UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA MECÂNICA
Curso de graduação em Engenharia Mecatrônica

SISTEMAS DIGITAIS

(FEELT39015**)**

SEMANA 12

Matheus Luiz Teixeira Silva **11311EMT025**

Uberlândia, 2021-1

QUESTÃO 1

1) Desabilitar o password de login do SSH ou Secure Socket Shell que é um protocolo de rede que permite que os administradores de um servidor acessem um computador remoto, evitando que algum hacker possa utilizar isto contra o usuário uma vez que ele poderia ter acesso a informações do usuário facilmente se tivesse acesso a esse password.

2)Desabilitar o acesso root do SSH, a recomendação vem de que é ideal sempre utilizar apenas os privilégios necessários à sua tarefa, uma vez que talvez ao executar a sua tarefa poderá ter algum risco de ter alguma informação interceptada ao longo disso, se o hacker tiver acesso ao root tendo aceso privilegiado isso representa um alto risco.

3) Mudar as portas padrões utilizadas, uma vez que por serem comuns e conhecidas o ideal é que não se utilizar as portas padrões, quanto menos informação os hackers tiverem para explorar essas brechas melhor será.

4)Desabilitar IPv6, manter apenas IPv4 o firewall trabalha melhor com o IPv4 uma vez que as configurações mais comuns são focadas nele, teoricamente teríamos uma melhor forma de controle ao ignorar o IPv6, porém não fica muito claro a vantagem umas vez que ainda temos que analisar de fato se as configurações estão corretas, de um modo geral pelo maior uso do IPv4 seria mais seguro se manter neste.

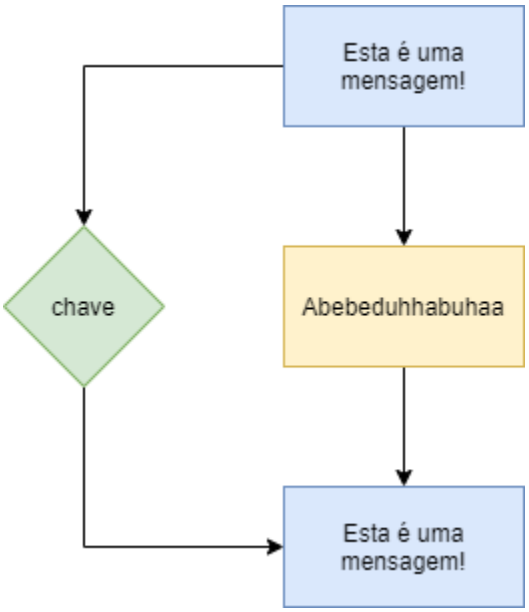
5)Configurar um firewall, mesmo que seja um simples, teremos várias opções e tipos, mas é importante ter pelo menos a mais simples delas, ele vai permitir que as aplicações do seu servidor possam acessar a internet, porem filtra quando algo está tentando acessar o servidor, gerando uma maior segurança.

6)Desabilitar os updates automáticos no servidor, uma vez que mesmo sendo algo bom em outras plataformas conhecidas, ter maior controle sobre como e quando o servidor é atualizado é a melhor opção pois te dá maior controle sobre o que está acontecendo.

QUESTÃO 2

a) Utilizar hashing junto com algum tipo de criptografia para ter certeza de que além de segura a informação está devidamente segura e que não foi alterada devido ao caminho, apesar de que na questão de segurança não temos apenas uma medida mas sim uma gama gigantesca de parâmetros para serem analisados.

b) Basicamente este tipo de criptografia é utilizado quando ambos origem e destino possuem acesso a mesma chave.



c) Temos que um sistema de criptografia basicamente faz uma troca de dados por meio de alguma lógica da forma em que ela possa ser transportada ou armazenada de forma segura de uma forma que ela possa ser armazenada seguramente e apenas acessada pelos dispositivos que possuam acesso a essa criptografia para esses dados específicos o hash de validação por sua vez é similar a uma impressão digital, tendo conhecimento dessa impressão podemos ter certeza se os dados foram ou não adulterados sem ter que analisar parte por parte, seria uma espécie de identidade dos dados armazenados.

QUESTÃO 3

a) O hash é gerado alterando vários número dos blocos até achar um hash específico que tenha a sequência específica de zeros a esquerda, pra isso teremos vários equipamentos utilizáveis como GPU's ou mesmo mineradores dedicados a isso como foi citado no vídeo, apenas o processador não é suficiente, logo utilizamos desses outros meios, quem consegue gerar esse hash primeiro é o detentor do bitcoin gerado. A quantidade de zeros desse hash é a dificuldade da mineração é uma espécie de competição, quem tem mais força de minerar acaba saindo na frente da competição uma vez que vai poder achar esses números gerados primeiro.

b) Basicamente o HTTPS é uma extensão segura do HTTP, entendendo isso sabemos que sites que configurarem um certificado SSL/TLS podem utilizar o protocolo HTTPS para estabelecer uma comunicação segura com o servidor, relacionando ao assunto de segurança temos que objetivo principal do SSL/TLS é tornar segura a transmissão de informações sensíveis como dados pessoais, relacionados a pagamentos, logins, contas e registros diversos.

c) O certificado digital ICP-Brasil é uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meio eletrônico. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, uma Autoridade Certificadora (AC).