Lab-Project 8: Cracking Linux Password Hashes with Hashcat

**Creating a Test User:**

+ Tại terminal, sau khi truy cập user **root**, sử dụng lệnh **adduser jose1** để thêm người dùng **jose1**   
+ Khi yêu cầu nhập New password, nhập mật khẩu là **password**

**+** Nhập lại mật khẩu lần nữa, skip các thông tin khác bằng **Enter**

A computer screen shot of a computer program

Description automatically generated

**Viewing the Password Hash:**

+ Tại terminal; gõ lệnh **sudo tail /etc/shadow** sẽ hiện thị một số dòng cuối trong file **/etc/shadow**

A screenshot of a computer screen

Description automatically generated

=> Mật khẩu của **jose1** có dạng $6$...$ biểu thị mật khẩu được mã hóa theo hàm SHA512

**Understanding the Hash Algorithm:**

Thuật toán băm được định nghĩa trong tệp /etc/login.defs. Để xem phần của tệp đó thảo luận về thuật toán băm mật khẩu, thực hiện lệnh grep này để xem 18 dòng sau dòng chứa chuỗi “ENCRYPTED\_METHOD”

Lệnh: **grep -A 18 ENCRYPT\_METHOD /etc/login.defs**



A screenshot of a computer

Description automatically generated

**Making a Hash file:**

+ Trong terminal, sử dụng lệnh: **tail -n 1 /etc/shadow > crack1.hash** => Tạo 1 file có tên crack1.hash chứa dòng cuối cùng của file **/etc/shadow**

**+** Chỉnh sửa file **crack1.hash** bằng lệnh **nano crack1.hash**

**+** Trong file này, các trường ngăn cách nhau bằng dấu “:” => Giữ lại trường thứ 2 ngăn cách bởi dấu “:” (Chính là trường mật khẩu đã bị mã hóa) và xóa các trường còn lại

A screenshot of a computer

Description automatically generated

=> Nhấn **Enter** và lưu thay đổi

**Downloading a Wordlist**:

+ Download file bằng lệnh **wget** với file có đường link: “**https://raw.githubusercontent.com/danielmiessler/SecLists/refs/heads/master/Passwords/Common-Credentials/10-million-password-list-top-500.txt**”

+ Thêm option **-O** và tên **500\_password.txt** để lưu tên file tải về sẽ có tên là **500\_password.txt**

**+** Hiển thị một số dòng đầu của file bằng lệnh **head 500\_password.txt** sau khi đã tải xong file

A computer screen shot of a computer code

Description automatically generated

**Cracking the Hash:**

**+** Công cụ sử dụng: **john**

**+** Lệnh: **john --wordlist=500\_password.txt --format=sha512crypt crack1.hash**

A screen shot of a computer

Description automatically generated

=> Mật khẩu đã được giải mã

**Getting the crack2.hash List**

+ Sử dụng lệnh: [**https://samsclass.info/123/proj10/crack2.hash**](https://samsclass.info/123/proj10/crack2.hash)để tải file crack2.hash về

A screen shot of a computer

Description automatically generated

+ Xem nội dung file bằng lệnh: **cat crack2.hash**

A computer screen shot of white text

Description automatically generated

**Cracking the Hashes:**

+ Sử dụng lệnh: **john --wordlist=500\_password.txt --format=sha512crypt crack2.hash**

A computer screen shot of a computer program

Description automatically generated

=> Các dòng mã hóa đã được giải mã