Write ups

CTF VM Game Of Thrones 1.0

Sulawesi I.T Security** & **iL 7Team

Target sudah di set dengan :
Target : 192.168.56.102 - kindom.GOT.com
*Machine Target dijalankan di virtualBox dengan set jaringan **Host-only Adapter.***
Savage & Dorne

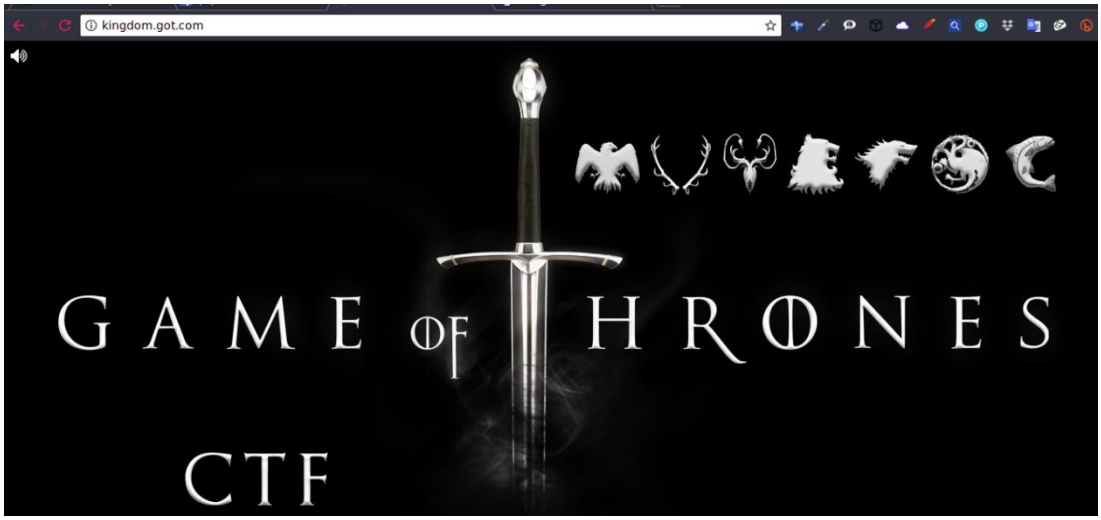
Karna ini VM (virtual machine) maka pertama tama kita scan pake nmap dahulu.

```
mcmillan@xeCURIty:~$ nmap -sV 192.168.56.102

Starting Nmap 6.40 ( http://nmap.org ) at 2018-05-18 13:53 WIB
Nmap scan report for kingdom.GOT.com (192.168.56.102)
Host is up (0.0035s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE     VERSION
21/tcp    open     ftp?
22/tcp    open     ssh         Linksys WRT45G modified dropbear sshd (proto
col 2.0)
53/tcp    open     domain      ISC BIND Bind
80/tcp    open     http        Apache httpd
143/tcp   filtered imap
3306/tcp  filtered mysql
5432/tcp  open     postgresql?
10000/tcp open     http        MiniServ 1.590 (Webmin httpd)
2 services unrecognized despite returning data. If you know the service/ver
sion, please submit the following fingerprints at http://www.insecure.org/c
gi-bin/servicefp-submit.cgi :
```

Port yang terbuka 21, 22, 53, 80, 143, 3306, 54332 & 10000. Terlihat bahwa port 80 lebih Luas di jelajahi dan terlebih lagi ini kita bermain CTF, jadi langsung kita buka di

browser



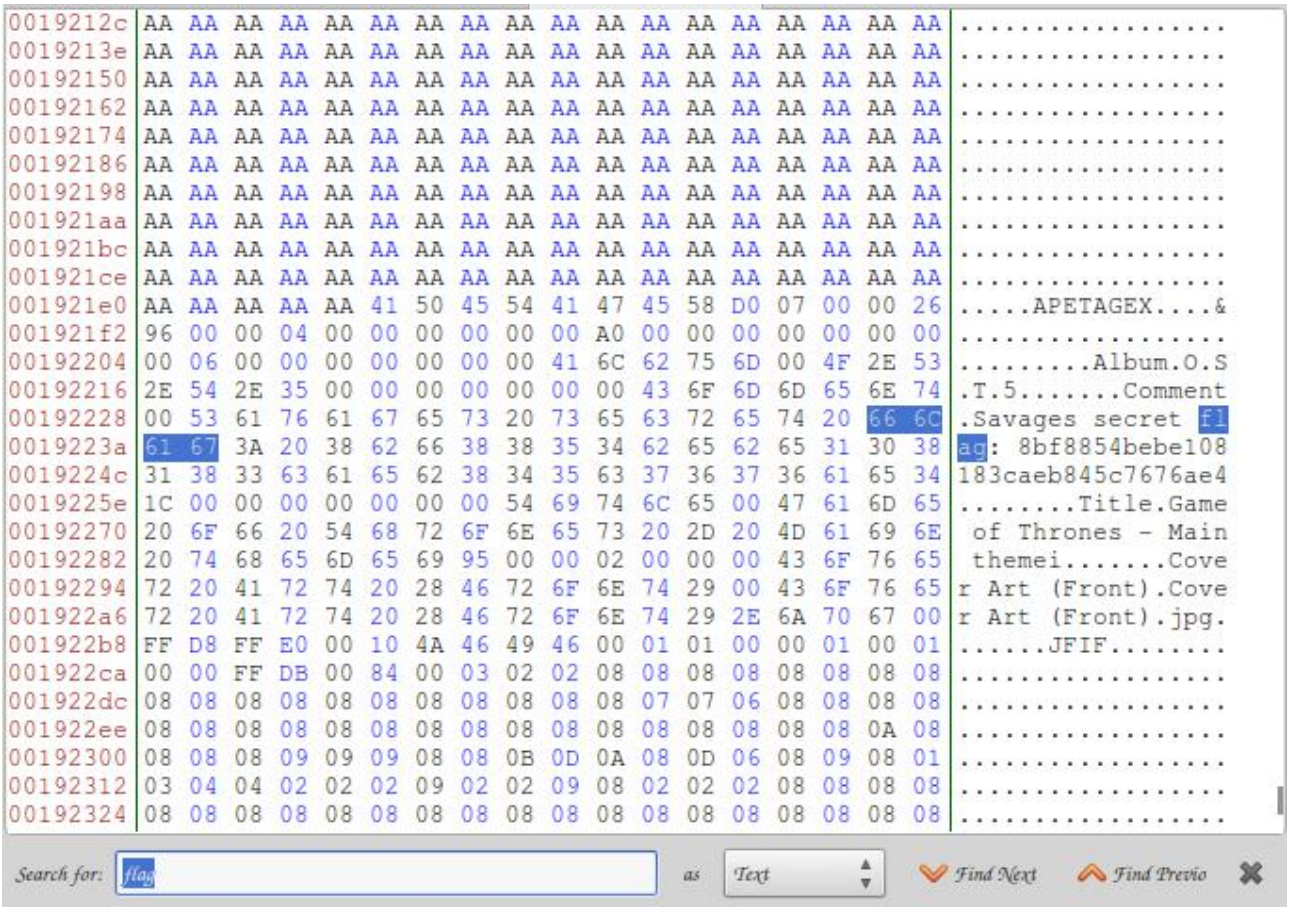
Kingdom.got.com <- kalian juga bisa ubah domain nya didalam file ***"/etc/hosts".***

Jika kita buka web nya langsung, dan ia langsung menampilkan img background game of thrones dan music, hanya itu saja. Setelah itu mari kita bongkar source nya

Terlihat ada file .css, .js, .mp3, .wav. Dan ada juga salam pembuka dari pembuat CTF nya dengan melampirkan Rules dan cara bermain.

Dari sini saya mulai menjelajahi setiap file" yang disediakan termasuk .css & js. Dan hasilnya gk menarik tapi kita bisa mencurigai .wav dan .mp3 ,ketika di play maka terdengar music apalah itu. Setelah itu kita download .wav dan .mp3

*Lihat kita sudah mulai curiga yang .mp3, langsung kita identifikasi menggunakan command **file, binwalk, strings, exiftool**. Jika kita sudah melakukan semuanya itu maka kita gak dapat hasil apapun :D penasaran tingkat tinggi karena cuman kedua file ini yang tersedia. Setelah itu saya mulai bongkar file .mp3 menggunakan **bless hex-editor** dan coba lihat, ketika saya mencari dengan perintah **flag** maka kita mendapatkan flag nya.*



Nah flag pertama telah kita dapatkan.

Savages secret flag : ***8bf8854bebe108183caeb845c7676ae4***

yang kita dapatkan hanyalah flag, lantas petunjuk selanjutnya gak kita dapatkan. Saya sudah membongkar .wav nya tetapi gak ada petunjuk sama sekali.

Dan saya ingat dengan rules yang diberikan.

```
Rules/guidelines to play:
- Start your conquer of the seven kingdoms
- You'll need hacking skills, no Game of Thrones knowledge is required. But if you play, it may contains spoilers of the TV series
- Difficulty of the CTF: Medium-High
- This is the start point, the base camp
- You must travel to westeros. First stop: Dorne. Last stop: King's Landing
- Don't forget to take your map (try to find it). It will guide you about the natural flag order to follow over the kingdoms
- Listen CAREFULLY to the hints. If you are stuck, read the hints again!
- Powerful fail2ban spells were cast everywhere. Bruteforce is not an option for this CTF (2 minutes ban penalty)
- The flags are 32 chars strings. Keep'em all! you'll need them

Good luck, the old gods and the new will protect you!

The game already started!! A couple of hints as a present.

"Everything can be TAGGED in this world, even the magic or the music" - Bronn of the Blackwater

"To enter in Dorne you'll need to be a kind face" - Ellaria Sand
```

Inti nya seperti ini :
Pertama kita harus berjalan ke westeros lalu berhenti di Dorne terakhir berhenti di King's landing dan jangan lupa ambil map untuk panduan mencari flag.

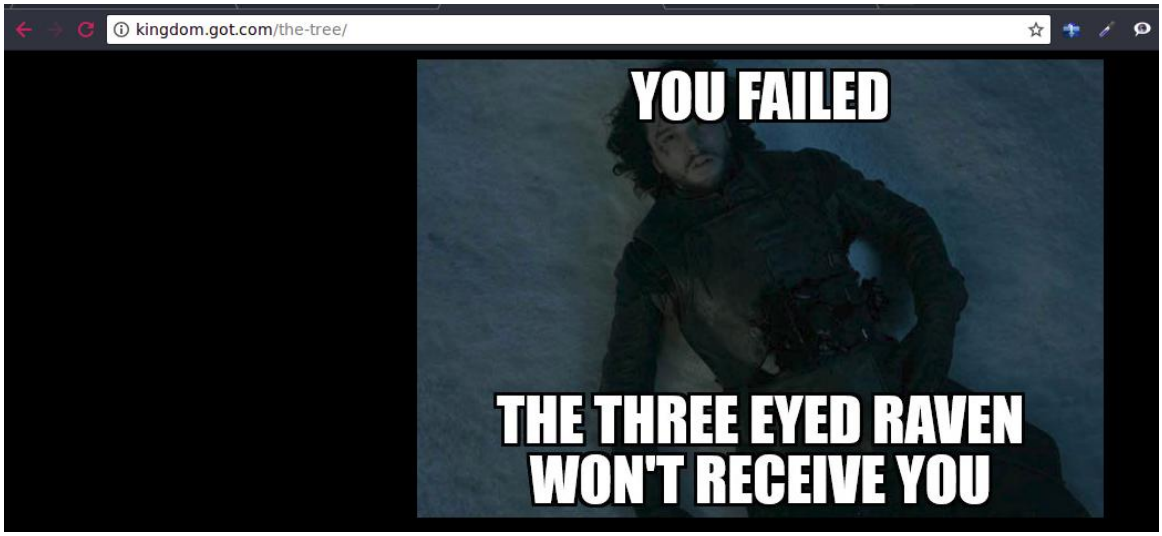
Sangat pusing untuk memikirkannya, saya langsung ambil jalan tengahnya yaitu scan web server nya menggunakan nikto, biasanya kita mendapatkan informasi lebih.

```
mcmillan@xeCURIty:~$ nikto -h 192.168.56.102
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          192.168.56.102
+ Target Hostname:    kingdom.GOT.com
+ Target Port:        80
+ Start Time:         2018-05-19 14:38:12
---------------------------------------------------------------------------
+ Server: Apache
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ robots.txt contains 3 entries which should be manually viewed.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/libr
ary/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-3092: /sitemap.xml: This gives a nice listing of the site content.
+ OSVDB-3092: /imgs/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2018-05-19 14:38:21 (9 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
mcmillan@xeCURIty:~$ _
```

Lihat, nikto mendapatkan petunjuk untuk kita yaitu file ***robots.txt, sitemap.xml, imgs*** *dan* ***/icons/README****. Pertama kita bongkar dulu* ***robots.txt.***

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

kita mendapatkan user-agent dan petunjuk bagus.



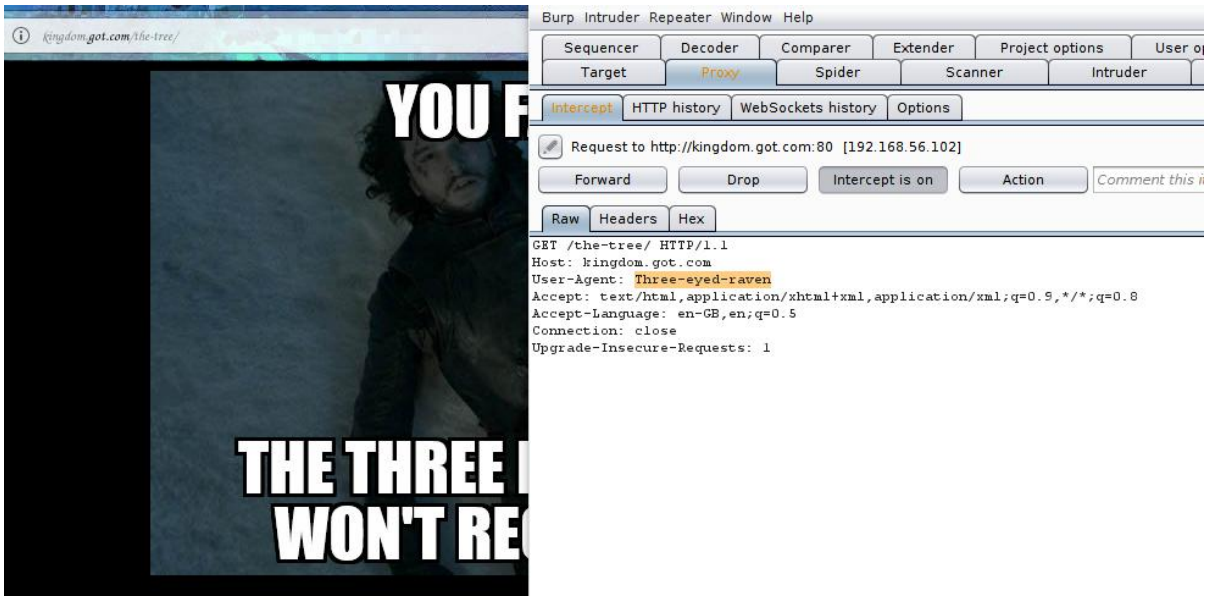
*Tapi ketika kita buka yang **/the-tree/** maka dia menampikan gambar, dan ketika kita bongkar source code nya maka kita mendapatkan petunjuk baru*

```
  <body class="main">
      <center>
          <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
>
```

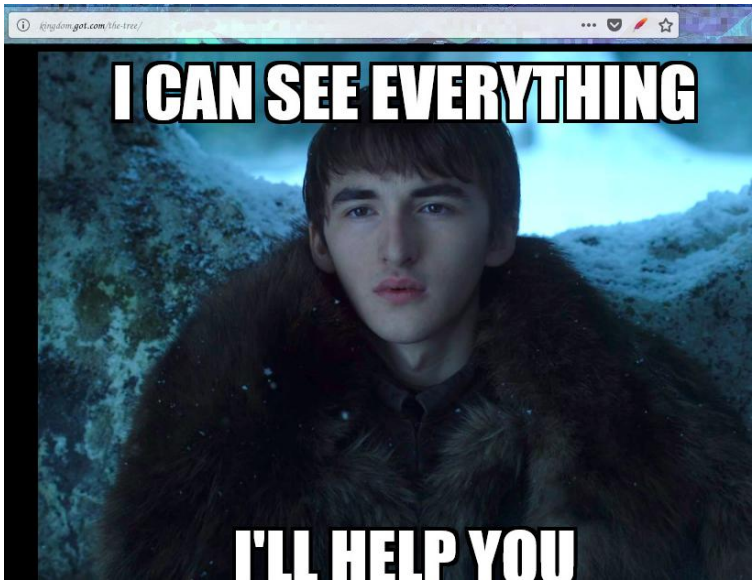
Kita disuruh mengganti user-agent yang kita dapatkan dari robots.txt

*User agent : **Three-eyed-raven***

*Untuk mengganti user-agent saya terbiasa dengan **burpsuite** ,*



*Jika sudah langsung **forward***



Kita langsung direct ke gambar ini. Mari kita bongkar lagi source code nya.

```
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
        <link rel="stylesheet" type="text/css" href="../css/game_of_thrones.css">
    </head>
    <body class="main">
        <center>
            <img src="meme4.jpg"/>
        </center>
    </body>
</html>
<!--
    "I will give you three hints, I can see the future so listen carefully" - The three-eyed raven Bran Stark

    "To enter in Dorne you must identify as oberynmartell. You still should find the password"
    "3487 64535 12345 . Remember these numbers, you'll need to use them with POLITE people you'll know when to use them"
    "The savages never crossed the wall. So you must look for them before crossing it"
-->
```

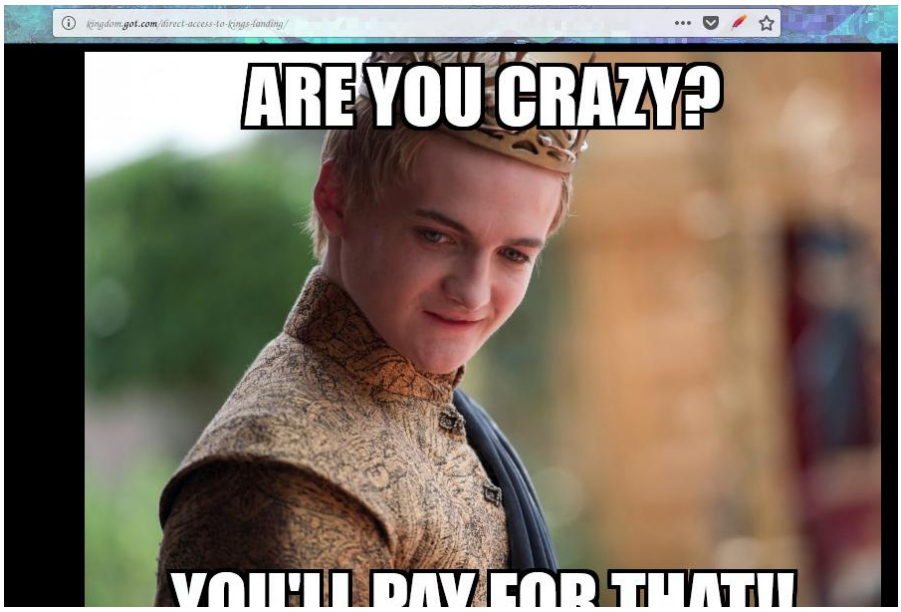
Lihat, kita diberi hints, apa katanya .. Untuk masuk ke Dorne kita harus menjadi oberymartell . Dan password cari lagi. Maksudnya kita udah dapat username , tapi passwordnya cari lagi. Untuk nomor kita abaikan saja dulu.

Kita belum dapat petunjuk setelah itu, tapi kita harus mencari password nya untuk masuk ke Dorne dan terlebih lagi kita belum dapat map.

*Sekarang mari kita ke **/secret-island** yang kita dapatkan dari **robots.txt***

Binggoo!! Kita mendapatkan map nya

*Go go go,, kita ke /**direct-access-to-kings-landing** yang kita dapatkan di **robots.txt***

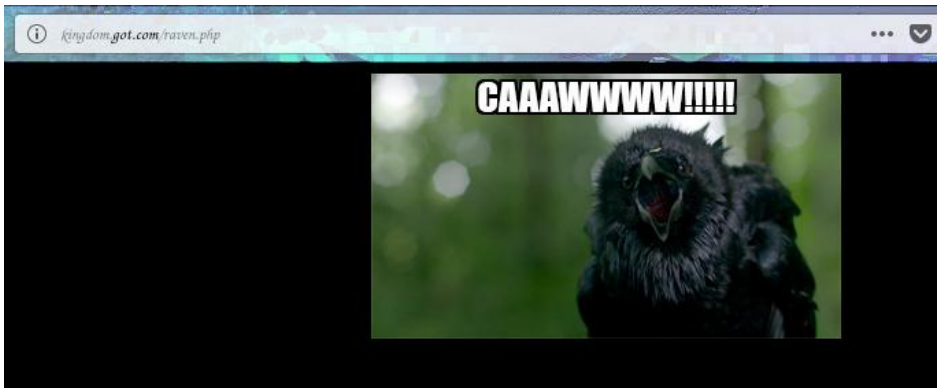


Langsung bongkar source code nya Dan gak dapat petunjuk sama sekali :D

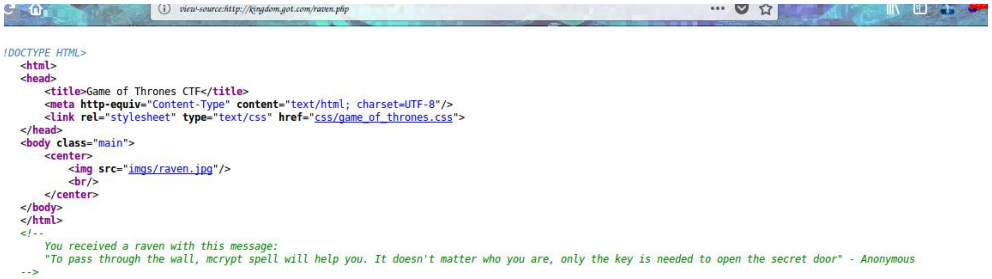
Sekarang mari kita ke page ini ***/sitemap.xml*** *yang kita dapatkan sebelumnya di* ***nikto.***


```
−<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>
```

Raven.php *mari kita jelajahi.*



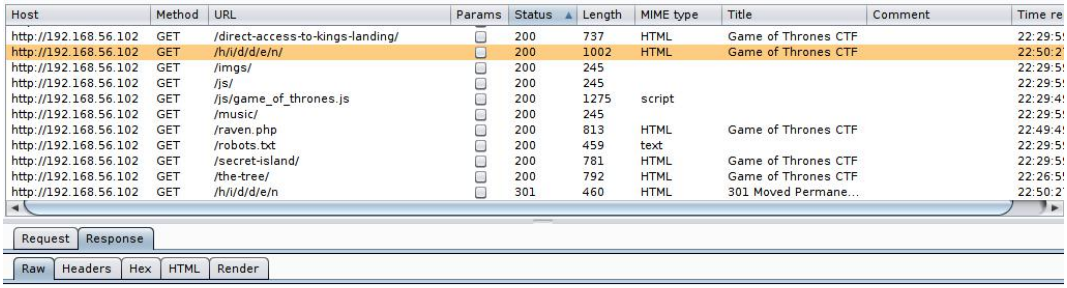
Gawwww!!!! Lihat source code nya lagi.



```
!DOCTYPE HTML>
  <html>
  <head>
      <title>Game of Thrones CTF</title>
      <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
      <link rel="stylesheet" type="text/css" href="css/game_of_thrones.css">
  </head>
  <body class="main">
      <center>
          <img src="imgs/raven.jpg"/>
          <br/>
      </center>
  </body>
  </html>
  <!--
      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
  -->
```

Semakin dekat dengan password kita, tapi kita dikasih clue lagi,dan belum dapat pencerahan untuk dapetin password nya.

Kini saatnya kita crawling semua directory dan file yang ada di VM menggunakan ***burpsuite*** *.*



Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time re
http://192.168.56.102	GET	/direct-access-to-kings-landing/	☐	200	737	HTML	Game of Thrones CTF		22:29:5
http://192.168.56.102	GET	/h/i/d/d/e/n/	☐	200	1002	HTML	Game of Thrones CTF		22:50:2
http://192.168.56.102	GET	/imgs/	☐	200	245				22:29:5
http://192.168.56.102	GET	/js/	☐	200	245				22:29:5
http://192.168.56.102	GET	/js/game_of_thrones.js	☐	200	1275	script			22:29:4
http://192.168.56.102	GET	/music/	☐	200	245				22:29:5
http://192.168.56.102	GET	/raven.php	☐	200	813	HTML	Game of Thrones CTF		22:49:4
http://192.168.56.102	GET	/robots.txt	☐	200	459	text			22:29:5
http://192.168.56.102	GET	/secret-island/	☐	200	781	HTML	Game of Thrones CTF		22:29:5
http://192.168.56.102	GET	/the-tree/	☐	200	792	HTML	Game of Thrones CTF		22:26:5
http://192.168.56.102	GET	/h/i/d/d/e/n	☐	301	460	HTML	301 Moved Permane...		22:50:2

Request | Response

Raw | Headers | Hex | HTML | Render

```
<!DOCTYPE HTML>
        <html>
        <head>
                <title>Game of Thrones CTF</title>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
                <link rel="stylesheet" type="text/css" href="../../../../../../css/game_of_thrones.css">
        </head>
        <body class="main">
                <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
        -->
```

Jika kita mau masuk ke dorne bilang aja "A_verySmallManCanCastAVeryLargeShadow". Ini adalah password nya. Jadi kita sudah dapat username dan password untuk masuk ke dorne.

Access to dorne port 21 ftp
u/p: ***oberynmartell / A_verySmallManCanCastAVeryLargeShad0w***

```
mcmillan@xeCURIty:~$ ftp 192.168.56.102
Connected to 192.168.56.102.
220-------------------------
220-"These are the Dorne city walls. We must enter!" - Grey Worm
220-
220-"A fail2ban spell is protecting these walls. You'll never get in" - One of the Sand Snake Gir
ls
220-------------------------
220 This is a private system - No anonymous login
Name (192.168.56.102:mcmillan): oberynmartell
331 User oberynmartell OK. Password required
Password:
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> _
```

Kita mendapatkan flag ke dua .

Flag Dorne : ***fb8d98be1265dd88bac522e1b2182140***