HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1

BÀI THỰC HÀNH 12

THỰC TẬP CƠ SỞ

Họ và tên : Đinh Quang Hiếu

Mã sinh viên: B19DCAT065

Giảng viên giảng dạy: Hoàng Xuân Dậu

HÀ NỘI, THÁNG 3/2022

1.Mục đích

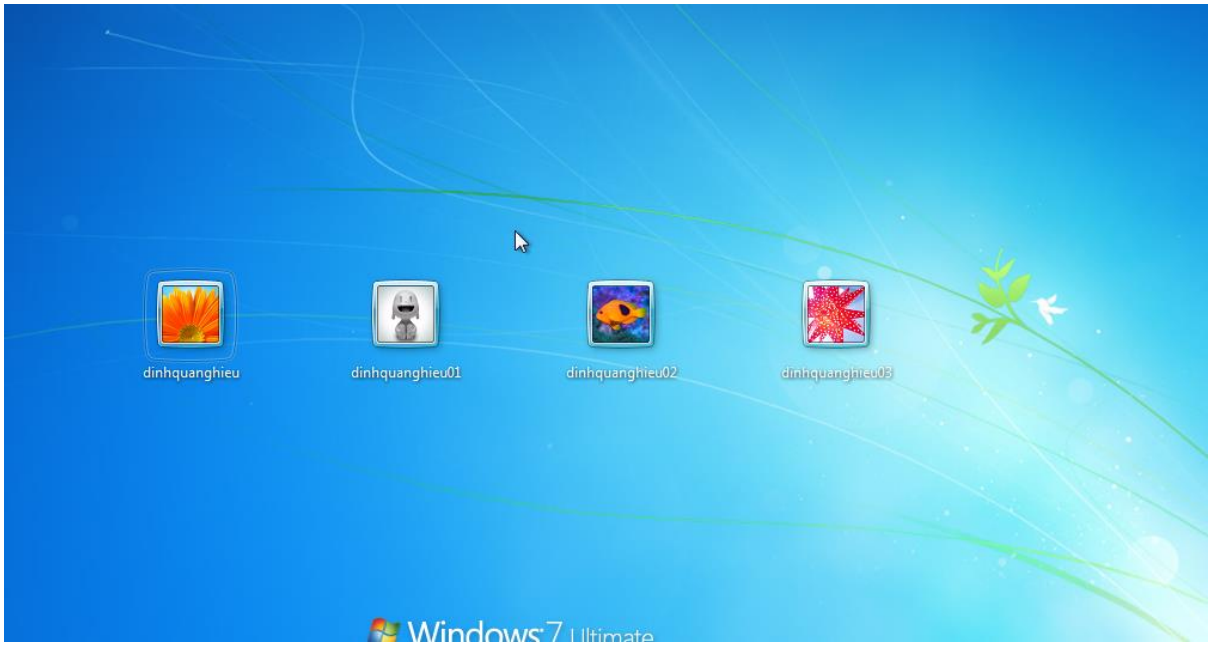
- Hiểu được mối đe dọa về tấn công mật khẩu.
- Hiểu được nguyên tắc hoạt động của một số công cụ Crack mật khẩu trên các hệ điều hành Linux và Windows.
- Biết cách sử dụng công cụ để Crack mật khẩu trên các hệ điều hành Linux và Windows.

2.Tóm tắt lý thuyết

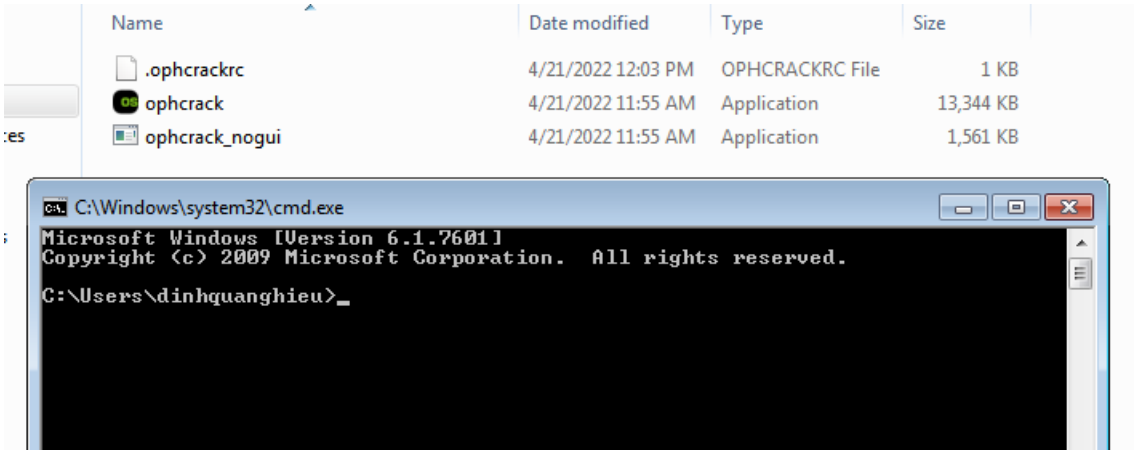
- OphCrack:
    - Ophcrack là một chương trình mã nguồn mở miễn phí bẻ khóa mật khẩu đăng nhập Windows.
    - Ophcrack bẻ khóa mật khẩu đăng nhập Windows bằng cách sử dụng hàm băm LM thông qua bảng cầu vồng . Chương trình bao gồm khả năng nhập các hàm băm từ nhiều định dạng khác nhau, bao gồm kết xuất trực tiếp từ các tệp SAM của Windows.
- John the Ripper:
    - John the Ripper là một công cụ phần mềm bẻ khóa mật khẩu ban đầu được phát triển cho hệ điều hành Unix kết hợp một số bộ cracker mật khẩu trong cùng một gói phần mềm, tự động phát hiện các kiểu mật khẩu và có một bộ cracker có khả năng tùy chỉnh.
    - John The Ripper sẽ chạy để tìm thuật toán hash, sau đó sẽ sử dụng danh sách mặc định của mình để crack hash. John được trang bị một danh sách password riêng, mặc dù danh sách này khá hạn chế.
    - Công cụ này có thể được chạy cho các định dạng mật khẩu đã được mã hóa chẳng hạn như các kiểu mật khẩu mã hóa vẫn thấy trong một số bản Unix khác (dựa trên DES, MDS hoặc Blowfish), Kerberos AFS và Windows NT/2000/XP/2003 LM hash.
    - John có thể chạy ở một vài chế độ khác, tuy nhiên để chạy nó trong chế độ mặc định, tất cả những gì bạn cần thực hiện là cung cấp file có chứa password hash Khi hoàn tất, John the Ripper sẽ hiển thị các mật khẩu đã được crack và lưu các kết quả vào file john.pot của nó. Trong hầu hết các trường hợp, chế độ crack mặc định là khá ổn, tuy nhiên John the Ripper cũng có các chế độ crack khác như:
        - Single Crack Mode – Sử dụng các biến tên tài khoản
        - Wordlist Mode – Dựa vào một từ điển để đoán mật khẩu
        - Incremental Mode – Dựa vào tấn công kiểu brute-force
        - External Mode – Dựa vào một ứng dụng khác (được người dùng cung cấp) để đoán mật khẩu.

3.Các bước thực hiện

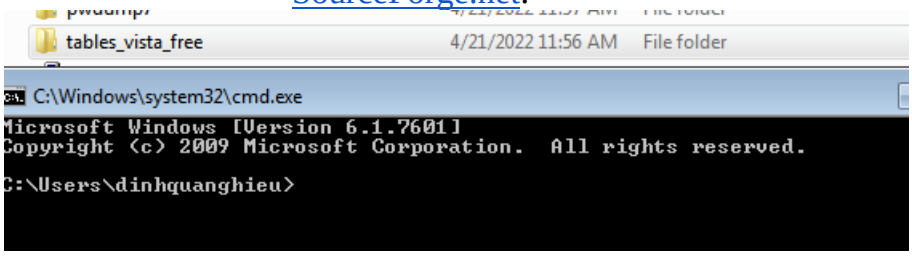
- Thử nghiệm crack mật khẩu trên hệ điều hành Windows với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự,... Các tên tài khoản này đều có phần đầu là mã sinh viên.
    - Tạo ra 3 tài khoản có mật khẩu 4 ký tự, 6 ký tự, 8 ký tự:



- Tải OphCrack tại [Ophcrack (sourceforge.io)]

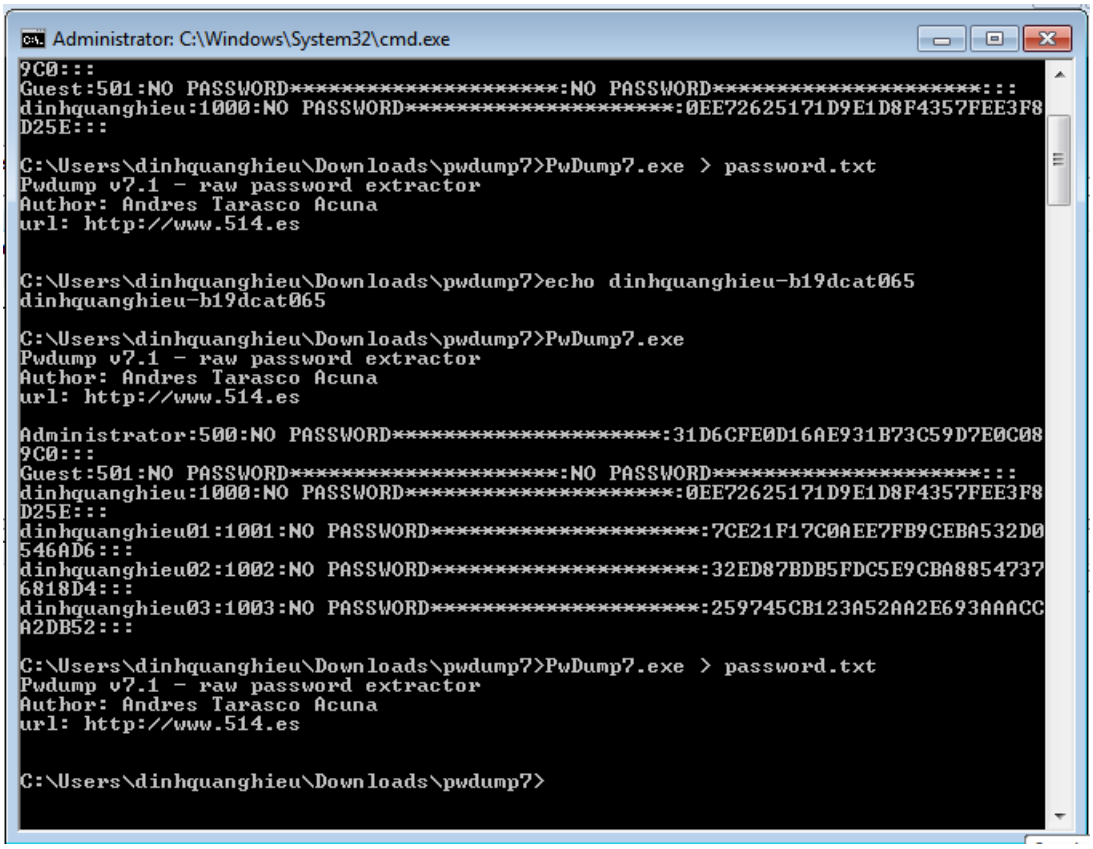


- Tải Vista Free Table tại [Download ophcrack from SourceForge.net]:

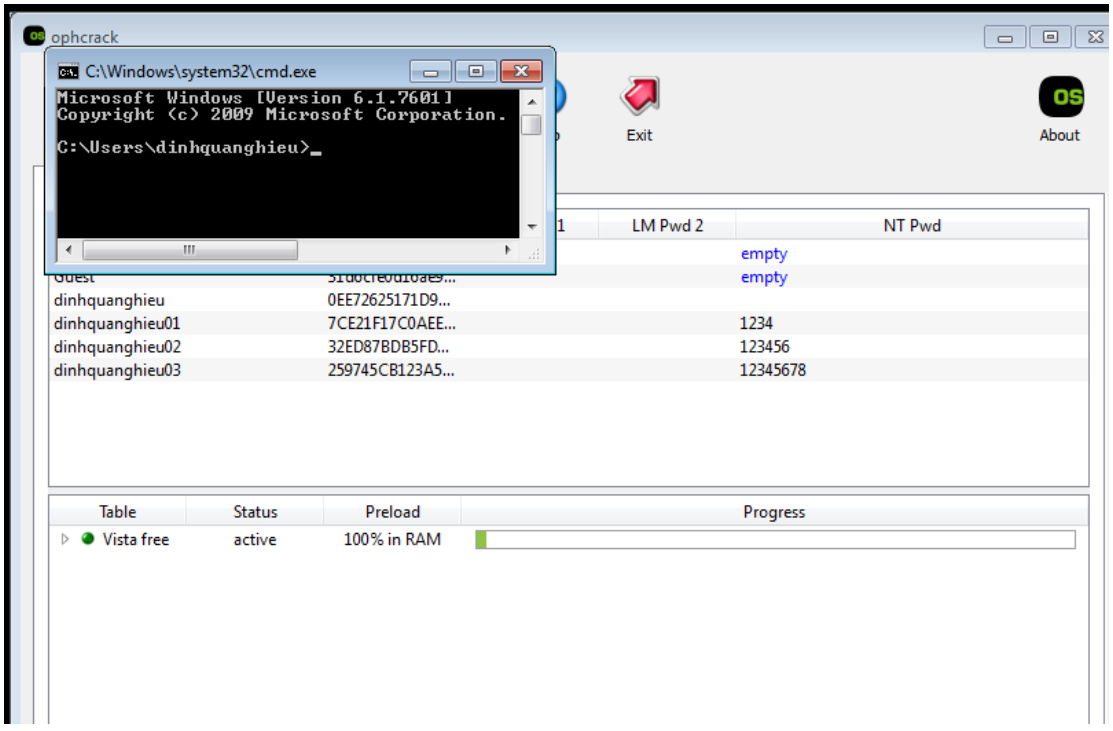


- Tiến hành crack mật khẩu:

- Trên Window
  - Lấy mã băm của các tài khoản

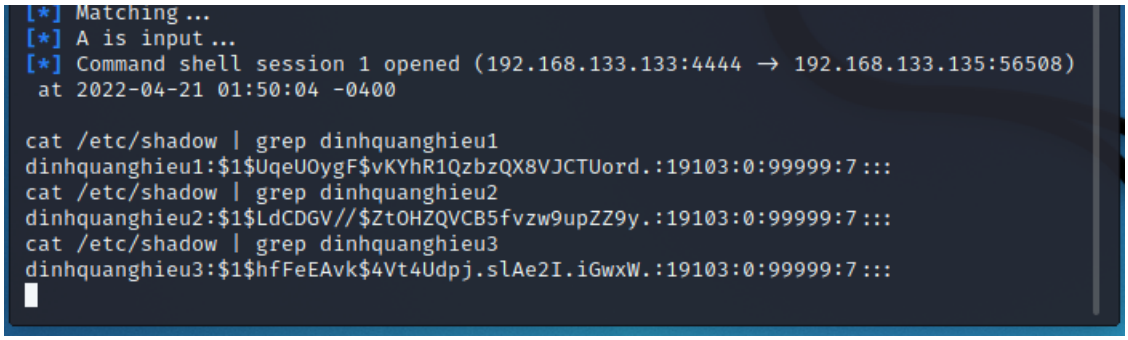


- Tiến hành crack mật khẩu:



- Trên Linux

- Lấy mã băm của các tài khoản



- Tiến hành crack mật khẩu: