Universidade Federal de Uberlândia

FEELT – Faculdade de Engenharia Elétrica

Guilherme Ferreira de Jesus 11811ETE008

Sistemas Embarcados

Roteiro 12

10/06/2021

1. **Apresente um resumo das 6 dicas apresentadas no vídeo.**
    - Desabilitar senha de login SSH: Como muitas pessoas com servidores SSH usam senhas fracas, muitos invasores online procuram um servidor SSH e começam a adivinhar as senhas aleatoriamente. Um invasor pode tentar milhares de senhas em uma hora e adivinhar até mesmo a senha mais forte com tempo suficiente. A solução recomendada é usar chaves SSH em vez de senhas. O protocolo SSH estabelece um túnel criptografado entre o cliente e o servidor, e a senha em texto puro é enviada para lá. Portanto, a senha é um texto não criptografado dentro do túnel, mas você não pode ver isso porque está fora do túnel. Então, no final das contas, não é realmente um texto claro. O ponto principal é que se recomenda que use chaves SSH, mas não por causa da segurança, mas sim por conveniência. Desativar o login por senha não torna o seu servidor mais seguro magicamente.
    - Desabilitar login direct root SSH: A conta root é frequentemente a conta mais visada pelos Hackers via SSH no Linux. Uma conta raiz SSH habilitada em um servidor Linux exposta a uma rede ou, pior, exposta na Internet pode representar um alto grau de preocupação de segurança para administradores de sistema. A conta raiz SSH deve ser desabilitada em todos os casos no Linux para fortalecer a segurança do seu servidor. Você deve fazer o login via SSH em um servidor remoto apenas com uma conta de usuário normal e, a seguir, alterar os privilégios para a conta root via sudo ou comando su.
    - Alterar a porta padrão SSH: Uma porta é simplesmente um ponto de extremidade de comunicação onde um processo é roteado assim que chega a um servidor. Para se conectar por SSH, um usuário requer o número da porta (por exemplo, 22) e um endereço IP público do servidor junto com um nome de usuário e uma senha. Para evitar que bots automatizados e usuários mal-intencionados façam força bruta em seu servidor, você deve considerar alterar a porta SSH padrão para outra. Um invasor inteligente ainda examinaria seu servidor para determinar portas abertas e serviços em execução neles. No entanto, alterar a porta SSH padrão bloqueará milhares desses ataques automatizados que não têm tempo para girar as portas quando têm como alvo um servidor Linux.
    - Desabilitar IPv6 para SSH: O IPv6 oferece um esquema de endereçamento muito maior do que o IPv4, que é uma das muitas razões pelas quais foi desenvolvido. Como alguns hardwares não aproveitam o IPv6 (e a maioria dos administradores ainda está trabalhando com IPv4), uma solução temporária e fácil é desabilitar o IPv6; o protocolo pode ser reativado quando chegar o momento em que o problema for resolvido permanentemente. Este método é mais efetivo que alterar a porta padrão SSH.
    - Configurar firewall básico: A maneira como os firewalls funcionam geralmente é bloquear as portas e, em seguida, basta desbloquear as que você precisa. Os firewalls, em essência, podem ajudar a impedir ataques usando portas se você configurar o firewall de maneira adequada. No

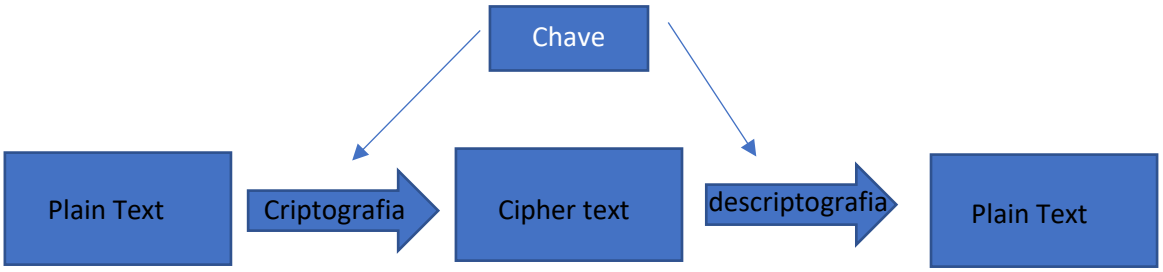
entanto, apenas configurá-lo sozinho para bloquear todas as portas, exceto as poucas que você precisa, não fará nada para aumentar sua segurança.

- Atualização Automático do servidor: A maioria dessas atualizações automáticas são benéficas. Porém em alguns casos não será uma desvantagem, ou seja, as vantagens de ter as atualizações automáticas são em grande parte contrariadas pelo risco de ter que consertar coisas em caso de interrupção causada pela atualização do pacote, mas o mais importante, você provavelmente terá que corrigir o software manualmente de qualquer maneira.

2. **A partir do vídeo, explique:**
   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 é utilizar criptografia unidirecional, ou seja, utilizar hashes. Uma função hash é qualquer função que pode ser usada para mapear dados de tamanho arbitrário para valores de tamanho fixo. Os valores retornados por uma função hash são chamados de valores hash, códigos hash, etc. Uma função hash recebe uma entrada como uma chave, que é associada a um dado ou registro e usada para identificá-lo para o aplicativo de armazenamento e recuperação de dados. As chaves podem ter comprimento fixo, como um número inteiro, ou comprimento variável, como um nome. Em alguns casos, a chave é o próprio dado. Uma boa função hash satisfaz duas propriedades básicas: 1) deve ser muito rápida para calcular; 2) deve minimizar a duplicação dos valores de saída (colisões). As funções de hash dependem da geração de distribuições de probabilidade favoráveis para sua eficácia, reduzindo o tempo de acesso a quase constante.

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



Os algoritmos de chave simétrica são algoritmos para criptografia que usam as mesmas chaves criptográficas para a criptografia e para descriptografia. As chaves podem ser idênticas ou pode haver uma transformação simples para ir entre as duas chaves. Na criptografia simétrica, quando queremos mandar uma mensagem para uma pessoa é muito simples. O que fazemos é utilizar a chave de criptografia para cifrar os dados. Note que somente o receptor tem essa mesma chave. Assim, somente ele poderá abrir essa mensagem.

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

Com o hash, você não tem como reverter o valor do hash (a string que você obtém após o hashing) de volta para o texto simples, enquanto que, com a criptografia, você tem uma chave que pode reverter o processo.

3. **A partir dos vídeos, explique:**
   a) **A relação entre sistemas de criptografia e a geração de hashes do bitcoin.**

A relação entres sistema de criptografia e a geração de hashes se dá a partir da necessidade de mineração do bitcoin. Hash é um algoritmo utilizado pelo protocolo do bitcoin e a função de hash criptográfico muitas vezes é conhecida simplesmente como hash. Portanto, esse código tem extrema importância nas transações realizadas na mineração de bitcoin. Os mineradores pegam informações de um bloco, aplicam uma fórmula matemática a ele e as transformam em outra coisa. Criam uma sequência nova e muito mais curta de números e letras aparentemente aleatórios. Essa sequência é conhecida como hash. O hash é armazenado dentro do bloco, o que quer que seja o fim da cadeia naquele momento.

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

O objetivo do SSL/TLS é garantir que somente uma pessoa – a pessoa ou organização para quem os dados estão sendo transmitidos – possa ter acesso às informações. Isso é particularmente importante quando consideramos a quantidade de dispositivos e servidores pelo qual a informação passa antes de chegar no seu destino.

Quando você instala um certificado SSL a transmissão de dados é configurada para ser feita via HTTPS. Ambas as tecnologias andam de mãos dadas e não funcionam uma sem a outra. URLs são procedidas por HTTP (Hypertext Transfer Protocol) ou HTTPS (Hypertext Transfer Protocol Secure). Isso é efetivamente o que determina como qualquer dado recebido ou enviado é transmitido.

   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).**

A certificação 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.

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. Ou seja, como seu nome indica, a ICP-Brasil é uma grande infraestrutura que envolve diversos órgãos e recursos visando possibilitar a validação de documentos em meio eletrônico, com a mesma equivalência dos documentos em papel.