

Avviare Windows 7 senza conoscere la password

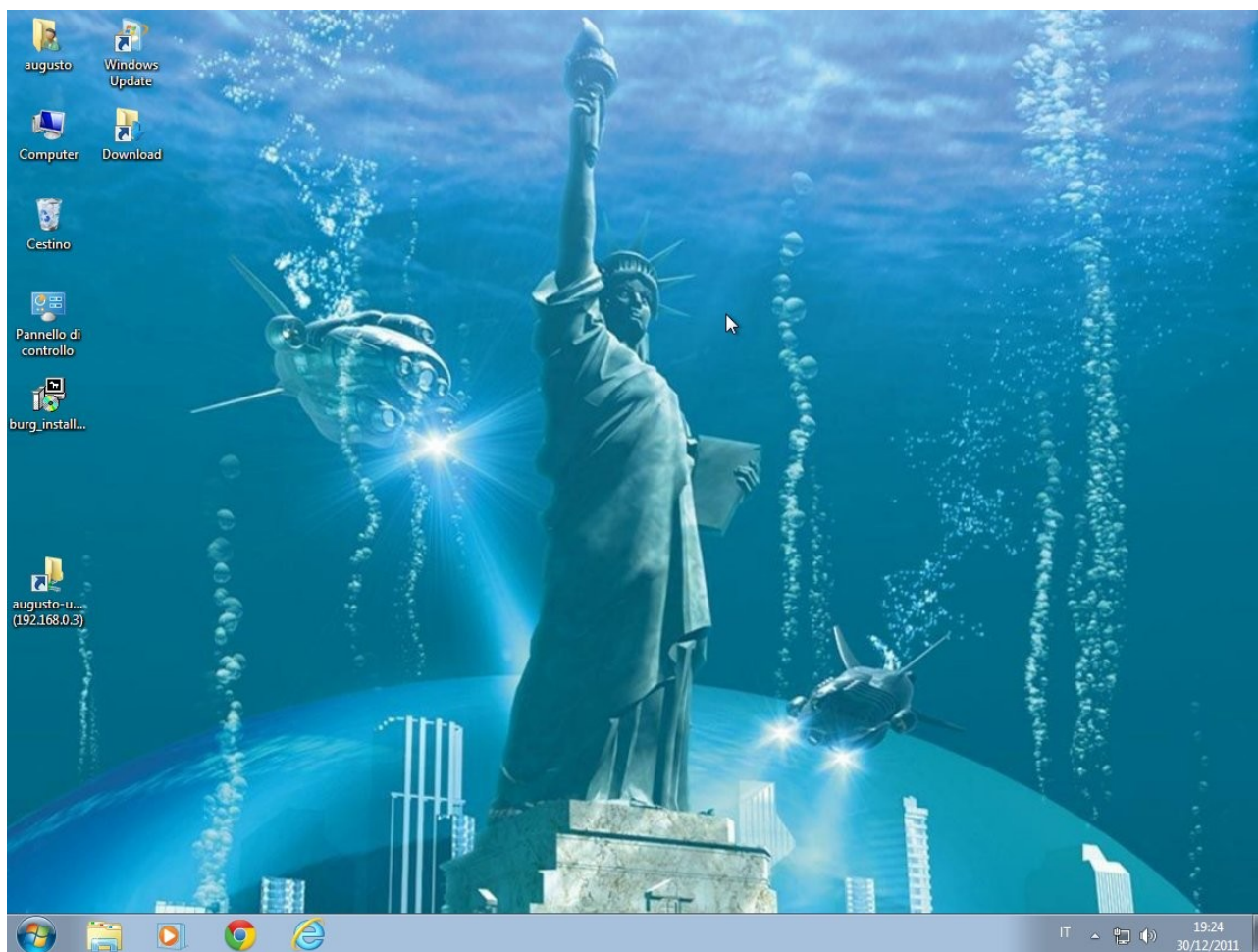
(basta avere un CD Live di GNU/Linux)

(guida valida anche per Windows XP)

Augusto Scatolini (webmaster@comunecampagnano.it) (a.scatolini@linux4campagnano.net)

Miniguia n. 155

Ver. 1.0 Dicembre 2011



Supponiamo di aver dimenticato la nostra password di Windows 7 o di Windows XP.

Possiamo sempre recuperare i dati (i file) con una distribuzione Live di GNU/Linux che è capace di leggere il file system NTFS e copiarceli su un disco esterno o di rete.

Possiamo craccarci la password con un Live CD come **Ophcrack** o con **KonBoot** ma se questi sistemi non dovessero risolvere il problema possiamo semplicemente azzerare la nostra password con il comando “**control userpasswords2**”.

Il problema è come avviare una finestra DOS per dare tale comando in fase di Login?

Questa che segue è una dimostrazione “passo passo”.

Siamo in fase di Login.

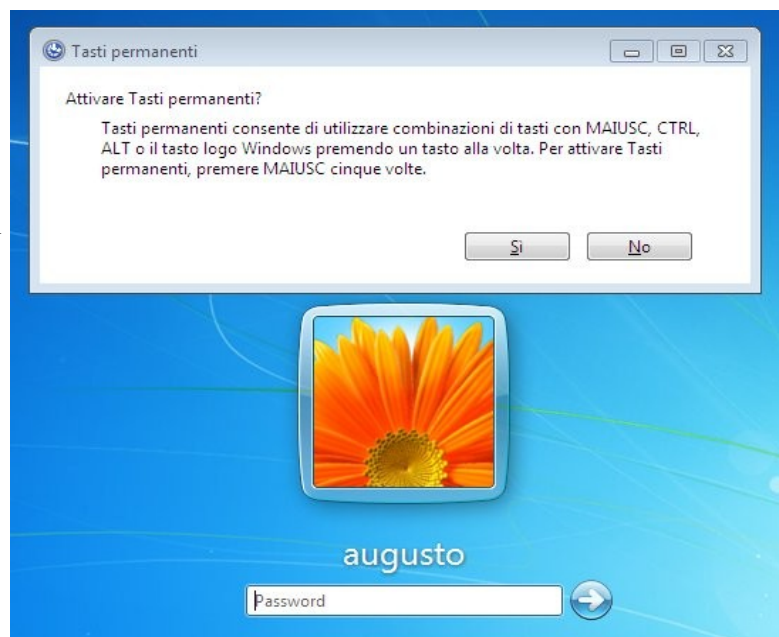


Proviamo una password (quella che ci ricordiamo) ma niente da fare.

Riceviamo un errore.



Ora, se in fase di Login, premiamo 5 volte di seguito il tasto sinistro **Shift**, si avvia il programma **sethc.exe** che serve a gestire i tasti permanenti.

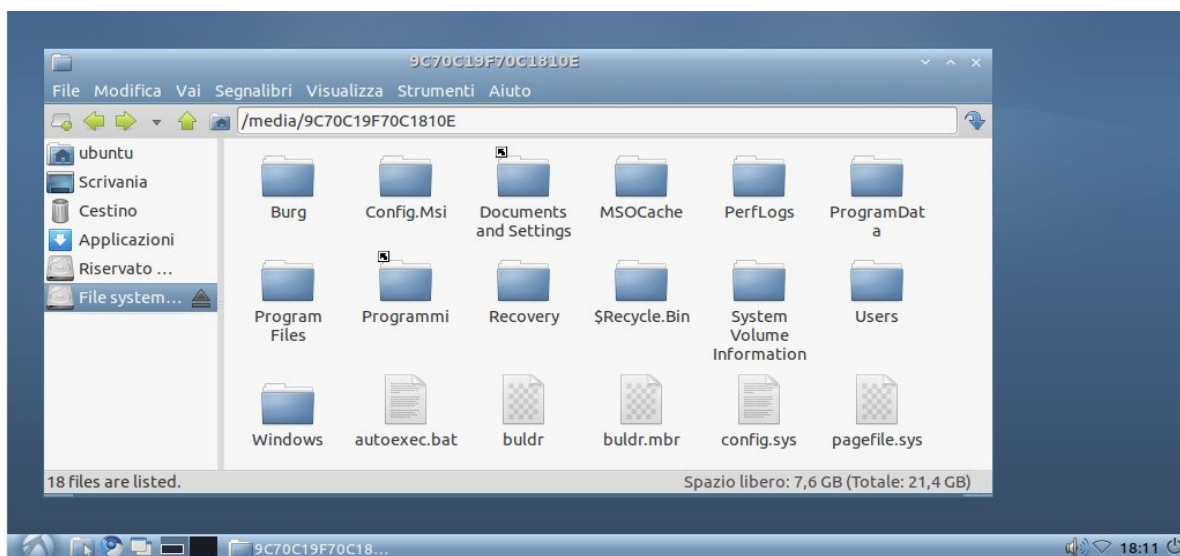


Ma allora la soluzione è semplice, bisogna solo trovare il modo di rinominare il file **sethc.exe** in qualche altro modo e copiare il file **cmd.exe** in **sethc.exe**

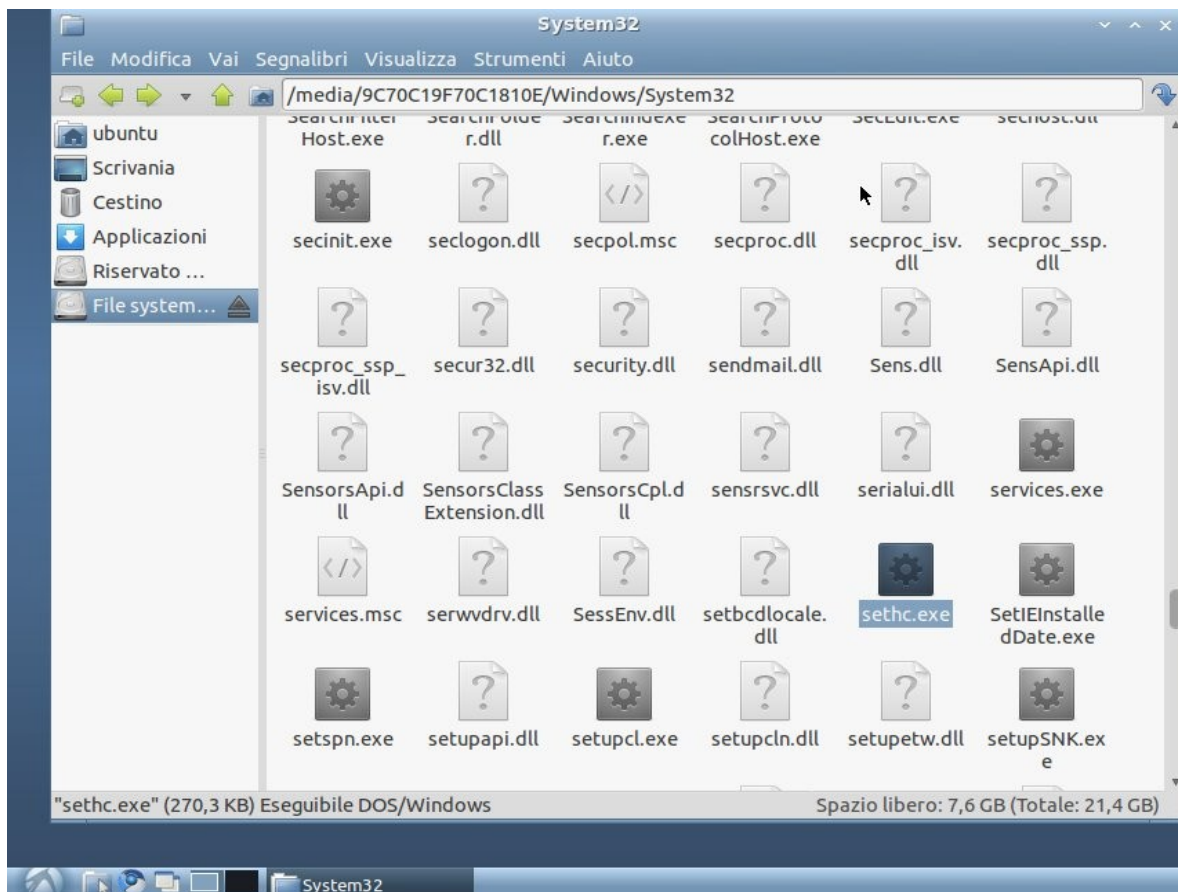
In questo modo, quando premeremo 5 volte il tasto sinistro Shift, invece del programma **sethc.exe** avvieremo il programma **cmd.exe** ovvero una finestra DOS

Quindi avviamo il PC con una distribuzione Live come Ubuntu con Desktop Environment LXDE (ovvero Lubuntu).

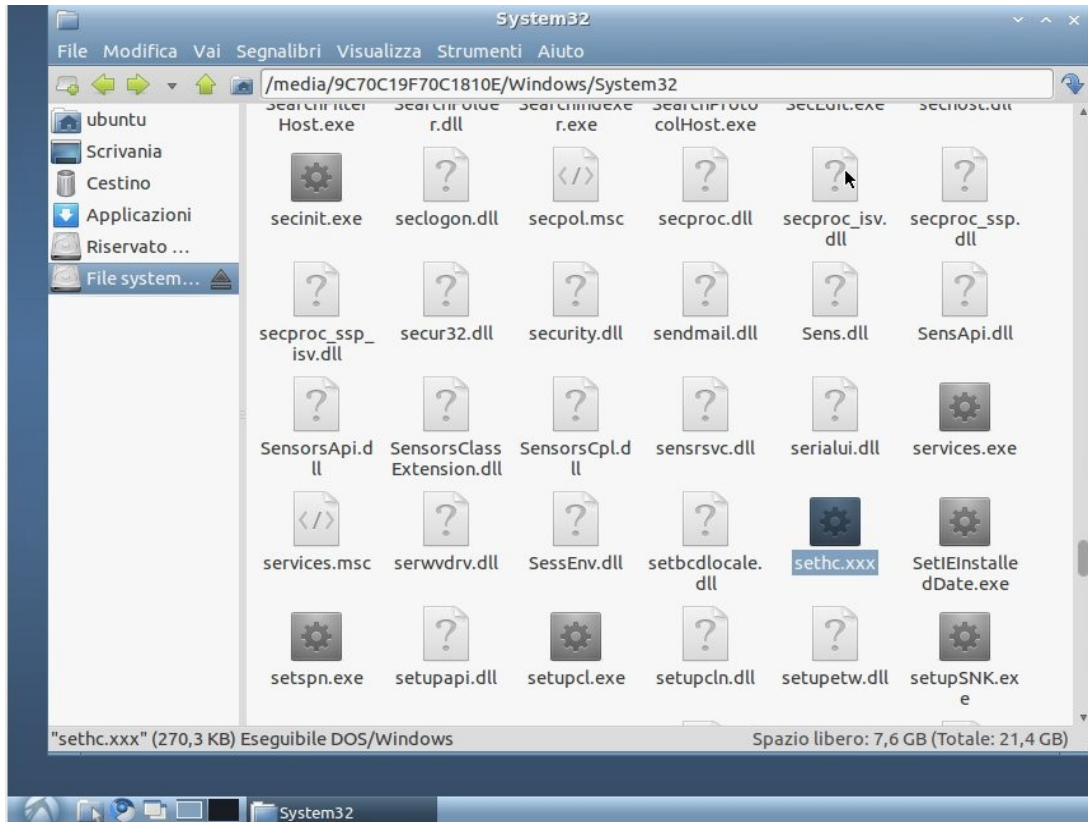
In questo modo possiamo accedere tranquillamente alla partizione Windows



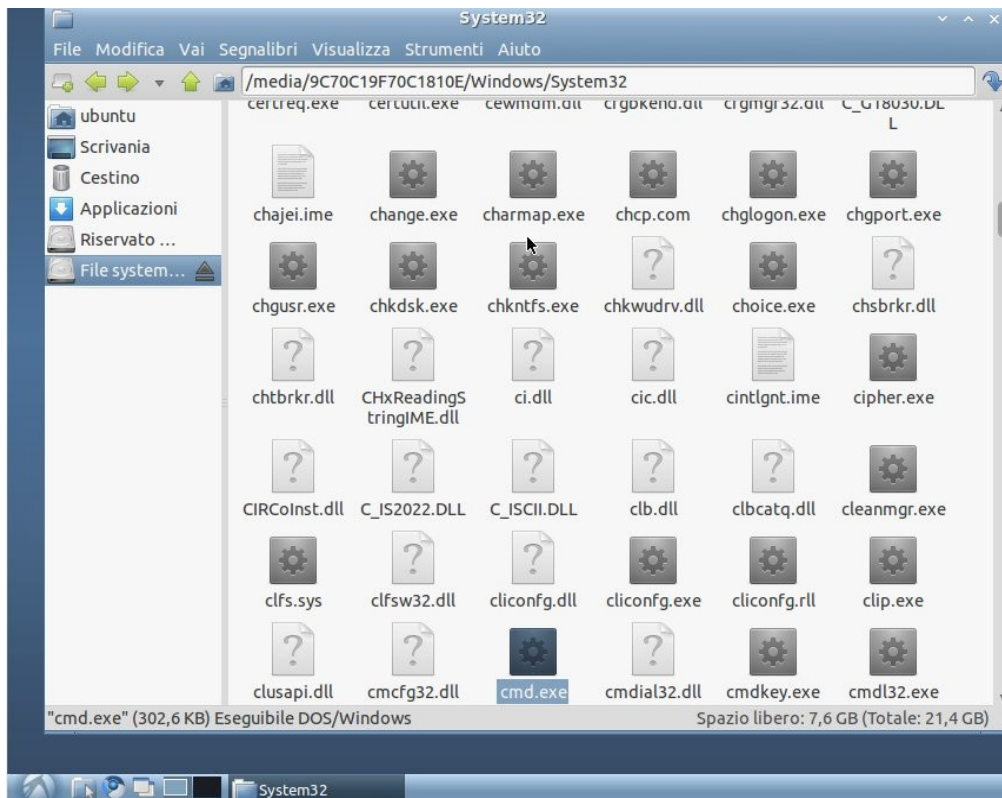
Navighiamo nel File System fino a C:\windows\system32, cerchiamo il file sethc.exe



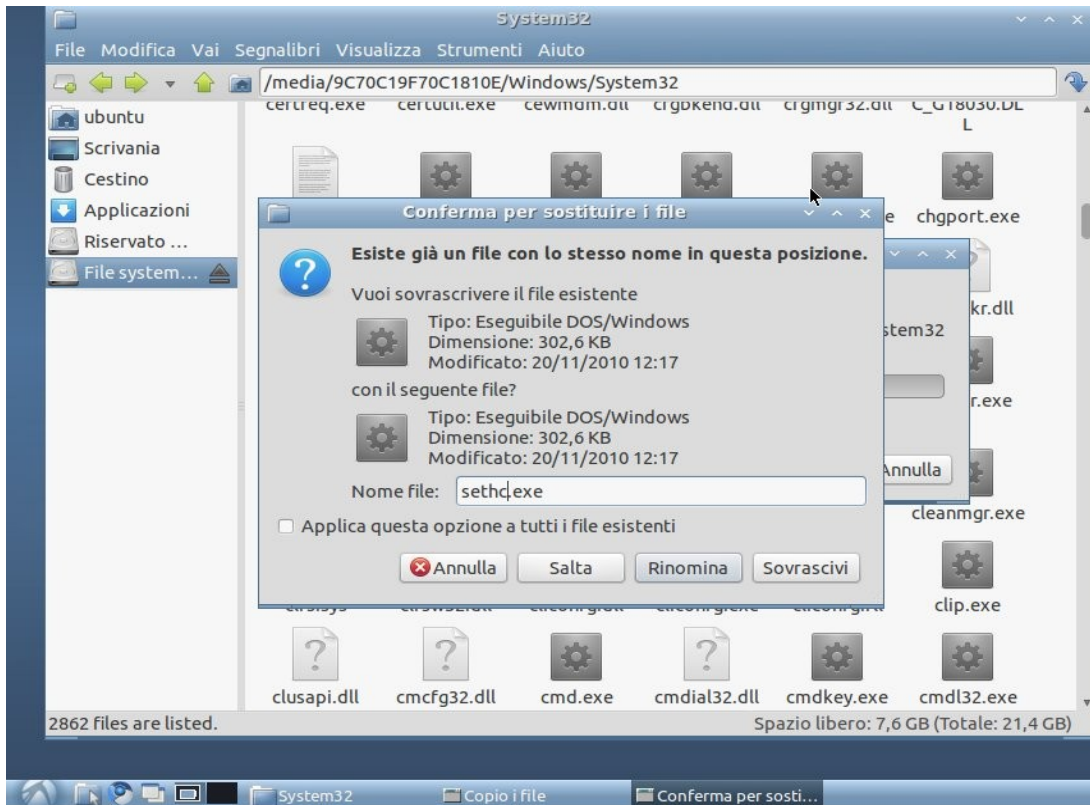
e rinominiamo il file come sethc.xxx



copiamo il file cmd.exe

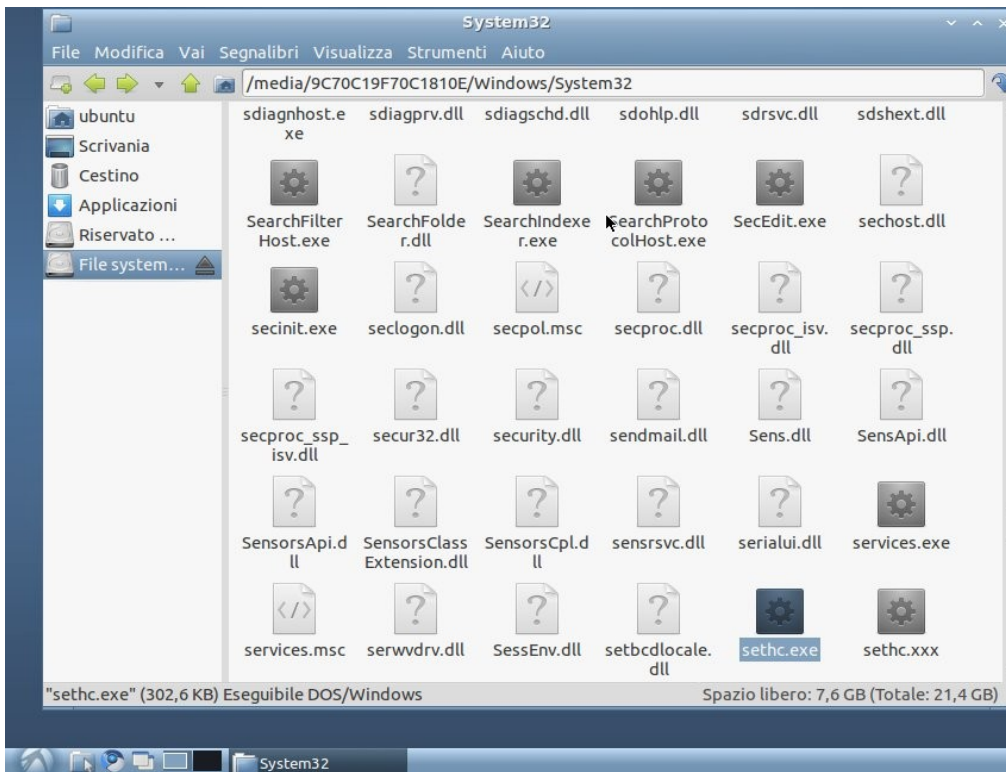


e lo rinominiamo sethc.exe

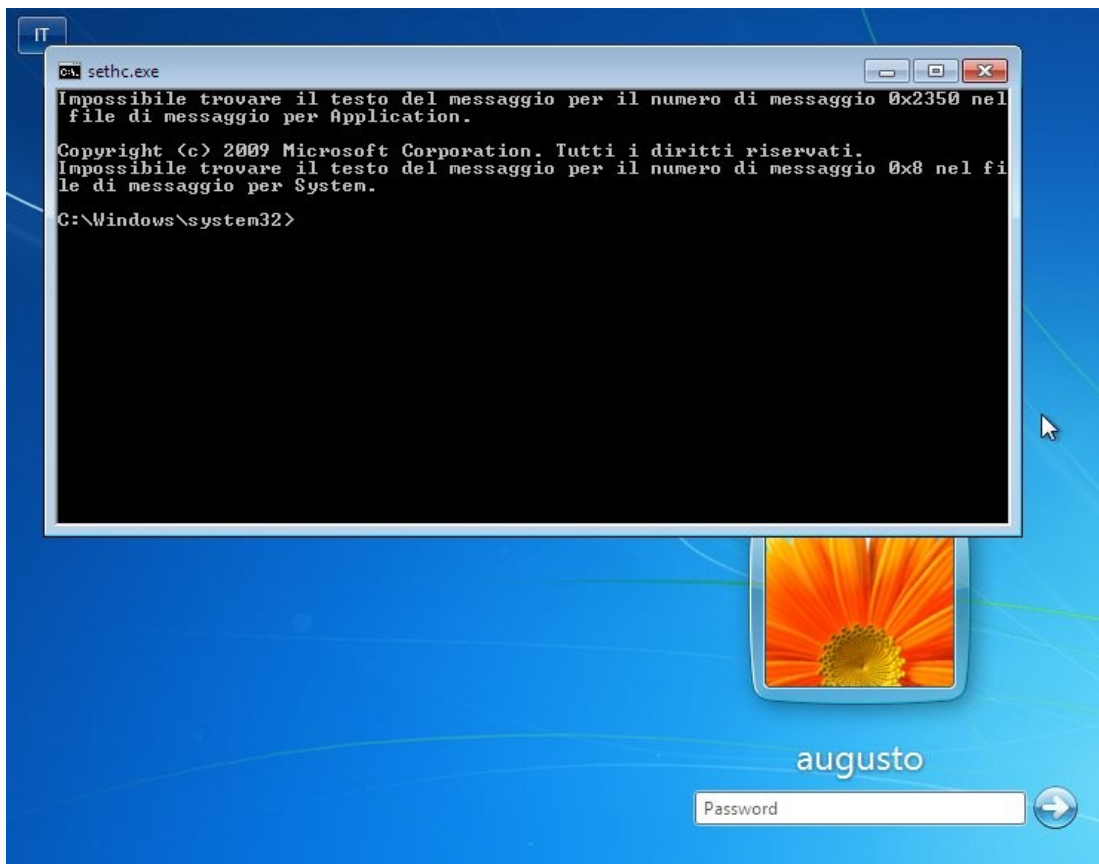


in questo modo avremo il vecchio sethc.exe rinominato ---> sethc.xxx

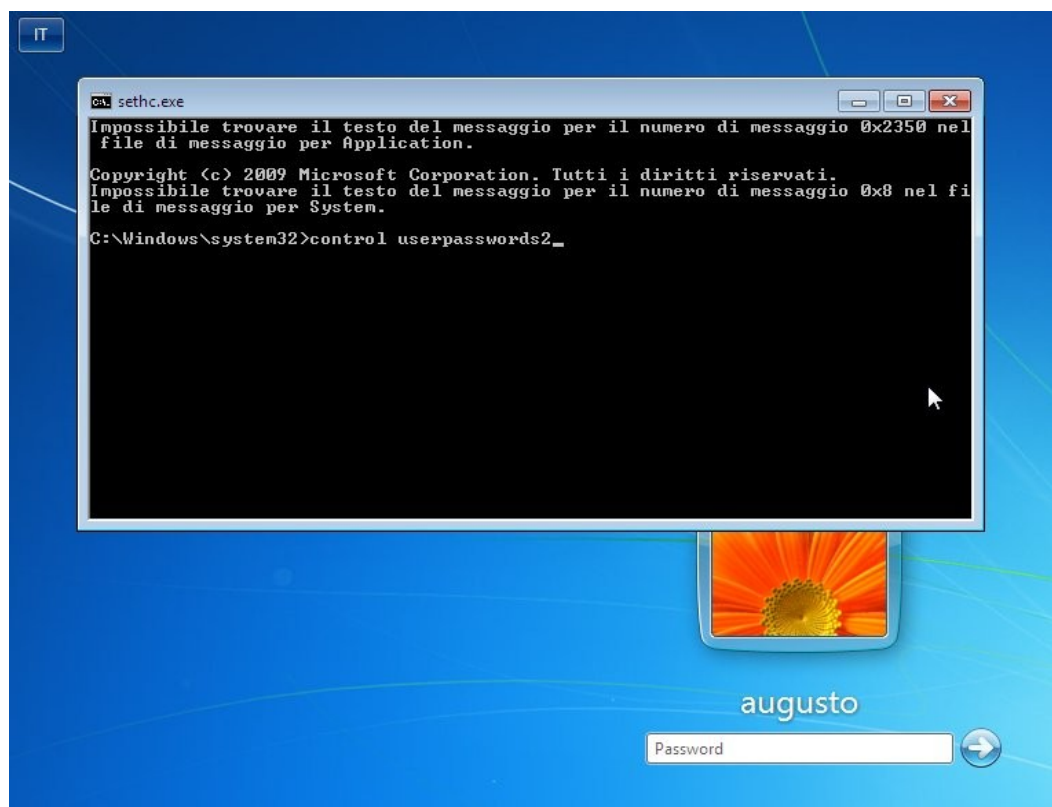
e il nuovo sethc.exe che altro non è che una copia di cmd.exe



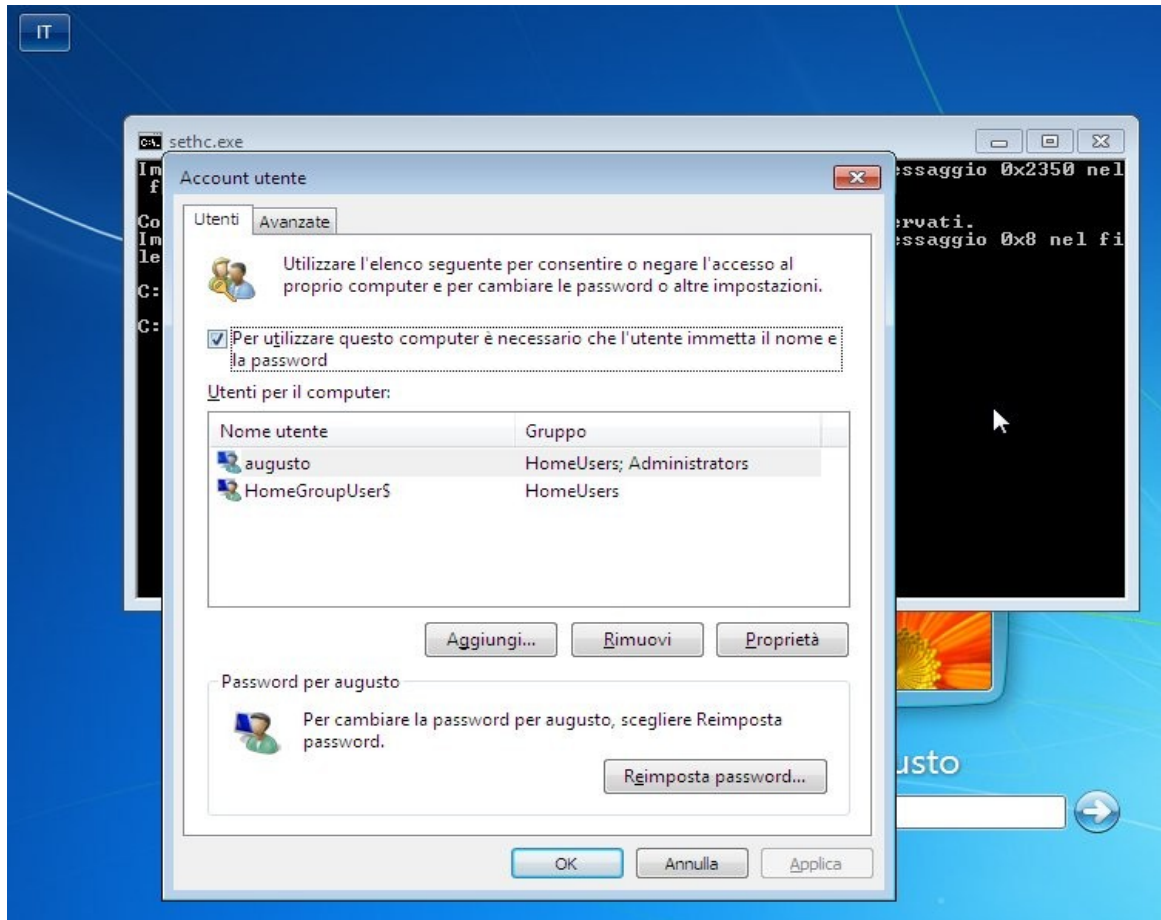
Ora, è sufficiente chiudere tutto, riavviare Windows 7 (o Windows XP) e quando siamo in fase di Login premere 5 volte il tasto sinistro Shift per avere la nostra utilissima finestra DOS



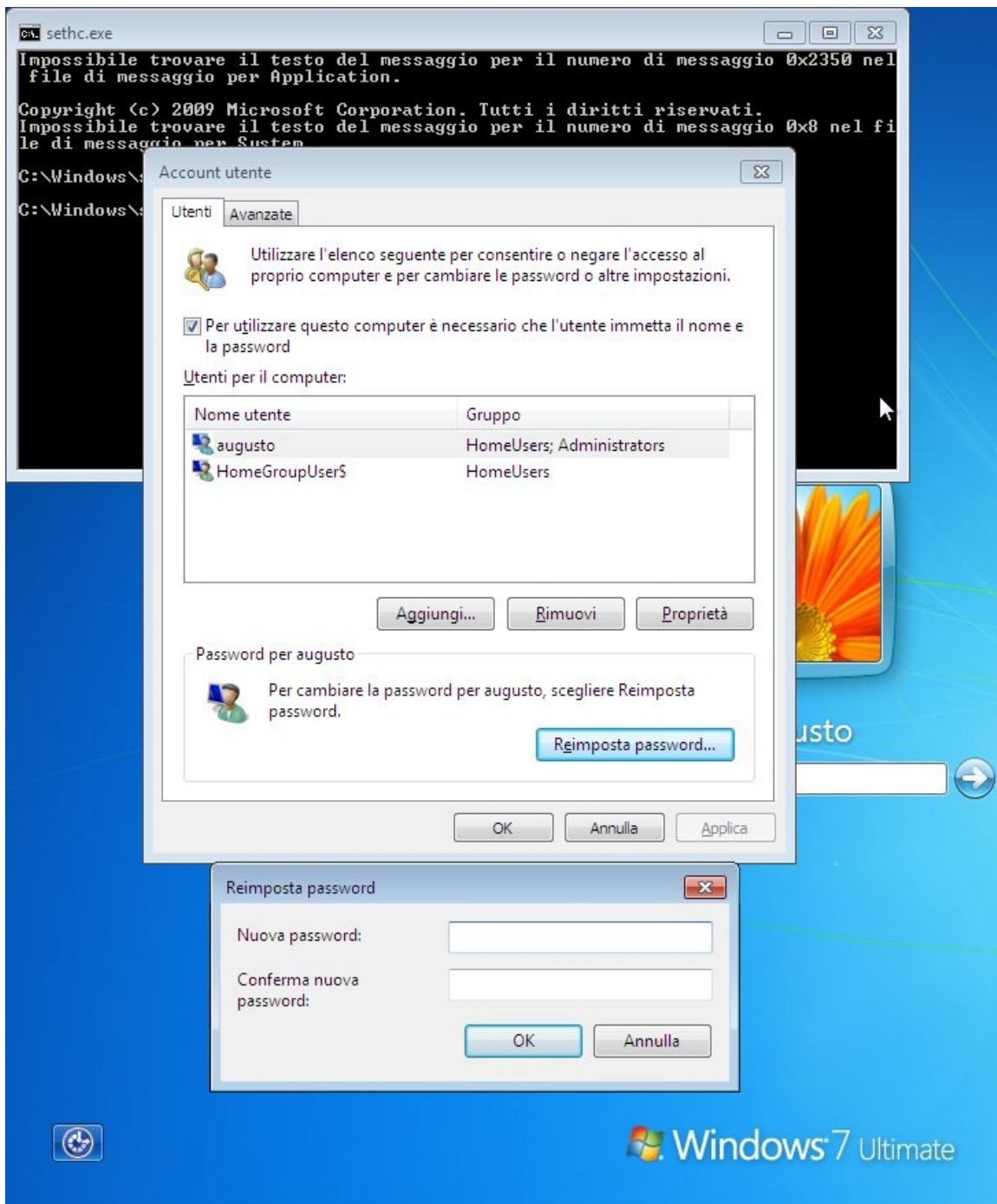
dove possiamo impartire il comando “control userpasswords2”



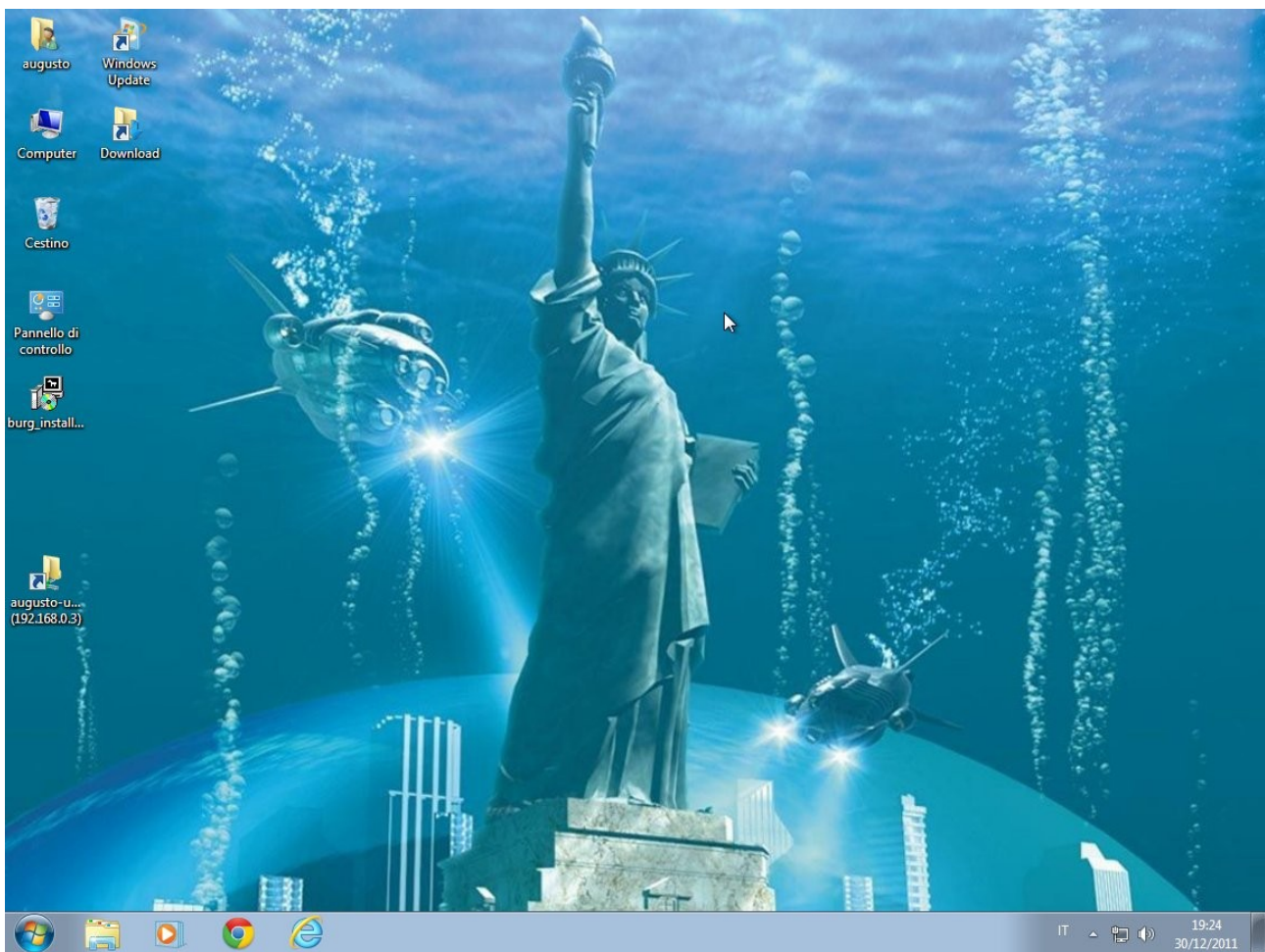
si aprirà il pannello della gestione degli utenti



dove potremo selezionare il nostro account (anche da amministratore) e azzerare la password



Una volta azzerata la password sarà sufficiente lasciare il campo password del Login vuoto e premere invio



FINE

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

altre miniguide su

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

oppure direttamente su <http://miniguide.tk>

sito consigliato: <http://www.linux4campagnano.net>

blog consigliato: <http://campagnanorap.blogspot.com>