

# **Sistemas Digitais para Mecatrônica**

## **Semana 12**

Rodrigo Souto Silva Mendes (**11321EMT011**)

Uberlândia, 2021

## **Questão 1**

Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas. O termo é aplicável a uma variedade de contextos, desde negócios até computação móvel, e pode ser dividido em algumas categorias comuns.

## **Questão 2**

### **2.1**

Desabilitar o password de login do SSH ou Secure Socket Shell que é um protocolo de rede que permite que os administradores de um servidor acessem um computador remoto, evitando que algum hacker possa utilizar isto contra o usuário uma vez que ele poderia ter acesso a informações do usuário facilmente se tivesse acesso a esse password.

### **2.2**

Desabilitar o acesso root do SSH, a recomendação vem de que é ideal sempre utilizar apenas os privilégios necessários à sua tarefa, uma vez que talvez ao executar a sua tarefa poderá ter algum risco de ter alguma informação interceptada ao longo disso, se o hacker tiver acesso ao root tendo acesso privilegiado isso representa um alto risco.

### **2.3**

Mudar as portas padrões utilizadas, uma vez que por serem comuns e conhecidas o ideal é que não se utilize as portas padrões, quanto menos informação os hackers tiverem para explorar essas brechas melhor será.

## **2.4**

Desabilitar IPv6, manter apenas IPv4 o firewall trabalha melhor com o IPv4 uma vez que as configurações mais comuns são focadas nele, teoricamente teríamos uma melhor forma de controle ao ignorar o IPv6, porém não fica muito claro a vantagem uma vez que ainda temos que analisar de fato se as configurações estão corretas, de um modo geral pelo maior uso do IPv4 seria mais seguro se manter neste.

## **2.5**

Configurar um firewall, mesmo que seja um simples, teremos várias opções e tipos, mas é importante ter pelo menos a mais simples delas, ele vai permitir que as aplicações do seu servidor possam acessar a internet, porém filtra quando algo está tentando acessar o servidor, gerando uma maior segurança.

## **2.6**

Desabilitar os updates automáticos no servidor, uma vez que mesmo sendo algo bom em outras plataformas conhecidas, ter maior controle sobre como e quando o servidor é atualizado é a melhor opção pois te dá maior controle sobre o que está acontecendo.

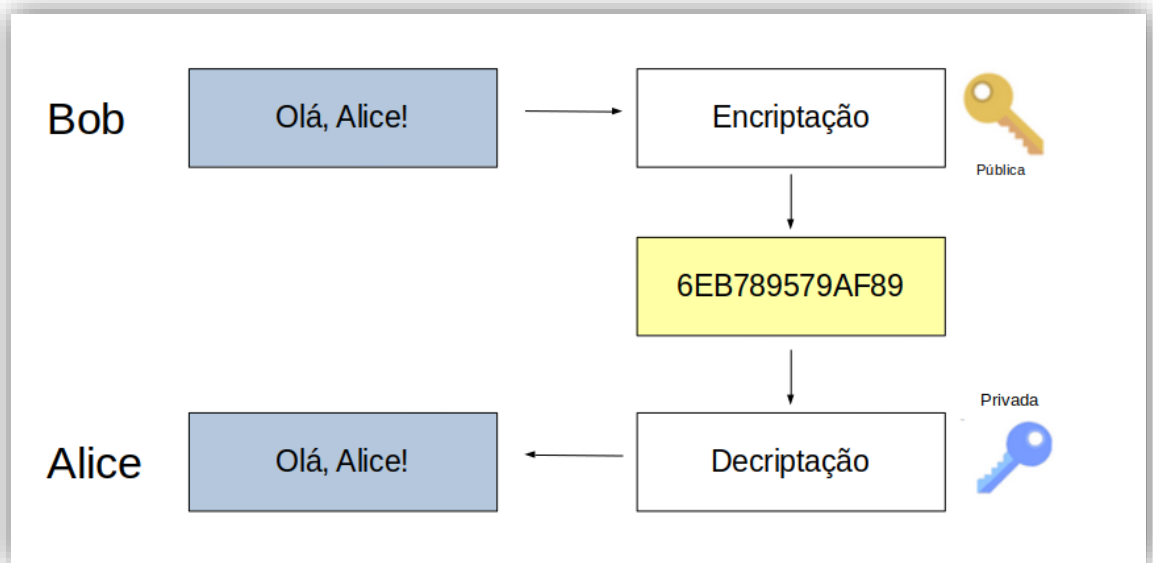
## **Questão 3**

### **3.a**

Utilizar hashing junto com algum tipo de criptografia para ter certeza de que além de segura a informação está devidamente segura e que não foi alterada devido ao caminho, apesar de que na questão de segurança não temos apenas uma medida mas sim uma gama gigantesca de parâmetros para serem analisados.

### 3.b

Basicamente este tipo de criptografia é utilizado quando ambos origem e destino possuem acesso a mesma chave, isto é, a mensagem é encriptada antes de ser enviada, e sem a chave que diz como essa mensagem pode ser “traduzida”, a mensagem não pode ser lida. Quando o destinatário recebe a mensagem e, se possuir a chave, ele pode descriptar . Abaixo temos uma ilustração.



### 3.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.