Semana 12 – Segurança e Criptografia

Nicolas Bruno Santos Pereira -11621EMT013

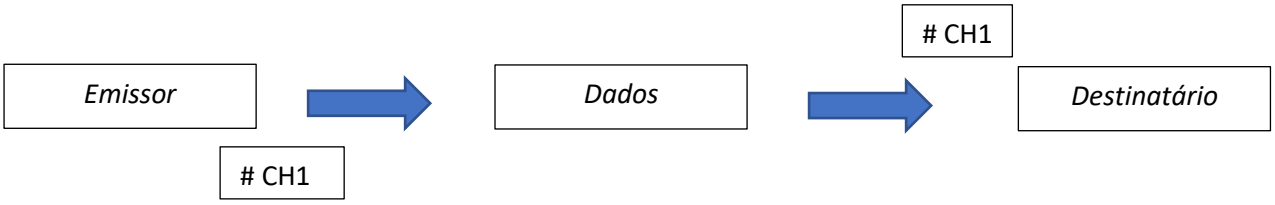
1) **Apresente um resumo das 6 dicas apresentadas no vídeo explicando a razão assumida para cara uma delas**
    - Desabilitar senhas de login SSH: embora não seja uma ação que garantirá segurança robusta, cria uma barreira a mais evitando que o comprometimento da máquina ocorra, já que, normalmente, as senhas são fracas.
    - Desabilitar login root SSH: impede que a senha não seja reutilizada na criação do usuário não privilegiado, não possibilitando o acesso como root (exemplo nginx), principalmente tratando-se de ambientes servidores.
    - Alterar porta padrão SSH: embora seja uma ação muito simples e fraca, garante apenas a proteção contra dispositivos que procuram servidores SSH com senhas fracas. É uma ação "snakeoil"
    - Desabilitar padrão IPv6: uma ação mais contundente nesse sentido seria programar o SSH para listar somente IPv6. Seria mais efetivo, inclusive, que o método de alteração de porta.
    - Configurar um firewall básico: o argumento baseia-se no bloqueio de todas as portas e abertura somente das necessárias para alguma ação. Outro snakeoil.
    - Atualizações automáticas de servidores: a maioria das atualizações são benéficas e o contexto envolvendo os servidores é mais complexo

2) **A partir do vídeo disponível no link abaixo, explique:**
    a. **Qual o melhor método para armazenar um conjunto de senhas em um sistema embarcado, conectado à rede?**

    Dentre os critérios apresentados no vídeo, pode-se dizer que a utilização de algoritmos por Data Encryption Standard (DES), escolhido pelo National Institute of Standards and Technology como padrão de encriptação do governo americano, seria um bom método. Não é aconselhável aos programadores criarem seus próprios algoritmos de encriptação.

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

A criptografia no modelo simétrico envolve um algoritmo e uma chave de segurança, os quais trabalham juntos para tornar um conteúdo sigiloso. A chave para acesso é compartilhada entre emissor e destinatário, sendo esta uma sequência única de bits. No diagrama, CH1 é a chave simétrica



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

A principal diferença entre eles é que o hash, diferentemente da criptografia, não consegue ser convertido na mensagem original após o processo.

3) A partir dos vídeos disponíveis no link abaixo, explique:

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

A relação surge devido a necessidade de mineração (transação) do bitcoin. O hash é um algoritmo utilizado pelo protocolo do bitcoin e é um hash criptográfico, o qual está associado a essas transações. É considerada parte essencial do sistema, pois mede e também representa a produtividade e eficiência da máquina de mineração utilizada.

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

O protocolo TLS criptografa o tráfego de internet de todos os tipos, sendo o mais comum o tráfego da web. Nesse sentido, quando a url web apresenta-se como https e há a presença de um pequeno cadeado, significa que o TLS/SSL está sendo utilizado. Ainda, a criptografia assimétrica envolve inúmeras possibilidades e problemas matemáticos difíceis, mas o TLS usa essa criptografia no início da sessão de comunicação entre cliente e servidor e um handshake é criado.

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).

Os certificados digitais encaixam-se como documento eletrônico dos cidadãos e utilizam o ciframento de mensagens, verificação de identidades e as assinaturas digitais para se tornar mais seguros e imunes a falhas de segurança. Já a "Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão". O sistema utiliza um conjunto de técnicas, práticas e procedimentos elaborado para suportar um sistema criptográfico com base em certificados digitais." O Comitê Gestor da ICP-Brasil estabelece a política, os critérios e as normas para regulamentar a operação de Autoridades Certificadoras (AC), Autoridades de Registro (AR) e demais prestadores de serviços de suporte em todos os níveis da hierarquia de certificação, credenciando as respectivas empresas para a emissão de certificados no meio digital brasileiro".