Episodio 1 - 1ª Parte

Vamos a la URL que nos dan en la prueba:
http://34.247.69.86/lacasadepapel/episodio1/puerta.php

Viendo el código fuente de la web vemos que llama a un javascript:

<script language="JavaScript" src="login.js"></script>

Descargamos el javascript y lo analizamos.

```
function conexion(){
   var Password =
"unescape%28String.fromCharCode%252880%252C%2520108%252C%252097%2
52C%2520110%2529%29:KZQWYZLOMNUWC===";
   for (i = 0; i < Password.length; i++)
   {
      if (Password[i].indexOf(code1) == 0)
      {
         var TheSplit = Password[i].split(":");
         var code1 = TheSplit[0];
         var code2 = TheSplit[1];
   }
}
```

Analizando el código vemos que cuando la condición del if se cumple parte la cadena Password en dos, así que tenemos dos códigos diferentes:

unescape%28String.fromCharCode%252880%252C%2520108%252C%252097%25
2C%2520110%2529%29

KZQWYZLOMNUWC===

La primera cadena la escapamos 2 veces con un URL encoder/decoder Online:
http://www.utilities-online.info/urlencode/

Resultado: unescape(String.fromCharCode(80, 108, 97, 110))

Ejecutandolo en la consola de google chrome por ejemplo tenemos que nos da la palabra:

"Plan"

Para la segunda parte … parece un cifrado base pero no es 64. Después de probar vi que era base32. Podemos decodificarlo en por ejemplo:
https://www.dcode.fr/code-base-32

El resultado es: Valencia

Introducimos las claves en el formulario:
Código1: Plan
Código2: Valencia

La web nos devuelve la contraseña para descomprimir el zip.

Una vez descomprimido .. vemos que contiene el archivo episodio1.exe.

Después de ejecutarlo en una Sandbox (no es por nada chicos) vemos una pista:

System_Date: 05/14/18
Wrong date R3m0!

Paso las strings a un fichero plano para analizarlas:

strings episodio1.exe > prova.txt

Busco la cadena de caracteres "System_Date" dentro del fichero de strings. Inmediatamente anterior a esto, veo las siguientes strings:

01/23/89
Congratulation!!, Stealing Money $$$...

Stolen: 1.000.000.000 $
Flag:

Esta fecha parece interesante … cambio la fecha del equipo a la fecha dada y ejecutamos otra vez el programa, el resultado es este:

Congratulation!!, Stealing Money $$$...

Stolen: 1.000.000.000 $

Flag: e30f35ad8d9cb6efc0778539a669fa85
.....
Presione una tecla para continuar . . .

Por otra parte … vemos que el md5 este el el md5 de la fecha que nos proponía el programa.

echo -n 01/23/89 | md5sum
e30f35ad8d9cb6efc0778539a669fa85 -

DarkEagle