

Introducció a la seguretat (Pt1)

ACTIVITATS

1. Quina diferència hi ha entre confidencialitat i integritat de les dades? Posa un exemple d'amenaça de la confidencialitat i de la integritat d'un sistema.

La **confidencialitat** es aquell element que garanteix que la informació només es accessible per aquell que te permisos mentre que la **integritat** es la que busca que la informació no sigui modificada ni tractada sense autorització.

Un exemple de amenaça de confidencialitat es el *phishing* el qual t'enganya perquè introdueixis les teves credencials (Usuari i Contrasenya).

Un exemple de amenaça a la integritat seria un *malware* (programa) que modifiqui arxius del sistema importants.

2. Què és un SAI (UPS en anglès)? A quin tipus de seguretat classificaries aquest mecanisme? Cerca un SAI i explica les seves característiques fent un anàlisi de amb el VA que disposa quin tipus d'equips podríem connectar i quant de temps.

Un SAI (sistema d'alimentació ininterrompuda) és un dispositiu que en cas que hi hagi una interrupció del subministrament elèctric, el SAI agafa tota la responsabilitat de mantenir-ne, temporalment, els dispositius elèctric amb corrent.

Aquest tipus de seguretat s'anomena **seguretat física**.

[Woxter UPS 1200 VA SAI](#)

Característiques:

- Potència: 1200 VA / 720 W.
- Tecnologia: Line-interactive amb estabilització automàtica.
- Entrada: 230 V amb marge de 165 a 290 V.
- Sortida: 230 V, ona senoidal pura.
- Bateria: 12 V, 9 Ah, recàrrega en 6-8 hores.
- Interfície: Connexions Schuko i USB.
- Proteccions: Sobrecàrrega, curtcircuit i sobreescalfament.

3. Quin creus què és el recurs que més s'ha de protegir: el hardware, el software o les dades? Raona la resposta.

El recurs que més s'ha de protegir son les dades degut a que son irremplaçables mentre que el hardware i el software es poden canviar el nucli de la informació son les dades.

4. Quin creus què és el punt més feble en qualsevol sistema de seguretat?

El punt més feble en qualsevol sistema de seguretat son les persones (usuaris) que son els que controlen i actuen sobre aquest sovintment, de manera que poden descarregar-se arxius amb algún virus maliciós o phishing.

5. Què és un atac de denegació de servei? Creus que pot ser una amenaça important per una petita empresa? En quin grup d'amenaques el classificaries? I un atac de denegació distribuït, quin element incorpora?

En un atac DDoS, un ciberatacant inunda un lloc web o servidor amb trànsit dolent per fer-lo lent o inaccessible. Utilitza dispositius infectats per enviar moltes sol·licituds alhora, bloquejant l'accés als usuaris normals.

Crec que per una empresa petita és una amenaça molt important pel fet que com és de baixos recursos, pot ser que no tingui backups o servidors de caiguda i així paraitzar tota la producció.

Son amenaces lògiques.

El DDoS distribuït incorpora botnets per enviar transit.

6. Fes una llista de 4 productes de sistemes biomètrics indicant les seves fortaleces i febleses a l'hora d'autenticar entitats, així com les seves característiques fonamentals. També indica a quin tipus de sistema biomètric pertanyen.

Escaneig de les empremtes dactilars: Les empremtes són úniques, proporcionant alta seguretat i una autenticació ràpida. Són econòmiques, però poden ser falsificades i no funcionen bé si les mans estan brutes. Hi ha preocupacions sobre la seguretat de les dades. Els sensors varien entre òptics, capacitius i tèrmiques, i s'utilitzen en mòbils i controls d'accés.

Escàner del iris: Aquest sistema biomètric reconeix persones a través de les característiques úniques del seu iris, que teòricament no es repeteixen. És molt efectiu i segur, però requereix sensors especials que limiten la seva adopció. Actualment, s'utilitza principalment en controls d'accés, i l'avenç en tecnologia més assequible està canviant aquesta tendència.

Reconeixement facial: Captura els trets del rostre per crear plantilles biomètriques i identificar persones. És ràpid i pot funcionar amb imatges en temps real, però planteja preocupacions sobre la privadesa i pot fallar amb mala il·luminació. S'aplica en seguretat i control d'accés.

Reconixement de veu: Aquest sistema biomètric genera una plantilla de la veu, ja que cada veu és diferent i presenta trets únics, especialment el to. No s'utilitza per al control d'accés, sinó en sistemes que funcionen mitjançant ordres de veu.

7. Explica què són els errors de falsos positius i els errors de falsos negatius. Què succeeix en un sistema de seguretat (control d'accés) amb una taxa de falsos negatius molt elevada?

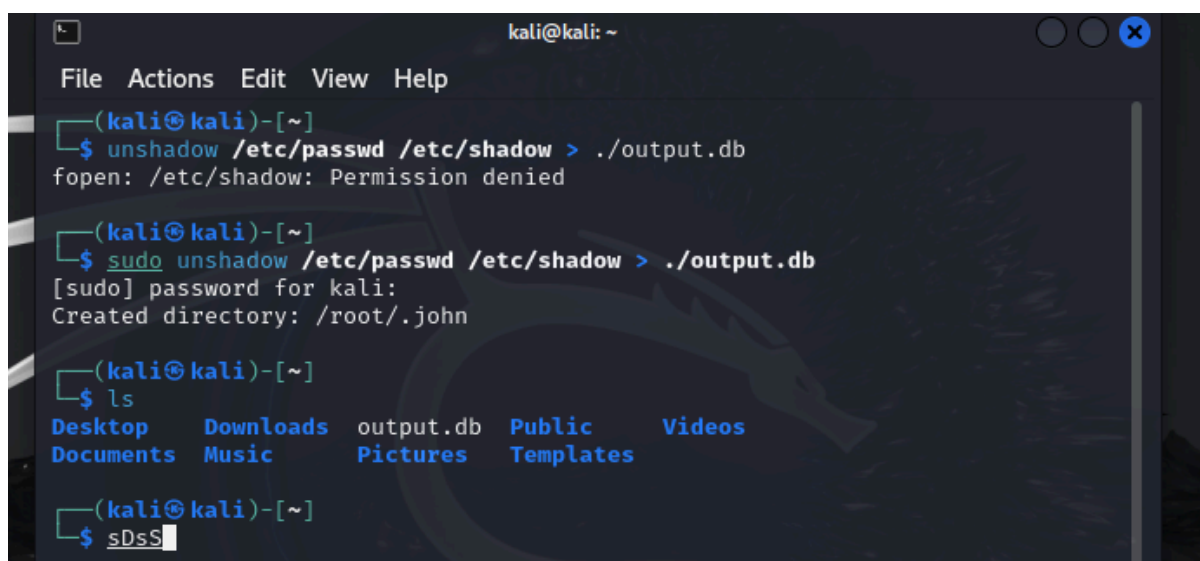
El fals positiu produeix una alarma quan en veritat no s'ha produït ningun atac mentre que el fals negatiu és totalment el contrari, si estan atacant la xarxa o el sistema operatiu, aquest error no activa ninguna alarma.

Si un sistema de seguretat te una taxa elevada de falsos negatius esta en perill la confidencialitat, integritat i disponibilitat porque estan en el teu dispositiu i no ets capaç de detectar-lo.

8. Busca informació sobre l'eina John the Ripper i comprova el seu funcionament. Expliqueu quin mecanisme fa servir per a esbrinar contrasenyes. Haureu d'investigar sobre l'eina i com fer-la servir.

Has pogut trobar alguna contrasenya al teu sistema? Per què? Posa un exemple de contrasenya que pot trobar "John the Ripper" amb molta facilitat.

John The Ripper el que fa es reconèixer els hash que hi ha dins de les passwords del sistema y va generant diferents HASHs, quan un d'aquests troba un que es igual a ell s'atura i esbrina quina es la contraseña.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ unshadow /etc/passwd /etc/shadow > ./output.db  
fopen: /etc/shadow: Permission denied  
(kali@kali)-[~]  
$ sudo unshadow /etc/passwd /etc/shadow > ./output.db  
[sudo] password for kali:  
Created directory: /root/.john  
(kali@kali)-[~]  
$ ls  
Desktop Downloads output.db Public Videos  
Documents Music Pictures Templates  
(kali@kali)-[~]  
$ sDsS
```



```
(kali@kali)-[~]  
$ sudo john output.db  
Using default input encoding: UTF-8  
No password hashes loaded (see FAQ)  
(kali@kali)-[~]  
$
```

MODE DICCIONARI

Primer posem el hash d'una password al .txt, un exemple 'password5' i utilitzem el següent fitxer:

- /usr/share/wordlists/rockyou.txt

```
(kali㉿kali)-[~]  
$ cat crack.txt  
edba955d0ea15fdef4f61726ef97e5af507430c0  
  
(kali㉿kali)-[~]  
$
```

```
(kali㉿kali)-[~]  
$ vim crack.txt  
  
(kali㉿kali)-[~]  
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 crack.  
txt  
  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 SSE2 4x])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password5 (?)  
1g 0:00:00:00 DONE (2024-10-16 09:45) 33.33g/s 110000p/s 110000c/s 110000C/s  
antonio1..larisa  
Use the "--show --format=Raw-SHA1" options to display all of the cracked pass  
words reliably  
Session completed.  
  
(kali㉿kali)-[~]  
$
```

Ha trobat la password que tenia el hash.

MODE INCREMENTAL

Primer de tot, fem el hash d'una password que nosaltres volguem, d'aquesta manera:

```
(kali㉿kali)-[~]  
$ echo -n '1234' | openssl passwd -6 -stdin  
$6$DKIcdpZlCoGAjpp.$IltVHFJAjVn2WPQ7hH96fN7WPN6Li48qi6PMJ.e4gRic3BOVUxU2Q6Zdr  
Ac35FXl2WLDzXuhDYhU.Z2IiwkIn1
```

Una vegada tenim aixó, la fiquem al nostre fitxer:

```
(kali㉿kali)-[~]  
$ echo '$6$DKIcdpZlCoGAjpp.$IltVHFJAjVn2WPQ7hH96fN7WPN6Li48qi6PMJ.e4gRic3BO  
VUxU2Q6ZdrAc35FXl2WLDzXuhDYhU.Z2IiwkIn1' > crack.txt  
  
(kali㉿kali)-[~]  
$ cat crack.txt  
$6$DKIcdpZlCoGAjpp.$IltVHFJAjVn2WPQ7hH96fN7WPN6Li48qi6PMJ.e4gRic3BOVUxU2Q6Zdr  
Ac35FXl2WLDzXuhDYhU.Z2IiwkIn1
```

I per ultim, fem aquesta comanda per a que **John The Ripper** busqui la contrasenya que hem fet el hash amb totes les possibilitats que aquest mètode cregui:

```
(kali㉿kali)-[~]
$ john --incremental crack.txt
Warning: detected hash type "sha512crypt", but the string is also recognized
as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type ins
tead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1234 (?)
1g 0:00:00:00 DONE (2024-10-16 10:05) 6.250g/s 800.0p/s 800.0c/s 800.0C/s 123
456..102520
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~]
$
```

Troba aquesta contrasenya perquè és molt senzilla.

JTR EN LINUX

Per utilitzar Jhon The Ripper a linux primer hem de trobar els hash de les contrasenyes que tenim:

```
(kali㉿kali)-[~]
$ sudo unshadow /etc/passwd /etc/shadow > ./output.db

(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ cat output.db | grep kali
kali:$y$j9T$zY1oKFxJlTgP2WcJhzbNl1$xhkUmB8R9fzETc/1kgL/nOPcWFTvhn17clxXCgyFjp
C:1000:1000:,,,:/home/kali:/usr/bin/zsh

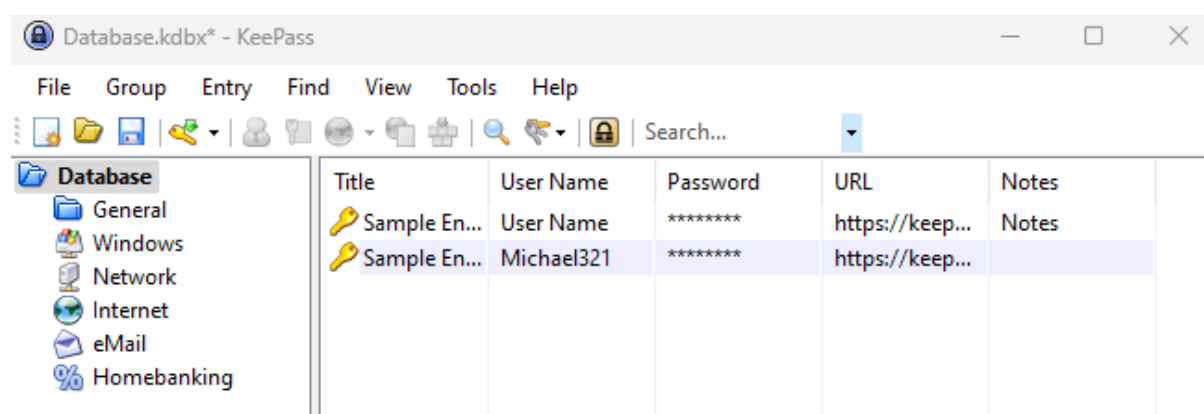
(kali㉿kali)-[~]
$
```

9. Busca informació sobre l'eina KeePass Safe i comprova el seu funcionament. Enumera les seves principals funcionalitats. Quina tècnica de seguretat utilitza per mantenir la confidencialitat i integritat de les contrasenyes que guarda?

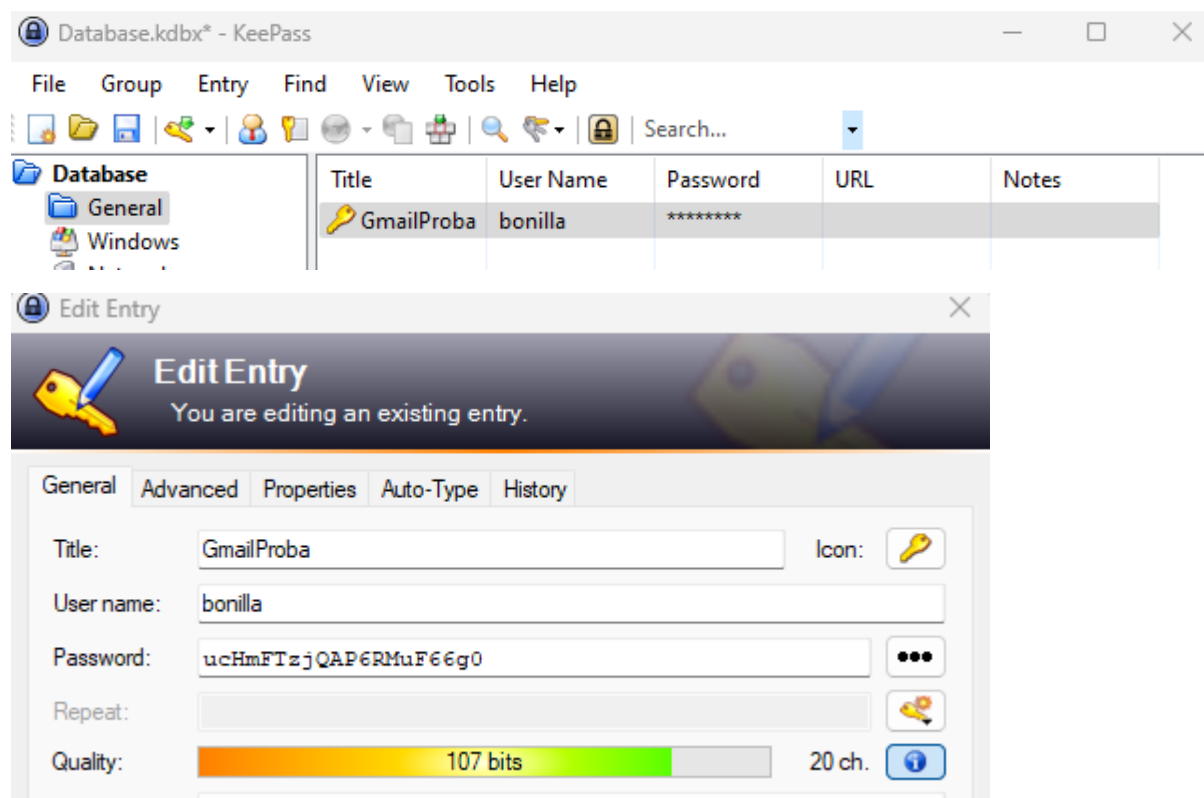
Les principals funcionalitats del KeePass Safe son les següents:

- Gestionar les contrasenyes
- Organitzar les credencials
- Crear contrasenyes mes forts

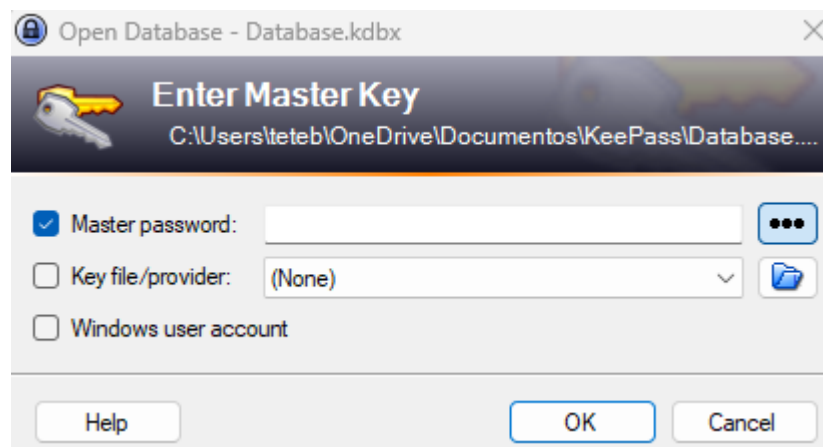
Aquesta aplicació el que fa es encriptar les claus amb els algorismes AES-256 o ChaCha20, de manera que només pots accedir a elles amb la teva clau maestra:



Vaig a general i creo una password (per defecte em crea una):



Si vull accedir de nou al KeePass em demana la clau maestra:



10. Respon amb verdader o fals les següents afirmacions. Raona la resposta:

a) La seguretat informàtica és un producte que normalment s'ha de contractar a empreses especialitzades, per exemple algun proveïdor d'antivirus.

Dit així es fals, però depèn si la empresa contracta a una empresa que no només posi l'antivirus, també faci formacions pels usuaris i tot això.

b) Un exemple d'amenaça d'interrupció és la denegació del servei de correu electrònic de l'empresa.

En una empresa, això es VERITAT, perquè estas aturant un medi de comunicació, com així el correu electrònic del usuari es l'eina de treball de algunes empreses.

c) El hardware i el software són els principals elements vulnerables d'un sistema i que cal protegir més inclús més que les pròpies dades.

FALS, les dades que més s'han de protegir són les dades i les més vulnerables també apart del software.

d) El procés d'autenticació permet saber quins drets d'accés tinc sobre un recurs del sistema, per exemple un directori.

FALS, no es el procés d'autenticació es d'autorització, això només es per verificar l'identitat.

e) Les ACL són el sistema d'autorització utilitzat per els sistemes operatius Windows a l'hora de definir els permisos de cada objecte del sistema de fitxers.

VERITAT

f) Els sistemes d'autenticació basats en contrasenyes són més forts que els que utilitzen biometria.

Es FALSA, perquè la biometria és molt més complexa a l'hora de suplantarla.

WEBGRÀFIA

1. A part de que he fet temes de riscos treballant y havia de saber que era *Confidencialitat*, *Integritat* i *Disponibilitat*, m'he guiat pel power:

https://drive.google.com/file/d/1VnzTLtwyj9KFKRptWy_CRlYDzFnKBLF/view

2. PcComponentes: <https://www.pccomponentes.com/que-es-un-sai-y-para-que-sirve>

<https://qloudea.com/blog/calcular-tiempo-de-un-sai-modo-baterias/>

5. <https://www.akamai.com/es/glossary/what-is-ddos>

6. <https://protecciondatos-lopd.com/empresas/sistemas-biometricos/>

8.

<https://www.freecodecamp.org/espanol/news/como-descifrar-contrasenas-usando-john-the-ripper-tutorial-de-pentesting/>

9. <https://www.redeszone.net/tutoriales/seguridad/proteger-contrasenas-keepass/>