HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO

BÀI 12: Crack mật khẩu

Giảng viên hướng dẫn: Vũ Minh Mạnh

Sinh viên thực hiện: Nguyễn Quốc Vượng

Mã sinh viên: B21DCAT227

Lớp: D21CQAT03-B

Hà Nội, 2023

Môn học Thực tập cơ sở

Bài 12: Crack mật khẩu

1. Mục đích

- Hiểu được mối đe dọa về tấn công mật khẩu.
- Hiểu được nguyên tắc hoạt động của một số công cụ Crack mật khẩu trên các hệ điều hành Linux và Windows.
- Biết cách sử dụng công cụ để Crack mật khẩu trên các hệ điều hành Linux và Windows.

2. Nội dung thực hành

2.1. Tìm hiểu lý thuyết

Sinh viên đọc trước các nội dung liên quan đến các nội dung thực hành tại một số tài liệu như.

- Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.
- Chapter 11 Authentication and Remote Access, sách Principles of Computer Security CompTIA Security+ and Beyond Lab Manual (Exam SY0-601) by Jonathan S. Weissman

➢ **Lý thuyết về các công cụ crack mật khẩu trên hệ điều hành Windows và Linux:**

Trên hệ điều hành Windows:

Các công cụ crack mật khẩu phổ biến trên Windows bao gồm:

1. **John the Ripper**: John the Ripper là một công cụ mạnh mẽ, được sử dụng rộng rãi để crack mật khẩu trên nhiều hệ điều hành, bao gồm Windows. Nó có thể crack mật khẩu từ các định dạng khác nhau như NTLM, LM, và các định dạng khác.
2. **Hashcat**: Hashcat là một công cụ phục hồi mật khẩu hàng đầu, chủ yếu dành cho GPU. Nó hỗ trợ nhiều loại hash và cung cấp hiệu suất cao khi sử dụng GPU.

Trên hệ điều hành Linux:

Trên Linux, các công cụ crack mật khẩu thường tập trung vào việc tìm kiếm lỗ hổng trong hệ thống hoặc sử dụng các phương pháp tấn công từ điển và brute-force. Các công cụ phổ biến bao gồm:

1. **John the Ripper**: Cũng như trên Windows, John the Ripper là một công cụ phổ biến để crack mật khẩu trên Linux. Nó có thể hoạt động trên nhiều định dạng hash và hỗ trợ các phương pháp tấn công từ điển và brute-force.
2. **Hydra**: Hydra là một công cụ tấn công mật khẩu qua mạng, hỗ trợ nhiều giao thức như SSH, FTP, Telnet, và nhiều hơn nữa.
3. **Aircrack-ng**: Aircrack-ng là một bộ công cụ phục hồi mật khẩu Wi-Fi, cho phép bạn thực hiện tấn công từ điển và brute-force trên mật khẩu Wi-Fi đã thu thập.

- **Cách thức hoặc phương pháp các công cụ sử dụng để crack mật khẩu trên hệ điều hành Windows và Linux:**

Trên hệ điều hành Windows:

- **John the Ripper**:
    - Sử dụng lệnh **john.exe** để chạy John the Ripper.
    - Cung cấp tệp hash cần crack.
    - Sử dụng tùy chọn **--format** để chỉ định định dạng của hash.
    - Sử dụng tùy chọn **--wordlist** hoặc **--incremental** để chọn phương pháp tấn công từ điển hoặc brute-force.
- **Hashcat**:
    - Sử dụng lệnh **hashcat.exe** để chạy Hashcat.
    - Cung cấp tệp hash cần crack và tệp từ điển hoặc sử dụng các tùy chọn khác để chỉ định các cài đặt tấn công.
    - Hashcat sẽ sử dụng GPU để thực hiện các phép tính toán, cung cấp hiệu suất cao hơn so với các công cụ chỉ sử dụng CPU.

Trên hệ điều hành Linux:

- **John the Ripper**:

    - Sử dụng lệnh **john** để chạy John the Ripper.
    - Tương tự như trên Windows, cung cấp tệp hash và lựa chọn phương thức tấn công.
- **Hydra**:
    - Sử dụng lệnh **hydra** để chạy Hydra.
    - Cung cấp địa chỉ IP hoặc tên máy chủ, cổng và giao thức.
    - Hydra sẽ thực hiện tấn công với từ điển hoặc brute-force để đoán mật khẩu.
- **Aircrack-ng**:
    - Sử dụng các công cụ trong bộ Aircrack-ng để thu thập gói tin Wi-Fi và tạo các bảng mật khẩu.
    - Sử dụng **aircrack-ng** để thực hiện tấn công từ điển hoặc brute-force trên các bảng mật khẩu đã tạo.

Các công cụ này cung cấp các tùy chọn linh hoạt để phù hợp với nhu cầu của bạn trong việc crack mật khẩu trên cả hai hệ điều hành Windows và Linux.

2.2. Chuẩn bị môi trường

- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- Phần mềm hệ điều hành Linux và Windows

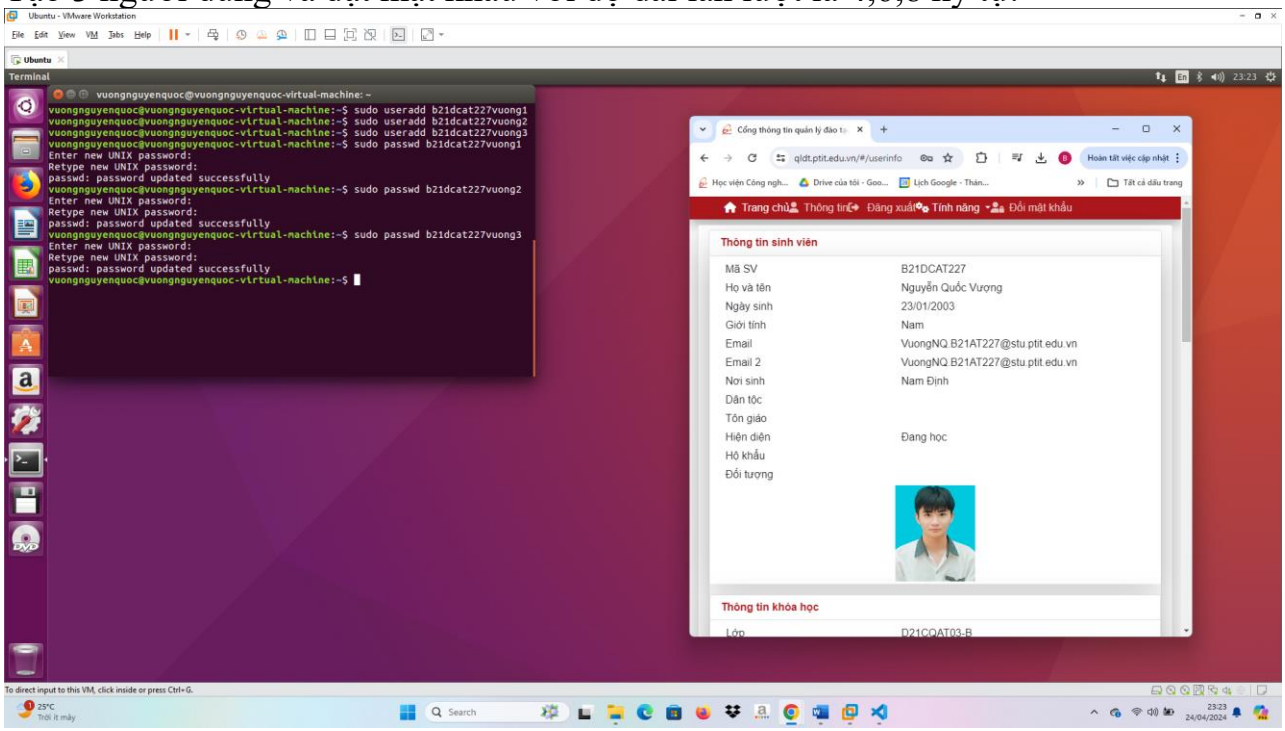
2.3. Các bước thực hiện

2.3.1. Chuẩn bị môi trường

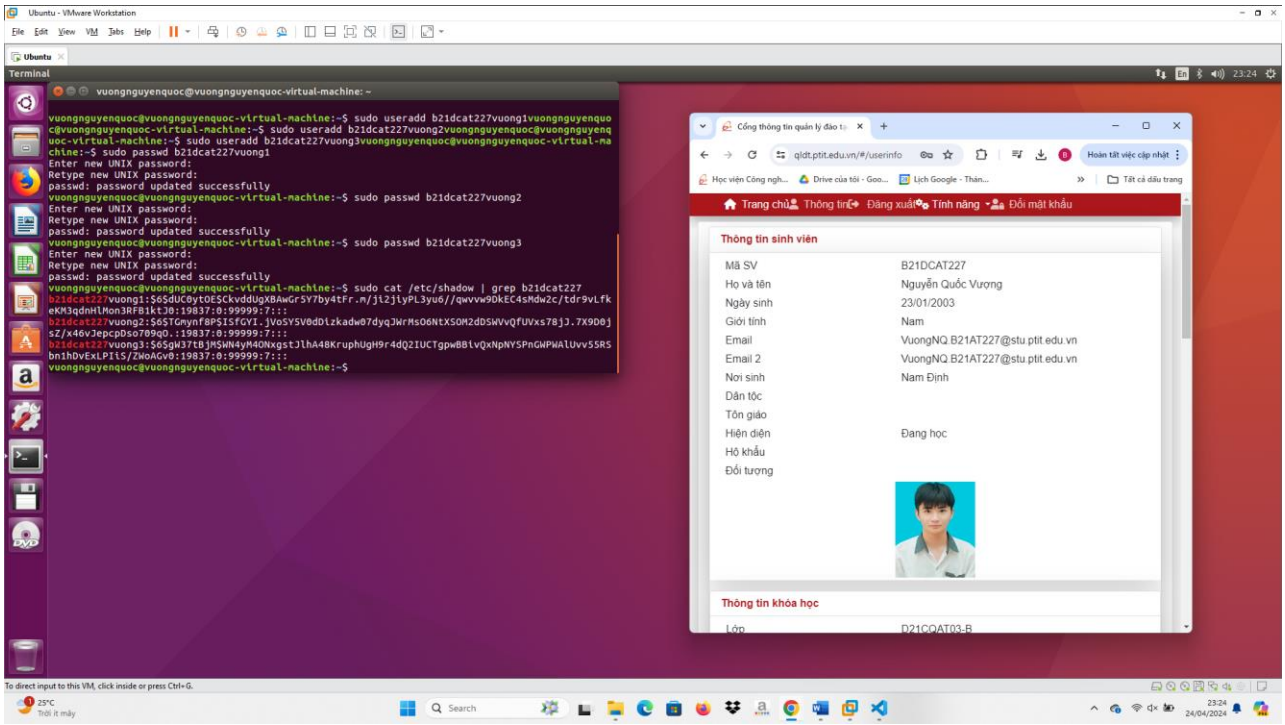
- Cài đặt công cụ ảo hóa.
- Phần mềm hệ điều hành Linux và Windows.

- Cài đặt các công cụ Crack mật khẩu trên hệ điều hành Linux

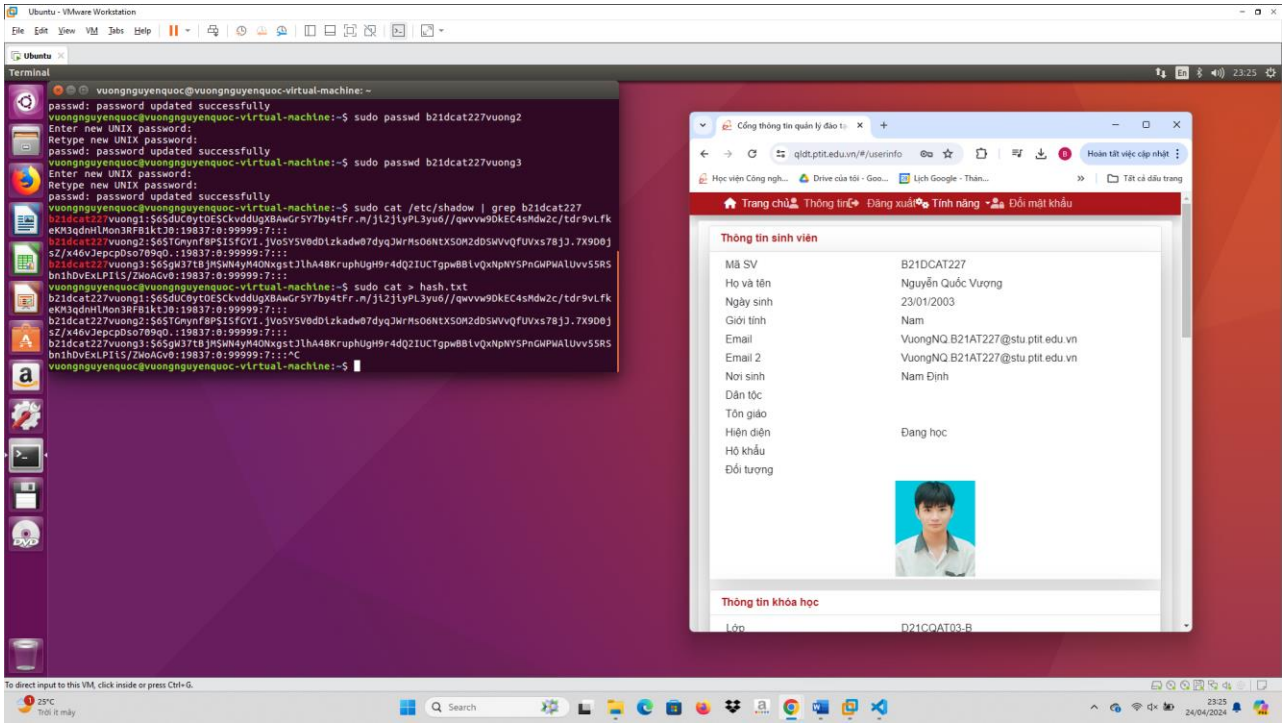
Tạo 3 người dung và đặt mật khẩu với độ dài lần lượt là 4,6,8 ký tự:



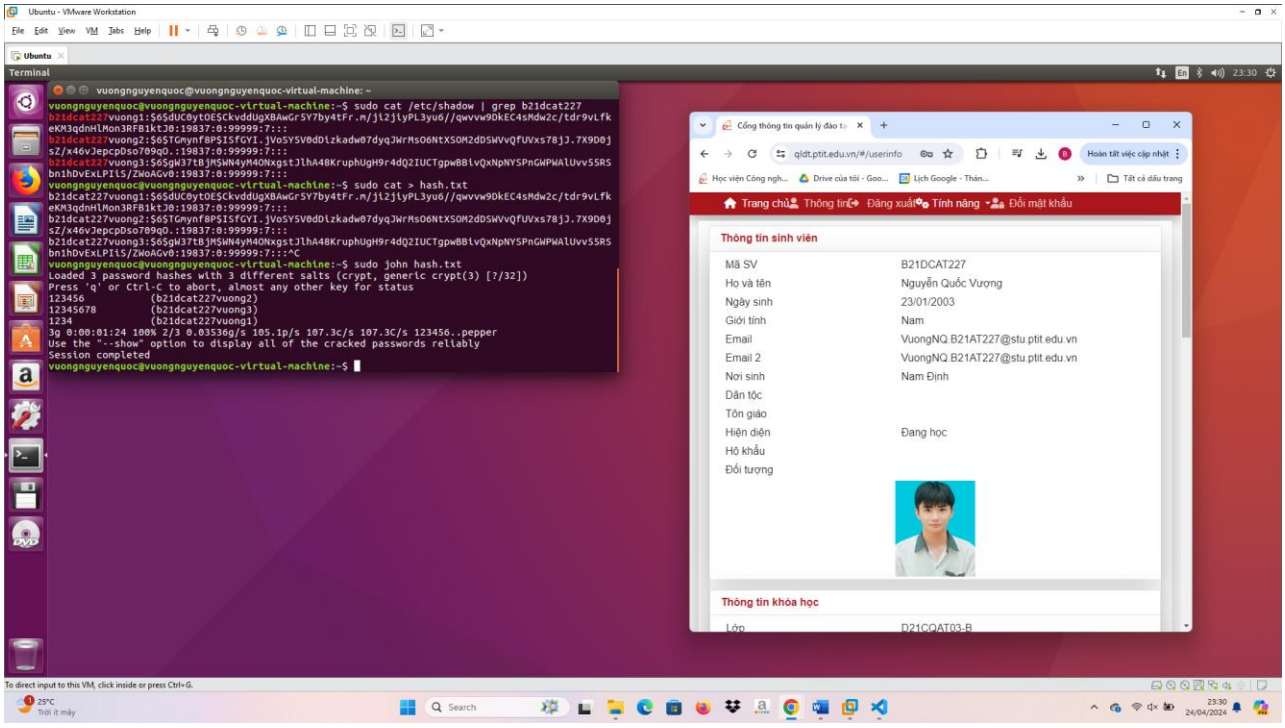
Lấy các mật khẩu đã được hash:



Lưu vào file hash.txt:

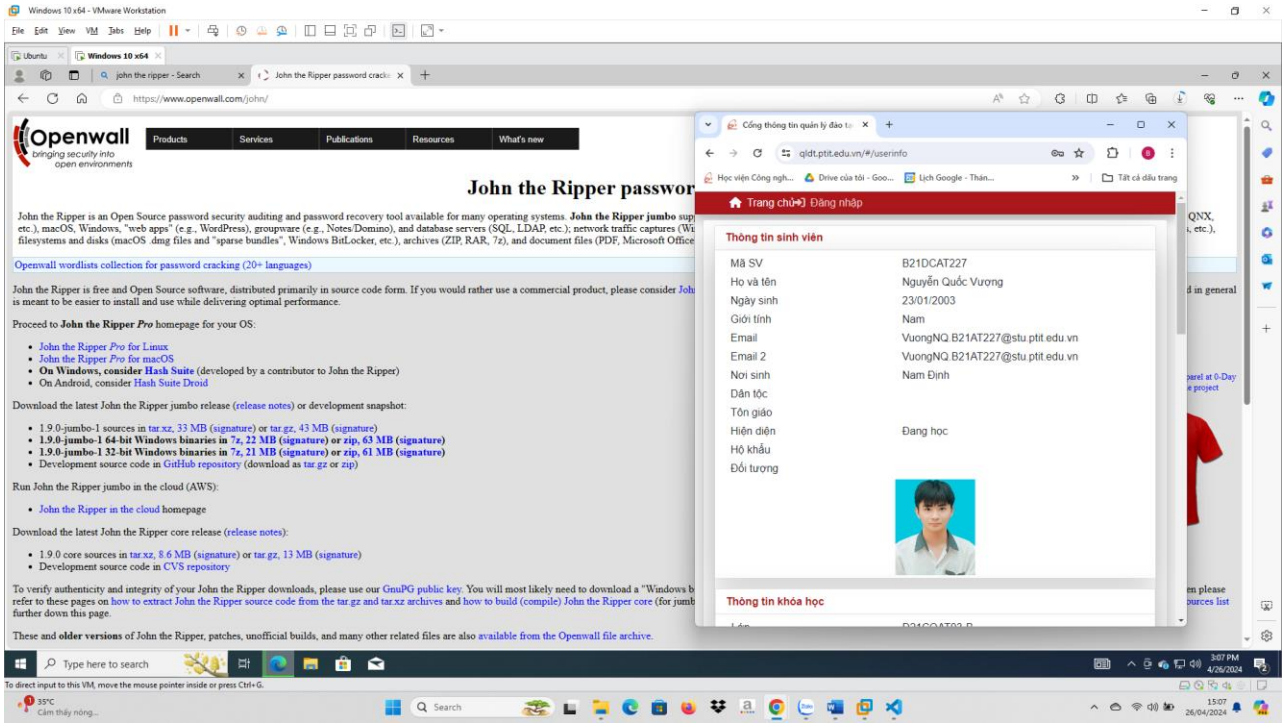


Sử dụng john the ripper để crack mật khẩu:



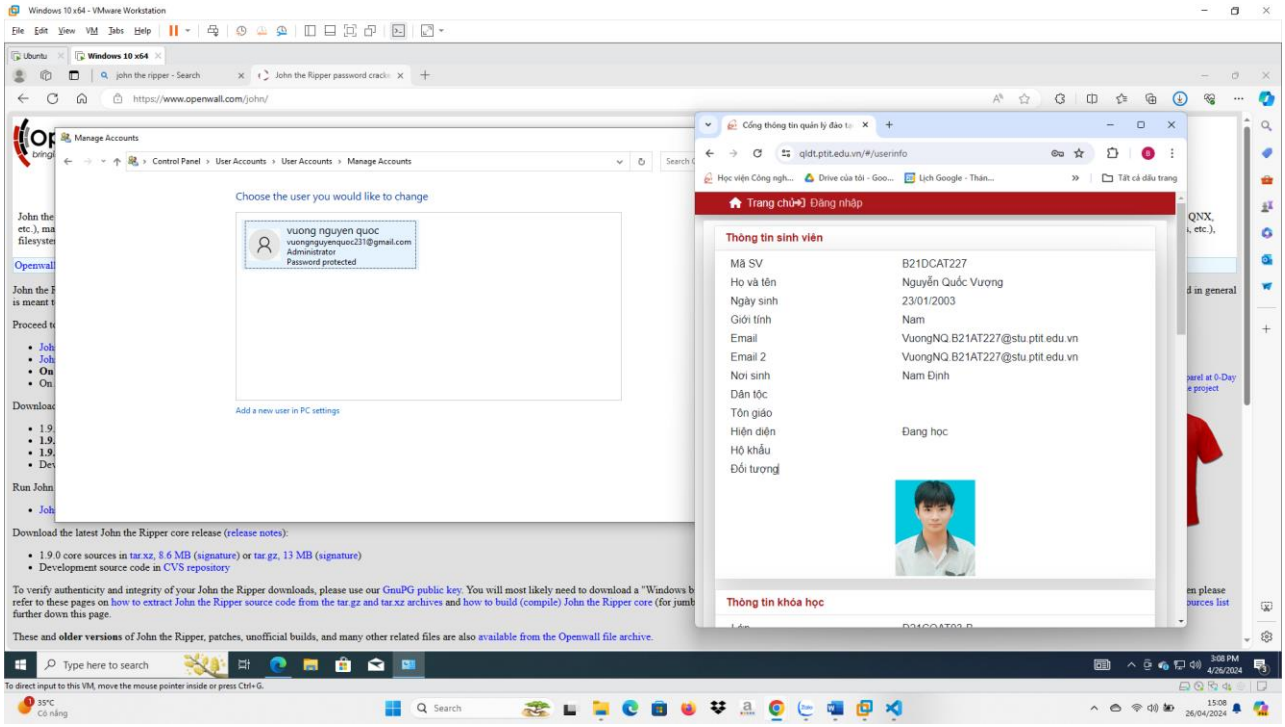
- Cài đặt các công cụ Crack mật khẩu trên hệ điều hành Windows

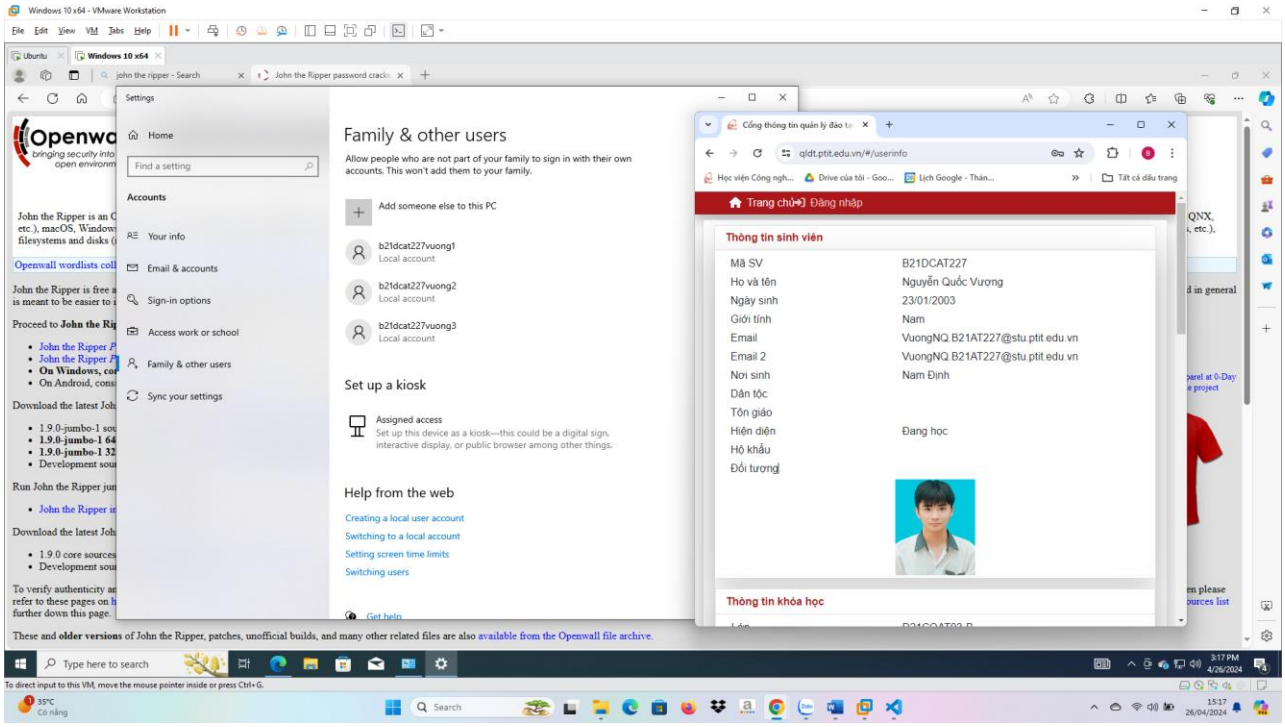
Cài John The Ripper từ trang web chính:



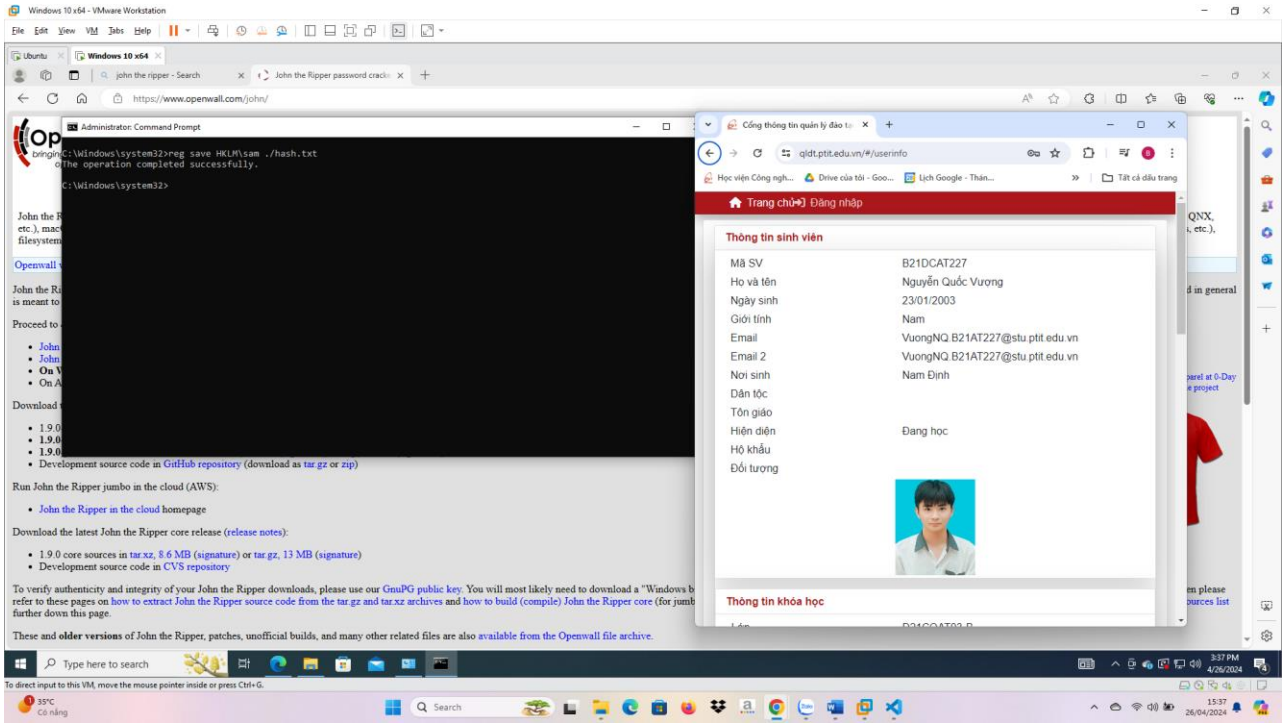
Tạo them 3 người dùng với mật khẩu có độ dài lần lượt là 4,6,8:

Control Panel => User Account => Add a new User in PC settings

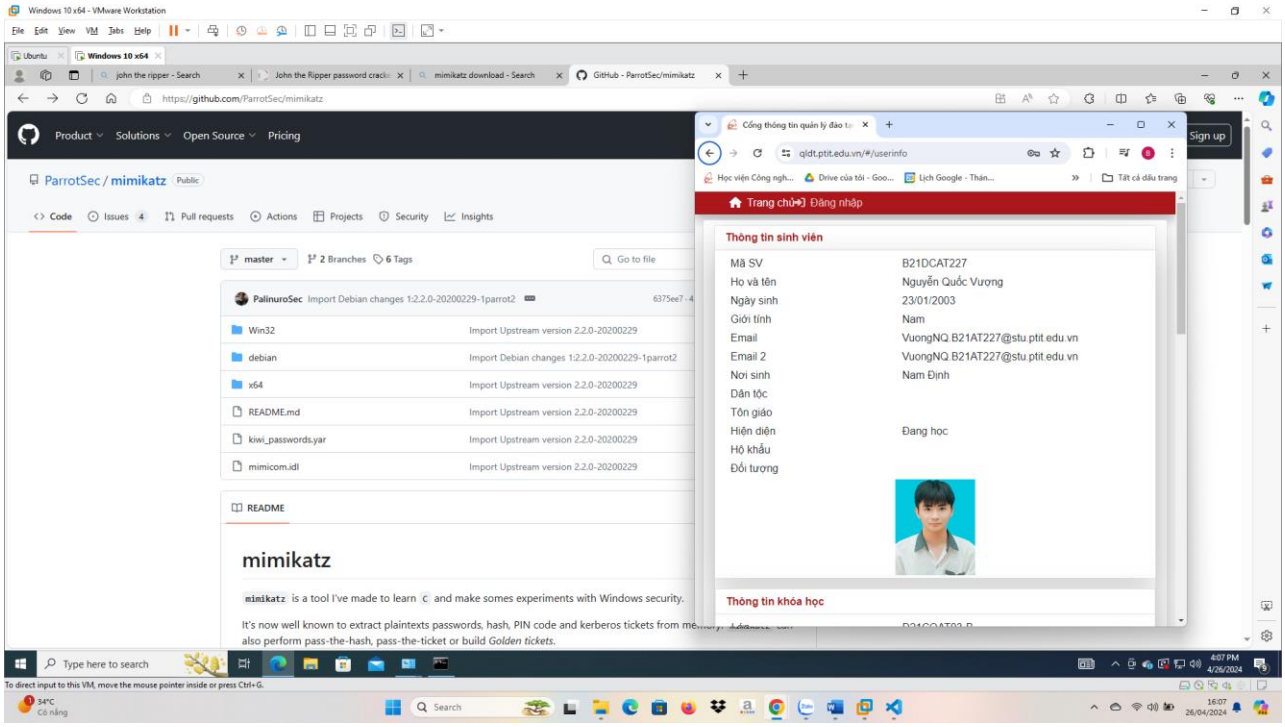




Mở cmd với quyền quản trị và sử dụng lệnh reg để lưu hash của mật khẩu người dung:



Cài mimikatz:

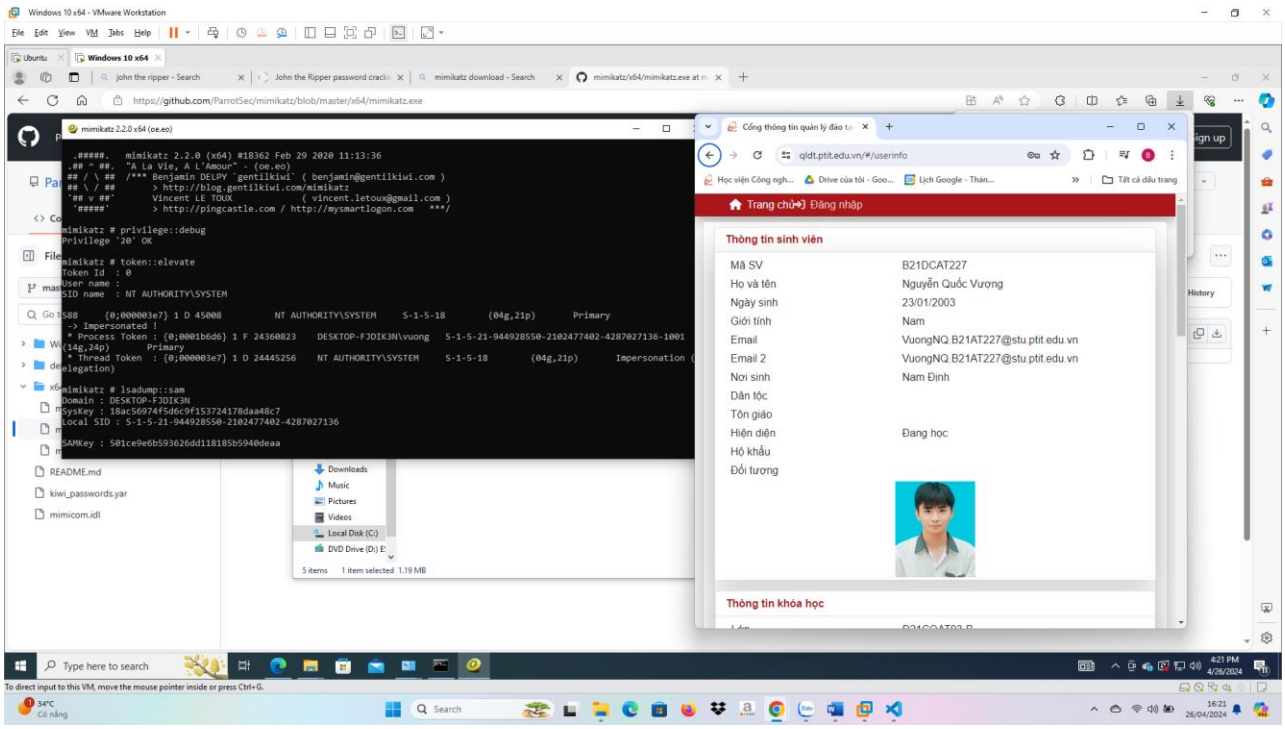


Chạy file mimikatz.exe với quyền administrator và chạy lần lượt các lệnh sau:

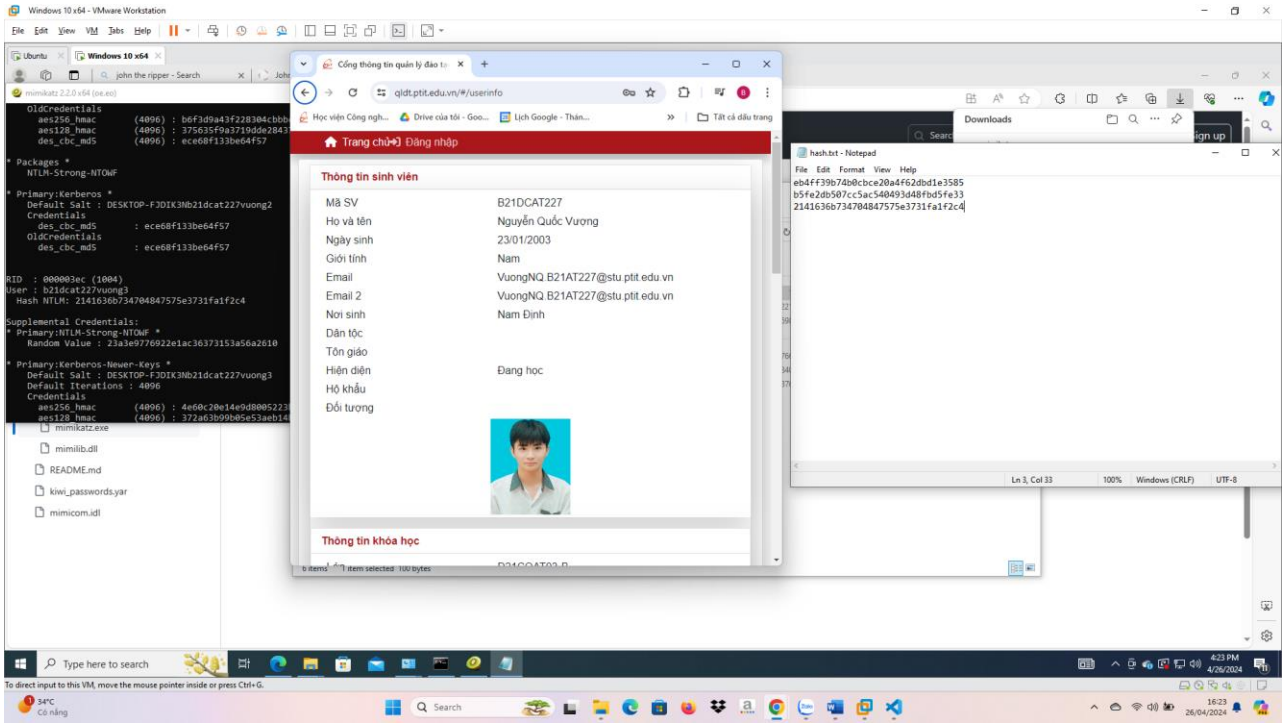
privilege::debug

token::elevate

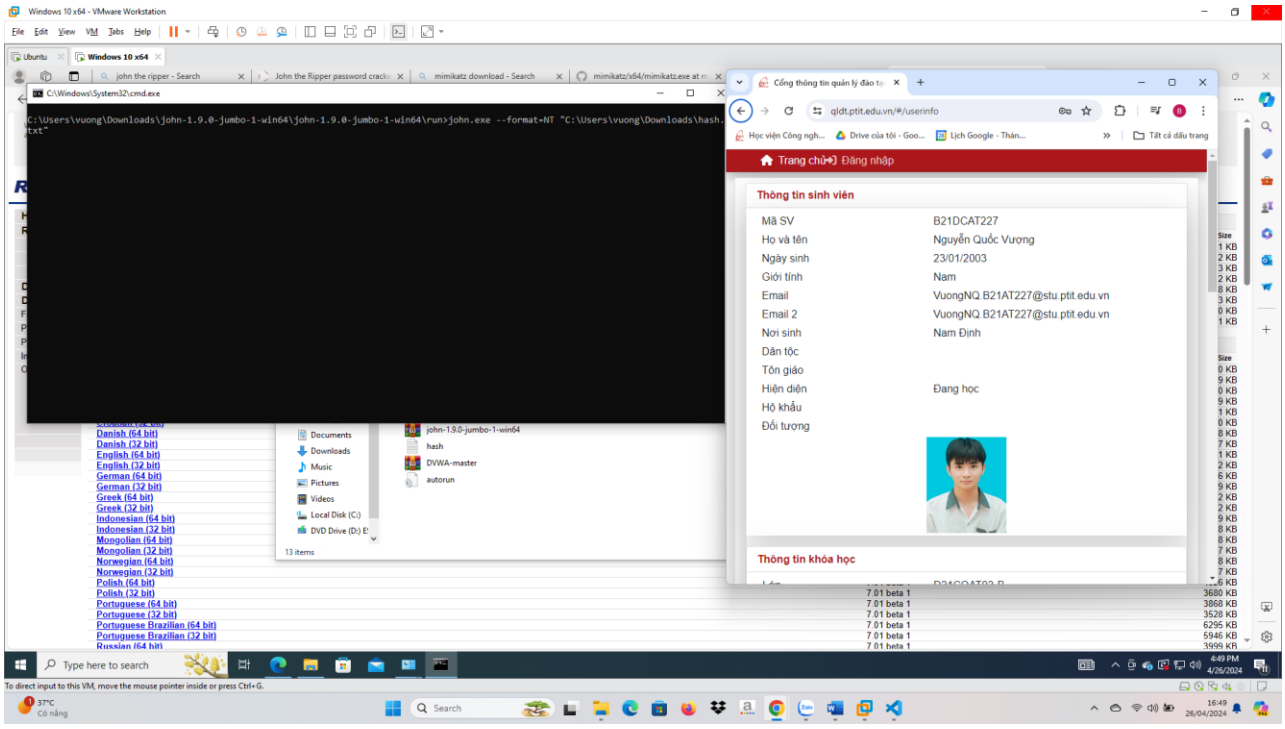
lsadump::sam



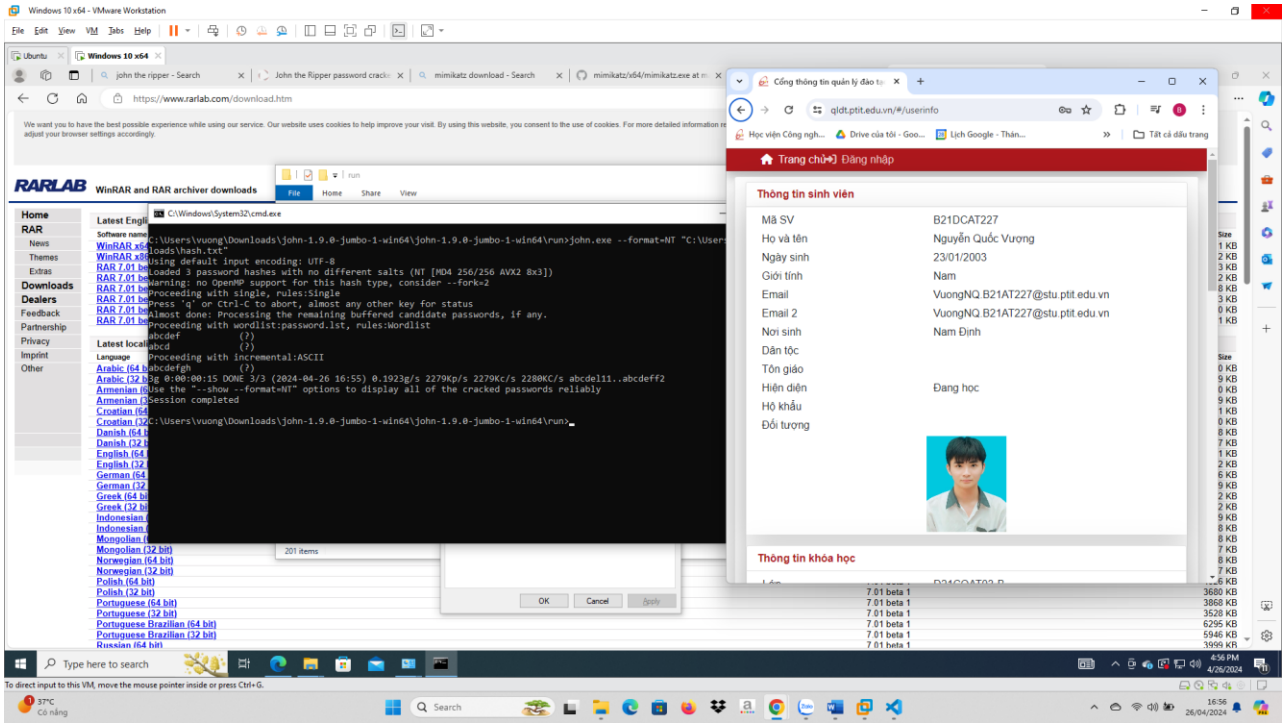
Lưu hash của người dùng vào file hash.txt



Sử dụng john để crack file hash.txt vừa lưu:



Crack thành công các mật khẩu:


Windows 10 x64 - VMware Workstation
Trang chủ
Đăng nhập
Thông tin sinh viên
Mã SV B21DCAT227
Họ và tên Nguyễn Quốc Vượng
Ngày sinh 23/01/2003
Giới tính Nam
Email VuongNQ.B21AT227@stu.ptit.edu.vn
Email 2 VuongNQ.B21AT227@stu.ptit.edu.vn
Nơi sinh Nam Định
Dân tộc
Tôn giáo
Hiện diện Đang học
Hộ khẩu
Đối tượng
Thông tin khóa học
C:\Windows\System32\cmd.exe
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:password.lst, rules:Wordlist
Proceeding with incremental:ASCII
3g 0:00:00:15 DONE 3/3 (2024-04-26 16:55) 0.1923g/s 2279Kp/s 2279Kc/s 2280KC/s abcdel11..abcdeff2
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
WinRAR and RAR archiver downloads

- Lưu ý: Sinh viên cần chứng minh các kết quả thực nghiệm là do chính mình tiến hành cài đặt và thực hiện trong báo cáo. Minh chứng có thể thực hiện theo các cách sau:
    - Đặt tên máy/tên người dùng là họ tên SV và Mã SV.
    - Mở cmd gõ “date” để hiển thị ngày tháng năm; gõ “echo” + “họ tên và Mã SV” để hiển thị thông tin của SV. Chụp ảnh phần này với nội dung đang thực hiện hoặc kết quả của bài.