Semana 12

Ricardo Henrique da Silva Assis- 11611EMT013

1)

- **Disable SSH Password Login:** Deve-se desativar o password pois eles são inseguros. Se o server for comprometido, o password de autentificação revela um usario e senha validos que o hacker pode usar, causando ainda mais danos.
- **Disabling Direct Root SSH Login:** Criar um usuário que não possua as permissões da raiz. É sempre melhor utilizar a menor quantidade possível de privilégios para cumprir determinada tarefa. Isso se deve ao fato que se determinado usuário for hackeado, o hacker não terá acesso aos privilégios da raiz.
- **Changing the Default SSH Port:** Em caso de hackers mais fracos, ou ataques mais comuns, esconder a porta que você usa pode ajudar a evitar problemas. Contudo, isso não ajuda em casos de ataques mais fortes.
- **Disabling IPv6 for SSH:** Alguns firewalls mal configurados podem cobrir/proteger apenas endereços IPv4.
- **Setting Up a Basic Firewall:** É necessário configurar o firewall de forma correta para que ele seja realmente útil contra ataques.
- **Unattended Server Auto Upgrading:** Upgrades automáticos são bons em certas aplicações, mas podem ocasionar em falhas que necessitarão de concertos manuais. Os upgrades automáticos também não aconselhados em aplicações em que se deve considerar o melhor momento para assim minimizar interruoções.

2)

a. HMAC.
b. A criptografia simétrica faz uso de uma única chave, que é compartilhada entre o emissor e o destinatário de um conteúdo. Essa chave é uma cadeia própria de bits, que vai definir a forma como o algoritmo vai cifrar um conteúdo. Como vantagem, a criptografia tem uma boa performance e a possibilidade de manter uma comunicação contínua entre várias pessoas simultaneamente. Caso a chave seja comprometida, basta efetuar a troca por uma nova, mantendo o algoritmo inicial. A seguir é mostrado um diagrama mostrando o funcionamento da criptografia simétrica:

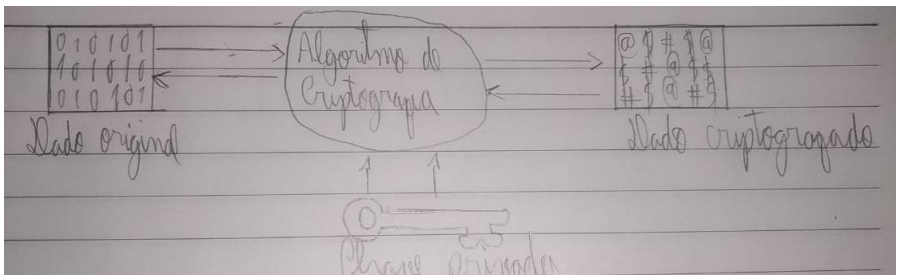

Figura 1: Diagrama esquemático da criptografia simétrica.

c. A diferença básica entre hash e criptografia é que 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.

3)

a. Utilizando-se de uma unidade de Antminer é possível uma quantidade bem maior de hashes do que seria possível utilizando-se apenas do poder de uma CPU ou de uma GPU

b. O HTTPS usa um certificado seguro (SSL) de um fornecedor terceirizado para proteger uma conexão e verificar se o site é legítimo. O que cria uma conexão segura e criptografada entre um navegador e um servidor, que protege a camada de comunicação entre os dois. Esse certificado criptografa uma conexão com um nível de proteção designado no momento da compra de um certificado SSL. Um certificado SSL fornece uma camada extra de segurança para dados confidenciais que você não quer que terceiros acessem. Essa segurança adicional pode ser extremamente importante quando se trata de gerenciar sites de e-commerce.

   O Protocolo TLS se situa entre as camadas de Aplicação e Transporte. Ele encapsula os protocolos de aplicação como o HTTP (Hypertext Transfer Protocol) e o FTP (File Transfer Protocol) e trabalha em cima de um protocolo de transporte como o TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol). Para que a transmissão seja confiável, deve ser utilizado o protocolo TCP, uma vez que o UDP está mais sujeito à perdas de informação, já que é datagrama.

c. O certificado digital é uma identidade eletrônica para pessoas ou empresas. Ele equivale à uma carteira de identidade do mundo virtual. Imagine uma versão eletrônica de todos os seus documentos, segura e com autenticidade garantida por criptografia complexa. Com ele, é possível garantir de forma inequívoca a identidade de um indivíduo ou de uma instituição, sem uma apresentação presencial. Na prática, funciona como um CPF ou um CNPJ eletrônico. A ICP-Brasil é uma grande infraestrutura que envolve diversos órgãos e recursos visando possibilitar a validação de documentos em meio eletrônico, com a mesma equivalência dos documentos em papel.