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 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 associated to 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 bé khóa trực tuyến dựa trên công nghệ RainbowTable

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

Performs Korek's and PTW  WEP attacks on 802.11 capture files containing enough WEP initialization vectors.

**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 and switches configuration files.

* [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)

Allows you to view all cached resources and relative passwords in clear text either from locked or unlocked password list files.

* [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)

Will retrieve the Boot Key used by the SYSKEY utility from the local registry or "off-line" SYSTEM files.

* [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)

Decode 802.11 capture files (wireshark, pcap) containing wireless frames encrypted with WEP or WPA-PSK.

**Password Dumpers**

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

Dumps the contents of the Local Security Authority Secrets.

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

Will retrieve the MSCACHE password hashes stored into the local registry.

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

Connects to an MySQL server via ODBC and extracts all users and passwords from the database.

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

Will retrieve the NT password hash from the SAM file regardless of whether Syskey in enabled or not.

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

Connects to an Oracle server via ODBC and extracts all users and passwords from the database.

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

Connects to an SQL server via ODBC and extracts all users and passwords from the master database.

**Password/Hash Calculators**

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

Produces the hash values of a given text.

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

Can calculate the RSA key given the token's .XML activation file.

**Sniffer**

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

Enables sniffing on switched networks and Man-in-the-Middle attacks.

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

Allows you to capture all data sent in HTTPS sessions on the network.

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

Allows you to capture all data sent in implicit FTPS sessions on the network.

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

Allows you to capture all data sent in implicit IMAPS sessions on the network.

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

Allows you to capture all data sent in implicit LDAPS sessions on the network.

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

Allows you to capture all data sent in implicit POP3S sessions on the network.

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

Allows you to capture all data sent in a Remote Desktop Protocol (RDP) session on the network. Provides interception of keystrokes activity client-side.

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

Allows you to capture all data sent in SSH-1 sessions on the network.

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

Grab certificates from HTTPS, IMAPS, POP3S, LDAPS, FTPS web sites and prepares them to be used by relative APR-\* sniffer filters.

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

Shows the state of local ports (like netstat).

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

A improved traceroute that can use TCP, UDP and ICMP protocols and provides whois client capabilities.

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

Can scan for wireless networks signal within range, giving details on its MAC address, when it was last seen, the guessed vendor, signal strength, the name of the network (SSID), whether it has WEP or not (note WPA encrypted networks will show up as WEPed), whether the network is an Ad-Hoc network or Infrastructure, what channel the network is operating at and at what speed the network is operating (e.g. 11Mbps). Passive scanning and WEP IVs sniffing are also supported using the AirpCap adapter from 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)

Provides a remote system shell on the remote machine.

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

Dumps the contents of the Local Security Authority Secrets present on the remote system.

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

Will retrieve the NT password hash from the SAM file regardless of whether Syskey in enabled or not; works on the Abel-side.

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

Enable to manage the route table of the remote system.

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

Shows the state of local ports (like netstat) on the remote system.