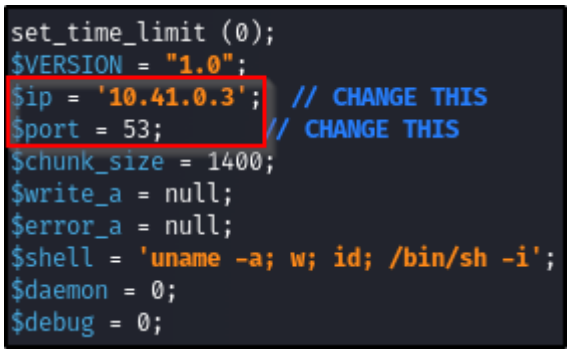
10

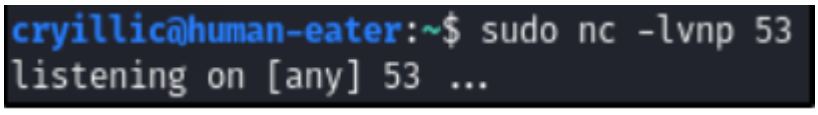
We have identified a potential attack surface that we can use to execute php and shell commands on. We are able to execute a reverse shell on the web shell in order to get a shell back on the machine.
Uploading a Reverse Shell
For the PHP reverse shell, we'll be using Pentest Monkey's reverse shell found here or in kali under /usr/share/webshells/php/php-reverse-shell.php
1.) Modify the reverse shell to your tun0 IP address and port.



PHP reverse shell IP and port

2.) Paste into the web shell.
Before executing the reverse shell you need to remove the "" last line of the reverse shell because pfSense only interprets PHP commands.

Adding our PHP reverse shell to the PHP web shell
3.) nc -lvnp 53



Starting a Netcat listener

4.) Execute your reverse shell

Catching our reverse shell following pressing 'execute' in the PHP prompt

Answer the questions below

What log file was found that is not a default log?

Correct Answer

What user was found within the log?

Correct Answer

What is the hash of the user?

Correct Answer

Submit flags for THROWBACK-FW01 in Task 4

Question Done