Habilitando uma Swap Criptografada

Quando a memória disponível cai abaixo de um certo ponto, o kernel do Linux irá mandar o conteúdo das páginas de memória para o espaço da swap.

Este conteúdo pode incluir informações confidenciais, como senhas, nomes de usuário, PINS, informações bancárias ou outras informações de identidade. Esses dados geralmente estão em texto simples e, portanto, podem ser lidos sem esforço. A criptografia do espaço de swap do sistema protege seu conteúdo contra acesso não autorizado e ataques caso o acesso ao disco rígido seja comprometido ou removido fisicamente.

Configurando uma Swap Criptografada

A discussão a seguir usará várias designações de unidade e partição. Ao implementar os procedimentos, certifique-se de ajustá-los para se adequarem ao seu próprio sistema.

As etapas a seguir podem ser usadas ao configurar inicialmente um sistema ou depois que o sistema já estiver em execução. Neste último caso, a primeira etapa necessária para criptografar a partição swap é desligando-a temporariamente. Feche todos os aplicativos desnecessários para liberar a memória usada e, assim, interromper o uso do espaço da swap. Embora muitos aplicativos possam ser configurados para não usar swap, isso não se aplica ao kernel. Se o espaço da swap ainda estiver sendo usado, você não conseguirá desligar a swap.

Embora não seja necessário, talvez a abordagem mais simples seja inicializar o sistema no modo de usuário único. Isso resulta em serviços mínimos em execução e um único shell de raiz.

A swap pode então ser desligada usando o seguinte comando:

```
# swapoff -a
```

Para garantir um espaço swap completamente limpo e estéril, você deve sobrescrever a partição swap usada anteriormente com dados aleatórios. Isso ajudará a evitar a recuperação de quaisquer dados gravados para swap antes do processo de criptografia. Existem várias maneiras de fazer isso.

As etapas a seguir destruirão o conteúdo atual no dispositivo/partição especificado!

Talvez o mais fácil seja usar o comando shred, que substitui o arquivo ou dispositivo especificado com dados aleatórios:

```
# shred -v /dev/sdaX
```

Como alternativa, sobrescrever o espaço com dados aleatórios de /dev/random ou /dev/urandom:

```
# dd if=/dev/random of=/dev/sdaX bs=512
```

ou

```
# dd if=/dev/urandom of=/dev/sdaX bs=512
```

Usar /dev/urandom não é tão seguro, entretanto é significativamente mais rápido do que usar /dev/random.

A próxima etapa é criar um arquivo, se ainda não existir, denominado crypttab em /etc. Os detalhes do crypttab podem ser encontrados na página do manual.

Uma entrada crypttab como segue cria um dispositivo de bloco criptografado chamado swap em /dev/mapper usando a partição /dev/sdX como o dispositivo de bloco de base e /dev/random como a senha de criptografia usando criptografia AES e vetores de inicialização variável.

```
swap /dev/sdaX /dev/random swap,cipher=aes-xts-essiv:sha256
```

Você então precisa editar /etc/fstab para apontar para o dispositivo de bloco criptografado, /dev/mapper/swap ao invés de /dev/sdaX.

Por exemplo, uma entrada atual de:

```
/dev/sdaX swap swap defaults 0 0
```

torna-se:

```
/dev/mapper/swap swap swap defaults 0 0
```

Ativando Swap Criptografada

Agora você pode habilitar a swap criptografada reiniciando o sistema ou emitindo os seguintes comandos no prompt do console.

```
# cryptsetup -d /dev/random create swap /dev/sdaX

# mkswap /dev/mapper/swap

# swapon -a
```

Para obter informações detalhadas sobre comandos específicos, consulte as páginas individuais do manual (man).

Fontes

Fonte original: Slackware Encrypted Swap Originalmente escrito por W. Dean Milner

howtos, security, encryption, swap

From:
https://docs.slackware.com/ - **SlackDocs**

Permanent link:
https://docs.slackware.com/pt-br:howtos:security:enabling_encrypted_swap

Last update: **2020/12/27 02:42 (UTC)**