REPORT

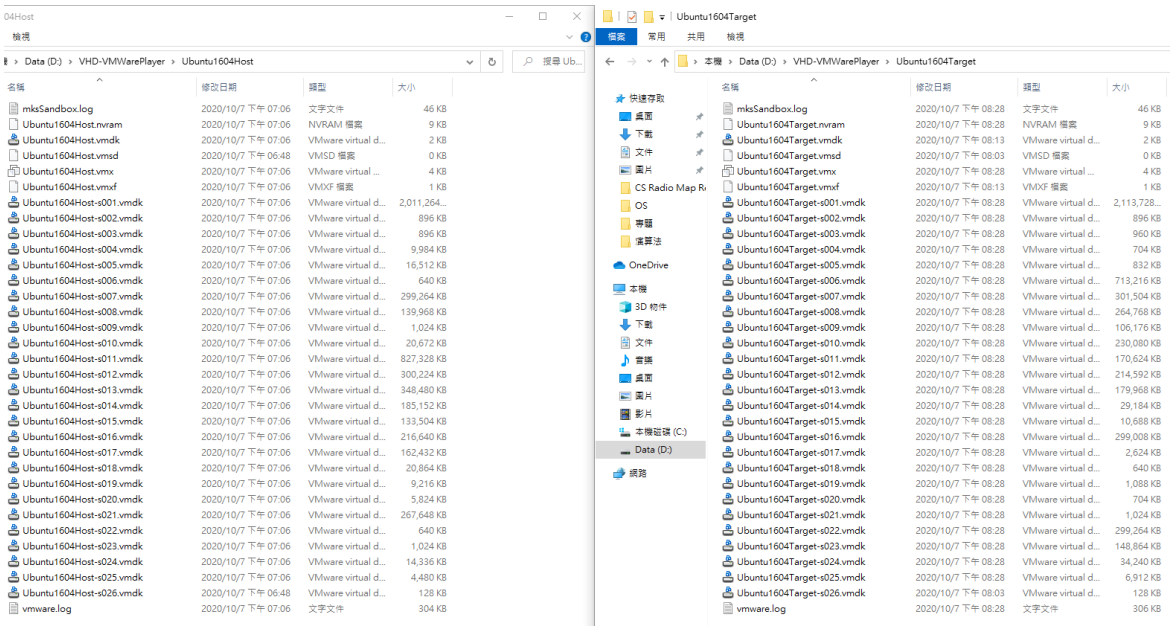
Video: https://youtu.be/AbDNHbzGXl8

The “gredit” file I say in 7:17 is actually grub.cfg.

I apologize for the length of my video, but I think it is necessary to explain my problem, sorry for the inconvenience.

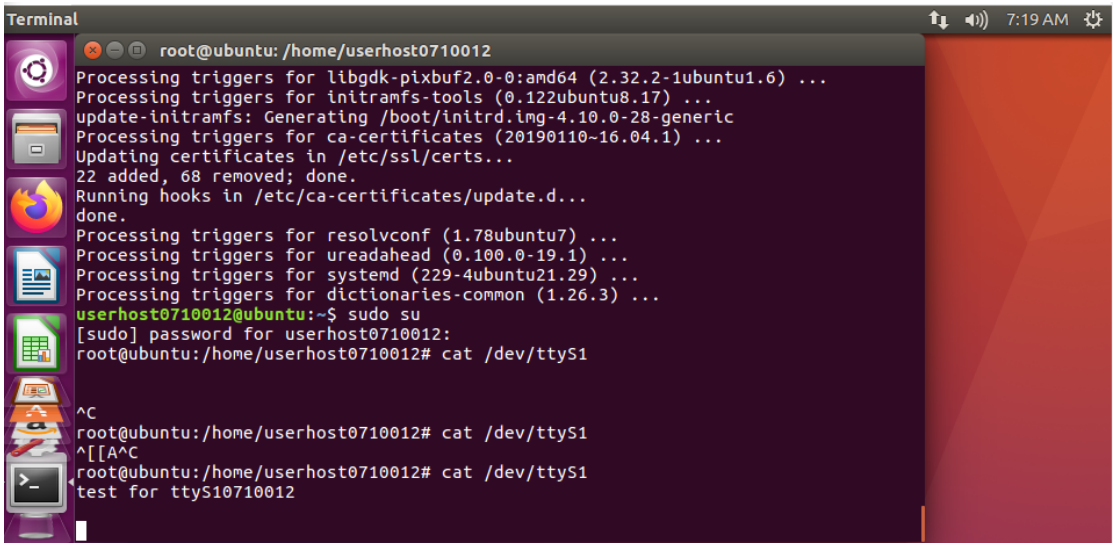
Screenshot 1:

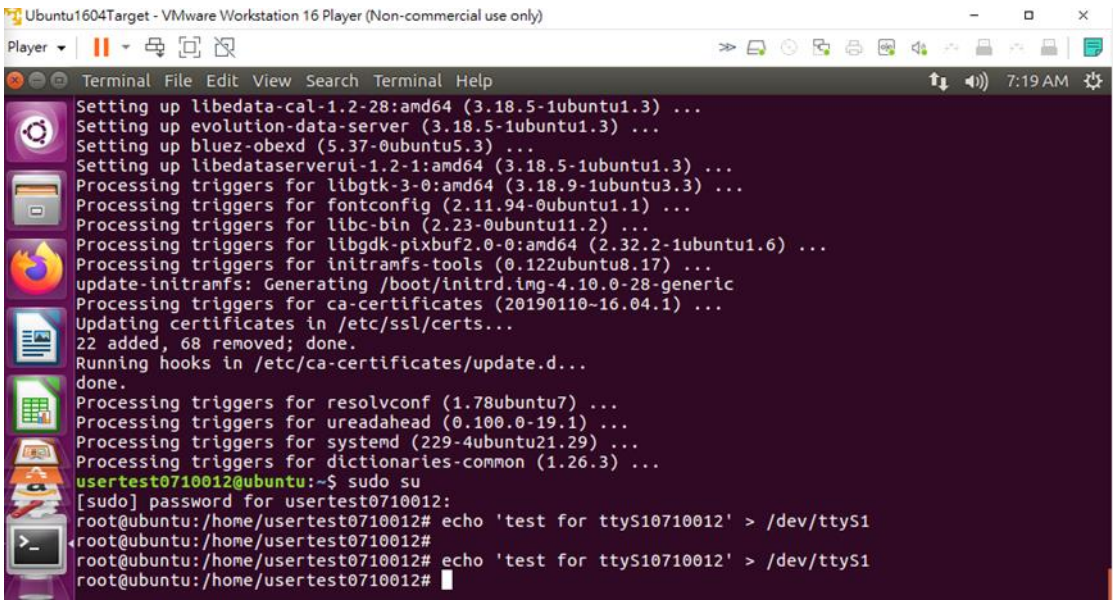
I create two virtual machine named one to be Ubuntu1604Target and make the username as usertest0710012 for the later kernel install, and the other virtual machine as Ubuntu1604Host and make the name as userhost0710012 for later kernel debugging with GDB



Screenshot 2:

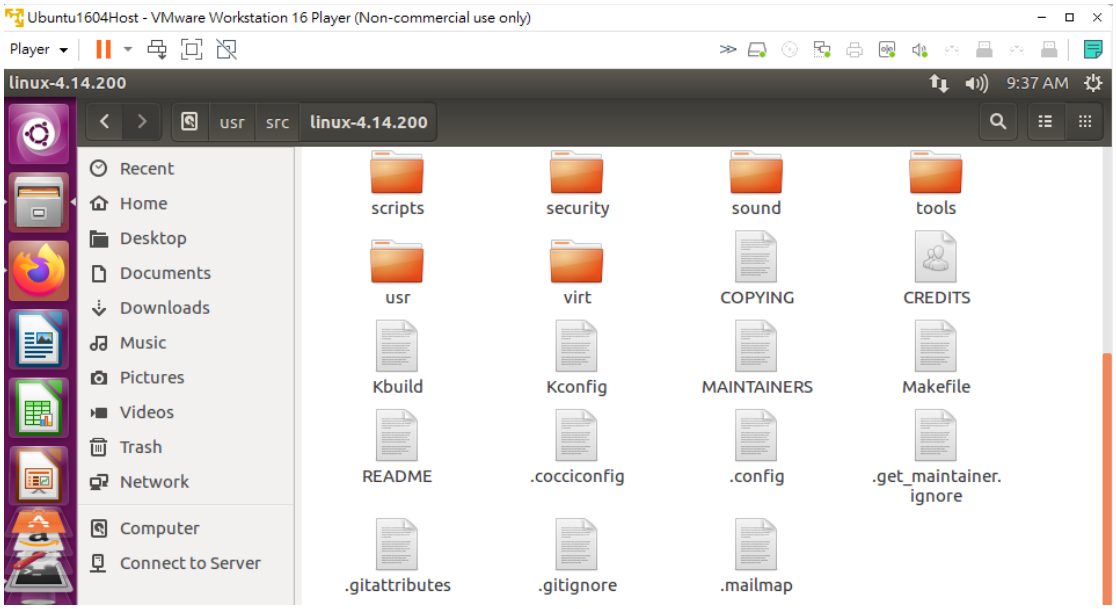
Use the host machine to cat a port(/dev/ttyS1), and print(echo) the sentence ‘test for ttyS10710012’ to check if the port is successfully connected.

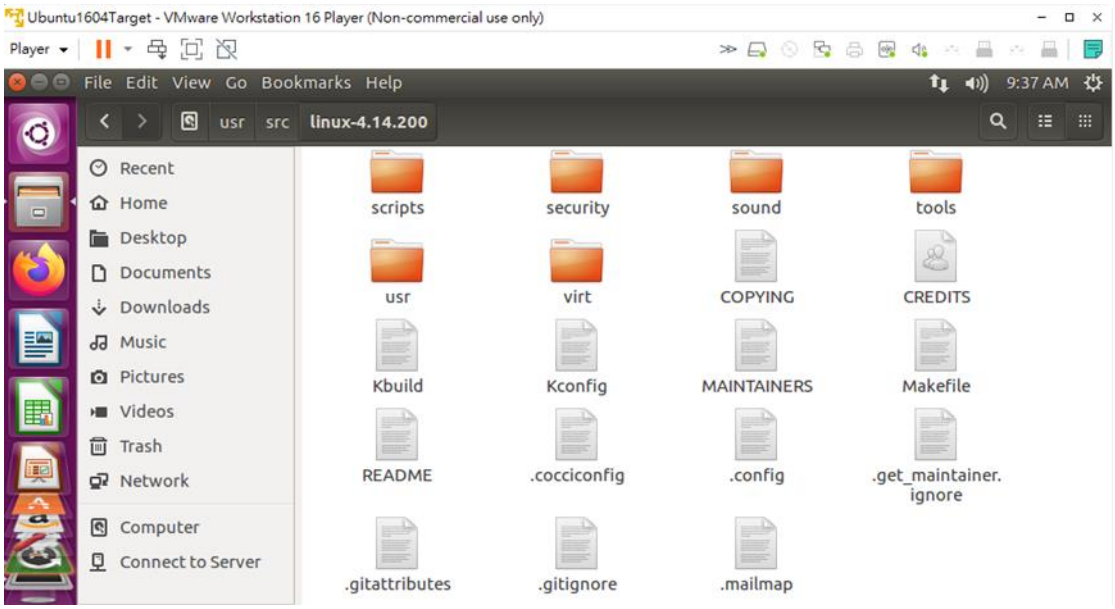




Screenshot 3:

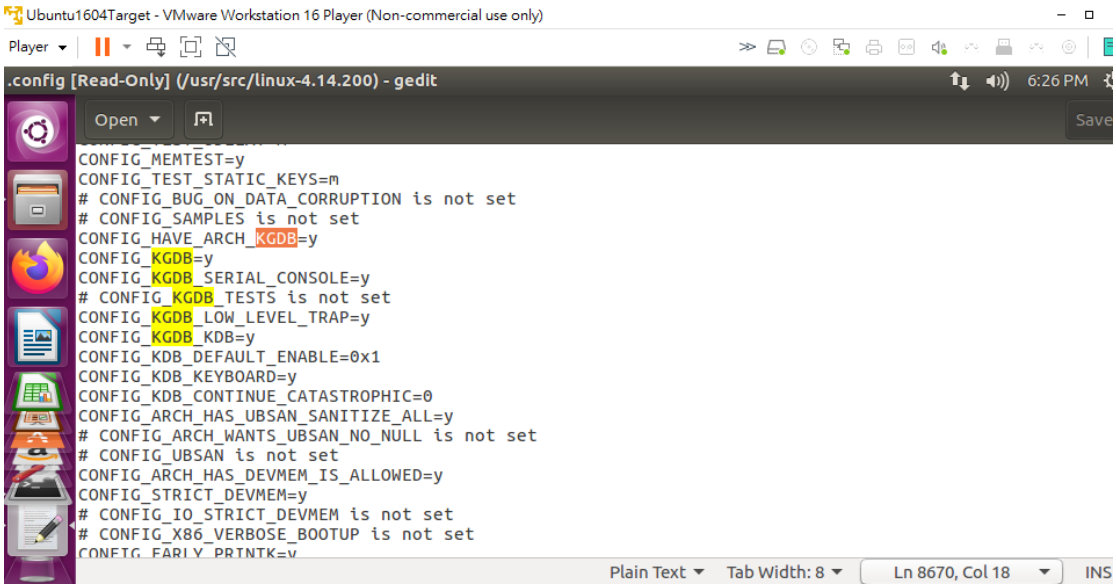
Download the new version of linux kernel and decompress, untar the folder. After that, we pre-build the additional kernel configuration by copying the .config file from the /boot/ folder to the new kernel folder and install the needed software in both target and host machine.





Screenshot 4:

First we find the and check if the command exist and their current status



Screenshot 5:

Use nano command to modify the mentioned commands to be in the status they should be to continue the process

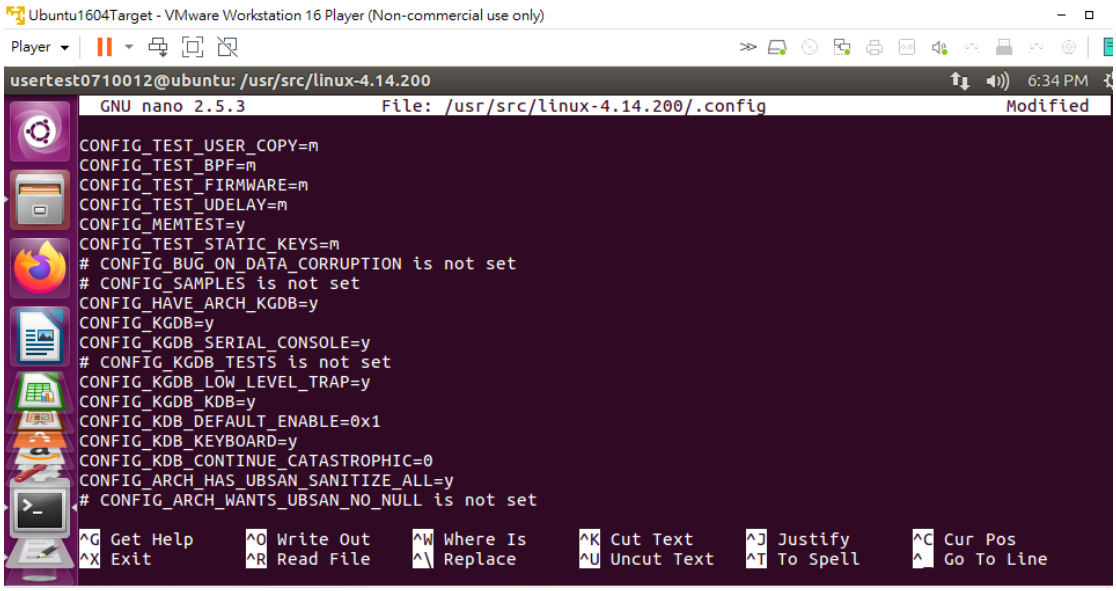
CONFIG_FRAME_POINTER→allow to compile the kernel through frame pointer

CONFIG_KGDB→allow the kernel GNU debugger to work

CONFIG_KGDB_SERIAL_CONSOLE→allow to use the kgdb over the serial console

CONFIG_KGDB_KDB→include the kdb frontend for kgdb

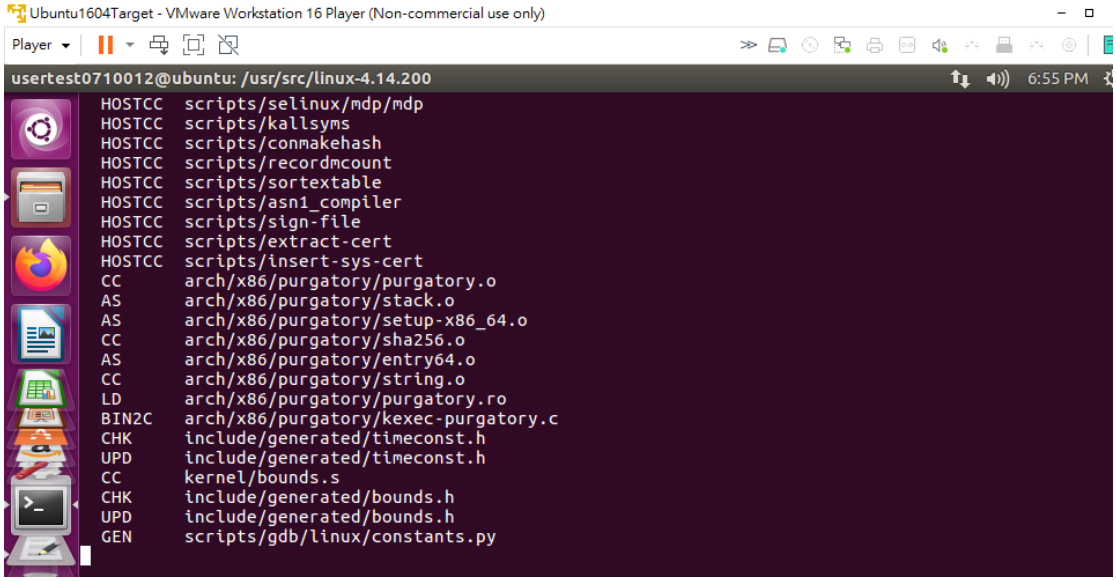
CONFIG_KDB_KEYBOARD→allow keyboard as input device

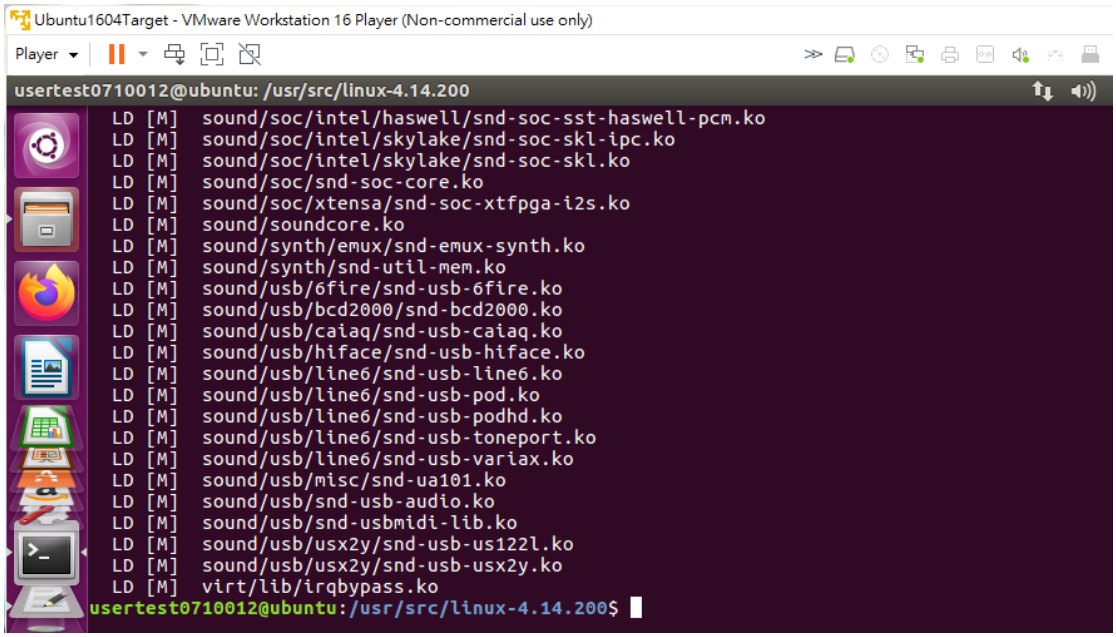


Screenshot 6:

Read the text in makefile and compile related files, and run two jobs simultaneously

sudo make -j 2

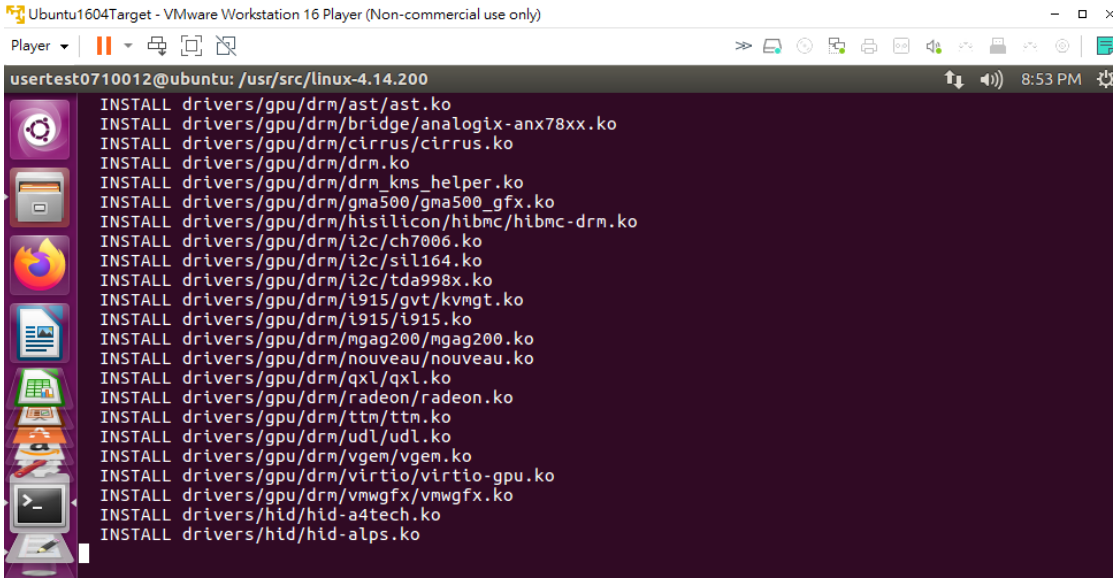


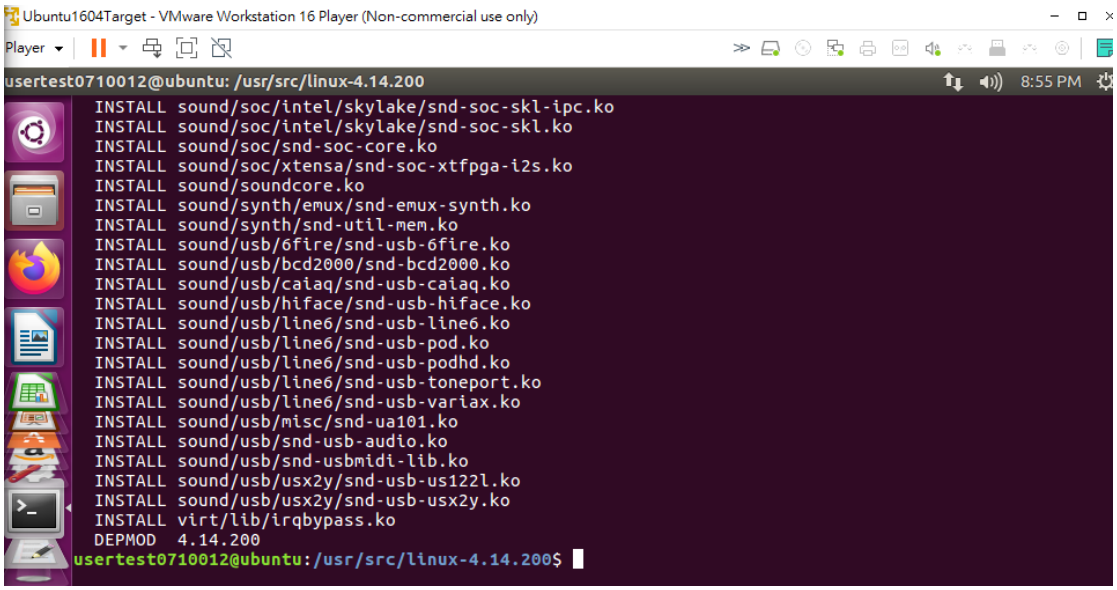


Screenshot7:

Install the module in the /lib/modules/`uname -r`

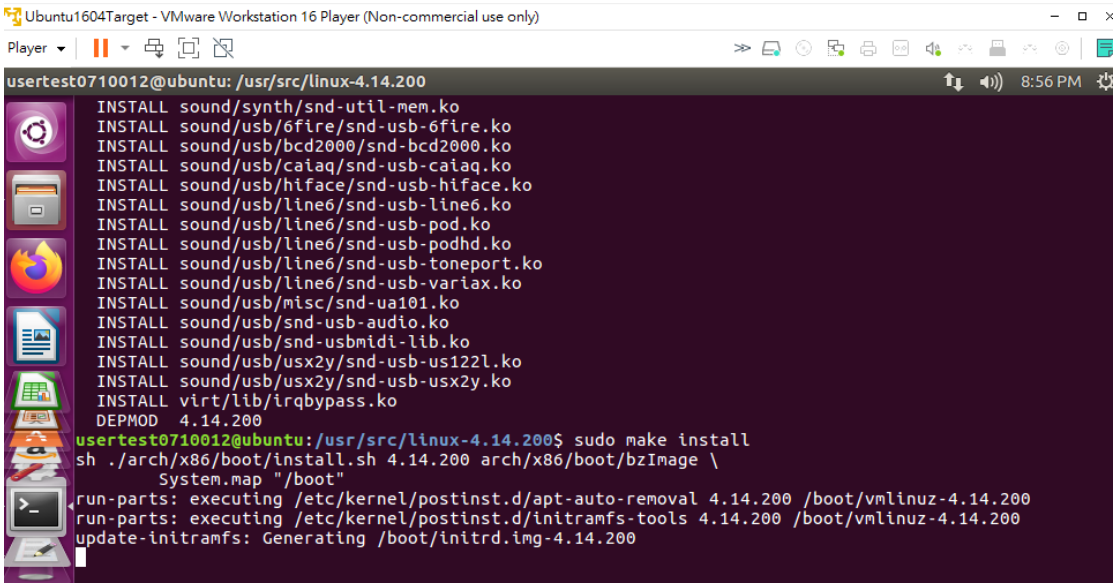
Sudo make modules_install

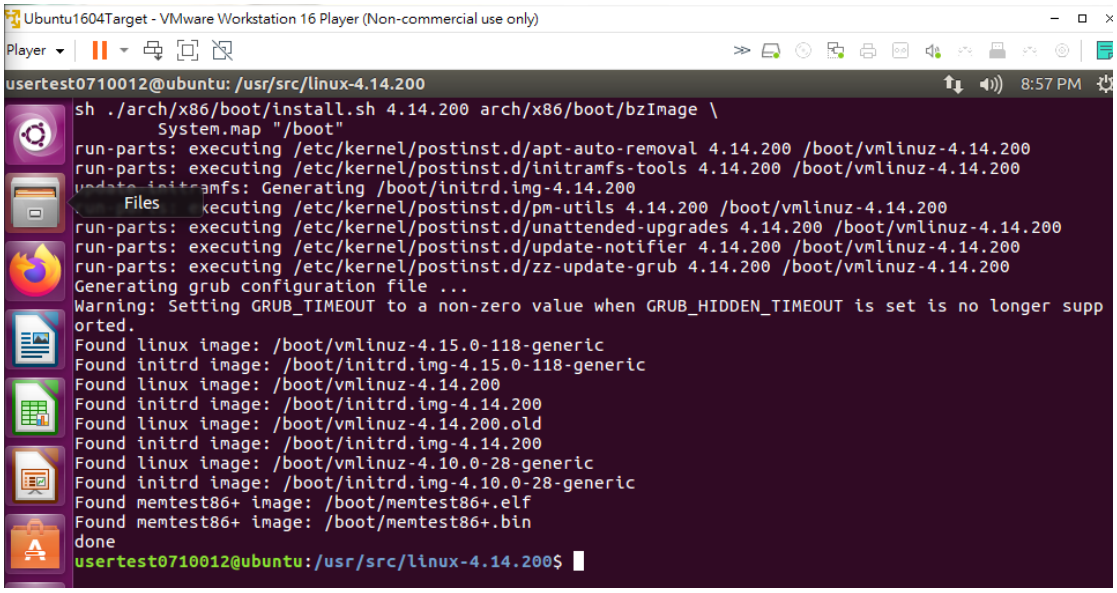




Screenshot 8:

Install the kernel to the machine



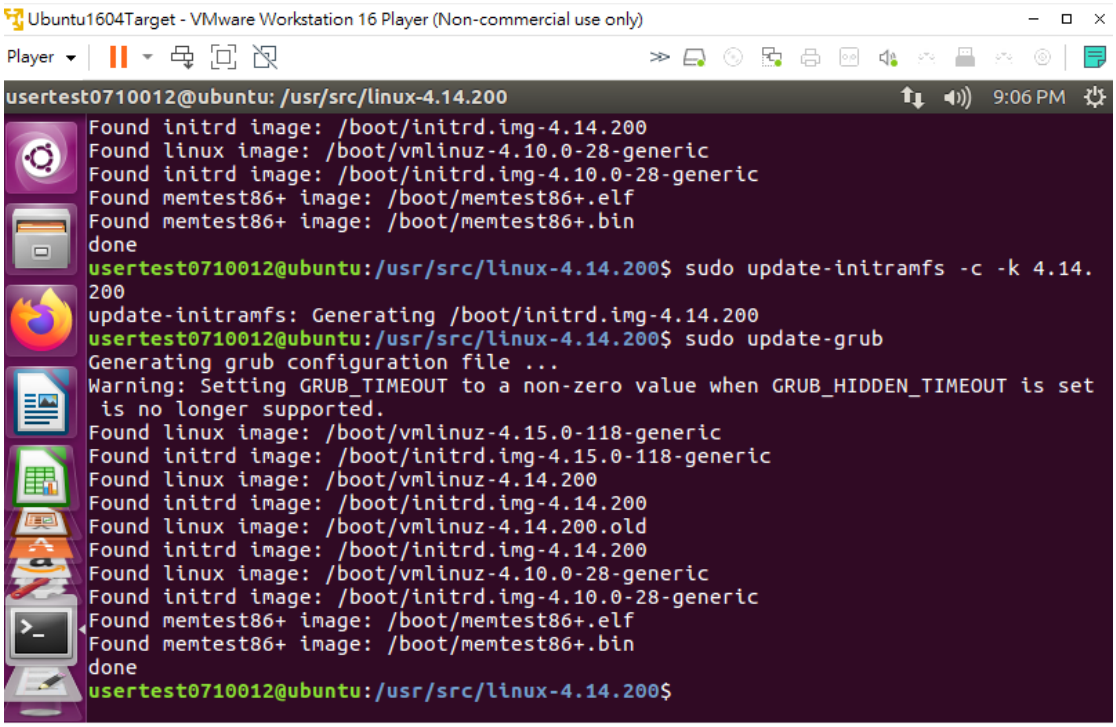


Screenshot 9:

Refresh the information in the grub after commenting out the two command

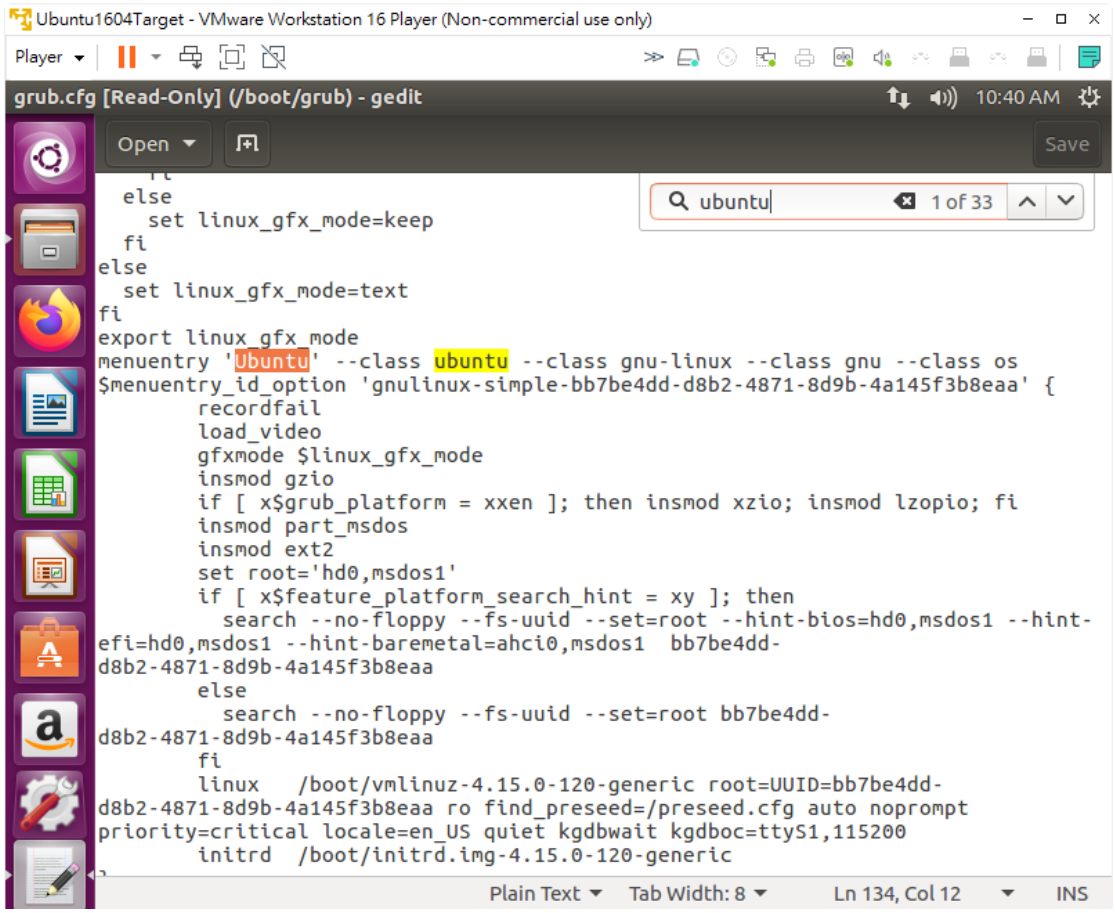
#GRUB_HIDDEN_TIMEOUT=0→can jump to the menu when jumping up the machine

#GRUB_HIDDEN_TIMEOUT_QUIET=true→won't show count down at the menu



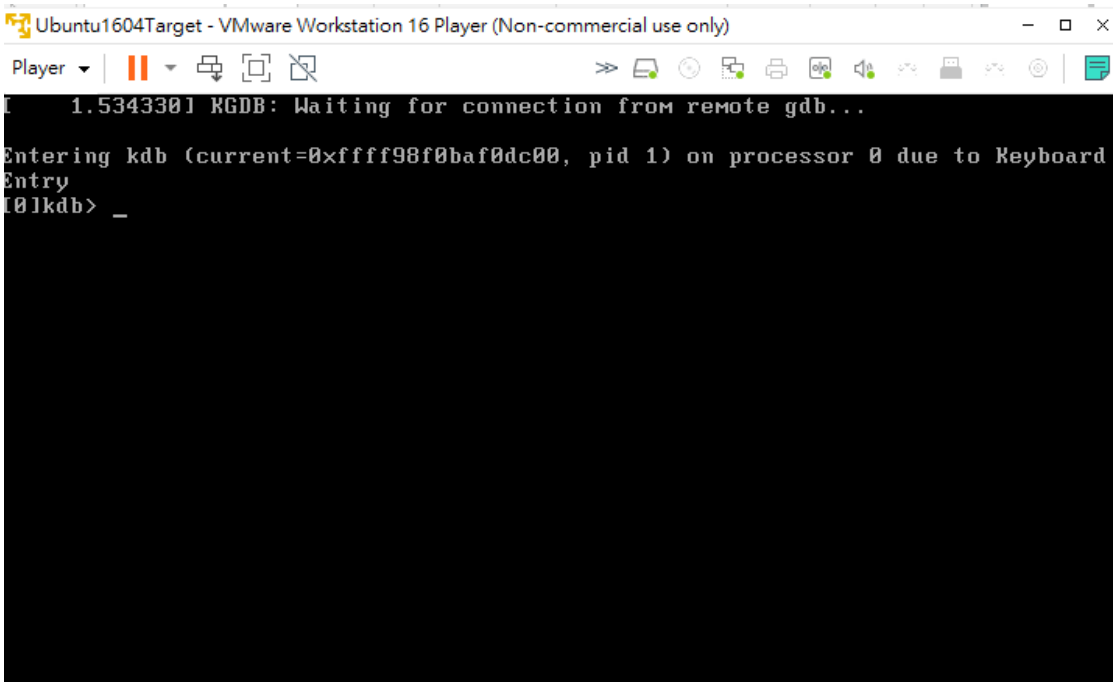
Screenshot 10:

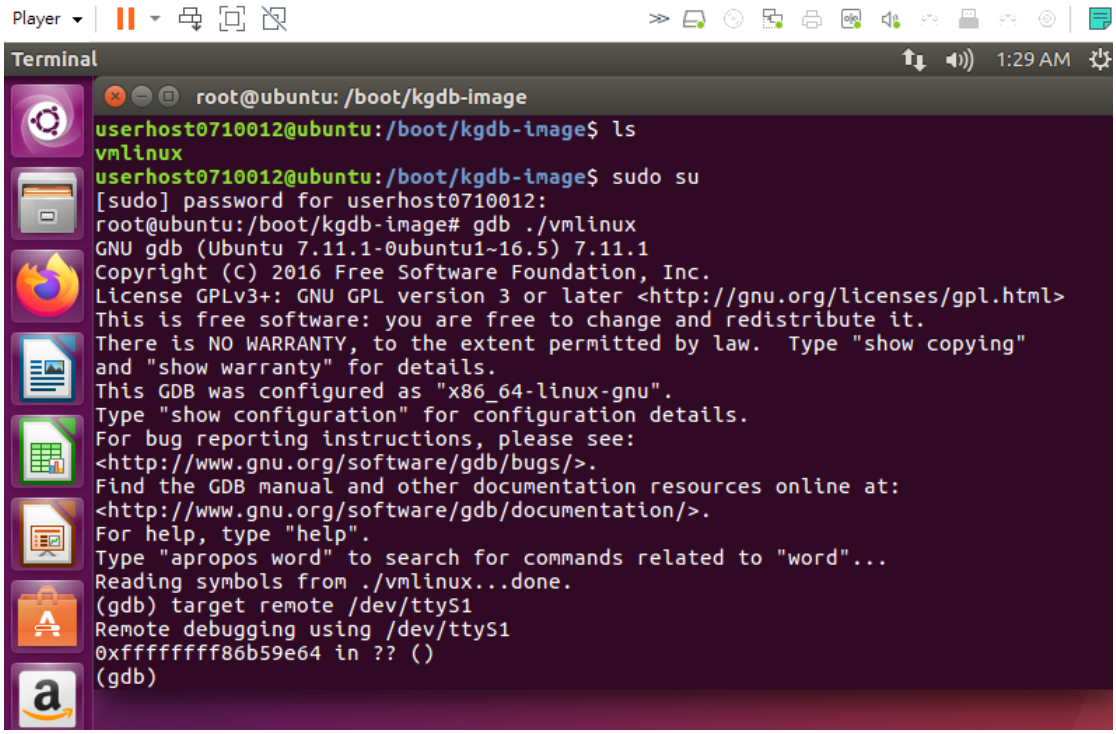
Use nano command to insert the command to the desired place, making the target machine able to wait for the remote gdb control



Screenshot 11:

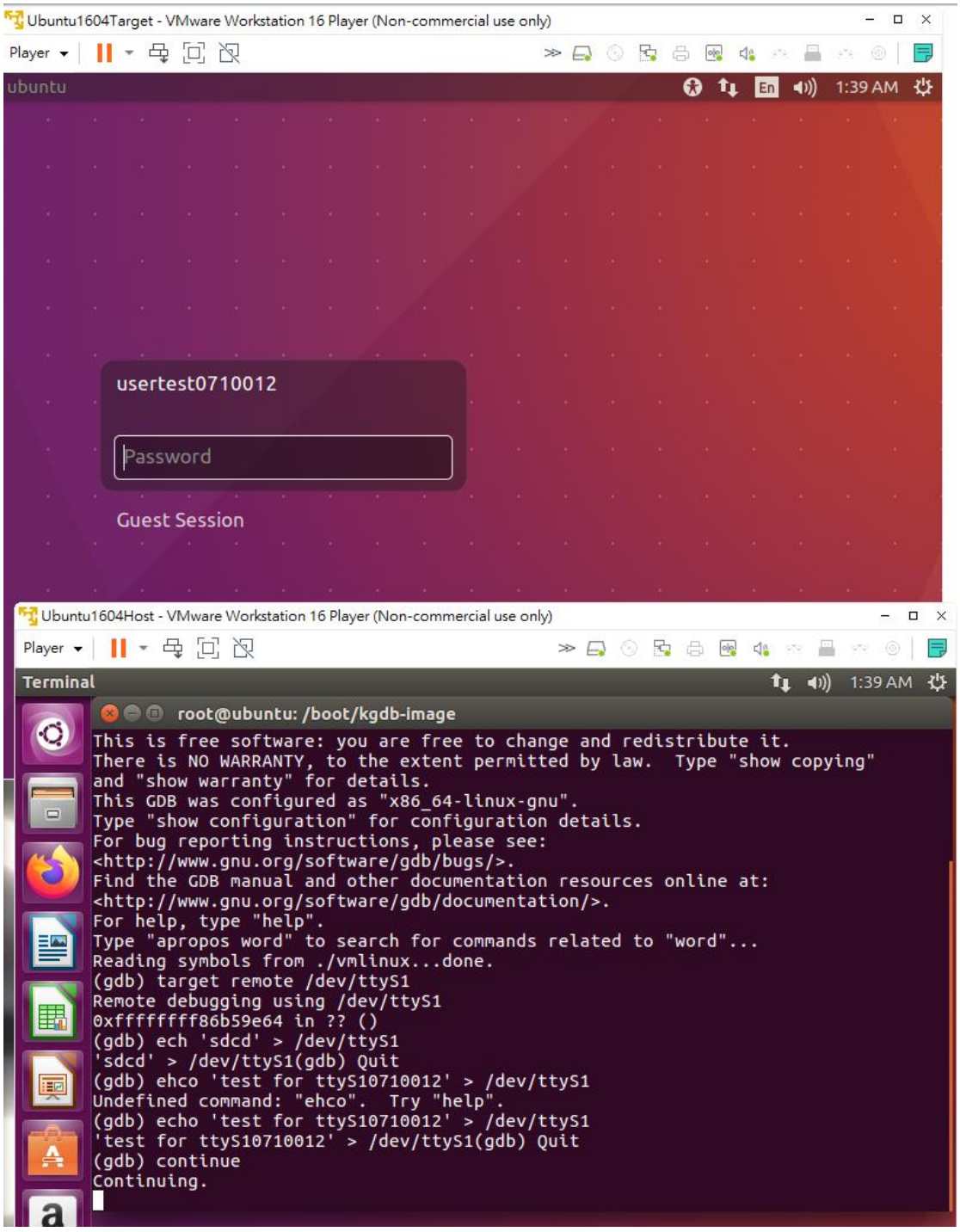
Activate gdb from the ./vmlinux file in kgdb-image and connect to the target machine through the /dev/ttyS1 prot





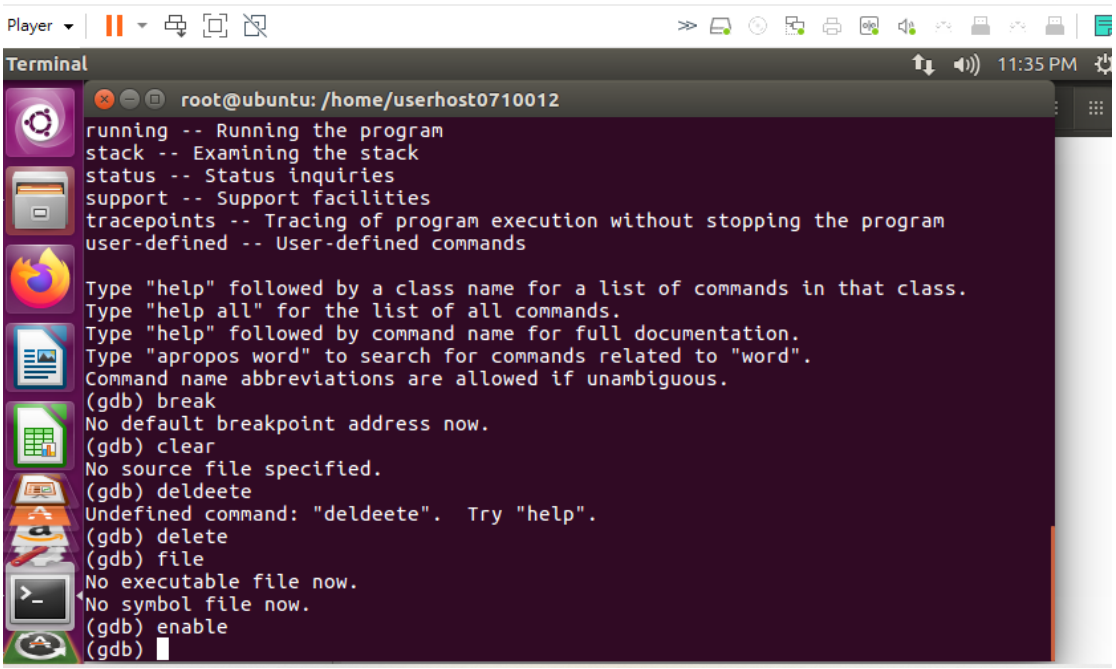
Screenshot 12:

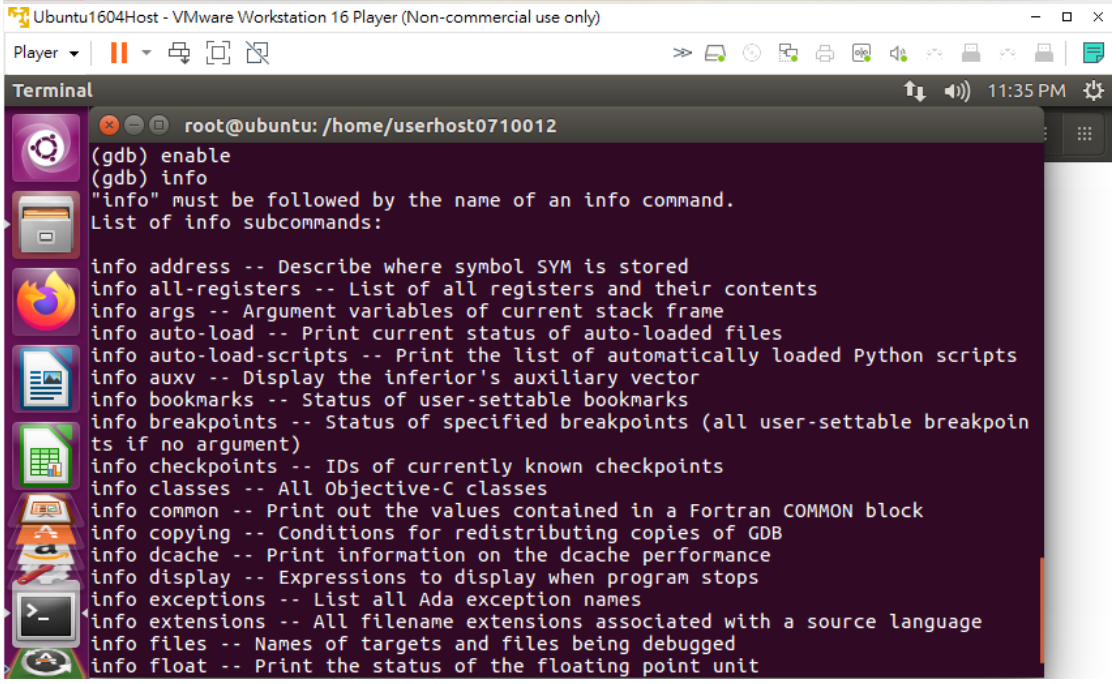
The target machine finish booting up process after the host command it to continue



Questions:

1. Kernel: the one program running at all time on the computer
   Mainline kernel: where new development and new features introduced
   Stable kernel: when mainline kernel is released, it is consider ”stable“. Bugfix version of mainline kernel
   Longterm kernel: for backporting bugfixes for older kernel tree
   Kernel panic: the action the operating system will take when it find a fatal error it can’t solve safely
2. building: to make a program executable
   debugging: modify the program to make it perform as the programmer wishes
   profiling: find out which part of the program takes most of the time, and optimize it
3. GCC: the GNU compiler collection, standard compiler for most projects related to GNU and Linux
   GDB: the GNU debugger, a free debugging program under Linux
   KGDB: debugger for the Linux kernel
4. /usr/: user system resources, has similar catalog as root, store user’s files
   /boot/: store the file when activate when the Linux machine turn on
   /home/: store normal user’s personal file
   /boot/grub: store bootloader
5. Have two machine, and install the kernel in one of them(target), after that, we use the other machine to run GDB and debug the kernel in the target machine through serial port.
6. Because we need one of the machine(target) to run the patched kernel and the other(host) to run GDB to debug the target.
7. Make: read the text in makefile and compile related files
   Make modules_install: install the module in the /lib/modules/`uname -r`
   Make install: install the kernel to the machine
8. Kgdbwait: command that makes kgdb to wait for a debugger connection during booting of a kernel
   Kgdboc=ttyS1,115200: kgbd over console, through port ttyS1 with 115200 Bdn data transfer speed
9. Grub: Grand unified bootloader, let user choose to boot one of the multiple OS, or select a specific kernel.
   Grub.cfg: a file containing information of grub, refresh when “update-grub” is run
10. Commands: ex, help, show, list, file, clear, info, delete, enable, disable, condition


Player
Terminal
11:35 PM
root@ubuntu: /home/userhost0710012
running -- Running the program
stack -- Examining the stack
status -- Status inquiries
support -- Support facilities
tracepoints -- Tracing of program execution without stopping the program
user-defined -- User-defined commands
Type "help" followed by a class name for a list of commands in that class.
Type "help all" for the list of all commands.
Type "help" followed by command name for full documentation.
Type "apropos word" to search for commands related to "word".
Command name abbreviations are allowed if unambiguous.
(gdb) break
No default breakpoint address now.
(gdb) clear
No source file specified.
(gdb) deldeete
Undefined command: "deldeete". Try "help".
(gdb) delete
(gdb) file
No executable file now.
No symbol file now.
(gdb) enable
(gdb)


Ubuntu1604Host - VMware Workstation 16 Player (Non-commercial use only)
Player
Terminal
11:35 PM
root@ubuntu: /home/userhost0710012
(gdb) enable
(gdb) info
"info" must be followed by the name of an info command.
List of info subcommands:
info address -- Describe where symbol SYM is stored
info all-registers -- List of all registers and their contents
info args -- Argument variables of current stack frame
info auto-load -- Print current status of auto-loaded files
info auto-load-scripts -- Print the list of automatically loaded Python scripts
info auxv -- Display the inferior's auxiliary vector
info bookmarks -- Status of user-settable bookmarks
info breakpoints -- Status of specified breakpoints (all user-settable breakpoin
ts if no argument)
info checkpoints -- IDs of currently known checkpoints
info classes -- All Objective-C classes
info common -- Print out the values contained in a Fortran COMMON block
info copying -- Conditions for redistributing copies of GDB
info dcache -- Print information on the dcache performance
info display -- Expressions to display when program stops
info exceptions -- List all Ada exception names
info extensions -- All filename extensions associated with a source language
info files -- Names of targets and files being debugged
info float -- Print the status of the floating point unit