

Azzerare la password di Administrator

(Offline NT Password & Registry Editor, Bootdisk)

Augusto Scatolini (webmaster@comunecampagnano.it)

Ver. 1.0 Luglio 2010

tradotto liberamente da <http://home.eunet.no/~pnordahl/ntpasswd/>



Dischetto di boot per modificare il registro e le password nei sistemi NT

Nel dischetto (floppy) praticamente c'è un sistema Linux essenziale (minilinux) più l'utility chntpw

Dimenticato la password da amministratore? (NT, Win2K, WinXP)

- Questa è un'utility per settare o resettare la password di qualunque utente, modificando le password crittografate nel file di registro SAM
- Non c'è bisogno di conoscere la vecchia password per settarne una nuova.
- Funziona off-line, cioè, devi spegnere il computer e fare il boot da floppy. Il dischetto contiene un programma (chntpw) capace di accedere alle partizioni NTFS
- Il programma rileva e permette di sbloccare utenti bloccati o disabilitati

Premessa

NT custodisce le informazioni degli utenti incluse le password crittografate in un file chiamato SAM, che si trova generalmente in `\winnt\system32\config`. Questo file è parte del registro, in formato binario privato precedentemente della documentazione e difficilmente accessibile. A tutt'oggi, Microsoft non permette in alcun modo di cambiare le password se non si accede al computer con gli appropriati privilegi di amministratore, a meno che non si ripristinino i file del registro dal "rescuefloppy" che ovviamente non hai altrimenti non saresti qui a leggere questa pagina.

QUESTO SOFTWARE VIENE DISTRIBUITO SENZA ALCUNA GARANZIA. NON SI RISPONDE PER EVENTUALI DANNI CAUSATI DALL'USO O DALL'USO IMPROPRIO DI QUESTO SOFTWARE!

D'altra parte se non provi questo software devi necessariamente formattare il disco o cercare qualche prodotto commerciale! Auguri!

Questo è un software ancora in versione ALPHA ed è basato su metodi e strutture non documentate.

Sei stato avvertito!

Il floppy contiene un programma capace di modificare le password di molti sistemi. Il floppy supporta standard (dual) IDE controllers, e molti SCSI-controllers. Non necessita di hardware particolare, gira su 486 o superiori, con un minimo di 32MB ram. Hardware non supportato: MCA e EISA non supportato, i2o potrebbe non funzionare, USB keyboard potrebbe non funzionare. Rari IDE e SCSI raid-controllers potrebbe non funzionare.

Se usato su utenti che hanno file crittografati EFS e il sistema è XP o con recenti service pack su win2k, tutti i file crittografati di quell'utente saranno ILLEGIBILI! e non potranno più essere decrittati senza conoscere la vecchia password

Come si usa?

- **SUGGERIMENTO: premi return/enter per accettare le scelte di default in [parentesi quadre]**
- Spegni la macchina e inserisci il floppy.
- Lascia che la macchina esegua il boot dal floppy.
- Appaiono alcuni banner e messaggi, informazioni sull'hardware etc.
- Vengono listati i drivers SCSI (se presenti), alla domanda SCSI-controller drivers, puoi:
 1. rispondere 'y' per verificare tutti i driver "scsi".
 2. rispondere 'n' per bypassare la ricerca delle schede SCSI. Scegli questa opzione se hai solo IDE-disks.
 3. o al prompt digitare il nome del modulo linux del driver. Il prompt compare di nuovo fino a quando rispondi 'n', così tutti i driver possono essere caricati, se necessario.
- Poi compare la lista di tutte le partizioni di tutti i dischi.
- Al prompt seleziona una partizione, viene selezionata di default la prima partizione NTFS bootable o la prima FAT bootable se non c'è quella NTFS.
- La partizione viene montata e ne viene specificato il tipo (NTFS o FAT).
- Poi devi sezionare il percorso della directory del registro. Generalmente è 'winnt/system32/config'.
- Poi seleziona il file da copiare nell'area temporanea del ramdisk. Per modificare le password 'sam' è il default. Per info on syskey 'system' è il default. Per syskey info aggiuntive in Win2K 'security' è il default.
- Ora c'è tutto il necessario per far girare l'utility '**chntp**' nella directory /tmp. Il menu principale ti permette di :
 1. Modificare le password.
 2. Controllare e disattivare syskey.
 3. Modificare il registro
- Modificare le password:
 1. Tutti gli utenti vengono listati.
 2. Scegli l'utente da modificare. Il prompt continua fino a quando si digita '!'. Per rivedere la lista digita '!'
 3. Se l'utente è bloccato o disabilitato puoi sbloccarlo o riabilitarlo.
 4. Digitare un singolo * quale password per annullare la password. Questo metodo sembra funzionare meglio rispetto a quello di settarne una nuova!
 5. Digita una nuova password, massimo 14 caratteri.
 6. Poi conferma le modifiche. (la scrittura vera sul disco avviene solo quando esci dal

programma)

- Uscire e confermare le modifiche:
 1. Se l'utility 'chntpw' ha successo, appare un prompt per confermare le modifiche del NT disk/filesystem. Solo 'y' è accettato per confermare i cambiamenti.
 2. Alla fine appare il prompt della shell "# ". A questo punto puoi resettare la macchina con Control-Alt-Del.

Download

Come usare il floppy

Il file [bd030426.zip](http://www.ol-service.com/sikurezza/offline_password_editor_bootdisk/bd030426.zip) scaricabile da

http://www.ol-service.com/sikurezza/offline_password_editor_bootdisk/bd030426.zip

contiene l'immagine del file [bd030426.bin](http://www.ol-service.com/sikurezza/offline_password_editor_bootdisk/bd030426.bin) che è la rappresentazione block-to-block del floppy. Il file .bin **non può essere copiato semplicemente su un floppy**. Deve essere usato un tool speciale capace di scrivere block by block. Per Dos, win95/98 & NT, puoi usare [rawrite2.exe](http://www.ol-service.com/sikurezza/offline_password_editor_bootdisk/rawrite2.exe) scaricabile da

http://www.ol-service.com/sikurezza/offline_password_editor_bootdisk/rawrite2.exe

o altri scrittori di immagini:

Sintassi per rawrite2

```
rawrite2 -f bd030426.bin -d A:
```

da unix, GNU/Linux:

```
dd if=bd030426.bin of=/dev/fd0 bs=18k
```

Io l'ho provato ed ha funzionato, **fatemi sapere**

~~~~~  
~~~~~

per coloro i quali avessero problemi con la creazione del floppy o non avessero il lettore di floppy, l'utility chntpw è presente nei seguenti GNU/Linux Live CD

IRItaly Live CD

<http://iritaly.crema.unimi.it/downloads.asp>

KANOTIX BUG HUNTER 9

<http://kanotix.com/info/index.php?lang=it>

PHLAK 0.2-1

<http://www.phlak.org/modules/mydownloads/>

Feather Linux

<http://featherlinux.berlios.de/download.htm>

Altro sistema (OPHCRACK)

<http://ophcrack.sourceforge.net/>

Un altro sistema ancora più semplice è utilizzare il live-cd OPHCRACK

Ophcrack è tool gratuito per craccare le password dei sistemi Windows basato su **rainbow tables**.

A rainbow table is a lookup table offering a time-memory tradeoff used in recovering the plaintext password from a password hash generated by a hash function, often a cryptographic hash function

http://en.wikipedia.org/wiki/Rainbow_table

E' un'implementazione molto efficiente delle "rainbow tables" fatta dagli inventori di questo metodo. Usa un'interfaccia grafica e "gira" su piattaforme multiple.

Si può scaricare un eseguibile installabile per Windows o un sorgente compilabile per i sistemi GNU/Linux. Ovviamente per poter installare il programma si deve essere Administrator o Root.

Oppure si può scaricare un'immagine ISO da masterizzare.

Praticamente, dopo aver avviato il programma o aver fatto il boot da cd-rom non si deve fare altro che aspettare che il programma scopra le password (tutte le password)

Prevenzione

Per prevenire l'uso di questi sistemi (chntpw e/o ophcrack) si potrebbe pensare di eliminare da computer floppy e cd-rom.

Ma è sempre possibile rimontarli.

Allora si potrebbe modificare la sequenza di boot del bios, settando come primo dispositivo di boot l'hard disk. In questo modo la macchina non farebbe il boot né da floppy né da cd-rom.

Ma è sempre possibile per chiunque ripristinare o modificare la sequenza di boot.

Allora si potrebbe proteggere la modifica del BIOS proteggendolo con una password.

Ma un'utente un po' più "geek" o "nerd" potrebbe cortocircuitare un ponticello e azzerare la password del BIOS

Allora non rimane che saldare (con la fiamma ossidrica) il case del computer per prevenire manomissioni.

Ma è sempre possibile scardinare il case. E allora?

L'unica e ultima forma di protezione consiste nel crittografare (con una bella chiave, meglio se asimmetrica) i file che si intendono proteggere.

FINE

Questo documento è rilasciato con licenza Copyleft
(tutti i rovesci sono riservati)
altre miniguide

<http://www.comunecampagnano.it/gnu/miniguide.htm>

oppure direttamente su

<http://miniguide.tk>