Disciplina Redes e Segurança

Mateus Avilla Machado IN231

1. **Por que toda a segurança é relativa?**

   Pois deve-se estabelecer um equilíbrio, levando em consideração diversos fatores como grau de importância, custos para adquirir e manter, manutenção, etc.

2. **Diferencie vulnerabilidade e ameaça**

   Vulnerabilidades são as falhas de segurança dentro de tal sistema ou infraestrutura, que possibilita um ataque, seja ele uma varredura de rede, um interceptador de tráfego, ataque tipo Força Bruta, entre outros. Já uma ameaça é quando algo ou alguma coisa pode causar uma violação na integridade da segurança, sendo intencional ou não.

3. **Quais as principais origens das vulnerabilidades?**

   Podem ser causadas por erros no desenvolvimento do sistema, o usuário acessou um link malicioso, erros na configuração de aplicativos de segurança e firewall, entre outros.

4. **Com relação aos ataques sobre o fluxo de informação, escreva sobre cada tipo de ataque. Classifique-os ainda como passivos ou ativos.**

   São classificados em:
   Interrupção: Este ataque afeta a disponibilidade do serviço ou sistema – é um ataque do tipo ativo.

   Intercepção: Este ataque intercepta as informações do determinado sistema ou serviço - passivo

   Modificação: Este ataque consegue acessar e modificar as informações de determinado sistema ou serviço – ativo

5. **O que é um vírus e como ele funciona? Diferencie o funcionamento de um vírus de boot e de um vírus de arquivo.**

   Um vírus nada mais é do que um software malicioso, que é projetado para invadir um sistema ou uma rede de computadores, para diversas finalidades. Os cibercriminosos que projetam esses vírus podem desenvolve-los de acordo com suas necessidades. Os vírus de arquivo são vírus projetados para agir em um determinado programa executável do Windows, que pode alterar ou sobrescrever o código do arquivo, podendo adicionar um código malicioso, podendo abrir uma backdoor no computador, para facilitar uma posterior entrada dos cibercriminosos. Já os vírus de boot são vírus que infectam a área de inicialização do sistema operacional, sendo muito difíceis de serem encontrados e removidos visto que muitas vezes esses vírus impedem a inicialização dos sistemas operacionais e dos computadores.

6. **Descreva o princípio de funcionamento de um cavalo de Tróia (trojan horse).**

   É um malware que se camufla, escondendo o seu real propósito. Estes malwares podem acessar informações pessoais do usuário, informações sensíveis como dados bancários, dados pessoais, dentre outros. Este malware, por conta de se camuflar, é difícil de ser encontrado por um usuário comum, principalmente sem o uso de um programa antivírus.

7. **Descreva um firewall e um servidor proxy.**

   Firewall é um equipamento dedicado ou um programa instalável que aplica e gerencia políticas de segurança, monitorando o tráfego da rede e gerenciando as informações que entram e saem. Já um servidor proxy é um servidor dedicado que serve como um intermediário entre o cliente e outros servidores que o usuário precisa acessar para obter certas informações.

8. **Criptografia: por que seu uso é tão importante em sistemas de informação?**

   A criptografia é importante pois ela garante que as informações criptografadas não sejam acessadas por pessoas não autorizadas. Existem diversos níveis de criptografia, o mais comum é a criptografia simétrica, que nada mais é do que a utilização de uma chave específica para codificar e traduzir as informações criptografadas, logo, apenas as pessoas que possuem essa chave podem acessar as informações.

9. **Por que dizemos que todo o sistema de segurança de uma empresa começa com uma política de segurança bem feita?**

   Pois quanto mais bem feita é uma política de segurança, especialmente de uma empresa, melhor será a proteção dos dados e informações vitais dessa empresa, garantindo a segurança dos dados e o bom funcionamento da empresa em um todo.

10. **O que é preciso ter em uma política de segurança? Quem são as pessoas que desenvolvem as políticas de segurança de uma empresa?**

    Deve constar na politica de segurança quais os dados que serão protegidos, por quais pessoas eles podem ser acessas, o grau de confidencialidade, integridade e disponibilidade das informações. As pessoas envolvidas vão desde o setor de T.I da empresa, até os chefes da empresa.