

**2. A segurança da informação se preocupa somente em lidar com ataques partindo de pessoas? Justifique.**

Não, a segurança da informação não se preocupa apenas com ataques feitos por pessoas. Ela também considera riscos relacionados a falhas técnicas, como *bugs* em sistemas, falhas de *hardware* e/ou *software*, desastres naturais (como incêndios ou inundações) e erros humanos. Além disso, vulnerabilidades em *softwares*, sistemas desatualizados ou até problemas internos (como funcionários descuidados) também são focos de preocupação na segurança da informação.

**3. O que é engenharia social?**

Engenharia social é uma técnica de manipulação usada para enganar pessoas e fazer com que elas revelem informações sensíveis, como senhas ou dados pessoais. Em vez de atacar um sistema diretamente, o atacante tenta enganar a vítima. Isso pode ser feito por telefone, e-mail, ou até pessoalmente onde o atacante se faz passar por uma pessoa ou instituição confiável para conseguir informações.

**4. O que é criptografia?**
a) Um processo de verificação de usuários em uma rede
b) Um método para codificar dados para proteger contra acesso não autorizado
c) Uma técnica de acesso direto a dados sigilosos
d) Uma configuração de *firewall* para proteger uma rede

**5. Em qual das situações abaixo a conexão é criptografada por padrão?**
a) Acesso a um site via navegador usando http
b) Envio de e-mail através de um cliente local
c) Conexão de terminal via ssh
d) Transferência de arquivos por ftp

**6. Considerando uma aplicação da cifra de César, utilizando somente as letras de A até Z e rotação 2 (por exemplo, A = C, B = D, Z = B) como ficaria a codificação da mensagem “BOA PROVA”? (Para fins de simplificação os espaços são copiados de maneira idêntica)**

DQC RTQXC

**7. Existem diferentes tipos de autenticação. Um desses tipos é realizar a autenticação com base em algo que o usuário tem (um crachá, um pendrive, etc). Quais as vantagens e desvantagens desse tipo de autenticação?**

Podemos citar como algumas das vantagens:

- Praticidade: O usuário não precisa lembrar de senhas ou PINs, pois o dispositivo físico (crachá, pendrive,etc) é o que garante o acesso;
- Maior segurança: Pode ser mais difícil de falsificar um objeto físico do que adivinhar uma senha simples;
- Um objeto físico é passível de ser emprestado, como uma chave, por exemplo.

Entretanto podemos citar, por exemplo, as seguintes desvantagens:

- Perda ou roubo: Se o usuário perder o dispositivo ou ele for roubado, o atacante pode ter acesso à conta ou sistema;
- Dependência de hardware: Se o dispositivo for danificado ou não funcionar corretamente, o usuário pode não conseguir acessar o sistema.

**8. Em se tratando de senhas, a senha “paralelepipedo” tem algumas desvantagens em relação a senha “fjr49fk”. Quais são essas desvantagens? E existe alguma vantagem?**

Desvantagens da senha “paralelepipedo”:

- A senha “paralelepipedo” é uma palavra do vocabulário, que pode ser adivinhada por ataques de dicionário, tornando-a menos segura;
- Falta de complexidade: Ela não mistura letras, números e caracteres especiais, o que a torna mais fácil de quebrar se o conjunto de caracteres (supondo que só sejam permitidas letras no caso).

Vantagens:

- “Paralelepipedo” pode ser mais fácil de lembrar para um ser humano, já que é uma palavra comum e sem combinação de caracteres aleatórios;
- Por possuir um tamanho maior (14 caracteres) um programa que tente todas possibilidades possíveis de números e letras irá demorar mais para tentar essa combinação.

**9. Cite três medidas que um usuário comum pode usar para fazer um uso mais seguro dos sistemas informatizados?**

Algumas das medidas possíveis incluem:

- O usuário deve configurar o seu sistema para pedir algum tipo de autenticação;
- Usar senhas fortes e únicas: Evitar senhas fáceis e garantir que cada serviço tenha uma senha diferente;

- Habilitar a autenticação de dois fatores (2FA): Isso adiciona uma camada extra de segurança, exigindo que o usuário forneça não apenas a senha, mas também um código temporário enviado por SMS ou gerado por um aplicativo;
- Manter o software atualizado: Instalar atualizações regularmente para corrigir vulnerabilidades de segurança nos sistemas operacionais e aplicativos;
- Realizar backup periodicamente dos dados considerados importantes.

**10. Considerando o contexto de um pentest, no que consiste a etapa de "mapeamento de hosts"?**

O mapeamento de hosts é uma etapa em que o pentester (profissional de testes de invasão) identifica quais dispositivos (computadores, servidores, roteadores, etc.) estão presentes em uma rede. O objetivo é descobrir quais são os hosts ativos, seus endereços IP, e os serviços que estão sendo executados nos mesmos. Isso ajuda a entender o ambiente de rede e a localizar possíveis vulnerabilidades nos dispositivos encontrados. Para isso, são usadas ferramentas que fazem varreduras e tentam identificar portas abertas, sistemas operacionais e outros detalhes sobre a rede.