UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA MECÂNICA
CURSO DE GRADUAÇÃO EM ENGENHARIA MECATRÔNICA

SISTEMAS DIGITAIS – FEELT49081

Prof. Éder Alves de Moura

SEMANA 11

Pedro Henrique Silva Oliveira 11611EMT007

Uberlândia, Junho de 2021

Questão 01

Dica 1: Desabilitar login de senha SSH: Na arquitetura do protocolo SSH, há uma seção sobre "Autenticação de senha" onde indica claramente a "fraqueza": "Se o servidor foi comprometido, usar a autenticação de senha revelará uma combinação válida de nome de usuário / senha para o invasor, o que pode levar a mais prejuízos". Desta forma, no final, "usar chaves SSH" é uma recomendação útil, mas não para segurança. É uma conveniência que diminui até a probabilidade de erros.

Dica 2: Desativar login SSH de raiz direta: O uso do servidor no final, ele funciona principalmente como root. Uma recomendação típica que anda de mãos dadas com o siabling do login root, é adicionar o usuário sem privilégios para o grupo sudo. Esses são recursos para praticidade, mas não protege "magicamente" seu servidor contra hackers.

Dica 3: Alterar porta SSH padrão, como recomendação, pois uma mudança de porta não seria suficiente para parar um invasor poderoso. Uma mudança de porta pode apenas ter um efeito contra script kiddies e scanners automatizados que procuram servidores ssh com senhas fracas.

Dica 4: Desativar IPv6 para SSH: Outra configuração ssh estranha que alguns desses guias de segurança recomendam é desabilitar o IPv6, e permitir acesso apenas via IPv4 IPv6 é melhor que IPv4, mas não é muito efetivo. Hackers o usam para enviar tráfego malicioso. Para redução da superfície de ataque é um paradigma muito bom.

Dica 5: Configurar um Firewall Básico, outra recomendação meio inútil. Claro que os firewalls em geral não são inúteis, mas você precisa ter o caso de uso correto para eles.

Dica 6: Atualização automática de servidor autônomo: Nem todas as atualizações são relevantes em termos de segurança para você. Os benefícios das atualizações automáticas do sistema autônomo, visto que não é um remédio para todas as suas dores de cabeça de atualização, é muito pouco, em comparação com a interrupção acidental do seu serviço e o trabalho manual necessário

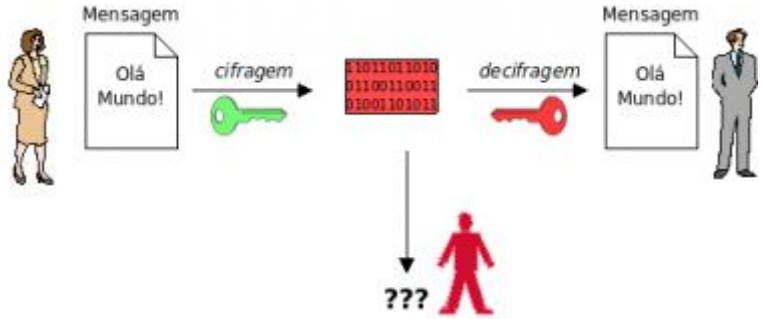
Questão 02 A)

O melhor método para armazenar um conjunto de senhas em um sistema embarcado deve utilizar um gerador de números aleatórios forte para criar um salt de 16 bytes ou mais, alimentar o salt e a senha no algoritmo PBKDF2, usar HMAC-SHA-256 como o hash central dentro do PBKDF2, executar 80.000 iterações ou mais [março de 2019], depois pegar 32 bytes (256 bits) de saída de PBKDF2 como o hash de senha final. Ademais, é necessário armazenar a contagem de iterações, o salt e o hash final em seu banco de dados de senhas e aumentar sua contagem de iterações regularmente para acompanhar as ferramentas de crackeamento mais rápidas. Por fim, recomenda-se que não tente criar seu próprio algoritmo de armazenamento de senha.

B)

O ciframento de uma mensagem (processo em que um conteúdo é criptografado) é baseado em 2 componentes: um algoritmo; e uma chave de segurança. O algoritmo trabalha junto com a chave, de forma que eles tornam um conteúdo sigiloso com um conjunto único de regras. 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. Como vantagem, a criptografia tem uma boa performance e a possibilidade de manter uma comunicação contínua entre várias pessoas

simultaneamente. Caso a chave seja comprometida, basta efetuar a troca por uma nova, mantendo o algoritmo inicial. Apesar do seu alto desempenho, a criptografia simétrica possui graves falhas de segurança. A gestão de chaves, por exemplo, torna-se mais complexa conforme o número de pessoas que se comunica aumenta. Para cada N usuários, são necessárias N^2 chaves. A criptografia simétrica também não possui meios que permitem a verificação da identidade de quem envia ou recebe um conteúdo. Além disso, não há como garantir o armazenamento em ambientes confiáveis das chaves de segurança.



C)

O sistema de criptografia e um hash de verificação apresenta uma diferença fundamental que está nos algoritmos de hashing são o que chamamos de one-way, direção única, isto é, são irreversíveis. Por outro lado, na encriptação simétrica como o TripleDES ou AES, é possível reverter o processo e decriptar do ciphertext para o plaintext. Temos que uma função de hashing pega um plaintext de tamanho variado e libera uma saída de tamanho fixo.

Questão 03 A)

Os sistemas de criptografia e a geração de hashes da bitcoin apresentam algumas similaridades. Apesar que nem todas as funções hash envolvam o uso de criptografia, as chamadas funções hash criptográficas são componentes fundamentais das criptomoedas. Por conta delas, blockchains e outros sistemas distribuídos são capazes de alcançar níveis significativos de integridade de dados e segurança, tornando o uso de criptomoedas confiável. Normalmente, os algoritmos de hashing das criptomoedas são projetados como funções de sentido único, o que significa que elas não podem ser facilmente revertidas sem empregar grandes quantidades de tempo e de recursos computacionais. Em geral, romper uma função hash criptográfica requer milhares de tentativas forçadas (brute-force attempts). Para uma pessoa “reverter” uma função hash criptográfica, seria necessário adivinhar qual foi o input através de tentativa e erro até conseguir finalmente gerar o output correspondente.

B)

O TLS consiste de diversos elementos variados. A fundação do TSL é o protocolo de registro, o protocolo subjacente responsável pela estrutura abrangente de todo resto. O protocolo de registro contém cinco subprotocolos distintos, cada um dos quais é formatado como registros:

1. Handshake - Utilizado para configurar os parâmetros para uma conexão segura.

2. Aplicativo - O protocolo do aplicativo começa após o processo de handshake, e é onde os dados são transmitidos de maneira segura entre as duas partes.

3. Alerta – Este protocole é usado por qualquer uma das partes em uma conexão para notificar o outro se houver algum erro, problemas de estabilidade ou um comprometimento potencial.

4. Change Cipher Spec - Usado pelo cliente ou servidor para modificar os parâmetros de criptografia.

5. Heartbeat - Esta é uma extensão TLS que permite um lado da conexão sabe se seu par ainda está ativo e evita que firewalls fechem inativos conexões.

Cada um desses subprotocolos são usados em diferentes estágios para comunicar diferentes tipos de mensagem. Os mais importantes e primordiais para compreensão são o handshake e o protocolo de aplicação, porque estes são responsáveis por estabelecer a conexão e, em seguida, transmitir os dados com segurança.

C)

Certificados digitais são documentos eletrônicos mostram a relação de um indivíduo ou entidade e sua chave pública. Este link é validado por uma autoridade de certificação (CA), que é uma organização confiável que verifica se os dois estão realmente relacionados, em seguida, usa sua própria reputação para conceder confiança ao certificado. Diferentes níveis de certificado representam vários graus de confiança. O principal ponto a se destacar é que se um cliente ou servidor tem um certificado confiável válido, então é razoável supor que a chave pública é legítima e que você não está lidando com um invasor.

A ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) é uma cadeia hierárquica composta por uma autoridade gestora de políticas e autoridades certificadoras que utilizam um conjunto de tecnologias, práticas, técnicas e procedimentos para realizar a transação de documentos eletrônicos com segurança. A validação requer um par de chaves, sendo que uma delas é de conhecimento geral, ou seja, de acesso ao público, e a outra de conhecimento apenas do proprietário. Por isso, seus dados precisam estar contidos em um certificado digital para que seja possível fazer a tramitação do documento.