Segurança de Redes – Curso de Ciência da Computação

Atividade de Revisão de Conteúdos

1. **Cite dois exemplos de ameaças internas e externas. E explique de que forma esses ameaças podem ocasionar em perda de dados.**

Ameaças internas podem ser diversos fatores, tanto uma invasão que se dá através da rede interna da empresa, isto é, com acesso físico ao local, ou funcionários com baixa instrução em boas práticas de segurança. Estes podem de forma não intencional acabar clicando em links maliciosos e fornecendo acesso aos invasores.

2. **O que seria um vetor de ataque de perda ou roubo de dados?**

Um link por exemplo pode ser considerado um vetor de ataque para roubo de dados, popularmente utilizado na técnica de Phishing. Um ataque de malware ou ransomware pode ser considerado como perda e roubo de dados, alguns malware excluem dados e ransomware sequestram os dados, normalmente solicitando um valor de resgate.

3. **Até que ponto um hacker deixa de ser ético e passa a ser um criminoso?**

À partir do momento que o hacker passa a utilizar de seus conhecimentos para atividades maliciosas e explora vulnerabilidades de uma maneira que infrinja as legislações de tecnologia vigentes ele passa a ser considerado um black hat ou hacker criminoso.

4. **Quais princípios da Segurança estão incorporados nos mecanismos de segurança por Criptografia?**

   Privacidade, autenticidade e confidencialidade.

5. **Como funciona o algoritmo de Hash?**

Um exemplo de algoritmo hash é o MD5, que produz um valor de hash de 128 bits. Foi projetado para uso em criptografia, mas vulnerabilidades foram descobertas ao longo do tempo, por isso não é mais recomendado para esse fim. No entanto, ele ainda é usado para partição de banco de dados e verificações de computação para validar transferências de arquivos.

6. **Descreva por meio de um exemplo como funciona o Phishing.**

Phishing nada mais é do que a disseminação de links maliciosos via e-mail, normalmente, embora atualmente tenha ficado comum via SMS e WhatsApp. Sempre levam a páginas falsas que visam realizar a coleta dos dados do usuário, estas possuem a mesma aparência das originais e confundem o usuário.

7. **Baseado em que informações, um filtro de pacote toma as decisões do que entra e sai de uma rede? Você utilizou firewall ou filtro de pacotes em seu trabalho final? Em caso positivo, explique em que situação. Em caso negativo, que tecnologias de segurança foram abordadas.**

   Não foi utilizado, mas as decisões são tomadas com base na tabela de roteamento. Acesso em roteadores através de ACLs, DMZ e outros.

8. **O que você destaca em seu trabalho final como ponto importante no estudo de Segurança?**

Embora todos conheçam sobre a LGPD, seus termos são abordados raramente, principalmente seu impacto para empresas de TI. Creio que por exemplo a necessidade de atualização dos termos dos contratos e as multas aplicadas para as empresas que tiveram vazamentos de dados. Sobre os termos dos contratos, justifica bem se relacionado a quantidade de empresas enviando e-mails solicitando a revisão dos termos que foram atualizados.