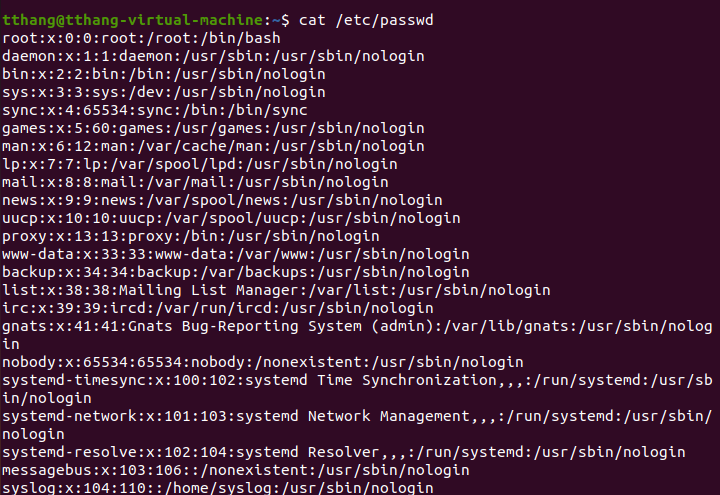
**17110230 - Nguyễn Văn thắng**

**Lab 3: Using John the Ripper to Crack Linux Passwords**

**Locating and Cracking Linux Passwords**

1. To view the contents of the passwd file, type:

* Xem nội dung file etc/passwd



1. View the permissions on the /etc/passwd file by typing the following command:



* Xem chi tiết file etc/passwd gồm có:

Tên file: /etc/passwd

Ngày tháng tạo file: Thg 10 2020

Dung lượng file: 2689 bytes

Group sở hữu: root

User sở hữu: root

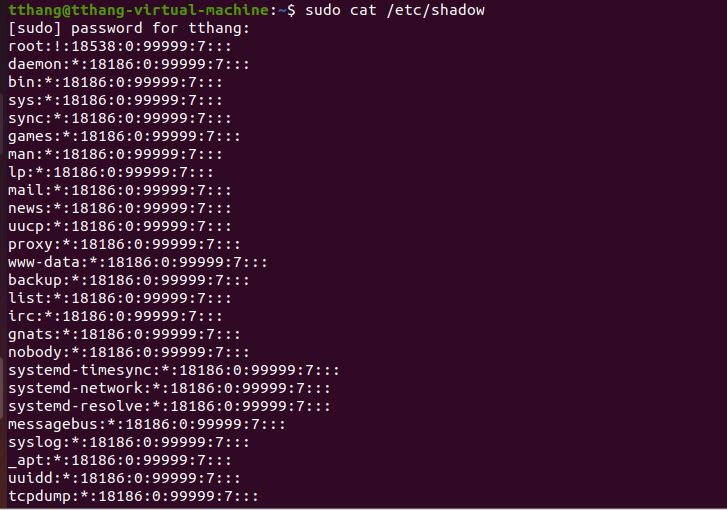
Các quyền –rw-r—r: + rw (đầu tiên): quyền đọc và ghi, quyền này là của user sở hữu

+ r (r ở giữa): quyền đọc quyền này là của group sở hữu

+ r (cuối cùng): quyền đọc, quyền này là của tất cả mọi người

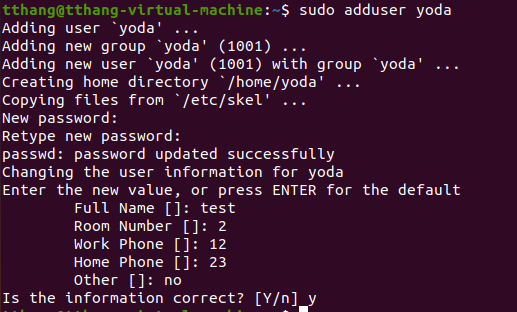
1. To view the contents of the shadow file, type:

* Nội dung file /etc/shadow



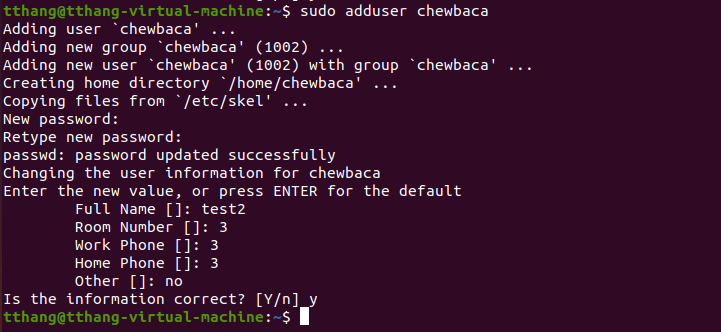
1. To create a new user named yoda, type the following command in the terminal:

* Thêm mới user yoda



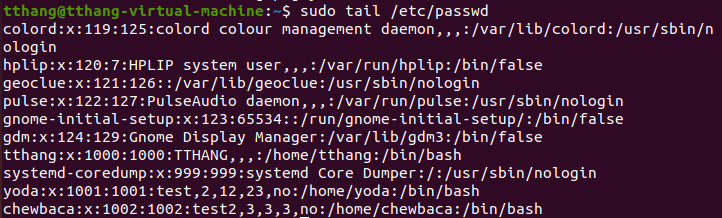
1. To create a new user named chewbacca, type the following command in the terminal:

* Thêm user mới là chewbaca



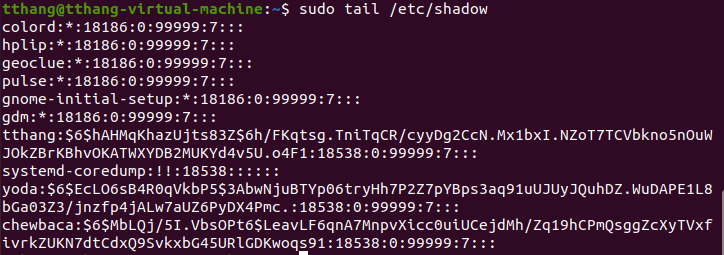
1. Now, view the changes made to the passwd file by typing the following:

* Sử dụng lệnh tail để xem 10 dòng cuối file /etc/passwd



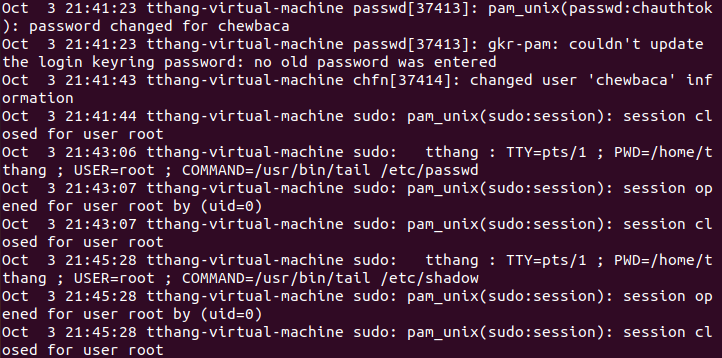
1. Next, examine the alterations to the shadow file by typing the following:

* Xem 10 dòng cuối file /etc/shadow. Dấu “!” của user yoda và chewbaca vừa tạo có ý nghĩa là hai user vừa tạo chưa được đặt mật khẩu.



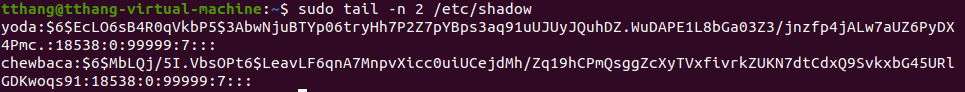
1. Examine the entries in the auth.log related to account changes by typing:

* Xem 10 dòng cuối file /var/log/auth.log. File auth.log sẽ ghi lại các thay đổi của tài khoản.



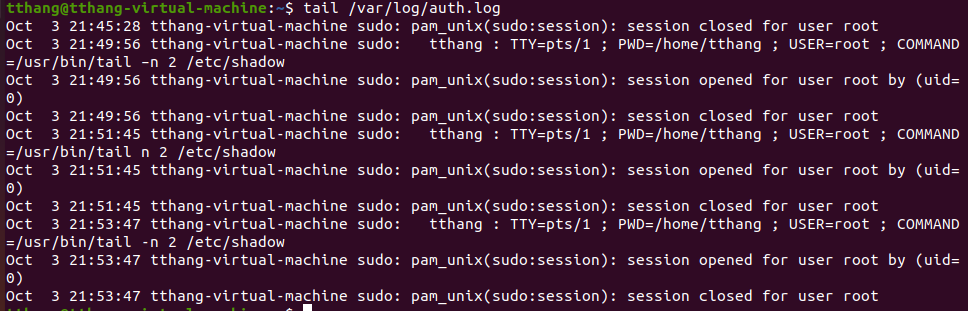
1. Next, examine the alterations to the shadow file by typing the following:

* Sử dụng option để xem 2 dòng cuối của file /etc/shadow.



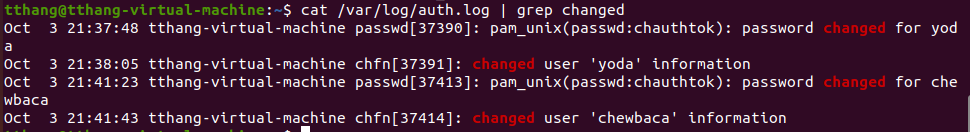
1. Examine the entries in the auth.log related to account changes by typing:

* Xem lại 10 dòng cuối file /var/log/auth.log.



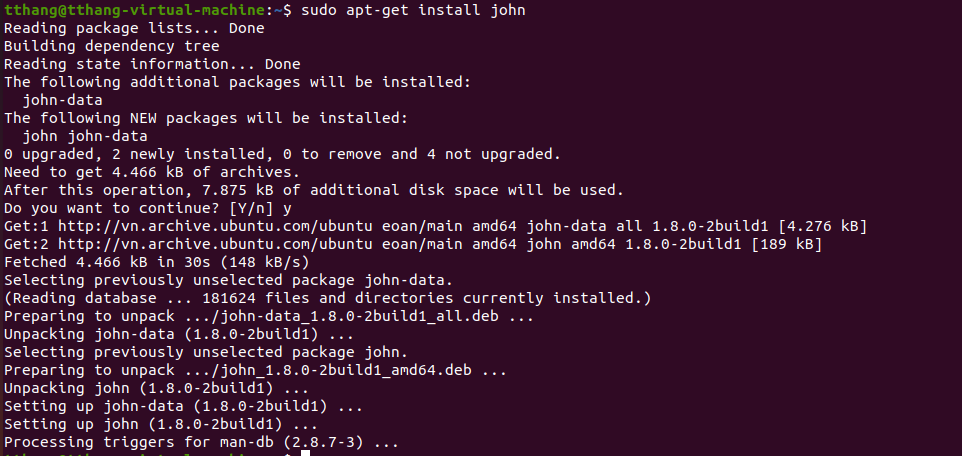
1. To look for specific information about password changes within auth.log, type:

* Xem sự thay đổi của các tài khoản bằng lệnh grep:



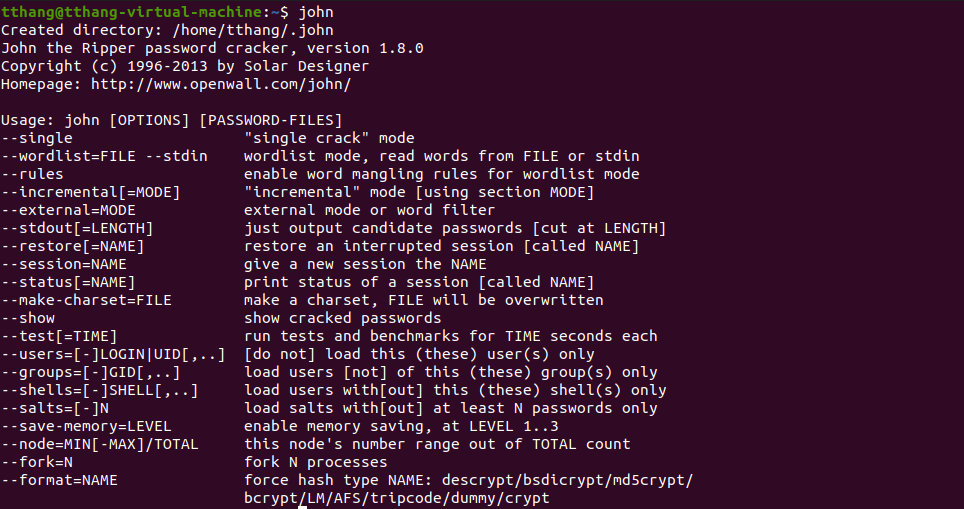
1. Install john by typing the following command:

* Cài đặt John the Ripper



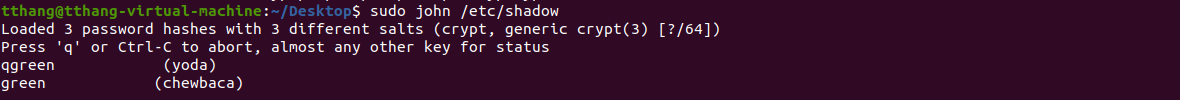
1. Type the following command to see available switches for the john command:

* Hiển thị các lệnh có sẵn với john



1. Type the following command to attempt to crack the passwords with john:

* Bẻ khoá mật khẩu với john chạy bằng quyền root



1. To view the password hashes and corresponding passwords, type the following:

* Xem mật khẩu được hash trong tệp john.pot



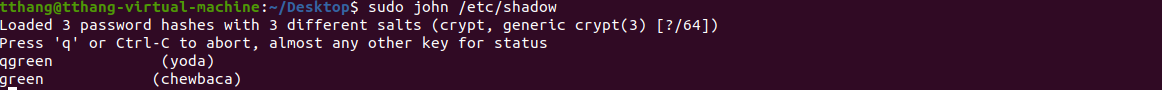
1. Type the following command to attempt to crack the passwords with john
2. Type the following command to remove the existing john.pot file:

* Xoá thông tin trong file /root/.john/john.pot



1. Type the following command to re-crack the passwords with john

* Tiếp tục bẻ khoá mật khẩu bằng lệnh john sau khi xoá thông tin trong tập tin john.pot



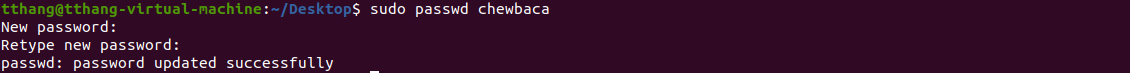
1. To view the first 20 lines of the file, type the following command in the terminal:

Xem 20 dòng đầu tiên trong file /usr/share/john/password.lst



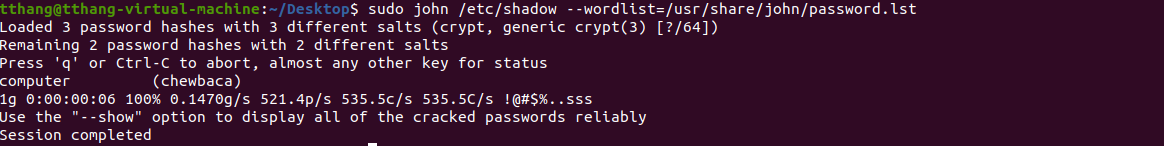
1. Set chewbacca’s password to computer by typing computer twice after typing

* Thay đổi mật khẩu user chewbaca thành “computer”



1. Type the following to run john again and the new password hash will be loaded

* Bẻ khoá mật khẩu với tập tin password.lst



1. To view the last 20 lines of the file, type the following command in the terminal:

* Xem 20 dòng cuối file password.lst



1. Set chewbaca’s password to 1q2w3e4r by typing twice after typing:

* Đổi mật khẩu user chewbaca thành “1q2w3e4r”



1. Type the following to run john again and the new password hash will be loaded:

* Tiếp tục bẻ khoá mật khẩu 1 lần nữa với tập tin password.lst

