UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA
DISCIPLINA: SISTEMAS EMBARCADOS II

Semana 12

Segurança e Criptografia de Sistemas Linux

Prof. Éder Alves de Moura

Ana Júlia Costa Santana – 11811ETE003

10 de Junho de 2021

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.

Dica 1: Desabilitar logins de senha para SSH
SSH (Secure Shell) é o padrão para acessar um servidor Linux remotamente, para diminuir chances de ser hackeado, é mais comum utilizar chaves, isso é feito atualizando o sshd_config e desabilitando o PasswordAuthentication. O servidor ssh tem sua própria chave privada, e usa sistema de túnel para as senhas, logo seu login com senhas é parecido com o https, e como são senhas você precisa criar senhas seguras, que não são fáceis de adivinhar ou que você usa repetidas vezes, uma forma de fazer isso é com um Gerenciador de Senhas que gera senhas únicas e aleatórias. Usar as chaves SSH te inibe desse processo, logo não torna seu servidor mais seguro, mas é conveniente.

Dica 2: Desabilitar login de root direto
A recomendação é criar um usuário sem privilégios sem permissões de root. Utilizar o mínimo de privilégios o possível é um aspecto de segurança muito importante para o software. No entanto, não faz tanto sentido assim, já que o propósito de um servidor e diferente do laptop na essa ação de trabalho local, no laptop você quase não usa root, e se você baixar algo com um malware, ele não vai ser instalado no root, o server por outro lado é para configurar um serviço e depois executá-lo e para instalados você precisa do root. Outra coisa que acompanha esta recomendação de desativação é de adicionar o usuário sem privilégios ao grupo sudo, assim ele pode executar comandos root, com o sudo, e esse processo para a perspectiva de segurança significa a mesma coisa, e mesmo que o sudo exija senha esse passo é facimenite contornado, logo esta dica também é uma conveniência, por exemplo, se você trabalha com um time é mais fácil adicioná-los ao grupo sudo do que dar a todos a senha root.

Dica 3: Mudar as Portas SSH padrão
Esta é uma recomendação obscura, pois para um hacker capaz de invadir um SSH, uma simples mudança de porta não iria impedi-lo. Isso só auxilia contra script kiddies e scanners automatizados que buscam servidores SSH com senhas fracas. Neste caso a solução é usar uma senha forte ou as chaves SSH.

Dica 4: Desabilitar IPv6
“IPv6 é melhor que o IPv4, mas o uso não é aproveitado porque ninguém mais o usa. Os hackers por sua vez o usam bastante para enviar tráfego malicioso.” Endereços IPv4 são mais raros, assim banir ou bloquear um deles é mais caro para o hacker o que não ‘ocorre’ no IPv6 que possui muitos endereços, mas os custos não são tão significativos. Outro caso é o uso de firewalls que só protegem o IPv4, assim o invasor pode usar o IPv6 para alcançar qualquer coisa, logo o problema é o firewall, o ipv4 NAT é o melhor firewall para se ter em casa, mas isso não é aplicável ao servidor alugado num centro de dados. Logo a melhor recomendação é fazer o SSH ouvir apenas em ipv6 e desabilitar o IPv4, porque isso é, mais efetivo que a mudança de portas.

Dica 5: Configure um Firewall Básico
A recomendação é usar iptables ou UWF(Firewall Descomplicado) , para bloquear portas. Mas se você está usando determinadas portas para comunicação, o firewall está permitindo o uso delas ou seja, ouvindo uma porta, você permite que o exterior interaja com a porta em questão, logo o uso do firewall não faz nada.

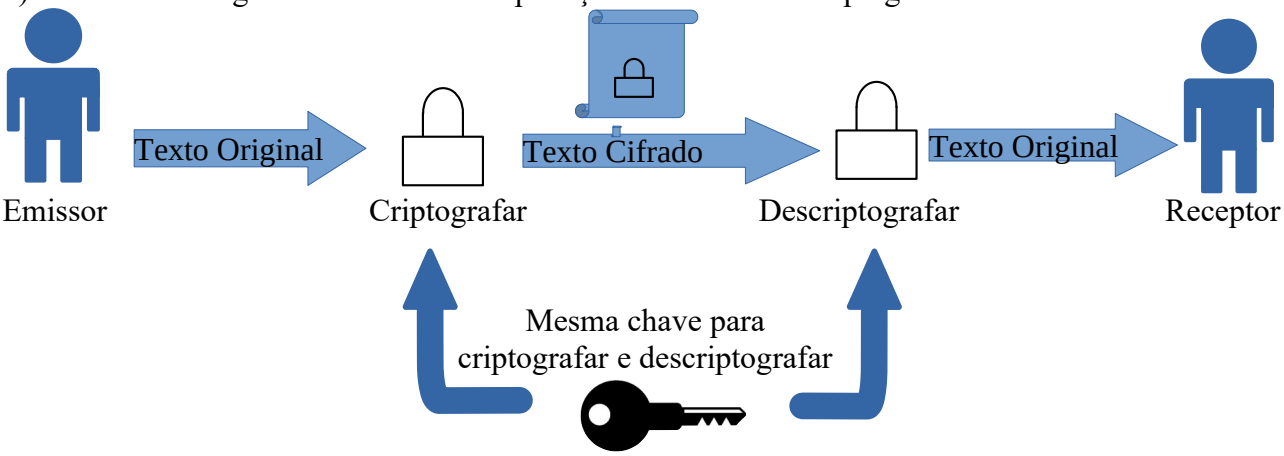
Dica 6: Atualizações Automáticas Autônomas de Servidor

Num servidor Ubuntu, você pode atualizar pacotes ou o próprio sistema, com o apt-get upgrade ou apt-get dist-upgrade. As atualizações automáticas são muito vitais para a segurança pública em geral, forçá-las um Windows, Android ou IPhone é ótimo, pois mantê-los atualizados é importante, mas uma estação de trabalho usada ativamente com muitos softwares e usuários que não entendem a tecnologia é diferente de um servidor onde um serviço está sendo executado. Se você deseja hospedar algo num servidor, habilitando ou desabilitando atualizações autônomas
é uma forma de quebrar e interromper o servidor, por que nem todas as atualizações são seguras ou relevantes neste caso. Numa empresa onde os dados dos clientes estão em jogo, é necessário ter um administrador de programa qu possa lidar com a situação. Se houver uma falha de segurança numa atualização você provavelmente ainda precisa fazer o patch na mão e qualquer app que está rodando no servidor é mais vulnerável, e não são cobertos pelas atualizações automáticas.

2 – A partir do vídeo disponível no link, explique:

a) Qual o melhor método para armazenar um conjunto de senhas em um sistema embarcado, conectado à rede.
Uma table de senhas em plaintext nunca deve ser utilizada, a criptografai também tem suas falas, e salvar apenas o hash pode gerar problemas devido as senhas comuns que os usuários utilizam, com dicionários ou rainbow tables e as chances de colisão, logo uma solução é concatenar um número grande(salt) junto da senha e gerar o hash a partir disso. Como Antiminers conseguem quebrar essa senha, podem ser usados algarismos de derivação de chaves com a capacidade de adicionar dificuldade no processo. PBKDF2. Derivando chaves a partir de senhas.

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



É uma função onde é passado um texto e um segredo como entrada, e a saída é o texto bagunçado, é considerada simétrica porque usar o texto bagunçado de volta para a função usando o mesmo segredo, o texto original é recuperado.

c) Diferença entre um sistema de criptografia e um hash de validação.
Um sistema de criptografia permite que o processo seja revertido, descripitando o ciphertext em plain text, os algoritmos de hash são *one-way* (direção única), logo irreversíveis, ela ega um plain text e cospe uma saída de tamanho fixo, e o mais indicado hoje é SHA3. E o problema do hash é a chance de colisão que matematicamente é algo muito comum de ocorrer.

3 – A partir dos vídeos disponíveis nos links 1 e 2, explique:

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

Os FPGAs são circuitos programáveis via software, os ASICs são chips feitos sob medida direto da fábrica, e existem os feitos especificamente para gerar hashes de mineração. O proof-of-work que é o processo de assinatura de um bloco de Bitcoin é basicamente achar um hash especial desse bloco, que quando um número dentro desse bloco é alterado ele altera o hash final até que um hash que tem um certo número de zeros a esquerda seja encontrado, essa sequência de zeros é a dificuldade de mineração., quem acha esse hash ganha a 'recompensa' em bitcoin. Usar uma versão derivada de um Antiminer que gera hashes normais, menos com o salt pode ser usada para comparar com um dicionário é um processo usado para quebrar senhas vai força bruta.

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

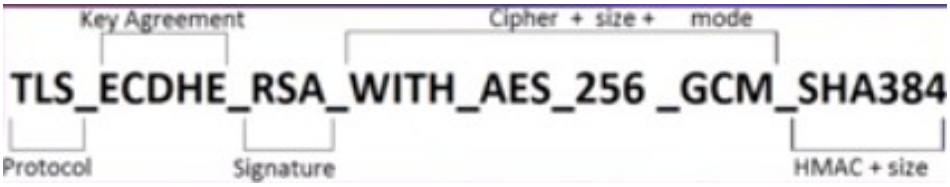


Figura 1: Diagrama de funcionamento da criptografia no portocolo TLS

Neste caso é feito apenas um hash simples via SHA2, e esse hash pode ser usado como segredo num algoritmo como o AES e enviar mensagens criptadas. Para o TSL e o SSH existe uma etapa nomeada negociação de Cipher, quando eles fazem o handsake, o servidor envia uma lista de combinações de ciphers que ele suporta, e o navegador vê sua própria lista e eles escolhem uma combinação que ambos suportam, isso é um Cipher Suite.
O Difie Hellman aplicado, pode sofrer atacques man in the midle, assim utiliza-se um STS, para providenciar autenticação a esse método. O SSL (Secure Sockets Layer) e seu sucessor TLS (Transport Layer Security) são protocolos de criptografia projetados para internet. Permitem a comunicação segura entre os lados cliente e servidor de uma aplicação web. A grande vantagem desses protocolos é que eles agem como uma subcamada nos protocolos de comunicação na internet (TCP/IP). É aí que entra a diferença entre o HTTP e o HTTPS, do qual o primeiro é trafegado em texto puro e o segundo encriptado com SSL/TLS. Ou seja, é possível operar com ou sem TLS (ou SSL), basta o cliente indicar ao servidor se quer configurar uma conexão segura ou não.

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).
Certificado digital é um documento eletrônico que contém dados sobre a pessoa física ou jurídica que o utiliza, servindo como uma identidade virtual que confere validade jurídica e aspectos de segurança digital em transações digitais., permite ao usuário assinar digitalmente documentos e ter acesso a sistemas eletrônicos restritos, principalmente de órgãos públicos na internet, como Receita Federal e INSS. Também comprova a identidade em sistemas virtuais integrados para realizar atividades profissionais de várias categorias. Basicamente equivale a uma carteira de identidade do mundo virtual, agindo como um CPF ou CNPJ.
Essa ferramenta está disponível no Brasil desde 2001, após a criação da Infraestrutura de Chaves Públicas Brasileira – ICP Brasil, que é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual de pessoas físicas ou jurídicas .Observa-se que o

modelo adotado pelo Brasil foi o de certificação com raiz única (chaves públicas), sendo que o Instituto Nacional de Tecnologia da Informação- ITI, além de desempenhar o papel de Autoridade Certificadora Raiz – AC-Raiz, também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos. Utiliza o sistema de confirmação de criptografia assimétrica. Existem os certificados : A, S, T e os subsequentes com tipos 1, 3 e 4. Claro o tipo 4 é o mai seguro dentre esses para cada uma das opções.