WRITE-UP GOT CTF VULNHUB

ELABORADO POR: ARSENICS

Primera fase: Information Gathering + ftp flag

Descargamos la ova, comprobamos el md5 conforme no ha sido alterada, la instalamos y hacemos un netdiscover para averiguar que ip se nos ha asignado a la máquina.

https://www.vulnhub.com/entry/game-of-thrones-ctf-1,201/

Tras ello lanzamos un nmap para descubrir q puertos tiene abiertos y ponernos manos a la obra.

Nmap -sV -sC ñ -a ip de la máquina

```
PORT      STATE    SERVICE    VERSION
21/tcp    open     ftp        Pure-FTPd
22/tcp    open     ssh        Linksys WRT45G modified dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 e6:5b:d7:78:6b:86:4f:9b:35:40:9f:c7:1f:dd:0d:9f (RSA)
|_  256 a9:f2:d8:ee:f0:93:49:d8:19:04:ff:ad:89:ee:df:7d (ED25519)
53/tcp    open     domain     (unknown banner: Bind)
| dns-nsid:
|_  bind.version: Bind
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|     bind
|_    Bind
80/tcp    open     http       Apache httpd
| http-robots.txt: 2 disallowed entries
|_/secret-island/ /direct-access-to-kings-landing/
|_http-server-header: Apache
|_http-title: Game of Thrones CTF
143/tcp   filtered imap
3306/tcp  filtered mysql
5432/tcp  open     postgresql PostgreSQL DB 9.6.4 - 9.6.6
10000/tcp open     http       MiniServ 1.590 (Webmin httpd)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Login to Stormlands
1 service unrecognized despite returning data. If you know the service/version, please submit the following
SF-Port53-TCP:V=7.70%I=7%D=6/24%Time=5D10D5A1%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,3F,"\0=\0\x06\x85\0\0\x01\0\x01\0\x01\0\0\x07version\x
SF:04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0\x05\x04Bind\xc0\x0c\
SF:0\x02\0\x03\0\0\0\0\0\x02\xc0\x0c");
MAC Address: 08:00:27:7D:EF:D5 (Oracle VirtualBox virtual NIC)
Service Info: Device: router
```

Ftp, ssh, dns, http, webmin, etc pues aquí hay trabajo que hacer esto va a ser largo jaja.
Comienzo con el http del puerto 80 a ver que me espera.

Lo primero que llama la atención es que hay música, luego puede haber algo de estego en el audio y los dibujos de las casas importantes de got:

Del audio extraemos la flag Savages:

```
APETAGEX
TAGGame of Thrones - Main theme
O.S.T.
Savages secret flag: 8bf8854be
```

Probando con la inicial de cada uno a ver si forma alguna palabra lógica pero sin éxito.

Aguila – A, Ciervo – B, Calamar – G, leon -L, lobo – S, Dragón – T, Pescao -T

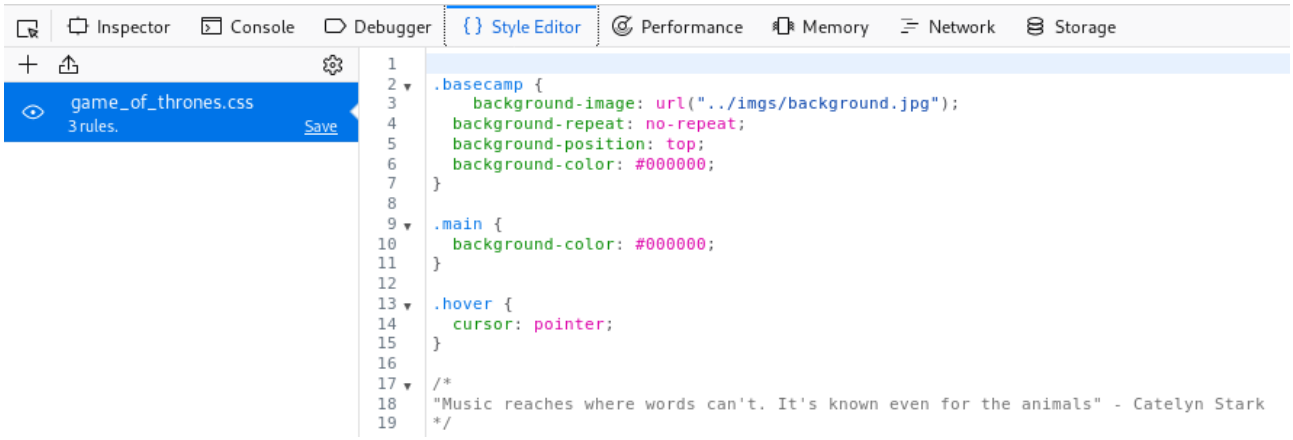
Mirando el robots.txt que me señala el nmap: vemos varios directorios. Voy a ver que se encuentra en cada uno de ellos.

```
User-agent: Three-eyed-raven
Allow: /the-tree/
User-agent: *
Disallow: /secret-island/
Disallow: /direct-access-to-kings-landing/
```

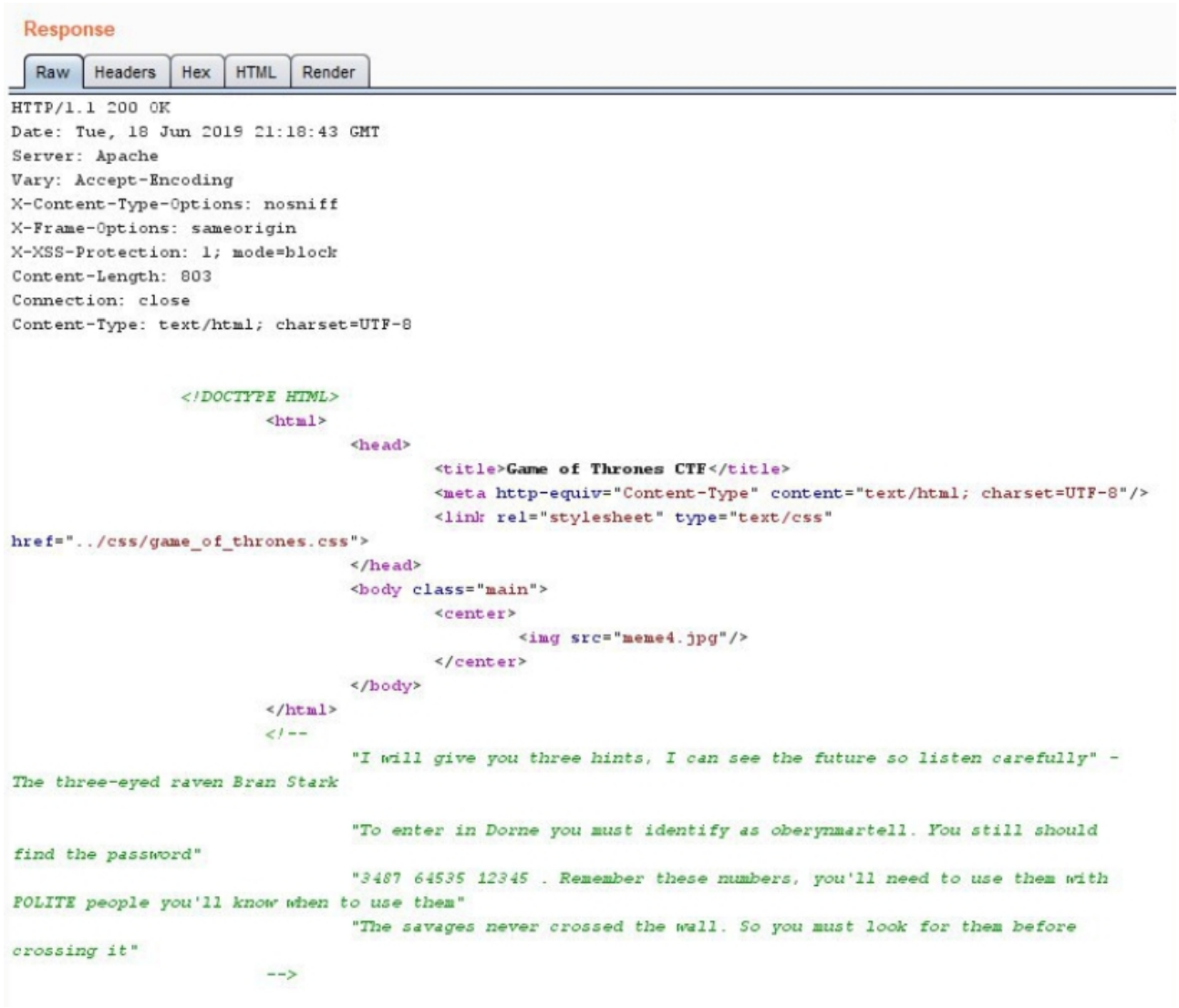
En ip/the-tree/ aparece un meme que al inspeccionar el elemento nos da el siguiente mensaje:

```
    <img src="meme5.jpg">
  </center>
 </body>
</html>
<!--"You mUSt changE your own shape and foRm if you wAnt to GEt the right aNswer from the Three-eyed raven" - Written on the tree by somebody-->
```

En esta del style editor hay pista de la flag the savage que encontramos en el mp3 anterior:



Al capturar con burp el acceso a /the-three enviarlo al repeater y ver la respuesta 3 nuevas pistas se dejan ver:



Bien ya tenemos el user para entrar en la flag 1 FTP. Sin embargo nos falta alcanza el pass.

En ip/secret-island/ al inspeccionar obtenemos un preciado mapa que nos indica el recorrido de las 11 flags a encontrar:

En ip/direct-access-to-kings-landing/ nos vuelven a insistir con la música de la flag the savages que ya tenemos en el style editor igual de nuevo.

```
      <img src="meme2.jpg">
    </center>
  </body>
</html>
<!--"I've heard the savages usually play music. They are not as wild as one can expect, are they?" - Sansa Stark-->
```

Lanzo dirb para listar nuevos directorios a ver que más tenemos:

dirb http://ip usr/share/dirb/wordlists/common.txt -r

Vale pues de aquí sacamos cosas más interesantes:

-sitemap.xml

-h/

```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.132/ ----
==> DIRECTORY: http://192.168.1.132/css/
+ http://192.168.1.132/favicon.ico (CODE:200|SIZE:1150)
==> DIRECTORY: http://192.168.1.132/h/
==> DIRECTORY: http://192.168.1.132/imgs/
+ http://192.168.1.132/index.php (CODE:200|SIZE:2601)
==> DIRECTORY: http://192.168.1.132/js/
==> DIRECTORY: http://192.168.1.132/music/
+ http://192.168.1.132/robots.txt (CODE:200|SIZE:135)
+ http://192.168.1.132/server-status (CODE:403|SIZE:222)
+ http://192.168.1.132/sitemap.xml (CODE:200|SIZE:214)
```

En sitemap.xml:

Nos localiza un nuevo php llamado raven.php

y al entrar en este directorio tenemos una nueva imagen del cuervo que al inspeccionar la imagen nos ofrece nueva pista. Segun dice vamos a necesitar mcrypt para la flag 2 “the wall”

```
−<urlset>
 −<url>
    <loc>index.php</loc>
    <changefreq>never</changefreq>
    <priority>1</priority>
  </url>
 −<url>
    <loc>raven.php</loc>
    <changefreq>never</changefreq>
    <priority>0.5</priority>
  </url>
</urlset>
```

```
<!--
You received a raven with this message: "To pass through the wall, mcrypt spell will help you. It doesn't matter who you are, only the key is needed
to open the secret door" - Anonymous
-->
```

```
<center>
  <img src="memel.jpg">
</center>
</body>
</html>
<!--
"My little birds are everywhere. To enter in Dorne you must say: A_verySmallManCanCastAVeryLargeShad0w . Now, you owe me" - Lord (The Spider) Varys
"Powerful docker spells were cast over all kingdoms. We must be careful! You can't travel directly from one to another... usually. That's what the
Lord of Light has shown me" - The Red Woman Melisandre
-->
```

Segimos enumerando y encontramos en */ h /i /d /d /e /n /* el ansiado pass para el FTP:

Ftp ip, ponemos user oberynmartell & pass A_verySmallManCanCastAVeryLargeShad0w

```
230-OK. Current directory is /
230-Welcome to:
230-  ____
230-|    \ ___ ___ ___ ___
230-|  |  | . |  _|   |  -_|
230-|____/|___|_| |_|_|___|
230-
230-Principality of Dorne was conquered. This is your first kingdom flag!
230 fb8d98be1265dd88bac522e1b2182140
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

He aquí la flag del FTP!!

Autoría: Arsenics