Tulio Jose Germano Martins 11211EMT005

1)

Disable SSH Password Login:

O password é desabilitado por não ser mais seguro. Caso o server for invadido, o password de autenticação vai apresentar uma senha e usuário valido e isso pode comprometer ainda mais server.

Disabling Direct Root SSH Login:

Cria-se um usuário que não possui as permissões raiz. Uma das formas de contornar esse problema é melhor colocar menos privilégios que ainda seja capaz de exercer determinadas tarefas, limitando assim o acesso ao hacker de maiores privilégios

Charnging the default SSH port:

Ocultar as portas de acesso para casos de ataques mais fracos ou corriqueiros, mas não deixa imune a ataques mais fortes.

Disabling IPv6 for SSH:

Firewalls mal configurados protegem somente endereços IPv4.

Setting Up a Basic Firewall:

Para que isso não ocorra,é necessário configurar o firewall corretamente para proteger de ataques externos

Unattended Server Auto Upgrading

Alguns upgrades automáticos podem deixar falhas nas aplicações ,e essas falhas podem apresentar brechas nas aplicações.O ideal é organizar o melhor momento para fazer esses upgrades para já identificar as brechas e conserta-las manualmente.

2)

a) O melhor método para armazenar um conjunto de senhas em um sistema embarcado é o HMAC.

b)

A criptografia simétrica utiliza uma única chave em que o emissor e o destinatário compartilham .Ela define a forma que o o algoritmo vai revelar o conteúdo.Ex:

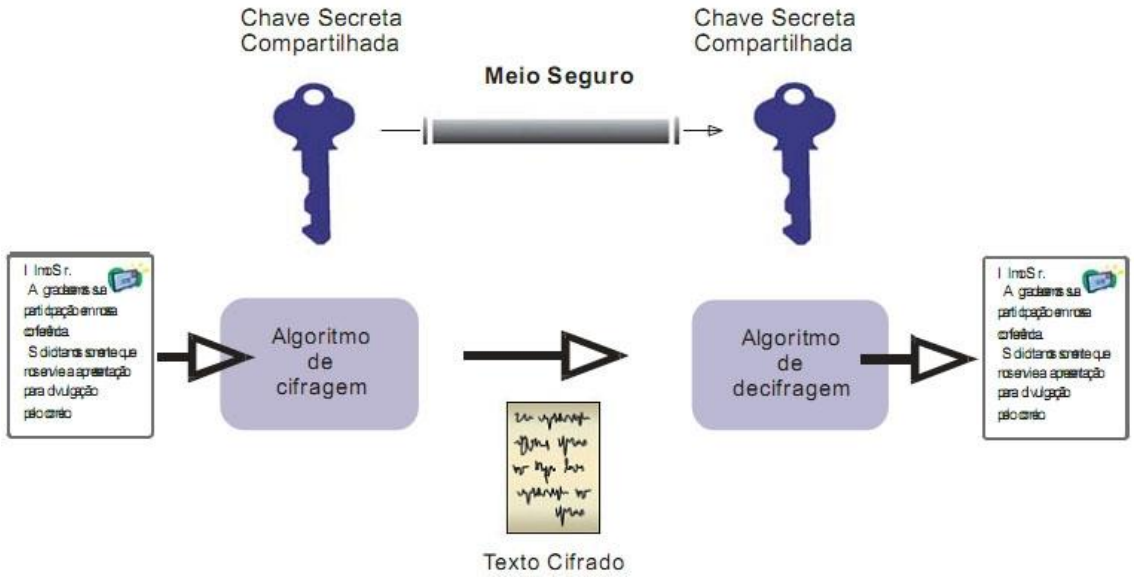


Figura 1: Diagrama esquemático da criptografia simétrica(https://www.gta.ufrj.br/grad/07_2/delio/Criptografiasimtrica.html)

c)

A diferença entre criptografia e a hash é que no método hash, gera numero a partir de uma sequencia de texto que é chamado de hash da mensagem. Já o método de criptografia utiliza algoritmos para criptografar e uma chave para retornar a mensagem a sua forma original.

3)

a)

Com a utilização de antminer, tem-se uma quantidade bem maior de hashs se comparado somente com a utilização de GPU e CPU para o processo.

b)

O **protocolo HTTPS** possui uma camada extra de proteção, indicando que sites e domínios que possuem esse protocolo são seguros para o usuário acessar.
O protocolo HTTPS é muito usado por sites com sistemas de pagamentos que dependem proteção para assegurar dados, informações de conta e cartão de créditos dos usuários.

Essa proteção é feita por certificação digital, que cria uma criptografia para impedir que ameaças e ataques na internet tenham acesso indevido às informações dos usuários.

O HTTPS aparece em um navegador quando o site acessado possui um certificado SSL instalado. O SSL cria um canal de proteção entre o cliente e o servidor, adicionando a letra “S” ao HTTP e reforçando uma camada extra de segurança

Transport Layer Security, o TLS, é um protocolo de segurança aplicado a web sites para garantir que todas as atividades realizadas naquele ambiente estejam protegidas contra ataques e vazamentos. Ele não impede consultas de domínios feitas pelo WHOIS, mas protege dados financeiros e pessoais de usuários que acessam e-commerces, sites e blogs.

O uso do TLS é amplo, já que seu padrão de atuação é internacional. Para as empresas que recorrem ao certificado em seus sites isso significa que, independentemente de onde o usuário estiver, o protocolo terá a mesma eficácia. Toda troca de dados fica devidamente protegida contra qualquer interceptação indevida que, se acontecer, não será capaz de acessar as informações de maneira legível.

O funcionamento do TLS

A base do funcionamento do TLS como um protocolo de segurança é sua capacidade de codificar mensagens e informações. Assim, quando um usuário navega por um site e informa dados como endereço, número de telefone, código de segurança do cartão de crédito, entre outros, o TLS é capaz de “esconder” esses registros de quem não deveria ter acesso a eles.

O protocolo faz isso codificando qualquer mensagem que vai de um ponto a outro, ou seja, do site ao usuário e vice-versa. São criadas chaves de acesso às quais só emissor e receptor têm acesso e, quando uma informação faz esse caminho, o certificado TLS autentica quem tentou acessar o conteúdo. Caso não seja um desses dois pontos, não há a possibilidade de acessar a mensagem.

As mensagens são criptografadas, ou seja, seu conteúdo original é escondido para que, por exemplo, em um ataque hacker, a informação interceptada não possa ser lida. Isso garante que todas as atividades realizadas em um site com o certificado TLS se mantenham protegidas, acessíveis apenas por emissor e receptor.

c)

O Certificado Digital é um documento eletrônico que funciona como um RG de pessoas físicas e jurídicas no meio virtual. Com ele, é possível assinar documentos, emitir notas fiscais e fazer diversas operações remotamente com validade jurídica.

Esta ferramenta garante proteção às transações via internet e outros serviços digitais, já que a tecnologia foi desenvolvida para fornecer segurança, autenticidade, confidencialidade e integridade às informações.

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.

Com o certificado digital é possível fazer transações, que antes seriam feitas presencialmente, de forma remota. Isso garante mais agilidade e ganho de tempo

Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é uma cadeia - ou elos - hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão e de empresas.

O modelo brasileiro é o de certificação com raiz única. A AC-Raiz é a primeira autoridade da cadeia de certificação, na ICP-Brasil a AC-Raiz é o ITI, que executa as Políticas de Certificados e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

O ITI, além de desempenhar o papel de Autoridade Certificadora Raiz – AC-Raiz, credencia e descredencia os demais participantes da cadeia, supervisiona e audita os processos.