**Lab Practical #03:**

TryHackMe Room: - **h4cked**

**TASK 1: Oh no! We’ve been hacked!**

Firstly, download the Task files. After Downloading open it with Wireshark.

1. **It seems like our machine got hacked by an anonymous threat actor. However, we are lucky to have a .pcap file from the attack. Can you determine what happened? Download the .pcap file and use Wireshark to view it.**

**Answer:** *No Answer Needed*

1. **The attacker is trying to log into a specific service. What service is this?**

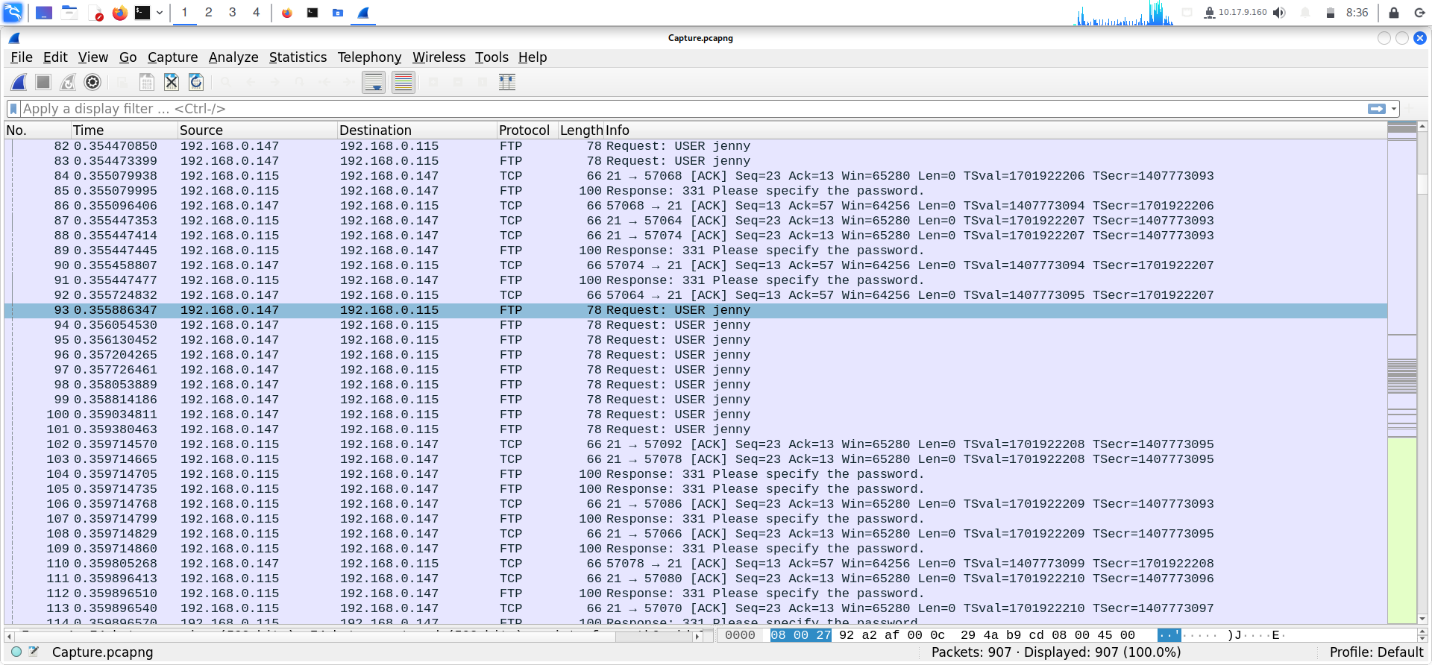
**Answer:** *FTP*

1. **There is a very popular tool by Van Hauser which can be used to brute force a series of services. What is the name of this tool?**

**Answer:** *hydra*

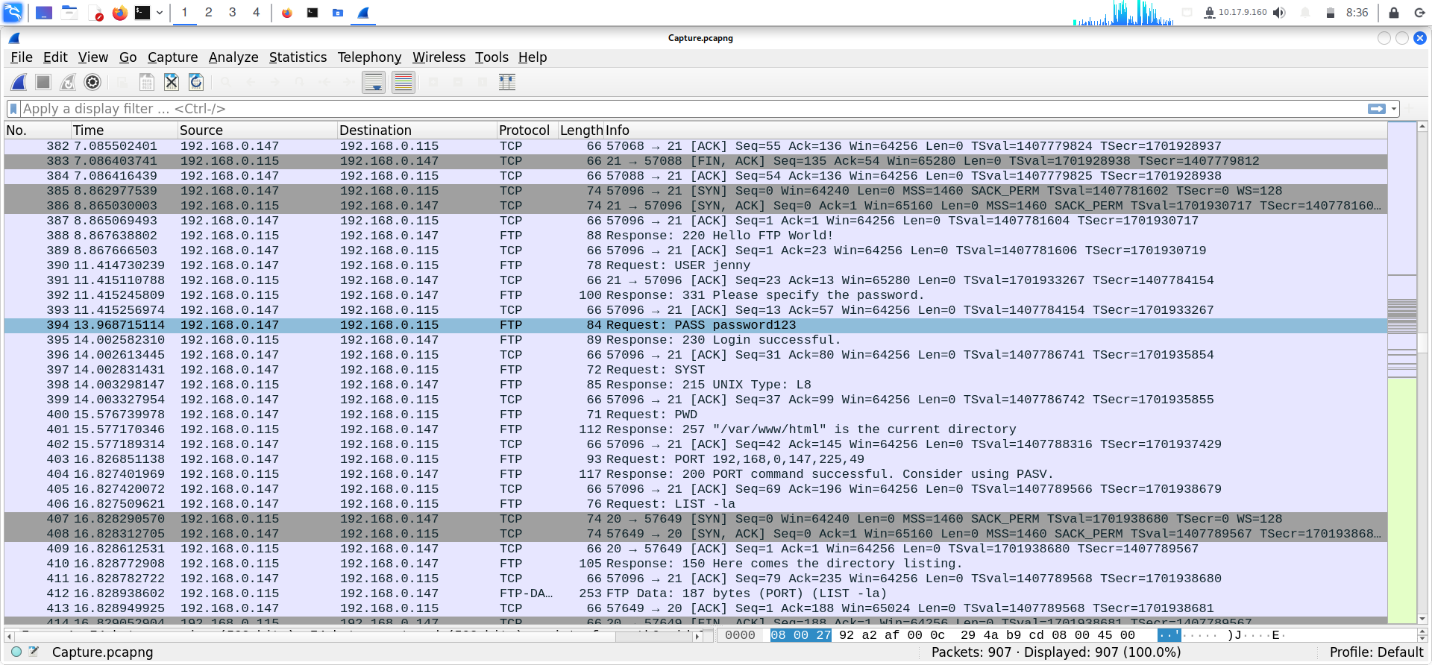
1. **The attacker is trying to log on with a specific username. What is the username?**

**Answer:** *jenny*



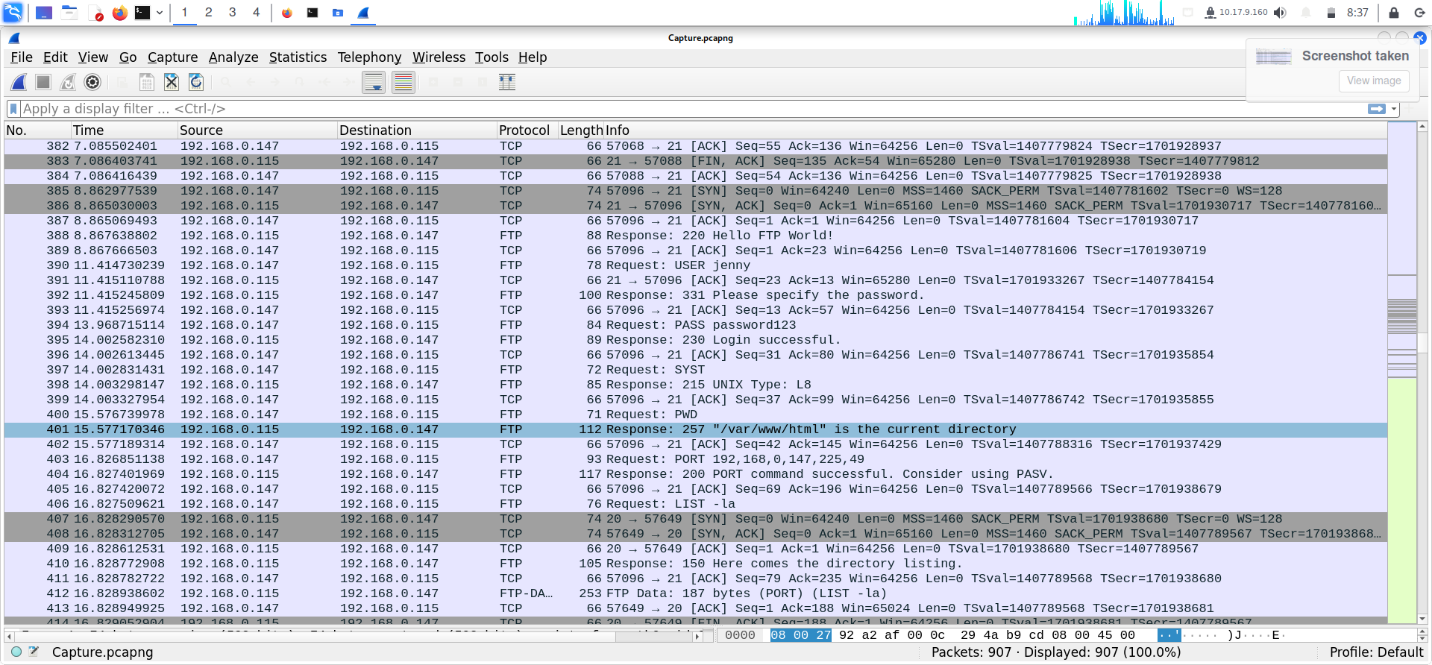
1. **What is the user’s password?**

**Answer:** *password123*



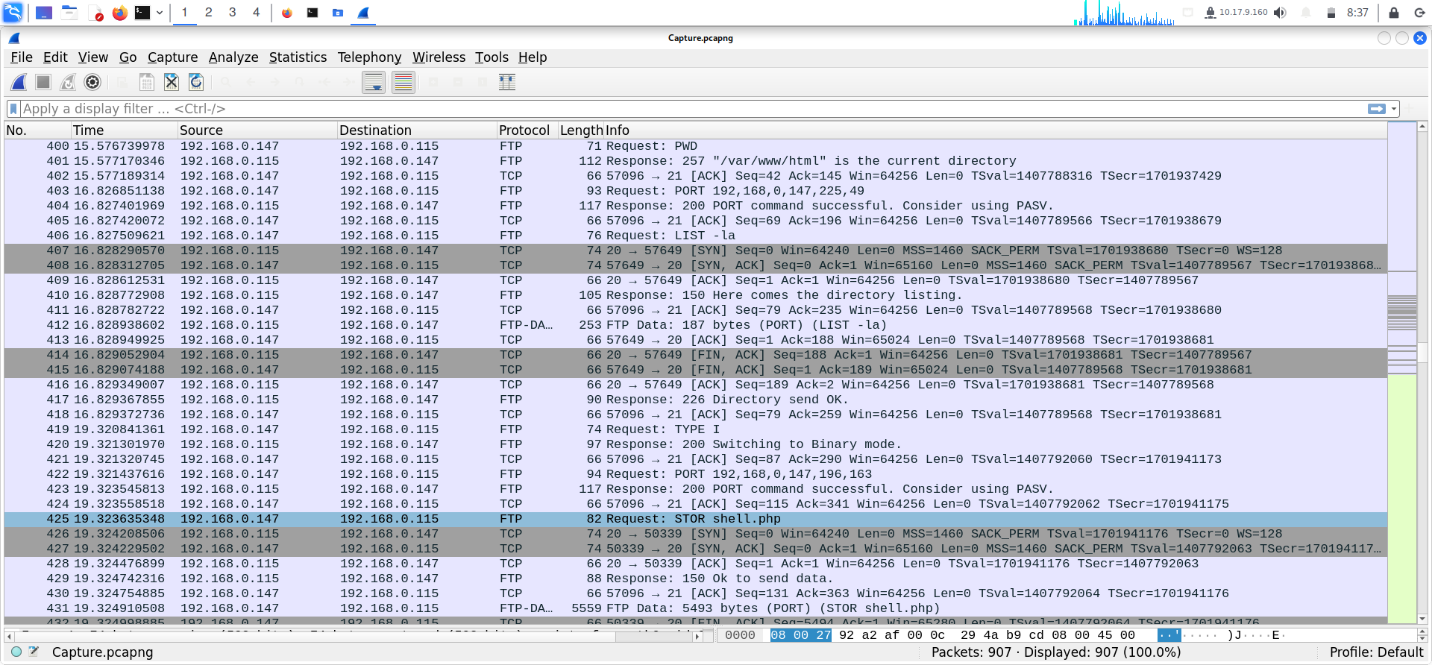
1. **What is the current FTP working directory after the attacker logged in?**

**Answer:** */var/www/html*



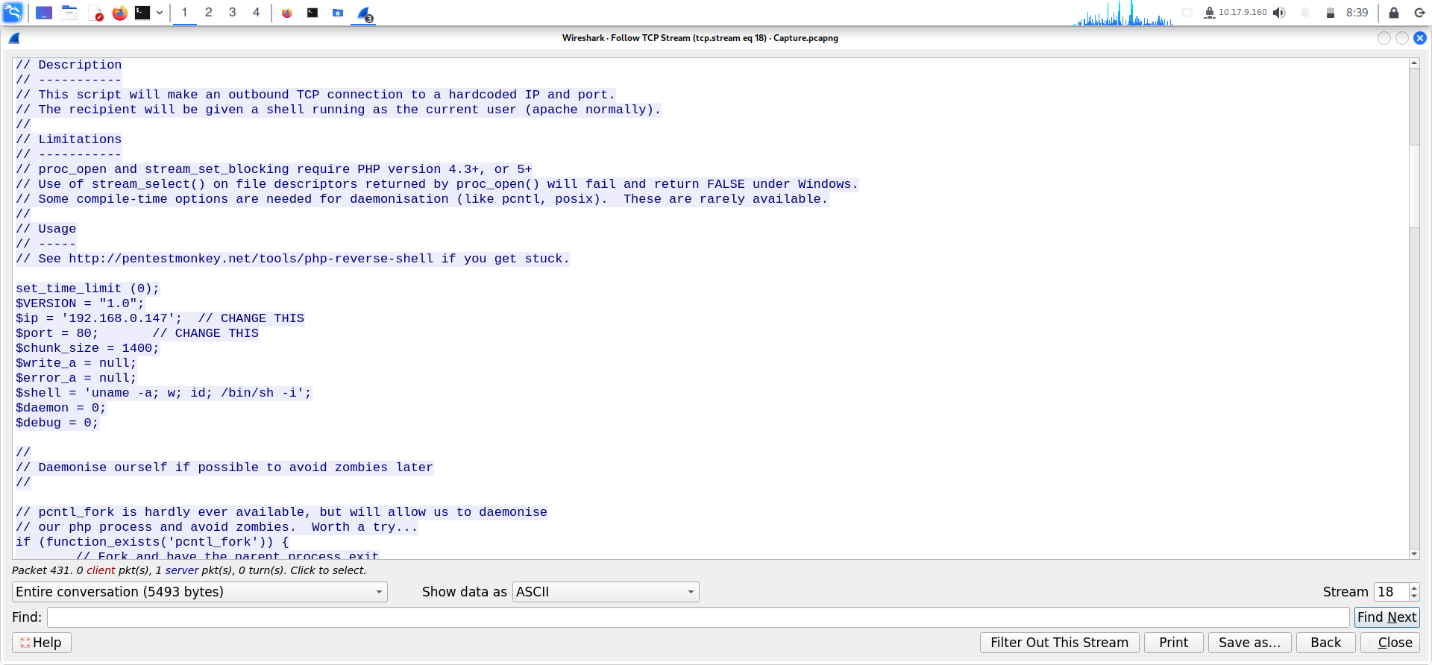
1. **The attacker uploaded a backdoor. What is the backdoor’s filename?**

**Answer:** *shell.php*



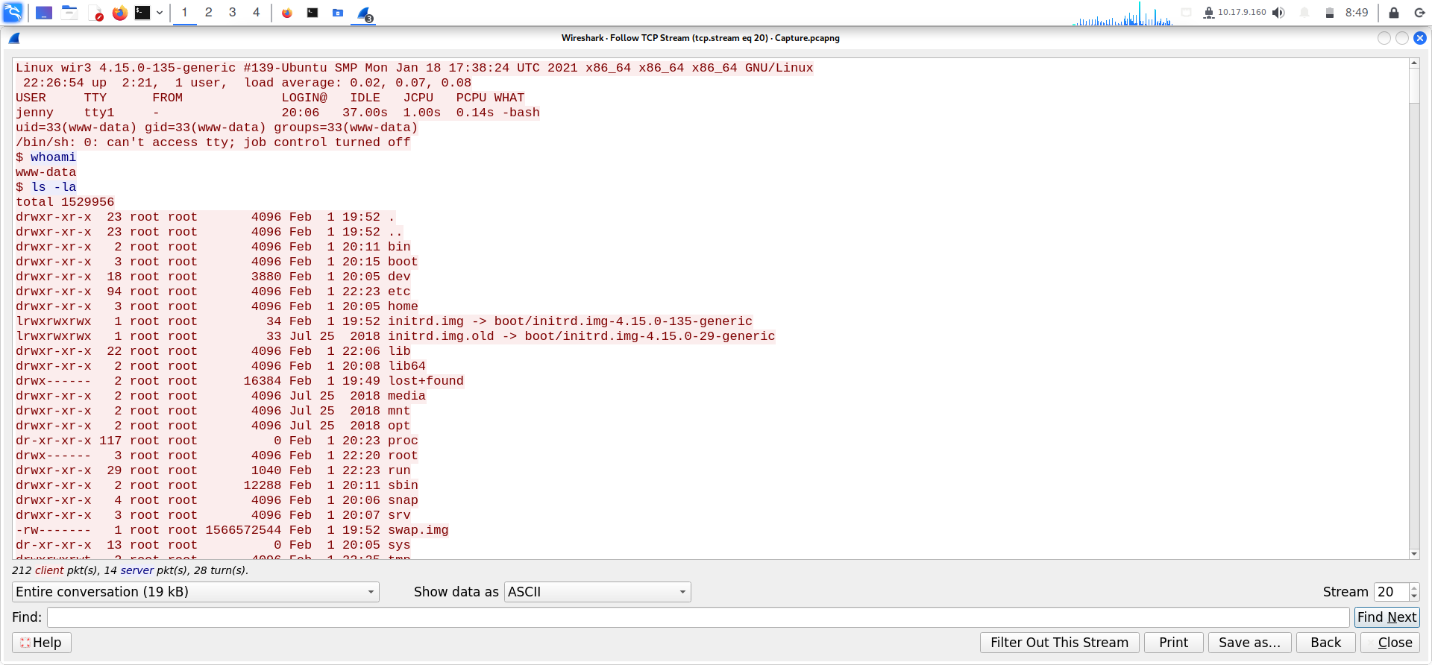
1. **The backdoor can be downloaded from a specific URL, as it is located inside the uploaded file. What is the full URL?**

**Answer:** [*http://pentestmonkey.net/tools/php-reverse-shell*](http://pentestmonkey.net/tools/php-reverse-shell)



1. **Which command did the attacker manually execute after getting a reverse shell?**

**Answer:** *whoami*

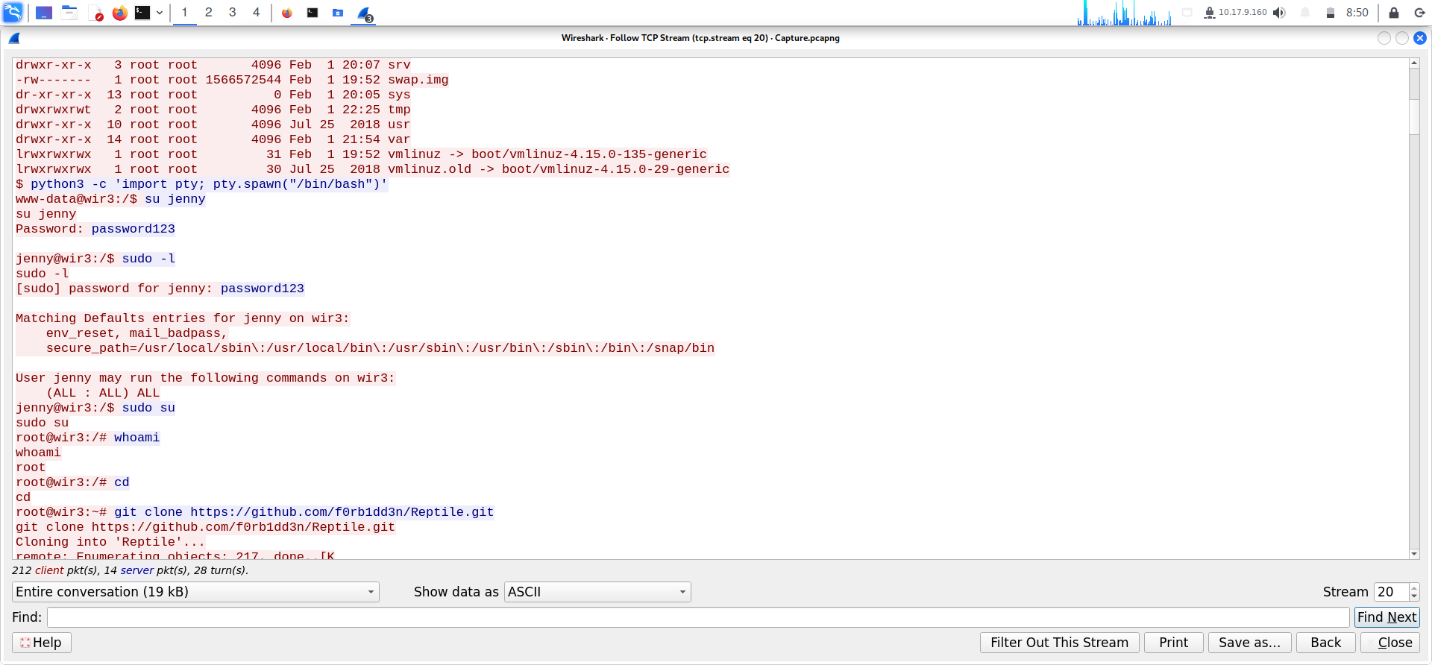


1. **What is the computer’s hostname?**

**Answer:** *wir3*

1. **Which command did the attacker execute to spawn a new TTY shell?**

**Answer:** *python3 -c ‘import pty; pty.spawn(“/bin/bash”)’*



1. **Which command was executed to gain a root shell?**

**Answer:** *sudo su*

1. **The attacker downloaded something from GitHub. What is the name of the GitHub project?**

**Answer:** *Reptile*

1. **The project can be used to install a stealthy backdoor on the system. It can be very hard to detect. What is this type of backdoor called?**

**Answer:** *rootkit*

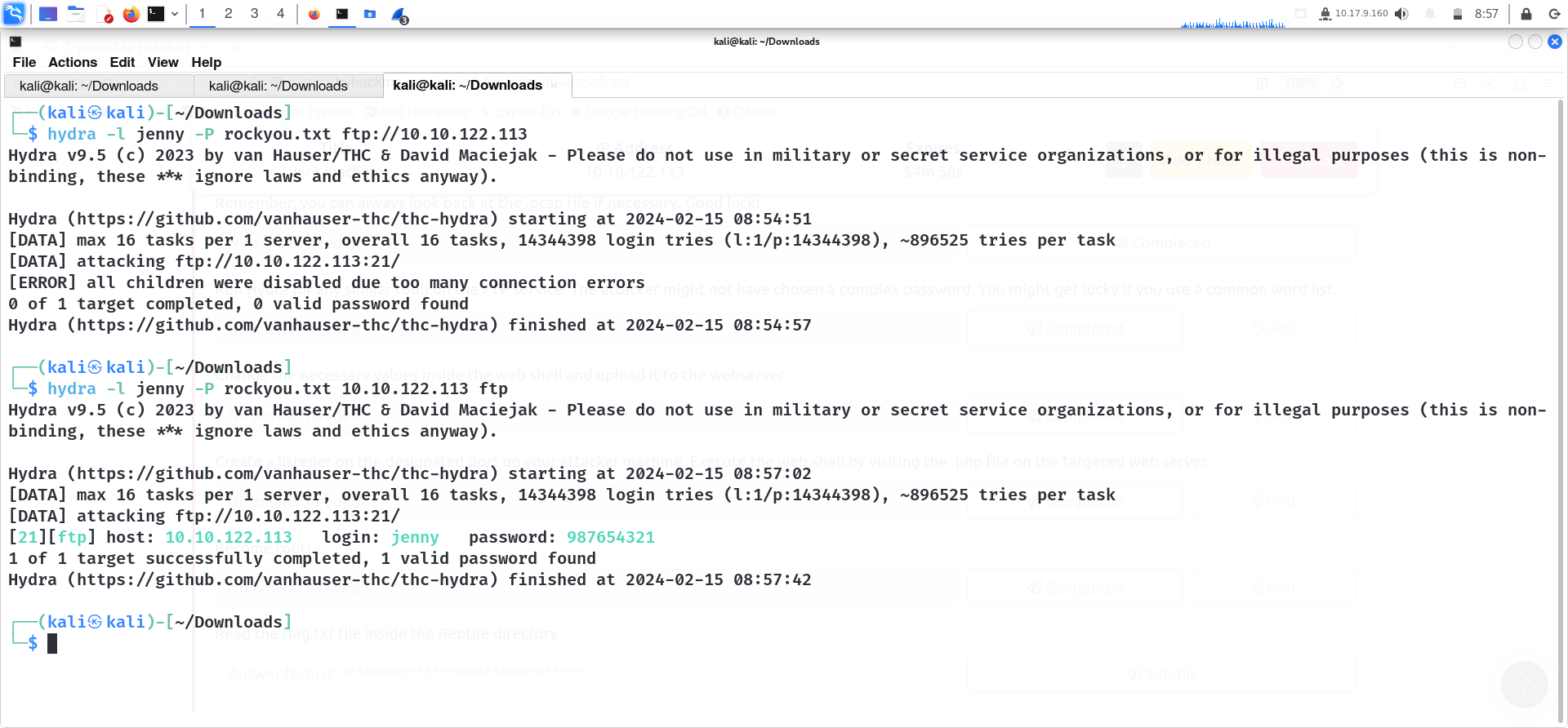
**TASK 2: Hack your way back into the machine.**

1. **The attacker has changed the user’s password! Can you replicate the attacker’s steps and read the flag.txt? The flag is located in the /root/Reptile directory. Remember, you can always look back at the .pcap file if necessary. Good luck!**

**Answer:** *No answer Needed*

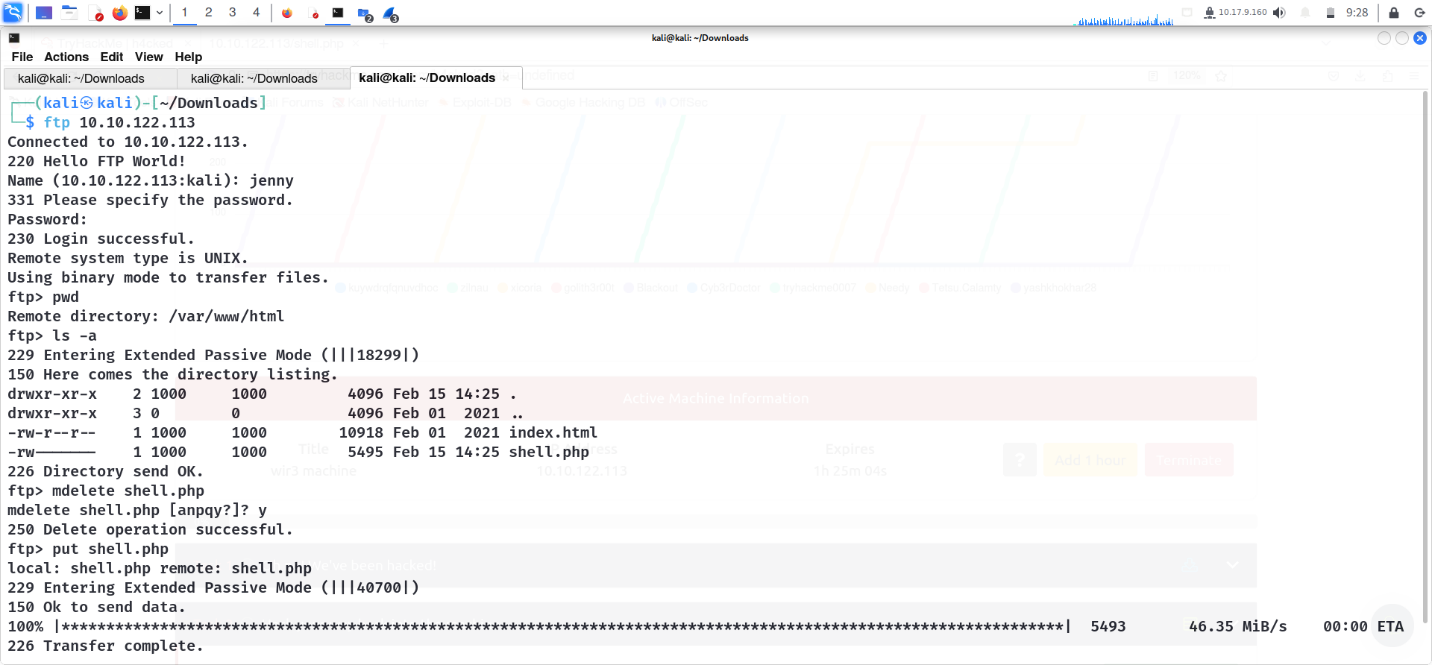
1. ***Run Hydra (or any similar tool) on the FTP service. The attacker might not have chosen a complex password. You might get lucky if you use a common word list.***

***Answer:*** *No answer Needed*



1. **Change the necessary values inside the web shell and upload it to the webserver.**

**Answer:***No answer Needed*



**Now we’ve successfully uploaded our shell. Now the important thing let’s start our netcat listener.**

1. **Create a listener on the designated port on your attacker machine. Execute the web shell by visiting the .php file on the targeted web server.**

**Answer:** *No Answer Needed*

Now we’re currently www-data let’s switch it to jenny.

Now let’s type sudo -l to see what we can run to switch to root user without password.

As you can see we can run anything. So we’all know to change your access from super user to root user we use sudo su. Let’s run it here.

We’re now root user.

1. **Become root!**

**Answer:** *No answer Needed*

1. **Read the flag.txt file inside the Reptile directory**

**Answer:** *ebcefd66ca4b559d17b440b6e67fd0fd*

