**John The Ripper**

Các thuật toán hashing được thiết kế để chúng chỉ hoạt động 1 chiều. Một hash không thể đảo ngược về plain-text ban đầu.

Mặc dù thuật toán không thể đảo ngược. Điều đó không có nghĩa là bẻ khóa hàm băm là không thể. Nếu bạn biết thuật toán hashing, bạn có thể dùng nó để hash 1 lượng lớn các từ trong wordlists. Sau đó so sánh chúng với hash bạn muốn crack.

Quá trình này gọi là dictionary attack và John the Ripper là 1 công cụ cho phép bạn thực hiện các cuộc tấn công dồn dập trên 1 danh sách lớn các loại hash.

**Cracking Basic Hashes**

**Cú pháp John cơ bản:**

john [options] [path to file]

**Automatic Cracking**

John có những tính năng được dựng sẵn để phát hiện loại hash và chọn các quy tắc thích hợp để crack nó. Đây không phải là ý tưởng tốt vì nó có thể không đáng tin.

john --wordlist=[path to wordlist] [path to file]

**Xác định hashes**

Thỉnh thoảng John không tự động nhận dạng và tải được hash.

Ta có thể dùng 1 công cụ khác để xác định hash và sau đó chỉ định John định dạng phù hợp.

wget https://gitlab.com/kalilinux/packages/hash-identifier/-/raw/kali/master/hash-id.py

**Format-Specific Cracking**

Khi bạn xác định được hash, bạn có thể yêu cầu john dùng nó trong khi crack hash:

john --format=[format] --wordlist=[path to wordlist] [path to file]

Ví dụ: john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash\_to\_crack.txt

**Lưu ý ở các định dạng:**

Khi bạn yêu cầu john dùng định dạng, nếu bạn gặp 1 hash type chuẩn như md5, bạn phải thêm tiền tố raw-

Để kiểm tra bạn có cần thêm tiền tố hay không, bạn có thể liệt kê tất cả định dạng của John:

john --list=formats

john --list=formats | grep -iF “md5”

**Cracking Windows Authentication Hashes**

Hashes xác thực là mật khẩu được hash lưu trữ bởi hệ điều hành. Có thể crack nó bằng phương pháp brute force chúng ta đã dùng. Để có được những hash như vậy, bạn phải là người dùng có đặc quyền.

**NTHash/NTLM**

NTHash là 1 định dạng hash mà hệ điều hành Windows sẽ lưu trữ người dùng và các mật khẩu dịch vụ.

Bạn có thể lấy được NTHash/NTLM hashes bằng cách dùng tool Mimikatz dump cơ sở dữ liệu SAM trên Windows hay từ cơ sở dữ liệu Active Directory: NTDS.dit. Bạn có thể không cần phải bẻ khóa hàm băm để tiếp tục leo thang đặc quyền, thay vào đó bạn thường có thể tiến hành 1 cuộc tiến công vượt qua hàm băm.

**Cracking /etc/shadow Hashes**

File /etc/shadow là tập tin trên máy ảo Linux lưu trữ hash của mật khẩu. Nó cũng lưu trữ thông tin khác như ngày mật khẩu thay đổi lần cuối và thông tin mật khẩu hết hạn. Nó chứa mỗi dòng cho mỗi người trên hệ thống. Tập tin này chỉ được truy cập bởi root.

**Unshadowing**

John có thể rất cụ thể về các định dạng nên nó cần thêm dữ liệu để làm việc chung. Để bẻ khóa /etc/shadow, bạn phải kết hợp nó với /etc/passwd. Để làm được điều đó, bạn dùng 1 công cụ được dựng sẵn trong John gọi là unshadow

unshadow [path to passwd] [path to shadow]

Ví dụ: unshadow local\_passwd local\_shadow > unshadowed.txt

Lưu ý: khi dùng unshadow, chúng ta có thể dùng toàn bộ /etc/passwd và /etc/shadow hoặc chỉ dùng 1 dòng từ mỗi tập tin.

File 1: local\_passwd

root:x:0:0::/root:/bin/bash

File 2: local\_shadow

root:$6$2nwjN454g.dv4HN/$m9Z/r2xVfweYVkrr.v5Ft8Ws3/YYksfNwq96UL1FX0OJjY1L6l.DS3KEVsZ9rOVLB/ldTeEL/OIhJZ4GMFMGA0:18576::::::

**Cracking**

john --wordlist=/usr/share/wordlists/rockyou.txt --format=sha512crypt unshadowed.txt

**Single Crack Mode**

Đến nay chúng ta đã quen với việc dùng wordlist mode của John. Nhưng John cũng có 1 chế độ khác gọi là Single Crack. Trong chế độ này, John chỉ dùng thông tin được cung cấp trong username để thử và tìm ra các mật khẩu theo kinh nghiệm bằng cách thay đổi một chút các chữ cái và số chứa trong username.

**Xáo trộn từ**

Cách tốt nhất để hiểu Single Crack mode là gì và word mangling là gì, đi qua 1 ví dụ sau:

Nếu ta lấy username: Markus

Mật khẩu có thể là:

* Markus1, Markus2, Markus3 (etc.)
* MArkus, MARkus, MARKus (etc.)
* Markus!, Markus$, Markus\* (etc.)

Kĩ thuật này gọi là xáo trộn từ. John đang dựng 1 từ điển dựa theo thông tin nó lấy được và sử dụng một bộ quy tắc được gọi là “quy tắc xáo trộn” xác định cách nó có thể biến đổi từ mà nó bắt đầu để tạo danh sách từ dựa trên các yếu tố liên quan đến mục tiêu mà bạn muốn bẻ khóa. Nó đang khai thác những mật khẩu yếu dựa trên thông tin về username hay dịch vụ nó đang đăng nhập.

**GECOS**

Gecos là gì? Nhớ trong bài trước chúng ta tìm kiếm các điểm vào ở /etc/shadow và /etc/passwd? Nếu bạn nhìn kỹ bạn sẽ thấy mỗi field cách nhau bằng dấu “:”. Mỗi field mà các bản ghi này được chia thành gọi là Gecos fields. John có thể lấy thông tin được lưu trong mỗi bản ghi như full name và tên thư mục home để thêm vào trong wordlist nó tự tạo khi bẻ /etc/shadow với single crack mode.

**Using Single Crack Mode**

Ví dụ chúng ta muốn bẻ gãy mật khẩu của user tên Mike bằng single mode:

john --single --format=[format] [path to file]

john --single --format=raw-sha256 hashes.txt

**Lưu ý:**

Nếu bạn muốn crack hashes trong chế độ single crack, bạn cần thay đổi định dạng file để john tự tạo wordlist từ nó

From: 1efee03cdcb96d90ad48ccc7b8666033

To: mike:1efee03cdcb96d90ad48ccc7b8666033

**Custom Rules**

Trong chế độ Single Crack Mode, bạn có thể khai báo 1 bộ quy tắc mà John sẽ dùng nó để tự động tạo mật khẩu. Điều này rất hữu ích khi bạn biết thêm thông tin về cấu trúc của mật khẩu khi tấn công.

**Common Custom Rules**

Nhiều tổ chức sẽ yêu cầu mật khẩu phức tạp để thử và chống lại dictionary attack.

Nếu bạn tạo 1 tài khoản, nhập mật khẩu: polopassword

Bạn có thể nhận thông báo: mật khẩu phải chứa ít nhất:

* 1 kí tự hoa
* số
* kí tự đặc biệt

Điều này là tốt! Tuy nhiên, ta có thể khai thác mật khẩu dễ đoán như: Polopassword1!

**Cách tạo Custom Rules**

Custom rules được khai báo trong tập tin john.conf, đặt ở /etc/john/john.conf

Dòng đầu tiên:

[List.Rules:THMRules] : khai báo tên rule

**Regex:**

* Az: lấy từ và nối nó với các ký tự bạn xác định
* A0: lấy từ và thêm vào đầu các ký tự bạn xác định
* c: in hoa kí tự

Cuối cùng, chúng ta cần khai báo các kí tự nên nối, thêm vào đầu bằng [] theo thứ tự. Biểu thức chính quy nằm trong dấu nháy kép “”

* [0-9] - Will include numbers 0-9
* [0] - Will include only the number 0
* [A-z] - Will include both upper and lowercase
* [A-Z] - Will include only uppercase letters
* [a-z] - Will include only lowercase letters
* [a] - Will include only a
* [!£$%@] - Will include the symbols !£$%@

Đặt tất cả những thứ này lại với nhau, để tạo 1 wordlist từ các rules hợp với mật khẩu “Polopassword1!” (giả sử polopassword trong wordlist):

[List.Rules:PoloPassword]

cAz"[0-9] [!£$%@]"

**Using Custom Rules**

Chúng ta có thể gọi rule này như 1 đối số của John

john --wordlist=[path to wordlist] --rule=PoloPassword [path to file]

**Cracking Password Protected Zip Files, Rar Archive, SSH Keys**

Chúng ta có thể dùng John để crack mật khẩu bảo vệ zip file. Chuyển đổi file zip sang 1 định dạng mà John có thể hiểu

**Zip2John**

Tương tự như unshadow chúng ta đã dùng trước đó, zip2john để chuyển đổi file zip sang 1 định dạng hash mà John có thể hiểu và hi vọng crack được

zip2john [options] [zip file] > [output file]

rar2john [rar file] > [output file]

ssh2john [id\_rsa private key file] > [output file]

**Cracking**

john --wordlist=/usr/share/wordlists/rockyou.txt zip\_hash.txt

john --wordlist=/usr/share/wordlists/rockyou.txt rar\_hash.txt

john --wordlist=/usr/share/wordlists/rockyou.txt id\_rsa\_hash.txt