

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



BÁO CÁO THỰC HÀNH

Bài 12: Tấn công mật khẩu

Họ và tên: Vũ Thành Long

Mã sinh viên: B21DCAT012

Nhóm: 06

Môn học: Thực tập cơ sở

Giảng viên giảng dạy: Nguyễn Hoa Cường

Hà Nội, 2024

Mục lục

| | |
|---------------------------------------|----|
| I. Tìm hiểu lý thuyết..... | 2 |
| 1. Phần mềm bẻ khoá mật khẩu..... | 2 |
| 2. Phương pháp bẻ khoá mật khẩu | 2 |
| II. Mô tả cài đặt & kết quả | 3 |
| 1. Trên Linux..... | 3 |
| 2. Trên Windows | 6 |
| III. Tài liệu tham khảo..... | 10 |

I. Tìm hiểu lý thuyết:

1. Phần mềm bẻ khoá mật khẩu:

- John the Ripper là một công cụ bẻ khóa mật khẩu miễn phí, có mặt trên nhiều hệ điều hành như Unix, DOS, Windows.
- Được phát triển bởi OpenWall, John là một trong những chương trình kiểm tra và phá mật khẩu phổ biến nhất vì nó kết hợp nhiều kỹ năng bẻ khóa mật khẩu vào một phần mềm và có khả năng tự động phát hiện các loại mã băm mật khẩu.
- John có thể phá mật khẩu được băm bởi nhiều thuật toán mã băm khác nhau như DES, MD5 hay Blowfish.
- Hash Suite là một công cụ bẻ khóa mật khẩu khác, được phát triển bởi một người đóng góp (contributor) của John.
- Hash Suite chỉ có mặt trên Android và Windows. Khác với John, Hash Suite có giao diện đồ họa (GUI).

2. Phương pháp bẻ khoá mật khẩu:

- Hầu hết các phần mềm bẻ khóa mật khẩu đều hỗ trợ hai phương pháp phổ biến nhất là Brute-force attack và Dictionary attack.
- Brute-force attack là kiểu tấn công mà kẻ tấn công thử tất cả các trường hợp có thể của mật khẩu để tìm ra mật khẩu đúng. Trong John, mỗi trường hợp của mật khẩu sẽ được băm sau đó John so sánh mã băm này với mã băm lấy được từ máy tính.
- Ưu điểm của Brute-force attack là chắc chắn sẽ tìm ra mật khẩu đúng nếu thời gian cho phép. Tuy nhiên, nhược điểm của brute-force là thời gian giải mã sẽ rất lâu nếu độ dài của khóa lớn. Ví dụ, thời gian bẻ khóa AES-256 lớn hơn 2^{128} lần so với AES-128. Nếu một siêu máy tính có thể thử 10^{14} trường hợp trong 1 giây, sẽ phải mất $3.67 * 10^{55}$ năm để kiểm tra tất cả các trường hợp trong AES-256.
- Dictionary attack, hay còn gọi là tấn công bằng từ điển, là khi kẻ tấn công thay vì thử tất cả các trường hợp có thể của mật khẩu, thì chỉ thử những mật khẩu thông dụng nhất. Danh sách các mật khẩu thông dụng được lưu trong một tệp văn bản gọi là wordlist. John sẽ lấy từng mật khẩu trong wordlist, băm rồi so sánh với mã băm lấy được từ máy tính. Ngoài ra, John cũng thử thay đổi một chút mật khẩu trong wordlist khi băm, ví dụ như thử mật khẩu "password" rồi không dừng lại mà thử tiếp "passw0rd" hay "password1".

- Một số mật khẩu thông dụng có thể kể đến như: password, pass, 123456, 12345678, qwerty, anhyeuem, matkhou, admin, root, v.v

II. Mô tả cài đặt & kết quả:

1. Trên Linux:

- Sinh viên sử dụng công cụ **john** có cài sẵn trên hệ điều hành Kali Linux.
- Trước hết, sinh viên tạo các người dùng mới bằng lệnh `useradd` và `passwd`:
 - Người dùng **B21DCAT012-Long1** mật khẩu **pass**.
 - Người dùng **B21DCAT012-Long2** mật khẩu **passwd**.
 - Người dùng **B21DCAT012-Long3** mật khẩu **password**.

```

kali@B21AT012-LongVT-Kali-Internal: ~
File Actions Edit View Help
└─$ sudo useradd -m -g users B21DCAT012-Long1
(kali@B21AT012-LongVT-Kali-Internal)-[~]
└─$ sudo useradd -m -g users B21DCAT012-Long2
(kali@B21AT012-LongVT-Kali-Internal)-[~]
└─$ sudo useradd -m -g users B21DCAT012-Long3
(kali@B21AT012-LongVT-Kali-Internal)-[~]
└─$ sudo passwd B21DCAT012-Long1
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
(kali@B21AT012-LongVT-Kali-Internal)-[~]
└─$ sudo passwd B21DCAT012-Long2
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
(kali@B21AT012-LongVT-Kali-Internal)-[~]
└─$ sudo passwd B21DCAT012-Long3
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
(kali@B21AT012-LongVT-Kali-Internal)-[~]
└─$
  
```

- Mật khẩu đã được mã hoá trên Linux được lưu ở `/etc/shadow`. Sinh viên thực hiện tìm và copy dòng chứa tên người dùng và mật khẩu đã mã hoá ở tệp tin này.

```
kali@B21AT012-LongVT-Kali-Internal: ~
File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ sudo grep B21DCAT012-Long /etc/shadow
B21DCAT012-Long1:$y$j9T$eYNDZ8luHXHlzMxVSN2Cx/$q34JN0rWDhni4KSL4xN0uW3Vd1NzpQEvo2Xmvn/MES9:1
9851:0:99999:7:::
B21DCAT012-Long2:$y$j9T$Cgh5ee5rcZ/LM62q6FXId1$2jyqe3.3L8uq3gN8aWUJcVkcxwoedzuzXDoq.jyobt7:1
9851:0:99999:7:::
B21DCAT012-Long3:$y$j9T$el1io.4jdnBph3e4kAu5z/$4gUa3jCvkGf5sOaMHph.Y7qKdXBkoD7MtwI8WcpioH8:1
9851:0:99999:7:::

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$
```

- Tiếp theo, sinh viên lưu dữ liệu trên vào một tệp văn bản (trong ví dụ là /home/kali/Downloads/hash).
- Tiếp theo sinh viên khởi động john để phá mật khẩu. Để ý thấy trên đoạn mật khẩu mã hoá có các kí tự **\$y\$**. Điều này có nghĩa là Kali Linux sử dụng thuật toán **yescrypt** để mã hoá mật khẩu.
- Trên terminal, điền lệnh **john --format=crypt /home/kali/Downloads/hash** và kiên nhẫn chờ đợi.

```
kali@B21AT012-LongVT-Kali-Internal: ~/Downloads
File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal)-[~/Downloads]
$ cat /home/kali/Downloads/hash
B21DCAT012-Long1:$y$j9T$eYNDZ8luHXHlzMxVSN2Cx/$q34JN0rWDhni4KSL4xN0uW3VdLNzpQEvo2Xmvn/MES9:1
9851:0:99999:7:::
B21DCAT012-Long2:$y$j9T$Cgh5ee5rcZ/LM62q6FXId1$2jyqe3.3L8uq3gN8aWUJcVkcxwoedzuzXDoq.jyobt7:1
9851:0:99999:7:::
B21DCAT012-Long3:$y$j9T$el1io.4jdnBph3e4kAu5z/$4gUa3jCvkGf5s0aMHph.Y7qKdXBkoD7MtWI8WcpioH8:1
9851:0:99999:7:::

(kali@B21AT012-LongVT-Kali-Internal)-[~/Downloads]
$ john --format=crypt /home/kali/Downloads/hash
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is
0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:14 4.73% 1/3 (ETA: 04:44:35) 0g/s 124.7p/s 124.7c/s 124.7C/s lbdcat-long12..Lbdca
t-longLbdcat-long
0g 0:00:00:20 6.57% 1/3 (ETA: 04:44:44) 0g/s 121.3p/s 121.3c/s 121.3C/s LONG3B21DCAT012-LONG
3..bb21dcat012-long33gnol-210tacd12bb
0g 0:00:00:45 13.50% 1/3 (ETA: 04:45:13) 0g/s 108.4p/s 108.4c/s 108.4C/s b21dcat012-long2lon
g2v..b21dcat012-long2"
0g 0:00:01:08 16.39% 1/3 (ETA: 04:46:34) 0g/s 100.3p/s 100.3c/s 100.3C/s l99999|..Lb21dcat01
2-long23
0g 0:00:01:13 16.83% 1/3 (ETA: 04:46:53) 0g/s 100.4p/s 100.4c/s 100.4C/s Long3999993..Long39
99998
0g 0:00:01:18 17.70% 1/3 (ETA: 04:47:00) 0g/s 100.6p/s 100.6c/s 100.6C/s Long1b21dcat012b..L
```

- Hình bên dưới là kết quả phá mật khẩu thành công. Mật khẩu và tên người dùng được in màu cam. Ngoài ra có thể dùng lệnh **john --show /home/kali/Downloads/hash** để in ra tên người dùng và mật khẩu.

```
kali@B21AT012-LongVT-Kali-Internal: ~/Downloads
File Actions Edit View Help
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is
0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:14 4.73% 1/3 (ETA: 04:44:35) 0g/s 124.7p/s 124.7c/s 124.7C/s lbdcat-long12..Lbdca
t-longlbdcat-long
0g 0:00:00:20 6.57% 1/3 (ETA: 04:44:44) 0g/s 121.3p/s 121.3c/s 121.3C/s LONG3B21DCAT012-LONG
3..bb21dcat012-long33gnol-210tacd12bb
0g 0:00:00:45 13.50% 1/3 (ETA: 04:45:13) 0g/s 108.4p/s 108.4c/s 108.4C/s b21dcat012-long2lon
g2v..b21dcat012-long2"
0g 0:00:01:08 16.39% 1/3 (ETA: 04:46:34) 0g/s 100.3p/s 100.3c/s 100.3C/s l99999|..Lb21dcat01
2-long23
0g 0:00:01:13 16.83% 1/3 (ETA: 04:46:53) 0g/s 100.4p/s 100.4c/s 100.4C/s Long3999993..Long39
99998
0g 0:00:01:18 17.70% 1/3 (ETA: 04:47:00) 0g/s 100.6p/s 100.6c/s 100.6C/s Long1b21dcat012b..L
ong1b21dcat012g
0g 0:00:01:19 17.70% 1/3 (ETA: 04:47:06) 0g/s 100.6p/s 100.6c/s 100.6C/s Long3b21dcat012b..L
ong3b21dcat012g
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (B21DCAT012-Long3)
passwd        (B21DCAT012-Long2)
pass          (B21DCAT012-Long1)
3g 0:00:09:18 DONE 2/3 (2024-05-08 04:48) 0.005369g/s 103.2p/s 108.3c/s 108.3C/s modem..sony
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@B21AT012-LongVT-Kali-Internal)-[~/Downloads]
$ █

kali@B21AT012-LongVT-Kali-Internal: ~
File Actions Edit View Help
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ john --show /home/kali/Downloads/hash
B21DCAT012-Long1:pass:19851:0:99999:7 :::
B21DCAT012-Long2:passwd:19851:0:99999:7 :::
B21DCAT012-Long3:password:19851:0:99999:7 :::

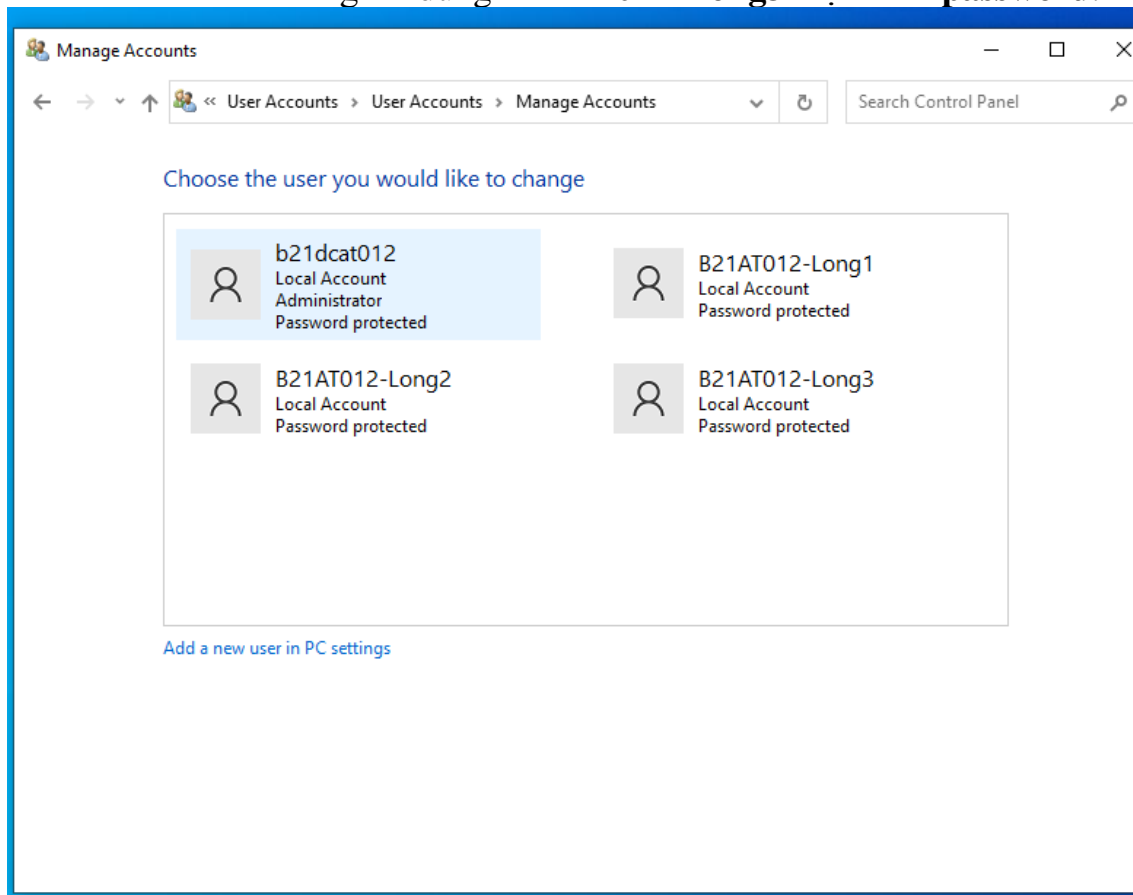
3 password hashes cracked, 0 left

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ █
```

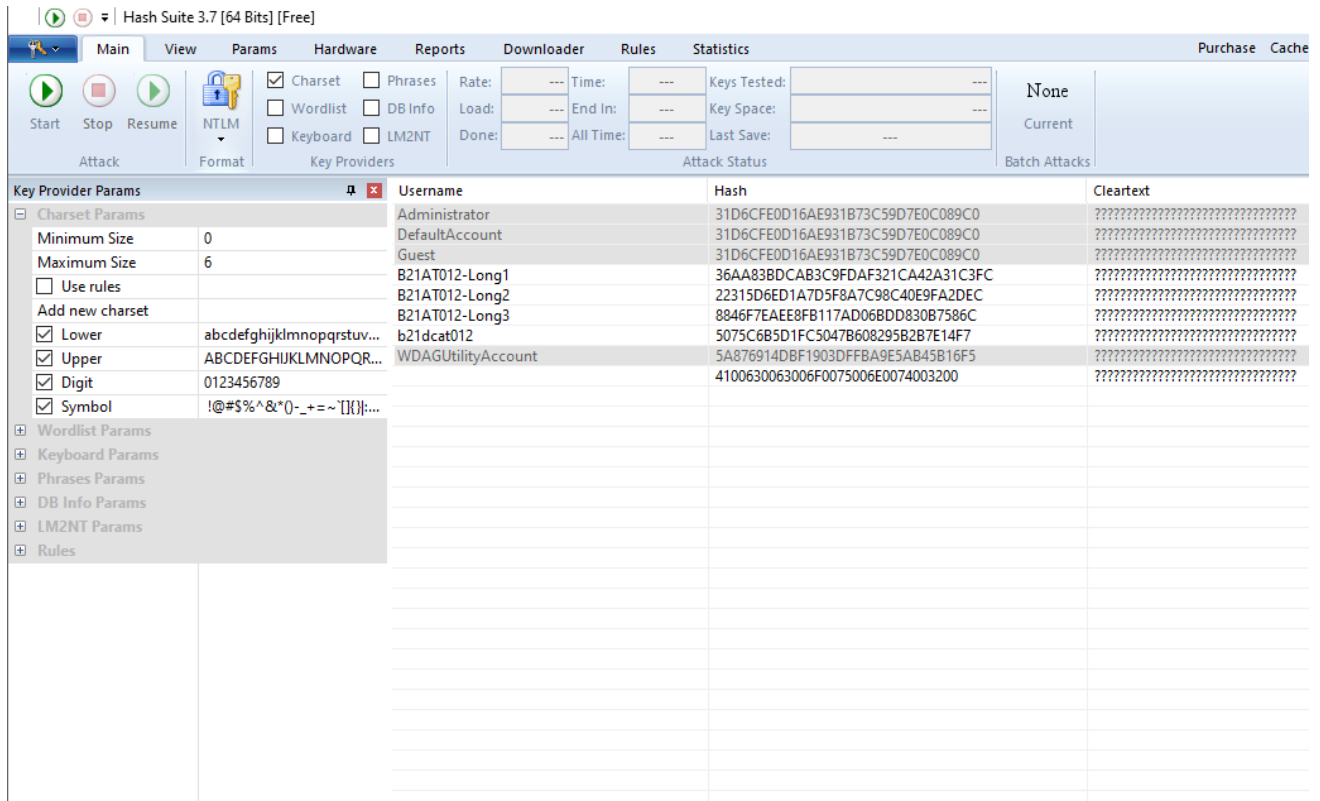
2. Trên Windows:

- Sinh viên sử dụng phần mềm Hash Suite. Tải và giải nén Hash Suite từ <https://hashsuite.openwall.net/download>
- Trên Windows, sinh viên tạo các tài khoản như sau:
 - Người dùng **B21AT012-Long1** mật khẩu **pass**.
 - Người dùng **B21AT012-Long2** mật khẩu **passwd**.

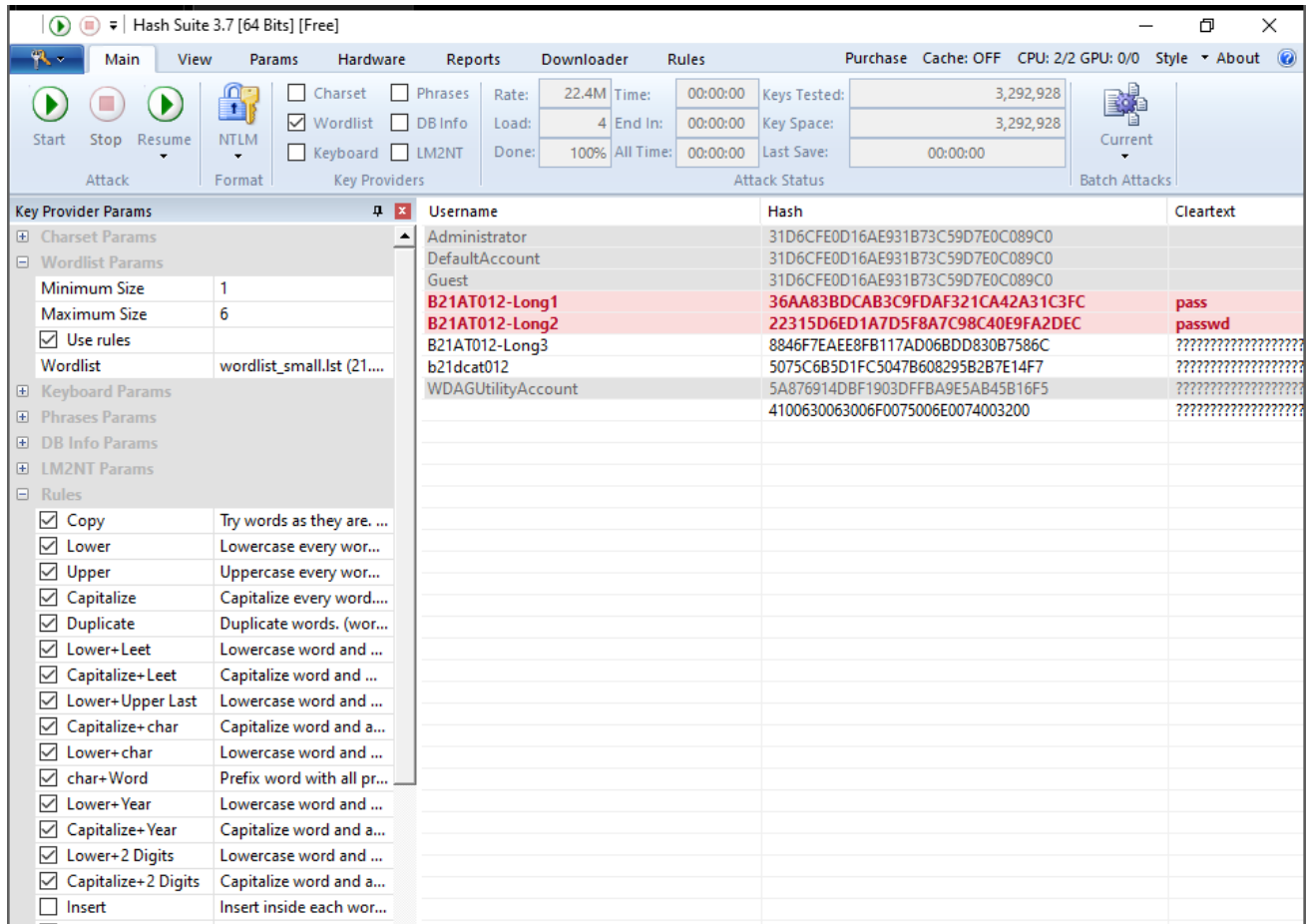
- Người dùng **B21AT012-Long3** mật khẩu **password**.



- Trên giao diện chính của Hash Suite, bấm vào nút màu xanh nước biển ở góc trên bên trái màn hình, chọn Import để nạp dữ liệu người dùng và mật khẩu đã mã hoá từ hệ điều hành.
- Ở tab Main, mục Format chọn NTLM thay vì LM.
- Kết quả hiển thị như hình dưới.



- Tại đây, người dùng có thể chọn các phương pháp bẻ khoá mật khẩu khác nhau như charset, wordlist, keyboard, phrases, v.v
- Để việc bẻ khoá mật khẩu diễn ra nhanh, sinh viên chọn wordlist vì pass, passwd, password đều là các từ thông dụng. Tất nhiên trong trường hợp thực tế thì kẻ tấn công không biết mật khẩu nên không thể biết phương pháp bẻ khoá nào là tối ưu nhất. Tuy nhiên vì đây là môi trường thử nghiệm, trên máy ảo có tài nguyên ít nên mong giảng viên thông cảm.



- Kết quả, Hash Suite bẻ khoá được mật khẩu của 2 tài khoản như hình trên. Phần mềm này là phiên bản miễn phí nên bị giới hạn bẻ khoá mật khẩu dưới 8 kí tự, nên sinh viên không thể bẻ khoá B21AT012-Long3. Mong giảng viên thông cảm.

III. Tài liệu tham khảo:

- Bài thực hành 1 bộ môn An toàn hệ điều hành, TS. Hoàng Xuân Dậu.