Mateus Antônio Souza Silva – 11711EMT013

Exercício da Semana 12

Questão 1:

- Desabilitar senha do login SSH: recomendável para criar barreiras de segurança, visto que, a efetividade de uma senha está relacionada com a sua força, sendo que as chaves SSH são muito mais convenientes para esses casos;
- Desabilitar acesso direto ao root via SSH: devido a diferentes tipos de processos, pode-se criar um usuário específico para o servidor com permissões especificas para os processos deste;
- Mudar a porta padrão do SSH: é recomendado mudar a porta de acesso padrão para evitar ataques que focam em portas padrões e senhas fracas;
- Desabilitar o IPv6 para o SSH: em virtude de o firewall cobrir apenas o IPv4 pode existir tráfego malicioso;
- Instalação de firewalls: bloquear portas desnecessárias, permitindo apenas a passagem dos processos necessários para a execução do servidor;
- Atualização automática: o operador deve decidir quando o sistema irá atualizar pois essas podem quebrar as aplicações em execução.

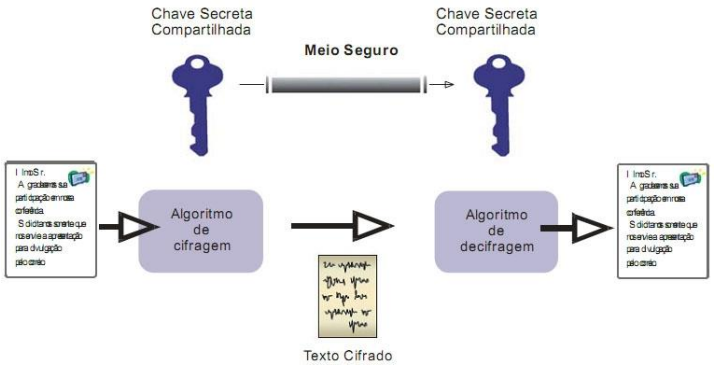
Questão 2:

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.

Questão 3:

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

Uma das características que tornaram o bitcoin famoso é o fato de ser possível conseguir moedas apenas “emprestando” o processamento do computador para auxiliar o protocolo a executar as transações, uma atividade chamada de mineração. Ele é responsável por criar hashs que validam cada operação e, por isso, recebe bitcoins como recompensa.

Sempre que pessoas enviam e recebem valores em bitcoin, o registro básico da operação é adicionado a uma base pública, chamada de blockchain. Também chamado de cadeia de blocos, esse banco de dados públicos armazena os valores de todas as transações feitas por meio do protocolo 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 HTTPS é uma extensão segura do HTTP. Os sites que configurarem um certificado SSL/TLS podem utilizar o protocolo HTTPS para estabelecer uma comunicação segura com o servidor. SSL significa Secure Sockets Layer, um tipo de segurança digital que permite a comunicação criptografada entre um site e um navegador. Atualmente a tecnologia se encontra depreciada e está sendo completamente substituída pelo TLS. TLS é uma sigla que representa Transport Layer Security e certifica a proteção de dados de maneira semelhante ao SSL. Como o SSL não está mais de fato em uso, esse é o termo correto que deveria ser utilizado.

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)

O Certificado Digital é a identidade digital da pessoa física e jurídica no meio eletrônico. Ele garante autenticidade, confidencialidade, integridade e não repúdio nas operações que são realizadas por meio dele, atribuindo validade jurídica. A Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz – AC-Raiz, também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.