Personalização da configuração do serviço OpeSSH

Objetivos

Desabilitar logins diretos como `root` e a autenticação baseada em senha para o serviço OpenSSH.

Configuração do servidor OpenSSH

Para editar o arquivo de configuração do openssh → /etc/ssh/sshd_config

A configuração padrão do servidor OpenSSH funciona bem para muitos casos de uso. No entanto, você pode fazer algumas alterações para fortalecer a segurança do seu sistema. Você pode proibir o login remoto direto para a conta `root` e pode proibir autenticação baseada em senha (em favor da autenticação de chave privada SSH).

Proibição do superusuário de fazer login

É uma boa prática proibir o login direto na conta de usuário `root` de sistemas remotos. Alguns riscos de permitir login direto com o usuário `root` incluem os seguintes casos:

- **O nome de usuário `root` existe em cada sistema Linux por padrão. Assim, um invasor em potencial precisa apenas adivinhar a senha, em vez de uma combinação de nome de usuário e senha válidos. Esse cenário reduz a complexidade de um invasor.**
- **O usuário `root` tem privilégios irrestritos, portanto, seu comprometimento pode levar a danos máximos ao sistema.**
- **Do ponto de vista da auditoria, pode ser difícil rastrear qual usuário autorizado fez login como o usuário `root` e fez alterações. Se os usuários tiverem que fazer login como um usuário comum e mudar para a**

conta `root`, você poderá ver um evento de log para fornecer responsabilidade.

Importante

A partir do Red Hat Enterprise Linux 9, o parâmetro `PermitRootLogin` é definido como o valor `prohibit-password` por padrão. Esse valor impõe o uso de autenticação baseada em chave em vez de senhas para fazer login com o usuário `root` e reduz o risco de ataques de força bruta.

O servidor OpenSSH usa a definição da configuração `PermitRootLogin` no arquivo `/etc/ssh/sshd_config` para permitir ou proibir usuários de fazer login no sistema com o usuário `root`, como no seguinte exemplo:

```
PermitRootLogin yes
```

Se o parâmetro `PermitRootLogin` estiver definido como o valor `yes`, qualquer pessoa poderá fazer login com o usuário `root` remotamente. Para evitar essa solicitação, defina o valor como `no`. Como alternativa, para evitar a autenticação baseada em senha, mas permitir autenticação baseada em chave privada para `root`, defina o parâmetro `PermitRootLogin` como `without-password`.

O servidor SSH (`sshd`) deve ser carregado novamente para aplicar as alterações.

```
[root@host ~]# systemctl reload sshd
```

Proibir a autenticação baseada em senha para SSH

Permitir somente logins baseados em chave privada à linha de comando remoto tem vantagens:

- **Os invasores não podem usar ataques de adivinhação de senha para invadir contas remotas no sistema.**
- **Com chaves privadas protegidas por senha, um invasor precisa da senha e de uma cópia da chave privada. Com senhas, um invasor precisa apenas da senha.**
- **Ao usar chaves privadas protegidas por senha com `ssh-agent`, a senha é digitada e exposta com menos frequência, além de o login ser mais conveniente para o usuário.**

O servidor OpenSSH usa o parâmetro `PasswordAuthentication` no arquivo `/etc/ssh/sshd_config` para controlar se os usuários podem usar a autenticação baseada em senha ao fazer login no sistema.

```
PasswordAuthentication yes
```

Com o valor padrão de `yes` para o parâmetro `PasswordAuthentication` no arquivo `/etc/ssh/sshd_config`, o servidor SSH permite que os usuários usem a autenticação baseada em senha ao fazer login. O valor `no` para `PasswordAuthentication` impede que os usuários usem a autenticação baseada em senha.

Sempre que você alterar o arquivo `/etc/ssh/sshd_config`, será necessário recarregar o serviço `sshd` para aplicar as alterações.

Importante

Se você desativar a autenticação baseada em senha para `ssh`, deverá garantir que o arquivo `~/.ssh/authorized_keys` do usuário no servidor remoto seja preenchido com sua chave pública, para que ele possa fazer login.