

Ethical hacking: software Cain&Abel

lunedì 27 novembre 2006

La guerra tra chi cerca di irrompere all'interno dei sistemi informatici e chi deve difenderli forse non avrà mai fine. Chi per lavoro cerca di migliorare la sicurezza delle reti è costretto da anni ad occuparsi del cosiddetto ethical hacking, cioè imparare a conoscere tecniche e strumenti dei propri avversari. Volevo segnalarvi che nell'ultimo mese Cain&Abel è passato dalla versione 3.0 alla 4.1: Cain & Abel (il manuale qui) è uno strumento per il recupero delle password che utilizza diversi sistemi, per lo sniffing di rete, decodifica di password criptate, attacchi Bruteforce.

Permette di recuperare chiavi di reti wireless, registrare conversazioni VoIP, scoprire password registrate nelle cache e analizzare protocolli di routing. Le ultime versioni hanno introdotto novità per quanto riguarda l'ARP Poison Routing, l'analisi dei protocolli SSH-1 e HTTPS, e soprattutto nell'analisi delle reti wireless. Caratteristiche (inglese): Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind 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 program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort. It covers some security aspects/weakness present in protocol's standards, authentication methods and caching mechanisms; its main purpose is the simplified recovery of passwords and credentials from various sources, however it also ships some "non standard" utilities for Microsoft Windows users.

Cain & Abel has been developed in the hope that it will be useful for network administrators, teachers, security consultants/professionals, forensic staff, security software vendors, professional penetration tester and everyone else that plans to use it for ethical reasons. The author will not help or support any illegal activity done with this program. Be warned that there is the possibility that you will cause damages and/or loss of data using this software and that in no events shall the author be liable for such damages or loss of data. Please carefully read the License Agreement included in the program before using it.

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

Fonte: downloadblog.it e oxid.it