Cain & Abel là bộ công cụ dò tìm, phát hiện và giải mã các mật khẩu trên hệ điều hành Microsoft. Cain & Abel hỗ trợ người dùng trong việc khôi phục lại nhiều loại mật khẩu phức tạp đã được mã hóa bằng cách sử dụng các thuật toán giải mã mạnh mẽ và hiện đại nhất. Cain & Abel được phát triển với hy vọng rằng nó là công cụ đắc lực cho các quản trị mạng, các nhân viên điều tra có thể truy cập dễ dàng vào các hệ thống máy tính bị mã khóa do hacker tấn công. Được biết, tác giá của công cụ phá mã này là  Massimiliano Montoro, một lập trình viên máy tính nổi tiếng thế giới.  
  
Cain & Abel hoạt động theo phương thức là sử dụng một số công nghệ tiên tiến để nhanh chóng phá các mật khẩu đã mã hóa bằng các phương pháp Dictionary, Brute-Force and Cryptanalysis, ghi âm các cuộc đàm thoại qua đường VoIP, giải mã các mật khẩu đã được bảo vệ, tìm ra file nơi chứa mật khẩu, phát hiện mật khẩu có trong bộ đệm, và phân tích các giao thức định tuyến.

Chương trình này không khai thác những lỗ hổng chưa được vá của bất kỳ phần mềm nào. Nó chỉ tập trung vào những khía cạnh/điểm yếu hiện có trong các chuẩn giao thức, các phương pháp đăng nhập và các kỹ thuật đệm

**Program Features**

**Cain: là phần đầu tiên của phần mềm, với một giao diện người dùng đơn giản, mục đích chính của nó là tập trung vào một số kỹ thuật xâm nhập và những công cụ giúp phục hồi mật khẩu và các authentication credentials từ nhiều nguồn khác nhau.**

* [Cisco Config Downloader/Uploader (SNMP/TFTP)](http://www.oxid.it/ca_um/topics/cisco_config_downloader_uploader.htm)

Tính năng này cho phép tải về hoặc tải lên tập tin cấu hình của các thiết bị Cisco thông qua SNMP / TFTP.

* [MAC Address Scanner with OUI fingerprint](http://www.oxid.it/ca_um/topics/mac_scanner.htm)

Sử dụng thư viện OUI, cho biết thông tin về một loại thiết bị dựa trên địa chỉ MAC của nó

* [Network  Enumerator](http://www.oxid.it/ca_um/topics/network_enumerator.htm)

Truy xuất tên người dùng, nhóm người dùng, các thư mục chia sẻ và các dịch vụ hiện đang chạy trên một máy trong network

* [Remote Registry](http://www.oxid.it/ca_um/topics/remote_registry.htm)

Cho phép sửa đổi các thông số registry từ network

* [Promiscuous-mode Scanner based on ARP packets](http://www.oxid.it/ca_um/topics/promiscuous-mode_scanner.htm)

Xác định các sniffers và các hệ thống phát hiện xâm nhập (Intrusion Detection) hiện có trên mạng LAN.

* [Route Table Manager](http://www.oxid.it/ca_um/topics/route_table_manager.htm)

Chức năng tương tự như một công cụ có sẵn trong Windows tên là "route.exe" có thêm giao diện người dùng

* [Service Manager](http://www.oxid.it/ca_um/topics/service_manager.htm)

Cho phép bắt đầu, dừng, kết thúc, tiếp tục hoặc gỡ bỏ một dịch vụ.

* [SID Scanner](http://www.oxid.it/ca_um/topics/sid_scanner.htm)

Trích xuất tên người dùng tương ứng với mỗi chứng nhận bảo mật Security Identifiers (SIDs) trên một hệ thống từ xa.

**Password Crackers**

* [Password Crackers](http://www.oxid.it/ca_um/topics/password_crackers.htm)

Cho phép phục hồi mật khẩu đã bị xáo trộn bởi một số hàm băm hoặc các thuật toán mã hóa thông thường. Chương trình hỗ trợ thuật toán [Dictionary](http://www.oxid.it/ca_um/topics/dictionary_password_cracker.htm) và [Brute-Force](http://www.oxid.it/ca_um/topics/brute-force_password_cracker.htm)

* [Cryptanalysis attacks](http://www.oxid.it/ca_um/topics/cryptanalysis.htm)

Cho phép bẻ mật khẩu sử dụng phương pháp ‘[Faster Cryptanalytictime – memory trade off](http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Oech03)’ của Philippe Oechslin. Kỹ thuật bẻ khóa này sử dụng một tập hợp các bảng lớn chứa các mật khẩu được mã hóa đã tính trước, bảng đó được gọi là Rainbow Tables, để cải thiện phương pháp trade-off được biết đến ngày nay nhằm tăng tốc độ phục hồi mật khẩu

* [Rainbowcrack-online client](http://www.oxid.it/ca_um/topics/rainbowcrack-online.htm)

Cho phép bẻ khóa mật khẩu bằng sức mạnh vượt trội của dịch vụ bẻ khóa trực tuyến dựa trên công nghệ RainbowTable

* [WEP Cracker](http://www.oxid.it/ca_um/topics/wep_cracker.htm)

Áp dụng phương pháp tấn công WEP của Performs Korek's và PTW trên chuẩn 802.11 để lấy các tập tin chứa các vectơ khởi tạo WEP.

**Password Decoders**

* [Access (9x/2000/XP) Database Passwords Decoder](http://www.oxid.it/ca_um/topics/access_database_passwords_decoder.htm)

Giải mã các mật khẩu đã được mã hóa từ các tập tin Microsoft Access Database.

* [Base64 Password Decoder](http://www.oxid.it/ca_um/topics/base64_password_decoder.htm)

Giải mã các chuỗi được mã hóa Base64

* [Box Revealer](http://www.oxid.it/ca_um/topics/box_revealer.htm)

Hiện các mật khẩu được hiển thị bằng dấu hoa thị trong hộp thoại password

* [Cisco Type-7 Password Decoder](http://www.oxid.it/ca_um/topics/cisco_type-7_password_decoder.htm)

Giải mã mật khẩu Cisco Type-7 được sử dụng trong router và các file cấu hình

* [Cisco VPN Client Password Decoder](http://www.oxid.it/ca_um/topics/cisco_vpn_client_password_decoder.htm)

Giải mã các mật khẩu Cisco VPN Client được lưu trữ trong những tập tin hồ sơ kết nối (connection profiles) (\*.pcf).

* [Credential Manager Password Decoder](http://www.oxid.it/ca_um/topics/credential_manager_password_decoder.htm)

Giải mã các mật khẩu được lưu trữ trong Enterprise và Local Credential Sets trên Windows XP/2003.

* [Dialup Password Decoder](http://www.oxid.it/ca_um/topics/dialup_password_decoder.htm)

Giải mã các mật khẩu được lưu trữ bởi các thành phần trong Windows "Dial-Up Networking"

* [Enterprise Manager Password Decoder](http://www.oxid.it/ca_um/topics/enterprise_manager_password_decoder.htm)

Giải mã các mật khẩu được sử dụng bởi Microsoft SQL Server Enterprise Manager (SQL 7.0 và 2000 cũng được hỗ trợ).

* [Protected Storage Password Manager](http://www.oxid.it/ca_um/topics/protected_storage_password_manager.htm)

Giải mã các mật khẩu cục bộ được lưu trữ trong Outlook, Outlook Express, Outlook Express Identities, Outlook 2002, Internet Explorer and MSN Explorer.

* [PWL Cached Password Decoder](http://www.oxid.it/ca_um/topics/pwl_cached_password_decoder.htm)

Cho phép xem tất cả các tài nguyên được lưu trữ và những mật khẩu liên quan dưới dạng văn bản từ danh sách các tập tin (dù bị khóa hay chưa khóa).

* [Remote Desktop Password Decoder](http://www.oxid.it/ca_um/topics/remote_desktop_password_decoder.htm)

Giải mã các mật khẩu trong Remote Desktop Profiles (các tập tin .RPD ).

* [Syskey Decoder](http://www.oxid.it/ca_um/topics/syskey_decoder.htm)

Khôi phục lại khóa khởi động được sử dụng bởi tiện ích SYSKEY từ local registry hoặc từ các tập tin hệ thống “offline”.

* [VNC Password Decoder](http://www.oxid.it/ca_um/topics/vnc_password_decoder.htm)

Giải mã các mật khẩu VNC trong registry đã được mã hóa.

* [Wireless Zero Configuration Password Dumper](http://www.oxid.it/ca_um/topics/wireless_zero_configuration_password_dumper.htm)

Khôi phục các mật khẩu wireless được lưu trữ trong Windows Wireless Configuration Service.

* [802.11 Capture Files Decoder](http://www.oxid.it/ca_um/topics/802.11_capture_files_decoder.htm)

Giải mã file chụp 802.11 (wireshark, pcap) bao gồm wireless frames được mã hóa với WEP hoặc WPA-PSK

**Password Dumpers**

* [LSA Secrets Dumper](http://www.oxid.it/ca_um/topics/lsa_secrets_dumper.htm)

Dump các nội dụng của Local Security Authority Secrets

* [MSCACHE Hashes Dumper](http://www.oxid.it/ca_um/topics/mscache_hashes_dumper.htm)

Lấy lại các mật khẩu băm MSCACHE được lưu trữ trong local registry.

* [MySQL Password Extractor via ODBC](http://www.oxid.it/ca_um/topics/mysql_passwords_extractor.htm)

Kết nối tới một MySQL server thông qua ODBC và lấy ra thông tin người dùng cũng như mật khẩu từ database

* [NT Hash Dumper + Password History Hases (works with Syskey enabled)](http://www.oxid.it/ca_um/topics/nt_hashes_dumper.htm)

Lấy lại mật khẩu NT bị phân rã từ file SAM bất kể Syskey có tồn tại hay không

* [Oracle Password Extractor via ODBC](http://www.oxid.it/ca_um/topics/oracle_passwords_exctractor.htm)

Kết nối tới một Oracle server thông qua ODBC và lấy ra thông tin người dùng cũng như mật khẩu từ database

* [Microsoft SQL Server 2000 Password Extractor via ODBC](http://www.oxid.it/ca_um/topics/sql_server_2000_password_extractor.htm)

Kết nối tới một SQL server thông qua ODBC và lấy ra thông tin người dùng cũng như mật khẩu từ database chính

**Password/Hash Calculators**

* [Hash Calculator](http://www.oxid.it/ca_um/topics/hash_calculator.htm)

Xuất ra các giá trị băm (hash) từ một đoạn text có sẵn

* [RSA SecurID Token Calculator](http://www.oxid.it/ca_um/topics/rsa_securid_token_calculator.htm)

Có thể tính khóa RSA từ tập tin kích hoạt XML có sẵn

**Sniffer**

* [APR (ARP Poison Routing)](http://www.oxid.it/ca_um/topics/apr.htm)

Cho phép nghe lên trên các mạng chuyển mạch và tấn công theo phương pháp Man-in-the-Middle

* [Full HTTPS sessions sniffer for APR (APR-HTTPS)](http://www.oxid.it/ca_um/topics/apr-https.htm)

Cho phép bắt (capture) tất cả dữ liệu được gửi trên các phiên truyền của giao thức HTTPS

* [Full FTPS sessions sniffer for APR (APR-FTPS)](http://www.oxid.it/ca_um/topics/apr-ftps.htm)

Cho phép bắt (capture) tất cả các dữ liệu được gửi qua các phiên truyền của giao thức ẩn FTPS trên mạng.

* [Full IMAPS sessions sniffer for APR (APR-IMAPS)](http://www.oxid.it/ca_um/topics/apr-imaps.htm)

Cho phép bắt (capture) tất cả các dữ liệu được gửi thông qua các phiên truyền của giao thức IMAPS trên mạng.

* [Full LDAPS sessions sniffer for APR (APR-LDAPS)](http://www.oxid.it/ca_um/topics/apr-ldaps.htm)

Cho phép bắt (capture) tất cả các dữ liệu được gửi thông qua các phiên truyền của giao thức ẩn LDAPS trên mạng.

* [Full POP3S sessions sniffer for APR (APR-POP3S)](http://www.oxid.it/ca_um/topics/apr-pop3s.htm)

Cho phép bắt (capture) tất cả các dữ liệu được gửi thông qua các phiên truyền của giao thức ẩn POP3S trên mạng.

* [Full RDP sessions sniffer for APR (APR-RDP)](http://www.oxid.it/ca_um/topics/apr-rdp.htm)

Cho phép sao chép lại tất cả các dữ liệu được gửi thông qua phiên truyền của giao thức Remove Deskstop Protocal (RDP) trên mạng. Ghi lại toàn bộ các dữ liệu mà người dùng nhập từ bàn phím.

* [Full SSH-1 sessions sniffer for APR (APR-SSH-1)](http://www.oxid.it/ca_um/topics/apr-ssh-1.htm)

Cho phép bắt (capture) tất cả các dữ liệu được gửi thông qua các phiên truyền của giao thức SSH-1 trên mạng.

* [Certificates Collector](http://www.oxid.it/ca_um/topics/certificates_collector.htm)

Lấy các tín chỉ từ các website HTTPS, IMAPS, POP3S, LDAPS, FTPS và sử dụng chúng cho các bộ lọc sniffer APR-\* tương ứng

* [TCP/UDP Table Viewer](http://www.oxid.it/ca_um/topics/tcp_udp_table_viewer.htm)

Cho biết tình trạng của các port cục bộ (như netstat)

* [TCP/UDP/ICMP Traceroute with DNS resolver and WHOIS client](http://www.oxid.it/ca_um/topics/traceroute.htm)

Một traceroute cải tiến có thể sự dụng các giao thức TCP, UDP and ICMP và cung cấp các khả năng của máy khách WHOIS.

* [Wireless Scanner](http://www.oxid.it/ca_um/topics/wireless_scanner.htm)

Có thể quét tín hiệu wireless, từ đó truy ra địa chỉ MAC, thời gian kết nối gần đây nhất, cường độ của tín hiệu, tên của mạng (SSID), được mã hóa kiểu gì (EWP hay WPA), là một mạng Ad-hoc hay một mạng cơ sở (Infrastructure), những kênh mạng đang hoạt động và tốc độ của nó (vd như 11 Mbps). Chương trình hỗ trợ chế độ quét tự động và nghe lén WEP IVs sử dụng bộ chuyển đổi AirpCap của hang CACE Technologies.

**Abel: là phần thứ hai của phần mềm, được thiết kế như một dịch vụ dành cho Windows NT gồm 2 file Abel.exe và Abel.dll, vì vậy không cần cài đặt ta vẫn có thể sử dụng được. Abel giao tiếp với Cain thông qua đường dẫn có dạng** **"\\computername\pipe\abel" và có thể kết nối từ nhiều host cùng một lúc. Tất cả dữ liệu truyền qua đường dẫn này đều được mã hóa bằng thuật toán mã hóa đối xứng RC4 với khóa là “Cain&Abel”**

* [Remote Console](http://www.oxid.it/ca_um/topics/remote_console.htm)

Cung cấp một shell cho hệ thống điều khiển từ xa trên một máy tính từ xa

* [Remote LSA Secrets Dumper](http://www.oxid.it/ca_um/topics/remote_lsa_secrets_dumper.htm)

Dump các nội dụng của Local Security Authority Secrets trên một hệ thống từ xa

* [Remote NT Hash Dumper + Password History Hases (works with Syskey enabled)](http://www.oxid.it/ca_um/topics/remote_nt_hashes_dumper.htm)

Lấy lại các mật khẩu băm NT từ tập tin SAM bất kể Syskey đã kích hoạt hay chưa; tính năng hoạt động từ phía Abel.

* [Remote Route Table Manager](http://www.oxid.it/ca_um/topics/remote_route_table_manager.htm)

Cho phép quản lý bảng định tuyến của hệ thống từ xa

* [Remote TCP/UDP Table Viewer](http://www.oxid.it/ca_um/topics/remote_tcp_udp_table_viewer.htm)

Cho biết tình trạng của các port cục bộ (như netstat) của hệ thống từ xa