PSP0201
Week 4
Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

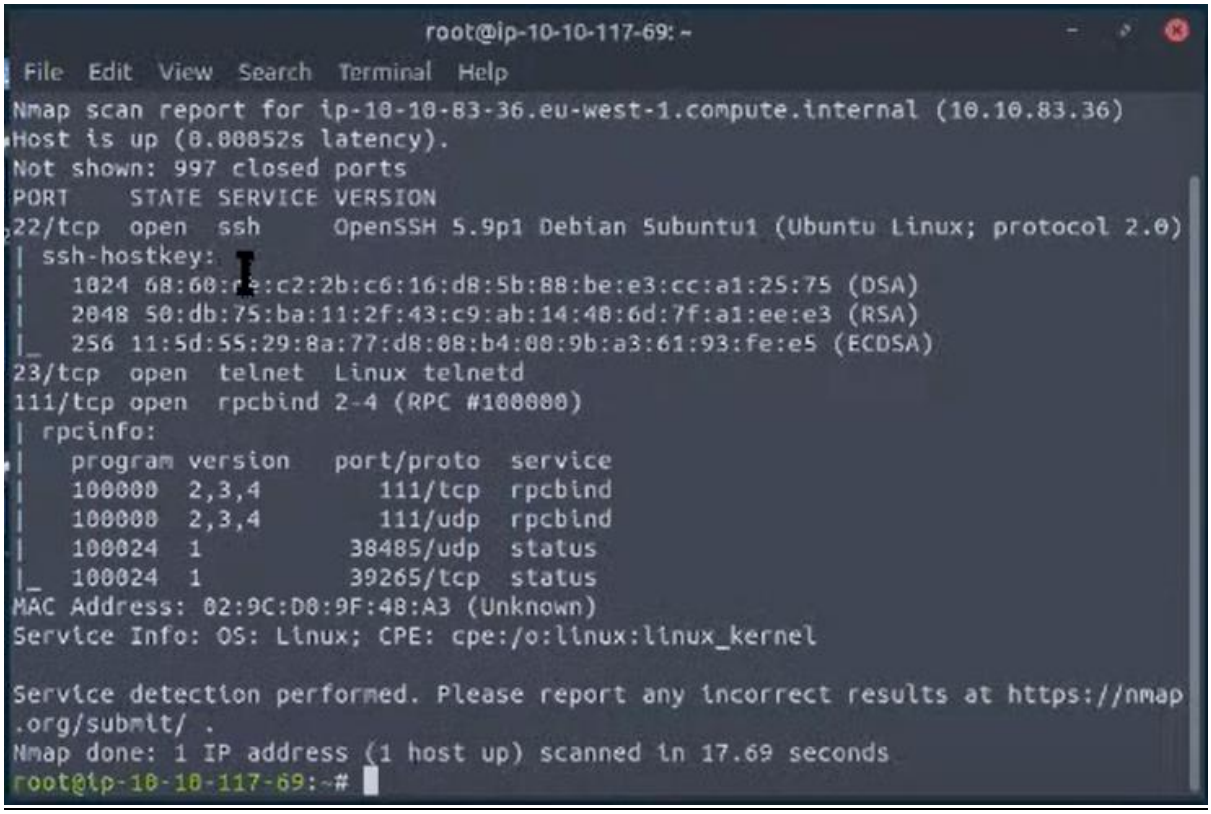
Day 13: Networking – Coal for Christmas

Tools used: Attackbox, Firefox, Virtualbox

Solution/walkthrough:

Question 1

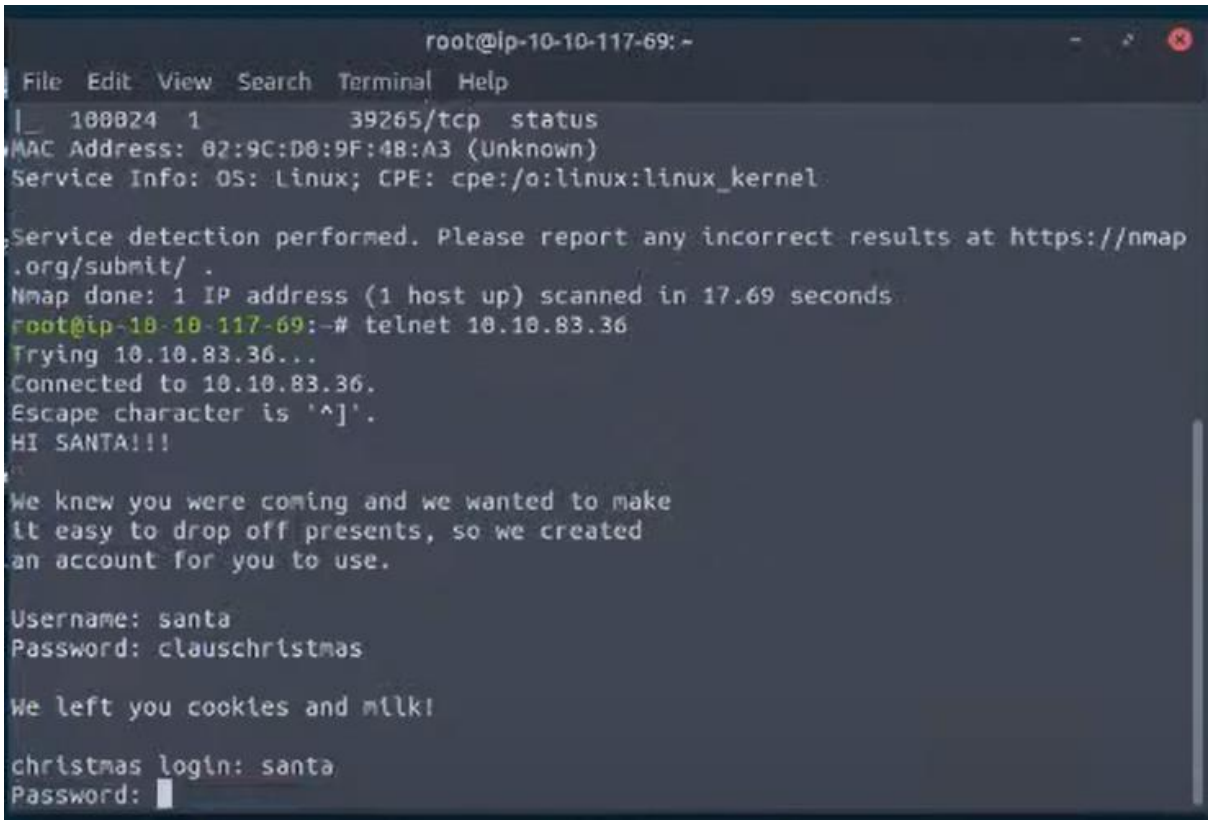
There are 3 ports opened. We have to check on the rcp and rpc.



Telnet is the old, deprecated protocol and service that is running.

Question 2

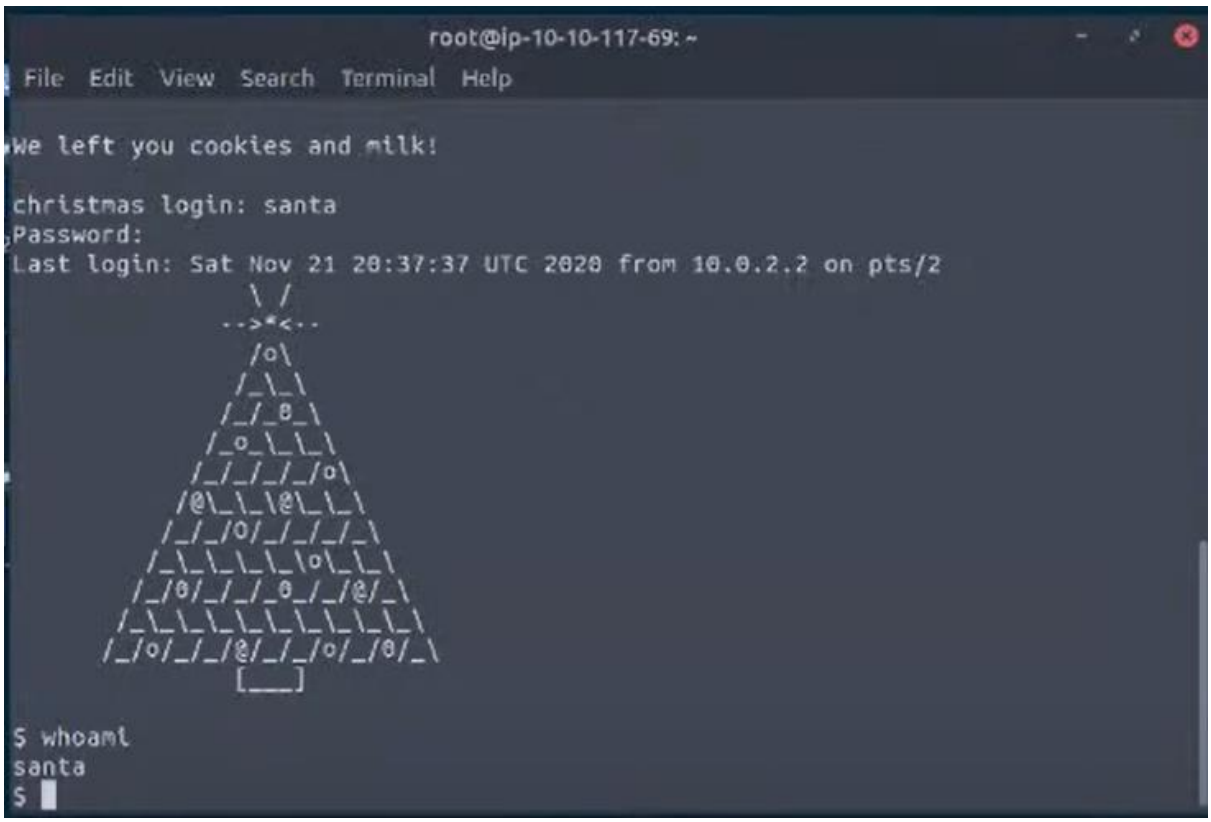
Go to telnet into the machine by using port 23. It shows us the login information such as username and password.



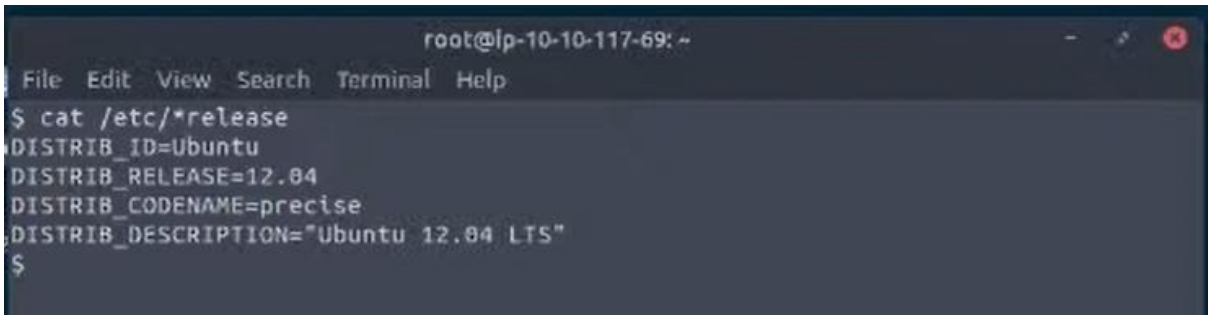
The credential left for us is clauschristmas.

Question 3

Use the ssh santa@10.10.22.241 by typing the username and password.



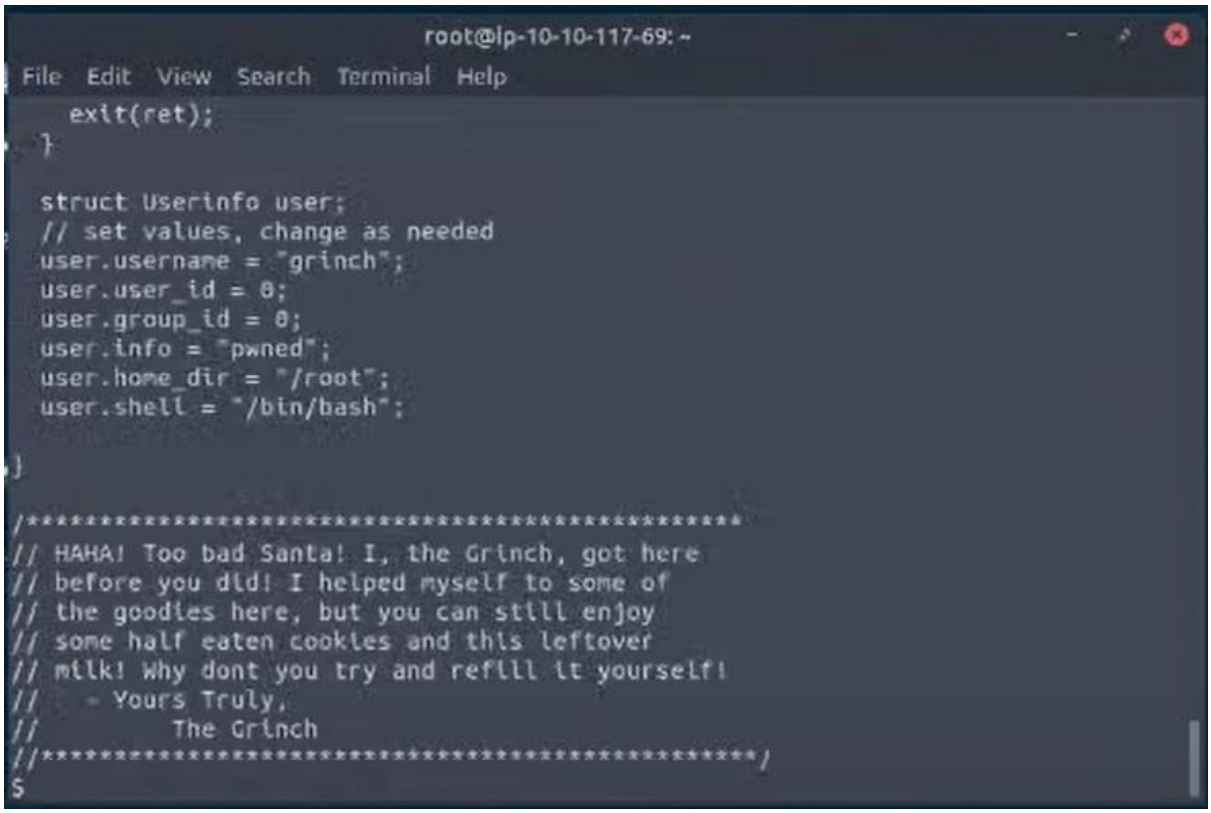
Find the version number of the server by using the 'cat/etc/*release' command.



The distribution of Linux and the version number is this server running is Ubuntu 12.04.

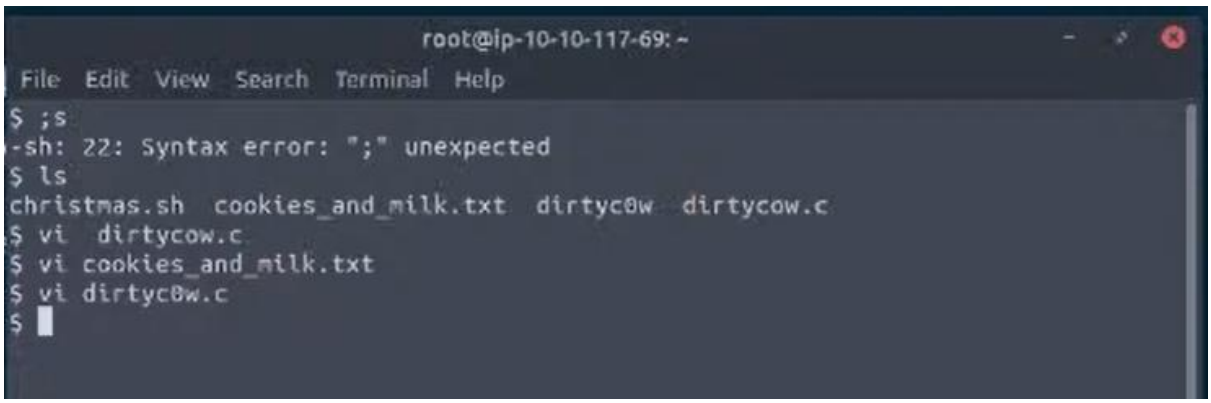
Question 4

By using ‘cat cookies_and_milk.txt’ command, we discover that the grinch was the one who got here first.



Question 5

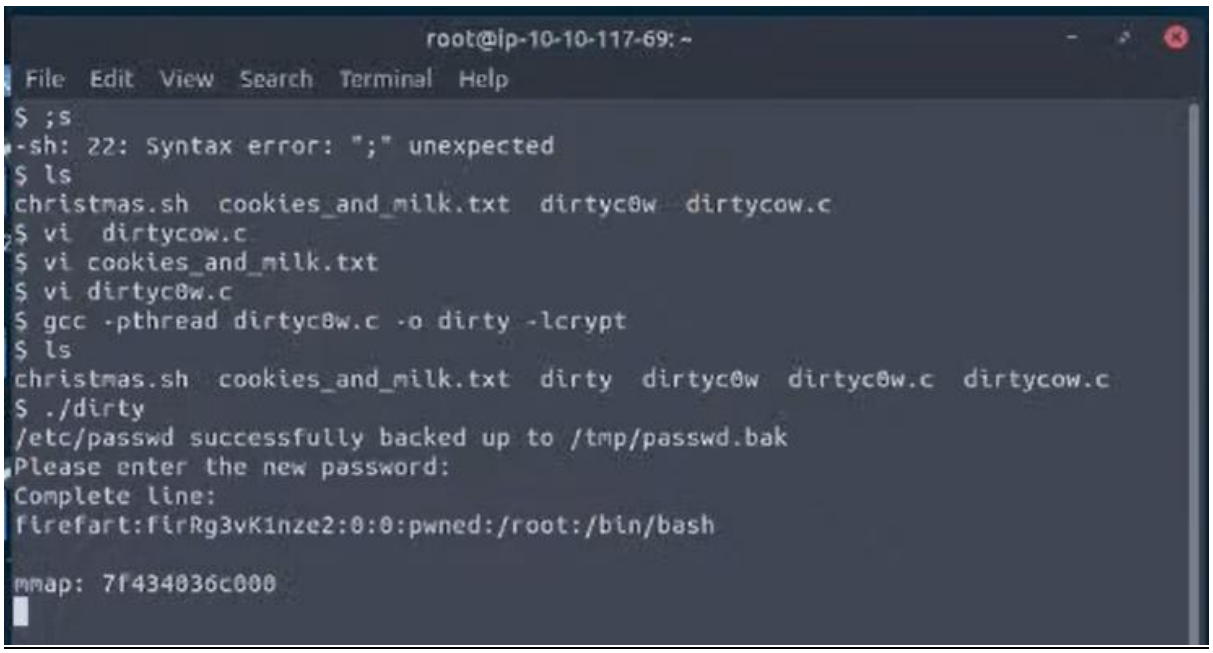
The syntax for compiling the exploit c file can be seen in the comment section of the script.



Thus, the verbatim syntax used is gcc -pthread dirty.c -o dirty -lcrypt.

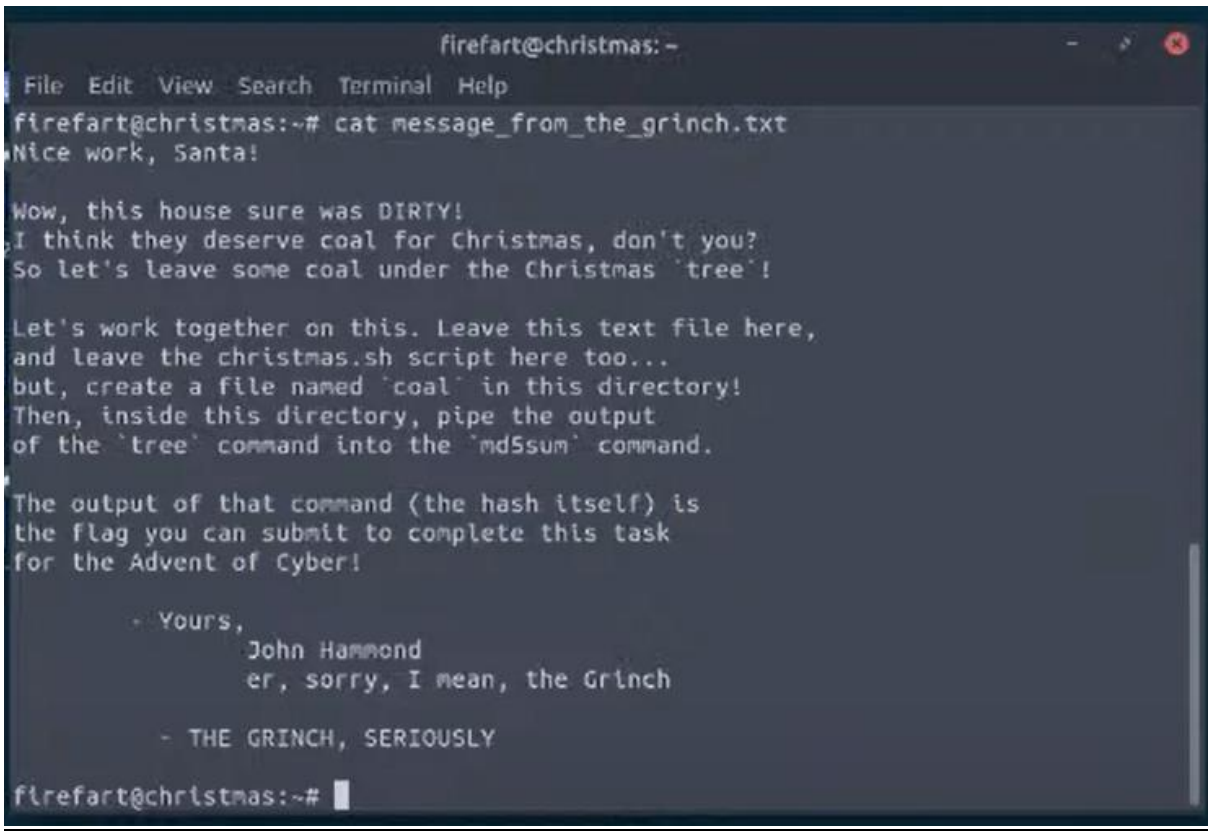
Question 6

The new username created is firefart.

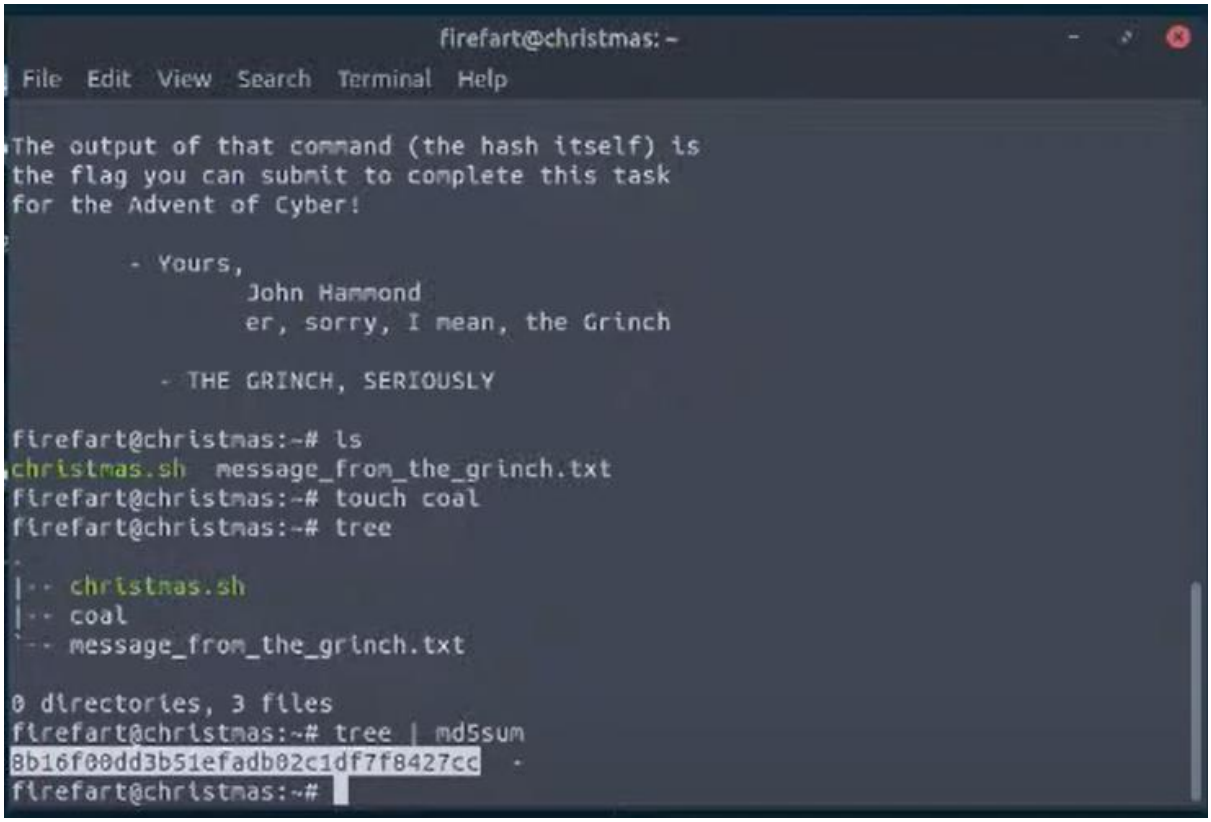


Question 7

Switch the accounts and look at what's in the directory. There was a text file. We display the content of the text file with cat command then follow the instructions written inside.



After leaving the coal behind, run the md5sum tree.



We can clearly see that the MD5 hash output is given.

Question 8

From the tryhackme page, we can see that the CVE for DirtyCow is (CVE-2016-5195)

Thought Process/Methodology:

There were 3 ports open. We needed to check rcp and rpc. Thus, the telnet is an old, obsolete protocol and service that is running. We went to telnet into the machine using port 23. It showed us login information such as username and password. The remaining credentials for us are clauschristmas. We achieved vertical escalation with the 'ssh santa@10.10.22.241' command with the username and password that we secured earlier. Then, we found the server version number. The Linux distribution and version number that this server is running on is Ubuntu 12.04. By reading the cookies_and_milk.txt file with the cat command, we knew that the grinch was the one who got here first. The syntax for compiling the exploit c file can be seen in the comments section of the script. Therefore, the verbatim syntax used is gcc -pthread dirty.c -o dirty -lcrypt. The new username created is firefart from the default operations of the real C source code. This username was written in the comment under the real C source code. We switched the accounts with the new username. After that, we checked what is in the directory where we found a text file which was a message left from the grinch. We display the content with cat command and follow the instructions given under it. After leaving the coal, run the md5sum tree. We can clearly see that the MD5 hash output is given. To answer the final question, we searched in Google for the CVE for DirtyCow.