1. Apresente um resumo das 6 dicas apresentadas no vídeo “Protect Linux Server From Hackers”:

   - Desabilitar senha de login do SSH: Senhas são supostamente inseguras, deve-se utilizar chaves públicas ao invés dessas senhas de login. Desta forma o cliente emitirá um alerta caso algo de errado esteja acontecendo com a conexão;
   - Desabilitar o root direto do login SSH: Fazendo isso um atacante não terá privilégios de root caso tenha sucesso de invadir a máquina alvo;
   - Alterar a porta padrão do SSH: Ao alterar a porta padrão, você acaba dificultando um pouco o trabalho do hacker, visto que ele terá que descobrir qual porta o SSH estará utilizando. Porém, esta dica não é muito eficiente;
   - Desabilitar o IPv6 para o SSH: Hackers geralmente utilizam o IPv6 para trafego malicioso. Geralmente o firewall não é bem configurado para proteger o IPv6, logo é melhor evitar de utilizá-lo e usar apenas o IPv4;
   - Configurar um firewall básico: Não configurar o firewall de forma correta não irá proteger as portas que estão abertas em sua máquina;
   - Atualização automática do servidor: Atualizações automáticas podem gerar problemas secundários em servidores. Logo, é melhor não deixar a atualização automática ligada, já que falhas de segurança nesse tipo de sistema são raras de serem descobertas.

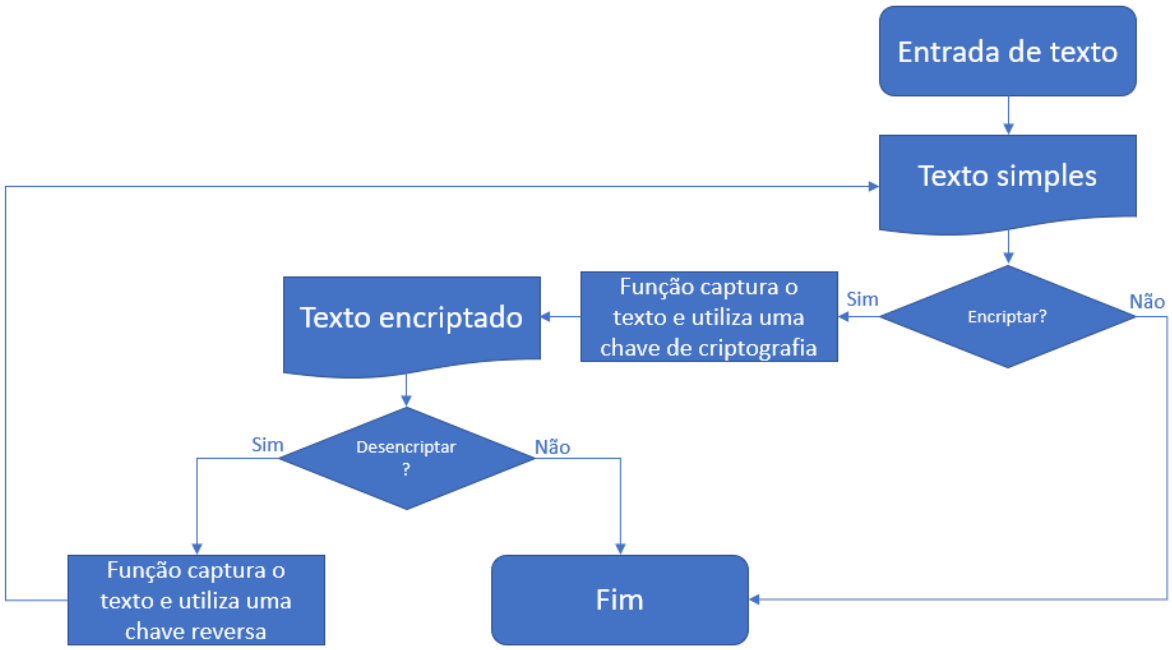
2. A partir do vídeo “Entendendo Conceitos Básicos de CRIPTOGRAFIA | Parte 1/2” respondas as seguintes questões:

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

   A melhor forma de armazenar senhas é utilizando hash de validação, ou seja, a senha em texto simples nunca será armazenada no banco de dados. Caso ocorra o vazamento de dados não é possível recuperar a senha em texto simples novamente.

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

   Para realizar uma criptografia simétrica é preciso de uma entrada, no caso abaixo trata-se de um texto simples, e uma chave (também chamada de segredo). Diversos segredos podem ser utilizados, sendo os mais básicos e menos seguros a troca de uma letra por outra. Porém a criptografia pode ser desfeita utilizando a mesma chave usada na criptografia da informação e desta forma recupera-se a mensagem original.




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

A principal diferença entre a criptografia e o hash de validação é que uma informação encriptada pode ser recuperada utilizando a chave de criptografia, já no caso do hash não é possível obter a informação original novamente. Neste caso, para verificação de uma informação que foi tratada por hashing é preciso fazer uma comparação entre o hash salvo e o hash de uma nova informação, caso os hashes sejam iguais podemos assumir que as informações originais são as mesmas.

3. A partir dos vídeos “c0mrade, o hacker mais novo a ser preso | Nerdologia Tech” e “Entendendo Conceitos Básicos de CRIPTOGRAFIA | Parte 2/2 explique:

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

   Algoritmos PBKDF2 que derivam chaves a partir senhas (criptografia) possuem fatores de dificuldade similares ao Proof-of-Work (processo de assinatura de um bloco de bitcoin).

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

Utilizando os conceitos de Diffie-Hellman é possível gerar duas chaves separadamente uma em cada uma das duas máquinas que irão enviar dados encriptados, porém, essa chave nunca irá trafegar pela rede.

O usuário 1 e o usuário 2 primeiramente combinam as seguintes informações que trafegam livremente pela rede:

Módulo p
Base g

Após isso o usuário 1 escolhe um número a, onde:

$A = g^a \ mod \ p$

E o usuário 2 escolhe um número inteiro b, onde:

$B = g^b \ mod \ p$

Os valores calculados A e B também são enviados pela rede.

Por último os dois usuários computam os seguintes valores:

$s = B^a \ mod \ p$ Usuário 1

$s = A^b \ mod \ p$ Usuário 2

Este valor s, calculado pelos dois usuários é o segredo da criptografia das informações e em momento algum trafegou pela rede.

Para resolver o problema de confiança entre os dois usuários e de Foward Secrecy utiliza-se são criadas novas chaves secretas assimétricas com RSA a cada seção e EAS-256 para estabelecer uma conexão segura. Desta forma temos o protocolo TLS/SSL

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).

O certificado digital é uma assinatura eletrônica (identidade virtual) que utiliza os dados do titular (PF ou PJ) e permite a identificação de quem gerou uma mensagem ou transação eletrônica. Essa tecnologia utiliza chaves criptográficas para gerar uma identidade segura. É composto pelas informações da pessoa, uma chave pública e uma assinatura de uma Autoridade Certificadora Confiável.

A Infraestrutura de Chaves Públicas Brasileira é uma hierarquia composta por uma autoridade gestora de políticas e autoridades certificadoras responsável pela transação segura de documentos eletrônicos. A hierarquia é composta da seguinte forma:

- 1º. Comitê Gestor (CG);
- 2º. Autoridade Certificadora (AC Raiz);
- 3º. Autoridades Certificadoras de 1º e 2º nível (ACs);
- 4º. Autoridades de Registros (ARs);
- 5º. usuário final.

A validação de documentos necessita de um par de chaves públicas e outro par de chaves privadas, e além disso, a entidade certificadora deve fazer parte da infraestrutura do governo e ter uma classificação de segurança.