Cifrado en el día a día

Bienvenidos – Welcome - Witam

Ponente: Juan Miguel Taboada Godoy
juanmi@centrologic.com - www.centrologic.com

LimaCON '13

Centrologic

Cifrado en el día a día

Algoritmos

DES

AES

Protocolos

SSL

OpenVPN

Disco

Juan Miguel Taboada Godoy

Málaga a 30 de noviembre de 2013

Centrologic

Cifrado en el día a día

DMCRYPT: LUKS

LVM: Logic Volume Manager

Juan Miguel Taboada Godoy
Málaga a 30 de noviembre de 2013

Centrologic

Cifrado en el día a día

cryptsetup luksFormat <dev>
cryptsetup luksOpen <dev> <nombre>

pvcreate /dev/maper/<nombre>
vgcreate <vol_name> /dev/mapper/<nombre>
lvcreate -L 500M -n swap <vol_name>
lvcreate -l 100%FREE -n home <vol_name>

mkswap /dev/<vol_name>/swap
mkfs.ext4 /dev/<vol_name>/home

Centrologic

Juan Miguel Taboada Godoy
Málaga a 30 de noviembre de 2013

Cifrado en el día a día

Vamos a usarlo a MANO

cryptsetup, vgchange, mount, ¿sólo?

Juan Miguel Taboada Godoy
Málaga a 30 de noviembre de 2013

Centrologic

Cifrado en el día a día

¡ABRE!

cryptsetup luksOpen <dev> <nombre>
vgchange -a y <vol_name>
swapon /dev/<vol_name>/swap
mount /dev/<vol_name>/home /home

¡CIERRA!

umount /home
swapoff /dev/<vol_name>/swap
vgchange -a n <vol_name>
cryptsetup luksClose <nombre>

Centrologic

Juan Miguel Taboada Godoy
Málaga a 30 de noviembre de 2013

Cifrado en el día a día

Vamos a usarlo a DIARIO

$ cat /etc/crypttab

<vol_name> UUID=<uuid> none luks

$ cat /etc/fstab

/dev/<vol_name>/home /home ext4 defaults 0 2
/dev/<vol_name>/swap none swap sw 0 0

Juan Miguel Taboada Godoy
Málaga a 30 de noviembre de 2013

Centrologic

Cifrado en el día a día

Estructura DMCRYPT

[phdr] [KM1] [KM2] … [KM8] […….....BULK.....]

phrd: partition header

Info de: Slots KM, agoritmos, iteraciones, salt, ...

KMx

Material encriptado con la llave maestra

Juan Miguel Taboada Godoy

Málaga a 30 de noviembre de 2013

Centrologic

Cifrado en el día a día

AF-Splitter

LUKS usa este sistema “anti-forensic”

Función que hace borrosos los datos añadiendo material extra en cada SLOT

Compatibilidad

Centrada sólo en BULK

Juan Miguel Taboada Godoy

Málaga a 30 de noviembre de 2013

Centrologic

Cifrado en el día a día

AF-Splitter

LUKS usa este sistema “anti-forensic”

Función que hace borrosos los datos añadiendo material extra en cada SLOT

PBKDF2

Protege la llave de fuentes débiles de entropía

Compatibilidad

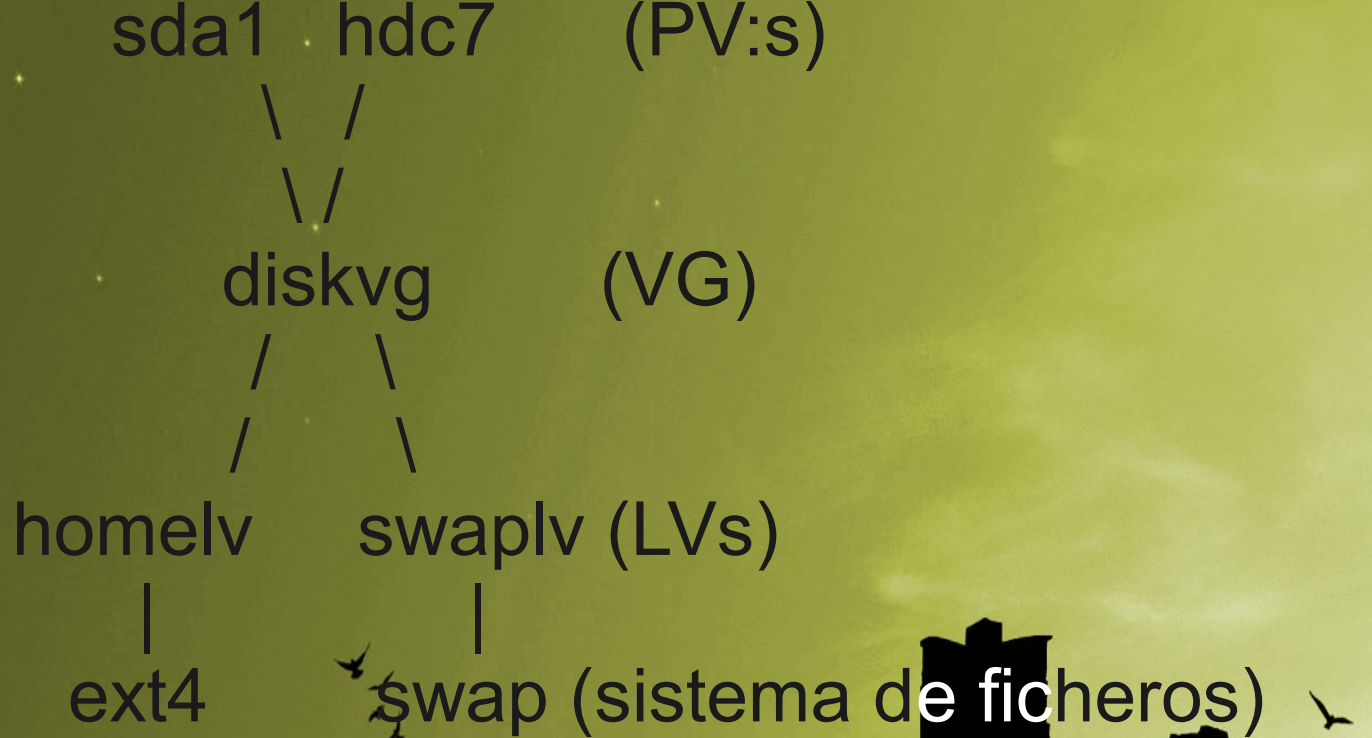
Centrada sólo en DATOS

Centrologic

Juan Miguel Taboada Godoy
Málaga a 30 de noviembre de 2013

Cifrado en el día a día

Y de LVM, ¿qué nos queda?



Juan Miguel Taboada Godoy
Málaga a 30 de noviembre de 2013

Centrologic

Cifrado en el día a día

¿Por qué DMCRYPT?

Seguridad - Seguridad - Seguridad

¿Por qué LVM?

En sistemas pequeños: crecimiento del disco

En sistemas grandes: permite aglutinar capacidad

Flexibilidad de arquitectura de datos

Cambio de disco “online” (espacio libre)

No necesidad de relocalizar ficheros en cambios

Centrologic

Juan Miguel Taboada Godoy
Málaga a 30 de noviembre de 2013

Cifrado en el día a día

¿PREGUNTAS?

Centrologic

Juan Miguel Taboada Godoy
Málaga a 30 de noviembre de 2013

Gracias – Thank you - Dziękujemy

Ponente: Juan Miguel Taboada Godoy
juanmi@centrologic.com - www.centrologic.com

Centrologic