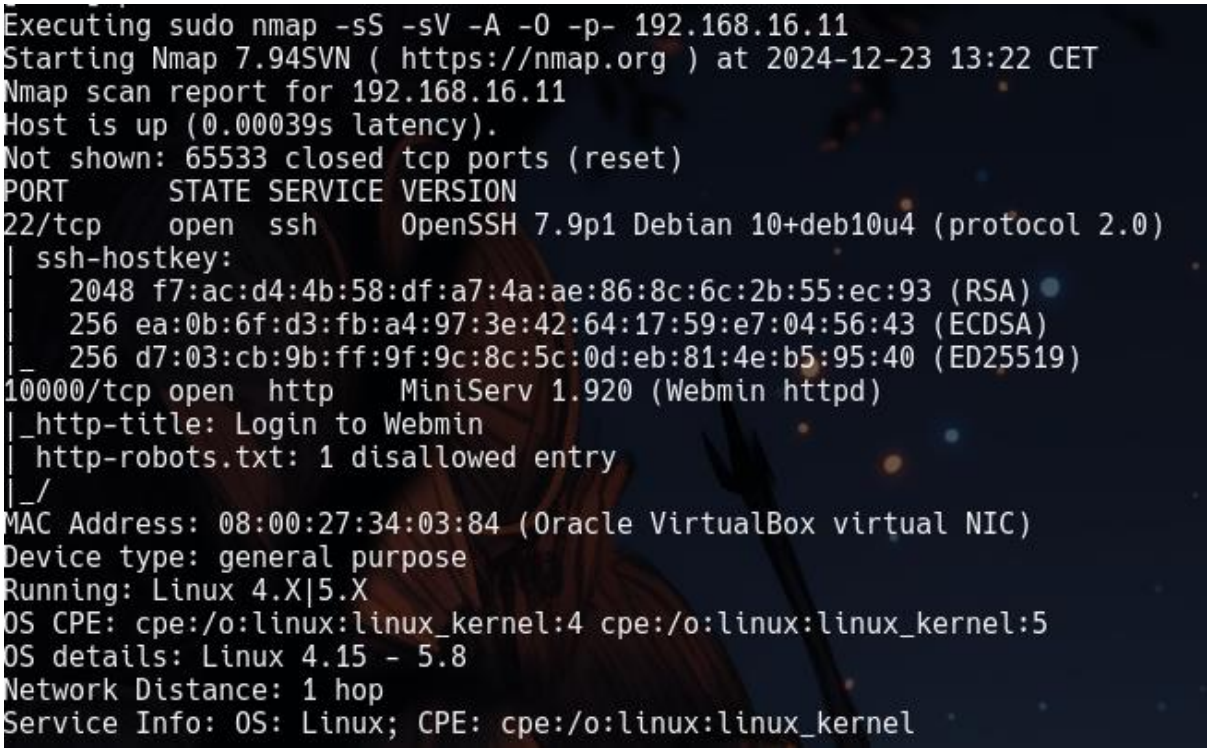
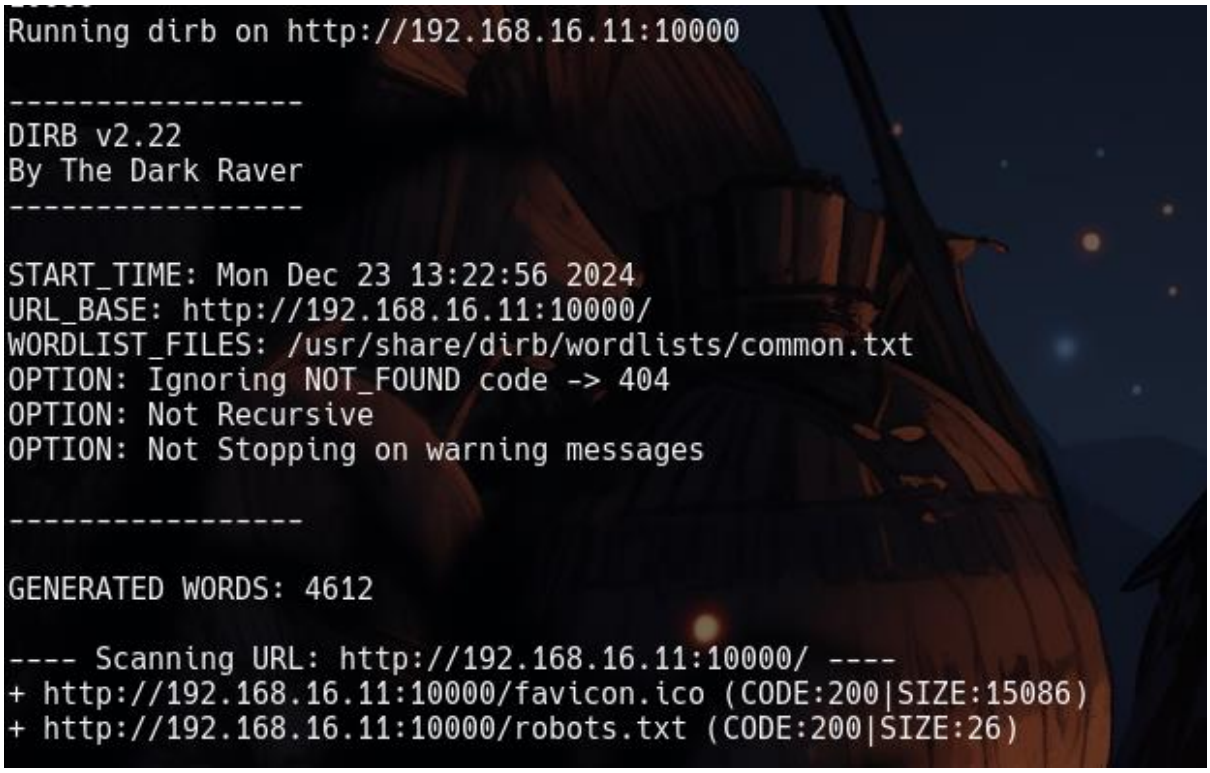
PAELLA


PAELLA
ACCEDER
PRINCIPIANTE
Creador: Condor Y Curiosidades De Hackers

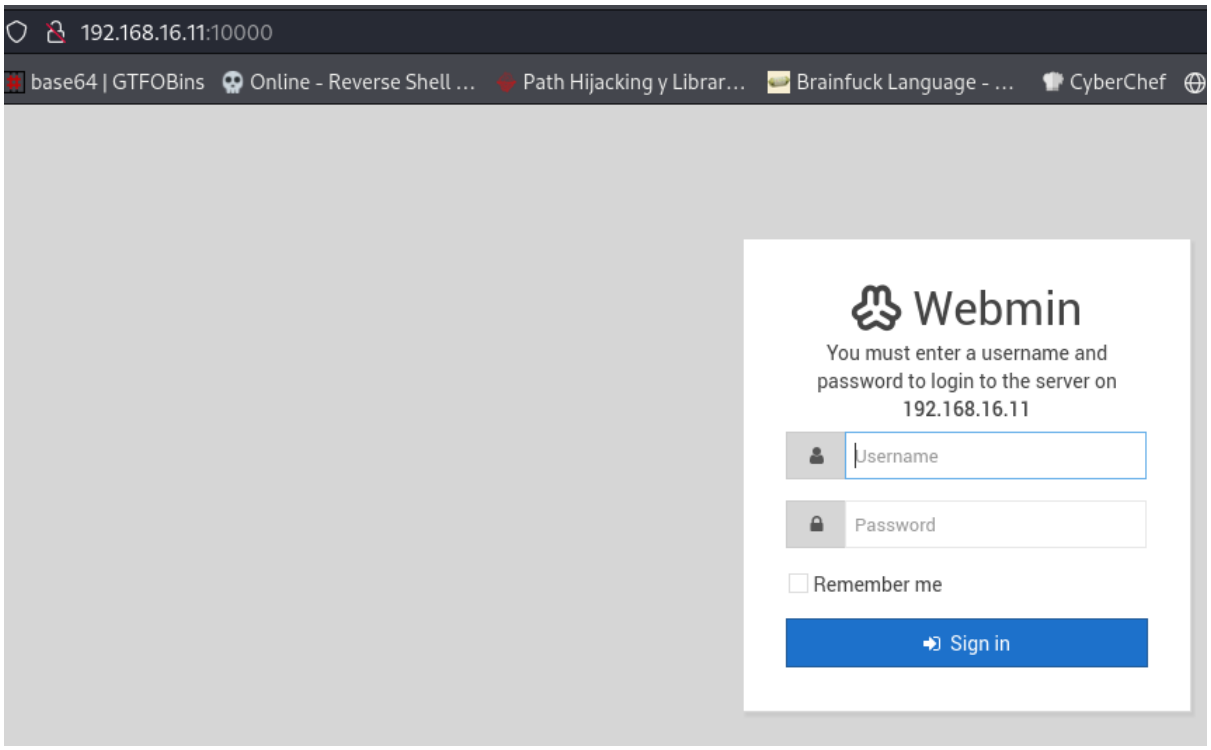
Ejecutamos nmap donde descubrimos solo 2 servicios corriendo, ssh en el 22 y webmin en el 10000.



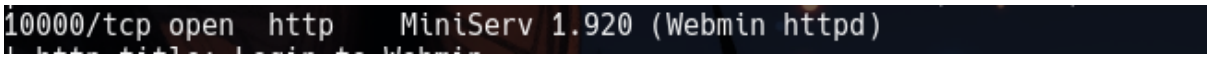


Accedemos al puerto 10000 en el navegador y nos encontramos el panel de login.

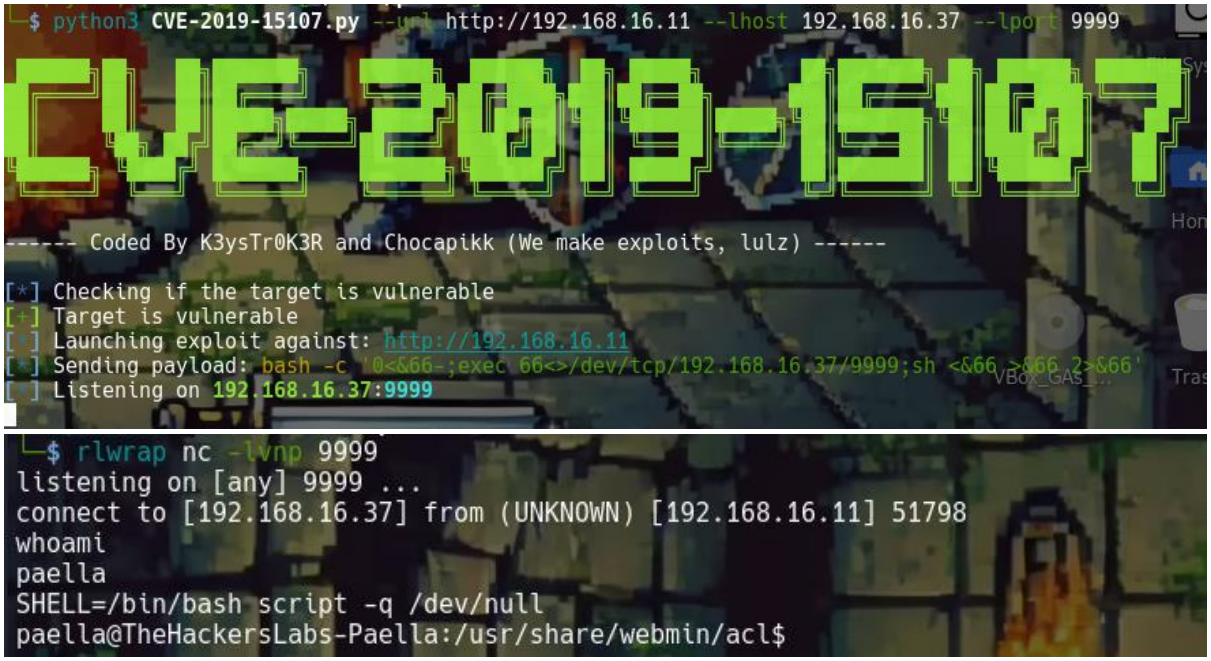
Aparentemente el login por defecto de webadmin es el mismo que el de root de la máquina instalada, por lo que descartamos esta vía.



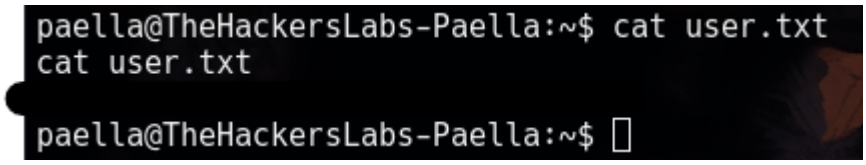
Si volvemos a echar un vistazo a la salida de nmap, podemos observar que la versión de webmin es la 1.9.20. Buscando por la red encontramos que es una versión muy vulnerable y existen multitud de exploits públicos incluyendo metasploit.



En nuestro caso usamos este script. El cual solo tendremos que poner nuestra máquina en escucha y poner los parámetros necesarios.



En el directorio del user paella obtenemos la flag de user.



Después de mucho buscar encontramos que el comando gdb tiene los permisos necesarios para cambiar el dueño de quien lo ejecuta.

Revisando la página de gtfobins encontramos los pasos para explotar estos permisos mal configurados cambiando el dueño de quién lo ejecuta por root y ejecutando una shell. Por último, vamos a por la deseada flag.