Habilitando la encriptacion de Swap

Cuando la memoria disponible cae por debajo de cierto punto, el kernel de Linux intercambiará el contenido de las páginas de memoria para intercambiar espacio.

Este contenido puede incluir información confidencial como contraseñas, nombres de usuario, PINS, información bancaria o de otra identidad. Estos datos suelen estar en texto plano y, por lo tanto, pueden leerse sin esfuerzo. El cifrado del espacio de intercambio del sistema protege su contenido contra el acceso no autorizado y los ataques en caso de que el acceso al disco duro se vea comprometido o eliminado físicamente.

Configuración de intercambio encriptado

La siguiente discusión utilizará varias designaciones de unidad y partición. Asegúrese de implementar los procedimientos para ajustarlos a su propio sistema.

Los pasos que siguen pueden usarse al configurar inicialmente un sistema, o después de que ya se está ejecutando un sistema. En este último caso, el primer paso necesario para cifrar la partición de intercambio es desactivar temporalmente el intercambio. Cierre todas las aplicaciones innecesarias para liberar la memoria usada y, por lo tanto, interrumpa el uso del espacio de intercambio. Si bien muchas aplicaciones se pueden configurar para que no usen swap, esto no se aplica al kernel. Si aún se está utilizando el espacio de intercambio, no podrá desactivar la swap.

Aunque no es necesario, quizás el enfoque más simple sea iniciar el sistema en modo de usuario único. Esto da como resultado que se ejecuten servicios mínimos y un solo shell raíz.

La swap se puede desactivar usando el siguiente comando:

```
# swapoff -a
```

Para garantizar un espacio de intercambio estéril completamente limpio, debe sobrescribir la partición de intercambio utilizada anteriormente con datos aleatorios. Esto ayudará a evitar la recuperación de cualquier dato escrito para intercambiar antes del proceso de cifrado. Hay varias formas de hacerlo.

Los siguientes pasos destruirán el contenido actual en el dispositivo/partición especificado!

Quizás lo más fácil es usar el comando shred que sobrescribe el archivo o dispositivo especificado con datos aleatorios:

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

Alternativamente, sobrescriba el espacio con datos aleatorios de /dev/random o /dev/urandom:

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

or

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

El uso de /dev/urandom no es tan seguro, sin embargo, es significativamente más rápido que usar /dev/random.

El siguiente paso es crear un archivo, si no existe, llamado crypttab en /etc. Los detalles para crypttab se pueden encontrar en man.

Una entrada de crypttab a continuación crea un dispositivo de bloque cifrado llamado swap at /dev/mapper usando la partición /dev/sdX como dispositivo de bloque base y /dev/random como la contraseña de cifrado utilizando el cifrado AES y los vectores de inicialización de variables.

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

Luego necesita editar /etc/fstab para apuntar al dispositivo de bloque cifrado, /dev/mapper/swap en lugar de /dev/sdaX.

Por ejemplo, una entrada actual de:

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

se convierte en:

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

Activar el intercambio cifrado

Ahora puede habilitar el intercambio encriptado ya sea reiniciando el sistema o emitiendo los siguientes comandos en el indicador de la consola.

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

```
# mkswap /dev/mapper/swap
```

```
# swapon -a
```

Para obtener información detallada sobre comandos específicos, consulte las páginas de manual (man) individuales.

Sources

Original source: Slackware Encrypted Swap Originally written by W. Dean Milner

howtos, security, encryption, swap