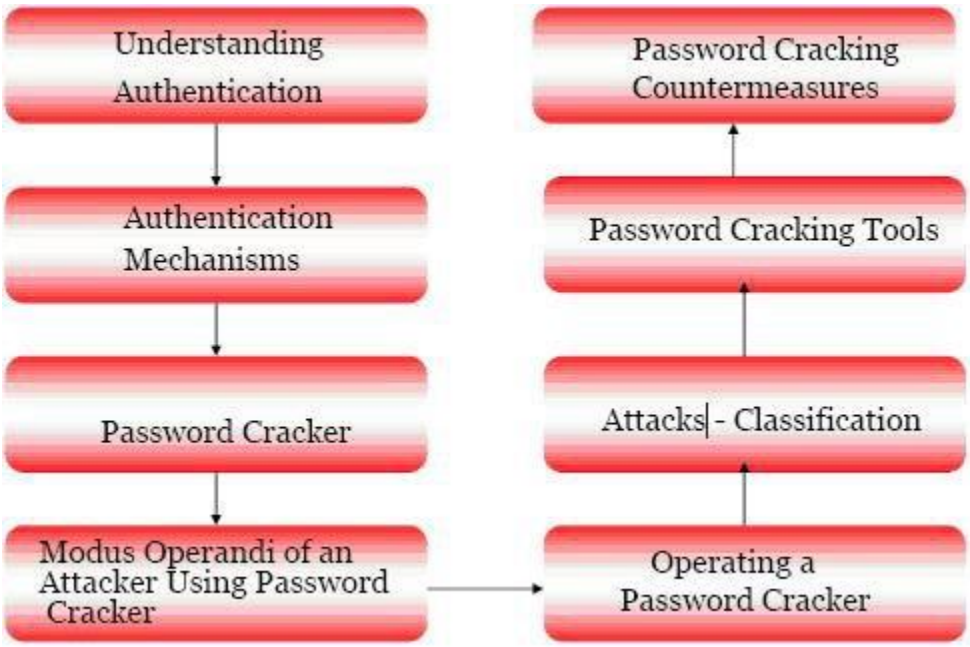
Các phương thức Crack Passwords

Username và Password là hai vấn đề nhạy cảm nhất trong một máy tính, một mạng nhỏ cho tới mạng Internet. Nó cũng là phương thức xác thực được sử dụng rất nhiều trong các hệ thống máy tính, website. Tuy nhiên, phương thức xác thực này vẫn còn tồn tại những lỗ hổng và có khả năng bị phá vỡ.

Trong bài viết này tôi trình bày với các bạn tổng quát về các phương thức xác thực, các cách **phá mật khẩu** và các Tools sử dụng để phá mật khẩu. Chúng tôi cũng đưa ra lời khuyên cho bạn về cách đặt mật khẩu an toàn, từ đó các bạn sẽ biết cách tạo mật khẩu mạnh cũng như tự bảo vệ mình trước các cuộc tấn công.

Các bước tiến hành trong quá trình tấn công phá mật khẩu:



1. Xác thực – Authentication

Xác thực là một quá trình nhận dạng người dùng. Trong hệ thống mạng máy tính, xác thực chủ yếu sử dụng LoginID (Username) và Password. Biết mật khẩu của một tài khoản là điều cần thiết để xác thực, nhưng Password có thể bị mất, bị đánh cắp, bị thay đổi và bị phá, điều này dẫn tới nguy cơ bảo mật cho hệ thống.

Bên cạnh mật khẩu có nhiều cách để xác thực người dùng, chúng ta sẽ đi tìm hiểu cụ thể trong phần tiếp theo.

2. Các phương thức xác thực

- Hầu hết các phương thức xác thực đều dựa trên:
    - Những gì bạn biết (Username Password)
    - Những gì bạn có (Smart Card, Certificate)
    - Những gì là bạn (Sinh trắc học)
- HTTP Authentication – Xác thực trên WEB.
    - Basic Authentication
    - Digest Authentication
- Kết hợp với phương thức xác thực NTLM của Windows
- Negotiate Authentication – Thỏa thuận xác thực
- Xác thực dựa vào Certificate.
- Xác thực dựa vào Forms
- Xác thực dựa vào RSA Secure Token
- Xác thực dựa vào Sinh trắc học (xác thực vân tay, mặt, mống mắt,.)

2. 1. HTTP Authentications

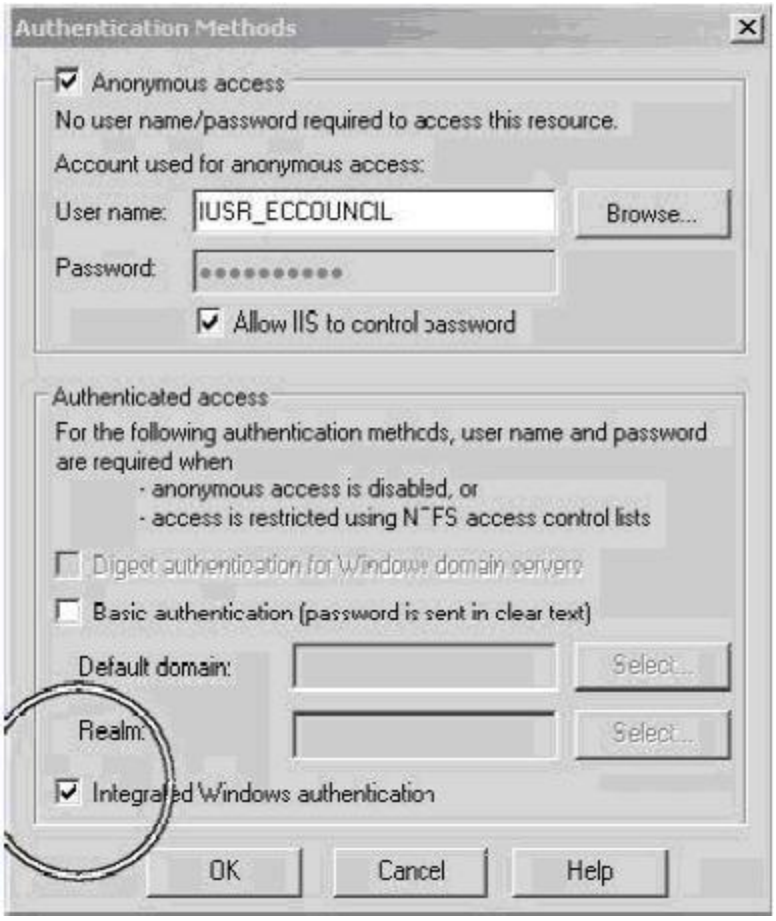
a. Basic Authentication

- Là một phương thức xác thực phổ thông có trên nền tảng ứng dụng Web.
- Nó sẽ xuất hiện ra khi Client yêu cầu những thông tin phải được xác thực.
- Giới hạn những giao thức, cho phép những kẻ tấn công khai thác.
- Sử dụng SSL để mã hóa dữ liệu Username Password để truyền giữa Client và Server.

b. Digest Authentication

- Được thiết kế để nâng cao bảo mật hơn phương thức Basic Authentication
- Được dựa trên nền tảng xác thực Challenge-Response
- Nâng cao bảo bảo mật hơn phương thức Basic Authentication, hệ thống sẽ mã hóa Usernaem Password trước khi truyền đi trên mạng.

2.2. Kết hợp với phương thức xác thực NTLM của Windows



- Sử dụng công nghệ xác thực NT LAN Manager (NTLM) cho HTTP
- Chỉ làm việc với IE và trên nền tảng Web server là IIS.
- Kết hợp với xác thực trên Windows sẽ thích hợp cho môi trường mạng cục bộ của doanh nghiệp
- Nó là một phương thức xác thực mà không phải truyền bất kỳ thông tin nào về Username password trên mạng.

2.3. Xác thực Negotiate

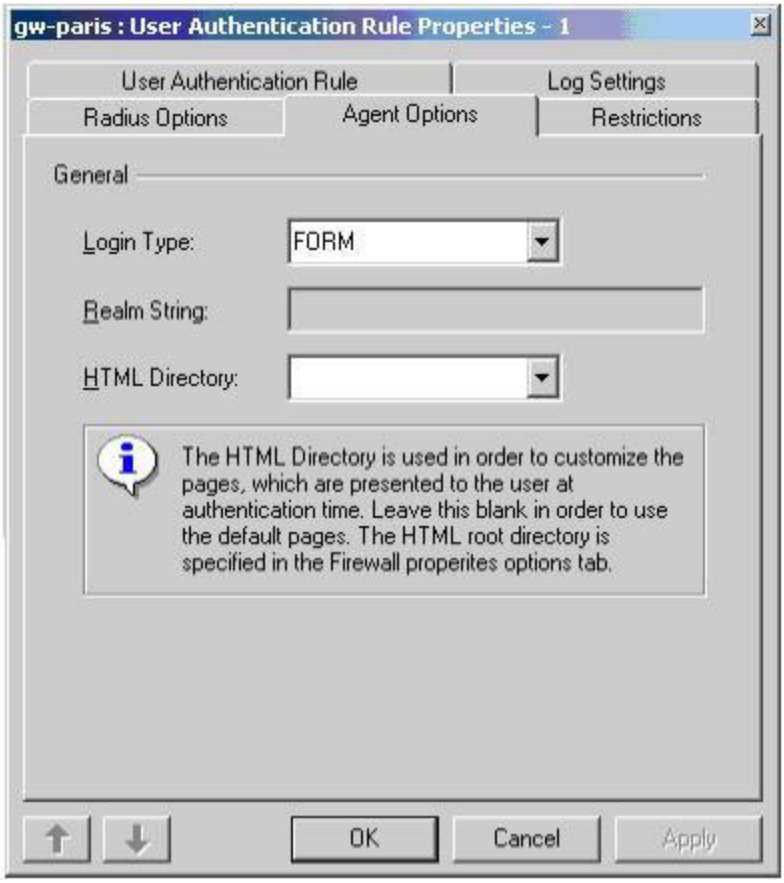
- Đây là một phương thức xác thực mở rộng cho NTLM Authentication
- Cung cấp xác thực dựa trên nền tảng Kerberos
- Sử dụng quá trình thương lượng để quyết định mức độ bảo mật được sử dụng.

- Nó được cấu hình và sử dụng không chỉ cho mạng cục bộ.

2.4. Xác thực dựa vào Certificate

- Sử dụng Public Key để mã hóa và chứng chỉ số (Digital Certificate) để xác thực người dùng.
- Nó được quan tâm và kết hợp với phương thức xác thực two-factor. Khi một người dùng biết được Username Password người đó còn phải cung cấp Certificate nữa thì mới được xác thực.
- Người dùng có thể bị đánh cắp Certtificate.
- Rất nhiều phần mềm hiện nay hỗ trợ xác thực qua chứng chỉ số.

2.5. Xác thực dựa vào Forms-Based

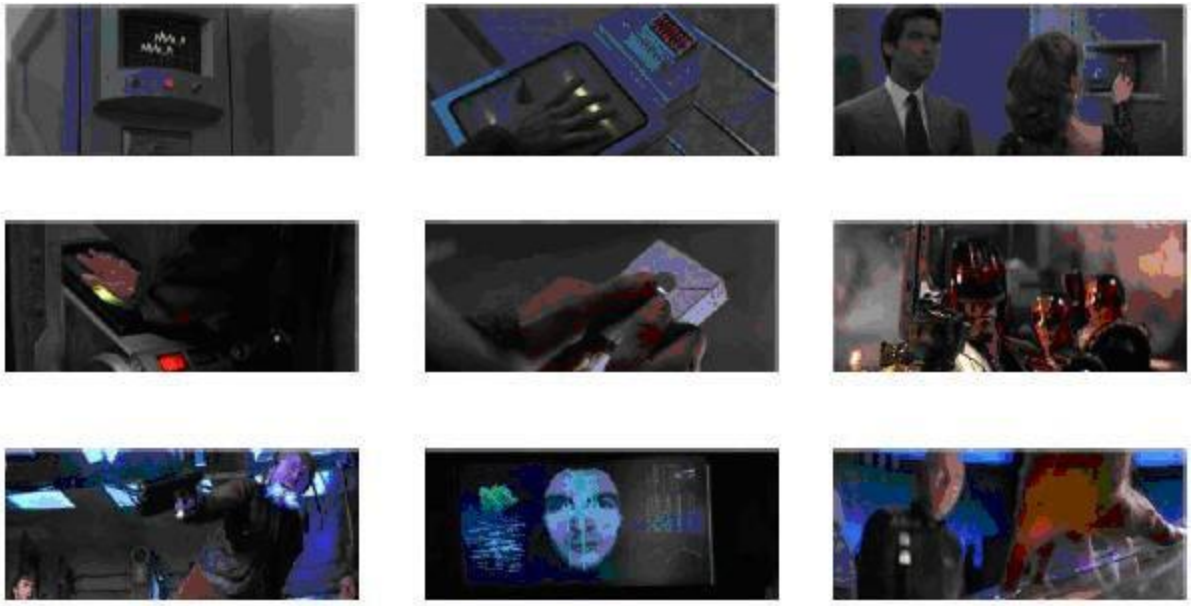


- Nó không được hỗ trợ trên nền tảng HTTP và SSL
  Nó là một lựa chọn cao cấp cho phương thức xác thực sử dụng một Form, và thường tích hợp dạng HTML.
  Là một phương thức xác thực rất phổ biết trên Internet.

2.6. Phương thức xác thực RSA SecurID Token

- Phương thức xác thực SecureID sử dụng một "token – Vé, card). Có một thiết bị phần cứng sẽ sinh ra các mã xác thực sau mỗi 60 giây và sử dụng một tấm Card để giải mã key.
- Một người dùng thực hiện quá trình xác thực và tài nguyên mạng sẽ phải điền mã PIN và số hiển thị cho SecureID cho mỗi thời gian đó.

2.7. Biometrics Authentications



- Một hệ thống xác thực dựa vào Sinh trắc học sẽ phải có những thiết bị nhận diện được người dùng dựa vào các yếu tố sinh học như: Vân tay, mắt, mặt, bàn tay….
- Đây là một phương thức xác thực có tính bảo mật rất cao và thuận tiện cho người sử dụng không phải nhớ mật khẩu hay mang theo một tấm Card.

3. Làm thế nào để có một mật khẩu bảo mật

Chúng tôi đã có một bài viết rất chi tiết về việc tạo mật khẩu an toàn với rất nhiều phương pháp và mẹo để bạn có thể tạo được một mật khẩu mạnh nhằm bảo vệ dữ liệu của mình. Dưới đây là những lưu ý cơ bản khi đặt mật khẩu.

- Áp đặt chính sách độ dài tối thiểu của mật khẩu là 8 và tốt nhất là 15
- Yêu cầu phải có những ký tự đặc biệt, số, chữ hoa, chữ thường trong một mật khẩu
- Không sử dụng bất kỳ từ khóa nào trong từ điển English hay những nước khác
- Không sử dụng Password giống tên Username, và phải thay đổi thường xuyên

- Chọn Password bạn dễ dàng sử dụng mà người khác khó đoán biết được.

4. Những khuyến cáo đặt password khác

- Đừng bao giờ chỉ đặt một ký tự đặc biệt sau một từ khóa ví dụ: Không đặt password là: vnexperts1
- Đừng bao giờ sử dụng ghép hai từ với nhau để được một Password ví như: vnevne
- Không đặt Password dễ đoán
- Không đặt password quá ngắn
- Không đặt Password mà từ thường xuyên gõ đúng như: asdf;lkj
- Hãy thay đổi mật khẩu thường xuyên ít nhất một tháng một lần – Hãy thay đổi ngay lập tức khi phát hiện ra mật khẩu của mình bị người khác sử dụng.
- Đừng bao giờ chứa Password trên máy tính của bạn – nhiều người có thói quen vào các trang web và lưu lại mật khẩu của mình điều này không bảo mật bởi mã hóa trong máy tính dễ dàng bị giải mã.
- Các mật khẩu trong Windows lưu vào các file .pwl không được bảo mật.
- Không nói cho người khác biết mật khẩu của mình.
- Không gửi mail và tránh đặt trùng Password trên nhiều ứng dụng
- Không ghi Password của mình ra cho dễ nhớ.
- Khi gõ Password hãy cẩn thận với các loại Keylogger và người xem trộm.

5. Hacker lấy mật khẩu của bạn qua những phương pháp nào?

- Xem bạn gõ mật khẩu

- Tìm xem bạn có ghi mật khẩu của mình ra giấy hay không
- Đoán mật khẩu dựa vào các số quen thuộc như: 123456, 654321…
- Sử dụng phương thức tấn công Brute Force: Đây là phương thức tổng hợp các ký tự lần lượt để tấn tìm ra mật khẩu, thử và sai liên tục cho đến khi tìm ra mật khẩu đúng.
- Sử dụng phương thức tấn công Dictionary Attack: Phương thức tấn công này tìm mật khẩu trong một bộ từ điển được sinh ra trước đó.
- Cách tạo ra một mật khẩu khó:
    - Chẳng hạn mật khẩu của tôi ban đầu định đặt là: yeuemnhieu
    - Giờ tôi viết hoa chữ Y và chữ U thành: YeUemnhieU
    - Chữ E trong bảng chữ cái đứng vị chí 5 mật khẩu tôi thành: Y5U5mnhi5U
    - Chữ i tôi đổi thành ! mật khẩu thành Y5U5mnh!5U
    - Password của tôi đủ 10 ký tự có số, có hoa, có thường, có ký tự đặc biệt.

6. Xóa Password đã được lưu trong Windows XP

Vào run gõ: **Rundll32.exe Keymgr.dll, KRShowKeyMgr**, sẽ hiện ra bảng danh sách website và bạn hãy xóa hết những mật khẩu đã được lưu trong hệ thống.

7. Phá mật khẩu tổng quát

Về định nghĩa một Password Cracker là chương trình có thể giải mã được mật khẩu hay có thể vô hiệu hóa được mật khẩu.

Password Cracker có hai phương pháp chính đó là: ***Brute Force*** và ***Dictionary Attack***, ngoài ra hiện nay mới có chương trình phá mật

khẩu thông minh hơn hai kiểu cổ điển trên đó là phương thức tìm Password: ***Smart Table Recovery*** – đáp ứng tốc độ tìm mật khẩu rất nhanh.

Password Cracker cũng có thể là một chương trình dùng để giải mã những mật khẩu đã được mã hóa, ví như các mật khẩu được lưu trong IE, Firefox,…

8. Mục tiêu của các chương trình tìm mật khẩu

Trên hệ thống Windows và Linux có hai tài khoản toàn quyền trong hệ thống đó là: root và Administrator, và mục tiêu tấn công là tìm được password của hai tài khoản đó

Khi tìm được Password của tài khoản có quyền quản trị kẻ tấn công sẽ có toàn quyền với máy đích.

Kẻ tấn công cũng có thể dùng các phần mềm Sniffer để tóm các gói tin Username Password được truyền đi trong hệ thống mạng.

Và ảnh hưởng của việc bị chiếm mất quyền quản trị tùy thuộc hoàn toàn vào dữ liệu và các ứng dụng trong hệt hống.

9. Chương trình Password Cracker hoạt động như thế nào

Để hiểu được một Password Cracker làm việc như thế nào chúng ta cần phải hiểu được các chương trình quản lý Password thực hiện ra sao. Hầu hết các chương trình quản lý Password đều mã hóa Password theo một phương thức nào đó.

Mật khẩu sau khi được tạo ra và lưu vào trong hệ thống sẽ được mã hóa, hệ thống sẽ chứa Key để giải mã mật khẩu. Những phần mềm Password Cracker sẽ tìm cách lấy được các đoạn mật mã đó. Sau khi đã lấy được các đoạn mật mã trên máy của nạn nhân chúng sẽ tiến hành giải mã mật khẩu bằng những phương thức cụ thể cho từng tình huống.

10. Các dạng Password Cracker

- *Dictionary Attack:* Tìm mật khẩu trong một file từ điển tạo sẵn

- *Brute Force Attack*: Tìm mật khẩu bằng cách tổ hợp các ký tự
- *Hybird Attack*: Lai giữa hai phương thức trên
- *Smart Table Recovery Attack*: Phương thức tấn công tìm mật khẩu thông minh nhất dựa trên các bảng dữ liệu – Khoảng 700MB dữ liệu text.

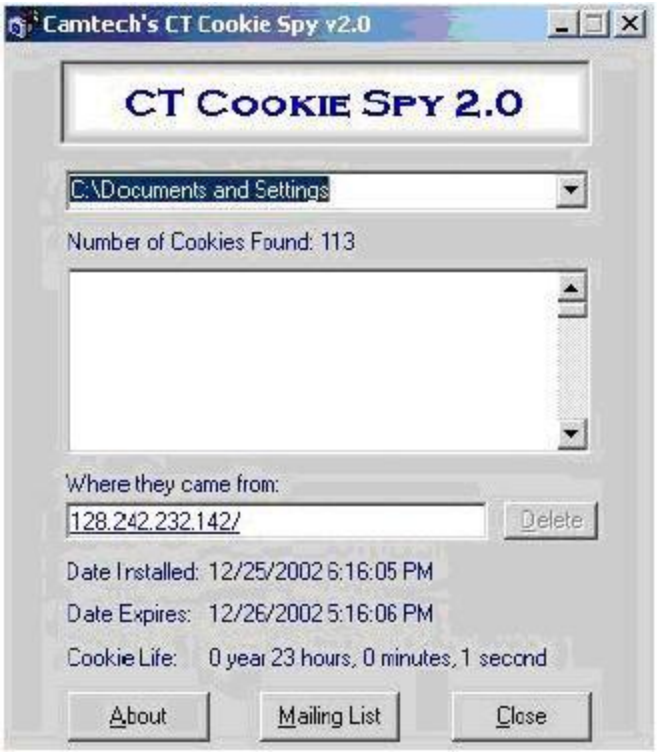
11. Tìm Password bằng phương thức đơn giản

Có 2 phương thức để tìm mật khẩu đơn giản là:

- Đoán mật khẩu
- Thay thế đoạn URL

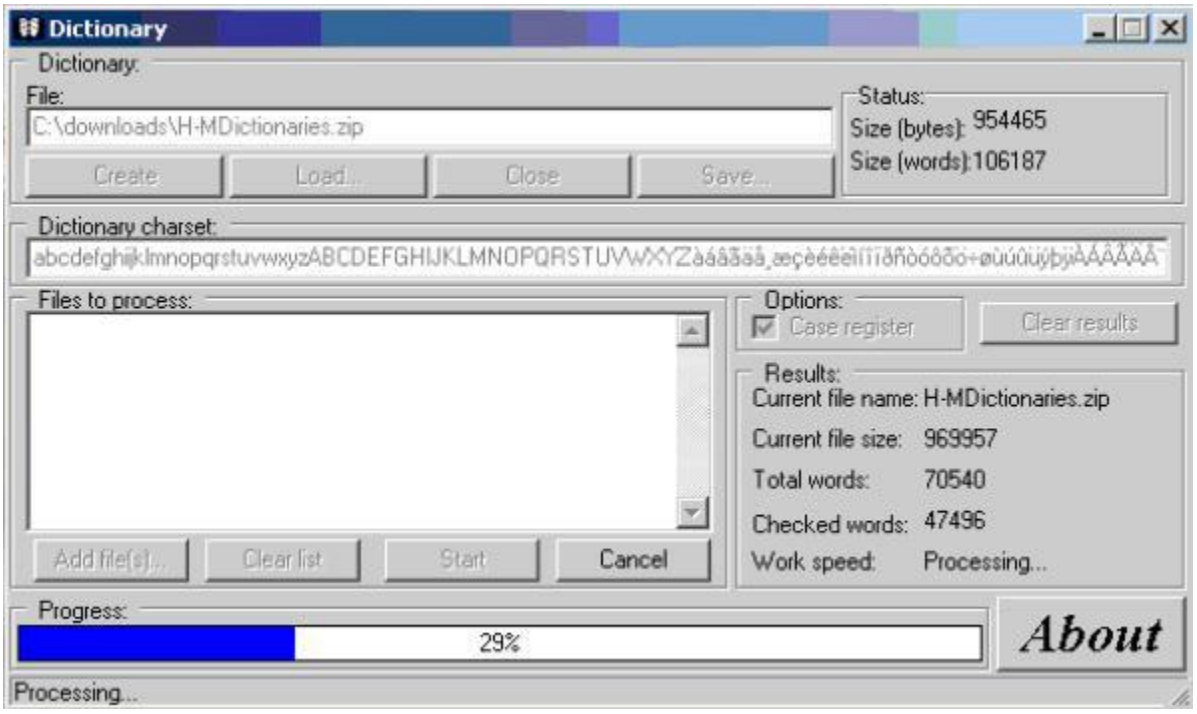
12. Tìm Password bằng giải mã Cookies

- Với chương trình CT cookie Spy 2.0
- Cookies thương lưu lại rất nhiều thông tin quan trọng của người dùng khi truy cập vào Internet như Username và Password truy cập vào một Website.
- Với phần mềm này bạn có thể tìm kiếm các Cookies được lưu dữ trong hệ thống và giải mã chúng để tìm Username Password.



13. Tấn công Dictionary Attack

Tạo từ điển dùng phần mềm: Dictionary Maker



14. Danh sách các Tools Password Crackers

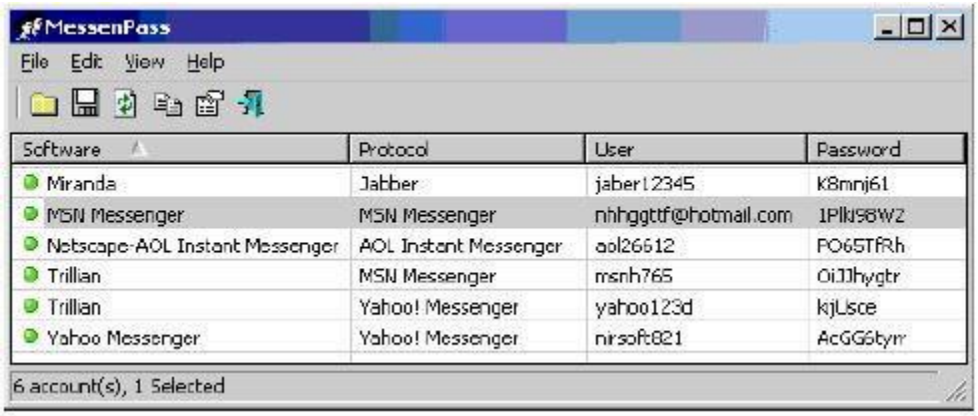
- Lophtcrack - WebCracker
- John The Ripper - Munga Bunga
- Brutus - ReadCookies
- Obiwan - SnadBoy
- Authforce - WinSSLMiM
- Hydra - RAR
- Cain & Abel Gammaprog

Hầu hết các tools này đều miễn phí và nếu có phí thì hoàn toàn crack được một cách dễ dàng.

Hầu hết chúng đều có khả năng sử dụng tất cả các loại tấn công trên, đều có thể Export Username Password từ một hệ thống Local hay Remote.

- Theo kinh nghiệm của tôi hay dùng đó là: Cain & Abel tuy nhiên phần mềm này mạnh về giải mã và Sniffer hơn. Lophcrack có lẽ crack khá nhanh bất kỳ password nào dài dưới 10 ký tự máy tính của tôi chỉ cần khoảng hơn 1 giờ là có thể giải mã được.
- John the Ripper đây là phần mềm chuyên phá mật khẩu trong môi trường Unix và sử dụng mã hóa DES, Extend DES, MD5 cũng tích hợp nhiều phương pháp giải mã.
- Brutus là một chương trình Online hay Remote Password Cracker. Tấn công tới một hệ thống như máy chủ IIS, Windows, Modem ADSL…. Chúng thử lần lượt Username và Password nhất định để tấn công vào máy chủ
- Obiwan khắc phục nhược điểm của Brutus là có độ trễ khi sử dụng Username Password sai.

- Authforce dựa vào HTTP Basic Authentication hỗ trợ việc thử Username Password tới một site nhất định
- MessenPass có thể giải nén được hầu hết các tài khoản chát như Yahoo, MSN…



- Lưu ý từ phiên bản YM 7 password không bao giờ được lưu ở máy Local lên phần mềm này không crack được.
- Wireless WEP Key Password Spy đây là một tools hỗ trợ giải mã để truy cập vào một hệ thống mạng vWireless đặt mật khẩu.