Universidade Federal de Uberlândia
Engenharia Mecatrônica
Sistemas Digitais para Mecatrônica
Murilo Marchi Pereira – 11521EMT005
Semana 12 – Segurança e Criptografia de Sistemas Linux

1. **Descreve o que é cyber segurança e os seis tipos apresentados no vídeo: https://www.youtube.com/watch?v=mo3R-LDTdos**

Segundo o vídeo, cyber segurança é o conjunto de práticas que protegem de ataques digitais os sistemas e redes de computadores. Os tipos de cyber seguranças citados são: segurança de redes; segurança de informação; segurança de nuvem, segurança de internet das coisas; e segurança de sistemas mobile.

2. **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.**

A primeira dica é desativar login de senha SSH (secure shell), pois se o servidor já tiver sido comprometido, o uso da autenticação por senha revelará uma combinação válida de nome de usuário e senha para o invasor podendo levar a outros comprometimentos. Porém, quando uma senha é digitada, esta não está criptografada, mas ela entra no túnel que está criptografado, dessa forma, utilizar senhas não é tão ruim assim, desde que não reutilize senhas e ela contenha símbolos, letras maiúsculas e minúsculas e, números. Portanto, a utilização de chaves SSH é recomendada por conveniência, e não por segurança.

A segunda dica é desabilitar o login root direto por meio do protocolo SSH, e colocar privilégios ao usuário sem permissão do root e colocar usuário e senha ao grupo SUDO, permitindo ao usuário executar comando root sem ser root. Esses aspectos ainda são também apenas por conveniência e não concedem maior proteção. Também pode-se alterar a porta SSH padrão para atrasar futuras invasões.

A quarta dica é desativar IPv6 para SSH, pois as possibilidades de endereço com IPv4 são menores do que o IPv6, portanto o bloqueio do IPv4 é mais caro para o invasor, já que banir o IPv6 é um pouco menos útil, havendo mais endereços para escolher. Um firewall mal configurado que cobre apenas endereços IPV4 também pode permitir que o invasor cruze o IPv6, mas neste caso o problema é o firewall mal configurado e não o IPv6. Logo, desabilitar o IPv6 não o torna mais seguro (especialmente desabilitar apenas o IPv6 para SSH).

A quinta dica é configurar um firewall básico. Firewalls geralmente bloqueiam as portas e (quando for necessário, basta desbloqueá-las) e, eles podem ajudar a impedir ataques usando portas se for configurado de maneira adequada. No entanto, apenas configurá-lo sozinho para bloquear todas as portas, exceto as necessárias, não fará aumentará a segurança.

A última dica é desativar a atualização automática de servidor autônomo. Essa atualização não ajuda nos casos de uma nova vulnerabilidade séria for encontrada e quando o *webapp* usado para o servidor é um alvo fácil de ser atacado 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 uma interrupção causada pela atualização do pacote e provavelmente será necessário corrigir o software manualmente de qualquer maneira.

3. **A partir dos vídeos disponíveis nos links:**

https://www.youtube.com/watch?v=CcU5Kc_FN_4
https://www.youtube.com/watch?v=fCcMfu_Ni4E

Descreva como a segurança de um sistema de embarcado deve ser pensado. Nessa descrição, considere:

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

O melhor método para encriptar senhas atualmente é o Advanced Ecrtyption Standard (AES). Este método encripta e decripta dados do disco rígido em tempo real. Um computador quântico é capaz apenas diminuir sua grandeza do AES. Tal algoritmo reverte o processo e decripta do chipertext para o plaintext.

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

Criptografia de chave simétrica se dá por meio de de uma função que encripta os dados em uma nova sequência encriptada utilizando uma mesma chave. Os diferentes tipos de implementação podem gerar resultados de tamanho variados; de mesmo tamanho; que se repetem de confrome a entrada, entre outros tipos. Pode-se ver de forma mais simples uma função M com entrada E e saída S, então:

$$S = M(E) \leftrightarrow E = M(S).$$

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

Um sistema hash converte os dados em um resumo (ou um hash) da mensagem, que é um número gerado a partir de uma sequência de texto, enquanto um sistema de criptografia utiliza um algoritmo e uma chave para criptografar a mensagem convertendo ela em um formato irreconhecível.

d) **Explique o que é STRIDE e 'Threat Model'.**

Threat Model é um processo onde possíveis ameaças podem ser identificadas, enumeradas e soluções podem ser propostas e priorizadas. Esse processo consiste no levantamento de riscos e avaliação dos *assets* e do custo para protege-los, tendo como resultado a modelagem do produto final.

e) **Segurança de boot**

O *Secure boot* tem o objetivo de proteger a integridade e autenticidade do código para se certificar que os binários executados foram por pessoas ou companhias confiáveis, porém esse mecanismo tem custos como maior tempo de inicialização e maior dificuldade de desenvolvimento da plataforma. Esse sistema é baseado na verificação de assinaturas digitais, onde cada componente do sistema deve ser verificado pelo componente anterior a ele, criando o que é chamado de cadeia-de-confiança.

f) Criptografia de dados e de código.

Criptografia de dados consiste na codificação de um conjunto de dados afim de certificar a proteção de propriedades intelectuais e a confidencialidades de dados individuais.

4. 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 sistema hash é utilizado no protocolo do bitcoin para transformar um número grande de informações em uma sequência numérica hexadecimal de tamanho fixo. Para cada hash, é gerado pelas GPUs na mineração um número de 512 bits.

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

Quando um certificado SSL é instalado, a transmissão de dados é configurada para https. Com isso, somente quem está na ponta (cliente/servidor) tem acesso conteúdo e, o enlace é 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 ICP-Brasil é um certificado de identidade virtual que permite a identificar o autor de uma transação feita em meio eletrônico e, esse documento 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, a um par de chaves criptográficas, uma entidade, pessoa ou processo servidor. Esse sistema de confirmação é conhecido como criptografia assimétrica. Cada parte recebe dois códigos na criação do certificado: um certificado público, que é compartilhado e, um certificado privado, é mantido em segurança. Dessa forma, um documento codificado com a chave pública, só pode ser decodificado com a respectiva chave privada.