Universidade Federal de Uberlândia

FEELT – Faculdade de Engenharia Elétrica

Sistemas Embarcados 2

Roteiro Semana 12

Aluno: Lucas Gonçalves e Silva 11811EAU016

08/06/2021

SUMÁRIO

1. EXERCÍCIO 1

Apresente um resumo das 6 dicas apresentadas no vídeo disponível em:
https://www.youtube.com/watch?v=fKuqYQdqRIs
explicando a razão assumida para cada uma delas.

1.1 Desativando o login de senha SSH

Mesmo não deixando o sistema o mais seguro possível, é recomendável por criar mais uma forma de defesa evitando o comprometimento da máquina e de seus dados.

1.2 Desativando 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.

1.3 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.

1.4 Desativando IPv6 para SSh

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

1.5 Configurando um Firewall Básico

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

1.6 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.

2. EXERCÍCIO 2

A partir do vídeo disponível no link abaixo, explique: https://www.youtube.com/watch?v=CcU5Kc_FN_4

2.1 Letra A

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

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.

2.2 Letra B

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

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.

2.3 Letra C

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

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

3. EXERCÍCIO 3

A partir dosvídeos disponíveis no linka baixo, explique: *https://www.youtube.com/watch?v=_qypi2NKCcg*

https://www.youtube.com/watch?v=HCHqtpipwu4

3.1 Letra A

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

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.

3.2 Letra B

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

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.

3.3 Letra 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 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.