André Tommasello Ramos - 11511EMT025
Semana 12 – Segurança e Criptografia de Sistemas Linux

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) Disable SSH Password Login: Esse tipo de password é inseguro. No caso de um comprometimento do servidor, esse password pode ser usado pra revelar usuário e senhas que o hacker pode usar pra causar mais danos ainda

1.2) Disable Direct Root SSH Login: Deve-se sempre atentar para as permissões de usuários. Dar permissões demais para um usuário pode comprometer a segurança do resto do sistema caso um usuário com mais controle for hackeado

1.3) Changing the Default SSH Port: Esconder a porta ajuda a evitar problemas em casos de ataques mais simples

1.4) Disabling IPv6 for SSH: Existem firewalls mal configurados que só protegem endereços IPv4. Logo, é melhor trabalhar com o que eles conseguem fazer

1.5) Setting up a Basic Firewall: O papel do firewall é essencial para a segurança do sistema, e não deve ser ignorado.

1.6) Unattended Server Auto Upgrading: Upgrades automáticos podem causar problemas que precisam de conserto manual. Além disso, eles podem acabar interrompendo o funcionamento do sistema em um momento crucial

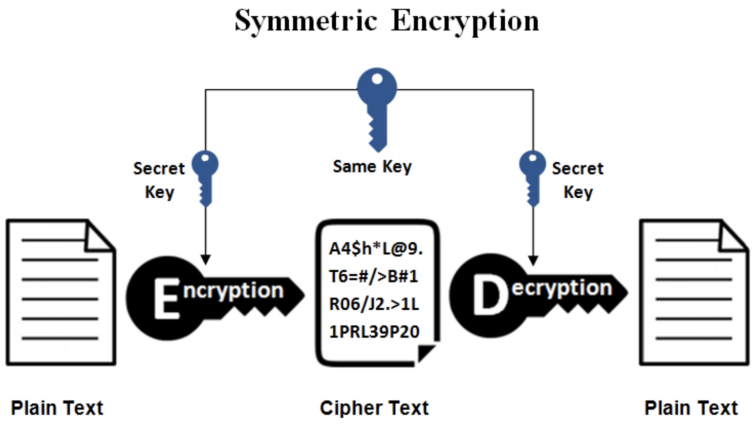
2. A partir do vídeo disponível no link à seguir:
https://www.youtube.com/watch?v=CcU5Kc_FN_4
Explique:
a) Qual o melhor método para armazenar um conjunto de senhas em um sistema embarcado, conectado à rede.

O melhor método é o HMAC

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

A criptografia simétrica usa uma chave única compartilhada entre quem emite e quem recebe a mensagem. Nesse sentido, essa chave é uma cadeia própria de bits, que define como um algoritmo será cifrado.

No caso do comprometimento da chave, só é necessário trocá-la por uma nova, mantendo o algoritmo inicial



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

Um sistema de criptografia é um sistema que usa algoritmos e uma chave para conversão das mensagens em um formato que é irreconhecível sem a chave.

Já o hash é uma conversão do dado em resumos onde, por definição, dois elementos nunca podem ter o mesmo hash resultante. Ou seja, é uma maneira segura de armazenar um dado sem guardar seu conteúdo em si.

3. A partir dos vídeos disponíveis no link abaixo, explique:
https://www.youtube.com/watch?v=_qypi2NKCcg
https://www.youtube.com/watch?v=HCHqtpipwu4

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

Funções de hash criptográficas adicionam ferramentas de segurança para funções de hash típicas, fazendo ser mais difícil de

detectar o conteúdo de uma mensagem ou informações sobre os recipientes ou remetentes

b) *Explique como funciona a comunicação e infraestrutura do sites https e a arquitetura de rede para a implementação do protocolo TSL/SSL.*

Protocolos SSL são usados em HTTP para proteger uma conexão e verificar a legitimidade do site. Nesse sentido, esse tipo de certificação fornece uma camada extra de segurança para dados confidenciais que o site deseja manter como confidenciais.

Já os protocolos TLS ficam entre as camadas de aplicação e transporte, no sentido de que ele encapsula protocolos de aplicação como HTTP e FTP, e trabalha em cima de protocolos como TCP e UDP. Lembrando que TCP é mais seguro do que o UDP

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).

Um certificado digital é um registro eletrônico de pessoas ou empresas. Ele é como uma carteira de identidade no mundo virtual. Nesse sentido , ele possibilita a identificação dessa pessoa/empresa sem uma apresentação presencial. A estrutura do ICP-Brasil envolve vários órgãos para viabilizar esse tipo de documentos em meios eletrônicos