**ASSIGNMENT 14**

**STEPS PERFORMED ON STARTUP CTF AND LINUX FUNDAMENTAL’S PART 2**

# **INDEX**

|  |  |  |
| --- | --- | --- |
| **SL NO** | **TOPIC** | **PAGE NO** |
| 1. | Summary report on different steps performed on Startup Ctf | 2-7 |
| 2. | Summary report on different steps performed on Linux Fundamentals Part 2 | 8-9 |

# **Topic: STEPS PERFORMED ON STARTUP CTF AND LINUX FUNDAMENTAL’S PART 2 (TRYHACK ME)**

ASSIGNMENT 14(DAY 16) Date:14-07-2022

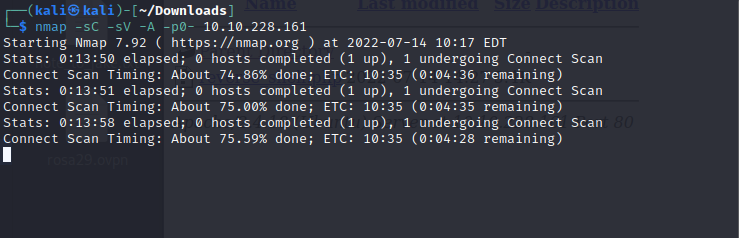
1. **Summary report on different steps performed on Startup CTF**

**Step 1:**

**Startup room was solved today on tryhackme. At first, the machine was started and we copied the IP Address which was provided by Tryhackme for port scanning then we opened the attack box.**

**Step 2:**

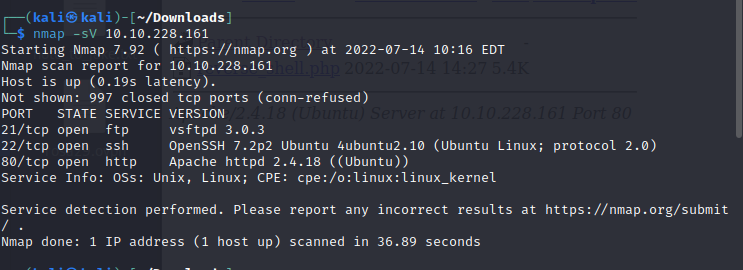
**Initially we created a folder name Startup in the desktop, and inside that folder we created 2 more folder as Web and Nmap. Then on the terminal in order to port scan we used the command nmap -sC -Sv -A -p0- 10.10.228.161. And we obtained the following results.**



**Step 3:**

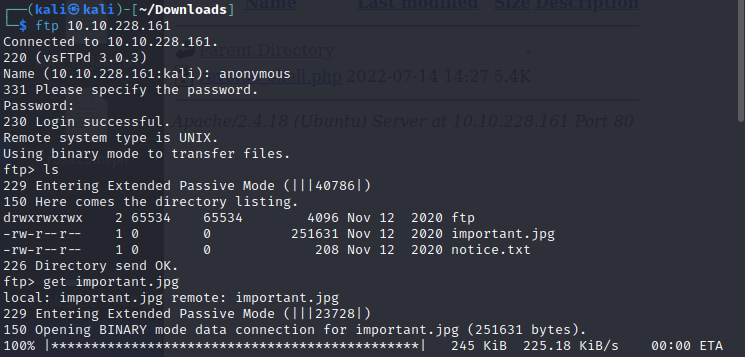
**Then we again performed another scan using command nmap -sV 10.10.228.161**

**and we got the following results.**



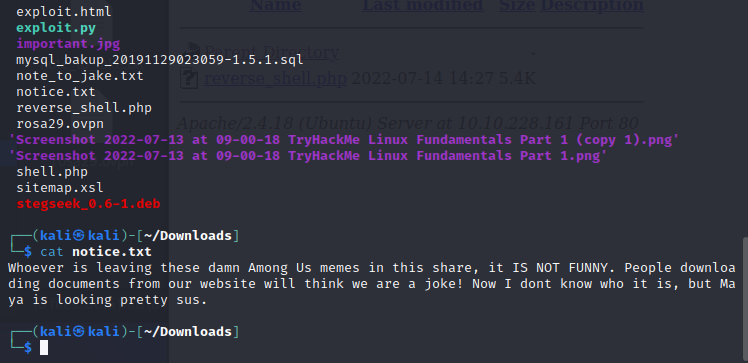
**Step 4:**

**In the previous nmap scan we found that the 21,22,80 ports are open, and there was an anonymous ftp so another scan was done to check for anonymous** [**ftp. For**](ftp://ftp.For) **this we used the command ftp 10.10.228.161. And here the username was anonymous. We found that anonymous ftp is available on this site.**



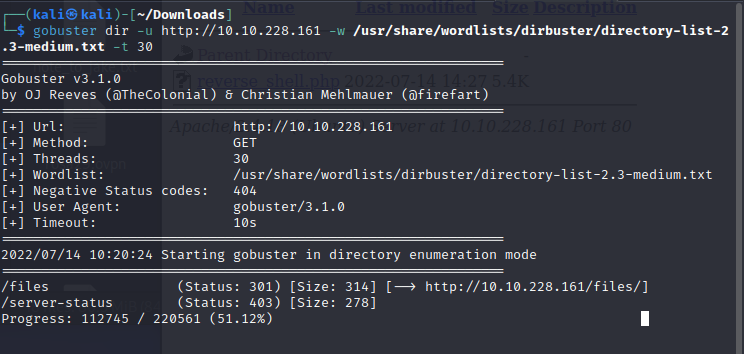
**Step 5:**

**The ftp which we got in the previous scan is a directory so we transferred the files as ‘notice.txt’ and ‘important.jpg’. We found that Important.jpg is an image file and is a meme so using cat command as cat notice.txt we displayed the contents of the notice.txt and we got the following results.**



**Step 6:**

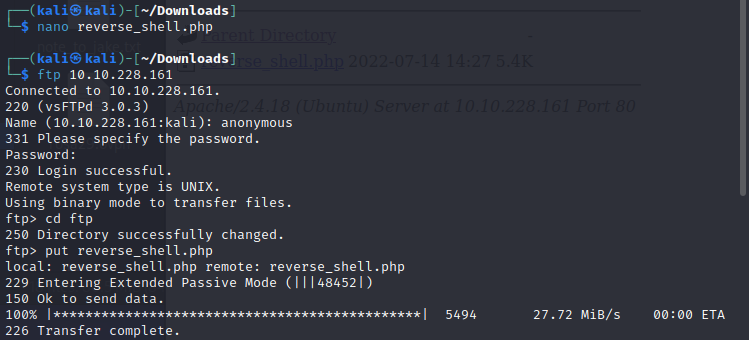
**Then we performed gobuster scan with the command dir -u http://** **10.10.228.161-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30 in order to find more about directories.**



**After the scan we found that there are two directories’ files and server-status which is not accessible. But the files directory has important.jpg, parent directory, notice.txt and an ftp directory.**

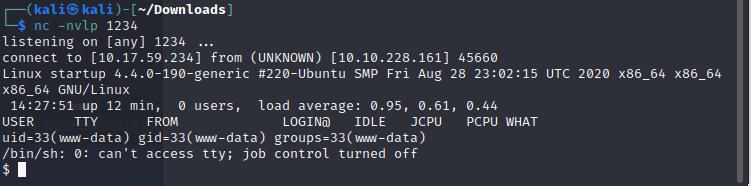
**Step 7:**

**Then nano command as nano reverse\_shell.php and the code for reverse shell from GitHub was run. After that ftp connection was made and the file was transferred.**



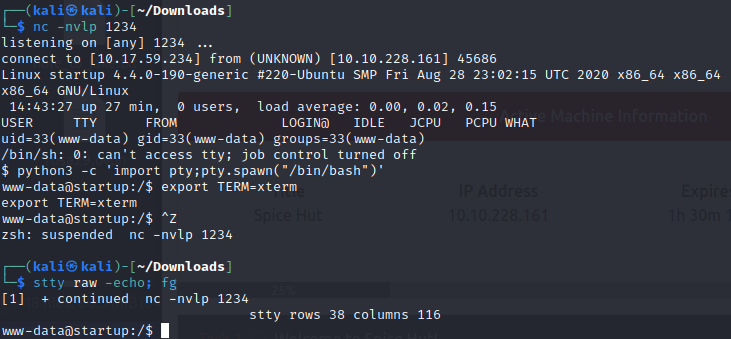
**Step 8:**

**In order to connect with the user, we used nc -nlvp 1234 command and made a connection.**



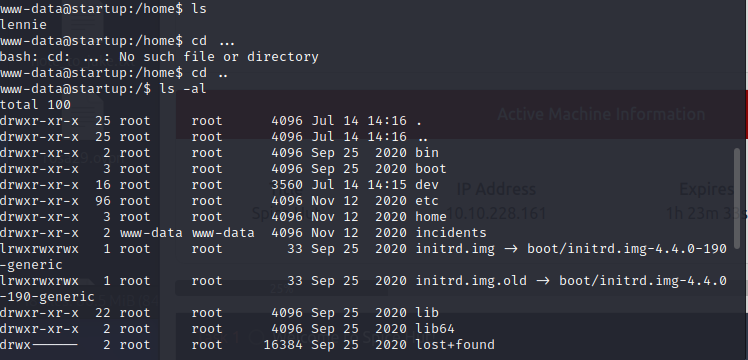
**Step 9:**

**Then in order to stabilize the reverse shell the following command were run.**



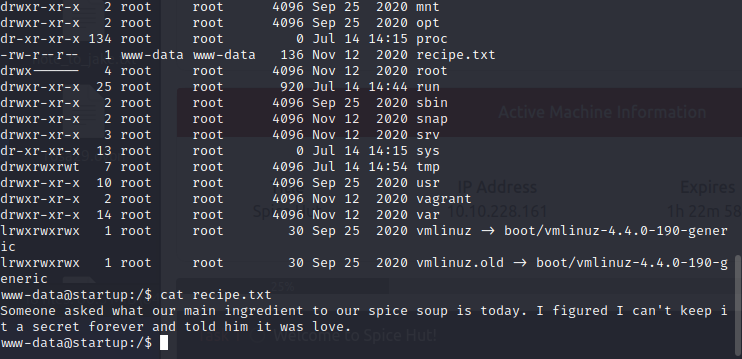
**Step 10:**

**Then we got into the home directory and got the username as Lennie and using the command ls -al we got the following results.**



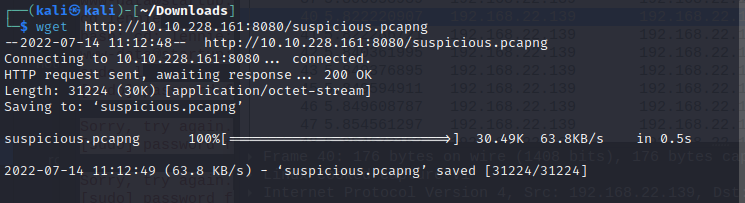
**Step 11:**

**Then with the help of cat command we got contents of the reciepe.txt file.**



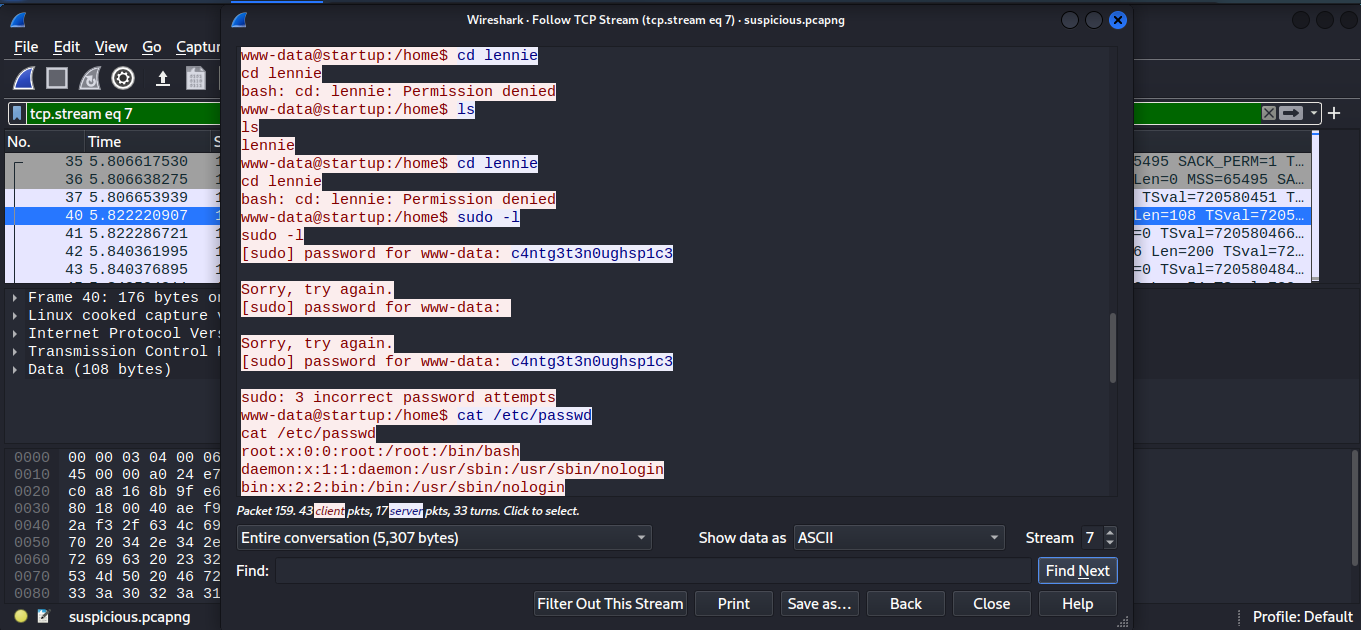
**Step 12:**

**Then we got a file as suspicious.pcanpng so we downloaded the file and then opened it in wireshark using command wget http:// 10.10.228.161:8080/suspiciois.pcapng.**



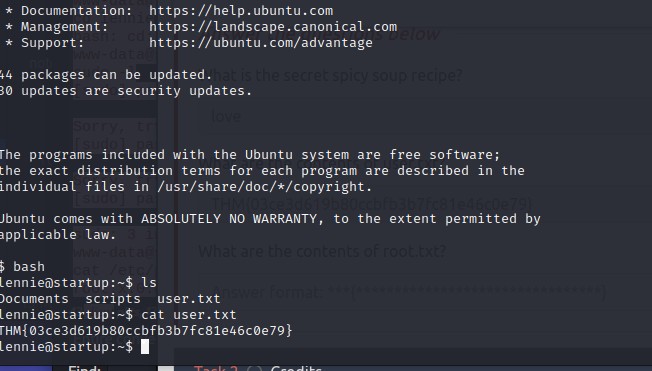
**Step 13:**

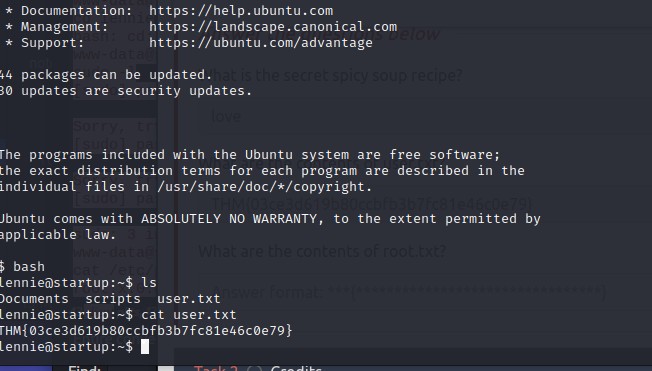
**Then by using Wireshark we opened the downloaded file and did the tcp stream. After the tcp stream we got the username and password.**



**Step 14:**

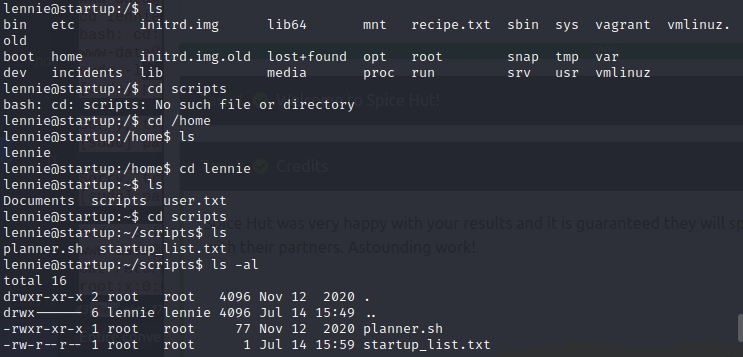
**Then we logged in and got all the directories and files present in it.We also got the user flag from user.txt file.**

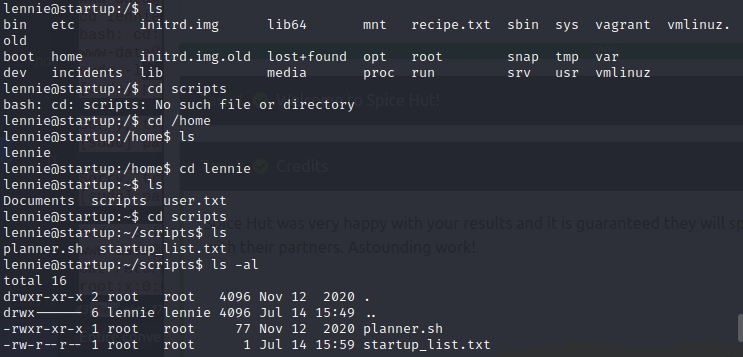




**Step 15:**

**Then we got into the root and found the root.txt and there we got the root flag.**

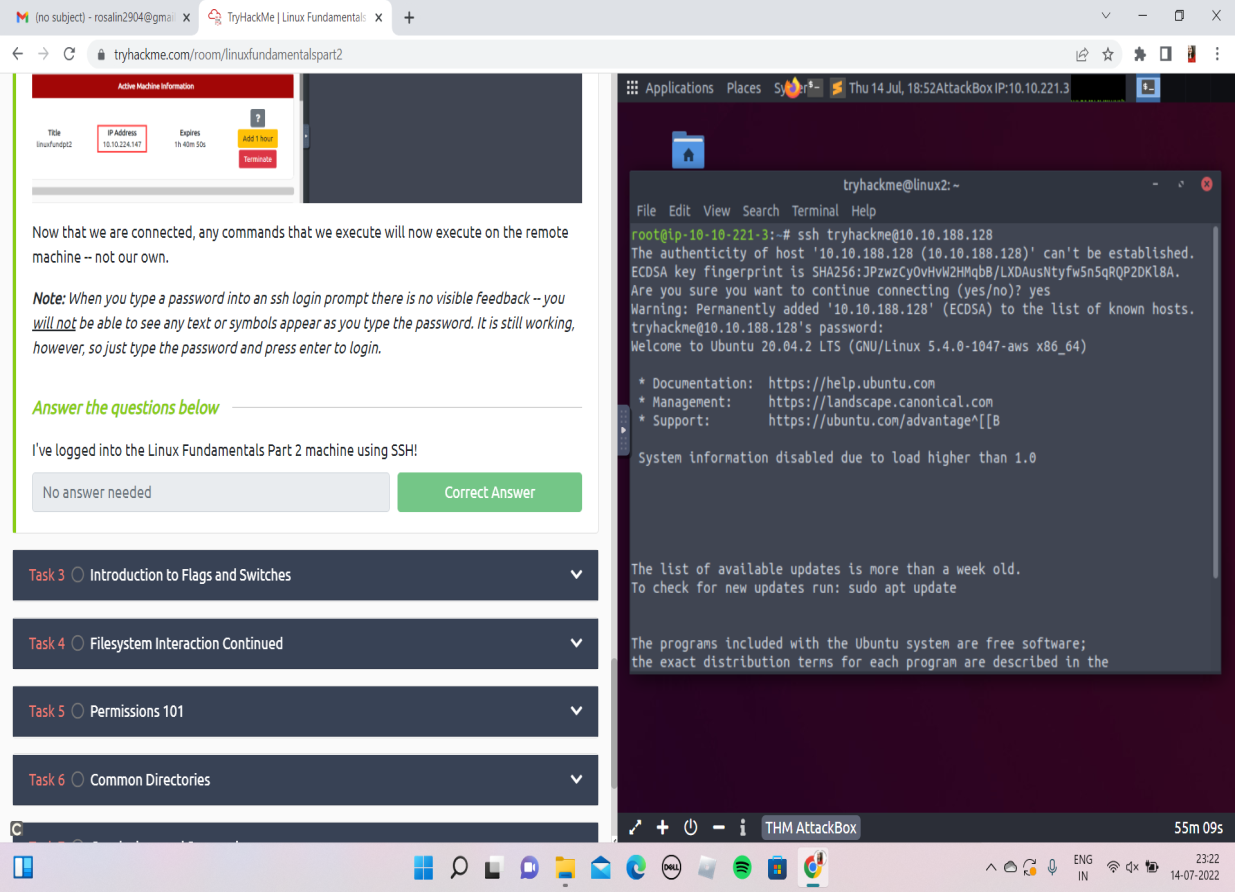




1. **Summary report on different steps performed on Linux Fundamentals Part 2.**

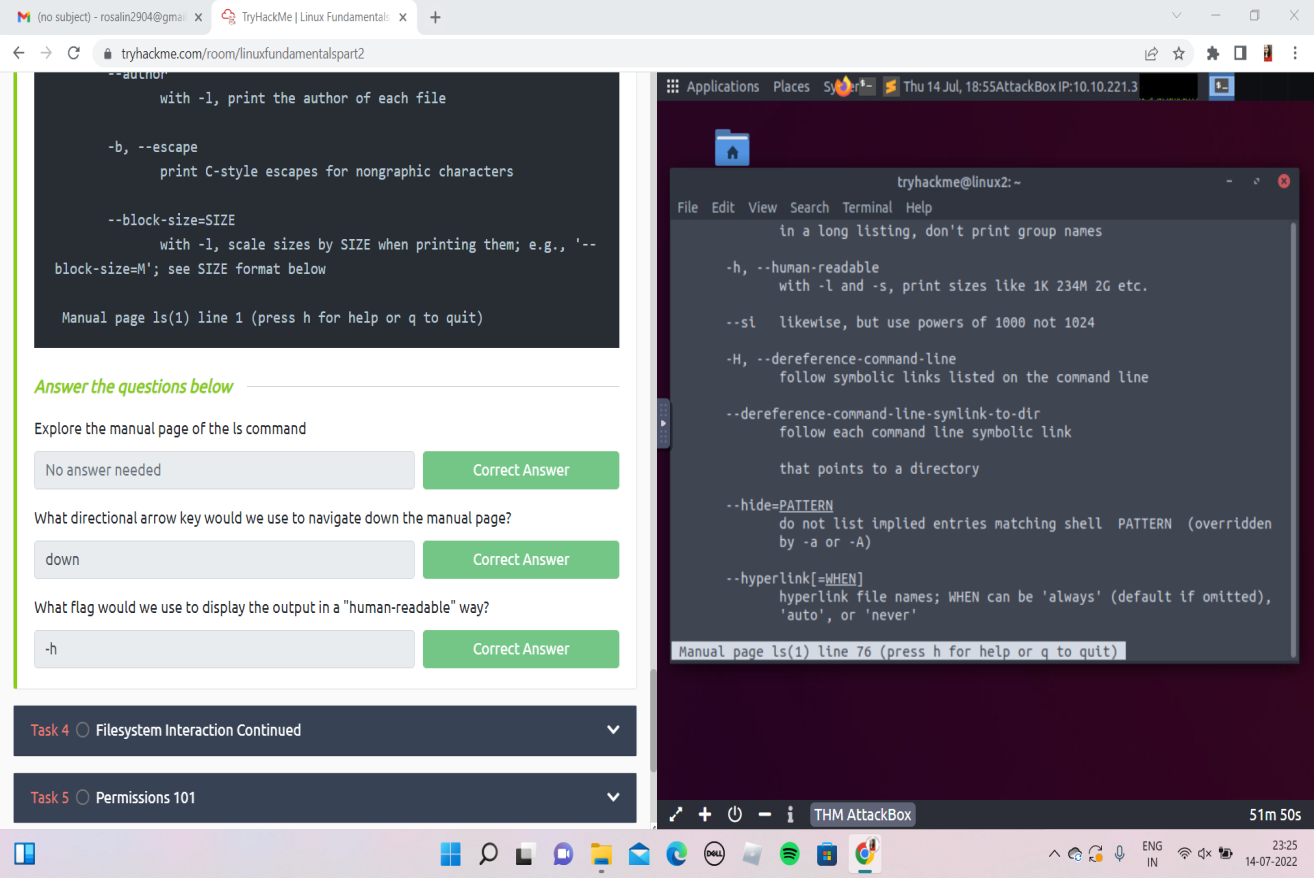
**Step 1:**

**Here we used ssh command.**

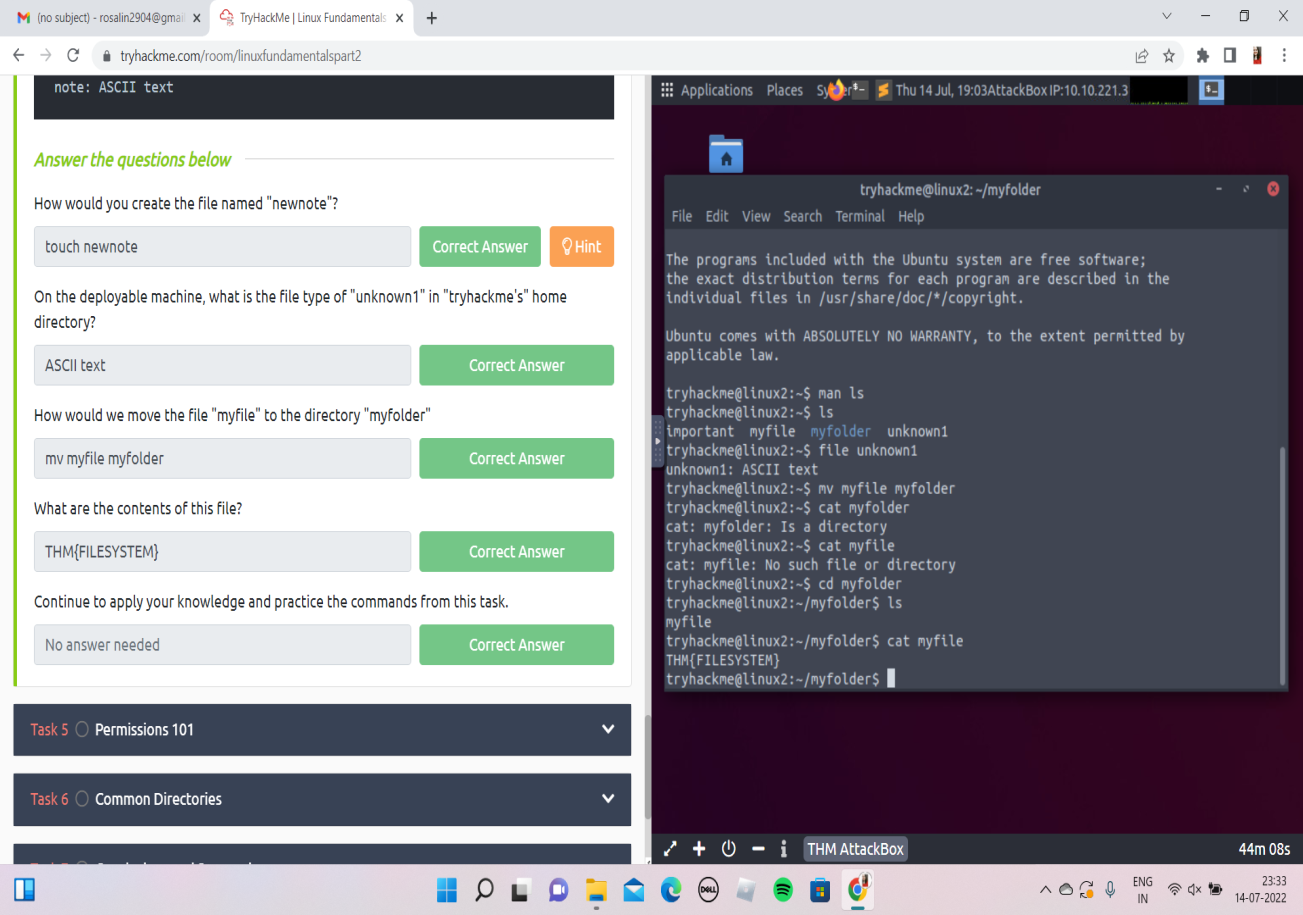


**Step 2:**

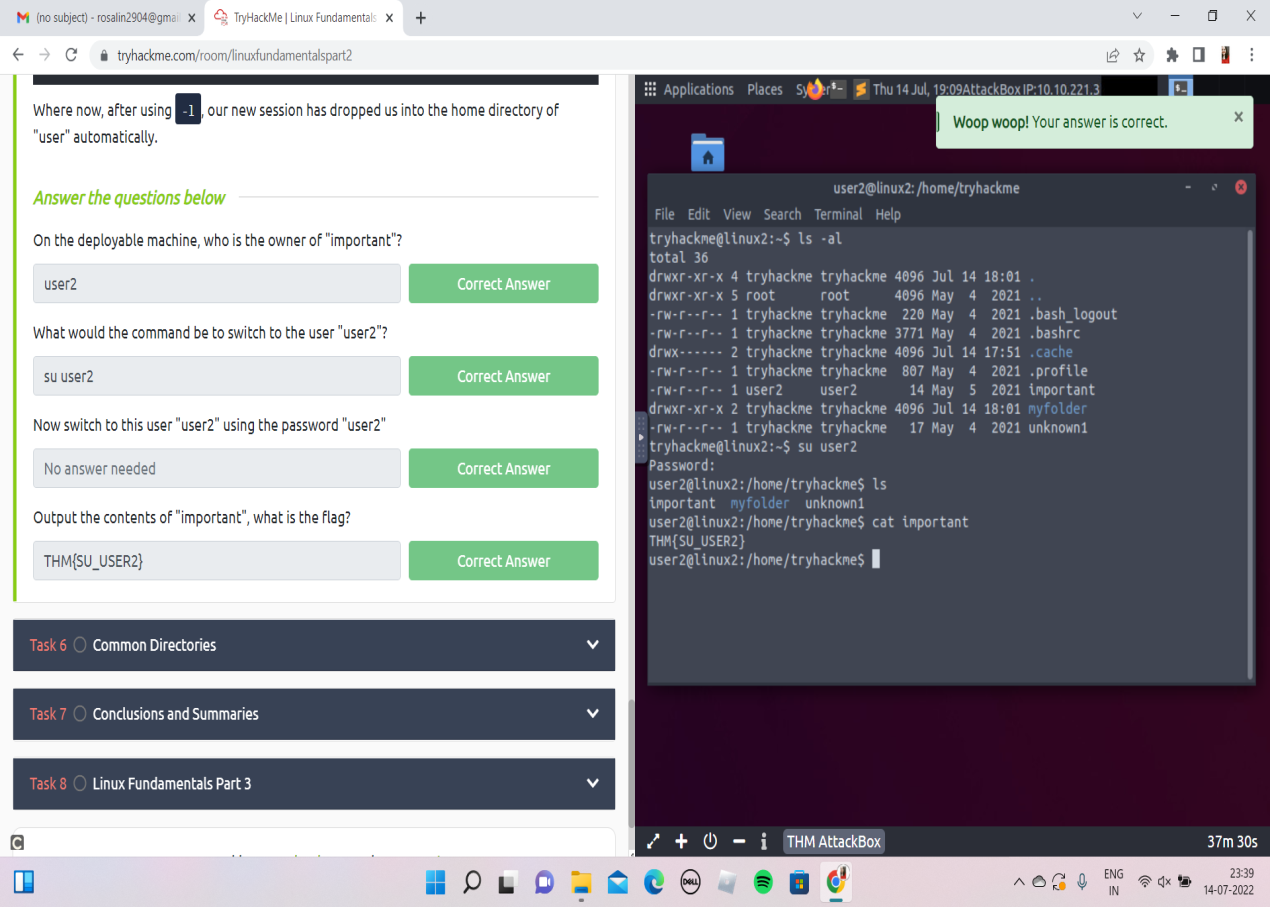
**Here we used man ls command.**



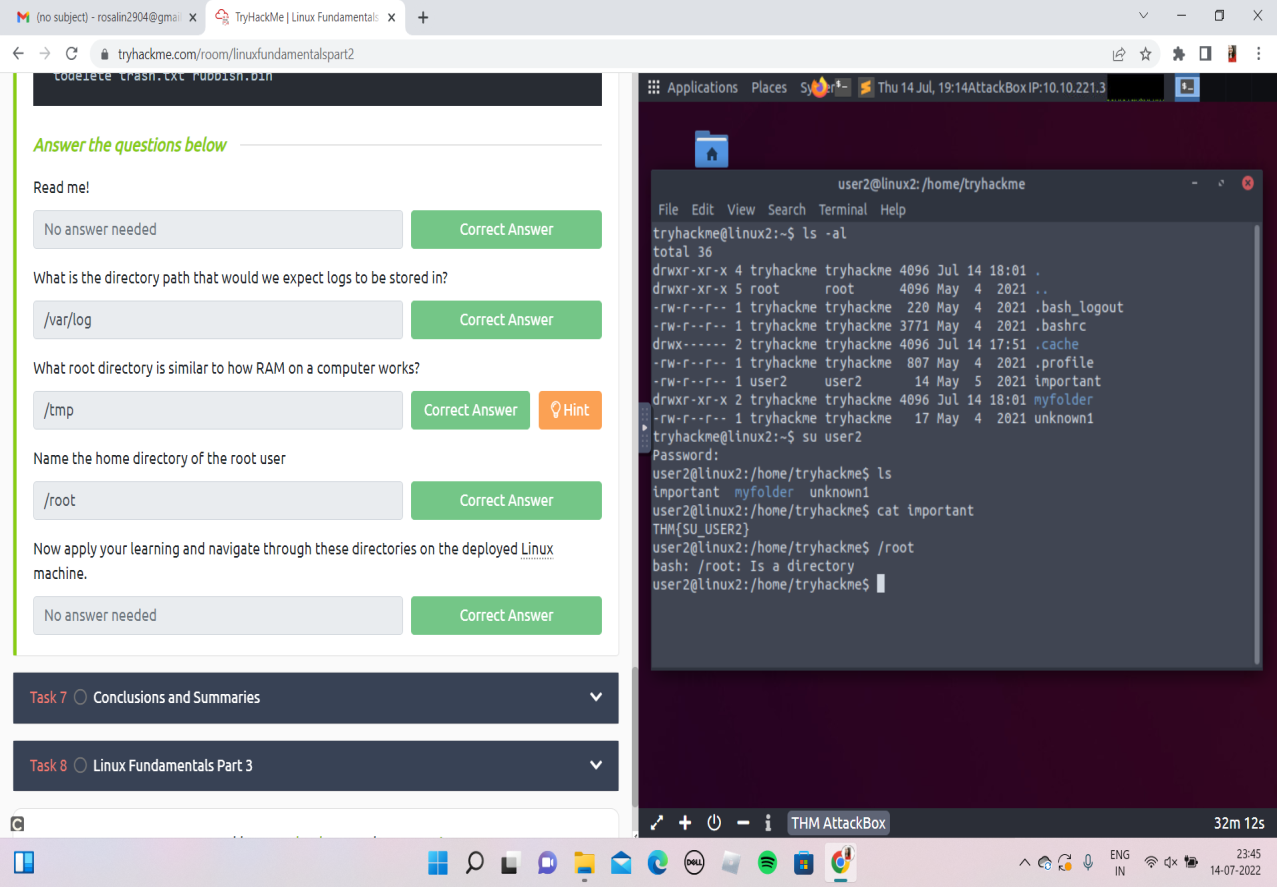
**Step 3:**



**Step 4:**



**Step 5:**



**NAME: I PRASANTI**

**SIC: 20BCEA56**

**BRANCH: CEN**