sử dụng John the Ripper để giải mã một số băm từ Windows và Linux

. Để sử dụng Hashcat để giải mã các băm mật khẩu từ các hệ thống Windows và Linux

· Để phân tích cách các tập tin quy tắc của Hashcat có thể giúp giải mã các băm thành công hơn

. Để so sánh hiệu suất của Hashcat với John the Ripper"

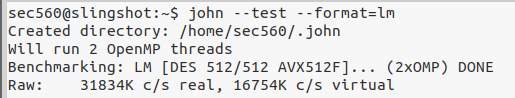
# 1. Benchmark John

John the Ripper (John) đã được cài sẵn. Đầu tiên call John ở test mode và thử nghiệm một vài loại hash khác nhau.

Thử xem tốc độ crack pass LM của John:

Tốc độ xử lý thực tế: 76742K ký tự mỗi giây

Tốc độ xử lý ảo: 39970K luồng xử lý ảo mỗi giây



Thử mã hóa md5:

Thực hiện benchmark hiệu suất với nhiều loại salt:

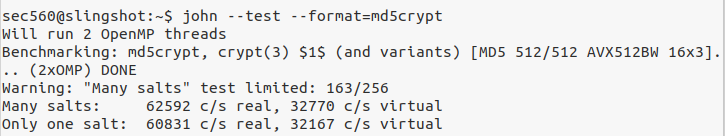
Tốc độ xử lý thực tế: 130368 ký tự mỗi giây

Tốc độ xử lý ảo: 66176 luồng xử lý ảo mỗi giây

Thực hiện benchmark hiệu suất với một loại salt:

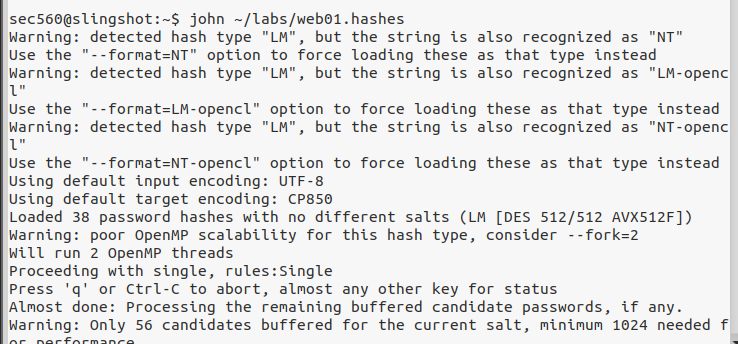
Tốc độ xử lý thực tế: 135730 ký tự mỗi giây

Tốc độ xử lý ảo: 69236 luồng xử lý ảo mỗi giây



# 2. Cracking windows hashes with John (LM)

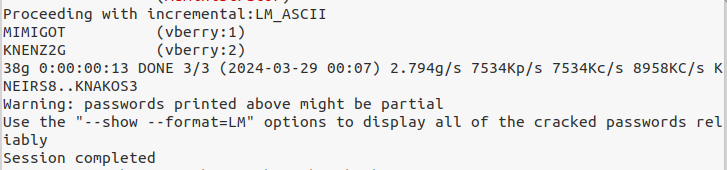
Giờ ta sẽ bẻ khóa một số giá trị hash trong tệp webe1.hashes có sẵn trên máy. Theo mặc định, John sẽ tập trung vào các giá trị hashes LM



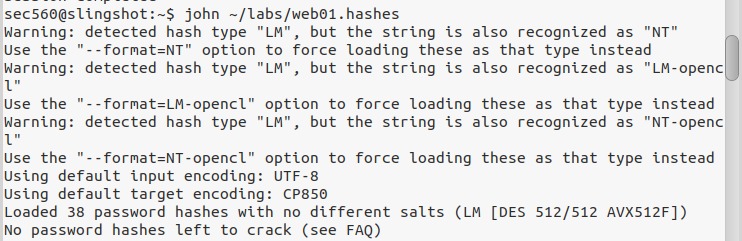
John đã phát hiện hàm băm là LM (LANMAN).

Note: pass mà John đã bẻ khóa được viết hoa hoàn toàn do LM chuyển hết password thành chữ hoa. Đồng thời, nếu password > 14 ký tự, LM sẽ chia nó làm 2 phần mỗi phần 7 ký tự, sử dụng DES key để mã hóa mỗi phần riêng biệt. Nửa đầu được biểu thị bằng username:1 và nửa sau là username:2

Nhận thấy rằng mật khẩu của hầu hết các tài khoản (dmckenzie và ckhan) đều có mật khẩu LM trống. Tuy nhiên user vberry có hash LM và John đã bẻ khóa. Không có user vberry:1 của vberry:2, đó là 2 phần của password. Kết hợp cả hai ta có password LM đầy đủ, MIMIGOTKNEN2G.

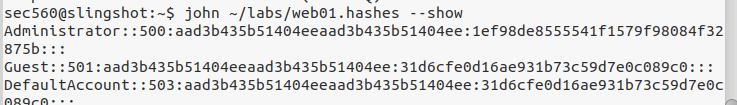


Chạy lại lệnh trên. Lưu ý rằng lần chạy thứ hai này các password tương tự không bị bẻ khóa:



Nếu John đã crack mật khẩu thì sẽ không crack lại nữa.

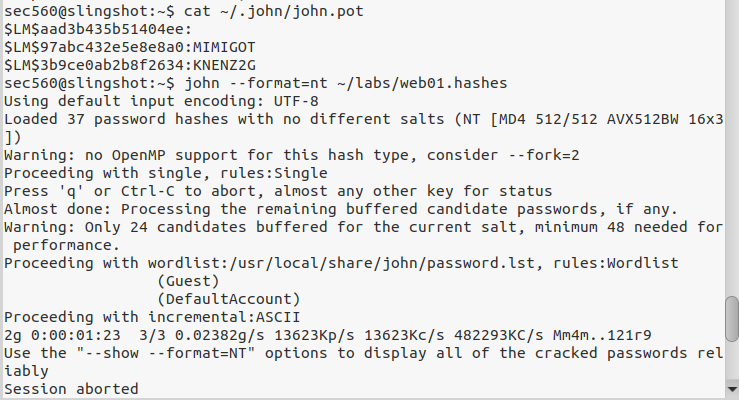
Để xem password đầy đủ (ghép 2 phần, mỗi phần 7 ký tự của LM pass lại với nhau) mà John crack thì chạy option –show:





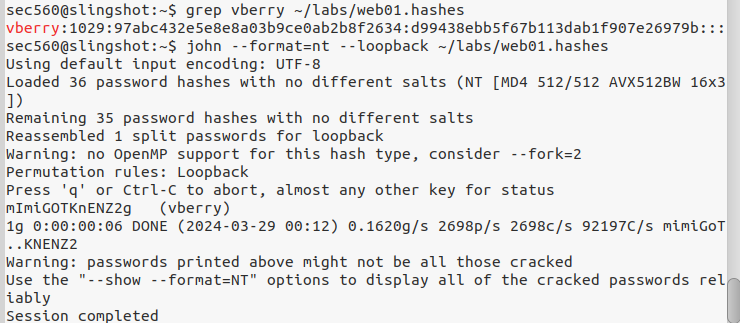
Lệnh này tìm kiếm các giá trị hashes trong webel.hashes bên trong tệp john.pot để in toàn bộ password được liên kết với user.

Dùng John bẻ khóa NT hash bằng option –format=nt. Mật khẩu trên hệ thống mục tiêu không có trong danh sách mật khẩu mặc định của John. Với NT thì mật khẩu khó bị bẻ khóa hơn LM



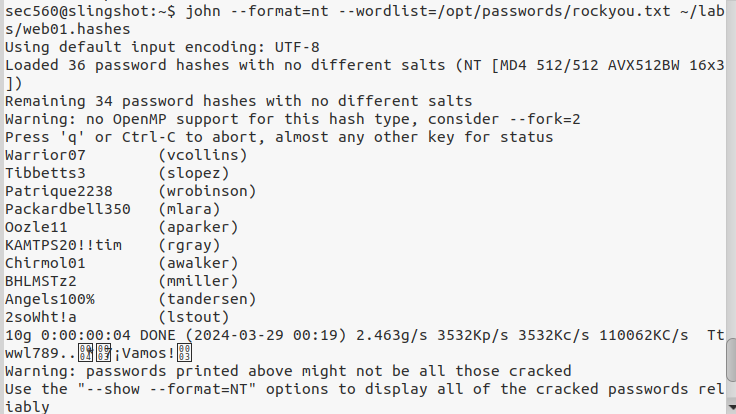
Ở đây có cả hash của LM và NT. LM hash bị bẻ khóa và cung cấp password viết hoa, có thể sử dụng password viết hoa này với NT password để khôi phục mật khẩu ban đầu.

Sử dụng password đã được viết hoa để so sánh với NT hash nhằm lấy mật khẩu có cả chữ hoa và thường, sử dụng options –loopback cho phép sử dụng tệp pot (lưu trữ hash/password đã bị crack) làm đầu vào của cracker => **Pass: mImiGITKnENZ2g**



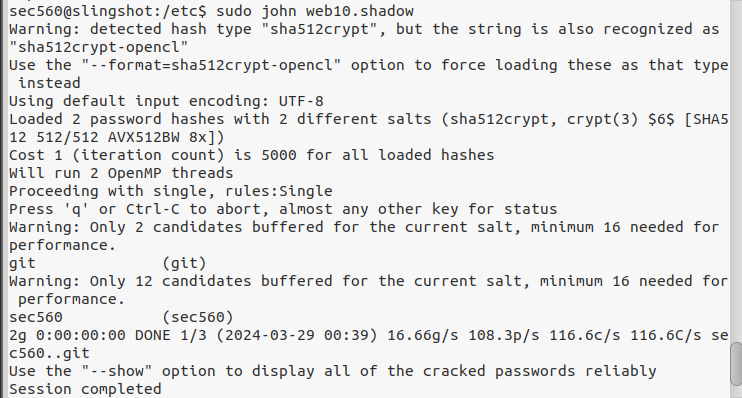
# 3. Cracking passwords with John and a Wordlist

Dùng wordlist rockyou.txt để tấn công NT hash phân biệt chữ hoa chữ thường:



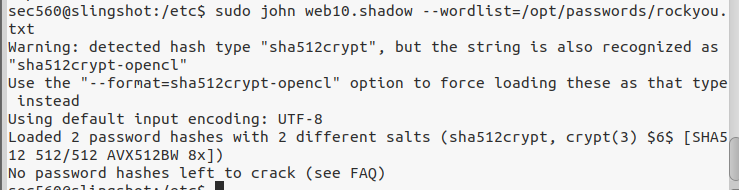
# 4. Cracking Linux passwords with John

Chạy John với file shadow



John không thể crack password này bằng danh sách mặc định

Sử dụng vói wordlist rockyou



Nhận thấy thuật toán sha512crypt mất nhiều thời gian hơn để bẻ khóa. Thuật toán này dùng salt và nhiều vòng băm không giống NT không dùng salt và một vòng băm duy nhất.

# 5. Hashcat basics

Theo sau option -m là loại hash, -a là chế độ tấn công: tức liệu Hashcat có sử dụng từ điển của mình không. Option -a hỗ trợ:

**0: Straight**: Mode này sử dụng các từ trong từ điển khi chúng xuất hiện trong từ điển Hashcat, với các quy tắc được áp dụng được chỉ định bởi option -r. VD: letmeni và password

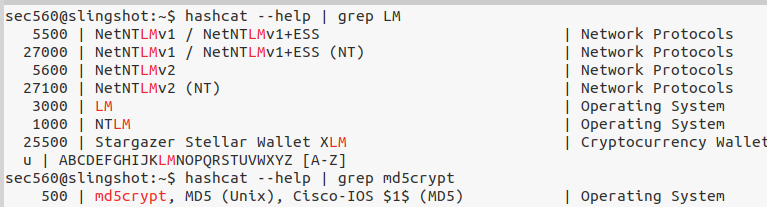
**1: Combination**: Mode này lấy từng từ trong từ điển và nối nó vào, về cơ bản là bình phương số lượng mật khẩu có khả năng từ một tệp từ. Nó cũng áp dụng các quy tắc được chỉ định bởi option -r (nếu có) cho các từ kết hợp. VD: letmeinpassword và passwordletmein

**3: Vét cạn**. Mode này thử tất cả các mật khẩu có khả năng trong một keyspace cho trước, thử lặp tất cả các ký tự. VD: 000, 001, 002

**6: Hybrid + Mask**: Mode này dùng từ điển nhưng thêm cả vét cạn. VD: letmein000,..

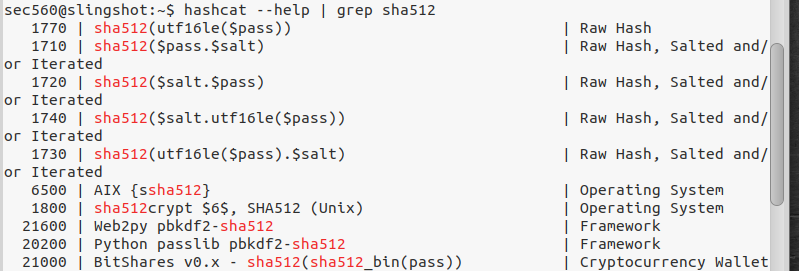
Ở lab này ta sẽ sử dụng -a e làm hình thức tấn công phổ biến, đơn giản nhất.

Tìm các giá trị hash LANMAN:



Ở phần output ta thấy 3000 | LM … cho biết nếu muốn bẻ khóa hash LM, mình sẽ gọi Hashcat với -m 3000

Tìm các giá trị hash sha512:



Thực hiện một số benchmark, bắt đầu bằng -m 3000 với LM hash. Lưu ý sẽ gọi Hashcat bằng flag -w 3, nghĩa là số lượng Workload Profile- cấu hình công việc (-w) bằng 3. Các option khác nhau cho -w bao gồm:

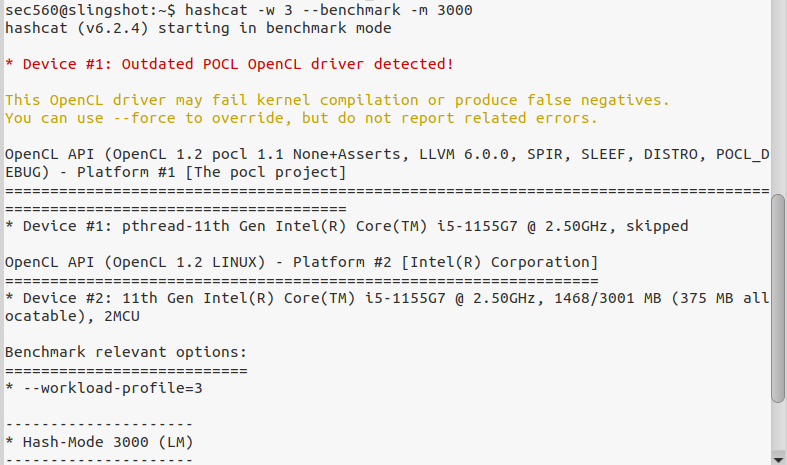
1: Low. Tác động tối thiểu lên hiệu suất GUI và mức tiêu thụ điện năng

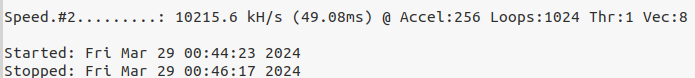
2: Default: Tác động nhẹ đến GUI và mức tiêu thụ điện năng tiết kiệm

3: High: Tiêu thụ điện năng cao và GUI có thể not responding

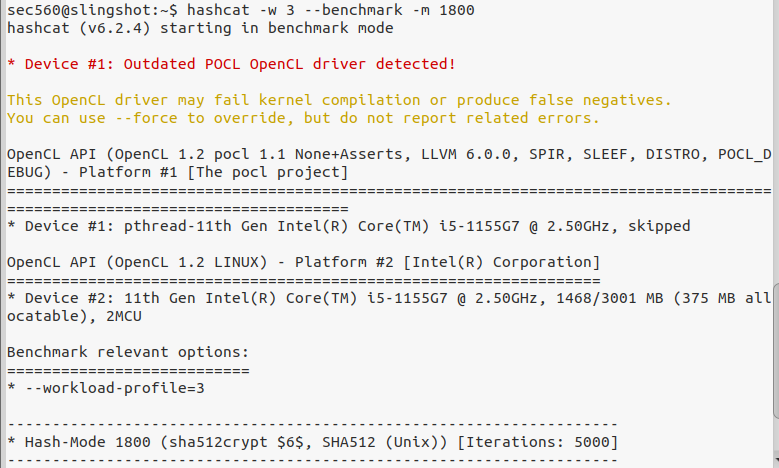
4: Nightmare: Tiêu thụ điện năng cực cao và server headless vì GUI không có đủ CPU hoặc GPU để respond

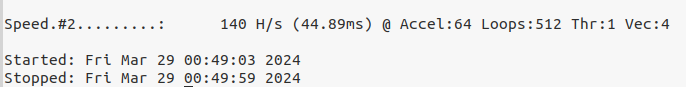
Ở lab này dùng -w 3 để có thể đạt được hiệu suất cao hơn khoảng 30% và GUI đủ để respond tiến hành lab.





10215 kh/s

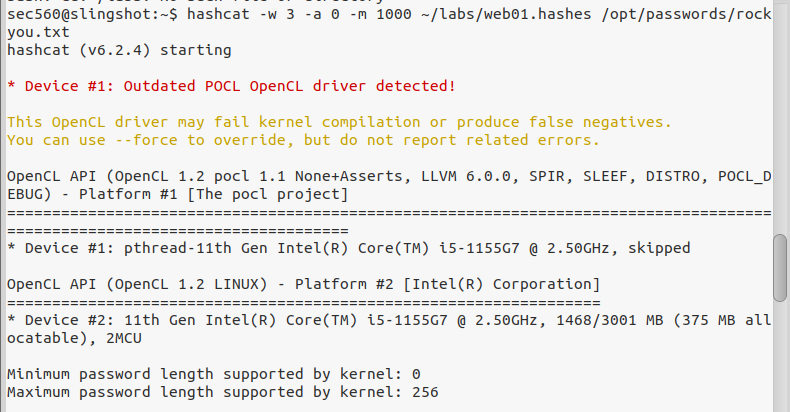




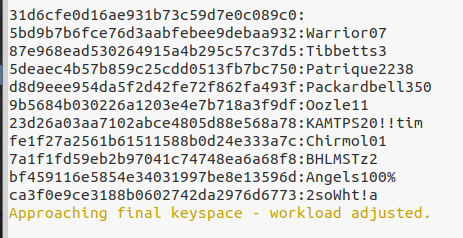
140H/s

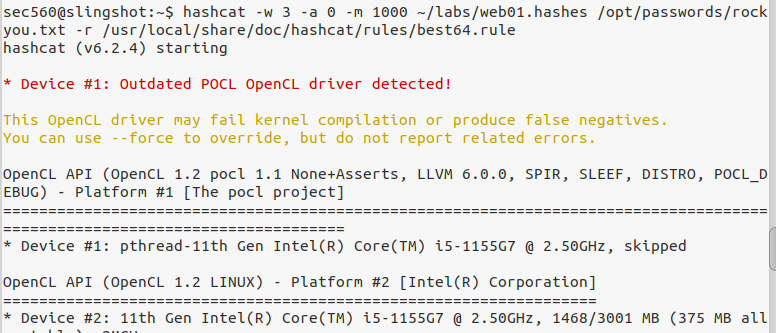
# 6. Cracking with hashcat

Tập trung vào NT hash, sử dụng từ điển rockyou và file web01.hashes

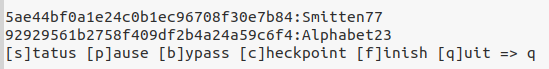


Bẻ khóa được 10 passwords

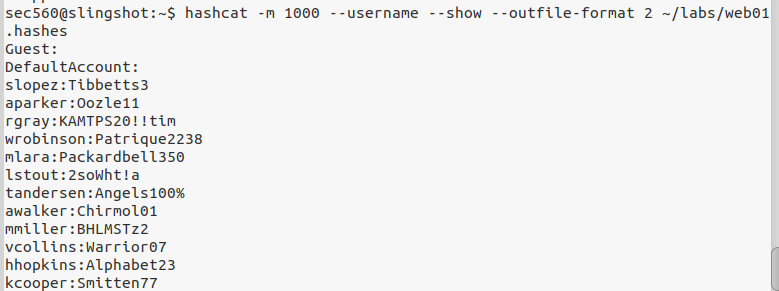




Hashcat bỏ 11 hashes vì nó đã bị crack trước đó.



Xem thông tin sau khi crack bằng hashcat

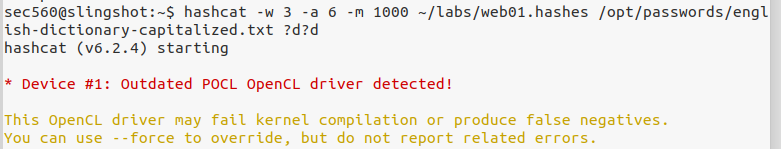


# 7.Hashcat and Masking

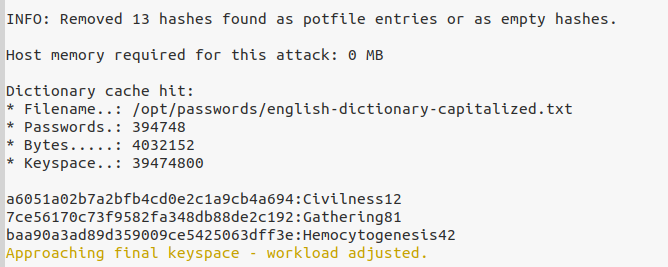
Thử tấn công mask bằng cách sử dụng tất cả các số có 2 chữ số. Ngoài ra dùng từ điển tiếng Anh làm từ điển password cơ bản. Dùng chế độ tấn công mode 6: hybrid +mask.

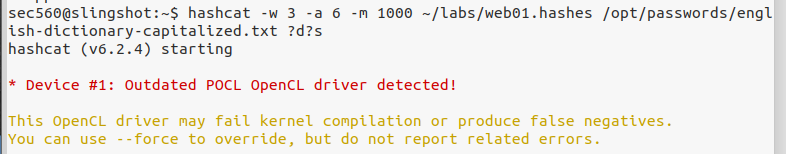
Ở đây có ?d?s: Tức là thêm 1 ký tự số và 1 ký tự đặc biệt.

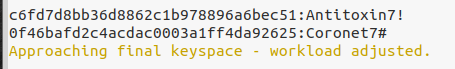
-m là chỉ định kiểu hàm băm sẽ dùng, ví dụ ở đây là NT hash (1000), sha512(1800)



hói quen đặt pass thường là 1 cụm từ với 1 ký tự đặc biệt, 1 chữ số





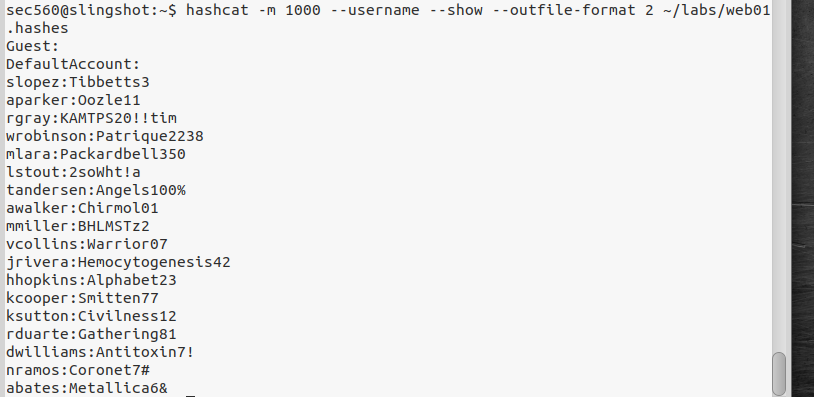


Thử lại với từ điển rockyou:



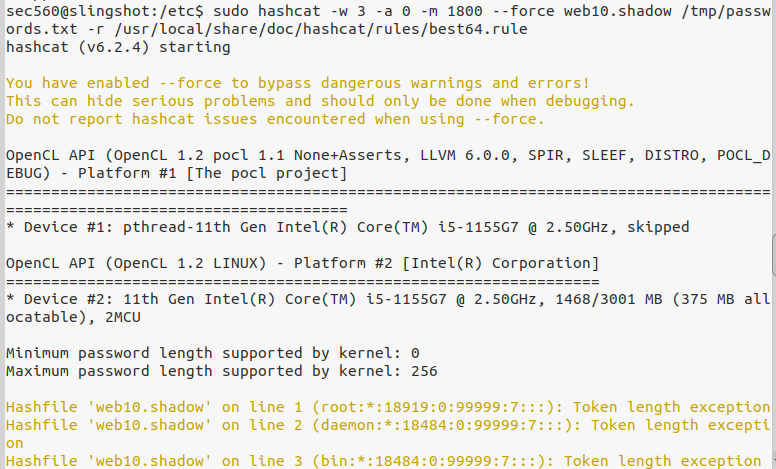


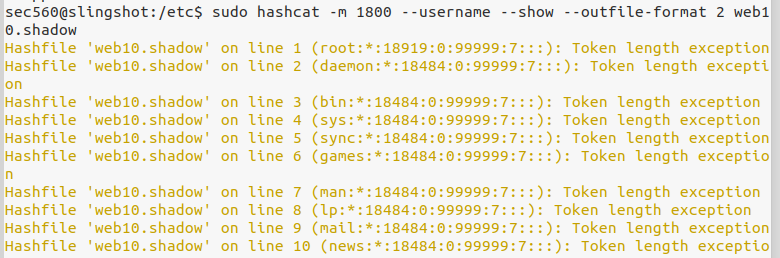
xem lại những password đã bị bẻ khóa:



# 8. Cracking Linux passwords with Hashcat

Hashcat để crack hash Linux:







Xem potfile của Hashcat. Ở đây sẽ thấy tất cả hash và password bị bẻ khóa.

