Universidade Federal de Uberlândia
Faculdade de Engenharia Mecânica
Engenharia Mecatrônica

Semana 12 – Segurança e Criptografia

Tércio de Melo Alves Júnior 11711EMT016

Junho
2021

Conteúdo

1 Questão 1

1.1 Desativar a senha do login SSH

Embora essa ação não garanta que ataques sejam efetuados com sucesso, é uma etapa a mais na segurança, dessa forma é importante faze-la. Dessa forma, transforma-se a palavra passe em uma senha mais robusta, mais resistente a ataques de força bruta.

1.2 Desativar acesso direto ao root via ssh

Essa ação serve para definir os acessos de um usuario principalmente a servidores, dessa forma, limitando quais processos podem ser utilizados sem o superuser.

1.3 Mudar a porta padrão do SSH

Ao se configurar o ssh, automaticamente, é configurada a porta de acesso à máquina em uma porta padrão. É recomendado mudar essa porta para evitar sofwares maliciosos que escaneiam portas que sabemos que são padrões e explore suas fraquezas.

1.4 Desabilitar o IPv6 para o SSH

Se deve ao fato do firewall cobrir somente o IPV4 dessa forma, pode haver acesso malicioso pelo ipv6.

1.5 Instalação de firewalls

Fazer o firewll entender o que é necessário e filtrar o desnecessário é tarefa do usuário, dessa forma a ação do firewall em bloquear portas e processos é mais eficiente.

1.6 Atualização Automática

Cabe ao usuário decidir o que instalar ou não, ao mesmo tempo que elas podem incrementar a segurança, podem interromper e parar o servidor.

2 Questão 2

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

Dentre os critérios apresentados no vídeo, pode-se dizer que a utilização de algoritmos por Data Encryption Standard (DES), escolhido pelo National Institute of Standards and Technology como padrão de encriptação do governo americano, seria um bom método. Não é aconselhável aos programadores criarem seus próprios algoritmos de encriptação.

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

A criptografia no modelo simétrico envolve um algoritmo e uma chave de segurança, os quais trabalham juntos para tornar um conteúdo sigiloso. A chave para acesso é compartilhada entre emissor e destinatário, sendo esta uma sequência única de bits. No diagrama, CH1 é a chave simétrica.

Figura 1: Esquema

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

A principal diferença entre eles é que o hash, diferentemente da criptografia, não consegue ser convertido na mensagem original após o processo.

3 Questão 3

3.1 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.

3.2 Explique como funciona a comunicação e infraestrutura do sites https e a arquitetura de rede para a implementação do protocoloTSL/ SSL.

Explique como funciona a comunicação e infraestrutura do sites https e a arquitetura de rede para a implementação do protocoloTSL/ SSL.

3.3 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 encaixam-se como documento eletrônico dos cidadãos e utilizam o ciframento de mensagens, verificação de identidades e as

assinaturas digitais para se tornar mais seguros e imunes a falhas de segurança. Já 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". O sistema utiliza um conjunto de técnicas, práticas e procedimentos elaborado para suportar um sistema criptográfico com base em certificados digitais." O Comitê Gestor da ICP-Brasil estabelece a política, os critérios e as normas para regulamentar a operação de Autoridades Certificadoras (AC), Autoridades de Registro (AR) e demais prestadores de serviços de suporte em todos os níveis da hierarquia de certificação, credenciando as respectivas empresas para a emissão de certificados no meio digital brasileiro"