GABRIEL ELISBAO DA SILVA – 11711EMT005

SEMANA 12

QUESTÃO 1

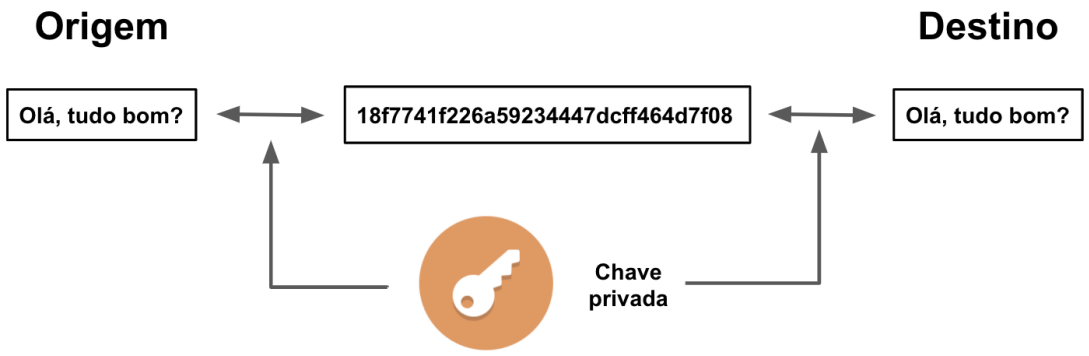
- Desabilitar SSH Password Login: O uso direto de senhas repassadas de forma simples diretamente aos servidores vem se tornando uma prática amplamente desencorajada, tanto porque já existem maneiras muito mais seguras de realizar esta autenticação quanto porque quando esta opção no contexto do protocolo SSH automaticamente ativa a comunicação, o que é não recomendado do ponto de vista de segurança.
- Desabilitar Direct root SSH Login: É mais vantajoso utilizar, assim como utilizado geralmente em diretórios do Linux para End Users, não utilizar o acesso de root diretamente, e ao invés disso configurar um usuário com acesso padrão e depois acessá-lo, pois assim teremos maior controle dos acessos repassados a possíveis atacantes, além de inserir uma camada extra de proteção até para possíveis erros ou confusões do próprio programador.
- Trocar a porta SSH padrão: Trocar a porta padrão de comunicação é uma atitude recomendada em vários ambientes da comunicação via internet pois ela diminui significativamente os riscos de ataques mais simples (mais igualmente perigosos) feitos por atacantes que não conhecem qual a porta utilizada e buscam presencialmente a porta padrão.
- Desabilitar IPv6 for SSH: Apesar de o IPv6 ser uma tecnologia em crescimento e com grandes chances de se tornar uma necessidade, do ponto de vista da segurança ele representa um grupo e funcionalidades muito maior do que o IPv4, porém na maior parte das vezes essas funcionalidades não estão sendo utilizadas pelo desenvolvedor do sistema, servindo apenas para abrir o leque de ferramentas de possíveis atacantes.
- Setup a Basic Firewall: O autor chama atenção especialmente para uma escolha consciente de qual o sistema de Firewall será utilizado pois muitas das vezes desenvolvedores utilizam firewalls altamente potentes de em ambientes q a sua função será simplesmente fechar as portas inutilizadas, gerando gastos desnecessários.
- Unattended Server Auto Upgrade Auto Upgrade é uma funcionalidade essencial em sistemas de usuário final, pois permite manter o usuário protegido de novas tipos de ataques, vírus e entre outros; porém essa realidade não se estende aos servidores, isso porque muitas vezes os serviços programados não conseguem se adaptar as mudanças tão facilmente quanto os usuários finais e dependem de características específicas dos sistemas utilizados ficando à mercê de bugs e vulnerabilidades quando estas atualizações acontecem.

GABRIEL ELISBAO DA SILVA – 11711EMT005

QUESTÃO 2

a) A melhor maneira de salvar as senhas de forma a proteger tanto a informação do usuário quanto a segurança do sistema seria passar sua senha por uma engine de IDs universais, exemplos clássicos destes modelos são: UUID e GUID.

b) Criptografia de chave simétrica é caracterizada pelo uso de uma função que encripta (ou decripta) os dados em uma nova sequência encriptada (ou decripta) utilizando uma mesma chave, embora os tipos de implementação possam ser os mais variados podendo gerar resultados de mesmo tamanho, tamanho variados, resultados que se repetem de acordo com a entrada e entre outros.



c) Temos que um sistema de criptografia basicamente faz uma troca de dados por meio de alguma lógica da forma em que ela possa ser transportada ou armazenada de forma segura de uma forma que ela possa ser armazenada seguramente e apenas acessada pelos dispositivos que possuam acesso a essa criptografia para esses dados específicos o hash de validação por sua vez é similar a uma impressão digital, tendo conhecimento dessa impressão podemos ter certeza se os dados foram ou não adulterados sem ter que analisar parte por parte, seria uma espécie de identidade dos dados armazenados.

GABRIEL ELISBAO DA SILVA – 11711EMT005

QUESTÃO 3

a) A bitcoin tem um sistema distribuído, a base por trás deste sistema é o uso de um sistema específico de criação de hashs os quais são guardados na famigerada Blockchain, o segredo do Bitcoin é permitir que estas operações altamente custosas de geração de hash possam ser feitas por qualquer um e oferecer grandes quantias pelo resultado assim alcançando a grande popularidade da moeda.

b) O HTTPS é uma extensão segura do HTTP de forma que os sites configuraram um certificado SSL/TLS para estabelecer uma comunicação segura com o servidor. SSL significa Secure Sockets Layer, um tipo de segurança digital que permite a comunicação criptografada entre um site e um navegador. Atualmente a tecnologia se encontra depreciada e está sendo completamente substituída pelo TLS. TLS é uma sigla que representa Transport Layer Security e certifica a proteção de dados de maneira semelhante ao SSL.

c) O Certificado Digital é uma maneira simples de garantir o gerador de determinado dado em um modelo altamente distribuido como a internet, geralmente esses sitemas se utilizam de uma caracteristica importante dos sistemas de chave dupla ou assimétricos quando se aplica o modelo de forma "inversa", ou seja, o gerador da mensagem utiliza a chave privada todos os receptores poderão utilizar a chave pública como uma espécie de assinatura única do arquivo. 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. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o 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.