El documento describe varios ejercicios relacionados con tecnologías y herramientas TCP/HTTP:

1. Ejercicios de codificación:

    1. Calcula el HASH MD5 del mensaje “Esto no es un juego” con el comando “md5”.
       $ md5sum
       Esto no es un juego
       54a78e9f876087f44cec1fc199b93da4 -
    2. Calcula el HASH SHA-1 del mensaje anterior con el comando “sha1sum”, ¿es posible recuperar el mensaje?
       $ sha1sum
       Esto no es un juego
       be34f2cee14f2e976b470081c00df195e5d50473 –

       No es posible recuperar el mensaje debido a que *SHA-1* realiza un resumen en forma de *hash*, lo que hace que no sea posible recuperar el mensaje original.
    3. Compara ambos mensajes, observa las diferencias, cambia una letra del mensaje anterior y compara los resultados. ¿es posible diferenciar los resultados entre funciones hash?
       La principal diferencia entre *MD5* y *SHA-1* es el número de *bytes* empleados.

       Si cambiamos el mensaje “Esto no es un juego” por “Esto ni es un juego”, se obtiene el siguiente *hash* utilizando *SHA-1*:
       $ sha1sum
       Esto ni es un juego
       7a3c31a5d6114865d927b7629f03b23ed767beb0 –

       Como se puede ver, cambiar una única letra del mensaje genera un *hash* completamente distinto, por lo que, **dados dos *hashes*, no se podrían saber las diferencias entre los mensajes originales**.
    4. Codifica el mensaje “Comunidad twitch” con el comando “base64”, verifica decodificando ¿es posible?
       $ base64
       Comunidad twitch
       Q29tdW5pZGFkIHR3aXRjaAo=

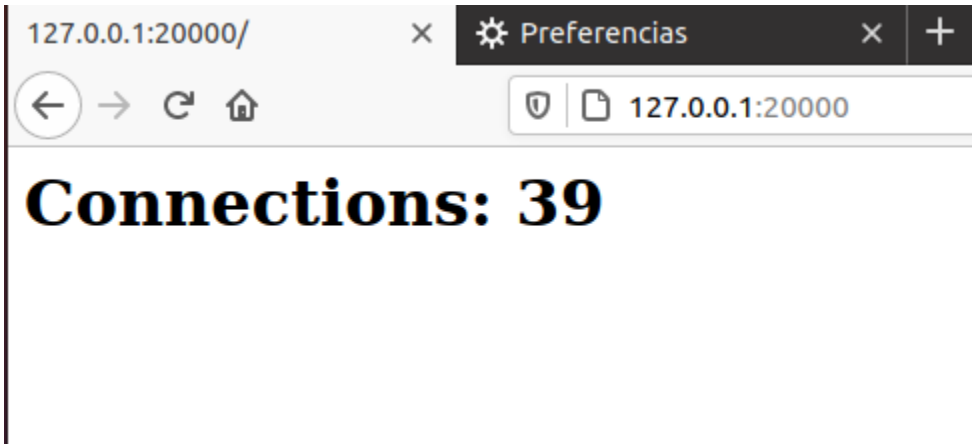
       $ base64 -d
       Q29tdW5pZGFkIHR3aXRjaAo=
       Comunidad twitch

       Es posible decodificar mensajes en base64 debido a que se trata de función de codificación, y no de resumen.
    5. Codifica en base64 el hash MD5 del mensaje “Juegos de guerra”.
       $ md5sum
       Juegos de guerra
       67f487f716a636a2b9de2be3a2de56cd –

$ base64
67f487f716a636a2b9de2be3a2de56cd
NjdmNDg3ZjcxNmE2MzZhMmI5ZGUyYmUzYTJkZTU2Y2QK

6. Busca una herramienta en Linux para codificar el hexadecimal del hash MD5 del mensaje “Juegos de guerra”.
   El comando de *Linux md5sum* realiza esta función.
7. Codifica el octal el resultado del ejercicio anterior.
   $ od
   NjdmNDg3ZjcxNmE2MzZhMmI5ZGUyYmUzYTJkZTU2Y2QK
   0000000 065116 066544 042116 031547 065132 074143 066516 031105
   0000020 075115 064132 066515 032511 043532 074525 066531 075125
   0000040 052131 065512 052132 031125 031131 045521 000012
   0000055

2. Instalar un uServidor Web/Seguro. Enlace



1. Busca una imagen PNG (mediana ~400px) y transforma en base64 su contenido, ¿Está en hexadecimal?
   No, está en *base64*. Se ha probado con la imagen *400x400.png* y la salida está en *output400x400.txt*.
2. ¿Cómo se puede incorporar a la página web este PNG? (no emplees ningún tipo de estilo css). Ayuda tag <img src=...>
   <img src=' base64 code' >