

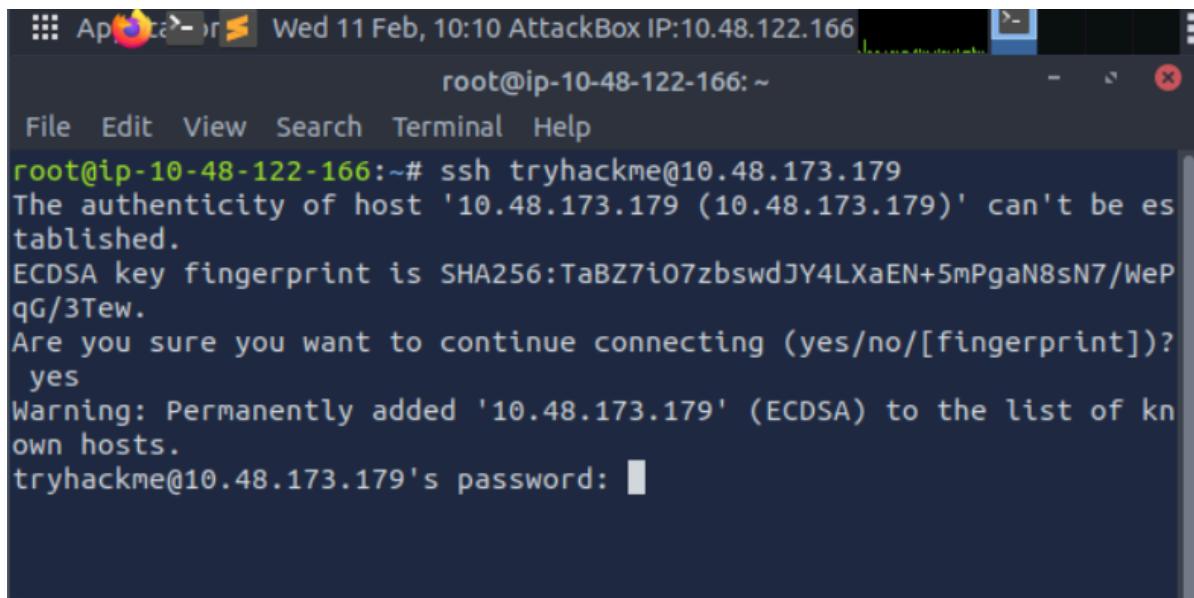
Room: Linux Fundamentals part 3 / Task-4

Objective: connecting to a pc remotely and flag capturing

Command used: ssh, cd, ls, scp, wget

Steps

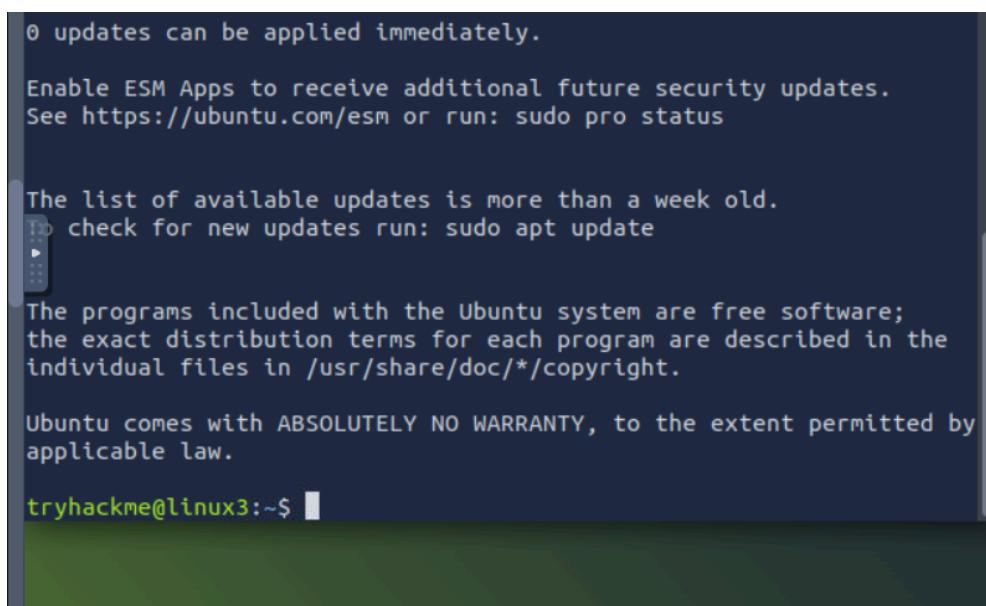
Firstly we have to connect to the machine we are attacking using the “ssh user@userIP” command and then enter the password of the user.



The screenshot shows a terminal window titled "root@ip-10-48-122-166:~". The user has run the command "ssh tryhackme@10.48.173.179". The system prompts for confirmation about the host's fingerprint, which the user accepts ("yes"). It then asks for the password of the target host ("tryhackme@10.48.173.179's password:").

```
root@ip-10-48-122-166:~# ssh tryhackme@10.48.173.179
The authenticity of host '10.48.173.179 (10.48.173.179)' can't be established.
ECDSA key fingerprint is SHA256:TaBZ7i07zbswdJY4LXaEN+5mPgaN8sN7/WePqG/3Tew.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
yes
Warning: Permanently added '10.48.173.179' (ECDSA) to the list of known hosts.
tryhackme@10.48.173.179's password:
```

After enter the password (given in the task which is “tryhackme”) we will see something like this:



The screenshot shows the output of the "sudo apt update" command. It displays information about available updates, ESM support, and the license for the Ubuntu software.

```
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

tryhackme@linux3:~$
```

Now our goal is to download the flag.txt from the remote pc (tryhackme) by running the server.

```
tryhackme@linux3:~$ ls  
task3  
tryhackme@linux3:~$ python3 -m http.server  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...  
192.168.184.250 - - [11/Feb/2026 10:43:09] "GET /.flag.txt HTTP/1.1" 200 -  
[
```

Then we just have to download the file using the “wget sourceaddress” command.

```
[(saif㉿kali)-~]$ wget http://10.48.173.179:8000/.flag.txt  
--2026-02-11 05:43:10-- http://10.48.173.179:8000/.flag.txt  
Connecting to 10.48.173.179:8000... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 20 [text/plain]  
Saving to: '.flag.txt.2'  
  
.flag.txt.2 100%[=====] 20 --.-KB/s in 0s  
2026-02-11 05:43:10 (3.14 MB/s) - '.flag.txt.2' saved [20/20]  
  
[(saif㉿kali)-~]$
```

Now that we have the file in our pc, we can easily check the content of the file. Since it is a .txt file we can print all data from it using the “cat filename” command.

```
[(saif㉿kali)-~]$ wget http://10.48.173.179:8000/.flag.txt  
--2026-02-11 05:43:10-- http://10.48.173.179:8000/.flag.txt  
Connecting to 10.48.173.179:8000... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 20 [text/plain]  
Saving to: '.flag.txt.2'  
  
.flag.txt.2 100%[=====] 20 --.-KB/s in 0s  
2026-02-11 05:43:10 (3.14 MB/s) - '.flag.txt.2' saved [20/20]  
  
[(saif㉿kali)-~]$ cat .flag.txt  
THM{WGET_WEB SERVER}  
[(saif㉿kali)-~]$
```