John the Ripper : password cracking

Hỗ trợ nhiều thuật toán: md5, sha, des, blowfish, ntlm

Các phương thức tấn công: Dictionary, brute force, hybrid, …

Web10 là nơi lưu giữ mật khẩu máy Linux

1. Benchmark John

Kiểm tra hiệu suất của 2 thuật toán lm và md5crypt

A screenshot of a computer program

AI-generated content may be incorrect.

1. Cracking windows hashes with John LM

Crack hashes trong file web01.hashes.

Chay john với tùy chọn mặc định để tập trung vào LM hashes

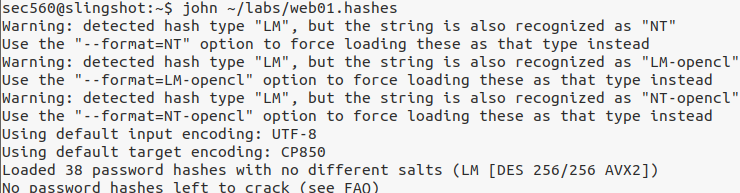
A screenshot of a computer program

AI-generated content may be incorrect.

John phát hiện được hash là LM. Nhưng để ý rằng mật khẩu mà John crack sẽ là viết hoa hết. Và John sẽ crack 7 kí tự đầu tiên và 7 kí tự sau hoàn toàn riêng biệt, coi mỗi nửa như thế là 1 mật khẩu khác nhau. Nửa đầu của user1, nửa sau là user2.

Như trên vberry1 hay vberry2 ko phải là user mà là 2 nửa của mật khuẩ. Kết hợp lại ta được full LM passwords

Chạy lại và mật khẩu sẽ ko được crack



Xem lại mật khẩu vừa crack



A close up of a computer code

AI-generated content may be incorrect.

Tiếp tục sử dụng John để crack nt hash bằng tùy chọn –format =nt

A screenshot of a computer screen

AI-generated content may be incorrect.

Có thể thấy quá trình xảy ra rất chậm vì mật khẩu ko nằm trong danh sách mật khẩu mặc định của John

Ta sẽ lợi dụng pot file ( lưu trữ những hash đã dược crack) đẻ có thể dễ dàng crack NT hash

A screenshot of a computer program

AI-generated content may be incorrect.

Thành công crack NT hash

1. Cracking Passwords with John and a Wordlist

Sử dụng file rockyou.txt

A screenshot of a computer program

AI-generated content may be incorrect.

Tìm được 10 user có mật khẩu trong file

1. Cracking Linux password with John

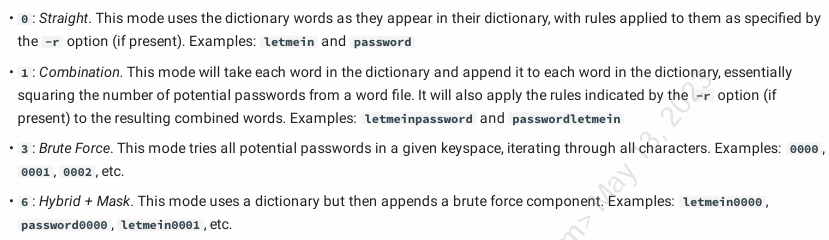
Ko thể crack bằng cách mặc định. Vì thế tiếp tục sử dụng file rockyou

A screenshot of a computer screen

AI-generated content may be incorrect.

Ở đây mật khẩu được mã hóa bằng sha512 nên sẽ tốn rất nhiều thời gian để crack. Thuật toán này khác với NT vì nó có thêm salt và có nhiều quá trình hash

1. Hashcat basics



Tìm những số thứ tự ứng với những loại hash khác nhau. Ta tìm được

LM – 3000

Md5crypt – 500

Sha512 – 1800

Kiểm tra hiệu suất của hashcat

* Với LM hash

A screen shot of a computer

AI-generated content may be incorrect.

* Với md5crypt

A screenshot of a computer program

AI-generated content may be incorrect.

* Với sha512

A screenshot of a computer

AI-generated content may be incorrect.

1. Cracking with Hashcat

Sử dụng Hashcat và Rockyou file để crack password trong web01.hashes

**hashcat -w 3 -a 0 -m 1000 ~/labs/web01.hashes /opt/passwords/rockyou.txt**

**-w 3: hiệu suất ở cấp 3**

**-a 0: dictionary attack**

**-m 1000: NTLM hash**

**A screenshot of a computer code

AI-generated content may be incorrect.**

Crack được 10 mật khẩu

Xem những rule trên hashcat

A computer screen shot of a computer code

AI-generated content may be incorrect.

Có rất nhiều rule và hãy sử dụng 1 trong những cái hữu dụng nhất là best64.rule

A screenshot of a computer

AI-generated content may be incorrect.

Lấy được 30 rule trong best64 hay sử dụng nhất như: đảo ngược pass, viết hoa chữ cái đầu, viết hoa mật khẩu hay là thêm 0 hoặc 00… vào sau mật khẩu

Hãy thử crack lại với file best64

A screenshot of a computer error

AI-generated content may be incorrect.

Tìm được thêm 2 mật khẩu và kết quả thì đã loại bỏ đi 11 hashes đã crack trước đó

Xem kết quả

A white background with black text

AI-generated content may be incorrect.

1. Hashcat and masking

Mặc dù những rule rất hữu ích, nhưng ta có thể tự tạo những rule theo ý mình. Nếu bạn muốn thêm vào 2 số đằng sau mật khẩu, b có thể dung ?d?d.

**hashcat -w 3 -a 6 -m 1000 ~/labs/web01.hashes /opt/passwords/english-dictionary-capitalized.txt ?d?d**

A screen shot of a computer

AI-generated content may be incorrect.

Tìm được thêm mật khẩu mới

Thêm 1 số và 1 kí tự đặc biệt

**hashcat -w 3 -a 6 -m 1000 ~/labs/web01.hashes /opt/passwords/english-dictionary-capitalized.txt ?d?s**

**A screenshot of a computer

AI-generated content may be incorrect.**

Tìm được thêm 2 mật khẩu

Sử dụng file rockyou và thêm 1 số + 1 kí tự đằng sau

**hashcat -w 3 -a 6 -m 1000 ~/labs/web01.hashes**

**/opt/passwords/rockyou.txt ?d?s**

**A screenshot of a computer error

AI-generated content may be incorrect.**

Tìm được thêm 1 mật khẩu

**A computer screen shot of a computer

AI-generated content may be incorrect.**

**Đây là tất cả mật khẩu t đã crack được**

1. Cracking Linux passwords with Hashcat

Crack hashes từ web10 bằng Hashcat.

Ta sẽ thêm tất cả các mật khẩu đã được crack vào 1 file để có thể sử dụng cho việc crack khi sau.

Thêm mật khẩu vào file passwords.txt

A screenshot of a computer

AI-generated content may be incorrect.

Ta sẽ sử dụng mật khẩu trong file để crack. Ngoài ra sử dụng thêm những biến thể trong file best64.rules

**Hashcat -w 3 -a 0 -m 1800 ~/labs/web10.shadow /tmp/passwords.txt -r /usr/local/share/doc/hashcat/rules/best64.rule**

**A screenshot of a chat

AI-generated content may be incorrect.**

Tìm được 2 mật khẩu

**A screenshot of a computer error

AI-generated content may be incorrect.**

Xem kết quả

A screenshot of a computer program

AI-generated content may be incorrect.



