Nome: Guilherme Gonzaga Silva nº 11621EMT021

1. **Apresente um resumo das 6 dicas apresentadas no vídeo disponível em: https://www.youtube.com/watch?v=fKuqYQdqRIs explicando a razão assumida para cada uma delas.**

- Desativando login de senha SSH (secure shell): Senhas não seguras, pois se o servidor já foi comprometido (hackeado), o uso da autenticação por senha revelará uma combinação válida de nome de usuário/senha para o invasor, o que pode levar outros comprometimentos. Porém, quando digitamos uma senha, ela ao digitar está não criptografada, mas ela entra no túnel que está criptografado, dessa forma, utilizar senhas não é tão ruim assim, desde que não reutilize senhas e utilizar senhas com símbolos, letras, número, etc. Logo, é recomendado que utilize chaves SSH, não por segurança, mas sim por conveniência.
- Desativando direct root login direct: outra dica seria desabilitar o login root direto por meio do protocolo SSH, e colocar privilégios a usuário se permissão do root e colocar usuário e senha ao grupo SUDO, permitindo ao usuário executar comando root mas sem ser root. Por isso, esses aspectos ainda são mais por conveniência também, logo desabilitar o root login SSH não protege de hackers.
- Alterando a porta SSH padrão: a afirmação “se você não consegue ver ou encontrar as portas que usamos, você não pode nos hackear” não é verdadeira. Esse método somente irá atrasar o “hack”, o ideal é seguir as recomendações anteriores.
- Desativando IPv6 para SSH: as possibilidades de endereço com IPv4 são menores do que o IPv6, logo bloquear o IPv4 é mais cara para o invasor pois banir o IPv6 é um pouco menos útil, pois há mais endereços para escolher e também um firewall mal configurado que cobre apenas endereços IPV4 pode permitir que o invasor cruze o IPv6, porém o problema será o firewall mal configurado e não o IPv6. Logo, desabilitar o IPv6 não o torna muito mais seguro (especialmente desabilitar apenas o IPv6 para ssh.
- Configurando um firewall básico: os firewalls geralmente bloqueiam as portas e, quando necessário, basta desbloquear. 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. Mas talvez você tenha se sentido bem por ter feito algo com fogo.
- Atualização automática de servidor autônomo: A atualização não ajuda nos casos de uma nova vulnerabilidade séria for encontrada e quando o webapp que você usa para o servidor é um alvo muito mais fácil de atacar que ssh ou nginx. Mas, as vantagens de ter atualização automática são em grande parte contrariadas pelo risco de ter que consertar coisas em caso de interrupção causada pela atualização do pacote e provavelmente será necessário corrigir o software manualmente de qualquer maneira.

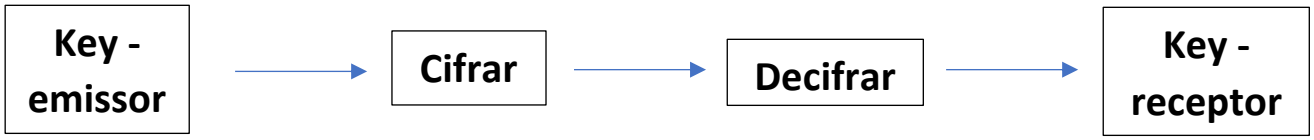
2. A partir do vídeo disponível no linka baixo, explique:

https://www.youtube.com/watch?v=CcU5Kc_FN_4

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

Atualmente, o melhor método para encriptação de senhas é o AES (Advanced Ecrtyption Standard) que é rápida o suficiente para encriptar e desencriptar dados do próprio hd em tempo real. Nem um computador quântico é capaz de quebrar o AES, somente diminuir sua grandeza. Tal algoritmo reverte o processo e decripta do chipertext pro plaintext.

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



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

O hash converte os dados em resumo ou hash da mensagem, que é um número gerado a partir de uma sequência de texto, enquanto a criptografia usa algoritmos de criptografia e uma chave para converter a mensagem em um formato irreconhecível.

2. **A partir dos vídeos disponíveis no link abaixo, explique:**

https://www.youtube.com/watch?v=_qypi2NKCcg

https://www.youtube.com/watch?v=HCHqtpipwu4

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

O hash é utilizado como algoritimo no protocolo do bitcoin e outras criptomoedas. Tem a função de transformar um grande número de informações em uma sequência numérica hexadecimal de tamanho fixo. Nesse caso, para cada hash, é gerado um número de 512 bits. Na mineração, as GPU's tem a função de gerar esses hashs.

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

Ao instalar um certificado SSL, a transmissão de dados é configurada para ser via HTTPS. Com isso, somente quem está na ponta (cliente/servidor) vê o conteúdo, o laço está encriptado.

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 ICP-Brasil é uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meio eletrônico. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, uma Autoridade Certificadora (AC). As regras estabelecidas pelo Comitê Gestor da ICP-Brasil, determinam que a assinatura associa uma entidade, pessoa, processo servidor a um par de chaves criptográficas. Esse sistema de confirmação é conhecido como criptografia assimétrica. Cada pessoa ou entidade recebe dois códigos ao criar o certificado: certificado público, que deve ser compartilhado; certificado privado, que deve ser mantido em segurança. Assim, quando um documento é codificado com a chave pública, ele só pode ser decodificado com a chave privada correspondente.