Igor Augusto – 11221EMT008

1.1 – Desativar o login com senha SSH

A utilização de senhas é insegura, pois a mesma é enviada do cliente para o servidor, por meio de texto puro em túnel, que pode ser comprometido. Ou mesmo, o compartilhamento de senhas com outros sites pode comprometer sua segurança. A utilização de chaves é mais segura, pois com a utilização da chave pública da máquina e a chave privada do usuário, quando houver uma tentativa de conexão com o IP de outra máquina, o servidor irá negar a conexão. Isso torna o sistema de login mais prático, mas não exatamente mais seguro.

1.2 – Desabilitar o login SSH direto na raiz

Desabilitar o login root, não protegerá contra a atividade de hackers, mas será possível evitar a atividade de usuários maliciosos, criando um alias sudo, para quem tentar executar atividades com esses privilégios, assim, o usuário não saberá que não executou o comando como sudo. Distribuir os privilégios sudo, gera registro das atividades e responsabilidade a quem foi delegado, e é mais seguro que fornecer a senha root para todos os usuários com privilégio sudo.

1.3 – Alterar a porta SSH padrão.

Altera a porta padrão é útil para conter scripts simples e scanners que verificam as portas padrão. Mas isso não protege contra hackeamento por senhas. Como citado anteriormente, para se proteger, a melhor forma é utilizar senhas fortes, ou uma chave SSH.

1.4 – Desativando IPv6 para SSH

Desabilitar o IPv6 apenas para SSH, não é muito útil, pois o restante do sistema ainda estará com ele habilitado. A alternativa seria desabilitar toda a interface de rede, mas isso poderia trazer erros relacionados a outros sistemas. Logo, essa diminuição na superfície de ataque, não é justificado, caso não esteja hospedando um servidor.

1.5 – Configurando um Firewall básico

Um firewall básico, irá aceitar qualquer tráfego que vier das portas que nele forem abertas. Se ele não for configurado de maneira correta, de modo a bloquear conexões de faixas de ip desconhecidas, não há uma real utilidade.

1.6 – Atualização automática autônomas em servidores

Atualizações nem sempre trazem benefícios, pois podem acarretar em erros, que terão que ser revertidos manualmente, causam vulnerabilidade, ou são pacotes desnecessários, portanto, atualizações automáticas não são uma boa ideia para servidores.

2.a – Guardando-as em uma tabela com dados protegidos por derivação de chaves, pois isso dificultaria o vazamento desses dados, em comparação com se estivessem em texto aberto ou criptografado

2.b –Ao passar uma entrada por uma função criptográfica, teremos uma saída, se passarmos essa mesma saída, pela função inversa, obteremos a entrada, isto é uma criptografia simétrica. Por exemplo, utilização um shift2 na palavra gato:

G A T O (SHIFT2>) I C V Q ; I C V Q (SHIFT2<) G A T O

2.c – A criptografia é uma função reversível, onde é possível obter a entrada, utilizando a função inversa e a saída, o hash é uma ferramenta unidirecional, onde não é possível obter a entrada a partir da saída. A criptografia transforma a entrada na saída, a partir de uma função, o hash transforma uma entrada de qualquer tamanho em uma saída de tamanho fixa, dependendo do protocolo que está sendo utilizado, dividindo a entrada em blocos de tamanho fixo, e realiza operações do primeiro com o segundo, sucessivamente, até sobrar o ultimo bloco, essas operações, assim como as funções, são específicas de cada método, podendo ser mais ou menos complexas, ter operações e parâmetros diferentes.

3.a – Para gerar um bloco de bitcoin, é necessário encontrar o hash inicial daquele bloco, para isso, é necessário poder de processamento para gerar muitos hashs por segundo, até acertar a combinação correta, quem acertar primeiro a combinação de um bloco, leva um valor em bitcoins. Todo o processo de geração de hashs envolve criptografia. Para alterar esses hashs, é utilizado o princípio da confusão e difusão de Shannon, onde, a confusão tende a criar uma função o mais complexa possível entre a entrada e a saída, e a difusão faz com que a estrutura da função fique o menos evidente possível, assim, aumentando a segurança das chaves.

3.b – Quando é iniciada a conexão cliente servidor, no handshake, há a definição de qual será a chave criptográfica, tendo a mesma definida, só o cliente e o servidor as conhecem, então, durante o envio dos pacotes encriptados, não há informações sobre a chave, tornando mais difícil, sua decriptação.

3.c - ICP brasil é o processo de certificação digital que dá validade aos certificados digitais brasileiros. As autoridades certificadoras distribuem, revogam e gerenciam titularidade das chaves, e conferem se as chaves privadas conferem com as chaves públicas. As autoridades de registro facilitam o contato entre os usuários e as autoridades certificadores. O certificado digital é composto por duas chaves, uma pública, que é compartilhada, e uma particular, que fica com o usuário, e é utilizada para atestar sua identidade, na assinatura de documentos, e acesso à sistemas, com a autenticação das duas chaves.