UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE ENGENHARIA MECÂNICA

Curso de graduação em Engenharia Mecatrônica

Disciplina: Sistemas Digitais para Mecatrônica

Professor: Éder Alves de Moura

Semana 12 – Segurança e Criptografia de Sistemas Linux

Larissa Teodoro da Silva **11321EMT021**

Uberlândia, Junho de 2021

6 dicas de Segurança

1. Desativar os login de senha SSH

A suposição é que as senhas são inseguras.
Se o servidor tiver sido comprometido, o uso da autenticação por senha revelará uma combinação válida de nome de usuário / senha para o invasor, o que pode levar a outros comprometimentos.

2. Desativar Login SSH de Raiz Direta

Devemos criar um usuário sem privilégios, sem root permissões. De modo geral, é sempre um bom método usar o mínimo de privilégios necessários para realizar uma tarefa.

3. Alterar porta SSH padrão

Tudo pode ser hackeado, logo é melhor esconder a porta ssh, e alterar a mesma.

4. Desativando IPv6 para SSH

O IPv6 não é tão seguro quanto o IPv4, pois as possibilidades de endereço no IPv4 são menores, logo é mais caro para o invasor. Ao desabilitar o IPv6, acaba diminuindo a superfície de ataque para um invasor.

5. Configurando um Firewall Básico

Os firewalls, em essência, podem ajudar a impedir ataques usando portas se você configurar o firewall de maneira adequada. No entanto, apenas configurá-lo sozinho para bloquear todas as portas, exceto as poucas que você precisa, não fará nada para aumentar sua segurança.

6. Atualização automática de servidor autônomo

O problema com a atualização automática de pacotes ou distribuições é que, às vezes, isso pode causar problemas e você terá que aplicar as correções manualmente. Além

disso, nem todas as atualizações são atualizações de segurança. O trabalho de um administrador de sistema é decidir quais atualizações são necessárias, bem como e quando atualizar os sistemas para minimizar interrupções.

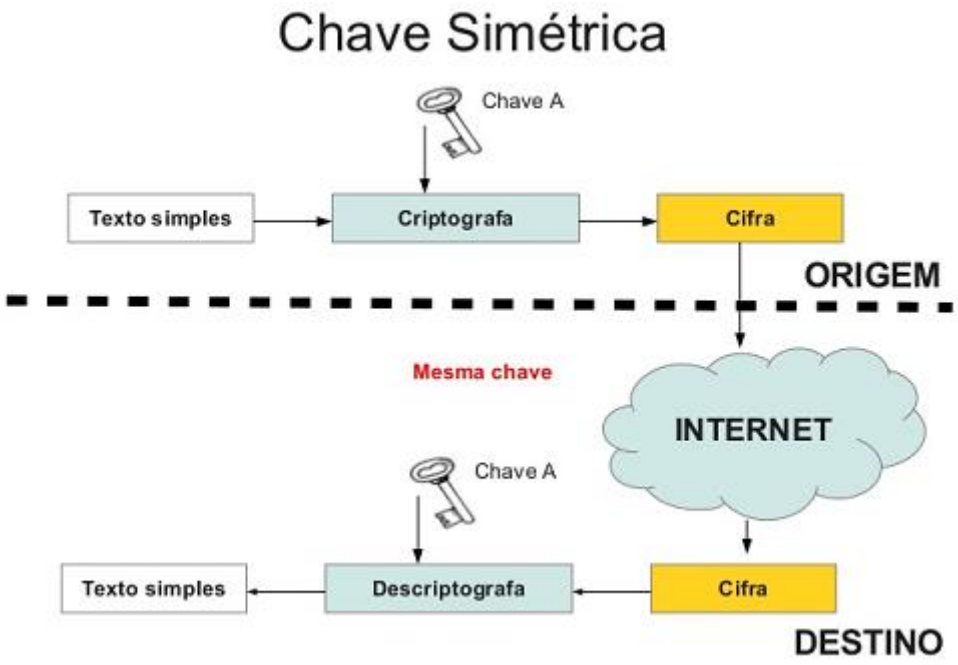
2.

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

O melhor método para armazenar um conjunto de senhas em um sistema embarcado é o AES.

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

É uma forma de criptossistema em que a criptografia e a decriptografia são realizadas usando a mesma chave. Também conhecida como criptografia convencional. Basicamente esta criptografia transforma um texto claro em texto cifrado, utilizando uma chave secreta e um algoritmo de criptografia. Utilizando a mesma chave e um algoritmo de decriptografia, é possível reverter o texto cifrado para o texto claro.



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

A diferença entre a criptografia e um hash, é que os algoritmos de Hash tem direção única, ou seja, são irreversíveis.

3.

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

A relação entre criptografia e a geração hashes de Bitcoin, é que quando falamos em Bitcoin uma parte essencial é a mineração, e as Hash criptografadas desempenham um papel na geração de novos endereços e chaves. E o sistema de Criptografia oferece mais segurança.

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

Os sites https funcionam da seguinte forma: o navegador envia um pedido de acesso a uma página, o servidor retorna uma resposta de permissão de acesso. Junto com ela são enviados também os arquivos da página que o usuário deseja acessar. Existe ainda uma camada de proteção, isso significa que os sites que utilizam esse protocolo são de acesso seguro. O protocolo HTTPS é comumente usado por sites com sistemas de pagamentos. Esse tipo de site depende de proteção que garanta a integridade dos dados, informações de conta e cartão de créditos dos usuários. A segurança é feita por meio de uma certificação digital, que cria uma criptografia para impedir ameaças e ataques virtuais.

Uma vez que o cliente e o servidor tenham decidido usar TLS/SSL, eles negociam um estado de conexão usando um procedimento de handshaking, no qual o cliente e o servidor concordam em vários parâmetros utilizados para estabelecer a conexão segura.

O protocolo HTTPS, é encriptado com SSL/TLS, assim sendo o seu funcionamento acontece da seguinte forma:

- O cliente envia ao servidor a versão que possui do TSL/SSL, as configurações de criptografia, os dados específicos da sessão (session ID), e outras informações que o servidor precisa para se comunicar com o cliente usando SSL.
- O servidor envia ao cliente a sua versão do TSL/SSL, as configurações de criptografia, os dados específicos da sessão, e outras informações que o cliente também precisa. O servidor também envia seu próprio certificado e, se o cliente está solicitando um recurso de servidor que requer autenticação do cliente, o servidor solicita o certificado do cliente.
- O cliente utiliza as informações enviadas pelo servidor para autenticar o servidor, ou seja, confirmar se todas as configurações recebidas pelo servidor são as esperadas para,

então, dar continuidade a conexão segura. Caso contrário, a solicitação é interrompida e o usuário é informado.

- Usando todos os dados gerados no handshaking até agora, o cliente (com a cooperação do servidor, dependendo da cifra em uso) cria o segredo pré-mestre para a sessão, criptografa com a chave pública do servidor (obtido a partir de certificado do servidor, enviado no passo 2), e, em seguida, envia o criptografado segredo pré-mestre para o servidor.
- Se o servidor solicitou autenticação do cliente (opcional), o cliente também assina outro pedaço de dados que é exclusivo para este handshaking e conhecido tanto pelo cliente quanto pelo servidor. Neste caso, o cliente envia os dados assinados e seu certificado para o servidor, juntamente com o criptografado segredo pré-mestre.
- Se o servidor solicitou autenticação do cliente, o servidor tenta autenticar o cliente. Se o cliente não pode ser autenticado, a sessão termina da mesma forma que no passo 3. Se o cliente é autenticado com sucesso, o servidor usa sua chave privada para descriptografar o segredo pré-mestre, e em seguida, executa uma série de etapas (que o cliente também realiza, a partir do mesmo segredo pré-mestre) para gerar o segredo principal.
- Tanto o cliente quanto servidor devem usar o segredo principal para gerar as chaves de sessão, que são chaves simétricas usadas para criptografar e descriptografar as informações trocadas durante a sessão TSL/SSL e para verificar a sua integridade (ou seja, para detectar quaisquer alterações nos dados entre o tempo que foi enviado e o momento em que é recebido através da conexão SSL).
- O cliente envia uma mensagem para o servidor, informando que as próximas mensagens do cliente serão criptografadas com a chave de sessão. Em seguida, envia uma mensagem separada (criptografada), indicando que a parte handshanking do cliente esta concluída.
- O servidor envia uma mensagem para o cliente também informando que suas próximas mensagens serão criptografadas com a chave de sessão. Em seguida, envia uma mensagem separada (criptografada), indicando que a parte handshaking do servidor esta concluída.O handshaking TSL/SSL está concluído e a sessão segura começa.

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).

Certificado digital é a tecnologia que, por meio da criptografia de dados, garante autenticidade, confidencialidade, integridade e não repúdio às informações eletrônicas. Trata-se de um documento digital utilizado para identificar pessoas e empresas no mundo virtual. Com o certificado digital é possível fazer transações, que antes seriam feitas presencialmente, de forma remota. Isso garante mais agilidade e ganho de tempo.

A ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) consiste em 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.

Além disso, é preciso que a entidade certificadora seja integrante da infraestrutura do governo e receba uma classificação quanto ao seu nível de segurança. Desse modo, é possível garantir a validade jurídica dos documentos eletrônicos, bem como sua autenticidade e integridade.