Aris Cahyadi Risdianto - 23210016
ET 5085 – Keamanan Jaringan Telekomunikasi

CAIN AND ABEL

Overview

Cain & Abel adalah password recovery tool untuk Sistem Operasi Microsoft, yang memungkinkan recovery dengan mudah untuk berbagai jenis password dengan cara melakukan *sniffing* di jaringan, *cracking* password yang terenkripsi dengan menggunakan kamus (Dictionary attack), Brute-Force dan Cryptanalysis attacks, merekam percakapan VoIP, decoding *scrambled* password, menemukan kunci jaringan wireless, membongkar password box, mengungkap password yang tersimpan pada *cache* dan menganalisis routing protokol.

Program ini tidak memanfaatkan kelemahan dari suatu perangkat lunak atau bug yang tidak dapat diperbaiki dengan mudah. Tetapi program ini juga mencakup beberapa aspek keamanan / kelemahan intrinsik standar protokol, metode otentikasi dan mekanisme caching dengan tujuan utamanya adalah mempermudah *recovery* password dan kredensial dari berbagai sumber, namun juga ada beberapa utilitas "non standard" untuk pengguna Microsoft Windows.

Cain & Abel telah dikembangkan dengan harapan akan berguna bagi administrator jaringan, guru, konsultan keamanan / profesional, staf forensik, vendor software keamanan, penguji penetrasi profesional dan semua orang yang berencana untuk menggunakannya untuk alasan yang etis.

Tools ini dibagi menjadi 2 bagian yaitu Cain and Abel.

Fitur dari Cain

1. *Protected Storage Password Manager*
   Membongkar password yang disimpan secara lokal dari Outlook, Outlook Express, Outlook Express Identities, Outlook 2002, Internet Explorer dan MSN Explorer.

2. *Credential Manager Password Decoder*
   Membongkar password disimpan dalam Enterprise and Local Credential Sets di Windows XP/2003.

3. *LSA Secret Dumper*
   Memindahkan semua isi Local Security Authority Secrets

4. *Dialup Password Decoder*
   Mengungkapkan password yang disimpan oleh komponen Windows "Dial-Up Networking".

5. *APR (ARP Poison Routing)*
   Mengaktifkan sniffing pada jaringan switching dan melakukan *Man-in-the-Middle attack*.

6. *Route Tabel Manager*
   Menyediakan fungsi yang sama dengan "route.exe" pada tool Windows dengan dilengkapi tampilan.

7. *SID Scanne*r
   Membongkar nama pengguna dengan *Security Identifier (SID)* pada suatu remote sistem.

8. *Network Enumerator*
   Mengambil, semua informasi yang mungkin, seperti nama pengguna, kelompok (group), sharing file/folder, dan layanan yang aktif pada suatu mesin.

9. *Service Manager*
   Memungkinkan untuk melakukan pemberhentian, memulai, memberhentikan sebentar / melanjutkan kembali atau menghapus layanan.

10. *Sniffer*
    Melakukan pengkopian password, hashing dan informasi otentikasi pada saat informasi tersebut dikirimkan melalui jaringan, termasuk beberapa filter untuk otentikasi aplikasi tertentu dan protokol routing. Filter VoIP juga memungkinkan penangkapan percakapan suara yang ditransmisikan dengan protokol / SIP RTP dan kemudian disimpan sebagai file WAV.

11. *Routing Protocol Monitor*
    Memonitor paket dari berbagai protokol routing (HSRP, VRRP, RIPv1, RIPv2, EIGRP, OSPF) untuk menangkap proses otentikasi dan tabel routing bersama.

12. *Full RDP session sniffer untuk APR(APR-RDP)*
    Memungkinkan untuk menangkap semua data dikirim dengan sesi Remote Desktop Protocol (RDP) melalui jaringan. Menyediakan interception dari tombol-tombol apa saja yang ditekan.

13. *Full session SSH-1 sniffer untuk APR (APR-SSH-1)*
    Memungkinkan untuk menangkap semua data yang dikirim dalam sesi SSH pada jaringan.

14. *Full session HTTPS sniffer untuk APR (APR-HTTPS)*
    Memungkinkan Anda untuk menangkap semua data dikirim dalam sesi HTTPS pada jaringan.

15. *Certificates Collector*
    Mengambil sertifikat dari situs web HTTPS dan mempersiapkan mereka untuk digunakan oleh APR-HTTPS.

16. *MAC Address Scanner dengan OUI fingerprint*
    Dengan menggunakan sidik jari OUI, dapat ditebak infrmasi tentang apa jenis alamat MAC device dari Vendor mana.

17. *Promiscuous-mode Scanner based on ARP packet*
    Mengidentifikasi sniffer dan Intrusion Detection sistem yang ada di LAN.

18. *Wireless Scanner*
    Dapat untuk mencari sinyal jaringan nirkabel dalam jangkauan, memberikan rincian tentang alamat MAC-nya, kapan terakhir kali terlihat, menebak jenis vendor , kekuatan sinyal, nama jaringan (SSID), baik yang memiliki WEP atau tidak (catatan WPA jaringan akan dienkripsi ditampilkan sebagai WEPed), apakah jaringan merupakan jaringan Ad-Hoc atau Infrastruktur, apa channel operasi jaringan dan pada kecepatan berapa jaringan yang beroperasi (misalnya 1 1Mbps). Pasif scanning dan sniffing WEP IVs juga didukung menggunakan adaptor AirpCap dari CACE Technologies.

19. *802.11 Capture File Decoder*
    Decode file 802.11 yang ditangkap (dari wireshark, pcap) yang mengandung frame nirkabel terenkripsi dengan WEP atau WPA-PSK.

20. *Access (9x/2000/XP) Database Password Decoder*
    Men-decode password yang terenkripsi dan disimpan dalam file Microsoft Access Database

21. *Base64 Password Decoder*
    Men-decode string disandikan Base64.

22. *Cisco Type-7 Password Decoder*
    Men-decode password cisco type 7 yang digunakan di file konfigurasi router dan switch.

23. *Cisco VPN Client Password Decoder*
    Men-decode password klien Cisco VPN yang tersimpan di profil koneksi (*. PCF).

24. *VNC Password Decoder*
    Men-decode password VNC yang terenkripsi di registri.

25. *Enterprise Manager Password Decoder*
    Men-decode password yang digunakan oleh Microsoft SQL Server Enterprise Manager (SQL 7.0 dan 2000 supported).

26. *Remote Desktop Password Decoder*
    Men-decode password dalam profil Remote Desktop file (RPD file.).

27. *PWL Password Decoder Cached*
    Memungkinkan untuk melihat semua cache dan password yang berhubungan dalam bentuk teks baik yang terkunci atau tidak dalam daftar file password.

28. *Password Crackers*
    Memungkinkan untuk membaca *clear text password yang* diacak menggunakan algoritma hashing atau beberapa enkripsi lainnya. Semua *crackers* mendukung serangan dengan Kamus dan Brute-Force.

29. *Cryptanalysis Attacks*
    Mengaktifkan password cracking dengan menggunakan 'Faster Cryptanalysis time - memori trade off' metode diperkenalkan oleh Philippe Oechslin. Teknik cracking ini menggunakan satu set tabel besar yang berisi password terenkrip yang belum didekrip, yang disebut Tabel Rainbow

30. *WEP Cracker*
    Melakukan Serangan WEP pada file 802.11 yang disimpan dan mengandung WEP vektor inisialisasi.

31. *Rainbow crack-online client*
    Mengaktifkan password cracking dengan menggunakan kekuatan on-line cracking services berbasis teknologi RainbowTable.

32. *NT Hash Dumper + Password History Hashes (bekerja dengan Syskey aktif)*
    Mengambil password hash NT dari file SAM terlepas dari apakah Syskey di diaktifkan atau tidak.

33. *Syskey Decoder*
    Untuk mengambil Boot kunci yang digunakan oleh utilitas Syskey dari registri lokal atau "off-line" SISTEM file.

34. *MSCACHE Hashes Dumper*
    Untuk mengambil MSCACHE password hash yang disimpan ke dalam registri lokal.

35. *Wireless Zero Configuration Password Dumper*
    Akan mengambil kunci nirkabel yang disimpan oleh Windows Wireless Configuration Services.

36. *Microsoft SQL Server 2000 Password Extractor via ODBC*
    Menyambung ke server SQL melalui ODBC dan meng-ekstrak semua pengguna dan password dari database.

37. *Oracle Password Extractor via ODBC*
    Menyambung ke server Oracle melalui ODBC dan ekstrak semua pengguna dan password dari database.

38. *MySQL Password Extractor via ODBC*
    Menyambung ke server MySQL melalui ODBC dan ekstrak semua nama user dan password dari database.

39. *Box Revealer*
    Menunjukkan password yang tersembunyi di balik tanda bintang dalam kotak dialog password.

40. *RSA SecurID Token Calculator*

Dapat menghitung kunci RSA apabila diberi token ASC file.

41. *Hash Calculator*
    Menghasilkan nilai hash dari suatu teks yang diberikan.

42. *TCP/UDP Tabel Viewer*
    Menunjukkan status port lokal yang terbuka(seperti netstat tool).

43. *TCP/UDP/ICMP Traceroute with DNS resolver WHOIS client*
    Perkembangan dari traceroute yang dapat menggunakan protokol TCP, UDP dan ICMP dan menyediakan kemampuan sebagai klien whois.

44. *Cisco Config Downloader / Uploader (SNMP / TFTP)*
    Download atau upload file konfigurasi dari / ke perangkat Cisco tertentu (IP atau nama host) jika diberikan SNMP read/write community string.

Fitur Dari Abel

1. *Remote Console*
   Menyediakan sistem remote shell pada remote mesin.

2. *Remote Route Tabel Manager*
   Memungkinkan untuk mengelola tabel routing dari remote sistem.

3. *Remote TCP / UDP Table Viewer*
   Menunjukkan status port lokal (seperti netstat) pada remote sistem.

4. *Remote NT Hash Dumper + Password History Hashes (bekerja apabila Syskey aktif)*
   Akan mengambil NT hash password dari file SAM, terlepas apakah Syskey di diaktifkan atau t idak, fitur ini bekerja pada sisi-Abel.

5. *Remote LSA Secret Dumper*
   Memindahkan isi dari Local Security Authority Secrets yang ada di remote sistem.

Sebagai peringatan bahwa ada kemungkinan akan menyebabkan kerusakan dan / atau kehilangan data dengan menggunakan software ini sehingga telah dibuat suatu Perjanjian Lisensi yang termasuk dalam panduan ini yang harus disepakati sebelum menggunakan program ini.

Referensi

1. Massimiliano Montoro, Cain & Abel - User Manual, http://www.oxid.it/ca_um/, 2009.

2. Cain & Abel – A useful hacking tool, http://twit88.com/blog/2007/10/16/cain-abel-a-useful-hacking-tool/, 2007.