CTF Writeups

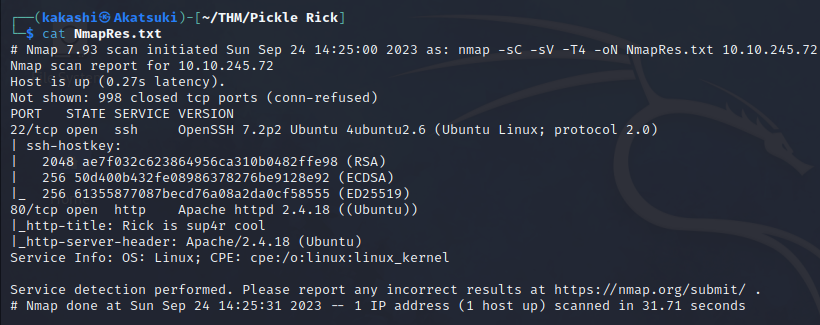
TryHackMe

Pickle Rick

Machine IP: 10.10.245.72

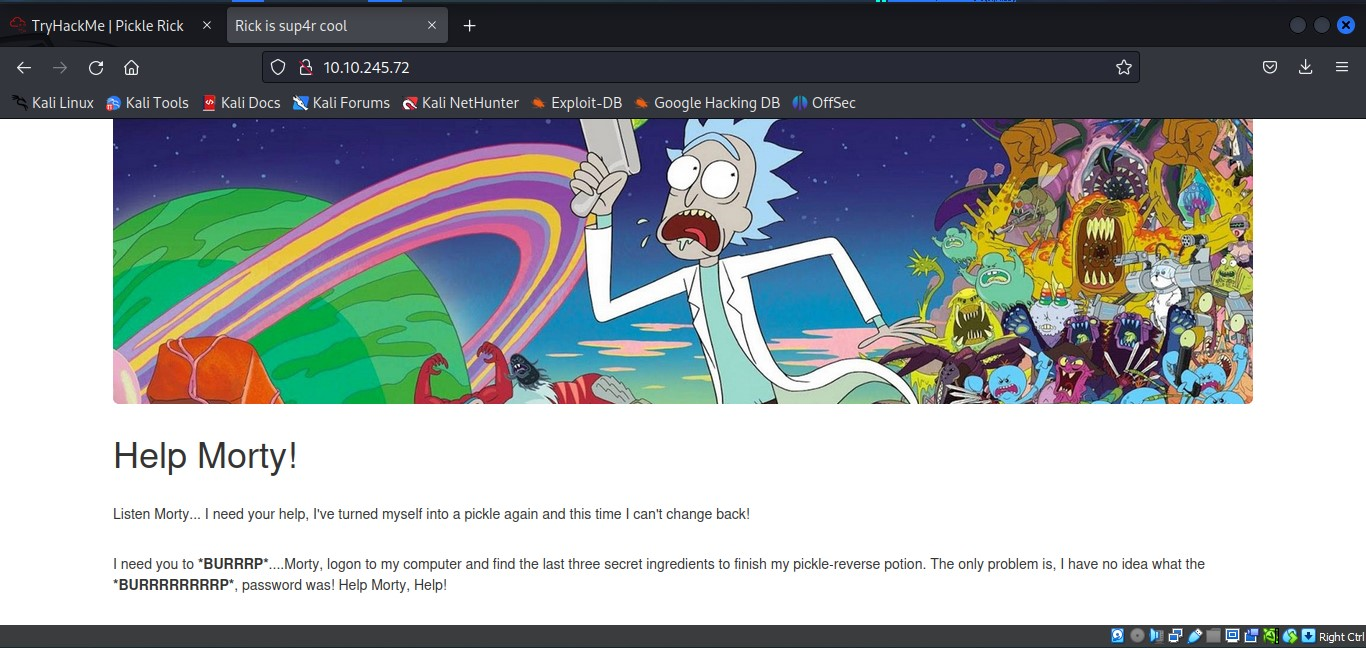
Step 1: Information Gathering

Finding open Ports via NMAP

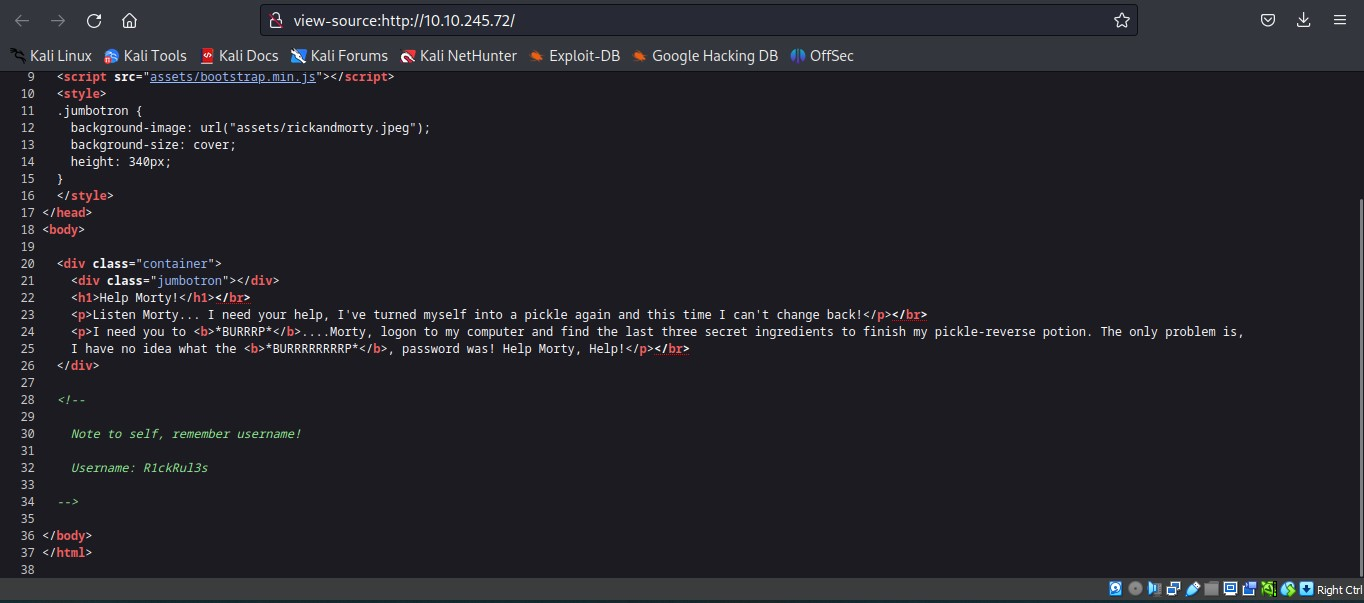


We Found that only HTTP and SSH is Open.

Lets analyze the website



There is no much information in the website, Lets analyze the website code by clicking view page source to find any hidden information.

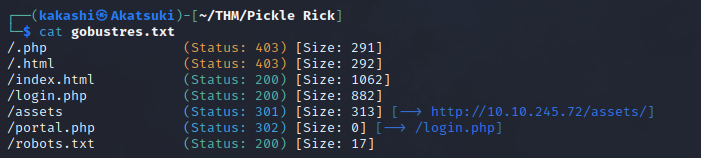


We found a username from the page source. We need to find the password.

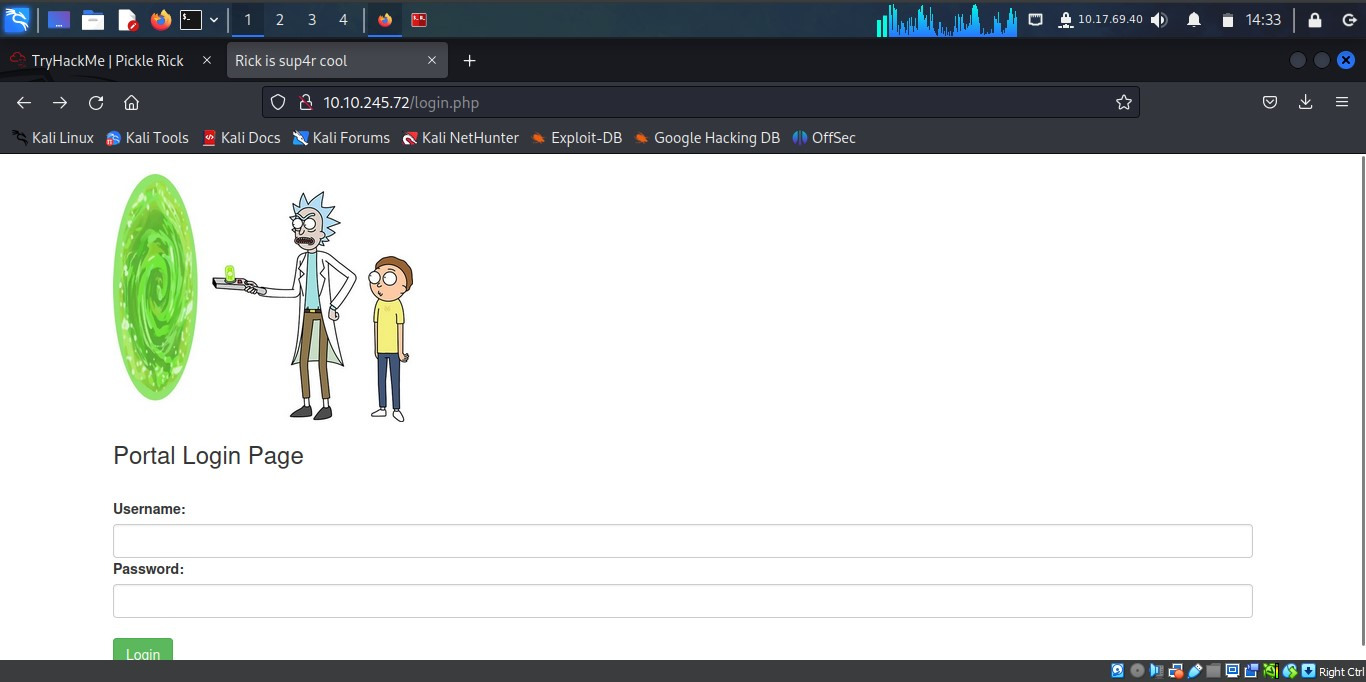
Step 2: Directory Enumeration

Using gobuster tool to find hidden directories in the website.

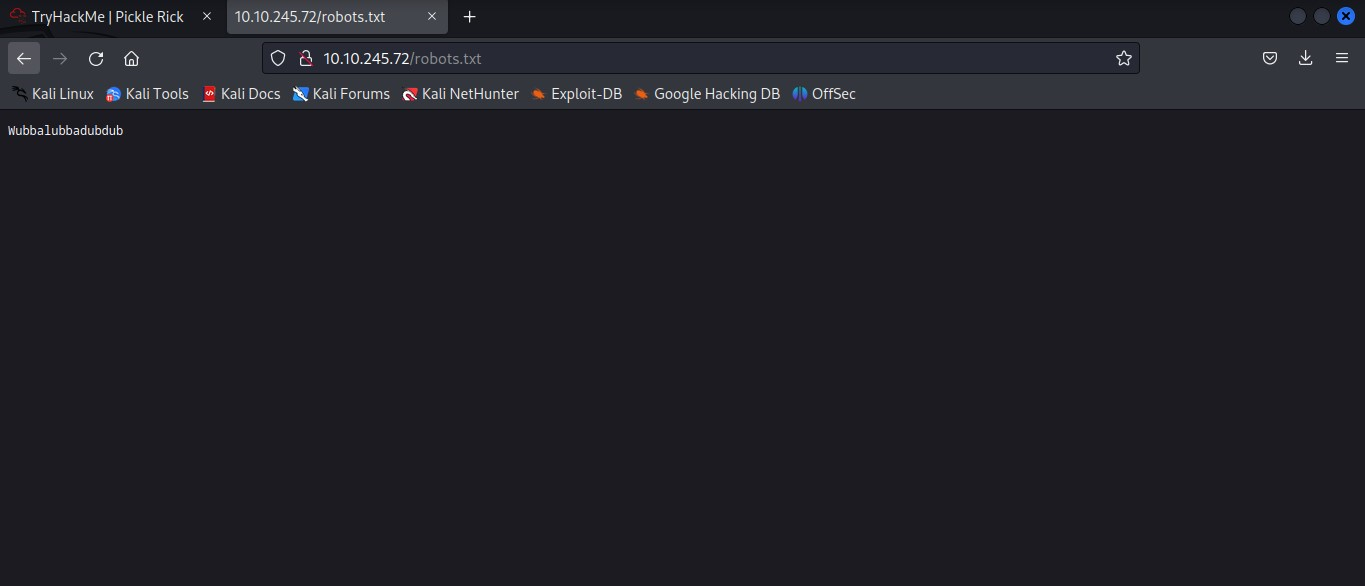
gobuster dir -u http://MACHINE-IP -w /usr/share/wordlists/dirbuster/directory-medium.txt -x php,html,txt -o gobusresult.txt



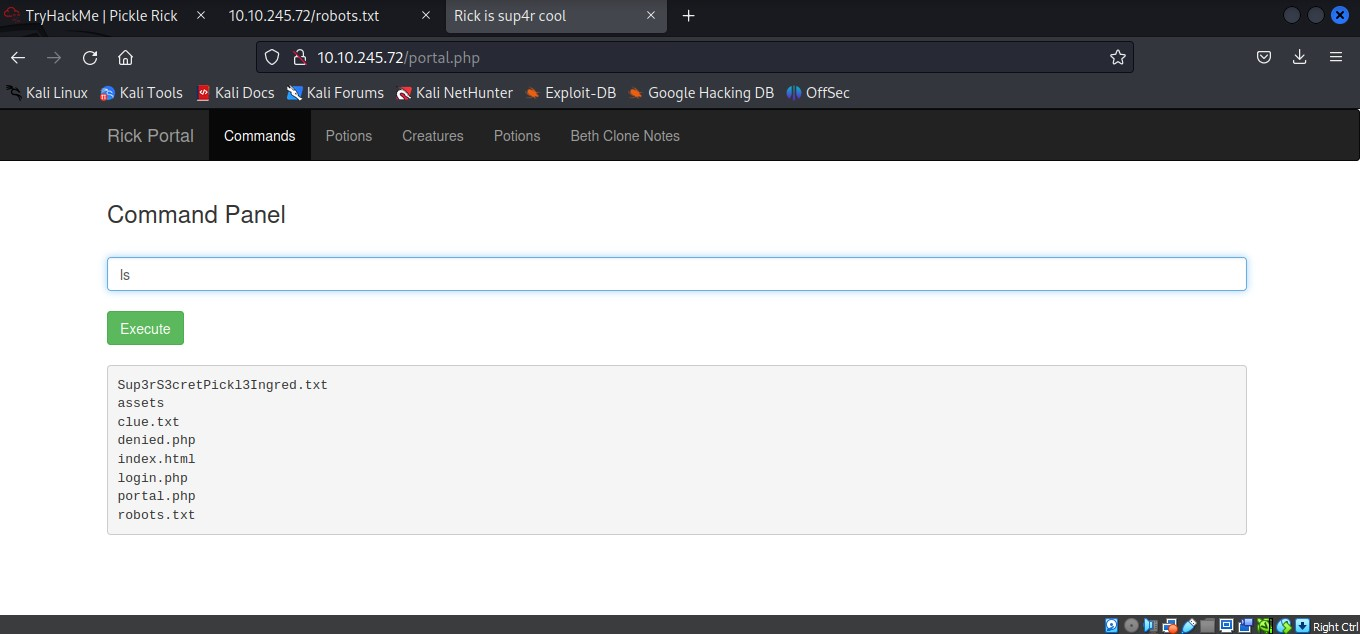
We found a login page and a robots.txt file lets check out one by one



We found the password for the username in robots.txt file



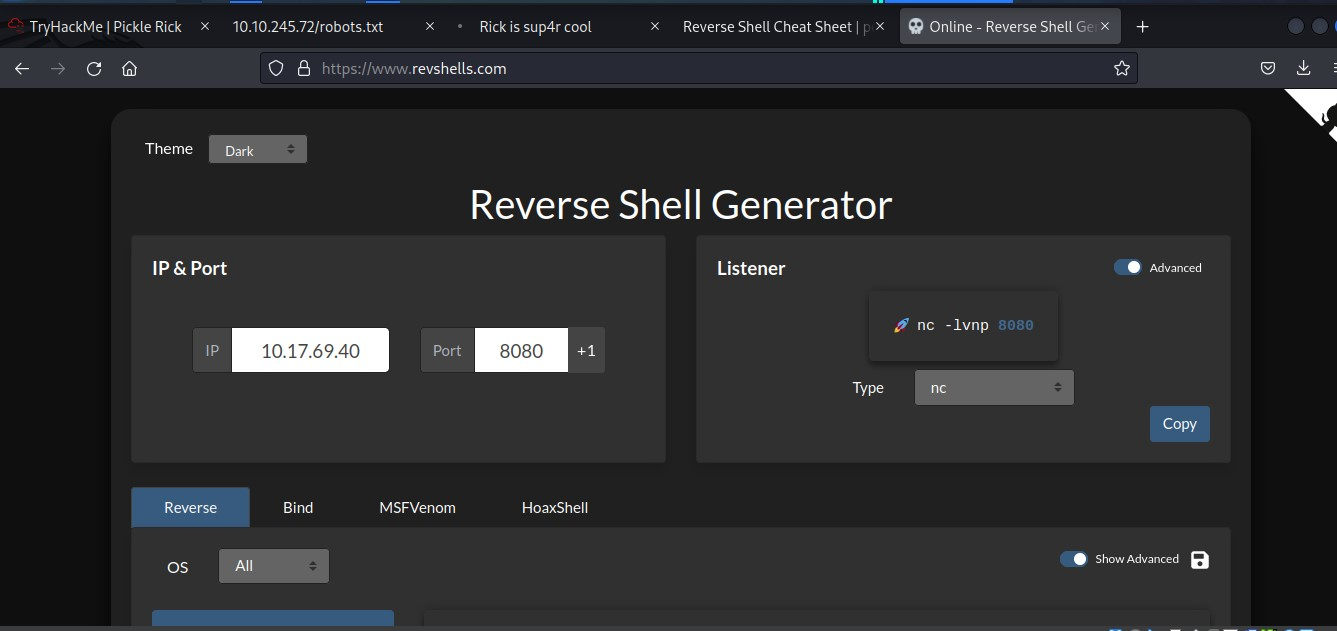
Lets Login and check whether there is any exploit or not.



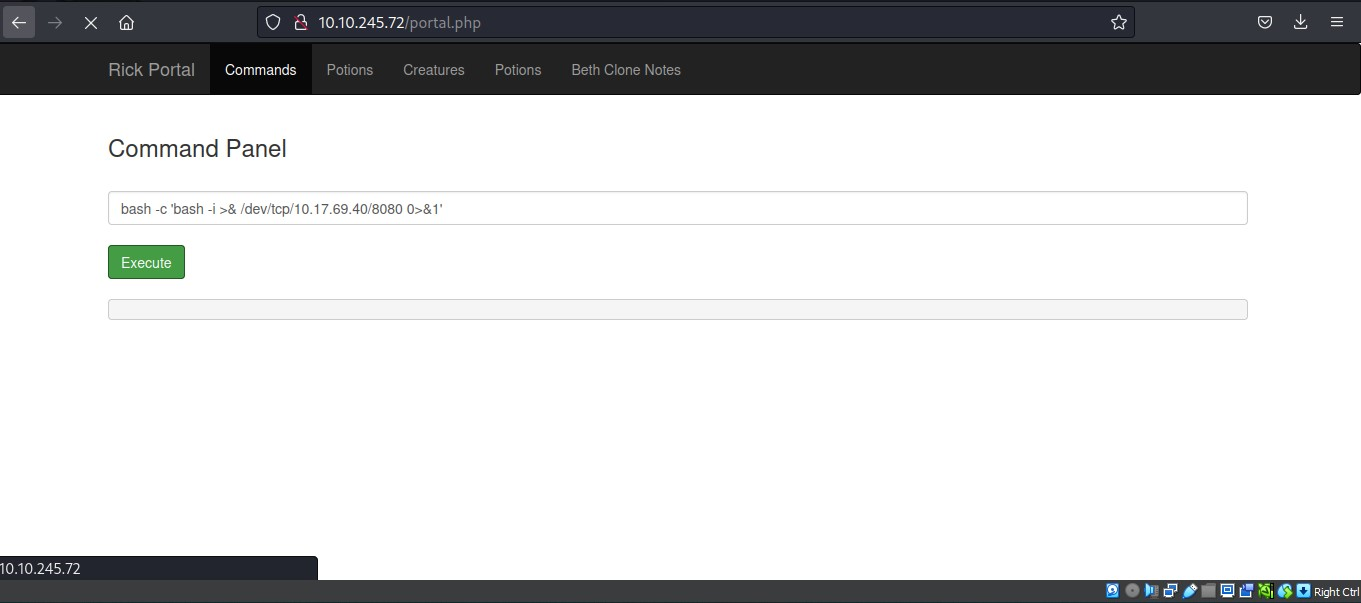
The Above input file is vulnerable to Command Line Injection, So we get a bash shell in there.

One way of getting reverse shell access to the web server is injecting command line injection to the above input field and gain a reverse shell using netcat.

The command to inject in the input field can be done with the help of pentest monkey website or revshells.com



Generate a netcat reverse shell from the above website and copy the command and paste it in the input field.



In the meantime run the following command on the terminal to listen the incoming traffic from the netcat.

nc -lvnp 8080



We got the Reverse shell from the web server, but the obtained shell is not stable, to make it stable we need to follow the below steps:

1. Check whether the webserver has python in it.



Using which command we have confirmed that python has installed in the web server.

1. Import python pty and spawn function

PTY stands for Pseudo Terminal in Python. This module is commonly used in scenarios where you need to automate command-line interactions, create interactive shells, or control terminal-based applications from Python code.

Enter the following python code:

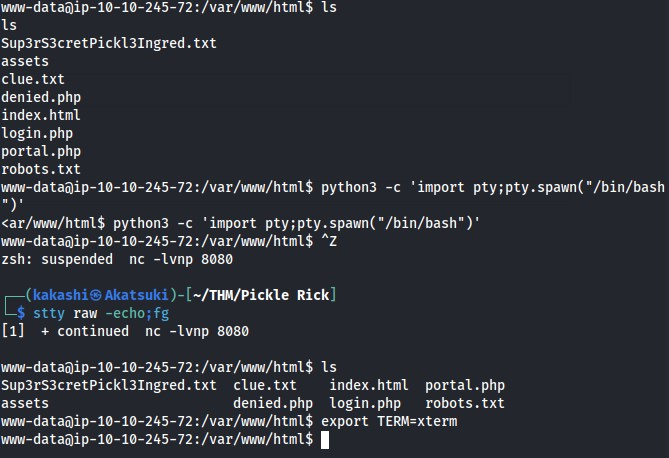
Python -c ‘import pty;pty.spawn(“/bin/bash”)’

Click ctrl+z this will suspend the netcat connection but does the close the connection.

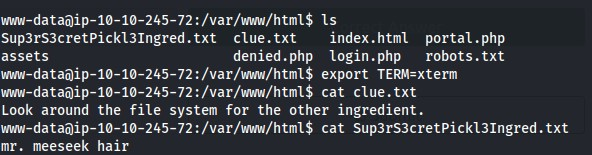
1. Open terminal and type the following command:

Stty raw -echo;fg

Export TERM=xterm

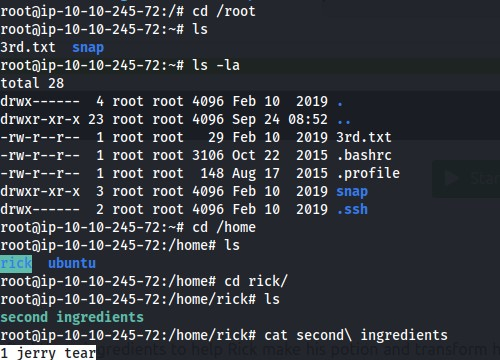


We got the stable shell, Lets find out the flag for the room:



We got our first flag, we need to find the second and third flag,

After Navigating to the home directory, we found a folder named rick, inside that we got our second flag:



To find the 3rd flag we need to escalate privilege to root:

Lets check the current user privileges by typing the following command:

sudo -l



We got this result (ALL) NOPASSWD: ALL which means we can switch to root without any password

Sudo su

The above command will give us a root shell, there we can find the third flag.

cd /root

cat snap

