UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA - CAMPUS SANTA MÔNICA
ENGENHARIA DE CONTROLE E AUTOMAÇÃO

Semana 12

Segurança e Criptografia de Sistemas Linux

Nicole Uchôa Leite Brito Amorim

Junho, 2021

1.

- Desabilitar acesso com senha ao SSH: é recomendável pois cria mais uma barreira de segurança, dificultando o acesso do hacker ao sistema.
- Desabilitar o login SSH de Raiz Direta: impede que a senha seja reutilizada para o acesso ao root, dessa maneira evita a invasão.
- Mudar a porta SSH Padrão: ação não muito eficaz. Garante a proteção contra sistemas que buscam servidores por senhas básicas.
- Desativar IPv6 para SSH: o SSH é programado para listar somente IPv6.
- Configurar um Firewall Básico: abrir somente as portas necessárias para as ações bloqueando as demais.
- Atualização de servidor autônomo automática: atualizações de segurança são programadas para serem efetuadas de forma automática, porém o restante das atualizações não convém ser automática pois elas podem vir com alguma falha/erro que possa facilitar a invasão.

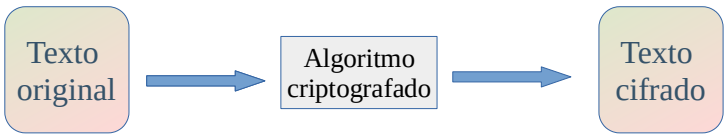
2.

a) **Qual o melhor método para armazenar um conjunto de senhas em um sistema embarcado, conectado à rede.**

Para armazenar conjuntos de senhas o método indicado é o de criptografia unidirecional, pois nesse método o sistema embarcado vai salvar apenas o código e quando a senha for solicitada ela é inserida. Não é aconselhável a criação de senhas em modo de texto ou encriptadas. Para isso é utilizado o método Data Encryption.

b) **Elabore um diagrama e uma breve explicação de como uma criptografia simétrica acontece.**

A criptografia simétrica faz uso de uma única chave, que é compartilhada entre o emissor e o destinatário de um conteúdo. Essa chave é uma cadeia própria de bits, que vai definir a forma como o algoritmo vai cifrar um conteúdo.



c) Diferença entre um sistema de criptografia e um hash de validação.

A criptografia converte para a mensagem original após o processo, já o hash não.

3.

a) **A relação entre sistemas de criptografia e a geração de hashes do bitcoin.**

A criptografia é necessária para proteger as transações. O hash é utilizado para que cada mineração concluída com sucesso tenha seu único algoritmo, o que é essencial para dificultar a resolução desse algoritmo e agregar rendimento ao bitcoin.

b) **Explique como funciona a comunicação e infraestrutura dos sites http se a arquitetura de rede para a implementação do protocolo TSL/SSL.**

O método TSL se difere na criptografia assimétrica pois ele utiliza a criptografia no começo da comunicação entre o cliente e o servidor. Já o protocolo TSL criptografa o tráfego de internet. Quando ele é utilizado é possível ver na barra de endereço um cadeado e o https confirmando o uso desse protocolo.

c) **Pesquise em outras fontes e explique o que é um certificado digital e como funciona o sistema ICP-Brasil, do Instituto Nacional de Tecnologia da Informação (ITI)**

Os certificados digitais são documentos eletrônicos que possuem mensagens, assinaturas e e verificações de identidade de forma criptografada. O responsável pela regulamentação e estabelecimento de critérios e políticas desses documentos é o ICP-Brasil, Infraestrutura de Chaves Públicas Brasileira. Ele também viabiliza a identificação virtual do cidadão brasileiro. Para que isso ocorra de forma funcional e segura é necessário um ótimo sistema criptográfico.