PRÁCTICA 3 – HASHING CIFRADO Y CERTIFICADOS

**Funciones de HASH**

* Funciones criptográficas
* Características:



* + Funciones de una sola vía f(texto) 🡪 resumen o hash



Porque desde el punto de vista computacional (tiempo y procesador) es muy fácil obtener dado el texto claro obtener la función de hash, pero dado un resumen es muy complicado obtener el texto que ha generado el resumen.

* + Misma longitud del resumen independientemente del tamaño de la entrada. Aunque le pases una entrada muy grande la salida siempre son 40 caracteres.
  + ¿Qué garantizan? 🡪 La integridad de la información, es decir que la información no se pueda alterar.

f(“hola”) 🡪 r1

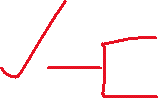
f(“h ola”)🡪 r2

1 carácter hexadecimal 🡪 4 bits

0 🡪 0000

1 🡪 0001

A 🡪 1010

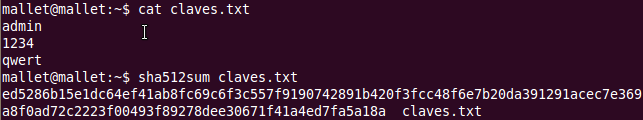


|  |  |  |
| --- | --- | --- |
| HASH | Tamaño salida | Colisiones |
| MD5 | 32 caracteres hexadecimal  128 bits | SI |
| SHA1 | 40 caracteres hexadecimal  160 bits | SI |
| SHA256 | 64 caracteres hexadecimal  256 bits | NO |
| SHA512 | 128 caracteres hexadecimal  512 bits | NO |

***Parte 1***

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

KALI LINUX O EN UN UBUNTU CON HASHID

Echo hola | md5sum

Hashid y le pasas lo que sale de arriba (te proporciona los diferentes funciones de hash que han podido generar ese resumen)

/etc/passwd tiene los usuarios del sistema

Texto

Descripción generada automáticamente

Sin superusuario o sin estar en el grupo shadow no puedes ver el fichero de claves /etc/shadow

Texto

Descripción generada automáticamente

Con que función de hash se corresponde $6$

Mallet 🡪 $6$ 🡪 SHA512



Texto

Descripción generada automáticamente

El root no tiene asignado un password

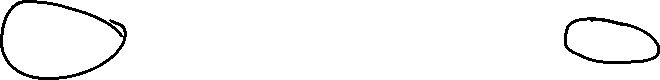


Para que vale un router?

* Conecta maquinas de una red con maquinas de otra red
* Tiene al menos dos interfaces de red
* La ip del router tiene que ser fija porque si es dirección ip cambia dejaría de prestar el servicio

La puerta de enlace de bob es 1.0.0.1/8 porque es la primera máquina que esta en su mismo segmento de red (ip similares) por la que tiene que pasar para comunicarse con Alicia.

Donde pongo el firewall?  
En el router , ya que es un punto muy crítico ya que tiene un trasiego constante de paquetes, en bob o alice se puede poner también en firewall, aunque hay menos trasiego.



Una red interna en virtual vox no tiene servicio de enrutado, ni de DNS, ni de DHCP.

Se usa red interna porque le puede poner el valor a la ip que te salga del bolo, y evitar problemas de solapamiento con virtual box

Un ping de alice a 1.0.0.1 funciona pero porque todavía no ha empezado a enrutar.

Routing 🡪