

# **M11 – Seguretat Informàtica – UF1**

## **Pràctica 2 – SEGURETAT LÒGICA: FUNCIO HASH CRIPTOGRÀFICA**

**Nil Massó**



ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

## Table of Contents

Pràctica 1 – Eines preventives.....	1
Exercici 2: Xifrat de fitxers amb VeraCrypt (3,25 punts).....	3
Exercici 3: Xifrat amb LUKS (3,75 punts).....	7
(Opcional) Exercici 4. Investigueu sobre les següents eines: (2 punts).....	9

- A l'hora d'avaluar i qualificar el treball es tindran en compte els aspectes estètics, de correctesa lingüística (sintàctica i ortogràfica) a més del que s'hagi comentat al cicle formatiu sobre la redacció de documentació tècnica i manuals.

- El mòdul professional pertany a uns estudis orientats al món laboral, cosa que fa que un cop complerts els requisits mínims la nota resultant serà condicionada per la quantitat i qualitat del treball individual realitzat per cada alumne.

## Pràctica 1 – Eines preventives

Fes els exercicis següents.

### Exercici 1: Hardening a GRUB (3 punts)

Una de les mesures més habituals que s'aplica en hardening (reducció de vulnerabilitat) consisteix en protegir el GRUB per evitar accessos no desitjats, o només permetre a segons quins usuaris entrar a segons quines entrades del GRUB, etc... Agafeu una màquina virtual Ubuntu 18.04.5 (us aconsello Desktop per poder treballar bé amb el mouse) i vigileu, perquè **podeu espatllar la màquina virtual si no ho feu bé**, pel que **feu-ne una còpia o feu-ho sobre una màquina nova que només serveixi per això**.

Per accedir al GRUB ho fareu prement SHIFT quan la màquina s'inicia si no us surt per defecte.

Recordeu que quan us surt el GRUB, si apreteu la lletra 'e' entreu al menú d'edició del GRUB.

Primer de tot cal arrancar el sistema i dins la Ubuntu cal que feu, com a root o amb sudo, la següent comanda:

#### ***grub-install --version***

us ha de sortir la versió 2.02-2ubuntu8.20, sinó, no us puc garantir que us funcioni igual.

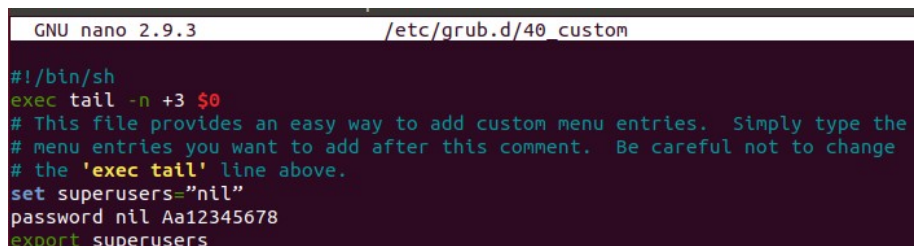
Poseu-me la captura de la versió i seguim.

Primer de tot caldrà doncs definir els usuaris i després activar la protecció. Per als usuaris, cal que com a root, aneu a **/etc/grub.d/** i allà hi tindreu els fitxers a tocar.

Inicialment cal tocar el fitxer **40\_custom**. Aquí es on es defineixen els usuaris, passwords, etc. (1,5 punts)

En aquest fitxer, al final, cal afegir:

```
set superusers="jpou"  
password jpou elteupassword  
export superusers
```



```
GNU nano 2.9.3 /etc/grub.d/40_custom  
#!/bin/sh  
exec tail -n +3 $0  
# This file provides an easy way to add custom menu entries. Simply type the  
# menu entries you want to add after this comment. Be careful not to change  
# the 'exec tail' line above.  
set superusers="nil"  
password nil Aa12345678  
export superusers
```

on heu de substituir **jpou** pel vostre nom d'usuari i **elteupassword** pel password que hi voleu assignar.

Un cop fet això cal dir-li a la configuració que faci servir el control d'accés. Per això heu d'editar el fitxer **10\_linux**. (1,5 punts)

Cal modificar 3 línies, la 132, la 134 i la 354. Us adjunto una captura amb la línia sense modificar i modificada per tal que hi feu els canvis convenients.

```
130c130
< echo "menuentry '$(echo "$title" | grub_quote)' ${CLASS} --users '' \${menuentry_id_option 'gnulinux-$version-$type-$boot_device_id' 't' | sed 's/^/$submenu_indentation/'"
---
> echo "menuentry '$(echo "$title" | grub_quote)' ${CLASS} \${menuentry_id_option 'gnulinux-$version-$type-$boot_device_id' 't' | sed 's/^/$submenu_indentation/'"
132c132
< echo "menuentry '$(echo "$os" | grub_quote)' ${CLASS} --unrestricted \${menuentry_id_option 'gnulinux-simple-$boot_device_id' 't' | sed 's/^/$submenu_indentation/'"
---
> echo "menuentry '$(echo "$os" | grub_quote)' ${CLASS} \${menuentry_id_option 'gnulinux-simple-$boot_device_id' 't' | sed 's/^/$submenu_indentation/'"
B46c346
< echo "submenu '$(gettext_printf "Advanced options for %s" "${OS}" | grub_quote)' --users '' \${menuentry_id_option 'gnulinux-advanced-$boot_device_id' 't'
---
> echo "submenu '$(gettext_printf "Advanced options for %s" "${OS}" | grub_quote)' \${menuentry_id_option 'gnulinux-advanced-$boot_device_id' 't'

```

De cada pack de 2 (132,134 i 354) es mostra primer la línia ja modificada i després la línia sense modificar.

Fixeu-vos que a la 132 cal afegir -> **--users ''**

A la 134 cal afegir -> **--unrestricted**

I a la 354 -> **--users ''**

Un cop fets els canvis,

```
GNU nano 2.9.3 /etc/grub.d/10_linux
    echo "menuentry '$(echo "$title" | grub_quote)' ${CLASS} --users '' \${menuentry_id_option 'gnulinux-$version-$type-$boot_device_id' 't' | sed 's/^/$submenu_indentation/'"
    else
    echo "menuentry '$(echo "$os" | grub_quote)' ${CLASS} --unrestricted \${menuentry_id_option 'gnulinux-simple-$boot_device_id' 't' | sed 's/^/$submenu_indentation/'"
    fi
    echo "submenu '$(gettext_printf "Advanced options for %s" "${OS}" | grub_quote)' --users '' \${menuentry_id_option 'gnulinux-advanced-$boot_device_id' 't' | sed 's/^/$submenu_indentation/'"
    fi
}

# TRANSLATORS: %s is replaced with an OS name
echo "submenu '$(gettext_printf "Advanced options for %s" "${OS}" | grub_quote)' --users '' \${menuentry_id_option 'gnulinux-advanced-$boot_device_id' 't' | sed 's/^/$submenu_indentation/'"
is_top_level=false
}

```

com a root, cal que llanceu -> **update-grub**

Per tal que s'apliquin els canvis. Reinicieu la màquina i veureu que tant per editar (recordar, prémer 'e' quan el grub està en pantalla) com per accedir a la consola de recuperació d'Ubuntu us demanarà usuari i password (demostrar-ho amb les captures).

```
Enter username:
nil
Enter password:
_

```

Recordeu però que el password està en text pla, i que el podem fer servir xifrat. Per això cal tornar a /**etc/grub.d/** i editar el fitxer **40-custom**. Primer de tot però, heu d'obtenir el password xifrat, i per això cal fer servir l'eina **grub-mkpasswd-pbkdf2**.

Un cop l'hàgiu executat i us hagi retornat el password xifrat, editeu el fitxer **40\_custom** i canvieu la línia d'abans de :

**password jpou elteupassword**  
per

**password\_pbkdf2 jpou elteupasswordXIFRAT**

no us oblideu de fer el **update-grub** després i tornar a demostrar que tot funciona OK.

```
Enter username:
nil
Enter password:
_
```

NOTA: és possible que en algunes versions no us surti el GRUB activat per defecte. Per això cal anar a /etc/default/grub i comentar amb # les dos línies que posa \*\*\*HIDDEN\*\*\*\* i després llançar un update-grub. Amb això ja us hauria de sortir el GRUB per pantalla al reiniciar.

## Exercici 2: Xifrat de fitxers amb VeraCrypt (3,25 punts)

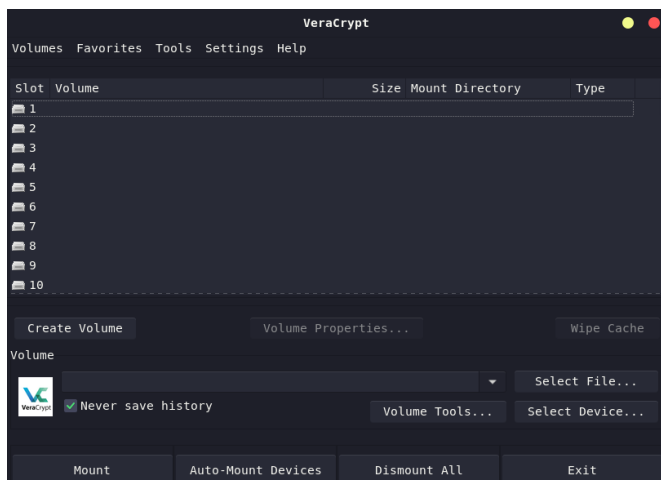
**Veracrypt** és un software lliure que us permet encriptar els vostres arxius. Encripta la informació i impedeix l'accés a tothom qui no tingui la contrasenya assignada. Funciona com una caixa forta electrònica on pots guardar els teus arxius de forma segura. Veracrypt protegirà els arxius encriptant-los amb contrasenya. Crea una zona protegida, que s'anomena **volum**, ja sigui al vostre propi ordinador o a un dispositiu d'emmagatzematge extern. Tot el volum s'allotja dins un únic arxiu que s'anomena **contenedor**, que es pot obrir (muntar dins el sistema) o tancar (desmuntar dins el sistema) amb el propi software **Veracrypt**. Recordeu que si perdeu la contrasenya perdeu tota la informació que hi hagi a aquell contenidor. No es pot recuperar la contrasenya perduda.

En aquest exercici cal que instal·leu **Veracrypt** (ho podeu fer al vostre Windows habitual) i creeu un volum on hi poseu un arxiu (el que vulgueu). Aleshores caldrà demostrar que per accedir-hi s'ha de muntar (i posteriorment desmuntar) el volum i que us demana contrasenya. Recordeu a adjuntar les captures corresponents que demostrin cada pas que es demana.

- Primer de tot cal que us descarregueu i instal·leu **Veracrypt**. Ho podeu fer des d'aquí <https://www.veracrypt.fr/en/Downloads.html>. L'enllaç directe a descarregar el fitxer -> <https://launchpad.net/veracrypt/trunk/1.25.7/+download/VeraCrypt%20Setup%201.25.7.exe>

No cal captura

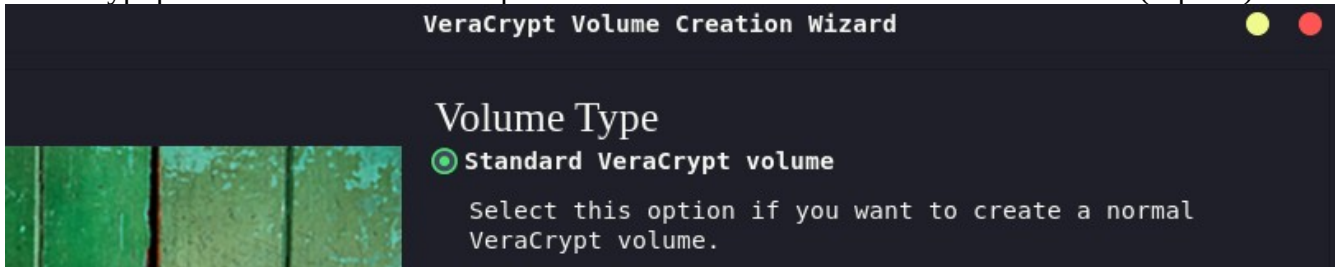
- Un cop tingueu l'aplicació instal·lada arranqueu-la i poseu-me una captura de la pantalla d'inici.



- Veracrypt us permet tant crear arxius xifrats com particions. En aquesta pràctica només farem arxius per tant cal que escollim la opció de crear un contenidor de dades xifrat (captura).



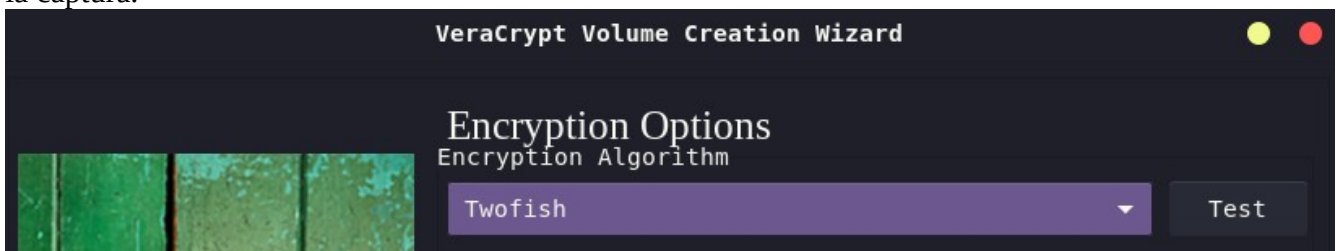
- Veracrypt permet treballar amb dos tipus de volum. Seleccionem un **volum estàndard** (captura)



- **IMPORTANT!** quan seleccioneu l'ubicació del volum, compte, **trieu un lloc NOU**, no feu servir una carpeta existent ja que us sobrescriurà el contingut. (poseu-me una captura del lloc que escolliu abans de fer el 'siguiente').



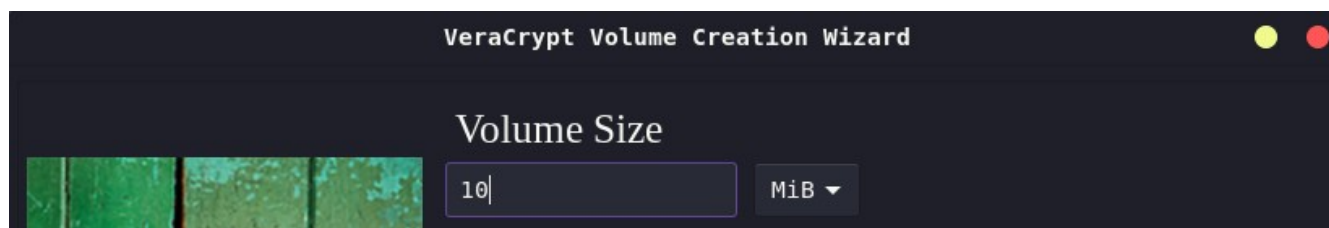
- Trieu l'algorisme de xifrat i de hash que vulgueu. Teniu el botó de comparativa si us cal. **NO es pot escollir la opció per defecte (AES i SHA-512)**. Com a **mínim n'heu de canviar un dels dos**. Feu-ne la captura.



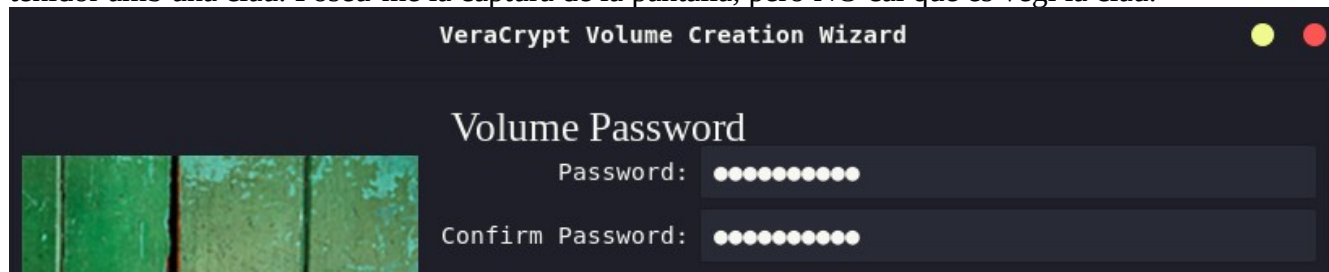
- Trieu la mida del volum. No hi farem res més que això per tant, no us passeu. **Màxim 100MB**. Feu una captura de la mida escollida.

---

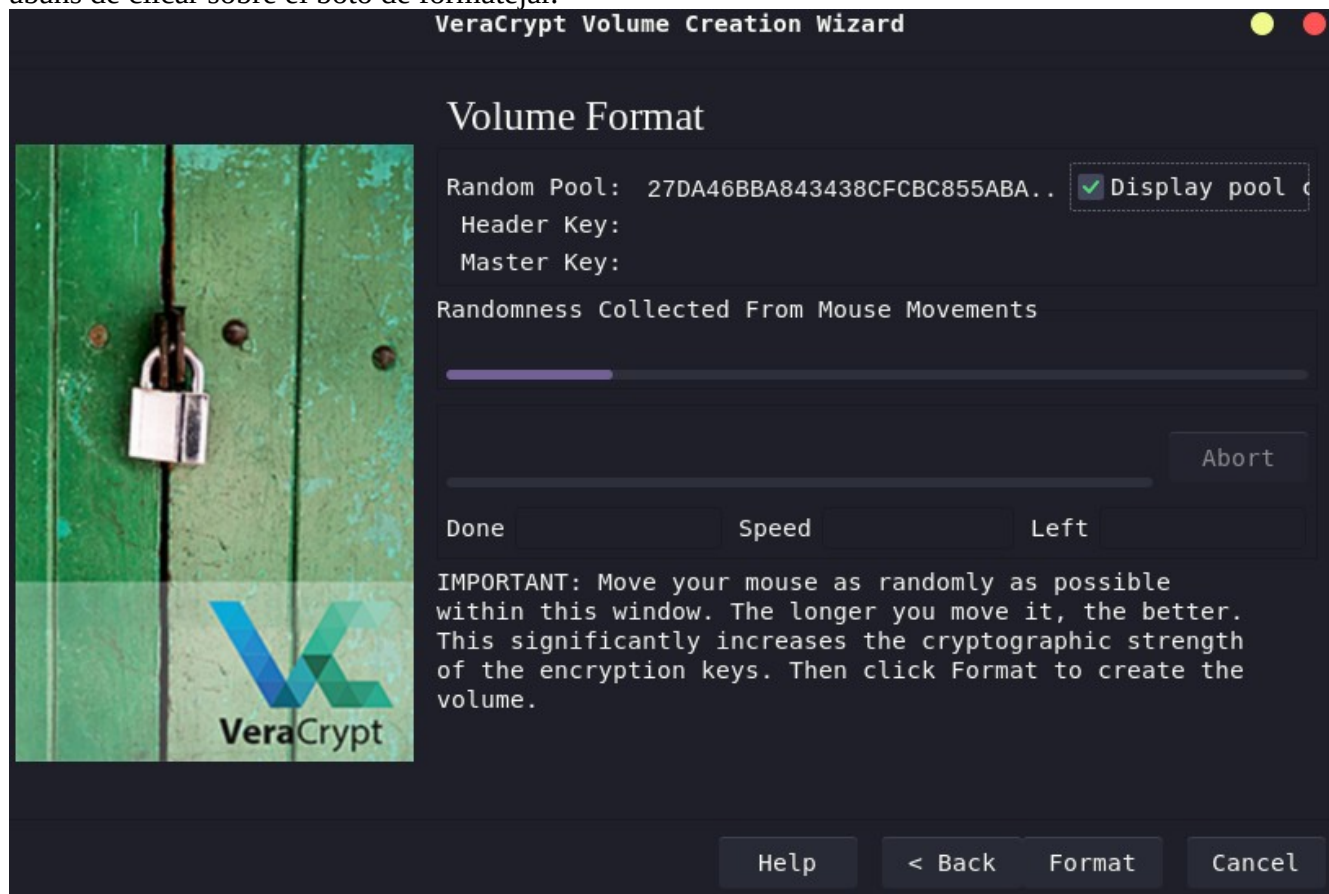




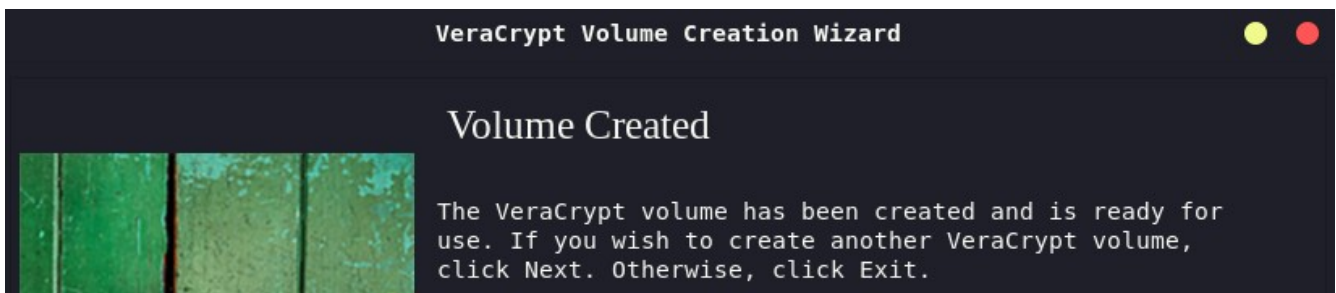
- com que estem treballant amb algorismes de clau simètrica, us demanarà que protegiu (xifreu) el contenidor amb una clau. Poseu-me la captura de la pantalla, però NO cal que es vegi la clau.



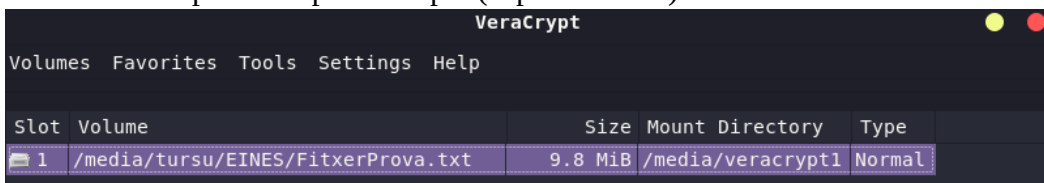
- procediu a donar-li format al volum. **Podeu deixar les opcions per defecte.** Feu-me la captura just abans de clicar sobre el botó de formatjar.



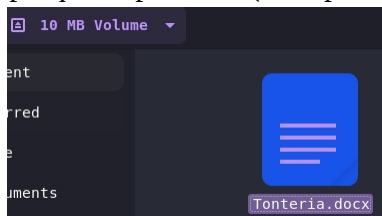
- tot hauria d'haver anat correctament pel que poseu-me la captura conforme el volum s'ha creat correctament. (0,5 punts)



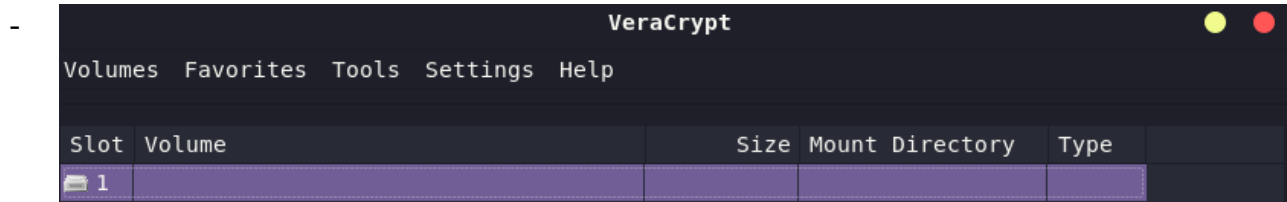
- Això només us ha creat el volum, encara no hi ha informació. Per poder-hi treballar, cal muntar el volum. Des de la pantalla principal, trieu una lletra d'unitat, poseu la ruta del volum que heu seleccionat al principi de la pràctica i munteu la unitat. Us demanarà la contrasenya. Una vegada muntat apareixerà a la pantalla principal (captura) i si aneu a 'Equip' del Windows també us sortirà com una nova unitat, com si fos un pendrive per exemple (captura també).



- poseu-hi l'arxiu que vulgueu i poseu-me una captura. Recordeu que sigui qualsevol tonteria d'arxiu, perquè el perdreu. (0,75 punts))



- Torneu a la pantalla principal i desmunteu tots els volums (poseu-me una captura quan estigui desmuntat que es vegi que la lletra d'unitat ja està lliure). Un cop fet, podeu esborrar el contenidor dins el vostre sistema.



Responen les següents preguntes:

a) Busca a internet informació sobre l'algorisme de hash i xifrat que has triat. És segur o és vulnerable? **Cita'n les fonts.** (1 punt)

<https://www.encryptionconsulting.com/education-center/what-is-twofish/>

twofish es el predecessor the Blowfish de Blowfish, utilitza encriptació simetria.

El motiu per el qual es tan segur i s'utilitza a serveis molt populars com, PGP, Truecrypt i el popular gestor de contrasenyes keepass es degut a que tot i la seva lentitut comparat amb altres algoritmes, el fet de utilitzar una clau de 128-bits fa que amb atacs de força bruta, i amb la tecnologia actual, el temps requerit per a desxifrar la clau sigui inhumanament elevat.

L'únic atac al que es susceptible, que es sapiga, es atacs laterals a la clau pre computada ja que depen de substitució per a generar-se



b) A la selecció de contrasenya, que hagués implicat fer servir la opció keyfile per autenticar? (1 punt)  
Resumidament es com si la contrasenya fos un arxiu cualsevol però configurat amb veracrypt per a ser un keyfile. Enlloc de posar una contrasenya per encrytar i desencryptar s'utilitza aquest arxiu.  
Extra: link que us pot ajudar ( i molt) -> <https://securityinabox.org/es/guide/veracrypt/windows/>

---

### Exercici 3: Xifrat amb LUKS (3,75 punts)

**LUKS** és un estàndard de xifrat dins de Linux. Ens permet fer-ne ús sobre discos, particions, volums lògics LV o fitxers *loop*. Dins els seus avantatges hi ha la seva senzillesa d'ús, que està inclòs dins el propi kernel i la seva capacitat per assignar, canviar i revocar diverses claus per un mateix dispositiu. Aquesta pràctica està feta sota Ubuntu 18.04.5 però podeu aprofitar-ne alguna de ja existent ja que no canviarem res i ho farem ja en un sistema amb tot instal·lat. Recordeu anar fent les captures corresponents.

- Primer de tot, llanceu el següent per instal·lar l'aplicatiu:

***sudo apt-get install cryptsetup***

Alguns ja ho tindreu activat segons la Ubuntu escollida.

- Posteriorment cal crear el contenidor de LUKS on hi posarem la informació:

***dd if=/dev/urandom of=/tmp/contenidor bs=1M count=100***

***ls -lh /tmp/contenidor***

| poseu-me la captura del resultat de les dos comandes

```
root@us-nmc:~# dd if=/dev/urandom of=/tmp/contenidor bs=1M count=100
100+0 records in
100+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 0.363596 s, 288 MB/s
root@us-nmc:~# ls -lh /tmp/contenidor
-rw-r--r-- 1 root root 100M Oct 29 19:17 /tmp/contenidor
```

Ara ho associem com a unitat LUKS amb protecció per contrasenya.

***cryptsetup --verify-passphrase luksFormat /tmp/contenidor***

| evidentment poseu captura quan estigui fet

```
root@us-nmc:~# cryptsetup --verify-passphrase luksFormat /tmp/contenidor

WARNING!
=====
This will overwrite data on /tmp/contenidor irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase for /tmp/contenidor:
Verify passphrase:
root@us-nmc:~# █
```

Cal que tingueu en compte una consideració. **A LUKS la contrasenya ens permet accedir al dispositiu, ens dóna l'autenticació per accedir-hi. NO es xifra amb aquesta contrasenya.** Un dels grans avantatges de LUKS es demostra aquí permetent que hi hagi diverses contrasenyes per al mateix dispositiu LUKS. Per xifrar es fa a través de la clau de xifrat. Es genera automàticament quan donem el format LUKS al dispositiu. Podem obtenir la informació de la capçalera LUKS (on hi consta aquesta informació) amb la següent comanda.

| ***cryptsetup luksDump /tmp/contenidor*** i mostreu la captura. (1,25 punts))

```

root@us-nmc:~# cryptsetup luksDump /tmp/contenidor
LUKS header information
Version:          2
Epoch:           3
Metadata area:    16384 [bytes]
Keyslots area:    16744448 [bytes]
UUID:             a4bcf6fb-7567-4d12-81b1-3923766b382a
Label:            (no label)
Subsystem:        (no subsystem)
Flags:            (no flags)

Data segments:
 0: crypt
    offset: 16777216 [bytes]
    length: (whole device)
    cipher: aes-xts-plain64
    sector: 512 [bytes]

Keyslots:
 0: luks2
    Key:           512 bits
    Priority:       normal
    Cipher:         aes-xts-plain64
    Cipher key:    512 bits
    PBKDF:          argon2i
    Time cost:      4
    Memory:         1048576
    Threads:        2
    Salt:           10 25 06 53 e3 e0 5c 6d 5f 7b 22 5f c3 cf 81 4b
                   a6 67 8c 12 67 f6 8e 76 d4 6c 31 ed 75 a3 f4 e4
    AF stripes:     4000
    AF hash:         sha256
    Area offset:    32768 [bytes]
    Area length:    258048 [bytes]
    Digest ID:      0

Tokens:
Digests:
 0: pbkdf2
    Hash:           sha256
    Iterations:     281875
    Salt:           73 d0 17 10 27 d4 af d4 30 d8 1b b3 01 44 64 82
                   04 6f c3 5a 79 f2 52 3d 9d 57 9e e2 b9 f4 19 7d
    Digest:         1e d8 71 77 6a 54 9f b2 d6 05 99 c0 00 93 0c 13
                   d4 20 4d f1 08 ad 1a 46 ad 5f 6c 8a 22 6c 3b e2

```

Fins aquí en el fons l'únic que hem fet és crear una unitat de emmagatzematge que es mantindrà xifrada. Cal doncs que ara "l'obrim" per poder-hi treballar (com si la connectéssim al sistema)

***cryptsetup luksOpen /tmp/contenidor LUKSkywalker***

el segon paràmetre és el nom que tindrà el dispositiu dins el sistema (el típic /dev/sda per exemple) per comprovar que ha anat tot bé feu el següent

***ls -l /dev/mapper/***

| I mostreu-me una captura (hauria de sortir una entrada de **LUKSkywalker**)

```
| lrwxrwxrwx 1 root root          7 Oct 29 19:24 LUKSkywalker -> ../dm-0
```

| Aquesta unitat per tal de poder-hi guardar informació, ha de tenir un sistema de fitxers, per tant cal donar-li format:

***mkfs.ext4 /dev/mapper/LUKSkywalker***

poseu-me la captura del resultat. Ara ja podem treballar amb ell com si fos un dispositiu més (un pendrive per exemple) per tant cal que el munteu dins el sistema.

```
| root@us-nmc:~# mkfs.ext4 /dev/mapper/LUKSkywalker  
mke2fs 1.45.5 (07-Jan-2020)  
Creating filesystem with 21504 4k blocks and 21504 inodes  
  
Allocating group tables: done  
Writing inode tables: done  
Creating journal (1024 blocks): done  
Writing superblocks and filesystem accounting information: done
```

***mkdir /tmp/activitat2***

***mount /dev/mapper/LUKSkywalker /tmp/activitat2***

| ***df -h*** (mostreu-me la captura) (1 punt)

```

root@us-nmc:~# df -h
Filesystem                Size      Used Avail Use% Mounted on
udev                     1.9G         0   1.9G   0% /dev
tmpfs                    394M       1.1M  393M   1% /run
/dev/vda2                25G       7.4G   16G  32% /
tmpfs                    2.0G         0   2.0G   0% /dev/shm
tmpfs                    5.0M         0   5.0M   0% /run/lock
tmpfs                    2.0G         0   2.0G   0% /sys/fs/cgroup
/dev/loop2                68M        68M     0 100% /snap/lxd/21835
/dev/loop0                62M        62M     0 100% /snap/core20/1328
/dev/loop3                64M        64M     0 100% /snap/core20/1623
/dev/loop4                68M        68M     0 100% /snap/lxd/22753
/dev/loop5                48M        48M     0 100% /snap/snapd/17029
tmpfs                    394M         0  394M   0% /run/user/1000
/dev/loop6                48M        48M     0 100% /snap/snapd/17336
/dev/mapper/LUKSkywalker   78M        24K    72M   1% /tmp/activitat2

```

podeu copiar qualsevol arxiu sense problemes. Poseu algun fitxer a dins de **/tmp/activitat2** i mostreu captura.

```

root@us-nmc:~# touch /tmp/activitat2/prova1
root@us-nmc:~# ls /tmp/activitat2/
lost+found  prova1

```

Ja podeu fer el **umount** :

***umount /tmp/activitat2***

I feu aquesta última comanda:

***cryptsetup luksClose /dev/mapper/LUKSkywalker***

Pregunta: Raona perquè cal fer aquesta comanda, quines implicacions pot tenir no fer-la? (1,5 punts)

No ferla implica que el «dispositiu» es segueix poguent muntar sense requerir de tornar a introduir la contrasenya

Info: <https://blog.inittab.org/administracion-sistemas/cifrando-discos-particiones-o-ficheros-con-luks/>

## (Opcional) Exercici 4. Investigueu sobre les següents eines: (2 punts)

Comenteu tot el que creieu destacable. Qui ho fa servir, per a què,...

- **Què és Metasploit?** Que permet fer aquesta eina? Quin paper hi té **rapid7**?
  - Es un projecte de codi obert centrat en la seguretat informàtica, sobretot enfocades al pentesting i detecció de intrusos a un sistema. Rapid7 es el desenvolupador del projecte.
- **I Metasploit framework?**
  - Es un dels seus subprojectes mes coneguts, permet desenvolupar i executar exploits contra maquines remotes.
- **I Metasploitable?** Quina utilitat té una màquina virtual d'aquest tipus?
  - Es una maquina virtual preconfigurada per a poderli realitzar atacs de pentesting i així aprendre a desenvolupar i utilitzar aquestes eines.