

## Password di Administrator in Windows 2000, XP e NT

In questa guida impareremo a ottenere la password di Administrator in un sistema basato su Windows 2000 o XP.

### Materiale:

- PC vittima con Win 2000 o Xp installato.
- PC su cui effettuare la ricerca (nel caso ci sia un buon antivirus sulla vittima).
- Linux Knoppix ([www.knoppix.de](http://www.knoppix.de))
- @stake LC4 ([www.@stake.com](http://www.@stake.com))

### Iniziamo:

La procedura per ottenere la password è molto utile in caso essa venga persa o comunque ci si voglia intrufolare in un sistema. Si suppone quindi che del computer vittima voi abbiate accesso solo come utenti limitati (con la facoltà di riavviare il sistema) e che sia installato un potente antivirus (in grado quindi di rilevare attività illecite nel sistema).

Come prima cosa dobbiamo sapere che Windows 2000 e Xp salvano le password per l'accesso alla macchina locale in un file chiamato SAM, esso naturalmente è criptato e protetto da Windows da qualsiasi accesso esterno al kernel. Il file SAM si trova nella directory del sistema operativo nella sottocartella *system32/config* e comunque proviate a copiarlo vi verrà negato l'accesso. E' utile sapere inoltre che in caso del danneggiamento del SAM principale, esiste un file SAM di default o di ripristino nella sottodirectory *repair* di Windows.

Ora che sappiamo dove sono contenute le password non dobbiamo fare altro che trovare il modo di estrarle e decriptarle.

Dato che a sistema operativo lanciato i file su disco rigido vengono protetti da qualunque tentativo di accesso, dovremo estrarre i file quando Windows dorme ossia non è in esecuzione. Per fare ciò ci serviremo di un altro sistema operativo del tutto esterno e lanciabile da boot in modo da non lasciare tracce dell'accesso, uno dei migliori è Knoppix, una distribuzione di Linux molto potente (basata su Debian) e lanciabile dal CD-ROM all'avvio del PC.

Ora riavviamo il computer e configuriamo il bios in modo che la sequenza di boot parta dall'unità CD-ROM, salviamo le modifiche e riavviamo nuovamente.

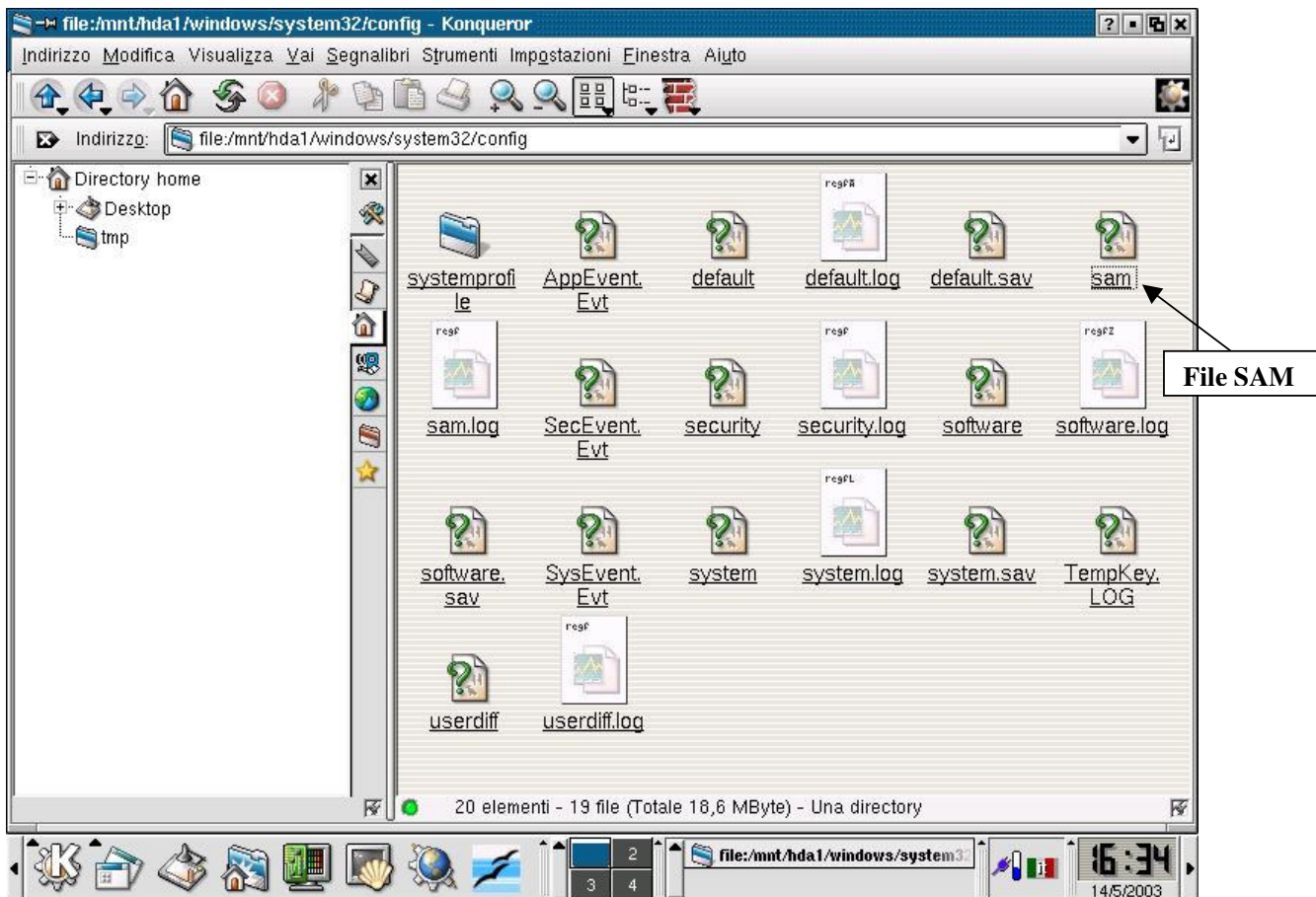
Se il bios è protetto da password dovrete utilizzare dei comandi speciali del bios oppure utilizzare dei programmini in grado di leggere dagli indirizzi di memoria del bios e di visualizzare la password.

Inseriamo ora il CD di Knoppix nel lettore e aspettiamo che venga caricato; la prima schermata permette di lanciare Linux con determinati parametri, visibili alla pressione di F2. In genere il più utile è *knoppix lang=it* che imposta la lingua italiana.

Premuto invio aspettiamo che vengano rilevate le periferiche e caricato il sistema operativo, quando anche KDE sarà lanciato potremo cominciare a muoverci (NOTA: se non dovesse partire l'interfaccia grafica o server X sarà necessario agire tramite il prompt dei comandi).

Ora che knoppix è lanciato, dobbiamo accedere al disco di Windows che il sistema ha già rilevato e posizionarci nella cartella di Win, in genere o *winnt* o *windows* e aprire la sottocartella *system32/config* e copiare il file SAM su un floppy o altrove sul disco rigido.

N.B. Copiare e non spostare il SAM altrimenti Windows non partirà o partirà con la password di default.



Ora abbiamo il file SAM a nostra disposizione e accessibile, non resta che decriptarlo infatti se tenterete di aprirlo con Notepad vedrete i nomi utenti e tanti caratteri strani che rappresentano password e informazioni supplementari.

Riavviamo il sistema e rimuoviamo il CD di Knoppix dal lettore (meglio rimettere a posto anche il bios).

La parte di lavoro che segue deve essere eseguita su un Pc con molta potenza di processore è possibile anche eseguirla sulla stessa vittima a patto che non sia installato un antivirus che solo administrator possa disattivare.

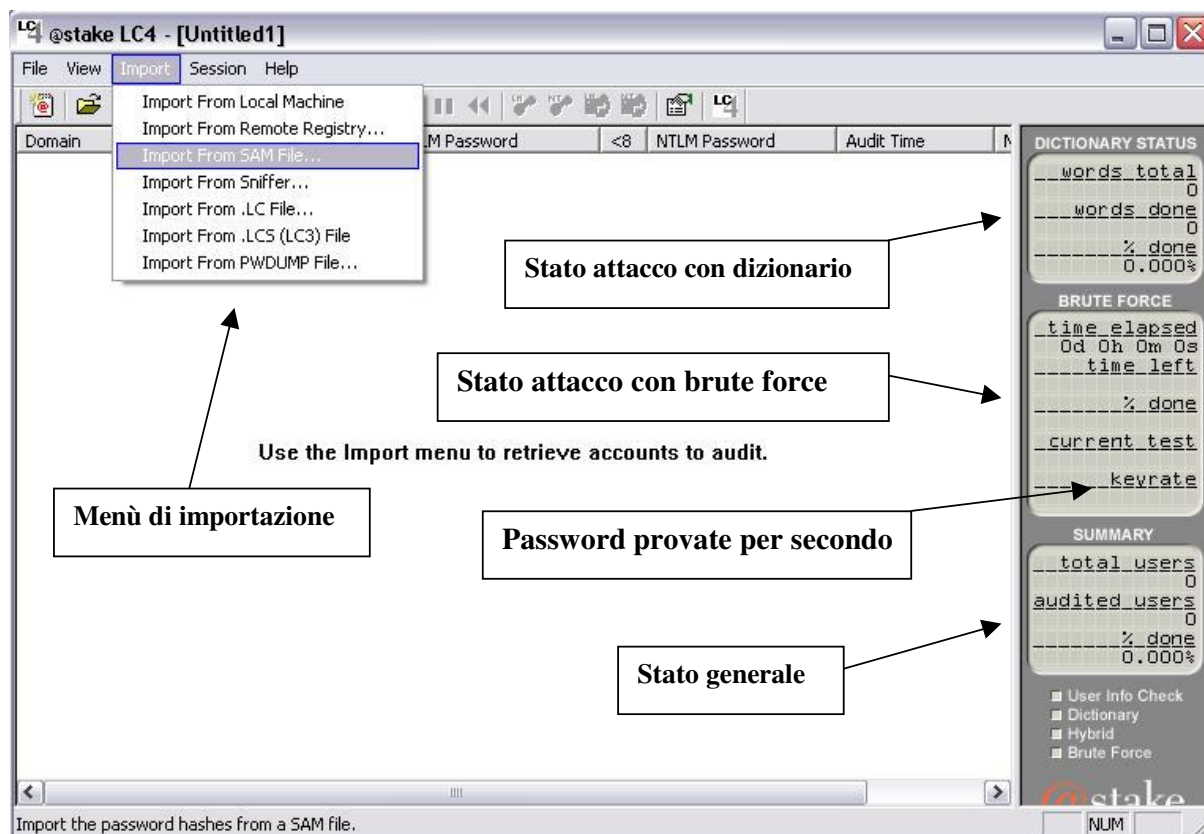
Per decriptare il file SAM ci serviremo di LC4, un programma creato da un gruppo di Hacker che di professione testano sistemi e forniscono soluzioni in caso di smarrimento di dati, essi lavorano per la @stake.

Lanciamo LC4 e chiudiamo la schermata di guida o wizard, dal menu *File* selezioniamo *New* e creiamo un nuovo progetto.

Ora dal menu *Import* selezioniamo *Import*

*From SAM File...*, LC4 vi chiederà la posizione del file SAM (dove l'avevate salvato) e lo caricherà.

Nota: Oltre alla voce di caricamento da file SAM esistono molteplici modi di ricerca password che verranno trattati nell'appendice, ma il nostro è senz'altro il modo migliore se si parte con pochi permessi e con un antivirus sulla macchina locale.



Il programma vi mostrerà ora gli utenti contenuti nel file e potrete effettuare 2 tipi di attacchi: con dizionario o brute force. Il primo consiste nell'avere a disposizione

un file di testo contenete tante parole che verranno provate come password, LC4 dispone d'un dizionario suo ma personalizzabile; i vantaggi di questo attacco stanno nella velocità d'esecuzione e nel fatto che vengono provate parole sensate e quindi provabili parole chiave.

Il brute force che è l'attacco per eccellenza significa provare tutte le possibili combinazioni di lettere fino a trovare la parola chiave, ovviamente è necessario fissare quanti caratteri e quali, numeri, lettere, ecc. Il problema di questo attacco e il tempo d'esecuzione che aumenta esponenzialmente all'aumento delle lettere, in genere è necessaria un'ottima cpu per ottenere risultati accettabili.

Facendo click sul pulsante *Play* rappresentato da una freccia verde, verrà avviato prima il metodo con dizionario, poi il metodo pseudo-dizionario (una via di mezzo) e infine il brute force.

Ovviamente tutti i parametri sono personalizzabili nelle opzioni

Non rimane che attendere il risultato e la tanto meritata password, potrete vedere lo stato d'avanzamento dell'operazione dal menu a destra.

### Appendice 1: Metodi alternativi per l'estrazione proposti da LC4

Oltre al metodo d'estrazione da altro sistema operativo LC4 mette a disposizione altri strumenti a seconda dei vostri permessi nel sistema.

- From Local Machine : Ottiene il file criptato dalla macchina locale, in genere non funziona su 2000 e Xp per la protezione di sistema.
- From Remote Registry: I dati criptati relativi alla password vengono estratti dal registro d'un computer remoto, i problemi sorgono sulla protezione del Pc bersaglio.
- From Sniffer: Si tenta di analizzare ed estrarre i dati che passano per controllo password relativo al registro.
- From LC o LCS: viene importato un progetto da un file di progetto esistente.
- From PWDUMP file: si utilizza un programma di estrazione dedicato che salva i risultati in un proprio formato; purtroppo su Win 2000 e Xp ha accesso negato.

### Appendice 2: Password su Windows NT

Su NT le cose sono più semplici grazie al fatto che esso comincia a diventare un pò vecchiotto. Infatti la dove 2000 e Xp negano l'accesso sembra che NT presenti qualche falla e programmi come PWDUMP riescono ad estrarre il file di password.

L'architettura di NT è simile ai suoi successori infatti sia il file system (NTFS) sia il file SAM sono i medesimi.

Quindi potete seguire le istruzioni per Windows 2000 oppure utilizzare un tool veramente ben fatto ossia LinNT, ovvero un mini kernel di Linux che parte da floppy all'avvio con il solo scopo di manipolare le password in NT.

Dovrete dare solo il percorso e il tipo d'operazione da fare.

LinNT è particolarmente utile in caso di perdita password perché permette di sostituirla a Windows spento.

Link su LinNT: [www.nttoolbox.com/public/tools/LinNT.zip](http://www.nttoolbox.com/public/tools/LinNT.zip)

#### Note Legali:

Declino ogni responsabilità a mio carico per un uso improprio di questa guida ai danni di altri sistemi o informazioni personali, essa vuole essere soltanto uno strumento d'informazione e/o di difesa.

Questa guida è sotto licenza DFL ossia è possibile modificarla a patto che le modifiche vengano spedite all'autore e non vengano diffuse con modifiche non autorizzate.

Copyright ALwarrior 2003 tutti i diritti riservati.

Web: <http://alwarrior.interfree.it/index.html>

Email: [alwarrior@hush.com](mailto:alwarrior@hush.com)