NOME: GUILHERME PERES SILVA LEMOS 11721ETE013

QUESTÃO 1

Desativar o login de senha SSH

Ainda que não deixe o sistema o mais seguro, recomenda-se criar mais uma forma de defesa evitando o comprometimento da máquina e de seus dados.

Desativar o login SSH de Raiz Direta

Não deixa acessar o root impedindo que a senha (para usuários não privilegiados) seja reutilizada. Importante quando se trata de servidores.

Mudando a porta SSH Padrão

Garante a proteção contra sistemas que buscam os servidores do tipo SSH com senhas básicas, é uma ação considerada ‘fraca’ e não é muito eficaz contra invasores.

Desativando IPv6 para SSh

É mais efetivo que a alteração da porta (método anterior), nesse método o SSh é programado para listar somente IPv6.

Configurando um Firewall Básico

Nesse método o conselho é abrir somente as portas necessárias para as ações bloqueando as demais.

Atualização de servidor autônomo automática

Atualizações de segurança podem ser 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.

QUESTÃO 2

2. A)

É aconselhável utilizar o método de criptografia unidirecional para armazenar conjuntos de senhas, 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. O método por Data Encryption é o método mais aconselhável de acordo com os critérios apresentados.

B)

A criptografia simétrica é composta por um algoritmo e uma chave de segurança, esses dois elementos cumprem o papel de assegurar e tornar o conteúdo sigiloso. Essa única chave é compartilhada entre o emissor e o destinatário e é composta de uma cadeia de bits. Encontrei um diagrama que representa muito bem o que é a criptografia simétrica, onde o texto original pode ser considerado o emissor e o texto cifrado o destinatário.

C)

O hash não consegue ser convertido para a mensagem original após o processo todo.

QUESTÃO 3

3 A)

Ao surgir a necessidade de mineração da criptomoeda bitcoin, a criptografia é algo muito relevante para proteger as transações. O algoritmo hash é utilizado no protocolo dos bitcoins e cada mineração concluída com sucesso possui um único algoritmo, pode ser considerado essencial pois é dificultando a resolução desse algoritmo ao longo do tempo que a mineração vai tendo seus rendimentos e eficiência.

B)

A implementação do protocolo TSL criptografa o tráfego de internet. É por isso que quando é realizado o acesso de algum site na web e possui um cadeado e o https na barra de endereços podemos confirmar que o protocolo TSL/SSL está sendo utilizado. O método TSL se difere na criptografia assimétrica pois ele utiliza a criptografia, de forma mais fácil, no começo da comunicação entre o cliente e o servidor.

C)

Os certificados digitais são considerados documentos eletrônicos que correspondem a cada pessoa, contendo mensagens, assinaturas e verificações de identidades de forma criptografadas para tornar essas informações mais segura para o cliente que utiliza o servidor.

O comitê que faz a gestão do ICP-Brasil é responsável por estabelecer os critérios e políticas para regulamentar a emissão desses certificados.

O Sistema ICP-Brasil, denominada de Infraestrutura de Chaves Públicas Brasileira, é uma forma de dividir de forma hierárquica viabilizando a geração/emissão dos certificados digitais para identificação virtual do cidadão. Para que o sistema funcione de forma correta, são necessárias várias técnicas e procedimentos feitos para aguentar um sistema criptográfico com base nos certificados digitais.