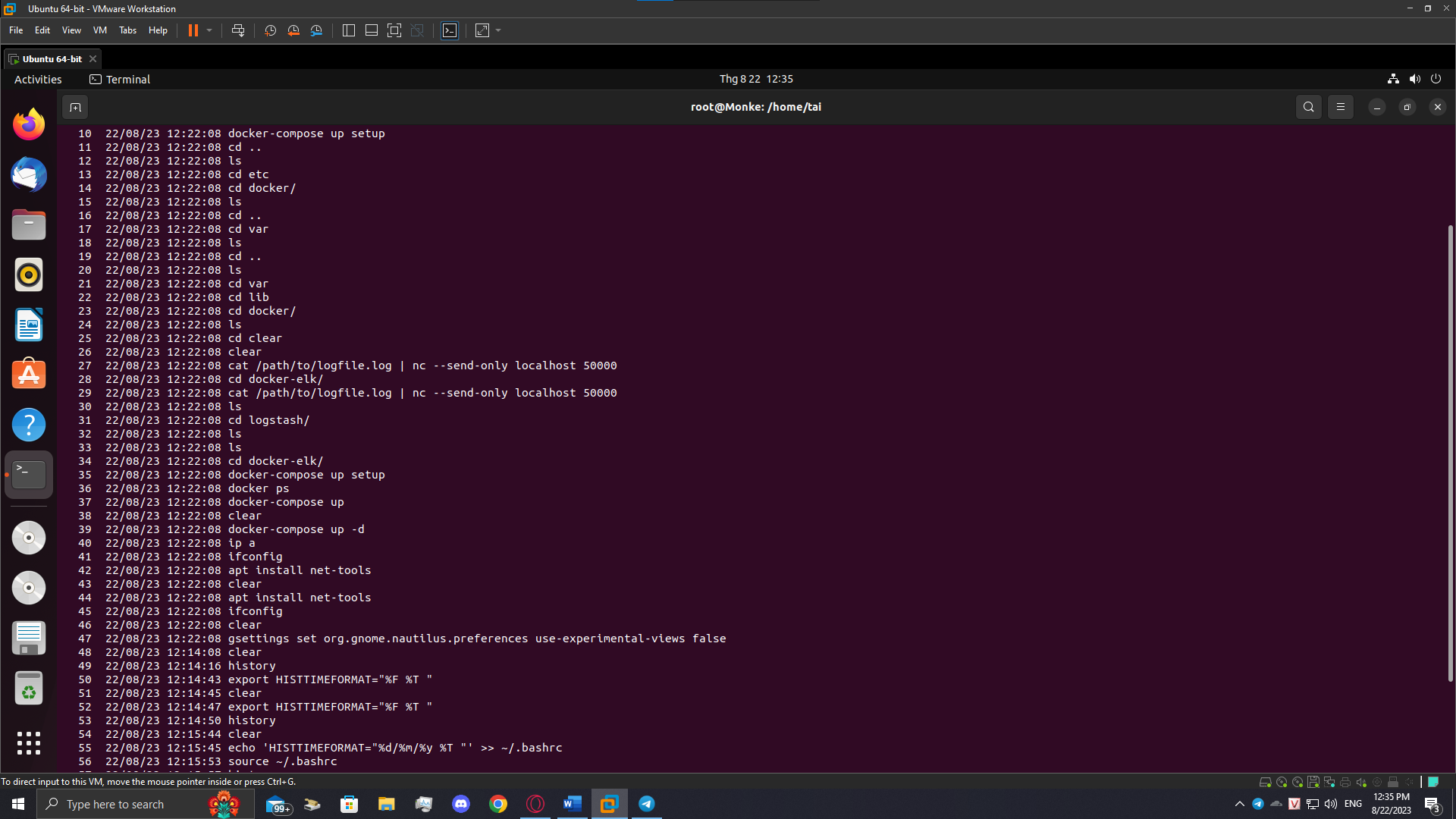
1. ***Log command with time***

Để log command với timestamp chúng ta sử dụng lệnh HISTTIMEFORMAT để thay đổi output của lệnh history

Có 2 cách để chỉnh format output:

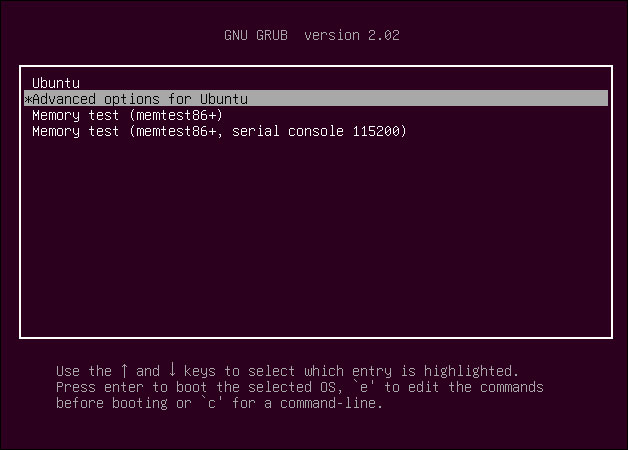
* HISTTIMEFORMAT="%d/%m/%y %T " # for e.g. “29/02/99 23:59:59”
  + %d: Biểu thị ngày trong tháng dưới dạng số hai chữ số (01 đến 31).
  + %m: Biểu thị tháng trong năm dưới dạng số hai chữ số (01 đến 12).
  + %y: Biểu thị năm dưới dạng số hai chữ số (00 đến 99).
  + %T: Biểu thị thời gian theo định dạng "HH:MM:SS" (đồng hồ 24 giờ).
* HISTTIMEFORMAT="%F %T " # for e.g. “1999-02-29 23:59:59”
  + %F: Biểu thị ngày đầy đủ trong định dạng "YYYY-MM-DD". Ví dụ: "2023-08-17".
  + %T: Biểu thị thời gian trong định dạng "HH:MM:SS" (đồng hồ 24 giờ).

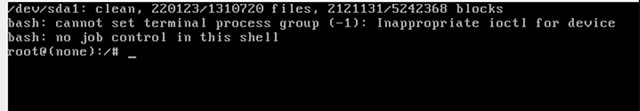


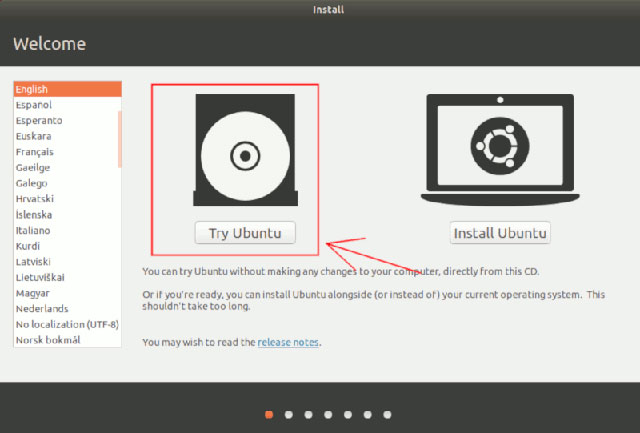
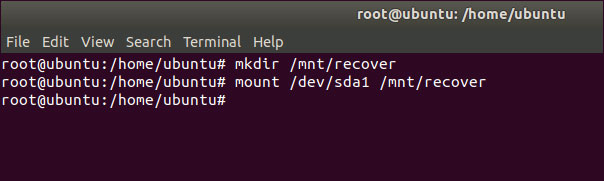
Đối với các lệnh đã chạy trước khi HISTTIMEFORMAT được thiết lập, thời gian hiện tại sẽ được lưu làm timestamp. Các lệnh chạy sau khi HISTTIMEFORMAT được thiết lập sẽ có timestamp chính xác được lưu trữ.

1. ***Lost root password***

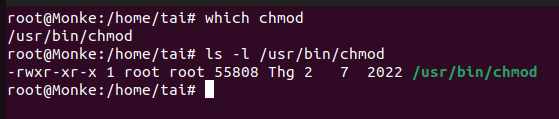
Có 2 cách chính để recover mật khẩu root

* Sử dụng grub menu
  + Trước hết, để khôi phục mật khẩu root, bạn cần khởi động lại Linux host.
  + Khi trang GRUB hiện ra, nhanh chóng chọn **Advanced options for GNU/Linux**bằng cách nhấn phím mũi tên và chọn **Enter.**
  + 
  + Nhấn phím E để chỉnh sửa lệnh
  + Bạn phải chỉnh sửa hoặc thay đổi từ chế độ read-only sang chế độ read-write. Hãy tìm dòng bắt đầu bằng từ “Linux”, sau đó tìm “ro” và đổi thành “rw”. Thêm init=/bin/bash vào cuối dòng.
  + 
  + Nhấn phím **F10.** Màn hình dưới đây sẽ hiện ra.

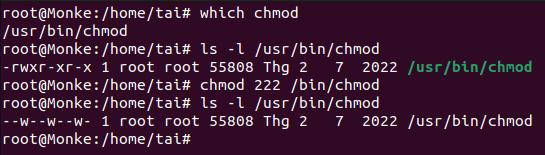


* + Đưa file hệ thống root vào chế độ read-write bằng lệnh:
    - mount -n -o remount,rw /
  + Giờ bạn có thể reset lại mật khẩu root đã mất bằng cách dùng lệnh:
    - passwd root
  + Hoặc đổi mật khẩu của siêu người dùng bằng lệnh sau:
    - passwd username
  + Khi hoàn thành, gõ lệnh sau đây để thoát và khởi động lại máy.
    - exec /sbin/init
* Sử dụng live cd
  + Tải bản mới nhất của Ubuntu, tạo Live CD/USB để boot từ đó và khởi động hệ thống từ đó.
  + Trên màn hình, chọn **Try Ubuntu** để mở ra màn hình Live CD.
  + 
  + Mở terminal và gõ dòng lệnh sau để root.
    - sudo su
  + Bây giờ cần tìm địa điểm của phân vùng ổ đĩa. Dùng lệnh dưới đây:
    - fdisk -1
  + Hầu hết các trường hợp có thể dùng lệnh /dev/sda1 dù có thể có khác biệt tùy thuộc vào việc bạn phân vùng ổ cứng ra sao.
  + Mở phân vùng ổ cứng cần khôi phục bằng lệnh sau:
    - mkdir /mnt/recover mount /dev/sda1 /mnt/recover
  + 
  + Bây giờ ta phải đưa mình vào thư mục mnt/recovery, nghĩa là giả vờ rằng mình đang dùng file hệ thống Linux thông thường, hay còn gọi là chroot.
    - chroot /mnt/recover
  + Dùng lệnh sau đây để khôi phục lại mật khẩu root.
    - passwd root
  + hoặc người dùng:
    - passwd username
  + để tạo mật khẩu cho siêu người dùng.
  + Sau khi hoàn thành, thoát khỏi shell chroot.
    - exit
  + Đóng phân vùng root bằng lệnh:
    - umount /mnt/recover
  + và thoát bằng lệnh:
    - exit

1. ***chmod 222 /bin/chmod – what do you do to fix?***



Chmod có thể chạy với đầy đủ quyền cho chủ sở hữu ("root"), cho phép đọc, ghi và thực thi. Nhóm "root" và người khác chỉ có thể đọc và thực thi tập tin.



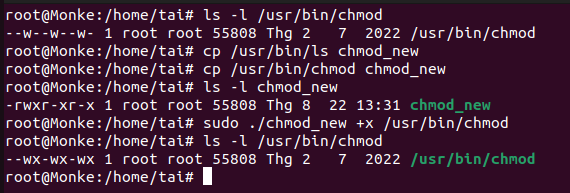
Thay đổi quyền của chmod sang chỉ write và không có read, execute

Để sửa lại chúng ta có thể dùng các cách sau:

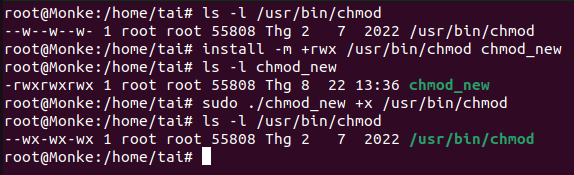
* Dynamic Loader



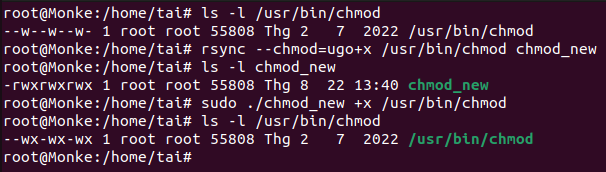
* + Dynamic loader có nhiệm vụ tải một tập tin thực thi và liên kết các thư viện chia sẻ cần thiết.Ví dụ, trên hệ điều hành Debian/Ubuntu 64 bit, chúng ta có thể tìm thấy trình tải tại /lib64/ld-linux-x86-64.so.2.
  + Ở đây, chúng ta đã sử dụng dynamic loader để chạy lệnh chmod như một tập tinthực thi và cấp cho chính nó quyền thực thi thông qua tùy chọn +x.
* Sử dụng cp



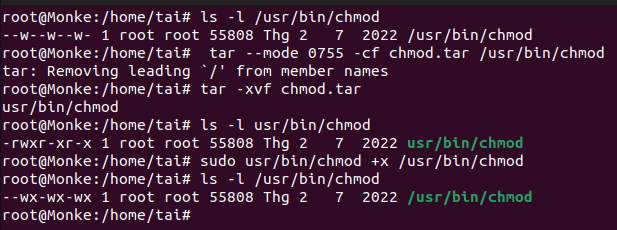
* + Một phương pháp khôi phục quyền thực thi của /usr/bin/chmod là sử dụng lệnh cp để tạo một tập tin thực thi mới. Chúng ta có thể làm như vậy trong hai bước:
  + Sao chép cả nội dung và quyền của một tập tin thực thi như /usr/bin/ls vào một tập tin tạm thời có tên là chmod\_new.
  + Sao chép chỉ nội dung của tập tin /usr/bin/chmod vào chmod\_new.
  + Bằng cách này, chmod\_new thừa hưởng quyền từ tập tin thực thi /usr/bin/ls, trong khi nội dung của nó đến từ /usr/bin/chmod. Như vậy, chmod\_new trở thành một lệnh chmod thực thi hoàn toàn:
  + Bằng cách sử dụng chmod\_new, chúng ta có thể khôi phục lại các quyền thực thi của /usr/bin/chmod thành công. Thực chất, ngoại trừ chủ sở hữu, cả hai tập tin đều trở thành các lệnh chmod tương đương. Phương pháp này hoạt động vì lệnh cp chỉ sao chép nội dung của tập tin mà không sao chép quyền khi tập tin đích đã tồn tại.
  + Cần lưu ý rằng nếu tập tin đích không tồn tại, lệnh cp sẽ sao chép quyền của tập tin nguồn hoặcquyền mặc định được xác định bởi umask, tùy thuộc vào cái nào hạn chế hơn.
* Sử dụng install



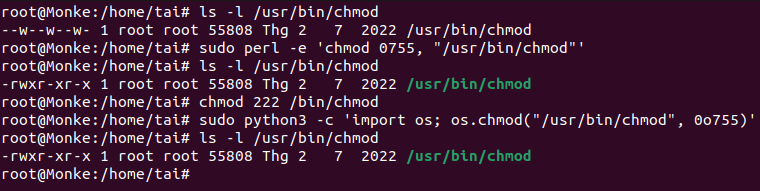
* + Một cách khác để khôi phục /usr/bin/chmod thành tập tin thực thi là thông qua lệnh install, một phần của gói GNU Coreutils. Lệnh này hoạt động tương tự như cp vì nó có thể sao chép tập tin, nhưng cũng có thể đặt quyền cần thiết bằng cách sử dụng tùy chọn -m:
  + Lệnh install sao chép nội dung của /usr/bin/chmod vào một tập tin có tên là chmod\_new và đặt quyền của tập tin này để cho phép tất cả người dùng đọc, viết và thực thi.
* Sử dụng rsync



* + Một cách khác, rsync cũng cho phép đặt quyền tập tin cho các tập tin đã sao chép:
  + Ở đây, chúng ta sử dụng tùy chọn --chmod để cấp quyền thực thi cho tất cả người dùng cho tập tin chmod\_new vừa tạo. Sau đó, chúng ta có thể sử dụng tập tin này để khôi phục lại quyền thực thi cho /usr/bin/chmod.
* Sử dụng tar
  + Một phương pháp khác là sử dụng lệnh tar, viết tắt của tape archive(r). Lệnh này cho phép đặt quyền tập tin thông qua tùy chọn --mode khi tạo tập tin lưu trữ:
  + tar --mode 0755 -cf chmod.tar /usr/bin/chmod
  + tar: Removing leading `/' from member names
  + Trong phương pháp này, lệnh tar đặt quyền bát phân 0755 cho tập tin đang được lưu trữ. Chúng ta sử dụng tùy chọn -c để tạo tập tin lưu trữ, trong khi tùy chọn -f chỉ định tên tập tin lưu trữ là chmod.tar.
  + Để giải nén nội dung của tập tin lưu trữ, chúng ta sử dụng lệnh tar với các tùy chọn xvf, trong đó --x giải nén tập tin lưu trữ, --v cung cấp đầu ra chi tiết và --f chỉ định tên tập tin lưu trữ:



* Sử dụng Interpreters
  + Chúng ta cũng có thể sử dụng các khả năng chmod của các ngôn ngữ lập trình như Perl và Python.
  + Ví dụ, chúng ta có thể sử dụng chmod của Perl với quyền bát phân 0755 cho tập tin /usr/bin/chmod:
  + Tùy chọn -e cho phép thực hiện một lệnh cụ thể được chỉ định ở đây trong dấu nháy đơn.
  + Tương tự, trong Python, chúng ta có thể bắt đầu bằng cách nhập thư viện os và sau đó sử dụng phương thức os.chmod() để đặt quyền:
  + Ở đây, chúng ta cần sử dụng tiền tố 0o khi chỉ định một hằng số bát phân.



Sử dụng Vim

* + Cuối cùng, chúng ta có thể sử dụng trình soạn thảo văn bản Vim để thay đổi quyền của /usr/bin/chmod bằng một lệnh đơn:
  + Tùy chọn -c cho phép thực hiện một lệnh ex trong Vim. Trong trường hợp này, chúng ta gọi hàm setfperm() có thể thay đổi quyền tập tin và chúng ta truyền cho nó tên tập tin và quyền cần thiết như đối số.
    - sudo vim -c "call setfperm('/usr/bin/chmod', 'rwxr-xr-x') | quit"
    - ls -l /usr/bin/chmod
    - -rwxr-xr-x 1 root root 64288 Feb 28 2019 /usr/bin/chmod
  + Bằng cách thay đổi quyền thành rwxr-xr-x, tập tin trở thành có thể thực thi trên toàn thế giới lại.

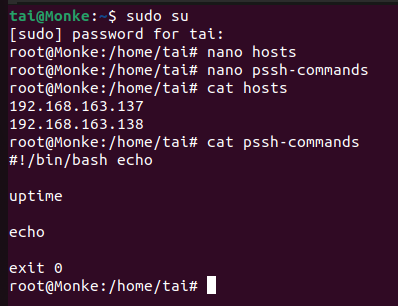
1. ***Execute a single command on multiple VMs***

Để chạy 1 lệnh trên nhiều máy cùng 1 lúc ta có thể sử dụng công cụ parallel-ssh

Tải pssh qua lệnh

pip install parallel-ssh

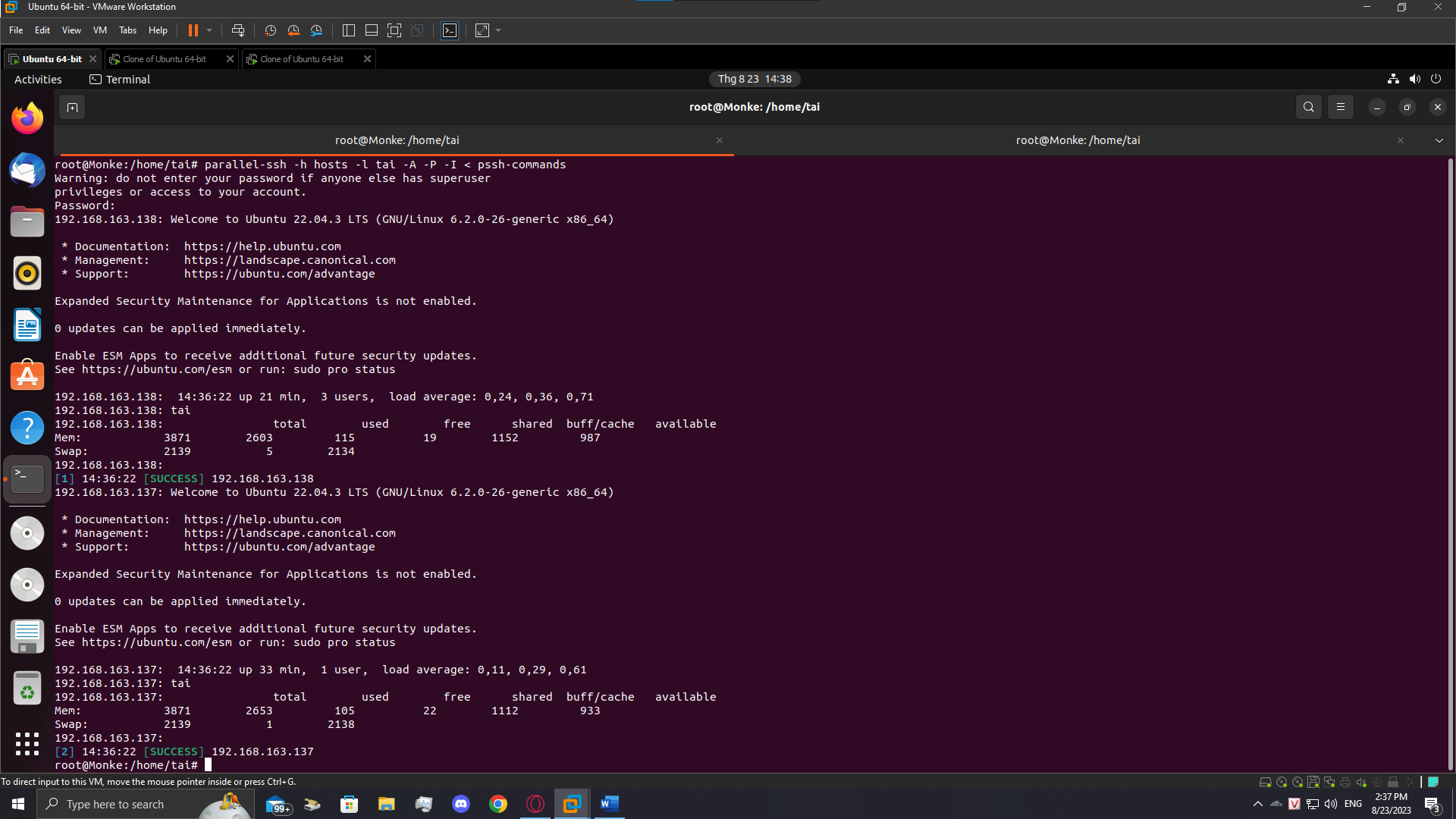
sau đó tạo file “hosts” bao gồm ip của các VM để chạy command và tạo 1 file “pssh-commands” bao gồm các lệnh để chạy trên các VM khác



Sau đó chạy lệnh

parallel-ssh -h hosts -A -P -I < pssh-commands

* **-A** chỉ định ổ cắm của trình quản lý xác thực.
* **-P** giới hạn số tiến trình song song thành 10 tiến trình.
* **-I** cung cấp đầu vào từ tệp tin **pssh-commands**.
* **-h** chỉ định tệp tin danh sách máy chủ.



Trong trường hợp bị lỗi “exited with error code 255 pssh” chúng ta cần phải establish kết nối ssh giữa các máy trước bằng cách:

* Ssh-keygen để tạo khóa
* Ssh-copy-id để copy private key sang máy cần chạy lệnh
* Sau đó kết nối ssh để thử độ ổn định, nếu thành công thì kết nối ssh đã được thiết lập