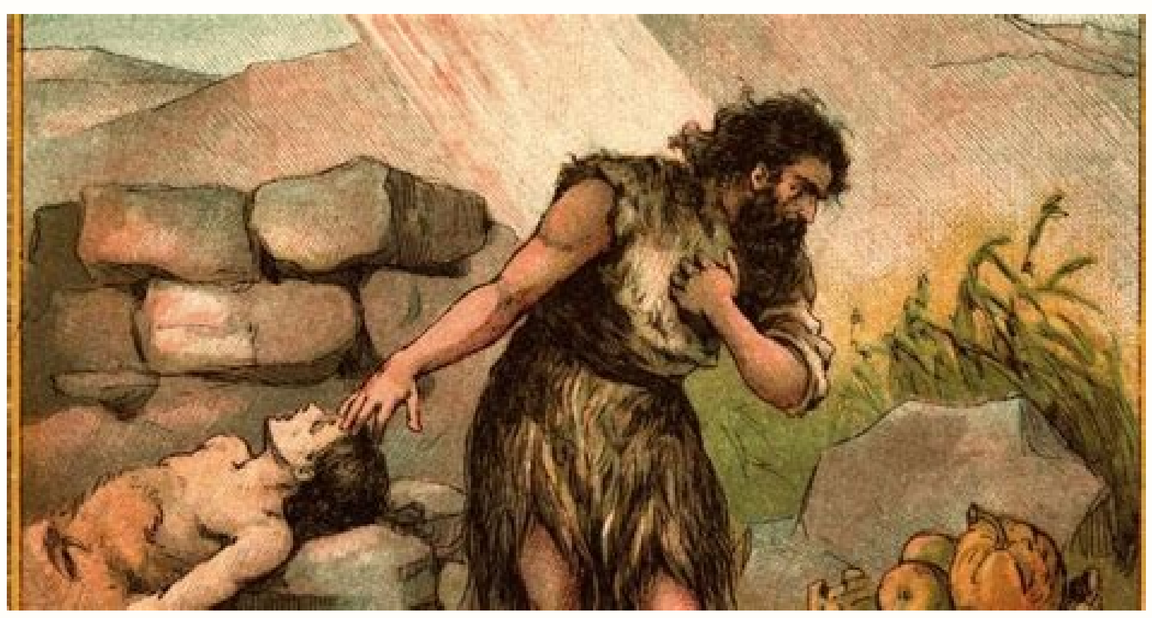
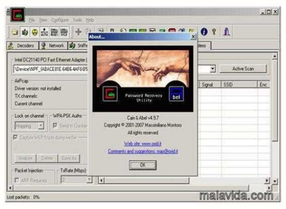
Oxid. it cain abel

I'm not robot!





Password recovery software Not to be confused with CAINE Linux in the List of digital forensics tools. Cain and AbelDeveloper(s)Massimiliano MontoroStable release4.9.56 / April 7, 2014; 8 years ago (2014-04-07) Operating systemMicrosoft WindowsTypePassword cracking/Packet analysisLicenseFreewareWebsite //www.oxid.it/cain.html Cain and Abel (often abbreviated to Cain) was a password recovery tool for Microsoft Windows. It could recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks.[1] Cryptanalysis attacks were done via rainbow tables which could be generated with the winrtgen.exe program provided with Cain and Abel.[2] Cain and Abel was maintained by Massimiliano Montoro[3] and Sean Babcock.[4] Features WEP cracking Speeding up packet capture speed by wireless packet injection Ability to record VoIP conversations Decoding scrambled passwords Calculating hashes Traceroute Revealing password boxes Uncovering cached passwords Dumping protected storage passwords ARP spoofing IP to MAC Address resolver Network Password Sniffer LSA secret dumper Ability to crack: LM & NTLM hashes NTLMv2 hashes Microsoft Cache hashes Microsoft Windows PWL files Cisco IOS - MD5 hashes Cisco PIX - MD5 hashes APOP - MD5 hashes CRAM-MD5 MD5 hashes OSPF - MD5 hashes RIPv2 MD5 hashes VRRP - HMAC hashes Virtual Network Computing (VNC) Triple DES MD2 hashes MD4 hashes MD5 hashes SHA-1 hashes SHA-2 hashes RIPEMD-160 hashes Kerberos 5 hashes RADIUS shared key hashes IKE PSK hashes MSSQL hashes MySQL hashes Oracle and SIP hashes Status with virus scanners Some virus scanners (and browsers, e.g. Google Chrome 20.0.1132.47) detect Cain and Abel as malware. Avast! detects it as "Win32:Cain-B [Tool]" and classifies it as "Other potentially dangerous program",[5] while Microsoft Security Essentials detects it as "Win32/Cain!4_9_14" and classifies it as "Tool: This program has potentially unwanted behavior." Even if Cain's install directory, as well as the word "Cain", are added to Avast's exclude list, the real-time scanner has been known to stop Cain from functioning. However, the latest version of Avast no longer blocks Cain. Symantec (the developer of the Norton family of computer security software) identified a buffer overflow vulnerability in version 4.9.24 that allowed for remote code execution in the event the application was used to open a large RDP file, as might occur when using the program to analyze network traffic.[6] The vulnerability had been present in the previous version (4.9.23) as well[7] and was patched in a subsequent release. See also Black-hat hacker White-hat hacker Hacker (computer security) Password cracking Aircrack-ng Crack DaveGrohl Hashcat John the Ripper L0phtCrack Ophcrack RainbowCrack References ^ "How to use Cain and Abel". Cybrary. Retrieved 2019-08-24. ^ "ECE 9609/9069: Introduction to Hacking". Whisper Lab. Archived from the original on 2019-08-24. Retrieved 2019-08-24. ^ Zorz, Mirko (2009-07-07). "Q&A: Cain & Abel, the password recovery tool". Help Net Security. Retrieved 2019-08-24. ^ Funk, Mark (2019-01-21). "Cain and Abel recovery tool". CybersGuards.com. Retrieved 2022-01-06. ^ Metev, Denis (2019-07-29). "What Is Brute-Force And How to Stay Safe?". Tech Jury. Retrieved 2019-08-24. ^ "Attack: Massimiliano Montoro Cain & Abel .rdp File BO: Attack Signature - Symantec Corp". www.symantec.com. Retrieved 2019-08-24. ^ "Massimiliano Montoro Cain & Abel Malformed '.rdp' File Buffer Overflow Vulnerability". www.securityfocus.com. Retrieved 2019-08-24. External links Official website (archived) Interview with Massimiliano Montoro, developer of Cain & Abel Retrieved from " hackingpasswordsecuritytoolsPlease log in to take part in the discussion (add own reviews or comments). According to the official website, Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols. The latest version is faster and contains a lot of new features like APR (ARP Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS and contains filters to capture credentials from a wide range of authentication mechanisms. The new version also ships routing protocols authentication monitors and routes extractors, dictionary and brute-force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders and some not so common utilities related to network and system security. Cain & Abel is a tool that will be quite useful for network administrators, teachers, professional penetration testers, security consultants/professionals, forensic staff and security software vendors. Requirements The system requirements needed to successfully setup Cain & Abel are: At least 10MB hard disk space Microsoft Windows 2000/XP/2003/Vista OS Winpcap Packet Driver (v2.3 or above) Airpcap Packet Driver (for passive wireless sniffer / WEP cracker) Installation First we need to download Cain & Abel, so go to the download page www.oxid.it/cain.html. After downloading it, just run the Self-Installing executable package and follow the installation instructions. Cain’s features Here’s a list of all of Cain’s features that make it a great tool for network penetration testing: Protected Storage Password Manager Credential Manager Password Decoder LSA Secrets Dumper Dialup Password Decoder Service Manager APR (ARP Poison Routing) Route Table Manager Network Enumerator SID Scanner Remote Registry Sniffer Routing Protocol Monitors Full RDP sessions sniffer for APR Full SSH-1 sessions sniffer for APR Full HTTPS sessions sniffer for APR Full FTPS sessions sniffer for APR Full POP3S sessions sniffer for APR Full IMAPS sessions sniffer for APR Full LDAPS sessions sniffer for APR Certificates Collector MAC Address Scanner with OUI fingerprint Promiscuous-mode Scanner Wireless Scanner PWL Cached Password Decoder 802.11 Capture Files Decoder Password Crackers Access (9x/2000/XP) Database Passwords Decoder Cryptanalysis attacks Base64 Password Decoder WEP Cracker Cisco Type-7 Password Decoder Rainbowcrack-online client Cisco VPN Client Password Decoder Enterprise Manager Password Decoder RSA SecurID Token Calculator Hash Calculator TCP/UDP Table Viewer TCP/UDP/ICMP Traceroute Cisco Config Downloader/Uploader (SNMP/TFTP) Box Revealer Wireless Zero Configuration Password Dumper Remote Desktop Password Decoder MSCACHE Hashes Dumper MySQL Password Extractor Microsoft SQL Server 2000 Password Extractor Oracle Password Extractor VNC Password Decoder Syskey Decoder Related definitions MAC: (from Wikipedia) “A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the Media Access Control protocol sub-layer of the OSI reference model. MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, the card’s read-only memory, or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer’s registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. A network node may have multiple NICs and will then have one unique MAC address per NIC.” Sniffing: (fromWikipedia) “A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet’s raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications.” ARP(from Wikipedia) “Address Resolution Protocol (ARP) is a telecommunications protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks. ARP was defined by RFC 826 in 1982. It is Internet Standard STD 37. It is also the name of the program for manipulating these addresses in most operating systems.” Usage Now after launching the application, we have to configure it to use appropriate network card.If you have multiple network cards, it’s better to know the MAC address of the network card that you will use for the sniffer.To get the MAC address of your network interface card, do the following: 1- Open CMD prompt. /p> 2- Write the following command “ipconfig /all”. 3- Determine the MAC address of the desired Ethernet adapters, write it on Notepad,and then use this information to help determine which NIC to select in the Cain application. Now clickConfigure on the main menu. It will open the configuration dialog box where you can select the desired network interface card. Now let’s go through the configuration dialog tabs and take a brief look at most of them: Sniffer tab: This tab allows us to specify which Ethernet interface card we will use for sniffing. ARP tab: This tab allows us to configure ARP poison routing to perform ARP poisoning attack, which tricks the victim’s computer by impersonating other devices to get all traffic that belongs to that device, which is usually the router or an important server. Filters and ports tab: This tab has the most standard services with their default port running on.You can change the port by right-clicking on the service whose port you want to change and then enabling or disabling it. Cain’s sniffer filters and application protocol TCP/UDP port. HTTP fields tab: There are some features of Cain that parse information from web pages viewed by the victim such as LSA Secrets dumper, HTTP Sniffer and ARP-HTTPS,so the more fields you add to the username and passwords fields, the more you capture HTTP usernames and passwords from HTTP and HTTPS requests. Here is an example: The following cookie uses the fields “logonusername=” and “userpassword=” for authentication purposes. If you don’t include these two fields in the list, the sniffer will not extract relative credentials. GET /mail/Login?domain=xxxxxx.xx&style=default&plain=0 HTTP/1.1 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */* Referer: Accept-Language: it Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; (R1 1.3); .NET CLR 1.1.4322) Host: xxx.xxxxxx.xx Connection: Keep-Alive Cookie: ss=1; logonusername=user@xxxxxx.xx; ss=1; srclng=it; srcdmn=it; srctrg=_blank; srcbld=y; srcauto=on; srcclp=on; srcsct=web; userpassword=password; video=c1; TEMPLATE=default; Traceroute tab: Traceroute is a technique to determine the path between two points by simply counting how many hops the packet will take from the source machine to reach the destination machine. Cain also adds more functionality that allows hostname resolution, Net mask resolution, and Whois information gathering. Certificate spoofing tab: This tab will allow Certificate spoofing.From Wikipedia: “In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document that uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users (“endorsements”). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.” We can simply think of it as some sort of data (cipher suites & Public key and some other information about the owner of the certificate) that has information about the destination server and is encrypted by trusted companies (CA) that are authorized for creating these types of data.The server sends its own certificate to the client application to make sure it’s talking to the right server. Certificate collector tab: This tab will collect all certificates back and forth between servers and clients by setting proxy IPs and ports that listen to it. Challenge spoofing tab: Here you can set the custom challenge value to rewrite into NTLM authentications packets. This feature can be enabled quickly from Cain’s toolbar and must be used with APR. A fixed challenge enables cracking of NTLM hashes captured on the network by means of Rainbow Tables. Password cracking Now it’s time to speak about the cracker tab,the most important feature of Cain.When Cain captures some LM and NTLM hashes or any kind of passwords for any supported protocols, Cain sends them automatically to the Cracker tab.We will import a local SAM file just for demonstration purposes to illustrate this point.Here is how to import the SAM file: Here are

the 4 NTLM and LM hashes which will appear like the following image: And here you will find all possible password techniques in the following image: As you can see from the previous image, there are various types of techniques that are very effective in password cracking.We will look at each of their definitions. Dictionary attack: From Wikipedia: “A dictionary attack uses a targeted technique of successively trying all the words in an exhaustive list called a dictionary (from a pre-arranged list of values). In contrast with a brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words for example a dictionary (hence the phrase dictionary attack). Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), single words found in dictionaries or simple, easily predicted variations on words, such as appending a digit. However these are easy to defeat. Adding a single random character in the middle can make dictionary attacks untenable.” Brute forcing attack: From Wikipedia: “In cryptography, a brute-force attack, or exhaustive key search, is a cryptanalytic attack that can, in theory, be used against any encrypted data (except for data encrypted in an information-theoretically secure manner). Such an attack might be utilized when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. It consists of systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire search space. The key length used in the cipher determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. A cipher with a key length of N bits can be broken in a worst-case time proportional to 2N and an average time of half that. Brute-force attacks can be made less effective by obfuscating the data to be encoded, something that makes it more difficult for an attacker to recognize when he/she has cracked the code. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute-force attack against it.” From Wikipedia: “A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering the plain text password, up to a certain length consisting of a limited set of characters. It is a practical example of a space-time tradeoff, using more computer processing time at the cost of less storage when calculating a hash on every attempt, or less processing time and more storage when compared to a simple lookup table with one entry per hash. Use of a key derivation function that employ a salt makes this attack infeasible. Rainbow tables are a refinement of an earlier, simpler algorithm by Martin Hellman.” How to make a rainbow table? There are many tools that create a rainbow table and there are many rainbow tables already available on the internet.Fortunately, Cain comes with a tool called winrtgen, which is located in its own folder in the installation. You will need to choose ahash algorithm, minimum andmaximum length of password, and finally the charset that the password will use.Then press OK. Conclusion Cain and Abel is a powerful tool that does a great job in password cracking. It can crack almost all kinds of passwords, and it’s usually just a matter of time before you get it. 1- www.wikipedia.org 2- www.oxid.it 3- www.thehackerslibrary.com